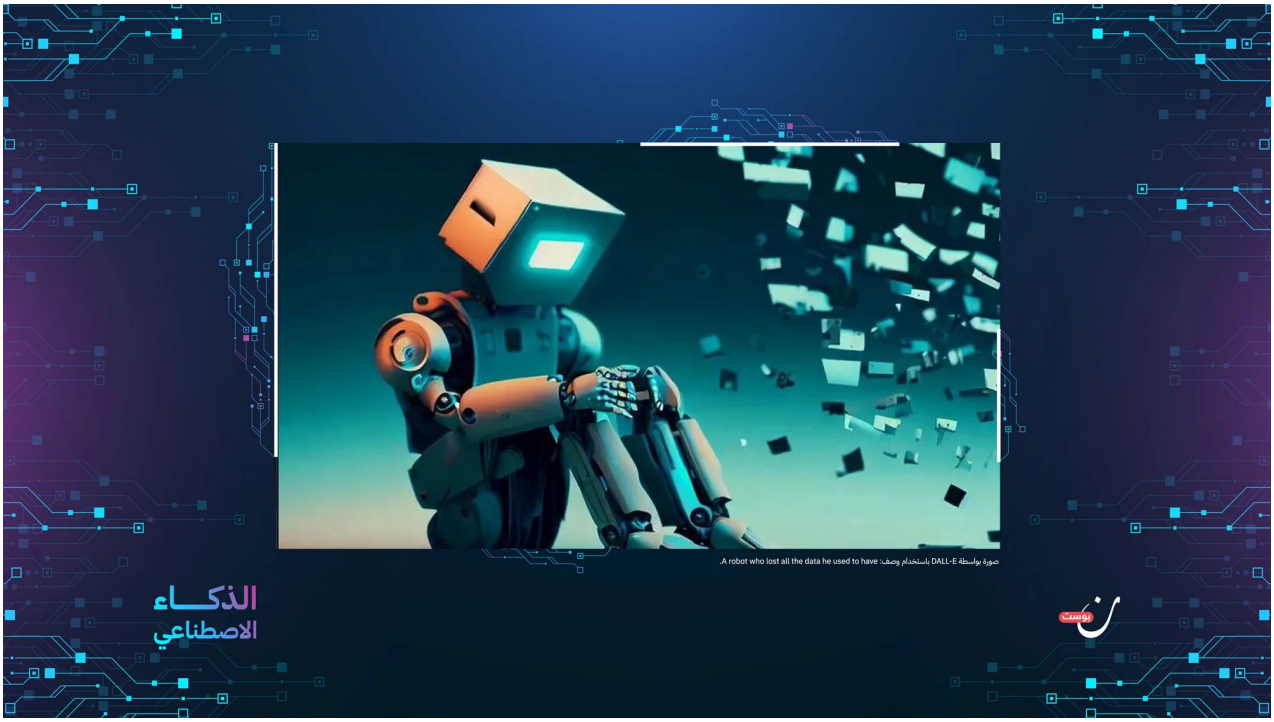
حق النسيان: هل يمكننا التخلص من ماضينا الرقمي؟



”البيانات شيء ثمين، وستستمر لفترة أطول من الأنظمة نفسها“ – تيم بيرنرز لي، مخترع الشبكة العنكبوتية.

في عام 2020، وصل حجم البيانات على شبكة الإنترنت إلى 64 زيتابايت (الزيتابايت تعادل تريليون (ألف مليار) غيغابايت)، حجم مهول من البيانات نشاركه كل لحظة، وصل في بعض الأحيان إلى 340 مليون تغريدة على منصة X (تويتر سابقًا)، و95 مليون صورة على منصة إنستغرام، وغيرها من ملايين البيانات هنا وهناك على بقية المنصات وفي بقية بقاع الإنترنت.

غير هذا وذاك، يكفينا فقط تصفح الإنترنت لنشارك آلاف البيانات مع المواقع التي نزورها والمتصفح الذي نعبر إلى الإنترنت من خلاله، لكن من يمتلك هذه البيانات؟ من يملك حق الوصول إليها وفيما يستخدمها؟ أصبحت مثل هذه الأسئلة تدور في رؤوس الكثيرين وزاد وعيهم فيما يخص البيانات ومشاركتها، خاصة بعد العديد من فضائح تسريب أو استخدام البيانات الخاطئ، كفضيحة كامبريدج أناليتيكا عام 2016.

عيّنة من الشركات التي تشاركها "باي بال" بيانات مستخدميها – المصدر: صحيفة at Knowledge Wharton

ليس هذا هو محور موضوعنا اليوم، إنما ما نحتاج معرفته حقًا هو ما الذي يجب أن يحدث إذا أصبحت البيانات التي شاركناها برغبتنا -أو من دونها- قديمة أو خاطئة، أو أصبحنا ببساطة لا نودّ مشاركتها مع العالم بعد الآن؟ أو لنسأل السؤال بصورة أبسط: هل بإمكاننا حذف بياناتنا من على الإنترنت وقتما نريد؟

حقّ النسيان (Forgotten be to Right)

لكل منا إرثه الرقمي، ولسوء الحظ بينما نتغير وتتغير أفكارنا والعالم، تبقى بياناتنا التي شاركناها في الماضي كما هي لا تتغير.

أطلق الاتحاد الأوروبي تشريعًا جديدًا يُدعى "Forgotten be to Right – الحق في أن تُنسى"، من أجل حماية البيانات، وهو مصطلح يعبّر عن حق الأفراد في طلب حذف أو إزالة معلوماتهم الشخصية من الإنترنت، ليصبح بإمكانهم التحكم في المعلومات التي تظهر عنهم، وذلك بغرض تقليل تأثير المعلومات القديمة أو غير الدقيقة على سمعة الأفراد وخصوصيتهم، إذا انتشرت أو استخدمها أحدهم بشكل خاطئ.

مع إطلاق هذا المصطلح، بدأت الكثير من الشركات في تقديم الحلول التي تمكّن الأفراد من حذف -بياناتهم الشخصية، إن كان كلها أو جزءًا منها، من على الإنترنت، وكانت من ضمن هذه الحلول أداة Off التي بياناتهم بحذف للمستخدمين لتسمح ،فيسبوك منصة أطلقتها التي Facebook Activity تستخدمها مواقع وتطبيقات الطرف الثالث، التي شاركها المستخدم في البداية مع المنصة.

لسوء الحظ، لم تلقَ هذه الأداة الكثير من الترحيب، خاصة بعدما خرج موقع Review Technology

التابع لمعهد ماساتشوستس للتكنولوجيا، مؤكدًا على أن الأداة –وأقتبس قولهم– "مضللة بعض الشيء، فلا يحذف فيسبوك أية بيانات من جهات الطرف الثالث، إنما هو فقط يفك ارتباطها ببياناته الخاصة بك".

كذلك انضمت جوجل إلى مقدمي خدمة حذف البيانات، من خلال أداة Activity My Google التي أعلنت عنها عام 2016، وهي أداة مخصصة لإدارة بياناتك التي تجمعها جوجل، ويمكنك حذف أحدها أو كلها إذا أردت.

وفي ديسمبر/ كانون الأول الماضي، أعطى الاتحاد الأوروبي الحق للمواطنين لحذف أية بيانات خاطئة تخصهم لاقت انتشارًا على محركات البحث مثل جوجل وبينغ وغيرهما، كما ظهر مقدمو خدمات آخرين مثل DeleteMe الذي يتعاون مع سماسرة ووسطاء البيانات، ليمكنك حذف بياناتك من عندهم مقابل مبلغ مالي تدفعه.

كل هذا رائع وجيد للغاية، لكن بالنسبة إلى منصات نستخدمها بأنفسنا، ونوفّر لها البيانات بمحض إرادتنا، فماذا عن نماذج الذكاء الاصطناعي؟

حقنة لفقدان الذاكرة

"المعلومات هي نفط القرن الـ 21، والتحليلات هي محرك الاحتراق". – بيتر سوندرغارد، بحوث غارتنر.

يختلف الأمر كليًا إذا تطرقنا للحديث عن نماذج الذكاء الاصطناعي وما تحتويه من بيانات، فالبيانات بالنسبة إلى هذه النماذج هي الوقود الذي تحتاجه لتعمل، ومن دونها لا تساوي شيئًا، فدورها باختصار هو تجميع وتحليل البيانات وتنظيمها لتصبح قادرة على توفير الإجابات والمساعدة، سواء على المستوى الشخصي من البيانات، أو على مستوى البيانات الصحية التي تستخدمها العديد من التطبيقات لمتابعة حالتك الصحية، وهي النوع الأهم من البيانات التي يتم مشاركتها باستمرار مع أنظمة ونماذج الذكاء الاصطناعي.

ببساطة، إذا تمّ اختراق أي من الأنظمة الجامعة للبيانات كالنماذج اللغوية الكبيرة (LLM) مثل ChatGPT، يريدونها التي بالكيفية ليستخدموها المخترقين أيدي تحت أجمع البشر بيانات ستصبح، وبعيدًا عن الاختراق، من منا يودّ أن يروي قصته لنموذج محادثة ليعطيه الحلول، فيجد أنه يستدل بقصته مع شخص آخر ليقنعه بحلّ لمشكلته أيضًا؟

دعني أطلب منك الآن أن تحاول نسيان أي معلومة أنت تعرفها مسبقًا، ستجد الأمر في غاية الصعوبة، وهذا هو تحديدًا ما تقرر فعله مع نماذج الذكاء الاصطناعي، حقنه بمرض فقدان الذاكرة

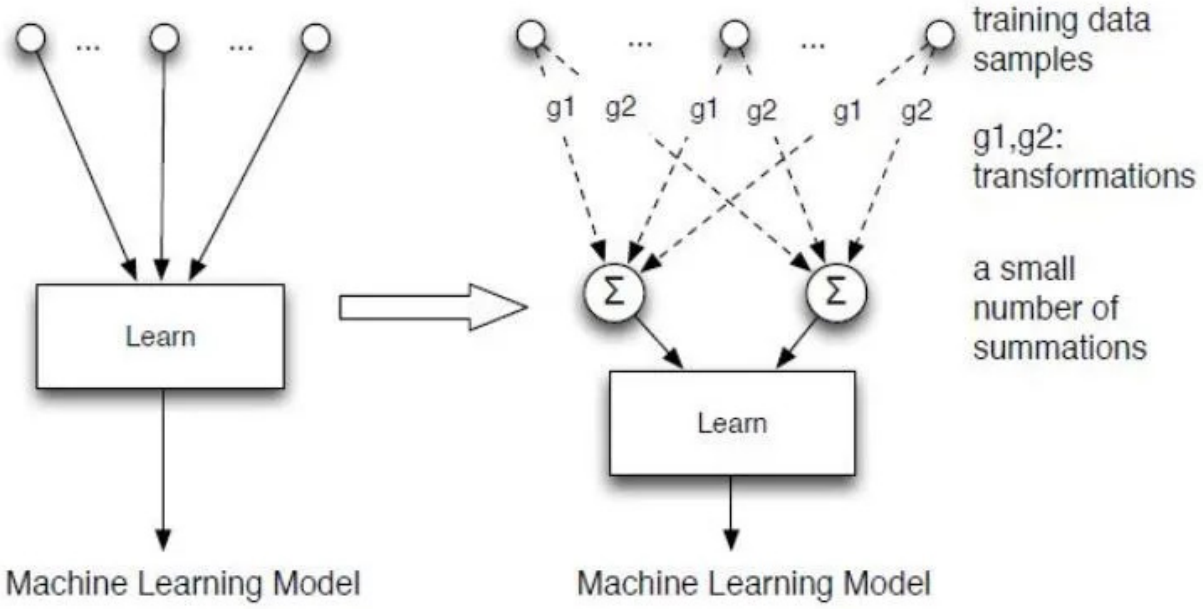
لكن لم يخرج الذكاء الاصطناعي من حسابات قانون "الحق في أن يُنسى"، بل أنه في عام 2021 حذّر مشرّعو قوانين البيانات في المملكة المتحدة مصنعي نماذج الذكاء الاصطناعي من أنه قد يأتي وقت يطلب منهم محو كافة البيانات التي يملكونها.

الأمر الصعب هنا هو في الكيفية التي تتعامل بها أنظمة ونماذج الذكاء الاصطناعي مع البيانات، فهي ببساطة أقرب إلى البشر منها إلى الآلات، بعد أن تغذي الذكاء الاصطناعي بمجموعة من البيانات، لن تملك وسيلة لمعرفة أين تكمن هذه المعلومة التي منحته إياها.

فرضًا، دعني أطلب منك الآن أن تحاول نسيان أي معلومة أنت تعرفها مسبقًا، ستجد الأمر في غاية الصعوبة إن لم يكن مستحيلًا دون إصاباتك بفقدان الذاكرة (Amnesia)، وهذا هو تحديدًا ما تقرر فعله مع نماذج الذكاء الاصطناعي، حقنه بمرض فقدان الذاكرة، من خلال ما يعرَف بالـ Machine Unlearning أو عدم تعلم الآلة.

عدم تعلم الآلة (Unlearning Machine)

ظهر مصطلح "عدم تعلم الآلة" لأول مرة عام 2015 على أيدي الباحثين ينزي كاو (Cao Yinzhi) وجونفينغ يانغ (Yang Junfeng) من جامعة تورنتو، وهو مصطلح يشير إلى عملية حذف وإزالة البيانات من أنظمة الذكاء الاصطناعي، دون التأثير على قدرتها على تنفيذ مهامها الأساسية، لكن قبل الاستفاضة في ماهية إلغاء تعلم الآلة، دعنا نوضّح ماهية تعلم الآلة باختصار وفيما يخص ما نتحدث عنه.



المبدأ الأساسي لإلغاء تعلم الآلة عن طريق تغيير طريقة تعلمها – المصدر: ينزي كاو وجونفينغ يانغ

تعلم الآلة، وتحديدًا التعلم العميق، هو عملية تحدث بشكل تدريجي، ما يعني أن المعلومات لا تعطى دفعة واحدة، إنما هي تمنح تباعًا وبالتدريج للنموذج، وذلك من خلال ما يعرف بالتحديثات.

كذلك إن ما يزيد الأمر صعوبة هو عندما نعطي نحن البيانات للنموذج لتلخيصها على سبيل المثال، نعم هو ينفذ المهمة على أكمل وجه، لكنه -وبغير قصد- يحفظ هذه البيانات ويصبح كما لو كان مدرّبًا عليها.

ما يعيب هذه العملية، حتى إن كان حفظ البيانات دون قصد ليس بعائق، هو عدم إمكانيتنا معرفة كيفية ترتيب أو تنظيم النموذج للبيانات المدخلة إليه، وهو ما يعني صعوبة تحديد جزء معيّن من البيانات والتحكم به، ولهذا ظهرت عدة طرق لتنفيذ عملية إلغاء تعلم الآلة.

كيف تتعلم الآلة أن تنسى؟

أول هذه الطرق هي الطريقة الأسهل نظريًا، وهي ببساطة عندما يطلب حذف مجموعة معينة من البيانات من نموذج ما ينشأ نموذج جديد تمامًا، وأثناء عملية التغذية بالمعلومات نتخطى تغذيته بالمعلومات غير المرغوبة.

لسوء الحظ، هذه الطريقة -رغم سهولة شرحها- إلا أنها مكلفة للغاية، فآخر التقارير تفيد أن عملية إنشاء نموذج اصطناعي تتخطى تكلفتها 4 ملايين دولار، لذا هي رغم بساطتها إلا أنها العملية الأقل كفاءة وفعالية والأسوأ من الناحية الاقتصادية.

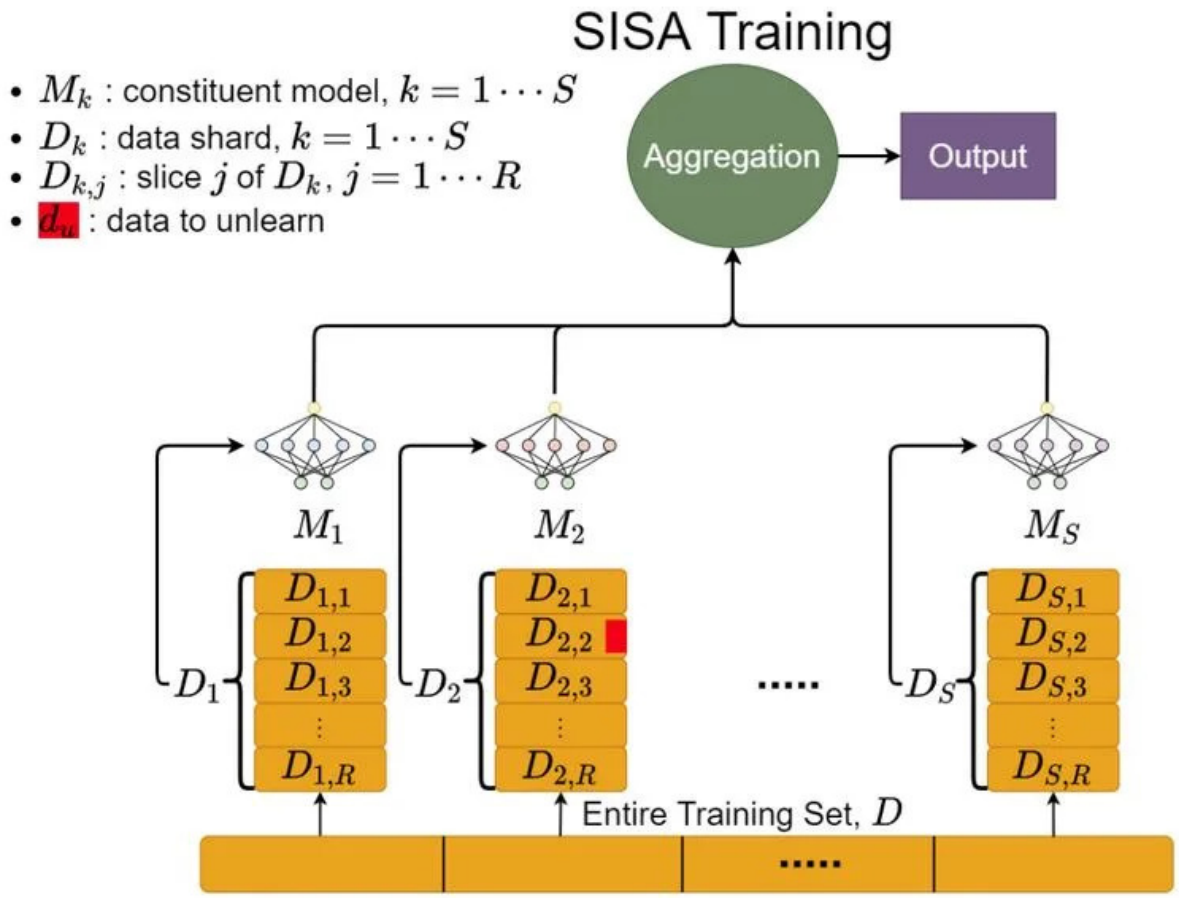
تخيل ببساطة أنه حتى إذا تمكنّا من أتمتة هذه العملية، فستتكلف الشركة المصنّعة للنموذج 4 ملايين دولارات مقابل كل طلب لحذف البيانات، هذا لا يقارب المنطق.

رئيس OpenAI التنفيذي سام آلتمان أثناء الإعلان عن دمج ChatGPT مع محرك البحث بينغ – المصدر: Redmond Jason | AFP | Images Getty

في الناحية الأخرى، ما يلي هذا الحل -من ناحية البساطة- هو حذف مجموعة البيانات غير المرغوبة من قاعدة بيانات النماذج الذكية، لكن لسوء الحظ لن تعلم أبدًا مدى تأثير المعلومة الواحدة على النموذج بشكل عام، وإذا قمت بحذف معلومة مفتاحية واحدة من القاعدة، سيفقد النموذج قدرته على العمل تمامًا.

هذا هو ما يصعّب عملية إلغاء تعلم الآلة، فهي تتكون من هدفين متعارضَين، أوّلا نسيان البيانات المطلوب نسيانها، وثانيًا الحفاظ على قدرة النموذج على تنفيذ المهام التي صُمّم من أجلها، لنصل إلى محطتنا الأخيرة.

في عام 2019، عرض الباحثون في جامعتي تورنتو وويسكونسن-ماديسون في كندا والولايات المتحدة، مقترحًا ثوريًا جديدًا لكيفية تنفيذ عملية إلغاء تعلم الآلة، عُرف هذا المقترح بـ"Training SISA" اختصارًا لـ"Training Aggregated Simultaneously and Independent Selectively"، لكن دعك من الاختصار ودعني أبسّط لك الأمر.



تعليم الآلة كيفية النسيان بواسطة SISA Training – المصدر io.Cleverhans

كما ذكرت سلفًا، ما يصعّب تنفيذ إلغاء تعلم الآلة هو عملية تحديد البيانات وأهميتها وأماكنها ومدى ترابطها ببعضها، وذلك بسبب الطريقة التقليدية لتدريب النماذج الذكية، من خلال مجموعة واحدة ضخمة للغاية من البيانات.

أما ما يقترحه تدريب SISA يعتمد على كيفية تعليم النموذج من البداية، وذلك من خلال تقسيم البيانات إلى مجموعات صغيرة مستقلة تمامًا تُدعى "نقاط البيانات (Points Data)"، وذلك بشكل متكرر، ليتعلم النموذج حينها كيفية التعامل مع كل نقطة بيانات بشكل منفصل.

بهذه الكيفية، عندما نريد حذف أية نقطة بيانات، سيمكننا ذلك ببساطة دون التأثير على النموذج ككل، ودون الحاجة إلى صنعه من البداية.

جوجل آخر المنضمّين إلى المبادرة

تعدّ شركة جوجل أحد أكبر المؤيدين -أو بالأحرى أكبر متجنّبي المشاكل- لقوانين الاتحاد الأوروبي، فبادرت بتنظيم أول تحدٍّ لإلغاء تعلم الآلة، الذي يقام في الوقت الذي تقرأ فيه المقال كجزء من مسار مسابقات NeurIPS 2023.

يهدف هذا التحدي إلى الوصول لطرق جديدة لحذف البيانات من أنظمة الذكاء الاصطناعي، وسيكون عبارة عن سيناريو واقعي يتم فيه تدريب أحد النماذج على صور للأوجُه، وبعد ذلك يطلب من المتسابقين أن يحذفوا مجموعة معيّنة من الأوجُه، وذلك بغرض حماية خصوصية المستخدمين وحقهم في النسيان.

في النهاية، كل ما سبق ما زال تحت الدراسة، إذ تحاول الشركات والباحثين بجدّ الوصول إلى طرق تمكّنهم من إلغاء تعلم الآلة، وهم يسابقون الزمن، فكل يوم يمرّ يتضاعف معه حجم البيانات المخزّنة في قواعد أنظمة الذكاء الاصطناعي، وهو ما يصعّب من إتمام العملية أكثر وأكثر.

لكن السؤال الأهم، والذي قد يصبح عقبة في وجه إفقاد الذكاء الاصطناعي ذاكرته، ما الذي يدعو شركة ما للموافقة على طلبي بحذف البيانات، بعدما قررت مشاركتها معهم من البداية؟

رابط المقال: https://www.noonpost.com/160976/