كيف نستخدم أدوات الذكاء الاصطناعي دون التفريط بخصوصيتنا؟

منذ ظهوره أواخر 2022، تحول برنامج "تشات جي بي تي Chatgpt" إلى أداة يومية للملايين حول العالم، يستخدمونها في الكتابة والبحث والترجمة وتنظيم المهام.

في خضم هذا الانتشار السريع، نشأت أسئلة عن مصير المعلومات التي يشاركها المستخدمون أثناء الدردشة: هل يحتفظ بها نموذج الذكاء الاصطناعي؟ وما مدى خصوصية البيانات التي ندخلها؟

أثارت هذه الأسئلة جدًلا واسعًا بين المنظمين والخبراء، خاصةً بعد أن فرضت محكمة أمريكية في 2025 على شركة OpenAI الاحتفاظ بجميع سجلات المحادثات ضمن دعاوى قضائية، وهو ما عدته منظمة الحقوق الرقمية EFF تهديدًا خطيرًا لحق المستخدمين في حذف بياناتهم.

وبعد أشهر من التقاضي ألغيت هذه الأوامر، لكن المخاوف حول الخصوصية والاستعمال الذكي للتقنية ظلت قائمة.

ماذا يحدث للمعلومات التي نشاركها؟

توضح شركة OpenAI في سياسة الخصوصية الخاصة بالمستخدمين أن المحادثات المحذوفة تُزال من حساب المستخدم فورًا وتُجدول للحذف النهائي من خوادم الشركة خلال 30 يومًا ما لم تُلزمها الأوامر القانونية أو متطلبات الأمان بالاحتفاظ بها.

هذه السياسة أعيد العمل بها في أكتوبر/تشرين الأول 2025 بعد انتهاء أمر قضائي سابق يفرض الاحتفاظ بسجلات محادثات جميع المستخدمين؛ وتؤكد الشركة أن المحادثات تُستخدم لتطوير النماذج وتحسينها ما لم يختر المستخدم تعطيل ذلك ضمن إعدادات الدردشة.

مع ذلك، تظهر تقارير مستقلة أن مستخدمي النسخة المجانية لا يملكون السيطرة الكاملة على طريقة

التعامل مع بياناتهم مقارنة بالنسخ الموجهة للأعمال، إذ تسمح خطط المؤسسات للمشتركين بالاحتفاظ الكامل ببياناتهم ومنع استخدامها في التدريب.

تقول OpenAI إنها تدعم إجراءات أمان متعددة تشمل تشفير البيانات أثناء النقل والتخزين، وإجراء اختبارات اختراق منتظمة، وسياج حماية متعدد العوامل للمستخدمين.

كما توضح الشركة في وثيقة "إعدادات الخصوصية للمستهلك" أن الوضع الافتراضي لا يستخدم بيانات التصفح عبر "Atlas ChatGPT" لتدريب النماذج، وأن المستخدم يمكنه مسح تاريخ التصفح أو فتح نافذة متخفية عند الحاجة.

وتؤكد نفس الوثيقة أن النماذج تُدرّب لتجنب معالجة المعلومات الخاصة وأنها تقلل من استخدام البيانات الشخصية في مجموعات التدريب. رغم ذلك، تذكر الشركة أن الأسئلة والأجوبة يمكن مراجعتها من قبل موظفين لأغراض الأمان والامتثال، ما يعني أن النصوص لا تعد سرية تمامًا.

تدريب النماذج من خلال محادثاتنا

لا تقتصر مخاوف الخصوصية على الاحتفاظ بالبيانات فقط، بل تشمل أيضًا استخدام المدخلات لتطوير نماذج اللغة.

أكد تقرير صادر عن معهد ستانفورد للذكاء الاصطناعي البشري أن ست شركات أمريكية رائدة، بينها OpenAI وGoogle وMeta، تستخدم بشكل افتراضي محادثات المستخدمين لتحسين نماذجها، ولا تتيح لبعض المستخدمين خيارًا واضحًا للانسحاب.

وبيّن التقرير أن هذه الشركات تحتفظ بمعلومات المستخدمين لفترات طويلة وقد تُدرّب النماذج على بيانات الأطفال دون توفير آليات واضحة لحذفها.

الدراسة نفسها تحذر من أن مشاركة معلومات صحية أو مالية قد تؤدي إلى تصنيف المستخدم ضمن فئات تستغل لاحقًا في الإعلانات أو خدمات شركات التأمين.

إلى جانب هذا، يشير تقرير لـ"مستقبل خصوصية المنتديات" (FPF) إلى أن معظم منصات الذكاء الاصطناعي تستخدم ما يقدمه المستخدم من نصوص وصور لتعزيز النماذج.

كما يوصي بتجنب رفع وثائق أو صور تحتوي على بيانات تعريفية أو حساسة قبل تنقيحها؛ لأن بيانات الصور قد تحمل تفاصيل عن الموقع أو الأشخاص دون قصد.

ويوضح أن على المستخدمين إدارة خاصية "الذاكرة" في تطبيقات الذكاء الاصطناعي؛ لأن تفعيلها يجعل النموذج يتذكر تفاصيل المستخدم على مدى جلسات متعددة، ما يزيد من مخاطر تجميع المعلومات.

هذه المخاوف تدعمها دراسة من ستانفورد توصلت إلى أن وثائق الخصوصية المعتمدة لدى شركات الذكاء الاصطناعي معقدة وغامضة، ما يصعب على المستخدمين فهم حقوقهم المتعلقة بحذف البيانات أو مشاركة المعلومات مع أطراف ثالثة.

تسريبات وثغرات وأضرار محتملة

تظهر حالات التسريب الأمني أن مخاطر الخصوصية ليست نظرية فقط. في نوفمبر/تشرين الثاني 2025 أعلنت OpenAI عن حادث أمني لدى مزود التحليلات Mixpanel.

أدى الحادث إلى تسريب أسماء وعناوين بريد إلكتروني ومواقع تقريبية لمستخدمي واجهة البرمجة وبعض مستخدمي ChatGPT الذين قدموا تذاكر دعم.

ورغم أن الشركة أكدت أن المحادثات والمفاتيح السرية لم تتسرب، فقد اعترفت بأن المعلومات

المسربة يمكن استخدامها في حملات تصيد أو هندسة اجتماعية.

الخطر لا يقتصر على ما يكتبه المستخدم بل أيضًا على ما يمكن للنموذج الوصول إليه

كما اضطر OpenAI لاحقًا إلى إنهاء استخدام Mixpanel وتعزيز مراجعة شركائها لضمان عدم تكرار الحادث.

التسريبات ليست الخطر الوحيد؛ فالدراسات التحليلية تشير إلى أن أكثر من 34.8% من مدخلات الموظفين إلى منصات الذكاء الاصطناعي في نهاية 2025 كانت تحتوي على معلومات حساسة، ما يمثل ارتفاعًا كبيرًا مقارنة بنسبة 11% في 2023.

وتشمل هذه البيانات معلومات تعريف شخصية وأسرار شركات وبرمجيات خاصة ووثائق داخلية، ما يعني أن العامل البشري قد يكون الحلقة الأضعف في حماية الخصوصية.

كما أن الخطر لا يقتصر على ما يكتبه المستخدم، بل أيضًا على ما يمكن للنموذج الوصول إليه عندما يُدمج مع تطبيقات مثل Drive Google أو Slack، حيث يمكنه استخراج معلومات غير مفترض مشاركتها.

استخدام غير مصرح وأوامر قضائية

المخاوف من استخدام غير مصرح للبيانات دفعت هيئات تنظيمية إلى اتخاذ خطوات ضد OpenAI.

في ديسمبر/كانون الأول 2024 فرضت هيئة حماية البيانات الإيطالية غرامة قدرها 15 مليون يورو على الشركة، بعد أن خلصت إلى أنها عالجت بيانات المستخدمين الشخصية لتدريب "تشات جي بي تي" دون أساس قانوني ملائم ولم توفر شفافية كافية حول جمع البيانات.

كما أنها لم تُفعّل نظامًا فعّالًا للتحقق من أعمار المستخدمين لمنع الوصول إلى المحتوى غير المناسب. وطالبت الهيئة الشركة بإطلاق حملة إعلامية لتوعية الجمهور حول كيفية عمل النموذج واستخدامه للبيانات.

على الصعيد القضائي في الولايات المتحدة، تعرضت OpenAI لأوامر قضائية أجبرتها على الاحتفاظ بسجلات محادثات المستخدمين كجزء من دعوى حقوق نشر.

انتقدت منظمة EFF هذه الأوامر بوصفها تجاوزًا خطيرًا يهدد حق المستخدمين في حذف بياناتهم.

وأشارت إلى أن ملايين الأشخاص يستخدمون "تشات جي بي تي" لأغراض شخصية كالتخطيط للسفر أو الحصول على معلومات طبية ومالية، وأن الحفاظ على هذه السجلات يتيح إمكانية الوصول إليها من قبل أطراف أخرى.

ورغم أن المحكمة رفعت هذا الأمر في سبتمبر/أيلول 2025، فإن الخلاف كشف هشاشة الضوابط القانونية على بيانات الذكاء الاصطناعي.

نصائح للاستخدام الذكي والآمن

1. لا تشارك أي معلومات شخصية أو مالية أو طبية

توصي شركة الأمن السيبراني ESET بأن يتجنب المستخدمون مشاركة أي معلومات شخصية أو مالية أو تجارية حساسة في الدردشة، وأن يتعاملوا مع ما يكتبونه كما لو أنه قد يصبح مرئيًا للجمهور.

فقد أظهر حادث خلل تقني في مارس/آذار 2023 أن خطأ برمجيًا في مكتبة Redis كشف عناوين بعض المحادثات وغيرها من البيانات، ما يوضح أنه حتى المنصات الكبرى قد تواجه ثغرات أمنية.

كما كشف خبراء الخصوصية في منظمة PIRG US أن المستخدمين يجب ألا يفترضوا خصوصية تامة للمحادثات لأن بعض السجلات تُحتفظ بها بقرار قضائي، ونصحوا بعدم إدخال معلومات لن يكونوا مرتاحين في قراءتها أمام الآخرين.

2. استخدم ميزات التحكم في البيانات والذاكرة المؤقتة

تتيح OpenAI للمستخدمين خيار تشغيل محادثات مؤقتة تحذف تلقائيًا بعد ثلاثين يومًا، وإدارة ما إذا كان النموذج يحتفظ بذاكرة عن المحادثات الطويلة. يمكن الدخول إلى الإعدادات لتعطيل استخدام المحادثات في التدريب أو حذف بيانات سابقة.

كما توفر الشركة أوضاعًا متقدمة في النسخ الموجهة للأعمال تتيح للمؤسسات تحديد مدة الاحتفاظ بالبيانات أو منع استخدامها نهائيًا في تدريب النماذج.

3. قلل مشاركة الملفات واحذف البيانات المضمنة

تنصح "FPF" بتجنب رفع الملفات والصور الكاملة إلى نماذج الذكاء الاصطناعي، لأنها قد تتضمن بيانات مخفية مثل الموقع الجغرافي أو هوية الأشخاص.5.

في حالة الحاجة إلى الاستعانة بالتوليد النصي لتحليل مستندات، يُفضّل حذف أو تعمية الأجزاء الحساسة قبل الرفع.

ويجب أيضًا التأكد من حذف البيانات التعريفية (Metadata) من الصور باستخدام برامج خاصة قبل مشاركتها.

4. إدارة إعدادات الذاكرة

تتميز بعض نماذج الذكاء الاصطناعي بقدرتها على تذكر السياق بين الجلسات، لكنها بذلك تجمع معلومات عن عادات المستخدم واهتماماته على المدى الطويل.

لذلك ينبغي مراجعة إعدادات "الذاكرة" أو "التخصيص" في التطبيق وتعطيلها إذا لم تكن هناك حاجة

حقيقية، أو مراجعة المعلومات المخزنة وحذف ما لا يراد الاحتفاظ به.

5. استخدام النسخ المخصصة للشركات

في بيئات العمل، يُفضّل استخدام نسخة "Enterprise ChatGPT" أو واجهة برمجية (API) بعقد عدم الاحتفاظ بالبيانات؛ فهذه الخدمات تمنع استخدام محتوى المحادثات في تدريب النماذج، وتمكّن المؤسسات من تحديد مكان تخزين البيانات ومدة الاحتفاظ بها.

ينصح خبراء أمن المعلومات بأن تسبق استخدام الذكاء الاصطناعي تقييمات داخلية للبيانات والحقوق؛ فدراسات ميتوميك تظهر أن تسرب البيانات الحساسة غالبًا ما يحدث بسبب امتيازات مبالغ فيها للتطبيقات المرتبطة بالذكاء الاصطناعي، وليس من النموذج نفسه.

6. احذر من الروابط والملحقات غير الموثوقة

أكدت OpenAI خلال مقال صدر في يناير/كانون الثاني 2026 أن استخدام النماذج للتصفح يمكن أن يستغل في تنفيذ هجمات "حقن التعليمات" عبر تضمين أوامر خبيثة في صفحات الإنترنت، لجر النموذج إلى فتح روابط تحتوي على معلومات سرية أو تنفيذ أوامر غير مرغوبة.

لذلك يجب توخي الحذر عند مشاركة روابط مع النموذج أو عند متابعة الروابط التي يقدمها، وعدم فتح روابط غير مألوفة من داخل الدردشة.

كما يجب تعطيل أو إزالة الملحقات غير الرسمية التي تعد بتحسين أداء ChatGPT لأنها قد تطلب صلاحيات واسعة وتعرض بيانات المستخدم لخطر التسرب.

7. تأمين الحسابات وتحديث كلمات المرور

الاعتماد على كلمات مرور قوية وتفعيل التحقق المتعدد العوامل (MFA) أمر أساسي لمنع الوصول غير المصرح به إلى حساب ChatGPT.

ففي حادثة سابقة، تم العثور على أكثر من 100 ألف بيانات اعتماد مسروقة لحسابات ChatGPT على الويب المظلم بسبب إصابة أجهزة المستخدمين ببرمجيات خبيثة.

تنصح OpenAI مستخدميها بالتحقق من مصادر رسائل البريد الإلكتروني وعدم الرد على أي رسائل مشبوهة قد تطلب بيانات شخصية.

الحاجة لإطار تنظيمي واضح

تشير الدراسات القانونية إلى أن سياسات الخصوصية الحالية لدى شركات الذكاء الاصطناعي مكتوبة بلغة قانونية معقدة، ولا تقدم للمستخدمين فهمًا واضحًا لحقوقهم، كما أنها تختلف من دولة لأخرى بسبب غياب إطار عالمي شامل.

يتوقع أن يفرض قانون الاتحاد الأوروبي للذكاء الاصطناعي (Act AI EU) عند دخوله حيز التنفيذ متطلبات صارمة على الشفافية والامتثال، بما في ذلك فرض قيود على استخدام البيانات الشخصية في تدريب النماذج وغرامات قد تصل إلى 35 مليون يورو أو 7% من الإيرادات للشركات المخالفة.

في الولايات المتحدة، تتنوع القوانين من ولاية لأخرى، بينما تسعى الدول الآسيوية والأفريقية إلى وضع أطرها الخاصة.

في ظل هذه البيئة القانونية المتغيرة، بات على المستخدمين والأفراد فهم مسؤولياتهم تجاه بياناتهم.

كما يتعين على الشركات المطورة للذكاء الاصطناعي تبني أقصى درجات الشفافية، وتوفير أدوات سهلة

لمحو البيانات والتحكم في استخدام المعلومات، والعمل على حماية خصوصية الأطفال والمجموعات الضعيفة.

الأحداث الأخيرة، مثل الغرامة الإيطالية على OpenAI، والحملة الإعلامية المفروضة عليها، والضغط المتزايد من مؤسسات حقوقية، تؤكد أن مسألة الخصوصية ليست تفصيلًا تقنيًا بل قضية حقوقية وسياسية.

في المحصلة، يمثل "تشات جي بي تي" فرصة مهمة لتسهيل الوصول إلى المعرفة وتحسين الإنتاجية، لكنه في الوقت ذاته يجلب معه مخاطر تتعلق بالخصوصية والأمان.

توضح القضايا التنظيمية والأمنية الحديثة أن المحادثات مع النماذج ليست سرية بالكامل، وأن المدخلات قد تُستخدم لتدريب النماذج، وأن تسريبات البيانات قد تحدث عبر طرف ثالث أو بسبب سوء استخدام.

لذلك، فإن استخدام النموذج بذكاء يتطلب وعيًا بالمخاطر، وتبني ممارسات حماية مثل تجنب مشاركة المعلومات الحساسة، واستخدام ميزات التحكم في البيانات، وإدارة الذاكرة، وتفعيل الأمان متعدد العوامل، والاعتماد على النسخ المؤسسية عند معالجة معلومات سرية.

رابط المقال: https://www.noonpost.com/356711/