مجلة الدراسات والبحوث القانونية
Journal of Legal Studies and Researches
e-ISSN: 2676-1688 p-ISSN: 2437-1084
المجلد 11 العـدد 2/ جوان (2026)، ص 225– 245
Vol: 11 N° 2, June 2026, p. 225–245

الحق في النسيان الرقمي في ظل أنظمة الذكاء الاصطناعي التوليدي

The Right to Digital Forgetting in the Context of Generative AI Systems

راسم قصارة* [1]، محمد حسن الحمادي [2]
Racem Gassara *[1], Mohamed AL Hamadi [2]
[1] كلية الحقوق، جامعة الشرقية، سلطنة عمان، racem.gassara@asu.edu.om
[1] College of Law, A'Sharqiyah University, Sultanate of Oman, racem.gassara@asu.edu.om,
https://orcid.org/0009-0002-1307-1097
[2] كلية الحقوق، جامعة الشرقية، سلطنة عمان، mohamed.alhamadi@asu.edu.om
[2] College of Law, A'Sharqiyah University, Sultanate of Oman, mohamed.alhamadi@asu.edu.om
https://orcid.org/0009-0003-1026-929X

تاريخ الاستلام: 2026/03/29 | تاريخ القبول: 2026/05/24 | تاريخ النشر: 2026/06/20 *Published:* *Accepted:* *Received:*

ملخص:

تبحث هذه الدراسة في إشكالية الحق في النسيان الرقمي في ظل أنظمة الذكاء الاصطناعي التوليدي، متخذة من ChatGPT نموذجًا لتحليل حدود تفعيله في البيئة الرقمية المعاصرة. وتخلص الدراسة إلى أن الصعوبة لا ترتبط فقط بطبيعة هذه الأنظمة التقنية، بل تمتد إلى نقل البيانات عبر الحدود وتعذر المحو الفعلي لها بعد معالجتها. كما توضح الدراسة أن الإقرار النظري بهذا الحق لا يكفي لضمان حمايته عمليًا. وتدعو الدراسة إلى حلول تقنية ملائمة، وآليات تنظيمية أشد صرامة، وإطار قانوني عابر للحدود يواكب خصوصية الذكاء الاصطناعي التوليدي.

الكلمات المفتاحية: حماية البيانات الشخصية، الحق في النسيان الرقمي، الذكاء الاصطناعي التوليدي.

Abstract:

This study explores the right to be forgotten in the age of generative AI, using ChatGPT as an example. It finds that deleting personal data is difficult because AI systems process data across borders and cannot always guarantee complete erasure. The study concludes that stronger regulations, better technical solutions, and international legal rules are needed to effectively protect this right.

Keywords: Personal Data Protection, Right to Digital Forgetting, Generative Artificial Intelligence.

* المؤلف المرسل

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.
هذه المقالة مفتوحة المصدر بموجب شروط ترخيص المشاع الإبداعي المنسوب للمؤلف - غير التجاري، والذي يسمح بالاستخدام والتوزيع وإعادة الإنتاج بأي وسيلة، شريطة الاستشهاد بالعمل الأصلي بشكل صحيح وعدم استخدامه لأغراض تجارية.

1. مقدمة:

أحدثت أنظمة الذكاء الاصطناعي التوليدي تحولًا عميقًا في طريقة إنتاج المحتوى الرقمي ومعالجة البيانات، لما أصبحت تتسم به من قدرة على التعلم من كميات ضخمة من المعطيات، واستنباط أنماط جديدة، وتوليد نصوص أو صور أو إجابات تبدو للوهلة الأولى ناتجة عن إدراك بشري. غير أن هذه القدرات التقنية، على أهميتها، تثير إشكالات قانونية تتصل في جوهرها بحماية البيانات الشخصية وصون الحقوق الأساسية للأفراد، وفي مقدمتها الحق في النسيان الرقمي.

ويكتسب هذا الحق أهمية خاصة في سياق الأنظمة التوليدية، لأن طبيعة عملها تجعل محو البيانات أمرًا شديد التعقيد ومثيرًا للجدل من الناحيتين القانونية والتقنية.

وتزداد هذه الإشكالية وضوحًا عند تحليل حالة ChatGPT بوصفه نموذجًا لأنظمة الذكاء الاصطناعي، إذ تشير الوقائع العملية إلى أن هذه النماذج قد تعالج بيانات شخصية سواء في مرحلة التدريب أو أثناء التفاعل مع المستخدمين، كما قد تعيد إنتاج معلومات شخصية أو استنتاجها من المعطيات المتاحة لها. وقد كشف تدخل هيئة حماية البيانات الشخصية الإيطالية سنة 2023، وتعليق خدمات ChatGPT مؤقتًا في إيطاليا، عن حجم التوتر القائم بين الابتكار التقني ومتطلبات الامتثال لقواعد اللائحة الأوروبية العامة لحماية البيانات، لا سيما عندما تطرح مسألة مشروعية المعالجة، وإمكانية ممارسة الحقوق المقررة للأشخاص المعنيين.

وقد أدى هذا الإنذار الذي أطلقته الهيئة الإيطالية إلى فتح تحقيق من قبل فريق عمل معني بـ ChatGPT، ونُشرت نتائجه من قبل اللجنة الأوروبية لحماية البيانات في 23 مايو 2024.[1] وكان هدف هذا الفريق تعزيز التنسيق بين مختلف هيئات الرقابة الوطنية في أوروبا، والتي نظرت في الشكاوى المقدمة بسبب انتهاك حق حماية البيانات الشخصية من قبل نظام ChatGPT للذكاء الاصطناعي، والذي أحدث طرحه في السوق في نوفمبر 2022 تغييرًا جذريًا في مداولات التنظيم الأوروبي بشأن الذكاء الاصطناعي.

وكان من نتائج هذه المداولات تبني تعريف أنظمة الذكاء الاصطناعي،[2] وإدخال مفهوم «نظام الذكاء الاصطناعي للأغراض العامة»، والذي يندرج تحته ChatGPT. وتكمن أهمية هذا التمييز المستحدث في أنه إذا كانت أنظمة الذكاء الاصطناعي «التقليدية» قادرة على التنبؤ، فإن

أنظمة الذكاء الاصطناعي للأغراض العامة قادرة على إنتاج محتويات جديدة. وقد كان لهذا التنظيم الأوروبي بشأن الذكاء الاصطناعي أثر بالغ الأهمية، حيث سلط الضوء على قدرات هذه الأنظمة وعلى المخاطر المرتبطة بها، ولا سيما فيما يتعلق بالحياة الخاصة. فمن الناحية العملية، يمكن أن يضطر ChatGPT إلى معالجة بيانات شخصية خلال مرحلة التدريب، التي تستخدم بيانات عامة، والتي يكون مصدرها المواقع المؤسسية الرسمية، أو موسوعة ويكيبيديا، أو الأعمال الأدبية، أو قواعد البيانات الكبيرة (مثل منصة Reddit على سبيل المثال)، وكذلك بناءً على طلب المستخدمين في إطار الاستفسارات («المطالبات») التي يوجهها هؤلاء إلى برنامج المحادثة الآلي. كما يمكن الحصول على البيانات عن طريق وسطاء البيانات، أو البيانات المخزنة مسبقًا في قواعد بيانات مقدمي خدمات الذكاء الاصطناعي التوليدي. وبالتالي، تُعالَج البيانات الشخصية في مرحلة تدريب نظام الذكاء الاصطناعي لأغراض عامة ونشره، مما يستلزم التفكير في حقوق الأشخاص المعنيين بهذه البيانات، ولا سيما الحق في محوها.

ونشر الصحفي شوبام أغاروال (Shubam Agarwal) المتخصص في مجال التكنولوجيا، في نوفمبر 2023، مقالًا في مجلة نيو ساينتست (New Scientist) ذكر فيه أن ChatGPT يتأثر في الردود التي يقدمها لمستخدمين آخرين بالتفاعلات السابقة التي أجريت معه. وإزاء هذا التصريح، حاول الصحفي الحصول على محو بياناته الشخصية، لكنه واجه استحالة حذفها.[3]

أهمية الموضوع:

تنبع أهمية الموضوع من كونه يضع في مواجهة مباشرة قيمتين محوريتين في القانون الرقمي المعاصر، فنجد من جهة أولى الابتكار التكنولوجي، وحماية الحياة الخاصة والبيانات الشخصية من جهة أخرى. فالمسألة لم تعد تتعلق بمجرد حق فردي في النسيان الرقمي، بل أصبحت تمس مدى قدرة الأدوات القانونية القائمة على حماية البيانات واستيعاب خصائص الذكاء الاصطناعي التوليدي. كما يكتسي النقاش بعدًا دوليًا متزايدًا بسبب انتقال البيانات عبر الحدود، وما يترتب عليه من تعقيد في تحديد القانون الواجب التطبيق والسلطة المختصة والوسيلة الفعالة للإنفاذ.

منهجية الدراسة:

تعتمد هذه الدراسة المنهج الوصفي التحليلي النقدي، مع الاستفادة من المقاربة القانونية التطبيقية، من خلال تحليل النصوص المرتبطة بحماية البيانات، والقواعد التي تتعلق بنقلها ومعالجتها، فضلًا عن دراسة الممارسات الواقعية، بما يسمح باختبار مدى قابلية الحق في النسيان الرقمي للإعمال داخل البيئة التكنولوجية التي تفرضها أنظمة الذكاء الاصطناعي التوليدية. كما تستند الدراسة إلى حالة ChatGPT نموذجًا لقياس الفجوة بين الاعتراف القانوني بالحق وبين صعوبات التنفيذ العملي.

إشكالية الدراسة:

في ظل التطور المتسارع لأنظمة الذكاء الاصطناعي التوليدي، التي باتت تعتمد على نماذج لغوية ضخمة قادرة على معالجة كميات هائلة من البيانات وإعادة إنتاجها بطرق غير متوقعة، برزت تحديات قانونية وتقنية تتعلق بحماية الحقوق الأساسية للأفراد، وفي مقدمتها الحق في النسيان الرقمي. فبينما يُعد هذا الحق أحد الضمانات المركزية في منظومات حماية البيانات، إذ يمنح الشخص المعني إمكانية طلب محو بياناته متى انتفت حاجة المعالجة إليها، فإن طبيعة عمل الأنظمة التوليدية — القائمة على التدريب العميق، واستخلاص الأنماط من مجموعات بيانات شاسعة — تجعل تنفيذ هذا الحق عمليًا أقرب إلى الاستحالة. ولا يقتصر التعقيد على البنية التقنية فحسب، بل يمتد إلى إشكالية نقل البيانات عبر الحدود وتضارب الأطر القانونية الوطنية، مما يثير تساؤلات حول مدى إمكانية إعمال الحق في النسيان الرقمي في مواجهة أنظمة الذكاء الاصطناعي التوليدي، في ضوء القيود التقنية المرتبطة بطبيعة عمل هذه الأنظمة، وتحديات نقل البيانات عبر الحدود؟

ويتفرع عن هذا السؤال عدد من التساؤلات، من أهمها:

- هل تكفي الآليات التي تعلنها الشركات المطورة، مثل OpenAI، لضمان محو البيانات؟
- هل يظل الحق في النسيان قابلاً للتحقق عمليًا عندما تُنقل البيانات إلى ولايات قضائية أخرى؟
- هل يفقد هذا الحق فعاليته كلما انتقل من الإطار النظري إلى التطبيق العابر للحدود؟

خطة الدراسة:

تتوزع الدراسة على محورين رئيسين، يتناول الأول القيود التقنية على إعمال الحق في النسيان الرقمي في أنظمة الذكاء الاصطناعي، من خلال بيان حدوده التقنية وعدم واقعية إعماله على نحو

كامل في سياسة الخصوصية الخاصة بـ OpenAI. بينما يعالج المحور الثاني أثر القيود الإقليمية على فعالية الحق في النسيان الرقمي، وأثر نقل البيانات خارج الحدود وغياب حق عالمي في النسيان يضمن فعاليته عبر مختلف النظم القانونية. وبذلك تسعى الدراسة إلى بيان أن الإقرار النظري بالحق في النسيان الرقمي لا يكفي لوحده، ما لم يقترن بآليات تقنية وقانونية أكثر ملاءمة لطبيعة الذكاء الاصطناعي التوليدي. ولاينطلق البحث حول الحق في النسيان الرقمي من مجرد فكرة «المحو»، بليتصل بتحول جوهري في مفهوم الخصوصية المعلوماتية ذاته. فإذا كانت الفلسفة التقليدية لحماية البيانات ترتكز على مبدأ «جمع البيانات لغرض محدد والاحتفاظ بها لمدة محدودة»، فإن الخصوصية في عصر الذكاء الاصطناعي التوليدي لم تعد تقتصر على التحكم في جمع البيانات أو تصحيحها، بل امتدت إلى القدرة على منع «استمرار أثرها» داخل الأنظمة التي تعلمت منها. وتشكل هذه المفارقة جوهر الإشكالية: فبقدر ما يكون الحق في النسيان تعبيرًا عن سلطة الفرد على مصير بياناته، بقدر ما يصبح تطبيقه في الأنظمة التوليدية اختبارًا حقيقيًا لمدى قدرة القانون على مجاراة التقنية، لا من حيث فرض الالتزام، بل من حيث إمكان التنفيذ المادي.

2. القيود التقنية على إعمال الحق في النسيان الرقمي في أنظمة الذكاء الاصطناعي

يواجه تطبيق الحق في النسيان الرقمي على أنظمة الذكاء الاصطناعي التوليدي، مثل ChatGPT، تضييقًا لنطاق تطبيقه نتيجة حدوده التقنية، وعدم واقعية الحق في النسيان الرقمي الوارد في سياسة الخصوصية لشركة OpenAI.

1.2. الحدود التقنية للحق في النسيان الرقمي

يتيح الحق في النسيان الرقمي المعترف به بموجب المادة 17 من اللائحة العامة الأوروبية لحماية البيانات،[4] من الناحية العملية، للفرد الذي يعلم أن بياناته الشخصية تخضع للمعالجة أن يطلب محوها. بيد أن هذا الحق، كما تشير الفقرة 1 من هذه المادة، ليس حقًا مطلقًا، بل يخضع لشروط.[5] إذ يجب أن يراعي تنفيذه أي حقوق أو مصالح معارضة أو متساوية معه في القيمة ضمن التسلسل الهرمي للقواعد، ومنها على سبيل المثال الحق في حرية التعبير أو المصلحة العامة.[6]

وتكتسي هذه الموازنة أهمية خاصة في سياق أنظمة الذكاء الاصطناعي التوليدي، لأن المعلومات التي قد تطلب إزالتها قد تكون جزءًا من محتوى تم توليده بناءً على أنماط إحصائية، وليس

بالضرورة معلومات منقولة بنصها. وهو ما يطرح التساؤل حول إعادة إنتاج النموذج لمعلومة شخصية عن فرد ما بمثابة «نشر» بالمعنى الذي يستدعي تطبيق استثناء حرية التعبير؟ أم أن طبيعة المعالجة الآلية تحول دون التمسك بهذا الاستثناء لأن الإعادة لا تعبر عن رأي أو قيمة إعلامية؟ وتذهب الفقيهة Lavinia Jacquet إلى أن محاكم الاتحاد الأوروبي قد تميل إلى تضييق استثناء حرية التعبير في هذه الحالات، متى ثبت أن النموذج يكرر المعلومة الشخصية دون إضافة تعليق أو سياق إعلامي، مما يجعلها مجرد «إعادة إنتاج فنية» لا تحميها المادة 17(3)(أ) من اللائحة العامة. كما تجعل الفقرة 2 من المادة 17 من مجموعة القيود التكنولوجية وتكاليف تنفيذ الحق في المحو عائقًا محتملاً أمام إعمال هذا الحق.[7] ويحدث ذلك بشكل خاص عندما تكون مسؤولية المعالجة مشتركة بين عدة مسؤولين، مما يجعل محو البيانات معقدًا.[8] وفي هذا الإطار، تنص اللائحة العامة لحماية البيانات على أنه «بالنظر إلى التكنولوجيا المتاحة وتكاليف التنفيذ، [يتخذ المسؤول عن المعالجة] التدابير المعقولة، بما في ذلك التدابير التقنية»[9] لإبلاغ المسؤولين الآخرين عن المعالجة بأن الشخص المعني قد طلب محو بياناته الشخصية، وأنه يتعين عليهم الامتثال لذلك.[10]

غير أن الأمر بمراعاة «التدابير المعقولة»، «بما في ذلك التدابير التقنية»، لمحو البيانات الشخصية للمستخدم، لا يستهدف تحديدًا فرضية برنامج محادثة آلي لا يمكنه نسيان البيانات الشخصية لمستخدميه، مثل ChatGPT. ويعود السبب في ذلك إلى حداثة ظهور أنظمة الذكاء الاصطناعي التوليدي قياسًا بتاريخ اعتماد اللائحة الذي يعود إلى سنة 2016.[11]

إلا أنه إزاء تصميم أدوات جديدة، مثل أنظمة الذكاء الاصطناعي للأغراض العامة، تترك اللائحة العامة لحماية البيانات الفقيه القانوني في حيرة. ذلك أن الحيثية 78 تنص على أنه يقع على عاتق منتجي ومقدمي السلع أو الخدمات ضمان تمكين المسؤولين عن المعالجة من الامتثال لحق حماية البيانات الشخصية.[12] ويُستخلص من ذلك أن ضمان محو البيانات الشخصية يقوم بالأساس على حلول تقنية وحسن نية مصممي و/أو مقدمي هذه الأدوات في تطبيقها، وليس على إطار ملزم يفرض بغض النظر عن الإعدادات التقنية.[13]

وتجدر الإشارة إلى أن مسألة فعالية الحق في النسيان الرقمي ليست جديدة. فالقيود التكنولوجية الناشئة عن الخوارزميات، «المصممة بحيث يمكنها اكتشاف العمليات التي يجب اتباعها

ذاتيًا والتطور بمرور الوقت انطلاقًا من تجربتها»،[14] والتي ظهرت منذ الثمانينيات من القرن العشرين، كانت تحول دون تفعيل هذا الحق. ومن ثم، فإن ظهور أنظمة الذكاء الاصطناعي للأغراض العامة وتعميم استخدامها يسمحان بإبراز صعوبات لم تكن قد استقطبت اهتمام الفقه القانوني حتى الآن.[15]

ولا يقتضي التنفيذ الفعال للحق في النسيان، من الناحية العملية، من قبل الشخص المعني محو البيانات التي تم جمعها فحسب، بل أيضًا محو البيانات المجاورة لها والمرتبطة بها، والتي قد تمكن من استنتاج معلومات من البيانات المحذوفة.[16] وينبغي، بالتالي، على المسؤول عن المعالجة محو أي بيانات تعتمد على المعلومات المحذوفة. غير أن هذه الإجراءات تتجاوز بكثير ما تقتضيه اللائحة العامة لحماية البيانات، أي حذف البيانات التي يرغب المستخدم في محوها فقط.[17]

وتفاقم تعقيدات أنظمة الذكاء الاصطناعي للأغراض العامة هذا التعدي على الحق في النسيان الرقمي، على الرغم من الاعتراف به في سياسة الخصوصية للشركة الأمريكية المطورة لـ ChatGPT.

2.2. عدم واقعية الحق في النسيان الرقمي الوارد في سياسة الخصوصية لشركة OpenAI

تعود تعقيدات برامج المحادثة الآلية وأنظمة الذكاء الاصطناعي للأغراض العامة إلى إدخال نوع جديد من الخوارزميات، في عام 2017، يسمى "المحول" (transformer)، القائم على «الشبكات العصبية»، والذي يتيح معالجة كمية ضخمة من البيانات ويحسن من قوة المعالجات وسعة ذاكرة النظم المعلوماتية بصورة غير مسبوقة.[18] ويقدم ملف اللجنة الوطنية الفرنسية للمعلوماتية والحريات (CNIL) المخصص لـ ChatGPT طريقة عمله خطوة بخطوة.[19] إذ تستخدم هذه الواجهة الرقمية مدخلات المستخدم أو «المطالبات» لتغذية خوارزميتها وتقديم نتائج مفهومة للبشر.[20] فيجب أولاً «ترميز» هذا النص، أي ترجمته إلى لغة مفهومة للآلة، وتُمثَّل القيم الرقمية لكل كلمة، ويُستنتج «معناها» وفقًا للسياق، أي بمقارنتها مع تمثيلات الكلمات الأخرى. وبمجرد الانتهاء من مرحلة الترميز، تسمح مرحلة فك الترميز بإنتاج نص عن طريق توليد الكلمات وفقًا لاحتمالية حدوثها. ولكي تكون ردود هذا الأخير أكثر ملاءمة لتوقعات المستخدمين، يجب «محاذاة» الخوارزمية، أي تحسينها بواسطة تقنيتي ضبط: تعلم خاضع للإشراف يستخدم «إجابات نموذجية» يتم صياغتها بواسطة بشر، وتعلم معزز يستخدم نموذجًا يتعرف على الإجابات الصحيحة. وتنطوي هذه المرحلة، التي تسمى أيضًا الضبط الدقيق (fine-tuning)، في غالبية الحالات على معالجة بيانات شخصية.

وبدون تفصيل، تحاول سياسة الخصوصية لشركة OpenAI بث الثقة لدى المستخدمين الذين تُعالَج بياناتهم الشخصية. إذ تشير الشركة إلى أنها تتيح للأشخاص المعنيين طلب محو البيانات الشخصية من سجلات الشركة،[21] وسحب موافقتهم، والحق في الاعتراض على معالجة بياناتهم. وتوضح الوثيقة أن الشركة تلتزم بتقييد الطريقة التي تعالج بها البيانات الشخصية. وتضيف الشركة أنه يمكن تصحيح أو محو الأخطاء المتعلقة بالبيانات الشخصية للمستخدم والتي يولدها النظام، بناءً على طلب المستخدم.[22] غير أن هذا الأمر لا يبدو قابلاً للتحقيق من وجهة نظر واقعية وتقنية. فبعد التدريب والضبط الدقيق، يستحيل إزالة البيانات الأولية (سواء كانت شخصية أم لا) من مجموعة معلمات أنظمة الذكاء الاصطناعي للأغراض العامة.[23] ولكي يكون المحو فعالاً، سيكون من الضروري محو جميع البيانات المنتجة، وإزالة البيانات الشخصية من مجموعات البيانات التي استخدمت في تدريبه، لتكوين مجموعة أخرى وتدريبه بدون هذه البيانات.

وتكتسي هذه العوائق التي تحول دون الحق في المحو أهمية خاصة، لأنه بعد مرحلة الضبط، لا تكون الحماية التقنية للبيانات الشخصية التي وضعها مطورو نماذج اللغة لتجنب أي إفشاء للبيانات فعالة. وبالتالي، يمكن للنموذج تخزين بيانات التدريب[24] و«اجترارها» عن غير قصد، والإفصاح عنها لمستخدم آخر[25]. ويجب التمييز بين هذه الظاهرة وشكل آخر من أشكال الخلل الذي يصيب أنظمة الذكاء الاصطناعي للأغراض العامة ويسمى «الهلاوس» (hallucinations)، والذي يكون نتيجة لمجموعات بيانات غير مكتملة وتنطوي على انحيازات مرتبطة باللغة أو بموقع البيانات، أو طريقة عمل النظام. بيد أن محو هذه البيانات أمر مستحيل، وهي حقيقة جديرة بالبحث خاصة بالنظر إلى المساس الذي قد تسببه بسمعة الأشخاص المعنيين.

وإذا كانت ظاهرة «الاجترار» تكشف عن بيانات سبق أن درب عليها النموذج، فإنها تطرح مسألة المسؤولية المدنية للمطور عن الضرر الناشئ عن إعادة إنتاج بيانات شخصية لم يعد يحوز سندًا قانونيًا للاحتفاظ بها. ففي القانون الخاص، تستند المسؤولية التقصيرية إلى خطأ وضرر وعلاقة سببية. ويمكن القول إن خطأ المطور يتحقق بمجرد تصميم نموذج يعلم – أو كان ينبغي له أن يعلم – بقابليته على «اجترار» البيانات الشخصية، دون أن يزوده بآليات فعالة لمنع ذلك أو إزالته. أما الضرر، فيتمثل في المساس بالسمعة أو بالحق في الخصوصية أو حتى في التمييز الآلي. غير أن إثبات علاقة السببية

يظل الأصعب، إذ قد يكون من العسير على الشخص المعني إثبات أن المعلومة التي كشف عنها النموذج مستمدة تحديدًا من بياناته هو لا من مصادر أخرى متقاربة. ويعيد هذا الواقع طرح الحاجة إلى تبني نظام للمسؤولية الموضوعية (المطلقة) أو على الأقل افتراض خطأ المطور في حالة حدوث «اجترار» غير مبرر، أسوة بما عرفته بعض التشريعات في مجال الذكاء الاصطناعي عالي المخاطر.

ولتجنب استخدام البيانات الشخصية أو محوها، ثمة حلول تقنية متاحة.[26] ومن بين السبل الممكنة اللجوء إلى البيانات المركبة، أي بيانات تعيد إنتاج خصائص البيانات الأصلية (الشخصية عند الاقتضاء) ولكنها لا تحتوي عليها. وعلى الرغم من هذا الحل التقني، تظل أخطار حماية البيانات الشخصية قائمة. وهذه النتيجة ليست مطمئنة، لا سيما وأن نقل البيانات الشخصية إلى الولايات المتحدة يستلزم تطبيق الحق في النسيان الرقمي خارج إقليم الدولة، مما يرتب انعدام الأمان القانوني فيما يتعلق بممارسة هذا الحق.

3. القيود الإقليمية على فعالية الحق في النسيان الرقمي

شركة OpenAI هي شركة أمريكية، يقع مقرها الرئيسي في سان فرانسيسكو بالولايات المتحدة.[27] وقد يهدد هذا الطابع الإقليمي للحق في النسيان الرقمي فعاليته، كما قد يضعف عدم وجود حق عالمي للحق في النسيان الرقمي قابليته للتطبيق.

1.3. الطابع الإقليمي للحق في النسيان الرقمي تهديد لفاعليته

يعالج الفصل الخامس من اللائحة العامة الأوروبية لحماية البيانات نقل البيانات الشخصية من الاتحاد الأوروبي إلى دول أخرى، وينص هذا الفصل على عدة آليات تضمن قيام الشركات أو الدول المتلقية لهذه البيانات بتوفير مستوى ملائم من الحماية مقارنة بمستوى الحماية المنصوص عليه في اللائحة رقم 679/2016.[28] وفيما يتعلق بالولايات المتحدة، اعتمدت المفوضية الأوروبية قرارين بشأن الملاءمة: الأول في عام 2000[29] والثاني في عام 2016،[30] وقد أُبطل كلا القرارين من قبل محكمة العدل الأوروبية (قضية شريمس الأولى[31] والثانية[32]). وكان من بين ما عيب على قرار 2016 عدم منعه وصول أجهزة الاستخبارات الأمريكية إلى البيانات التي جمعها مقدمو خدمات الوصول إلى الإنترنت وخدمات الاتصالات.[33] كما لم ينص القرار على آليات كافية لتمكين الأفراد من ممارسة حقوقهم. وقد اعتمدت المفوضية قرارًا جديدًا بشأن الملاءمة في 10 يوليو 2023،[34] ويجيز نقل

البيانات الشخصية إلى الولايات المتحدة، بقدر ما يكون مستوى الحماية الذي تضمنه مكافئًا لمستوى الحماية المنصوص عليه في اللائحة العامة لحماية البيانات. ويستند هذا القرار إلى المرسوم الذي اعتمده الرئيس بايدن في أكتوبر 2022،[35] والذي يسعى إلى تعزيز الضمانات الممنوحة للأشخاص المعنيين بجمع البيانات الشخصية من قبل أجهزة الاستخبارات الأمريكية. وتقوم آلية الحماية على إلزام الهيئات التي تعالج البيانات الشخصية لمواطني الاتحاد الأوروبي بالانضمام إلى إطار حماية البيانات الشخصية بين الاتحاد الأوروبي والولايات المتحدة، من خلال التصديق على أنها تعالج البيانات الشخصية وفقًا للشروط المنصوص عليها في هذا الاتفاق.[36]

ومن جهة أولى، يثير موقف شركة OpenAI في هذا الصدد الدهشة، فالشركة لم تنضم رسميًا إلى الإطار الذي وضعه الاتحاد الأوروبي. غير أنها تشير في سياسة الخصوصية الموجهة لمستخدمي المملكة المتحدة وسويسرا والمقيمين في المنطقة الاقتصادية الأوروبية إلى أن عمليات النقل إلى دول أخرى تخضع لقرارات الملاءمة التي اتخذتها المفوضية، وفي حالة عدم وجودها، تخضع لبنود تعاقدية نموذجية.[37] وقد يتبادر إلى ذهن المستخدم أنه بالنسبة لعمليات النقل إلى الولايات المتحدة، تعتمد الشركة على قرار الملاءمة الصادر عن المفوضية الأوروبية. غير أنه ورد في قرار المفوضية الأوروبية أنه يتعين على الهيئة المنضمة أن تعلم الأشخاص المعنيين بدقة بأن الشركة تلتزم بإطار حماية البيانات الشخصية بين الاتحاد الأوروبي والولايات المتحدة.[38] وبالتالي، فإن شركة OpenAI مقصرة في التزامها بالشفافية الناشئ عن هذا القرار.

ومن جهة أخرى، فإن إطار الخصوصية (Privacy Framework) قابل للتحسين.[39] وتشدد اللجنة الأوروبية لحماية البيانات على أنه على الرغم من التحسينات التي يضمنها المرسوم الأمريكي لعام 2022، لا تزال هناك ثغرات تتعلق بممارسة حقوق الأشخاص.[40] وفي رأيها رقم 2023/5 الصادر في 28 فبراير 2023، تؤكد أن المواطنين الأوروبيين لا يحق لهم طلب محو بياناتهم إذا تم الحصول عليها من سجلات عامة.[41] وعلاوة على ذلك، في حالة وجود تهديد للأمن القومي، فإن جمع البيانات الشخصية، بما في ذلك بيانات المواطنين الأوروبيين، لن يتطلب إذنًا من سلطة إدارية أو قضائية مستقلة.[42] وعلى الرغم من هذه الثغرات، التي تفاقمت بسبب اعتماد دونالد ترامب أمرًا تنفيذيًا أضعف استقلالية لجنة التجارة الفيدرالية المسؤولة عن الإشراف على الامتثال لإطار حماية

البيانات الشخصية بين الاتحاد الأوروبي والولايات المتحدة،[43] وكذلك بسبب إقالة الأعضاء الديمقراطيين الثلاثة في مجلس الإشراف على الخصوصية والحريات المدنية،[44] فقد أكدت محكمة العدل الأوروبية أن إطار الخصوصية متوافق مع قانون الاتحاد الأوروبي.[45] غير أن هذا الوضع لا يعزز الأمن القانوني للحق في النسيان الرقمي، لا سيما في حالة ما إذا طُلب من شركة OpenAI إحالة البيانات الشخصية للمواطنين الأوروبيين، وبشكل خاص أن الشركة لم تنضم إلى الإطار الذي وضعه الاتحاد الأوروبي.

والأخطر من ذلك أن الاستقرار القانوني لإطار الخصوصية بين الاتحاد الأوروبي والولايات المتحدة يظل رهينًا بالتقلبات السياسية والإدارية الأمريكية. فمع عودة إدارة الرئيس ترامب في يناير 2025، صدر الأمر التنفيذي رقم 14147 الذي أضعف استقلالية لجنة التجارة الفيدرالية (FTC) بصورة غير مسبوقة، وتلاه إقالة الأعضاء الديمقراطيين في مجلس الإشراف على الخصوصية والحريات المدنية .(PCLOB) وتمس هذه التغييرات بشكل مباشر بجوهر الضمانات التي اعتمدت عليها المفوضية الأوروبية في قرار الملاءمة الصادر سنة 2023، لا سيما ما يتعلق بآليات التظلم المستقلة والرقابة الفعالة على أجهزة الاستخبارات، مما يعيد فتح نافذة عدم اليقين القانوني بشأن نقل البيانات الشخصية لمواطني الاتحاد الأوروبي إلى الولايات المتحدة عبر خدمات مثلChatGPT ، ويجعل الحق في النسيان الرقمي معلقًا بين التزام نظري للشركة واضطراب في إطار الحماية الدولي.

وعلى الرغم من أن المقر الرئيسي لشركة OpenAI يقع في ولاية كاليفورنيا، التي تعترف بالحق في النسيان الرقمي،[46] فإنه في ظل غياب قانون فيدرالي لحماية البيانات، ناهيك عن الاعتراف بالحق في النسيان في الولايات المتحدة،[47] فإن المادة 17 من اللائحة العامة الأوروبية لحماية البيانات الشخصية قد تواجه تشريعات متعارضة معها في صورة ما إذا تم تغيير المقر الرئيسي لشركة OpenAI.[48] ويُستخلص من ذلك أن عدم وجود حق عالمي في النسيان الرقمي يضعف قابليته للتطبيق.

2.3. عدم وجود حق عالمي في النسيان الرقمي يضعف قابليته للتطبيق

تنص المادة 3 من اللائحة العامة لحماية البيانات، والمعنونة «النطاق الإقليمي»، على أنها تسري كلما «وجَّه المسؤول عن المعالجة عروض سلع أو خدمات إلى أي مقيم في أراضي الاتحاد

الأوروبي»، ويُستخلص من ذلك أن تطبيقها يمتد حتى خارج إقليم الاتحاد الأوروبي. ويترتب على ذلك أن الحق في النسيان الرقمي، الذي تكرسه المادة 17 من اللائحة العامة لحماية البيانات، من المفترض أن ينطبق أيضًا خارج إقليم الاتحاد الأوروبي.[49]

غير أن التطبيق خارج الإقليم يعد استثناءً من مبدأ الانطباق الإقليمي للقانون، وعلى هذا النحو، فإن تنفيذه خارج إقليم الدولة ليس بالأمر الهين. ويمكن الإشارة في هذه النقطة إلى اجتهاد قضائي صادر عن محكمة العدل الأوروبية يعود إلى عام 2019. تدور هذه القضية حول الحق في إلغاء الإشارة (déréférencement) المستند إلى المادة 17 من اللائحة العامة لحماية البيانات، والذي يعد التجسيد الرئيسي للحق في النسيان في المنازعات المعروضة على محكمة العدل الأوروبية. ويتضمن، بشكل أكثر دقة، الحق في إلغاء الإشارة ومحو الروابط إلى المعلومات بمجرد إدخال اسم الشخص المعني ولقبه في شريط محرك البحث.[50]

وفي حكمها الصادر في قضية اللجنة الوطنية للمعلوماتية والحريات ضد Google لعام 2019،[51] قررت محكمة العدل الأوروبية أن الحق في إلغاء الإشارة ليس من المفترض أن ينطبق على نطاق عالمي.[52] غير أنها تترك للجهات القضائية للدول الأعضاء هامشًا من المناورة لإجراء تطبيق عالمي متى كانت حماية حقوق الشخص المعني تبرر ذلك.[53] وتجدر الإشارة إلى أن الحق في إلغاء الإشارة لا يعني المحو الكامل للبيانات، بل فقط الروابط إلى هذه البيانات.[54] وترى الهيئة القضائية في هذه النقطة أن حق الشخص في الحصول على محو هذه الروابط ليس حقًا مطلقًا، إذ يجب موازنته مع حق المستخدمين في الإعلام وفقًا لمبدأ التناسب.[55] ويُستخلص من ذلك أن قضاة محكمة العدل الأوروبية سيكونون أكثر حذرًا في الاعتراف بحق عالمي في النسيان الرقمي، بما هو حق في المحو النهائي للبيانات الشخصية للشخص المعني المنتشر على كامل شبكة الإنترنت.

ومن جانبها، ترى اللجنة الوطنية الفرنسية للمعلوماتية والحريات أن حذف المعلومات من النسخة الموجهة إلى بلد إقامة الشخص المعني لن يكون كافيًا لضمان فعالية إلغاء الإشارة، بقدر ما تظل هذه البيانات متاحة على نطاقات أخرى.[56] وبالتالي، فإن اجتهاد المحكمة يتعارض مع موقف هيئة حماية البيانات الفرنسية، ويطعن في التوجيهات الصادرة عن مجموعة العمل (G29) في إطار تطبيق حكم قضية Google Spain،[57] الذي كرس لأول مرة الحق في إلغاء الإشارة.[58]

وتجدر الإشارة من جهة أخرى إلى أن شركة Google، وإن كانت تضمن هذا الحق، فإنها لا تعمل على محو البيانات الشخصية من محرك البحث.[59] ويتم الاحتفاظ بهذه البيانات، حتى وإن لم تكن مرئية بشكل مباشر.

ويُستخلص من ذلك أن قصر الحق في النسيان على أراضي دول الاتحاد الأوروبي لا يؤثر فقط على قابلية هذا الحق للتطبيق، بل أيضًا على فعاليته. ففي سياق عالمي تنتقل فيه المعلومات بلا حدود، كيف يمكن حماية البيانات الشخصية إذا لم يمتد محوها إلى جميع أنظمة العالم؟

ويضاف إلى ذلك تعقيد ذو طابع إجرائي، يتمثل في تعدد السلطات القضائية المختصة. فلو أراد شخص مقيم في فرنسا ممارسة حقه في النسيان الرقمي ضدChatGPT ، وتبين أن بياناته قد عولجت في خوادم موجودة في الولايات المتحدة، وأن النموذج لا يزال يعيد إنتاجها لمستخدمين في اليابان، فمن أي محكمة سيطلب الإنفاذ؟ هل من محكمة مقر الشركة (كاليفورنيا)؟ أم من محكمة إقامته (فرنسا)؟ أم أن عليه اللجوء إلى كل ولاية قضائية على حدة؟ ولا يزيد هذا التشتت الإجرائي من تكاليف التقاضي ويعقده فقط، بل قد يؤدي إلى أحكام متناقضة، ويشجع الشركات المطورة على الاحتماء بـ«الملاذات القضائية» الأقل تشددًا في حماية البيانات. ولمعالجة هذا العائق، يقترح بعض الفقه،[60] إنشاء «محكمة بيانات دولية» (International Data Tribunal) ذات اختصاص لتسوية المنازعات المرتبطة باستخدامت الذكاء الاصطناعي، أو على الأقل إلزام الشركات المطورة بالخضوع للتحكيم الإلكتروني العابر للحدود كشرط مسبق لتسويق خدماتها في أسواق متعددة.

4. خاتمة:

خلصت هذه الدراسة إلى أن الحق في النسيان الرقمي، على أهميته بوصفه أحد الضمانات الجوهرية لحماية الحياة الخاصة والبيانات الشخصية، يواجه في سياق أنظمة الذكاء الاصطناعي التوليدي حدودًا عملية وقانونية واضحة تُضعف من فعاليته عند الانتقال من المستوى النظري إلى مستوى التطبيق الفعلي. ويظهر ذلك بوجه خاص عند تحليل نموذج ChatGPT، حيث تتداخل صعوبات المحو التقني مع طبيعة المعالجة القائمة على التدريب، وإعادة التوليد، وتداخل البيانات، بما يجعل حذف البيانات الشخصية أمرًا بالغ التعقيد، وقد يبلغ في بعض الحالات حد الاستحالة العملية.

كما بينت للدراسة أن الإقرار الشكلي أو النظري بالحق في النسيان داخل سياسات الخصوصية الخاصة بالمطورين لا يكفي وحده لتوفير حماية قانونية فعالة، ما لم يكن مدعومًا بآليات تقنية قابلة للتنفيذ، وبضمانات قانونية واضحة تُلزم المسؤولين عن المعالجة بوسائل محو حقيقية لا تقتصر على التعهدات العامة أو التدابير غير المحددة. وقد أظهرت الدراسة أن تعقيد النماذج التوليدية، واعتمادها على بيانات ضخمة، وما قد يطرأ عليها من «اجترار» للبيانات الشخصية، يجعل من إعادة التدريب أو استخدام المرشحات حلولاً مطروحة، لكنها ليست خالية من الكلفة أو من الإشكالات العملية.

وتزداد هذه الصعوبات حدّة عندما يتعلق الأمر بالطابع الإقليمي لقواعد حماية البيانات، حيث يظل إنفاذ الحق في النسيان مرهونًا بتباين الأطر القانونية، وغياب حق عالمي موحد في المحو، وتعدد السلطات المختصة، وعدم استقرار مستوى الحماية بين نظام وآخر. ومن ثم، انتهت الدراسة إلى أن التحدي لم يعد قانونيًا فقط، بل أصبح تقنيًا وتنظيميًا وعابرًا للحدود في آن واحد.

وعليه، فإن مسألة إعمال الحق في النسيان الرقمي في مواجهة أنظمة الذكاء الاصطناعي التوليدي لا تزال بعيدة عن الحل النهائي، ولا يمكن حسمها إلا من خلال مقاربة تجمع بين تطوير الحلول التقنية، وتحديث الإطار القانوني، وتعزيز التنسيق الدولي بين سلطات حماية البيانات، بما يضمن التوازن بين الابتكار التكنولوجي وصون الحقوق الأساسية للأفراد.

النتائج:

أولاً: ثبت أن الحق في النسيان الرقمي ليس حقًا مطلقًا، بل يخضع لقيود تتعلق بالمصالح المتعارضة، وبخاصة حرية التعبير والمصلحة العامة، فضلًا عن القيود التقنية وتكاليف التنفيذ.

ثانيًا: أظهرت الدراسة أن البنية التقنية للأنظمة التوليدية تجعل محو البيانات الشخصية، أو البيانات المرتبطة بها، أمرًا معقدًا للغاية، لأن حذف البيانات الأصلية لا يكفي لوحده لضمان إزالة آثارها من النموذج أو من المخرجات المستقبلية.

ثالثًا: انتهت الدراسة إلى أن سياسة الخصوصية الخاصة بـ OpenAI، وإن كانت تقر ببعض الحقوق المتعلقة بالمحو أو الاعتراض أو سحب الموافقة، فإن هذا الإقرار لا يرتقي إلى ضمان فعالية حقيقية لحق النسيان في الواقع التقني للنماذج التوليدية.

رابعًا: تبين أن الطابع الإقليمي لقواعد حماية البيانات يضعف قابلية الحق في النسيان للتطبيق خارج حدود الاتحاد الأوروبي، خاصة في ظل انتقال البيانات إلى الولايات المتحدة، وفي ظل عدم وجود حق عالمي موحد يضمن محو البيانات أينما وجدت.

خامسًا: أظهرت الدراسة أن الحلول التقنية المطروحة، مثل إعادة تدريب النماذج أو تطبيق المرشحات أو استخدام البيانات المركبة، تمثل خيارات واعدة، لكنها تظل مكلفة وغير مضمونة النتائج، الأمر الذي يستدعي تطويرها ضمن إطار تشريعي وتنظيمي أوضح.

التوصيات:

توصي الدراسة بضرورة تحديث النصوص المنظمة لحماية البيانات بما يراعي الخصائص البنيوية لأنظمة الذكاء الاصطناعي التوليدي، على نحو يميز بين المحو التقليدي للبيانات ومحو آثارها داخل النماذج والخوارزميات.

كما توصي الدراسة بفرض التزامات تقنية أكثر دقة على مطوري الأنظمة التوليدية، تتعلق بإمكانية تتبع البيانات الشخصية، والحد من إعادة إنتاجها، وتيسير الاستجابة لطلبات المحو والاعتراض بشكل عملي وشفاف.

وتوصي الدراسة أيضا بضرورة تعزيز الإشراف الرقابي على سياسات الخصوصية الخاصة بالشركات المطورة، مع إلزامها ببيان واضح لآليات المعالجة، وحدود النقل الدولي، ومدى انضمامها الفعلي إلى الأطر الدولية ذات الصلة.

وتوصي الدراسة أخيرا بتوحيد المعايير الدنيا لحماية الحق في النسيان الرقمي في البيئة العابرة للحدود من أجل تقليل التفاوت بين الأنظمة القانونية. والبحث عن حلول تقنية مرافقة مثل إعادة التدريب الجزئي، والمرشحات، والبيانات المركبة، مع تقييم مدى تناسبها وكلفتها وفاعليتها، حتى لا يبقى الحق في النسيان مجرد ضمانة نظرية غير قابلة للتنفيذ.

5. الهوامش:

[1] تقرير عن الأعمال التي اضطلعت بها فرقة العمل المعنية بـ ChatGPT، 24 مايو 2024، متاح على الرابط التالي:
https://www.edpb.europa.eu/our-work-tools/our-documents/edpb_20240523_report-chatgpt-taskforce_en.pdf.

[2] «نظام آلي يمكن أن يظهر قدرة على التكيف، ويستنتج من المدخلات التي يتلقاها كيفية توليد مخرجات مثل التنبؤات، أو المحتوى، أو التوصيات، أو القرارات...»، لائحة الاتحاد الأوروبي 1689/2024، المشار إليها سابقًا، المادة 3، الفقرة 1

[3] Agarwal Shubham, « With privacy concerns rising, can we teach AI chatbots to forget? », NewScientist, 8 novembre 2023, disponible à l'adresse: https://www.newscientist.com/article/2400702-with-privacy-concerns-rising-can-we-teach-ai-chatbots-to-forget./

يظهر هذا المثال أنه بمجرد إدخال البيانات في عملية المعالجة، يصبح من الصعب تقنيًا، بل ومن المستحيل في بعض الأحيان، محوها. بالإضافة إلى ذلك، هناك عنصر آخر يجعل تحليل ChatGPT في ضوء الحق في النسيان معقدًا، ألا وهو أن شركة OpenAI، المطورة لـ ChatGPT، تعلن في سياسة الخصوصية الخاصة بها أنها تنقل البيانات التي تم جمعها إلى الشركة الأم الموجودة في الولايات المتحدة.

[4] لائحة الاتحاد الأوروبي 679/2016 المؤرخة في 27 أبريل 2016 المتعلقة بحماية الأشخاص الطبيعيين فيما يخص معالجة البيانات الشخصية وبحرية تداول هذه البيانات، والتي تلغي التوجيه EC/46/95، الجريدة الرسمية للاتحاد الأوروبي، 4 مايو 2016، ص 1-88.

[5] اللائحة العامة لحماية البيانات، المادة 17، الفقرة 1.

[6] انظر المجلس الأوروبي لحماية البيانات، المبادئ التوجيهية 2019/05 بشأن الحق في النسيان، المعتمدة في 4 ديسمبر 2019، المنقحة في 7 يوليو 2020، الصفحة 5، متاحة على الرابط التالي:

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_droit_a_leffacement_apres_consultation_fr.pdf.

[7] اللائحة العامة لحماية البيانات، المرجع السابق.

[8] Juliette Sénéchal, « L'AI Act dans sa version finale -- provisoire --, une hydre à trois têtes », Dalloz Actualité, 1er mars 2023, https://www.dalloz-actualite.fr/flash/l-ai-act-dans-sa-version-finale-provisoire-une-hydre-troistetes.

[9] اللائحة العامة لحماية البيانات، المادة 17، الفقرة 2.

[10] قبل 15 فبراير 2024، لم يكن لشركة OpenAI مقر في أراضي الاتحاد الأوروبي، مما كان يمنع هيئات الرقابة المختصة بحماية البيانات من ممارسة اختصاصاتها بشكل كامل وفعّال. انظر: اللجنة الأوروبية لحماية البيانات، تقرير الأعمال التي قام بها فريق العمل المعني بـ ChatGPT، 24 مايو 2024، ص 3، متاح على العنوان التالي:

https://www.edpb.europa.eu/our-work-tools/our-documents/edpb_20240523_report-chatgpt-taskforce_en.pdf.

[11] لائحة الاتحاد الأوروبي 1689/2024 المؤرخة في 13 يونيو 2024، والتي وضعت قواعد بشأن الذكاء الاصطناعي وتعدل اللوائح رقم 2008/300، و2013/167، و168/2013، و858/2018، و1139/2018 و2144/2019 وكذلك التوجيه 90/2014، الجريدة الرسمية للاتحاد الأوروبي، 1689/2024، 12 يوليو 2024، المادة 3 «تعريفات»، الفقرة 1، متاحة على العنوان التالي:

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L_202401689

[12] اللائحة العامة لحماية البيانات، الحيثية 78.

[13] Dossier IA générative -- « ChatGPT : un beau parleur bien entraîné », article en ligne, publié le 19 mai 2023, disponible à l'adresse : https://linc.cnil.fr/fr/dossier-ia-generative-chatgpt-un-beau-parleur-bien-entraine.

[14] Alexis Beuve, « Les algorithmes », La Revue des droits de l'homme, 2018, en ligne, disponible à l'adresse : https://journals.openedition.org/revdh/4721.

[15] بخصوص تعريف «أنظمة الذكاء الاصطناعي للأغراض العامة»، انظر لائحة الاتحاد الأوروبي 1689/2024، المشار إليها سابقًا، المادة 3، الفقرة 36.

[16] Lavinia Jacquet, « ChatGPT et le RGPD : les défis de l'intelligence artificielle générative face au droit à l'effacement », Communication & Commerce électronique, n° 6, juin 2023, étude 11.

[17] اللائحة العامة لحماية البيانات، المادة 17، الفقرة 1.

[18] Olivier Blazy, « L'intelligence artificielle générative et la protection des données personnelles : l'exemple de ChatGPT », Recueil Dalloz, 2023, p. 1012.

[19] Dossier IA générative, « ChatGPT : un beau parleur bien entraîné », précité.

[20] Generative AI: The Data Protection Implications, CEDPO AI Working Group 16 October 2023, p. 7, disponible à l'adresse : https://www.cedpo.eu/wp-content/uploads/CEDPO-Generative-AI-White-Paper-16Oct23.pdf.

[21] البند 5 «الحقوق»: «تعالج OpenAI بياناتك الشخصية لغرض توفير خدماتنا، ويجوز لنا مشاركة بياناتك الشخصية مع الشركات التابعة لـ OpenAI، والكيانات الخاضعة لسيطرتها، أو التي تسيطر على OpenAI، أو التي تخضع لسيطرة مشتركة مع OpenAI. وقد تتواجد شركاتنا التابعة خارج بلدك، بما في ذلك الولايات المتحدة». OpenAI، سياسة الخصوصية، متاح على الرابط التالي :

https://openai.com/fr-FR/policies/row-privacy-policy/

[22] OpenAI، سياسة الخصوصية، المرجع المشار إليه سابقًا، البند 5 « حقوقك ».

[23] Lavinia Jacquet, « ChatGPT et le RGPD : les défis de l'intelligence artificielle générative face au droit à l'effacement », précité.

[24] Nicholas Carlini, Daphne Ippolito, Matthew Jagielski, Katherine Lee, Florian Tramer, Chiyuan Zhang, « Extracting Training Data from Large Language Models », 30th USENIX Security Symposium, août 2021, p. 2636-2640, disponible à l'adresse suivante : https://www.usenix.org/system/files/sec21-carlini-extracting.pdf.

[25] Lavinia Jacquet, « ChatGPT et le RGPD : les défis de l'intelligence artificielle générative face au droit à l'effacement », précité.

[26] Generative AI : The Data Protection Implications, précité, p. 12.

[27] OpenAI, « About », disponible à l'adresse suivante : https://openai.com/about/

[28] اللائحة العامة لحماية البيانات، المواد من 44 إلى 50.

[29] قرار المفوضية الأوروبية CE/520/2000 المؤرخ 26 يوليو 2000 الذي قرر الحماية المكفولة بموجب مبادئ "الملاذ الآمن" (Safe Harbor) لحماية الخصوصية والمسائل المرتبطة بها، الصادرة عن وزارة التجارة بالولايات المتحدة الأمريكية، الجريدة الرسمية للاتحاد الأوروبي، 25 أغسطس 2000، الصفحات 7-47.

[30] القرار التنفيذي للاتحاد الأوروبي 1250/2106 الصادر عن المفوضية بتاريخ 12 يوليو 2106 الذي قرر الحماية المكفولة بموجب درع حماية البيانات بين الاتحاد الأوروبي والولايات المتحدة، الجريدة الرسمية للاتحاد الأوروبي 207، 1 أغسطس 2106، الصفحات 1-112.

[31] محكمة العدل للاتحاد الأوروبي، 6 أكتوبر 2015، ماكسيميليان شرامس ضد مفوض حماية البيانات فيسبوك أيرلندا، القضية رقم C-362/14، ECLI:EU:C:2015:650.

[32] محكمة العدل للاتحاد الأوروبي، 16 يوليو 2020، ماكسيميليان شرامس ضد مفوض حماية البيانات فيسبوك أيرلندا، القضية رقم C-311/18، ECLI:EU:C:2020:559.

[33] محكمة العدل للاتحاد الأوروبي، 16 يوليو 2020، القضية رقم C-311/18، المشار إليها سابقًا.

[34] القرار التنفيذي للاتحاد الأوروبي 1795/2023 الصادر عن المفوضية بتاريخ 10 يوليو 2023 الذي قرر الحماية المكفولة بموجب إطار حماية البيانات بين الاتحاد الأوروبي والولايات المتحدة، الجريدة الرسمية للاتحاد الأوروبي 231، 20 سبتمبر 2023، الصفحات 118-147.

[35] الأمر التنفيذي للاتحاد الأوروبي رقم 14086، «تعزيز الضمانات لأنشطة استخبارات الإشارات بالولايات المتحدة»، 7 أكتوبر 2022، متاح على الرابط التالي:

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

[36] القرار التنفيذي للاتحاد الأوروبي 1795/2023، المشار إليه سابقًا، المادة 3.

[37] OpenAI ، سياسة الخصوصية، المرجع المشار إليه سابقًا، البند 7 « نقل البيانات إلى جهات أجنبية ».

[38] القرار التنفيذي للاتحاد الأوروبي 1795/2023 الصادر عن المفوضية بتاريخ 10 يوليو 2023 الذي قرر الحماية المكفولة بموجب إطار حماية البيانات بين الاتحاد الأوروبي والولايات المتحدة، الجريدة الرسمية للاتحاد الأوروبي 231، 20 سبتمبر 2023، الصفحات 118-147، مرجع سابق.

[39] المجلس الأوروبي لحماية البيانات، الرأي 2023/5 بشأن مشروع قرار التنفيذ الصادر عن المفوضية بشأن إطار حماية البيانات بين الاتحاد الأوروبي والولايات المتحدة، 28 فبراير 2023، متاح على الرابط التالي:

https://www.edpb.europa.eu/our-work-tools/our-documents/avis-edpb/avis-52023-sur-le-projet-de-decision-dexecution-de-la_fr

[40] المرجع السابق، ص. 16.

[41] المرجع السابق، ص. 11.

[42] المرجع السابق، ص. 13.

[43] الأمر التنفيذي رقم 14147، «ضمان المساءلة والشفافية في مجال الذكاء الاصطناعي»، 23 يناير 2025، متاح على الرابط التالي:

https://www.whitehouse.gov/presidential-actions/2025/01/executive-order-ensuring-accountability-and-transparency-in-artificial-intelligence/

[44] The White House, « President Trump Announces Appointments and Departures », communiqué de presse, 27 janvier 2025, disponible à l'adresse : https://www.whitehouse.gov/presidential-actions/2025/01/president-trump-announces-appointments-and-departures/

[45] محكمة العدل للاتحاد الأوروبي، 10 أبريل 2025، ماكسيميليان شرامس ضد المفوضية الأوروبية، القضية رقم T-354/23، غير منشور.

[46] قانون خصوصية المستهلك في كاليفورنيا، القسم 1798.105 من قانون كاليفورنيا المدني، الذي يعترف بالحق في النسيان (right to delete).

[47] لجنة التجارة الفيدرالية، «الخصوصية والأمان»، متاح على الرابط التالي:

https://www.ftc.gov/privacy-and-security

[48] بخصوص تنازع القوانين في مجال حماية البيانات الشخصية في الولايات المتحدة، انظر على وجه الخصوص:

Anupam Chander, Margot E. Kaminski, William McGeveran, « Catalyzing Privacy Law », University of Chicago Law Review, vol. 87, n° 5, 2020, p. 1245-1258.

[49] اللائحة العامة الأوروبية لحماية البيانات، المادة 3، الفقرة 2، (أ).

[50] بخصوص قابلية تطبيق اللائحة العامة لحماية البيانات خارج إقليم الاتحاد الأوروبي، انظر على وجه الخصوص:

Etienne Farnoux, « L'application territoriale du RGPD : une révolution silencieuse », Revue trimestrielle de droit européen, 2018, p. 735.

[51] محكمة العدل للاتحاد الأوروبي، 13 مايو 2014، الوكالة الإسبانية لحماية البيانات ضد جوجل إسبانيا، ماريو كوستيخا غونزاليس، القضية رقم C-131/12، ECLI:EU:C:2014:317، الفقرة 41.

[52] محكمة العدل للاتحاد الأوروبي، 24 سبتمبر 2019، اللجنة الوطنية للمعلوماتية والحريات (CNIL) ضد جوجل، القضية رقم C-507/17، ECLI:EU:C:2019:772.

[53] المرجع السابق، الفقرة 62.

[54] المرجع السابق، الفقرة 74.

[55] المرجع السابق، الفقرة 73.

[56] اللجنة الوطنية الفرنسية للمعلوماتية والحريات (CNIL)، «الحق في إلغاء الإشارة المرجعية: قرار محكمة العدل للاتحاد الأوروبي يفرض تطبيقًا إقليميًا»، بيان صحفي، 25 سبتمبر 2019، متاح على الرابط التالي:

https://www.cnil.fr/fr/droit-au-dereferencement-la-decision-de-la-cjue-impose-une-application-territoriale

[57] فريق العمل المعني بالمبادئ التوجيهية بشأن تنفيذ حكم محكمة العدل للاتحاد الأوروبي في قضية «جوجل إسبانيا»، في 26 نوفمبر 2014، الوثيقة WP 225، الصفحتان 4-5، المتاحة على الرابط التالي:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_fr.pdf

[58] المرجع السابق، ص. 10.

[59] Google, « Supprimer des informations personnelles des résultats de recherche Google », Centre d'aide, disponible à l'adresse : https://support.google.com/websearch/answer/2744324?hl=fr

[60] Anupam Chander, Is Data Localization a Solution for Schrems II?, Journal of International Economic Law, Volume 23, Issue 3, September 2020, Pages 771–784, https://doi.org/10.1093/jiel/jgaa024

References

-Agarwal Shubham, « With privacy concerns rising, can we teach AI chatbots to forget? », NewScientist, 8 novembre 2023, disponible à l'adresse: https://www.newscientist.com/article/2400702-with-privacy-concerns-rising-can-we-teach-ai-chatbots-to-forget./

-Alexis Beuve, « Les algorithmes », La Revue des droits de l'homme, 2018, en ligne, disponible à l'adresse : https://journals.openedition.org/revdh/4721.

-Anupam Chander, Is Data Localization a Solution for Schrems II?, Journal of International Economic Law, Volume 23, Issue 3, September 2020, Pages 771–784, https://doi.org/10.1093/jiel/jgaa024

-Anupam Chander, Margot E. Kaminski, William McGeveran, « Catalyzing Privacy Law », University of Chicago Law Review, vol. 87, n° 5, 2020, p. 1245-1258.

-Dossier IA générative -- « ChatGPT : un beau parleur bien entraîné », article en ligne, publié le 19 mai 2023, disponible à l'adresse : https://linc.cnil.fr/fr/dossier-ia-generative-chatgpt-un-beau-parleur-bien-entraine.

-Etienne Farnoux, « L'application territoriale du RGPD : une révolution silencieuse », Revue trimestrielle de droit européen, 2018, p. 735.

-Generative AI: The Data Protection Implications, CEDPO AI Working Group 16 October 2023, p. 7, disponible à l'adresse : https://www.cedpo.eu/wp-content/uploads/CEDPO-Generative-AI-White-Paper-16Oct23.pdf.

-Google, « Supprimer des informations personnelles des résultats de recherche Google », Centre d'aide, disponible à l'adresse : https://support.google.com/websearch/answer/2744324?hl=fr

-Juliette Sénéchal, « L'AI Act dans sa version finale -- provisoire --, une hydre à trois têtes », Dalloz Actualité, 1er mars 2023, https://www.dalloz-actualite.fr/flash/l-ai-act-dans-sa-version-finale-provisoire-une-hydre-troistetes.

-Lavinia Jacquet, « ChatGPT et le RGPD : les défis de l'intelligence artificielle générative face au droit à l'effacement », Communication & Commerce électronique, n° 6, juin 2023, étude 11.
-Nicholas Carlini, Daphne Ippolito, Matthew Jagielski, Katherine Lee, Florian Tramer, Chiyuan Zhang, « Extracting Training Data from Large Language Models », 30th USENIX Security Symposium, août 2021, p. 2636-2640, disponible à l'adresse suivante : https://www.usenix.org/system/files/sec21-carlini-extracting.pdf.
-Olivier Blazy, « L'intelligence artificielle générative et la protection des données personnelles : l'exemple de ChatGPT », Recueil Dalloz, 2023, p. 1012.
-The White House, « President Trump Announces Appointments and Departures », communiqué de presse, 27 janvier 2025, disponible à l'adresse : https://www.whitehouse.gov/presidential-actions/2025/01/president-trump-announces-appointments-and-departures/.