مركز البيان للدراسات والتخطيط
Al-Bayan Center for Studies and Planning

2026/1/26

الذكاء الاصطناعي والخصوصية في الفضاء الاقتصادي الرقمي العراقي

التحديات والحلول مع التعريف بإجراءات حماية الخصوصية في العراق والنرويج

د. سناء عبد القادر مصطفى

● ورقة سياسات

سلسلة اصدارات مركز البيان للدراسات والتخطيط

الذكاء الاصطناعي والخصوصية في الفضاء الاقتصادي الرقمي العراقي
التحديات والحلول مع التعريف بإجراءات حماية الخصوصية في العراق والنرويج

سلسلة اصدارات مركز البيان للدراسات والتخطيط /قسم الأبحاث / الدراسات الاقتصادية

الاصدار / ورقة سياسات

الموضوع / الاقتصاد والتنمية

د. سناء عبد القادر مصطفى/ أستاذ جامعي - النرويج - دكتوراه في الاقتصاد الصناعي

عن المركز

مركزُ البيان للدراسات والتخطيط مركز مستقلٌ، غيرُ ربحيٍّ، مقرُّه الرئيس في بغداد، مهمته الرئيسة -فضلاً عن قضايا أخرى- تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاص، ومنطقة الشرق الأوسط بنحو عام. ويسعى المركز إلى إجراء تحليلٍ مستقلٍّ، وإيجاد حلول عملية جليّة لقضايا معقدة تهمُّ الحقليْنِ السياسي والأكاديمي.

ملحوظة:

لا تعبّر الآراء الواردة في المقال بالضرورة عن اتجاهات يتبناها المركز، وإنّما تعبّر عن رأي كتابِها.

حقوق النشر محفوظة © 2026

١. الملخص التنفيذي:

- يتزايد نشر تطبيقات الذكاء الاصطناعي في العراق بسرعة من نظم الخدمات العامة وتحليل بيانات الصحة إلى أنظمة يتزايد نشر تطبيقات الذكاء الاصطناعي في العراق بسرعة، من نظم الخدمات العامة وتحليل بيانات الصحة إلى أنظمة المراقبة والتسويق الإلكتروني. وهذا النمو يفتح فرصاً اقتصادية واجتماعية كبيرة، لكنه يعرّض خصوصية المواطنين وممارسات الحوكمة الرقمية لمخاطر جسيمة.
- يبيّن الواقع العراقي أن هناك ثلاث قضايا رئيسة في الفضاء الرقمي: جمع البيانات المفرط، ضعف الأطر القانونية، إلى جانب التهديدات السيبرانية ونقص الوعي الرقمي.
- يحتاج العراق إلى إطار قانوني واضح لحماية البيانات، وممارسات تقنية مثل التصميم لحماية الخصوصية، التشفير، الرقابة على الخوارزميات، فضلاً عن بناء قدرات مؤسساتية ومجتمعية.
- على صانع القرار البدء بحوار متسلسل ومتسق حول التطبيق المتدرج للحماية القانونية للمعلومات، مع التأكيد على أن الحوار مع القطاع الخاص والمجتمع المدني ضروري لضمان توازن بين الابتكار ومراعاة الحقوق.
- لا يوجد قانون شامل ينظم حماية البيانات في العراق، بما في ذلك في القطاع الخاص، ومع ذلك توجد بعض الأحكام التي تنظم الخصوصية بشكل عام، وتوفر حماية للبيانات الشخصية في الاتصالات الهاتفية والبرقيات والوثائق الحكومية.

- لا ترتقي الأحكام المعمول بها في العراق إلى مستوى معايير حماية البيانات الدولية، مثل تلك التي وضعها النظام الأوروبي العام لحماية البيانات (GDPR)، ومنظمة التعاون الاقتصادي والتنمية (OECD)، ومنظمة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC)، ومبادرة حماية البيانات الشخصية (PIPL)، مما يجعلها غير مناسبة لمعالجة مخاوف حماية البيانات في ظل التطور التكنولوجي المتسارع.
- في البعد الاقتصادي، تعمل الدول على وضع قوانين للتحكّم في جوانب مختلفة من هذا المجال، مثل الاختصاص القضائي وتوطين البيانات. لذلك، ينبغي مراعاة تعريفات ومبادئ النظام الأوروبي العام لحماية البيانات (GDPR) والأطر الأخرى عند تحديد الخصوصية على الإنترنت وحماية البيانات في العراق.
- غياب القواعد الدولية في العراق يعيق وضع ضوابط متسقة مع المعايير الدولية، مما يجعل المواطنين عرضة لاستغلال البيانات والجرائم الإلكترونية، كما يزيد من صعوبة التعاون الدولي لمواجهة الجرائم الإلكترونية العابرة للحدود وانتهاكات البيانات.
- يتناول مشروع قانون مكافحة الجرائم الإلكترونية في معظمه جرائم الحاسوب، ويفتقر إلى الكثير فيما يتعلق بحماية البيانات.
- لا تستطيع القوانين التقليدية المعمول بها في العراق التعامل مع التحديات الجديدة التي يفرضها العصر الرقمي أو

استيعابها، ويواجه المواطنون مخاطر تهدد الأمن القومي والمصالح الاقتصادية.

- العراق بحاجة إلى بذل جهود عاجلة وسريعة لتنظيم وحماية البيانات عبر الإنترنت لمعالجة المخاطر المتزايدة في المجال الرقمي.
- من الضروري تعديل القوانين الحالية لمعالجة القضايا المعاصرة الحرجة المتعلقة بحماية البيانات، وضمان توافقها مع التحديات التكنولوجية والمجتمعية الراهنة.
- يجب على العراق إبرام اتفاقيات متعددة الأطراف وثنائية لتعزيز حماية البيانات عبر الحدود وضمان الأمن.
- يجب مراجعة مشروع قانون الجرائم الإلكترونية ليشمل مبادئ حماية البيانات المعاصرة.

II. المقدمة:

تكمن الأهمية العملياتية لخصوصية الذكاء الاصطناعي في الفضاء الرقمي العراقي في اعتماد الذكاء الاصطناعي على البيانات كمصدر رئيسي للتعلم والتطور. وتشمل البيانات المستخدمة: سلوكيات المستخدمين، مواقعهم الجغرافية، تفضيلاتهم الاستهلاكية، وحتى بياناتهم البيومترية. هذا الاعتماد المكثف يجعل حماية البيانات تحدياً استراتيجياً. وتتمثل المخاطر على الخصوصية في عدة جوانب، منها:

- المراقبة الخفية: خوارزميات تتبع المستخدمين على الإنترنت دون موافقة صريحة.
- إعادة تحديد الهوية: حيث يمكن ربط البيانات المجهولة بأفراد معينين.
- التمييز والتحيز: في خوارزميات اتخاذ القرار، مما قد يؤدي إلى نتائج مجحفة في مجالات مثل التوظيف والتأمين.
- الاختراقات الأمنية: إذ يمكن لأنظمة الذكاء الاصطناعي أن تصبح هدفاً لهجمات سيبرانية تستهدف البيانات الحساسة.

لقد تبنت اللائحة العامة لحماية البيانات الأوروبية (GDPR) في عام 2018 الأبعاد القانونية والأخلاقية، ووضعت إطاراً صارماً لتنظيم جمع البيانات واستخدامها. في المقابل، ما تزال تشريعات العديد من الدول العربية والنامية، بما فيها العراق، غير مواكبة للتحديات التقنية.

ومن الناحية الأخلاقية، يثار سؤال ملكية البيانات وحق الأفراد في التحكم بمعلوماتهم الشخصية. وتشمل الحلول التقنية الممكنة:

- التشفير وإخفاء الهوية والحوسبة الآمنة.
- الخصوصية التفاضلية (Differential Privacy) لضمان حماية البيانات عند تحليلها.
- الشفافية: إلزام الشركات والمؤسسات بالإفصاح عن سياسات جمع البيانات.
- المساءلة: إنشاء هيئات رقابية لمحاسبة الجهات المنتهِكة للخصوصية.
- التثقيف الرقمي: رفع وعي الأفراد بأهمية حماية بياناتهم وكيفية السيطرة عليها.

III. الذكاء الاصطناعي والخصوصية الرقمية في عصر التحول التكنولوجي

دخلت تقنيات الذكاء الاصطناعي إلى قلب التحوّل الرقمي في العراق، بدءاً من تحسين تقديم الخدمات الحكومية وصولاً إلى أتمتة العمليات في القطاع الخاص. ومع هذه الفوائد، تظهر أسئلة حرجة حول مدى حماية خصوصية الأفراد وحقوقهم الرقمية. يعالج هذا التحليل التحديات الرئيسة في المشهد الرقمي العراقي ويقدّم حلولاً عملية قابلة للتطبيق. وفي عام 2025، أصبح الذكاء الاصطناعي (AI) جزءاً أساسياً من حياتنا اليومية، حيث يُستخدم في مجالات متعددة مثل: الرعاية الصحية، التعليم، الأعمال التجارية، والأمن. ومع هذا التوسع، تزداد المخاوف بشأن كيفية تأثير هذه التقنيات على الخصوصية الرقمية للأفراد. تشير الدراسات إلى أن 57% من المستهلكين يعتبرون أن الذكاء الاصطناعي يشكل تهديداً كبيراً لخصوصيتهم، بينما يشعر 27% بالحياد تجاه هذه المسألة، و12% فقط لا يعتقدون أن الذكاء الاصطناعي يؤثر سلباً على خصوصيتهم.[1]

يشهد العالم طفرة غير مسبوقة في مجال الذكاء الاصطناعي، حيث أصبح يُوظف في مختلف القطاعات الاقتصادية والاجتماعية والأمنية والصحية. هذا التطور السريع يطرح تحديات متعلقة بحماية البيانات الشخصية والخصوصية الرقمية للأفراد، خصوصاً في ظل تضخم حجم البيانات التي تعتمد عليها خوارزميات التعلم الآلي.

1. 10 Under-the-Radar AI Companies to Watch in 2026, https://www.eweek.com/news/under-the-radar-ai-companies-2026/

وتكمن أهمية هذا البحث في إبراز العلاقة بين الذكاء الاصطناعي وخصوصية المعلومات في العراق، وتحديد المخاطر والحلول الممكنة لضمان فضاء رقمي آمن يسهم في تنمية الاقتصاد الوطني العراقي. كما تهدف الدراسة إلى تسليط الضوء على أهم التحديات التي قد تواجه حماية خصوصية الذكاء الاصطناعي في الفضاء الرقمي العراقي، من حيث:[2]

1. بيان وتحديد الأسباب الحقيقية التي تشكل عائقاً أمام حماية خصوصية الذكاء الاصطناعي في الفضاء الرقمي العراقي في القطاعات العامة والخاصة والمختلطة، اعتماداً على التحليل العلمي الذي تحدده منهجية هذا البحث.

2. طرح الحلول العملية لتحقيق خصوصية الذكاء الاصطناعي في الفضاء الرقمي العراقي من خلال الخطط الاقتصادية الطويلة والمتوسطة الأمد، بما يضمن تحقيق تنمية اقتصادية شاملة ومستدامة، وتطوير الاستثمار في الاقتصاد الوطني العراقي.

سوف تتناول هذه الورقة مفاهيم محددة لكيفية معالجة التحديات التي تواجه مسألة خصوصية الذكاء الاصطناعي في الفضاء الرقمي العراقي في القطاعات العامة والخاصة والمختلطة، والتي تعيق تطورها، مع التعرف على إجراءات حماية الخصوصية في العراق والنرويج.

2. Data Protection in Iraq: Limitations of Existing Laws Amid the Tech Wave, TWEJER journal, Vo.8, Issue: 4, Nov. 2025. pp.468-469. https://journals.soran.edu.iq/index.php/Twejer/article/view/2066/1081

وتطرح الورقة فرضية وجود شركات تأمين ومؤسسات مالية في العراق تهدف إلى تأمين خصوصية الذكاء الاصطناعي في الفضاء الرقمي، وذلك ضمن القطاعات العامة والخاصة والمختلطة التي تعيق تطورها بشكل عام. كما تعتمد الورقة على التخطيط الاستراتيجي طويل الأمد (خطط لعشر سنوات) وخطط اقتصادية خمسية تتلاءم مع طبيعة العمل في العراق وبيئته الاجتماعية، بهدف تحقيق الأهداف التنموية الاقتصادية والاجتماعية المنشودة.

إن نظم المعلومات في المؤسسات والمشاريع الإنتاجية الصناعية التي لها علاقة مباشرة بالاقتصاد الوطني هي من الدعائم الأساسية المساهمة في حل معظم مشاكل توفير وتأمين خصوصية الذكاء الاصطناعي في الفضاء الرقمي العراقي في القطاعات العامة والخاصة والمختلطة والتي تعيق تطورها في المجمل من خلال اتخاذ القرارات الرشيدة والقضاء على البيروقراطية الإدارية وكذلك التداخل في المهام الإدارية بين الوحدات التنظيمية المختلفة حتي يتم تأمين خصوصية الذكاء الاصطناعي في الفضاء الرقمي العراقي في القطاعات العامة والخاصة والمختلطة والتي تعيق تطورها بالمجمل.

١٧. لماذا الخصوصية مهمة في سياق الذكاء الاصطناعي؟

يعتمد الذكاء الاصطناعي على كميات ضخمة من البيانات، بعضها شخصي وحساس. وإن استُخدمت هذه البيانات بلا ضوابط، فقد يؤدي ذلك إلى تمييز آلي، انتهاك للخصوصية، وتسريب معلومات حساسة، كما قد يردع الأفراد عن استخدام الخدمات الرقمية، مما يقلل من الفوائد الاقتصادية والاجتماعية. وتبرز التحديات الرئيسة في الفضاء الرقمي العراقي في هذا السياق، وهي كما يلي:[3]

1. نقص الأطر التشريعية الواضحة والتطبيق الضعيف: القوانين الحالية غير متكاملة أو غير قابلة للتطبيق بشكل صارم فيما يخص حماية البيانات الشخصية، ولا توجد آليات رقابية فعّالة على استخدام تقنيات الذكاء الاصطناعي.
2. جمع بيانات مفرط وغياب مبدأ التقليل من البيانات: العديد من المؤسسات تجمع بيانات لا حاجة واقعية لمعالجتها، أو تخزنها لفترات طويلة دون أهداف واضحة.
3. عدم الشفافية: استخدام خوارزميات مغلقة يعرقل إمكانية التدقيق والتدخل عند حدوث تحيّز أو أخطاء.
4. نقص القدرات التقنية والأمنية: ضعف البنية التحتية للأمن السيبراني، ومحدودية الخبرات المحلية في حماية البيانات وإدارة مخاطر الذكاء الاصطناعي.

3. ناظم حسن ومي ابلحد، تدقيق التحيز في الذكاء الاصطناعي في ضوء اطار عمل تدقيق الذكاء الاصطناعي لمعهد المدققين الداخليين «دراسة نظرية تحليلية»، مجلة الدراسات التجارية والاقتصادية المعاصرة، المجلد 6 العدد 1، 2023. صفحات متفرقة.

5. مخاطر التجسس والمراقبة: أدوات المراقبة أو أنظمة التعرف قد تُستخدم بطريقة تنتهك الحريات المدنية، خصوصاً في غياب إشراف قانوني مستقل.
6. وعي منخفض لدى الجمهور والمؤسسات: قلة فهم المواطنين لحقوقهم الرقمية، وضعف ممارسات الشركات في الإفصاح والحصول على موافقات صحيحة.

لذلك تتطلب الإجراءات سن قانون لحماية البيانات الشخصية يحدد: قواعد جمع البيانات، غاياتها، حقوق الأفراد (الوصول، التصحيح، الحذف)، والعقوبات على الانتهاكات، وإنشاء هيئة رقابية مستقلة للبيانات والذكاء الاصطناعي مع صلاحيات تحقيق وفرض عقوبات، مع تطبيق مبدأ الخصوصية منذ التصميم (Privacy by Design) بحيث تلزم المشاريع الحكومية والخاصة بتضمين حماية الخصوصية في مراحل التصميم الأولى لأنظمة الذكاء الاصطناعي، واعتماد تقييم الأثر على الخصوصية (DPIA) قبل نشر أي نظام جديد يتعامل مع بيانات حساسة.

من الضروري وضع قيود عملية على تجميع وتخزين البيانات، بفرض مبدأ التقليل من البيانات ورفع متطلبات الاحتفاظ (حدود زمنية واضحة)، وتشجيع أنماط المعالجة المجهولة أو المشفّرة حيثما أمكن كما تعد الشفافية والمساءلة في الخوارزميات من الأمور الهامة ، منها اشتراط نشر ملخصات تفسيرية عن آليات عمل الخوارزميات وتأثيراتها المتوقعة على حقوق المستخدمين، وآليات مستقلة لمراجعة

الخوارزميات المستخدمة في قرارات تؤثر على الحقوق الأساسية (مثل العمل، الرفاه، الخدمات الاجتماعية)، و بناء القدرات الوطنية والأمن السيبراني من برامج تدريبية للعاملين في القطاع العام والخاص على إدارة بيانات المستخدمين وأمن الأنظمة، الى استثمارات في البنية التحتية للأمن السيبراني وأدوات تشفير قوية.

إلى جانب ذلك، سيكون من الضروري التثقيف العام وتعزيز ثقافة الموافقة الواعية من خلال حملات توعية تشرح حقوق المستخدمين، مخاطر مشاركة البيانات، وطرق حماية الخصوصية الشخصية. كما ينبغي إدخال مفاهيم الحقوق الرقمية في المناهج الجامعية وبرامج التدريب المهني.

ويعد تحقيق الشراكة بين القطاعين العام والخاص والمجتمع المدني خطوة مهمة، من خلال إنشاء مؤسسات مشتركة لصياغة إرشادات عملية، وإجراء اختبارات تجريبية للسياسات قبل التطبيق الوطني الكامل، مع إشراك منظمات حقوق الإنسان والخبراء التقنيين في آليات الرقابة لضمان فعالية حماية الخصوصية وحقوق المستخدمين.

٧. الأبعاد الاقتصادية

إن حماية الخصوصية في الأنظمة الرقمية ليست عبئاً فقط، بل تمثل فرصة اقتصادية، حيث تعزز ثقة المستخدمين في الأنظمة الرقمية، وتشجع على تبنّي خدمات الذكاء الاصطناعي، كما تزيد من الاستثمار في المشاريع الاقتصادية المختلفة. وعند وجود تنظيم جيد للشفافية والحوكمة، يمكن جذب شركات تقنية، مما يقلل من مخاطر الخسائر المالية الناتجة عن تسريبات المعلومات المهمة، ويعزز قيمة البيانات كمورد مستدام.

وتشمل الأبعاد الاقتصادية للبند التالي:

1. **جمع البيانات واستخدامها: الأساس الذي يعتمد عليه الذكاء الاصطناعي**

تعتمد خوارزميات الذكاء الاصطناعي على كميات ضخمة من البيانات لتدريب النماذج وتحسين أدائها، وتشمل هذه البيانات معلومات شخصية مثل:

- التفاعلات على وسائل التواصل الاجتماعي.
- سجلات البحث والتصفح.
- البيانات الصحية والمالية.
- الموقع الجغرافي والتفضيلات الشخصية.

ومع تزايد استخدام الذكاء الاصطناعي، تزداد المخاوف بشأن كيفية جمع هذه البيانات، ومن يملكها، وكيفية استخدامها ومشاركتها.

2. **المخاطر على الخصوصية: التحديات التي تواجه الأفراد والمجتمعات**

تتمثل أبرز المخاطر المرتبطة بالذكاء الاصطناعي على الخصوصية فيما يلي:

- المراقبة المستمرة: استخدام تقنيات مثل التعرف على الوجه والتتبع الجغرافي لمراقبة الأفراد دون علمهم أو موافقتهم.
- التمييز والتحيز: تدريب النماذج على بيانات غير متوازنة قد يؤدي إلى اتخاذ قرارات تمييزية ضد مجموعات معينة.
- القرارات غير الشفافة: صعوبة فهم كيفية اتخاذ النماذج للقرارات، مما يقلل من مستوى المساءلة والشفافية.
- الاختراقات الأمنية: تعرض البيانات الشخصية للاختراق قد يؤدي إلى تسريب معلومات حساسة تؤثر على الأفراد والمجتمعات.

3. الحلول والسياسات الممكنة: تعزيز الخصوصية في عصر الذكاء الاصطناعي

لمواجهة هذه التحديات، تم تطوير مجموعة من الحلول والسياسات التي تهدف إلى تعزيز الخصوصية الرقمية:

أ- الأطر القانونية والتنظيمية

- **اللائحة العامة لحماية البيانات ((GDPR**: تُعد من أبرز التشريعات التي تهدف إلى حماية خصوصية الأفراد في الاتحاد الأوروبي.
- **قانون الذكاء الاصطناعي في الاتحاد الأوروبي (EU AI Act):** يهدف إلى تنظيم استخدام الذكاء الاصطناعي وضمان توافقه مع معايير الخصوصية والأخلاقيات.
- **القوانين المحلية**: مثل قانون حماية الخصوصية في كاليفورنيا (CCPA) في الولايات المتحدة، الذي يمنح الأفراد حقوقاً إضافية بشأن بياناتهم الشخصية.

ب- التقنيات الحديثة لحماية الخصوصية

- التعلم الفيدرالي (Federated Learning): يتيح تدريب النماذج على البيانات المحلية دون الحاجة إلى نقلها إلى الخوادم المركزية، مما يقلل من مخاطر تسريب البيانات.
- التشفير المتقدم: استخدام تقنيات مثل التشفير المتماثل وغير المتماثل لحماية البيانات أثناء النقل والتخزين.

- الخصوصية التفاضلية ((Differential Privacy تقنية تهدف إلى إضافة تشويش إلى البيانات لضمان عدم الكشف عن معلومات فردية عند تحليل البيانات.
- التوعية والتعليم: رفع مستوى الوعي بين الأفراد حول حقوقهم الرقمية وكيفية حماية بياناتهم الشخصية من خلال:
  - برامج تدريبية وورش عمل.
  - حملات توعية عبر وسائل الإعلام.
  - توفير أدوات وتقنيات تساعد الأفراد على التحكم في بياناتهم.

VI. أمثلة واقعية: تطبيقات الذكاء الاصطناعي وتأثيرها على الخصوصية

تم تغريم شركة Clearview AI بمبلغ 30.5 مليون يورو من قبل الهيئة الهولندية لحماية البيانات، لاستخدامها صوراً من وسائل التواصل الاجتماعي دون إذن لتدريب نماذج التعرف على الوجه.[4] كما خضعت شركة X (تويتر سابقاً) للتحقيق من قبل لجنة حماية البيانات الإيرلندية لاستخدامها بيانات المستخدمين الأوروبيين

4. Dutch regulator slaps Clearview AI with $33 million fine and threatens executive liability, Dutch regulator slaps Clearview AI with $33 million fine, threatens executive liability | The Verge

لتدريب روبوت المحادثة "Grok" دون موافقة صريحة.[5] كما تم منع شركة ميتا (META) من إطلاق نموذج الذكاء الاصطناعي المتقدم "Llama" في الاتحاد الأوروبي بسبب المخاوف التنظيمية، بما في ذلك قوانين حماية البيانات الصارمة.[6] وبينما يقدم الذكاء الاصطناعي فرصاً هائلة لتحسين حياتنا، من الضروري تبني سياسات وتقنيات تضمن حماية الخصوصية الرقمية. ويجب تحقيق توازن بين الابتكار وحماية حقوق الأفراد من خلال:

- تطوير أطر قانونية مرنة تواكب التطورات التكنولوجية.
- استثمار في تقنيات تحمي البيانات وتضمن الشفافية.
- تعزيز الوعي والتعليم بين الأفراد والمؤسسات.

من خلال هذه الجهود المشتركة، يمكننا بناء بيئة رقمية تحترم الخصوصية وتعزز من ثقة الأفراد في استخدام تقنيات الذكاء الاصطناعي.

5. EU hits Elon Musk's X with 120 million euro fine for breaching bloc's social media law, https://apnews.com/article/x-elon-musk-twitter-european-union-regulations-0a135601e050518d5aa0a0155f973177
6. Meta pulls plug on release of advanced AI model in EU, Meta pulls plug on release of advanced AI model in EU | Meta | The Guardian.

VII. الذكاء الاصطناعي وحماية الخصوصية في النرويج: التوجهات والسياسات لسنة 2025

أ- المبادرات الحكومية والاستراتيجيات الوطنية

تسعى النرويج إلى أن تكون رائدة في مجال الذكاء الاصطناعي ذي المسؤولية القانونية المحدودة، مع التركيز على احترام الخصوصية وحماية البيانات. وقد أعلنت الحكومة النرويجية، في آذار 2025، عن خطط لتطبيق لائحة الاتحاد الأوروبي للذكاء الاصطناعي (EU AI Act)، وتطوير قانون نرويجي متخصص في الذكاء الاصطناعي، بهدف تنفيذ القانون الجديد بحلول صيف عام 2026. وتُشرف هيئة الاتصالات النرويجية (Nkom) على تطبيق هذه السياسات، بما في ذلك تنظيم استخدام الذكاء الاصطناعي في القطاعين العام والخاص، وضمان الامتثال للمعايير الأوروبية.

ب- التشريعات المحلية المتعلقة بالخصوصية وحماية البيانات

في كانون الثاني/يناير2025، دخل قانون الاتصالات الإلكترونية الجديد (Ekomloven) حيز التنفيذ، والذي ينظم استخدام بيانات المرور في شبكات الاتصالات. ويُشترط بموجب هذا القانون أن يتم مسح أو إخفاء هوية بيانات المرور عندما لا تكون ضرورية للغرض المحدد، مع السماح بالاحتفاظ بها فقط إذا كانت تُستخدم لتقديم خدمة ذات قيمة مضافة وبموافقة صريحة من المستخدم.[7]

7. Data protection laws in Norway, Data protection laws in Norway - Data Protection Laws of the World

ج- التعاون مع الاتحاد الأوروبي والامتثال للمعايير الدولية

تلتزم النرويج بتطبيق لائحة الاتحاد الأوروبي للذكاء الاصطناعي (EU AI Act)، والتي دخلت حيز التنفيذ في آب /أغسطس 2024. تُعتبر النرويج جزءاً من المنطقة الاقتصادية الأوروبية (EEA)، مما يعني أن التشريعات الأوروبية تُطبق عليها بشكل مباشر، بما في ذلك تلك المتعلقة بالذكاء الاصطناعي وحماية البيانات.

د- التوجهات المستقبلية والتحديات

على الرغم من التقدم في تطوير السياسات والتشريعات، تشير الدراسات إلى أن تبني الذكاء الاصطناعي في النرويج يسير بوتيرة أبطأ من المتوقع، سواء في القطاع العام أو الخاص. وتُظهر البيانات المستمدة من مسح "OKIOS" لسنة 2024 أن استخدام الذكاء الاصطناعي لا يزال في مراحله المبكرة، على الرغم من التوقعات العالية لاستخدامه في المستقبل.[8]

VIII. تطبيقات الذكاء الاصطناعي في القطاع العام النرويجي لسنة 2025: الابتكار والامتثال

أ- المبادرات الحكومية والإستراتيجيات الوطنية

تسعى النرويج إلى أن تكون رائدة في مجال الذكاء الاصطناعي المسؤول، مع التركيز على احترام الخصوصية وحماية البيانات. أعلنت

8. Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024, [2412.19273] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024

الحكومة النرويجية في آذار/مارس 2025، عن خطط لتطبيق لائحة الاتحاد الأوروبي للذكاء الاصطناعي (EU AI Act) وتطوير قانون نرويجي متخصص في الذكاء الاصطناعي، مع استهداف تنفيذ القانون الجديد بحلول صيف 2026، وتشرف هيئة الاتصالات النرويجية (Nkom) على تطبيق هذه السياسات، بما في ذلك تنظيم استخدام الذكاء الاصطناعي في القطاعات العامة والخاصة، وضمان الامتثال للمعايير الأوروبية.[9]

ب- التشريعات المحلية المتعلقة بالخصوصية وحماية البيانات

في كانون الثاني/يناير2025، دخل قانون الاتصالات الإلكترونية الجديد (Ekomloven) حيز التنفيذ، والذي ينظم استخدام بيانات المرور في شبكات الاتصالات. يُشترط بموجب هذا القانون أن يتم مسح أو إخفاء هوية بيانات المرور عندما لا تكون ضرورية للغرض المحدد، مع السماح بالاحتفاظ بها فقط إذا كانت تُستخدم لتقديم خدمة ذات قيمة مضافة وبموافقة صريحة من المستخدم.[10]

ج- التعاون مع الاتحاد الأوروبي والامتثال للمعايير الدولية

تلتزم النرويج بتطبيق لائحة الاتحاد الأوروبي للذكاء الاصطناعي (EU AI Act)، والتي دخلت حيز التنفيذ في شهر اب/أغسطس 2024، وتعتبر النرويج جزءاً من المنطقة الاقتصادية الأوروبية (EEA)، مما يعني

9. AI in Norway: Innovation, KI-Norge, and Compliance in 2025, Norway AI 2025: KINorge & Responsible Compliance | Nemko Digital
10. Data protection laws in Norway, Data protection laws in Norway - Data Protection Laws of the World

أن التشريعات الأوروبية تُطبق عليها بشكل مباشر، بما في ذلك تلك المتعلقة بالذكاء الاصطناعي وحماية البيانات.[11]

د- التوجهات المستقبلية والتحديات

على الرغم من التقدم في تطوير السياسات والتشريعات، تشير الدراسات إلى أن تبني الذكاء الاصطناعي في النرويج يسير بوتيرة أبطأ من المتوقع، سواء في القطاع العام أو الخاص. وتُظهر البيانات المستمدة من مسح "NOKIOS" لعام 2024 أن استخدام الذكاء الاصطناعي لا يزال في مراحله المبكرة، على الرغم من التوقعات العالية لاستخدامه في المستقبل.[12]

تشهد النرويج في العام 2025، تقدماً ملحوظاً في تطبيقات الذكاء الاصطناعي ضمن القطاع العام، مع التركيز على الابتكار المسؤول والبنية التحتية المستدامة. وفيما يلي أبرز المشاريع والمبادرات الحكومية الرائدة في هذا المجال:

1. **مشروع "Stargate Norway" – مركز بيانات متقدم للذكاء الاصطناعي**

أعلنت شركات Aker Nscaleg عن خطط لبناء مركز بيانات متطور في منطقة نارفيك شمال النرويج، بالشراكة مع OpenAI سيُطلق على

11. Key Data & Cybersecurity Laws, Key Data & Cybersecurity Laws | Norway | Global Data and Cyber Handbook | Baker McKenzie Resource Hub.
12. Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024, [2412.19273] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024

المشروع اسم "Stargate Norway"، وهو يهدف إلى إنشاء أول «مصنع ذكاء اصطناعي» في أوروبا، مزود بـ 100 الف معالج من نوع NVIDIA، ويعمل بالكامل بالطاقة المتجددة. من المتوقع أن يُسهم هذا المشروع في تعزيز قدرة النرويج على تطوير نماذج الذكاء الاصطناعي المتقدمة، بما في ذلك تطبيقات الدفاع والأمن، في إطار التعاون مع حلف الناتو.[13]

2. KI-Norge مركز التنسيق الوطني للذكاء الاصطناعي

تأسس "KI-Norge" (الذكاء الاصطناعي النرويجي) تحت إشراف وكالة الرقمنة النرويجية (Digdir)، ليكون منصة وطنية تهدف إلى تعزيز الاستخدام المسؤول للذكاء الاصطناعي. يشمل المشروع "AI Sandbox" الذي يتيح للمؤسسات الحكومية والشركات الصغيرة والمتوسطة اختبار حلول الذكاء الاصطناعي في بيئة آمنة ومراقبة، مما يعزز الابتكار مع الامتثال للمعايير القانونية والأخلاقية.[14]

3. دعم البحث والتطوير في الذكاء الاصطناعي

خصصت النرويج تمويلاً قدره 62 مليون كرونة نرويجية (6.2 مليون يورو) لدعم مشاريع الدكتوراه في القطاع العام والصناعي في مجال الذكاء الاصطناعي لسنة 2025. وتهدف هذه المبادرة الى تعزيز التعاون بين الجامعات والمؤسسات الحكومية لتطوير حلول مبتكرة

13. Røkkes datasenter kan bli Natos nye AI-våpen, Røkkes datasenter kan bli Natos nye AI-våpen – E24
14. AI in Norway: Innovation, KI-Norge, and Compliance in 2025, Norway AI 2025: KINorge & Responsible Compliance | Nemko Digital

في مجالات مثل الرعاية الصحية والإدارة العامة والطاقة.[15]

4. تطبيقات الذكاء الاصطناعي في القطاع الصحي

يعتبر القطاع الصحي في النرويج من الرواد في تبني تقنيات الذكاء الاصطناعي، حيث يتم استخدامها في تحليل البيانات الطبية، تحسين تشخيص الأمراض وتخصيص العلاجات، تتم هذه التطبيقات بالتعاون بين المستشفيات العامة والجامعات والشركات التكنولوجية، مما يسهم في تحسين جودة الرعاية الصحية وكفاءتها.[16]

ه- استراتيجية النرويج الرقمية 2024–2030

تهدف استراتيجية النرويج الرقمية إلى جعل البلاد الأكثر رقمنة في العالم بحلول العام 2030، وتركز الاستراتيجية على تعزيز استخدام الذكاء الاصطناعي في الإدارة العامة، تحسين البنية التحتية الرقمية، وضمان حماية البيانات الشخصية. تشمل المبادرات تطوير شبكات اتصال سريعة وآمنة، وتسهيل مشاركة البيانات بين القطاعات المختلفة.[17] ومن خلال هذه المشاريع والمبادرات، تسعى النرويج إلى تعزيز مكانتها كمركز رائد في مجال الذكاء الاصطناعي، مع التركيز على الابتكار المسؤول، الاستدامة، وحماية الخصوصية.

15. The Artificial Intelligence Initiative, The Artificial Intelligence Initiative
16. Artificial Intelligence 2025, Artificial Intelligence 2025 - Norway | Global Practice Guides | Chambers and Partners
17. Norway›s Digital Priorities, Norway›s Digital Priorities

و- استراتيجية النرويج الوطنية للذكاء الاصطناعي 2025

أعلنت الحكومة النرويجية عن استراتيجية وطنية تهدف إلى تعزيز استخدام الذكاء الاصطناعي في مجالات ذات أولوية، منها الإدارة العامة. تشمل الاستراتيجية تشجيع الهيئات الحكومية على تنفيذ مشاريع تجريبية لاكتساب الخبرة وفهم التكنولوجيا بشكل أفضل، تُعتبر هذه المشاريع التجريبية خطوة مهمة نحو تقييم فعالية الذكاء الاصطناعي في تحسين الخدمات الحكومية.[18]

ز- مراكز البحث الوطنية في الذكاء الاصطناعي

أطلقت النرويج ستة مراكز بحثية متخصصة في الذكاء الاصطناعي، بدعم حكومي يصل إلى 1 مليار كرونة نرويجية بهدف تعزيز التعليم والبحث في هذا المجال ومن بين هذه المراكز:

- **مركز AI Learn**: يركز على تعزيز التعلم البشري باستخدام الذكاء الاصطناعي، ويشمل تدريب 16 باحث دكتوراه.
- **معهد: TRUST** يهدف إلى تطوير أنظمة ذكاء اصطناعي موثوقة وآمنة، ويعمل على بناء القدرات في بيئات البحث وزيادة الكفاءة المجتمعية في هذا المجال.[19]

18. The National Strategy for Artificial Intelligence, The National Strategy for Artificial Intelligence - regjeringen.no
19. TRUST is one of six new research centres for artificial intelligence, TRUST is one of six new research centres for artificial intelligence - Department of Geosciences

- **منصة KI-Norgeالوطنية للذكاء الاصطناعي:** تأسست KI-Norge (الذكاء الاصطناعي النرويجي) كمنصة وطنية تهدف إلى تعزيز الاستخدام المسؤول للذكاء الاصطناعي في التعليم والقطاعات الأخرى. تشمل هذه المبادرة إنشاء "AI Sandbox" لاختبار الأنظمة في بيئة آمنة، مما يدعم الابتكار والامتثال للمعايير الأوربية[20].

تطوير المناهج التعليمية

تم تشكيل لجنة حكومية جديدة للإشراف على دمج الذكاء الاصطناعي في التعليم العالي. تعمل اللجنة على تقديم التوجيه للمؤسسات التعليمية حول كيفية دمج الذكاء الاصطناعي في المناهج الدراسية، وضمان الاستخدام المسؤول للتكنولوجيا من قبل الطلاب.[21]

برامج تدريبية ومبادرات تعليمية

أ- استخدام الذكاء الاصطناعي في التعليم الأساسي والثانوي

تعمل النرويج على دمج الذكاء الاصطناعي في التعليم الأساسي والثانوي من خلال تطوير أدوات تعليمية ذكية تساعد في تخصيص التعلم وتقديم الدعم الفردي للطلاب. يهدف ذلك إلى تحسين جودة التعليم وضمان الوصول المتساوي للفرص التعليمية.

20. AI in Norway: Innovation, KI-Norge, and Compliance in 2025, op cit,
21. Wasson and Færstad join the government›s AI committee for higher education, Wasson and Færstad join the government's AI committee for higher education | News | UiB

ب- التحديات والفرص

على الرغم من التقدم المحرز، تواجه النرويج تحديات في ضمان تكافؤ الفرص في الوصول إلى تقنيات الذكاء الاصطناعي، خاصة في المناطق الريفية. ومع ذلك، توفر المبادرات الحكومية والبرامج التعليمية فرصاً لتعزيز الكفاءة الرقمية وتطوير المهارات اللازمة لمواكبة التطورات التكنولوجية.

مشاريع الدكتوراه في القطاع العام

في إطار دعم البحث والتطوير، خصصت النرويج تمويلاً قدره 62 مليون كرونة نرويجية لدعم مشاريع الدكتوراه في القطاع العام، مع التركيز على تطبيقات الذكاء الاصطناعي. تستهدف هذه المبادرة تعزيز التعاون بين الجامعات والمؤسسات الحكومية لتطوير حلول مبتكرة في مجالات مثل الرعاية الصحية، الإدارة العامة، والطاقة.[22]

22. The Artificial Intelligence Initiative, op cit,

الخاتمة

تؤكد الورقة أن الذكاء الاصطناعي يقدّم فرصاً هائلة لتطوير المجتمعات، لكنه في الوقت نفسه يطرح تهديدات جدية على الخصوصية الرقمية. يكمن التحدي الرئيسي في إيجاد توازن بين الابتكار التكنولوجي وضمان حقوق الأفراد الرقمية. لذلك، يظل التعاون بين المشرّعين والشركات والمجتمع المدني ضرورة ملحّة لضمان فضاء رقمي أكثر أماناً وعدالة.

ولهذا، فإن الاستفادة الكاملة من الذكاء الاصطناعي في العراق تتطلب خلق توازن دقيق بين الابتكار وحماية الخصوصية. ويستلزم ذلك وضع إطار قانوني واضح، وتوفير أدوات تقنية فعّالة، إلى جانب بناء قدرات مؤسسية ومجتمعية قوية. كما أن التنفيذ المنهجي والمتدرّج لهذه الحلول قادر على تحويل المخاطر المحتملة إلى فرص اقتصادية واجتماعية ملموسة.

المراجع:

- ناظم حسن ومي ابلحد، تدقيق التحيز في الذكاء الاصطناعي في ضوء اطار عمل تدقيق الذكاء الاصطناعي لمعهد المدققين الداخليين «دراسة نظرية تحليلية»، مجلة الدراسات التجارية والاقتصادية المعاصرة، المجلد 6 العدد 1، 2023.
- 10 Under-the-Radar AI Companies to Watch in

2026, https://www.eweek.com/news/under-the-radar-ai-companies-2026/

- AI in Norway: Innovation, KI-Norge, and Compliance in 2025, Norway AI 2025: KINorge & Responsible Compliance | Nemko Digital

- Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024, [2412.19273] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024

- Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024, [2412.19273] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024

- Artificial Intelligence 2025, Artificial Intelligence 2025 - Norway | Global Practice Guides | Chambers and Partners

- Data protection laws in Norway, Data protection laws in Norway - Data Protection Laws of the World

- Data protection laws in Norway, Data protection laws in Norway - Data Protection Laws of the World

- Data Protection in Iraq: Limitations of Existing Laws Amid the Tech Wave, TWEJER journal, Vo.8, Issue: 4, Nov. 2025. pp.468-469. https://journals.soran.edu.iq/index.php/Twejer/article/view/2066/1081

- Dutch regulator slaps Clearview AI with $33 million fine and threatens executive liability, Dutch regulator slaps Clearview AI with $33 million fine, threatens executive liability | The Verge.

- EU hits Elon Musk's X with 120 million euro fine for breaching bloc's social media law, https://apnews.com/article/x-elon-musk-twitter-european-union-regulations-0a135601e050518d5aa0a0155f973177

- Key Data & Cybersecurity Laws, Key Data & Cybersecurity Laws | Norway | Global Data and Cyber Handbook | Baker McKenzie Resource Hub.

- Meta pulls plug on release of advanced AI model in EU, Meta pulls plug on release of advanced AI model in EU | Meta | The Guardian.

- Norway's Digital Priorities, Norway's Digital Priorities

- Røkkes datasenter kan bli Natos nye AI-våpen, Røkkes datasenter kan bli Natos nye AI-våpen – E24

- The Artificial Intelligence Initiative, The Artificial Intelligence Initiative

- The National Strategy for Artificial Intelligence, The National Strategy for Artificial Intelligence - regjeringen.no

- TRUST is one of six new research centres for artificial intelligence, TRUST is one of six new research centres for artificial intelligence - Department of Geosciences

- Wasson and Færstad join the government's AI committee for higher education, Wasson and Færstad join the government's AI committee for higher education | News | UiB

لِدولةٍ فاعلةٍ ومجتمعٍ مُشارِك

www.bayancenter.org
info@bayancenter.org