

Deep Learning IA : la reconnaissance faciale

Veille Cybersécurité

Préparé par Sivasurijaan UTHAYAKUMARAN

Introduction au Deep Learning

Le Deep Learning, ou apprentissage profond, est une branche de l'intelligence artificielle qui vise à imiter le fonctionnement du cerveau humain pour analyser des données complexes.

Qu'est-ce que l'IA ?

Intelligence Artificielle

L'IA désigne la capacité des machines à imiter l'intelligence humaine.

Apprentissage Automatique

L'IA implique des algorithmes et des modèles qui améliorent leur performance à travers l'expérience.

Prise de Décision

Les systèmes d'IA peuvent prendre des décisions sans intervention humaine en s'appuyant sur des données.



Qu'est-ce que le Deep Learning ?

- **Définition** : Le Deep Learning est une branche de l'intelligence artificielle qui se concentre sur l'apprentissage automatique à partir de données non structurées ou de modèles abstraits.
- **Neurones artificiels** : Les réseaux de neurones artificiels sont la base du Deep Learning, ils imitent le fonctionnement du cerveau humain pour traiter les données.
- **Applications** : Le Deep Learning est utilisé dans la reconnaissance d'images, la traduction automatique, la reconnaissance vocale, et bien d'autres domaines.

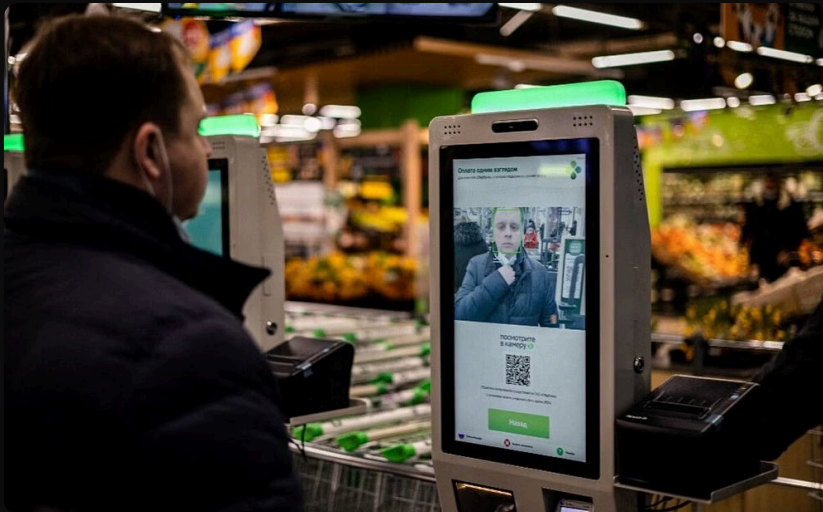
La reconnaissance faciale

La reconnaissance faciale est une technologie d'IA s'appuyant sur le Deep Learning pour identifier et vérifier une personne à partir d'une image ou d'une vidéo.

Elle est largement utilisée dans la sécurité, les smartphones, le contrôle d'accès et suscite des débats sur la vie privée.



Les applications de la reconnaissance faciale



Paiement Mobile

La reconnaissance faciale est utilisée pour authentifier les paiements mobiles, offrant une méthode sécurisée et pratique.



Contrôle d'Accès

Elle est utilisée pour le contrôle d'accès sécurisé aux bâtiments et aux zones restreintes.

Les avantages et les inconvénients de la reconnaissance faciale

Avantages

- Identification précise des individus
- Amélioration de la sécurité dans les lieux publics
- Utilisation efficace pour les contrôles d'accès

Inconvénients

- Violation de la vie privée
- Risque de surveillance et de tracking abusif
- Possibilité d'erreurs et de discrimination liées aux données utilisées

Les enjeux de sécurité liés à la reconnaissance faciale

1

Protection des données personnelles

La collecte et le stockage des données biométriques soulèvent des préoccupations majeures concernant la protection de la vie privée.

2

Vulnérabilité à la falsification

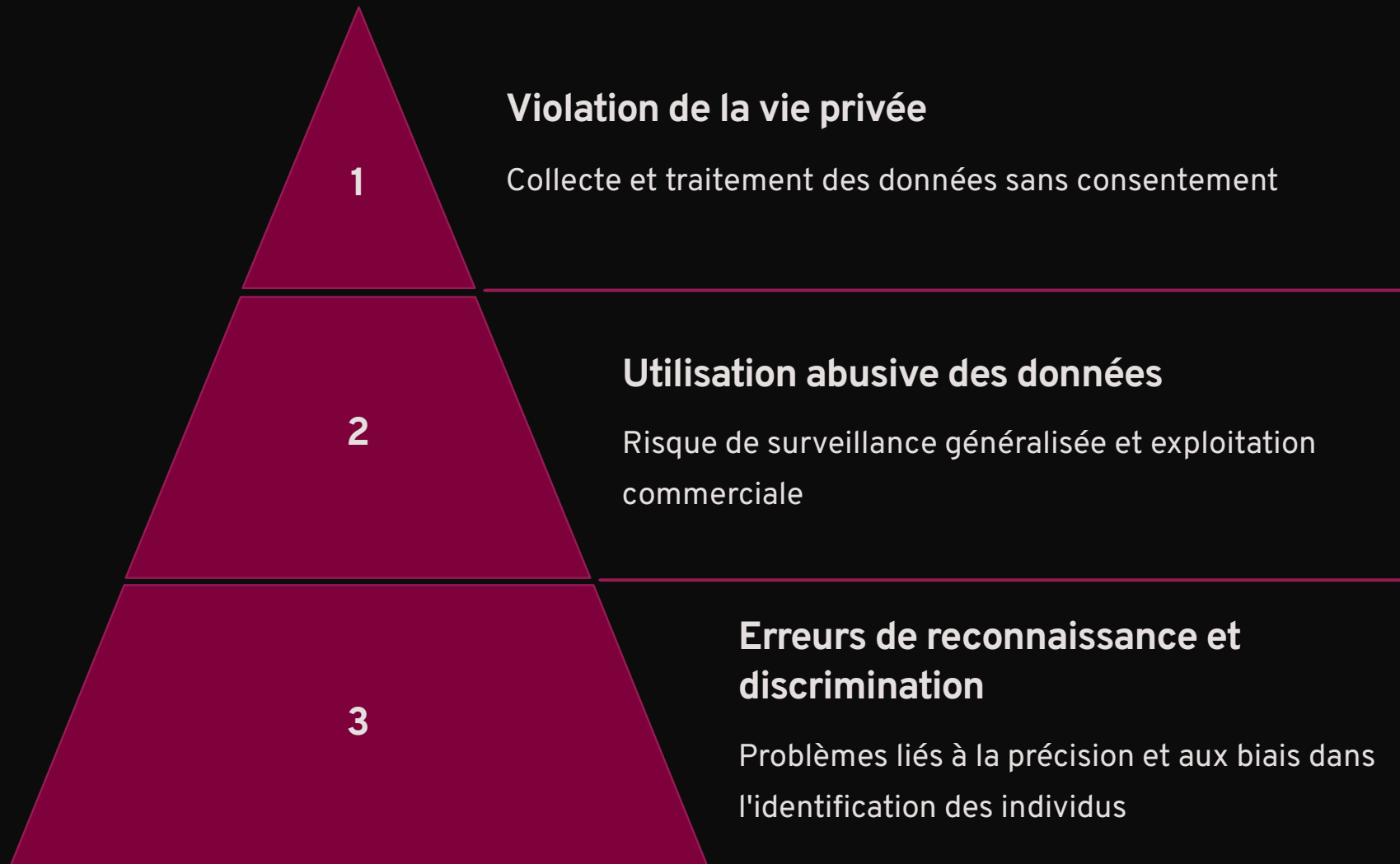
Les systèmes de reconnaissance faciale sont sujets à la contrefaçon, ce qui compromet leur fiabilité et leur sécurité.

3

Biais et discrimination

Les algorithmes de reconnaissance faciale peuvent présenter des biais et engendrer une discrimination injuste, en particulier à l'égard de certaines communautés.

Les risques de la reconnaissance faciale en matière de vie privée



Les réglementations et les normes entourant la reconnaissance faciale

GDPR	Règlement général sur la protection des données de l'Union Européenne
Lois sur la vie privée	Réglementations spécifiques concernant la collecte et l'utilisation des données biométriques
Normes de sécurité	Exigences de sécurité pour le stockage et le traitement des données de reconnaissance faciale
Règlements sectoriels	Directives spécifiques pour l'utilisation de la reconnaissance faciale dans des secteurs particuliers, tels que la santé et la finance

Les tendances Actuelles

PimEyes : un logiciel d'intelligence artificielle.

La reconnaissance faciale vers la police criminelle.

Non autorisée en Allemagne pour cause de protection des données oblige. En France rien ne l'interdit, tant qu'il est utilisé à condition que cela se fasse dans le cadre d'une procédure judiciaire avec l'autorisation d'un magistrat.

Conclusion et perspectives d'avenir

■ Expansion de l'utilisation de la reconnaissance faciale

La technologie de reconnaissance faciale devrait continuer à se répandre dans divers domaines, y compris la sécurité, les paiements, et la gestion des services publics.

■ Préoccupations croissantes liées à la confidentialité

La protection de la vie privée et la réglementation autour de la collecte et de l'utilisation des données biométriques devraient devenir des sujets de préoccupation majeure.

■ Évolution des normes et des réglementations

Des efforts accrus pour encadrer et réguler l'utilisation de la reconnaissance faciale afin de protéger les droits fondamentaux des individus sont attendus.