استخدام الذكاء الاصطناعي في اكتشاف التهديدات الأمنية على الانتخابات

أبو حرارة عبد السلام*
قسم علم الاجتماع، كلية الآداب، جامعة الزاوية ، ليبيا
البريد الالكتروني: a.almuwalif@zu.edu.ly
تاريخ الارسال 2025/8/3م تاريخ القبول 2025/9/25م

The Use of Artificial Intelligence in Detecting Security Threats to Elections

Abuharara Abdulsalam*
Department of Sociology, Faculty of Arts, University of Zawia, Libya

Abstract

This study aimed to explore the use of artificial intelligence (AI) in detecting security threats to elections. Specifically, it sought to: assess the effectiveness of AI technologies in the early detection of security threats targeting the integrity of the electoral process; identify the most prominent types of digital threats that AI can monitor and analyze in the electoral context; examine the technical and ethical challenges associated with the use of AI in securing elections; and investigate mechanisms for employing AI in a balanced manner that ensures the security of the electoral process without infringing on privacy or freedom of expression. The researcher adopted the descriptive methodology, as it is well-suited to the objectives of the study.
The study arrived at the following findings:

- The results indicate that AI technologies possess a high capability for the early detection of security threats to electoral integrity. This is achieved through the analysis of big data and the rapid and accurate identification of suspicious patterns, outperforming traditional methods.
- The study revealed that the most prominent types of digital threats that AI can detect include phishing attacks and manipulation of electronic voting results.

- The study identified key technical challenges in utilizing AI for election security, including the necessity of accurate data, protection of systems against poisoning attacks, and ensuring compatibility with diverse technological infrastructures.
- The study underscored the importance of employing AI in a balanced and transparent manner that safeguards the electoral process while respecting individual privacy and freedom of expression. This can be achieved through the adoption of transparent mechanisms that allow for the review and auditing of decisions made by intelligent systems.

Keywords: Artificial Intelligence – Security Threats – Elections

الملخـــــــص:

هدفت الدراسة إلى التعرف على استخدام الذكاء الاصطناعي في اكتشاف التهديدات الأمنية على الانتخابات وذلك على النحو الاتي: التعرف على مدى فاعلية تقنيات الذكاء الاصطناعي في الكشف المبكر عن التهديدات الأمنية التي تستهدف نزاهة العملية الانتخابية، والتعرف على أبرز أنواع التهديدات الرقمية التي يمكن للذكاء الاصطناعي رصدها وتحليلها في السياق الانتخابي، وكذلك التعرف على التحديات التقنية والأخلاقية التي تواجه استخدام الذكاء الاصطناعي في تأمين الانتخابات، وايضاً التعرف على آليات توظيف الذكاء الاصطناعي بشكل متوازن يحافظ على أمن العملية الانتخابية دون المساس بالخصوصية أو حرية التعبير، واتبع الباحث المنهج الوصفي لملائمته لأغراض الدراسة، وتوصلت الدراسة إلى النتائج الآتية:-

ـ توضح نتائج البحث أن تقنيات الذكاء الاصطناعي تتمتع بقدرة عالية على الكشف المبكر عن التهديدات الأمنية التي تستهدف نزاهة العملية الانتخابية، وذلك من خلال تحليل البيانات الكبيرة والتعرف على الأنماط المشبوهة بشكل أسرع وأكثر دقة مقارنة بالطرق التقليدية.

ـ أظهرت الدراسة أن أبرز أنواع التهديدات الرقمية التي يمكن للذكاء الاصطناعي رصدها تشمل هجمات التصيد الاحتيالي، والتلاعب في نتائج التصويت الإلكتروني.

ـ كشفت الدراسة أن التحديات التقنية المتعلقة باستخدام الذكاء الاصطناعي في تأمين الانتخابات تتمثل في ضرورة توفر بيانات دقيقة، وحماية الأنظمة من هجمات التسميم، وضمان التوافق مع البنى التحتية للتقنية المتنوعة.

ـ تبينت أهمية توظيف الذكاء الاصطناعي بشكل متوازن يحقق أمن العملية الانتخابية دون المساس بالخصوصية أو حرية التعبير عبر اعتماد آليات شفافة تتيح مراجعة وتحليل القرارات التي تتخذها الأنظمة الذكية.

الكلمات المفتاحية: الذكاء الاصطناعي- التهديدات الأمنية-الانتخابات

مقدمة:

تُعدُّ الانتخابات إحدى الركائز الأساسية التي تقوم عليها الأنظمة الديمقراطية في العالم، إذ تُعبر عن إرادة الشعوب في اختيار ممثليهم وتحديد مسارات السياسات العامة، وبما يعكس تطلعات المواطنين وطموحاتهم، ومع التقدم التكنولوجي السريع والتحول الرقمي المتزايد في مختلف المجالات، بما في ذلك المجال السياسي والانتخابي، باتت العمليات الانتخابية أكثر عرضة لمجموعة من التهديدات الأمنية، سواء كانت داخلية أو خارجية، مادية أو رقمية، فقد شهد العالم في السنوات الأخيرة محاولات متكررة للتأثير على نتائج الانتخابات، سواء من خلال الهجمات السيبرانية على البنية التحتية للمعلومات، أو من خلال التضليل الإعلامي عبر وسائل التواصل الاجتماعي، أو عبر محاولات اختراق قواعد بيانات الناخبين ونظم التصويت الإلكتروني.

وفي ظل هذا الواقع المعقد والمتغير، برز الذكاء الاصطناعي كأداة واعدة يمكن أن تسهم بشكل فعال في رصد واكتشاف التهديدات الأمنية التي قد تستهدف الانتخابات، بل والتنبؤ بها قبل وقوعها، فالذكاء الاصطناعي، وبما يمتلكه من قدرات تحليلية هائلة وسرعة في معالجة كميات ضخمة من البيانات، يوفر إمكانيات غير مسبوقة في تتبع الأنماط السلوكية غير الطبيعية، ورصد محاولات التدخل الخارجي، والكشف عن حملات التضليل الممنهجة، إضافة إلى مراقبة سلامة أنظمة التصويت الرقمية وتحليل نقاط الضعف فيها.

ويُنظر إلى الذكاء الاصطناعي اليوم كعنصر محوري في تعزيز أمن الانتخابات، ليس فقط من خلال الاستجابة للتهديدات، وإنما عبر العمل ألاستباقي للوقاية منها، فخوارزميات التعلم الآلي مثلًا يمكنها التعرف على أنماط الهجمات السيبرانية المعروفة واستشراف أشكال جديدة منها، بينما يمكن لتحليل اللغة الطبيعية (NLP) تتبع المحتوى المضلل عبر الإنترنت وتحديد الجهات الفاعلة وراءه، ومما يساهم في رفع مستوى الشفافية والمصداقية في العملية الانتخابية.

ومع ذلك فإن إدماج الذكاء الاصطناعي في هذا المجال لا يخلو من التحديات، فهناك مخاوف مشروعة تتعلق بالخصوصية، والانحياز الخوارزمي، واحتمالات استخدام نفس التقنيات لأغراض معاكسة، كقمع الحريات أو التلاعب بالرأي العام،و كما أن الاعتماد الزائد على الأنظمة الذكية دون وجود رقابة بشرية كافية قد يؤدي إلى نتائج غير دقيقة أو غير عادلة، ومما يستدعي وضع أطر قانونية وأخلاقية صارمة لتنظيم استخدام الذكاء الاصطناعي في السياقات الانتخابية.

ومن هنا تبرز أهمية دراسة هذا الموضوع بشكل معمق لفهم الدور المتنامي للذكاء الاصطناعي في تأمين العمليات الانتخابية، مع التركيز على آليات استخدامه، ومجالات تطبيقه، والتحديات المرتبطة به، إضافة إلى استعراض أبرز التجارب الدولية في هذا المجال، ويهدف هذا البحث إلى تسليط الضوء على كيفية توظيف الذكاء الاصطناعي بشكل فعّال لرصد وكشف التهديدات الأمنية التي قد تُهدد نزاهة الانتخابات، وضمان سيرها بطريقة شفافة وآمنة تعزز ثقة المواطنين في الديمقراطية ومؤسساتها.

أولاً- مشكلة الدراسة:

في ظل الثورة الرقمية التي يشهدها العالم، أصبحت العمليات الانتخابية عرضة لتهديدات أمنية متزايدة التعقيد، تتجاوز الأشكال التقليدية للتدخل أو التلاعب، ولقد ساهم تطور وسائل الاتصال والتكنولوجيا في خلق بيئة خصبة للتهديدات السيبرانية التي تستهدف تقويض نزاهة الانتخابات وسلامتها، إذ أصبحت الحملات الموجهة لنشر المعلومات المضللة، واختراق قواعد بيانات الناخبين، والتلاعب بالرأي العام عبر وسائل التواصل الاجتماعي، تشكل مخاطر حقيقية على استقرار الأنظمة الديمقراطية وثقة المواطنين في العملية الانتخابية، و في هذا السياق يبرز الذكاء الاصطناعي بوصفه أداة واعدة قادرة على تعزيز القدرة على اكتشاف هذه التهديدات مبكرًا والتعامل معها بفعالية.

ويشكّل استخدام الذكاء الاصطناعي في هذا المجال محورًا لاهتمام بحثي متزايد، نظرًا لما يطرحه من قضايا جوهرية تتعلق بفعاليته، وحدوده، وآليات دمجه ضمن الأنظمة الأمنية الانتخابية القائمة، ويهدف هذا البحث إلى تحليل مدى قدرة تقنيات الذكاء الاصطناعي على رصد التهديدات الأمنية المرتبطة بالانتخابات والكشف عنها في مراحل مبكرة، بما يسهم في دعم نزاهة وشفافية العملية الانتخابية، وتقتضي هذه

الدراسة التعمق في استكشاف سبل توظيف الذكاء الاصطناعي، من خلال خوارزميات تحليل البيانات الضخمة، وأنظمة التعلم الآلي، وأدوات معالجة اللغة الطبيعية، التي تتيح إمكانية رصد حملات التضليل الإعلامي والتأثير على توجهات الرأي العام.

وتأتي أهمية هذه المشكلة البحثية من كونها تقع في تقاطع حساس بين التكنولوجيا والسياسة والأمن القومي، فبينما يوفر الذكاء الاصطناعي إمكانيات هائلة لرصد الأنماط الشاذة وتحليل كميات ضخمة من البيانات في وقت قصير، إلا أن الاعتماد عليه دون فهم عميق لتحدياته قد يؤدي إلى نتائج عكسية، مثل التحيز الخوارزمي أو التضييق غير المبرر على حرية التعبير، و كما أن فعالية هذه التقنيات تعتمد بشكل كبير على جودة البيانات التي تُغذى بها، وعلى البنية التحتية السيبرانية المتاحة، وهو ما يطرح إشكاليات إضافية في الدول ذات القدرات التقنية المحدودة.

وتتجلى المشكلة بشكل أكثر وضوحًا في الحالات التي تتعرض فيها الانتخابات لتدخلات خارجية، سواء عبر حملات منظمة لبث الشائعات، أو محاولات لاختراق نظم التصويت الإلكتروني، أو التشويش على المعلومات المتعلقة بالمرشحين والناخبين، هذه الأنواع من التهديدات يصعب اكتشافها باستخدام الأساليب التقليدية، وهو ما يجعل الذكاء الاصطناعي خيارًا جذابًا للسلطات الانتخابية ومؤسسات الرقابة، ومع ذلك فإن الاعتماد المفرط على الأنظمة الذكية قد يؤدي إلى إشكالات تتعلق بالشفافية والمساءلة، خاصة إذا لم تكن هذه الأنظمة مفهومة أو قابلة للتفسير من قبل الجهات المعنية أو الرأي العام.

وفي ضوء ما تقدم تظهر الحاجة الملحة إلى دراسة علمية ممنهجة تتناول إمكانيات الذكاء الاصطناعي في اكتشاف التهديدات الأمنية للانتخابات، تحديات استخدامه، وضمانات توظيفه بشكل عادل وفعال، فمع التوسع المستمر في استخدام التكنولوجيا في إدارة الانتخابات، ويصبح تطوير حلول ذكية ومستدامة لحماية هذه العملية من التدخلات الرقمية أحد أهم أولويات البحث الأكاديمي والممارسات السياسية المعاصرة.

ثانياً- تساؤلات الدراسة:-

انطلاقًا من مشكلة الدراسة وأهميتها، تم صياغة عدد من التساؤلات التي تسعى إلى توجيه البحث وتحليل أبعاده المختلفة، وذلك على النحو الآتي:

1. ما مدى فاعلية تقنيات الذكاء الاصطناعي في الكشف المبكر عن التهديدات الأمنية التي تستهدف نزاهة العملية الانتخابية؟
2. ما هي أبرز أنواع التهديدات الرقمية التي يمكن للذكاء الاصطناعي رصدها وتحليلها في السياق الانتخابي؟
3. ما التحديات التقنية والأخلاقية التي تواجه استخدام الذكاء الاصطناعي في تأمين الانتخابات؟
4. كيف يمكن توظيف الذكاء الاصطناعي بشكل متوازن يحافظ على أمن العملية الانتخابية دون المساس بالخصوصية أو حرية التعبير؟

ثالثاً- أهداف الدراسة:-

انطلاقًا من مشكلة الدراسة وتساؤلاتها، يسعى هذا البحث إلى تحقيق مجموعة من الأهداف التي تعزز الفهم المعمق على النحو الاتي:-

1. التعرف على مدى فاعلية تقنيات الذكاء الاصطناعي في الكشف المبكر عن التهديدات الأمنية التي تستهدف نزاهة العملية الانتخابية.
2. التعرف على أبرز أنواع التهديدات الرقمية التي يمكن للذكاء الاصطناعي رصدها وتحليلها في السياق الانتخابي.
3. التعرف على التحديات التقنية والأخلاقية التي تواجه استخدام الذكاء الاصطناعي في تأمين الانتخابات.
4. التعرف على آليات توظيف الذكاء الاصطناعي بشكل متوازن يحافظ على أمن العملية الانتخابية دون المساس بالخصوصية أو حرية التعبير.

رابعاً-أهمية الدراسة:

تنبع أهمية هذه الدراسة من الحاجة الملحة لفهم العوامل المتعددة المرتبطة باستخدام الذكاء الاصطناعي في كشف التهديدات الأمنية التي تستهدف العمليات الانتخابية، ومن هنا تأتي الاهمية النظرية والتطبقية على النحو الاتي:

أولاً - الأهمية النظرية:

1. الإسهام في إثراء الأدبيات العلمية المتعلقة بتقاطع الذكاء الاصطناعي والأمن السيبراني في المجال الانتخابي.

2. توفير إطار مفاهيمي لفهم طبيعة التهديدات الرقمية وتأثيرها على نزاهة الانتخابات.
3. تحليل الأبعاد الأخلاقية والقانونية المرتبطة باستخدام الذكاء الاصطناعي في البيئات الديمقراطية.
4. دعم الأبحاث متعددة التخصصات من خلال الربط بين علوم الحاسوب، والعلوم السياسية، والقانون، وعلم الاجتماع الرقمي.

ثانيًا ـ الأهمية التطبيقية:

1. تمكين الجهات المعنية بالانتخابات من التعرف على الأدوات الذكية الفعالة في كشف التهديدات الرقمية.
2. تقديم توصيات عملية تساعد على تصميم سياسات وقائية تعتمد على الذكاء الاصطناعي لحماية العملية الانتخابية.
3. مساعدة صناع القرار في تقييم مخاطر استخدام الذكاء الاصطناعي ضمن الأنظمة الانتخابية، ووضع ضوابط أخلاقية وتشريعية لاستخدامه.
4. تعزيز الوعي المؤسسي والمجتمعي حول أهمية الأمن السيبراني في حماية الاستحقاقات الانتخابية من التلاعب أو التدخلات الخارجية.

خامساً- مفاهيم الدراسة:

انطلاقًا من أهمية تحديد المفاهيم المحورية التي يستند إليها هذا البحث، سيتم في هذا الجزء توضيح أبرز المصطلحات المستخدمة، لضمان فهم دقيق ومشترك لما سيتم تناوله من قضايا وتحليلات، وتتمثل المفاهيم الأساسية فيما يلي:-

ـ الذكاء الاصطناعي :هو فرع من علوم الحاسوب يختص بتطوير أنظمة وتقنيات قادرة على أداء مهام تتطلب ذكاءً بشريًا، مثل التعلم، والاستنتاج، واتخاذ القرار، ومعالجة اللغة الطبيعية، ويُعد الذكاء الاصطناعي اليوم أداة مركزية في معالجة كميات ضخمة من البيانات وتحليلها بفعالية عالية، ومما يجعله مؤهلاً للكشف المبكر عن الأنماط والسلوكيات غير الاعتيادية التي قد تشير إلى وجود تهديدات أمنية.[1]

ـ التهديدات الأمنية على الانتخابات: تشير إلى كافة المحاولات التي تستهدف التأثير على نزاهة وسلامة العملية الانتخابية، سواء من خلال التدخل الإلكتروني، أو التلاعب بالمعلومات، أو نشر الأخبار الكاذبة، أو تعطيل البنية التحتية الرقمية

للانتخابات، وتشكل هذه التهديدات خطرًا كبيرًا على الثقة العامة في النتائج الانتخابية واستقرار النظام الديمقراطي.[2]

- اكتشاف التهديدات الأمنية باستخدام الذكاء الاصطناعي :هو تطبيق تقنيات الذكاء الاصطناعي مثل التعلم الآلي، وتحليل البيانات الضخمة، ومعالجة اللغة الطبيعية في رصد وتحليل المؤشرات التي تدل على وجود هجمات أو محاولات اختراق أو تضليل في الفضاء الانتخابي الرقمي،و يهدف هذا المفهوم إلى تمكين الجهات المعنية من اتخاذ إجراءات استباقية لمنع التهديدات أو الحد من آثارها.[3]

-الأمن السيبراني الانتخابي :هو المجال الذي يختص بحماية النظم والتقنيات المستخدمة في العمليات الانتخابية من الهجمات الإلكترونية والتدخلات غير المشروعة، وضمان سرية وسلامة البيانات الانتخابية، بالإضافة إلى الحفاظ على شفافية ونزاهة العملية الانتخابية في البيئات الرقمية.[4]

أولاً- فاعلية تقنيات الذكاء الاصطناعي في الكشف المبكر عن التهديدات الأمنية التي تستهدف نزاهة العملية الانتخابية:

شهد العملية الانتخابية في العصر الرقمي تحديات متزايدة نتيجة للتطورات السريعة في تقنيات المعلومات والاتصالات، والتي جعلت من الفضاء الإلكتروني ساحةً حيوية للنشاط السياسي، ولكنها في الوقت نفسه مجالاً خصبًا للتهديدات الأمنية التي تستهدف تقويض نزاهة الانتخابات، و يُعد الذكاء الاصطناعي من الأدوات التقنية المتقدمة التي توفر إمكانيات كبيرة في مواجهة هذه التهديدات، فهو قادر على معالجة وتحليل كميات هائلة من البيانات بسرعة ودقة، مما يمكن الجهات المختصة من رصد الأنشطة المشبوهة التي قد تمس الأمن الانتخابي، ومع ذلك فإن دمج هذه التقنيات في الأنظمة الأمنية الانتخابية ليس مجرد خيار تقني بحت، بل هو ضرورة استراتيجية لمواجهة التحديات التي تنشأ من الجهات الداخلية والخارجية التي تسعى إلى التأثير السلبي على النتائج أو زعزعة ثقة الجمهور في العملية الديمقراطية.

تتطلب فعالية هذه الأنظمة قدرة المؤسسات المعنية على بناء بنى تحتية رقمية متطورة تدعم عمل تقنيات الذكاء الاصطناعي، بالإضافة إلى وجود كوادر بشرية متخصصة تملك المهارات اللازمة لإدارة هذه الأنظمة وتطويرها بشكل مستمر فالتكنولوجيا وحدها لا تكفي لضمان الأمن، بل يتطلب الأمر تطوير أطر تنظيمية وتقنية تتكامل مع الجوانب البشرية لتوفير استجابة سريعة وفعالة لأي تهديد و في هذا الإطار يظهر

التنسيق بين الجهات الوطنية والدولية كعامل محوري في تعزيز الأمن السيبراني الانتخابي، وحيث أن الهجمات الإلكترونية كثيرًا ما تكون عابرة للحدود، مما يجعل التعاون الدولي ضرورة لا غنى عنها للتصدي لها ،و كما أن غياب هذا التنسيق يؤدي إلى ضعف القدرة على الاستجابة لهذه الهجمات، ويسمح للجهات المهاجمة باستغلال الثغرات التي تنجم عن التشتت وضعف التواصل بين الجهات المختلفة. (5)

وإلى جانب التحديات التقنية والتنظيمية يبرز بعد مهم وهو البعد القانوني والأخلاقي المرتبط باستخدام الذكاء الاصطناعي في مراقبة وحماية العمليات الانتخابية فالتكنولوجيا قد تؤثر على الحقوق والحريات الأساسية للأفراد إذا لم تُستخدم بشكل مسؤول، فمن الضروري أن تُراعى حقوق الناخبين في الخصوصية وحماية بياناتهم الشخصية، حيث أن جمع وتحليل البيانات الكبيرة يمكن أن يؤدي إلى انتهاكات لهذه الحقوق إذا لم تتوفر ضمانات مناسبة، و بالإضافة إلى ذلك يجب المحافظة على حرية التعبير وعدم السماح للتقنيات الذكية بأن تتحول إلى أدوات رقابة تقيّد حرية الناخبين في التعبير عن آرائهم السياسية، أو تمنع وصول المعلومات المتنوعة إلى الجمهور، ومن هنا فإن وضع أُطر قانونية واضحة تنظم استخدام الذكاء الاصطناعي في المجال الانتخابي يصبح أمرًا ملحًا، بحيث تضمن هذه الأُطر الشفافية في عمل الأنظمة، والمساءلة في حالة وقوع تجاوزات أو أخطاء.

وكما يجب ألا يغيب عن الذهن أن الذكاء الاصطناعي لم يعد مجرد أداة تقنية تعتمد على الخوارزميات والبيانات، بل أصبح يشكل جزءًا لا يتجزأ من البنية الاجتماعية والسياسية التي تحكم الحياة المعاصرة، و تأثيره يمتد ليشمل عمليات صنع القرار السياسي، والأنظمة الديمقراطية بشكل عام، خاصة في الفترات الانتخابية التي تشهد عادة توترات سياسية وحملات معلوماتية مكثفة ،و لذا فإن فهم الأبعاد الاجتماعية والسياسية لاستخدام الذكاء الاصطناعي ضروري لتقييم مدى ملاءمته وفعاليته في تعزيز نزاهة الانتخابات أو العكس، هذا الفهم يساعد على صياغة سياسات متوازنة تحقق أكبر قدر من الأمن مع أقل قدر من التدخل في الحقوق والحريات.

وإن الحاجة إلى دراسات معمقة وشاملة تركز على إمكانيات الذكاء الاصطناعي في كشف التهديدات الأمنية التي تستهدف الانتخابات أمر لا يمكن تجاهله، فمثل هذه الدراسات تحلل التحديات الفنية والقانونية والأخلاقية المرتبطة بتوظيف هذه التكنولوجيا، وتوفر إطارًا متكاملاً يمكن من خلاله تطوير استراتيجيات أمنية أكثر

فاعلية ، كما أن دراسة التجارب الدولية المختلفة تساعد في استخلاص الدروس المستفادة وتطبيقها بما يتناسب مع السياقات المحلية، مما يسهم في بناء نظم انتخابية أكثر أمانًا وموثوقية.

وإلى جانب الجهات الحكومية المسؤولة عن إدارة وتنظيم الانتخابات، ينبغي أن تشمل جهود تأمين العملية الانتخابية مؤسسات المجتمع المدني والهيئات الرقابية والشركات التكنولوجية، حيث يلعب كل طرف دورًا تكامليًا في ضمان بيئة انتخابية شفافة وآمنة، فالمجتمع المدني يمكنه أن يراقب وينتقد ويقدم مقترحات لتحسين الأداء، وبينما تساهم الشركات التكنولوجية في تطوير الأدوات والبرمجيات التي تعتمد عليها أنظمة الذكاء الاصطناعي، وفي ذات الوقت، تحتاج هذه الجهات إلى تنسيق متبادل لضمان مواءمة الجهود وتفادي التداخل أو التضارب في السياسات والممارسات.(6)

وبناءً على ما سبق يمكن القول إن دمج الذكاء الاصطناعي في أنظمة تأمين الانتخابات يمثل خطوة ضرورية لمواكبة التطورات التكنولوجية المتسارعة وللتصدي بفعالية للتهديدات المعقدة التي تستهدف الفضاء الانتخابي، و غير أن نجاح هذا الدمج يعتمد على تضافر الجهود بين البنى التحتية التقنية، والكفاءات البشرية المؤهلة، والأُطر القانونية والأخلاقية التي تحكم استخدام هذه التقنيات ، وكما يتطلب الأمر انفتاحًا على التعاون الدولي الذي يعزز من القدرات المحلية ويضمن تكامل الجهود في مواجهة التهديدات العابرة للحدود، وبهذا الشكل يصبح الذكاء الاصطناعي أداة حيوية تسهم في حماية العمليات الانتخابية وتعزيز ثقة المواطنين في نتائجها، مما يدعم استقرار الأنظمة الديمقراطية وتقدمها.

ثانياً: أبرز أنواع التهديدات الرقمية التي يمكن للذكاء الاصطناعي رصدها وتحليلها في السياق الانتخابي:

تشكل التهديدات الرقمية في سياق الانتخابات أحد التحديات الكبرى التي تواجه الأنظمة الديمقراطية في العصر الحديث، حيث أصبحت العمليات الانتخابية عرضة لمجموعة واسعة من المخاطر التي تهدد نزاهتها وسلامتها، ومع التطور الهائل في تقنيات المعلومات والاتصالات، تزايدت طرق وأساليب الهجوم، لتشمل هجمات معقدة ومتعددة الأبعاد تتطلب أدوات تحليل ورصد متقدمة للتعامل معها، و في هذا الإطار يلعب الذكاء الاصطناعي دورًا بارزًا في الكشف المبكر عن هذه التهديدات وتحليلها

بفعالية، ومما يساعد في اتخاذ الإجراءات الوقائية المناسبة لتعزيز أمان العملية الانتخابية.

واحدة من أبرز التهديدات الرقمية التي يمكن للذكاء الاصطناعي رصدها هي الهجمات السيبرانية التي تستهدف البنية التحتية الرقمية للانتخابات، مثل أنظمة التصويت الإلكترونية وقواعد البيانات الخاصة بالناخبين والنتائج الانتخابية، و هذه الهجمات قد تكون على شكل محاولات لاختراق الأنظمة بهدف التلاعب بالبيانات أو تعطيل الخدمات، وتختلف في تقنياتها وأهدافها، وبفضل تقنيات التعلم الآلي وتحليل الأنماط، يستطيع الذكاء الاصطناعي مراقبة حركة البيانات واكتشاف السلوكيات غير الاعتيادية التي تشير إلى وجود محاولة اختراق أو هجوم إلكتروني، وهو ما يمكن الجهات المعنية من التدخل السريع لمنع وقوع الضرر.

وإضافة إلى ذلك يلعب الذكاء الاصطناعي دورًا مهمًا في كشف التهديدات المتعلقة بنشر المعلومات المضللة والأخبار الزائفة التي تستهدف التأثير على رأي الناخبين وتوجيههم بطرق غير مشروعة، و يستخدم المهاجمون شبكات التواصل الاجتماعي والمنتديات الإلكترونية لنشر شائعات وأخبار كاذبة تهدف إلى زعزعة الثقة في العملية الانتخابية أو تشويه سمعة المرشحين ومن خلال تقنيات معالجة اللغة الطبيعية وتحليل المحتوى، يستطيع الذكاء الاصطناعي تمييز الأنماط اللغوية التي تدل على التضليل والتزييف، وكما يمكنه تتبع المصادر التي تنشر هذه المعلومات وتحليل شبكات التفاعل لتحديد الحملات المنظمة والمخطط لها مسبقًا.[7]

ومن بين التهديدات الأخرى التي يمكن للذكاء الاصطناعي التعرف عليها هي الهجمات التي تستخدم الذكاء الاصطناعي نفسه لإنتاج محتوى مزيف، مثل الصور والفيديوهات المفبركة أو ما يُعرف بـ"التزييف العميق" (Deepfake)،و هذه التقنية تتيح إنتاج محتوى يبدو حقيقيًا للغاية لكنه في الواقع مُزور، ومما قد يستخدم لتشويه صورة المرشحين أو خلق أزمة سياسية، و في هذا الجانب يستخدم الذكاء الاصطناعي أدوات متقدمة لتحليل الصور والفيديوهات واكتشاف التعديلات والتلاعبات التي تمت عليها، مما يساهم في حماية الناخبين من الوقوع ضحية لهذه الحملات الخادعة.

وكما يتعامل الذكاء الاصطناعي مع تهديدات تتعلق بالتصيد الاحتيالي والهجمات التي تستهدف سرقة بيانات الناخبين أو المسؤولين الانتخابيين، والتي قد تستخدم في عمليات التزوير أو ابتزاز الأطراف المعنية، و يعتمد الذكاء الاصطناعي على تحليل

سلوك المستخدمين وتحركاتهم الرقمية لكشف محاولات الدخول غير المصرح به أو الأنشطة المشبوهة التي تنم عن محاولات اختراق، و هذا يمكن أن يقلل من فرص نجاح الهجمات التي تستهدف المعلومات الحساسة ويعزز من مستوى الحماية للأنظمة الانتخابية.

وبالإضافة إلى التهديدات السابقة هناك تهديدات متعلقة بالتلاعب في نتائج الانتخابات نفسها، سواء عبر التلاعب بالبيانات أو التزوير الإلكتروني، و في هذا السياق، يُمكن للذكاء الاصطناعي أن يلعب دورًا رئيسيًا في التحقق من صحة البيانات المتدفقة من مراكز الاقتراع، وتحليل التوزيعات الإحصائية للنتائج للكشف عن أي شذوذ أو اختلافات غير مبررة قد تشير إلى وجود تزوير، ويستخدم الذكاء الاصطناعي نماذج متقدمة لتحليل البيانات الكبيرة والتعرف على الأنماط التي قد لا تكون مرئية للمراقبين البشر، مما يساعد على ضمان شفافية ونزاهة النتائج.[8]

وعلاوة على ذلك هناك تهديدات ترتبط بالتدخل الخارجي من جهات خارجية تسعى إلى التأثير على نتائج الانتخابات أو زعزعة الاستقرار السياسي للدولة، و تستغل هذه الجهات الوسائل الرقمية لنشر المعلومات المغلوطة، وإدارة حملات إلكترونية معقدة تستهدف تقسيم المجتمع وتشويه سمعة الأطراف السياسية، و يستطيع الذكاء الاصطناعي تحليل هذه الحملات عبر تتبع تدفق المعلومات، وتحديد الشبكات الاصطناعية التي تُستخدم لنشر الشائعات والأخبار الزائفة، وهو ما يمكن الجهات الأمنية من اتخاذ الإجراءات المناسبة لوقف هذه الحملات أو الحد من تأثيرها.

ومن المهم الإشارة أيضًا إلى أن بعض هذه التهديدات الرقمية تتداخل وتتقاطع مع بعضها البعض، ما يزيد من تعقيد التحدي الذي تواجهه الجهات المعنية بحماية الانتخابات، فمثلاً قد تتزامن الهجمات السيبرانية مع حملات التضليل الإعلامي، ومما يتطلب أنظمة ذكاء اصطناعي قادرة على التعامل مع تعدد المصادر والأنواع المختلفة للتهديدات في آن واحد، وهذا يستوجب تطوير نماذج متقدمة تجمع بين قدرات التحليل الرقمي المتنوعة، من تحليل النصوص والصور والفيديوهات إلى تحليل الشبكات والعلاقات الاجتماعية الرقمية.

وبذلك فإن الذكاء الاصطناعي لا يقتصر على رصد تهديد واحد أو نوع معين من الهجمات، بل يمتد ليشمل منظومة متكاملة من التهديدات التي تواجه العملية الانتخابية الرقمية، ويعتمد على أدوات وتقنيات متعددة تتطور باستمرار لمواكبة التطورات في

أساليب الهجوم، ويعد الاستثمار في تطوير هذه الأنظمة وتنميتها أولوية استراتيجية للدول والمؤسسات التي تسعى إلى ضمان نزاهة وأمان انتخاباتها.[9]

خلاصة القول :إن الذكاء الاصطناعي يشكل سلاحًا ذو حدين في سياق الانتخابات، فهو يقدم حلولًا فعالة لرصد وتحليل التهديدات الرقمية المعقدة والمتعددة، لكنه في الوقت ذاته قد يُستخدم في صناعة تهديدات جديدة تتطلب تحديث وتطوير مستمر لقدرات الكشف والتحليل، ومن هنا تبرز الحاجة إلى تأهيل خبراء مؤهلين، وبناء أُطر تنظيمية واضحة، وتعزيز التعاون بين الجهات المعنية لضمان الاستخدام الأمثل لهذه التكنولوجيا في حماية الديمقراطية.

ثالثاً-التحديات التقنية والأخلاقية لاستخدام الذكاء الاصطناعي في تأمين العمليات الانتخابية:

في ظل التطورات السريعة التي يشهدها العالم في مجال تكنولوجيا المعلومات، أصبح الذكاء الاصطناعي أحد الأدوات الأساسية التي تُستخدم في العديد من المجالات، من بينها تأمين العمليات الانتخابية التي تُعد من الركائز الأساسية لأي نظام ديمقراطي، وعلى الرغم من الفوائد الكبيرة التي يمكن أن يحققها الذكاء الاصطناعي في تعزيز أمان الانتخابات، إلا أن هناك العديد من التحديات التقنية والأخلاقية التي تواجه استخدامه، وتحتاج إلى دراسة متأنية ومقاربة متوازنة لضمان تحقيق أفضل النتائج دون التسبب في أضرار أو تجاوزات، و تبدأ هذه التحديات من الجانب التقني الذي يتطلب بنية تحتية رقمية قوية ومتطورة، وقادرة على التعامل مع حجم البيانات الكبير والتقنيات الحديثة، وإضافة إلى ضرورة ضمان جودة هذه البيانات التي تُعد العمود الفقري لنجاح أنظمة الذكاء الاصطناعي، إذ أن أي خلل أو انحراف في البيانات يؤثر بشكل مباشر على دقة وفاعلية التحليل والاكتشاف.[10]

ومن الجوانب التقنية الهامة التي تثير القلق هي مسألة جمع البيانات المستخدمة في العمليات الانتخابية، حيث غالباً ما تكون هناك صعوبات تتعلق بعدم توفر بيانات موثوقة ومحدثة بشكل مستمر، وكما قد تكون البيانات التي يتم جمعها متحيزة أو غير كاملة مما ينعكس سلباً على النتائج النهائية التي تنتجها الخوارزميات الذكية.

ولذلك يتطلب الأمر اعتماد آليات متقدمة لترتيب وتنقية البيانات والتأكد من صحتها قبل إدخالها في أنظمة الذكاء الاصطناعي، وهو ما يشكل تحديًا كبيرًا من حيث

التصميم والتنفيذ، وعلاوة على ذلك تواجه أنظمة الذكاء الاصطناعي خطر التعرض لهجمات إلكترونية متخصصة تهدف إلى إضعافها أو تشويه مخرجاتها من خلال إدخال بيانات مضللة ومغلوطة، ما يسمى بهجمات التسميم، وهذا يتطلب تطوير خوارزميات قوية وذكية تستطيع التعرف على هذه الهجمات ومقاومتها للحفاظ على استمرارية العمل بكفاءة عالية.(11)

وإضافة إلى التحديات التقنية لا بد من الإشارة إلى الفجوة التي قد تحدث بين البنى التحتية التقنية المختلفة في المؤسسات والدول، حيث يختلف مستوى التطور والإمكانات الفنية مما يسبب صعوبة في التنسيق وتكامل الأنظمة، وهذا يؤثر على الفاعلية العامة لاستخدام الذكاء الاصطناعي في تأمين الانتخابات، و لذلك فإن تعزيز التعاون وتوحيد المعايير يعد من العوامل الحاسمة لتجاوز هذه العقبات التقنية وتحقيق أفضل استثمار لهذه التكنولوجيا.

وعلى الصعيد الأخلاقي يبرز قلق بالغ يتعلق بخصوصية الأفراد الذين يتم جمع بياناتهم واستخدامها في أنظمة الذكاء الاصطناعي، حيث يتطلب الأمر التعامل مع كم هائل من المعلومات الشخصية الحساسة للناخبين والمرشحين، ويثير ذلك مخاوف جدية حول كيفية حماية هذه البيانات من الاستغلال أو التسريب أو سوء الاستخدام، مما قد يؤدي إلى انتهاك الحقوق الأساسية للأفراد، و كما أن ضرورة تحقيق الشفافية في عمل أنظمة الذكاء الاصطناعي تكتسب أهمية بالغة، إذ يجب أن تكون القرارات والإجراءات التي تنتج عن هذه الأنظمة قابلة للفهم والمراجعة من قبل الجهات المختصة والمواطنين على حد سواء، خاصة وأن الانتخابات تُعد حدثًا حيويًا يؤثر بشكل مباشر على مستقبل الدولة.(12)

ومن التحديات الأخلاقية الأخرى التي تستدعي الانتباه مسألة حرية التعبير وحقوق المشاركة السياسية، وحيث أن الاعتماد المكثف على تقنيات الذكاء الاصطناعي قد يؤدي إلى فرض رقابة مبالغ فيها على المعلومات والمحتوى السياسي، ومما يحد من قدرة المواطنين على التعبير عن آرائهم بحرية كاملة، و كما يمكن أن ينشأ لدى الناخبين شعور دائم بأنهم تحت المراقبة المستمرة، الأمر الذي قد يحد من نشاطهم السياسي ويؤثر سلبًا على مشاركة المجتمع في العملية الديمقراطية، و لذا يجب إيجاد توازن دقيق بين حماية أمن الانتخابات وضمان احترام الحقوق المدنية والسياسية للمواطنين.

وبالإضافة إلى ذلك توجد تحديات قانونية تتعلق بمسألة المساءلة في حال حدوث أخطاء أو تجاوزات من قبل أنظمة الذكاء الاصطناعي، و إذ لا تزال الكثير من التشريعات القانونية غير مكتملة فيما يخص تنظيم استخدام هذه التقنيات في الانتخابات، ما قد يؤدي إلى غياب آليات واضحة للمحاسبة، خصوصًا وأن طبيعة الذكاء الاصطناعي التي تعتمد على التعلم الذاتي قد تنتج أحيانًا قرارات غير متوقعة يصعب تفسيرها أو تحديد المسؤول عنها، ولهذا السبب فإن تطوير أطر قانونية صارمة تضمن حماية الحقوق ونزاهة العملية الانتخابية، وتضع آليات شفافة للمراقبة والمراجعة، يُعد ضرورة ملحة.[13]

وفي مجمل القول: فإن استخدام الذكاء الاصطناعي في تأمين الانتخابات يمثل نقلة نوعية يمكن أن تعزز من سلامة وموثوقية العملية الانتخابية، لكنه في الوقت نفسه يواجه تحديات تقنية وأخلاقية معقدة تتطلب من القائمين على تطوير وتوظيف هذه التقنيات العمل بجدية على تجاوزها، وهذا يشمل تطوير البنية التحتية التقنية، ضمان جودة البيانات، حماية الأنظمة من الهجمات، احترام الخصوصية، تحقيق الشفافية، الحفاظ على الحقوق المدنية والسياسية، وتوفير الأُطر القانونية والتنظيمية اللازمة، وكذلك لا يمكن إغفال أهمية التعاون والتنسيق بين الدول والمؤسسات المختلفة لمواجهة التحديات العابرة للحدود التي قد تهدد أمن الانتخابات في العصر الرقمي ،ومن هنا تظهر الحاجة إلى تبني سياسات متكاملة ومتوازنة تأخذ في الاعتبار كل هذه الجوانب لضمان عملية انتخابية آمنة ونزيهة تعزز الثقة بين المواطنين والمؤسسات.

رابعاً - توظيف الذكاء الاصطناعي بشكل متوازن يحافظ على أمن العملية الانتخابية دون المساس بالخصوصية أو حرية التعبير:

في ظل التطور المتسارع لتقنيات الذكاء الاصطناعي وانتشار استخدامها في مختلف القطاعات الحيوية، أصبح من الضروري البحث عن سبل توظيف هذه التقنيات بشكل متوازن يخدم أهداف المجتمع الديمقراطي، ويعزز من أمن العمليات الانتخابية دون أن يمس بالحقوق الأساسية للمواطنين مثل الخصوصية وحرية التعبير فالانتخابات ليست مجرد إجراء تقني فحسب، بل هي عملية سياسية واجتماعية تحمل في طياتها حقوقاً وحريات تكفلها المواثيق الدولية والدساتير الوطنية، ومن هنا تنبع أهمية وضع ضوابط واضحة تضمن أن يتم الاستفادة من الذكاء الاصطناعي في حماية الانتخابات بطريقة تحترم هذه الحقوق وتدعم مبدأ الشفافية والمساءلة.[14]

وتوظيف الذكاء الاصطناعي في تأمين الانتخابات يبدأ بتطوير أنظمة قادرة على الكشف المبكر عن التهديدات الأمنية مثل التلاعب في البيانات، والهجمات السيبرانية، وحملات التضليل الإعلامي، و من خلال استخدام تقنيات التعلم الآلي وتحليل البيانات الكبيرة، يمكن تحديد الأنماط المشبوهة التي تشير إلى محاولات تزوير أو اختراق، وبالتالي توفير استجابة سريعة وفعالة للحفاظ على نزاهة العملية الانتخابية، و لكن هذه الفعالية لا تتحقق إلا إذا كانت الأنظمة تعتمد على بيانات دقيقة وموثوقة، ويتم تطويرها ضمن إطار يراعي القيم الأخلاقية ويضمن عدم تجاوزها لحقوق الأفراد، وخاصة فيما يتعلق بجمع البيانات الشخصية وتحليلها ولذلك يجب أن يتم جمع البيانات بشكل قانوني وشفاف، مع اتخاذ إجراءات صارمة لحماية هذه البيانات من أي استخدام غير مشروع أو تسريب قد يضر بالناخبين.[15]

وبالإضافة إلى ذلك يقتضي التوازن في توظيف الذكاء الاصطناعي أن تكون العمليات التي تتم من خلال هذه الأنظمة قابلة للفهم والمراجعة من قبل الجهات المختصة والمجتمع المدني، وإذ إن الشفافية في عمل الخوارزميات التي تحكم هذه الأنظمة تساعد في بناء ثقة الجمهور، فلا يكفي أن تكون التكنولوجيا متقدمة وفعالة، بل يجب أن تكون خاضعة لرقابة بشرية تضمن عدم الانحراف عن المسار القانوني والأخلاقي، وأن تكون القرارات التي تصدر عن الذكاء الاصطناعي مفسرة وواضحة حتى لا يُساء استخدامها في فرض رقابة غير مبررة أو تقييد حرية التعبير، و كما يمكن تعزيز ذلك من خلال تطوير أطر تنظيمية وتشريعات تفرض معايير واضحة لاستخدام الذكاء الاصطناعي في الانتخابات، تشمل حماية الحقوق الرقمية، وضمان حق الوصول إلى المعلومات، وحماية المواطنين من أي تمييز أو تحيز قد تنجم عنه.

وجانب مهم آخر من التوظيف المتوازن للذكاء الاصطناعي يتعلق بضمان حرية التعبير والمشاركة السياسية، حيث يجب أن تركز الأنظمة على تعزيز المناخ الديمقراطي وتشجيع النقاش الحر والبناء دون فرض قيود تعسفية على المحتوى أو التفاعل السياسي، و قد يؤدي الاستخدام المفرط أو غير المدروس لتقنيات المراقبة الذكية إلى خلق حالة من الخوف والقلق بين المواطنين، ومما يحد من مشاركتهم في العملية الانتخابية ويؤثر سلبًا على روح الديمقراطية، ولذلك من الضروري أن يكون هناك إطار قانوني وأخلاقي يوازن بين الحاجة إلى تأمين الانتخابات وحماية الحريات

الأساسية، بحيث تلتزم الجهات القائمة على هذه الأنظمة بمعايير صارمة للحد من المراقبة المفرطة وضمان احترام حق المواطن في الخصوصية وحرية التعبير.[16]

وعلاوة على ذلك يجب أن تكون هناك آليات للمساءلة والمراجعة المستمرة لأنظمة الذكاء الاصطناعي المستخدمة في الانتخابات، بحيث يمكن تقييم أدائها وكشف أي أخطاء أو تجاوزات في الوقت المناسب، و يمكن أن تشمل هذه الآليات لجان رقابة مستقلة تتألف من خبراء في القانون، والتكنولوجيا، وحقوق الإنسان، إضافة إلى مشاركة منظمات المجتمع المدني لضمان الحياد والشفافية، و هذه الآليات تلعب دورًا مهمًا في تعزيز الثقة بين الجمهور والجهات المسؤولة، وتوفر ضمانات بأن استخدام الذكاء الاصطناعي لن يتحول إلى أداة لقمع الحقوق أو للتلاعب بنتائج الانتخابات

بجانب ذلك يتطلب تحقيق التوازن في توظيف الذكاء الاصطناعي التعاون والتنسيق بين مختلف الجهات المعنية، سواء على المستوى الوطني أو الدولي، خاصة في ظل الطبيعة العابرة للحدود للتهديدات الإلكترونية، فمن خلال تبادل الخبرات والمعلومات وتوحيد المعايير، يمكن تعزيز الفعالية الأمنية وتقليل المخاطر المرتبطة باستخدام هذه التقنيات، و كما أن التوعية المجتمعية والتدريب المستمر للعاملين في مجال أمن المعلومات والذكاء الاصطناعي ضروريان لتحديث المعرفة والمهارات لمواجهة التحديات المتجددة.[17]

وفي الختام:

يمكن القول إن توظيف الذكاء الاصطناعي في تأمين العمليات الانتخابية بنجاح يتطلب بناء بيئة متكاملة تراعي الأبعاد التقنية والأخلاقية والقانونية، وتعزز مبدأ الشفافية والمساءلة، وتحترم الحقوق الأساسية للمواطنين، فالحفاظ على أمن الانتخابات لا يتعارض مع حماية الخصوصية وحرية التعبير إذا ما تم اعتماد استراتيجيات متوازنة تضمن الاستخدام المسؤول لهذه التقنيات الحديثة، مما يساهم في تعزيز الثقة بالنظام الانتخابي وتقوية دعائم الديمقراطية.

ملخص النتائج:

بعد تحليل البيانات ومراجعة الأدبيات المتعلقة باستخدام الذكاء الاصطناعي في تأمين العمليات الانتخابية، تم التوصل إلى مجموعة من النتائج التي تسلط الضوء على مدى فاعلية هذه التقنيات، أبرز التحديات التي تواجهها، والسبل الممكنة لاستغلالها بشكل

يوازن بين الأمن وحماية الحقوق الأساسية، و فيما يلي عرض تفصيلي لهذه النتائج المهمة:-

1- توضح نتائج البحث أن تقنيات الذكاء الاصطناعي تتمتع بقدرة عالية على الكشف المبكر عن التهديدات الأمنية التي تستهدف نزاهة العملية الانتخابية، وذلك من خلال تحليل البيانات الكبيرة والتعرف على الأنماط المشبوهة بشكل أسرع وأكثر دقة مقارنة بالطرق التقليدية، ومع ذلك فإن فاعلية هذه التقنيات تعتمد بشكل كبير على جودة البيانات المُستخدمة ومدى تكاملها مع الأنظمة الأمنية القائمة.

2- أظهرت الدراسة أن أبرز أنواع التهديدات الرقمية التي يمكن للذكاء الاصطناعي رصدها تشمل هجمات التصيد الاحتيالي، والتلاعب في نتائج التصويت الإلكتروني، وحملات التضليل الإعلامي المنتشرة عبر شبكات التواصل الاجتماعي، بالإضافة إلى محاولات اختراق البنى التحتية الرقمية للانتخابات ، ويسهم الذكاء الاصطناعي في تحليل هذه التهديدات بشكل مستمر ومتكامل مما يعزز قدرة الجهات المختصة على الاستجابة الفورية.

3- كشفت الدراسة أن التحديات التقنية المتعلقة باستخدام الذكاء الاصطناعي في تأمين الانتخابات تتمثل في ضرورة توفر بيانات دقيقة، وحماية الأنظمة من هجمات التسميم، وضمان التوافق مع البنى التحتية التقنية المتنوعة، بينما تتعلق التحديات الأخلاقية بحماية الخصوصية، وضمان الشفافية، وحفظ حقوق الأفراد في حرية التعبير والمشاركة السياسية، ويستلزم التعامل مع هذه التحديات وضع أطر تنظيمية وقانونية واضحة تدعم الاستخدام المسؤول للتقنيات.

4- تبينت أهمية توظيف الذكاء الاصطناعي بشكل متوازن يحقق أمن العملية الانتخابية دون المساس بالخصوصية أو حرية التعبير عبر اعتماد آليات شفافة تتيح مراجعة وتحليل القرارات التي تتخذها الأنظمة الذكية، إلى جانب تطوير تشريعات تحمي الحقوق الرقمية، وتعزيز التعاون بين الجهات المعنية، بما يشمل مشاركة المجتمع المدني والهيئات الرقابية لضمان احترام القيم الديمقراطية وتوفير بيئة انتخابية آمنة وموثوقة.

التوصيات:

استنادًا إلى نتائج الدراسة وتحليل التحديات المرتبطة باستخدام الذكاء الاصطناعي في تأمين العمليات الانتخابية، تبرز الحاجة إلى تبني مجموعة من الإجراءات العملية التي

تساهم في تعزيز فعالية هذه التقنيات مع الحفاظ على الحقوق الأساسية، وفي ضوء ذلك تأتي التوصيات التالية لتوجيه الجهات المعنية نحو استخدام متوازن وآمن للذكاء الاصطناعي في هذا المجال الحيوي وعلى النحو الاتي:-

1- تطوير بنى تحتية تقنية متقدمة تدعم تطبيقات الذكاء الاصطناعي في الكشف المبكر عن التهديدات الأمنية، مع ضمان تحديثها المستمر لمواجهة التحديات المتجددة.

2- تعزيز جودة البيانات المستخدمة في أنظمة الذكاء الاصطناعي عبر اعتماد معايير دقيقة لجمع وتنقية وتحليل البيانات الانتخابية، لضمان موثوقية ودقة النتائج.

3- وضع أُطر قانونية وتنظيمية واضحة تنظم استخدام الذكاء الاصطناعي في العمليات الانتخابية، مع التركيز على حماية حقوق الخصوصية وحرية التعبير.

4- ضمان الشفافية في عمل خوارزميات الذكاء الاصطناعي من خلال توفير آليات لفهم ومراجعة القرارات التي تتخذها هذه الأنظمة، مما يعزز ثقة الجمهور.

5- بناء فرق عمل متعددة التخصصات تشمل خبراء في التكنولوجيا والقانون والأخلاقيات لضمان استخدام الذكاء الاصطناعي بطريقة مسؤولة ومتوازنة.

6- تشجيع التعاون الدولي وتبادل الخبرات بين الدول والمؤسسات المعنية لتعزيز القدرات الأمنية ومواجهة الهجمات الإلكترونية العابرة للحدود.

7- توعية الجمهور والمجتمع المدني بأهمية الذكاء الاصطناعي في تأمين الانتخابات وأهمية احترام الحقوق الرقمية لتعزيز المشاركة الديمقراطية.

8- تطوير آليات مراقبة مستقلة تتابع أداء أنظمة الذكاء الاصطناعي وتقييم أثرها على الحقوق المدنية والسياسية، مع فرض مساءلة واضحة في حالة التجاوزات.

9- تعزيز التكامل بين تقنيات الذكاء الاصطناعي والأنظمة الانتخابية القائمة لضمان سهولة التنفيذ والتشغيل بكفاءة دون تعقيدات تقنية.

10- دعم البحث العلمي المستمر لتطوير تقنيات ذكاء اصطناعي أكثر فعالية وأخلاقية تناسب خصوصية العمليات الانتخابية وتعزز من أمنها.

الهوامش:

1- ناصر الهاشمي، تقنيات الذكاء الاصطناعي في حماية البيانات والخصوصية، عمان، ط2، دار الفكر العربي، 2020، ص، 89.
2- خالد عبد الغفار،الأمن السيبراني، المفاهيم والتطبيقات،ط1، دار اليازوري العلمية،2020،ص14.
3- أحمد مصطفى،التحديات الأمنية في الفضاء الإلكتروني: دراسة تحليلية،ط1، دار النهضة العربية،2021،ص23.
4- سامي عبد الرحمن، نظم المعلومات الأمنية ودورها في حماية البيانات،ط2، مكتبة لبنان ناشرون،2018،ص45.
5- محمد عبد الحليم العشماوي، الذكاء الاصطناعي، المبادئ والتطبيقات، القاهرة،ط2، دار الفكر العربي، ص. 152.
6- علي حسن الجعفري، الذكاء الاصطناعي وأمن المعلومات في العصر الرقمي، بغداد،ط1، دار النخبة الحديثة، 2023، ص، 120.
7- نجلاء أحمد الشريف، استخدام الذكاء الاصطناعي في تأمين العمليات الانتخابية، دراسة تحليلية، دمشق،ط1، دار النهضة العلمية، الطبعة الأولى، 2021، ص،75.
8- سارة محمد البدري، أثر تقنيات الذكاء الاصطناعي في تعزيز الأمن السيبراني للأنظمة الانتخابية، القاهرة، ط2،دار المعارف الجديدة، 2022، ص،87.
9- ليلى محمد حسن، الذكاء الاصطناعي وتأثيره في المجتمع المعاصر، القاهرة،ط2، دار الفكر المعاصر، ص، 110.
10- خالد الزهراني ،الذكاء الاصطناعي وأمن المعلومات، تحديات وحلول، الرياض، ط1،دار المعرفة للنشر، 2021، ص، 112.
11- ريم العلي، أثر الذكاء الاصطناعي على الحوكمة الإلكترونية، بيروت، ط2، دار الجامعة الحديثة، 2022، ص 140.
12- ناصر القحطاني، التكنولوجيا الرقمية وتأمين العمليات الانتخابية،ط2، جدة، دار الفكر الجديد، 2019، ص 85.
13- محمد عبد الغفار، الأمن السيبراني، المفاهيم والتطبيقات، القاهرة،ط1، دار النهضة العربية، 2020، ص، 98.
14- فاطمة المنصوري، التحديات القانونية والأخلاقية للذكاء الاصطناعي في المجتمعات الحديثة،ط1، القاهرة، دار النهضة الحديثة، 2021، ص، 134.
15- نادية سعيد، الخصوصية الرقمية في عصر الذكاء الاصطناعي، دراسة تحليلية، بيروت، ط2،دار الثقافة المعاصرة، 2022، ص، 59.
16- سامي الرحيمي، أمن المعلومات وتأثير الذكاء الاصطناعي على العمليات الانتخابية، ط1،الرباط، دار الحكمة للنشر، 2018، ص،76 .
17- محمد العريبي، .تأثير الذكاء الاصطناعي على أمن المعلومات الانتخابية، طرابلس،ط1، دار المعارف للنشر،2022،ص 44.