سياسات خصوصية بيانات المستفيدين من المكتبات الجامعية في عصر الذكاء الاصطناعي : دراسة تحليلية (الجزء الأول)(*)

Privacy Policies of University Libraries' User Data in the Age of Artificial Intelligence: An Analytical Study (Part I)

د. سمية سيد محمد محمد

مدرس بقسم المكتبات والوثائق والمعلومات

كلية الآداب - جامعة القاهرة

Email:s.amer0509@gmail.com

Orcid: 0009-0009-5533-954X

المستخلص:

هدفت الدراسة إلى تقصي الوضع الراهن لسياسات خصوصية المستفيدين من المكتبات الجامعية الأجنبية والعربية، التي شرعت في الاعتماد على تطبيقات الذكاء الاصطناعي في تقديم خدماتها للمستفيدين منها، وذلك فيما يخص مستوى الحماية التقنية والتشريعية التي تكفلها هذه السياسات لحماية خصوصية المستفيدين من المكتبات في ظل تطبيق تقنيات الذكاء الاصطناعي، ولتحقيق ذلك عمدت الدراسة إلى تحليل محتوى هذه السياسات بالاعتماد على المنهج الوصفي بأسلوبه المسحي، والذي يكفل تحقيق هذا الهدف بالاستعانة بعدد من أدواته لجمع البيانات، التي اعتمدت عليها الدراسة فكانت قائمة المراجعة، وتحليل المحتوى، والملاحظة المباشرة؛ لرصد أوجه التغيرات الجوهرية التي اتسمت بها هذه السياسات في ظل تطبيق هذه التقنيات، وقد انتهت الدراسة بنتيجة عامة مفادها اتسام مستوى الحماية التي توفرها سياسات خصوصية المستفيدين من المكتبات مجتمع الدراسة بالضعف الشديد سواء كان على مستوى الحماية التقنية أو التشريعية، مما يتطلب إعادة النظر وضرورة إيلاء الاهتمام البالغ بتطوير هذه السياسات؛ لتتوافق ومستوى الحماية المطلوب مع استخدام تقنيات الذكاء الاصطناعي، وما تمثله من تهديدات لخصوصية المستخدم، وهذا مما أوصت به هذه الدراسة.

الكلمات المفتاحية: سياسات خصوصية المكتبات- الذكاء الاصطناعي وخصوصية البيانات-

(*) يُنْشَر القسم الثاني من الدراسة في العدد رقم ٣٥ (سبتمبر ٢٠٢٥).

خصوصية المستفيدين من المكتبات والذكاء الاصطناعي– سياسات الخصوصية والذكاء الاصطناعي– أخلاقيات الذكاء الاصطناعي

Abstract

The study aimed to investigate the current status of users'privacy policies of foreign and Arab university libraries that have begun to rely on artificial intelligence applications in providing their services, with regard to the level of technical and legislative protection that these policies guarantee to protect the privacy of libraries' users in light of the application of these technologies. To achieve this, the study analyzed the content of these policies based on the descriptive approach in its survey style, which ensures the achievement of this goal by using several of its tools to collect data, which were the checklist, content analysis, and direct observation. The study concluded with a general result that the level of protection provided by the privacy policies of libraries' users in the study community is very weak, whether at the level of technical or legislative protection, which requires reconsideration and the need to pay great attention to developing these policies; to be consistent with the level of protection required with the use of artificial intelligence technologies and the threats they represent to user privacy, which is what this study recommended.

Keywords: Library Privacy Policies - Artificial Intelligence and Data Privacy - Library User Privacy and Artificial Intelligence - Privacy Policies and Artificial Intelligence - AI Ethics.

أولًا: المقدمة المنهجية:

تمهيد:

تعتمد تقنيات الذكاء الاصطناعي بصفة أساسية على تجميع البيانات لتقوم بعملها على أكمل وجه، وتحديدًا التقنيات التي تنتمي إلى فئة الذكاء الاصطناعي التوليدي Generative AI، وتعد البيانات ومجموعاتها Datasets هي العنصر المغذي الأساسي لهذه التقنيات؛ لكي تُدَرَب نماذج التعلم، فضلًا عن التعلم العميق Deep Learning، والذي يتطلب قدرًا أضخم من البيانات، ولم يتوقف الأمر على تجميع البيانات الشخصية فحسب عن المستخدمين لهذه التقنيات، بل تعدى إلى تجميع البيانات المتعلقة بسلوكهم في البحث عن المعلومات والتعامل مع مواقع الإنترنت والتطبيقات، حتى وصل إلى تفضيلاتهم الشخصية بالقدر الذي يسهل معه التنبؤ بالسلوك المستقبلي، الأمر الذي أصبح يشبه المراقبة الشخصية، وحسبه البعض دربًا من دروب التجسس.

ومع بدء شيوع تطبيق الحلول الذكية من قبل العديد من المؤسسات والخدمات، أُثيرت

الكثير من المخاوف بشأن ما تقوم به هذه التقنيات من تجميع من بيانات إلى الحد الذي بلغ الإفراط في هذا التجميع، خاصة وأن العديد من هذه البيانات تُجمَع بدون علم المستخدم، فضلًا عن القرارات التي تُتَخَذ بشأنه من قِبل النظم الذكية التي يتعامل معها، مما أثار قضية خصوصية المستخدم.

لذلك أشارت الكثير من مواثيق ومبادئ أخلاقيات الذكاء الاصطناعي إلى ضرورة إعلام المستخدم بالممارسات المتعلقة بتجميع ومعالجة البيانات من قِبل مقدمي هذه الخدمات، وتعد سياسة الخصوصية هي الوسيلة الفعلية المستخدمة لإعلام المستخدم بهذه الممارسات؛ لذا كانت سياسات خصوصية المكتبات في ظل تطبيق تقنيات الذكاء الاصطناعي محور هذه الدراسة بالفحص والتحليل.

١. مصطلحات الدراسة:

أ. تقنيات تعزيز الخصوصية Privacy Enhancement Technologies (PETs)

مجموعة الأدوات والتقنيات والأساليب المصممة لحماية خصوصية الأفراد، وتهدف تقنيات تعزيز الخصوصية إلى تمكين المستخدمين من الحفاظ على بياناتهم الشخصية، والحد من الوصول إلى المعلومات الحساسة من قبل الأطراف غير المصرح لهم، من أمثلة هذه التقنيات الخصوصية بالتصميم، الخصوصية التفاضلية، تقييم تأثير الخصوصية، التشفير، التخزين الآمن للبيانات، وغيرها. (Piwik PRO., 2024).

ب. تقييم تأثير الخصوصية Privacy Impact Assessment (PIA)

تحليل وتقييم لكيفية التعامل مع البيانات التي تُجمَع في نظام معلومات إلكتروني؛ لضمان توافق التعامل مع المتطلبات القانونية والتنظيمية المعمول بها فيما يتعلق بالخصوصية؛ لتحديد المخاطر والآثار المترتبة على هذا التجميع للبيانات، والمعالجة، والاستخدام، والتخزين، والنشر، والتخلص منها، وفحص وتقييم إجراءات الحماية والعمليات البديلة للتعامل مع هذه البيانات للتخفيف من مخاطر وتهديدات الخصوصية المحتملة (National Institute of Standards and Technology, 2024).

جـ. الخصوصية التفاضلية Differential Privacy

ترتبط الخصوصية التفاضلية بخوارزميات تعلُّم الآلة؛ حيث تتم عملية التعلم من قبل نماذج البيانات وجمع الإحصاءات حول البيانات الشخصية التي جُمِّعَت، وحُلِّلَت، وشوركت مع مراعاة إجراءات حماية خصوصية الأفراد. (الهيئة السعودية للبيانات والذكاء الاصطناعي

ومجمع الملك سلمان العالمي للغة العربية ،٢٠٢٢).

د. الخصوصية التنبؤية Predictive Privacy

تتضمن المعلومات التي يمكن تخمينها عن الأفراد من خلال مطابقتها مع معلومات العديد من الأشخاص الآخرين ذوي الصلة بالشخص أو ذوي الاهتمامات المتشابهة معه، ويمكن عن طريقها التنبؤ بمعلومات حساسة عنه دون علمه وبدون رغبته (تعريف إجرائي).

هـ. الخصوصية بالتصميم Privacy by Design

يُقصَد بها بناء ميزات حماية البيانات والخصوصية في التقنيات الجديدة منذ بداية تصميمها ومراحل تصنيعها، بدلاً من تنفيذها لاحقا (Termly Inc., 2024).

٢. مشكلة الدراسة وأهميتها:

تتبلور مشكلة الدراسة في الرغبة في رصد واقع التغيرات الجوهرية التي لا بد وأن تطرأ على سياسات خصوصية بيانات المستفيدين من المكتبات الجامعية على مستوى العالم، التي استخدمت تقنيات الذكاء الاصطناعي المختلفة في تقديم خدماتها، فبتطبيق هذه التقنيات يتحتم على المكتبات أن تعيد النظر في سياساتها لخصوصية بيانات المستفيدين من خدماتها، وتعمل على تطوير هذه السياسات بما يتوافق ومستوى الحماية للبيانات التي ستُجمَع وتُعَالج من قبل هذه التقنيات، لذا ظهرت الحاجة البحثية إلى رصد وتحليل محتوى هذه السياسات؛ للتعرف على واقعها وتقديم التوصيات التي تعزز من جدوى هذه السياسات عند التعامل مع والاستفادة من خدمات المكتبات في عصر الذكاء الاصطناعي.

وتستمد الدراسة أهميتها من أهمية خصوصية بيانات المستخدم لتقنيات الذكاء الاصطناعي، ذلك التهديد الذي يحاصر المستخدمين لهذه التقنيات، والذي يعد من أبرز المخاطر المتعلقة بها، بوصفها محاولة للحد من هذا التهديد عن طريق الاهتمام بما يجب أن تكون عليه سياسات خصوصية المستخدم في هذا العصر، بوصفها إحدى الأدوات ذات الدور الحيوي في تحقيق أمن وحماية البيانات وخصوصيتها.

٣. أهداف الدراسة:

تسعى الدراسة لتحقيق هدف عام رئيس، يتعلق برصد التطورات الراهنة لمحتوى سياسات خصوصية بيانات المستفيدين من المكتبات الجامعية المستخدمة لتقنيات الذكاء الاصطناعي في تقديم خدماتها.

ويتحقق هذا الهدف عن طريق الأهداف الفرعية التالية:

أ. حصر المكتبات الجامعية التي اعتمدت على تقنيات الذكاء الاصطناعي في تقديم خدماتها.

ب. استكشاف وتحليل مظاهر تأثر سياسات خصوصية المكتبات مجتمع الدراسة بتطبيق هذه التقنيات.

ج. تحديد المكتبات الجامعية التي احتلت أعلى المراتب من حيث توافر عناصر تحقيق الخصوصية في سياساتها في ظل تطبيق تقنيات الذكاء الاصطناعي.

د. التحقق من مستوى الحماية التي تقدمها المكتبات لخصوصية بيانات المستفيدين في ظل استخدام هذه التقنيات.

٤. تساؤلات الدراسة:

انطلقت الدراسة من عدة تساؤلات تنبثق من الأهداف التي تسعى إلى تحقيقها، فكان تساؤلها الرئيس ماذا عن التطورات الراهنة لمحتوى سياسات خصوصية المستفيدين من المكتبات الجامعية المستخدمة لتقنيات الذكاء الاصطناعي في تقديم خدماتها؟

وتتحدد تساؤلاتها الفرعية في التساؤلات التالية:

أ. ما المكتبات الجامعية التي اعتمدت على تقنيات الذكاء الاصطناعي في تقديم خدماتها؟

ب. ما مظاهر تأثر سياسات خصوصية المكتبات مجتمع الدراسة بتطبيق هذه التقنيات؟

جـ. أي من المكتبات الجامعية مجتمع الدراسة احتلت أعلى المراتب من حيث توافر عناصر تحقيق الخصوصية في ظل تطبيق تقنيات الذكاء الاصطناعي؟

د. ما مستوى الحماية التي تقدمها المكتبات لخصوصية بيانات المستفيدين في ظل استخدام هذه التقنيات؟

٥. مجال الدراسة وحدودها:

ركزت الدراسة في حدودها الموضوعية على سياسات خصوصية بيانات المستفيدين من المكتبات والتطورات المتوقع أن تحققها في ظل تطبيق تقنيات الذكاء الاصطناعي؛ لتتمكن من الدور الذي تنهض به في تحقيق حماية هذه البيانات، وكوسيلة للحد من مخاطر انتهاك الخصوصية.

وعلى مستوى الحدود النوعية فقد تخصصت الدراسة في تناول أحد مخاطر الذكاء

الاصطناعي دونا عن المخاطر الأخرى فكانت قضية خصوصية البيانات، بالإضافة إلى تناولها لهذه القضية على مستوى المكتبات الجامعية بوصفها إحدى فئات المكتبات؛ وذلك لأنها الفئة الأكثر عددًا من حيث تطبيق هذه التقنيات؛ بسبب امتلاك الغالبية العظمى من الجامعات التي تنتمي إليها لمعامل بحثية وتكنولوجية تتولى البحث والتطوير في العديد من التطورات التكنولوجية المعاصرة، ومنها الذكاء الاصطناعي.

وقد سعت الدراسة إلى رصد وتحليل سياسات خصوصية المستفيدين لتشمل المكتبات الجامعية على مستوى عدد من الدول الأجنبية والعربية والمضاهاة بينهما، كانت هذه الدول الولايات المتحدة الأمريكية، وجنوب إفريقيا، واليابان، وباكستان، وسنغافورة، وألمانيا، وجمهورية مصر العربية، هذا فيما يتعلق بالحدود المكانية، وقد وقع الاختيار على عدد من مكتبات هذه الدول لأن هذه المكتبات توافرت فيها معايير الانتقاء الخاصة بهذه الدراسة، والتي سيتم ذكرها في الجزء الخاص بمجتمع الدراسة.

وعلى مستوى الحدود الزمنية، فلم تتقيد الدراسة بحدود زمنية محددة سواء فيما يتعلق بتاريخ تطوير أو تحديث سياسات خصوصية المستفيدين، أو فيما يتعلق بتاريخ تبني المكتبات مجتمع الدراسة لتقنيات الذكاء الاصطناعي واستخدامها في خدماتها.

منهج الدراسة وأدواتها:

١,٦ منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي بأسلوبه المسحي؛ ذلك المنهج الممكن من عملية الوصف والتحليل لواقع التطورات الراهنة لسياسات خصوصية المستفيدين من المكتبات، التي وقع عليها الاختيار بوصفها مجتمعًا للدراسة، فضلًا عن القيام بعملية المسح للمكتبات الجامعية التي قامت بتطبيق تقنيات الذكاء الاصطناعي المختلفة، والمسح للتقنيات المطبقة بالفعل بهذه المكتبات.

٢,٦ أدوات جمع البيانات:

ولكي تتمكن الدراسة من تحقيق أهدافها والخروج بنتائجها، توسلت الدراسة بعدد من أدوات جمع البيانات التي يكفلها المنهج المعتمد من جانبها، كانت هذه الأدوات على النحو التالي:

أ. قائمة المراجعة[١] Checklist: تضمنت العناصر المراد التحقق من توافرها بسياسات

١. ملحق (١) قائمة المراجعة.

خصوصية المستفيدين من المكتبات، والتي تعكس التطورات المفترض أن تتوافر على مستوى سياسات الخصوصية في ظل استخدام الذكاء الاصطناعي، وقد رُوجِعَت هذه القائمة من قبل أ.د. أسامة السيد محمود، أستاذ المكتبات والمعلومات المتفرغ بقسم المكتبات والوثائق والمعلومات، كلية الآداب، جامعة القاهرة.

ب. تحليل المحتوىContent Analysis : وقد استُعين بإحدى أدوات الذكاء الاصطناعي المتخصصة في تحليل محتوى واستخلاص عناصر سياسات خصوصية البيانات، تلك الأداة التي تعرف بـ PrivacyAnalyzerGPT[٢]، والتي تعمل على التحقق من توافر عدد من عناصر خصوصية البيانات بسياسات الخصوصية، كتحديد فئات البيانات التي تُجمَع، والغرض من هذا التجميع وطرقه، ومشاركة البيانات مع أطراف ثالثة، وعناصر تأمين البيانات، وذلك وفقًا للائحة العامة لحماية البيانات (GDPR).General Data Protection Regulation .

جـ. الملاحظة المباشرة: لمواطن التغير والتطور لمحتوى سياسات خصوصية المستفيدين من المكتبات مجتمع الدراسة، ولاستيفاء عناصر قائمة المراجعة المعتمدة من قبل الدراسة.

٣,٦ مجتمع الدراسة:

تألف مجتمع الدراسة من ١٨ مكتبة جامعية[٣]، تنوعت ما بين ١٧ مكتبة أجنبية توزعت على مختلف دول العالم فكانت الولايات المتحدة الأمريكية، وجنوب إفريقيا، وألمانيا، وباكستان، واليابان، وسنغافورة، ومكتبة عربية واحدة بجمهورية مصر العربية هي مكتبة جامعة مصر للعلوم والتكنولوجيا (MUST) Misr University for Science & Technology Library، جُمِعت هذه المكتبات وفقًا لمعايير الانتقاء التالية:

- معايير الانتقاء:
  - أن تعتمد المكتبة على إحدى تقنيات الذكاء الاصطناعي في تقديم خدماتها.
  - أن تتوافر للمكتبة سياسة خصوصية على موقعها الإلكتروني، وإذا كانت للمكتبة صفحة بموقع الجامعة التي تنتمي إليها، فيُعتَمد على سياسة خصوصية الجامعة المتاحة على موقعها، شرط نص سياسة خصوصية موقع الجامعة على شمول

٢. قام بتطوير هذه الأداة مجموعة من الخبراء في مجال تحقيق الأمن على مستوى العديد من منتجات تكنولوجيا المعلومات ينتمون لمنظمة تدعى Security.org بالولايات المتحدة الأمريكية، هذه الأداة متاحة على الرابط https://www.security.org/digital-safety/privacy-policy-analyzer/

٣. ملحق (٢) قائمة المكتبات مجتمع الدراسة.

وتطبيق بنودها على كافة مرافق ومؤسسات الجامعة وخدماتها، والتي من بينها المكتبة.

وقد حُصِرَت مفردات مجتمع الدراسة من المكتبات الجامعية عن طريق الدراسات البحثية التي تناولت تجارب المكتبات الجامعية في تطبيق واستخدام الذكاء الاصطناعي، فضلًا عن التواصل مع بعض المكتبات الأخرى، التي بُحِث عنها للتحقق من تطبيق هذه التقنيات.

٧. الدراسات السابقة:

١,٧ مصادر الحصول على الدراسات السابقة:

١. قواعد البيانات العربية والأجنبية المتاحة عن طريق بنك المعرفة المصري، كقاعدة بيانات دار المنظومة، وعدد من قواعد البيانات الأجنبية، هي Springer Link, Science Direct, IEEExplore, Taylor & Francis Online.

٢. دليل الإنتاج الفكري العربي في مجال المكتبات والمعلومات والمتاح بقاعدة بيانات الهادي.

٣. بالإضافة إلى محرك الباحث العلمي Google Scholar، والمكتبات الرقمية مثل ACM Digital Library ، وبعض المستودعات الرقمية مثل مستودع arxiv.

وذلك اعتمادًا على استراتيجيات البحث التالية:

- الخصوصية والمكتبات، الذكاء الاصطناعي، والمكتبات الجامعية، وخصوصية البيانات، الخصوصية والذكاء الاصطناعي.
- Privacy AND Libraries- Artificial Intelligence AND Libraries Privacy Policies - Artificial Intelligence AND Privacy - Artificial Intelligence AND Privacy AND Academic Libraries.
- وقد نُظِمَت الدراسات زمنيًّا من الأقدم إلى الأحدث تحت مجموعة من المحاور الموضوعية.

٢,٧ الدراسات العربية والأجنبية:

أ. سياسات خصوصية المستفيدين من المكتبات:

اقترحت دراسة (Singley, E. 2020) نهجًا تعاونيًّا شاملًا لضمان خصوصية المستفيدين من المكتبات الجامعية في ظل ما تشهده المكتبات من تحديات تقنية متتالية، وقد قُدِم هذا النهج من منظور الباحثة كإحدى أمناء المكتبات، حيث إن المكتبات الأكاديمية

بحاجة إلى إعادة النظر في ممارسات الخصوصية الخاصة بها لتتوافق بشكل أفضل مع واقع الإنترنت وتطورات تقنيات المعلومات ووسائل الاتصالات، مما يدفعها إلى تطوير ممارسات قائمة على الأسس الأخلاقية؛ حتى يمكن لأمناء المكتبات الأكاديمية البدء في استعادة ثقة المستفيدين منها.

هدفت دراسة (إيمان عبد الحميد يس وأماني محمد السيد، ٢٠٢٢) إلى تقصي الوضع الراهن للمكتبات الجامعية المصرية سواء كانت الحكومية أو الخاصة، فيما يتعلق بتطبيقها للقانون المصري لحماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، ومدى توافق سياساتها لخصوصية البيانات معه، معتمدة في ذلك على المنهج المسحي الميداني وأسلوبه الوصفي التحليلي؛ للتوصل إلى نتائج الدراسة والتي تلخصت في عدم توافر سياسات لخصوصية بيانات المستفيدين من هذه المكتبات، وما تقوم به المكتبات هي مجرد ممارسات متعارف عليها من الميثاق الأخلاقي للمهنة، دون تدريب لأمناء هذه المكتبات على ممارسات حماية البيانات، وقد أوصت بضرورة رفع الوعي بقضايا خصوصية البيانات، واعتماد سياسة خصوصية موحدة لقطاع المكتبات الجامعية من قبل وزارة التعليم العالي.

سعت (هبة أحمد المتبولي، ٢٠٢٢) إلى تقديم نموذج مُقترح لسياسة خصوصية بيانات للمستفيدين من المكتبات على صعيد الوطن العربي، وذلك بعد دراسة وتحليل سياسات الخصوصية لعينة من المكتبات الأجنبية لاستخلاص أبرز العناصر والبنود الواردة فيها، وما تغطيه هذه السياسات من مجالات لتحقيق حماية البيانات. وقد اعتمدت لتحقيق أهداف الدراسة على المنهج المسحي بشقيه الوصفي والتحليلي. ومن أهم النتائج التي توصلت إليها الدراسة؛ عدم حرص المكتبات عينة الدراسة في سياساتها على ذكر العديد من العناصر بالغة الأهمية مثل الهدف من وضع سياسة الخصوصية، وخصوصية التعامل مع الأطفال، وأوصت الدراسة بضرورة اهتمام المكتبات بتوفير بيئة آمنة ومحمية حتى يتمكن المستفيدون من إتاحة معلوماتهم الشخصية بأمان وذلك عن طريق تطوير وتحديث سياساتها للخصوصية، أيضًا ضمان حماية بيانات المستفيدين الشخصية بما يتوافق والقوانين والتشريعات التي تتبعها كل دولة.

عملت (ندا مصطفى لبيب، ٢٠٢٣) على تقديم نموذج لسياسة خصوصية بيانات المستفيدين من المكتبات الجامعية بمصر، وذلك بعد أن قامت برصد الإجراءات المتبعة لحماية الخصوصية في هذه المكتبات، والتعرف على مستوى وعي أمناء المكتبات بقضية الخصوصية وأهمية تطبيقها، مستعينة في ذلك بالمنهج الوصفي التحليلي وأسلوبه المسحي.

وتعد أبرز النتائج التي توصلت إليها ضرورة العمل على إنشاء سياسات لحماية خصوصية بيانات المستفيدين بالمكتبات الجامعية المصرية. وقد أوصت بضرورة توافر دليل عملي للمكتبات يرشد إلى إجراءات حماية خصوصية البيانات، فضلًا عن تنمية وعي أمنائها فيما يتعلق بهذه القضية.

وضع (Bettinger, E. C. et al., 2023) خريطة طريق لتحول الممارسات في بيئة المكتبات الأكاديمية لتحقيق خصوصية بيانات المستفيدين، وتوظيف الإجراءات والإمكانات بما يحقق هذا المفهوم؛ حيث إن حقيقة حماية الخصوصية في بيئة المعلومات في القرن الحادي والعشرين أكثر تعقيدًا بكثير مما كانت عليه في الوقت السابق، وقد ناقش السؤال المطروح: لماذا تعد الخصوصية في بيئة المكتبات مشكلة شائكة في الوقت الراهن؟ كما عمل على شرح لماذا يعد تحقيق خصوصية المستفيد هدفًا ضروريًّا؟

يؤكد (Dahlian P., et al 2024) أهمية الأمن السيبراني للمكتبات الرقمية، فيما يتعلق بامتثالها للمعايير التكنولوجية والتنظيمية لحماية بيانات المستخدم وضمان الخصوصية عند الوصول إلى والتعامل مع المصادر الإلكترونية للمكتبة؛ حيث تواجه المكتبات تحديات مختلفة في قضية حماية البيانات الشخصية، وقد عرضت الدراسة لموضوعات مثل خصوصية المستخدم، وتشفير البيانات، وإدارة الوصول، والامتثال لقوانين الخصوصية، وقد انتهت الدراسة بتقديم رؤى وحلول لمعالجة هذه التحديات، وضمان قدرة المكتبات الرقمية على العمل بأمان وكفاءة فيما يتعلق بخصوصية البيانات.

ب. خصوصية البيانات في عصر الذكاء الاصطناعي:

حلل (Bartlett, M. 2021) التحديات التي فرضها الذكاء الاصطناعي على قوانين الخصوصية في عدد من الدول، وهي أستراليا، ونيوزيلندا، واللائحة العامة لحماية البيانات في الاتحاد الأوروبي، ففي حين تحمي هذه القوانين قضية الخصوصية، فإن الذكاء الاصطناعي قد يعتمد على فئات بيانات أوسع مما قد حددته تلك القوانين من بيانات تستحق الحماية، فضلًا عن قدرته على القيام بالتنبؤات المختلفة والمستخرجة من البيانات التي يقوم بتجميعها، ويوضح أيضًا كيف أن هذه الأطر التشريعية لا تكفي لتحقيق هذه الحماية، فهناك حاجة ماسة إلى أنظمة قانونية جديدة لضمان هذه الحماية.

قامت (ريم غريب علي، ٢٠٢٢) بالتعرف على المخاطر التي يثيرها الذكاء الاصطناعي فيما يتعلق بالخصوصية، وكيفية مواجهتها عن طريق التشريعات وتحديدا التشريعات الإمارتية، مقارنة بالقانون المصري لحماية البيانات الشخصية، وفي ضوء ما

حددته اللائحة العامة لحماية البيانات. وقد اعتمدت الدراسة المنهج الوصفي التحليلي لتحقيق أهدافها، وتوصلت إلى عدم مواءمة القوانين الحالية مع مستوى المخاطر التي يثيرها الذكاء الاصطناعي، ووجوب تطوير النصوص التشريعية لتتناسب مع هذه المخاطر، وهذا مما أوصت به الدراسة.

تأتي دراسة (عبد الله شيباني ووداد بن سالم، ٢٠٢٣) للتعرف على تهديدات الخصوصية التي فرضها الذّكاء الاصطناعي، وموقف القانون من التعامل مع هذه التهديدات، وقد استخدمت الدراسة المنهج الوصفي التحليلي، وتوصلت إلى أن استخدام الذكاء الاصطناعي دون رقابة وضوابط قانونية يعد خطرًا يهدد خصوصية الأفراد، وعليه أوصت الدراسة بضرورة تحديد ضوابط استخدام هذه التقنيات من قِبل الدول، وتطوير البنية التشريعية لحماية البيانات والحفاظ على الخصوصية.

قدم (Villegas-Ch, W., & García-Ortiz, J. , 2023) إطار عمل لمعالجة القضايا والتحديات الراهنة التي فرضها الذكاء الاصطناعي فيما يتعلق بأمن البيانات وخصوصيتها، حيث قام بتحديد الثغرات والفجوات التي تتطلب الاهتمام من أجل تحسين أطر العمل المعمول بها حاليًا، كما نبه لأهمية حماية البيانات المستخدمة في نماذج الذكاء الاصطناعي، ووصف السياسات والممارسات التي تضمن أمنها، بالإضافة إلى الأساليب الممكنة للحفاظ على سلامة هذه البيانات، بالإضافة إلى ذلك فقد أوصى بأهمية تقييم وفحص أمن أنظمة الذكاء الاصطناعي، وتحليل نقاط الضعف والمخاطر الموجودة في هذه الأنظمة، كما قدم أمثلة على الهجمات المحتملة والتلاعبات الخبيثة، ذلك مع ضرورة تطوير وتبني الأطر الأخلاقية والتنظيمية المتعلقة بالأمن والخصوصية في الذكاء الاصطناعي.

عمل (عبد الرازق عبد الكريم، ٢٠٢٤) على اقتراح رؤية لأخلاقيات الذكاء الاصطناعي، تتضمن المعايير الأخلاقية التي تضبط استخدام الذكاء الاصطناعي بما يضمن حقوق الإنسان وخصوصية بياناته، وذلك بالاستعانة بالمنهج الوصفي التحليلي، وقد توصل إلى عدة نتائج أبرزها افتقار الذكاء الاصطناعي إلى الحد الأدنى من القيم الأخلاقية، فضلًا عن الغياب التام للمسألة القانونية، وقد وجه توصياته إلى المسؤلين في مختلف الدول بضرورة العمل على وضع المعايير الأخلاقية لهذه الأنظمة وتطبيقاتها.

اهتم (Edwin Frank, 2024) بالجوانب الرئيسة لخصوصية البيانات وأمنها في أنظمة الذكاء الاصطناعي، حيث عرض لقضية حماية المعلومات الشخصية التي تُجمَع وتُعَالج بواسطة أنظمة الذكاء الاصطناعي، وما يكتنف ذلك من مخاطر مرتفعة، فعمل على

سرد التقنيات الممكنة لتحقيق هذه الحماية، فكان منها تقنيات التشفير، وتقييم تأثير الخصوصية، والخصوصية بالتصميم وغيرها من التدابير والتقنيات الأخرى، كما نبه إلى ضرورة الانصياع إلى الأطر التشريعية المستحدثة لضمان تكامل هذه الحماية.

جـ. المكتبات والذكاء الاصطناعي وقضية الخصوصية:

قدم (Bradley, F., 2022) بعض التصورات التنظيمية لاستخدامات الذكاء الاصطناعي ودور المكتبات في هذه العمليات، كما قدم ملخصًا لكيفية أداء أنشطة المكتبات في ضوء هذه التصورات موضحا أن المكتبات هي الأجدر على القيام بمهمة حماية البيانات وتحقيق خصوصية المستفيدين؛ لأنها تمتلك الخبرة المطلوبة في هذا الصدد، فضلًا عن اضطلاعها بأدوار فريدة فيما يتعلق بالقضايا التنظيمية ذات الصلة بما في ذلك حقوق النشر وحماية البيانات، ويقترح عدد من الفرص للإسهام في مستقبل الذكاء الاصطناعي الأخلاقي والجدير بالثقة والأكثر شفافية.

حدد كلٌ من (Kautonen, H., & Gasparini, A. A. , 2023) التهديدات والاعتبارات الأخلاقية التي يواجهها أمناء المكتبات البحثية عندما يتعاملون مع تقنيات الذكاء الاصطناعي المستحدثة، وقدمت الدراسة مفاضلة بين مدونة قواعد السلوك الدولية للمكتبات Iinternational Code of Conduct for Libraries والمبادئ التوجيهية الأوروبية للذكاء الاصطناعي The European AI Guidelines؛ للخروج برؤية شاملة حول ما يجب أن تكون عليه القواعد الأخلاقية الحاكمة للذكاء الاصطناعي في المكتبات، وتشير الدراسة أيضًا إلى الحاجة إلى تحديث قواعد السلوك الدولية للمكتبات في عصر الذكاء الاصطناعي، مما يساعد أمناء المكتبات على توجيه أنفسهم بشكل أفضل نحو مستقبل جدير بالثقة ومستدام في ظل استخدام أنظمة الذكاء الاصطناعي.

استكشفت دراسة (Soni, D., 2023) الدور المحوري للذكاء الاصطناعي في علوم المعلومات والمكتبات، وعملت على توضيح الفرص والتحديات والآثار الأخلاقية المترتبة على استخدام تقنياته المختلفة، كما بحثت في كيفية تأثير هذه التقنيات على عمليات استرجاع المعلومات، والتنظيم لمصادر المعلومات، وخدمات المستفيدين، فضلًا عن عمليات صنع القرار داخل المكتبات، بالإضافة إلى ذلك ناقشت الدراسة الاعتبارات الأخلاقية المحيطة باستخدام الذكاء الاصطناعي في علوم المعلومات والمكتبات، مع تأكيد أهمية تبني المكتبات لما يُعرَف بالذكاء الاصطناعي المسؤول، والعمل على معالجة

التحيزات المحتملة ومخاوف الخصوصية والآثار المترتبة على ذلك مجتمعيًّا.

سعت (أمل حسين عبد القادر، ٢٠٢٤) إلى التوعية بتداعيات تطبيقات الذكاء الاصطناعي فيما يتعلق بحماية خصوصية البيانات، وذلك في ضوء ما أصدِرَ وطنيًّا وإقليميًّا وعالميًّا من أطر عامة وسياسات لحماية خصوصية البيانات، وعلى رأسهم ما أصدرته جمعية المكتبات الأمريكية من إرشادات تتعلق بحماية خصوصية البيانات والإجراءات المنوطة بها في ظل استخدام الذكاء الاصطناعي. وقد اعتمدت الدراسة على منهج دراسة الحالة بشقيه الوصفي والتحليلي، ومن أهم النتائج التي توصلت إليها أن الإرشادات التوجيهية التي أصدرتها جمعية المكتبات الأمريكية، تعد من أفضل الإرشادات لتحقيق حماية وأمن البيانات للمكتبات في ظل الذكاء الاصطناعي. وقد أوصت بضرورة تبني المكتبات لهذه الإرشادات، وضرورة التعليم والتدريب المستمر لأمناء المكتبات فيما يتعلق باستخدام نظم الذكاء الاصطناعي بما يراعي خصوصية البيانات.

تناولت (مهرة سليمان، ٢٠٢٤) أبرز التحديات المتعلقة بالذكاء الاصطناعي وتأثيرها على خصوصية الأفراد، وكيفية مواجهة هذه التحديات من منظور إسلامي ومنظور قانوني، مستعينة في ذلك بالمنهج الوصفي التحليلي، وقد توصلت الدراسة إلى أن هناك ضعفًا في مستوى وعي الأفراد بهذه التحديات، وما يتعلق منها بخصوصية البيانات، وتوصي بضرورة وضع الأطر الأخلاقية والسياسات التي تحفظ الخصوصية وتحد من مخاطر انتهاكها.

استكشفت دراسة (Hodonu-Wusu, J. O., 2024) الاستخدام الأخلاقي والعادل للذكاء الاصطناعي في المكتبات، وما يجب على أمناء المكتبات مراعاته عند استخدام هذه التقنيات، وقد أظهرت الدراسة كيف يمكن تحقيق التوازن فيما بين استخدام هذه التقنيات واستثمار مميزاتها والفرص التي أتاحتها لتعزيز تجارب المستخدم، وتحقيق الاستخدام الأخلاقي الجدير بالثقة بما يحقق حماية خصوصية وأمن البيانات.

د. تطبيقات الذكاء الاصطناعي في مجال الخصوصية:

عمل (Alabduljabbar, A., & Mohaisen, D. ,2022) على استخدام تقنيات الذكاء الاصطناعي، تحديدًا تقنية معالجة اللغة الطبيعية ونماذج التعلم العميق Deep Learning Model في الإسهام في فهم سياسات خصوصية عدد من المواقع الإلكترونية، وذلك من خلال التركيز على التحليل المقارن لمحتوى هذه السياسات، حيث قامت الدراسة بتحليل عدد من السياسات بلغ ١٥٦٢ سياسة، ولقد تُوصِل إلى أن المواقع الإلكترونية المتميزة أكثر شفافية في الإبلاغ عن ممارساتها المتعلقة بالخصوصية، وخاصة فيما يتعلق بعملية

الاحتفاظ بالبيانات وعدم التتبع مقارنة بالمواقع الإلكترونية ذات المحتوى المجاني. أما عن سياسات الخصوصية الخاصة بالمواقع الإلكترونية ذات المحتوى المجاني، فهي أكثر تشابهًا مع بعضها بعضًا، وأكثر عمومية مقارنة بسياسات الخصوصية الخاصة بالمواقع الإلكترونية المتميزة.

اقترح (Mylrea, M., & Robinson, N., 2023) إطار عمل لمعالجة تحديات الخصوصية التي ارتبطت بتقنيات الذكاء الاصطناعي؛ حيث قام على استخدام خوارزمية Entropy من أجل تعزيز الشفافية والثقة في أنظمة الذكاء الاصطناعي، وتعمل هذه الخوارزمية على تقييم وقياس جدارة هذه النظم بالثقة من حيث جودة تصميمها، ومراعاتها لاعتبارات الخصوصية، وحماية البيانات وتطبيقها لمبدأ الحد الأدنى من البيانات في عملية التجميع.

حاولت (Wagner, I. , 2023) تتبع تاريخ تطور محتوى سياسات خصوصية البيانات لعدد من المواقع والخدمات على مدار ٢٥ عامًا، منذ عام ١٩٩٦ حتى عام ٢٠٢١ باستخدام خوارزميات تعلم الآلة ومعالجة اللغة الطبيعية والشبكات العصبية Neural Networks؛ لتقديم تحليل شامل لمحتوى هذه السياسات من حيث الممارسات المتعلقة بتجميع ومعالجة البيانات، والحقوق التي تمنحها للمستخدمين، والحقوق التي تحتفظ بها للجهات التي تنتمي إليها، وقد عملت على استكشاف التغييرات التي طرأت على محتوى هذه السياسات، استجابةً للوائح الخصوصية الأخيرة كاللائحة العامة لحماية البيانات GDPR، حيث لُوحِظ بعض التغييرات الإيجابية مثل انخفاض عناصر جمع البيانات، في مقابل ذلك لُوحِظت مجموعة من الممارسات المثيرة للقلق مثل جمع البيانات الضمنية على نطاق واسع. وقد اختتمت الدراسة بعرض لميزات الذكاء الاصطناعي المضافة لجعل سياسات الخصوصية قابلة للقراءة آليًا من جانب المستخدم، الأمر الذي من شأنه مساعدة المستخدمين على مطابقة تفضيلات الخصوصية الخاصة بهم مع السياسات التي تقدمها خدمات ومواقع الويب.

قيمت دراسة (Yan, C. et al, 2024) مستوى جودة سياسات الخصوصية لتطبيقات المساعد الشخصي الافتراضية Virtual Personal Assistant (VPA)، كالمساعد الرقمي المقدم من شركة أمازون Alexa، وشركة جوجل Google Assistant، وذلك في ضوء أربعة معايير تحقق جودة هذه السياسات، وهي التحديث وضمانات الإتاحة والاكتمال وإمكانية القراءة لهذه السياسات، وذلك بالاعتماد على تطبيق QuPer الذي طور ليستخرج

الميزات الوصفية لهذه السياسات كسجل التحديثات، والميزات اللغوية كدلالات الجمل، ويقيم جودتها، والذي يعتمد بصفة أساسية على خوارزميات تعلم الآلة ومعالجة اللغة الطبيعية، وقد انتهت نتيجة التحليل لمستوى جودة هذه السياسات إلى أن ١,١٧% فقط من سياسات الخصوصية لهذه التطبيقات قد توافرت فيها المعايير المطبقة من قبل الدراسة.

وتعليقًا على الدارسات السابقة:

- حظيت قضية خصوصية البيانات وحمايتها بأهمية بالغة على مستوى الدراسات العربية والأجنبية على حد سواء، سواء كان ذلك على مستوى التطورات التقنية فيما قبل شيوع الذكاء الاصطناعي، أو بعد الاستخدام لهذه التقنيات.
- توقف اهتمام الدراسات العربية التي قامت على دراسة سياسات خصوصية المستفيدين من المكتبات –على الرغم من حداثتها– على الاهتمام بالقضايا التقنية فيما قبل الذكاء الاصطناعي، وهذا ما اجتهدت الدراسة الحالية لاستكماله بدراسة الوضع الراهن لهذه السياسات في ظل استخدام المكتبات لتقنيات الذكاء الاصطناعي.
- اهتمت الدراسات الأجنبية من بين ما اهتمت به في قضية الخصوصية بمجالات تطبيق تقنيات الذكاء الاصطناعي لخدمة هذه القضية، وهذا ما لم تتعرض له الدراسات العربية.

ثانيًا: الإطار النظري

١. نظرة عامة على قضية الخصوصية وحمايتها

١,١ الخصوصية وفئاتها:

لكل فرد الحق في أن يعيش حرًا بعيدًا عن محاولات التطفل، وأن يسلم من تدخل الآخرين في تفاصيل شؤونه الخاصة، وله الحق أيضًا في التحكم في الإطار الذي يمكن أن يصل إليه معلوماته الشخصية للمحيطين به، فضلًا عن التحكم في أوجه استخدام هذه المعلومات إذا حُصِلَ عليها من قبل أطراف آخرين، وهذا ما كفلته العديد من القوانين والتشريعات على اختلاف درجاتها ونطاقها، والخصوصية في أبسط صورها هي "الحق في أن يترك المرء وشأنه"، كما عرفها القاضي كولي Cooley بالولايات المتحدة الأمريكية عام ١٨٨٠، كما أنها الحق في أن لا يُكشَف عن هوية الفرد (لويد، إيان جيه،٢٠١٧،ص ٢٧–٢٨) (Dunne, R. , 2009).

ولم يقتصر حق الأفراد في الحفاظ على خصوصية الحياة الشخصية فقط، بل تعددت صور خصوصية الأفراد لتشمل جوانب أخرى كالتالي:

أ. خصوصية الجسد: والتي تُعنى بالحماية الجسدية ضد الانتهاكات المتعلقة به.

ب. خصوصية الاتصالات: بأن تكون اتصالات ومراسلات الفرد بمنأى عن أي تتبع أو مراقبة.

ج. خصوصية المسكن: أن يأمن الفرد في مسكنه، وأن يأمن المسكن نفسه ضد أي تهديدات أو اختراقات لخصوصيته (منى تركي الموسوي، جان سيريل فضل الله، ٢٠١٣).

د. خصوصية البيانات: ويقصد بها خصوصية البيانات الشخصية للأفراد كالاسم، والسن، وعنوان الإقامة، وبزيادة تفصيل فئات هذه البيانات تزداد خصوصيتها فميا يعرف بخصوصية البيانات ذات الحساسية، والتي تشمل البيانات المالية، البيانات الصحية، بيانات الأصل أو العرق، معلومات القياسات الحيوية، المعلومات الوراثية، السجلات الجنائية، المعتقدات الدينية أو الأيديولوجية، الميول السياسية (لويد، إيان جيه ،٢٠١٧، ص٩٦).

هـ. الخصوصية المعلوماتية: وتعني خصوصية بيانات الأشخاص، والتي تعالج وتختزن بالنظم الآلية، وقد ارتبط هذا المصطلح بالتطورات التكنولوجية في مجال الاتصالات والمعلومات، وعلى رأسها الإنترنت (عائشة بن قارة، ٢٠١٧)

٢,١ الخصوصية والحماية التشريعية.

وقد حفظت العديد من التشريعات والقوانين الحق في الخصوصية وكفلته لجميع الأفراد، ومن قبلها الكثير من النصوص الدينية المختلفة (فوزية شريط، ٢٠١٩)، كما صدرت تجاه هذه القضية العديد من المواثيق الدولية بدايةً من الميثاق العالمي لحقوق الإنسان لعام ١٩٤٨، حتى التشريعات واللوائح الدولية والإقليمية والعربية والمحلية، وترجع أبرز هذه الجهود إلى عدد من المنظمات الدولية كمنظمة التعاون الاقتصادي والتنمية Organization for Economic Co-operation and Development (OECD) في إصدار دليل إرشادي لحماية الخصوصية المعلوماتية عام ١٩٧٨، والمجلس الأوروبي في وضعه اتفاقية لحماية بيانات الأفراد من المخاطر المحتملة للمعالجة الآلية للبيانات ومراحلها المختلفة عام ١٩٨١ (عائشة بن قارة، ٢٠١٧)، ويأتي على رأس هذه الجهود اللائحة العامة لحماية البيانات General Data Protection Regulation (GDPR)،

والتي دخلت حيز التنفيذ مايو ٢٠١٨، والتي تعد بمثابة قانون أوروبي لحماية البيانات والتي صدرت لتوحيد قوانين خصوصية البيانات في جميع أنحاء أوروبا، وعلى مستوى جهود الدول منفردة، فقد صدر العديد من التشريعات بالولايات المتحدة الأمريكية، وفرنسا، وألمانيا وغيرها من الدول الأخرى، والتي تناولتها الكثير من الدراسات من قبل (Boehm, F. , 2015) (De Bruin, R. , 2022) .

وعلى مستوى الجهود العربية فقد أولت جامعة الدول العربية اهتمامًا ملحوظًا بقضية حماية البيانات وخصوصيتها؛ حيث تولت إصدار الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات عام ٢٠١٠، والتي شغلت قضية حماية البيانات العديد من بنودها ومضمونها (الأمانة العامة لجامعة الدول العربية، ٢٠١٠)، كما اهتمت العديد من تلك الدول بإصدار قوانين وتشريعات حماية البيانات، ومن أحدث هذه التشريعات نظام حماية البيانات الشخصية رقم (م/١٩) بالمملكة العربية السعودية لعام ٢٠٢١، وقانون حماية البيانات الشخصية لعام ٢٠٢٠ بالمملكة الأردنية الهاشمية، وقانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ بجمهورية مصر العربية (ندا لبيب، ٢٠٢٢).

وبمراجعة ما أصدِر من تشريعات تتعلق بحماية خصوصية بيانات المستخدم، لم يحظ مجال الذكاء الاصطناعي حتى الآن بالعديد من هذه التشريعات المنظمة لقضية حماية الخصوصية ولا تنظيم استخدامه بشكل عام إلا بصدور قانون الاتحاد الأوروبي للذكاء الاصطناعي EU AI Act من قبل البرلمان الأوروبي، والذي كانت بداية اقتراحه في أبريل عام ٢٠٢١، واعتماده مارس ٢٠٢٤، ووُفِقَ عليه مايو ٢٠٢٤، ومن المنتظر دخوله حيز التنفيذ، ويعد بمثابة أول تشريع لتنظيم استخدام الذكاء الاصطناعي على مستوى دول الاتحاد الأوروبي، وقد شمل القانون جميع فئات أنظمة الذكاء الاصطناعي على اختلاف مجالات استخدامها ومستوياتها، وقد صنفها لأربع فئات وفقًا لخطورتها، والتي تشمل أنظمة الذكاء الاصطناعي منخفضة المخاطر، والأنظمة ذات المخاطر المحدودة، والأنظمة عالية المخاطر والتي ستخضع لالتزامات صارمة تحد من خطورتها، إلى جانب الأنظمة ذات المخاطر غير المقبولة، تلك التي يحظر تسويقها في دول الاتحاد الأوروبي (European Parliament, 18June 2024). وكانت قضية الخصوصية وحماية البيانات من ضمن القضايا التي حظيت بالاهتمام من قبل هذا القانون من بين العديد من القضايا الأخرى؛ بهدف تحقيق الاستخدام الهادف لهذه التقنيات بما ينفع الحياة البشرية ولا يقوض من حقوق الأفراد، ويحسن من مستوى العديد من الخدمات، فضلًا عن دفع عجلة الابتكار في هذا المجال بما يحقق جدارتها بالثقة.

٢. تقنيات المعلومات وقضية خصوصية البيانات:

دفعت التطورات التقنية المتسارعة إلى تسليط الضوء على قضية خصوصية بيانات المستخدم وتخصيص المزيد من الاهتمام بها، خاصة بعد تطور وشيوع الاعتماد على شبكة الإنترنت في العديد من مناحي الحياة ومجالات العمل والخدمات المختلفة؛ حيث كان الغرض من تلك التطورات تحسين مستوى الخدمات وإدخال الميزات للعديد من العمليات والخدمات، وتعزيز القيمة المضافة لها، لكن ذلك لن يتأتى إلا بحصول هذه التقنيات على القدر الكافي من المعلومات التي تؤهلها إلى تقديم خدمات أكثر ملاءمة للمستخدم، فضلًا عن معالجتها واختزانها والإفادة منها ومشاركتها، والتي يمكن أن تتم مع أطراف ثالثة، وعلى الرغم من أن ذلك يتم لأغراض هادفة ويجلب النفع لمستخدمها، ويدفع الكثير من مواطن الخطر المحتملة كمكافحة الإرهاب والجرائم الخطيرة، فإن ذلك يشكل تهديدًا ويُخشى من إساءة استخدام ما جُمِع وعُولِج من بيانات، فضلًا عن احتمالية حدوث الأخطاء الواردة من قبل هذه التقنيات كحالات الخطأ في التحقق من الهوية، وعمليات المضاهاة غير الدقيقة والمزيفة، وعدم صحة بعض الاستدلالات والاستنتاجات التي تتم بطرق آلية، بالإضافة إلى التعامل مع الشكوك على أنها مسلمات، فضلًا عن الانتهاكات الأمنية واردة الحدوث (لويد، إيان جيه، ٢٠١٧، ص ٢١-٢٢) (عذراء ياسر وحسين عبد الصاحب عبد الكريم، ٢٠٢٣).

وفي ظل التطور المستمر فائق السرعة لثورة تقنيات المعلومات، لم يعد هناك حاجة لوسائل التجسس التقليدية والقيام بالاستجوابات المرهقة للتعرف على أدق تفاصيل أنشطة الأفراد؛ إذ يسرت هذه التقنيات التعرف على هذه التفاصيل دون أدنى مجهود، حيث يكفي الاعتماد على الكميات الهائلة من المعلومات المخزنة في قواعد وبنوك المعلومات وخوادم الشركات ومقدمي الخدمات المختلفة، مما يشكل عددًا من التداعيات غير المرحب بها وعلى رأسها انتهاك خصوصية الأفراد (لويد، إيان جيه،٢٠١٧، ص ٢٢).

١,٢ جهات وآليات تجميع بيانات المستخدم لشبكة الإنترنت.

تتعدد مجالات تجميع بيانات المستخدم لشبكة الإنترنت وخدماتها المختلفة لتتضمن الجهات والآليات التالية:

أ. مزودي خدمة الإنترنت Internet Service Providers (ISPs):

عن طريق رقم بروتوكول الإنترنت الخاص بالمستخدم Internet Protocol (IP) Address، يستطيع مزود خدمة الإنترنت تحديد موقع المستخدم، ووقت تصفحه لشبكة الإنترنت، والمواقع التي زارها، ونظام التشغيل والمواصفات المادية للحاسب الآلي الخاص

بالمستخدم، وغيرها من البيانات الأخرى.

ب. مواقع الإنترنت:

تعتمد على العديد من الأدوات والآليات لتجميع البيانات عن المستخدم كملفات الارتباط، والتي تعرف بملفات الكوكيز Cookies Files، وسجلات الخادم Server Logs، وغيرها، والتي تهدف إلى تجميع مختلف البيانات عن المستخدم كالمتصفح الذي يعتمد عليه في عملية التصفح، والذي يفضي بطبيعة الحال إلى معرفة عنوان البريد الإلكتروني للمستخدم، نوع الجهاز الخاص بالمستخدم، تتبع حركته وبصمته الرقمية بالمواقع التي زارها والصفحات التي ولجها، الروابط الفائقة التي نُقِرَ عليها، والمدد الزمنية التي قُضِيَت بالموقع، والأشياء التي بُحِثَ عنها بمحركات البحث المختلفة، وأسماء المحركات المستخدمة في عملية البحث، والغرض من كل ما سبق تتبع حركة المرور على الموقع ورصد سلوك المستخدم.

هذا بالإضافة إلى تقنيات التنقيب عن البيانات Data Mining، والتي تستخدم من قبل العديد من مواقع الإنترنت ومقدمي الخدمات الإلكترونية، والتي تهدف إلى استخراج الأنماط من بيانات المستخدمين، والتي تُوصِل إليها عن طريق ملفات الكوكيز، فضلًا عن البيانات المتعلقة بالمستخدم والتي تُتَبَادل عن طريق الشبكات المختلفة، مما ينتج عنه استكشاف حقائق جديدة عن الأشخاص. (Tavani, H. T. , 2007)

ج. مخترقو الإنترنت Internet Hackers:

وما يقومون به من استغلال لبعض الثغرات الأمنية بالبرامج وأجهزة الحاسب الآلي لتحقيق الدخول غير المسموح به للنظم وتجميع المعلومات عن المستخدم، والذي يتحقق عن طريق بعض الروابط المزيفة التي تؤدي إلى حدوث عملية الاختراق والتي يمكن إرسالها للمستخدم، أو من خلال بعض البرمجيات التي تيسر من هذه العملية، وقد يؤدي ذلك إلى التجسس على المستخدم، أو العبث ببياناته المخزنة على حاسبه الشخصي، أو تحقيق الابتزاز والنصب والسرقات المالية أو المعلوماتية.

د. بعض فيروسات الحاسب الآلي:

يمكنها القيام بعمليات التطفل على المستخدم وبياناته الخاصة، مثل فيروس حصان طروادة Trojan Horse Virus والذي يمنح المتسللين الوصول عن بعد إلى أجهزة الحاسبات الآلية المصابة، مما قد يؤدي إلى التجسس وسرقة البيانات وسرقة الهوية.

هـ. استمارات تجميع البيانات Web Forms:

تتيح الفرصة للمستخدم لإدخال بياناته الخاصة به من أجل الاشتراك في خدمة ما، أو القيام بإحدى عمليات الشراء الإلكتروني، أو من أجل إنشاء حساب للمستخدم على الموقع User Account، أو إنشاء بريد إلكتروني جديد، وتشبه النماذج الورقية التي يقوم المستخدم بملئها وإدخال البيانات بها، ولكنها عبارة عن صفحة إلكترونية تفاعلية مكتوبة بإحدى لغات العنكبوتية العالمية World Wide Web (منى تركي الموسوي، جان سيريل فضل الله، ٢٠١٣) (عائشة بن قارة، ٢٠١٧).

2.2 سياسات خصوصية البيانات ودورها بمواقع الإنترنت:

لقد تنوعت وسائل الحد من مخاطر عمليات تجميع البيانات فيما بين الوسائل التقنية، والتي من بينها تقنيات تشفير البيانات، وأدوات إخفاء هوية المستخدم، وبرامج الحماية من الفيروسات والتجسس وغيرها (وفاء حميد، ٢٠١٨)، إلى جانب التشريعات التي تم سنها لتقنين هذه العمليات وتحجيم مخاطرها، وكان من بين هذه الوسائل ما يُعَرف بسياسات خصوصية البيانات، أو سياسات خصوصية المستخدم User Privacy Policies، والتي أصبحت إحدى أدوات حماية بيانات المستخدم، وإحدى المكونات الأساسية واجبة الحضور بمواقع الإنترنت وتطبيقات الهواتف الذكية ومواقع التواصل الاجتماعي.

وتعد سياسات الخصوصية بمثابة اتفاقيات بين مطوري التطبيقات ومقدمي الخدمات الإلكترونية ومواقع الإنترنت وبين المستخدمين لهذه الخدمات والمواقع والمنتفعين منها؛ حيث يُعلَن من خلالها عن الممارسات التي ستتم في التعامل مع البيانات، وتعتبر أساسًا لحل المنازعات في حالة حدوث اختراق للبيانات؛ لذا يشترط فيها صياغتها بوضوح وبطريقة تبتعد تمامًا عن الغموض واللبس (Yan, C. et al, 2024).

فعلى الرغم من أهميتها، تشكل التحديات المتعلقة بصعوبة قراءتها وفهمها وتفسير بنودها خاصة التشريعية منها، ويعتبر طول محتوى هذه السياسات عائقًا يؤدي إلى عدم قراءة المستخدمين لها، والقيام بالموافقة على بنودها وعلى إجراءاتها التي تتضمنها للتعامل مع البيانات دون الاطلاع عليها، ويمثل ذلك إحدى العقبات الأساسية لتحقيق مغزاها وفعاليتها (Wagner, I. ,2023)، وقد عبر عن هذه العقبة Bartlett, M. في دراسته عام ٢٠٢١ من واقع إحدى الدراسات التجريبية، بأن ٥٤٣ مشاركًا ممن تمت عليهم الدراسة طُلب منهم الانضمام إلى خدمة جديدة عبر الإنترنت، وقد أمضوا في المتوسط ما يقرب من ١٤ ثانية لقراءة الشروط والأحكام المدرجة بسياسة خصوصية الموقع، في حين ذكر

الباحثون أن هذه السياسة تتطلب ٤٥ دقيقة على الأقل من القراءة لفهمها بشكل كافٍ.

٣. خصوصية البيانات في عصر الذكاء الاصطناعي:

مع التطورات غير المسبوقة لتقنيات وخدمات الذكاء الاصطناعي، وما تقوم به من عمليات تجميع هائلة لكم ضخم من البيانات عن المستخدم، وسلوكه، وهواياته، ومهاراته، ومشاعره وغير ذلك، تفاقمت حدة مشكلة خصوصية البيانات، الأمر الذي جعلها ضمن أبرز المخاوف والقضايا الأخلاقية الشائكة ومسالب الذكاء الاصطناعي المنتسبة إليه، على الرغم مما أضافه من ميزات وتيسير للعديد من العمليات على مستوى الكثير من الخدمات في جميع مناحي الحياة المختلفة، الأمر الذي زاد الوضع تعقيدًا، فضلًا عن تطور هذه التقنيات بمعدلات فائقة السرعة، مما يعدد من تنوع صور التحديات المتعلقة بها، وخاصة ما يتعلق منها بصور انتهاك خصوصية البيانات، ويتزامن ذلك في ظل الافتقار الشديد إلى ما ينظم استخدام هذه التقنيات من تشريعات وقوانين مخصصة وموجهة إلى هذا المجال (عبد الرازق عبد الكريم، ٢٠٢٤).

١,٣ تقنيات وأدوات تجميع البيانات في ظل الذكاء الاصطناعي وأغراض ذلك:

أ. تقنيات وأدوات تجميع البيانات:

تعتمد نظم الذكاء الاصطناعي على عدد من الآليات والتقنيات للقيام بعملية تجميع البيانات عن المستخدم لها، منها ما سبقت الإشارة إليه من قبل، ومنها ما ارتبط بتطور هذه النظم كتقنيات المحادثة الآلية Chatbot، وتقنية التعرف على الأوجه، وتقنيات التعرف على الأصوات، وتطبيقات إنترنت الأشياء IOT، ونظم تحديد المواقع العالمي GPS، وشبكات الواي فاي Wi-Fi، بالإضافة إلى عدد من الآليات الأخرى كسلوكه في البحث عن المعلومات وتصفح المواقع المختلفة، والتعبير عن إعجابه ببعض المنشورات على وسائل التواصل الاجتماعي، وفئات الموضوعات التي تحظى باهتمامه والتي تعرف عن طريق فترة مكوثه على الصفحة التي تعرضها، فضلًا عن سرعة التصفح وعرض الصفحات والمرور على ما ينشر بها Scrolling Speed، وذلك كله بدون علم من المستخدم بما يُجَمَّع عنه وبطرق ضمنية غير مباشرة، وتُخَزَّن بيانات المستخدم التي جُمِعَت بواسطة خدمات الحوسبة السحابية Cloud Computing، والتي يكمن أحد أوجه مخاطرها في ضمانات الحماية والأمن للبيانات المخزنة بها، إلى جانب إمكانيات مشاركة البيانات مع أطراف أخرى (عبد الله شيباني، وداد بن سالم، ٢٠٢٣) (United Nations Educational, Educational Scientific and Cultural Organization, 2021).

ب. أغراض تجميع البيانات من قبل تقنيات الذكاء الاصطناعي:

وتتنوع أغراض عملية تجميع البيانات من قبل هذه التقنيات ما بين قيامها بعملية التعلم الآلي وتحسين جودة وفعالية عملية التعلم، فضلًا عن تحسين جودة ما تقدمه من خدمات، والمساعدة في دعم اتخاذ القرارات بالنسبة لمستخدمها، أيضًا دعم عمليات المعالجة والتحليل والتي لن تتم بكفاءة مرتفعة إلا إذا توافر قدر كبير من البيانات؛ وذلك من أجل التعرف على ميول المستخدم واحتياجاته الحالية، والقدرة على التنبؤ باهتماماته وميوله المستقبلية، هذا إلى جانب الأغراض التجارية والتسويقية لتحقيق أعلى عائد من الأرباح؛ حيث أصبحت بيانات المستخدمين موردًا اقتصاديًّا تتسابق العديد من الجهات التجارية وجهات الدعاية والإعلان على الحصول عليها بمختلف الطرق حتى وإن خالفت القانون، مما يعد انتهاكًا واضحا لخصوصية البيانات (عبد الله شيباني، وداد بن سالم، ٢٠٢٣).

٢,٣ صور انتهاك خصوصية البيانات في عصر الذكاء الاصطناعي.

وتتنوع صور انتهاك خصوصية البيانات في ظل استخدام هذه التقنيات ليُذكر منها: (مهرة سليمان، ٢٠٢٤):

أ. التجسس والتنصت:

هاتان العمليتان اللتان تتحققان عن طريق كلٍّ من المراقبة المستمرة، وبرامج التتبع؛ حيث تنطوي العديد من تطبيقات الذكاء الاصطناعي المختلفة وما تقدمه من خدمات على بعض الإمكانات التي تحمل في طياتها مراقبة مستمرة وتتبع لمستخدمها، كتطبيقات المساعد الرقمي الشخصي كإحدى تلك الخدمات الذكية، والتي يمكنها أن تبقى على علم دائم بتحركات المستخدم، وتفضيلاته، وما يقوم بالبحث عنه، ومواعيده المهمة، وغيرها من تفصيلات الحياة الشخصية الأخرى ذات الأهمية بالنسبة لمستخدمها، وتقوم هذه التطبيقات باختزان كل هذه المعلومات، ومن ثم القيام بمعالجتها وتحليلها لتكوين رؤى عن المستخدم والتنبؤ بسلوكياته المستقبلية المحتملة.

ب. التعرف على الأوجه بدون علم المستخدم:

ويظهر ذلك في عمليات المراقبة لتحقيق الأمن في بعض الأماكن، خاصة باستخدام خوارزميات رؤية الحاسب الآلي (CV) Computer Vision بدون علم من جانب يُصوَّرون، ويتفاقم الأمر إذا أسيء استخدام هذه البيانات أو مشاركتها مع أطراف خارجية أو بيعها لأطراف ثالثة، الأمر الذي قد ينطوي على انتهاكات صارخة لحقوق وخصوصية المستخدم.

وللحد من ذلك قامت مؤسسة الخصوصية الدولية Privacy International بإطلاق حملة للحفاظ على الخصوصية في الأماكن العامة بعنوان The End of Privacy in Public في يونيو عام ٢٠٢٣، كان الغرض منها تقويض استخدام تقنية التعرف على الأوجه في الأماكن والطرق العامة، مما له الأثر على خصوصية المواطنين ومراقبتهم (Privacy International, November 2023).

جـ. جمع البيانات واستخدامها لغير الأغراض التي جُمِعَت من أجلها وبدون موافقة المستخدم:

أظهرت تقنيات الذكاء الاصطناعي تفوقًا في عمليات جمع البيانات على اختلاف فئات هذه البيانات وأشكالها؛ نتيجة لاندماج تطبيقاته وتداخلها في مختلف المجالات، سواء كانت هذه البيانات بيانات شخصية، أو بيانات تفضيلات المستخدم، أو بيانات الأماكن التي يتردد عليها، أو بيانات القياسات الحيوية، حتى أنها برعت في تجميع البيانات عن الحالة المزاجية الخاصة به نتيجة لقيامها بتحليل مشاعر المستخدم، الأمر الذي كفل لها القدرة على انتهاك الخصوصية بفئاتها المختلفة، والتي سبقت الإشارة إليها من قبل؛ حيث بلغت قدرات الذكاء الاصطناعي مستوى غير مسبوق من تجميع البيانات على اختلاف فئاتها فضلًا عن عمق وضخامة هذا التجميع، تحديدًا تلك التي لم تحظَ من قبل بعمليات التجميع كالمشاعر على سبيل المثال.

ولم يتوقف الأمر على القيام بعمليات تجميع البيانات من المستخدم، بل تطورت إمكانيات الذكاء الاصطناعي إلى القدرة على التنبؤ بالبيانات التي لم يدلِ بها المستخدم، فضلًا عن قدرته على عملية مراقبة الأفكار قبل الإفصاح عنها، وتوقع السلوكيات قبل حدوثها، تلك الإمكانية التي أفضت تقنيات تعلم الآلة Machine Learning (ML) إليها فيما يعرف بالتحليلات التنبؤية Predictive Analytics، والتي ينتج عنها القدرة على التنبؤ بالمعلومات الشخصية غير المعروفة، والتي لم يفصح عنها المستخدم، تلك القضية التي لم يتم تغطيتها حتى الآن في اللائحة العامة لحماية البيانات (GDPR)، والتي تعرف بالخصوصية التنبؤية Predictive Privacy.(Mühlhoff, R. 2023) .

٣,٣ المبادئ الأخلاقية للحد من مسالب الذكاء الاصطناعي ذات العلاقة بالخصوصية:

نهضت العديد من المنظمات الدولية والحكومات بالإسراع من عملية إصدار المواثيق والمبادئ الأخلاقية للذكاء الاصطناعي، فضلًا عن شروع العديد من الدول إلى إصدار التشريعات والقوانين المنظمة لاستخدام تقنيات الذكاء الاصطناعي بما لا يتنافى مع القيم

والمبادئ الإنسانية، وبما يُؤَمِّن استخدام هذه التقنيات؛ تفاديًا لما تنطوي عليه من تحديات متنوعة، وقد تنوعت المبادئ التي وردت بهذه المواثيق لتشمل:

أ.السلامة والأمن: عن طريق درء الأضرار ومواطن الضعف التي يمكن أن تؤدي إلى تعرض أنظمة الذكاء الاصطناعي للاختراق، وذلك طوال دورة ومراحل تطويرها، أيضًا العمل على وضع الأطر المستدامة لأمن وسلامة البيانات بما يحقق خصوصيتها، مما ينتج عنه أمن وسلامة البشر نتيجة نهائية.

ب. الحق في الخصوصية وحماية البيانات: ينبغي مراعاة جانب خصوصية البيانات طوال مراحل تطوير ودورة حياة أنظمة الذكاء الاصطناعي، وأن تتم عمليات التجميع، والمعالجة، والتحليل، والاختزان، والمشاركة للبيانات، وحذفها والتخلص منها، بما يتوافق والقوانين والتشريعات المعمول بها وطنيًّا وإقليميًّا ودوليًّا، هذا فضلًا عن عمليات المتابعة والتقييم المستمر لهذه الأنظمة طوال فترة عملها للتأكد من حمايتها لخصوصية البيانات، كما يجب أن تكون عملية تجميع البيانات بهذه الأنظمة في حدها الأدنى.

جـ. الشفافية والقابلية للشرح: ذلك المبدأ المنوط بإعلام مستخدمي أنظمة الذكاء الاصطناعي بكيفية عمل خوارزمياته، والقرارات التي تُؤخَذ تجاه المستخدم بناءً على معلوماته الشخصية، خاصة القرارات التي تمس حقوق الإنسان، وانطلاقًا من هذا المبدأ يحق للمستخدم طلب المعلومات التوضيحية حول هذه القرارات، وإعادة النظر فيها وتصحيحها.

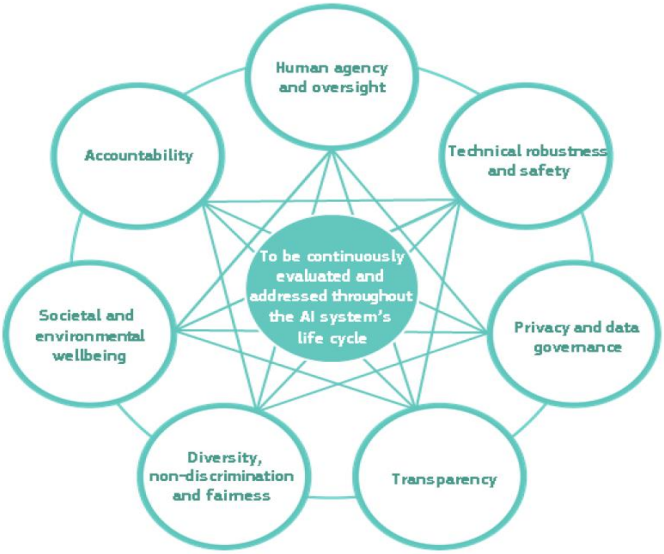
د. الحوكمة وسُبل التعاون متعددة الأطراف والقابلة للتكيف: وينص على ضرورة احترام القانون الدولي والسيادة الوطنية عند استخدام ومعالجة البيانات، حيث يمكن للدول المختلفة وفقًا لأحكام هذا القانون أن تتولى عملية تنظيم البيانات المنتجة في أراضيها أو بخارجها، بما يحقق حماية هذه البيانات وخصوصيتها.

هـ. المسئولية والمساءلة: وتختص بمسؤولية الجهات المطورة لنظم وتقنيات الذكاء الاصطناعي عن تحقيق حماية المستخدم والحفاظ على حقوقه وفقًا لما تنص عليه القوانين والمواثيق الدولية لحماية حقوق الإنسان، فضلًا عن مسؤوليتها عن تقييم ومتابعة عمل هذه النظم بصفة دورية مستمرة؛ للتأكد من عدم مخالفتها للقواعد المتبعة لحماية حقوق الإنسان ومعايير تحقيق ذلك، إلى جانب التوعية بمخاطر هذه التقنيات وتوعية المستخدم والمجتمع بأسره بحقوقه وخصوصيته.

(United Nations Educational, Scientific and Cultural Organization,2021)

٤,٣ الذكاء الاصطناعي الجدير بالثقة Trustworthy AI:

حددت المفوضية الأوروبية European Commission مجموعة من المبادئ التوجيهية لأنظمة الذكاء الاصطناعي بلغت ٧ مبادئ رئيسة؛ حتى تُعتَبَر نظمًا جديرة بالثقة، وتحظى جميع هذه المبادئ بالقدر نفسه من الأهمية ويدعم كل منهم الآخر، ويتحتم تنفيذها ومتابعة حضورها طوال دورة حياة نظام الذكاء الاصطناعي. يعكس الشكل (١) المبادئ التوجيهية للذكاء الاصطناعي الجدير بالثقة.



شكل (١)

المبادئ التوجيهية للذكاء الاصطناعي الجدير بالثقة (European Commission, 2019)

ويلاحظ أن من بين هذه المبادئ جاءت خصوصية البيانات لتعكس محورًا مهمًا ليتسم الذكاء الاصطناعي بالثقة، فأصبح من الضروري عمل هذه الأنظمة على توفير المقومات التي تعمل على تحقيق الخصوصية، وأن تضمن توافر الآليات المنوطة بحوكمة البيانات، والتي تتحقق عن طريق ما يضمن أمن البيانات وخصوصيتها ودقتها وتوافرها وإمكانية استخدامها بما لا يتعارض مع القوانين والتشريعات المعمول بها في هذا الشأن، وضمان الوصول المشروع إليها (European Commission, 2019).

ويعزز من هذه الثقة قيام المؤسسات التي تتبنى أنظمة الذكاء الاصطناعي في عملها وتقديم خدماتها بتطوير فئة مستحدثة من السياسات التي تحكم وتنظم عمل هذه الأنظمة، عرفت هذه السياسات بسياسات الذكاء الاصطناعيAI Policy؛ حيث شرعت العديد من

المؤسسات والهيئات المطبقة لتقنيات وأنظمة الذكاء الاصطناعي بنشر سياستها المتعلقة بهذه التقنيات من حيث مجالات عملها، والبروتوكولات والضوابط التي تحكمها، ومنها المبادئ الأخلاقية التي تحكم عمل هذه الأنظمة مثل الشفافية والمساءلة والإنصاف وخصوصية البيانات وحمايتها، والتوازن الذي ينبغي تحقيقه والمنوط بالتدخل البشري في مراجعة مخرجات ونتائج المعالجة التي تقوم بها هذه النظم قبل استخدام هذه المخرجات والاعتماد عليها.

وتعد سياسة الذكاء الاصطناعي عنصرًا أساسيًا في ضمان النهج الناجح للذكاء الاصطناعي، ويأتي ذلك مع انتشار استخدام الذكاء الاصطناعي وتطبيقاته على نطاق واسع، لتصبح سياسة الذكاء الاصطناعي جزءًا من إطار الحوكمة الذي تعمل به أي منظمة، كما أنها أصبحت جزءًا لا يتجزأ من العصر الجديد الذي نشهده.

وفي أحد التقارير السنوية للقيادة الرقمية[٤]، تم استطلاع آراء قادة التكنولوجيا في جميع أنحاء العالم، واستكشاف الوضع الراهن فيما يتعلق بسياسات الذكاء الاصطناعي وحوكمة إجراءاته وعملياته، فكانت واحدة فقط من كل خمس مؤسسات لديها سياسة للذكاء الاصطناعي، وبمرور الوقت أظهرت النتائج الخاصة باستطلاع Pulse لقادة التكنولوجيا تضاعف هذه النسبة لتصل إلى ٤٢٪، كما يخطط ٣٨٪ من المؤسسات إلى إنشاء واحدة (Nash Tech., June 26, 2024).

٥,٣ آليات الحفاظ على الخصوصية في عصر الذكاء الاصطناعي:

اهتمت الكثير من الدراسات برصد آليات تحقيق خصوصية الأفراد وحماية بياناتهم في ظل التهديدات والمخاطر التي حملتها التطورات التقنية الحديثة للذكاء الاصطناعي، وبرصد هذه الآليات والطرق التي وردت بهذه الدراسات تحددت في المزج بين الجانب التشريعي والأخلاقي، والجانب التقني كتشفير البياناتData Encryption ، والتشويش عليهاData Obfuscation ، بالإضافة إلى تقنيات إخفاء هوية البياناتData Anonymization ، ويعتبر المزج بين كل من الجانبين النهج الشامل لضمان الأمن والخصوصية والامتثال الأخلاقي عند تطبيق هذه التقنيات (Villegas-Ch, W., & García-Ortiz, J) . (٢٠٢٣).(Zhu, T., et al, 2022) .

أ. الخصوصية التفاضلية Differential Privacy:

ومن ضمن التقنيات التي يعتمد عليها للحفاظ على خصوصية البيانات خاصة البيانات

(٤) قدم هذا التقرير مجموعة من الخبراء في مجال التكنولوجيا والحلول الذكية، وتعرف مؤسستهم باسم Nash Tec. https://www.nashtechglobal.com/about-us /

الشخصية عالية الحساسية ما يعرف بتقنية الخصوصية التفاضلية Differential Privacy، والمنوطة بإخفاء هوية البيانات والتشويش عليها أثناء معالجتها بتقنيات الذكاء الاصطناعي، تحديدًا تقنية تعلم الآلة، فتتم عمليات التعلم الآلي من البيانات المستخدمة وتحقيق الفائدة المرجوة منها دون التأثير على خصوصية البيانات ومعرفة إلى أي شخص تنتمي (Al-Rubaie, M., & Chang, J. M., 2019).

ب. المشاركة السرية Secure Sharing:

هذا إلى جانب أساليب المشاركة السرية للبيانات Secure Sharing، والتي تعتمد على تجزئة البيانات التي ستُشَارك بين عدة أطراف ستتولى عملية المعالجة، وحين انتهاء كل طرف من عملية معالجة الجزء الخاص به، تُجمَّع النواتج الجزئية لهذه المعالجات وتُدمَّج معًا للحصول على النتيجة النهائية، وتعد هذه الطريقة أكثر كفاءة من الطرق التي تعتمد على تشفير البيانات عند معالجتها بواسطة تقنيات تعلم الآلة(Al-Rubaie, M., & Chang, J. M., 2019) .

جـ. المعالجات الآمنة Secure Processors:

أيضًا الاعتماد على المعالجات الآمنة Secure Processors، والتي تضمن سلامة وسرية العمليات البرمجية من الوصول غير المصرح به بواسطة البرامج غير الموثوقة مما يحافظ على خصوصية البيانات أثناء عمليات المعالجة بواسطة تقنيات تعلم الآلة، وتؤدي الخصوصية التفاضلية، والمشاركة السرية، والمعالجة الآمنة إلى ما يعرف بتعلم الآلة المحافظ على الخصوصية (Al- Privacy-Preserving Machine Learning (PPML) Rubaie, M., & Chang, J. M., 2019).

د. تقييم تأثير الخصوصية Privacy Impact Assessment (PIA).

تعد من الإجراءات المتخذة لتقييم تأثير تقنيات الذكاء الاصطناعي وما تقوم به من معالجات وتحليلات على خصوصية البيانات؛ وذلك لتحديد وتخفيف هذه المخاطر، وتنفيذ الإجراءات اللازمة لمعالجتها، ويتم ذلك قبل البدء في عملية المعالجة للبيانات بواسطة هذه التقنيات، وجدير بالذكر أنها أحد البنود التي نصت عليها اللائحة العامة لحماية البيانات، ولكن تستخدم باعتبارها أحد الإجراءات لحماية خصوصية البيانات في ظل استخدام الذكاء الاصطناعي. (Intersoft Consulting, n.d) (Edwin Frank, 2024).

هـ. الخصوصية بالتصميم Privacy by Design:

وتعرف أيضا بالخصوصية بوصفها وضعًا افتراضيًّا Privacy by Default، وتعني مراعاة

جوانب الخصوصية أثناء تصميم وتطوير النظم منذ البداية، وقد عُبِرَ عن الأفكار الأولى لها في السبعينيات من القرن الماضي، ودُمِجَت في التسعينيات في توجيه حماية البيانات RL 95/46/EC، والذي ينص على ضرورة اتخاذ التدابير الفنية والتنظيمية في وقت التخطيط والتصميم لنظام معالجة البيانات لضمان الحماية والسلامة (Intersoft Consulting, n.d).

و. استخدام تقنيات الذكاء الاصطناعي بما يحقق خصوصية المستخدم.

- التغلب على مشكلة قراءة وفهم سياسات الخصوصية.

على الرغم من التهديدات التي تسبب فيها الذكاء الاصطناعي لقضية الخصوصية، فإنه يقدم حلولا لمعالجة بعض جوانب هذه القضية كنوع من المساعدة على تحقيقها؛ حيث ظهرت العديد من الأدوات والحلول الذكية التي تعتمد فكرة عملها على تيسير عملية قراءة وفهم سياسات خصوصية البيانات وتحليل عناصرها وتقييمها؛ للتعرف على مدى الحماية التي تقدمها لبيانات المستخدم وخصوصيته، وذلك بالاعتماد على عدد من التقنيات المرتبطة به، وعلى رأسها تعلم الآلة (ML)، ومعالجة اللغة الطبيعية (NLP) بوصفها تقنية أساس لقراءة وفهم وتحليل سياسات خصوصية البيانات (Bui, D. et al, 2021).

ومن أشهر هذه الأدوات تطبيق Privacy Policy Beautifier[٥]، الذي يعتمد على تقنية (NLP) لتمييز نصوص سياسات خصوصية البيانات، وتلخيص محتواها، ومدى التزام السياسات بعناصر اللائحة العامة للبيانات (GDPR)، وتمثيل النتائج عن طريق الرسوم البيانية وسحب الكلمات Word Clouds..(Kaili, M., & Kapitsaki, G. M., 2022)

إلى جانب ذلك قدمت أداة PrivacyCheckV3 نموذجًا لتقنيات تعزيز الخصوصية Privacy Enhancement Technologies (PET)، فبالإضافة إلى إعلام المستخدم ببنود الخصوصية وتحليلها وتعزيز فهم محتواها، تعمل هذه الأداة على البحث عن والعثور على المنافسين الأفضل من حيث الممارسات المتعلقة بخصوصية البيانات والمفاضلة بينهم، فضلًا عن المتابعة للتغييرات التي تطرأ على سياسات الخصوصية التي وافق عليها المستخدم وإخطاره بها، وتعتمد هذه الأداة في عملها على خوارزميات تعلم الآلة (Nokhbeh Zaeem. et al, 2022) .

- **تقييم جدارة نظم الذكاء الاصطناعي بالثقة:**

أيضًا الاعتماد على بعض خوارزميات الذكاء الاصطناعي لتقييم الأنظمة التي تعتمد عليه في عملها؛ للتعرف على مدى الثقة فيها وفي مراعاة جوانب خصوصية البيانات في تصميمها،

(5) https://34ml.com/ar-beautifier-privacy-policy/

ومن أشهر هذه الخوارزميات خوارزمية Entropy (Mylrea, M., & Robinson, N., 2023).

فاستخدام الذكاء الاصطناعي في هذا المجال يفضي إلى تنمية وعي المستخدمين بقضية الخصوصية، والتغلب على بعض مشكلاتها كالمشكلة التي تتعلق بسياسات خصوصية البيانات من صعوبة قراءة وفهم وطول محتواها، مما يساعد المستخدم على قراءتها، فضلًا عن تحقيق الحماية المسبقة لخصوصية البيانات بتقييم هذه النظم والتحقق من مدى جدارتها بالثقة.

بعد استعراض الآليات والتقنيات المتنوعة لحماية الخصوصية في عصر الذكاء الاصطناعي، يمكن القول بأن مطلب حماية البيانات وخصوصية الأفراد لا يعد مبدأ إنسانيًا وحقوقيًا يُلزِم به القانون فحسب، بل يمكن اعتباره ميزة تنافسية لهذه النظم، تستطيع من خلاله التنافس فيما بين غيرها من النظم الأخرى بوصفها إحدى الميزات التي تقدمها لمستخدميها.

٤. خصوصية البيانات في مجال المكتبات:

حظيت الخصوصية باهتمام متزايد من قبل مجال المكتبات ومؤسسات المعلومات كغيرها من المجالات الأخرى الخدمية كمجال الخدمات الصحية، والخدمات الحكومية في عصر تقنيات المعلومات علاوة على عصر الذكاء الاصطناعي، حيث تتوقف جودة ما تقدمه هذه المجالات من خدمات على مدى توافر البيانات وكفاءة عملية إدارتها، تلك الخدمات التي تقوم بتخزين الكميات الضخمة من سجلات العملاء والمواطنين، والتي تتضمن بياناتهم الشخصية والتي يمكن أن ترقى لمرتبة البيانات الحساسة، واهتماماتهم، والأنشطة التي قاموا بها وميولهم الشخصية، ومع توافر الإمكانيات الهائلة لمعالجة وتحليل هذه البيانات فضلًا عن إمكانيات النقل والمشاركة لها في غضون ثوان معدودة، فقد هدد ذلك بطريقة مباشرة خصوصية هذه البيانات خاصة مع تزايد أعداد عمليات اختراق البيانات، مما كان له بالغ الأثر على عمل هذه الخدمات ومؤسساتها، وعلى حياتنا الخاصة وأعمالنا بشكل عام (منى تركي الموسوي، جان سيريل فضل الله، ٢٠١٣).

وتنهض المكتبات بعمليات تجميع بيانات المستفيدين؛ ليتسنى لها تقديم الخدمات التي تلبي احتياجاتهم على أكمل وجه بما يتوافق واهتماماتهم، بالإضافة إلى تقديمها لهذه الخدمات بأسرع الطرق، مما يدفعها إلى جعل عملية الحصول على بيانات المستفيد شرطًا أساسًا للاشتراك في المكتبة وخدماتها، كما تتولى إنشاء ملفات تعريف لهم بالنظام الآلي لإدارة المكتبة (إيمان عبد الحميد يس، أماني محمد السيد، ٢٠٢٢).

فالمكتبة بما تقدمه من خدمات ومصادر معلومات موطن لمعرفة الاتجاهات الفكرية للقراء والمستفيدين، فضلًا عن الاهتمامات الموضوعية وما يتطلع المستفيد إليه من أجل تنمية وعيه وثقافته ووقع ذلك على تشكيل رصيده المعرفي، بما يحتم على المكتبة توفير الحماية اللازمة لهذه البيانات التي تمس بصفة أساسية شخص المستفيد، وتقع في نطاق خصوصيته (ندا مصطفى لبيب، ٢٠٢٣، ص٥٧).

الأمر الذي دفع المنظمات والمؤسسات الدولية في مجال المكتبات ومؤسسات المعلومات إلى إصدار المواثيق الأخلاقية والبيانات الإعلامية، التي تحث على المحافظة على خصوصية بيانات المستفيدين وحمايتها، على اعتبار أن المكتبات ومؤسسات المعلومات هي أكثر الجهات التي يفترض أنها تحقق أقصى درجات الحماية لما تختزنه عن المستفيدين من بيانات، حتى بلغ الأمر اعتبار هذه البيانات سرية (International Federation of Library Associations and Institutions ,2015) (محمد فتحي عبد الهادي و نجلاء محمود خليل، ٢٠١٤).

١,٤ مجالات تجميع بيانات المستخدم داخل المكتبات:

تعد المكتبات وسجلاتها سواء الورقية أو الإلكترونية مصدرًا ضخمًا لبيانات المستفيدين، ويمكن قصدها لمعرفة العديد من المعلومات عن شخص ما، وتحديدًا ما يعتقده وخليفته الفكرية والموضوعية، والتي تشكل جزءًا كبيرًا من دوافعه وسلوكه الشخصي، وهنا يكمن موطن خصوصية المستفيد، والتي تلعب دورًا مهمًا في تشكيل العلاقة بين المستفيدين والمكتبة وخاصة ما يتعلق بجانب الثقة في هذه العلاقة، فضلًا عن تأثيرها على حرية الوصول إلى المعلومات من جانب المستفيدين، وتتعدد روافد تجميع بيانات المستفيدين من المكتبة لتتضمن:

أ. خدمات المعلومات المقدمة من جانب المكتبة وخاصة خدمة حجز الكتب، والاستعارة، والاطلاع الداخلي، وخدمة الإحاطة الجارية، والبث الانتقائي للمعلومات، وخدمة الإمداد بالوثائق، والخدمة المرجعية.

ب. البحث في المصادر الإلكترونية وقواعد البيانات التي تتيحها المكتبة سواء كان وصول المستفيد لها من داخل المكتبة أو من خارجها.

ج. عمليات التنقيب عن البيانات لمعرفة أنماط استفادة مجتمع المستفيدين من مصادر المعلومات بالمكتبة، وسلوكهم في البحث عن المعلومات؛ وذلك من أجل التنبؤ بالاحتياجات المستقبلية الخاصة بهم، والمساعدة في عمليات اتخاذ القرارات الاستراتيجية بالمكتبة.

د. بيانات والتبرع للمكتبة والدفع الإلكتروني. (فاطمة يحيى، ٢٠٢٠)

٢,٤ مجالات انتهاك خصوصية البيانات داخل المكتبات:

تتمثل المجالات الممكنة لانتهاك خصوصية بيانات المستفيدين داخل المكتبات ومراكز المعلومات فيما يلي:

أ. التعرف على ورصد العادات القرائية والميول المعرفية الخاصة بالمستفيدين.

ب.نشر قوائم المستعيرين، والتي تتضمن ربط الكتب المستعارة بمن استعاروها من المكتبة.

جـ. سلوك البحث عن المعلومات الخاص بالمستفيدين من قواعد بيانات المكتبة.

د. فترات تردد المستفيد على المكتبة والأوقات التي يقضيها فيها، ومواعيد دخوله وخروجه منها، والأماكن والقاعات التي يتردد عليها.

هـ. الأنشطة والفعاليات التي يحرص على الاشتراك فيها وعلاقاته الشخصية بمجتمع المستفيدين من المكتبة.

و. كاميرا مراقبة الأمن داخل المكتبات دون علم المستفيدين.

ز. القوائم الببليوجرافية الناتجة عن الخدمات المرجعية لخدمة مستفيد بعينه، فضلًا عن قوائم العلاج بالقراءة بالمكتبات التي تقدم هذا النوع من الخدمات (ندا مصطفى لبيب، ٢٠٢٣، ص٦٥-٧٣).

ح. ما يقوم به الموردون والناشرون من تتبع ومراقبة وتحليل لسلوك المستخدم وتجاربه في التعامل مع وقياس الاستخدام للمصادر الرقمية التي تشترك المكتبة فيها (Singley, E., 2020).

هذا إلى جانب تطبيق المكتبات للعديد من التقنيات الرقمية في كثير من عملياتها وخدماتها، والتي تؤثر تأثيرًا بالغًا على خصوصية المستفيدين كوسائل التخزين السحابية، والشبكات الداخلية للمكتبة والسماح للمستفيدين بالدخول عليها من حواسيبهم الخاصة، مما يزيد من احتمالات الانتهاك والاختراق لقواعد بيانات مجتمع المستفيدين من المكتبة إذا لم تتوافر تقنيات الحماية الملائمة (ندا مصطفى لبيب، ٢٠٢٣، ص٧٥).

٥. المكتبات وخصوصية البيانات والذكاء الاصطناعي:

لم تكن المكتبات ومؤسسات المعلومات بمنأى عن التطورات التقنية المعاصرة والتي يمثلها الذكاء الاصطناعي؛ حيث طالت هذه التقنيات مؤسسات المعلومات وأثرت في مجالات عملها، والعمليات التي تنهض بها، والخدمات التي تقدمها لمجتمع المستفيدين منها،

الأمر الذي أثار الانتباه إلى ضرورة الاهتمام بقضية خصوصية البيانات بوصفها إحدى القضايا المثارة على ساحة العمل على مستوى الجمعيات المهنية والمنظمات الدولية المعنية بمجال المكتبات ومؤسسات المعلومات في الوقت الراهن، فضلًا عن المكتبات نفسها والتي تسري فيها هذه القضية بتحدياتها على أرض الواقع.

بينما تُشَجَع المكتبات والمتاحف والأرشيفات والمعارض على استخدام الذكاء الاصطناعي؛ لإبراز مقتنياتها والارتقاء بمستوى خدماتها (UNESCO,2021)، تبادر المنظمات الدولية والجمعيات المهنية في مجال المكتبات بإصدار المواثيق والمنشورات المُنظِمة لاستخدام الذكاء الاصطناعي بمؤسسات المعلومات؛ للحد من مخاطره، والعمل على حسن استثماره (American library Association, 2019a)؛ حيث مثلت تطورات تقنيات الذكاء الاصطناعي الراهنة تعارضًا مع القيم الجوهرية للمكتبات، كالخصوصية وتجنب التحيز وانفتاح المستفيد تجاه الوصول للمعرفة دون ما يثير قلقه وارتيابه (Cox, A. 2024).

١,٥ تطور خدمات المكتبات وتأثيرها على خصوصية المستفيدين:

لعب الذكاء الاصطناعي دورًا جوهريًّا في تطور الخدمات المقدمة من جانب المكتبات؛ حيث أصبحت تُؤَّدى في ثوب جديد على الرغم من الحفاظ على فلسفتها ومفهوم ووظيفة كل خدمة منها، فإنها أصبحت تُؤدَّى بأكثر الطرق تلبية وتوافقًا وتكييفًا لاحتياجات المستفيدين من المكتبة، ومن أبرز الخدمات التي لحقت بها أوجه التطور، والتي بلا شك تؤثر على خصوصية المستفيد الخدمات التالية:

أ. خدمة الرد على استفسارات المستفيدين، والتي تعد أحد جوانب الخدمة المرجعية، والتي أصبحت تؤدَّى عن طريق تقنية المحادثة الآلية Chatbot.

ب. خدمة البث الانتقائي للمعلومات، والتوصية بمصادر المعلومات ذات الصلة باحتياجات المستخدم، والتي أصبحت تقدَّم عن طريق نظم التوصية Recommendation Systems، والتي استُخْدِمَت أيضًا في خدمة الإعارة.

جـ. التواصل مع المستفيدين والتفاعل معهم والرد على استفساراتهم واصطحابهم في الجولات الإرشادية عن طريق تقنية الروبوت المطبقة بالمكتبة (أمل حسين عبدالقادر، ٢٠٢٤).

د. تجارب التعلم التكيفية، والتي يسهل الذكاء الاصطناعي من توافرها داخل المكتبات من خلال تخصيص تجارب التعلم بناءً على تفاعلات المستخدم وأدائه، وتعمل هذه الأنظمة على ضبط توصيل المحتوى ومسارات التعلم لتتناسب مع أنماط التعلم

واحتياجات المستخدمين المتنوعة.(Soni, D., 2023).

هذا فضلًا عن عمليات دراسة سلوك المستفيدين، والذي تتولى خوارزميات تعلم الآلة الجانب الأكبر منه؛ لتقديم ما يتوافق مع احتياجات المستفيدين من خدمات، هذا إلى جانب تقييم ما تقدمه المكتبة من خدمات اعتمادًا على تقنية تحليل المشاعر Sentiment Analysis؛ لمعرفة وتحليل التغذية المرتدة Feedback الخاصة بالمستفيد؛ من أجل تطوير ما تقدمه من خدمات وتعزيز تجارب المستخدم.

٢,٥ سياسات خصوصية المستفيدين من المكتبات في عصر الذكاء الاصطناعي:

تمثل المكتبات بوابات للاستكشاف المعرفي غير المحدود، وبمجرد شعور المستفيد بأنه مراقب سيفضي ذلك إلى تقييد حريته في سلوكه في البحث عن المعلومات ومصادرها المتنوعة، مما ينتج عنه تقييد سبل التعلم والاستكشاف (Bettinger, E. et al, 2023). ومن المبادئ الأخلاقية الرئيسة في مهنة المكتبات تسهيل عملية الوصول إلى المعلومات وليس مراقبتها.

وتعد سياسات خصوصية المستفيد من الأدوات الأساسية التي تمكن المكتبة من تنفيذ هذا المبدأ وجعله واقعًا ملموسًا، وتقوم المكتبات بالالتزام بها وبما يتوافق معها من قوانين وتشريعات سواء كانت محلية أو دولية، ومن الضروري أن تحافظ المكتبات على سياسة خصوصية محدثة ومتاحة للجمهور توضح البيانات التي تُجمَع، والجهات التي ستشارك البيانات معها، ومدة الاحتفاظ بها، وتتحمل إدارة المكتبة وأمناؤها– بما في ذلك المتطوعون– مسؤولية الحفاظ على بيئة تحترم وتحمي خصوصية جميع المستخدمين، وتقع على عاتق المكتبة مسؤولية توفير التعليم والتدريب المستمرين بشأن الخصوصية للعاملين في المكتبات والمستخدمين من أجل الوفاء بهذه المسؤولية (American library Association, 2019b).

وقد أجمعت العديد من الدراسات على أن سياسات خصوصية المستفيدين والمعدة بإحكام، تعد من أدوات بناء الثقة للمستخدم للتعامل مع المكتبة، وخدماتها، وموقعها الإلكتروني، وأي تطبيق تصدره المكتبة في ظل استخدامها لتقنيات الذكاء الاصطناعي المختلفة، ويعد الامتثال للوائح حماية البيانات والخصوصية أمرًا حاسمًا بالنسبة للمكتبات. (Dahlian P., et al, 2024).

جدول رقم (١)

سياسات خصوصية المستفيدين من المكتبات قبل الذكاء الاصطناعي وبعده.

وجه المقارنة	قبل الذكاء الاصطناعي	بعد الذكاء الاصطناعي
البيانات المجمعة	• تركز بشكل أساسي على البيانات الشخصية مثل الأسماء، وأرقام الهواتف، وعناوين المنازل، وعناوين البريد الإلكتروني. • بيانات الإعارة وخدمة البحث والاسترجاع، وغيرهم.	• توسع نطاق البيانات المجمعة لتضم بيانات الاستخدام مفصلة، والاهتمامات والتفضيلات الشخصية، وسلوك البحث والتصفح الخاص بالمستخدم، وقد تصل إلى بيانات القياسات الحيوية. • استنتاج المعلومات الأكثر حساسية: تتوافر له القدرة على الاستدلال على المعلومات الحساسة من خلال قيامه بتحليل البيانات المجمعة، ويتم ذلك بدون تجميعه لهذه المعلومات بشكل مباشر بطلب من المستخدم.
الغرض من تجميع البيانات	• تَمكُن المكتبات من تقديم الخدمات. • تقديم خدمات تتوافق مع احتياجات المستخدم.	• الغرض الأساسي تدريب نماذج الذكاء الاصطناعي. • تحسين جودة الخدمات، وتعزيز تجارب المستخدم. • التنبؤ بالاحتياجات والتفضيلات المستقبلية.
وسائل الحماية التشريعية	قوانين عامة؛ تتبع السياسات القوانين العامة لحماية البيانات.	قوانين أكثر تخصصا؛ موجهة لحماية البيانات في عصر الذكاء الاصطناعي وما أثاره من تحديات.
وسائل الحماية التقنية	تشفير البيانات، التشويش على البيانات، بروتوكولات نقل النصوص الفائقة الآمنة HTTPs	الخصوصية التفاضلية، الخصوصية بالتصميم، تقييم تأثير الخصوصية PIA.
الروابط الفائقة الخارجية	ضرورة إعلام المستخدم بأجزاء الموقع والخدمات التي تضم روابط خارجية والإشارة إلى ضرورة قراءة سياسة الخصوصية لهذه الخدمات.	ضرورة إعلام المستخدم بالخدمات الخارجية المدرجة بالموقع والتي تعتمد على الذكاء الاصطناعي في عملها كخدمات الناشرين والموردين.

٣,٥ سياسات خصوصية المستفيدين من المكتبات قبل وبعد الذكاء الاصطناعي.

مع تطور تقنيات الذكاء الاصطناعي وتوسع نطاق استخدامها، وجب على سياسات الخصوصية بصفة عامة وسياسات خصوصية المكتبات على وجه الخصوص إجراء عدد من التحولات الجوهرية لمحتوياتها وبنودها، ويستعرض الجدول رقم (١) عددًا من هذه التغيرات.