CYBERSÉCURITÉ · IA · DROIT

# Volontaire sur le papier. *Opposable en pratique.*

Ce que la première norme ISO consacrée à la sécurité des systèmes d'IA change pour votre responsabilité.

**Maître Mohamed Zied El Air**

Avocat aux Barreaux de Paris et de Tunis · DPO certifié

Faites défiler →

Publiée le 14 octobre 2026 · 1re édition · ISO/IEC JTC 1/SC 27

# Ce que votre pare-feu *ne voit pas.*

01

## Empoisonnement

Des données d'entraînement altérées faussent le modèle.

02

## Évasion

Des entrées conçues pour tromper le modèle en production.

03

## Vol de modèle

Des requêtes d'apparence légitime suffisent à le copier.

04

## Inversion de modèle

Reconstituer des données d'entraînement à partir des sorties.

05

## Inférence d'appartenance

Savoir si une personne figure dans le jeu d'entraînement.

06

## Injection de prompt

Des instructions dissimulées détournent le système.

**Leur point commun : elles passent sous le radar du pare-feu, du SIEM et de l'IAM.**

STATUT JURIDIQUE

# Un simple guide ?

## Ni certifiable.

Contrairement à l'ISO/IEC 27001 et à l'ISO/IEC 42001.

## Ni obligatoire.

Aucune réglementation ne la rend directement applicable.

## Ni norme harmonisée.

Aucune présomption de conformité à l'AI Act (art. 40).

**Et pourtant, trois mécanismes vont la rendre opposable :**

1 L'état de l'art

2 L'AI Act

3 Les données personnelles

MÉCANISME 1 / 3 · L'ÉTAT DE L'ART

# L'état de l'art ne se décrète pas. *Il se constate.*

**RGPD · art. 32**

Des mesures de sécurité appropriées, compte tenu de l'état des connaissances.

**NIS2 · art. 21**

L'état des connaissances et, s'il y a lieu, les normes internationales pertinentes.

**En sécurité de l'IA, cet état des connaissances dispose désormais d'un référentiel publié.**

Après un incident, régulateur et juge sauront où regarder.

MÉCANISME 2 / 3 · L'AI ACT

# L'article 15 *nomme déjà* les attaques.

Les systèmes d'IA à haut risque doivent résister aux tentatives d'exploitation de leurs vulnérabilités, notamment :

- → l'empoisonnement des données d'entraînement
- → l'empoisonnement des composants pré-entraînés
- → les exemples contradictoires et l'évasion
- → les attaques contre la confidentialité

Calendrier · règlement (UE) 2026/1744

**Annexe III** ~~2 août 2026~~ → **2 décembre 2027**

*Un délai de mise en conformité, pas un sursis.*

MÉCANISME 3 / 3 · LES DONNÉES PERSONNELLES

# Un modèle vulnérable *reste un traitement* de données personnelles.

| | |
|---|---|
| **Inversion et inférence d'appartenance** | Des scénarios de violation de données (RGPD, art. 33 et 34) : notification à la CNIL et, le cas échéant, information des personnes. |
| **EDPB · avis 28/2024** | La résistance du modèle à ces attaques est un critère d'appréciation de son caractère anonyme. |
| **Pour le DPO** | L'ISO/IEC 27090 devient une grille de lecture des analyses d'impact (AIPD) des projets d'IA. |

LE CHANTIER PRIORITAIRE

# Six clauses à vérifier dans *vos contrats IA.*

- ☐ Provenance et intégrité des données d'entraînement
- ☐ Interdiction d'entraîner les modèles sur vos données sans accord exprès
- ☐ Notification des incidents propres à l'IA : empoisonnement, extraction de modèle, injection de prompt
- ☐ Encadrement des mises à jour et des réentraînements
- ☐ Journalisation, audit et réversibilité
- ☐ Répartition des responsabilités calquée sur le couple fournisseur / déployeur de l'AI Act

**Secteur financier**

Articulation avec les clauses contractuelles de DORA (art. 30).

**Tunisie**

Audits de sécurité du décret-loi n° 2023-17 relatif à la cybersécurité.

MA CONVICTION

# Le jour d'un incident, on ne vous demandera pas si vous étiez certifié. *On vous demandera si vos mesures étaient à l'état de l'art.*

Vos registres de risques et vos contrats fournisseurs intègrent-ils déjà les menaces propres à l'IA ?

**Maître Mohamed Zied El Air**

Avocat aux Barreaux de Paris et de Tunis

DPO certifié · RGPD, cybersécurité et IA

www.elair-avocat.com