AL-NAHRAIN JOURNAL OF LEGAL SCIENCE Vol.27 2025, pp. 1-14

AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW

ISSN:3006- 0605 DOI:10.58255

مجلة النهرين للعلوم القانونية عدد: مؤتمر (الفراهيدي) المجلد: ٢٧ تموز ٢٠٢٥

Received:1/3/2025 Accepted: 7/4/2025 Published: 1/6/2025

Artificial Intelligence Ethics: A Legal Framework for Privacy and Data in Iraq

Prof. Dr. Qahtan Abdul Sattar Taha

Abstract

This study addresses the ethical and legal challenges associated with artificial intelligence (AI) applications, focusing specifically on the framework of privacy and data protection in Iraq. The article highlights risks such as algorithmic bias, privacy violations, and the difficulty of determining legal accountability for AI system errors. It reviews fundamental ethical principles including fairness, transparency, and accountability in alignment with international initiatives like the OECD framework. In the Iraqi context, the study points to the absence of a comprehensive data protection law, weak legislative enforcement, and the lack of an independent regulatory body, while noting the ongoing discussions around the Personal Data Protection Bill (2021). The research concludes by emphasizing the need to strengthen local legislation, align it with global standards, and establish effective oversight mechanisms to address challenges arising from the rapid evolution of AI and data collection technologies.

أخلاقيات الذكاء الاصطناعي: إطار قانوني للخصوصية والبيانات في العراق

أ.د.م. قحطان عبد الستار طه
جامعة الفراهيدي \ كلية القانون

المستخلص

تتناول هذه الدراسة التحديات الأخلاقية والقانونية المرتبطة بتطبيقات الذكاء الاصطناعي، مع تركيز خاص على الإطار القانوني للخصوصية وحماية البيانات في العراق.إذ يبرز البحث المخاطر الناتجة عن التحيز الخوارزمي، وانتهاكات الخصوصية، وصعوبة تحديد المسؤولية القانونية عن أخطاء أنظمة الذكاء الاصطناعي.ويستعرض المبادئ الأخلاقية الأساسية كالعدالة والشفافية والمساءلة، وفقاً للمبادرات الدولية مثل إطار منظمة التعاون الاقتصادي والتنمية (OECD). أما في السياق العراقي، فتشير الدراسة إلى غياب قانون شامل لحماية البيانات، وضعف التنفيذ التشريعي، والافتقار إلى هيئة رقابية مستقلة، مع الإشارة إلى مشروع قانون حماية البيانات الشخصية الذي لا يزال قيد المناقشة. ويخلص البحث إلى ضرورة تعزيز التشريعات المحلية، ومواءمتها مع المعايير الدولية، وإنشاء آليات رقابية فعالة لمواجهة التحديات الناشئة عن التطور المتسارع للذكاء الاصطناعي ولا سيما آليات رقابية على جمع البيانات.

المقدمة

تتعدد القضايا الأخلاقية والقانونية المرتبطة بالذكاء الاصطناعي، ولاسيّما مع تسارع التطور التكنولوجي وزيادة الاعتماد على الأنظمة الرقمية بشكل عام والأنظمة الذكية بشكل خاص في مختلف المجالات. ومن التحديات الأخلاقية الجوهرية: التحيز الخوارزمي،إذ تشير الدراسات إلى أن الأنظمة المدربة على بيانات منحازة قد تعزز التمييز العرقي أو التمييز على أساس الجنس، كما في حالات أنظمة التوظيف الذكية[١]، بالإضافة الى موضوع الخصوصية و البيانات. على اعتبار أن البيانات هي المحرك الأساسي لتطوير الأنظمة الذكية، و هنا يظهر التحدي الأكبر المرتبط بعملية جمع البيانات و ما قد يتخلله من انتهاك لخصوصية الأفراد و المنظمات و الشركات، و يضاف الى ما سبق التحدي الجوهري من وجهة نظر قانونية المتمثل بتحديد المسؤولية القانونية الناتجة عن الأخطاء في قرارات أنظمة الذكاء الاصطناعي.[٢]

إن الذكاء الاصطناعي يحمل إمكانيات هائلة لتحسين حياتنا في العديد من المجالات، ولكن في الوقت نفسه يطرح تحديات أخلاقية كبيرة يجب معالجتها،إذ يتناول هذا البحث الإطار القانوني للخصوصية والبيانات في العراق مع اقتراح توصيات مناسبة لحل هذه المشكلة.

المبحث الأول
ماهية الذكاء الاصطناعي وتقنياته

الذكاء الاصطناعي هو تطوير أنظمة قادرة على أداء مهام تتطلب ذكاءً بشرياً، مثل التعلم، والتفكير، واتخاذ القرارات، والإدراك، وفهم اللغة الطبيعية، بدأ بوصفه حقلاً بحثياً في منتصف القرن العشرين، وتطور بشكل كبير مع التقدم في البنى الصلبة والبيانات الضخمة.

إن الذكاء الاصطناعي هو مجال من علوم الحاسوب يهدف إلى تصميم أنظمة قادرة على محاكاة العمليات الذكية البشرية أو تجاوزها، من خلال تحليل البيانات، والتعلم الذاتي، والتكيّف مع البيئات الديناميكية، واتخاذ قرارات مُعقّدة دون تدخل بشري مباشر.[٣]

المطلب الأول
المحاور الرئيسية للذكاء الاصطناعي

التعلم الآلي (Machine Learning - ML): وهو تطوير خوارزميات تتعلم تلقائياً من البيانات دون برمجة صريحة وله ثلاث أصناف رئيسية:

التعلم الموجَّه (Supervised Learning): أو التعليم بمعلم ومن تطبيقاته التصنيف والانحدار.

التعلم غير الموجَّه (Unsupervised Learning): أو التعليم بدون معلم ومن تطبيقاته التجميع (Clustering) واكتشاف الأنماط.

التعلم التعزيزي (Reinforcement Learning): وهي أنظمة تتعلم عبر التجربة والمكافأة (مثال: ألعاب الفيديو، الروبوتات).

---

[١] باحثو معهد ماساتشوستس للتكنولوجيا (MIT). (2019). *التحيز الخوارزمي في التوظيف: دراسة حالة لأنظمة الذكاء الاصطناعي*. تم الاسترداد في ١٧ /٣/ ٢٠٢٥ من https://news.mit.edu/2019/study-finds-gender-bias-ai-tools-0109

[٢] الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA). (2023). *المبادئ الأخلاقية للذكاء الاصطناعي*. الرياض، المملكة العربية السعودية. تم الاسترداد في ١٧ /٣/ ٢٠٢٥ من https://sdaia.gov.sa/ar/SDAIA/about/Documents/ai-principles.pdf

[٣] الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA). (2023). *المبادئ الأخلاقية للذكاء الاصطناعي*. الرياض، المملكة العربية السعودية. تم الاسترداد في ١٧ /٣/ ٢٠٢٥ من https://sdaia.gov.sa/ar/SDAIA/about/Documents/ai-principles.pdf

التعلم العميق (Deep Learning): وهو فرع من التعلم الآلي يعتمد على الشبكات العصبية الاصطناعية متعددة الطبقات التي تحاكي إلى حدٍ بعيد آلية عمل الدماغ البشري[١].
معالجة اللغة الطبيعية (Natural Language Processing - NLP): وهي تفاعل الحواسيب مع اللغة البشرية مثال: الترجمة الآلية، تحليل المشاعر، المساعدات الصوتية.
الرؤية الحاسوبية (Computer Vision): وهي تمكين الآلات من تحليل الصور أو الفيديو ومن تطبيقاتها التعرف على الوجوه والسيارات ذاتية القيادة[٢].
الروبوتات والأنظمة الذكية: وهي دمج الذكاء الاصطناعي مع الروبوتات لأتمتة المهام في الصناعة والطب والخدمات المنزلية و غيرها.
الأنظمة الخبيرة (Expert Systems): وهي برامج تحاكي قرارات الخبراء البشريين في المجال المدروس، مثال: التشخيص الطبي[٣].

المطلب الثاني

علم البيانات والذكاء الاصطناعي

علم البيانات: يهدف إلى استخراج الأنماط الخفية والقيمة من البيانات عبر تحليلها وتنظيفها وتفسيرها لاتخاذ قرارات سليمة، ويظهر التداخل الكبير بين علم البيانات والذكاء الاصطناعي من خلال استخدام علم البيانات لتقنيات تعلم الآلة بشكل رئيسي وفيما يلي الخطوات الرئيسية لتنفيذ مشروع كامل في علم البيانات:

- تحديد المشكلة: تحديد المشكلة أو الهدف الذي يسعى المشروع لحله.
- جمع البيانات: تحديد مصادر البيانات (قواعد بيانات، مسوح إحصائية، استبيانات، مستشعرات، كاميرات، مواقع إلكترونية، ملفات Excel، .....).
- تنظيف البيانات وتحليلها الأولي.
- تحضير البيانات للنمذجة
- تطوير النموذج: اختيار خوارزميات التعلم الآلي المناسبة، تدريب النموذج على البيانات.
- ومن ثم بقية الخطوات التقنية والبرمجية من تحقيق للنظام واختباره وربطه.

المطلب الثالث

تطبيقات الذكاء الاصطناعي في الحياة اليومية

مع تطور تقنيات الذكاء الاصطناعي وانتشارها الواسع فقد أصبحت تطبيقاتها في كافة جوانب حياة البشر الاقتصادية والصناعية والصحية والاجتماعية والسياسية وغيرها ونذكر منها:

- الرعاية الصحية: تشخيص الأمراض عبر تحليل الصور الطبية، اكتشاف الأدوية.
- التمويل: كشف الاحتيال، التداول الآلي.
- التعليم: أنظمة تعليم مُكيفة مع مستوى الطالب.
- التجارة الإلكترونية: أنظمة توصية واقتراح كما في، Amazon Netflix
- السيارات الذاتية القيادة، مثال: سيارات Tesla
- الزراعة الذكية: مراقبة المحاصيل عبر الطائرات المسيرة.

---

[١] بيشوب، ك. م. (٢٠٠٦). *التعرف على الأنماط وتعلُّم الآلة*. *Pattern Recognition and Machine Learning*. : سبرنجر ص١٣٧ ، ص ٤٢٣ .

[٢] سزيليسكي، ر. (٢٠٢٠). *الرؤية الحاسوبية: الخوارزميات والتطبيقات* (فريق مركز التعريب والترجمة، مترجم.). دار النشر العربية للعلوم، بيروت. (العمل الأصلي نُشر عام ٢٠١٠) ص٣ .

[٣] ابراهيم، م. خ. (١٩٨٥). تطبيقات في الذكاء الصناعي. Iraqi Journal for Computers and Informatics, 14(2) ، ص 56–29. https://doi.org/10.25195/ijci.v14i2.178

- المراقبة الذكية: هي أنظمة مراقبة متطورة تعتمد على تقنيات الذكاء الاصطناعي وإنترنت الأشياء[1].

المطلب الرابع
التحديات والمخاطر

لا يمكن اعتبار أنظمة الذكاء الاصطناعي خالية من العيوب برغم حداثتها وتطورها، يوجد الكثير من الثغرات التقنية التي ينتج عنها إشكاليات مختلفة أثناء تطبيقها على أرض الواقع ونذكر منها:

- التحيز: تحيز البيانات يؤدي إلى قرارات غير عادلة.
- الخصوصية: جمع البيانات الضخمة يهدد الخصوصية.
- الأمان: إساءة استخدام الذكاء الاصطناعي في الهجمات الإلكترونية أو التزييف العميق.
- التوظيف: أتمتة الوظائف التقليدية.
- الشفافية: صعوبة فهم قرارات أنظمة الذكاء الاصطناعي المعقدة (مشكلة الصندوق الأسود)[2].

الذكاء الاصطناعي يغير العالم بسرعة، لكن نجاحه يعتمد على موازنة الابتكار مع المسؤولية الاجتماعية والأخلاقية والقانونية.

المبحث الثاني
إطار مفاهيمي وقانوني وتحديات معاصرة لأخلاقيات الذكاء الاصطناعي والخصوصية والبيانات

تشمل أخلاقيات الذكاء الاصطناعي مجموعة من المبادئ والقيم التي تهدف إلى توجيه سلوك أنظمة الذكاء الاصطناعي وتحديد استخداماتها بشكل أخلاقي ومسؤول. يُعتبر هذا المجال جزءًا من الفلسفة التطبيقية،إذ يدرس المبادئ الأخلاقية والقيم الاجتماعية التي يجب أن توجه تصميم وتطوير ونشر أنظمة الذكاء الاصطناعي. وتهدف هذه الأخلاقيات إلى ضمان أن تكون الأنظمة عادلة وشفافة ومسؤولة، ومتوافقة مع حقوق الإنسان[3].

المطلب الاول
المبادئ الأساسية لأخلاقيات الذكاء الاصطناعي

وفقاً لإطار منظمة التعاون الاقتصادي والتنمية (OECD) والمبادرات العالمية الأخرى، تشمل المبادئ الرئيسة:

العدالة والإنصاف: تجنب التحيز الخوارزمي الناتج عن بيانات تدريب غير تمثيلية أو خوارزميات تمييزية ومثال على ذلك أنظمة التعرف على الوجوه التي تُظهر دقةً أقل للأقليات العرقية.

- **الشفافية والشرح:** ضرورة فهم كيفية اتخاذ الأنظمة للقرارات ولاسيّما في المجالات الحيوية مثل الطب أو القضاء ومثال على ذلك تحدي الصندوق الأسود في نماذج التعلم العميق.
- **المسؤولية والمساءلة:** تحديد الجهة المسؤولة عن أخطاء الأنظمة (المطورون، المشرعون، أو المستخدمون) ومثال على ذلك من المسؤول عن حادث سيارة ذاتية القيادة، إذ لا بد من إطار قانوني يُحدد المسؤولية الجنائية والمدنية.

---

[1] ابراهيم، م. خ. (١٩٨٥). تطبيقات في الذكاء الصناعي. Iraqi Journal for Computers and Informatics, 14(2) https://doi.org/10.25195/ijci.v14i2.178 ، ص ٢٩–٥٦.

[2] **المركز الوطني للذكاء الاصطناعي(SDAIA) ،*تموز ٢٠٢٥* ، التحيز في أنظمة الذكاء الاصطناعي،** https://sdaia.gov.sa/ar/MediaCenter/KnowledgeCenter/ResearchLibrary/BiasInAISystems.pdf

[3] الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA). (2023). *المبادئ الأخلاقية للذكاء الاصطناعي* . الرياض، المملكة العربية السعودية. تم الاسترداد في ١٧ /٣/ ٢٠٢٥ من https://sdaia.gov.sa/ar/SDAIA/about/Documents/ai-principles.pdf

- **الخصوصية وحماية البيانات:** حماية البيانات الشخصية من الاستغلال، ولاسيّما في أنظمة المراقبة أو التتبع ومثال على ذلك جمع البيانات الضخمة من دون موافقة مسبقة.
- **الاستدامة والرفاهية الاجتماعية:** تجنب استخدام الذكاء الاصطناعي في تطبيقات تهدد البيئة أو تزيد عدم المساواة، ومثال على ذلك أتمتة الوظائف دون إعادة تدوير العمالة[1].

ومن الأمثلة الواقعية على خروقات أخلاقية لأنظمة الذكاء الاصطناعي:

- التحيز في أنظمة التوظيف: أداة التوظيف في أمازون التي تميزت ضد النساء بسبب تدريبها على سير ذاتية تاريخية لذكور.
- المراقبة الجماعية في الصين: استخدام التعرف على الوجوه لقمع الأقليات (الإيغور) وتحديات حقوق الإنسان.
- الأسلحة المستقلة: الجدل الأخلاقي حول أنظمة الذكاء الاصطناعي التي تُتخذ قرارات القتل دون تدخل بشري.

المطلب الثاني

التحديات الرئيسية لتعميم أخلاقيات الذكاء الاصطناعي

مع مراقبة تطور تقنيات وأنظمة الذكاء الاصطناعي يمكننا أن نلحظ الديناميكية العالية والتطور المتسارع لها مقارنةً مع الأنظمة والضوابط والقوانين الحاكمة لها لنجد الكثير من التحديات أمام تعميم و تقنين أخلاقيات الذكاء الاصطناعي و نذكر بعض هذه التحديات:

- **التناقض بين الأخلاقيات العالمية والمحلية:**إذ تختلف القيم الثقافية والدينية بين المجتمعات، مثل مفهوم الخصوصية في الغرب والشرق.
- **التفاوت التكنولوجي:** تركيز تطوير الذكاء الاصطناعي في دول محدودة، مما يعمق الفجوة بين الدول الغنية والفقيرة.
- **أخلاقيات الذكاء العام الاصطناعي:** وهي مخاطر افتراضية لأنظمة ذكاء تفوق البشر وضرورة وضع ضوابط استباقية.
- **الصراع بين الابتكار والتنظيم:** كيف نُوازن بين تشجيع الابتكار وحدود أخلاقية صارمة[2].

أخلاقيات الذكاء الاصطناعي ليست ترفاً فكرياً، بل ضرورةً لضمان أن تخدم التكنولوجيا البشرية بدلاً من استغلالها. يتطلب تحقيق هذا التوازن تعاوناً عالميًا، تشريعات مرنة، ووعيًا مجتمعيًا بمخاطر الذكاء الاصطناعي غير المنضبط.

هذا الإطار يُقدم أساساً نظريّاً لفهم التعقيدات الأخلاقية للذكاء الاصطناعي، مع إمكانية توسيعه عبر دراسات حالة أو تحليلات فلسفية أعمق.

---

[1] منظمة التعاون الاقتصادي والتنمية (OECD). (٢٠١٩). مبادئ منظمة التعاون الاقتصادي والتنمية للذكاء الاصطناعي. الموقع الإلكتروني لمنظمة التعاون الاقتصادي والتنمية. تم الاسترداد في [١٠ /٣/ ٢٠٢٥] من https://www.oecd.org/en/topics/sub-issues/ai-principles.html

[2] Ultralytics. (٢٠٢٤/٧/١٩). *الاستخدام الأخلاقي للذكاء الاصطناعي: موازنة بين الابتكار والنزاهة*. مدونة Ultralytics الإلكترونية. تم الاسترداد في [٢٠٢٥/٢/١٠] من https://www.ultralytics.com/ar/blog/the-ethical-use-of-ai-balances-innovation-and-integrity

[3] جبار، ب. ح. (٢٠٢٤). أخلاقيات الذكاء الاصطناعي. *مجلة جامعة بابل للآداب، ١٧* (1/2)، ص ١–٢١١. بابل، العراق: كلية الآداب / جامعة بابل.

المطلب الثالث
الخصوصية والبيانات في أنظمة الذكاء الاصطناعي

ومن خلال ما تم سرده سابقا يمكن ان نستنتج ان تطوير أنظمة الذكاء الاصطناعي وتطبيقات علوم البيانات ترتكز على ثلاثة محاور رئيسة وهي:

- **تطوير الخوارزميات**
- **البيانات**
- **تطوير أدوات الحوسبة**

يمكن اعتبار البيانات هي المحرك الرئيسي او كما تسمى أحياناً هي وقود الذكاء الاصطناعي و من دون بيانات جيدة و كافية لا يمكن تطوير أيّ نظام ذكاء اصطناعي فعال.

تتنوع البيانات التي تستخدمها انظمة الذكاء الاصطناعي من أجل مختلف التطبيقات لتشمل: البيانات الرقمية والنصية (المحرفية)، الصور، مقاطع الفيديو، المقاطع الصوتية.

إن أنظمة الذكاء الاصطناعي الحديثة تحتاج الى آلاف وقد تصل الى ملايين او مئات من الملايين من العينات اللازمة لتدريب نماذج الذكاء الاصطناعي المختلفة و لا سيّما نماذج تعلم الآلة التي تعتبر الأكثر شيوعاً و استخداماً.

تتنوع طرق جمع البيانات اللازمة لتشمل:

- واجهات برمجة التطبيقات (APIs) التي تمكن من الوصول الى بيانات خارجية و من مواقع التواصل الاجتماعي بشكل أساسي.
- استخلاص البيانات من الويب
- إنشاء استبيانات واستطلاعات رأي
- التحميل من قواعد بيانات الصور
- التقاط الصور باستخدام الكاميرات
- استخراج البيانات من كاميرات المراقبة أو الطائرات المسيرة
- جمع بيانات الفيديو في الوقت الحقيقي من الكاميرات الأمنية أو الدرونات
- جمع بيانات الصوت باستخدام الميكروفونات وتحليلها لاحقًا
- أجهزة الاستشعار والمستشعرات الذكية
- بيانات الأقمار الصناعية والاستشعار عن بعد
- مجموعات البيانات الجاهزة[1]

يبدو جلياً أن طرق جمع البيانات اللازمة لتطوير أنظمة الذكاء الاصطناعي كافة تعرض العينات البشرية المدروسة لانتهاك واضح للخصوصية ولا سيّما في تطبيقات التكنلوجيا التفاعلية وأنظمة دعم اتخاذ القرار المرتبطة بشكل وثيق مع البيانات الشخصية لمستخدمي هذه الأنظمة.

إن خصوصية البيانات هي أحد المفاهيم الأساسية في علم البيانات وأمن المعلومات، إذ تشير إلى قدرة الأفراد والمؤسسات على التحكم في كيفية جمع بياناتهم الشخصية، واستخدامها، وتخزينها ومشاركتها.

ومع التطور السريع للتكنولوجيا وزيادة الاعتماد على البيانات الضخمة والذكاء الاصطناعي، أصبحت خصوصية البيانات قضية رئيسية تتطلب سياسات وتشريعات لحمايتها.

تُعرف خصوصية البيانات بأنها مجموعة من المبادئ والممارسات التي تهدف إلى حماية المعلومات الشخصية من الوصول غير المصرح به، أو الاستخدام غير القانوني، أو التعديل غير

[1] الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA). (2023). *المبادئ الأخلاقية للذكاء الاصطناعي*. الرياض، المملكة العربية السعودية. تم الاسترداد في ١٧ /٣/ ٢٠٢٥ من https://sdaia.gov.sa/ar/SDAIA/about/Documents/ai-principles.pdf

المرغوب فيه. وتشمل هذه الخصوصية حماية المعلومات الحساسة، مثل الهوية، والبيانات المالية، والسجلات الصحية، بالإضافة إلى السلوك عبر الإنترنت[1].

تُعد خصوصية البيانات عنصراً حيوياً في العصر الرقمي الحالي،إذ يتعين تحقيق توازن بين استخدام البيانات لأغراض التحليل والابتكار، وحماية حقوق الأفراد في التحكم ببياناتهم. ومن ثَمَّ، ينبغي على الأفراد والمؤسسات الالتزام بأفضل الممارسات القانونية والتقنية لضمان الخصوصية والأمان في إدارة البيانات[2].

المطلب الرابع
القوانين والتشريعات المتعلقة بخصوصية البيانات عالمياً

تُعد حماية خصوصية البيانات تحدياً رئيساً في العصر الرقمي،ولاسيّما مع زيادة جمع البيانات الشخصية عبر المنصات التكنولوجية.إذ تعمل التشريعات العالمية على تنظيم عمليات جمع البيانات ومعالجتها وتخزينها وتبادلها، بهدف تحقيق توازن بين الابتكار التكنولوجي وحماية الحقوق الأساسية للأفراد. ومن بين النماذج الرائدة في هذا المجال، توجد لوائح مثل GDPR في الاتحاد الأوروبي وCCPA في كاليفورنيا.

اللائحة العامة لحماية البيانات (GDPR) - الاتحاد الأوروبي:

النطاق: تُطبق على جميع الكيانات التي تتعامل مع بيانات مواطني الاتحاد الأوروبي، بغض النظر عن موقعها الجغرافي.

المبادئ:

- الحد الأدنى من البيانات (Data Minimization).
- الشفافية في الإفصاح عن أغراض المعالجة.
- الإبلاغ عن خروقات البيانات خلال ٧٢ ساعة.
- العقوبات: تصل إلى ٤% من الإيرادات العالمية أو ٢٠ مليون يورو[3].

قانون خصوصية المستهلك في كاليفورنيا (CCPA):

النطاق: يُلزم الشركات التي تعمل في كاليفورنيا وتجمع بيانات أكثر من ٥٠،٠٠٠ مستهلك.

المبادئ:

- الحق في معرفة البيانات التي تُجمع وأسبابها.
- الحق في رفض بيع البيانات الشخصية.
- العقوبات: غرامات تصل إلى ٧،٥٠٠ دولار لكل انتهاك متعمد[4].

قانون الحماية العامة للبيانات (LGPD) – البرازيل:

النطاق: يشبه GDPR ويُطبق على جميع الشركات التي تتعامل مع بيانات البرازيليين.

المبادئ:

- تعيين مسؤول عن حماية البيانات (DPO).
- تقييم تأثير حماية البيانات (DPIA) للمشاريع عالية المخاطر[5].

---

[1] Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399.

[2] جبار، ب. ح. (٢٠٢٤). أخلاقيات الذكاء الاصطناعي. مجلة جامعة بابل للآداب، ١٧(٢/١)، ص ١–٢١١. بابل، العراق: كلية الآداب / جامعة بابل.

[3] European Parliament and Council. *Regulation (EU) 2016/679 (General Data Protection Regulation)*. OJ L119, 2016.

[4] California Civil Code §1798.100 et seq. (2024)

[5] Brasil. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União.

قانون حماية البيانات الشخصية (PDPA) – سنغافورة:

النطاق: يُلزم جميع الكيانات باحترام مبادئ الموافقة والغرض المحدد.

المبادئ:

- نقل البيانات عبر الحدود يتطلب ضمانات كافية.
- عقوبات تصل إلى ١ مليون دولار سنغافوري[١].

لائحة خصوصية البيانات في الصين (PIPL):

النطاق: تُطبَّق على الشركات المحلية والدولية التي تتعامل مع بيانات المواطنين الصينيين.

المبادئ:

- قيود على نقل البيانات خارج الصين من دون موافقة.
- عقوبات تصل إلى ٥٠ مليون يوان أو ٥% من الإيرادات السنوية[٢].

المطلب الخامس

القوانين والتشريعات المتعلقة بخصوصية البيانات في العراق

وحتى الآن، لا يمتلك العراق قانوناً شاملاً خاصاً ينظم حماية البيانات الشخصية، ولكن هناك نصوص متفرقة في تشريعات مختلفة تشير إلى حماية الخصوصية. ويُعتبر الوضع التشريعي في هذا المجال ضعيفاً مقارنةً بالمعايير الدولية، مثل GDPR، لاسيّما مع التحديات الأمنية والسياسية التي حالت دون تطوير أطر قانونية حديثة. ومع ذلك، بدأت تظهر مبادرات جديدة، مثل مشروع قانون حماية البيانات الشخصية لعام ٢٠٢١، تهدف إلى سدّ هذه الفجوة.

الإطار التشريعي الحالي يتضمن:

الدستور العراقي (٢٠٠٥)

- المادة ١٧: تكفل حماية الخصوصية الفردية،إذ تنص على أن "لكل فرد الحق في الخصوصية الشخصية، بما لا يتنافى مع حقوق الآخرين والآداب العامة".
- المادة ٣٨: تحمي سرية المراسلات البريدية والهاتفية والإلكترونية إلا بموجب قرار قضائي[٣].

قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩

- المادة ٤٣٤: تعاقب كل من اطلع على مراسلات أو مكالمات خاصة من دون إذن بالسجن حتى ٣ سنوات.
- المادة ٤٣٥: تجرّم انتهاك حرمة المساكن أو التنصت[٤].

قانون المبادلات الإلكترونية رقم ٧٨ لسنة ٢٠١٢

ينظم المعاملات الإلكترونية ويُلزم بحماية البيانات أثناء التبادل، لكنه لا يتناول تفاصيل خصوصية البيانات[٥].

قانون الاتصالات رقم ٦٥ لسنة ٢٠١٦

المادة ١٢: تلزم شركات الاتصالات بحماية بيانات المشتركين وعدم الكشف عنها إلا بموجب أمر قضائي[٦].

مشروع قانون حماية البيانات الشخصية (٢٠٢١)

1Singapore. (2012). Personal Data Protection Act 2012 (PDPA), No. 26 of 2012

2China. (2021). Personal Information Protection Law (PIPL), Order No. 91 of the President of the People's Republic of China.

[٣] جمهورية العراق. (٢٠٠٥). دستور جمهورية العراق لعام ٢٠٠٥. الجريدة الرسمية

[٤] جمهورية العراق. (١٩٦٩). قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩. الجريدة الرسمية

[٥] قانون المبادلات الإلكترونية رقم ٧٨ لسنة ٢٠١٢، الجريدة الرسمية، العدد ٤٢٩٢، ٢٠١٢

[٦] قانون الاتصالات رقم ٦٥ لسنة ٢٠١٦، الجريدة الرسمية، ٢٠١٦.

الوضع: قيد المناقشة في البرلمان، ويستند إلى مبادئ دولية مثل الموافقة المستنيرة وحق الوصول إلى البيانات.
التحديات: غياب آلية تنفيذية واضحة وموارد تقنية لدعمه.
يوجد العديد من التحديات التشريعية لحماية خصوصية البيانات في العراق متضمنة
أولاً - غياب قانون خاص بحماية البيانات: لا يوجد إطار شامل ينظم جمع البيانات الشخصية أو معالجتها أو تخزينها، ولاسيّما في القطاعين العام والخاص.
ثانياً - ضعف التنفيذ: القوانين الحالية لا تُطبق بشكل فعال بسبب الفساد الإداري وغياب الوعي المجتمعي.
ثالثاً - التقنيات الحديثة: لا تتعامل التشريعات مع تحديات مثل البيانات الضخمة، التعرف على الوجوه، أو استخدام الذكاء الاصطناعي في المراقبة.
رابعاً - الافتقار إلى هيئة رقابية: لا توجد هيئة مستقلة (مثل مكتب مفوضية الخصوصية في دول أخرى) لمراقبة الانتهاكات.
ونذكر بعض الحالات الواقعية التي تضمنت انتهاكات لخصوصية البيانات في العراق:
أولاً - استخدام البيانات في القطاع الحكومي: تُجمع بيانات المواطنين في السجلات السكانية والبطاقة الوطنية من دون ضمانات كافية ضد الاختراق أو الاستغلال.
ثانياً: انتهاكات شركات الاتصالات: تسريب بيانات المشتركين لجهات غير مصرحٍ بها، مع غياب عقوبات رادعة.
وبإجراء مقارنة إقليمية نلخص النتائج بالجدول الآتي:

المعيار	الأردن (قانون حماية البيانات ٢٠٢٣)[١]	الإمارات (قانون البيانات ٢٠٢١)[٢]	العراق
القانون الشامل	موجود	موجود	غير موجود
الهيئة الرقابية	موجودة	موجودة	غير موجودة
العقوبات	غرامات تصل إلى ٢٠٠،٠٠٠ دولار	غرامات تصل إلى ٥ ملايين درهم	محدودة (حتى ٣ سنوات سجن)

المطلب السادس
المسؤولية القانونية لجمع البيانات في العراق

تخضع مسؤولية جمع البيانات في العراق لعدد محدود من النصوص القانونية المتفرقة، ويغيب إطار تشريعي شامل ينظم عملية جمع البيانات الشخصية ومعالجتها. تُحدد المسؤولية القانونية استنادًا إلى قوانين جزئية، مثل قانون العقوبات وقانون الاتصالات، لكنها تظل غير كافية لمواكبة التحديات الرقمية الحديثة، ولاسيّما في ظلّ تطبيقات الذكاء الاصطناعي وعلوم البيانات، التي تعتبر البيانات المحرك الأساسي لتطويرها. وتزداد المخاطر مع استخدام تقنيات مراقبة متطورة دون وجود ضوابط قانونية واضحة.

تحدد المسؤولية القانونية في حالات جمع البيانات من دون موافقة واضحة وفقاً للأنظمة التشريعية في مختلف الدول، إذ توجد تشابهات في المبادئ الأساسية برغم اختلاف التفاصيل.

[١] المملكة الأردنية الهاشمية، قانون رقم (٢٤) لسنة ٢٠٢٣ قانون حماية البيانات الشخصية.
[٢] الامارات العربية المتحدة ، مرسوم بقانون اتحادي رقم (٤٥) لسنة ٢٠٢١ بشأن حماية البيانات الشخصية

أنواع المسؤولية القانونية

أ. المسؤولية الجنائية

- الجهة المسؤولة: الأفراد أو الكيانات التي تجمع بيانات دون إذن أو تنتهك الخصوصية.
- العقوبات: وفقاً لقانون العقوبات، قد تشمل الحبس أو الغرامة[١].
- مثال: موظف في شركة اتصالات يبيع بيانات المشتركين لجهات غير مصرح بها.

ب. المسؤولية المدنية

- التعويضات: يُمكن للمتضررين رفع دعاوى تعويض عن الأضرار المادية أو المعنوية الناتجة عن انتهاك الخصوصية[٣].
- الإسناد: يُطلب إثبات العلاقة السببية بين جمع البيانات والضرر الحاصل.

ج. المسؤولية الإدارية

الجهات الحكومية: قد تتحمل الوزارات أو المؤسسات مسؤولية إدارية إذا أساءت استخدام البيانات المُجمعة (مثل تسريب سجلات المواطنين).

التحديات في تحديد المسؤولية

- **غياب قانون خاص:** لا يوجد نص صريح يُجرم جمع البيانات غير المصرح به خارج نطاق محدود (كالمراسلات).
- **صعوبة الإثبات:** نقص الخبرة التقنية لدى القضاء في التعامل مع قضايا البيانات الإلكترونية.
- **اللامركزية في الإدارة:** تعدد الجهات التي تجمع البيانات (الحكومة، الشركات، الجهات الأمنية) من دون تنسيق.
- الافتقار إلى آليات رقابية: لا توجد هيئة مستقلة لمراقبة الامتثال أو التحقيق في الانتهاكات.

ويمكن ذكر بعض الأمثلة الواقعية على حالات تسريب بيانات في العراق:

تسريب بيانات البطاقة الوطنية

- في ٢٠١٩، تعرضت قاعدة البيانات البيو مترية (البطاقة الوطنية) لاختراق أمني، مما أدى إلى تسريب بيانات ملايين العراقيين[٤].
- المسؤولية: لم تُحدد جهة مسؤولة بسبب غياب نصوص واضحة، برغم وجود شبهات بإهمال إداري.

انتهاك خصوصية المرضى في المستشفيات

- بعض المستشفيات تبيع بيانات المرضى لشركات الأدوية من دون موافقة.
- المسؤولية: يُمكن تطبيق المادة ٤٤١ من قانون العقوبات، لكن الإجراءات نادرة بسبب قلة الخبرة.

---

[١] قانون العقوبات العراقي (رقم ١١١ لسنة ١٩٦٩) ، المادة ٤٣٠ ، المادة ٤٣٤

[٢] قانون الاتصالات العراقي (رقم ٦٥ لسنة ٢٠٠٤) ، المادة ٣٧

[٣] القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١ ، المادة ٢٠٢، المادة ٢٠٥ .

[4] SMEX Cybersecurity. (2020). *Cybersecurity risk assessment in the public sector*. Retrieved from https://smex.org

وبالمقارنة مع دول الجوار يمكن تلخيص نتائج المقارنة بالجدول الآتي:

المعيار	الأردن (قانون حماية البيانات ٢٠٢٣)[1]	العراق
المسؤولية الجنائية	غرامات تصل إلى ٢٠٠،٠٠٠ دولار وسجن	محدودة (حسب قانون العقوبات)
المسؤولية المدنية	تعويضات جماعية وحماية منهجية	تعويضات عبر دعاوى فردية
الهيئة الرقابية	هيئة حماية البيانات الشخصية	غير موجودة

ولتحديد الجهة المسؤولة عن انتهاك خصوصية البيانات:

- المتحكم بالبيانات (Data Controller): يتحمل المسؤولية الرئيسية عن أيّ انتهاكٍ، سواء تم الجمع مباشرةً أو عبر طرف ثالث.
- المعالج (Data Processor): يُلزم بضمان الامتثال للقوانين أثناء معالجة البيانات، وقد توقع عليه عقوبات مستقلة إذا قام بمعالجة غير مصرح بها[2].

النتائج:

١. **غياب الإطار التشريعي الشامل :**يُلاحظ عدم وجود قانون عراقي متخصص في حماية البيانات الشخصية، مما يعيق قدرة البلاد على مواجهة التحديات الناشئة عن الذكاء الاصطناعي وتقنيات جمع البيانات الضخمة.
٢. **ضعف التنفيذ والقصور التشريعي :**القوانين الحالية غير كافية للتصدي لانتهاكات الخصوصية، مع غياب آليات رقابية فعّالة لضمان الامتثال.
٣. **تحديات تقنية وأخلاقية :**تزايد مخاطر التحيز الخوارزمي، وانتهاك الخصوصية عبر أنظمة المراقبة الذكية، وصعوبة تحديد المسؤولية القانونية عن أخطاء أنظمة الذكاء الاصطناعي.
٤. **التفاوت مع المعايير الدولية :**التشريعات العراقية متخلفة عن النماذج العالمية، مثلGDPR ، مما يُعمق الفجوة في حماية الحقوق الرقمية للمواطنين.

التوصيات:

استناداً إلى ما تم استعراضه في بحثنا، نوصي بما يلي:

١. **اعتماد مشروع قانون حماية البيانات الشخصية :**يجب تعزيز مشروع القانون ببنود تلزم الشركات والحكومة بضمان شفافية جمع البيانات وحماية الخصوصية، مع تضمين عقوبات رادعة للانتهاكات، مثل فرض غرامات مالية وعقوبات بالسجن للمخالفين.
٢. **إنشاء هيئة رقابية مستقلة :**يُستحسن تأسيس "هيئة وطنية لحماية البيانات" للإشراف على تطبيق التشريعات، والتحقق من التزام الجهات العامة والخاصة بالمعايير الأخلاقية والقانونية.
٣. **تعزيز الوعي المجتمعي والتقني :**ينبغي تنظيم حملات توعوية حول حقوق الأفراد في التحكم ببياناتهم، بالإضافة إلى تدريب القضاة والملاكات القانونية على التعامل مع قضايا البيانات الإلكترونية وتقنيات الذكاء الاصطناعي.

[1] المملكة الأردنية الهاشمية، قانون رقم (٢٤) لسنة ٢٠٢٣ قانون حماية البيانات الشخصية.
[2] Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 4, 24, 28. Available at: https://gdpr-info.eu

٤. **التعاون الدولي والإقليمي :**يجب الاستفادة من تجارب دول الجوار، مثل الإمارات والأردن، في بناء إطار تشريعي مرن، والانضمام إلى الاتفاقيات الدولية ذات الصلة.
٥. **موازنة الابتكار والحماية :**يتعين تشجيع تبني تقنيات الذكاء الاصطناعي مع ضمان تصميم أنظمة تتوافق مع مبادئ العدالة والشفافية، مثل إلزام المطورين بتوضيح آلية عمل الخوارزميات، لتفادي مشكلة الصندوق الأسود.

تسعى هذه التوصيات إلى سدّ الفجوة بين التقدم التكنولوجي والضمانات الأخلاقية، وتعزيز ثقة المواطنين في الأنظمة الرقمية.

المراجع العربية:

1. باحثو معهد ماساتشوستس للتكنولوجيا (MIT). (٢٠١٩). التحيز الخوارزمي في التوظيف: دراسة حالة لأنظمة الذكاء الاصطناعي. تم الاسترداد في ١٧ /٣/ ٢٠٢٥ من https://news.mit.edu/2019/study-finds-gender-bias-ai-tools-0109 .
2. الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA). (٢٠٢٣). المبادئ الأخلاقية للذكاء الاصطناعي. الرياض، المملكة العربية السعودية. تم الاسترداد في ١٧ /٣/٢٠٢٥ من https://sdaia.gov.sa/ar/SDAIA/about/Documents/ai-principles.pdf
3. بيشوب، ك. م. (٢٠٠٦). التعرف على الأنماط وتعلُّم الآلة : Pattern Recognition and Machine Learning. سبرنجر ص١٣٧ ، ص ٤٢٣ .
4. سزيليسكي، ر. (٢٠٢٠). الرؤية الحاسوبية: الخوارزميات والتطبيقات (فريق مركز التعريب والترجمة، مترجم). دار النشر العربية للعلوم، بيروت. (العمل الأصلي نُشر عام ٢٠١٠) ص٣ .
5. ابراهيم، م. خ. (١٩٨٥). تطبيقات في الذكاء الصناعي. Iraqi Journal for Computers and Informatics, 14(2) https://doi.org/10.25195/ijci.v14i2.178 ، ص ٢٩–٥٦.
6. المركز الوطني للذكاء الاصطناعي (SDAIA)، تموز ٢٠٢٥ ، التحيز في أنظمة الذكاء الاصطناعي، https://sdaia.gov.sa/ar/MediaCenter/KnowledgeCenter/ResearchLibrary/BiasInAISystems.pdf
7. منظمة التعاون الاقتصادي والتنمية (OECD). (٢٠١٩). مبادئ منظمة التعاون الاقتصادي والتنمية للذكاء الاصطناعي. الموقع الإلكتروني لمنظمة التعاون الاقتصادي والتنمية. تم الاسترداد في [١٠ /٣/ ٢٠٢٥] من https://www.oecd.org/en/topics/sub-issues/ai-principles.html
8. Ultralytics. (٢٠٢٤). الاستخدام الأخلاقي للذكاء الاصطناعي: موازنة بين الابتكار والنزاهة. مدونة Ultralytics الإلكترونية. تم الاسترداد في [٢٠٢٥/٢/١٠] من https://www.ultralytics.com/ar/blog/the-ethical-use-of-ai-balances-innovation-and-integrity
9. جبار، ب. ح. (٢٠٢٤). أخلاقيات الذكاء الاصطناعي. مجلة جامعة بابل للآداب، ١٧(٢/١)، ص ١–٢١١. بابل، العراق: كلية الآداب / جامعة بابل.
10. جمهورية العراق. (٢٠٠٥). دستور جمهورية العراق لعام ٢٠٠٥. الجريدة الرسمية
11. جمهورية العراق. (١٩٦٩). قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩. الجريدة الرسمية
12. قانون المبادلات الإلكترونية رقم ٧٨ لسنة ٢٠١٢، الجريدة الرسمية، العدد ٤٢٩٢، ٢٠١٢
13. قانون الاتصالات رقم ٦٥ لسنة ٢٠١٦، الجريدة الرسمية، ٢٠١٦.
14. المملكة الأردنية الهاشمية، قانون رقم (٢٤) لسنة ٢٠٢٣ قانون حماية البيانات الشخصية.

15. الامارات العربية المتحدة، مرسوم بقانون اتحادي رقم (٤٥) لسنة ٢٠٢١ بشأن حماية البيانات الشخصية
16. قانون العقوبات العراقي (رقم ١١١ لسنة ١٩٦٩) ، المادة ٤٣٠ ، المادة ٤٣٤
17. قانون الاتصالات العراقي (رقم ٦٥ لسنة ٢٠٠٤) ، المادة ٣٧.
18. القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١ ، المادة ٢٠٢، المادة ٢٠٥ .

المراجع الانكليزية:

1. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399.
2. European Parliament and Council. Regulation (EU) 2016/679 (General Data Protection Regulation). OJ L119, 2016.
3. California Civil Code §1798.100 et seq. (2024).
4. Brasil. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União.
5. Singapore. (2012). Personal Data Protection Act 2012 (PDPA), No. 26 of 2012.
6. China. (2021). Personal Information Protection Law (PIPL), Order No. 91 of the President of the People's Republic of China.
7. SMEX Cybersecurity. (2020). Cybersecurity risk assessment in the public sector. Retrieved from https://smex.org
8. Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 4, 24, 28. Available at: https://gdpr-info.eu .