

Intelligence artificielle : la CNIL poursuit ses travaux pour une IA innovante et respectueuse de la vie privée

10 juin 2024

En soumettant à consultation publique de nouvelles fiches pratiques relatives au développement de systèmes d'intelligence artificielle, la CNIL montre comment le règlement général sur la protection des données (RGPD) permet la promotion d'IA innovantes et responsables.

Répondre aux questions posées par le développement de l'IA sur la protection des données et de la vie privée

L'année 2022 a été marquée le déploiement et l'utilisation de systèmes d'IA par et pour le grand public. La CNIL a pu observer, depuis, une accélération de la volonté d'adoption de ces technologies, et cela dans tous les secteurs d'activités : santé, services publics, sécurité publique, etc. Elle est consciente que l'adoption de cette technologie est, pour la France, un facteur majeur de compétitivité, d'innovation et de souveraineté pour les prochaines années.

Par ailleurs, la législation européenne garantit un haut niveau de protection des droits fondamentaux et de nombreuses questions doivent être résolues concernant l'encadrement de ces technologies et leurs effets sur les individus. Le besoin de réponses se fait donc de plus en plus pressant, afin de permettre un développement de l'IA dans un cadre de confiance.

Construire l'articulation entre le RGPD et le règlement IA

Alors que **le règlement européen sur l'IA vient d'être adopté** et entrera en application de façon échelonnée dans les prochains mois, **la CNIL souhaite apporter de la sécurité juridique aux acteurs du secteur en anticipant l'articulation entre règlement IA et RGPD**. En effet, le RGPD s'applique aux fournisseurs de systèmes, indépendamment du règlement IA, lorsque ceux-ci utilisent des données personnelles pour leur développement.

C'est dans ce contexte que la CNIL ouvre, pour la deuxième fois, une consultation auprès de tous les acteurs pour élaborer ses recommandations :

- les fiches mises en consultation traitent plusieurs questions majeures d'innovation et de protection : l'usage du moissonnage sur le web (« **web scraping** »), largement répandu notamment pour les

modèles de langage, la publication de modèles d'IA en source ouverte (« **open source** ») mais aussi la **gestion des droits des personnes**, qui constitue la clé de voûte du cadre juridique sur les données personnelles ;

- la CNIL propose également un questionnaire sur le sujet de l'application du RGPD aux modèles d'IA entraînés avec des données personnelles.

Cette mise en consultation fait suite à [de premières recommandations](#) récemment publiées à la suite d'une consultation publique.

[> Participer à la consultation publique](#)

Consulter et échanger pour construire des IA innovantes et responsables

Entreprises, laboratoires, pouvoirs publics, syndicats professionnels de salariés, fédérations professionnelles... la CNIL a eu l'occasion d'avoir **de nombreux échanges avec les parties prenantes impliqués dans la conception et le développement de systèmes d'IA**. Ceux-ci ont fait remonter un besoin de clarification sur le cadre juridique applicable pour les pratiques les plus répandues du secteur afin de **construire des IA innovantes et responsables**.

L'intérêt légitime est la base légale la plus couramment mobilisée pour le développement de systèmes d'IA

Si plusieurs bases légales peuvent être mobilisées pour justifier un traitement de données personnelles aux fins de développer un système d'IA, la base de « l'intérêt légitime » de l'organisme qui réalise l'entraînement semble la plus souvent retenue. Cette base requiert la mise en place d'une évaluation des risques pour les personnes et peut exiger des conditions de mise en œuvre spécifiques destinées à protéger les individus et leurs données. La CNIL propose des éléments concrets pour les responsable de traitement, notamment lors de l'usage de techniques de moissonnage (*web scraping*) ou la publication d'IA en source ouverte (*open source*).

[Le moissonnage ou « web scraping » de données doit être particulièrement encadré](#)

Le développement de systèmes d'IA nécessite, dans certains cas, l'accès à des bases de données de grandes taille qui peuvent être constituées à partir de données collectées en ligne. Des garanties techniques et organisationnelles importantes sont indispensables pour assurer le respect des droits, car dans la plupart des cas, les personnes dont les données sont utilisées ne sont pas informées de l'existence de ces traitements. Pour améliorer l'information et faciliter l'exercice des droits par les personnes, la CNIL propose de centraliser un registre volontaire de ces pratiques.

La diffusion en source ouverte « open source » est une pratique souvent positive aussi pour la protection des données

L'écosystème IA se construit historiquement autour du partage et de la collaboration communautaire. Ce mouvement est bénéfique, car il améliore la transparence sur le fonctionnement des modèles et systèmes d'IA et permet la mise en discussion, la vérification par les pairs et l'amélioration de ces modèles. Il peut cependant accentuer certains risques, tels que ceux d'utilisation malveillante ou relatifs à la sécurité.

La CNIL considère que la diffusion en source ouverte (open source) est bénéfique pour la protection des données car elle apporte en particulier une transparence accrue pour les personnes. Cette pratique suppose, toutefois, que l'ouverture soit réelle et que des garanties nécessaires soient mises en œuvre, en particulier en ce qui concerne les possibilités de réutilisation offertes ainsi que le suivi des modèles et de leurs évolutions au fil du temps, afin de permettre une information et un exercice des droits effectifs.

L'information et l'exercice des droits des personnes doivent être centraux dans la réflexion des acteurs

Informier et permettre l'exercice effectif des droits sont essentiels pour la conformité des systèmes d'IA développés à l'aide de données personnelles. La CNIL propose des clés de lecture sur les moyens à mettre en œuvre pour remplir ces obligations vis-à-vis des personnes concernées et indique dans quels cas des dérogations pourraient trouver à s'appliquer. Elle propose également des éléments de réponse concernant certains droits qui se heurtent à la nature statistique des IA : droit de rectification et droit de suppression notamment.

L'applicabilité du RGPD aux modèles d'IA questionnée

L'apprentissage automatique ou *machine learning* repose sur la création de modèles. Ces derniers sont des représentations apprises à partir des données d'entraînement. Depuis 2010 environ, un champ de recherche en informatique a émergé sur le sujet de la sécurisation des modèles d'IA et, en particulier, les possibilités de mémorisation, d'extraction ou de régurgitation d'informations issues de l'entraînement. Celles-ci peuvent avoir des répercussions importantes pour la confidentialité des données personnelles et la question de l'application du RGPD aux modèles eux-mêmes se pose, lorsque qu'ils ne sont pas considérés comme anonymes. **Par un questionnaire dédié accessible sur [la page de consultation publique](#)**, la CNIL sollicite donc les professionnels que cette question impacte pour l'aider à élaborer sa future position.

Le développement de systèmes d'IA est conciliable avec les enjeux de protection de la vie privée. Plus encore, la prise en compte de cet impératif permettra de faire émerger des dispositifs, outils et applications éthiques respectueux des droits et libertés fondamentaux. C'est à cette condition que les citoyens feront confiance à ces technologies.

[> Voir les recommandations de la CNIL](#)

Pour approfondir

- [IA : la CNIL publie ses premières recommandations sur le développement des systèmes d'intelligence artificielle](#)
 - [Développement des systèmes d'IA : les recommandations de la CNIL pour respecter le RGPD](#)
-