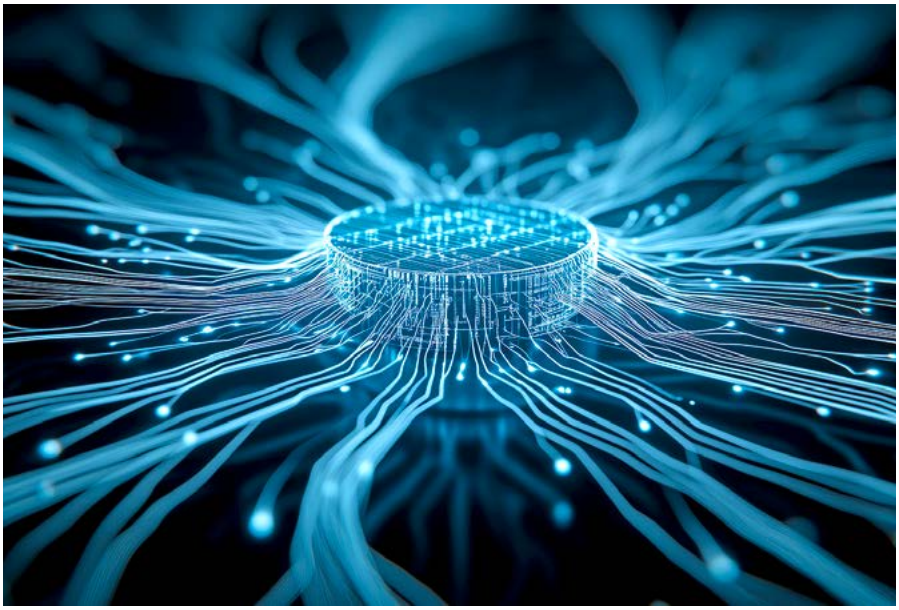
Le recours à l'IA doit se faire dans le respect des lois

Intelligence artificielle : la confidentialité, un enjeu majeur

Contrairement à l'Union européenne qui s'est dotée d'un règlement complet sur l'intelligence artificielle (EU AI Act), la Suisse n'a, pour l'heure, pas édicté de règles spécifiques. Ce sont ainsi la loi sur la protection des données (LPD), le Code des obligations (CO) ou encore le Code pénal (CP) qui sont applicables.

Martina Guillod



Transmission de données

Le point de départ est simple: l'utilisation de l'IA implique-t-elle la transmission de données à des tiers ? Très souvent, la réponse sera affirmative. Pire, les données peuvent être transférées à l'étranger. Par exemple, ChatGPT traite les données sur des serveurs aux États-Unis, tandis que DeepSeek les traite en Chine. Et ce n'est pas tout : ces outils peuvent aussi exploiter les données que vous leur fournissez (par exemple les questions que vous leur posez ou les fichiers que vous leur soumettez pour analyse) pour entraîner et améliorer leurs modèles. Concrètement, cela veut dire que les données que vous fournissez à ces outils sont susceptibles d'apparaître dans les réponses qu'ils donnent à un autre utilisateur ou à une autre utilisatrice.

Données personnelles

La LPD n'interdit en principe pas de transmettre des données personnelles à une personne tierce. Toutefois, selon l'article 19 LPD, la personne dont on traite les données personnelles doit être informée, notamment, des destinataires ou des catégories de destinataires auxquels les données sont transmises. C'est un exercice plutôt difficile lorsque l'on ne sait pas où les données rentrées dans l'outil referont surface.

On pourrait envisager de demander le consentement de la personne concernée. Cependant, ce consentement ne serait pas juridiquement valable. L'IA peut transférer des données personnelles sans que la personne concernée sache à qui, où et dans quel contexte. Un éventuel consentement donné serait ainsi très général, ce qui n'est pas suffisant. De plus, face à l'opacité des algorithmes et de l'IA en général, l'utilisateur ou l'utilisatrice ne peut pas être informé·e de manière claire et compréhensible sur l'utilisation de ses données, ce qui exclut un consentement éclairé.

Il est donc très problématique, sous l'angle de la LPD, de traiter des données personnelles à l'aide d'outils IA librement accessibles. C'est pour cette raison que nous déconseillons cette démarche (voir aussi l'*Info Patronale* N° 331). Si des données personnelles doivent être traitées par l'IA, il convient de s'assurer que les données ne soient pas utilisées pour l'entraînement des outils. Il peut aussi être utile de faire appel à des spécialistes afin de développer une IA interne.

Autres données

La même problématique se présente pour des données qui ne sont certes pas personnelles, mais secrètes. Leur transmission par les outils IA ne contreviendra pas à la LPD, mais peut enfreindre plusieurs autres normes légales. Mentionnons ici, à titre d'exemple, l'obligation de secret du collaborateur ou de la collaboratrice (art. 321a CO) ou la violation du secret professionnel (art. 321 CP).

Conclusion

L'IA offre des perspectives prometteuses, mais elle soulève aussi des défis majeurs en matière de confidentialité et de respect du cadre légal. Les entreprises doivent s'assurer que leur utilisation de l'IA respecte les lois en vigueur, sous peine de conséquences juridiques et éthiques. Il est recommandé d'avoir recours à des solutions internes ou à des spécialistes qui peuvent accompagner l'entreprise dans ces démarches.