

L'INTELLIGENCE ARTIFICIELLE : L'IA A QUOI CA SERT ?



« L'intelligence artificielle promet d'énormes avantages mais comporte également des risques réels. Certains de ces risques se matérialisent déjà en préjudices pour les individus et les sociétés : biais et discrimination, polarisation des opinions, atteintes à la vie privée, et problèmes de sécurité. Une IA digne de confiance appelle les gouvernements du monde entier à développer des approches interopérables basées sur les risques en matière de gouvernance de l'IA et une compréhension rigoureuse des incidents et des dangers liés à l'IA. »

Extrait du site de l'OCDE au sujet de l'IA »

Les personnages principaux en lien avec l'IA et quelques données



Les Pionniers

75% d'entre nous ont déjà utilisé au moins une fois une IA : la révolution est en marche !



Le Protagoniste

Le Chat bot/programme informatique basé sur l'IA comme Chat GPT est l'outil star, utilisé pour rédiger, inspirer et rechercher.



La Quête de Savoir

Dans le monde 85% des individus voudraient se former facilement et sans effort.



L'Antagoniste

Plus de 45% de la population est consciente des risques, mais ne sait par où commencer !

ILS DOMINAIENT LE MONDE AVANT DE DISPARAÎTRE

Des exemples d'entreprises qui n'ont pas cru à l'évolution technologique.

Il faut vivre avec son temps !

Kodak

Le roi de la pellicule photo qui a ignoré
le numérique qu'il avait lui-même
inventé

Blockbuster

Le géant de la location de films qui a ri
au nez de Netflix et du streaming

Virgin Mégastore

Le temple du CD et du DVD, submergé
par la musique en ligne.

D'autres ont transformé la menace en opportunité et ont évolué



Face aux vendeurs en ligne, les concessions automobiles ont misé sur le service et la confiance.



Défiées par les réseaux sur internet, les agences Immobilières ont renforcé leur expertise locale.



Face à Amazon, les libraires sont devenus des lieux de conseil et de communauté.



Face à Booking, les agences de voyages se sont spécialisées dans le sur-mesure.

Les risques d'une utilisation non ciblée et structurée



Fuites de Données

Chaque information sensible que nous lui confions (stratégies, données personnelles) peut devenir une faille de sécurité béante, exploitable par des acteurs malveillants.



Biais & Discrimination

Nourrie avec des données humaines, l'IA reproduit nos pires préjugés. Elle peut écarter un CV à cause d'un nom ou d'une adresse, créant des injustices invisibles et systématiques.



"Hallucinations"

L'IA ne dit pas "je ne sais pas". Elle invente. Une affirmation erronée, présentée avec une confiance absolue, peut conduire à des décisions désastreuses basées sur des mensonges.

L'hallucination correspond à une erreur produite par un modèle génératif qui invente une information sans fondement, tandis qu'un deepfake est une falsification volontaire de contenus existants, créée pour tromper en manipulant images, vidéos ou voix.

Evolutions ?

Depuis 2022, l'IA générative a bouleversé le grand public et les entreprises, ouvrant la voie à de nouvelles formes de création automatisée.



D'ici 2026, la consommation électrique mondiale des data centers (poussée par l'IA) pourrait dépasser celle du Japon.

Un questionnaire de 10 à 50 questions avec une IA « boit » ou «consomme » l'équivalent d'une bouteille d'eau de 500ml pour refroidir les serveurs.



La révolution a un coût que l'on ne peut plus ignorer. Faut-il pour autant s'en passer ?

Comment réduire notre impact ?

3 réflexes simples et conseils

1

Soyez précis

Un prompt clair et détaillé du premier coup évite de multiples allers-retours énergivores. Ex dans un mail, il vaut mieux rédiger n message de 150 mots..." que de faire des allers-retours entre correspondant... . Le questionnement avec l'IA est identique.

2

Regroupez vos demandes

Intégrer la politesse ou les instructions secondaires dans votre demande principale. "Pourrais-tu me faire X, en adoptant un ton formel s'il te plaît ?" consomme moins que deux prompts séparés.

3

Évitez le superflu

Chaque interaction a un coût. Les conversations inutiles, les tests "pour voir" ou les questions redondantes s'additionnent. Pensez avant de « prompter », préparer votre demande.

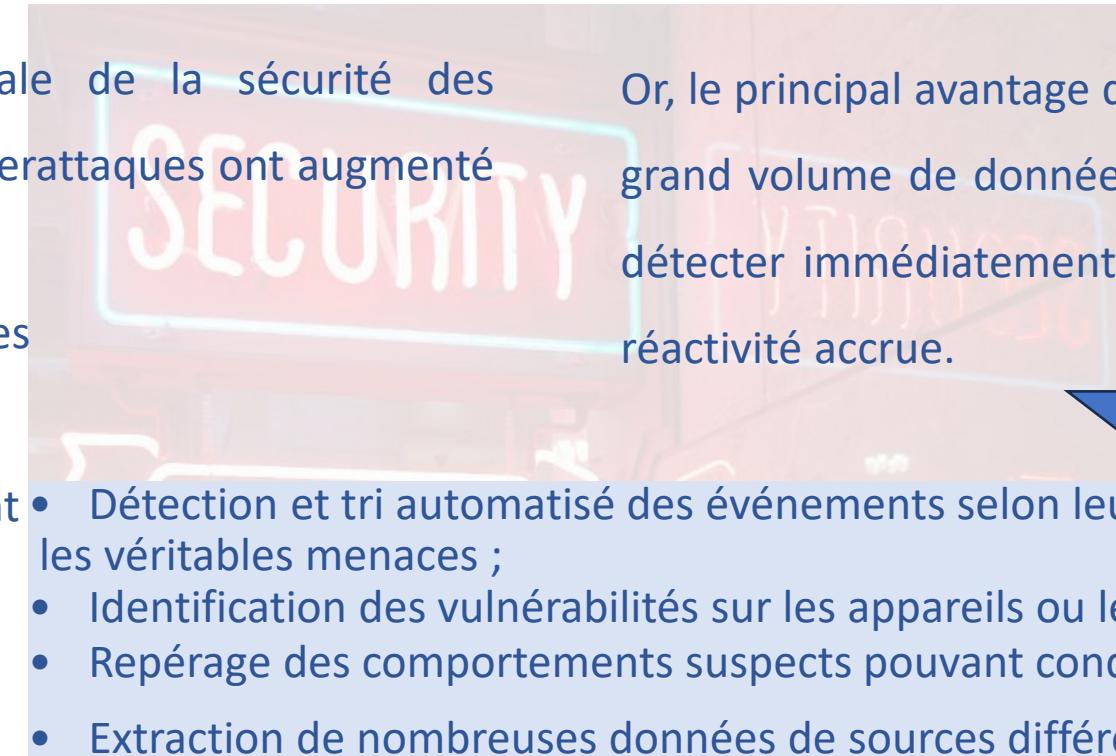
Les risques et la solution ?

Les risques !

Selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information), les cyberattaques ont augmenté de 15 % en 2024.

Parmi les victimes, les entreprises sont particulièrement touchées.

Ainsi, TPE, PME, ETI représentent 37 % des victimes et les entreprises stratégiques 12 %.



La solution ?

Or, le principal avantage de l'IA est sa capacité à traiter un grand volume de données en temps réel. Elle peut donc détecter immédiatement les incidents et permettre une réactivité accrue.



- Détection et tri automatisé des événements selon leur importance, qui permet d'identifier les véritables menaces ;
- Identification des vulnérabilités sur les appareils ou les applications ;
- Repérage des comportements suspects pouvant conduire à des cyberattaques ;
- Extraction de nombreuses données de sources différentes afin de les analyser précisément.

Comment faire ?

Il est préconisé à ce jour, de suivre les préconisations page 7

Nous ne pouvez pas vous empêcher vos salariés (en dehors de votre règlement intérieur et consignes particulières) de faire des recherches de la sorte, cependant, nous vous préconisons la plus grande vigilance sur vos types de recherche. Nous vous invitons à aller sur le site de la CNIL et d'utiliser son Mooc sur le RGPD, Vous pouvez aussi partager avec vos salariés le glossaire mis à la disposition de tous par la CNIL,

Les Liens :

- **Mooc de la Cnil** : <https://video.cnil.fr/w/1S54Gw3mZNP8gS1Z9YuTcP>
- **Inscription** : <https://atelier-rgpd.cnil.fr/login/index.php>

Glossaire de l'IA

Vous trouverez toutes les définitions dans ce glossaire, issu de la CNIL.

Glossaire de l'intelligence artificielle (IA) : <https://www.cnil.fr/fr/intelligence-artificielle/glossaire-ia>