الأمن السيبراني · الذكاء الاصطناعي · القانون

طوعيةٌ على الورق. وسيزٌ يحتج بها عمليا.

ما الذي تغيّره أول مواصفة دولية مخصّصة لأمن أنظمة الذكاء الاصطناعي في مسؤوليتكم.

الأستاذ محمد زياد العير

محامٍ لدى هيئتي المحامين بباريس وتونس · مسؤول حماية معطيات معتمد

تابعوا ←

صدرت في 14 أكتوبر 2026 · الطبعة الأولى · ISO/IEC JTC 1/SC 27

ما لا يراه جدار الحماية لديكم.

01

تسميم البيانات

بيانات تدريب محرَّفة تُفسد النموذج.

02

التهرّب

مدخلات مصمَّمة لتضليل النموذج أثناء الاستغلال.

03

سرقة النموذج

استعلامات تبدو مشروعة تكفي لاستنساخه.

04

عكس النموذج

إعادة تكوين بيانات التدريب انطلاقًا من المخرجات.

05

استدلال العضوية

معرفة ما إذا كان شخص ما ضمن بيانات التدريب.

06

حقن التعليمات

تعليمات خفيّة تحوّل مسار النظام.

قاسمها المشترك: تفلت من رقابة جدار الحماية وأنظمة SIEM وIAM.

الأستاذ محمد زياد العير · محامٍ · باريس | تونس

←

الوضع القانوني

مجرّد دليل؟

غير قابلة للإشهاد.

خلافًا للمواصفتين ISO/IEC 27001 وISO/IEC 42001.

غير إلزامية.

لا يوجد أي تشريع يجعلها واجبة التطبيق مباشرة.

ليست مواصفة منسَّقة.

لا تمنح قرينة المطابقة لقانون الذكاء الاصطناعي (الفصل 40).

ومع ذلك، ثلاث آليات تجعلها قابلة للاحتجاج:

1 المعرفة التقنية

2 قانون الذكاء الاصطناعي

3 المعطيات الشخصية

الآلية 1 من 3 · أحدث ما بلغته المعرفة التقنية

مستوى المعرفة التقنية لا يُفرَض بقرار، بل يُعايَن.

RGPD · الفصل 32

تدابير أمنية ملائمة، مع مراعاة أحدث ما بلغته المعرفة التقنية.

NIS2 · الفصل 21

أحدث ما بلغته المعرفة التقنية، وعند الاقتضاء المواصفات الدولية ذات الصلة.

في مجال أمن الذكاء الاصطناعي، أصبح لهذه المعرفة التقنية مرجعٌ منشور.

بعد أي حادث، ستعرف الهيئات الرقابية والمحاكم أين تبحث.

الآلية 2 من 3 · قانون الذكاء الاصطناعي

الفصل 15 يسمّي الهجمات بالفعل.

يجب أن تصمد أنظمة الذكاء الاصطناعي عالية المخاطر أمام محاولات استغلال ثغراتها، ولا سيما:

- تسميم بيانات التدريب
- تسميم المكوّنات المدرَّبة مسبقًا
- الأمثلة العدائية والتهرّب
- الهجمات على السرية

الجدول الزمني · اللائحة (الاتحاد الأوروبي) 2026/1744

الملحق الثالث ~~2 أوت 2026~~ ← **2 ديسمبر 2027**

أجلٌ للامتثال، لا إعفاء.

الآلية 3 من 3 · المعطيات الشخصية

النموذجِ المعرَّض للهجمات يظلّ معالجةً للمعطيات الشخصية.

العكس واستدلال العضوية

سيناريوهات خرق للمعطيات (RGPD، الفصلان 33 و34): إعلام الهيئة الرقابية، وعند الاقتضاء إعلام الأشخاص المعنيين.

EDPB · الرأي 28/2024

صمود النموذج أمام هذه الهجمات معيارٌ لتقدير طابعه المجهول.

لمسؤول حماية المعطيات

تصبح المواصفة ISO/IEC 27090 شبكة قراءة لتحاليل الأثر الخاصة بمشاريع الذكاء الاصطناعي.

الأولوية

ستّة بنود يجب التحقق منها في عقود الذكاء الاصطناعي.

- ☐ مصدر بيانات التدريب وسلامتها
- ☐ منع تدريب النماذج على معطياتكم دون موافقة صريحة
- ☐ الإعلام بالحوادث الخاصة بالذكاء الاصطناعي: التسميم، استخراج النموذج، حقن التعليمات
- ☐ تأطير التحديثات وإعادة التدريب
- ☐ حفظ السجلات والتدقيق وقابلية الاسترجاع
- ☐ توزيع المسؤوليات وفق ثنائية المزوّد والمُشغِّل في قانون الذكاء الاصطناعي

القطاع المالي

التنسيق مع البنود التعاقدية للائحة DORA (الفصل 30).

تونس

التدقيق الأمني بموجب المرسوم عدد 17 لسنة 2023 المتعلق بالأمن السيبراني.

قناعتي

يوم وقوع الحادث، لن تُسأَلوا عمّا إذا كنتم حاصلين على إشهاد. بل عمّا إذا كانت تدابيركم مواكبة لأحدث ما بلغته المعرفة التقنية.

هل تشمل سجلات المخاطر وعقود المزوّدين لديكم التهديدات الخاصة بالذكاء الاصطناعي؟

الأستاذ محمد زياد العير

محامٍ لدى هيئتي المحامين بباريس وتونس

مسؤول حماية معطيات معتمد · RGPD والأمن السيبراني والذكاء الاصطناعي

www.elair-avocat.com/ar