

أمن استعمالات الذكاء الاصطناعي

عمليات المراقبة الواجب إجراؤها قبل استعمال أدوات الذكاء الاصطناعي التوليدي وأثناءه

ترتب هذه القائمة عمليات المراقبة الأمنية الخاصة بأدوات الذكاء الاصطناعي التوليدي: الحسابات، والمعطيات، والوثائق المعالجة، والإضافات، والإجراءات المؤتمتة، والحوادث. وهي تكمل السياسة الأمنية للهيئة دون أن تحل محلها.

1. الحسابات والولوج

- ☐ إحصاء الحسابات التي تتيح الولوج إلى أدوات الذكاء الاصطناعي، بما فيها الحسابات الشخصية المستعملة في العمل.
- ☐ تفعيل المصادقة الثنائية على كل حساب.
- ☐ ربط الحسابات المهنية بالهيئة لا بعناوين شخصية.
- ☐ سحب صلاحيات الولوج عند مغادرة أحد المتعاونين.

2. المعطيات

- ☐ تحديد المعطيات المحظور إدخالها في أداة موجهة للعموم وتعميمها على المستعملين.
- ☐ التحقق، بالنسبة إلى كل أداة، من استعمال المحادثات لأغراض التدريب، ومن إعادة قراءتها من طرف أشخاص، ومن مدة حفظها.
- ☐ إيقاف استعمال المحادثات لتحسين النماذج عندما تتيح الأداة ذلك.
- ☐ قصر المعطيات ذات الطابع الشخصي والمعطيات السرية على العروض الخاضعة لعقد معالجة.

3. الوثائق والتعليمات المخفية

- ☐ معاملة الوثائق وصفحات الويب والرسائل الإلكترونية المعروضة على أداة باعتبارها مادة للتحليل، لا باعتبارها تعليمات.
- ☐ عدم عرض وثائق مجهولة المصدر على أداة تتوفر على صلاحيات للتنفيذ.
- ☐ مراقبة الروابط والمرفقات التي تنتجها أداة قبل فتحها أو إحالتها.

4. الإضافات والموصّلات والإجراءات المؤتمتة

- ☐ إخضاع تثبيت إضافات المتصفح وتطبيقات الذكاء الاصطناعي لإذن مسبق.
- ☐ حصر الموصّلات (البريد الإلكتروني، التخزين، الأجنحة) في صلاحيات الولوج الضرورية وحدها.
- ☐ اشتراط مصادقة بشرية قبل أي إجراء ذي أثر خارجي: الإرسال، أو النشر، أو الأداء، أو الحذف.
- ☐ الاحتفاظ بأثر للإجراءات التي تنفذها أداة مؤتمتة.

5. الحوادث

- ☐ تعيين الشخص الذي يُبلغ إليه عن أي إدخال عرضي أو تسريب أو محتوى خاطئ تم نشره.
- ☐ تقييد كل حادث: التاريخ، والأداة، والمعطيات المعنية، والتدابير المتخذة.
- ☐ دراسة الالتزامات المترتبة على القانون رقم 09.08، في حال تعلق الأمر بمعطيات ذات طابع شخصي.
- ☐ دراسة التزامات التصريح المنصوص عليها في القانون رقم 05.20، بالنسبة إلى الكيانات الخاضعة له.

وثيقة إعلامية عامة، لا تشكل استشارة قانونية ولا رأياً بشأن وضعية خاصة. ويتعين التحقق من المراجع القانونية في صيغتها السارية في تاريخ الاستعمال. مكتب استشارة غير مسجل في هيئة المحامين؛ لا تمثيل أمام المحاكم ولا أي عمل محفوف للمهن القانونية المنظمة.

المراجع

- القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 22 من صفر 1430 (18 فبراير 2009)، الجريدة الرسمية عدد 5711 بتاريخ 23 فبراير 2009 (النشرة العامة) وعدد 5714 بتاريخ 5 مارس 2009 (نشرة الترجمة الرسمية)، المادة 23.
- القانون رقم 05.20 المتعلق بالأمن السيبراني، الصادر بتنفيذه الظهير الشريف رقم 1.20.69 بتاريخ 4 ذي الحجة 1441 (25 يوليوز 2020)، الجريدة الرسمية عدد 6904 بتاريخ 30 يوليوز 2020 (النشرة العامة)، ص. 4160، وعدد 6906 بتاريخ 6 غشت 2020 (نشرة الترجمة الرسمية)، المواد 8 و14 و30 و33.
- OWASP، «LLM01:2025 Prompt Injection»، OWASP Top 10 for LLM Applications 2025، <https://genai.owasp.org/llmrisk/llm01-prompt-injection> (صفحة أُطلع عليها في 21 أكتوبر 2026).
- OWASP، «LLM06:2025 Excessive Agency»، OWASP Top 10 for LLM Applications 2025، <https://genai.owasp.org/llmrisk/llm062025-excessive-agency> (صفحة أُطلع عليها في 21 أكتوبر 2026).