



Commission nationale de l'informatique et des libertés

Présentation de la loi relative à l'usage des systèmes d'intelligence artificielle en matière de sécurité intérieure

Adoptée en première le 28 mars 2023

Entrée en vigueur le 3 avril 2024

Modifiée le 8 mai 2025



Référence du dossier : DJP/IA-S1/2025/041

Département de justice et police

Office de la sécurité intérieure

L'usage des systèmes d'intelligence artificielle en matière de sécurité intérieure

A. Centralisation des dispositifs de surveillance	Art. 1 L'État est autorisé à centraliser l'ensemble des flux vidéo issus des dispositifs de captation installés dans l'espace public sur le territoire national, en vue de leur traitement algorithmique à des fins de sécurité publique.
B. Traitement algorithmique automatisé	Art. 2 Les images issues des dispositifs de surveillance peuvent faire l'objet d'un traitement automatisé à l'aide de systèmes d'intelligence artificielle, dans le but d'identifier des comportements ou événements présentant un risque pour la sécurité nationale.
C. Garanties éthiques et techniques	Art. 3 Le traitement algorithmique visé à l'article 2 doit répondre aux conditions suivantes : <ol style="list-style-type: none">1. être proportionné aux risques identifiés ;2. être encadré par un audit de conformité aux principes de nécessité, de finalité, de transparence et de minimisation des données ;3. faire l'objet d'un contrôle par une autorité administrative indépendante compétente en matière de libertés publiques.
E. Interdiction de la reconnaissance biométrique généralisée	Art. 4 La reconnaissance biométrique à distance en temps réel dans les espaces publics est interdite, sauf : <ol style="list-style-type: none">1. en cas de menace terroriste avérée et imminente ;2. pour la recherche active de victimes disparues ;3. pour l'identification de personnes signalées dans le cadre d'enquêtes criminelles graves, sur autorisation judiciaire motivée.
F. Données sensibles	Art. 5 Toute extraction ou croisement de données à caractère personnel à des fins de profilage est interdit, sauf consentement explicite de la personne concernée ou cadre légal expressément prévu par une autorité judiciaire compétente.

Niveaux de risques

Le règlement sur l'IA protège les citoyennes et citoyens contre les risques liés à l'intelligence artificielle. Il classe les systèmes en quatre niveaux selon leur impact sur la vie privée, la sécurité ou les droits fondamentaux. Certaines IA sont interdites, d'autres encadrées ou soumises à des obligations de transparence. Ce cadre s'applique à tous les usages de l'IA, de la santé à la sécurité, en passant par l'emploi et la création de contenu.

Niveau de risque	Description	Exemples	Obligations
Inacceptable	Systèmes d'IA jugés contraires aux droits fondamentaux	Notation sociale, exploitation de personnes vulnérables, reconnaissance faciale généralisée	Interdiction totale
Haut	IA avec impact fort sur les droits, la sécurité ou la vie des personnes	Recrutement automatisé, systèmes biométriques, usage par les forces de l'ordre	Encadrement strict : documentation, audit, etc.
Modéré	IA ayant un impact plus faible mais nécessitant de la transparence	Chatbots, génération automatique de contenu (texte, image)	Obligations d'information pour les usagers
Minimal	Systèmes avec peu ou pas de risque identifié	Filtres anti-spam, outils de productivité simples	Pas d'obligation spécifique