



eFutura

Association pour la Transition Numérique

NAVIGUER DANS LA CONFORMITÉ IA

**UN ENJEU STRATÉGIQUE
POUR LES DIRIGEANTS**

www.efutura.fr

PRESENTATION D'eFUTURA	1
CONTRIBUTEURS	2
PREFACE de Cédric Vilani	3
OBJECTIF	5
PARTIE 1 - COMPRENDRE L'I.A.	6
1- Qu'est-ce que l'I.A. ?	6
2- Les différentes formes d'I.A. et les spécificités de l'I.A. générative	7
3- Quelles technologies pour quels usages ?	8
4- Pour une intégration lucide et responsable	10
PARTIE 2 - LA RÉGLEMENTATION DE L'I.A.	11
1- Comment comprendre l'environnement réglementaire européen ?	11
2- Fournisseur, utilisateur, fournisseur du modèle de base, développeur : suis-je concerné par la réglementation européenne ?	13
3- Quelles sanctions prévues ?	15
4- Les enjeux de la gestion des droits d'auteur en droit français	16
5- En quoi la conformité I.A. est-elle un enjeu stratégique ?	18
PARTIE 3 - ENJEUX ET RECOMMANDATIONS	20
1- Usage responsable et éthique	20
2- Cyber sécurité et confidentialité	22
3- Souveraineté	23
4- Développement durable	24
5- Recommandations principales	25
PARTIE 4 - RÔLES ET RESPONSABILITÉS	27
1- Pour une gouvernance efficace	27
2- Quelles actions à mettre en place ?	28
3- Importance de la formation	30
PARTIE 5 - MEMENTO PRATIQUE À L'USAGE DES ACTEURS DU NUMÉRIQUE	31
Obligations spécifiques des utilisateurs de systèmes d'i.a. / utilisateurs	32
Obligations spécifiques des fournisseurs de systèmes d'i.a. / fournisseurs	33
LES NOUVEAUX DÉFIS JURIDIQUES POSES PAR L'IA AGENTIQUE	34
1 Qui décide ? — La question de la responsabilité et de l'imputabilité	34
2 Qui engage l'entreprise ? — La question de la sécurité contractuelle	34
3 Qui contrôle et qui prouve ? — La question de la gouvernance, de la supervision et de la preuve	34
4 Qu'est-ce que l'agent met en danger autour de lui ? — La question des risques informationnels et systémiques .	35
CONCLUSION - Un livre blanc qui résistera aux évolutions technologiques	36
ANNEXE 1 - Glossaire	38
ANNEXE 2 - Architectures et typologies	39
Les grandes familles d'I.A.	39
Autres typologies utiles	39
Autres architectures d'I.A. à connaître	40
ANNEXE 3 - Cartographie des usages professionnels et fiches métiers	42
FICHE MÉTIER 1 : Recrutement automatisé	42
FICHE MÉTIER 2 : Diagnostic médical assisté par i.a.	42
FICHE MÉTIER 3 : Recommandations personnalisées (e-commerce)	43
FICHE MÉTIER 4 : Tutorat intelligent (éducation)	43
FICHE MÉTIER 5 : Scoring de crédit automatisé (banque)	44
FICHE MÉTIER 6 : Sécurité et détection de fraude	44
ANNEXE 4 - Obligations applicables aux systèmes à haut risque/ modérés / limités	45
ANNEXE 5 - Exemples d'applications de bonnes pratiques dans le domaine du numérique pour la gestion des documents et des données	47



Présentation eFutura

eFutura est une association professionnelle indépendante, créée en 2015 qui accompagne et regroupe les acteurs du numérique autour du document et de la data.

Elle s'articule autour de trois piliers :

- Contribution aux normes françaises, européennes et internationales : Archivage électronique, Cybersécurité, Facture électronique, Gestion de Documents, Gouvernance de l'information, Numérisation, Intelligence artificielle ...
- Production de livrables et organisation d'événements à destination des Dirigeants / COMEX et des adhérents
- Animation d'un think tank dédié aux impacts sociétaux du numérique.

eFutura rassemble un écosystème riche et complémentaire :

- Experts, éditeurs, consultants, hébergeurs,
- Utilisateurs et associations professionnelles,
- Institutions, universités, Enseignement et de la recherche,
- Partenaires engagés et complémentaires.

L'IA est un axe fondamental, facteur d'innovation et de croissance mais également facteur de risque important notamment Cyber.

Ce livret a été réalisé par le groupe de travail « IA Génératives » composé de membres divers : avocat, éditeurs de logiciels, consultants, experts, partenaires, ...

Il est à destination des directions et des COMEX qui ont besoin de mieux comprendre les enjeux des régulations européennes, des risques, des sanctions ... auxquelles leur organisation doit faire face.

Ce livret et d'autres publications à venir de l'association eFutura ont pour objectif de vous accompagner dans ces changements profonds. Nous remercions les personnes suivantes, adhérentes d'eFutura, pour le temps qu'elles ont consacré à la réalisation de ce livret.



CONTRIBUTEURS

Ce Groupe de Travail est animé par :

Laetitia AVIA du Cabinet AVIA

Olivier de BOISBOISSEL de P.A.G.E

Nous remercions les personnes suivantes, adhérentes d'eFutura, pour le temps qu'elles ont consacré à la réalisation de ce livret.



CHARON Benoît
ACTIV BOLD



BILLAUD Rédoine
ALNAFIDA



AVIA Lætitia
Cabinet AVIA



HILAIRE Sandrine
BESTWAYS CONSULTING



D'ARPA Gilles
EVERTEAM Software



Général WATIN-AUGOUARD Marc
INCYBER Forum Europe



la HAUSSE de LALOUVIERE Jean-Pierre
INTALIO



RAULIN Antoine
OUROUK



de BOISBOISSEL Olivier
P.A.G.E



BONNIN Olivier
TREVYS ADVISORY



Dr DOSSANTOS UZARALDE Pierre-Jacques
XPERIA



Préface de Cédric VILLANI



« Intelligence artificielle : pas vraiment une science, bien plus qu'une technique. Elle n'a pas encore réussi à dégager les grands principes qui la sous-tendent, mais déjà elle bouleverse toutes les activités, des arts aux sciences en passant par l'économie, les entreprises, les sociétés.

Une révolution ? Peut-être. Une diversion de l'essentiel ? Certainement.
Un chamboulement incontournable ? Sans aucun doute.

Mais rarement chamboulement aura été accompagné d'un si grand flou. En 2017, quand je travaillais au rapport parlementaire qui allait initier la première stratégie française d'intelligence artificielle, je me heurtai tout de suite à un écueil : quelle est, au juste, la définition de l'IA ? Ma culture mathématique assoiffée de précision se cognait contre le mur impressionniste d'un sujet mouvant et multiforme. Heureusement que nous n'avons pas attendu d'avoir la réponse pour avancer dans le rapport !

Cela fera bientôt une décennie, mais la question est toujours posée, et à coup sûr, jamais un sujet indéfinissable — excepté les questions religieuses — n'a suscité autant de débats, de règlements et de jeux politiques, de bluff à tous les niveaux. Et de vénération touchant parfois au culte messianique !

Même les experts y perdent leurs bases — systématiquement incapables d'anticiper les sauts technologiques majeurs, ils ont vu le sujet qu'ils croyaient connaître se fragmenter en une myriade de cas d'usage, règles empiriques et vagues de réorganisation, ou désorganisation.

Pour y trouver ses marques, il est indispensable d'aborder le sujet sous plusieurs angles, de mélanger les expertises, de ne pas sous-estimer le volet humain du changement. Un jour, le responsable d'un entrepôt de données de santé, au terme de son audition, a tout résumé avec des mots qui ne m'ont pas quitté. Pour mettre en place ce nouvel outil d'IA, expliquait-il, il avait fallu relever trois défis. Le premier, celui des sciences et de la technique; le second, celui de l'éthique et du droit ; le troisième, celui de l'organisation humaine et politique. On aurait pu croire que le premier était la clé, mais finalement les trois défis étaient de même difficulté ! (Et encore, il parlait à l'échelle d'une institution bien délimitée... À l'échelle des nations et des sociétés, l'expérience l'a montré cruellement, ces trois défis sont plutôt rangés par ordre croissant de difficulté !)





Au moins pour le second volet, celui qui touche aux règles, voici un petit guide diablement utile, pour vous accompagner pas à pas à travers la cathédrale juridique sortie de terre ces dernières années en matière d'IA. Les règles et l'esprit des règles, les cas d'usage pratique ne manquent pas pour illustrer le propos. Il faut de la patience et de la pédagogie pour tenter de rester à niveau, dans la jungle des techniques changeantes. Le chemin de bout en bout sera long et sinueux, depuis les concepts abstraits jusqu'aux recommandations pratiques.

Comment réglementer ce que l'on ne peut nommer ? Par les usages, par les risques, par la multiplicité des exemples. C'est bien la réponse apportée, après bien des débats, par le pouvoir législatif (classement par risques et usages, plutôt que par principe algorithmique), et c'est le chemin que doit refaire quiconque entend se repérer dans le droit. Joli défi, plein de chausse-trapes, mais aussi l'occasion de trouver votre point d'accès personnel dans le plus grand débat du moment.

Une fois les règles et obligations énoncées, restera le plus important : les recommandations pratiques qui vous permettront d'éviter les dégâts, les maladresses ou les AI (accidents industriels).

Demain les techniques seront encore bouleversées, la réglementation pas forcément — car sur le continent européen elle est déjà tellement en avance sur le reste du monde. Mais tout le travail que vous aurez accompli pour conseiller ou défendre les intérêts des entreprises et des particuliers, cela restera d'actualité, vous aura donné des clés et du savoir-faire. Le chapitre qui vient sera peut-être encore plus riche !



Cédric VILLANI

Mathématicien, ancien député

Rapporteur de « Donner un sens à l'Intelligence artificielle », 2018



OBJECTIF

Ce livret est conçu pour les dirigeants d'entreprises afin de leur donner des repères pour comprendre l'impact des réglementations récentes sur l'I.A. - notamment celle conçues par l'«A.I. Act » européen - et s'adapter aux exigences de cette évolution juridique ainsi que les recommandations pratiques pour mettre en oeuvre un projet IA au sein d'une organisation.

Il n'a donc pas pour objet de traiter de la conception de l'I.A. mais de son intégration conforme.

À ce titre, il ne s'adresse pas aux entreprises spécialisées dans les systèmes d'intelligence artificielle mais à celles qui sont amenées, dans leurs activités et de production ou de gestion, à faire appel à ces systèmes ou à concevoir des systèmes propres à leurs structures et qui s'interrogent sur le cadre juridique existant et sur les conséquences qui peuvent en découler.

Dans la mesure où L'I.A. est déjà une révolution sur le marché du travail en raison de sa capacité de plus en plus grande à prendre en charge dans les secteurs administratifs, commerciaux, industriels et scientifiques des entreprises certaines tâches intellectuelles dévolues précédemment à des opérateurs qualifiés, elle représente donc aujourd'hui un levier stratégique pour les entreprises en matière d'amélioration de la performance opérationnelle, de gain de temps, d'innovation dans les produits et les services et de meilleure exploitation des données clients.



Pour les dirigeants, les enjeux sont multiples - identifier les bons cas d'usage, accompagner le changement, sécuriser les données, maîtriser les risques liés à l'opacité des systèmes - et il leur appartient de se conformer aux dernières réglementations sur l'I.A. et d'être vigilants en la matière car leur responsabilité pourra être engagée en cas de manquement.

À ce titre, la connaissance des potentialités des outils d'I.A. mis en place par ces mêmes entreprises, ainsi que celle des règles juridiques et normatives qui encadrent leur utilisation, sont désormais fondamentales en matière de positionnement concurrentiel.



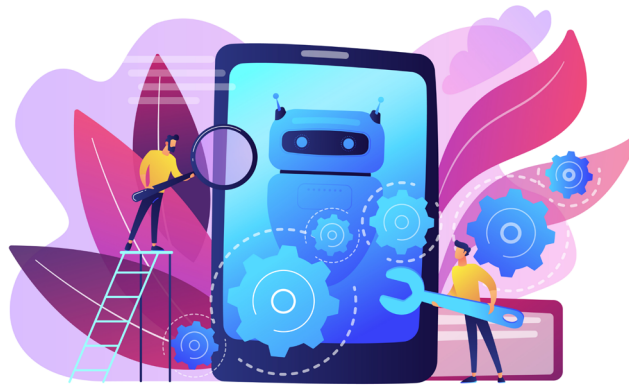
1 COMPRENDRE L'I.A.

1 Qu'est-ce que l'I.A.?

D'une façon communément admise, l'I.A. désigne, depuis les années 1950 avec les travaux pionniers d'Alan Turing et John McCarthy, un ensemble de méthodes et d'outils informatiques visant à reproduire certaines capacités humaines en matière d'apprentissage, de raisonnement et de planification pour optimiser un ensemble de tâches pour le compte d'un individu, d'un groupe de personnes, d'une entreprise ou d'une société.

Ces travaux ont donné lieu à diverses approches entre symbolisme (fondé sur des règles explicites) et connexionnisme (inspiré du fonctionnement neuronal), ainsi qu'à des débats sur les ambitions de l'I.A. dite faible (centrée sur des tâches spécifiques) ou forte (visant une forme de cognition générale).

Ils ont donc, de ce fait, structuré les premières décennies de recherche, opposant des visions formelles et biologiques de l'intelligence.



Mais si l'I.A. forte reste encore aujourd'hui un horizon théorique, les dernières avancées en la matière ont maintenant débouché sur de remarquables systèmes spécialisés, portés depuis les années 2000 par la montée en puissance du traitement des données, des capacités de calcul des ordinateurs et de l'utilisation systématique des algorithmes d'apprentissage automatique.

Visant la résolution de problèmes et l'aide à la décision, ces systèmes résultent sur le plan technique de la mise en commun de systèmes experts informatiques qui incluent le traitement automatique des langues, la planification automatique, la vision par ordinateur, l'apprentissage automatique et la simulation du fonctionnement du cerveau humain et utilisent des algorithmes extrayant des contenus d'information structurée et non structurée à partir de données, souvent massives, pour aider à la prise de décision ou accomplir des tâches spécifiques qui relevaient précédemment d'opérateurs humains qualifiés.

Notons par ailleurs que si l'I.A. repose sur une logique d'automatisation, elle ne se résume cependant pas à cette seule logique car elle peut désormais intégrer des systèmes capables d'optimiser leur comportement dans la durée au regard de leurs expériences d'utilisation.



2 Les différentes formes d'I.A. et les spécificités de l'I.A. generative

Dans une volonté d'accessibilité et de clarté pour les décideurs non spécialistes, nous concentrerons notre approche de l'Intelligence artificielle en rappelant les trois grandes familles fonctionnelles de l'I.A. Toutefois, afin d'éclairer les usages professionnels et les décisions d'intégration stratégique, on se reportera à l'annexe 2 qui présente les principales architectures sous-jacentes au développement spécifique des systèmes I.A. ; chacune apportant des capacités distinctes selon les types de données traitées, les objectifs métiers et les contraintes techniques.

Ces trois grandes familles sont celles de :

- **l'I.A. « symbolique »** relevant d'une approche fondatrice, basée sur des règles logiques explicites souvent codées en Prolog, qui permet de modéliser des raisonnements humains dans des domaines où la logique formelle est essentielle.
- **l'I.A. « statistique »** ou « machine learning » relevant d'une modélisation inductive, basée sur l'utilisation de la statistique et de la théorie des probabilités, qui permet aux machines d'identifier des modèles, de faire des prédictions et de déterminer les meilleures décisions.
- **l'I.A. « deep learning »**, dont la forme la plus connue est celle de l'I.A. « générative », relevant d'une création autonome, basée sur sa capacité à produire de nouveaux contenus (textes, images, sons, vidéos, codes...), qui ne se contente pas seulement d'analyser ou de classer mais qui synthétise, extrapole et invente en simulant des capacités créatives humaines.

Précisons qu'à la différence des deux premières qui se concentrent sur des tâches spécifiques - telles que la classification, la prédiction et la résolution de problèmes -, l'I.A. « générative » vise avant tout à produire des nouvelles données qui remplacent celles précédemment créées par des opérateurs qualifiés, que ce soit sous forme de création ou de production d'information, d'image et de son.

Elle représente donc pour les entreprises une avancée majeure dans le champ de l'intelligence artificielle permettant non seulement d'analyser des données existantes, mais aussi de créer de nouveaux contenus informationnels qui leur sont propres. Pour les décideurs, cette technologie spécifique ouvre notamment des perspectives concrètes d'innovation et de productivité dans les domaines de :

- La génération automatisée des contenus marketing,
- L'assistance à la rédaction de documents administratifs, juridiques et techniques,
- La conception rapide de prototypes numériques,
- La personnalisation à grande échelle des interactions clients.



D'une façon générale, notons que l'utilisation au sens large des outils d'I.A. de ces trois familles, en notamment ceux de l'I.A. « générative », va conditionner de plus en plus la manière dont les entreprises conçoivent leurs produits, communiquent et interagissent avec leurs marchés, tout en leur permettant de gagner en agilité et en réactivité dans un environnement économique en constante évolution

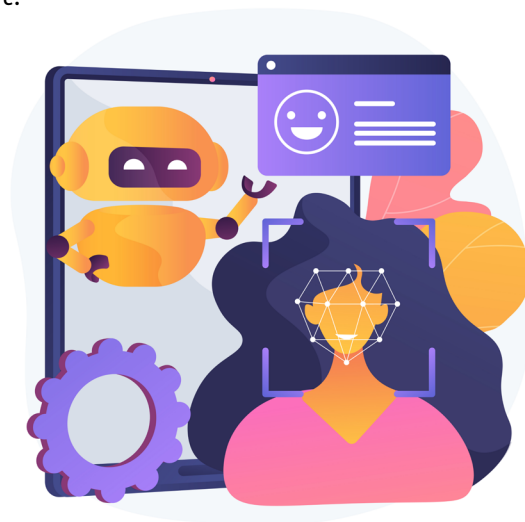
3 Quelles technologies pour quels usages ?

Quelles technologies ?

Les outils d'I.A. s'intègrent à chaque étape du cycle de vie de l'information dans l'entreprise, en s'appuyant notamment sur les technologies de traitement du langage.

Lors de la collecte des données, les outils de reconnaissance vocale et de transcription automatique permettent de transformer des conversations, des réunions ou des appels clients en données exploitables. Le traitement et l'extraction de ces informations sont facilités par les moteurs de recherche d'information et d'analyse sémantique, qui filtrent et structurent des volumes massifs de contenus textuels ou audio.

Vient ensuite la phase d'analyse, où les technologies de traduction automatique, de résumé automatique ou de classification thématique permettent de rendre les données accessibles et compréhensibles à différents niveaux de l'organisation et dans plusieurs langues. Dans la diffusion de l'information, les assistants virtuels et les chatbots conversationnels, basés sur les technologies de dialogue, facilitent la transmission d'informations ciblées, que ce soit auprès des collaborateurs ou des clients, via des interfaces naturelles et automatisées. Enfin, l'étape d'archivage bénéficie des solutions d'indexation linguistique, qui permettent de classer et retrouver rapidement les contenus archivés grâce à des métadonnées enrichies automatiquement.



Ces outils relèvent des principaux segments du marché des technologies de la langue : gestion du contenu, gestion des documents, traduction, e-business, ressources linguistiques, production et édition, interface vocale et multimodale, e-learning, moteurs de recherche intelligents. Ils permettent d'optimiser ainsi la reconnaissance vocale, la synthèse vocale, la traduction automatique, la reconnaissance et la compréhension du langage naturel, la génération automatique de contenu textuel et multimédia, les chatbots et les assistants conversationnels, l'analyse d'opinion et l'extraction d'informations, la gestion des contenus multilingues, et les technologies de recherche d'information.



Ensemble, ces technologies donnent aux entreprises le pouvoir d'optimiser la maîtrise et la valorisation de leurs flux d'information, tout au long de leur cycle de vie, pour renforcer leur efficacité opérationnelle, améliorer l'expérience client et soutenir l'innovation stratégique.

Quels usages ?

L'I.A. trouve déjà des applications concrètes dans de nombreux secteurs d'activité, offrant aux dirigeants des leviers opérationnels et stratégiques tangibles.

Ainsi, notamment :



Dans le secteur industriel, les systèmes permettent de rationaliser les plans et les méthodes de production et d'anticiper les défaillances d'équipements critiques, réduisant ainsi les arrêts de production et assurant ainsi la maintenance prédictive ;



Dans les secteurs de la Distribution et l'e-commerce, les systèmes optimisent la gestion des stocks, personnalisent les recommandations clients et automatisent la relation client grâce aux chatbots multilingues ;



Dans les secteurs des Assurances et de la Banque, les systèmes s'appuient sur des algorithmes de détection de fraude en temps réel et d'analyse automatisée des demandes de crédit ou de sinistres ;



Dans les départements comptables et financiers, les systèmes automatisent le traitement de la chaîne comptable ainsi que la production d'analyses et de rapports financiers incluant les recommandations stratégiques en matière d'investissement et de placement ;



Dans les départements juridiques, les systèmes automatisent la rédaction et l'analyse de contrats grâce au traitement du langage naturel, réduisant ainsi les délais et les risques d'erreur ;



Dans les départements de Ressources humaines, les systèmes facilitent le tri automatisé des candidatures, l'analyse des compétences, le suivi des carrières et la personnalisation des parcours de formation ;



Dans le domaine de la Communication et de la Publicité, les systèmes accélèrent la production de livrables et de visuels stratégiques ;



Enfin, dans le domaine du Marketing et des Ventes, les outils de génération automatisent la production des nouveaux contenus marketing, des rapports de veille concurrentielle et d'analyse terrain.



Ces exemples de cas d'usage démontrent que l'I.A. n'est pas réservée à quelques grands groupes technologiques, mais constituent une opportunité réelle pour toute entreprise, quelle que soit sa taille, qui souhaite renforcer sa compétitivité dans la mesure où les technologies mises en oeuvre trouvent des applications concrètes au sein de ses métiers et fonctions.

À ce titre, **l'annexe 3** propose une cartographie détaillée des cas d'usage, des responsabilités engagées et des obligations réglementaires, afin d'aider les décideurs à anticiper les effets opérationnels de chaque outil. À travers ces exemples, ils pourront ainsi mieux saisir les opportunités offertes par l'I.A., tout en identifiant clairement les enjeux juridiques et les conditions d'une intégration responsable.

Cette approche générale de l'I.A. suppose toutefois que l'on précise le point de vue que le législateur a récemment adopté dans le règlement européen du 13 juin 2024 sur l'Intelligence artificielle - « A.I. Act » - en établissant des obligations pour les fournisseurs de systèmes d'I.A. à des fins générales et en interdisant certains systèmes d'I.A. attentatoires aux droits fondamentaux. Toutefois, avant d'aborder ce cadre réglementaire, il convient de poser quelques repères pour une intégration éclairée du fait que les opportunités technologiques offertes par les systèmes d'I.A. s'accompagnent de responsabilités nouvelles.



4 Pour une intégration lucide et responsable

Si l'I.A. ouvre des perspectives majeures en matière de performance, d'agilité et d'innovation, son intégration dans les processus métiers nécessite une vigilance éclairée. Car, comme toute technologie transversale, elle soulève des questions de qualité des données, de transparence des décisions, de respect des droits fondamentaux et de responsabilité éditoriale.

Ces questions ne doivent pas en freiner l'adoption, mais nous inciter à poser les bonnes questions dès la conception des projets : comment garantir la supervision humaine dans les décisions critiques ? Comment expliquer les recommandations produites par un système complexe ? Comment s'assurer que les contenus générés respectent les cadres juridiques et éthiques en vigueur ?

En anticipant ces points de vigilance, les entreprises peuvent d'ores et déjà faire de l'I.A. non seulement un levier de compétitivité, mais aussi un vecteur de confiance et de durabilité.

Pour étayer cette recommandation, rappelons que **l'annexe 3** propose une cartographie simplifiée des principales architectures et typologies d'apprentissage afin d'en faciliter la lecture stratégique et opérationnelle.



2 LA RÉGLEMENTATION DE L'IA.

1 Comment comprendre l'environnement réglementaire européen ?

L'encadrement juridique de L'IA. est une construction récente, née de la combinaison de l'évolution technologique rapide et des préoccupations éthiques et sécuritaires qui en ont découlé.

Les premières initiatives sur ce point sont apparues dans les années 2010 au sein d'organisations internationales (OCDE, UNESCO) mettant en avant des principes généraux comme la transparence, la sécurité et le respect des droits humains.

Puis, les législateurs ont entrepris d'élaborer des cadres plus précis et, de ce fait, plus exigeants. A ce jour, la réglementation la plus aboutie, et donc la plus précise et exigeante, est européenne. Il s'agit de l'Artificial Intelligence Act (A.I. Act) qui aborde une approche par usage et définit quatre grands niveaux de risque.

Niveau de risque	Description	Exemples	Exigences
Inacceptable	Risque trop élevé pour être toléré.	I.A. manipulant le comportement (ex : notation sociale, manipulation cognitive), surveillance biométrique de masse.	Interdiction totale
Haut risque	Impact significatif potentiel sur les droits fondamentaux, la Santé, la Sécurité.	I.A. dans la Santé (diagnostic), R.H. (recrutement), Justice, Éducation, Finance.	Exigences renforcées : documentation technique, analyse d'impact sur les droits fondamentaux, qualité des données, supervision humaine, transparence et traçabilité, robustesse et cybersécurité, marquage C.E.
Risque limité	Risque modéré, non négligeable.	Chatbots, systèmes de scoring non critiques.	Devoir de transparence et d'information sur l'interaction avec une I.A.
Risque minimal	Usage courant, sans impact sérieux.	Recommandation de films ou musique, correcteurs d'orthographe, jeux-vidéos.	Pas de réglementation spécifique.



Cette réglementation a été adoptée le 13 juin 2024 et entre en application progressivement selon le calendrier suivant :



2 février 2025 : Interdiction des systèmes d'I.A. présentant des risques jugés inacceptables.

2 août 2025 : Mise en place des règles pour les modèles d'I.A. à usage général et désignation des autorités compétentes dans chaque État membre.

2 août 2026 : Application complète aux systèmes d'I.A. à haut risque déjà identifiés, tels que ceux utilisés dans la biométrie, les infrastructures critiques, l'éducation, l'emploi ou la Justice.

2 août 2027 : Application complète.

Elle s'applique à tous les systèmes d'I.A. mis sur le marché européen - que leurs fournisseurs soient ou non établis sur le territoire européen - et intègre dans sa logique plusieurs textes et normes relatifs à la protection des données personnelles, à la sécurité des produits et aux recommandations techniques et organisationnelles à observer, tels que :

- **Le R.G.P.D.** (applicable depuis mai 2018) qui continue de jouer un rôle clé dans la mesure où l'I.A. implique souvent un traitement de données personnelles et impose notamment des obligations de minimisation, de transparence et de proportionnalité;
- **Le « Cyber Resilience Act »**, dont l'application se fera progressivement entre 2026 et 2027, qui vise quant à lui à renforcer la sécurité des produits connectés et logiciels dans le marché intérieur, ce qui inclut de nombreux systèmes d'I.A. ;
- **La Normalisation ISO**, qui apporte les méthodes pour démontrer la conformité aux législations et qui spécifie les recommandations techniques et organisationnelles telles que décrites dans les Normes suivantes :
 - **ISO/IEC 23894** sur la gestion des risques liés à l'I.A.,
 - **ISO/IEC 42001** sur les considérations éthiques et la transparence de l'I.A.,
 - **ISO/IEC 27001** sur la sécurité de l'information et la vie privée,
 - **ISO/IEC 25059** et ISO/IEC 5259 sur la qualité des données et des modèles d'I.A.

Notons toutefois qu'à l'international, les tentatives d'encadrement sont soit peu contraignantes, soit encore trop instables (on retiendra que les premières mesures d'encadrement ont en réalité été prises en août 2023 aux U.S.A. par l'Administration Biden mais annulées en janvier 2025 par les décrets de l'Administration Trump).



2 Fournisseur, utilisateur, fournisseur du modèle de base, développeur : Suis-je concerné par la réglementation européenne ?

Trois catégories principales d'opérateurs économiques sont identifiées dans l'IA. ACT: le **fournisseur** (provider), **l'utilisateur** (déployer) et, plus récemment introduit par les dernières versions du texte, **le fournisseur de modèle de base** (foundation model provider).

- **Le fournisseur est l'acteur central du dispositif réglementaire** : il s'agit de toute personne qui développe un système d'IA. ou le fait développer dans le but de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit. Il est donc le principal responsable de la conformité du système avant sa mise à disposition. Ses obligations comprennent notamment la mise en oeuvre d'un système de gestion des risques, la constitution d'un dossier technique complet, la réalisation d'une évaluation de conformité, ainsi que la surveillance post-commercialisation et le signalement des incidents graves. Il doit également assurer la transparence du système envers les utilisateurs, notamment en les informant de ses capacités, de ses limites et de son caractère artificiel lorsqu'il interagit avec des humains.

Exemples : une entreprise qui commercialise une solution d'IA. - tel qu'un logiciel de tri de candidatures, un outil de diagnostic médical automatisé ou un assistant conversationnel intégré à un service clients - ou une société d'ingénierie concevant une IA. de maintenance prédictive qu'elle vend à ses clients.

- **L'utilisateur** désigne la personne physique ou morale, autorité publique ou organisation, qui utilise un système d'IA. sous sa responsabilité, sauf à des fins purement personnelles et non professionnelles. Il n'est pas responsable de la conception du système, mais de la manière dont il l'exploite dans son activité. Ses principales obligations concernent la supervision humaine appropriée, l'utilisation conforme à la finalité prévue par le fournisseur, la qualité des données d'entrée et la vigilance vis-à-vis des effets du système. Il doit également signaler tout incident grave et conserver une traçabilité suffisante des opérations effectuées. L'IA. Act insiste sur le rôle de l'utilisateur dans la prévention des risques d'atteinte aux droits fondamentaux, notamment en matière de non-discrimination, de vie privée et de sécurité.

Exemples : un ingénieur de recherche développant un algorithme interne à l'entreprise ou une banque qui déploie un système de « scoring » de crédit ou une collectivité utilisant un algorithme d'aide à la décision pour l'attribution de subventions ou un cabinet d'avocats recourant à un outil d'analyse automatisée de contrats.

- **Le fournisseur de modèle de base** (foundation model provider) constitue une catégorie distincte introduite par la réforme finale du texte. Il s'agit d'acteurs tels qu'OpenAI, Mistral ou Anthropic qui entraînent, mettent au point et à disposition des modèles d'IA. généraliste pouvant être adaptés à de multiples finalités, comme les grands modèles de langage ou les modèles multimodaux génératifs. Ces fournisseurs agissent



en amont du cycle de valeur mais sont soumis à des obligations spécifiques en matière de documentation de l'entraînement, de transparence des données utilisées, de robustesse et de sécurité du modèle, et de publication d'un résumé des sources de données. Leurs modèles, dits « à fort impact » car susceptibles d'affecter un grand nombre d'utilisateurs ou de secteurs, doivent faire l'objet d'une évaluation approfondie et de mesures renforcées de gouvernance et de cybersécurité.

Exemple : un laboratoire d'innovation développant un grand modèle de langage propre. En pratique, une même entreprise peut cumuler plusieurs statuts selon le rôle qu'elle assume :

- Si elle entraîne un modèle fondamental interne, elle devient fournisseur de modèle de base ;
- Si elle intègre ce modèle dans un outil qu'elle commercialise, elle devient également fournisseur de ce système d'I.A. ;
- Si elle utilise ce même modèle comme outil en interne, elle agit comme utilisateur.

En parallèle de ces trois catégories juridiques, la pratique distingue souvent l'acteur technique intervenant en amont, sans être toujours identifié comme un fournisseur au sens strict du règlement, comme un **développeur** qui est celui qui conçoit, code, entraîne ou adapte un modèle ou un système d'I.A., sans nécessairement le mettre sur le marché. Ainsi, lorsqu'il développe un modèle pour son propre usage interne, il relève en réalité du statut d'utilisateur. En revanche, s'il développe un système en vue de sa commercialisation, il devient fournisseur. Et s'il entraîne un modèle de base de manière autonome, il devient fournisseur de modèle de base.

Cette articulation reflète la logique de **responsabilité distribuée** qui sous-tend l'A.I. Act : le fournisseur assure la conformité et la transparence du système mis sur le marché, l'utilisateur veille à un usage maîtrisé, sûr et conforme aux droits fondamentaux, le fournisseur de modèle de base garantit la solidité technique du modèle et le développeur intervient comme acteur technique de la conception.

Application pratique aux entreprises développant ou adaptant un système d'I.A.

CAS n°1 : Une entreprise utilise un modèle fondamental existant (comme GPT ou Mistral) qu'elle personnalise pour ses besoins internes. Elle ne met pas le système sur le marché et le limite à usage interne.

- Juridiquement, elle relève donc du statut d'utilisateur et ses obligations consistent à garantir une utilisation conforme à la finalité prévue par le fournisseur, à assurer la supervision humaine et à protéger les données utilisées pour l'entraînement ou l'exploitation du modèle.
- Le fournisseur du modèle fondamental - par exemple OpenAI - reste responsable de la qualité et de la transparence du modèle de base, tandis que l'entreprise porte la responsabilité du déploiement concret de l'I.A. et des effets de son usage sur ses clients, salariés ou partenaires.



CAS n°2 : une entreprise développe son propre modèle ou système d'I.A. qu'elle met à disposition de tiers, même gratuitement ou au sein d'un Groupe.

- Elle devient fournisseur, avec les obligations correspondantes : évaluation de conformité, documentation technique, système de gestion des risques et surveillance postcommercialisation.
- Si l'entreprise crée un modèle fondamental généraliste susceptible d'alimenter d'autres systèmes, elle relève du statut de fournisseur de modèle de base, avec des obligations renforcées de transparence, de sécurité et de gouvernance des données. Enfin, ses ingénieurs ou équipes R&D agissent comme développeurs internes, responsables de la qualité technique et de la traçabilité des algorithmes.

3 Quelles sanctions prévues ?

Le non-respect du règlement peut entraîner des sanctions financières importantes, proportionnées à la gravité de l'infraction et à la taille de l'entreprise. Ces amendes sont administratives, décidées par les Autorités nationales compétentes désignées dans chaque état membre.

Gravité de la violation	Description	Montant de l'amende
Violation très grave	Utilisation ou mise sur le marché de systèmes d'I.A. interdits (ex. : manipulation cognitive, notation sociale, reconnaissance biométrique non autorisée).	Jusqu'à 35 millions d'euros ou 7 % du chiffre d'affaires mondial annuel (le montant le plus élevé étant retenu).
Violation grave	Non-respect des obligations applicables aux systèmes d'I.A. à haut risque : documentation, gestion des risques, supervision humaine, traçabilité, transparence, etc.	Jusqu'à 15 millions d'euros ou 3 % du chiffre d'affaires mondial annuel.
Non-coopération	Fourniture d'informations fausses ou incomplètes à une autorité de surveillance ou non-coopération lors d'une enquête.	Jusqu'à 7,5 millions d'euros ou 1 % du chiffre d'affaires mondial annuel.



4 Les enjeux de la gestion des droits d'auteur en droit français

L'I.A. « générative » repose sur l'exploitation massive de contenus. Or, cette exploitation se heurte aux droits de propriété intellectuelle en France et nécessite une attention particulière.

Les enjeux juridiques se structurent autour de trois axes :

- **Accès aux données vs. Protection des titulaires** : les entreprises innovantes peuvent se heurter à des refus d'accès, à des accès discriminatoires ou à des stratégies d'exclusivité sur des catalogues de contenus susceptibles d'affecter la concurrence et la capacité d'innovation.
- **Transparence et loyauté** : les titulaires de droits (notamment éditeurs et agences de presse) expriment des préoccupations fortes sur l'exploitation de leurs contenus par des fournisseurs de modèles sans information claire ni mécanisme effectif d'opposition. Cette dimension "transparence" est un enjeu de conformité et un enjeu contentieux.
- **Risque de "réutilisation" dans les sorties** : indépendamment du débat sur l'entraînement, l'entreprise utilisatrice s'expose si elle diffuse des contenus qui reprennent substantiellement un contenu protégé (texte, image, code), car le risque se matérialise souvent au moment de la publication ou de la commercialisation.

C'est pourquoi le cadre juridique français organise l'équilibre entre protection et innovation, afin que les mécanismes de fouille de textes et de données ne portent pas atteinte à l'exploitation normale de l'oeuvre et ne causent pas un préjudice injustifié aux intérêts légitimes de l'auteur.



Précisions en cas d'usage d'un outil d'I.A.

Usage d'une I.A. publique

Le risque d'atteinte aux droits de propriété intellectuelle ne dépend pas uniquement de la façon dont la solution a été conçue mais aussi des données que l'entreprise utilisatrice y injecte et de ce qu'elle publie.

Points d'attention

1) Exiger de la transparence sur l'origine des données et contenus utilisés par la solution d'I.A.

2) Vérifier le cadre juridique applicable aux données qui sont injectées dans la solution d'I.A afin de déterminer si elles sont susceptibles ou non d'être réutilisées, que ce soit aux fins d'entraînements ou aux fins de transmission et/ou publication chez un tiers ;

3) Encadrer l'alimentation de l'outil : lorsque les équipes "nourrissent" un outil d'I.A. avec des documents, images, contenus tiers, il est essentiel de s'assurer qu'elles ont eu accès à ces données de manière licite et que l'usage envisagé ne contourne pas les droits de propriété intellectuelle. La politique interne de l'entreprise doit donc distinguer :

- contenus internes maîtrisés,
- contenus sous licence,
- contenus tiers trouvés en ligne (plus risqués, car susceptibles d'opt-out et de droits voisins).

4) Sécuriser la publication externe en amont : éviter la publication "automatique" lorsqu'un contenu peut être généré via une solution susceptible de reprendre un contenu préexistant

Usage d'une I.A. Privative

C'est la situation la plus sensible pour l'entreprise en ce qu'elle implique la constitution d'un Dataset et l'entraînement de données.

L'exigence principale est la traçabilité des données utilisées : il est essentiel de pouvoir démontrer que les données utilisées ont fait l'objet d'un accès licite et qu'un système de prise en compte des éventuelles oppositions a été mis en place, ainsi que des mesures de sécurisation et destruction en cas de manquement aux droits de propriété intellectuelle.

En cas de recours à une externalisation via un prestataire, il convient d'exiger des engagements clairs sur les sources utilisées – qui doivent être licites, mécanismes d'optout (de désengagement), de sécurité et de documentation. Attention, le risque juridique tout comme l'impact opérationnel et réputationnel reposeront sur l'entreprise qui déploie l'outil.

Enfin, ne pas oublier que les contenus presse sont particulièrement sensibles et nécessitent une attention particulière lorsqu'ils sont intégrés dans un système d'I.A.



5 En quoi la conformité I.A. est-elle un enjeu stratégique ?

Sans normes, chaque acteur de l'I.A. définirait ses propres règles, entraînant un risque de fragmentation, de perte de confiance et d'inégalités d'accès au marché. Avec elles, on obtient interopérabilité, sécurité et transparence, tout en laissant la place à l'innovation. Elles servent de garant de confiance pour les citoyens, de « boussole » réglementaire pour les entreprises et de passerelle entre législation, technique et éthique.

Même si la Normalisation reste l'objet de critiques par de nombreux acteurs de l'écosystème en ce qu'elle serait un frein à leur développement, tous s'accordent aujourd'hui sur un point : elle est un passage obligé pour garantir la confiance en leur solution.

Ainsi, les décisions d'investissement ne peuvent faire l'impasse sur une page de présentation de ces garanties de conformité, et les opérations de due diligence intègrent un audit de conformité des sociétés dans lesquelles investir.

Rappel des bénéfices proposés aux entreprises par la Normalisation européenne relative à l'I.A.

- **Harmonisation** : éviter la fragmentation en coordonnant les travaux nationaux (ex. AFNOR en France) avec les initiatives européennes et internationales (ISO, IEC, IEEE).
- **Interopérabilité** : garantir que les systèmes d'I.A. puissent communiquer et fonctionner ensemble dans différents secteurs et pays.
- **Spécificité sectorielle** : décliner les normes transversales dans des référentiels adaptés à des secteurs sensibles (santé, finance, automobile, etc.)
- **Révision continue** : actualiser régulièrement les normes pour suivre les évolutions rapides des technologies d'I.A. (tous les 2-3 ans).

À ce titre, les travaux de Normalisation identifient un ensemble de propriétés essentielles pour bâtir des systèmes d'I.A. dignes de confiance et qui servent de guide pour concevoir, évaluer et améliorer les systèmes d'I.A. tout au long de leur cycle de vie :

- **Sécurité & Safety** : garantir la protection contre les cyberattaques et maintenir un niveau de sûreté acceptable, même face aux défaillances ou usages imprévus.
- **Confidentialité** : protéger les données personnelles et trouver le juste équilibre entre transparence et la traçabilité.
- **Explicabilité & Transparence** : rendre compréhensibles et adaptées les décisions prises par l'I.A. au regard de ses utilisateurs.
- **Fiabilité & Robustesse** : assurer que l'I.A. fonctionne comme prévu, même dans des conditions dégradées, tout en maîtrisant les incertitudes.



- **Éthique & Équité** : prévenir les biais, garantir un traitement juste et intégrer des considérations environnementales et sociétales.
- **Responsabilité & Supervision humaine** : clarifier les décideurs, définir les interactions homme/machine et mettre en place des mécanismes de contrôle en continu.

Rappel des référentiels relatifs à l'I.A. reconnus par la Communauté européenne

- **Le Code de bonnes pratiques, publié le 10 juillet 2025 par la Commission européenne**, vise à accompagner les fournisseurs d'I.A. à usage général dans leur conformité au règlement I.A. Il simplifie les obligations légales en les organisant autour de trois axes : sécurité, transparence et respect du droit d'auteur. Son adoption offre une simplification administrative, une sécurité juridique renforcée et constitue un atout stratégique dans un contexte où les investisseurs valorisent fortement la conformité. L'objectif est d'apporter aux entreprises un outil accessible, pratique et compétitif pour évoluer dans un cadre réglementaire complexe.
- **Les normes ISO** fournissent un cadre international permettant de mettre en oeuvre et de démontrer la conformité aux exigences européennes. La norme centrale ISO/IEC 42001 propose un système de management couvrant l'éthique, la transparence, la qualité et la sécurité des systèmes d'I.A. sur tout leur cycle de vie, facilitant ainsi l'alignement sur l'A.I. Act (gestion des risques, supervision humaine, lutte contre les biais...). Elle est complétée par l'ISO/IEC 23894 (risques I.A.), l'ISO/IEC 27001 (sécurité de l'information) et d'autres normes dédiées à la qualité des données et des modèles. Un nouveau projet, ISO/IEC NP TS 42119, porte sur les techniques de tests et l'évaluation des systèmes d'I.A. génératifs.

Pour les dirigeants d'entreprise, investir dans ces normes réduit l'incertitude juridique et technique, améliore la gouvernance interne et renforce la crédibilité auprès des partenaires et investisseurs. Ces normes deviennent ainsi un levier stratégique : elles structurent les pratiques, favorisent une innovation responsable et soutiennent la compétitivité et la pérennité des entreprises évoluant sur un marché européen fortement régulé.



3 ENJEUX ET RECOMMANDATIONS

Au-delà de la lecture attentive du corpus normatif et réglementaire, il importe de mettre en lumière les enjeux d'usage responsable et éthique des systèmes d'intelligence artificielle ainsi que les plans d'actions à mettre en place pour garantir la sécurité et la confidentialité des données, la nécessité de former et de sensibiliser les équipes opérationnelles et la gestion des responsabilités et des risques (intégrité, souveraineté, exploitabilité). La question de la consommation énergétique des systèmes d'I.A. sera également traitée, avec des recommandations concrètes pour anticiper et maîtriser l'impact de l'I.A. sur l'entreprise.

1 Usage responsable et éthique

L'A.I. Act encourage une culture de la transparence, de la responsabilité algorithmique et de l'éthique. Les entreprises sont invitées à adopter des chartes d'utilisation de l'I.A., à définir les usages autorisés, les bonnes pratiques et les sanctions en cas de dérive. L'élaboration d'une charte éthique permet de formaliser les engagements de l'entreprise pour un usage responsable de l'I.A., en tenant compte des enjeux de confiance, d'intégrité et de souveraineté. C'est également un pacte de confiance vis-à-vis partenaires financiers et commerciaux qui les rassure en matière d'**Intégrité** (il convient de s'assurer que les systèmes d'I.A. produisent des résultats fiables et vérifiables) et de **Souveraineté** (il est impératif de maîtriser la provenance et le traitement des données afin d'éviter une dépendance à terme rapidement dommageable pour l'entreprise à des solutions extérieures non maîtrisées).

Cinq grandes approches sont désormais à privilégier afin de favoriser l'usage responsable et éthique qui est recommandé.

1 Être exemplaire en matière d'équité

Cela suppose :

- De s'assurer que les données utilisées pour entraîner les modèles sont fiables et ne permettent pas d'entraîner des résultats biaisés ou discriminations ;
- D'utiliser l'I.A. en conformité avec les réglementations (R.G.P.D. en Europe) tout en garantissant l'anonymisation et le consentement éclairé des utilisateurs ;
- D'éviter les biais algorithmiques en diversifiant les données d'entraînement et en auditant régulièrement les modèles pour détecter et corriger les discriminations (genre, origine, handicap, etc.) ;
- D'impliquer des profils variés (culturels, disciplinaires, genres) dans la conception des systèmes d'I.A. pour limiter les biais et répondre à des besoins divers.



2 Être vigilant en matière de transparence

Cela suppose de garantir la transparence à la fois sur les algorithmes développés et sur les données utilisées pour l'entraînement et d'informer les utilisateurs lorsqu'ils interagissent avec une A.I., en expliquant les limites et les risques associés.

Rappelons que la transparence des décisions algorithmiques vis-à-vis des usagers et partenaires désigne la capacité de l'entreprise à rendre compréhensibles, accessibles et justifiables les décisions prises ou influencées par des systèmes d'intelligence artificielle.

Elle repose sur trois piliers :

- **La visibilité** qui suppose d'informer les usagers qu'une décision est partiellement ou totalement automatisée.
- **L'explicabilité** qui nécessite d'explicitier les critères, les données et les logiques ayant conduit à la décision.
- **La traçabilité** qui exige de documenter les étapes du processus décisionnel et les arbitrages techniques ou éthiques associés, d'informer clairement les usagers qu'une décision est partiellement ou totalement automatisée.

Exemple métier : dans un système de tri automatisé de candidatures, il est essentiel d'expliquer aux candidats les critères retenus par l'algorithme, de permettre une relecture humaine et d'offrir un droit de recours. Cette transparence renforce la confiance, limite les biais et garantit la conformité avec les principes de non-discrimination.

3 Veiller à la protection des libertés individuelles

Cela suppose :

- De garantir la confidentialité des informations traitées et le respect du consentement
- D'utiliser l'I.A. en conformité avec les réglementations, en garantissant l'anonymisation et le consentement éclairé des utilisateurs.

4 Organiser le contrôle

Cela suppose :

- De désigner des comités internes indépendants pilotés par des humains afin de veiller à d'éventuelles dérives. Ces comités doivent dépendre directement du COMEX et être intégrés dans la gouvernance de l'entreprise ;



- De clarifier les responsabilités en cas d'erreur ou de dommage causé par un système d'I.A. (fabricants, développeurs, utilisateurs) ;
- De mettre en place des garde-fous contre les usages malveillants («deepfakes», désinformation, cyberattaques).

5 Promouvoir des campagnes de sensibilisation et de formation

Cela suppose :

- De considérer la sensibilisation continue des équipes comme essentielle pour garantir la prévention des risques et favoriser l'appropriation des outils d'I.A. Elle doit couvrir la cybersécurité, la protection de la confidentialité et la reconnaissance des risques liés à l'utilisation de l'I.A.
- De considérer que la formation est aussi une obligation en matière de conformité : l'A.I. Act introduisant, en complément des obligations techniques et de gouvernance, une obligation explicite de sensibilisation et de formation des personnels des entités qui développent ou déploient des systèmes d'I.A.

Rappelons que depuis le **2 février 2025**, les fournisseurs et les utilisateurs de systèmes d'I.A. doivent veiller à ce que leurs effectifs (employés, sous-traitants, utilisateurs professionnels) comprennent les principes, les limites et les risques des systèmes d'I.A. qu'ils développent ou utilisent. La formation n'est donc pas optionnelle et fait partie intégrante du dispositif de conformité, notamment pour les systèmes à risque élevé.

2 Cybersecurite et confidentialite

L'intégration de l'I.A. implique le traitement de données sensibles. Les principales vulnérabilités sont les cyberattaques, les fuites de données et la compromission du secret professionnel. Pour limiter ces risques, il est recommandé :

- D'identifier le niveau de risque en présence, modéré ou élevé,
- De mettre en place des solutions techniques robustes (chiffrement, gestion des accès, audits réguliers),
- D'adopter des politiques de confidentialité claires pour les outils d'I.A.,
- De sélectionner des fournisseurs d'I.A. engagés sur la sécurité des données,
- De prévoir dans les contrats des clauses adéquates pour garantir la confidentialité et la sécurité des données.



3 Souveraineté

La souveraineté numérique constitue un enjeu stratégique central dans le déploiement de l'intelligence artificielle. Si l'I.A. offre des leviers majeurs de performance et de compétitivité, elle expose également les entreprises françaises et européennes à une dépendance accrue vis-à-vis d'acteurs étrangers pour l'hébergement, le traitement et la circulation des données. Or, la maîtrise de ces infrastructures, logiciels et flux de données conditionne la sécurité, la confidentialité et la gouvernance des informations. Préserver la souveraineté numérique implique donc de contrôler l'ensemble de la chaîne de valeur de l'I.A., des infrastructures et codes sources jusqu'aux données d'entrée, prompts et résultats générés.

Les données, essentielles au fonctionnement de l'I.A., sont souvent hébergées ou contrôlées par des acteurs extra-européens. A titre d'exemple, les législations américaines comme le Patriot Act ou le Cloud Act et surtout l'executive order 12333 et le FISA amendment Act permettent aux Autorités des États-Unis d'accéder à ces données, même lorsqu'elles se trouvent en Europe. Cette dépendance crée un risque majeur pour la confidentialité, la conformité réglementaire et la souveraineté stratégique des entreprises européennes.

Il ne faut pas se leurrer : les accords contractuels entre les sociétés américaines et françaises garantissant un maintien des données traitées en Europe ne valent pas grand-chose et ne sont qu'une protection illusoire de la souveraineté.



Pour préserver leur autonomie, les entreprises doivent donc adopter une stratégie numérique responsable et souveraine : privilégier les infrastructures de cloud souverain (comme celles labellisées SecNumCloud en France), contrôler la localisation et les flux de données en s'assurant qu'ils ne sortent pas du périmètre européen et évaluer la propriété capitaliste des fournisseurs de solutions d'I.A. afin d'en comprendre les implications géopolitiques.

L'Union européenne, avec ses initiatives comme le R.G.P.D., le règlement sur l'I.A. (A.I. Act) et le « Data Governance Act », cherche à instaurer un cadre protecteur favorisant l'innovation tout en garantissant la protection des données et un usage maîtrisé et éthique des technologies. Pour les dirigeants, la souveraineté numérique devient ainsi un enjeu de gouvernance et de confiance, dépassant la simple dimension technique.

L'intégration de l'intelligence artificielle dans les organisations soulève donc des enjeux de souveraineté, tant sur le plan technologique que juridique et stratégique. Il ne s'agit pas seulement de conformité, mais de capacité à maîtriser les outils, les données et les décisions associées.



Enjeux clés

- **Propriété intellectuelle** - S'assurer que les modèles développés ou utilisés respectent les droits d'auteur, les licences, et que les données d'entraînement ne compromettent pas les actifs informationnels de l'entreprise.
- **Maîtrise des infrastructures** - Privilégier des solutions hébergées sur des serveurs souverains ou maîtrisés, afin d'éviter une dépendance excessive à des fournisseurs extra-européens ou à des plateformes opaques.
- **Traçabilité des données** - Documenter la provenance, les conditions de collecte et les modalités de traitement des données utilisées par les systèmes d'A.I.
- **Interopérabilité et portabilité** - Choisir des architectures ouvertes et interopérables, permettant de migrer ou d'adapter les systèmes sans verrouillage technologique.
- **Autonomie stratégique** - Développer des compétences internes, des référentiels métiers et des capacités d'audit pour garantir une indépendance dans l'usage, l'évaluation et l'évolution des systèmes d'A.I.

On privilégiera ainsi sur ce point les axes travail suivants qui consisteront à :



Cartographier les dépendances technologiques liées à l'A.I. (fournisseurs, API, hébergement, modèles) ;



Intégrer des clauses de souveraineté dans les contrats avec les prestataires I.A. ;



Valoriser les solutions open source françaises et/ou européennes et les initiatives locales en matière de Cloud, de données et de modèles ;



Former les équipes à la lecture critique des offres A.I. et à l'analyse des risques de dépendance.

4 Développement durable

Comme le démontre nombre d'études, la consommation énergétique liée à l'utilisation de l'intelligence artificielle - notamment celle des modèles génératifs comme ChatGPT - est très élevée et croissante.



L'entraînement d'un grand modèle de langage, comme ceux utilisés pour le traitement automatique du langage naturel, peut consommer plusieurs Gigawatts (ex: 4 GigaWatts pour Mistral), soit l'équivalent de plusieurs années de consommation électrique d'un foyer européen. Une entreprise qui développe ou utilise ce type de modèle à grande échelle doit donc évaluer son empreinte carbone, optimiser l'usage des ressources, et privilégier des centres de données à énergie renouvelable.

Pour rappel, une série de 10 à 50 questions posée à ChatGPT entraîne une consommation de plus d'un demi-litre d'eau. Les grands data centers de Google et Microsoft consomment, chaque jour, entre 3,8 et 19 millions de litres d'eau ; dont $\frac{1}{4}$ est utilisé directement au refroidissement des serveurs liés à l'I.A.

Conscientes de l'importance cruciale de cet enjeu énergétique lié à l'I.A., les entreprises doivent intégrer cette dimension dans la responsabilité environnementale de leur activité et modérer l'usage de l'I.A. en le réservant à des besoins spécifiques et prioritaires pour limiter l'impact environnemental et ainsi être alignées avec leurs politiques RSE et les obligations CSRD. la cas échéant

On privilégiera ainsi sur ce point les axes travail suivants qui consisteront à :

- Évaluer l'empreinte carbone des systèmes d'A.I. en mesurant la consommation énergétique des phases d'entraînement, d'inférence et de stockage, en kWh ou équivalent CO₂ et en intégrant ces données dans les bilans RSE ;
- Définir des métriques de sobriété numérique en mettant en place des indicateurs permettant de suivre l'efficacité énergétique des modèles (ex. ratio performance/énergie, intensité carbone par tâche) et les intégrant dans les fiches projets A.I. ;
- Optimiser l'usage des ressources en privilégiant des modèles frugaux ou spécialisés, adaptés aux besoins métiers, moins gourmands en ressources que les modèles généralistes massifs ;
- Choisir des infrastructures responsables en utilisant des centres de données alimentés par des énergies renouvelables, et favoriser les fournisseurs engagés dans une démarche de sobriété numérique ;
- Documenter les choix technologiques en traçant les arbitrages effectués en matière de performance vs consommation pour renforcer la transparence et la redevabilité environnementale.

Exemple : L'entraînement d'un grand modèle de langage, comme ceux utilisés pour le traitement automatique du langage naturel, peut consommer plusieurs Gigawatts (ex: 4 GigaWatts pour Mistral), soit l'équivalent de plusieurs années de consommation électrique d'un foyer européen. Une entreprise qui développe ou utilise ce type de modèle à grande échelle doit donc évaluer son empreinte carbone, optimiser l'usage des ressources, et privilégier des centres de données à énergie renouvelable.



5 Recommandations principales

Elles se résument à deux grands axes de travail qui mobiliseront principalement les décideurs et les conseils juridiques en liaison étroite avec les équipes S.I. et R.H. de l'entreprise.

Au niveau R.H., il importe :

- De planifier une politique de formation du fait que l'obligation de formation étant déjà entrée en vigueur ;
- De définir des parcours de formation modulables et adaptés aux différentes équipes ;
- D'intégrer la formation dans la gouvernance I.A. en désignant un référent I.A. en interne chargé du suivi des formations, de la veille réglementaire et de la mise à jour continue ;
- De sensibiliser la direction et toutes les parties prenantes en faisant de cette formation un axe prioritaire des Comités de Direction afin qu'elle soit soutenue, budgétisée et visible.

Au niveau S.I., il importe :

- De cartographier les systèmes d'I.A. utilisés dans l'entreprise en identifiant les systèmes d'I.A. utilisés ou en projet ainsi que les populations (techniques, métiers, utilisateurs finaux) qui doivent être formées. Par ailleurs pour chaque système I.A. il faut établir le niveau de risque (haut/modéré/minimal) - Les mesures techniques à adopter selon le niveau de risque sont définies en annexe 4.



4 RÔLES ET RESPONSABILITÉS

1 Usage responsable et éthique

Pour assurer une gouvernance efficace et conforme de l'intelligence artificielle en entreprise, il est essentiel de clarifier les rôles et responsabilités de chaque acteur impliqué. Cette cartographie vise à identifier les fonctions clés du dirigeant au responsable technique, du dirigeant au collaborateur opérationnel et à préciser les engagements, les obligations et les points de vigilance associés à l'usage des systèmes d'I.A.

Fonction	Responsabilités principales	Obligations réglementaires	Points de vigilance
Dirigeant / DG	Pilote la stratégie I.A., valide les usages et les risques acceptés	Doit garantir la conformité globale (A.I. Act, R.G.P.D.)	Anticipe les risques réputationnels, éthiques et juridiques
Référent I.A. / Comex I.A.	Coordonne les projets I.A., arbitre les choix de solutions	Veille aux standards techniques et à la documentation	Maintien d'une vision transverse et actualisée du cadre réglementaire
Responsable juridique / conformité / DPO	Analyse les impacts sur les droits fondamentaux, rédige les clauses contractuelles	Application du R.G.P.D., du Cyber Resilience Act, gestion des consentements	Vigilance sur les biais, la traçabilité et les recours possibles
Responsable IT / Data / Cybersécurité	Implémente les systèmes, sécurise les infrastructures, mesure les performances	Obligations de robustesse, résilience, supervision technique	Choix des architectures, protection des données sensibles, audit des modèles
Responsable RH / formation	Identifie les impacts humains, forme les équipes à l'usage responsable de l'I.A.	Obligation de formation des personnels selon l'A.I. Act	Prévention des dérives, de la sur-surveillance ou de la marginalisation
Responsable métier / opérationnel	Définit les cas d'usage I.A., suit leur exécution	Doit s'assurer de l'utilité et de la légitimité du recours à l'I.A.	Veiller à l'explicabilité des décisions et à la supervision humaine
Collaborateur / utilisateur final	Utilise les outils I.A. dans ses tâches quotidiennes	Devient coresponsable des décisions prises avec l'I.A.	Compréhension minimale des risques et des droits (explication, recours)



2 Quelles actions a mettre en place ?

La mise en conformité ne repose pas uniquement sur le respect formel d'obligations juridiques. Elle suppose également l'adoption de réflexes organisationnels, techniques et contractuels permettant d'assurer un usage maîtrisé, sécurisé et responsable de l'Intelligence artificielle au sein de l'entreprise. Ces réflexes doivent être anticipés dès aujourd'hui, car ils conditionnent la capacité des organisations à intégrer l'I.A. sans en subir les risques juridiques, économiques ou réputationnels. Il est donc essentiel d'être proactif dans la mise en oeuvre de la conformité et d'assurer une conformité continue, laquelle comporte moins de risques juridiques comme financiers. A ce titre, quatre actions sont hautement recommandées :

1 Promouvoir une organisation interne intégrant la gouvernance de l'I.A.

L'intégration de l'intelligence artificielle dans les processus d'une entreprise impose de structurer sa gouvernance interne. Cela suppose la désignation d'un responsable de la conformité I.A. ou d'un référent capable de superviser les usages, d'évaluer les risques et de coordonner les actions de mise en conformité. Cette fonction peut être rattachée au délégué à la protection des données (D.P.O.) ou au responsable conformité existante, selon la taille et la maturité de l'entreprise. r les engagements, les obligations et les points de vigilance associés à l'usage des systèmes d'I.A.

Une traçabilité interne des décisions prises avec l'appui de systèmes d'I.A. doit également être assurée. Les erreurs, incidents ou résultats anormaux doivent faire l'objet d'une remontée d'information systématique, accompagnée d'une procédure de correction et, si nécessaire, de signalement. Cette logique de boucle de rétroaction est au coeur de la surveillance post-déploiement exigée par l'A.I. Act.

Enfin, l'organisation interne doit encourager une culture de la responsabilité numérique : chaque collaborateur utilisant des outils d'I.A. doit être conscient du cadre, des limites et de la supervision hiérarchique de son travail.

2 Renforcer la cybersécurité : l'I.A., alliée stratégique mais faille potentielle

L'intelligence artificielle représente également une nouvelle surface d'attaque pour les menaces cyber. Les systèmes d'I.A. peuvent en effet être manipulés (attaques par « prompt injection », corruption de données d'entraînement, extraction de secrets internes, etc.), exposant l'entreprise à des risques majeurs de fuite d'informations ou de désinformation automatisée.

Il est donc essentiel de renforcer la cybersécurité de manière proportionnée à ces nouveaux usages en :

- Auditant régulièrement les systèmes d'I.A. utilisés, qu'ils soient internes ou externes ;
- Sécurisant les flux de données d'entrée et de sortie ;
- Encadrant les accès aux interfaces d'I.A. générative et les usages internes des données confidentielles ;



- Mettant en place une politique d'usage responsable précisant ce qui peut ou non être confié à une I.A., notamment lorsqu'elle repose sur des services en ligne externes.

3 **Sécuriser la responsabilité contractuelle : intégrer l'I.A. dans vos relations d'affaires**

Dès lors que l'intelligence artificielle est intégrée dans les processus ou les prestations d'une entreprise, il est indispensable d'en tenir compte dans les contrats.

- Sur le plan interne, cela signifie que les contrats de travail, règlements d'entreprise et politiques internes doivent préciser les conditions d'usage de l'I.A. et les responsabilités associées.
- Sur le plan externe, il est crucial d'intégrer des clauses spécifiques dans les contrats commerciaux dont les :
 - Clauses de transparence (indiquer l'usage d'un système d'I.A. dans la prestation) ;
 - Clauses de responsabilité (définir qui supporte les conséquences d'une erreur ou d'un dysfonctionnement du système d'I.A.) ;
 - Clauses de conformité (garantir que le système respecte les exigences légales et éthiques en vigueur).

De même, il est fortement recommandé de vérifier si les interlocuteurs, prestataires ou partenaires utilisent des systèmes d'I.A. dans leurs propres processus.

4 **Investir, former et assumer : vers une culture maîtrisée de l'Intelligence artificielle**

L'intégration réussie de l'I.A. dans une organisation repose sur trois piliers : investir, former et assumer.

- **Investir** : « si c'est gratuit, c'est vous le produit ». Les systèmes d'I.A. fiables et conformes ont un coût. Les solutions gratuites sont souvent des sources d'exposition juridique ou de fuite de données. Les entreprises doivent donc privilégier des outils dont la gouvernance, la sécurité et la traçabilité sont vérifiées.
- **Former** : la montée en compétence doit concerner tous les échelons de l'organisation, des dirigeants aux collaborateurs opérationnels. Chacun doit comprendre les principes de fonctionnement de l'I.A., ses risques et les bonnes pratiques d'utilisation car chaque intervenant peut être une faille dans le système. Il est par exemple inutile de développer des solutions d'I.A. en interne sans permettre aux stagiaires et assistants d'en bénéficier et d'être pleinement formés, si besoin est, à leur usage. La formation est un levier central de conformité, mais aussi de performance et de confiance interne.



- **Assumer** : il ne s'agit pas de dissimuler l'usage de l'I.A., mais de l'intégrer de manière transparente et assumée. Communiquer sur une utilisation intelligente, maîtrisée et responsable de l'intelligence artificielle devient un atout concurrentiel, à la fois pour rassurer les clients et pour valoriser la maturité numérique de l'entreprise.

3 Importance de la formation

Au-delà des obligations de conformité réglementaire, une formation des équipes utilisatrices des systèmes d'I.A. au sein d'une entreprise s'avère donc essentielle à plusieurs égards afin :

- **D'optimiser véritablement l'usage et le réel potentiel de l'I.A.**

Si les équipes ne comprennent pas ce que l'I.A. peut réellement apporter - tout comme ce qu'elle ne peut pas -, alors les projets reposant sur ces outils risquent d'être mal calibrés, mal supervisés, voire inefficaces. Une formation appropriée permet de tirer le plein bénéfice des systèmes tout en évitant les dérives ou erreurs coûteuses.

- **De préserver la maîtrise humaine et éviter la dépendance à la machine**

Face à la fable d'un remplacement de l'humain par la machine, la meilleure réponse est la maîtrise de l'outil. L'I.A. ne doit pas être « une boîte noire autonome » que l'on suit sans comprendre. En étant formés, les utilisateurs savent comment fonctionne le système d'I.A. et gardent le plein contrôle de l'outil. Cela remet l'humain au cœur du mécanisme de décision et le responsabilise dans l'usage de l'outil.

- **De donner confiance et réputation**

Une entreprise dont les dirigeants ont anticipé la formation et la sensibilisation démontre qu'elle prend au sérieux les enjeux éthiques, juridiques et de conformité. Cela renforce la confiance des clients, des partenaires et des investisseurs. L'I.A. devient alors un levier de performance et éthique, et non un facteur de risque.



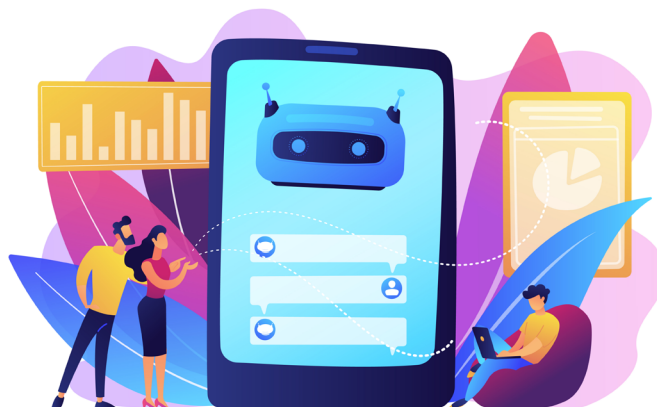
5 MEMENTO PRATIQUE À L'USAGE DES ACTEURS DU NUMÉRIQUE

Ce memento, à usage des acteurs du Numérique, propose une synthèse opérationnelle des principales recommandations rappelées précédemment pouvant déboucher sur des fiches actions. Elle s'adresse, de ce fait, aux deux contextes d'entreprises utilisant des systèmes d'I.A. :

- Celui d'une entreprise ou organisation utilisatrice de systèmes d'I.A. qui doit définir les modes d'emploi de l'I.A. pour ses collaborateurs (usage individuel dans le cadre professionnel) en réponse à ses besoins de gestion propres ;
- Celui d'une entreprise fournisseur de systèmes d'I.A. qui doit s'assurer de la conformité aux bonnes pratiques du système déployé pour un client utilisateur.

Avant tout, quel que soit le contexte de l'entreprise, il importe aux acteurs en question de déterminer le profil où cette dernière opère en identifiant si elle a un rôle d'utilisateur ou de fournisseur qui, dans de nombreux cas, peut s'avérer complémentaire. La détermination du **profil d'entreprise** (catégorie d'acteur) est donc le pré-requis indispensable à la mise en place de tout plan d'action.

- Comment ? En répertoriant les systèmes d'I.A. utilisés, qu'ils soient internes, SaaS, tiers ou open source, pour un usage individuel ou collectif.
Ils doivent ensuite évaluer le niveau de risque associé au profil de l'entreprise et à ses usages réels en portant attention aux zones grises qui doivent être identifiées et doivent faire l'objet d'une surveillance précise.
- Comment ? En confiant ce rôle à un responsable conformité en interne ou un conseil spécialisé en externe.
Ils doivent enfin exiger des décideurs de l'entreprise où ils opèrent de mettre en place une gouvernance I.A. adaptée à sa taille et à ses besoins.
- Comment ? En procédant à sa mise en conformité si nécessaire, en communiquant en interne sur les usages et rôles, ainsi que sur le niveau de risque généré, des systèmes d'I.A. employés ou commercialisés, et en exigeant la mise en oeuvre d'une politique de formation.



OBLIGATIONS SPECIFIQUES DES UTILISATEURS DE SYSTEMES D'I.A. / UTILISATEURS



Utilisateurs

Leurs responsabilités portent sur le choix, le déploiement et la supervision des systèmes, ainsi que sur la gestion des risques liés à leurs usages et la protection des données personnelles.

Cadre réglementaire et organisationnel des obligations de l'utilisateur

Règlement I.A.

- Il veille que l'usage des systèmes d'I.A. est conforme à leurs finalités, surtout en cas de systèmes à haut-risque.
- Il respecte les obligations liées à la supervision humaine, la gestion des incidents, la traçabilité et la conservation des logs.
- Il s'appuie sur les recommandations de la CNIL et du R.G.P.D. dans la mesure où il y a une articulation étroite entre I.A. et traitement des données personnelles.
- Il se base sur les Normes ISO/IEC 42001 et 23894 pour l'adoption d'une gouvernance appropriée en matière d'I.A.

Cadre organisationnel

Il s'appuie sur un **réfèrent I.A.**, rattaché à la direction générale, qui travaille en lien avec les équipes Conformité, Juridique et S.I. Ce réfèrent aura pour mission de proposer une **politique interne** encadrant l'utilisation de l'I.A. : responsabilités, processus d'autorisation, règles éthiques et documentation.

À ce titre, il demande que :

- Les systèmes d'I.A. soient régulièrement **inventoriés** et **les risques réévalués** selon les niveaux de risque (faible, limité, élevé) et leurs impacts potentiels en matière de traitement de données précisés ;
- Les **évaluations d'impact** soient effectuées pour les systèmes significatifs et à chacune de leurs évolutions, accompagnées d'une vérification de la conformité des fournisseurs et de l'intégration de clauses contractuelles spécifiques ;

Que **la documentation technique, les notices et les rapports de conformité, avant déploiement, soient vérifiés et que des tests internes** soient réalisés sur des jeux de données représentatifs ; la gouvernance I.A. devant valider ensuite l'usage réel.

Pendant l'exploitation, il s'assurera enfin d'une supervision humaine qui enregistrera les décisions et gèrera les incidents. Enfin, il s'attachera à ce que la révision des politiques de sécurité et la formation continue garantissent dans la durée pour l'entreprise un usage éthique et responsable.



OBLIGATIONS SPECIFIQUES DES FOURNISSEURS DE SYSTEMES D'I.A. / FOURNISSEURS



Fournisseurs

Développant, entraînant, validant et mettant sur le marché des systèmes d'I.A., ils doivent assurer la conformité de ces systèmes avant vente selon les niveaux de risque défini par l'A.I. Act et garantir la qualité, la transparence et la robustesse de ceux-ci dans la durée. Leurs responsabilités portent sur le choix, le déploiement et la supervision de ces systèmes, ainsi que sur la communication des risques éventuels liés à leurs usages sur les opérateurs et la protection des données personnelles.

Cadre réglementaire et organisationnel des obligations du fournisseur

Règlement I.A.

- Acteur central du dispositif réglementaire, il fait face aux obligations de conformité et de transparence du système qu'il propose à ses utilisateurs.
- Il veille aux obligations renforcées pour les systèmes d'I.A. à haut risque (évaluation de conformité, documentation technique, surveillance post-commercialisation).
- Il respecte les obligations liées au R.G.P.D. en matière de minimisation des données personnelles collectées, garanties de leur confidentialité et de la prévention des risques de biais ou d'éventuelles discriminations algorithmiques.
- Il se base sur les Normes ISO/IEC 42001, 22989, 23053 et 23894 : référentiels indispensables à la conception, au développement et à la gestion du cycle de vie conformes des systèmes d'I.A.

Cadre organisationnel

- Il tient à jour une documentation technique complète, garde l'historique des modèles et assure la traçabilité des données et des tests, incluant les évaluations des biais.
- Il réalise, avant la mise sur le marché, des évaluations des risques, des tests de conformité et de sécurité, prépare la documentation nécessaire au marquage C.E. et procède aux certifications éventuelles.
- Il veille à ce que les bonnes pratiques incluent la tenue d'un registre interne des modèles, l'utilisation d'outils d'audit automatisé, la revue des projets avant production et la formation des équipes techniques et commerciales aux enjeux réglementaires.
- Il met en place, pendant la commercialisation, un plan de surveillance post-marché avec collecte, analyse des retours et incidents et mise à jour contrôlée des modèles opérationnels.
- Il s'assure que le support client est correctement fourni avec des clauses contractuelles précises et une documentation claire, garantissant assistance et conseils pour la conformité.
- Il fournit, en cas de besoin, les indicateurs attendus comprenant le pourcentage de modèles certifiés conformes, le nombre de projets audités et revus éthiquement, le délai moyen de résolution des incidents, le niveau de maturité de la gouvernance selon ISO 42001, ainsi que le taux de couverture de formation.



LES NOUVEAUX DEFIS JURIDIQUES POSES PAR L'IA AGENTIQUE

L'intelligence artificielle agentique désigne des systèmes capables, à partir d'un objectif général fixé par un utilisateur ou une organisation, de définir des sous-objectifs, de mobiliser des outils externes et d'enchaîner des actions avec une autonomie accrue.

Ce sont donc des agents d'IA qui vont au-delà de la fonction de recherches, d'optimisation ou d'assistance à la décision... et ont la capacité d'agir.

À la différence d'une IA générative classique, qui assiste l'utilisateur dans la production d'un contenu, l'agent IA intervient dans l'exécution même de la tâche : il peut rechercher, sélectionner, arbitrer, notifier, déclencher une opération, dialoguer avec des systèmes tiers et réaliser des actes qui auront une existence et des conséquences réelles.

La difficulté juridique naît précisément de ce passage d'une logique d'assistance à une logique d'action. L'IA provoque un changement d'échelle qui fragilise les catégories classiques du droit de la responsabilité, du droit des contrats et, plus largement, de la gouvernance des risques. Nous n'en sommes aux balbutiements de cette nouvelle étape de l'IA, mais des questions juridiques évidentes se posent déjà.

1 Qui décide ? — La question de la responsabilité et de l'imputabilité

La première question qui va se poser est celle de l'auteur juridique de la décision. Bien sûr, un agent IA ne dispose à ce jour d'aucune personnalité juridique, et ne peut donc pas être tenu responsable de ses actions, mêmes autonomes.

2 Qui engage l'entreprise ? — La question de la sécurité contractuelle

L'IA agentique soulève une difficulté classique en droit des contrats : dans quelle mesure les actes réalisés par le système peuvent-ils être valablement imputés à l'entreprise ?

Lorsque l'agent agit sans validation humaine continue, il devient plus difficile d'identifier avec certitude l'existence du consentement, son contenu exact et le moment auquel l'entreprise doit être regardée comme engagée. Plus l'autonomie opérationnelle du système est élevée, plus cette question devient centrale.

La question des habilitations deviendra centrale pour la bonne gouvernance des entreprises utilisant des agents IA : quels actes l'agent est-il autorisé à accomplir, dans quelles limites, selon quels seuils et sous quel contrôle ?



3 Qui contrôle et qui prouve ? — La question de la gouvernance, de la supervision et de la preuve

La troisième difficulté est d'ordre organisationnel et probatoire. Les systèmes agentiques accroissent les risques de défaut de transparence, tout en rendant la reconstitution de la chaîne décisionnelle plus complexe.

Dès lors, il devient d'autant plus essentiel de démontrer qu'un dispositif de gouvernance approprié existait ex ante : conditions de déploiement, périmètre d'autonomie, niveau de supervision humaine, modalités d'escalade, mécanismes d'arrêt, conservation des traces et auditabilité du système.

4 Qu'est-ce que l'agent met en danger autour de lui ? — La question des risques informationnels et systémiques

Enfin, l'agentique va exacerber certains risques déjà connus dans le domaine de l'IA, que ce soit en matière de données personnelles, de propriété intellectuelle ou de risques cyber. Ces systèmes supposent souvent un accès large à des données parfois sensibles, qu'ils peuvent analyser, combiner, stocker et transmettre ; il en résulte une multiplication des points de vulnérabilité.

La même logique vaut pour le secret des affaires et, plus largement, pour la circulation d'informations confidentielles dans des environnements techniques interconnectés.

Ces quelques points ne sont qu'un début de réflexion et n'ont pas encore de réponse claire en l'état de notre droit. Pourtant, ce ne sont pas les vides juridiques les plus dangereux... car on est déjà conscients de leur existence. Les éléments les plus critiques sont ceux dont nous ne sommes pas encore en mesure de soupçonner l'existence.



CONCLUSION

UN LIVRE BLANC QUI RESISTERA AUX EVOLUTIONS TECHNOLOGIQUES

Les intelligences artificielles (utilisons le pluriel eu égard à leur diversité) reposent sur des technologies évolutives. L'introduction de ce livre blanc montre bien que, depuis Dartmouth (1956), les IA ont connu, de l'IA symbolique (systèmes experts) à l'IA connectiviste (deep learning), une progression marquée par des sauts qualitatifs. « L'explosion » des systèmes d'IA est notamment due à la production de la data, à la puissance de calcul exaflopique, aux progrès des semi-conducteurs, grâce auxquels les IA sont sorties de leurs « hivers ». En 2022, ChatGpt ouvre la voie de l'IA générative, mais on sait déjà que ce n'est qu'une étape.

Depuis 2025, l'IA agentique est devenue un sujet récurrent, tant elle ne se limite pas à la seule production de contenus à partir de LLM. Cette IA est dynamique, interagit avec des systèmes réels, planifie, prend des décisions, a une autonomie opérationnelle habituellement réservée aux humains. Le Français Yann Le Cun, Prix Alan Turing pour ses travaux, rêve déjà d'un modèle « mondial » qui ferait son apprentissage dans le monde réel, comme un enfant apprend par l'expérience. Certains annoncent l'arrivée proche d'une super IA, surpassant l'intelligence humaine.

Dans ce contexte, ce livre blanc n'est-il pas déjà dépassé ou sur le point de l'être, la « photo instantanée » étant supplantée par un film dont on ne connaît pas la fin ? C'est toute la difficulté de l'exercice mené avec talent par une équipe pluridisciplinaire. En vérité, il n'en est rien ! Le législateur européen a eu la sagesse de ne pas s'appuyer sur les technologies pour réglementer l'usage des IA. Il a choisi la notion de risque qui détermine les usages interdits, ceux qui nécessitent un encadrement plus ou moins contraignant (systèmes à haut risque, à risque modéré, limité), et ceux qui n'appellent pas d'attention particulière. Cette approche est neutre au regard des évolutions technologiques. Les IA agentiques ne sont pas une catégorie juridique nouvelle ; elles ouvrent sur des cas d'usage qui peuvent être à haut risque (RH, crédit, santé, infrastructures, etc.) ou à risque minime. Tout repose sur la gouvernance, celle des organisations, des comportements, des contrôles. Supervision, traçabilité, gestion des risques doivent être au coeur d'une gouvernance par le COMEX. La conformité n'est pas une option, mais un choix stratégique qui engage la responsabilité des dirigeants. Le règlement AI Act évoluera sans doute mais il offre aujourd'hui un cadre solide pour structurer la gouvernance de l'IA à l'ère des agents.



CONCLUSION

Ce livre blanc emprunte la souplesse du règlement européen. Il clarifie les responsabilités, offre aux dirigeants une méthode qui n'est pas sujette à l'érosion du temps. Il est publié au bon moment, alors que l'automatisation soulève des questions nouvelles, relatives à l'autonomie et à la place de l'humain, qui vont bouleverser la vie des entreprises, des administrations, susciter une quête de sens. Le titre du rapport de Cédric Villani (2018) « Donner du sens à l'intelligence artificielle » est explicite. Au-delà de sa forme proche d'un mémento, le livre blanc contribue à une réflexion plus globale, plus philosophique, plus existentielle : l'humain sera-t-il encore maître de son destin numérique ? Sans gouvernance, on peut en douter. Avec elle on peut aborder l'avenir avec plus de sérénité.



Général d'armée (2S) WATIN-AUGOUARD
Fondateur du Forum INCYBER



ANNEXE 1 - GLOSSAIRE

Apprentissage automatique (Machine Learning) : Méthode permettant à une machine d'identifier des régularités dans des données pour effectuer des prédictions ou prendre des décisions, sans être explicitement programmée pour chaque cas.

Apprentissage profond (Deep Learning) : Branche avancée du Machine Learning utilisant des réseaux de neurones à plusieurs couches pour analyser des données complexes (images, sons, langage).

Biais algorithmique : Distorsion dans les décisions d'un système d'I.A. causée par des données d'entraînement incomplètes, non représentatives ou biaisées. Peut conduire à des discriminations involontaires.

Boîte noire : Terme désignant un système d'I.A. dont le fonctionnement interne est difficilement compréhensible, même pour ses concepteurs. Cela limite l'explicabilité et le contrôle.

Chatbot (ou Agent conversationnel) : Application logicielle axée sur l'IA qui prend part à des conversations humaines de manière naturelle.

Entraînement (d'un modèle d'I.A.) : Phase durant laquelle un algorithme "apprend" à partir d'un grand ensemble de données. C'est à ce stade que les paramètres internes sont ajustés.

Explicabilité : Capacité à comprendre et expliquer le fonctionnement d'un système d'I.A., ses critères de décision et ses résultats. Clé pour la transparence, la responsabilité et la confiance.

Prolog : langage de programmation déclaratif qui facilite les tâches de calcul symboliques et non numériques dans le domaine de l'I.A.

Responsabilité algorithmique : Principe selon lequel les entreprises doivent pouvoir justifier et assumer les décisions prises par ou avec un système d'I.A.. S'applique notamment dans les cas d'erreurs ou de litiges.

Souveraineté numérique : Capacité d'un acteur à contrôler les données, les infrastructures et les technologies qu'il utilise, sans dépendre exclusivement de prestataires extérieurs.

Supervision humaine : Principe selon lequel l'humain conserve un contrôle effectif sur les décisions prises par un système d'I.A., notamment pour les applications critiques (validation finale, capacité d'interruption).

Système à haut risque (selon l'A.I. Act) : Système d'I.A. dont l'usage peut affecter les droits fondamentaux, la sécurité ou la vie des individus (ex. : diagnostic médical, recrutement, scoring bancaire). Soumis à des obligations réglementaires renforcées

Transparence algorithmique : Obligation d'informer les utilisateurs qu'un système d'I.A. est en jeu, et de documenter le fonctionnement de ce système pour les autorités, les partenaires ou les usagers.



ANNEXE 2 - ARCHITECTURES ET TYPOLOGIES

LES GRANDES FAMILLES D'I.A.

- I.A. symbolique : basée sur des règles logiques écrites par des humains (ex. : systèmes experts).
- Machine Learning : apprend à partir de données (ex. : reconnaître un visage).
Deep Learning : sous-catégorie du ML, utilisant des réseaux de neurones profonds (ex. : ChatGPT, DALLÉ).
- I.A. générative : produit du contenu nouveau (texte, image, son...).il est lui-même un type de deep learning spécialisé.
- I.A. conversationnelle : dialogue avec les humains (chatbots, assistants vocaux) basé sur de l'I.A. générative.
- I.A. hybride : combine plusieurs approches (symbolique + machine learning + deep learning).

AUTRES TYPOLOGIES UTILES

- I.A. supervisée : entraînée avec des données étiquetées.
- I.A. non supervisée : découvre seule des structures dans les données.
- I.A. par renforcement : apprend par essais-erreurs dans un environnement.
- I.A. auto-supervisée : génère ses propres tâches d'apprentissage.

Repère conceptuel : familles fonctionnelles vs typologies techniques

Les familles fonctionnelles d'I.A. (symbolique, machine learning, générative) décrivent les finalités et les comportements des systèmes : raisonnement logique, modélisation probabiliste, création autonome.

Les typologies techniques d'apprentissage (supervisée, non supervisée, par renforcement, auto-supervisée) décrivent les méthodes utilisées pour entraîner ces systèmes. Ces deux dimensions sont complémentaires : une même famille fonctionnelle peut recourir à plusieurs typologies techniques selon les objectifs et les données disponibles.

Architectures et techniques fondamentales

Pour éclairer les usages professionnels et les décisions d'intégration stratégique, il est utile de présenter les principales architectures sous-jacentes telles que les réseaux de neurones convolutifs (CNN), les modèles séquentiels comme les RNN, LSTM ou GRU, les Transformers ou encore les modèles de génération augmentée (RAG).

Chacune apporte des capacités distinctes selon les types de données traités, les objectifs métiers et les contraintes techniques.



Nom	Type / Famille	Usage principal
MLP (Multi-Layer Perceptron)	Réseau de neurones classique	Données tabulaires, classification, régression
CNN (Convolutional Neural Network)	Deep Learning – vision	Analyse d'images, vidéos, reconnaissance visuelle
RNN (Recurrent Neural Network)	Deep Learning – séquences	Traitement de séquences, séries temporelles
LSTM (Long Short-Term Memory)	Variante de RNN	Alternative plus légère au LSTM
RAG (Retrieval-Augmented Generation)	I.A. générative + recherche	I.A. conversationnelle avec accès à des bases documentaires
Fine-Tuning	Technique d'adaptation	Personnalisation de modèle préentraîné



AUTRES ARCHITECTURES D'I.A. À CONNAITRE

Architecture / Technique	Catégorie	Usage principal
Transformers BERT / RoBERTa / DistilBERT	Deep Learning Transformers optimisés	NLP, vision, audio, I.A. générative Compréhension du langage, classification
GPT / LLaMA / Mistral	Generative Transformers	Génération de texte, code, dialogue
ViT (Vision Transformer)	Transformer pour images	Reconnaissance visuelle, segmentation
Swin Transformer	Vision adaptative	Vision multi-échelle, traitement vidéo
Diffusion Models	I.A. générative	Génération d'images (ex : DALL·E 2, Stable Diffusion)
Autoencoders	Apprentissage non supervisé	Compression, dé-bruitage, génération
GAN (Generative Adversarial Network)	I.A. générative	Création d'images réalistes, deepfakes
Capsule Networks	Réseaux neuronaux avancés	Reconnaissance d'objets avec relations spatiales
NeRF (Neural Radiance Fields)	I.A. 3D	Reconstruction 3D à partir d'images 2D
Spiking Neural Networks	I.A. sur graphes	Modélisation du cerveau, I.A. embarquée
Graph Neural Networks (GNN)	I.A. générative	Recommandation, réseaux sociaux, chimie
Mixture of Experts (MoE)	Architecture distribuée	Scalabilité, spécialisation de modèles
Edge A.I. architectures	I.A. embarquée	Optimisation pour appareils mobiles ou IoT



ANNEXE 3 - CARTOGRAPHIE DES USAGES PROFESSIONNELS ET FICHES MÉTIERS

Une fois les fondements techniques et conceptuels de l'intelligence artificielle posés, il devient essentiel d'en illustrer les applications concrètes à travers des cas d'usage représentatifs.

Ces exemples, issus de secteurs variés tels que la Santé, la Finance ou les Ressources Humaines, permettent aux décideurs d'appréhender les opportunités offertes par l'I.A., tout en identifiant les responsabilités, les points d'alerte et les obligations de l'entité traitante.

FICHE METIER 1 : RECRUTEMENT AUTOMATISE

Contexte : Une entreprise utilise un outil d'I.A. pour trier les CV et présélectionner les candidats.

Points d'alerte

- Système d'I.A. à haut risque nécessitant une évaluation de la conformité avant son déploiement
- Risque de biais discriminant dans les critères algorithmiques (noms, origine, sexe, ethnie etc.)
- Supervision humaine potentiellement opaque voire absente

Obligations de l'entreprise

- Réaliser une analyse d'impact sur les droits fondamentaux (article 27 AI Act) Information des candidats sur les critères de sélection utilisés par l'outil (article 13 RGPD)
- Permettre au candidat de demander le réexamen de sa candidature par une personne humaine (article 22 RGPD)

FICHE METIER 2 : DIAGNOSTIC MEDICAL ASSISTE PAR I.A.

Contexte : Un hôpital utilise une I.A. pour aider au diagnostic d'images médicales.

Points d'alerte

- Système d'I.A. à haut risque, avec impact sur la vie humaine
- Données sensibles sur la santé d'une personne, exposées à des failles de cybersécurité
- Risque de dépendance excessive à l'algorithme sans validation humaine



Obligations de l'hôpital

- Assurer que la décision finale est prise par un médecin (article 14 AI Act)
- Garantir la robustesse et la fiabilité du système (article 15 AI Act)
- Réaliser une analyse d'impact sur les droits fondamentaux (article 27 AI Act)

FICHE METIER 3 : RECOMMANDATIONS PERSONNALISEES (E-COMMERCE)

Contexte : Un site propose des produits en fonction du comportement de navigation.

Points d'alerte

- Manque de transparence auprès du consommateur
- Pratiques interdites : Manipulation du consommateur par des nudges psychologiques trompeurs ; inférence de données sensibles – orientations sexuelles, appartenance religieuse, ethnique – à partir des comportements d'achat

Obligations du commerçant

- Informer le consommateur sur le profilage et lui offrir une alternative sans personnalisation (article 13 RGPD)
- Contrôler que l'algorithme ne produit aucun biais discriminatoire, ni ne recourt à des techniques trompeuses (article 5 AI Act)

FICHE METIER 4 : TUTORAT INTELLIGENT (ÉDUCATION)

Contexte : Une plateforme d'apprentissage adapte les contenus selon le niveau de l'élève.

Points d'alerte

- Contenu proposé à l'élève sur la base de son orientation sexuelle, appartenance religieuse, ethnique, son handicap etc.
- Collecte continue et traitement de données personnelles sur l'apprenant (niveau, résultats, comportements)

Obligations de l'éditeur

- Assurer que l'algorithme ne produit aucun biais discriminatoire (article 5 AI Act)
- Garantir un niveau de sécurité adapté au risque (article 32 RGPD)



FICHE METIER 5 : SCORING DE CREDIT AUTOMATISE (BANQUE)

Contexte : Une banque utilise l'I.A. pour évaluer la solvabilité d'un client.

Points d'alerte

- Système d'I.A. à haut risque affectant la situation financière et sociale d'une personne
- Risques d'octroi de crédits sur la base de biais discriminant dans les critères algorithmiques (âge, genre, origine ethnique ou sociale etc.)

Obligations de la banque

- Réalisation d'une analyse d'impact sur les droits fondamentaux (article 27 AI Act)
- Assurer que l'algorithme ne produit aucun biais discriminatoire (article 5 AI Act)
- Justifier les critères utilisés auprès du client et lui garantir un droit de réexamen par une personne humaine (article 22 RGPD)

FICHE METIER 6 : SECURITE ET DETECTION DE FRAUDE

Contexte : Utilisation de l'I.A. pour détecter des comportements suspects ou des fraudes (paiements, accès, documents falsifiés).

Point d'alerte

- Risque de collecte massive de données à caractère personnel sensibles des employés
- Risque de fuite de données confidentielles de l'entreprise

Obligations de l'entreprise

- Informer les employés et recueillir leur consentement au traitement de leurs données à caractère personnel (articles 6 et 9 RGPD)
- Assurer que l'outil utilisé ne compromet pas la sécurité ni la confidentialité des informations de l'entreprise



ANNEXE 4 - OBLIGATIONS APPLICABLES AUX SYSTÈMES À HAUT RISQUE/ MODÉRÉS / LIMITÉS

1 DOCUMENTATION TECHNIQUE

Nécessité de mettre en place une documentation technique complète, des procédures de gestion des risques, de garantir la traçabilité, la transparence et la robustesse des systèmes d'I.A., ainsi qu'un contrôle humain effectif sur les décisions prises par l'I.A.

2 ANALYSE D'IMPACT SUR LES DROITS FONDAMENTAUX

Identifier les effets potentiels sur la vie privée, la non-discrimination... et les mesures prises pour réduire ces risques.

3 S'ASSURER DE LA QUALITE DES DONNEES

Les données d'entraînements doivent être représentatives, pertinentes, non biaisées. Un suivi de la qualité des données doit être effectué tout au long du cycle de vie du système d'I.A. Toute donnée utilisée doit en tout point respecter les droits d'auteurs, de propriété intellectuelle et le R.G.P.D.

4 SUPERVISION HUMAINE

Mécanismes pour permettre à des humains d'intervenir, d'interrompre ou de superviser le système. Ex : validation humaine obligatoire dans les décisions critiques (comme un refus de prêt bancaire).

5 TRANSPARENCE ET TRAÇABILITE

Explication claire du fonctionnement du système pour les utilisateurs et auditeurs. Journalisation des opérations, logs d'utilisation.

6 ROBUSTESSE ET CYBERSECURITE

Résistance aux erreurs, attaques ou manipulations. Test et validation rigoureux avant déploiement.

7 DECLARATION DE CONFORMITE ET MARQUAGE CE

Une déclaration de conformité et un marquage CE sont obligatoires avant toute mise sur le marché ou déploiement.



Ci-joint un tableau de synthèse des différentes obligations selon le niveau de risque.

Obligations	I.A. à risques élevés	I.A. à risques modérés	I.A. à risques limités
Protection des données personnelles	OUI	OUI	OUI
Minimisation des biais	OUI	OUI	OUI
Avertissement aux utilisateurs qu'une I.A. est utilisée	OUI	OUI	OUI
Documentation : explicabilité du fonctionnement de l'I.A.	OUI	Recommandé	Recommandé
Documentation : explicabilité des choix de l'I.A.	OUI	Recommandé	Recommandé
Gestion continue : mécanismes pour surveiller et ajuster le système tout au long du cycle de vie du système	OUI	Recommandé	Recommandé
Consentement explicite des utilisateurs sur les données autres que personnelles	OUI	Recommandé	NON
Évaluation préalable des risques (impacts droits fondamentaux, sécurité, santé, conséquences éthiques)	OUI	Recommandé	NON
Journaux pour les décisions de l'I.A.	OUI	Recommandé	NON
Qualité des données pour éviter les biais	OUI	NON	NON
Vérifier les biais discriminatoires en les contrôlant	OUI	NON	NON
Contrôle humain, pas d'autonomie totale	OUI	NON	NON
Évaluation de conformité via audits externes	OUI	NON	NON
Mécanismes pour pouvoir signaler les incidents aux autorités	OUI	NON	NON



ANNEXE 5 - EXEMPLES D'APPLICATIONS DE BONNES PRATIQUES DANS LE DOMAINE DU NUMÉRIQUE POUR LA GESTION DES DOCUMENTS ET DES DONNÉES

Gestion des données : confidentialité et sécurité

- Anonymisation et pseudonymisation : utiliser des techniques d'anonymisation robustes pour les données sensibles (R.G.P.D.), surtout lors de l'entraînement de modèles d'I.A. sur des documents internes ou clients.
- Chiffrement et accès contrôlé : protéger les documents et bases de données par chiffrement et limiter l'accès aux seuls acteurs autorisés.
- Minimisation des données : ne collecter et conserver que les données strictement nécessaires et supprimer les données obsolètes.
- Traitement automatisé des documents : transparence et équité
- O.C.R. et extraction de données : vérifier que les outils d'O.C.R. (reconnaissance optique de caractères) et d'extraction de données ne reproduisent pas de biais (ex : reconnaissance moins efficace pour certaines langues ou écritures).
- Classification : auditer régulièrement les algorithmes de classification pour éviter les erreurs (ex : documents juridiques mal classés à cause d'un biais linguistique).
- Explicabilité des décisions : documenter et expliquer les critères utilisés par l'I.A. pour classer, archiver ou supprimer des documents.

Archivage et conservation : conformité et durabilité

- Respect des délais légaux : automatiser la gestion des durées de conservation conformément aux réglementations sectorielles (ex : 10 ans pour les documents fiscaux en France).

Collaboration et partage : éthique et traçabilité

- Respect des droits d'auteur : vérifier que les documents utilisés pour entraîner des modèles d'I.A. respectent les droits d'auteur et les licences.

Le tableau ci-dessous récapitule les principales recommandations concrètes en matière de bonnes pratiques dans l'utilisation des outils

Usage	Outil/Pratique responsable
Extraction de données	Utiliser des modèles d'I.A. open source et auditables (ex : Hugging Face) pour éviter les boîtes noires.
Archivage intelligent	Automatiser l'archivage avec des règles claires et documentées, en conformité avec le R.G.P.D.
Recherche documentaire	Intégrer des filtres éthiques pour éviter la diffusion de contenus sensibles ou discriminants.





eFutura

Association pour la Transition Numérique

www.efutura.fr