Données personnelles et IA : l'apport des normes ISO/IEC 27701 et 42001

02 avril 2024

La norme internationale ISO/IEC 27701 décrit la gouvernance et les mesures de sécurité à mettre en place pour les traitements de données personnelles. La norme ISO/IEC 42001 est, quant à elle, destinée aux organismes qui fournissent ou utilisent des systèmes d'IA.

Des normes pour la protection des données personnelles

Qu'est-ce que la norme 27701 ?

Depuis de nombreuses années, la sécurité informatique bénéficie de deux **normes internationales** reconnues :

- l'ISO/IEC 27001, qui certifie un « **système de management de la sécurité de l'information** » ;
- l'ISO/IEC 27002, qui détaille les bonnes pratiques pour la mise en œuvre des **mesures de sécurité** nécessaires.

Afin de standardiser et de renforcer la protection des données personnelles, la norme ISO/IEC 27701, publiée en août 2019, complète ces deux normes en définissant :

- un « **système de management de la protection de la vie privée** » étendu pour inclure les particularités des traitements de données personnelles :
    - détermination du rôle de l'organisme à certifier (responsable de traitement, sous-traitant) ;
    - gestion unifiée des risques informatiques pour l'organisme et des risques pour la vie privée des personnes, désignation d'un responsable pour la protection de la vie privée (dans le cadre de l'ISO/IEC 27701, il s'agit du délégué à la protection des données) ;
    - sensibilisation des personnels, classification des données, protection des supports amovibles, gestion des accès et chiffrement des données, sauvegarde des données, journalisation des événements ;
    - conditions de transferts de données, protection de la vie privée dès la conception et par défaut (*privacy by design and by default*), gestion des incidents ;
    - conformité aux exigences légales et réglementaires, etc.

- des **mesures spécifiques aux traitements de données personnelles**, en tenant compte du rôle de l'organisme (responsable de traitement, sous-traitant, sous-traitant de sous-traitant) :

- principes fondamentaux : finalité de traitement, base légale, recueil et retrait du consentement, inventaire des traitements, évaluation des impacts pour la vie privée ;
- droits des personnes : information, accès, rectification, suppression, décision automatisée ;
- protection de la vie privée dès la conception et par défaut (privacy by design and by default) : minimisation, dé-identification et suppression des données, durée de conservation ;
- contrats de sous-traitance, transferts et partage de données.

Des contributions d'experts et d'autorités de protection des données

Cette norme a été rédigée au niveau international, avec les contributions d'experts provenant de tous les continents et la participation de nombreuses autorités de protection des données. Les experts de la CNIL y ont activement œuvré, avec le soutien de l'AFNOR et du Comité européen de la protection des données (CEPD).

Le RGPD a été pris en compte, ainsi que les autres grands textes de protection des données (dont ceux adoptés par l'Australie, le Brésil, la Californie, le Canada). La proximité de la norme avec le RGPD est ainsi matérialisée par une annexe dédiée, qui établit la correspondance entre les articles de la norme et ceux du RGPD. Et la mise en place d'un système de management, avec la gestion et la documentation de la protection des données, répond au principe général de responsabilité (*accountability*) du RGPD.

En résumé, **la norme ISO/IEC 27701 a une portée mondiale**. Elle présente l'état de l'art en protection de la vie privée et elle permet aux organismes qui l'adoptent de monter en maturité et de démontrer une démarche active de protection des données personnelles. Elle n'est pas spécifique au RGPD et ne constitue pas, en tant que telle, une certification au sens de l'article 42 du RGPD.

Elle a donc été adaptée par le comité européen de normalisation en électronique et électrotechnique (CEN-CENELEC) avec la nouvelle norme EN 17926 « Système de management de la protection de la vie privée conformément à l'EN ISO/IEC 27701 - **Affinements relatifs au contexte européen** », publiée en novembre 2023.

Il s'agit d'une extension de l'ISO/IEC 27701 qui rend obligatoire toutes les mesures imposées par le RGPD (notamment les droits des personnes concernées) et précise certaines mesures dans ce contexte (par exemple, le délai de notification d'une violation de données). Un schéma de certification européen est également en cours de préparation.

Des normes pour l'intelligence artificielle

En parallèle, **la nouvelle norme ISO/IEC 42001**, publiée en décembre 2023, **propose un « système de management pour l'intelligence artificielle »** destiné aux organismes qui fournissent ou utilisent des systèmes d'IA.

Cette norme décrit les processus pour gérer les préoccupations liées à la fiabilité des systèmes d'IA : sécurité, sûreté, équité, transparence, qualité des données et des systèmes tout au long du cycle de vie. De plus, cette norme apporte une série de mesures opérationnelles et des recommandations pour les mettre en oeuvre : conduire l'analyse des différents impacts et risques d'un système d'IA, assurer un développement et un usage responsables, effectuer la documentation et la surveillance du système, etc.

Enfin, à la demande de la Commission européenne, le Comité européen de normalisation en électronique et en électrotechnique (CEN-CENELEC) a lancé un programme de travail pour **développer des « normes harmonisées »** qui aideront les organismes à démontrer leur **conformité au règlement européen**

sur l'IA. Ces normes permettront d'en préciser l'application pratique, par exemple concernant « les mesures appropriées de gestion des risques ».

Pour approfondir

- La norme ISO/IEC 27701:2019 (contenu payant) - AFNOR
- La norme EN 17926:2023 (contenu payant) - AFNOR
- La norme ISO/IEC 42001:2023 (contenu payant) - AFNOR
- Un nouveau guide de la sécurité des données personnelles
- Guide du sous-traitant
- DPO : réussir sa conformité avec la norme ISO/IEC 27701 - Le club DPO