

IA agentique et données personnelles : la CNIL et le Conseil de l'IA et du Numérique publient une note exploratoire

20.7.2026 - | Commission Nationale de l'Informatique et des Libertés

Les innovations à l'ère de l'IA générative se poursuivent avec la démocratisation de l'IA agentique, désormais capable d'agir sur son environnement à la place de son utilisateur. La délégation des tâches qui lui sont confiées, facilitée par des interactions hyperpersonnalisées, implique des chaînes de traitement complexes, parfois opaques. Dans une note coécrite avec le CIANum (Conseil de l'IA et du Numérique), la CNIL explore les enjeux pour la protection des données.

La CNIL et le CIANum (Conseil de l'IA et du Numérique) ont mené une réflexion commune sur les enjeux soulevés par l'IA agentique pour la protection des données personnelles. Ces travaux font écho aux échanges engagés sur ce sujet par la CNIL avec ses homologues internationaux, notamment dans le cadre du G7 des autorités de protection des données et de la vie privée organisé par la CNIL à l'occasion de la présidence française du G7.

Un changement d'échelle dans le traitement des données personnelles

Le passage de l'intelligence artificielle (IA) générative à l'IA agentique marque un changement d'échelle qui renouvelle et amplifie les risques pour les données personnelles des utilisateurs. Capables d'accéder et de traiter d'importants volumes de données à partir des multiples sources auxquelles elles sont connectées, mais aussi d'agir sur leur environnement, les IA agentiques impliquent la circulation de données personnelles entre de nombreux services. Par ailleurs, la conservation de l'historique des interactions avec l'utilisateur et le recours à des mémoires persistantes participent également à augmenter les données conservées par ces systèmes sur des supports variés. Ces mécanismes favorisent ainsi la création de profils utilisateurs hyperpersonnalisés et une autonomie décisionnelle accrue.

Ces flux de données peuvent être difficiles à appréhender par l'utilisateur, créant un risque réel de perte de maîtrise sur ses données personnelles et mettant ainsi en tension les principes du règlement général sur la protection des données (RGPD).

Des systèmes autonomes qui complexifient la maîtrise des risques

Les systèmes d'IA agentique posent également des questions de partage des responsabilités entre les acteurs, par la délégation de pouvoir qu'ils permettent. En effet, les capacités d'action autonome des systèmes agentiques et d'interaction avec d'autres applications leur permettent d'automatiser des processus décisionnels faisant intervenir de multiples acteurs. Ce fonctionnement décentralisé complexifie l'identification des responsabilités de chacune des parties et étend les risques liés à la cybersécurité à l'ensemble des services connectés aux systèmes d'IA agentique.

Au regard des risques que présentent le développement et le déploiement de systèmes d'IA agentique, le cadre juridique applicable apparaît comme un levier essentiel de maîtrise de ces nouveaux usages. Si les principaux instruments du droit européen de la protection des données et de la régulation de l'intelligence artificielle leur sont déjà applicables, leurs caractéristiques propres – autonomie décisionnelle, mémoire persistante, capacité d'interagir avec une pluralité de services et d'agir au nom de l'utilisateur – appellent à une adaptation des modalités de mise en œuvre de ces règles.

Télécharger la note

<https://www.cnil.fr/fr/ia-agentique-cnil-cianum-note>