# Fiche Pratique N°53 : Utilisez l'IA sans livrer votre vie privée V1.3

7 nov, 2026 · @Gabriel

***Objectif :*** *profiter de l'intelligence artificielle en privilégiant les IA qui fonctionnent sur votre propre ordinateur et les assistants européens, ne rien confier de sensible aux autres, et régler au plus strict ceux des géants américains (ChatGPT, Claude, Gemini, Copilot) si vous les utilisez encore.*

- ***Public visé :*** *débutant à intermédiaire*
- ***Temps estimé :*** *15 minutes pour les réglages ; 30 minutes pour essayer une IA locale*
- ***Difficulté :*** *★☆☆☆☆ avec un assistant européen (Lumo, Euria), ★★★☆☆ pour une IA locale*
- ***Fiches associées :*** *N°13 (Linux), N°16 (mots de passe), N°26 (chiffrer ses fichiers), N°46 (gestes de base), N°47 (arnaques en ligne)*

## 1. Pourquoi faire attention ? (Le problème)

Un assistant d'IA donne l'impression d'une conversation privée. En réalité, chaque question part sur les serveurs d'une entreprise, souvent américaine, où elle peut être conservée, relue et réutilisée.

| Ce qui peut arriver à vos questions | Exemple |
|---|---|
| Conservées dans un historique | Pendant des mois, voire des années selon le service et les réglages |
| Utilisées pour entraîner les modèles | Souvent activé par défaut dans les versions gratuites |
| Relues par des humains | Pour « améliorer le service » ; Google l'indique pour Gemini |
| Soumises au Cloud Act | Les données d'une entreprise américaine restent accessibles aux autorités américaines, même stockées en Europe |
| Exposées en cas de fuite | Comme toute base de données |

**Le risque :** confier sans y penser un dossier médical, un contrat, les coordonnées d'un proche ou un secret professionnel, comme on parlerait à un ami.

**Le bénéfice :** garder les avantages de l'IA (rédiger, résumer, expliquer) en décidant vous-même de ce qui sort de chez vous.

**Une règle simple :** n'écrivez à un assistant en ligne que ce que vous accepteriez d'envoyer sur une carte postale.

## 2. Ce qu'on ne confie jamais à un assistant en ligne

| À ne pas confier | À la place |
|---|---|
| Mots de passe, codes, numéros de carte | Jamais, sous aucune forme |
| Numéro de sécurité sociale, pièce d'identité, RIB | Remplacez par « [numéro] » |
| Données de santé nominatives | Décrivez la situation sans nom ni date de naissance |


gabriel.ananda@mailo.com
CC BY SA

| À ne pas confier | À la place |
|---|---|
| Noms, adresses, téléphones de proches ou de clients | Prénoms inventés, « Monsieur X » |
| Documents confidentiels de travail ou d'association | Un résumé anonymisé, ou une IA locale (section 3) |
| Photos de personnes, de documents, de votre domicile | Recadrer, flouter, ou s'abstenir |
| Conversations privées copiées-collées | L'accord des personnes concernées d'abord |

**La méthode des crochets :** avant d'envoyer un texte, remplacez chaque nom, adresse ou numéro par un repère entre crochets : « [Client A] habite [ville] ». La réponse reste utile, et vous remettez les vrais noms ensuite, chez vous.

**Le texte en dit plus que vous ne croyez :** même sans nom, une IA peut deviner votre ville, votre niveau de revenu ou votre sexe à partir de votre façon d'écrire et des détails donnés en passant (lieux, dates, vocabulaire de métier). Une étude a aussi trouvé des données personnelles dans près de la moitié des demandes de traduction (48 %) : on colle un courriel entier sans penser aux noms, adresses et signatures qu'il contient. Les crochets réduisent ce risque sans le supprimer.

**Découpez les sujets sensibles :** posez les différentes parties d'une question délicate dans des conversations séparées, voire à des assistants différents, pour qu'aucun ne dispose du dossier complet.

## 3. Choisir : du plus souverain au moins souverain

| Priorité | Solution | Vos questions vont… | Pour qui |
|---|---|---|---|
| 1 | IA sur votre ordinateur : Jan, Ollama (GPT4All n'est plus mis à jour depuis 2025) | Nulle part : tout reste chez vous, même hors connexion | Documents sensibles, et tous ceux qui ont un ordinateur récent |
| 2 | Assistant européen : Lumo de Proton (Suisse), sans entraînement ni journaux, utilisable sans compte ; Euria d'Infomaniak (Suisse), gratuit, hébergé en Suisse et sans entraînement ; Vibe de Mistral (France), une fois l'entraînement désactivé | En Europe, sous le RGPD ou la loi suisse | Usage quotidien, sans rien installer |


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°53 : Utilisez l'IA sans livrer votre vie privée V1.3

| Priorité | Solution | Vos questions vont… | Pour qui |
|---|---|---|---|
| 3 | En dernier recours : assistant américain ou chinois, réglé au plus strict (section 4) | Aux États-Unis ou en Chine | Seulement si vous ne pouvez pas faire autrement |

**Notre conseil :** pour l'usage courant, choisissez **Lumo** ou **Euria** ; pour tout ce qui est personnel ou confidentiel, une **IA locale**. Les assistants des géants américains (ChatGPT, Gemini, Copilot) sont conçus pour s'intégrer à leurs autres services et apprendre de vous : n'y créez pas de compte si vous n'en avez pas déjà un.

## Essayer une IA locale avec Jan (le plus simple)

1. Téléchargez **Jan** depuis son site officiel, `jan.ai` (Windows, macOS ou Linux), et installez-le comme un logiciel ordinaire. Aucun compte n'est demandé.
2. Au premier lancement, choisissez un **petit modèle** proposé dans la liste (quelques gigaoctets) et laissez-le se télécharger.
    - **Vous devez voir :** le modèle marqué comme installé.
3. **Coupez le Wi-Fi**, puis posez une question.
    - **Vous devez voir :** une réponse, sans connexion. La preuve que rien ne sort de votre ordinateur.
4. Pour un texte confidentiel, collez-le directement dans la conversation : il ne quitte pas votre ordinateur.

**À savoir :** une IA locale est plus lente et un peu moins brillante qu'un grand service en ligne. Un ordinateur récent avec 16 Go de mémoire est confortable ; avec 8 Go, choisissez les plus petits modèles. Pour résumer, reformuler ou corriger un texte, elle suffit largement.

**« Open source » ne veut pas dire « chez vous » :** un modèle libre (comme ceux de DeepSeek ou de Mistral) utilisé sur le site de son éditeur envoie vos questions sur ses serveurs, comme n'importe quel service en ligne. Seule l'installation sur votre ordinateur (priorité 1) garde tout chez vous.

⚠️ **Sans compte, mais pas sans géants :** Duck.ai, de DuckDuckGo, donne accès à plusieurs modèles connus sans inscription. Il masque votre adresse IP, et les fournisseurs s'engagent à ne pas entraîner leurs modèles sur ces échanges et à les effacer sous 30 jours. Vos questions partent tout de même chez ces fournisseurs, souvent américains : la règle de la carte postale s'applique toujours.

## 4. Si vous utilisez encore un assistant américain ou chinois : le régler au plus strict

Si vous gardez un de ces assistants, ou si vous utilisez Vibe de Mistral, trois réglages comptent : **l'entraînement** (vos échanges servent-ils à améliorer le modèle ?), **l'historique** (combien de temps sont-ils gardés ?), et la **conversation temporaire** (une discussion qui ne laisse pas de trace dans l'historique).


gabriel.ananda@mailo.com
CC BY SA

| Assistant | Où régler | Ce qu'il faut faire |
|---|---|---|
| ChatGPT (OpenAI, États-Unis) | Paramètres › Contrôles des données | Désactiver « Améliorer le modèle pour tous » ; utiliser la « Discussion temporaire » pour les sujets sensibles ; dans les contrôles publicitaires, refuser la personnalisation des publicités fondée sur vos conversations |
| Claude (Anthropic, États-Unis) | Paramètres › Confidentialité (claude.ai/settings/data-privacy-controls) | Désactiver « Aider à améliorer Claude » : vos conversations sont alors gardées 30 jours au lieu de 5 ans ; pour les sujets sensibles, ouvrir une « conversation incognito » (icône fantôme en haut à droite), jamais utilisée pour l'entraînement |
| Gemini (Google, États-Unis) | gemini.google.com › Paramètres et aide › Activité | Désactiver « Garder l'activité » (« Désactiver » ou « Désactiver et supprimer l'activité ») ; les échanges restent alors gardés jusqu'à 72 heures |
| Copilot (Microsoft, États-Unis) | Icône de profil › votre nom › Confidentialité ; puis Mémoire › Personnalisation et mémoire | Désactiver l'entraînement sur vos conversations écrites et vocales, puis la personnalisation et la mémoire |
| Vibe, ex-Le Chat (Mistral, France) | Paramètres › Confidentialité (sur mobile : « Contrôle des données et du compte ») | Désactiver « Autoriser l'utilisation de vos interactions avec Vibe pour entraîner les modèles » (sur mobile : décocher « Activer le partage des données »), activé par défaut en version gratuite |
| DeepSeek (Chine) | Menu › votre nom › Paramètres › Données | Désactiver « Améliorer le modèle pour tous » ; mais lisez d'abord l'avertissement ci-dessous |

⚠️ **DeepSeek : vos données partent en Chine.** D'après sa politique de confidentialité, DeepSeek stocke vos conversations sur des serveurs en Chine, soumis au droit chinois. L'Italie a fait retirer l'application des magasins d'applications début 2025, et la commissaire allemande à la protection des données a demandé en juin 2025 à Apple et Google de la retirer, faute de preuve d'une protection équivalente au RGPD. **Conseil :** n'utilisez pas l'application ni le site DeepSeek pour quoi que ce soit de personnel. Les modèles DeepSeek sont en revanche publiés en accès libre : vous pouvez en faire tourner une version allégée sur votre ordinateur avec Jan ou Ollama (section 3), et rien ne part alors en Chine.

⚠️ Les boutons « pouce en l'air / pouce en bas » envoient souvent la conversation pour analyse, quels que soient vos réglages. Évitez-les sur les sujets sensibles.

**La mémoire, le réglage qu'on oublie :** la plupart des assistants retiennent désormais, d'une conversation à l'autre, ce qu'ils apprennent de vous (métier, proches, lieux). Chez Claude, elle est proposée aussi en


gabriel.ananda@mailo.com
CC BY SA

version gratuite depuis mars 2026 : vérifiez son état dans Paramètres › Mémoire ; chez ChatGPT, elle se règle dans Paramètres › Personnalisation › Mémoire ; chez Vibe, dans l'onglet des mémoires (« Memories »). Désactivez-la, ou relisez régulièrement ce qu'elle contient, et revérifiez après chaque mise à jour de l'application.

⚠️ **Supprimer une conversation ne suffit pas.** Ce que l'assistant en a retenu reste dans sa mémoire (Claude, ChatGPT), et sur ChatGPT les fichiers que vous y aviez joints restent dans la « Bibliothèque ». Chez Vibe, désactiver la mémoire n'efface pas les mémoires déjà enregistrées. Videz donc la mémoire et la bibliothèque à part, avant de désactiver.

**Lien de partage = page publique :** toute personne qui reçoit le lien d'une conversation partagée peut la lire. En juillet 2025, environ 4 500 conversations ChatGPT partagées sont apparues dans les résultats de Google, et OpenAI a dû retirer l'option en cause. Ne partagez pas de conversation personnelle, et considérez tout lien créé comme public, même après l'avoir supprimé.

**Compte fourni par l'employeur ou l'association :** son responsable peut accéder à vos conversations. Chez Claude, par exemple, le propriétaire principal d'un compte Team ou Enterprise peut exporter celles de tous les membres. Réservez ce compte au travail, et utilisez un compte personnel pour le reste.

**Pour finir :** supprimez de temps en temps l'historique des conversations que vous ne voulez pas garder, et refusez que l'assistant ait accès à vos courriels, à votre agenda ou à vos fichiers si vous n'en avez pas besoin.

⚠️ **Assistants qui agissent à votre place (« agents ») :** de plus en plus d'assistants peuvent naviguer sur le web, lire vos courriels ou remplir des formulaires pour vous. Une page, un courriel ou un document peut contenir des instructions cachées, invisibles pour vous mais lues par l'IA, qui la détournent : c'est l'« injection de prompt ».

- Donnez-leur le moins d'accès possible : pas de messagerie ni de fichiers sans vrai besoin.
- Gardez la demande de confirmation avant chaque action, et lisez-la vraiment.
- Ne tapez jamais un mot de passe ni un numéro de carte dans la tâche : reprenez la main et saisissez-les vous-même sur le site.
- Ne branchez que des extensions ou services dont vous connaissez l'éditeur.
- Surveillez les tâches importantes, et arrêtez l'agent s'il fait autre chose que prévu.

## 5. Garder son esprit critique

La souveraineté, c'est aussi celle de notre jugement.

- **Une IA peut se tromper avec aplomb :** elle invente parfois des chiffres, des sources ou des lois. Vérifiez tout ce qui compte (santé, argent, droit) auprès d'une source fiable.
- **Gardez la main :** l'IA propose, vous décidez. Relisez et corrigez ce qu'elle rédige avant de l'envoyer. Avant de conclure, demandez-vous : cette conclusion est-elle la mienne, ou celle de l'IA ?
- **Elle cherche à vous plaire :** une IA a tendance à aller dans votre sens. En avril 2025, OpenAI a dû retirer une mise à jour de ChatGPT jugée « trop flatteuse ». Posez des questions neutres (« Quels sont les avantages et les inconvénients de… ? » plutôt que « N'est-ce pas que… ? »), ou demandez successivement les arguments pour et contre.


gabriel.ananda@mailo.com
CC BY SA

- **Exigez les sources, puis vérifiez-les :** demandez d'où viennent les affirmations, ouvrez chaque lien pour vérifier qu'il existe et dit bien ce qu'on lui prête, et jugez la fiabilité du site. Archivez une source importante sur la Wayback Machine (`web.archive.org`) pour la retrouver même si la page change ou disparaît.
- **Croisez les réponses :** pour une question importante, interrogez deux assistants d'éditeurs différents ; s'ils divergent, creusez. Mais deux IA d'accord peuvent se tromper ensemble : seule une source fiable tranche.
- **Méfiez-vous des contrefaçons :** des applications imitent les assistants connus pour voler des données ou de l'argent. Installez-les depuis les sources officielles (fiche N°47).
- **Voix et images truquées :** l'IA sait imiter la voix d'un proche. En cas d'appel urgent et inhabituel demandant de l'argent, raccrochez et rappelez la personne sur son numéro habituel.

## 6. À savoir avant de se lancer

| Crainte fréquente | La réalité |
|---|---|
| « Sans IA, je vais être dépassé. » | On peut l'utiliser, simplement en choisissant ce qu'on lui confie. |
| « Une IA locale, c'est pour les informaticiens. » | Jan s'installe comme un logiciel ordinaire, sans compte. |
| « Ces réglages, c'est trop compliqué. » | Un interrupteur par assistant, une seule fois. |
| « L'IA européenne est moins bonne. » | Pour l'usage courant (rédiger, résumer, expliquer), la différence est faible. |
| « Je dois garder ChatGPT, tout le monde l'utilise. » | Rien ne vous y oblige : un assistant européen ou local fait la même chose pour l'essentiel, sans nourrir un géant de vos questions. |

## 7. Challenge 7 jours

- **Jour 1 :** faire la liste des assistants d'IA que vous utilisez, y compris ceux intégrés au téléphone, au navigateur ou à la messagerie.
- **Jour 2 :** essayer Lumo ou Euria pour une tâche habituelle.
- **Jour 3 :** supprimer l'historique dont vous n'avez pas besoin, puis relire et vider la mémoire de l'assistant.
- **Jour 4 :** pratiquer la méthode des crochets sur un vrai texte.
- **Jour 5 :** si vous gardez un assistant américain, désactiver l'entraînement et la mémoire (section 4), ou supprimer le compte.
- **Jour 6 :** installer Jan et lui poser une question hors connexion.
- **Jour 7 :** vérifier une réponse d'IA auprès d'une source fiable.


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°53 : Utilisez l'IA sans livrer votre vie privée V1.3

## 8. En résumé (ce que vous gagnez)

| Action | Bénéfice |
|---|---|
| Ne rien confier de sensible | Votre vie privée et celle de vos proches protégées |
| Désactiver l'entraînement | Vos échanges ne nourrissent plus le modèle |
| Vider la mémoire de l'assistant | Il oublie ce qu'il avait retenu de vous |
| Conversation temporaire | Pas de trace dans l'historique |
| Assistant européen | Vos données restent sous le RGPD |
| IA locale | Aucune donnée ne sort de chez vous |

## 9. À retenir absolument

- **La règle de la carte postale :** n'écrivez rien que vous n'enverriez pas à découvert.
- **Les crochets :** [nom], [adresse], [numéro] avant d'envoyer.
- **Local et européen d'abord :** Jan pour le sensible, Lumo ou Euria pour le quotidien.
- **Un interrupteur à couper :** l'entraînement sur vos conversations, si vous gardez un assistant américain.
- **Supprimer ne suffit pas :** videz aussi la mémoire, et ne partagez pas de lien de conversation.
- **Pour le sensible : une IA locale**, qui fonctionne sans Internet.
- **L'IA propose, vous décidez :** vérifiez ce qui compte.

**Test final :** posez une question à Jan, Wi-Fi coupé, puis rédigez une demande à Lumo ou Euria avec la méthode des crochets. Si vous y arrivez, vous avez réussi ✅

## Références


- CNIL – intelligence artificielle
- Siècle Digital – 5 réglages ChatGPT à modifier (août 2026)
- Anthropic – mise à jour des conditions grand public de Claude (août 2025)
- Anthropic – utiliser les conversations incognito
- MacRumors – désactiver l'entraînement de Claude (août 2025)
- Google – gérer l'activité dans les applis Gemini
- Microsoft – contrôles de confidentialité de Copilot
- Clubic – Mistral Vibe et vos données (octobre 2026)
- AlternativeTo – Le Chat devient Vibe (mai 2026)
- DeleteMe – réglages de confidentialité de DeepSeek (2026)
- Anonyome – DeepSeek et la vie privée (2026)
- Mac4Ever – l'Allemagne exige le retrait de DeepSeek (juin 2025)
- Computerworld – l'Italie bloque DeepSeek (janvier 2025)
- Proton – confidentialité de Lumo
- Jan – site officiel



gabriel.ananda@mailo.com
CC BY SA

- PromptQuorum – test de Jan (2026)
- PromptQuorum – GPT4All sans mise à jour depuis 2025
- Anthropic – mémoire de Claude
- Anthropic – export des données d'une organisation
- MacRumors – mémoire de Claude pour les comptes gratuits (mars 2026)
- OpenAI – mémoire et nouveaux contrôles de ChatGPT
- PCWorld – la Bibliothèque de fichiers de ChatGPT (mars 2026)
- PC Gamer – conversations ChatGPT indexées par Google (août 2025)
- Mistral – mémoires de Vibe
- Google – utiliser Gemini Agent (injection de prompt)
- Mireshghallah et al. – « Trust No Bot », données personnelles dans les conversations (2024)
- Staab et al. – « Beyond Memorization », déduire des informations d'un texte (2023)
- TechCrunch – ChatGPT trop flatteur (avril 2025)
- Infomaniak – découvrir Euria
- DuckDuckGo – Duck.ai et la confidentialité
- Internet Archive – Wayback Machine



gabriel.ananda@mailo.com
CC BY SA