Journal of Al-Farahidi's Arts, No Conference (10 th)N(V)295-309
Doi: https://doi.org/10.25130/jfa.conf.10.4.17

Proceedings of the (10) Conference وقائع المؤتمر العلمي العاشر

P-ISSN : 2074-9554 | E-ISSN: 2663-811
Journal of Al-Farahidi's Arts
available online at : fja.tu.edu.iq/index.php/fja

Tikrit University J.F.A Journal of Al-Frahedis

Balancing the Monitoring of Students' Digital Behavior through Artificial Intelligence to Protect Them from Bullying and Their Right to Privacy: A Study of Ethical and Security Risks in Iraqi Educational Institutions

Sameeh Abdulghafour Jassim
QAYS NEAMAH IBRAHIM

E-Mail: prog85sameeh@gmail.com

Keywords:
Artificial Intelligence, Cyberbullying, Digital Privacy, Technological Ethics, Data Protection, E-Learning

Article history:

Received	11/9/2025
Received in revised form	3/10/2025
Accepted	19/10/2025
Available online	9/12/2025

E-mail Jaa@ tu.edu.iq

©THIS AN OPEN ACCESS ARTICLE UNDER THE CCBY LICENSE
http:// creativecommons.org/licenses/by/4.0

A B S T R A C T

The COVID-19 pandemic has accelerated the digital transformation of Iraq's educational sector, leading to the widespread adoption of e-learning platforms. However, this shift has contributed to a rise in cyberbullying, prompting proposals to utilize Artificial Intelligence (AI) to monitor student behavior and detect early signs of bullying. While potentially effective, these surveillance tools raise significant ethical concerns regarding student privacy, transparency, and digital rights. This paper utilizes a critical analytical method to examine the necessary balance between safeguarding students from cyberbullying and respecting their privacy, specifically within the Iraqi context. The study reviews recent literature, local and international legal regulations, and associated ethical risks. The findings highlight two critical deficiencies: the lack of a distinct Iraqi legal framework for personal data protection and inadequate cybersecurity measures in educational institutions. These gaps compromise the ethics and effectiveness of digital monitoring. Consequently, the study recommends developing comprehensive national strategies, implementing "privacy by design" principles, and enhancing digital literacy among students and teachers to ensure a safe and ethical digital learning environment..

التوازن بين رصد سلوك الطلاب الرقمي بواسطة الذكاء الاصطناعي لحمايتهم من التنمر وحقهم في الخصوصية: دراسة للمخاطر الأخلاقية والأمنية في المؤسسات التعليمية العراقية

م.د. سميح عبدالغفور جاسم المولى/ المديرية العامة لتربية الانبار
م.م. قيس نعمة ابراهيم جاسم / المديرية العامة لتربية الانبار

المستخلص:

يشهد القطاع التعليمي في العراق تحولاً رقمياً متسارعاً، يُعزى في المقام الأول إلى جائحة كوفيد-19، مما أدى إلى اعتماد منصات التعلم الإلكتروني والتطبيقات التفاعلية في القطاع التعليمي. في هذا السياق، لوحظ تزايد المخاوف بشأن انتشار التنمر الإلكتروني بين الطلاب، مما أدى إلى طرح بعض المقترحات التي تتضمن استخدام الذكاء الاصطناعي لمراقبة سلوك الطلاب الرقمي والتعرف على بدايات التنمر مبكراً. ورغم فعالية هذه الأدوات في الوقاية من الأمراض، إلا أنها تُثير التساؤلات حول خصوصية الطلبة وشفافيتهم وحقوقهم في العالم الرقمي. يهدف هذا البحث إلى مناقشة التوازن الضروري بين حماية الطلاب من التنمر الإلكتروني واحترام حقوقهم في الخصوصية، مع التركيز على السياق العراقي. يعتمد البحث على منهج تحليلي نقدي قائم على دراسة الأدبيات الحديثة والقوانين الدولية والمحلية، ودراسة المخاطر الأخلاقية والأمنية التي ينطوي عليها ذلك. كشفت الدراسة أن غياب إطار قانوني عراقي واضح لحماية البيانات الشخصية، وضعف البنية التحتية الأمنية في المؤسسات التعليمية، يُعدّان من أبرز المخاوف التي قد تؤثر على أخلاقيات وفعالية استخدام أنظمة المراقبة الرقمية. وتوصي الدراسة وضع استراتيجيات وطنية شاملة، وتطبيق مبدأ "الخصوصية من خلال التصميم"، وتعزيز التعليم الرقمي بين الطلاب والمعلمين، باعتبارهما أساسيين لخلق بيئة تعليمية رقمية آمنة وأخلاقية

الكلمات المفتاحية : الذكاء الاصطناعي، التنمر الإلكتروني، الخصوصية الرقمية، الأخلاقيات التكنولوجية، حماية البيانات، التعليم الإلكتروني

المقدمة:

شهدت المؤسسات التعليمية في العراق مؤخرًا تحولًا ملحوظًا نحو الرقمنة، نتيجةً للحاجة إلى الحفاظ على استمرارية التعليم خلال الأزمات الصحية وتحسين جودة العملية التعليمية (سرحان ومحمود وراضي، ص104، 2021). وقد أدى الانتشار المتزايد للمنصات الرقمية، مثل منصة نيوتن، وجوجل كلاس روم، ومايكروسوفت تيمز (Microsoft Teams)، ووسائل التواصل الاجتماعي المستخدمة لأغراض تعليمية، إلى ظهور ظاهرة جديدة ومخيفة في الأوساط التعليمية وهي التنمر الإلكتروني(Cyberbullying) أو التنمر عبر الإنترنت. يتميز التنمر الإلكتروني بسلوك عدواني متكرر يُمارس عبر الوسائط الرقمية، ويتورط فيه عدد كبير من الأفراد الذين لا يستطيعون الدفاع عن أنفسهم بسهولة(Atanasova-Pacemska, T. (2024)). وعلى الرغم من أنه لا يزال من غير المؤكد ما إذا كانت المعايير الثلاثة المتضمنة في **التعريف الشائع للتنمر** (Bullying) قابلة للتطبيق بالكامل على ظاهرة التنمر الإلكتروني، فإن **التعريف الأكثر شيوعاً** للتنمر الإلكتروني حتى الآن يتبنى هذا الافتراض، وينص على أنه: "عمل عدواني متعمد يُنفذ من قِبل فرد أو مجموعة من الأفراد، باستخدام أشكال الاتصال الإلكترونية، وبشكل متكرر وعلى مدى فترة من الزمن، ضد ضحية لا تستطيع الدفاع عن نفسها بسهولة" (Smith et al., 2008; Menesini et al., 2013; Hinduja & Patchin, 2015).

تشير الدراسات الأولية إلى أن حوالي 39.1٪ من طلاب المدارس الثانوية في المدن الرئيسية في العراق قد تعرضوا للتنمر الإلكتروني، وأن معظم هذه الحوادث وقعت عبر الرسائل الخاصة، أو الدروس، أو التعليقات على المنشورات. وفي ظل غياب آليات رقابة فعّالة، يزداد القلق بشأن العواقب النفسية والاجتماعية الخطيرة المحتملة، والتي تشمل الانتحار أو العزلة الاجتماعية(Yahya et al., 2015, 221-224)..

في المقابل، بدأت بعض المؤسسات التعليمية في الدول المتقدمة باستخدام الذكاء الاصطناعي لرصد السلوك الرقمي للطلاب، مستخدمةً تحليل المشاعر (Teferra et al., 2024, e55067)، ونمذجة اللغة الطبيعية(Teferra et al., 2024, e55067)، والتعلم الآلي (Hossain et al., 2025, 3332) للتعرف على بداية التنمر أو الخطر النفسي مبكرًا. ورغم أن هذه الأدوات قد تُعتبر وقائية، إلا أنها تطرح سؤالًا أخلاقيًا مهمًا: **هل يُبرر غرض**

الحماية تجاهل خصوصية الطلاب؟ وينطبق هذا بشكل خاص على بيئة مثل العراق، التي تفتقر إلى قواعد رسمية تتعلق بحماية البيانات الشخصية، وتفتقر إلى المعرفة بحقوق الخصوصية الرقمية.

1.1. أهداف البحث

يهدف هذا البحث إلى الإجابة عن التساؤلات التالية:

1. ما هي الفرص التي يوفرها الذكاء الاصطناعي في رصد وحماية الطلاب من التنمر الرقمي؟
2. وما هي أبرز المخاطر الأخلاقية والأمنية المترتبة على ذلك، خصوصًا في المؤسسات التعليمية العراقية؟
3. وكيف يُمكن تحقيق توازن دقيق بين الأخلاقيات والأمن عند استخدام الذكاء الاصطناعي لرصد التنمر الإلكتروني في المؤسسات التعليمية؟

2. الأساس النظري: العنف والتنمر التقليدي والإلكتروني والذكاء الاصطناعي

يركز هذا القسم على جوانب مهمة أبرزها تعاريف العنف والتنمر التقليدي والالكتروني واستخدام الذكاء الاصطناعي في البيئة التعليمية والتنمر الإلكتروني في سياق التعليم العراقي.

2. 1. تعريف العنف

يشير **العنف** في سياق العلوم الاجتماعية، وفقًا لـــ (عيد، 2019، ص ٥٧٥)، إلى **سلوك يهدف القائم به إلى إيذاء الآخرين عن قصد.** كما يعرف العنف، طبقاً لقاموس كامبردج لعلم الاجتماع، بأنه "التعبير الأكثر تطرفًا عن **القوة**"، حيث يشمل أقصى درجات القوة الكلية وتتضمن أشكاله :**الضرر، والاغتصاب، والتعذيب، والقتل**(عبدي، فاطمة. 2023. ص29-42).

2. 2. تعريف التنمر التقليدي(Face-to-Face Bullying)

يُعرف **التنمر التقليدي** أو **التنمر وجهًا لوجه** بأنه **سلوك متعمد ومتكرر** ينتج عنه إلحاق الأذى بالآخرين، سواء كان هذا الأذى **بدنيًا أو نفسيًا** .وهو من أنماط العنف السائدة في المدارس.

ويمكن أن يتخذ هذا العنف شكلين رئيسيين:(Boulton et al., 2008, 474-475)

- **عنف مباشر** :كالعنف البدني.

- **عنف غير مباشر** :كالعزل الاجتماعي ونشر الإشاعات.

2. 3. تعريف التنمر الإلكتروني(Cyberbullying)

يُعرف **التنمر الإلكتروني (Cyberbullying)** وفقًا لـــ (Tokunaga, 2010, 12) على أنه: "تعرض الإنسان للتنمر عندما يوجه له **أفعال سلبية** من أشخاص آخرين بشكل **متكرر** في فترة زمنية، وفي نفس الوقت يكون **ضعيف القدرة على الدفاع عن نفسه**."(القحطاني، اثيل حسين ناصر. 2023. 60-93)

2. 4. استخدام الذكاء الاصطناعي في البيئة التعليمية

يُستخدم الذكاء الاصطناعي في قطاع التعليم لأغراض متعددة، بما في ذلك التعليم المُخصص، والتقييم الآلي، ومراقبة السلوك (Zawacki-Richter, 2024, 32). فيما يتعلق بمكافحة التنمر، تستخدم الأنظمة الحديثة نماذج لغوية تُحلل المواد المكتوبة (مثل الرسائل والتعليقات والمنشورات) للتعرف على الكلمات أو العبارات العدائية أو المهددة أو حتى المُزعجة. كما يُمكن دمج تحليل الصوت والفيديو في نظام يكشف عن أي تغيرات في الصوت أو تعابير الوجه التي تُشير إلى ضغوط نفسية(كاكايارودون، 2015).

2.5. التنمر الإلكتروني في سياق التعليم العراقي

على عكس التنمر التقليدي، يتميز التنمر الإلكتروني بغياب القيود المادية أو الزمنية، وسرعة انتشاره، وصعوبة تتبع مرتكبه. في العراق، تتفاقم هذه المشكلة بسبب:

1. شيوع استخدام الهواتف الذكية بين المراهقين دون إشراف الوالدين.
2. الفجوة الرقمية بين الآباء والمعلمين.
3. غياب سياسات مُحددة بشأن هذه الظاهرة في المدارس والجامعات.

3. التعقيدات الأخلاقية لرصد السلوك الرقمي

يقدم هذا القسم شرحا مفصلاً عن أهم التعقيدات الأخلاقية التي تواجه عملية الرصد للسلوك الرقمي مثل انتهاك الخصوصية والتحيز الخوارزمي والفساد وانعدام الشفافية.

3. 1. انتهاك الخصوصية

حتى 2025، لم يُسنّ في العراق قانون حماية البيانات الشخصيّة ليكون شاملًا ومطبّقًا على نطاق واسع؛ توجد مسودات ومشروعات لقوانين حماية البيانات، لكن الفجوة التشريعية لا

تزال قائمة مقارنة بدول أخرى. هذا الفراغ يشكّل مخاطرة لتبنّي أنظمة رصد دون ضمانات قانونية واضحة لحقوق الطلبة وواجبات المؤسسات التعليمية. كما تُشير قواعد الاعتماد والنشر في المجلات المحلية إلى ضرورة الحصول على موافقات أخلاقية قبل إجراء دراسات تتعامل مع بيانات بشريّة (Law Gratis، موقع الكتروني). كما وتُعتبر المراقبة المستمرة للطلاب، حتى لأسباب أمنية، شكلاً من أشكال المراقبة واسعة النطاق، مما يؤدي إلى خلق بيئة يسودها الشك والخوف، مما يُضعف الثقة بين الطلاب والمعلمين. إضافةً إلى ذلك، يُعد جمع البيانات الشخصية (مثل سجلات الدردشة، وأنماط الاستخدام، وحتى المعلومات الجغرافية) دون موافقة الطالب انتهاكًا لمبادئ الخصوصية الرقمية (حمد، أماني علي محمد مصطفى. 2021. 18-52).

يُعرّف **الحق في الخصوصية** في مفهومه التقليدي بأنه حق الفرد في أن يقرر بنفسه متى وإلى أي مدى يمكن للآخرين الاطلاع على شؤونه الخاصة(حمد، أماني علي محمد مصطفى. 2021. 18-52).

ومع تزايد الاعتداءات على الحياة الخاصة التي تفرضها التطورات التقنية والمعلوماتية، أصبح من الضروري إعادة النظر في هذا المفهوم. فقد باتت التقنيات الحديثة، مثل(الموسوي، منى تركي وفضل الله، جان سيريل. 2013. 307):

- كاميرات المراقبة.
- بطاقات الهوية الإلكترونية.
- قواعد البيانات الشخصية.
- وسائل اعتراض ومراقبة البريد والاتصالات.
- رقابة بيئة العمل.

تشكل جميعها مخاطر تهدد الخصوصية، مما زاد الاهتمام بهذا الحق في ظل التقدم التكنولوجي والمعلوماتي المتسارع. كما تنوعت نظم الرصد المستعملة ومن أبرزها (S. KAVIN. 2025. 350-358):

- **مراقبة المحتوى النصّي والرسائل:** وهي أنظمة تفحص محادثات البريد الإلكتروني أو منصات المحادثة باستخدام نماذج تصنيف لاكتشاف كلمات أو عبارات ذات دلالة على تنمّر أو انتحار.

- **تحليل السلوك عبر الأفعال الرقمية:** وهي نماذج تقيس أنماط التصفح، توقيت النشاط، وتكرار رسائل معيّنة لكشف سلوك شاذ.
- **رصد عبر الرؤية الحاسوبية (كاميرات الصفّ):** وهي عملية الكشف عن تعابير الوجه أو حركة الجسم لاستخلاص مؤشرات مزاجية أو سلوك عدائي.

ومن أهداف أنظمة الرصد وفوائدها المتوقعة هو كشف مبكر للتنمر أو العنف أو الحالات العقلية الخطرة وتيسير تدخل مشرفي المدرسة أو خدمات الصحة النفسية وتوفير الاستجابة السريعة لحماية الطلاب.

3. 1. 1. تصنيفات الخصوصية

يمكن تقسيم مفهوم الخصوصية، المرتبط ببعضه البعض، إلى عدة مفاهيم فرعية(الموسوي، منى تركي وفضل الله، جان سيريل. 2013. 12-18)

- **خصوصية المعلومات:** وتشمل القواعد المنظمة لجميع إجراءات إدارة **البيانات الخاصة**، كالمعلومات المدرجة في بطاقات الهوية.
- **الخصوصية المادية (الجسدية):** تتعلق بتوفير **الحماية الجسدية للأفراد** ضد أي إجراءات تمس النواحي المادية، مثل فحوصات المخدرات.
- **خصوصية الاتصالات:** تتضمن ضمان **سرية وخصوصية المراسلات الهاتفية، والبريد الإلكتروني**، وغيرها من أشكال الاتصالات.
- **الخصوصية الإقليمية :**تتعلق بالقواعد التي تنظم **الدخول إلى المنازل، وبيئة العمل، والأماكن العامة.**

3. 2. التحيز الخوارزمي

من المرجح أن تكون النماذج المستخدمة في الذكاء الاصطناعي غير دقيقة، نظرًا لتدريبها في البداية على بيانات لا علاقة لها بالبيئة العراقية. على سبيل المثال، قد تُعتبر اللغة المحلية أو التقاليد الثقافية مُخيفة أو مُتنمرة. وهذا يؤدي إلى عقوبات مُضللة أو ازدراء للطلاب الأبرياء. كما وتُظهر بعض الدراسات أن نماذج التعلم الآلي قد تكون متحيّزة ضد مجموعات طلابية معينة (نوعًا اجتماعيًا أو لغويًا أو عرقيًا)، ما يؤدي إلى معدلات إنذار زائفة أعلى لفئات

معيّنة، وبالتالي تكون هناك إجراءات غير عادلة ضدهم. مما يستوجب عملية تقييم هذه الأنظمة لعدم التحيّز قبل التطبيق(Pikhart. 2025. 1-10).

3. 3. الفساد وانعدام الشفافية

تتميز العديد من أنظمة الذكاء الاصطناعي بـــ"الصناديق السوداء"، مما يجعل من المستحيل فهم كيفية اتخاذ القرارات. وفي حالة عدم وجود آليات فعالة للتظلم، قد يُحرم الطالب من حق الاعتراض على قرار محوسب من شأنه أن يؤثر على مستقبله الأكاديمي أو الاجتماعي.

3. 4. أخطار إساءة الاستخدام ومشاركة البيانات مع جهات خارجية

قد تُشارك الشركات المزودة لأدوات الرصد بيانات مُعرّفة أو غير مُعرّفة مع جهاتٍ تجارية أو حكومية. غياب رقابة تشريعية صارمة يزيد احتمال استخدام البيانات لأغراض غير معلنة (مثلاً المراقبة التأديبية أو أمنية)، وهو ما يثير مخاوف خاصة في البيئات السياسية الحساسة(IAPP، موقع الكتروني).

4. تحقيق التوازن

لتحقيق التوازن المطلوب بين حماية الطلاب بالذكاء الاصطناعي واحترام خصوصيتهم، يجب على المؤسسات التعليمية والجهات الحكومية في العراق تبني إطار عمل متعدد الأبعاد يركز على الأخلاقيات والشفافية والأمن:

4. 1. الإطار التنظيمي والتشريعي

1. **إصدار قانون حماية البيانات التعليمية** :يجب على الحكومة العراقية الإسراع في تطوير وإقرار **تشريعات وطنية** لحماية البيانات الشخصية للطلاب على غرار اللائحة العامة لحماية البيانات((General Data Protection Regulation (GDPR) ، تحدد بوضوح أنواع البيانات المسموح بجمعها، مدة تخزينها، وإجراءات حذفها (المركز الديمقراطي العربي، 2024).
2. **مبدأ الغرض المخصص والتقليل** :يجب أن يُنص على أن رصد سلوك الطلاب يتم فقط لغرض "مكافحة التنمر والسلامة" حصرًا، وتطبيق **مبدأ تقليل البيانات (Data Minimization)**، أي جمع الحد الأدنى من البيانات الضرورية لتحقيق هذا الهدف.

3. **إلزامية الشفافية والمساءلة :**إلزام المؤسسات بـــ "**شرح القرار** "المتخذ بواسطة الذكاء الاصطناعي، وتوفير آليات تظلم للطلاب وأولياء الأمور للطعن في قرارات الرصد.

4. 2. الإجراءات الفنية والأمنية

1. **الخصوصية بالتصميم (Privacy by Design)** : يجب أن تُبنى أنظمة الذكاء الاصطناعي المستخدمة في الرصد على مبدأ إخفاء الهوية والتشفير القوي لبيانات الطلاب منذ اللحظة الأولى للجمع.
2. **مراجعة التحيز الخوارزمي:** إجراء تدقيق أخلاقي دوري ومراجعات مستقلة للنماذج للتأكد من خلوها من أي تحيز ضد مجموعات طلابية محددة.
3. **الأمن السيبراني والبنية التحتية:** الاستثمار في تعزيز قدرات الأمن السيبراني للمؤسسات التعليمية وتدريب الكوادر الفنية على أحدث بروتوكولات حماية البيانات لتقليل مخاطر الاختراق(Alsammarraie. 2025. 65-79).

4. 3. التثقيف والتوعية

1. **الموافقة المستنيرة :**الحصول على **موافقة صريحة ومستنيرة** من أولياء الأمور والطلاب على عملية الرصد، مع تزويدهم بمعلومات واضحة حول كيفية استخدام بياناتهم.
2. **التثقيف على المواطنة الرقمية :**إطلاق برامج تدريبية للطلاب والمعلمين على **المواطنة الرقمية المسؤولة**، وأهمية الخصوصية والسلوك المحترم عبر الإنترنت، بدلاً من الاعتماد الكلي على المراقبة الآلية.

5. المبادئ التأسيسية لأخلاقيات الذكاء الاصطناعي في المنظومة الأكاديمية

يُعدّ تعريف **أخلاقيات الذكاء الاصطناعي (Artificial Intelligence Ethics)** أمرًا جوهريًا لترسيخ الممارسات المسؤولة في تطوير وتطبيق هذه التقنيات. يمكن بلورة تعريف أخلاقيات الذكاء الاصطناعي كما عرفها (Nasim ، 55) بأنها: "مجموعة من **المبادئ والقيم** التي توجه **السلوك الأخلاقي** في تطوير واستخدام أنظمة وتطبيقات الذكاء الاصطناعي، بطريقة **عادلة ومسؤولة وأخلاقية**، وتحمي حقوق الإنسان والقيم الاجتماعية". وهناك تعريف آخر لأخلاقيات الذكاء الاصطناعي عرفها (عبدالكريم، 2024) بأنها "مجموعة من **المبادئ والقيم الناظمة** التي

تسيطر وتضبط أداء الآلات، ومحتواها، ومستخدميها، والبرامج المتحكمة فيها. وتهدف هذه المنظومة إلى مساعدة **مخترعي وباحثي تطبيقات الذكاء الاصطناعي** على **التمييز بين الصواب والخطأ**، وتمكينهم من العمل بطريقة مسؤولة ومحاسبة. وتُعدّ هذه المنظومة **ميثاقاً أخلاقياً ملزماً** لجميع الأطراف المعنية".

5. 1. الأهمية التأسيسية لأخلاقيات الذكاء الاصطناعي

تعد الأخلاق الحجر الأساسي في تحديد التفاعلات الإنسانية المجتمعية، والمنظمات، وهي المحرك الأساسي لسلوك الفرد والمجتمع. في سياق الثورة الرقمية، باتت **منظومة أخلاقيات الذكاء الاصطناعي (AI Ethics Framework)** ضرورة ملحة وأكثر أهمية من أي وقت مضى، كونها تؤثر على كافة جوانب حياة الأفراد والمجتمعات. لا تهدف هذه المنظومة إلى وضع قيود، بل توجيه تطبيقات الذكاء الاصطناعي لضمان تحقيقها للمصلحة البشرية العليا (OECD, 2019). كما وتُعد هذه المبادئ ركيزة لأي مؤسسة تعليمية أو بحثية تتبنى تقنيات الذكاء الاصطناعي لضمان استخدام آمن ومسؤول.

5. 2. المبادئ الأخلاقية المعتمدة عالمياً

تستند المبادئ الأخلاقية للذكاء الاصطناعي إلى إطارات عمل دولية صادرة عن منظمات رائدة مثل منظمة التعاون الاقتصادي والتنمية (OECD) في عام 2019، ومنظمة اليونسكو (UNESCO)في عام 2021. وتشمل هذه المبادئ التأسيسية ما يلي:

5. 2. 1. التنمية المستدامة(Sustainability)

يركز هذا المبدأ على ضرورة تسخير تطبيقات الذكاء الاصطناعي لخدمة **أهداف التنمية الشاملة والمستدامة**، بما يضمن تحقيق النفع العام للأفراد والمجتمعات. ويشمل ذلك تعزيز الأثر الإيجابي للتقنيات، وضمان الرفاهية، والحفاظ على الموارد البيئية للأجيال القادمة (UNESCO, 2021).

5. 2. 2. حقوق الإنسان(Human Rights)

يؤكد هذا المبدأ على ضرورة إنتاج واستخدام الذكاء الاصطناعي بطريقة تدعم **حقوق الإنسان** وتتوافق مع المواثيق الدولية. ويتطلب ذلك اتخاذ التدابير اللازمة لتقليل احتمالية **انتهاك الخصوصية**، أو تهديد حياة الأفراد، أو التسبب بأي شكل من أشكال العنف أو الضرر النفسي.

كما يشدد على مبادئ **المساواة والعدل، وعدم التمييز، والشفافية، والنزاهة** في التعامل مع البيانات والممتلكات(OECD, 2019) .

5. 2. 3. توفير بيئة آمنة(Safety and Security)

يهدف هذا المبدأ إلى إرساء الشعور بالأمان والثقة عند التعامل مع تطبيقات الذكاء الاصطناعي، وذلك من خلال توفير حد عالٍ من **الأمن الرقمي**. ويتطلب ذلك آليات قوية للتصدي للتهديدات الإلكترونية، بما في ذلك الجرائم الإلكترونية، والقرصنة، والابتزاز، وانتهاك البيانات، وحماية الملكية الفكرية، وضمان سلامة الأنظمة ضد أي تهديدات أمنية محتملة.

5. 2. 4. المساءلة والمسؤولية(Accountability and Responsibility)

يركز هذا المبدأ على ضرورة وجود **أطر تنظيمية** واضحة لتسيير عملية تصميم، واستخدام، وتطوير أنظمة الذكاء الاصطناعي. كما يوجب **تحديد المسؤولية** القانونية والأخلاقية بوضوح عند وقوع أخطاء تقنية أو إخفاقات، أو في حال غياب تطبيق العقوبة القانونية لأخطار تطبيقات الذكاء الاصطناعي(UNESCO, 2021) .

6. الجهود العالمية لصياغة أخلاقيات الذكاء الاصطناعي

تعد صياغة إطار عالمي لأخلاقيات الذكاء الاصطناعي مسعى تعاونياً تشارك فيه الحكومات، والمنظمات الدولية، والأوساط الأكاديمية، والقطاع الخاص. تهدف هذه الجهود إلى تجاوز التحديات العابرة للحدود التي يفرضها الذكاء الاصطناعي، لا سيما في مجالات الخصوصية والتحيز والمساءلة.

6. 1. المنظمات الدولية والمبادرات الرئيسية

- **منظمة التعاون الاقتصادي والتنمية(OECD) :** أصدرت في عام 2019 **مبادئ الذكاء الاصطناعي الخمسة**، التي تُعد أول مجموعة مبادئ متفق عليها بين الحكومات لتوجيه صناع السياسات والجهات الفاعلة في مجال الذكاء الاصطناعي. تركز المبادئ على النمو الشامل، والرفاهية، وقيم الإنسان، والشفافية، والمساءلة، والأمن (OECD, 2019).

- **منظمة الأمم المتحدة للتربية والعلم والثقافة (UNESCO)** : تبنت في عام 2021 **توصية أخلاقيات الذكاء الاصطناعي**، وهي أول وثيقة عالمية تضع إطاراً أخلاقياً للذكاء الاصطناعي، تركز بشكل خاص على الجوانب الثقافية والتعليمية والبيئية، وتشدد على ضرورة "إضفاء الطابع الإنساني" على الذكاء الاصطناعي (UNESCO, 2021).
- **الاتحاد الأوروبي (EU)** : يعمل على تطوير **قانون الذكاء الاصطناعي(AI Act)** ، الذي يهدف إلى وضع إطار تنظيمي شامل ومستقبلي يعتمد على منهجية المخاطر، حيث يفرض متطلبات صارمة على أنظمة الذكاء الاصطناعي عالية المخاطر (European Commission, 2023).

6. 2. دور الأوساط الأكاديمية والمجتمع المدني

تلعب الجامعات ومراكز الأبحاث دوراً محورياً في هذا الإطار من خلال:

1. **البحث والتدقيق:** إجراء أبحاث معمقة لفهم التحديات الأخلاقية والخوارزمية للذكاء الاصطناعي، ووضع أدوات لـــ**تدقيق التحيز والشفافية**.
2. **التوعية والتعليم:** إدماج أخلاقيات الذكاء الاصطناعي ضمن المناهج التعليمية لتدريب الجيل القادم من المطورين والمستخدمين على المسؤولية الرقمية.
3. **تطوير المعايير:** المساهمة في وضع المعايير التقنية والأخلاقية اللازمة لتصميم الأنظمة الذكية بطريقة تحترم الخصوصية والسلامة منذ مرحلة التصميم **(Privacy by Design)**.

7. توصيات عملية ومقترحات سياسة للجامعات والمدارس العراقية

7. 1. مبادئ توجيهية عامة

1. **الشفافية:** إعلام الطلاب وأولياء الأمور بوضوح عن وجود نظام الرصد، أهدافه، البيانات المجمعة، ومَن يمتلكها.
2. **التقليل من الجمع (Data Minimization)** : جمع أقل قدر ممكن من البيانات الضرورية لغرض محدد ومقنن.

3. **الموافقة الصريحة والمستنيرة:** موافقة كتابية من أولياء الأمور للطلبة القُصّر، مع حق سحب الموافقة.
4. **التحقق البشري قبل اتخاذ الإجراء:** أي تنبيه تصدره الخوارزمية يجب أن يخضع لمراجعة إنسانية قبل أي إجراء صارم .

7. 2. تدابير تقنية وأمنية

1. **تشفير قوي** للبيانات عند النقل والتخزين، مع سياسات إدارة مفاتيح صارمة.
2. **تقليل الاحتفاظ بالبيانات** : سياسات حذف دورية للبيانات غير الضرورية.
3. **اختبارات اختراق وتدقيق أمني دوري** لضمان عدم تسريب أو تحوّل الاستخدام .

7. 3. سياسات مؤسسية وقانونية

على المستوى الوطني، تشجيع تسريع سنّ تشريع حماية البيانات الشخصية يحدد حقوق الأفراد وواجبات المؤسسات. حتى مع عدم وجود قانون شامل، يتعيّن على الجامعات تبني سياسات داخلية تحاكي معايير الخصوصية الدولية .

7. 4. التعليم والتوعية

تدريب المعلمين، الطلبة، وأولياء الأمور على مخاطر وفوائد نظم الرصد، وخلق قنوات تواصل عادلة للبلاغات عن إساءة الاستخدام.

8. الاستنتاجات

يمثل رصد السلوك الرقمي للطلاب بواسطة الذكاء الاصطناعي في المؤسسات التعليمية العراقية سلاحًا ذا حدين. فبقدر ما يقدم من إمكانات غير مسبوقة للكشف عن التنمر الرقمي وحماية الطلاب، فإنه يفتح الباب واسعًا أمام مخاطر أخلاقية وأمنية كبيرة تهدد حقهم في الخصوصية، خاصة في ظل النقص التشريعي وضعف البنى التحتية الوطنية.

يتطلب تحقيق التوازن الفعال تبني **استراتيجية وطنية شاملة** للذكاء الاصطناعي في التعليم، لا تركز فقط على الجانب التقني، بل تضع **أخلاقيات الذكاء الاصطناعي وحماية البيانات الشخصية للطالب** في صلب أولوياتها. إن غياب إطار قانوني وتنظيمي شفاف وعادل يهدد بتحويل تقنية الحماية إلى أداة للمراقبة وانتهاك الخصوصية، مما يقوض الثقة في المنظومة

التعليمية الرقمية برمتها. لذا، فإن الدعوة لتطوير تشريعات متخصصة وتدريب الكوادر الأمنية والأخلاقية أصبحت أمرًا حتميًا لضمان مستقبل رقمي آمن وأخلاقي للطلاب في العراق.

أولاً: المراجع العربية

1. حمد، أماني علي محمد مصطفى. (2021). "واقع القيم الأخلاقية لدى جامعة أسيوط في العصر الرقمي (دراسة ميدانية)". المجلة التربوية لتعميم الكبار – كلية التربية – جامعة أسيوط. المجلد الثالث – العدد الثاني، ص 18–52.
2. سرحان، مصطفى طه ومحمود، شيماء صفاء و راضي، رسمية خريبط. (2021) " جاهزية المؤسسات التعليمية العراقية على العمل بنظام التعليم الرقمي في ظل جائحة كورونا". وقائع المؤتمر الدولي الأول– التعليم الرقمي في ظل جائحة كورونا–. ملحق مجلة الجامعة العراقية. العدد (2/15).
3. عبدالكريم، عبدالرزاق عبدالكريم عبدالرزاق. (2024). "المخاطر الأخلاقية لتطبيقات الذكاء الاصطناعي "دراسة تحليلية"". مجلة كلية التربية، بنها، العدد (137) ج1. ص 329–376.
4. عبدي، فاطمة. (2023). "ماهية العنف: مفهومه، انواعه، مظاهره، وأهم النظريات المفسرة له" مجلة العلوم الاجتماعية والإنسانية، جامعة باتنة. المجلد (24) العدد (01)، ص29–42.
5. عيد ، محمود عمر احمد. (2019). "واقع التنمر الالكتروني على شبكات التواصل الاجتماعي بين طلاب الجامعة : دراسة حالة لجامعة الفيوم، جامعة سوهاج–كلية التربية.
6. القحطاني، أثيل حسين ناصر. (2023). " التنمر الالكتروني على مواقع التواصل الاجتماعي". مجلـــة أقلام، المجلد (02) العـــــــدد: (01)، ص60–93.
7. كاكايار دون، إغينيو وكال، دانيت وألفي، تياغو، و مارتينيز، غابرييلا. (2015). مكافحة خطاب الكراهية في الانترنت. UNESCO Publishing، ISBN: 978–92–3–600040–4.

8. المركز الديمقراطي العربي. (2024). كتاب "مستقبل الذكاء الاصطناعي تحديات قانونية وأخلاقية". الطبعة الأولى. القاهرة. ص174–199.
9. الموسوي، منى تركي وفضل الله، جان سيريل. (2013). "الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها". مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد خاص بمؤتمر الكلية.

ثانياً: المواقع الالكترونية:

1. "Data protection and privacy laws now in effect in 144 countries | IAPP." https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries?utm_source=chatgpt.com (accessed Sep. 03, 2025).
2. "Law Gratis." https://www.lawgratis.com/blog-detail/privacy-law-at-iraq?utm_source=chatgpt.com (accessed Sep. 01, 2025).

ثالثاً: المراجع الأجنبية:

1. Alsammarraie, R. M. (2025). Artificial Intelligence and Digital Transformation in Iraq: Strategic Integration Framework. Journal of Madenat Alelem University College, 17(1), 65-79.
2. Atanasova-Pacemska, T. (2024). A Cross-National Perspective of Prejudice-Based Cyberbullying and Cybervictimization (Chapter IX) International Perspectives on Migration, Bullying, and School.
3. Boulton, M. J., Trueman, M., & Murray, L. (2008). Associations between peer victimization, fear of future victimization and disrupted concentration on class work among junior school pupils. British Journal of Educational Psychology, 78(3), 473-489.
4. European Commission. (2023). Artificial Intelligence Act: A European approach to AI.
5. Hinduja, S., & Patchin, J. W. (2015). Bullying beyond the schoolyard: Preventing and responding to cyberbullying (2nd ed.). Thousand Oaks, CA: Sage Publications.
6. Hossain, M. M., Hossain, M. S., Mridha, M. F., Safran, M., & Alfarhood, S. (2025). Multi task opinion enhanced hybrid BERT model for mental health analysis. Scientific Reports, 15(1), 3332.
7. Menesini, E., Nocentini, A., Palladino, B. E., Scheitauer, H., Schultze-Krumbholz, A., Frisèn, A., Berne, S., Luik, P., Naruskov, K., Ortega, R., Calmaestra, J., & Blaya, C. (2013). Definitions of cyberbullying. In: P. K. Smith & G. Steffgen (Eds.), Cyberbullying through the new media: Findings from an international network. Abingdon-on-Thames, Oxfordshire: Psychology Press.

8. Nasim, S. F., Ali, M. R., & Kulsoom, U. (2022). Artificial intelligence incidents & ethics a narrative review. International Journal of Technology Innovation and Management (IJTIM), 2(2), 52-64.
9. OECD. (2019). OECD Principles on Artificial Intelligence. Organisation for Economic Co-operation and Development.
10. Pikhart, M., & Al-Obaydi, L. H. (2025). Reporting the potential risk of using AI in higher Education: Subjective perspectives of educators. Computers in Human Behavior Reports, 18, 100693.
11. S. KAVIN, Dr. A. ADHISELVAM, "AI-Based Classroom Monitoring System," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), (2025), DOI 10.17148/IJIREEICE.2025.13458 , PP. 350-358.
12. Smith, P. K. , Mahdavi, J. , Carvalho, M. , Fisher, S. , Russel, S. N. and Tippett, N. (2008). Cyberbullying: It's nature and impact in secondary school pupils'. Journal of Child Psychology and Psychiatry, 49, 376–385.
13. Teferra, B. G., Rueda, A., Pang, H., Valenzano, R., Samavi, R., Krishnan, S., & Bhat, V. (2024). Screening for depression using natural language processing: literature review. Interactive Journal of Medical Research, 13(1), e55067.
14. Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in human behavior, 26(3), 277-287.
15. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. United Nations Educational, Scientific and Cultural Organization.
16. Yahya, H. M., Hashim, M. T., Al-Kaseer, E. A., & Al-Diwan, J. K. (2015). Bullying victimization among school-going adolescents in Iraq. Journal of the Faculty of Medicine Baghdad, 57(3), 221-224.
17. Zawacki-Richter, O., Bai, J. Y., Lee, K., Slagter van Tryon, P. J., & Prinsloo, P. (2024). New advances in artificial intelligence applications in higher education?. International Journal of Educational Technology in Higher Education, 21(1), 32.