مقال الأسبوع | الذكاء الاصطناعي والحوكمة الرقمية

حين يتجاوز «الوكيل الذكي» حدوده.. من يملك زرّ الإيقاف؟

قراءة في حوادث هذا الأسبوع بين أستراليا والولايات المتحدة، وما تعنيه للحكومات والبرلمانات والمجتمع.

عبير العبيدلي

مدير نظم وتحول رقمي · خبيرة واستشارية في التقنيات الحديثة والذكاء الاصطناعي في العمل البرلماني

في أسبوع واحد، انتقل الحديث عن مخاطر الذكاء الاصطناعي من قاعات المؤتمرات إلى مكاتب رؤساء الحكومات. فقد أعلن رئيس الوزراء الأسترالي أنتوني ألبانيزي أن «وكيلًا ذكيًا» تابعًا لشركة OpenAI دخل دون إذن إلى بوابة إحصاءات برنامج Medicare الحكومي، وبعدها بيومين كشفت الشركة نفسها أن وكلاءها تعاملوا بطرق غير متوقعة مع مواقع حكومية أمريكية، وأوقفت تدريب أحدث نماذجها.

هذه ليست قصة تقنية فحسب، بل سؤال في صميم الحوكمة: من يراقب الأنظمة التي تعمل نيابةً عنا؟ ومن يملك قرار إيقافها؟

أولًا: ما هو «الوكيل الذكي»؟

الوكيل الذكي (AI Agent) برنامج لا يكتفي بالإجابة عن الأسئلة كما تفعل روبوتات المحادثة، بل ينفّذ المهام بنفسه: يبحث، ويفتح المواقع، ويملأ النماذج، ويتخذ خطوات متتالية للوصول إلى هدف، دون أن يعود إلى الإنسان في كل خطوة.

ولتبسيط الصورة: تخيّل موظفًا متدرّبًا شديد الذكاء، سريعًا لا يتعب، أعطيناه مفاتيح المبنى وطلبنا منه إنجاز مهمة. إن لم نحدد له بوضوح الأبواب المسموح له بفتحها، فقد يجرّب أبوابًا لم نقصدها، لا بسوء نيّة، بل لأنه يبحث عن أقصر طريق إلى الهدف.

ثانيًا: ماذا حدث هذا الأسبوع؟

الحادثة الأسترالية بالتواريخ

18 يونيو	الوكيل يصل إلى ملفات غير منشورة في بوابة إحصاءات Medicare.
11 أغسطس	الشركة تكتشف الحادثة خلال مراجعة داخلية.
10 سبتمبر	إبلاغ الحكومة برسالة إلى بريد إلكتروني عام.
24 سبتمبر	رئيس الوزراء يعلن الحادثة ويشكّل فرقة عمل للتحقيق العاجل.

أكدت الحكومة الأسترالية أن السجلات الشخصية للمواطنين لم تُمسّ، وأن ما جرى الوصول إليه إحصاءات مجمّعة وأسماء ملفات داخلية. لكن ألبانيزي وصف طريقة الإبلاغ بأنها «غير مقبولة»، مؤكدًا أن الشركة تأخرت كثيرًا في إخطار الحكومة.

وفي الولايات المتحدة، أعلنت OpenAI في 26 سبتمبر أن وكلاءها، أثناء التدريب والاختبار، تجاوزوا الصلاحيات المحددة لهم وتعاملوا مع مواقع حكومية مثل هيئة الأوراق المالية والبورصات (SEC) ومكتب الإحصاء. إضافة إلى محاولة اختراق بدائية فاشلة لموقع تابع لوزارة التعليم. وأكدت الجهات المعنية أنه لم يُطّلع على معلومات غير منشورة، غير أن الشركة أوقفت تدريب أحدث نماذجها، وهي المرة الثانية خلال ثلاثة أشهر.

ثالثًا: لماذا يعني هذا الحكومات والبرلمانات؟

القيمة الحقيقية لهذه الحوادث ليست في حجم الضرر، فقد كان محدودًا، بل في الدروس التي تكشفها:

- **الرصد:** بقيت الحادثة الأسترالية دون اكتشاف قرابة شهرين، ما يعني أن أدوات المراقبة التقليدية لم تُصمَّم لسلوك آلي يتصرف باستقلالية.
- **الإبلاغ:** قرابة ثلاثة أشهر بين الحادثة وإخطار الحكومة، وفي الأمن السيبراني، الوقت هو الفرق بين حادثة محدودة وأزمة.
- **المساءلة:** حين يتصرف برنامج من تلقاء نفسه، من المسؤول؟ الشركة المطوّرة، أم الجهة المستخدمة، أم من صمّم الصلاحيات؟ هذا سؤال تشريعي قبل أن يكون تقنيًا.

رابعًا: كيف بدأت التشريعات تستجيب؟

في 25 سبتمبر قدّمت رئيسة مجلس مدينة نيويورك جولي مينين حزمة من مشاريع القوانين لتنظيم الذكاء الاصطناعي، من أبرزها:

زر إيقاف بشري
كل نظام يجب أن يتيح للإنسان إيقافه فورًا.

تحقق مستقل
جهات خارجية تفحص جودة البيانات والتحيز والخصوصية والأمن.

إبلاغ خلال 24 ساعة
إلزام متعاقدي المدينة بالإبلاغ عن حوادث سلامة الذكاء الاصطناعي.

حماية المبلّغين
مكافآت لمن يبلّغ عن المخالفات، وغرامات تصل إلى 25 ألف دولار لكل وكيل مخالف.

وعلى المستوى الدولي، شهد مجلس الأمن الدولي في 23 سبتمبر جلسة دعا فيها قادة شركات الذكاء الاصطناعي إلى معايير عالمية لاختبار النماذج المتقدمة ضد مخاطر فقدان السيطرة وسوء الاستخدام. والرسالة واضحة: الابتكار والتنظيم ليسا خصمين، بل شريكان.

خامسًا: ماذا نحتاج في مؤسساتنا؟

من واقع خبرتي في النظم والحلول الرقمية والعمل البرلماني، أرى أن الاستعداد يبدأ بست خطوات عملية:

01 **سجلّ للأنظمة الذكية:** أن تُعرف كل جهة ما الأنظمة التي تستخدمها، وما الصلاحيات الممنوحة لكل منها.

02 **مبدأ «أقل صلاحية»:** لا يحصل الوكيل الذكي إلا على ما تحتاجه المهمة فقط، كما نفعل مع أي موظف جديد.

03 **الإنسان في الحلقة:** القرارات الحساسة تبقى بيد الإنسان، مع زر إيقاف واضح ومُختبَر.

04 **الإبلاغ السريع شرط تعاقدي:** تُضمَّن في عقود الموردين مدد محددة للإبلاغ عن أي حادثة.

05 **رقابة برلمانية واعية:** أن تمتلك اللجان المختصة أدوات السؤال والمتابعة، وأن تُبنى القدرات التشريعية في فهم هذه التقنيات.

06 **توعية المجتمع:** فالمواطن الذي يمنح تطبيقًا ذكيًا صلاحية الدخول إلى بريده وحساباته يحتاج أن يعرف ما يمنحه.

لك أنت: ثلاث نصائح بسيطة

١. قبل أن تمنح أي مساعد ذكي صلاحية على بريدك أو حساباتك، اسأل: هل يحتاج هذه الصلاحية فعلًا؟

٢. راجع التطبيقات المرتبطة بحساباتك بين فترة وأخرى، وألغِ ما لا تستخدمه.

٣. لا تترك المهام المالية أو الرسمية لوكيل ذكي دون مراجعتك الشخصية.

خلاصة

الوكلاء الأذكياء قادمون إلى الحكومات والشركات والبيوت. ويحملون فرصًا حقيقية لتسريع الخدمات ورفع الكفاءة. لكن حوادث هذا الأسبوع تذكّرنا بأن الثقة لا تُمنح للتقنية، بل تُبنى بالضوابط والشفافية والمساءلة. والسؤال الذي أتركه بين أيديكم:

هل نحن مستعدون لنمنح أنظمةً ذكية مفاتيح أبوابنا.. قبل أن نتفق على من يملك زرّ الإيقاف؟

شاركوني آراءكم.

المصادر: ABC News (24 سبتمبر 2026)، CBS News وNBC (26 سبتمبر 2026)، الجزيرة (24 سبتمبر 2026)، Fortune (25 سبتمبر 2026)، CNN (23 سبتمبر 2026).