Les impacts sociétaux

L’IA ACT ou Règlement (UE) 2024/1689 du 13 juin 2024 établit des règles harmonisées concernant l’intelligence artificielle. Il définit l’IA comme « un système automatisé qui est conçu pour fonctionner à différents niveaux d’autonomie et peut faire preuve d’une capacité d’adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu’il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels » (Article 2). Ce règlement vise à garantir, par son article 4 entré en application le 2 février 2025, la maîtrise des systèmes d’IA, en protégeant des valeurs fondamentales telles que les droits humains, la démocratie, l’état de droit, la santé, la sécurité et l’environnement. Il interdit certaines pratiques jugées dangereuses, comme la manipulation comportementale subliminale, la notation sociale, ou la reconnaissance biométrique en temps réel dans les lieux publics.

- Impacts éthiques
- Impacts environnementaux
- Sécurité

Impacts éthiques

La CNIL (Commission Nationale de l'Informatique et des Libertés) a animé un débat public en 2017 sur les enjeux éthiques des algorithmes et de l'intelligence artificielle (IA). Un rapport, résultat de contributions, a été publié. Il explore les implications de l'utilisation croissante des algorithmes et de l'IA et propose des recommandations pour encadrer leur développement de manière éthique et responsable. Ce rapport1 souligne la nécessité d'une approche collective et pluridisciplinaire pour relever les défis éthiques posés par les algorithmes et l'IA, et propose des pistes pour une gouvernance éthique de ces technologies.
Différents rapports indiquent que la diffusion de l'IA dans notre quotidien, entraînera certainement une évolution des métiers. Certaines tâches seront automatisées, de nouvelles verront le jour. Le potentiel d'automatisation de nombreuses activités, peut permettre d'augmenter la productivité. En aidant à automatiser des actions répétitives et routinières, l'IA laisse la possibilité de se concentrer sur des tâches plus complexes et à plus forte valeur ajoutée.
Il est donc crucial d'investir dans la formation pour permettre à tous les collaborateurs de s'adapter aux changements apportés par l'IA.
La CNIL recommande que le déploiement de l'IA soit accompagné d'un dialogue social et d'une régulation appropriée
pour s'assurer que les bénéfices de l'IA sont partagés équitablement et que les risques salariés sont maîtrisés. Cela peut se matérialiser par la mise en place de politiques pour protéger les personnes contre les abus potentiels de l'IA, comme la surveillance excessive ou la perte d'autonomie au travail.



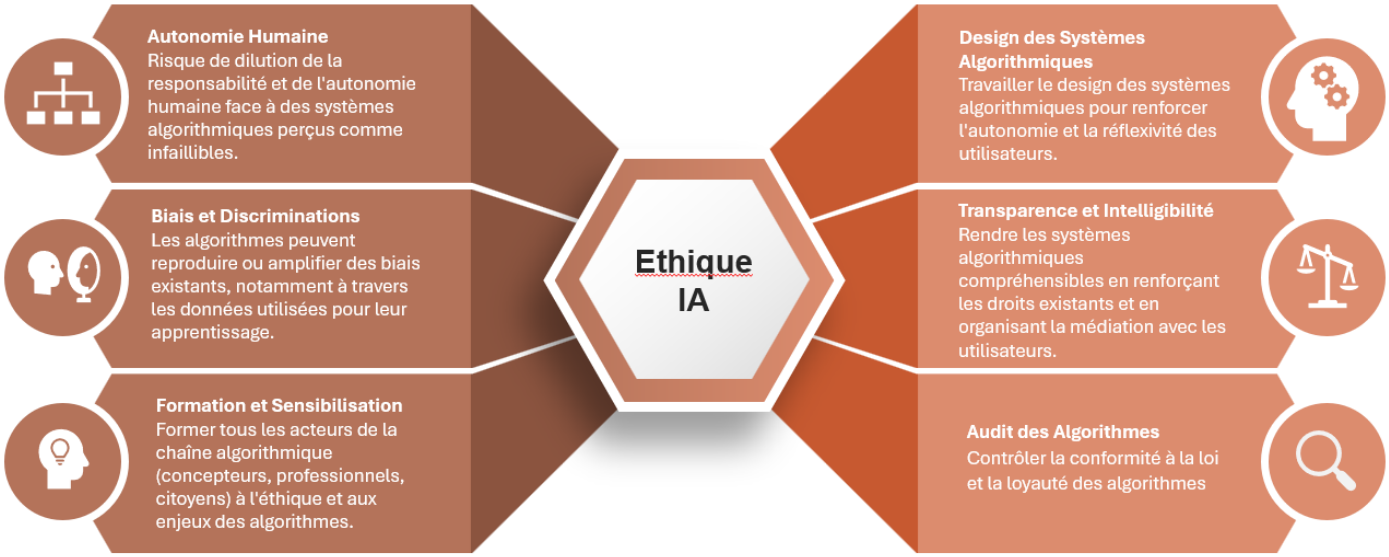
Les lignes directrices en matière d'éthique pour une IA digne de confiance, IA Act adopté en 2024, définissent :

- Les fondements d'une IA digne de confiance qui nécessitent de reconnaître et de résoudre les tensions entre les 4 principes éthiques que sont le respect de l'autonomie humaine, la prévention de toute attente, l'équité, l'explicabilité.
- La réalisation d'une IA de confiance qui nécessite d'évaluer et de répondre de manière continue tout au long du cycle de vie du système IA à 7 exigences essentielles que sont action humaine et contrôle humain, robustesse technique et sécurité, respect de la vie privée et gouvernance des données, transparence, diversité non-discrimination et équité, bien-être sociétal et environnemental, responsabilité.
- L'évaluation d'une IA digne de confiance.

Commission européenne, Direction générale des réseaux de communication, du contenu et des technologies et Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji,

Lignes directrices en matière d'éthique pour une IA digne de confiance, Publications Off ice,2019,

Illustration d'éléments de risques et solutions identifiées dans les lignes directrices en matière d'éthique pour une IA digne de confiance



Des labels IA, comme Labelia (Labelia, le label — Labelia (ex Substra Foundation), se sont développés pour donner des indications sur le respect de l'éthique dans les solutions proposées.

Points clés
→ Intégrer les risques et impacts de l'IA dans la politique RSE,
→ Développer des formations de sensibilisation à l'IA, à la conduite du changement IA,
→ Favoriser les systèmes d'IA renforçant l'autonomie et la réflexivité des utilisateurs.

Impacts environnementaux

Plusieurs chercheurs ont exploré les implications de l'adoption généralisée de l'IA, en particulier des modèles de langage de grande taille comme ChatGPT sur la consommation d'électricité mondiale des centres de données.

Consommation Énergétique et Ressources :

> « Depuis 2022, l'IA a connu une croissance rapide. L'essor des applications d'IA générative, comme ChatGPT, entraîne une augmentation continue de la demande en ressources énergétiques et en eau. Par exemple, l'entraînement de modèles d'IA complexes peut générer une quantité de CO2 équivalente à celle émise par un vol commercial transcontinental ou par plusieurs voitures sur toute leurdurée de vie, incluant leur fabrication » (L'intelligence artificielle : une pollution cachée au coeur de l'innovation - Institut Supérieur de l'Environnement - ISE).

Les centres de données consomment environ 1% de l'électricité mondiale. L'augmentation de l'utilisation de l'IA pourrait entraîner une hausse significative de cette consommation.

Efforts pour Réduire l'Impact Environnemental :

Des entreprises fournisseurs de solutions IA s'engagent à réduire l'impact environnemental de leurs outils d'IA. Elles fournissent des moyens de calculer les émissions de CO2 associées à l'utilisation de l'IA, prenant en compte l'énergie nécessaire pour chaque requête et entraînement, la fréquence de ces entraînements, et la quantité de CO2 produite par la source d'énergie utilisée. Elles cherchent à optimiser l'efficacité énergétique et à utiliser des sources d'énergie renouvelable pour atténuer l'empreinte carbone de leurs technologies. Toutefois les modèles qui se veulent moins énergivores comme le modèle BLOOM a consommé 433 MWh d'électricité lors de son entraînement. La phase d'inférence, où les modèles génèrent des résultats à partir de nouvelles données, est également significative en termes de consommation d'énergie. Des études suggèrent que cette phase pourrait représenter une grande partie des coûts énergétiques totaux des modèles d'IA. Des améliorations en termes d'efficacité énergétique des modèles et des algorithmes pourraient atténuer cet impact, mais paradoxalement l'augmentation de l'efficacité pourrait entraîner une hausse de la demande.

Régulation et Transparence : L'Union européenne a adopté l'IA ACT en 2024.



L'exigence 6 pour la réalisation d'une IA de confiance est « Bien-être sociétal et environnemental » et comprend la durabilité et le respect de l'environnement.

Paragraphe 84 : *« IA durable et respectueuse de l'environnement. Les systèmes d'IA promettent de contribuer à répondre à certaines des plus vives préoccupations de la société ; il faut cependant veiller à ce que les réponses apportées soient aussi respectueuses de l'environnement que possible. Il convient, à cet égard, d'évaluer le processus de mise au point, de déploiement et d'utilisation du système, ainsi que toute sa chaîne d'approvisionnement, par exemple au moyen d'un examen critique de l'utilisation des ressources et de la consommation d'énergie au cours de l'entraînement, en réalisant les choix les moins préjudiciables. Il convient d'encourager les mesures permettant de garantir que l'ensemble de la chaîne d'approvisionnement du système d'IA respecte l'environnement.»*

Il est impératif de considérer la nécessité d'utiliser l'IA et de peser les bénéfices par rapport aux coûts énergétiques. Les régulateurs pourraient envisager d'introduire des exigences spécifiques de divulgation environnementale pour améliorer la transparence dans la chaîne d'approvisionnement de l'IA.

> Alex de Vries dans l'article « The growing energy footprint of artificial intelligence », souligne l'importance de tempérer les attentes tant optimistes que pessimistes concernant l'impact énergétique de l'IA. Bien que l'IA puisse entraîner une augmentation significative de la consommation d'électricité, divers facteurs de ressources sont susceptibles de limiter cette croissance à court terme. Il est également peu probable que les améliorations en termes d'efficacité énergétique compensent entièrement les changements à long terme dans la consommation d'énergie liée à l'IA.



L’impact environnemental de l’IA doit être mis en regard de ses potentiels bénéfices. Grâce à la capacité d’optimiser des processus complexes, l’IA pourrait permettre de réduire fortement les émissions de gaz à effet de serre dans de nombreux secteurs : énergie, transports, agriculture, logement...
Par ailleurs, l’IA pourrait accélérer la transition écologique en diminuant la dépendance au sentier de l’innovation. Des cas concrets d’accélération de l’innovation apparaissent, mais doivent encore être soutenus.
Recommandation n° 5 Faire de la France un pionnier de l’IA pour la planète en renforçant la transparence environnementale, la recherche dans des modèles à faible impact, et l’utilisation de l’IA au service des transitions énergétique et environnementales.

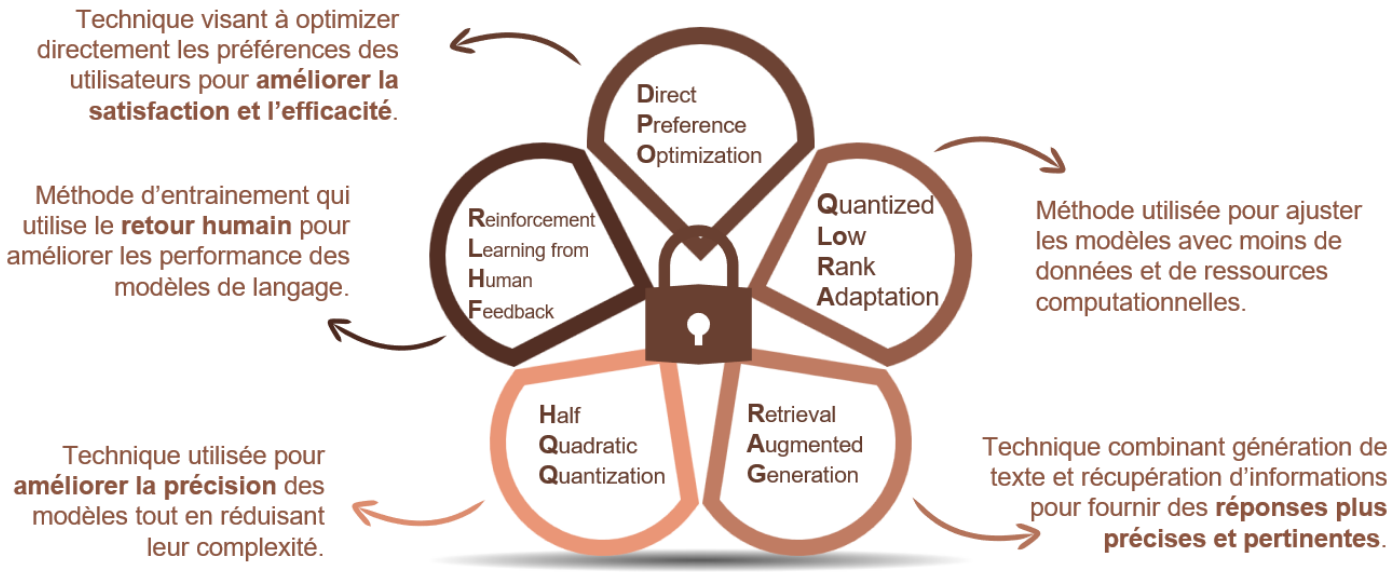
Points clés
→ Mettre au regard de l’impact environnemental de l’IA ses potentiels bénéfices, peser le coût énergivore du déploiement de l’IA et le levier de réduction carbone,
→ Intégrer la stratégie environnementale dans la gouvernance de l’IA,
→ Intégrer l’IA dans les scopes 3 et dans la stratégie climat, faire des choix technologiques éclairés, déployer des solutions d’IA frugales dès la conception.

Sécurité

Imperfections

Les IA génératives suscitent un paradoxe : nous attendons d'elles qu'elles inventent et créent, tout en étant précises et fiables. Or, les IA peuvent créer des réponses incorrectes ou incohérentes en cherchant à créer (hallucinations). Le grounding, qui consiste à ancrer les réponses dans des données réelles et contextuelles, permet de de réduire les risques d'erreurs.
Le risque de sécurité lié aux IA génératives est le risque le moins souvent cité par les coopératives lors de notre enquête, l'IA générative étant actuellement moins présente que les autres types d'IA dans les coopératives de nutrition animale.
Nous pouvons citer quelques types d'imperfections :
→ L'injection indirecte de prompt peut être une source d'erreur pour l'assistant virtuel. Il répondra à des instructions
cachées dans des documents analysés.
→ Le piratage dans un contexte de récompense, les modèles de langage peuvent exploiter des failles dans les
spécifications pour obtenir des scores élevés sans répondre à la véritable intention de l'utilisateur.
→ Glitch tokens, une requête avec un mot mal orthographié conduit l'assistant virtuel à répondre de manière
incohérente en lien avec une erreur non détectée dans l'algorithme.

Pour aller plus loin, OWASP a publié le top 10 des risques pour les LLM et application d'IA générative. Des solutions ont été développées pour remédier à ces imperfections (Cf schéma ci-dessous).



Malveillance

L'hyper connectivité, leur niveau d'automatisation en environnement OT (technologique-opérationnel) expose les coopératives de nutrition animale à la cybercriminalité, au cyberterrorisme, à la biosécurité, à la désinformation.
Lors de l'enquête menée auprès des coopératives de nutrition animale en mai 2025, cyberattaque, fuite des données, perte de confidentialité, blocage du fonctionnement, perte de maîtrise de l'outil, malveillance, sont les risques liés à l'IA très majoritairement cités. La sécurité est bien perçue comme un facteur à prendre en compte lors de la mise en place de solutions IA.
Si l'utilisation de l'IA peut augmenter l'exposition aux algorithmes malveillants, l'IA grâce à sa capacité d'entraînement et de traitement de données massives permet en contrepartie d'apporter des solutions à la cybersécurité industrielle, analyse des risques, détection proactive, adaptation aux modèles d'attaque. De multiples solutions ont été développées par un panel d'acteurs pour trouver des solutions de défense adaptées aux besoins.
L'**Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)** a publié en mai 2025 un **article** sur les nouveaux risques inhérents à l'introduction de nouvelles technologies dans le domaine des systèmes industriels à travers l'exemple de l'Industrial Internet of Things (IIoT). Il propose un modèle d'architecture de passerelle d'interconnexion sécurisée entre les mondes industriel et de gestion sans nécessiter la refonte de l'architecture du système industriel en profondeur. L'article vise un **public de DSI**.

L'European Union Agency for cybersecurity (ENISA) propose également des **référentiels de management du risque**.

> « Giskard s'est donné comme mission de combler le fossé entre la technologie complexe de l'intelligence artificielle (IA) et son application dans des scénarios réels, en garantissant la robustesse et la transparence. Giskard est une solution en open source, dédiée à l'amélioration de la qualité de l'IA. En minimisant les erreurs de l'IA telles que les biais éthiques et les risques de sécurité, Giskard permet la création de modèles d'IA supérieurs pouvant être déployés en production. » (Alex Combessie, co-fondateur de Giskard).

Souveraineté

A travers l'enquête menée en mai 2025, les coopératives de nutrition animale expriment leur besoin de souveraineté, au sens contrôle de leurs données, sécurisation de leurs infrastructures, maîtrise de leurs algorithmes.
Le besoin de maîtrise au niveau du territoire national ou au sein de d'un espace de confiance comme l'union Européenne est perceptible. Les fournisseurs de solutions, d'algorithme, d'espaces de stockage, les API, les sources et partages de données des modèles sont à prendre en compte pour répondre à ce besoin de maîtrise.

> Mistral AI, est une startup française pionnière en intelligence artificielle fondée en avril 2023. Elle s'est fixée comme mission : démocratiser l'intelligence artificielle grâce à des modèles, produits et solutions IA open-source, efficaces et innovants.

Les fuites de données sont parfois liées à l'utilisation de l'IA générative par les personnes avec leurs outils de travail.
Elles peuvent être tentées d'utiliser l'IA générative en libre accès, s'ils leur semblent que la mise en place est trop lente dans leur structure. Cette Shadow IA peut présenter un danger si la coopérative n'a pas mis en place les sécurités nécessaires. Une charte d'utilisation de l'IA peut s'avérer utile.

> **Points clés**
> **→ Trouver le bon équilibre entre besoin de créativité et nécessité d'avoir des données sûres et fiables,**
> **→ Intégrer dans les algorithmes des solutions pour lutter contre les imperfections,**
> **→ Analyser les risques pour la cybersécurité, intégrer l'IA pour la cyberdéfense,**
> **→ Faire des choix technologiques éclairés en lien avec la volonté de souveraineté de la coopérative.**