إطار وطني لحوكمة الذكاء الاصطناعي لضمان السيادة الرقمية وتعزيز الأمن الداخلي نموذجاً للحكومة الليبية

دكتورة وفاء سلمان عبود ـ رئيس هيئة في ديوان الرقابة الاتحاديه

البريد الإلكتروني: Wf4dma@gmail.com

تاريخ التقديم للنشر ٢٠٢٥/١١/٢ تاريخ القبول للنشر ٢٠٢٥/١٢/٢٣

الملخص.

يهدف هذا البحث إلى تقديم إطار وطني متكامل لحوكمة الذكاء الاصطناعي في الحكومة الليبية بما يضمن تعزيز السيادة الرقمية ودعم الأمن الداخلي، وذلك عبر تحليل الأبعاد التقنية والقانونية والمؤسسية والاجتماعية المرتبطة بتوظيف هذه التقنيات داخل القطاع العام .وتكمن أهمية البحث في أن الذكاء الاصطناعي أصبح أداة استراتيجية تمس الأمن القومي للدول، إذ يمكن توظيفه في تحليل البيانات الضخمة، وإدارة المخاطر، وتعزيز كفاءة الخدمات الحكومية، فضلًا عن استخدامه في مجالات الأمن الداخلي ومكافحة الجريمة المنظمة والإرهاب(1) .

ويركز البحث على التحديات التي تواجه الدولة الليبية في مجال حماية البيانات الوطنية، وبناء بنية تحتية رقمية سيادية، وتطوير قدرات الأمن السيبراني، إضافة إلى ضرورة ضبط الشفافية والمساءلة في القرارات الآلية المعتمدة على الخوارزميات .كما يستعرض البحث نماذج دولية رائدة في مجال حوكمة الذكاء الاصطناعي، ويقدّم إطارًا عمليًا شاملًا يتضمن الهيكل المؤسسي، التشريعات والسياسات اللازمة، وآليات قياس الأداء، وخطة تنفيذ مرحلية قابلة للتطبيق.

ويخلص البحث إلى أن نجاح ليبيا في الانتقال نحو دولة رقمية آمنة يعتمد على بناء منظومة حوكمة وطنية تضمن الاستخدام المسؤول للذكاء الاصطناعي، وتحد من المخاطر الأمنية والاقتصادية المرتبطة بالتبعية التكنولوجية، وتحقق التوازن بين الابتكار وحماية الأمن الداخلي.

Abstract.

This research aims to propose a comprehensive national framework for Artificial Intelligence (AI) governance in the Libyan government in order to strengthen digital sovereignty and enhance internal security. The study analyzes the technical, legal, institutional, and social dimensions associated with the integration of AI technologies into the public sector. It highlights

the strategic importance of AI as a transformative tool capable of improving governmental efficiency, supporting decision-making processes, and enhancing security systems through advanced data analysis and predictive modeling.

The research also examines the major challenges facing Libya in adopting AI, including weak digital infrastructure, fragmented governmental databases, limited cybersecurity capabilities, and the absence of comprehensive legislation regulating data protection, algorithmic accountability, and automated decision-making. Moreover, the study emphasizes that excessive reliance on foreign technological providers represents a significant risk to national security and data sovereignty, especially regarding sensitive security and financial information. In addition, the research reviews international experiences in AI governance, including the European Union's regulatory model, the United States' risk-management approach, China's digital sovereignty strategy, and selected Arab experiences such as the United Arab Emirates and Saudi Arabia. Based on these models, the study proposes a practical governance framework for Libya that includes the establishment of a national AI council, a specialized AI governance authority, a sovereign national data center, and a national cybersecurity center, supported by clear legal and policy reforms. The research concludes that Libya's successful transition toward a secure digital government requires strong political commitment, institutional coordination, legislative development, capacity-building programs, and long-term investment in national digital infrastructure. A well-designed AI governance system is essential to ensure responsible and secure use of AI

technologies while reducing risks related to technological dependency and cyber threats.

Keywords: Artificial Intelligence Governance, Digital Sovereignty, Cybersecurity, Internal Security, Libyan Government, Data Protection.

المقدمة.

شهد العالم خلال العقد الأخير تطورًا متسارعًا في تقنيات الذكاء الاصطناعي، مما جعله أداة مركزية في إدارة البيانات وتحسين الخدمات الحكومية وتطوير القدرات الأمنية للدول .ولم يعد الذكاء الاصطناعي مجرد مفهوم نظري أو تقنية مستقبلية، بل أصبح واقعًا تستخدمه الحكومات في إدارة المؤسسات العامة، وتقديم الخدمات الإلكترونية، وتحسين كفاءة اتخاذ القرار، ومراقبة الحدود، وتحليل أنماط الجريمة، وإدارة المخاطر الاقتصادية .وقد أكدت الأدبيات الحديثة أن الذكاء الاصطناعي أصبح يمثل تحولًا جوهريًا في طبيعة الحكم وإدارة الدولة بسبب قدرته على تقليل التكاليف الإدارية، ورفع كفاءة المؤسسات، وتقديم خدمات رقمية أسرع وأكثر دقة(1) .

وتشير العديد من الدراسات إلى أن التحول نحو الحكومة الرقمية يعتمد بدرجة كبيرة على إدماج الذكاء الاصطناعي في الإدارة العامة، إذ يتيح تحليل كميات ضخمة من البيانات بصورة فورية، ويقدم نماذج تنبؤية تساعد صناع القرار في مواجهة الأزمات .كما أن التطور المتسارع في الخوارزميات جعل بعض الدول تعتمد على الذكاء الاصطناعي في إدارة السياسات الأمنية، بما في ذلك نظم المراقبة الذكية وتحليل الاتصالات ومراقبة الجرائم الإلكترونية(2) .

وفي السياق الليبي، يمثل الذكاء الاصطناعي فرصة استراتيجية لتعزيز الأمن الداخلي وتحسين الأداء المؤسسي ودعم التنمية الاقتصادية والاجتماعية، إلا أن هذا التحول الرقمي يفرض تحديات جوهرية تتعلق بحماية البيانات الوطنية والسيادة الرقمية وبناء الأطر القانونية والقدرات المؤسسية اللازمة . كما أن الاعتماد المتزايد على الحلول التقنية الأجنبية يثير مخاوف سيادية وأمنية، خاصة عندما يتعلق الأمر بالبيانات الأمنية والمالية الحساسة التي يمكن أن تؤثر على الأمن القومي للدولة(3) .

إن ليبيا، كغيرها من الدول النامية التي تمر بمرحلة إعادة بناء مؤسساتها، تحتاج إلى إطار وطني لحوكمة الذكاء الاصطناعي يضمن الاستخدام الآمن والمسؤول لهذه التقنيات، ويمنع تحولها إلى أدوات تهديد للأمن الداخلي أو انتهاك للخصوصية .فغياب الحوكمة قد يؤدي إلى مخاطر خطيرة مثل

تسرب البيانات السيادية، أو إساءة استخدام أدوات المراقبة، أو الاعتماد الكلي على شركات أجنبية تسيطر على البيانات والبنية التحتية الرقمية.

وعليه، تهدف هذه الدراسة إلى تقديم تصور شامل لإطار وطني لحوكمة الذكاء الاصطناعي في ليبيا، يستند إلى المبادئ الدولية المعتمدة، ويأخذ في الاعتبار خصوصية البيئة الليبية من حيث البنية المؤسسية والتحديات الأمنية والسياسية.

المبحث الأول :الإطار النظري لحوكمة الذكاء الاصطناعي والسيادة الرقمية.

المطلب الأول :مفهوم الذكاء الاصطناعي.

الذكاء الاصطناعي هو مجموعة من الأنظمة والخوارزميات التي تتيح للحواسيب محاكاة القدرات البشرية مثل التعلم والتحليل والاستنتاج واتخاذ القرار .وقد تطور مفهوم الذكاء الاصطناعي ليشمل أنظمة قادرة على التعلم من البيانات الضخمة وتحليلها واستخراج الأنماط منها، وهو ما جعله من أهم أدوات الثورة الصناعية الرابعة .ويرى Russell وNorvig أن الذكاء الاصطناعي يمثل علم تصميم "وكلاء أذكياء "قادرين على التفاعل مع البيئة المحيطة، وتحقيق أهداف محددة من خلال اتخاذ قرارات عقلانية(1) .

ويشمل الذكاء الاصطناعي تطبيقات متعددة مثل التعلم الآلي، التعلم العميق، معالجة اللغة الطبيعية، والرؤية الحاسوبية، والتي تُستخدم في مجالات عديدة تشمل الأمن السيبراني، مراقبة الحدود، تحليل الأنماط الإجرامية، وإدارة المؤسسات الحكومية .ومن المهم الإشارة إلى أن نجاح هذه الأنظمة يعتمد على جودة البيانات المتاحة، لأن البيانات تمثل الوقود الأساسي الذي يحدد مستوى دقة المخرجات.

وفي مجال الأمن الداخلي، يتم استخدام الذكاء الاصطناعي لتحليل الكاميرات، ورصد السلوكيات المشبوهة، وتتبع الشبكات الإجرامية، وتحليل الاتصالات الرقمية، فضلًا عن استخدامه في مكافحة الجرائم الإلكترونية .كما يمكن توظيفه في التنبؤ بالمخاطر الأمنية المحتملة عبر تحليل البيانات التاريخية وربطها بالمتغيرات الاجتماعية والسياسية.

غير أن الذكاء الاصطناعي يحمل في طياته مخاطر محتملة، من أبرزها التحيز الخوارزمي، إذ قد تنتج الخوارزميات قرارات خاطئة أو غير عادلة إذا كانت البيانات المدخلة غير متوازنة أو غير دقيقة .كما أن استخدام الذكاء الاصطناعي في الأمن الداخلي قد يؤدي إلى انتهاكات حقوق الإنسان إذا لم يتم ضبطه بإطار قانوني صارم(4) .

المطلب الثاني: مفهوم السيادة الرقمية.

تشير السيادة الرقمية إلى قدرة الدولة على التحكم الكامل في بياناتها الوطنية وبنيتها التحتية الرقمية، وضمان استقلالية القرار الوطني في المجال التقني .ويعد مفهوم السيادة الرقمية امتدادًا لمفهوم السيادة السياسية التقليدية، إلا أنه يرتبط بالفضاء الإلكتروني والبيانات والشبكات .وقد أصبحت السيادة الرقمية قضية استراتيجية للدول بسبب تحول البيانات إلى مورد اقتصادي وأمني بالغ الأهمية، حيث تُستخدم البيانات في التخطيط الاقتصادي وإدارة الأمن الوطني والتحكم في الخدمات العامة(5) .

وتتطلب السيادة الرقمية بناء مراكز بيانات وطنية وسحابة حكومية، إضافة إلى تطوير تشريعات تحمي البيانات الشخصية وتمنع تسرب البيانات السيادية .كما تتطلب استثمارًا في تطوير قدرات وطنية في الأمن السيبراني والذكاء الاصطناعي لضمان عدم الاعتماد الكامل على مزودي خدمات أجانب.

ويرى Kuner أن تدفقات البيانات عبر الحدود أصبحت أحد أبرز مظاهر العولمة الرقمية، إلا أنها في الوقت نفسه تمثل تهديدًا للسيادة الوطنية عندما تفقد الدول السيطرة على بياناتها الحساسة، خصوصًا في المجالات الأمنية والمالية(5) .

وفي السياق الليبي، تصبح السيادة الرقمية أكثر أهمية بسبب طبيعة الوضع الأمني والسياسي، إذ يمكن أن يؤدي أي تسرب للبيانات الأمنية أو العسكرية إلى تهديد مباشر للاستقرار الداخلي.

المطلب الثالث :مفهوم حوكمة الذكاء الاصطناعي

حوكمة الذكاء الاصطناعي تعني وضع قواعد قانونية وتنظيمية ومعايير تقنية وأخلاقية تضبط تصميم وتطوير واستخدام أنظمة الذكاء الاصطناعي بما يضمن سلامتها وأمنها وشفافيتها ومساءلتها. وتعد الحوكمة عنصرًا أساسيًا لأن أنظمة الذكاء الاصطناعي قد تتسبب في أخطاء أو تحيزات إذا لم يتم التحكم في مصادر البيانات أو ضبط الخوارزميات(6) .

كما ترتبط الحوكمة بمفهوم العدالة الرقمية، حيث يجب أن تضمن الأنظمة الذكية عدم التمييز ضد فئات اجتماعية أو مناطقية، وأن تكون القرارات المعتمدة على الذكاء الاصطناعي قابلة للتفسير والمراجعة من قبل الجهات الرقابية.

وقد أصدرت منظمة اليونسكو توصيات عالمية بشأن أخلاقيات الذكاء الاصطناعي، أكدت فيها أن الحوكمة يجب أن تقوم على مبادئ حقوق الإنسان، والشفافية، وحماية الخصوصية، ومنع استخدام الذكاء الاصطناعي في القمع أو انتهاك الحريات(6) .

المبحث الثاني :واقع الحكومة الليبية والتحديات الرقمية.

المطلب الأول :واقع التحول الرقمي في ليبيا.

يعاني التحول الرقمي في ليبيا من تحديات تتعلق بالبنية التحتية الرقمية وضعف خدمات الإنترنت في بعض المناطق، فضلًا عن تشتت البيانات الحكومية وغياب استراتيجية وطنية موحدة لإدارة البيانات والتحول الرقمي .كما أن الاعتماد على الإجراءات الورقية في العديد من المؤسسات يزيد من البيروقراطية ويؤدي إلى ارتفاع تكاليف الإدارة الحكومية(7) .

إن ضعف الربط بين المؤسسات يؤدي إلى تكرار البيانات وعدم دقتها، مما يحد من إمكانية توظيف الذكاء الاصطناعي بشكل فعال، لأن نجاح الأنظمة الذكية يتطلب قواعد بيانات موحدة ومنظمة.

كما أن ضعف الأنظمة الإدارية وعدم استقرار المؤسسات الحكومية يعرقل بناء مشاريع رقمية مستدامة، إذ إن أي نظام ذكاء اصطناعي يحتاج إلى بيئة مستقرة لضمان تحديث البيانات وصيانة البنية التحتية التقنية.

المطلب الثاني :التحديات القانونية والمؤسسية.

أولًا :التحديات القانونية

تشمل التحديات القانونية غياب قانون شامل لحماية البيانات الشخصية وضعف التشريعات المنظمة للأمن السيبراني .كما أن عدم وجود قوانين واضحة تنظم القرارات الآلية يجعل من الصعب تحديد المسؤولية القانونية عند وقوع أخطاء أو إساءة استخدام أنظمة الذكاء الاصطناعي(8) .

كما أن ليبيا تحتاج إلى وضع قواعد قانونية تنظم استخدام الذكاء الاصطناعي في المجالات الأمنية، لأن غياب الضوابط قد يؤدي إلى استخدام الأنظمة الذكية في عمليات مراقبة غير قانونية أو في إصدار قرارات أمنية خاطئة قد تمس حقوق المواطنين.

ثانيًا :التحديات المؤسسية

أما التحديات المؤسسية فتتمثل في نقص الكفاءات التقنية وضعف التنسيق بين الوزارات والمؤسسات، إضافة إلى محدودية التمويل المخصص للتحول الرقمي .ويستلزم ذلك تطوير برامج تدريب وطنية بالتعاون مع الجامعات الليبية لإعداد كوادر متخصصة في الذكاء الاصطناعي والأمن السيبراني(9) .

كما أن ضعف الثقافة الرقمية داخل المؤسسات الحكومية يمثل عائقًا مهمًا، إذ لا تزال العديد من المؤسسات تعتمد على أنظمة تقليدية لا تسمح بالتكامل مع الأنظمة الذكية الحديثة.

المبحث الثالث :الإطار الوطني المقترح لحوكمة الذكاء الاصطناعي في ليبيا.

المطلب الأول :المبادئ الأساسية للإطار المقترح.

يقوم الإطار الوطني المقترح على مبادئ السيادة الرقمية، الأمن السيبراني، الشفافية، المساءلة، العدالة وعدم التمييز، ودعم التنمية المستدامة .كما يجب أن يقوم على مبدأ التوازن بين الابتكار وحماية الأمن الوطني، بحيث يتم تشجيع تطوير الأنظمة الذكية دون تعريض البيانات الوطنية للخطر(10) .

ومن الضروري أن يكون الإطار الوطني منسجمًا مع المبادئ الدولية، مثل مبادئ OECD، ومعايير NIST، ومعايير ISOالخاصة بإدارة المخاطر(11) .

المطلب الثاني :الهيكل المؤسسي المقترح.

يقترح البحث إنشاء مجلس وطني أعلى للذكاء الاصطناعي والسيادة الرقمية يتبع مجلس الوزراء، تكون مهمته وضع الاستراتيجية العامة واعتماد المشاريع الكبرى .كما يقترح إنشاء هيئة وطنية لحوكمة الذكاء الاصطناعي تتولى التنفيذ والمتابعة، إضافة إلى مركز وطني للبيانات السيادية لإدارة البيانات الحكومية وتوحيدها، ومركز وطني للأمن السيبراني لحماية الأنظمة الرقمية من الهجمات . (12)

ومن الضروري أن تتضمن هذه المؤسسات وحدات متخصصة في تقييم المخاطر الأخلاقية والتدقيق التقني للخوارزميات، لضمان عدم وجود تحيز أو أخطاء تؤثر على القرارات الحكومية.

المطلب الثالث :التشريعات والسياسات اللازمة

يستلزم تطبيق الإطار المقترح إصدار قوانين تشمل حماية البيانات الشخصية، تنظيم استخدام الذكاء الاصطناعي، الأمن السيبراني، والمسؤولية القانونية عن القرارات الآلية .كما يجب اعتماد سياسات تصنيف البيانات الوطنية ومنع تخزين البيانات السيادية خارج ليبيا(5) .

ومن الضروري أن تتضمن التشريعات نصوصًا تمنع استخدام منصات أجنبية لمعالجة البيانات الأمنية أو المالية الحساسة دون موافقة رسمية، إضافة إلى وضع عقوبات قانونية رادعة في حال تسريب البيانات أو إساءة استخدامها.

المطلب الرابع :التجارب الدولية في حوكمة الذكاء الاصطناعي (موسع)

أولًا :الاتحاد الأوروبي ونموذج التشريع التنظيمي

يعد الاتحاد الأوروبي من أبرز النماذج الدولية في مجال حوكمة الذكاء الاصطناعي، إذ عمل على إصدار تشريع شامل يعرف باسم قانون الذكاء الاصطناعي الأوروبي EU AI Act، والذي يقوم على تصنيف أنظمة الذكاء الاصطناعي إلى مستويات خطورة مختلفة، منها أنظمة محظورة وأنظمة عالية الخطورة وأنظمة محدودة الخطورة .ويُلزم هذا القانون المؤسسات بتطبيق إجراءات تقييم المخاطر، وتوفير شفافية أكبر في القرارات الخوارزمية، ومنح المواطنين حق الاعتراض على القرارات الآلية(13) .

ثانيًا :الولايات المتحدة وإطار إدارة المخاطر NIST

اعتمدت الولايات المتحدة نهجًا مختلفًا قائمًا على إدارة المخاطر بدلًا من التشريعات الصارمة .فقد أصدر المعهد الوطني للمعايير والتكنولوجيا (NIST)إطارًا لإدارة مخاطر الذكاء الاصطناعي يركز على مبادئ الحوكمة والتقييم المستمر للأداء، ويشدد على ضرورة أن تكون الأنظمة قابلة للقياس والتفسير، مع وضع آليات للتعامل مع المخاطر الأمنية(10) .

ثالثًا :الصين ونموذج السيادة الرقمية الصارمة

تتبنى الصين نموذجًا قائمًا على السيطرة الصارمة على البيانات، حيث تعتبر البيانات جزءًا من الأمن القومي، وتسعى إلى بناء منظومة وطنية متكاملة للذكاء الاصطناعي تعتمد على شركات محلية وتطوير بنية تحتية سيادية .كما تستخدم الصين الذكاء الاصطناعي على نطاق واسع في المراقبة الأمنية والتعرف على الوجه وإدارة المدن الذكية(14) .

رابعًا :الإمارات العربية المتحدة وتجربة التحول الذكي

تعد الإمارات من الدول العربية الرائدة في إدماج الذكاء الاصطناعي ضمن الإدارة الحكومية، حيث أنشأت وزارة للذكاء الاصطناعي، وأطلقت استراتيجية وطنية شاملة، وطبقت مشاريع في مجالات الشرطة الذكية، والخدمات الرقمية، وإدارة الحدود .كما ركزت الإمارات على بناء شراكات عالمية وتطوير قدرات بشرية محلية(15) .

خامسًا :السعودية وهيئة SDAIA

اعتمدت المملكة العربية السعودية نموذجًا متقدمًا في حوكمة الذكاء الاصطناعي من خلال إنشاء هيئة البيانات والذكاء الاصطناعي SDAIA، والتي تعمل على بناء منظومة بيانات سيادية وتطوير تطبيقات ذكية في قطاعات الأمن والاقتصاد والخدمات العامة(16) .

سادسًا :اليونسكو والأمم المتحدة ومبادئ الأخلاقيات

أصدرت اليونسكو توصيات أخلاقية بشأن الذكاء الاصطناعي ركزت على منع التمييز، وحماية حقوق الإنسان، وضمان الشفافية، ومنع الاستخدام غير المشروع للذكاء الاصطناعي في الحروب أو القمع السياسي(6) .

المبحث الرابع :آليات التنفيذ المرحلي والتقييم والرقابة الوطنية لحوكمة الذكاء الاصطناعي في ليبيا.

المطلب الأول :أهمية التنفيذ المرحلي في الحالة الليبية

تُعد ليبيا من الدول التي تواجه تحديات كبيرة في الاستقرار المؤسسي والبنية التحتية الرقمية، لذلك فإن تنفيذ إطار حوكمة الذكاء الاصطناعي يجب أن يتم بشكل تدريجي ومدروس، بحيث لا يتم الانتقال إلى تطبيقات أمنية حساسة قبل توفير بيئة قانونية وتقنية مناسبة(18) .

المطلب الثاني :مراحل التنفيذ المقترحة

المرحلة الأولى :التأسيس 2–1سنة

وتشمل إصدار قانون حماية البيانات، وإنشاء المجلس الوطني الأعلى للذكاء الاصطناعي، وبناء مركز البيانات السيادية، ووضع سياسة تصنيف البيانات الوطنية، وإطلاق برامج تدريب وطنية.

المرحلة الثانية :التشغيل التجريبي 4–2)سنوات(

وتشمل تطبيق مشاريع تجريبية منخفضة المخاطر مثل الخدمات البلدية والمرور، وتطوير بوابات حكومية رقمية موحدة، وبناء وحدات التدقيق الخوارزمي.

المرحلة الثالثة :التشغيل الكامل 5)سنوات فأكثر(

وتشمل إدماج الذكاء الاصطناعي في الأمن الداخلي ومراقبة الحدود، وتطوير أنظمة للتنبؤ بالجرائم المنظمة، وربط المؤسسات الأمنية والمالية بقواعد بيانات وطنية موحدة.

المطلب الثالث :مؤشرات قياس الأداء (KPIs)

يمكن قياس نجاح الإطار الوطني عبر مؤشرات أهمها :عدد المؤسسات المرتبطة بمنصة البيانات الوطنية، ونسبة البيانات المصنفة سياديًا، وعدد مشاريع الذكاء الاصطناعي التي تم تدقيقها، ومعدل الهجمات السيبرانية والاستجابة لها، ومستوى رضا المواطنين عن الخدمات الرقمية(19) .

المطلب الرابع :التدقيق الخوارزمي وحماية حقوق المواطن.

يعد التدقيق الخوارزمي عنصرًا جوهريًا في حوكمة الذكاء الاصطناعي، إذ يجب مراجعة الخوارزميات دوريًا لضمان عدم التحيز ضد فئات اجتماعية، وسلامة البيانات المدخلة، ودقة النتائج، وحماية الخصوصية(20) .

الخاتمة.

خلص البحث إلى أن حوكمة الذكاء الاصطناعي تمثل ضرورة استراتيجية لضمان الاستخدام الآمن والمسؤول للتقنيات الحديثة داخل الحكومة الليبية .ويعد إنشاء إطار وطني متكامل خطوة أساسية لتعزيز السيادة الرقمية، حماية البيانات الوطنية، ورفع كفاءة الأمن الداخلي، إضافة إلى دعم التنمية الاقتصادية والاجتماعية.

كما بيّن البحث أن نجاح ليبيا في هذا المسار يعتمد على الإرادة السياسية، وتطوير التشريعات، وبناء القدرات البشرية، والاستثمار في البنية التحتية الرقمية الوطنية، إلى جانب الاستفادة من التجارب الدولية مع مراعاة الخصوصية الليبية.

إن بناء منظومة حوكمة وطنية ليس ترفًا إداريًا، بل هو ضمانة لحماية الدولة من المخاطر المرتبطة بالتبعية التكنولوجية، وضمان أن يبقى الذكاء الاصطناعي أداة للتنمية والأمن بدلًا من أن يتحول إلى مصدر تهديد.

الحواشي: وفق نظام شيكاغو.

1- Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (London: Pearson, 2020), 45.

2- European Commission, Artificial Intelligence Policy in the European Union (Brussels: EU Publications, 2021), 18.

3- United Nations, Digital Government and Cybersecurity Framework (New York: UN Publications, 2020), 51.

4- Kate Crawford, Atlas of AI (New Haven: Yale University Press, 2021), 66.

5- Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford: Oxford University Press, 2020), 112.

6- UNESCO, Recommendation on the Ethics of Artificial Intelligence (Paris: UNESCO, 2021), 35.

7- OECD, Digital Government Index Report (Paris: OECD Publishing, 2020), 33.

8- OECD, OECD Principles on Artificial Intelligence (Paris: OECD Publishing, 2019), 22.

9- Shoshana Zuboff, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019), 88.

10- NIST, AI Risk Management Framework (Washington: National Institute of Standards and Technology, 2023), 14.

11- ISO/IEC, ISO/IEC 23894: Artificial Intelligence Risk Management (Geneva: ISO, 2022), 29.

12- World Economic Forum, Global AI Governance Report (Geneva: WEF, 2020), 63.

13- European Parliament, EU Artificial Intelligence Act (Brussels: European Union Publications, 2023), 41.

14- Kai-Fu Lee, AI Superpowers: China, Silicon Valley, and the New World Order (Boston: Houghton Mifflin Harcourt, 2018), 103.

15- UAE Government, UAE National Strategy for Artificial Intelligence 2031 (Abu Dhabi: Government Press, 2019), 11.

16- SDAIA, Saudi National Strategy for Data and Artificial Intelligence (Riyadh: SDAIA Publications, 2020), 25.

17- United Nations Development Programme (UNDP), Human Development Report: Digital Transformations (New York: UNDP, 2022), 91.

18- Mariarosaria Taddeo and Luciano Floridi, "How AI Can Be a Force for Good," Science 361, no. 6404 (2018): 751.

19- World Economic Forum, Global AI Governance Report (Geneva: WEF, 2020), 70.

20- Reuben Binns, "Fairness in Machine Learning: Lessons from Political Philosophy," Proceedings of Machine Learning Research (2018): 5.

قائمة المراجع.

Binns, Reuben. "Fairness in Machine Learning: Lessons from Political Philosophy." Proceedings of Machine Learning Research (2018).

Crawford, Kate. Atlas of AI. New Haven: Yale University Press, 2021.

European Commission. Artificial Intelligence Policy in the European Union. Brussels: EU Publications, 2021.

European Parliament. EU Artificial Intelligence Act. Brussels: European Union Publications, 2023.

ISO/IEC. ISO/IEC 23894: Artificial Intelligence Risk Management. Geneva: ISO, 2022.

Kai-Fu Lee. AI Superpowers: China, Silicon Valley, and the New World Order. Boston: Houghton Mifflin Harcourt, 2018.

Kuner, Christopher. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2020.

NIST. AI Risk Management Framework. Washington: National Institute of Standards and Technology, 2023.

OECD. OECD Principles on Artificial Intelligence. Paris: OECD Publishing, 2019.

OECD. Digital Government Index Report. Paris: OECD Publishing, 2020.

Russell, Stuart, and Peter Norvig. Artificial Intelligence: A Modern Approach. London: Pearson, 2020.

SDAIA. Saudi National Strategy for Data and Artificial Intelligence. Riyadh: SDAIA Publications, 2020.

Taddeo, Mariarosaria, and Luciano Floridi. “How AI Can Be a Force for Good.” Science 361, no. 6404 (2018).

UAE Government. UAE National Strategy for Artificial Intelligence 2031. Abu Dhabi: Government Press, 2019.

UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021.

United Nations. Digital Government and Cybersecurity Framework. New York: UN Publications, 2020.

United Nations Development Programme (UNDP). Human Development Report: Digital Transformations. New York: UNDP, 2022.

World Economic Forum. Global AI Governance Report. Geneva: WEF, 2020.

Zuboff, Shoshana. The Age of Surveillance Capitalism. New York: PublicAffairs, 2019.