Webinaire : sécurité des systèmes d'IA, enjeux et bonnes pratiques

L'intelligence artificielle (IA) se développe partout et dans tous les domaines pour révolutionner notre quotidien notamment au travers de nouveaux produits ou services. Elle repose sur des algorithmes nécessitant principalement l'utilisation de nombreuses données, souvent personnelles, ce qui engendre des risques de sécurité spécifiques par comparaison avec des systèmes d'information classiques. D'autant que les capacités d'apprentissage automatique (machine learning) augmentent la surface d'attaque de ces systèmes, en introduisant de nouvelles vulnérabilités.

Envisager les attaques et défaillances des systèmes d'IA

Pour aider les entreprises à mieux comprendre les nouveaux enjeux de ces dispositifs et à sécuriser les systèmes d'IA qu'elles mettent en place, la CNIL propose un webinaire qui leur permettra de répondre à de nombreuses questions comme : Comment envisager les attaques et défaillances possibles de son système d'IA en pratique ? Quelles mesures mettre en œuvre pour les limiter ?

Pour regarder le webinaire : www.cnil.fr