

10 questions à poser à un cabinet IA sur ses agents conversationnels

10 questions essentielles à poser à un cabinet IA sur ses agents conversationnels

1. Architecture et transparence

« Quelle méthodologie utilisez-vous pour documenter l'architecture de vos agents (modèles de langage, sources de données, mécanismes de décision) ? »

(Exigences de traçabilité technique et conformité à des cadres comme la Loi 25 au Québec)^[1]
^[2]

2. Explicabilité des réponses

« Comment garantissez-vous l'explicabilité des réponses générées, notamment face aux risques d'hallucinations ou de biais ? »

(Référence aux bonnes pratiques en XAI et gestion des incertitudes)^[3] ^[4]

3. Gestion des données

« Quelles mesures prenez-vous pour assurer l'anonymisation des données et le consentement éclairé des utilisateurs ? »

(Alignement sur la Loi 25 et standards de protection des renseignements personnels)^[5] ^[2]

4. Biais algorithmiques

« Comment testez-vous et corrigez-vous les biais discriminatoires dans les réponses de vos agents ? »

(Audits adversariaux et méthodes de débiaisage mentionnées dans les cadres éthiques)^[3] ^[4]

5. Conformité réglementaire

« Vos agents sont-ils conformes aux obligations d'explicabilité de l'article 52 du règlement européen sur l'IA et aux projets de loi canadiens (C-27) ? »

(Anticipation des normes transnationales et juridictionnelles)^[6] ^[2]

6. Mises à jour et supervision

« Quelle est votre stratégie pour mettre à jour les connaissances des agents et superviser leurs interactions en temps réel ? »

(Maintenance des modèles et journalisation des requêtes)^{[5] [4]}

7. Sécurité des interactions

« Comment protégez-vous les conversations contre les attaques par injection de prompts ou l'extraction de données sensibles ? »

(Mesures de cybersécurité spécifiques aux LLM)^{[7] [4]}

8. Reddition de comptes

« Proposez-vous un registre public des algorithmes ou une fiche de transparence algorithmique pour chaque agent déployé ? »

(Engagement envers les registres proactifs comme le préconise l'OBVIA)^{[2] [4]}

9. Formation des utilisateurs

« Offrez-vous des guides de bonnes pratiques pour la formulation de prompts et la vérification des réponses générées ? »

(Référence aux recommandations pédagogiques comme celles de l'Université Laval)^{[8] [7]}

10. Responsabilité juridique

« Comment gérez-vous la responsabilité légale en cas d'erreur dommageable commise par un agent conversationnel ? »

(Clauses contractuelles et assurances spécifiques aux systèmes d'IA générative)^{[6] [2]}

Ces questions couvrent les **enjeux techniques, éthiques et juridiques** critiques, en s'appuyant sur les normes émergentes (ISO/IEC 42001), les lois québécoises (Loi 25) et les bonnes pratiques internationales en IA responsable^{[3] [2] [4]}.

✱

1. <https://reptic.ca/wp-content/uploads/2023/04/foire-aux-questions-agents-conversationnels-2023-03.pdf>
2. https://www.obvia.ca/sites/obvia.ca/files/ressources/202501-OBV-Pub-DanslOeildeObvia_Jan2025_0.pdf
3. <https://www.ibm.com/fr-fr/think/topics/ai-transparency>
4. <https://www.aoc.cat/fr/ia-transparencia-xatbots-amb-ia-generativa/>
5. <https://www.enseigner.ulaval.ca/numerique/intelligence-artificielle-generative>
6. <https://www.osfi-bsif.gc.ca/sites/default/files/documents/AIQuestionnaire-QuestionnaireIA-fr.xlsx>

7. <https://enseigner.hec.ca/outils/intelligence-artificielle-generative/>
8. <https://pressbooks.etsmtl.ca/construiremareussite/chapter/chatgpt/>