# Guide de mise en œuvre de l'*AI Act*

## Partie 1 : Obligations

### 1.2 Recueil de notes thématiques sur les principaux enjeux juridiques

Cigref
RÉUSSIR LE NUMÉRIQUE

numeum
Engager le numérique

# Introduction

Ce recueil de notes thématiques a pour objectif de fournir aux praticiens du numérique une vision claire et concise des principaux enjeux juridiques liés au règlement (UE) 2024/1689 sur l'intelligence artificielle (IA) (également désigné « *AI Act* ») en abordant les points d'attention spécifiques utiles à connaître sur chacun des sujets suivants :

- ***la propriété intellectuelle*** : défis liés au respect des droits de propriété intellectuelle existants, aux obligations de transparence et à l'exigence de la publication d'un « *résumé suffisamment détaillé* » pour les fournisseurs de modèles d'IA à usage général ;
- ***le secret d'affaires / la confidentialité*** : préservation des informations sensibles, qu'il s'agisse de secrets professionnels ou de secrets d'affaires ;
- ***la protection des données*** : personnelles ou non ;
- ***la cybersécurité*** : bonnes pratiques pour garantir la sécurité des systèmes d'IA et prévenir les cybermenaces.

Ce présent livret sur les principaux enjeux juridiques vient compléter la « Cartographie des obligations applicables aux organisations » (partie 1.1 du « Guide de mise en œuvre de l'*AI Act* »).

Pour rappel, le « *Guide de mise en œuvre de l'AI Act* » est composé de plusieurs parties indépendantes et complémentaires :

***Points clés de l'AI Act – Introduction***

***Partie 1 – Obligations***

- Cartographie des obligations applicables aux organisations selon l'*AI Act*, en fonction de la nature de l'IA, de son niveau de risque, et de la place de l'organisation dans la chaîne de valeur
- Recueil de notes thématiques sur les principaux enjeux juridiques

***Partie 2 – Gouvernance***

- Mode d'emploi et outils pour mettre en place une gouvernance

***Partie 3 – Contrats et responsabilité***

- Identification des responsabilités et mise en place des contrats adéquats

Une ***annexe*** permettra de lister des recommandations et mesures à mettre en place, de traduire opérationnellement les obligations légales, et enfin de présenter quelques cas pratiques pour faciliter la compréhension.

# Table des matières

# 1. Propriété intellectuelle et intelligence artificielle

L'objet principal de l'*AI Act* n'est pas de réglementer la protection du droit d'auteur. Néanmoins, l'*AI Act* impose certaines obligations de transparence spécifiques en matière de propriété intellectuelle.

Cette fiche a pour objectif d'aider les praticiens à identifier leurs obligations en matière de propriété intellectuelle dans le cadre de l'*AI Act* (**1.1.**) et met en lumière les exigences essentielles relatives à la propriété intellectuelle (**1.2.**). Elle présente également les enjeux spécifiques de propriété intellectuelle liés aux intelligences artificielles génératives (IAG), en dehors du périmètre de l'*AI Act* (**1.3.**) et liste des bonnes pratiques pouvant être adoptées (**1.4.**).

## 1.1. La propriété intellectuelle au sein de l'*AI Act*

Les références à la propriété intellectuelle dans l'*AI Act* sont limitées : le « *droit d'auteur* » est mentionné une petite quinzaine de fois, les « *droits d'auteur* » 1 seule fois, les « *droits voisins* » 4 fois et la « *propriété intellectuelle* » seulement 8 fois. Seuls, quelques articles abordent véritablement ces sujets :

### 1.1.1 Droit d'auteur et droits voisins

- Article 53, paragraphe 1, c) : « *1. Les fournisseurs de modèles d'IA à usage général : […] c) mettent en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins, et notamment à identifier et à respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790* »

### 1.1.2 Propriété intellectuelle

- Article 25, paragraphe 5 : « *Les paragraphes 2 et 3 [qui traitent des responsabilités tout au long de la chaîne de valeur de l'IA] sont sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle, les informations confidentielles de nature commerciale et les secrets d'affaires conformément au droit de l'Union et au droit national.* »
- Article 52, paragraphe 6 : « *La Commission veille à ce qu'une liste des modèles d'IA à usage général présentant un risque systémique soit publiée et tient cette liste à jour, sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national.* »
- Article 53, paragraphe 1, b) : « *1. Les fournisseurs de modèles d'IA à usage général : […] b) élaborent, tiennent à jour et mettent à disposition des informations et de la documentation à l'intention des fournisseurs de systèmes d'IA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs systèmes d'IA. Sans préjudice de la nécessité d'observer et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national, ces informations et cette documentation* »
- Article 78, paragraphe 1, a) : « *1. La Commission, les autorités de surveillance du marché et les organismes notifiés, ainsi que toute autre personne physique ou morale associée à*

*l'application du présent règlement respectent, conformément au droit de l'Union ou au droit national, la confidentialité des informations et des données obtenues dans l'exécution de leurs tâches et activités de manière à protéger, en particulier: a) les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires des personnes physiques ou morales, y compris le code source, à l'exception des cas visés à l'article 5 de la directive (UE) 2016/943 du Parlement européen et du Conseil* »

- Annexe VII, paragraphe 4.5 : « *Lorsque cela est nécessaire pour évaluer la conformité du système d'IA à risque élevé avec les exigences énoncées au chapitre III, section 2, après que tous les autres moyens raisonnables de vérifier la conformité ont été épuisés et se sont révélés insuffisants, et sur demande motivée, l'accès aux modèles d'entraînement et aux modèles entraînés du système d'IA, y compris à ses paramètres pertinents, est aussi accordé à l'organisme notifié. Cet accès est soumis au droit de l'Union existant en matière de protection de la propriété intellectuelle et des secrets d'affaires.* »

## 1.2. Les obligations spécifiques en matière de propriété intellectuelle au sein de l'*AI Act*

Plusieurs obligations sont explicitement mentionnées[1]. En effet, l'*AI Act* prévoit en son article 53 l'obligation pour les fournisseurs de modèles d'IA à usage général de prendre des mesures visant à respecter le droit d'auteur et, notamment, le cadre posé par la directive (UE) 2019/790 du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique (DAMUN).

Au cœur de ces mesures, figure l'obligation, pour les fournisseurs, d'élaborer et de rendre disponible publiquement « *un résumé suffisamment détaillé* »[2] des données utilisées pour entraîner le modèle d'IA à usage général. Cette transparence sur les sources devrait, en principe, permettre aux titulaires de droits d'auteur et de droits voisins de vérifier que les conditions d'accès licite et d'utilisation de leurs œuvres et prestations ont été respectées (et permettre, le cas échéant, la mise en œuvre de leur opposition à toute fouille de données, c'est-à-dire leur « *opt-out* »[3]).

Cette obligation s'appliquera douze mois après l'entrée en vigueur du règlement (soit le 2 août 2025). C'est le Bureau de l'IA, créé par une décision de la Commission européenne du 24 janvier 2024, qui sera chargé d'élaborer un modèle de résumé simple et efficace des données d'entraînement utilisées par les IA. La description des types d'informations à fournir ne sera pas disponible avant le printemps 2025. L'obligation de respecter le droit d'auteur, et de fournir ce résumé, s'appliquera aux fournisseurs d'IA proposant des modèles dans l'UE, peu importe le lieu d'entraînement de ces modèles.

Par ailleurs, le gouvernement a confié **deux missions** sur le droit d'auteur au Conseil supérieur de la propriété littéraire et artistique (CSPLA) :

[1] Article 53 de l'AI Act intitulé « *Obligations incombant aux fournisseurs de modèles d'IA à usage général* ».

[2] Article 53, paragraphe 1, d) : « *Les fournisseurs de modèles d'IA à usage général : […] d) élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle d'IA à usage général, conformément à un modèle fourni par le Bureau de l'IA.* »

[3] L'exception de fouille de textes et de données (*Text and Data mining*) figure à l'article 4, paragraphe 3 de la directive (UE) 2019/790 : https://eur-lex.europa.eu/eli/dir/2019/790/oj et à l'article L122-5-3 du Code de la propriété intellectuelle : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044363192

- la première mission, relative à la mise en œuvre du règlement européen établissant des règles harmonisées sur l'intelligence artificielle[4] : dans le cadre de cette première mission le CSPLA a (i) expertisé la portée de l'obligation de transparence et (ii) établi la liste des informations paraissant devoir nécessairement être communiquées selon les secteurs culturels concernés, pour permettre aux auteurs et aux titulaires de droits voisins d'exercer leurs droits.

  Le rapport de cette mission, publié le 11 décembre 2024, propose un « *résumé détaillé* »[5] du contenu utilisé pour l'entraînement des modèles d'IA à usage général[6]. Ce rapport recommande une « *approche par type de contenus, avec un degré de détail croissant* » selon que les contenus sont libres de droit ou plus sensibles. L'objectif est de permettre l'exercice des droits, le résumé devrait être « *complet en termes de contenu* » sans pour autant révéler les techniques utilisées. En sus, le modèle de résumé devrait aussi intégrer la politique de conformité exigée par l'article 53§1 c), en particulier concernant l'exercice du droit d'« *opt-out* » issu de l'article 4 de la directive (UE) 2019/790 du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique (« *Damun* »).

- l'autre mission, relative à la rémunération des contenus culturels utilisés par les systèmes d'intelligence artificielle[7] : dans le cadre de cette deuxième mission le CSPLA va (i) analyser les enjeux économiques sous-jacents à l'accès aux données protégées par des droits de propriété littéraire et artistique lorsque celles-ci sont utilisées par les IA et (ii) examiner les mécanismes juridiques envisageables pour chaque secteur, afin de garantir aux ayants droit l'effectivité de leurs droits lors de l'utilisation des œuvres par les fournisseurs d'IA. Les conclusions de ce rapport seront présentées courant 2025[8].

---

[4] CSPLA, « *Le CSPLA lance une mission relative à la mise en œuvre du règlement européen établissant des règles harmonisées sur l'intelligence artificielle* », 17 avril 2024 : https://www.culture.gouv.fr/Nous-connaitre/Organisation-du-ministere/Conseil-superieur-de-la-propriete-litteraire-et-artistique-CSPLA/Travaux-et-publications-du-CSPLA/Missions-du-CSPLA/avril-2024-le-cspla-lance-une-mission-relative-a-la-mise-en-aeuvre-du-reglement-europeen-etablissant-des-regles-harmonisees-sur-l-intelligence-art

[5] Conseil supérieur de la propriété littéraire et artistique (CSPLA), Rapport de mission relative à la mise en œuvre du règlement européen établissant des règles harmonisées sur l'intelligence artificielle (« *template* »), 11 décembre 2024 : https://www.culture.gouv.fr/fr/nous-connaitre/organisation-du-ministere/Conseil-superieur-de-la-propriete-litteraire-et-artistique-CSPLA/Travaux-et-publications-du-CSPLA/Missions-du-CSPLA/ia-et-transparence-des-donnees-d-entrainement-publication-du-rapport-d-alexandra-bensamoun-sur-la-mise-en-aeuvre-du-reglement-europeen-etablissant

[6] Pour rappel, l'article 53§1 c) oblige les fournisseurs de modèles d'IA à usage général à mettre en œuvre des mesures visant à respecter le droit d'auteur et les droits voisins. L'*AI Act* impose également à ces derniers d'élaborer et de rendre publiquement disponible un « *résumé suffisamment détaillé* » des donnés ayant servi à l'entraînement de leur modèle (article 53§1 d).
À noter que le « *résumé suffisamment détaillé* » proposé par le CSPLA reste une simple suggestion. Il faudra donc attendre la publication du résumé officiel de la Commission pour évaluer sa portée exacte et les obligations qui en découleront pour les acteurs concernés.

[7] CSPLA, « Le CSPLA lance une mission relative à la rémunération des contenus culturels utilisés par les systèmes d'intelligence artificielle », 17 avril 2024 : https://www.culture.gouv.fr/Nous-connaitre/Organisation-du-ministere/Conseil-superieur-de-la-propriete-litteraire-et-artistique-CSPLA/Travaux-et-publications-du-CSPLA/Missions-du-CSPLA/avril-2024-le-cspla-lance-une-mission-relative-a-la-remuneration-des-contenus-culturels-utilises-par-les-systemes-d-intelligence-artificielle

[8] À noter que deux notes d'étape juridique et économique ont été présentées lors de la séance plénière du 9 décembre 2024 : https://www.culture.gouv.fr/nous-connaitre/organisation-du-ministere/Conseil-superieur-de-la-propriete-litteraire-et-artistique-CSPLA/Travaux-et-publications-du-CSPLA/Missions-du-CSPLA/mission-relative-a-la-remuneration-des-contenus-culturels-utilises-par-les-systemes-d-intelligence-artificielle

## 1.3. La propriété intellectuelle et l'IA générative (hors *AI Act*)

Indépendamment de l'*AI Act*, les intelligences artificielles génératives (IAG) suscitent de nombreuses interrogations en matière de propriété intellectuelle.

### 1.3.1 Sur le droit d'auteur

Au niveau mondial, plusieurs décisions ont déjà tranché la question relative à la protection d'une œuvre générée par une IAG :

- ***US Copyright Office*, 21 février 2023 – Affaire « *Zarya of the Dawn* »**[9] : un déposant sollicitait la protection par le droit d'auteur d'un *comics* créé à l'aide du logiciel *Midjourney*. L'USPTO a conclu que le *comics* composé d'un texte rédigé par l'homme et combiné à des images générées par *Midjourney* constituait une œuvre protégeable par le droit d'auteur, mais que les images individuelles elles-mêmes ne pouvaient pas être protégées par le droit d'auteur[10].
- ***US District Court for the District of Columbia*, 18 août 2023, Stephen Thaler v. Shira Perlmutter, n°22-1564 (BAH)**[11] : un plaignant possède un système informatique *Creativity Machine* qui, selon lui, a généré une œuvre de son propre chef. Il a cherché à enregistrer l'œuvre pour obtenir un droit d'auteur, en citant le système informatique comme auteur et en expliquant que le droit d'auteur devrait lui être transféré en tant que propriétaire du système informatique. La question était de savoir si une œuvre générée exclusivement par un système d'IA sans intervention humaine devrait être éligible au droit d'auteur. La Cour a apporté une réponse négative sans équivoque : « *Must that originator be a human being to claim copyright protection ? The answer is yes* ».
- ***Beijing internet court, Civil Judgment*, 27 novembre 2023, (2023) Beijing 0491 Republic of China No. 11279**[12] **:** un plaignant, ayant utilisé une intelligence artificielle pour créer des images qu'il a ensuite partagées sur une plateforme, a découvert qu'un défenseur avait intégré ces créations dans un article qu'il a publié. Cette situation a conduit le plaignant à engager une action en justice. Compte tenu de la précision des « *prompts* » ayant permis de générer l'image en question, la Cour a estimé que le demandeur avait apporté la preuve d'un investissement intellectuel suffisant pour revendiquer la titularité d'un droit d'auteur sur les œuvres.
- **Cour d'Internet de Guangzhou, 8 février 2024, SCLA c./ Tab. :** la Cour d'Internet de Guangzhou, en Chine, a retenu la responsabilité d'un fournisseur de services d'IA générative dans la contrefaçon des œuvres japonaises *Ultraman*. Ce fournisseur a été condamné pour avoir manqué à son devoir de vigilance, imposé à tous les prestataires de services d'IA générative, en enfreignant les droits de propriété intellectuelle.
- **Tribunal judiciaire de Changshu, Province du Jiangsu, 28 octobre 2024, Décision n° (2024) Su 0581 Min Chu 6697, M. Lin c/ Gaosi et Qin Hong** : Le demandeur, M. Lin, a créé l'image

[9] *United States Copyright Office, February 21, 2023, Zarya of the Dawn (Registration # VAu001480196)* : https://www.copyright.gov/docs/zarya-of-the-dawn.pdf

[10] À noter que l'USPTO a depuis fourni des lignes directrices énonçant sa doctrine : https://www.copyright.gov/ai/ai_policy_guidance.pdf

[11] *US District Court for the District of Columbia*, 18 août 2023, *Stephen Thaler v. Shira Perlmutter, n°22-1564 (BAH)* : https://law.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2022cv01564/243956/24/

[12] *Beijing internet court, Civil Judgment*, 27 novembre 2023, *(2023) Beijing 0491 Republic of China No. 11279* : https://mp.weixin.qq.com/s/Wu3-GuFvMJvJKJobqqq7vQ

*Coeur à cœur* à l'aide des logiciels *Midjourney* et *Photoshop*, puis l'a enregistrée auprès des autorités compétentes.
Une société intitulée « *Gaosi* » a conçu un ballon en forme de cœur, intégré à un projet commercial de Qin Hong, pour attirer des visiteurs et promouvoir le projet via des publications sur WeChat. Entre septembre 2023 et janvier 2024, Gaosi a diffusé des vidéos et images de l'installation sur Xiaohongshu et son site officiel. Malgré des différences mineures, la structure reproduit substantiellement l'œuvre de M. Lin, qui dénonce une violation de ses droits d'auteur. Le tribunal reconnaît la protection de l'œuvre au titre du droit d'auteur, tout en rappelant que l'originalité est essentielle à sa qualification. Il condamne les défendeurs pour atteinte au droit de communication au public, mais limite l'indemnisation en raison de l'originalité jugée faible et du caractère modéré de l'atteinte.

Au-delà de la protection des œuvres générées par l'IAG, la question de la titularité des droits demeure centrale. À ce jour en France, aucun texte ni aucune jurisprudence ne permet de déterminer précisément à qui appartiennent ces droits lorsque l'IAG est utilisée dans le processus de création.

Dans ce contexte, les utilisateurs d'IAG doivent veiller à plusieurs points :

- **Analyser attentivement les conditions générales d'utilisation (CGU) des outils d'IAG**[13], notamment les clauses de propriété intellectuelle précisant les droits relatifs aux instructions données par l'utilisateur via les *prompts* et aux données de sortie, *outputs*.
- **Documenter le processus créatif**, en apportant des preuves de leur intervention humaine : par exemple, la complexité et le temps passé sur les *prompts* (nombre d'heures de travail), ou encore les étapes post-création telles que l'utilisation de logiciels de retouches.

### 1.3.2 Sur la propriété industrielle

- **Publication de lignes directives par l'Administration nationale chinoise de la propriété intellectuelle (CNIPA) relatives aux demandes de brevet pour des inventions liées à l'intelligence artificielle**[14] : le 6 décembre 2024, la CNIPA a publié des lignes directrices pour les

[13] À titre d'illustration :
- OpenAI précise dans ses CGU : « *Propriété du Contenu. Dans le cadre de votre relation avec OpenAI, et dans la mesure où la loi applicable le permet, vous (a) conservez vos droits de propriété sur les Données d'Entrée et (b) êtes titulaire des droits de propriété sur les Données de Sortie. Par la présente, nous vous cédons tous nos droits, titres et intérêts, le cas échéant, sur les Données de Sortie.* » : [lien vers les CGU d'OpenAI : https://openai.com/fr-FR/policies/terms-of-use/]
- Midjourney prévoit dans ses CGU : « *Content Rights. Your Rights and Obligations. You own all Assets You create with the Services to the fullest extent possible under applicable law. There are some exceptions:*
*- Your ownership is subject to any obligations imposed by this Agreement and the rights of any third-parties.*
*- If you are a company or any employee of a company with more than $1,000,000 USD a year in revenue, you must be subscribed to a "Pro" or "Mega" plan to own Your Assets.*
*- If you upscale the images of others, these images remain owned by the original creators.*
*Please consult Your own lawyer if You want more information about the state of current intellectual property law in Your jurisdiction. Your ownership of the Assets you created persists even if in subsequent months You downgrade or cancel Your membership.*
*Inputs, Assets, and other content such as messages, photos, videos, and documents that you may provide to the Services (such as through uploading, posting, sharing, or chat messages) are collectively, "Content". You are responsible for all Content that you provide or generate, including ensuring that it does not violate any applicable laws or this Agreement, and that you have all necessary rights and permissions to provide the Content.* » CGU de Midjourney : https://docs.midjourney.com/docs/terms-of-service]

[14] Lignes directives par l'Administration nationale chinoise de la propriété intellectuelle (CNIPA) relatives aux demandes de brevet pour des inventions liées à l'intelligence artificielle : https://www.cnipa.gov.cn/art/2024/12/6/art_75_196483.html

demandes de brevet relatives à l'IA, ce qui clarifie sa position sur la possibilité de reconnaître une intelligence artificielle dans les demandes de brevet.
En particulier, pour l'identification des inventeurs, elle rappelle d'abord que la signature de l'inventeur doit être celle d'une personne physique, avant de distinguer deux hypothèses : (i) pour les inventions réalisées avec l'aide de l'IA, une personne physique qui a apporté une contribution créative aux caractéristiques substantielles de l'invention pourra être désignée comme l'inventeur de la demande de brevet et (ii) pour les inventions générées par l'IA, il ne sera pas possible d'accorder le statut d'inventeur à l'IA dans le contexte juridique actuel de la Chine.

- **Approche de l'Office européen des brevets relative à l'intelligence artificielle**[15] : pour l'heure, l'Office européen des brevets (OEB) n'a adopté aucune ligne directrice relative à la détermination de la personne physique qui pourrait être désignée comme inventeur dans le cadre d'une demande de brevet lorsque l'invention a été conçue en utilisant une IA ; cette question relève donc du ressort de chaque pratique nationale des États contractants de la Convention sur le brevet européen.
  L'OEB a néanmoins distingué trois catégories d'inventions en lien avec l'IA : (i) les inventions d'origine humaine ayant recours à l'IA pour la vérification des résultats, (ii) les inventions dans le cadre desquelles un être humain identifie un problème et utilise l'IA pour trouver une solution et (iii) toutes les inventions créées par une IA dans le cadre desquelles l'IA identifie un problème et propose une solution sans intervention humaine. L'OEB rappelle, notamment, qu'il est communément admis que l'inventeur est un être humain et que l'inventeur désigné dans la demande doit être un être humain et non une machine.

- **Publication par l'USPTO de son « *Inventorship Guidance for AI-Assisted Inventions* »**[16] (guide de l'inventeur pour les inventions assistées par IA) : l'objectif de ce guide est d'aider les déposants à identifier à qui doit revenir la paternité d'une invention lorsqu'une IA a été utilisée au cours du processus inventif ; l'USPTO énonce, à ce titre, cinq principes directeurs, incluant notamment le fait que l'utilisation par une personne physique d'un système d'IA pour créer une invention assistée par l'IA ne remet pas en cause les contributions de cette personne comme inventeur.

- **Affaires DABUS** : DABUS est une intelligence artificielle qui a réalisé seule deux inventions. Suite aux dépôts de multiples demandes de brevets, seule l'Afrique du Sud a délivré un brevet pour les inventions réalisées par DABUS[17].

En l'absence de critères établis par l'OEB en Europe pour identifier la personne physique pouvant être légitimement désignée comme inventeur dans une demande de brevet, et compte tenu de la vocation de nombreuses demandes déposées en Europe à être étendues aux États-Unis, les déposants peuvent se référer aux lignes directrices de l'USPTO. Il leur est ainsi recommandé de faire documenter par les inventeurs l'utilisation d'un système d'IA au cours du processus inventif.

---

[15] Office européen des brevets, actualités « Intelligence artificielle » : https://www.epo.org/fr/news-events/in-focus/ict/artificial-intelligence

[16] USPTO, « *Inventorship Guidance for AI-Assisted Inventions* », 13 février 2024 : www.govinfo.gov/content/pkg/FR-2024-02-13/pdf/2024-02623.pdf

[17] A noter que la protection en matière de brevet a été majoritairement écartée, tel est notamment le cas des Etats-Unis (lien : https://www.wipo.int/wipolex/en/text/590863 https://www.wipo.int/wipolex/en/text/590863 ), de l'Australie (lien : https://artificialinventor.com/wp-content/uploads/2021/08/Thaler-v-Commissioner-of-Patents-2021-FCA-879.pdf) ou encore de l'Office européen des brevets (lien : https://www.epo.org/boards-of-appeal/decisions/pdf/j200008eu1.pdf et https://www.epo.org/boards-of-appeal/decisions/pdf/j200009eu1.pdf https://www.epo.org/boards-of-appe ).

### 1.3.3 En droit des bases de données[18]

Pour rappel, le droit d'auteur en France protège la « *structure de la base* » (également appelée le « *contenant* »). Celle-ci doit être originale, autrement dit, sont protégées les bases de données « *qui, par le choix ou la disposition des matières, constituent des créations intellectuelles* » (Article L.112-3 alinéa 1er du Code de la propriété intellectuelle). En principe, la titularité des droits revient au créateur personne physique de l'œuvre dès la création (article L.111-1 du Code de la propriété intellectuelle). Pour l'heure, la jurisprudence ne s'est pas encore prononcée sur le droit des bases de données et l'IA, néanmoins il est déjà possible de percevoir les futures difficultés relatives au(x) titulaire(s) des droits d'une base de données lorsque celle-ci sera créée de manière autonome par une IA.

## 1.4. Les bonnes pratiques

Plusieurs bonnes pratiques peuvent d'ores et déjà être mises en place :

- sensibilisation et formation continue des équipes : les équipes, qu'elles soient juridiques ou techniques, doivent être formées aux enjeux de la propriété intellectuelle relatifs aux systèmes d'IA. Il est essentiel d'organiser régulièrement des sessions de formation afin que les collaborateurs/salariés - étant précisé que ces formations doivent être adaptées au(x) rôle(s) de ces derniers - soient à jour des implications juridiques de ces technologies émergentes.
- veille juridique proactive et continue : un système de veille juridique régulier doit être mis en place pour surveiller les évolutions législatives et jurisprudentielles en matière de propriété intellectuelle et d'IA. Il est important de suivre les décisions des juridictions, les nouvelles régulations, ainsi que les travaux des organismes de normalisation, afin d'anticiper les changements et d'adapter les pratiques pour assurer la conformité aux obligations futures. À titre d'illustration, une première ébauche du Code de bonnes pratiques pour l'IA à usage général, rédigée par des experts indépendants, a été publiée le 14 novembre dernier[19], puis une seconde ébauche a été publiée le 19 décembre 2024[20].
- Anticipation des évolutions réglementaires : d'autres régulations spécifiques pourraient voir le jour en matière de droit de la propriété intellectuelle[21]. Il est recommandé de participer aux consultations publiques et de rester informé des débats. À titre d'illustration, aux États-Unis, le Copyright Office a publié, le 31 juillet 2024, la première partie du rapport qui traite des répliques numériques[22].

---

[18] À noter que, dans un arrêt du 28 février 2024, opposant LBC France (Leboncoin) et Directannonces concernant l'extraction non autorisée d'une base de données en renouvellement, Leboncoin a été reconnu comme producteur de bases de données. Cet arrêt, bien que ne portant pas directement sur l'intelligence artificielle, pourrait tout à fait constituer un risque de condamnation sur le fondement des dispositions relatives aux bases de données pour les fournisseurs de systèmes d'IA (Cour de cassation, 28 février 2024, LBC France (Leboncoin) c/ Directannonces).

[19] À noter que les codes de bonne pratique sont prêts au plus tard le 2 mai 2025 (article 56§9, *AI Act*).

[20] Commission européenne, actualités, 14 novembre 2024 : https://digital-strategy.ec.europa.eu/fr/news/commission-publishes-first-draft-general-purpose-artificial-intelligence-code-practice#:~:text=Le%20code%20de%20bonnes%20pratiques%20vise%20%C3%A0%20faciliter,%C3%A0%20usage%20g%C3%A9n%C3%A9ral%20fiables%20et%20s%C3%BBrs%20dans%20l%E2%80%99UE ; Commission européenne, actualités, 19 décembre 2024 : https://digital-strategy.ec.europa.eu/en/library/second-draft-general-purpose-ai-code-practice-published-written-independent-experts

[21] À titre d'illustration : Assemblée Nationale, Proposition de loi n°1630 visant à encadrer l'intelligence artificielle par le droit d'auteur, 12 septembre 2023 : https://www.assemblee-nationale.fr/dyn/16/textes/l16b1630_proposition-loi

[22] U.S. Copyright Office, Copyright and Artificial Intelligence, 31 juillet 2024 : https://www.copyright.gov/ai/

# 2. Secret d'affaires/confidentialité et intelligence artificielle

Il existe une grande diversité de secrets consacrés par la loi, tels que les secrets médicaux, bancaires, de la défense nationale, de l'instruction, des affaires, professionnels ou encore celui des correspondances.

Dans le cadre de l'intelligence artificielle (IA), les risques liés au traitement de données couvertes par ces secrets peuvent survenir tant du côté du fournisseur que du déployeur d'un système d'IA (**2.2.**), ainsi il est essentiel de mettre en œuvre des bonnes pratiques (**2.3.**). Cette analyse s'inscrit dans la continuité de celle portant sur la prise en compte des secrets par l'*AI Act* (**2.1.**).

## 2.1. La notion de « *secret* » au sein de l'*AI Act*

L'*AI Act* contient peu de référence à la notion de secret :

- Article 25, paragraphe 5 : « *Les paragraphes 2 et 3 [qui traitent des responsabilités tout au long de la chaîne de valeur de l'IA] sont sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle, les informations confidentielles de nature commerciale et les secrets d'affaires conformément au droit de l'Union et au droit national.* »
- Article 31, paragraphe 7 : « *[…]. Le personnel des organismes notifiés est lié par le secret professionnel pour toutes les informations dont il a connaissance dans l'exercice de ses fonctions au titre du présent règlement, sauf à l'égard des autorités notifiantes de l'État membre où il exerce ses activités.* »
- Article 52, paragraphe 6 : « *La Commission veille à ce qu'une liste des modèles d'IA à usage général présentant un risque systémique soit publiée et tient cette liste à jour, sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national.* »
- Article 53, paragraphe 1, b) : « *Les fournisseurs de modèles d'IA à usage général : […] élaborent, tiennent à jour et mettent à disposition des informations et de la documentation à l'intention des fournisseurs de systèmes d'IA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs systèmes d'IA. Sans préjudice de la nécessité d'observer et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national, ces informations et cette documentation.* »
- Article 53, paragraphe 7 : « *Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée conformément aux obligations de confidentialité énoncées à l'article 78.* »
- Article 55, paragraphe 3 : « *Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée conformément aux obligations de confidentialité énoncées à l'article 78.* »
- Article 100, paragraphe 5 : « *Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties disposent d'un droit d'accès au dossier du Contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des personnes ou entreprises concernées en ce qui concerne la protection de leurs données à caractère personnel ou de leurs secrets commerciaux.* »
- Annexe VII, paragraphe 4.5 : « *[…] Cet accès est soumis au droit de l'Union existant en matière de protection de la propriété intellectuelle et des secrets d'affaires.* »

L'essentiel découle de **l'article 78** intitulé **« confidentialité »** :

« *La Commission, les autorités de surveillance du marché et les organismes notifiés, ainsi que toute autre personne physique ou morale associée à l'application du présent règlement respectent, conformément au droit de l'Union ou au droit national, la confidentialité des informations et des données obtenues dans l'exécution de leurs tâches et activités de manière à protéger, en particulier: a) les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires des personnes physiques ou morales, y compris le code source, à l'exception des cas visés à l'article 5 de la directive (UE) 2016/943 du Parlement européen et du Conseil ( 57);* »

La Commission, les autorités de surveillance du marché, les organismes notifiés, ainsi que toute autre personne physique ou morale impliquée dans l'application de l'*AI Act*, ont l'obligation de protéger les informations confidentielles de nature commerciale ou les secrets d'affaires.

## 2.2. Les risques de traitement des données couvertes par un secret

### 2.2.1. Côté fournisseur[23]

Les fournisseurs doivent être vigilants face à divers risques, parmi lesquels :

- le risque de divulgation involontaire de données confidentielles : les fournisseurs peuvent exposer accidentellement des informations confidentielles (par exemple, lorsque, accidentellement, des informations confidentielles ont été utilisées pour l'entraînement du modèle d'IA) ;
- le risque d'exploitation abusive des données : les données utilisées pour l'entraînement peuvent être détournées ou mal exploitées par des tiers, compromettant ainsi des secrets commerciaux ou d'autres informations soumises à des obligations de confidentialité ;
- le non-respect d'obligations légales : un manquement aux obligations de protection des données confidentielles ou des secrets d'affaires peut entraîner des sanctions civiles et pénales pour les fournisseurs, ainsi qu'une perte de confiance de la part de leurs clients et partenaires. En sus, les fournisseurs ayant conclu des contrats avec leurs clients peuvent voir leur responsabilité contractuelle engagée du fait d'un manquement à l'obligation de confidentialité, en particulier dans le cas où les fournisseurs utilisent des données de leurs clients pour entraîner le système et/ou le modèle d'IA.

[23] Article 3, paragraphe 3 de l'AI Act : un fournisseur est « *une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit* ».

### 2.2.2. Côté déployeur[24]

Par ailleurs, les utilisateurs sont exposés à des risques, notamment lors des instructions génératives ou « *prompts* »[25] qui peuvent contenir des secrets. Ces informations peuvent être divulguées, que ce soit au fournisseur du système d'IA ou à des tiers.

## 2.3. Les bonnes pratiques

### 2.3.1. Côté fournisseur

Pour réduire ces risques, les fournisseurs peuvent adopter les pratiques suivantes :

- mise en place d'une gouvernance solide des données : il est crucial d'établir une politique de gouvernance des données qui assure une protection adéquate des données tout au long du cycle de vie du système et/ou du modèle d'IA, avec une attention particulière pour les données couvertes par un secret légal ;
- protection des données industrielles : le *Data Act* autorise la circulation des données industrielles, mais impose des mesures de protection pour préserver la confidentialité des secrets d'affaires. Les fournisseurs doivent définir des accords clairs avec les détenteurs de données et les tiers pour réguler l'utilisation, le stockage et la transmission des informations sensibles ;
- sensibilisation et formation des équipes : la formation régulière des équipes sur la gestion des données sensibles et le respect des obligations légales en matière de confidentialité est essentielle pour garantir que les bonnes pratiques sont respectées à toutes les étapes du processus de développement et d'entraînement des systèmes d'IA.

### 2.3.2. Côté déployeur

Pour réduire les risques, les déployeurs peuvent notamment adopter les pratiques suivantes :

- restriction des outils d'IA génératives : il est possible de limiter l'accès à ces IA génératives pour certains collaborateurs et/ou salariés (par exemple, en mettant en place une charte IA restreignant l'utilisation d'IA générative à seulement certains outils) ;
- limitation des usages possibles en cas d'utilisation d'IA génératives : il est également possible de limiter les usages des IA génératives (par exemple, en mettant en place une charte IA limitant l'utilisation d'IA générative à seulement certaines pratiques, comme pour la création marketing) ;
- formation continue des équipes : sensibiliser régulièrement les collaborateurs et/ou salariés aux risques spécifiques liés à l'IA et fournir des recommandations pratiques pour garantir une utilisation sécurisée des IA. Cela peut inclure des sessions de formation sur les risques de divulgation et les bonnes pratiques pour protéger les informations sensibles.

---

[24] Article 3, paragraphe 3 de l'*AI Act* : un déployeur est « *une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel* ».

[25] À noter qu'une « instruction générative » ou un « *prompt* » peut prendre la forme « *d'un texte à compléter, d'une question, d'une consigne à respecter dans la production de la réponse, voire d'un ou de plusieurs exemples de résultats attendus* ». (source : Liste relative au vocabulaire de l'intelligence artificielle (termes, expressions et définitions adoptés), JORF n°0212 du 6 septembre 2024, Texte n°51 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050185686

# 3. Protection des données et intelligence artificielle

Dans le cadre de l'*AI Act*, les données occupent une place centrale et sont mentionnées à plusieurs reprises (**3.1.**). S'agissant des données personnelles, le texte intègre des principes fondamentaux du RGPD applicables aux systèmes d'IA (**3.2.**). Pour les données non personnelles, les organisations doivent veiller à l'articulation entre l'*AI Act* et le *Data Act* (**3.3.**). Enfin, les praticiens peuvent mettre en œuvre des bonnes pratiques pour assurer une conformité optimale (**3.4.**).

## 3.1. Les données au sein de l'*AI Act*

Contrairement aux « *données à caractère non personnel* », les termes de « *données* » et de « *données à caractère personnel* » sont présents à de nombreuses reprises au sein de l'*AI Act* :

- ***Données à caractère personnel*** :
  - Article 2, paragraphe 7 : « *Le droit de l'Union en matière de protection des données à caractère personnel, de respect de la vie privée et de confidentialité des communications s'applique aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement. Le présent règlement n'a pas d'incidence sur le règlement (UE) 2016/679 ou le règlement (UE) 2018/1725, ni sur la directive 2002/58/CE ou la directive (UE) 2016/680, sans préjudice de l'article 10, paragraphe 5, et de l'article 59 du présent règlement.* »
  - Article 3 :
    - Paragraphe 34 : « données biométriques », les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, telles que des images faciales ou des données dactyloscopiques »
    - Paragraphe 37 : « *catégories particulières de données à caractère personnel, les catégories de données à caractère personnel visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679, à l'article 10 de la directive (UE) 2016/680 et à l'article 10, paragraphe 1, du règlement (UE) 2018/1725* »
    - Paragraphe 50 : « *« données à caractère personnel », les données à caractère personnel définies à l'article 4, point 1), du règlement (UE) 2016/679* »
    - Paragraphe 51 : « *« données à caractère non personnel », les données autres que les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679* »
  - Article 7, paragraphe 2, c) : « *la nature et la quantité des données traitées et utilisées par le système d'IA, en particulier le traitement ou l'absence de traitement des catégories particulières de données à caractère personnel* »
  - Article 10 :
    - Paragraphe 2, b) : « *les processus de collecte de données et l'origine des données, ainsi que, dans le cas des données à caractère personnel, la finalité initiale de la collecte de données* »
    - Paragraphe 5 : « *Dans la mesure où cela est strictement nécessaire aux fins de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à risque élevé, conformément au paragraphe 2, points f) et g), du présent article,*

*les fournisseurs de ces systèmes peuvent exceptionnellement traiter des catégories particulières de données à caractère personnel, sous réserve de garanties appropriées pour les droits et libertés fondamentaux des personnes physiques. Outre les dispositions des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive (UE) 2016/680, toutes les conditions suivantes doivent être réunies pour que ce traitement puisse avoir lieu:[…] : b) les catégories particulières de données à caractère personnel sont soumises à des limitations techniques relatives à la réutilisation des données à caractère personnel, ainsi qu'aux mesures les plus avancées en matière de sécurité et de protection de la vie privée, y compris la pseudonymisation ; c) les catégories particulières de données à caractère personnel font l'objet de mesures visant à garantir que les données à caractère personnel traitées sont sécurisées, protégées et soumises à des garanties appropriées, y compris des contrôles stricts et une documentation de l'accès, afin d'éviter toute mauvaise utilisation et de veiller à ce que seules les personnes autorisées ayant des obligations de confidentialité appropriées aient accès à ces données à caractère personnel; d) les catégories particulières de données à caractère personnel ne doivent pas être transmises, transférées ou consultées d'une autre manière par d'autres parties; e) les catégories particulières de données à caractère personnel sont supprimées une fois que le biais a été corrigé ou que la période de conservation des données à caractère personnel a expiré, selon celle de ces deux échéances qui arrive en premier; f) les registres des activités de traitement visés dans les règlements (UE) 2016/679 et (UE) 2018/1725 et dans la directive (UE) 2016/680 comprennent les raisons pour lesquelles le traitement des catégories particulières de données à caractère personnel était strictement nécessaire pour détecter et corriger les biais, ainsi que la raison pour laquelle cet objectif n'a pas pu être atteint par le traitement d'autres données.* »

- Article 19, paragraphe 1 : « *Les fournisseurs de systèmes d'IA à risque élevé assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à risque élevé, visés à l'article 12, paragraphe 1, dans la mesure où ces journaux se trouvent sous leur contrôle. Sans préjudice du droit de l'Union ou du droit national applicable, les journaux sont conservés pendant une période adaptée à la destination du système d'IA à risque élevé, d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicable, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.* »
- Article 26 :
  - Paragraphe 6 : « *Les déployeurs de systèmes d'IA à risque élevé assurent la tenue des journaux générés automatiquement par ce système d'IA à risque élevé dans la mesure où ces journaux se trouvent sous leur contrôle, pendant une période adaptée à la destination du système d'IA à risque élevé, d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicable, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.* »
  - Paragraphe 10 : « *10. Sans préjudice de la directive (UE) 2016/680, dans le cadre d'une enquête en vue de la recherche ciblée d'une personne soupçonnée d'avoir commis une infraction pénale ou condamnée pour avoir commis une infraction pénale, le déployeur d'un système d'IA à risque élevé pour l'identification*

*biométrique à distance a posteriori demande l'autorisation, ex ante ou sans retard injustifié et au plus tard dans les 48 heures, d'une autorité judiciaire ou administrative dont la décision est contraignante et soumise à un contrôle juridictionnel, pour l'utilisation de ce système, sauf lorsqu'il est utilisé pour l'identification initiale d'un suspect potentiel sur la base de faits objectifs et vérifiables directement liés à l'infraction. Chaque utilisation est limitée à ce qui est strictement nécessaire pour enquêter sur une infraction pénale spécifique. Si l'autorisation demandée en application du premier alinéa est rejetée, l'utilisation du système d'identification biométrique à distance a posteriori lié à l'autorisation demandée est interrompue avec effet immédiat et les données à caractère personnel liées à l'utilisation du système d'IA à risque élevé pour lequel l'autorisation a été demandée sont supprimées.* »

- Article 50, paragraphe 3 : « *Les déployeurs d'un système de reconnaissance des émotions ou d'un système de catégorisation biométrique informent les personnes physiques qui y sont exposées du fonctionnement du système et traitent les données à caractère personnel conformément au règlement (UE) 2016/679, au règlement (UE) 2018/1725 et à la directive (UE) 2016/680, selon le cas. Cette obligation ne s'applique pas aux systèmes d'IA utilisés pour la catégorisation biométrique et la reconnaissance des émotions dont la loi autorise l'utilisation à des fins de prévention ou de détection des infractions pénales ou d'enquêtes en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers et conformément au droit de l'Union.* »
- Article 57, paragraphe 10 : « *Les autorités nationales compétentes veillent à ce que, dans la mesure où les systèmes d'IA innovants impliquent le traitement de données à caractère personnel ou relèvent à d'autres titres de la surveillance d'autres autorités nationales ou autorités compétentes assurant ou encadrant l'accès aux données, les autorités nationales chargées de la protection des données et ces autres autorités nationales ou autorités compétentes soient associées à l'exploitation du bac à sable réglementaire de l'IA et participent au contrôle des aspects qui relèvent de leurs tâches et pouvoirs respectifs.* »
- Article 59 :
  - Paragraphe 1 : « *Dans le bac à sable réglementaire de l'IA, les données à caractère personnel collectées légalement à d'autres fins peuvent être traitées uniquement aux fins du développement, de l'entraînement et de la mise à l'essai de certains systèmes d'IA dans le bac à sable, lorsque l'ensemble des conditions suivantes sont remplies* »
  - Paragraphe 1, d) : « *les données à caractère personnel à traiter dans le cadre du bac à sable se trouvent dans un environnement de traitement des données séparé, isolé et protégé sur le plan fonctionnel, placé sous le contrôle du fournisseur potentiel, et seules les personnes autorisées ont accès à ces données* »
  - Paragraphe 1, f) : « *aucun traitement de données à caractère personnel effectué dans le cadre du bac à sable ne débouche sur des mesures ou des décisions affectant les personnes concernées ni n'a d'incidence sur l'application des droits que leur confère le droit de l'Union en matière de protection des données à caractère personnel* »
  - Paragraphe 1, g) : « *les données à caractère personnel traitées dans le cadre du bac à sable sont protégées par des mesures techniques et organisationnelles*

*appropriées et supprimées une fois que la participation au bac à sable a cessé ou que la période de conservation de ces données à caractère personnel a expiré* »

- Paragraphe 1, h) : « *les registres du traitement des données à caractère personnel dans le cadre du bac à sable sont conservés pendant la durée de la participation au bac à sable, sauf disposition contraire du droit de l'Union ou du droit national* »
- Paragraphe 2 : « *Aux fins de la prévention et de la détection d'infractions pénales, ainsi que des enquêtes et des poursuites en la matière ou de l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, sous le contrôle et la responsabilité des autorités répressives, le traitement des données à caractère personnel dans les bacs à sable réglementaires de l'IA est fondé sur une disposition spécifique du droit de l'Union ou du droit national et soumis aux mêmes conditions cumulatives que celles visées au paragraphe 1.* »
- Paragraphe 3 : « *Le paragraphe 1 est sans préjudice du droit de l'Union ou du droit national excluant le traitement des données à caractère personnel à des fins autres que celles expressément mentionnées dans ce droit, ainsi que sans préjudice du droit de l'Union ou du droit national établissant le fondement du traitement des données à caractère personnel qui est nécessaire aux fins du développement, de la mise à l'essai et de l'entraînement de systèmes d'IA innovants, ou de toute autre base juridique, dans le respect du droit de l'Union relatif à la protection des données à caractère personnel.* »

- Article 60 :
  - Paragraphe 4, i) : « *les participants aux essais en conditions réelles ont donné leur consentement éclairé conformément à l'article 61 ou, dans le cas des services répressifs, lorsque la recherche d'un consentement éclairé empêcherait de réaliser les essais du système d'IA, les essais proprement dits et les résultats des essais en conditions réelles n'ont pas d'effet négatif sur les participants, et leurs données à caractère personnel sont supprimées une fois les essais réalisés* »
  - Paragraphe 5 : « *Tout participant aux essais en conditions réelles, ou son représentant légal, selon le cas, peut, sans encourir de préjudice et sans devoir se justifier, se retirer des essais à tout moment, en révoquant son consentement éclairé et peut demander la suppression immédiate et définitive de ses données à caractère personnel. Le retrait du consentement éclairé n'affecte pas les activités déjà menées.* »
- Article 70, paragraphe 3 : « *Les États membres veillent à ce que leurs autorités nationales compétentes disposent de ressources techniques, financières et humaines suffisantes, ainsi que d'infrastructures pour mener à bien efficacement les tâches qui leur sont confiées en vertu du présent règlement. En particulier, les autorités nationales compétentes disposent en permanence d'un personnel en nombre suffisant, qui possède, parmi ses compétences et son expertise, une compréhension approfondie des technologies de l'IA, des données et du traitement de données, de la protection des données à caractère personnel, de la cybersécurité, des droits fondamentaux, des risques pour la santé et la sécurité, et une connaissance des normes et exigences légales en*

*vigueur. Chaque année, les États membres évaluent et, si nécessaire, mettent à jour les exigences portant sur les compétences et les ressources visées au présent paragraphe.* »

- Article 71, paragraphe 5 : « *La base de données de l'UE ne contient des données à caractère personnel que dans la mesure où celles-ci sont nécessaires à la collecte et au traitement d'informations conformément au présent règlement. Ces informations incluent les noms et les coordonnées des personnes physiques qui sont responsables de l'enregistrement du système et légalement autorisées à représenter le fournisseur ou le déployeur, selon le cas.* »
- Article 100, paragraphe 5 : « *Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties disposent d'un droit d'accès au dossier du Contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des personnes ou entreprises concernées en ce qui concerne la protection de leurs données à caractère personnel ou de leurs secrets commerciaux.* »
- Annexe V, paragraphe 5 : « *lorsqu'un système d'IA nécessite le traitement de données à caractère personnel, une déclaration qui atteste que ledit système d'IA est conforme aux règlements (UE) 2016/679 et (UE) 2018/1725 ainsi qu'à la directive (UE) 2016/680* »

- ***Données à caractère non personnel*** :
  - Article 3, paragraphe 51 : « *Aux fins du présent règlement, on entend par : « données à caractère non personnel* », les données autres que les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679 »
  - Article 59, paragraphe 1, b) : « *les données traitées sont nécessaires pour satisfaire à une ou plusieurs des exigences visées au chapitre III, section 2, lorsque ces exigences ne peuvent être satisfaites de manière efficace en traitant des données anonymisées, synthétiques ou autres à caractère non personnel* »

## 3.2. Les données personnelles : articulation entre le RGPD et l'*AI Act*

### 3.2.1 Les principes clés du RGPD applicables à l'IA et listés dans l'*AI Act*

Plusieurs principes clés du règlement (UE) 2016/679 du 27 avril 2016 désigné comme « *règlement général sur la protection des données* » ou « *RGPD* », sont applicables à l'IA et se retrouvent également dans l'*AI Act*, tels que :

- l'*AI Act* n'a pas pour but d'altérer les obligations des responsables de traitement et des sous-traitants au sens du RGPD ;
- les bases de données qui nourrissent l'IA doivent respecter le principe d'exactitude, conformément à l'article 5§1, d) du RGPD ;
- l'*AI Act* et le RGPD prévoient des dispositions en matière de responsabilité administrative ; cependant, seul le RGPD prévoit un mécanisme de responsabilité civile extracontractuelle spécifique, conformément à l'article 82§1 ;
- les dispositions de l'*AI Act* ne constituent pas une exception à l'interdiction du profilage au sens de l'article 22§2, point b) du RGPD ; et la combinaison du RGPD et de l'*AI Act* a pour conséquence de conférer au traitement de données personnelles via l'identification biométrique à distance, un statut spécifique et posent une interdiction de principe dans le cas des systèmes d'identification

biométrique à distance, utilisés dans le cadre d'activités répressives pour mener à une surveillance aveugle (Cf. Considérant 95, *AI Act*).

**Actuellement, aucun texte de droit français ou de l'Union européenne n'impose la mise en place d'une charte IA dans les organisations. Néanmoins, certaines dispositions de l'AI Act laissent penser que l'implémentation d'une charte spécifique sur l'IA est une bonne solution. La partie gouvernance du guide aborde ce sujet.**

### 3.2.2 Le rôle des autorités de régulation

À côté de la gouvernance au niveau de l'Union européenne, l'*AI Act* prévoit la désignation d'autorités nationales compétentes (article 70, *AI Act*). À ce titre, chaque État membre doit établir ou désigner en tant qu'autorités nationales compétentes « *au moins une autorité notifiante et une autorité de surveillance de marché* » :

- Dans une déclaration commune, les autorités de protection des données du G7 - incluant la CNIL en France - rappellent que de nombreuses technologies d'IA reposent sur le traitement des données personnelles. Or, les autorités du G7 ont un rôle à jouer dans la gouvernance de l'IA, en particulier eu égard à leur expérience et leur expertise dans les domaines suivants : la supervision des traitements de données personnelles dans les technologies d'IA, le suivi des évolutions technologiques, l'analyse et la rédaction d'avis sur les propositions législatives en matière d'IA, la coopération avec d'autres régulateurs, l'accompagnement des acteurs, et la sensibilisation et l'éducation au numérique du grand public. Ainsi, en France, la CNIL pourrait être désignée en tant qu'autorité compétente.
- Par ailleurs, d'autres autorités sectorielles vont naturellement se positionner sur le rôle d'autorité de surveillance du marché. Ainsi, l'ACPR se dit prête à assumer cette fonction en France pour le secteur financier[26].

En tout état de cause, les États membres devront désigner les autorités de surveillance au niveau national avant le 2 août 2025, afin de superviser l'application et la mise en œuvre de l'*AI Act*.

## 3.3. Les données non personnelles : articulation entre le *Data Act* et l'*AI Act*

### 3.3.1. Présentation du *Data Act*

- **Objectif du *Data Act*** :

Le règlement (UE) 2023/2854 du 13 décembre 2023 sur les données, également désigné comme « *Data Act* »[27], vise à garantir une meilleure répartition entre les acteurs économiques, de la valeur issue de

[26] Forum Fintech ACPR-AMF – Paris, 14 octobre 2024, Discours de François Villeroy de Galhau, Gouverneur de la Banque de France, Président de l'Autorité de contrôle prudentiel et de résolution : https://www.banque-france.fr/fr/interventions-gouverneur/reussir-lalliance-des-innovateurs-et-des-regulateurs

[27] Règle. (UE) 2023/2854, 13 déc. 2023, concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202302854

l'utilisation des données, qu'elles soient personnelles ou non personnelles, en particulier dans le cadre de l'utilisation des objets connectés et du développement de l'Internet des objets.

- **Principales dispositions du *Data Act***:

- obligation de rendre accessibles les données générées par l'utilisation de produits ou de services liés (article 3 du *Data Act*) : la principale disposition du *Data Act* prévoit une obligation de rendre les données générées par l'utilisation de produits ou de services liés, directement accessibles à l'utilisateur ;

- droit d'accès aux données (article 4 du *Data Act*) : le *Data Act* octroie à l'utilisateur un droit d'accès aux données générées par l'utilisation de produits ou de services liés et un droit d'utilisation de ces données ;

- droit de partager des données avec des tiers (article 5 du *Data Act*) : le *Data Act* prévoit un « *droit de partager des données avec des tiers* ». Ce « *droit au partage* » est essentiel afin de permettre aux fournisseurs de systèmes d'IA d'accéder à une masse de données. Toutefois, le tiers doit supprimer « *les données lorsqu'elles ne sont plus nécessaires à la finalité convenue* » (sauf exceptions ; article 6 du *Data Act*).

### 3.3.2. Points communs entre le *Data Act* et l'*AI Act*

- **Absence explicite de l'IA dans le *Data Act***:

Bien que le *Data Act* ne mentionne pas expressément l'intelligence artificielle (cette notion n'apparaît pas dans le texte), cette technologie reste au cœur de ses objectifs. En effet, l'une des finalités principales du *Data Act* est de favoriser la circulation des données, élément essentiel pour encourager les innovations technologiques, en particulier dans le domaine de l'IA. Les données jouent donc un rôle crucial dans l'entraînement des modèles d'IA, faisant du *Data Act* un cadre facilitateur pour le développement de ces technologies.

- **Références limitées au *Data Act* dans l'*AI Act***:

L'*AI Act* contient peu de dispositions faisant référence au *Data Act*. En réalité, ce dernier n'est mentionné qu'une seule fois dans l'*AI Act*[28]. Cela reflète la relative indépendance des deux textes, bien que leurs objectifs puissent se croiser.

- **Application du *Data Act* aux opérateurs (au sens de l'*AI Act*)** :

Bien que les deux régulations aient peu de liens explicites, les opérateurs concernés par l'*AI Act* (fournisseurs, déployeurs, etc.) devront, s'ils relèvent du champ d'application du *Data Act*, en respecter les dispositions. En d'autres termes, les acteurs du secteur de l'IA devront s'assurer de leur conformité avec le *Data Act* lorsqu'ils y sont soumis.

[28] Considérant 141 de l'AI Act : « En ce qui concerne le transfert de données, il convient en outre d'envisager que les données collectées et traitées aux fins des essais en conditions réelles ne soient transférées vers des pays tiers que lorsque des garanties appropriées et applicables en vertu du droit de l'Union sont en place, en particulier conformément aux bases pour le transfert de données à caractère personnel prévues par le droit de l'Union en matière de protection des données, et que des garanties appropriées soient mises en place pour les données à caractère non personnel conformément au droit de l'Union, notamment les règlements (UE) 2022/868 ( 42) et (UE) 2023/2854 ( 43) du Parlement européen et du Conseil »
Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données : https://eur-lex.europa.eu/eli/reg/2023/2854/oj

## 3.4. Les bonnes pratiques

Plusieurs bonnes pratiques peuvent être mises en place par les praticiens :

- Consulter les fiches IA conçues par la CNIL[29] : la CNIL a publié des fiches numérotées de 1 à 12 permettant d'accompagner les divers professionnels. Ces fiches portent sur plusieurs thèmes incluant notamment la détermination du régime applicable aux traitements de données personnel en phase de développement (fiche 1), la définition d'une finalité (fiche 2), ou encore la détermination de la qualification juridique des fournisseurs de systèmes d'IA (fiche 3).
- Consulter la doctrine administrative publiée par les autorités européennes : à titre d'illustration, le 16 juillet 2024, le Comité européen de la protection des données (CEPD) a adopté une déclaration dans laquelle les autorités de protection des données précisent le rôle qu'elles souhaitent jouer dans la mise en œuvre de l'*AI Act*. En outre, le 18 décembre 2024, le CEPD a adopté un avis sur le traitement de données personnelles pour le développement et le déploiement de modèles d'IA. À noter que, dans son avis, le CEPD s'est prononcé sur trois points : (i) les conditions dans lesquelles les modèles d'IA peuvent être considérés comme anonymes ; (ii) si l'intérêt légitime peut être utilisé comme base juridique pour développer ou utiliser des modèles d'IA ; et (iii) les conséquences du développement illicite d'un modèle d'IA sur son utilisation.
- Consulter la doctrine administrative publiée par les Cnil étrangères : par exemple, la Cnil Belge a publié un guide pratique intitulé « *Les systèmes d'intelligence artificielle et le RGPD sous l'angle de la protection des données* » qui aborde les enjeux juridiques liés à la conception, au développement et au déploiement de solutions d'IA. Il s'adresse aux professionnels du droit, délégués à la protection des données (DPO), développeurs et responsables du traitement et les sous-traitants impliqués dans le développement et le déploiement de systèmes d'IA.
- Renforcer le rôle du DPO au sein de votre entreprise[30] : l'obligation de formation continue des Délégués à la Protection des Données (DPO) inclut non seulement leur propre formation à l'*AI Act*, mais également la formation du personnel de l'entreprise, conformément à l'article 39§1, b) du RGPD.

[29] CNIL, Les fiches pratiques IA, 8 avril 2024 : https://www.cnil.fr/fr/les-fiches-pratiques-ia

[30] À noter que le renforcement du rôle du DPO devrait s'accompagner de la mise à disposition de formations de la part de l'employeur puisque, pour rappel, les fournisseurs et les déployeurs de système d'IA doivent prendre des mesures pour garantir « *un niveau suffisant de maîtrise de l'IA pour leur personnel et les autres personnes s'occupant du fonctionnement et de l'utilisation des systèmes d'IA pour leur compte* » (article 4, *AI Act*).

# 4. Cybersécurité et intelligence artificielle

Bien que la cybersécurité soit peu abordée dans les articles de l'*AI Act* (**4.1.**), certaines exigences en matière de cybersécurité et de gestion des risques peuvent s'imposer (**4.2.**). Ainsi, les praticiens doivent porter une attention particulière à certains points clés (**4.3.**) et peuvent adopter des bonnes pratiques pour renforcer la conformité et la sécurité (**4.4.**).

## 4.1. La cybersécurité au sein de l'*AI Act*

La cybersécurité est peu présente au sein des articles de l'*AI Act* :

- Article 13, paragraphe 3, b), ii) : « *La notice d'utilisation contient au moins les informations suivantes : […] b) les caractéristiques, les capacités et les limites de performance du système d'IA à haut risque, notamment : […] ii) le niveau d'exactitude, y compris les indicateurs utilisés de robustesse et de cybersécurité, visé à l'article 15 qui a servi de référence pour les tests et la validation du système d'IA à risque élevé et qui peut être attendu, ainsi que toute circonstance connue et prévisible susceptible d'avoir une incidence sur ce niveau attendu d'exactitude, de robustesse et de cybersécurité.* »
- Article 15[31] :
  - Paragraphe 1 : « *La conception et le développement des systèmes d'IA à risque élevé sont tels qu'ils leur permettent d'atteindre un niveau approprié d'exactitude, de robustesse et de cybersécurité, et de fonctionner de façon constante à cet égard tout au long de leur cycle de vie.* »
  - Paragraphe 5, alinéa 2 : « *[…] Les solutions techniques visant à garantir la cybersécurité des systèmes d'IA à risque élevé sont adaptées aux circonstances pertinentes et aux risques.* »
- Article 31, paragraphe 2 : « *Les organismes notifiés se conforment aux exigences en matière d'organisation, de gestion de la qualité, de ressources et de procédures qui sont nécessaires à l'exécution de leurs tâches, ainsi qu'aux exigences appropriées en matière de cybersécurité.* »
- Article 42, paragraphe 2 : « *Les systèmes d'IA à risque élevé qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité conformément au règlement (UE) 2019/881 et dont les références ont été publiées au Journal officiel de l'Union européenne sont présumés conformes aux exigences de cybersécurité énoncées à l'article 15 du présent règlement, dans la mesure où ces dernières sont couvertes par tout ou partie du certificat de cybersécurité ou de la déclaration de conformité.* »
- Article 55, paragraphe 1, c) : « *Outre les obligations énumérées aux articles 53 et 54, les fournisseurs de modèles d'IA à usage général présentant un risque systémique : […] d) garantissent un niveau approprié de protection en matière de cybersécurité pour le modèle d'IA à usage général présentant un risque systémique et l'infrastructure physique du modèle.* »
- Article 58, paragraphe 2, i) : « *Les actes d'exécution visés au paragraphe 1 garantissent que: […] i) que les bacs à sable réglementaire de l'IA facilitent le développement d'outils et d'infrastructures pour la mise à l'essai, l'étalonnage des performances, l'évaluation et l'explication des aspects des systèmes d'IA pertinents pour l'apprentissage réglementaire, tels que la précision, la solidité et la*

[31] L'article 15 est intitulé « Exactitude, robustesse et cybersécurité ».

- Article 66, h) : « *Le Comité IA conseille et assiste la Commission et les États membres afin de faciliter l'application cohérente et efficace du présent règlement. À cette fin, le Comité IA peut notamment : […] h) coopérer, lorsqu'il y a lieu, avec d'autres institutions, organes et organismes de l'Union, ainsi que des groupes d'experts et réseaux compétents de l'Union, en particulier dans les domaines de la sécurité des produits, de la cybersécurité, de la concurrence, des services numériques et des services de médias, des services financiers, de la protection des consommateurs, de la protection des données et des droits fondamentaux.* »
- Article 70 :
  - Paragraphe 3 : « *Les États membres veillent à ce que leurs autorités nationales compétentes disposent de ressources techniques, financières et humaines suffisantes, ainsi que d'infrastructures pour mener à bien efficacement les tâches qui leur sont confiées en vertu du présent règlement. En particulier, les autorités nationales compétentes disposent en permanence d'un personnel en nombre suffisant, qui possède, parmi ses compétences et son expertise, une compréhension approfondie des technologies de l'IA, des données et du traitement de données, de la protection des données à caractère personnel, de la cybersécurité, des droits fondamentaux, des risques pour la santé et la sécurité, et une connaissance des normes et exigences légales en vigueur. Chaque année, les États membres évaluent et, si nécessaire, mettent à jour les exigences portant sur les compétences et les ressources visées au présent paragraphe.* »
  - Paragraphe 4 : « *Les autorités nationales compétentes prennent des mesures appropriées pour garantir un niveau adapté de cybersécurité.* »
- Article 78, paragraphe 2 : « *Les autorités associées à l'application du présent règlement conformément au paragraphe 1 demandent uniquement les données qui sont strictement nécessaires à l'évaluation du risque posé par les systèmes d'IA et à l'exercice de leurs pouvoirs conformément au présent règlement et au règlement (UE) 2019/1020. Elles mettent en place des mesures de cybersécurité adéquates et efficaces pour protéger la sécurité et la confidentialité des informations et des données obtenues, et suppriment les données collectées dès qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été obtenues, conformément au droit de l'Union ou au droit national applicable.* »
- Annexe IV, paragraphe 2, h) : « *La documentation technique visée à l'article 11, paragraphe 1, contient au moins les informations ci-après, selon le système d'IA concerné : […] une description détaillée des éléments du système d'IA et de son processus de développement, y compris : […] les mesures de cybersécurité qui ont été prises.* »

## 4.2. Les exigences en matière de cybersécurité et, plus largement, de gestion des risques

L'*AI Act* liste une méthodologie de gouvernance des risques liés à l'IA, incluant notamment :

- **une cartographie des risques** : les organisations doivent cartographier les entités partenaires pour partie responsables de la gestion des risques (article 25, *AI Act*) ;
- **la mise en place d'un système de gestion des risques pour les systèmes d'IA à risque élevé** : un système de gestion des risques devra être établi, mis en œuvre, documenté et tenu à jour pour les systèmes d'IA à risque élevé (article 9, *AI Act*) ;
- **des exigences d'exactitude, de robustesse et de cybersécurité** : la conception et le développement des systèmes d'IA à risque élevé doivent permettre d'atteindre un niveau approprié d'exactitude, de robustesse et de cybersécurité (article 15, *AI Act*) ;

- **un signalement des incidents graves** : les fournisseurs qui mettent des systèmes d'IA à risque élevé sur le marché de l'UE, doivent signaler tout incident grave aux autorités de surveillance des États membres dans lesquels cet incident s'est produit (article 73, *AI Act*) ;
- **le pouvoir de procéder à des évaluations** : le Bureau de l'IA, après consultation du Comité IA, peut procéder à des évaluations du modèle d'IA à usage général pour évaluer le respect des obligations prévues par l'*AI Act* par le fournisseur ou pour enquêter sur les risques systémiques des modèles d'IA à usage général présentant un risque systémique (article 92, *AI Act*) ;
- **un devoir de transparence et de fourniture d'informations aux déployeurs** : la conception et le développement des systèmes d'IA à risque élevé sont tels que le fonctionnement de ces systèmes doit être suffisamment transparent pour permettre aux déployeurs d'interpréter les sorties d'un système et de les utiliser de manière appropriée (article 13, *AI Act*) ;
- **un devoir d'information** : lorsque le système d'IA présente un risque au sens de l'article 79§1, c'est-à-dire un risque pour « *la santé ou la sécurité, ou pour les droits fondamentaux des personnes* », et que le fournisseur prend conscience de ce risque, il doit en rechercher immédiatement les causes et en informer les autorités de surveillance de marché compétentes ainsi que, le cas échéant, l'organisme notifié qui a délivré un certificat pour ce système d'IA à risque élevé (article 20, *AI Act*) ;
- **une documentation technique et la conservation des documents** : une documentation technique doit être établie - avant que ce système ne soit mis sur le marché ou mis en service - et être tenue à jour de manière à démontrer que le système d'IA à risque satisfait aux exigences de l'*AI Act* (article 11, *AI Act*). Cette documentation doit être conservée pendant dix ans après la mise sur le marché ou la mise en service du système d'IA à risque élevé (article 18, *AI Act*) ;
- **l'enregistrement du système d'IA à risque élevé dans la base de données de l'UE** : l'enregistrement du fournisseur (ou du mandataire) et du système, pour les systèmes d'IA à risque élevé visés à l'annexe III, dans la base de données de l'UE visée à l'article 71 du système d'IA à risque élevé, doit intervenir avant de mettre sur le marché ou de mettre en service le système d'IA susvisé (article 49, *AI Act*) ;
- **la surveillance** : les fournisseurs établissent et documentent un système de surveillance après commercialisation d'une manière qui soit proportionnée à la nature des technologies et des risques du système d'IA à risque élevé. Le système de surveillance après commercialisation collecte, documente et analyse, de manière active et systématique, les données pertinentes qui peuvent être fournies par les déployeurs ou qui peuvent être collectées via d'autres sources sur les performances des systèmes d'IA à risque élevé tout au long de leur cycle de vie (article 72, *AI Act*) ;
- **l'analyse d'impact des systèmes d'IA à risque élevé sur les droits fondamentaux** : les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics et les déployeurs de système d'IA à risque élevé visés à l'annexe III, points 5), b) et c), effectuent une analyse de l'impact sur les droits fondamentaux que l'utilisation de ce système peut produire (article 27, *AI Act*) ;
- **l'évaluation de la conformité** : pour les système d'IA à risque élevé listés à l'annexe III, point 1, le fournisseur doit suivre les normes harmonisées ou spécifications communes, puis choisir une procédure d'évaluation de conformité (article 43, *AI Act*) ;
- **la gouvernance de l'IA** : les systèmes d'IA à risque élevé faisant appel à des techniques qui impliquent l'entraînement de modèles d'IA au moyen de données sont développés sur la base de jeux de données d'entraînement, de validation et de test qui satisfont aux critères de qualité énoncés à l'article 10§2 à 5 à chaque fois que ces jeux de données sont utilisés (article 10, *AI Act*) ;
- **l'enregistrement des journaux** : les systèmes d'IA à risque élevé permettent, techniquement, l'enregistrement automatique des événements (journaux) tout au long de la durée de vie du système (article 12, *AI Act*).

À noter que la CNIL a listé plusieurs mesures de sécurité à envisager pour le développement d'un système d'IA, relatives aux données d'entraînement, au développement du système d'IA ou encore au fonctionnement du système d'IA[32].

## 4.3. Les points d'attention pour les praticiens

### 4.3.1 Les points d'attention des praticiens dans le cadre de l'*AI Act*

Pour les praticiens, plusieurs points doivent être pris en compte afin de respecter les exigences de l'*AI Act* :

- la traçabilité : les systèmes d'IA doivent être accompagnés d'une documentation détaillée couvrant l'ensemble de leur fonctionnement, depuis la conception jusqu'à la mise en œuvre des mesures de sécurité ;
- la transparence : il est essentiel de communiquer clairement sur les mesures de cybersécurité mises en place. Cela inclut la divulgation des risques potentiels associés aux systèmes d'IA, ainsi que les protocoles adoptés pour les atténuer. Cette transparence permet aux utilisateurs, développeurs et régulateurs de comprendre les mécanismes de sécurité, de gérer les risques efficacement et d'instaurer une confiance dans l'utilisation du système. Elle contribue également à renforcer la conformité aux exigences réglementaires ;
- la gestion des vulnérabilités : les systèmes d'IA doivent être continuellement surveillés pour identifier les vulnérabilités potentielles. Il est important de mettre en place des processus proactifs pour détecter rapidement toute faille de sécurité, tout en garantissant une réponse immédiate pour les isoler et les corriger. Les praticiens peuvent, par exemple, définir des protocoles de gestion des incidents, incluant la documentation des incidents, les potentiels correctifs et la validation des mesures correctives après leur mise en œuvre.

### 4.3.2 Les points d'attention des praticiens en dehors de l'*AI Act*

L'*AI Act* s'intègre dans une stratégie européenne consistant à définir un cadre harmonieux permettant de favoriser l'innovation tout en préservant la sécurité des systèmes d'information :

- **le règlement européen (UE) 2023/1114 sur les crypto-actifs (MiCA)**[33] : ce règlement établit des règles uniformes pour les émetteurs de crypto-actifs qui n'ont pas été réglementés par d'autres actes de l'Union européenne relatifs aux services financiers, et pour les prestataires de services liés à ces crypto-actifs (prestataires de services sur crypto-actifs) ;
- **le règlement (UE) 2022/868 sur la gouvernance européenne des données (*Data Governance Act*)**[34] : ce règlement vise à rendre davantage de données disponibles pour la réutilisation et à faciliter le partage des données dans des domaines tels que la santé, l'environnement, l'énergie, l'agriculture, la mobilité, la finance, l'industrie manufacturière, l'administration publique et les compétences, au profit

[32] Commission Nationale de l'Informatique et des Libertés (CNIL), Les fiches pratiques IA, fiche 12 : "*IA : Garantir la sécurité du développement d'un système d'IA*", 10 juin 2024 : https://www.cnil.fr/fr/ia-garantir-la-securite-du-developpement

[33] Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) no 1093/2010 et (UE) no 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32023R1114

[34] Règlement (UE) 2022/868 sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (acte sur la gouvernance des données) : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R0868

des citoyens et des entreprises de l'Union européenne, en créant des emplois et en stimulant l'innovation ;

- **le règlement (UE) 2023/2854 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (Règlement sur les données)**[35] : ce règlement garantit l'équité dans la répartition de la valeur des données entre les parties prenantes de l'économie des données. Il précise qui peut utiliser quelles données et dans quelles conditions ;
- **le règlement du Parlement européen et du Conseil concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques (CRA)**[36] : la nouvelle loi introduit des exigences en matière de cybersécurité à l'échelle de l'UE pour la conception, le développement, la production et la mise à disposition sur le marché de produits matériels et logiciels afin d'éviter le chevauchement des exigences découlant de différents textes législatifs dans les États membres de l'UE ;
- **la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (Directive SRI 2 ou « *NIS 2* »)**[37] : elle établit un cadre réglementaire commun en matière de cybersécurité visant à améliorer le niveau de cybersécurité dans l'Union européenne (UE), en exigeant des États membres de l'UE qu'ils renforcent leurs capacités en matière de cybersécurité et en introduisant des mesures de gestion des risques de cybersécurité et des rapports dans les secteurs critiques, ainsi que des règles en matière de coopération, de partage d'informations, de supervision et d'application de la loi ;
- **le règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier**[38] : ce règlement établit des règles uniformes en matière de sécurité des réseaux et des systèmes d'information des entités financières, telles que les banques, les compagnies d'assurance et les entreprises d'investissement.

## 4.4. Les bonnes pratiques

- Clarification des chaînes de responsabilités : il est indispensable de déterminer qui est responsable de quoi et vis-à-vis de qui. Par exemple, il peut être utile, pour les fournisseurs en aval ou les déployeurs, de mettre en place une check-list de documentations à compléter par le fournisseur au moment du référencement pour s'assurer qu'il est capable de fournir toutes les informations nécessaires.
- Mise en place d'un plan de réponse aux incidents : ce plan doit prévoir une réponse rapide et efficace aux cyberattaques, et s'assurer que le système puisse être restauré rapidement tout en préservant l'intégralité des données.
- Tests réguliers et audits externes: pour garantir la robustesse et la cybersécurité, il est recommandé d'effectuer des tests réguliers pour identifier les failles potentielles avant qu'elles ne soient exploitées et, en cas de besoin, des audits de prestataires externes.

---

[35] Règlement (UE) 2023/2854 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données)

[36] Règlement du Parlement européen et du Conseil concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n°168/2013 et (UE) 2019/1020 et la Directive (UE) 2020/1828 (Règlement sur la cyber résilience) : https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/fr/pdf

[37] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022L2555

[38] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R2554

- Accompagnement par des experts en cybersécurité : les praticiens devraient collaborer avec des spécialistes pour évaluer régulièrement les mesures de cybersécurité et garantir la mise en conformité avec les normes les plus récentes.
- Prise en compte des éléments de réglementation(s) sectorielle(s).
- Consultation des fiches pratiques publiées par la CNIL : en particulier, consulter la fiche 12 intitulée « *Garantir la sécurité du développement d'un système d'IA* »[39] .
- Consultation des recommandations de sécurité pour un système d'IA générative par l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[40] : l'ANSSI recommande d'adopter « *une posture de prudence* » lors du déploiement d'un système d'IA générative et de son intégration dans un système d'information existant. Ce guide s'intéresse à « *la sécurisation d'une architecture de système d'IA générative* ».

[39] CNIL, Fiche 12 « *Garantir la sécurité du développement d'un système d'IA* » : https://www.cnil.fr/fr/ia-garantir-la-securite-du-developpement

[40] Agence nationale de la sécurité des systèmes d'information (ANSSI), Recommandations de sécurité pour un système d'IA générative, 29 avril 2024 : https://cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative

# Remerciements

Le Cigref et Numeum souhaitent remercier chaleureusement les pilotes du groupe de travail « Mise en œuvre de l'*AI Act* », côté Cigref, **Lionel Chaine**, DSI de BPI France et **Jean-Claude Laroche**, Directeur de Mission auprès de la Présidence du COE France d'EDF, côté Numeum, **Katya Lainé**, CEO de TALKR.ai et **Thibault de Tersant**, *Senior executive Vice President* de Dassault Système.

Nous remercions également les différents participants, membres de nos deux associations, qui ont contribué à l'élaboration des livrets de ce guide.

Nous avons eu le plaisir d'être accompagnés tout au long de notre démarche par l'expertise de quatre grands cabinets d'avocats : August Debouzy, DLA Piper, Racine et Bird & Bird. Nous remercions plus particulièrement **Mahasti Razavi**, managing partner chez August Debouzy, **Anne-Sophie Lampe**, IT/IP Partner chez Bird & Bird, **Jeanne Dauzier** Partner et **Maria Aouad**, avocate chez DLA Piper et **Charles Bouffier**, avocat associé, et **Naomi Meynle-Hamza**, juriste doctorante, chez Racine.

**Rédaction :**
**Marine de Sury**, Directrice de mission, Cigref
**Anissa Kemiche**, Déléguée aux affaires européennes, Numeum

**Relecture : Chantal de Bardies**, Directrice de la qualité des contenus, Cigref

**Direction artistique et graphisme :**
**Emilie Grange**, Chargée de communication, Cigref
**Laura Pineau**, Chargée du digital et du graphisme, Numeum

Cigref
RÉUSSIR
LE NUMÉRIQUE

numeum
Engager
le numérique