Newsletter N° 17 – Mars 2026

IA et secret professionnel :

le trou dans la raquette des pros

Le risque que la plupart des professionnels ne voient pas, et qu'ils prennent tous les jours.

Le scénario est devenu banal. Un avocat copie-colle dans ChatGPT les pièces d'un dossier pour préparer ses conclusions.

Un médecin saisit le compte-rendu détaillé d'une consultation pour obtenir une aide à la synthèse.

Un expert-comptable importe le bilan d'un client pour repérer des incohérences.

Un consultant en stratégie partage des données confidentielles pour analyser un marché.

Chacun de ces gestes, parfaitement compréhensibles dans une logique de productivité, est aussi une violation potentielle du secret professionnel. Et la plupart de ceux qui les commettent n'en ont pas conscience.

Newsletter N° 17 – Mars 2026

Il y a là un trou dans la raquette qui mérite d'être regardé en face.

Le cadre juridique : pas de zone grise

Le secret professionnel n'a rien d'une option morale. En France, il est protégé par l'article 226-13 du Code pénal, qui punit d'un an d'emprisonnement et 15 000 euros d'amende sa violation, qu'elle soit volontaire ou par négligence. Et la jurisprudence est constante : la divulgation à un tiers non habilité, quelle qu'en soit la forme, constitue une violation.

La question n'est donc pas de savoir si un fournisseur d'IA est un tiers au sens du secret professionnel.

La question est : quand vous saisissez une information couverte par le secret dans ChatGPT, Claude ou Gemini, à qui la communiquez-vous exactement ? La réponse, dans la majorité des cas, est inconfortable : vous la communiquez à une société commerciale, généralement de droit américain, dont les serveurs sont à l'étranger, et qui dans ses conditions générales se réserve souvent le droit d'utiliser ces données à des fins d'amélioration de ses services.

Autrement dit, le simple fait de coller une information confidentielle dans un chatbot grand public peut, dans certaines configurations, constituer une violation du secret professionnel. Pas potentiellement. Effectivement.

Ce qui se passe vraiment avec vos données

La plupart des utilisateurs ont une représentation floue de ce qui se passe quand ils envoient un texte à un LLM. Il est utile de clarifier.

Premier point : votre saisie transite par internet, généralement vers des serveurs situés hors de France et souvent hors de l'Union européenne.

Le simple transfert constitue déjà un traitement au sens du RGPD si la donnée contient des éléments personnels.

Deuxième point : la donnée est stockée, au moins temporairement, sur les serveurs du fournisseur. Selon les politiques de chaque service, la durée de conservation varie.

Les versions grand public conservent souvent les conversations pendant des durées qui se comptent en mois, parfois plus.

Troisième point, le plus sensible : selon les options choisies par l'utilisateur, et selon les conditions générales du service, vos saisies peuvent être utilisées pour entraîner les modèles futurs.

Concrètement, le texte de votre conversation peut nourrir une version future du modèle, qui pourra alors restituer des fragments dans les réponses faites à d'autres utilisateurs.

Ce risque, baptisé fuite par mémorisation, est documenté par la recherche.

Quatrième point, souvent oublié : les métadonnées. Même quand le contenu lui-même n'est pas conservé, les informations sur votre usage (fréquence, horaires, types de requêtes, adresse IP, identifiant de compte) sont presque toujours collectées.

Ces métadonnées peuvent révéler beaucoup, parfois plus que le contenu lui-même.

Les vraies solutions, et celles qui n'en sont pas

Face à ce constat, plusieurs réflexes circulent dans les milieux professionnels. Tous ne se valent pas.

Newsletter N° 17 – Mars 2026

La fausse solution numéro un : l'anonymisation manuelle. Remplacer les noms par des prénoms inventés, masquer les dates, transformer M. Dupont en M. X. Le problème est que cette anonymisation est presque toujours insuffisante. Le contexte (lieu, profession, montants, dates approximatives) reste souvent assez précis pour permettre une réidentification.

Et surtout, elle est fastidieuse, donc pratiquée à moitié, donc inefficace.

La fausse solution numéro deux : se contenter de désactiver l'option d'entraînement dans les paramètres. C'est utile, mais cela ne change rien à la question du transit, du stockage, et du fait que vous communiquez l'information à un tiers.

La violation du secret peut être constituée sans qu'il y ait entraînement.

La vraie solution numéro un : utiliser les offres entreprise (Claude for Work, ChatGPT Enterprise, ou équivalents). Ces offres incluent généralement un engagement contractuel de non-utilisation des données pour l'entraînement, des serveurs européens dans certaines configurations, et des garanties contractuelles opposables.

Elles ont un coût, mais elles transforment la relation juridique.

La vraie solution numéro deux : pour les usages les plus sensibles, le déploiement local de modèles open source (Llama, Mistral, Qwen). Le modèle

tourne sur votre infrastructure, les données ne sortent jamais.

Cette option est techniquement plus exigeante mais offre le plus haut niveau de garantie. Plusieurs cabinets et études ont franchi le pas.

La vraie solution numéro trois : la formation des équipes. Le maillon faible, c'est presque toujours l'humain qui copie-colle sans réfléchir.

Une charte d'usage interne, claire et appliquée, vaut mieux que les meilleures protections techniques contournées par habitude.

Les cas concrets qui doivent alerter

Quelques situations méritent une vigilance particulière, parce qu'elles cumulent les risques.

Le dossier complet d'un client copié dans un chatbot pour gagner du temps sur la rédaction. Risque maximal. La quantité d'information, sa nature, le caractère identifiable du client, tout converge.

Le compte-rendu médical détaillé saisi pour aider à formuler un courrier au patient. Données de santé, donc catégorie particulière au sens du RGPD, donc protection renforcée. Risque maximal également.

Newsletter N° 17 – Mars 2026

Le tableau de bord financier d'une PME importé pour générer une note de synthèse. Données économiques sensibles, parfois couvertes par des clauses de confidentialité contractuelle qui n'autorisent pas ce type de transfert.

La conversation à caractère stratégique avec un client, retranscrite dans une IA pour en extraire les points clés.

Souvent fait par les commerciaux, presque toujours problématique.

Le brouillon d'un acte juridique soumis à relecture par une IA. Si l'acte concerne une transaction sensible, une fusion, un litige en cours, le simple fait de le faire transiter pose problème.

Une responsabilité qui ne se délègue pas

Un point souvent évoqué pour minimiser le risque : la responsabilité repose sur le fournisseur d'IA, pas sur l'utilisateur. C'est inexact. Le secret professionnel s'impose à la personne qui en est dépositaire, et c'est elle qui répond de sa violation. Le fait d'avoir confié l'information à un système tiers ne dégage pas sa responsabilité.

Pire : le caractère intentionnel ou négligent de la divulgation n'est pas une cause d'exonération. Le délit de violation du secret professionnel est constitué

dès lors que l'information protégée a été divulguée à une personne non habilitée à la recevoir, indépendamment de la conscience qu'avait l'auteur du caractère problématique de son geste.

Cela signifie, pour les professionnels concernés, qu'on ne peut pas se retrancher derrière le je ne savais pas que ChatGPT gardait les données. La défense ne tient pas.

Et au-delà du risque pénal, il y a le risque disciplinaire, le risque civil en cas de préjudice subi par le client, et le risque réputationnel qui peut être considérable.

Une question d'hygiène professionnelle

Tout cela ne signifie pas qu'il faille renoncer à l'IA dans les professions à secret. Cela signifie qu'il faut adopter une hygiène d'usage rigoureuse.

Concrètement, 3 règles simples permettent de limiter le risque dans la grande majorité des cas. D'abord, ne jamais utiliser un service grand public pour traiter une information couverte par le secret.

Si l'usage est ponctuel, anonymiser et abstraire au maximum. Si l'usage est régulier, basculer sur une offre entreprise. Ensuite, séparer les outils : un

compte personnel pour les usages courants, un compte professionnel sécurisé pour les usages métier. Ne pas tout mélanger sur un même service.

Enfin, garder une trace écrite de la posture adoptée. Une note interne, une charte, une procédure. En cas de question, c'est ce qui permet de démontrer la diligence.

Le secret professionnel a survécu à l'arrivée du téléphone, du fax, du courrier électronique. Il survivra à l'IA. Mais à condition que les professionnels concernés prennent la mesure du risque avant qu'il ne se matérialise.

Passez une excellente journée

Gabriel PAPP

gpappAI.com