

Comment déployer une IA générative ? La CNIL apporte de premières précisions

18 juillet 2024

Vous souhaitez déployer un système d'intelligence artificielle générative au sein de votre organisme mais vous vous interrogez sur le cadre à respecter ? La CNIL publie des premières réponses pour un déploiement responsable et respectueux de la protection des données.

Qu'est-ce que l'IA générative ?

L'intelligence artificielle dite « générative » désigne les systèmes capables de créer des contenus (texte, code informatique, images, musique, audio, vidéos, etc.). Lorsqu'ils permettent de réaliser un large éventail de tâches, ces systèmes peuvent être qualifiés de systèmes d'IA à usage général. C'est par exemple le cas des systèmes intégrant des grands modèles de langage (en anglais *large language models* ou LLM).

Leur utilisation vise généralement à accroître la créativité et la productivité des personnes qui les utilisent en leur permettant de générer de nouveaux contenus, mais aussi en analysant ou en retravaillant des contenus préexistants (par exemple en proposant des résumés, corrections ou traductions automatiques).

Toutefois, du fait de leur nature probabiliste, **ces systèmes sont susceptibles de générer des résultats inexacts qui peuvent, pourtant, paraître plausibles.**

Par ailleurs, leur développement nécessite un entraînement sur de larges volumes de données, lesquelles comportent souvent des informations sur les personnes physiques, ou données personnelles, de même que les données fournies lors de l'utilisation de ces systèmes.

Il convient donc de prendre un certain nombre de précautions pour respecter les droits des personnes sur leurs données.

Comment déployer de tels systèmes ?

De nombreux acteurs sollicitent la CNIL pour savoir comment déployer des systèmes d'IA générative, en particulier sur les mesures et la gouvernance à adopter afin de se conformer aux règles applicables, en particulier pour la protection des données personnelles.

La publication de ces questions-réponses a vocation à guider les organismes qui envisagent de déployer ces systèmes en leur proposant une approche responsable et sécurisée.

En synthèse, la CNIL recommande de :

- **Partir d'un besoin concret**, c'est-à-dire d'éviter de déployer un système d'IA générative sans but précis, mais pour répondre à un ensemble d'usages déjà identifiés.
- **Encadrer les usages** en définissant une liste d'utilisations autorisées et interdites compte tenu de ces risques (par exemple ne pas fournir de données personnelles au système, ou bien ne pas confier de prise de décision).
- **Ne pas occulter les limitations de ces systèmes**, en particulier au regard des risques qu'ils peuvent engendrer pour les intérêts et droits des personnes concernées.
- **Choisir un système robuste et un mode de déploiement sécurisé**, par exemple en privilégiant le recours à des systèmes locaux, sécurisés et spécialisés (*fine-tuned* en anglais). A défaut, il faut déterminer dans quelle mesure le prestataire opérant le système est susceptible de réutiliser les données fournies au système d'IA, et adapter l'usage en conséquence.
- **Former et sensibiliser les utilisateurs finaux** tant vis-à-vis des usages interdits que des risques encourus dans le cadre des usages autorisés.
- **Mettre en œuvre une gouvernance adaptée** pour s'assurer du bon respect du RGPD et de ces préconisations, notamment en impliquant dès le début toutes les parties prenantes ([délégué à la protection des données](#), responsable des systèmes d'information, RSSI, responsables « métiers », etc.).

[> Lien vers la FAQ](#)

Comment s'assurer de la conformité d'un système d'IA générative en particulier ?

Ces premières réponses ne concernent que le déploiement ou l'utilisation de ces systèmes.

La conception, l'ajustement (*fine-tuning*) ou l'amélioration de ces modèles ou systèmes posent des enjeux complexes en termes de conformité, car ils requièrent généralement de vastes quantités de données provenant de différentes sources (Internet, sources tierces sous licence, interactions avec les utilisateurs, etc.).

À cet égard, [la CNIL a publié ses premières recommandations sur le développement des systèmes d'IA](#). Elle a aussi récemment soumis [de nouvelles recommandations à consultation publique](#).

Conformément à [son plan d'action sur l'IA](#), elle prévoit encore de publier prochainement **de nouvelles recommandations au sujet des systèmes d'IA générative**.

Pour approfondir

- [Tous les contenus de la CNIL sur l'intelligence artificielle](#)
 - [RGPD : Passer à l'action](#)
 - [Tous les contenus de la CNIL sur la cybersécurité](#)
-