

# Surveillance numérique et technologies de reconnaissance faciale

*Des défis techniques et  
un cadre juridique ...*

---

Louiza-Zahra CHEKRAOUI

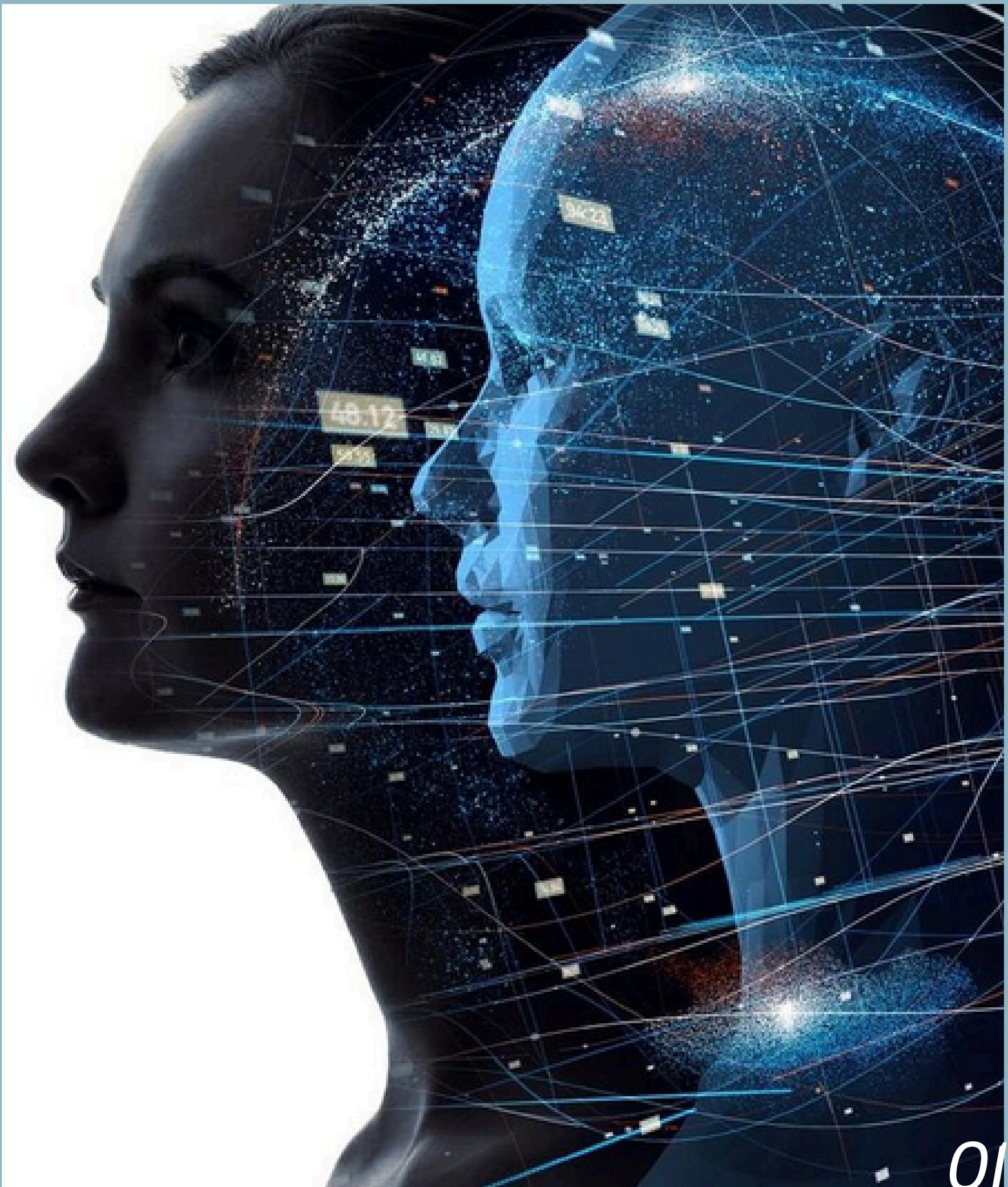
Hana ISTFALEN

Khadija AKKAR

Salma EL KHATRI

Safae BELAHRACH

Younes BAKKAS



# Sommaire

01

*Présentation de la controverse*

02

*Présentation des acteurs*

03

*Les noyaux d'ignorance*

04

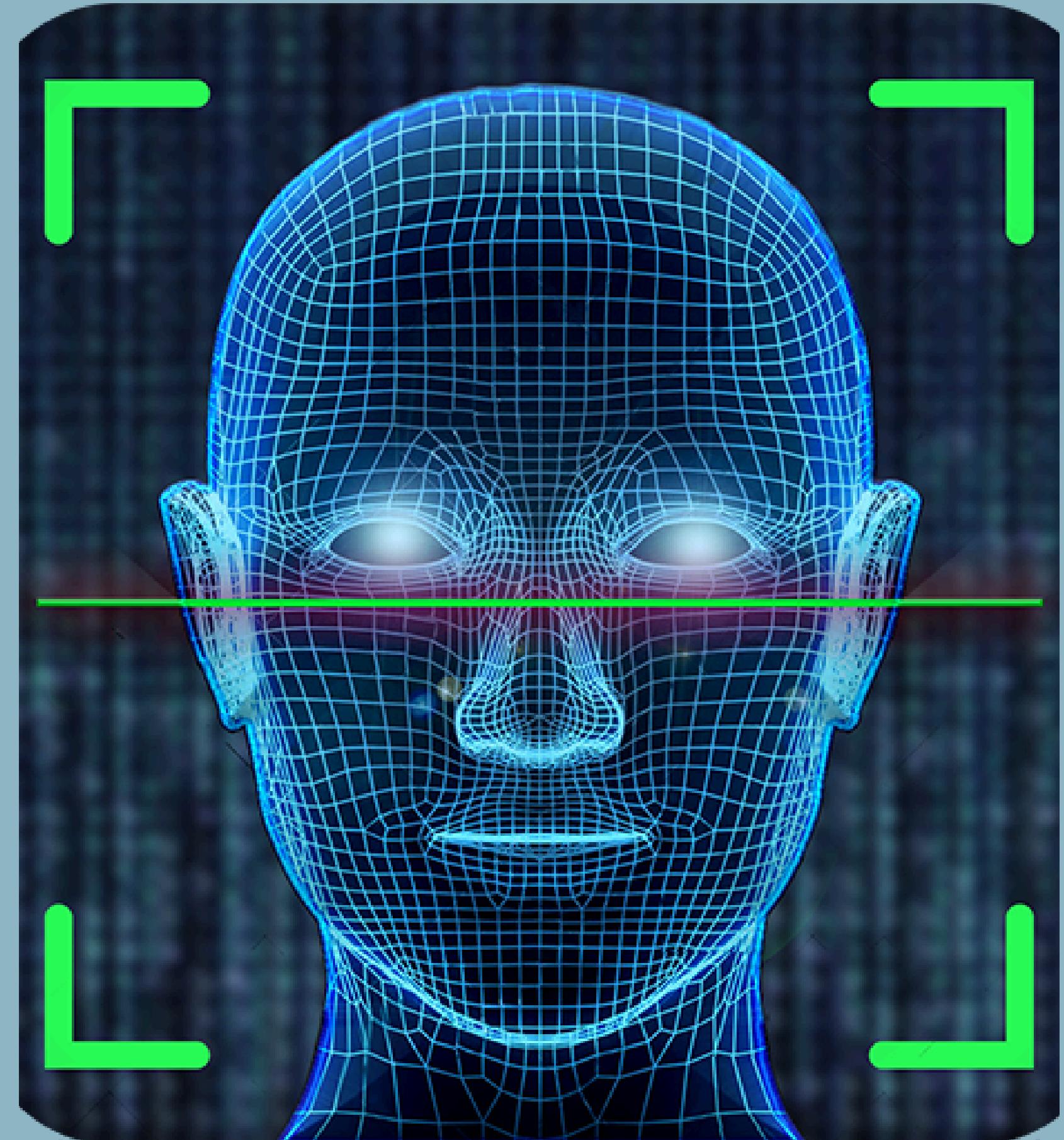
*Les sorties potentielles*

05

*Conclusion*

01

## *Présentation de la controverse*



03

02

## *Présentation et Cartographie des acteurs*



04

## Présentation des acteurs



*Gouvernements et forces de l'ordre*

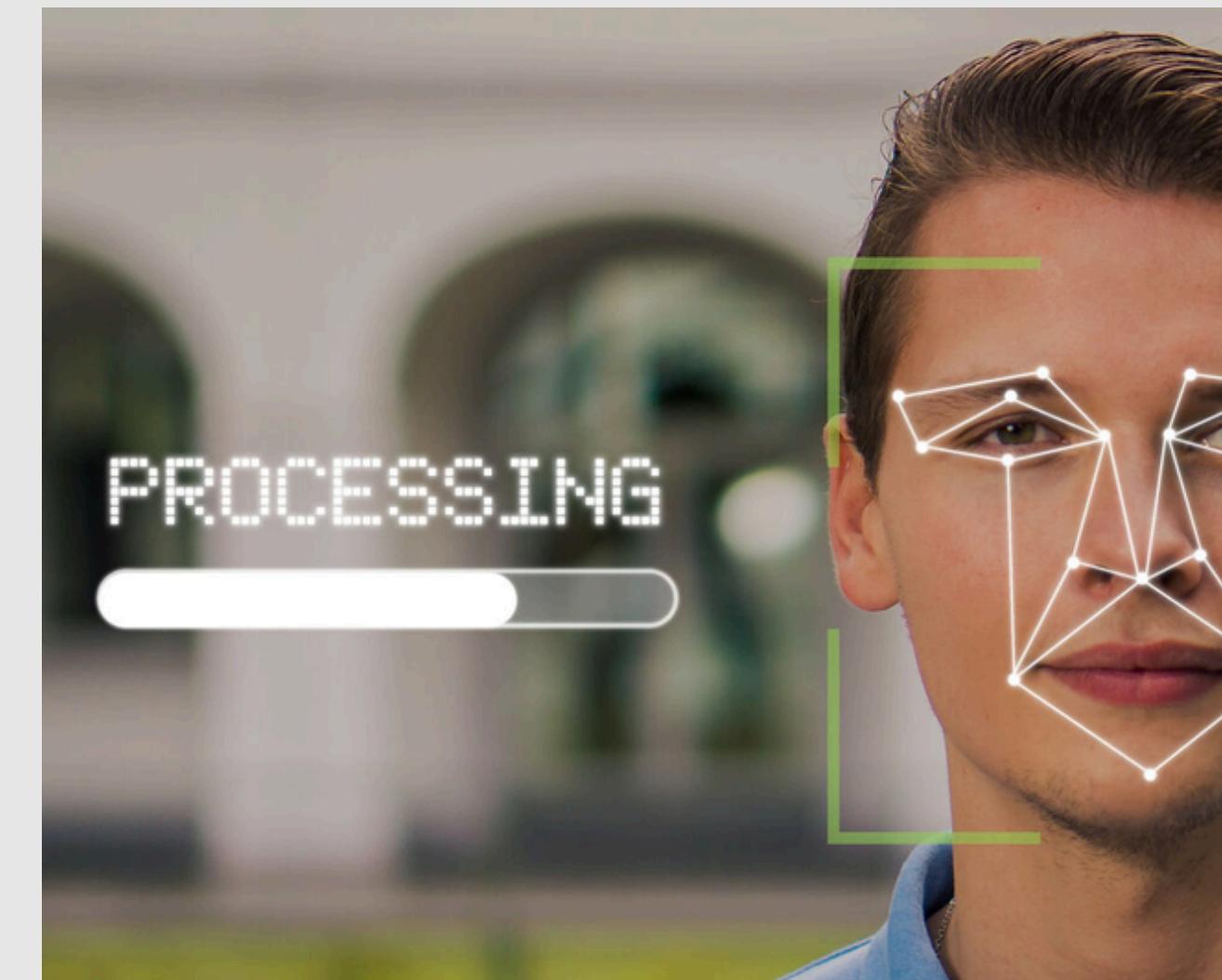
*ONG et associations de défense des droits*

*Entreprises technologiques*

*Chercheurs et universitaires*

*Encadrement Juridique*

*Citoyens et médias*



03

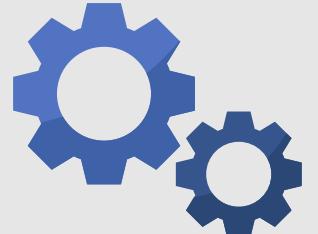
## *Les noyaux d'ignorance*



# Défis socio-techniques



## Défis techniques

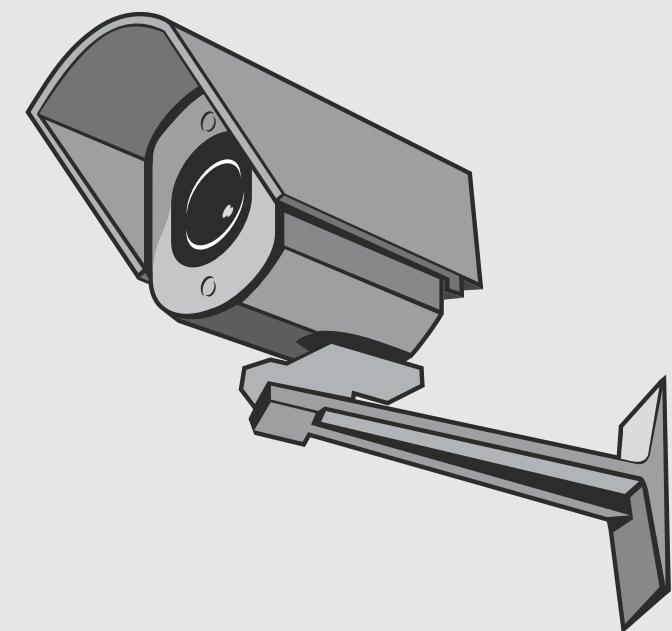


- *Précision variable selon les conditions et les populations.*
- *Biais algorithmiques entraînant des erreurs d'identification plus fréquentes.*
- *Problèmes d'interopérabilité entre les systèmes publics et privés.*

## Défis sociaux



- *Utilisation dans les espaces publics (transports, événements, surveillance urbaine).*
- *Impact sur les métiers de la sécurité et automatisation des contrôles.*





# Vie Privée



## Sécurité vs vie privée

- Les mesures actuelles de sécurité ne sont pas toujours suffisantes pour protéger les données faciales collectées.
- La reconnaissance faciale dans les espaces publics permet une surveillance constante des citoyens, avec peu ou pas de contrôle.
- Les données collectées à des fins de sécurité peuvent être exploitées à des fins commerciales sans transparence.



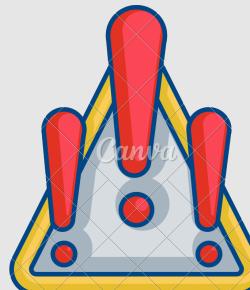
## Risques d'abus / Fuites de données

- Le stockage de grandes quantités de données biométriques dans des bases centralisées expose à des risques de fuites
- Les données biométriques peuvent être réutilisées à des fins non prévues (publicité, ciblage marketing, surveillance commerciale)
- La technologie peut être utilisée à des fins de contrôle social ou de discrimination.

# Encadrement juridique



*Le Règlement Général sur la Protection des Données (RGPD) érige en principe, en son article 9, l'interdiction des traitements de données biométriques*



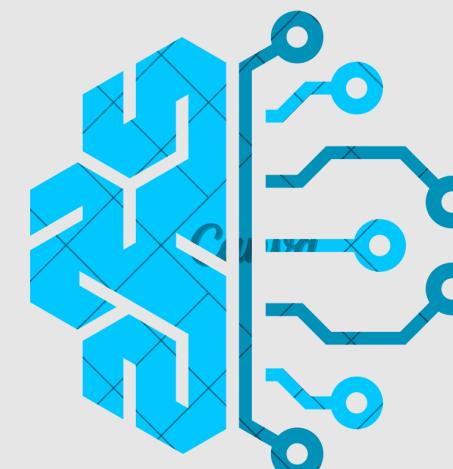
*Exceptions :*



*Sécurité Nationale*



*Enquêtes criminelle*



*Systèmes*

04

## *Les sorties potentielles*

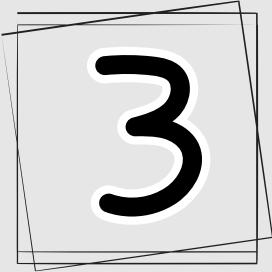




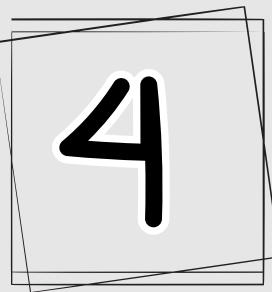
**Sécurité vs. libertés individuelles**



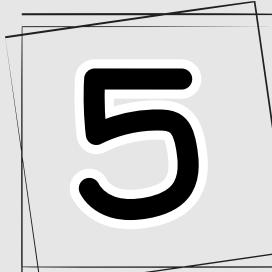
**Éthique et responsabilité**



**Protection des données**



**Discriminations algorithmiques**



**Régulations divergentes**

05

# Conclusion





Merci pour votre  
attention !