Une image contenant motif, blanc, conception, noir et blanc

Le contenu généré par l’IA peut être incorrect.

Intelligence artificielle

Bonnes pratiques

Contributeurs

**Matthieu GRALL**, expert-conseil en management des données, sécurité de l’information, protection de la vie privée et nouvelles technologies

<autres contributeurs>

Versions

| Version | Action | Éditeur | État |
| --- | --- | --- | --- |
| 06/04/2025 | Création du document | Matthieu GRALL | Document de travail |
| 10/04/2025 | Rédaction de l’introduction, réorganisation et harmonisation des bonnes pratiques, ajout de l’annexe, corrections mineures (reformulations, mises en cohérences) | Matthieu GRALL | Document de travail |

Documents de référence

Les références suivantes sont utilisées entre crochets dans le corps du document :

| Libellé court | Libellé long |
| --- | --- |
| [EN 301 549] | Exigences d’accessibilité pour les produits et services ICT, *European Telecommunications Standards Institute* (ETSI, 2018)  🡪 [Lien](https://accessibilite.numerique.gouv.fr/doc/fr_301549v020102p.pdf) |
| [Guide d’hygiène de l’ANSSI] | Guide d’hygiène informatique, Agence nationale de la sécurité des systèmes d’information (ANSSI, 2017)  🡪 [Lien](https://cyber.gouv.fr/sites/default/files/2017/01/guide_hygiene_informatique_anssi.pdf) |
| [Guide sécurité de la CNIL] | Sécurité des données personnelles, Commission nationale de l’informatique et des libertés (CNIL, 2024)  🡪 [Lien](https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_2024.pdf) |
| [ISO/IEC 27002] | Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information, *International Organization for Standardization* (ISO, 2022)  🡪 [Lien](https://www.iso.org/fr/standard/75652.html) |
| [ISO/IEC 42001] | Technologies de l’information – Intelligence artificielle – Système de management, *International Organization for Standardization* (ISO, 2023)  🡪 [Lien](https://www.iso.org/fr/standard/81230.html) |
| [Lignes directrices IA de l’UE] | Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain COM(2019) 168 final (2019)  🡪 [Lien](https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52019DC0168) |
| [Loi I&L] | Loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et libertés, modifiée  🡪 [Lien](https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/) |
| [Recommandations IA de l’ANSSI - 2024] | Recommandations de sécurité pour un système d’IA générative, Agence nationale de la sécurité des systèmes d’information (ANSSI, 2024)  🡪 [Lien](https://cyber.gouv.fr/sites/default/files/document/Recommandations_de_s%C3%A9curit%C3%A9_pour_un_syst%C3%A8me_d_IA_g%C3%A9n%C3%A9rative.pdf) |
| [Recommandations IA de l’ANSSI - 2025] | Développer la confiance dans l’IA par une approche par les risques cyber (ANSSI, 2025)  🡪 [Lien](https://cyber.gouv.fr/sites/default/files/document/analyse_commune_haut_niveau_des_risques_cyber_ia.pdf) |
| [Recommandations IA de la CNIL] | Recommandations sur le développement des systèmes d’intelligence artificielle, Commission nationale de l’informatique et des libertés (CNIL, 2024)  🡪 [Lien](https://www.cnil.fr/fr/les-fiches-pratiques-ia) |
| [Règlement IA] | Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l’intelligence artificielle […] (règlement sur l’intelligence artificielle, 2024)  🡪 [Lien](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1689) |
| [RGAA] | Référentiel général d’amélioration de l’accessibilité (RGAA), Direction interministérielle du numérique (DINUM, 2023)  🡪 [Lien](https://accessibilite.numerique.gouv.fr/doc/RGAA-v4.1.2.pdf) |
| [RGESN] | Référentiel général d’écoconception de services numériques (RGESN), Autorité de régulation de la communication audiovisuelle et numérique (ARCOM, 2024)  🡪 [Lien](https://ecoresponsable.numerique.gouv.fr/docs/2024/rgesn-mai2024/referentiel_general_ecoconception_des_services_numeriques_version_2024.pdf) |
| [RGI] | Référentiel général d’interopérabilité (RGI), Direction interministérielle du numérique (DINUM, 2020)  🡪 [Lien](https://www.numerique.gouv.fr/documents/7/Referentiel_General_Interoperabilite_V2.pdf) |
| [RGIAF] | Référentiel général pour l’IA frugale (RGIAF), ministère de la transition écologique et de la cohésion des territoires (2024)  🡪 [Lien](https://greentechinnovation.fr/storage/2024/06/Referentiel-general-pour-lIA-frugale.pdf) |
| [RGPD] | Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données  🡪 [Lien](https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr) |
| [US EO 13960] | *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, *Executive Order* 13960 (2020)  🡪 [Lien](https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-promoting-use-trustworthy-artificial-intelligence-federal-government/) |
| [WCAG] | Règles pour l’accessibilité des contenus Web (*Web Content Accessibility Guidelines* - WCAG), *World Wide Web Consortium* (W3C, 2023)  🡪 [Lien](https://www.w3.org/WAI/standards-guidelines/wcag/fr) |

Ressources utilisées

**Page de garde** : Grid, par Magic Creative, de PIXABAY.

Sommaire

[1 Objet du document 5](#_Toc195168819)

[2 Introduction 5](#_Toc195168820)

[3 Bonnes pratiques pour l’IA 6](#_Toc195168821)

[3.1 Gouvernance responsable 6](#_Toc195168822)

[3.2 Fiabilité et sûreté 6](#_Toc195168823)

[3.3 Équité 7](#_Toc195168824)

[3.3.1 Réduction des biais liés à la formulation du cas d’usage 7](#_Toc195168825)

[3.3.2 Réduction des biais liés aux données d’entrée 7](#_Toc195168826)

[3.3.3 Réduction des biais liés aux données d’entrainement 7](#_Toc195168827)

[3.3.4 Réduction des biais liés à l’algorithme d’entrainement / l’architecture du modèle 8](#_Toc195168828)

[3.3.5 Réduction des biais liés aux données de sortie 8](#_Toc195168829)

[3.4 Transparence 8](#_Toc195168830)

[3.5 Sécurité des informations 8](#_Toc195168831)

[3.6 Protection des droits et libertés 9](#_Toc195168832)

[3.7 Maintenabilité et évolutivité 9](#_Toc195168833)

[3.8 Interopérabilité 10](#_Toc195168834)

[3.9 Respect de l’environnement 10](#_Toc195168835)

[3.10 Accessibilité 10](#_Toc195168836)

[Annexe : « déclaration d’applicabilité » 12](#_Toc195168837)

# Objet du document

**Ce document propose une liste de bonnes pratiques qui permettent de respecter les critères de confiance que tout système d’intelligence artificielle (IA) devrait respecter.**

Il s’inscrit dans un ensemble de documents méthodologiques en amélioration continue, destinés à aider les organismes à gérer les risques liés à l’IA, et qui peuvent être utiles ensemble ou séparément :

1. [Exemples de micro-cas d’usages de l’IA] 🡪 Lien ;
2. [Critères de confiance de l’IA] 🡪 Lien ;
3. [Bonnes pratiques de l’IA] 🡪 Lien ;
4. [Méthode de gestion des risques de l’IA] 🡪 Lien.

Il peut être directement utilisé dans le cadre des projets de nouveaux services qui reposent sur l’IA pour comparer ce qui est prévu ou mis en œuvre aux bonnes pratiques, et peut également être intégré à une démarche de gestion des risques.

# Introduction

**La multiplicité des documents de référence**, spécifiques à l’IA[[1]](#footnote-1) ou applicables à tous les systèmes[[2]](#footnote-2), **apporte de la confusion** chez ceux qui doivent ou souhaitent les appliquer.

Ils peuvent en effet sembler :

* **chacun incomplet**, car leurs périmètres diffèrent (par domaines comme la sécurité de l’information ou la protection des droits et libertés, par techniques d’IA comme les LLM[[3]](#footnote-3), par phases comme le développement, etc.). Ceci est notamment dû au fait que les problématiques liées à l’IA imposent une vision globale, alors que les périmètres de compétences et spécialités des organismes émetteurs sont restreints ;
* **tous incohérents**, car leurs structures, bonnes pratiques et terminologies diffèrent, mêmes si elles ont des similarités, et que les normes internationales[[4]](#footnote-4) ne sont pas encore matures.

Or, quand on veut mettre en œuvre un système basé sur l’IA, on doit ou on souhaite **respecter l’ensemble des références applicables, et ce, de manière cohérente** !

Ainsi, **ce document propose des bonnes pratiques harmonisées**, organisées selon les [Critères de confiance de l’IA], qui considèrent les différents [Exemples de micro-cas d’usages de l’IA], et qui peuvent être utilisées dans le cadre de la [Méthode de gestion des risques de l’IA].

L’Annexe : « déclaration d’applicabilité » peut être utilisé pour présenter les pratiques mises en œuvre en comparaison aux bonnes pratiques.

Note : un renvoi vers les documents de référence est privilégié quand cela est opportun.

# Bonnes pratiques pour l’IA

## Gouvernance responsable

Objectif : instaurer un cadre de gouvernance qui permet de partager et contrôler l’éthique des processus mis en œuvre dans les projets qui reposent sur l’IA.

Principale(s) référence(s) : [Règlement IA], [Lignes directrices IA de l’UE], [ISO/IEC 42001].

1. Formaliser les responsabilités des parties intéressées

Identifier les parties intéressées (usagers, organisations, développeurs d'IA, fournisseurs d'IA, fournisseurs de données, formateurs, institutions, etc.) et formaliser leurs responsabilités dans le cadre de l’ensemble du cycle de vie des systèmes d’IA.

1. Partager les valeurs éthiques

Impliquer, voire former, les parties intéressées pour assurer que les technologies liées à l'IA sont produites et utilisées conformément à des valeurs éthiques, en surveillant les préjugés, la confidentialité et les abus, tout en promouvant l'innovation et la confiance.

1. Déterminer des mécanismes de contrôle

Trouver et mettre en œuvre le(s) moyen(s) le(s) plus efficace(s), c’est-à-dire cohérent(s) avec la taille, la maturité et les processus existants de l’organisme, pour vérifier régulièrement que l’éthique est effectivement considérée dans les projets qui reposent sur de l’IA (ex : *reporting*, revue annuelle, indicateurs basés sur des objectifs prédéfinis, audits, rapports de gouvernance, comité d’éthique).

## Fiabilité et sûreté

Objectif : assurer la robustesse des systèmes qui reposent sur l’IA afin d’améliorer leur fiabilité et la sécurité des biens et des personnes.

Principale(s) référence(s) : [Règlement IA], [Lignes directrices IA de l’UE].

1. Vérifier les données d’entrée possibles

Vérifier les particularités des données futures, par exemple à l’aide de modules spécifiques dans la chaine de traitements de données.

1. Vérifier la robustesse du modèle

Vérifier que le modèle ne peut pas être attaqué pour produire un résultat indésirable, par exemple dans le cadre d’une chaine de modèles.

1. Éprouver les limites du système dans sa globalité

Mettre en place des mesures pour éprouver et consolider le système d’IA (ex : tests de charge et de stress, simulations d’attaques, redondances techniques, procédures de réponse aux incidents) en considérant l’amont et l’aval du système d’IA.

1. Évaluer les performances du système

Faire des mesures quantitatives pour évaluer les performances du modèle dans diverses conditions de stress, notamment les attaques contradictoires, le bruit et les changements de distribution des données (ex : taux de faux positifs/négatifs, étude de l’erreur quadratique moyenne – MSE, distance de Wasserstein, score de Brier).

1. Mettre en place les mesures de sûreté nécessaires

Tester et valider le système d’IA pour répondre aux normes de sûreté et aux exigences réglementaires dans les applications où la sûreté est primordiale (ex : véhicules autonomes, soins de santé), intégrer plusieurs mesures redondantes pour gérer les pannes sans causer de dommages ni de perturbations significatives, laisser la main à l’humain, en particulier dans le cadre de prises de décisions critiques, pour intervenir, outrepasser ou guider les actions de l'IA si nécessaire.

## Équité

Objectif : détecter et corriger les biais par des mécanismes de vérification et d’audit des algorithmes.

Principale(s) référence(s) : [Règlement IA de l’UE], [Recommandations IA de la CNIL].

### Réduction des biais liés à la formulation du cas d’usage

1. Définir clairement le(s) cas d’usage(s)

Décrire précisément le cas d’usage, les limitations et les exceptions, et s’assurer que les personnes en charge de la conception et du développement des outils en ont connaissance et les comprennent.

### Réduction des biais liés aux données d’entrée

1. Diversifier les données d’entrée

Utiliser des sources de données diverses et représentatives.

1. Rendre les données exploitables

Limiter les données qu’à celles qui seront traitées, les transformer / intégrer de façon cohérente (ex : via une ontologie qui sert de pivot), et les nettoyer de manière approfondie, afin de faciliter leur traitement, de ne pas traiter de données inutilisables, inutiles, sujettes à des règles internes ou externes, ou qu’on ne souhaite pas traiter.

### Réduction des biais liés aux données d’entrainement

1. S’assurer de la qualité des données d’entrainement

Vérifier la pertinence des données par rapport au problème à résoudre, leur fiabilité (crédibles et/ou de sources objectives), et la légalité de leur collecte et de leur traitement.

1. Faire des échantillonnages équilibrés des données d’entrainement

Respecter les bonnes pratiques d’échantillonnage pour que les échantillons soient équilibrés.

1. Corriger les corrélations indésirables

Identifier les corrélations entre les caractéristiques ou les variables, évaluer leur impact et gérer ceux qui ne sont pas acceptables.

1. Collecter de nouvelles données dès que cela est nécessaire

Recourir à de nouvelles données d’entrée jusqu’à avoir l’assurance que les biais sont suffisamment réduits.

### Réduction des biais liés à l’algorithme d’entrainement / l’architecture du modèle

1. Évaluer la qualité du modèle

Mesurer l'équité à l’aide de modèles mathématiques, comme l'indépendance statistique, les intervalles de confiance, l'étude de séparation et l'étude de suffisance.

1. Évaluer les performances du modèle

Évaluer les performances de l'algorithme de manière régulière.

1. Faire auditer le modèle

Réaliser un audit pour identifier et corriger les biais.

### Réduction des biais liés aux données de sortie

1. Valider les données de sorties

Valider les résultats produits, si possible de manière continue, voire consulter des experts en éthique et inclusion.

1. Obtenir les retours des usagers

Collecter régulièrement les commentaires et retours d'expérience des usagers, pour détecter et corriger les biais dans les résultats.

## Transparence

Objectif : rendre explicites les algorithmes et les processus de décision via une documentation accessible, des interfaces interactives et des explications techniques adaptées aux différents publics.

Principale(s) référence(s) : [Règlement IA], [Lignes directrices IA de l’UE].

1. Formaliser les éléments utiles à la transparence

Élaborer les explications[[5]](#footnote-5) nécessaires à la transparence[[6]](#footnote-6), notamment pour expliquer d’où les données proviennent les données, la forme qu’elles prennent et leur utilisation par l’organisme, et les faire connaître[[7]](#footnote-7) aux personnes chargées de créer et de maintenir les modèles et les flux de données, aux usagers, et aux autorités compétentes.

## Sécurité des informations

Objectif : appliquer les bonnes pratiques de sécurité de l’information au système d’IA, pour réduire les risques sur l’organisme en cas de disparition de données, de modification non désirée de données ou d’accès non autorisé à des données, tout le long du cycle de vie du système.

Principale(s) référence(s) : [Recommandations IA de l’ANSSI - 2024], [Recommandations IA de l’ANSSI - 2025].

1. Respecter les recommandations de l’ANSSI

Appliquer les [Recommandations IA de l’ANSSI - 2024] (chapitre 5) applicables dans le cas d’un système d’IA générative et les [Recommandations IA de l’ANSSI - 2025] (annexe I).

1. Adopter des bonnes pratiques de sécurité de l’information

Appliquer la politique de sécurité des systèmes d’information, ou les bonnes pratiques de sécurité de l’information applicables selon la maturité de l’organisme en la matière (ex : [Guide sécurité de la CNIL], [Guide d’hygiène de l’ANSSI], [ISO/IEC 27002]).

## Protection des droits et libertés

Objectif : appliquer les grands principes de la protection de la vie privée au traitement de données par IA, pour réduire les risques sur les personnes concernées en cas de disparition de données, de modification non désirée de données ou d’accès non autorisé à des données.

Principale(s) référence(s) : [Recommandations IA de la CNIL], [Loi I&L], [RGPD].

1. Respecter les recommandations de la CNIL

Appliquer les [Recommandations IA de la CNIL] applicables dans le cas d’une phase de développement.

1. Mettre le traitement en conformité avec la réglementation

Formaliser les éléments nécessaires[[8]](#footnote-8) à la personne / au service en charge de la protection de la vie privée pour bâtir la conformité du traitement de données à caractère personnel à la [Loi I&L] / au [RGPD].

## Maintenabilité et évolutivité

Objectif : assurer performances, maintien en conditions opérationnelle et de sécurité, intégration de nouvelles fonctionnalités, et comptabilité ascendante, tout le long du cycle de vie du système d’IA.

Principale(s) référence(s) : [Règlement IA], [ISO/IEC 42001].

1. Adopter un principe de modularité et de réutilisabilité

Mettre en œuvre une conception modulaire du système d'IA, pour réutiliser/remplacer les composants de la chaîne sans affecter l'ensemble du système.

1. Documenter le système

Élaborer une documentation complète, qui comprend des commentaires sur le code, des manuels d'utilisation et une documentation sur le prétraitement des données, la formation des modèles et les processus de déploiement.

1. Contrôler la qualité du code

Appliquer les bonnes pratiques de développement pour produire un code de haute qualité, notamment des conventions de nommage appropriées, un style cohérent et des algorithmes efficaces.

1. Permettre l’évolutivité

Concevoir le système pour gérer des charges accrues et évoluer selon les besoins. Ceci implique également le maintien des performances et la gestion des ressources.

1. Maîtriser les évolutions

Mettre en œuvre un processus de gestion des évolutions, qui intègre la veille technologique, les tests de comptabilité ascendante, l’automatisation des correctifs et mises à jour, le contrôle des versions[[9]](#footnote-9), et la surveillance des performances.

## Interopérabilité

Objectif : assurer l’interopérabilité fluide des données et des technologies sur lesquelles elles reposent.

Principale(s) référence(s) : [RGI].

1. Assurer la comptabilité des données

Identifier les sources de données, les données consommées, les traitements de données effectués et les données produites, vérifier que ces données sont référencées (ex : dans une ontologie pivot) pour faciliter leur interopérabilité et leur réutilisation.

1. Adopter des bonnes pratiques d’interopérabilité

Appliquer les bonnes pratiques applicables du [RGI] et, le cas échéant, vérifier la conformité aux outils autorisés en interne pour favoriser l’interopérabilité des technologies[[10]](#footnote-10).

## Respect de l’environnement

Objectif : réduire globalement les besoins en ressources matérielles et énergétiques et les impacts environnementaux associés.

Principale(s) référence(s) : [RGESN], [RGIAF].

1. Adopter des bonnes pratiques d’écoconception

Identifier la consommation d'énergie des centres de données (*data centers*) lors de l’entrainement des modèles, l'économie circulaire du matériel, l'empreinte carbone, l'obsolescence et les déchets électroniques, et appliquer les bonnes pratiques applicables du [RGESN] ou du [RGIAF].

## Accessibilité

Objectif : intégrer les principes d’accessibilité numérique dès la conception et tester régulièrement l’interface pour garantir une utilisation inclusive.

Principale(s) référence(s) : [RGAA], [EN 301 549], [WCAG].

1. Adopter des bonnes pratiques d’accessibilité

Se conformer au [RGAA] en appliquant les bonnes pratiques applicables de l’[EN 301 549] ou des [WCAG][[11]](#footnote-11), en visant l'accessibilité et l'autonomisation des usagers, pour favoriser une expérience d'IA positive et inclusive pour tous les usagers.

# Annexe : « déclaration d’applicabilité »

Notes :

* l’objectif est d’une part de vérifier qu’on n’a rien oublié, et d’autre part d’apporter des éléments nécessaires à la prise de décision d’accepter ou non la mise en exploitation du système d’IA ;
* les bonnes pratiques ne sont pas toutes applicables à un projet donné : certaines ne sont pas applicables (ex : si elles concernent un type d’IA qui n’est pas celui considéré), n’ont pas besoin d’être appliquées (ex : si le sujet est traité par ailleurs), ou sont exclues par l’organisation.

| Bonnes pratiques | Applicabilité | Si oui, comment ? Si non, pourquoi ? |
| --- | --- | --- |
| **Gouvernance responsable** | | |
| Formaliser les responsabilités des parties intéressées | Oui  Non  Ne sait pas |  |
| Partager les valeurs éthiques | Oui  Non  Ne sait pas |  |
| Déterminer des mécanismes de contrôle | Oui  Non  Ne sait pas |  |
| **Fiabilité et sûreté** | | |
| Vérifier les données d’entrée possibles | Oui  Non  Ne sait pas |  |
| Vérifier la robustesse du modèle | Oui  Non  Ne sait pas |  |
| Éprouver les limites du système dans sa globalité | Oui  Non  Ne sait pas |  |
| Évaluer les performances du système | Oui  Non  Ne sait pas |  |
| Mettre en place les mesures de sûreté nécessaires | Oui  Non  Ne sait pas |  |
| **Équité** | | |
| Définir clairement le(s) cas d’usage(s) | Oui  Non  Ne sait pas |  |
| Diversifier les données d’entrée | Oui  Non  Ne sait pas |  |
| Rendre les données exploitables | Oui  Non  Ne sait pas |  |
| S’assurer de la qualité des données d’entrainement | Oui  Non  Ne sait pas |  |
| Faire des échantillonnages équilibrés des données d’entrainement | Oui  Non  Ne sait pas |  |
| Corriger les corrélations indésirables | Oui  Non  Ne sait pas |  |
| Collecter de nouvelles données dès que cela est nécessaire | Oui  Non  Ne sait pas |  |
| Évaluer la qualité du modèle | Oui  Non  Ne sait pas |  |
| Évaluer les performances du modèle | Oui  Non  Ne sait pas |  |
| Faire auditer le modèle | Oui  Non  Ne sait pas |  |
| Valider les données de sorties | Oui  Non  Ne sait pas |  |
| Obtenir les retours des usagers | Oui  Non  Ne sait pas |  |
| **Transparence** | | |
| Formaliser les éléments utiles à la transparence | Oui  Non  Ne sait pas |  |
| **Sécurité des informations** | | |
| Respecter les recommandations de l’ANSSI | Oui  Non  Ne sait pas |  |
| Adopter des bonnes pratiques de sécurité de l’information | Oui  Non  Ne sait pas |  |
| **Protection des droits et libertés** | | |
| Respecter les recommandations de la CNIL | Oui  Non  Ne sait pas |  |
| Mettre le traitement en conformité avec la réglementation | Oui  Non  Ne sait pas |  |
| **Maintenabilité et évolutivité** | | |
| Adopter un principe de modularité et de réutilisabilité | Oui  Non  Ne sait pas |  |
| Documenter le système | Oui  Non  Ne sait pas |  |
| Contrôler la qualité du code | Oui  Non  Ne sait pas |  |
| Permettre l’évolutivité | Oui  Non  Ne sait pas |  |
| Maîtriser les évolutions | Oui  Non  Ne sait pas |  |
| **Interopérabilité** | | |
| Assurer la comptabilité des données | Oui  Non  Ne sait pas |  |
| Adopter des bonnes pratiques d’interopérabilité | Oui  Non  Ne sait pas |  |
| **Respect de l’environnement** | | |
| Adopter des bonnes pratiques d’écoconception | Oui  Non  Ne sait pas |  |
| **Accessibilité** | | |
| Adopter des bonnes pratiques d’accessibilité | Oui  Non  Ne sait pas |  |

1. Notamment [ISO/IEC 42001], [Recommandation IA de l’OCDE], [Recommandations IA de l’ANSSI - 2024], [Recommandations IA de l’ANSSI - 2025], [Recommandations IA de la CNIL], [Règlement IA] et [RGIAF]. [↑](#footnote-ref-1)
2. Notamment [Loi I&L] (dont [RGPD]), [RGAA], [RGESN], et [RGI]. [↑](#footnote-ref-2)
3. LLM : *large language models* (grands modèles linguistiques). [↑](#footnote-ref-3)
4. Ex : [ISO/IEC 42001]. [↑](#footnote-ref-4)
5. L’explicabilité peut reposer sur des méthodes agnostiques ou spécifiques, intrinsèques ou post-hoc, locales ou globales, a priori ou a posteriori. Des outils tels que LIME ou SHAP peuvent notamment contribuer à cette explicabilité. [↑](#footnote-ref-5)
6. La transparence s’applique aux algorithmes (logique et modèle), aux interactions (via l’interface utilisateur), et à la société (impact social de cette interaction). [↑](#footnote-ref-6)
7. Ex : publier de la documentation technique, développer des interfaces explicatives, créer des tutoriels et guides d’usage, organiser des ateliers d’information. [↑](#footnote-ref-7)
8. Finalité, données traitées, durées de conservation, destinataires, mesures prévues pour assurer la minimisation et la qualité des données, mesures prévues pour assurer l’information et les droits des personnes concernées (le cas échéant, d’accès, à la portabilité, de rectification, d’effacement, de limitation et d’opposition) et, le cas échéant, mesures prévues pour encadrer la sous-traitance et le transfert en dehors de l’UE. [↑](#footnote-ref-8)
9. Recourir à un système de contrôle de version permet de suivre les modifications, de collaborer avec d'autres et de revenir aux versions précédentes si nécessaire. [↑](#footnote-ref-9)
10. Notamment : utiliser des standards ouverts, respecter les API publiques, favoriser la portabilité des données, assurer la documentation des interfaces. [↑](#footnote-ref-10)
11. Cela implique notamment de concevoir des interfaces ergonomiques, ou plusieurs modes d’interactions, en tenant compte de facteurs tels que la diversité linguistique et l’accessibilité pour les personnes handicapées, et de les tester avec des usagers en situation de handicap. [↑](#footnote-ref-11)