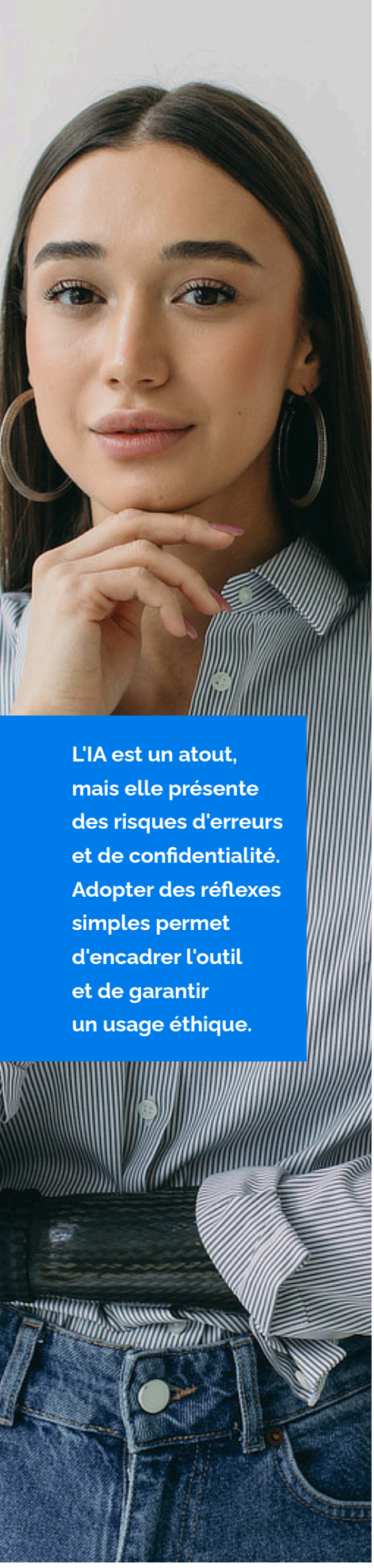

L'IA est un atout, mais elle présente des risques d'erreurs et de confidentialité. Adopter des réflexes simples permet d'encadrer l'outil et de garantir un usage éthique.

Fiabilité, confidentialité

3 réflexes à adopter pour limiter les risques avec l'IA

Astuce de formateur Cegos

Avec l'IA, ne faites pas confiance : faites le tri ! Cela vaut pour vos prompts (secrets) et pour les réponses de l'IA (hallucinations).

1 Ne jamais saisir de données sensibles

Les informations que vous soumettez à l'IA via vos prompts peuvent exposer votre savoir-faire et les données de vos clients. Ces précautions peuvent vous en prémunir :

- ✓ **Je ne colle jamais de devis, de facture ou d'informations clients dans l'IA.**
  (Un devis dans ChatGPT peut être réutilisé ailleurs sans votre accord.)
- ✓ **Je remplace les données personnelles ou financières par des termes génériques : « Client A », « X€ ».**
  (Elles pourraient être réutilisées par l'IA dans la réponse donnée à un autre utilisateur.).
- ✓ **Je désactive l'historique des conversations sur mon outil IA.**
  (Sinon, vos échanges peuvent rester enregistrés sur les serveurs.)
- ✓ **Je vérifie la politique de confidentialité de mon outil.**
  (Les versions gratuites ne garantissent pas toujours la sécurité des données.)
- ✓ **Je rappelle ces règles à mon équipe.**
  (Un rappel, même informel lors de la pause-café, peut éviter une erreur coûteuse.)

2 Vérifier, vérifier, vérifier (le réflexe anti-hallucination)

L'IA fournit toujours une réponse, même fausse : elle peut inventer des faits ou des chiffres (hallucinations).

- ✓ **Je reste critique à l'égard des résultats générés.**
- ✓ **Je demande toujours à l'IA d'indiquer ses sources et je vérifie les informations.**
- ✓ **Je relis, je modifie et j'ajoute ma touche personnelle.**

3 Définir un cadre pour l'équipe

Toute entreprise, même la plus petite, a besoin d'un code de conduite IA.

C'est un document qui précise les usages autorisés et les précautions à prendre. Il peut inclure des règles concernant la confidentialité des données, la vérification des contenus générés, etc.

- ✓ **Je formalise dans un document ce qui est autorisé ou non pour mon entreprise.**
  Par exemple : « Vérifiez toujours les résultats. Ne partagez jamais de données sensibles. Mentionnez quand un contenu est produit avec IA. »
- ✓ **Je partage ce document en équipe, et je l'affine au fil du temps.**