جامعة السلطان قابوس
مجلة الآداب والعلوم الاجتماعية

Sultan Qaboos University
Journal of Arts & Social Sciences

تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية: دراسة حالة في سلطنة عمان

ابتسام بنت سعيد الشهومية

أخصائي وثائق ومحفوظات
هيئة الوثائق والمحفوظات الوطنية
سلطنة عُمان
ibtisamalshuhoumi@gmail.com

سالم بن سعيد الكندي

أستاذ مشارك
قسم دراسات المعلومات
كلية الآداب والعلوم الاجتماعية
جامعة السلطان قابوس
salimsk@squ.du.om

محمد بن ناصر الصقري

أستاذ
قسم دراسات المعلومات
كلية الآداب والعلوم الاجتماعية
جامعة السلطان قابوس
saqrim@squ.edu.om

تاريخ الاستلام: ٢٠٢٢/٠٥/٣١
تاريخ القبول للنشر: ٢٠٢٣/٠٣/٢٧

تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية: دراسة حالة في سلطنة عمان

ابتسام بنت سعيد الشهومية، سالم بن سعيد الكندي، محمد بن ناصر الصقري

الملخص

هدفت الدراسة الحالية إلى التعرف على تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية للأفراد والمؤسسات في سلطنة عمان من حيث التعرف على استخداماتها على الشبكات الاجتماعية، والبرمجيات مفتوحة المصدر، والتعرف على التحديات الناجمة عن استخدامها. اعتمدت الدراسة المنهج النوعي، واستخدمت مجموعات التركيز التي بلغ عددها ثلاث مجموعات، والمقابلات شبه المقننة التي بلغ عددها ثمان مقابلات كأدوات لجمع البيانات. شمل مجتمع الدراسة المؤسسات التي لها ممارسات في استخدام تطبيقات الذكاء الاصطناعي وتلك التي تتعامل مع الأنظمة التقنية والتشريعية ذات العلاقة. وقد تم اختيار عينة الدراسة بشكل قصدي، وتألفت من ست مؤسسات؛ منها أربع مؤسسات حكومية، ومؤسستان خاصة. وتوصلت الدراسة إلى مجموعة من النتائج أبرزها: تستخدم بعض الشركات الكبرى تطبيقات الذكاء الاصطناعي، ضمن مواقع الشبكات الاجتماعية والبرمجيات مفتوحة المصدر في انتهاك الخصوصية، والتعدي على بيانات المستخدمين عن طريق تحليلها وبيعها لمؤسسات أخرى، لتحقيق أهداف سياسية أو ربح مادي. كما أوضحت النتائج أن تطبيقات الذكاء الاصطناعي قد تستخدم في ارتكاب جرائم معلوماتية كالابتزاز الإلكتروني، وسرقة البيانات الحكومية، وتعطيل الأنظمة، أو يمكن تطويعها من قبل المهندسين الاجتماعيين لارتكاب الجرائم الإلكترونية بطرق أكثر تقدمًا. وخلصت الدراسة إلى جملة من التوصيات من أهمها: ضرورة تصميم برنامج للعاملين في المؤسسات لتعزيز ورفع مستوى الوعي التقني، التشريعي، والتنظيمي في التعامل مع التقنيات الحديثة والمتطورة.

الكلمات المفتاحية: الاحتيال الإلكتروني؛ الشبكات الاجتماعية؛ الابتزاز الإلكتروني؛ الهندسة الاجتماعية؛ الذكاء الاصطناعي.

The Impact of Using Artificial Intelligence Applications on Digital Privacy: A Case Study in the Sultanate of Oman

Ibtisam Said Alshuhoumi, Salim Said Alkindi, and Mohammed Nasser Alsaqri

Abstract

The current study aimed to investigate the impact of using artificial intelligence applications on the digital privacy for individuals and institutions in Oman. It examined their use in social networks and open-source software, and identified the challenges arising from their use. The study adopted a qualitative approach, using three focus groups and eight semi-structured interviews as data collection tools. The study population included institutions that actively use artificial intelligence applications as well as those dealing with relevant technical and legislative systems. The sample was purposefully selected, consisting of six institutions: four government agencies and two private institutions. The study revealed that some major companies use artificial intelligence applications on social media platforms and open-source software to infringe upon privacy and violate user data by analyzing and selling it to other institutions for political or financial gains. The results also indicated that artificial intelligence applications could be used to commit information crimes such as electronic blackmail, theft of government data, and system disruptions. Additionally, they could be exploited by social engineers to perpetrate more advanced forms of cybercrime. The study concluded with several recommendations, including the need to design a program for employees in institutions to enhance and raise their technical, legislative, and regulatory awareness in dealing with modern and advanced technologies.

Keywords: Electronic fraud; social media; blackmail; Social Engineering; Artificial Intelligence.

المقدمة

شهد القرن الماضي تقدمًا تكنولوجيًا هائلًا، أحدث تأثيرًا على تطور وازدهار الحياة البشرية في كافة المجالات، من خلال ظهور أجهزة الحاسب الآلي التي سهلت عمل الإنسان، وبسبب التطورات السريعة في السعة التخزينية، والبرامج، ولغات البرمجة ظهرت تقنية الذكاء الاصطناعي التي تهتم بجعل الآلة تقوم بكافة الأعمال التي يقوم بها الإنسان بشكل أتقن منه، وتوصف بأنها ذكية (عمر، ٢٠٠٦؛ أبوبكر، ٢٠١٧). وعرّف John McCarthy الذي استخدم مصطلح الذكاء الاصطناعي لأول مرة في عام ١٩٥٦ بأنه علم ووسيلة لتصنيع الآلات بطريقة ذكية. وهو أداة ووسيلة لاستخدام الحاسب الآلي بطريقة مشابهة للطريقة التي يفكر بها البشر .(Lin& Hazelbaker, 2019; Gupta& Dhawan, 2018)

يستطيع الذكاء الاصطناعي تغيير طريقة تفاعل الإنسان مع التكنولوجيا، وبالأخص تفاعل البيانات الشخصية مع البرمجيات الذكية التي يستخدمها الإنسان بشكل مستمر ودائم. ويعد نظام Watson الذي يعتمد على خوارزميات التعلم في الوصول إلى البيانات، والتعرف على التهديدات المحتملة، وطريقة التعامل معها بكفاءة عالية. ومن جانب آخر قد تؤثر تقنيات الذكاء الاصطناعي على استقرار الوطن وأمنه، من خلال استخدام برامج الذكاء الاصطناعي في عمليات القرصنة والهندسة الاجتماعية، كما يقوم بها المهندسين الاجتماعيين (Peters, 2019; Dickson, 2017).

وعليه فقد ظهر اهتمام أكاديمي كبير بأخلاقيات الذكاء الاصطناعي بشكل يتزامن مع التطورات المتلاحقة في أدوات وتقنيات الذكاء الاصطناعي، وهو ما أدى إلى وضع قواعد أخلاقية في كيفية التعامل مع الذكاء الاصطناعي من قبل مجموعة من الشركات العملاقة (Wasilow & Thorpe, 2019). ومن هذا المنطلق سعت الدراسة للتعرف على تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية للأفراد والمؤسسات في سلطنة عمان؛ من حيث التعرف على استخدامات تطبيقات الذكاء الاصطناعي على الشبكات الاجتماعية، والبرمجيات مفتوحة المصدر، والتعرف على التحديات والمخاطر الناجمة عن استخدام تطبيقات الذكاء الاصطناعي. ويؤمل أن تخرج هذه الدراسة بتصور شامل لموضوع القضايا الأخلاقية لتطبيقات الذكاء الاصطناعي.

مشكلة الدراسة

حقق التطور التقني تغييرات إيجابية في كافة المجالات والأنشطة، وكان سببا رئيسا في ظهور الجرائم الإلكترونية التي نتج عنها مجموعة من الجرائم المادية الخطيرة، لذا فإنه سلاح ذو حدين يستخدم في النفع والضرر (الملا، ٢٠١٧).

ولا يزال موضوع أخلاقيات الذكاء الاصطناعي غير مألوف لدى العديد من المهتمين والباحثين، ويحتاج إلى مراجعة عميقة لمناقشته، وصياغة تعريفات قانونية توفر الحماية التامة للمستخدمين، بالإضافة إلى وضع مبادئ تنظيمية تحكم عملية الاستخدام المثالي لتلك التقنيات (Baranov et al., 2019; Dahlan, 2018). الأمر الذي أدى إلى تزايد نسبة المخاوف على خصوصية البيانات لدى المستخدمين.

تعرضت الدول المتقدمة لعدد هائل من الانتهاكات على خصوصية المستخدمين، والجرائم الإلكترونية باستخدام تطبيقات الذكاء الاصطناعي كانتهاك بيانات المستخدمين وسرقة هوياتهم استنادًا إلى ما أشارت إليها مجموعة من الدراسات مثل: دراسة Yeoh (٢٠١٩) التي توصلت إلى أن جرائم التعدي على البيانات الشخصية وسرقتها جاءت في المرتبة الثالثة على مستوى الجرائم في الولايات المتحدة الأمريكية، وبلغ عدد الأشخاص الذين تعرضوا للتعدي على بياناتهم الشخصية نحو أكثر من ملياري شخص. في حين احتلت الجرائم الإلكترونية مثل سرقة البيانات في المملكة المتحدة نصف جرائم البلاد، وبلغت تكلفة تصدي تلك الهجمات حوالي (٢٦٧٠٠٠) دولار أمريكي. ولم تقتصر الجرائم الإلكترونية على الدول المتقدمة فقط، وإنما شملت الدول النامية ايضًا، وكانت دول جنوب أفريقيا من أبرز الدول النامية التي تعرضت للهجمات الإلكترونية وسرقة المعلومات (Katzan, 2011; Ezeji & Olutola, 2018). في حين نجد أن الدول العربية تعرضت لعدد قليل نسبيًا لجرائم الذكاء الاصطناعي بالمقارنة مع الدول المتقدمة، وهو ما دعا إلى ضرورة إصدار مبادئ تنظيمية وتشريعية توفر الحماية الكاملة للمستخدمين، وضرورة إثراء النتاج الفكري العربي بمخاطر تقنيات الذكاء الاصطناعي، وكيفية التصدي لها (الملا، ٢٠١٧).

واستنادًا لما سبق عرضه من مخاطر استخدام تطبيقات الذكاء الاصطناعي، ولقلة النتاج الفكري العربي المتخصص في هذا الموضوع، فإن هذه الدراسة تسعى إلى التعرف على تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية للأفراد والمؤسسات في سلطنة عمان من حيث التعرف على استخدامات تطبيقات الذكاء الاصطناعي على الشبكات الاجتماعية، والبرمجيات مفتوحة المصدر، والتعرف على التحديات والمخاطر الناجمة عن استخدام تطبيقات الذكاء الاصطناعي.

أهداف الدراسة وأسئلتها

سعت الدراسة إلى التعرف على تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية للأفراد والمؤسسات في سلطنة عمان من حيث:

- التعرف على آليات توظيف تطبيقات الذكاء الاصطناعي على الشبكات الاجتماعية، والبرمجيات مفتوحة المصدر من وجهة نظر المتخصصين.

- التعرف على التحديات والمخاطر الناجمة عن استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية من وجهة نظر المتخصصين.

وتحاول الدراسة الإجابة عن الأسئلة البحثية الآتية:

١. ما آليات توظيف تطبيقات الذكاء الاصطناعي على الشبكات الاجتماعية والبرمجيات مفتوحة المصدر؟
٢. ما التحديات والمخاطر الناجمة عن استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية؟

أهمية الدراسة

الجانب النظري: تسعى الدراسة للكشف عن الآثار الأخلاقية لتطبيقات الذكاء الاصطناعي على الخصوصية الرقمية في سلطنة عمان. ويعد هذا الموضوع مهم جدًا للمؤسسات الحكومية والخاصة في السلطنة في ظل دخول تطبيقات الذكاء الاصطناعي كافة المجالات، وسعي السلطنة نحو زيادة استخدامها وتفعيلها لتلك التقنيات الذكية؛ لذلك يؤمل أن تحقق الدراسة إضافة للنتاج الفكري العربي المتخصص في هذا المجال، وتفتح آفاقًا جديدة للمزيد من الدراسات حول هذا الموضوع في ضوء المستجدات الحديثة.

الجانب العملي: يؤمل أن تفيد هذه الدراسة الجهات والفئات الآتية:

- شرطة عمان السلطانية: تركز الدراسة على الجرائم والانتهاكات الأخلاقية التي يتعرض لها المستخدمون نتيجة استخدام تطبيقات الذكاء الاصطناعي، وكيفية التصدي لها، مما يوضح الحاجة لوضع وسائل تحمي المستخدمين وبياناتهم من أي اختراق أو انتهاك.
- أفراد المجتمع: تقدم الدراسة جملة من المخاطر التي يتعرض لها المستخدمون والأفراد نتيجة استخدام تطبيقات الذكاء الاصطناعي، وسبل حماية بياناتهم من تلك الانتهاكات.
- الباحثين والمهتمين بالموضوع: تساهم الدراسة في فتح آفاق جديدة لإجراء المزيد من الدراسات في الموضوع نفسه، من خلال دراسة الواقع الحالي لتطبيقات الذكاء الاصطناعي، والكشف عن الآثار الأخلاقية لاستخدام تلك التطبيقات.

حدود الدراسة

الحدود الموضوعية: تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية: دراسة حالة في سلطنة عمان

الحدود المكانية: مجموعة من المؤسسات بالسلطنة (وزارة النقل والاتصالات وتقنية المعلومات – شرطة عمان السلطانية – المركز الوطني للإحصاء والمعلومات – الادعاء العام – بنك مسقط – محامين).

الحدود الزمنية: أكتوبر ٢٠١٩ – مارس ٢٠٢٣م.

الدراسات السابقة

تعد الدراسات التي تناولت موضوع الأثار الأخلاقية لتطبيقات الذكاء الاصطناعي مهمة وضرورية في الوقت الحالي نظرًا لدخول الذكاء الاصطناعي في كافة المجالات واعتماد المؤسسات الحكومية والخاصة حول العالم عليها. تبين من خلال مراجعة النتاج الفكري المنشور التنوع الكبير للدراسات الأجنبية التي تناولت موضوع التأثير الأخلاقي لاستخدام تطبيقات الذكاء الاصطناعي، ويعالجه من زوايا واتجاهات مختلفة بينما ركز النتاج الفكري العربي على مخاطر التقنيات الحديثة بشكل عام، وخصوصية المستخدم من نظرة قانونية فقط وأهمل موضوع التحديات الناجمة عن استخدام تطبيقات الذكاء الاصطناعي والتدابير لحماية الأفراد والمؤسسات من ذلك. وعرضت الدراسات السابقة وفق محورين، تناول المحور الأول الذكاء الاصطناعي والخصوصية الرقمية، في حين ركز المحور الثاني على مخاطر الذكاء الاصطناعي.

الذكاء الاصطناعي والخصوصية الرقمية

تعد قضية إساءة استخدام البيانات الشخصية، وانتهاك الخصوصية الرقمية، من أهم القضايا التي تشغل اهتمام الحكومات والأفراد، نظرًا للقدرة العالية التي يتمتع بها الذكاء الاصطناعي في تخزين البيانات، ومراقبة سلوك الأفراد، مما جعل الخصوصية الرقمية قيمة اجتماعية أساسية لابد من التركيز عليها (شاهين، ٢٠١١؛ LÓPEZ et al., 2014).

وأظهرت دراسة Atkinson (٢٠١٨) أن الذكاء الاصطناعي يستطيع جمع، وتحليل، ومعالجة البيانات بسرعة عالية، وهو ما يؤثر سلبًا على خصوصية الأفراد. من جهة أخرى أشارت دراسة Such, Espinosa, and García-Fornes (٢٠١٤) إلى أن السبب الرئيس في زيادة المخاوف حول خصوصية البيانات هو انتشار تقنيات الذكاء الاصطناعي، إذ إن الخصوصية كانت وما زالت مصدر قلق للأشخاص منذ القدم، ومن غير الممكن ربط ظهور قضية الخصوصية الرقمية باستخدام تقنيات الذكاء الاصطناعي.

وفي استطلاع أجراه Elhai et al.(٢٠١٧) للكشف عن النتائج المترتبة نتيجة شعور المستخدمين بالقلق من اختراق تقنيات الذكاء الاصطناعي لبياناتهم الشخصية. وتم استخدام مقياس Generalized Anxiety Disorder-7 (GAD-7) لقياس مستوى القلق. تبين أن (٩١٪) من المشاركين البالغ عددهم (٣٠٥) يشعرون بالقلق من قدرة التقنيات الذكية في الوصول إلى بياناتهم الشخصية بطرق غير قانونية. وتوصلت دراسة استقصائية أخرى إلى أن (٨٠٪) من المشاركين البالغ عددهم (٢٣٠٠٠) أعربوا عن خوفهم من وصول تقنيات الذكاء الاصطناعي إلى بياناتهم الشخصية، والاستفادة منها من خلال

بيعها لشركات تجارية أخرى. كما توصلت دراسة Brubaker (٢٠١٨) إلى أن (٤٥٪) من الأمريكيين يشعرون بالقلق بشأن انتهاك بياناتهم وخصوصيتهم على الإنترنت. وقام (٧٤٪) منهم بتقليل استخدامهم للإنترنت بسبب مخاوفهم المتزايدة اتجاه تقنيات الذكاء الاصطناعي. وأوضحت دراسة Sundaram and Omar (٢٠١٩) أن ازدياد الاهتمام بقضية انتهاك الخصوصية بين الأفراد هو اعتذارات شركات التكنولوجيا والذكاء الاصطناعي الغير مبررة لانتهاكاتها الواسعة على خصوصية المستخدمين، مما أدى إلى عدم وثوق الأشخاص بها.

شكلت قضية انتهاك الخصوصية خطراً على الأفراد والمؤسسات بسبب نموها المتسارع مع تطور تقنيات الذكاء الاصطناعي، وقدرتها في الوصول إلى معلومات سرية وغير مصرح بها قد تؤثر سلبًا على حياة الفرد أو إنتاجية المؤسسة ذاتها. وهذا ما أكدته دراسة Raban and Hauptman (٢٠١٨) إلى أن أنظمة الذكاء الاصطناعي تمتلك القدرة الفائقة على الهجوم والاختراق، وأصبحت قادرة على مهاجمة الأنظمة، ونشر الفيروسات الضارة، واختراق البيانات.

وفي دراسة Kumar and Balaramachandran (٢٠١٨) التي شكلت عينة الدراسة (١٥٠) شخص من عملاء البنوك، والمحللين، وصناع القرار في مختلف المؤسسات والشركات. توصلت إلى أن معظم عينة الدراسة يواجهون صعوبة في الوثوق بخوارزميات الذكاء الاصطناعي وبرامج الروبوت. وفي الوقت نفسه. في حين أضافت دراسة FERREIRA and KAWAKAMI (٢٠١٨) إلى أن برامج الفدية (ransomware) هي أقوى مهدد لخصوصية بيانات المستخدمين التي تعمل على إعاقة الوصول للبيانات، بالإضافة إلى سرقة البيانات للمستخدمين الذين يحجبون أجهزتهم.

مخاطر الذكاء الاصطناعي

استطاعت الكثير من المؤسسات والشركات إلى اختراق بيانات المستخدمين بهدف معالجتها لتحقيق أهداف سياسية أو تسويقية، وهو ما أوضحته دراسة تومي (٢٠١٧) إلى استخدام البيانات لتنفيذ إعلانات تسويقية، أو دعم أحزاب سياسية، أو استغلالها لإلحاق الضرر بأصحابها. وأكد القائمون على Amazon و Google حسب ما أشارت له دراسة Brubaker (٢٠١٨) عن استخدامهم لخوارزميات خاصة تستطيع تحليل البيانات بسرعة عالية بهدف تحديد الفئة المستفيدة من الإعلانات. وهذا ما أكدته دراسة Wasilow and Thorpe (٢٠١٩) التي أشارت إلى أن التسويق هو الهدف الأساسي لجمع وتحليل بيانات المستخدمين الشخصية. أوضحت دراسة الملا (٢٠١٧) إلى وجود طرق غير مباشرة للتلاعب في البيانات كالتحايل، والقدرة على التحكم فيها، عن طريق استبدالها، أو إضافة تعديلات عليها.

وتوصلت دراسة Yeoh (٢٠١٩) إلى تعرض أكثر من ملياري مستخدم لاختراق بياناتهم الشخصية، بتكلفة تقدر (٦٠٠) مليار دولار أمريكي، أي حوالي (٠,٨٪) من الدخل العالمي، لذلك احتلت جرائم التعدي على البيانات الشخصية وسرقتها المرتبة الثالثة بعد الفساد الحكومي وتهريب المخدرات. وفي المملكة المتحدة بلغت تكاليف الهجمات الإلكترونية حوالي (٢٦٧٠٠٠) دولار أمريكي. كما أكدت دراسة Katzan (٢٠١١) عن اختراق بيانات بليون شخص، ومن ضمنها سجلات طبية لأكثر من (١٠٠) مليون أمريكي.

وفي الإطار نفسه أشارت دراسة Kuhn (٢٠١٨) إلى أن اختراق Equifax في عام ٢٠١٧م هو أقوى اختراق تعرضت له الولايات المتحدة الأمريكية، وبلغ عدد الذين تعرضوا لهذا الاختراق هو (١٤٧) مليونا أمريكيا. ولم تقتصر الجرائم الإلكترونية على الدول المتقدمة فقط، وإنما توسعت لتشمل الدول النامية أيضًا مثل دول جنوب أفريقيا، إذ تعرضت لمجموعة من الهجمات المخطط لها، وسرقة المعلومات والملكية الفكرية (Katzan, 2011 ; Ezeji & Olutola, 2018). كما أن الجرائم الإلكترونية لم تقتصر على قطاع معين وإنما غطت معظم القطاعات بما فيها القطاع الصحي، نظرًا لاستخدام تقنيات الذكاء الاصطناعي في الآلات والأنظمة الطبية، وقدرتها على جمع بيانات المرضى عن طريق اختراق السجلات الطبية التي تحتوي على معلومات شاملة عن المريض كتاريخ مرضه وفترة علاجه، وهو ما أدى إلى انتهاك خصوصية المرضى (Dhshan, 2020). وهو ما أشارت إليه دراسة حسن (٢٠٢٢) إلى قيام الذكاء الاصطناعي بجمع بيانات المرضى وتقديم تقارير عن كل مريض لمساعدة الأطباء على تشخيص الحالة واختيار العلاج المناسب، ولكن قد تشكل تلك التقنيات مخاوف فيما يتعلق بمصير تلك البيانات التي تم جمعها واستخدامها لأغراض تجارية أو تسويقية. أضافت دراسة Kumar and Kumar (٢٠١٦) إلى تعرض (٩٤٪) من المستشفيات لاختراق واحد بسبب تقنيات الذكاء الاصطناعي. وفي جميع هذه الجرائم الإلكترونية كانت تقنيات الذكاء الاصطناعي عاملا مشتركا وأساسيا في حدوثها، وتطورها، وانتشارها.

وأوضحت دراستا تومي (٢٠١٧)، ومصطفى (٢٠١٦) إلى قدرة تقنيات الذكاء الاصطناعي من استخدام برمجيات تنصت، وتجسس، وتتبع، بالإضافة إلى جمع البيانات بشكل آلي وسريع للغاية. وهذا ما أكدته دراسة أبو منصور (٢٠٢٠) إلى استغلال تقنيات الذكاء الاصطناعي في اختراق الخصوصية من خلال مراقبة الاتصالات، وتسجيلات الدوائر التلفزيونية المغلقة، وحسابات التواصل الاجتماعي ومتابعتها، وهو ما خلق مقاومة لدمج تقنيات الذكاء الاصطناعي في القطاعات الأمنية والعسكرية. وأضافت دراسة قده وكحيط (٢٠٢٢) إلى قدرة الذكاء الاصطناعي على السيطرة ومراقبة الأجهزة الحكومية بالأخص الأجهزة الأمنية والعسكرية، والسيطرة على وسائل النقل العامة، وتهديد

البنية التحتية للدول من خلال ربط الأجهزة المتصلة بالانترنت مع أجهزة الأتمتة المنزلية (التشغيل الآلي)، الأمر الذي أدى إلى زيادة فرص الغزو على الحياة الخاصة بالأفراد والإضرار بها. وهو ما أكدته دراسة Power (٢٠١٦)، إلى أن تقنيات الذكاء الاصطناعي تمكنت من حفظ وتحرير بيانات مقاطع الفيديو والصوت، بالإضافة إلى قدرتها على مراقبة عدد كبير من الأشخاص في آن واحد قد يصل إلى (٢٠) مليون شخص، وتتم مراقبتهم بشكل مرئي أو صوتي. وفي السياق نفسه أوضحت دراسة (٢٠١٨) Denton, Pauwels, He, and Johnson أن تقنيات الذكاء الاصطناعي استطاعت على تحليل وتحسين صور الوجه من خلال استخدام وسائل التعرف على الوجه، بغرض جمع بيانات المستخدمون لأغراض سياسية متعلقة بالتجسس الاستخباري. وأضافت دراسة مراد (٢٠٢٢) إلى قدرة تقنيات الذكاء الاصطناعي على تحليل أكثر من ٦٠٠ ساعة من مقاطع الفيديو في اليوتيوب بغرض التنبؤ بالسلوك البشري والوصول إلى أكبر قدر من بيانات المستخدمين والاستفادة منها من خلال بيعها أو استخدامها في التسويق.

وأشارت دراسة Wasilow and Thorpe (٢٠١٩) إلى مشروع Project Arachnid الذي تبناه المركز الكندي لحماية الطفل، استطاع المشروع تتبع جميع الصور ومقاطع الفيديو المتعلقة بالاعتداء على الأطفال عبر الإنترنت وازالتها بشكل دائم، وفي المقابل تطرقت الدراسة إلى استخدام Edward Snowden لبرنامج زاحف بهدف جمع (٢٠٠٠٠٠) وثيقة سرية تقريباً، من خوادم وكالة الأمن القومي الأمريكية. وكشفت دراسة Lauterbach (٢٠١٩) عن قدرة تقنيات الذكاء الاصطناعي من إعادة معالجة الصور والبيانات لخداع الشبكات والأجهزة الأخرى، كما أن هجمات حجب الخدمة DDoS وما تحتويه من تحيزات وبرامج ضارة المسؤول عنها هو الذكاء الاصطناعي.

منهجية الدراسة وإجراءاتها

اعتمدت الدراسة على المنهج النوعي Qualitative Method لدراسة تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية للأفراد والمؤسسات في سلطنة عمان، وتسليط الضوء على استخدامات تطبيقات الذكاء الاصطناعي والتحديات الناجمة عن استخدامها. تم استخدام هذا المنهج لتحقيق أهداف الدراسة من خلال التحليل العميق للآثار، والتحديات، والمبررات التي سيكشفها المنهج النوعي.

اعتمدت الدراسة على أداتين وهما أداة مجموعات التركيز (Focus Group) وأداة المقابلة شبه المقننة (Semi- structured interview): اشتملت الدراسة على ثلاث مجموعات تركيز، تضمنت كل مجموعة، من (٦-٩) مشاركين، إذ تتكون مجموعات التركيز في العادة، من (٦-١٢) مشاركا (Walden, 2006)، أو من (٨-١٠) مشاركين (Kumar, 2010)، والغاية ألا يقل عدد المشاركين عن (٦) أفراد، ولا يزيد عن (١٢) فردًا، وهو المقياس المتبع في معظم الدراسات التي تعتمد على هذه الأداة. في حين ساهمت أداة المقابلة شبه المقننة في الحصول على المعلومات من عينة الدراسة المتعلقة بالإجابة على الأسئلة البحثية وتحقيق أهداف الدراسة، والتعرف على وجهات نظرهم المختلفة، الأمر الذي يساعد في الحصول على أكبر قدر ممكن من المعلومات للوصول إلى نتائج أدق (عبد المؤمن، ٢٠٠٨). واعتمدت الدراسة على أداة المقابلة شبه المقننة التي بلغ عددها أربعة، وتم اختيارها بشكل قصدي. ويوضح الجدول رقم (١) عينة الدراسة لأداة مجموعات التركيز وأداة المقابلة.

جدول (١): عينة الدراسة لأداة مجموعات التركيز

م	المؤسسة	نوعها	عدد المشاركين	نوع الأداة
١	وزارة النقل والاتصالات وتقنية المعلومات	تقنية	٨	مجموعة تركيز
٢	المركز الوطني للإحصاء والمعلومات	خدمية	٦	مجموعة تركيز
٣	الادعاء العام	قضائية	٩	مجموعة تركيز
٤	شرطة عمان السلطانية	أمنية	٣	مقابلات شبه مقننة
٥	بنك مسقط	اقتصادية	١	مقابلات شبه مقننة
٦	محاميين	خاصة	٤	مقابلات شبه مقننة

تمت عملية تحليل البيانات التي حصلنا عليها من مجموعات التركيز والمقابلات عن طريق اتباع المراحل الست الكبرى، كما وضحها Braun and Clarke (٢٠٠٦)، وهي:

١. جمع البيانات وتحويلها من الشكل المنطوق إلى الشكل المكتوب.
٢. إدراج رموز للبيانات المهمة التي تثير اهتمام الباحث.
٣. جمع كل البيانات المرمزة، والتحليل الواسع للموضوعات، ثم تقسيمها إلى أفكار رئيسة، وعرضها على شكل جداول أو خرائط ذهنية.
٤. عرض المواضيع ومراجعة الأفكار.
٥. التحليل والتعديل المستمر للأفكار، والوصول إلى الموضوعات الخاصة، وتسمية كل فكرة رئيسة.
٦. التحليل النهائي للمقابلة بربط موضوع الدراسة وأهدافها ومناقشتها بالرجوع إلى الدراسات السابقة.

نتائج الدراسة ومناقشتها

الآثار الأخلاقية لتطبيقات الذكاء الاصطناعي

تناول هذا المحور الآثار الأخلاقية لتطبيقات الذكاء الاصطناعي من وجهة نظر المشاركين، وتم تقسيم النتائج إلى قسمين:

القسم الأول: استخدامات تطبيقات الذكاء الاصطناعي ويناقش تطبيقات الذكاء الاصطناعي على الشبكات الاجتماعية، وتطبيقات الذكاء الاصطناعي على البرمجيات مفتوحة المصدر.

القسم الثاني: تحديات ومخاطر استخدام تطبيقات الذكاء الاصطناعي الذي يتطرق إلى معالجة البيانات لأغراض الابتزاز الإلكتروني، وسرقة البيانات الحكومية وتعطيل الأنظمة.

١. آليات توظيف تطبيقات الذكاء الاصطناعي

تطبيقات الذكاء الاصطناعي على الشبكات الاجتماعية

استطاعت تطبيقات الذكاء الاصطناعي على تبسيط عمل الشبكات الاجتماعية وتوسيع خدماتها لأكبر قدر ممكن من الأفراد، كما قامت الشبكات الاجتماعية باستغلال خوارزميات الذكاء الاصطناعي في جمع وتحليل بيانات المستخدمين، مما أدى إلى شعور المستخدمين بالخوف من انتهاك خصوصيتهم والوصول إلى البيانات التي قاموا بمشاركتها مع أطراف أخرى على الشبكات الاجتماعية، وهو ما تطرق له مختص في تقنية المعلومات (G3-2) إن تطبيقات الذكاء الاصطناعي سلاح ذو حدين، يمكن استخدامها لارتكاب جرائم معلوماتية وانتهاك خصوصية المستخدم، ولاسيما في شبكات التواصل الاجتماعي، ويمكن استخدامها في الوقت ذاته لتحسين أمن المعلومات. وأضاف مدير دائرة في الادعاء العام (G1-7) إلى قيام معظم شبكات التواصل الاجتماعي بجمع بيانات مستخدميها من خلال استغلال البيانات التي يقوم المستخدم بإدخالها عند التسجيل في المرة الأولى، ثم بيعها لمؤسسات وأطراف أخرى لتحقيق عائد مادي.

لقد أكد الطرح السابق من اتفاق أفراد مجتمع الدراسة في مجموعات التركيز والمقابلات شبه المقننة إلى أن تطبيقات الذكاء الاصطناعي تستخدم من قبل شبكات التواصل الاجتماعي من أجل تحسين جودة الخدمات المقدمة للمستخدمين، بالإضافة إلى انتهاك خصوصيتهم وسرقة بياناتهم. واتفقت هذه النتيجة مع نتائج دراسة Elhai et al. (٢٠١٧) التي أشارت إلى أن (٩١٪) من المشاركين أبدوا خوفهم من وصول التقنيات الذكية إلى بياناتهم وسرقتها بطرق غير مباشرة. في حين شعر (٨٠٪) من المشاركين عن قلقهم حول بيع بياناتهم لشركات أخرى لأغراض تجارية أو أمنية. وجاءت دراسة Brubaker (٢٠١٨) متفقة معها، وأضافت أن (٤٥٪) من الأمريكيين يشعرون بالقلق بشأن انتهاك بياناتهم وخصوصيتهم على الإنترنت. وقام (٧٤٪) منهم بتقليل استخدامهم للإنترنت بسبب مخاوفهم المتكررة اتجاه تقنيات الذكاء الاصطناعي.

أتفق جميع أفراد عينة الدراسة في مجموعات التركيز على اعتماد شبكات التواصل الاجتماعي في استخدام تقنيات الذكاء الاصطناعي لانتهاك بيانات مستخدميها، وتحليلها، وبيعها لمؤسسات تجارية أو بحثية بحاجة إلى معرفة نمط حياة مجتمع ما، واتجاهاتهم، وهو ما تطرق له استشاري في وزارة النقل والاتصالات وتقنية المعلومات (G3-6) إلى حاجة بعض المؤسسات البحثية والتجارية لمعرفة اتجاهات الأفراد واهتماماتهم، ويتم ذلك من خلال شراء تلك البيانات عن طريق شبكات التواصل الاجتماعي، في ظل عدم وجود قانون يمنعها من بيع أو شراء بيانات المستخدمين. وعند تحليل النتاج الفكري نجد أن نتائج الدراسة الحالية متوافقة مع نتائج دراسات: Ikram and Kepli (٢٠١٨) و Van Otterlo (٢٠١٤) و Lachman (٢٠١٣) في استغلال شبكات التواصل الاجتماعي لتقنيات الذكاء الاصطناعي في تحليل احتياجات وتوجهات المستخدمين، والتنبؤ بتطلعاتهم المستقبلية، وتنظيم عملية جمع وتحليل البيانات. ومن جهة أخرى أصبحت تثير الكثير من المخاوف المتعلقة بخصوصية البيانات. لذلك اقترحت دراسة Horvitz and Mulligan (٢٠١٥) الإسراع في وضع أطر وضوابط حول طرق جمع البيانات وتحليلها، وضرورة مراقبة تقنيات الذكاء الاصطناعي لتوفير الحماية المطلقة لخصوصية المستخدمين في شبكات التواصل الاجتماعي. وهو ما أكدته دراسة onik et al.(٢٠١٩) التي كشفت عن دور الذكاء الاصطناعي في تسريب كم هائل من المعلومات الشخصية، ومعالجة الصور، وسبب ذلك عدم وجود معيار للخصوصية، بالإضافة إلى أن عملية جمع البيانات تتم دون طلب موافقة المستخدم.

إن توافق هذه النتائج في مجملها مع نتائج الدراسات السابقة يعد إشارة واضحة لانتهاك خصوصية المستخدمين من قبل شبكات التواصل الاجتماعي التي تعتمد اعتماد كلي على تطبيقات الذكاء الاصطناعي. وعند تحليل النتاج الفكري ومتابعة الأحداث اليومية في المجالات المختلفة كالأخبار التقنية، تظهر كثير من القضايا ذات العلاقة باستخدام تلك التطبيقات الذكية؛ ولعل أبرزها قضية Facebook، فلقد تطرق أفراد عينة الدراسة عن استغلال شركة Facebook لبيانات مستخدميها، وبيعها إلى أطراف أخرى.

وقد يعزى استثمار القطاع الخاص لتطبيقات الذكاء الاصطناعي على شبكات التواصل الاجتماعي لعدد من الأسباب؛ منها قدرة تلك التقنيات على تحليل البيانات ومعالجتها، لأغراض تجارية أو سياسية تعود بالنفع عليها، كما أن استغلال تطبيقات الذكاء الاصطناعي في استخدام المقاييس الحيوية في مواقع متعددة للكشف عن البيانات المتعلقة بالموقع نفسه، وتعدُّ انتهاكًا واضحًا لخصوصية المستخدمين وأمنهم.

تطبيقات الذكاء الاصطناعي على البرمجيات مفتوحة المصدر

تمكنت المؤسسات التي تستخدم في عملها البرمجيات مفتوحة المصدر تحقيق أقصى استفادة من تقنيات الذكاء الاصطناعي من خلال رفع عدد المستخدمين وزيادة استقطابهم، وتحسين جودة الخدمات المقدمة، ورفع كفاءة العمليات التحليلية. من جانب آخر استغلت تلك المؤسسات تقنيات الذكاء الاصطناعي في انتهاك خصوصية المستخدمين سواء كان أفراد أو مؤسسات، وسرقة بياناتهم وبيعها لجهات أخرى لتحقيق أغراض ربحية أو سياسية. وهو ما أكده أغلب أفراد عينة الدراسة في مجموعات التركيز إلى استغلال البرمجيات مفتوحة المصدر للخوارزميات الذكية في جمع بيانات المستخدمين ومعالجتها وبيعها لجهات أخرى، الأمر الذي أدى إلى ظهور مجموعة من القضايا الأخلاقية التي تركت أثرًا سلبًيا في المجتمع. وأوضح مختص في تقنية المعلومات (G3-7) عن قيام شركة ما بشراء بيانات الأفراد من إحدى الشركات المختصة بتصنيع وبيع فرشاة الكترونية لتنظيف الأسنان، وذلك لمعرفة أوقات الذروة التي ترتفع حاجة الأفراد إلى التنقل.

في الشأن نفسه تطرق رئيس قسم بالمركز الوطني للإحصاء والمعلومات (G2-6) إلى انتشار البرمجيات الآلية (الروبوتات) المبنية على خوارزميات الذكاء الاصطناعي التي تقوم بالأعمال المنزلية، وتقوم بجمع بيانات المستخدم وإرسالها إلى خوادم خاصة، تتمثل تلك البيانات في تحديد عدد أفراد الأسرة، وموقع المنزل، وصور للأفراد وتحركاتهم، في ظل عدم إدراك المستخدمين خطورة تلك الأجهزة.

بسبب القضايا الأخلاقية الناجمة عن استخدام البرمجيات الآلية والذكية، قامت بعض الدول بحظر وإيقاف استخدام بعض الأنظمة الذكية، مثل: تقنية Facial Recognition، إذ تم حظر استخدامها في الأماكن العامة في بعض مدن أمريكا، لتقليل الآثار الأخلاقية الناجمة عن تلك التقنية (G3-6).

لقد أكد الطرح السابق ما تناولته أفراد عينة مجموعات التركيز مستشهدين بالأخبار العالمية التي كشفت القضايا الأخلاقية الناتجة عن استخدام البرمجيات مفتوحة المصدر. وهو ما أشارت إليه دراسة Brubaker (٢٠١٨) عن قيام شركة Amazon و Google باستغلال خوارزميات الذكاء الاصطناعي في جمع البيانات وتحليلها، بهدف بيعها وتحقيق عائد مادي في نهاية المطاف. وهذا ما أكدته دراسة Wasilow and Thorpe (٢٠١٩) في أن الهدف الأساسي لجمع بيانات المستخدمين وتحليلها هو التسويق وتحقيق أهداف أرباح عالية. وتوصلت دراسة تومي (٢٠١٧) إلى أن البيانات الشخصية أصبحت سلعة يتم استخدامها سياسيًا لدعم أحزاب معينة، وتجاريًا لإطلاق إعلانات تسويقية. أضافت دراسة Barton et al.(٢٠١٧) أن أنظمة الذكاء الاصطناعي تقوم بجمع بيانات المستخدمين بشكل مستمر، وتركز على جمع البيانات الشخصية والحساسة.

في الشأن نفسه أشار أفراد عينة الدراسة عن حظر تقنيات التعرف على الوجه في بعض المدن في الدول الكبرى، نتيجة قدرتها على نشر صور المستخدمين على الإنترنت، ومعالجتها، واستخدامها في الإعلانات الترويجية دون علم أصحابها. واتفقت هذه النتيجة مع نتائج دراسة Denton et al (٢٠١٨). التي توصلت إلى قدرة تقنيات الذكاء الاصطناعي على تحليل صور الوجه ومعالجتها، والتسجيلات الصوتية بغرض المراقبة والتجسس. وهذا ما أكدته دراسة Power (٢٠١٦) إلى إمكانية تقنيات الذكاء الاصطناعي على مراقبة (٢٠) مليون شخص بشكل مرئي أو صوتي في الوقت نفسه. وأضافت دراسة Manheim and Kaplan (٢٠١٨) عن قيام الحكومة الفيدرالية بمراقبة الأفراد بشكل قانوني أو غير قانوني باستخدام البرمجيات مفتوحة المصدر.

٢. تحديات ومخاطر استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية

أشار أفراد عينة الدراسة إلى مجموعة من التحديات والمخاطر التي تواجه الأفراد والمؤسسات نتيجة استخدامهم لتقنيات الذكاء الاصطناعي في مختلف القطاعات، وتتمثل تلك التحديات والمخاطر في معالجة البيانات لأغراض الابتزاز الإلكتروني، وسرقة البيانات الحكومية وتعطيل الأنظمة.

معالجة البيانات لأغراض الابتزاز الإلكتروني

استطاعت مجموعة من الشركات والأفراد في استغلال تقنيات الذكاء الاصطناعي عن طريق استخدام البرمجيات مفتوحة المصدر، أو شبكات التواصل الاجتماعي في ابتزاز وتهديد أفراد المجتمع من خلال جمع البيانات ومعالجتها، والتجسس، والتنصت. وتتم عملية الابتزاز من خلال إجبار الضحايا على القيام بأفعال سيئة تلحق الضرر به وبالمجتمع، أو دفع مبلغ مالي. وقد أشار جميع أفراد عينة الدراسة أن تطبيقات الذكاء الاصطناعي قد تستخدم في أغراض الابتزاز الالكتروني على مستوى الأفراد والمؤسسات في العالم أجمع، وفيما يتعلق بسلطنة عمان لم يسبق لأي مؤسسة تعرضها لعمليات ابتزاز كان سببها تقنيات الذكاء الاصطناعي، ولكن في المقابل تعرضت لحالات تصيد الضحايا عن طريق الهندسة الاجتماعية من خلال البريد الإلكتروني باستخدام الطرق التقليدية كإرسال روابط مشبوهة، يستطيع من خلالها المهندس الاجتماعي الوصول إلى البيانات بمجرد النقر عليها ثم تبدأ عمليات الابتزاز.

وهذا دليل واضح على قوة التطبيقات المستخدمة في السلطنة نتيجة كفاءة المعايير والأسس التي وضعت عند اختيارها، إذ شهدت السلطنة حسب ما أشار إليه موقع وزارة النقل والاتصالات وتقنية المعلومات (٢٠٢٠) منذ عام ٢٠١١م، حتى عام ٢٠١٦م، حوالي (٢٦٩) حالة ابتزاز الإلكتروني. و(١٦١) حالة

ابتزاز في عام ٢٠١٦م، وهو مؤشر واضح عن وعي الأفراد بآلية التبليغ عن الابتزاز الإلكتروني. في الإطار نفسه أشارت دراسة تومي (٢٠١٧)، ودراسة مصطفى (٢٠١٦) أن تقنيات الذكاء الاصطناعي تمتلك برمجيات خاصة للتتبع، والتنصت، والتجسس. وأكدت دراسة Power (٢٠١٦) قدرة تقنيات الذكاء الاصطناعي على مراقبة عدد كبير من الأفراد في وقت واحد يصل إلى (٢٠) مليون شخص وأكثر، وتتم مراقبتهم بشكل مرئي، أو صوتي، ثم ابتزازهم بشكل مباشر.

أشار أفراد عينة الدراسة أن خوارزميات الذكاء الاصطناعي سهلت عمليات الابتزاز التي يقوم بها المهندس الاجتماعي، من خلال إجراء تعديلات على الصور أو مقاطع الفيديو، وابتزاز الأفراد بها، بالإضافة إلى بناء سيناريو أكثر تعقيدًا باستخدام تقنيات الذكاء الاصطناعي، واتفقوا على أن مخاوف الهندسة الاجتماعية تتمثل في استخدام المقياس الحيوي بهدف الاستدراج والابتزاز الإلكتروني. وفي هذا الشأن أشار رئيس قسم في المركز الوطني للإحصاء والمعلومات (G2-6) أن عمليات الابتزاز في ظل انتشار تقنيات الذكاء الاصطناعي تتصف بالتعقيد، نتيجة صعوبة معرفة ماهية الطرف الذي قام بالابتزاز؛ هل هو فرد أم آلة؟ وذلك لقدرة الآلة على محاكاة البشر، وهو ما شكل صعوبة على المؤسسات الأمنية في التعامل مع هذه القضايا. وأشار مختص في وزارة النقل والاتصالات وتقنية المعلومات (G3-5) إلى ظهور مجموعة من المهندسين الاجتماعيين الذين قاموا بإجراء حظر للشركات التقنية المطورة للحد من إمكانيتها في الوصول إلى التقنيات، مما تتيح لهم الفرصة في الوصول إلى التقنيات الذكية والتلاعب فيها لخدمة مآربهم التي يسعون إليها. وهذه النتائج تتوافق مع ما توصلت إليه دراسة Raban and Hauptman (٢٠١٨) التي أشارت عن قيام المهندسين الاجتماعيين بمحاكاة الأصوات، ومقاطع الفيديو، والصور، بالاعتماد على تقنيات الذكاء الاصطناعي، الأمر الذي أدى إلى تسهيل عمليات الابتزاز. وفي الجانب نفسه أشارت دراسة Lauterbach (٢٠١٩) إلى قدرة الذكاء الاصطناعي على إعادة تصنيع الصور، ومعالجة البيانات لخداع الشبكات والأجهزة الأخرى، ونتج عن ذلك ارتفاع نسبة استخدام المهندسين الاجتماعيين لها لتسهيل جرائمهم الإلكترونية وأهمها الابتزاز.

يحدث الابتزاز الإلكتروني نتيجة تعزيز عمليات التنصت والتجسس، ومعالجة الصور أو مقاطع الفيديو في شبكات التواصل الاجتماعي أو البرمجيات مفتوحة المصدر، وتتمكن تقنيات الذكاء الاصطناعي من محاكاة الأصوات والصور لابتزاز الضحية مقابل دفع مبلغ مالي أو القيام بأفعال سيئة، وهو ما تطرق له استشاري في وزارة النقل والاتصالات وتقنية المعلومات (G3-6) أنه يتم استخدام تقنيات تحليل الصور Image Analysis، وتقنيات معالجة الصور Image Processing في إجراء تعديلات باستخدام تقنيات الذكاء الاصطناعي وابتزاز الأفراد. وهو ما أشارت إليه دراسة محرم (٢٠٢٢) إلى أن قدرة تقنيات الذكاء الاصطناعي لا تقف عند تزييف الصور ومقاطع الفيديو وإنما تستطيع توليد أصوات مطابقة للشخص المستهدف لغرض ابتزازه أو تشويه سمعته أو لأغراض أخرى مثلما حدث مع الرئيس الأوكراني خلال فترة غزو روسيا لأوكرانيا، إذ ظهر مقطع مرئي مفبرك لرئيس أوكرانيا يدعو فيه الجنود والشعب إلى الاستسلام أمام القوات الروسية، ثم تبين لاحقًا أن المقطع تمت معالجته وهو خالي من الصحة. واتفقت معها دراسة جيلالي وكوثر (٢٠٢٢) وأضافت أنه في عام ٢٠١٨ قام بعض الأشخاص باستخدام تقنيات الذكاء الاصطناعي في تزييف الأصوات ومقاطع الفيديو بنشر فيديو للرئيس الأمريكي السابق باراك أوباما وهو يتحدث عن موضوع Deepfake، وفي عام ٢٠١٩ تم نشر مقطع فيديو آخر مزيف للرئيس الأمريكي دونالد ترامب لأغراض سياسية وأمنية. وأضافت دراسة King, Aggarwal, Taddeo, and Floridi (٢٠٢٠) إلى وجود مجموعة من البرامج التي تساعد تقنيات الذكاء الاصطناعي في تركيب الصوت مثل: Adobe's voice editing and generation software، وهو ما يساعد في تزوير الهوية والقدرة على استخدام الحسابات البنكية من خلال التحدث مع موظفي البنك أو فتح الأبواب، والخزائن، والمركبات التي تتطلب صوت العميل.

سرقة البيانات الحكومية وتعطيل الأنظمة

استطاعت تقنيات الذكاء الاصطناعي في الولوج إلى الأنظمة الحكومية واختراق المواقع الحكومية والعسكرية بغرض الوصول إلى بيانات سرية ومعلومات حساسة، أو بقصد العبث والتخريب بمحتوياتها، بالإضافة إلى إلحاق الضرر بالأفراد والمؤسسات، والمس بالأمن الوطني والدولي، وهو ما أشارت إليه دراسة Manheim and Kaplan (٢٠١٨) عن قيام خوارزميات الذكاء الاصطناعي بالتلاعب بنتائج تصويت الناخبين من خلال اختراق أنظمة التصويت وسرقة المعلومات الانتخابية، بالإضافة إلى استخدام تقنيات الذكاء الاصطناعي في الدخول إلى البوابات الإلكترونية للمؤسسات الحكومية باستخدام أسماء وهمية أو أسماء أشخاص حقيقيين، وتقديم بلاغات غير صحيحة، والدخول إلى المواقع الإلكترونية الحكومية، وسحب البيانات منها. وأضافت دراسة إدلبي (٢٠٢٣) أن بعض الجرائم الناجمة عن تقنيات الذكاء الاصطناعي سببها قيام بعض المصنعين، أو المالكين، أو المبرمجين بالتعمد في إدخال بيانات غير صحيحة أو استخدام برمجة معينة من أجل اختراق المواقع الحكومية، وإلحاق الضرر بها، والوصول إلى بيانات حساسة تهدد الأمن الوطني.

اتفق أفراد العينة أن المهندسين الاجتماعيين استفادوا من تقنيات الذكاء الاصطناعي في اختراق وتعطيل المواقع الحكومية لتحقيق أهداف مادية، أو سياسية، أو إثارة الرأي العام. وهو ما تطرق له مساعد المدعي العام (G1-3)، إلى حجم الآثار السلبية الناجمة عن جرائم انتهاك البيانات الشخصية والحكومية بعيدة المدى. ويؤكد محامٍ مختص بالجرائم التقنية (I2-4) أن تقنيات الذكاء الاصطناعي تستخدم في الخير والشر، إذ تمكنت من اختراق مواقع حكومية وعسكرية بهدف الاستحواذ على معلومات سرية، وبيانات خاصة بالدولة أو بهدف العبث بمحتويات الأنظمة. وجاءت دراسة مقلد (٢٠١٨) مؤكدة على ذلك، وتوصلت إلى أن تطور ونمو تقنيات الذكاء الاصطناعي ينعكس ايجابًا على التطور التلقائي لسرقة البيانات الحكومية، مما يشكل خطراً على خصوصية الأفراد والمؤسسات. ومن ثمّ فإن نتائج الدراسة الحالية مع المختصين في المجال تؤكد أن أنظمة الذكاء الاصطناعي أصبحت قادرة على الدخول في الشبكات، وسرقة البيانات، ونشر فيروسات ذكية، ومهاجمة أنظمة المؤسسات وتعطيلها كما ذكر Raban and Hauptman (٢٠١٨) في دراسته، وشاركه في الوقت نفسه Wasilow and Thorpe (٢٠١٩) إلى استخدام Edward Snowden لبرنامج زاحف بهدف جمع (٢٠٠٠٠٠) وثيقة سرية تقريباً، من خوادم وكالة الأمن القومي الأمريكية. وأضافت دراسة Manheim and Kaplan (٢٠١٨) عن استخدم الذكاء الاصطناعي في إضعاف المؤسسات الديمقراطية وتقليص حريتها، وتعطيل الانتخابات الديمقراطية، واختراق أنظمة التصويت من قبل جهات مجهولة المصدر.

ومما سبق يتضح أنه بالرغم من الدور الكبير الذي تلعبه تقنيات الذكاء الاصطناعي في تبسيط الخدمات وفعاليتها، إلا أنها شكلت خطورة في عمل المؤسسات بكافة أنواعها المدنية والاعتبارية على مستوى العالم، إذ لم تقتصر الانتهاكات على دولة معينة أو مؤسسة محددة، وإنما شملت كافة المؤسسات. ونظرًا لحساسية البيانات وسريتها لاسيما في أنظمة المؤسسات الأمنية والمصرفية التي بالإمكان الوصول إليها عن طريق الخوارزميات الذكية أو المهندسين الاجتماعيين فإن ذلك سيشكل خطرا واسعا ومتشعبا على الحكومات، الأمر الذي يتسبب في خسائر مادية طائلة، ويؤثر سلبًا على مواصلة العمل.

أشارت جريدة الرؤية إلى جهود وزارة النقل والاتصالات وتقنية المعلومات في صد ما يزيد عن (٨٣٤) مليون هجمة إلكترونية، منها (٧٢) مليون هجمة على المؤسسات الحكومية. ويتضح من ذلك كله حرص المؤسسات في السلطنة على تجنب استخدام التطبيقات مفتوحة المصدر خاصة في المؤسسات الأمنية والمؤسسات التي تتعامل مع البيانات ذات التصنيف السري، وذلك لعدم اتاحة الفرصة لأطراف خارجيين كالمهندسين الاجتماعيين من اختراق الأنظمة وسرقة البيانات.

الخاتمة

توصلت الدراسة إلى مجموعة من النتائج التي يمكن تلخيصها فيما يلي:

- تعتمد بعض المؤسسات والشركات على تقنيات الذكاء الاصطناعي، ضمن مواقع الشبكات الاجتماعية والبرمجيات مفتوحة المصدر في اختراق البيانات وسرقتها، والتعدي على خصوصية المستخدمين من خلال بيعها لأطراف أخرى، لتحقيق ربح مادي أو أهداف سياسية، الأمر الذي نتج عنه انتشار مجموعة من القضايا الأخلاقية التي تركت تأثيرا سلبيا على الفرد والمجتمع كافة.
- أوضحت النتائج قدرة تقنيات الذكاء الاصطناعي التي تستخدم ضمن البرمجيات مفتوحة المصدر، أو شبكات التواصل الاجتماعي في ارتكاب جرائم معلوماتية كالابتزاز الإلكتروني، وسرقة البيانات الحكومية، وتعطيل الأنظمة، كما يمكن تطويعها من قبل ما يطلق عليهم المهندسين الاجتماعيين لارتكاب الجرائم الإلكترونية بطرق أكثر تقدمًا.
- شكّلت تقنيات الذكاء الاصطناعي خطورة بالغة على المؤسسات الأمنية، والمصرفية، والمدنية، والعسكرية في العالم أجمع، نظرًا لإمكانية الخوارزميات الذكية أو المهندسين الاجتماعيين في اختراق أنظمتها والوصول الى البيانات الحساسة أو البيانات ذات التصنيف السري، مما أثّر سلبًا في مواصلة العمل وتقديم الخدمات، والتسبب في خسائر مادية طائلة.

بناءً على النتائج التي توصلت إليها الدراسة، يقدم الباحثون مجموعة من التوصيات؛ تمثلت في التالي:

- ضرورة العمل على وضع مجموعة من التدابير التقنية، والتشريعية، والتنظيمية لحماية البيانات والحد من انتهاك خصوصية الأفراد والمؤسسات، من خلال تحديث قانون مكافحة جرائم تقنية المعلومات بما يتناسب مع التطورات التكنولوجية الحديثة.
- ضرورة تصميم برنامج للعاملين في المؤسسات لتعزيز ورفع مستوى الوعي التقني، التشريعي، والتنظيمي في التعامل مع التقنيات الحديثة والمتطورة.
- تعزيز التعاون بين المؤسسات في السلطنة لإطلاق مجموعة من حملات التوعية لأفراد المجتمع حول آلية حماية بياناتهم، وعدم مشاركتها مع أطراف أخرى.

المراجع

أبوبكر، خوالد (٢٠١٧). تطبيقات الذكاء الاصطناعي في خدمة المصارف العربية. مجلة الدراسات المالية والمصرفية: الاكاديمية العربية للعلوم المالية والمصرفية - مركز البحوث المالية

والمصرفية، ٢٥(٢)، ٥٧-٦٠. http://search.mandumah.com/Record/826190

أبو منصور، حسين (٢٠٢١). الذكاء الاصطناعي وأبعاده الأمنية. أوراق السياسات الأمنية، جامعة نايف العربية للعلوم الأمنية، ٢(١)، ١-١٨. https://doi.org/10.26735/SKHN3682

إدلبي، عمر محمد منيب (٢٠٢٣). المسؤولية الجنائية الناتجة عن أعمال الذكاء الاصطناعي (Master's thesis). جامعة قطر، المستودع الرقمي Q Space. تم الاسترداد من https://qspace.qu.edu.qa/handle/10576/40641?locale-attribute=ar

تومي، فضيلة (٢٠١٧). إيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق. مجلة العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح – ورقلة، (٣٠)، ٤١-٥٠.

جيلالي، ماينو؛ كوثر، عروس (٢٠٢٢). الجريمة السيبرانية في صورها المستحدثة. مجلة القانون والتنمية، ٤(١)، ٥٠-٦٧.

حسن، محمد جبريل إبراهيم (٢٠٢٢). المسئولية الجنائية الناشئة عن مضار استخدام الذكاء الاصطناعي في المجال الطبي دراسة تحليلية، مجلة الدراسات القانونية والاقتصادية، (٨)، ١-٦٤.

شاهين، أحمد إبراهيم (٢٠١١). خصوصية المعلومات وسريتها بمواقع الحكومات الإلكترونية العربية: دراسة مقارنة. الاتجاهات الحديثة في المكتبات والمعلومات. مصر، المكتبة الأكاديمية، ١٦ (٣٥)، ٨٩-١٤٠.

عبد المؤمن، علي معمر (٢٠٠٨). البحث في العلوم الاجتماعية: الأساسيات والتقنيات والأساليب. ليبيا: منشورات جامعة ٧ أكتوبر.

عمر، هيثم عبد اللطيف (٢٠٠٦). تطبيقات الذكاء الاصطناعي الحالية، مجلة كلية الرافدين الجامعة للعلوم، (١٨)، ٣١ – ٤١.

قده، حمزة؛ كحيط، إيمان (٢٠٢٢). توظيف تطبيقات الذكاء الاصطناعي في مواجهة الجريمة الالكترونية. المؤتمر العلمي الدولي الثالث حول: التكنولوجيا الرقمية من التأصيل الى الابتكار- مؤسسات التعليم العالي ومستقبل سوق العمل العربي، جامعة أم القيوين.

مراد، بن عودة حسكر (٢٠٢٢). إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي. مجلة الحقوق والعلوم الانسانية، ١٥(١)، ١٨٧-٢٠٥.

محرم، أحمد مصطفى (٢٠٢٢). استخدامات الذّكاء الاصطناعي (AI) استخدام تقنية التزييف العميق (Deepfake)) في قذف الغير نموذجًا دراسة فقهية مقارنة معاصرة. مجلة البحوث الفقهية والقانونية، ٣٩(٣٩)، ٢٤٩١-٢٥٨٩.

مصطفى، عائشة بن قارة (٢٠١٦). الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية. مجلة الندوة للدراسات القانونية: قارة وليد، (١٣)، ٧٤-٩٠.

مقلد، أشرف عمر وهبة (٢٠١٨). مخاطر التقنيات الحديثة وبرمجيات إدارة الوثائق على خصوصية الأفراد والهيئات. Cybrarians Journal: البوابة العربية للمكتبات والمعلومات، (٥٠)، ١-٥٢.

الملا، إبراهيم حسن عبد الرحيم (٢٠١٧). الذكاء الاصطناعي والجريمة الإلكترونية، مجلة الأمن والقانون: أكاديمية شرطة دبي، ٢٦(١)، ١١٤-١٧٧.

وزارة التقنية والاتصالات (٢٠٢٠). شاركونا أفكاركم للقضاء على الابتزاز الإلكتروني في بلادنا. www.ita.gov.om

المراجع الأجنبية

Atkinson, R. D. (2018). "It is going to kill us!" and other myths about the future of artificial intelligence. IUP Journal of Computer Sciences, 56-7 ,(4)12. https://search.proquest.com/docview/2159117153?accountid=27575.

Baranov, P. P., Mamychev, A. Y., Plotnikov, A. A., Voronov, D. Y., & Voronova, E. M. (2019). Problems of legal regulation of robotics and artificial intelligence in russia: Some approaches to the solution. Dilemas Contemporáneos : Educación, Política y Valore, I https://search.proquest.com/docview/2245652841?accountid=27575.

Barton, D., Woetzel, J., Seong, J., & Tian, Q. (2017). Artificial intelligence: implications for China.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 101-77 ,(2)3. Doi: 1478088706/10.1191qp063oa.

Brubaker, K. (2018). Artificial Intelligence: Issues of Consumer Privacy, Industry Risks, and Ethical Concerns (Doctoral dissertation, Utica College).

Dahlan, H. A. (2018). Future interaction between man and robots from Islamic perspective. International Journal of Islamic Thought, 51-44 ,13. doi: http://dx.doi.org/10.24035/ijit.13.2018.005.

Denton, S., Pauwels, E., He, Y., & Johnson, W. (2018). Nowhere to Hide: Artificial intelligence and privacy in the fourth Industrial Revolution. https://www.researchgate.net/publication/324451812_Nowhere_to_Hide_Artificial_Intelligence_and_Privacy_in_the_Fourth_Industrial_Revolution.

Kuhn, M. L. (147 .(2018 million social security numbers for sale: Developing data protection legislation after mass cybersecurity breaches. Iowa Law Review, ,(1)104 445-417. Retrieved from https://search.proquest.com/docview/2188134315?accountid=27575.

Kumar, K. N., & Balaramachandran, P. R. (2018). ROBOTIC PROCESS AUTOMATION - A STUDY OF THE IMPACT ON CUSTOMER EXPERIENCE IN RETAIL BANKING INDUSTRY. Journal of Internet Banking and Commerce, 27-1 ,(3)23. Retrieved from https://search.proquest.com/docview/2216876148?accountid=27575.

Kumar, P., & Kumar, R. (2016). Cyber security's significance in health information technology (HIT). International Journal of Advanced Studies in Computers, Science and Engineering, 14-8 ,(2)5. Retrieved from https://search.proquest.com/docview/1776319407?accountid=27575

Kumar, R. (2010). Research methodology: A step-by-step guide for beginners. Sage Publications Limited

Lachman, V. D. (2013). Social media: managing the ethical issues. Medsurg Nursing, .330-326 ,(5)22

Lauterbach, A. (2019). Artificial intelligence and policy: Quo vadis? Digital Policy, Regulation and Governance, 263-238 ,(3)21.

doi:http://dx.doi.org/10.1108/DPRG0054-2018-09-.

Lin, P., & Hazelbaker, T. (2019). Meeting the challenge of artificial intelligence: what CPAs need to know: Certified public accountant. The CPA Journal, ,(6)89 52-48. Retrieved from https://search.proquest.com/docview/2239578361?accountid=27575

LÓPEZ, M., PEDRAZA, J., CARBÓ, J., & MOLINA, J. M. (2014). The awareness of privacy issues in ambient intelligence. ADCAIJ : Advances in Distributed Computing and Artificial Intelligence Journal, 84-71 ,(2)3. doi: http://dx.doi.org/10.14201/ADCAIJ2014327184.

Manheim, K. M., & Kaplan, L. (2018). Artificial Intelligence: Risks to Privacy and Democracy

Onik, M. M. H., Chul-Soo, K. I. M., & Jinhong, Y. A. N. G. (2019, February). Personal data privacy challenges of the fourth industrial revolution. In 21 2019st International Conference on Advanced Communication Technology (ICACT) (pp. 638-635). IEEE

Dhshan, Y. I. (2020). Criminal Liability for Artificial Intelligence Crimes. YDhshan.

Dickson, B. (2017). Artificial Intelligence creates new job opportunities. PC Magazine, .122-114 ,(6)9

Elhai, J. D., Levine, J. C., & Hall, B. J. (2017). Anxiety about electronic data hacking. Internet Research, 649-631 ,(3)27.

doi: http://dx.doi.org/10.1108/IntR0070-2016-03-.

Ezeji, C. L., & Olutola, A. A. (2018). The use of intelligence-led policing in combating technology-based crimes in south africa. Journal of African Foreign Affairs, 188-167 ,(2)5.

doi: http://dx.doi.org/2018/5658-2056/10.31920/v5n2a9.

FERREIRA, M., & KAWAKAMI, C. (2018). Ransomware - kidnapping personal data for ransom and the information as hostage. ADCAIJ : Advances in Distributed Computing and Artificial Intelligence Journal, 5 ,(3)7. doi:http://dx.doi.org/10.14201/ADCAIJ201873514.

Gupta, B. M., & Dhawan, S. M. (2018). Artificial Intelligence Research in India: A Scientometric Assessment of Publications Output during 16-2007. DESIDOC Journal of Library & Information Technology, 422-416 ,(6)38. Retrieved from Doi: http://dx.doi.org/10.14429/djlit.38.6.12309.

Horvitz, E., & Mulligan, D. (2015). Data, privacy, and the greater good. Science, 255-253 ,(6245)349.

Ikram, N. A. H. S., & Kepli, M. Y. Z. (2018). Establishing Legal Rights and Liabilities for Artificial Intelligence. IIUM Law Journal, ,(1)26 161. Retrieved from https://search.proquest.com/docview/2164441551?accountid=27575.

Katzan, H.,Jr. (2011). Ontology of trusted identity in cyberspace. Journal of Service Science, ,(1)4 11-1. Retrieved from https://search.proquest.com/docview/868857882?accountid=27575.

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. Science and engineering ethics, 120-89 ,26.

Sundaram, J. K., & Omar, R. (2019, Jan 29). Ethics for artificial intelligence.Inter Press Service. Retrieved from https://search.proquest.com/docview/2172301573?accountid=27575.

Van Otterlo, M. (2014). Automated experimentation in walden 3.0: The next step in profiling, predicting, control and surveillance. Surveillance & Society, 272-255 ,(2)12. doi:http://dx.doi.org/10.24908/ss.v12i2.4600.

Walden, G. R. (2006). Focus group interviewing in the library literature: A selective annotated bibliography 2005-1996. Reference services review, .241-222 ,(2)34

Wasilow, S., & Thorpe, J. B. (2019). Artificial intelligence, robotics, ethics, and the military: A canadian perspective. AI Magazine, 48-37 ,(1)40. Retrieved from https://search.proquest.com/docview/2213786823?accountid=27575.

Yeoh, P. (2019). Artificial intelligence: accelerator or panacea for financial crime?. Journal of Financial Crime, 646-634 ,(2)26.

Peters, K. (21 .(2019st century crime: How malicious artificial intelligence will impact homeland security. Homeland Security. Retrieved from Affairs, https://search.proquest.com/docview/2266265939?accountid=27575

Power, D. J. (2016). "Big brother" can watch us. Journal of Decision Systems, 588-578 ,25. doi:http://dx.doi.org/12460125.2016.1187420/10.1080.

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. Foresight : The Journal of Futures Studies, Strategic Thinking and Policy, 363-353 ,(4)20. doi:http://dx.doi.org/10.1108/FS0020-2018-02-.

Such, J. M., Espinosa, A., & García-Fornes, A. (2014). A survey of privacy in multi-agent systems. The Knowledge Engineering Review, 344-314 ,(3)29. doi:http://dx.doi.org/10.1017/S0269888913000180.