Jordanian Legislative Efforts in Artificial Intelligence and their Impact on Cybersecurity[#]

Ruba "Mohammed Saeed" Al-Ruwaiss [(1)*]

(1) Researcher, Mafraq - Jordan.

Received: 1/2/2026
Accepted: 10/5/2026
Published: 23/7/2026

* *Corresponding Author:*
-

DOI:
https://doi.org/10.59759/law.v5i2.2117

Abstract

Artificial intelligence has become an important part of our daily lives, strongly establishing itself in many scientific and practical fields, such as medicine, education, agriculture, engineering, commerce, industry, domestic services, and other fields. These fields have contributed to improving the quality of life and increasing its efficiency. For this reason, countries have sought to focus on it and make it a tangible reality, far from remaining a mere idea. It offers countless advantages that have aroused curiosity, as it has contributed to the development of scientific research, improved criminal investigations, and the implementation of many tasks with high efficiency, and with reduced costs and effort. In contrast, AI has had several negative consequences, including its replacement of human labor, which has undermined and limited human creativity. Furthermore, it has been used illegally, facilitating the spread of cybercrime using advanced methods that are beyond the ability of current legislation to keep pace with it. These negatives have also posed a significant challenge to national cybersecurity, which must be taken into account. The most important of these is the ability of legislation to adapt to the realities it imposes. The Hashemite Kingdom of Jordan has not been immune, as it has been quick to keep pace with this major technological development. The relevant authorities have continued to strengthen their legislative and security efforts to ensure the safe use of AI and mitigate its risks.

Keywords :Jordanian Legislation, Artificial Intelligence, Cybersecurity, Cybercrimes, Cybercrime Unit, Personal Data Protection, National Artificial Intelligence Strategy.

[#] A special issue for the Third International Conference, entitled: **Artificial Intelligence, A Legal Vision Towards a Sustainable Future**.

الجهود التشريعية الأردنية في الذكاء الاصطناعي واثرها على الامن السيبراني

ربا "محمد سعيد" الرويس[1]

(1) باحث، المفرق – الأردن.

ملخص

لقد أصبح الذكاء الاصطناعي جزءاً مهماً من حياتنا اليومية، حيث فرض نفسه بقوة في العديد من المجالات العلمية والعملية كالطب، والتعليم، والزراعة، والهندسة، والتجارة،، والصناعة، والخدمات المنزلية، وغيرها من المجالات، التي أسهمت في تحسين جودة الحياة و زيادة كفاءتها، و من أجل ذلك سعت الدول الى الاهتمام فيه، و جعله واقعاً ملموساً بعيداً عن بقائه مجرد فكرة، لتقديمه مميزات لا حصر لها اثارت الفضول، إذ أنه ساهم في **تطوير البحث العلمي، و تحسين التحقيقات الجنائية، و تنفيذ العديد من المهام بكفاءة عالية، و بتكاليف وجهد أقل.** [1]

وعلى النقيض من ذلك، فقد كان لذكاء الاصطناعي سلبيات عدة، و منها احلاله للعمل بدلًا من العنصر البشري، مما قيض فكرة الابداع البشري و حد منها، بالإضافة الى ارتفاع تكاليف صيانة البرامج و الآليات العاملة بالذكاء الاصطناعي، كما انه استخدم بطرق غير قانونية، ساعدت في انتشار الجرائم الإلكترونية بأساليب متقدمة فاقت قدرة التشريعات الحالية على مجاراتها، و غيرها الكثير من السلبيات، الأمر الذي شكل تحديًا كبيرًا للأمن السيبراني الوطني [2]، كان لا بد من اخذها بعين الاعتبار، ومن اهمها قدرة التشريعات على التكيف و الواقع الذي يفرضه عليها[3]، و لم تكن المملكة **الأردنية الهاشمية** بمنأى عن الدول، حيث سارعت إلى مواكبة هذا التطور

[1] يوسف كريستيان، (2019)، المسؤولية المدنية عن فعل الذكاء الاصطناعي، رسالة ماجستير منشورة، الجامعة اللبنانية، لبنان، ص8.

[2] ابراهيم، خالد، (2022)، التنظيم القانوني للذكاء الاصطناعي، دار الفكر الجامعي، الاسكندرية، مصر، ط1، ص49.

[3] الدحيات، عماد عبد الرحمن، (2020)، نحو تنظيم قانوني للذكاء الاصطناعي في حياتنا، اشكالية العلاقة بين البشر والآلة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد8، العدد5 ، ص16.

التكنولوجي الكبير، وواصلت الجهات المختصة تعزيز جهودها التشريعية و الأمنية، لضمان الاستخدام الآمن للذكاء الاصطناعي، و الحد من مخاطره.

الكلمات المفتاحية: التشريعات الأردنية، الذكاء الاصطناعي، الامن السيبراني، الجرائم الالكترونية، وحدة الجرائم الالكترونية، حماية البيانات الشخصية، الاستراتيجية الوطنية للذكاء الاصطناعي.

خطة البحث

المبحث الأول: التشريعات الأردنية المنظمة الذكاء الاصطناعي.

المطلب الأول: القوانين المتعلقة بالذكاء الاصطناعي في الأردن.

- الفرع الأول: قانون حماية البيانات الشخصية الأردني.
- الفرع الثاني: قانون الجرائم الالكترونية الأردني.

المطلب الثاني: الميثاق والاستراتيجية الوطنية للذكاء الاصطناعي في الأردن.

- الفرع الأول: الميثاق الوطني لأخلاقيات الذكاء الاصطناعي.
- الفرع الثاني: الاستراتيجية الأردنية للذكاء الاصطناعي(2023-2027) .

المبحث الثاني: الآليات المستحدثة لضبط استخدام الذكاء الاصطناعي وتأثيره على الأمن السيبراني.

المطلب الأول: دور وحدة الجرائم الإلكترونية في مكافحة الجرائم السيبرانية المقترفة بالذكاء الاصطناعي.

- الفرع الأول: المهام التي تقوم بها وحدة الجرائم الالكترونية.
- الفرع الثاني: انجازات وحدة الجرائم الالكترونية.

المطلب الثاني: دور المركز الوطني للأمن السيبراني في تعزيز الأمن الرقمي.

- الفرع الأول: الخدمات الرئيسية التي يقدمها المركز الوطني للأمن السيبراني الأردني للجهات الحكومية.
- الفرع الثاني: التشريعات الفاعلة في المركز الوطني للأمن السيبراني.

الخاتمة.

التوصيات.

قائمة المصادر والمراجع.

المقدمة.

أصبح الذكاء الاصطناعي أداة فاعلة في عالمنا المعاصر، فقد ظهرت أهميته التي لا يمكن تجاهلها في تطوير الأنظمة الرقمية، و تحليل كميات ضخمة من البيانات، و تعزيز الأمن على المستويين الوطني و الدولي، و مع تزايد تأثيره على جوانب اكثر حساسية، و خطورة كالأمن السيبراني، ارتبط المفهومين ببعضهما البعض، من خلال استخدام تطبيقات الذكاء الاصطناعي المؤثرة في الامن السيبراني، و قد واجه محللو الأمن السيبراني تحدياً في التحقق من جميع الأنشطة الممارسة على الانظمة، كمراقبة حركة المرور، و تحليل نشاط الخوادم بدقة، و تقييم المخاطر المحتملة لها، و اكتشاف التهديدات التي قد تنشأ بسببها، و توقع المستقبلي منها، و تقليل الوقت و التكاليف المتطلبة لذلك[1] .

ومن اجل ذلك بدت الحاجة الملحة للتدخل التشريعي، ليضع إطاراً قانونياً ينظم استخدام هذه التكنولوجيا، ويحد من المخاطر المحتملة، لضمان استخدامها بشكل مسؤول، يساهم في حماية البيانات المخزنة، ويعزز الأمن الرقمي الوطني.

ولإدراكنا مدى اهمية وتأثير الذكاء الاصطناعي على عصرنا الرقمي، وجب تسليط الضوء على التشريعات الأردنية الناظمة له، ودورها في بسط حدود لاستخدامه، من خلال تحليل النصوص، وبيان مدى نجاحها في توفير الحماية المطلوبة، لضمان توفير بيئة رقمية آمنة، ومن ثم التوصية بما يفيد تطوير تشريعات أكثر تكيفاً والواقع الحالي.

تبرز اشكالية الموضوع في قلة المصادر وقلة الدراسات الوطنية المتعلقة بالموضوع، على الرغم من ضرورة الاقدام على ذلك، لدراسة الواقع الذي نعيشه وبيان مدى توافق تشريعاتنا الحالية وكفايتها، في ظل التطورات المتزايدة في استخدام الذكاء الاصطناعي وتنوعها، وتأثيرها الكبير على الامن السيبراني.

بالإضافة الى القاء النظر على مدى توافق هذه التشريعات والمعايير الدولية، التي قد تصطدم معها في الكثير من الجرائم الالكترونية المرتكبة دولياً، والمؤثرة على أمنا السيبراني الوطني.

---

[1] حداوي ، أميرة هاتف، ومسلم، ضرغام علي، ومحمد، صفاء تايه، (2023)، القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات، دراسة تحليلة لآراء عينة من العاملين في المصارف الأهلية في النجف الأشرف، مجلة العلوم الإنسانية والطبيعية.

ولهذا فقد سعت هذه الدراسة الى تحليل ما أمكن من النصوص القانونية، والتطرق الى الميثاق واالاستراتيجية الوطنية بالذكاء الاصطناعي، وبيان مدى فعاليتها لمواجهة هذا الخطر عند استخدامه بطرق غير مشروعة، مع ابراز اهم التحديات التي قد تواجه المشرع في ذلك.

ومن اجل ذلك فقد تم تقسيم البحث الى مبحثين حسب الآتي:

- المبحث الأول: التشريعات الأردنية المنظمة الذكاء الاصطناعي.
- المبحث الثاني: الآليات المستحدثة لضبط استخدام الذكاء الاصطناعي وتأثيره على الأمن السيبراني.

الكلمات المفتاحية: التشريعات الأردنية، الذكاء الاصطناعي، الأمن السيبراني.

❖ المبحث الأول: التشريعات الأردنية المنظمة الذكاء الاصطناعي.

لقد كانت المملكة الأردنية الهاشمية من اوائل الدول التي تعاملت مع خدمة الانترنت حيث كان ذلك في عام(1994) [1]، ومع ازدياد استخدامه في شتى المجالات، سعت المملكة الى استحداث ما يعرف " بالحكومة الإلكترونية" التي هدفت الى تقديم الخدمات الى افراد مجتمعها بمختلف شرائحه، من خلال اتباع منهجية للتعامل مع الافراد متلقي الخدمة، لتتماشى والواقع الالكتروني [2]، كما نفذت العديد من المعاملات الحكومية من خلال التطبيقات الذكية والانظمة الرقمية، ومن ابرزها تطبيق " سند" الذي وفر العديد من المميزات والمعلومات للحصول على خدمات حكومية رقمية للوصول الى المعلومات اللازمة [3]، ولم يقتصر هذا التحول على الحكومة فقط، وانما ارتأى المشرع الأردني ايضًا الانصياع نحو التطور بتحديث قوانينه الوضعية، لتتلاءم والتغيرات التكنولوجية الحالية المتسارعة التي نواجهها، ولإدراكه ضرورة اصدار العديد من القوانين الرامية الى تنظيم المستجدات الالكترونية المرتكبة، ولإيمانه بحقيقة مفادها ان الذكاء الاصطناعي واقع فرض

[1] حيث تصدرت دولة تونس استخدام الانترنت عام 1991، تليها دولة الكويت عام 1992 ، ومن ثم مصر والامارات عام 1993، النوايسة، عبد الاله، جرائم تكنولوجيا المعلومات، شرح الاحكام الموضوعية في قانون الجرائم الالكترونية، دار وائل للنشر والتوزيع، ص74.

[2] موقع الاسكوا ، http://opengov.unescwa.org/ar/node/1196، تاريخ الزيارة 2025/3/27.

[3] http://sanad.gov.jo .

نفسه على عالمنا، ومنحه العديد من المميزات كالسرعة في الانجاز والاتقان والتقليل من الخطأ البشري [1]، كما منحت التشريعات للقاضي سلطة تقديرية في تحديد العقوبة ومقدارها، ونوع التدبير الاحترازي بحق من تمت ادانته [2]، وعلى الرغم من جميع هذه الجهود المتخذة الا ان مصطلح الذكاء الاصطناعي لم يدرج في القوانين المشرعة بشكل صريح، واكتفي بالإيماء له في القوانين كقانون الجرائم الالكترونية، وقانون حماية البيانات الشخصية وقوانين اخرى، و ترك الباب مفتوحاً لذلك، من خلال عدم تحديد طريقة ارتكاب الجريمة الالكترونية، و معاقبة الجرم مهما كانت الطريقة المستخدمة لارتكابه، فقد تكون مقترفة بواسطة الذكاء الاصطناعي، ولأجل ذلك، تم استدراك الامر، و اعتماد مصطلح الذكاء الاصطناعي و ذكره صراحةً في المواثيق والاستراتيجيات التي تم اعتمادها من قبل مجلس الوزراء الموقر، والتي سيتم دراستها لاحقاً في المطلب الثاني من هذا المبحث.

- **المطلب الأول: القوانين المتعلقة بالذكاء الاصطناعي في الأردن.**

لقد خلت القوانين الأردنية من ذكر لفظ الذكاء الاصطناعي صراحة كما أسلفنا، في حين عالجت في متنها العديد من الجرائم التي ارتكبت بشتى الطرق الالكترونية، وقد يكون الذكاء الاصطناعي واحدة منها، او غيرها من الطرق الالكترونية اخرى، وقد تكون جريمة سيبرانية، تؤثر على الامن الوطني السيبراني او الدولي، ومن بين اهم القوانين المستحدثة التي اصدرت، وأخرى الاقت تعديلات في الآونة الاخيرة، هي قانون حماية البيانات الشخصية رقم (24) لسنة2023، وقانون الجرائم الالكترونية رقم (17) لسنة 2023.

الفرع الأول: قانون حماية البيانات الشخصية:

سن المشرع الأردني قانون حماية البيانات الشخصية رقم (24) لسنة 2023، وألزمت جميع الجهات التي تتعامل بهذا النوع من البيانات بتوفيق اوضاعها وفقاً لأحكامه، خلال مدة لا تتجاوز

[1] إبراهيم، خالد (2022)، التنظيم القانوني للذكاء الاصطناعي، دار الفكر الجامعي، مصر، الاسكندرية، ط1، ص40.

[2] الوريكات، محمد عبد الله،2019، اصول علمي الاجرام والعقاب، دار وائل للنشر والتوزيع، عمان، الأردن، ص13 وما بعدها.

سنة تنتهي بتاريخ 2025/3/16.

أكد قانون حماية البيانات الشخصية الأردني على ماهية البيانات الشخصية الخاضعة لنصوصه، وعرفت البيانات التي يفرض القانون حمايته عليها، بأنها البيانات التي تم جمعها ومعالجتها[1]، وان كانت قبل نفاذ احكامه، واستثنى من ذلك البيانات الشخصية التي يعالجها الشخص نفسه لأغراضه الشخصية.[2]

وأكمل القانون آنف الذكر حمايته للبيانات الشخصية حين قيد حرية المتعامل بالبيانات المودعة بموافقة الشخص المعني بذلك[3]،او في الاحوال المصرح بها قانوناً[4]، مشترطاً شكلا معيناً لها[5]، مع قدرته على الاطلاع على البيانات لدى المسؤول عنها والحصول عليها، بالإضافة الى امكانية سحب الموافقة التي اقرها، او تعديل، او تصحيح، او تحديث البيانات الخاصة به، وتحديد نطاق المعالجة لها، او الاعتراض على المعالجة، او محو، او اخفاء البيانات، وغيرها من الصلاحيات.

الا ان قانون حماية البيانات الشخصية، قد استثنى حالات في متن المادة (6) منه، حيث اجاز من خلالها اجراء معالجة البيانات بشكل قانوني وبطريقة مشروعة، دون الحصول على موافقة مسبقة، او اعلام الشخص المعني، ومن اهمها المعالجة التي تقوم بها الجهات الحكومية، او الشركات التي تم التعاقد معها على ذلك، او لأغراض طبية، او حماية مصالح حيوية، او لمنع ارتكاب جريمة، او لكشفها، او ملاحقتها، او بناء على امر قضائي، او تشريع يسمح بذلك وغيرها

[1] رجب، هبة رمضان،2024 ، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، مجلة العلوم المالية والاقتصادية، جامعة عين شمس، مصر، ص419 وما بعدها.

[2] المادة (3) من قانون حماية البيانات الشخصي لسنة 2023.

[3] وإننا اذ نرى تقييد المشرع الموافقة بالشخص المعني (الشخص الطبيعي) كما ورد في نص المادة الرابعة من القانون، دون ذكر الشخص المعنوي، وهو مانعتبره سهوا للمشرع يستدعي التعديل، ليشمل الجميع، انظر ماورد: الراعي، أشرف ، 2025 ، الجرائم الالكترونية (الأحكام الموضوعية لجرائم تقنية المعلومات والذكاء الاصطناعي) ، البديل للنشر والتوزيع ، عمان ، الأردن ، ط1 ، ص 60 .

[4] نصت المادة (4) من قانون حماية البيانات الشخصية لسنة 2023.

[5] نص المادة (5) من ذات قانون حماية البيانات الشخصية لسنة 2023.

من الحالات الواردة في متن المادة [1].

وقد حدد قانون حماية البيانات الشخصية مفهوم المسؤول، حيث بين بأنه أي شخص طبيعي، أو اعتباري سواء أكان داخل المملكة أم خارجها تكون البيانات في عهدته[2].

ولم يكتف قانون حماية البيانات الشخصية الأردني بتعيين مسؤول عن البيانات فقط، بل بتعيين شخص طبيعي للإشراف على قواعد البيانات والمعالجة، وفقا لأحكام هذا القانون يسمى بالمراقب، وآخر مختصاً بمعالجة البيانات سواء اكان شخصاً طبيعياً ام اعتبارياً يسمى بالمعالج، وأوكل لكل منهم مجموعة من الالتزامات التي لا بد من مراعاتها في عملهما. [3]

الفرع الثاني " قانون الجرائم الالكترونية الأردني:

تطور **قانون الجرائم الإلكترونية في الأردن**، استجابة لتزايد التهديدات الناتجة عن الاستخدام الواسع للتكنولوجيا والإنترنت، حيث أدركت الحكومة الأردنية أهمية وجود إطار قانوني لمكافحة الجرائم التي تحدث في الفضاء الإلكتروني، والتي تؤثر على الأفراد والمؤسسات، والاقتصاد الوطني، وقد مر القانون في العديد من مراحل التطور، كان اخرها قانون الجرائم الالكترونية رقم (17) لسنة 2023، الذي حظي بخلاف واسع ما بين مؤيد ومعارض.

شهد القانون توسعًا في عدد مواده لتصل إلى (41) مادة، مقارنةً بقانون الجرائم الإلكترونية السابق، الذي كان يتضمن (18) مادة فقط، ويعد هذا تطورًا إيجابيًا، حيث أضاف القانون الجديد نصوصًا تجرم أشكالًا حديثة من الجرائم الإلكترونية، التي لم تكن مشمولة في القانون السابق.

وتوسع المشرع الأردني في إدراج تعريفات جديدة ضمن المادة الثانية منه، مع الحفاظ على التعريفات التي وردت في القانون السابق، وهو ما يحسب له، باعتبارها خطوة إيجابية لتحديث التشريعات بما يتناسب مع التطورات التقنية الحديثة، ومن بين هذه التعريفات المستحدثة تعريفه لكل من(تقنية المعلومات، خط سير بيانات الحركة، منصة التواصل الاجتماعي، العنوان

[1] نصت المادة (6) من قانون حماية البيانات الشخصية لسنة 2023.

[2] نص المادة (2) من قانون حماية البيانات الشخصية الأردني لسنة 2023.

[3] نص المواد (11) و(12) من قانون حماية البيانات الشخصية الأردني لسنة 2023..

البروتوكولي، مزود **الخدمة**، و**البنى التحتية الحرجة**).[1]

كما وسع القانون الجديد من دائرة التجريم، حيث عدل بعض احكامه للجرائم الواردة في القانون الذي سبقه، وشدد من مقدار العقوبة، في حين استحدث العديد من الجرائم الجديدة، التي جرم ارتكابها بشتى الطرق التكنولوجية، والتي يمكن ادراج الذكاء الاصطناعي كواحدة منها، وان لم يذكر ذلك صراحة.

كما بين قانون الجرائم الالكترونية كيفية التعامل مع الجرائم المرتكبة، ومن خلال الابلاغ عنها بعدة طرق، منها الابلاغ المباشر، او الاتصال الهاتفي، او عن طريق البريد الالكتروني (cyber.crimes@psd.gov.jo)، او **تقديم البلاغ عبر منصة الخدمات الإلكترونية**، او **التواصل عبر تطبيق الهواتف الذكية**، او **زيارة مراكز الشرطة المحلية، او التبليغ عبر وسائل التواصل الاجتماعي.**

وقد منحت الدعاوى الخاصة بهذه الجرائم صفة الاستعجال بالنظر والفصل.[2]

المطلب الثاني: الميثاق والاستراتيجية الوطنية للذكاء الاصطناعي.

سعى الأردن الى السير قدماً نحو التعامل مع الذكاء الاصطناعي لأهمية الدور الذي يلعبه في مجتمعنا، ولم يكتفي بتحديث قوانينه فحس، بل عززها من خلال مواثيق واستراتيجيات تتعلق بالذكاء الاصطناعي.

ولهذا كانت له رؤيته بما عرف "بخطة الأردن 2025 "، التي تهدف الى تحقيق التنمية المستدامة في المملكة الأردنية الهاشمية خلال العقد المقبل، مع التركيز على تعزيز الاقتصاد الوطني، وتحقيق التقدم في مختلف القطاعات الاجتماعية والاقتصادية، وقد تضمنت الخطة مجموعة من المبادرات، التي تهدف إلى تحسين جودة حياة المواطنين، ودعم التحول الرقمي والابتكار، كجزء أساسي من التنمية المستقبلية، من خلال تعزيز التحول الرقمي في مختلف القطاعات الحكومية والخاصة، مع استخدام تقنيات الذكاء الاصطناعي، وتطوير بنية تحتية رقمية قوية، لتحسين

[1] المادة (2) من قانون الجرائم الالكترونية الأردني لسنة 2023.

[2] المادة (34) من قانون الجرائم الالكترونية لسنة 2023.

الخدمات الحكومية، و زيادة كفاءة العمل .[1]

الفرع الأول: الميثاق الوطني للذكاء الاصطناعي:

ادركت الحكومة الأردنية الموقرة، بإيعاز من جلالة الملك عبد الله الثاني –حفظه الله – المخاوف الناجمة عن الحلول التكنولوجية المستندة الى الذكاء الاصطناعي، ومجموعة الاخطار التي تواجهها، ولهذا ارادت صياغة ميثاق وطني لأخلاقيات الذكاء الاصطناعي، يستند الى السياسة الأردنية للذكاء الاصطناعي، حيث ارادت من خلاله إطلاق مبادرات وطنية بالتعاون مع الجامعات، ومراكز البحث المتخصصة في الذكاء الاصطناعي، وبالتنسيق مع الجهات الحكومية والخاصة، ومنظمات المجتمع المدني، للاستفادة من التجارب، والممارسات الدولية الرائدة في هذا المجال.

كما شمل هذا الميثاق مجموعة من المبادئ والإرشادات، التي تركز على اتخاذ قرارات شفافة وعادلة، والعمل على تعزيز قابلية المساءلة للأنظمة المعتمدة على الذكاء الاصطناعي، مع ضمان حماية خصوصية البيانات وتجنب التحيز في معالجتها، وضمان تطبيق هذه المبادئ بشكل يحقق العدالة، والشفافية في جميع مراحل استخدام تقنيات الذكاء الاصطناعية، من خلال انشاء بيئة رقابية تضمن تقييم التطبيقات في المراحل التجريبية، وتقيم المخرجات بشكل مناسب من خلال استخدام بيئة **(الساندبوكس)**.[2]

الفرع الثاني: الإستراتيجية الوطنية للأمن السيبراني:

استكملت الحكومة الأردنية جهودها في تنظيم عملية التعامل بالذكاء الاصطناعي، من خلال اقرار مجلس الوزراء الموقر، وبالاستناد الى الميثاق الوطني لأخلاقيات الذكاء الاصطناعي آنف الذكر، الاستراتيجية الوطنية للذكاء الاصطناعي والخطة التنفيذية للفترة (2023–2027)، والتي تم تطويرها بالتعاون مع الاتحاد الاوروبي، ولجنة الامم المتحدة الاقتصادية والاجتماعية، ومنظمة الامم المتحدة للتنمية الاصطناعية، بالإضافة اعدادها من خلال التشاور مع الجهات المعنية من

[1] وزارة التخطيط والتعاون الدولي، كانون أول، (2021).

[2] هي آلية حماية، يقوم مبدأها على عزل البرامج التخريبية ومنع تأثيرها على بقية البرامج او اجزاء الكمبيوتر /صحيفة اليوم السابع، الأربعاء ،12 يوليو 2017.

القطاعات العامة، والخاصة، والأكاديمية، والأمنية، والمجتمع المدني.

وتضمنت الاستراتيجية رؤية واضحة تهدف إلى جعل الأردن من الدول الرائدة، والمنافسة في هذا المجال على مستوى الإقليم، من خلال إنشاء بيئة تشريعية وتكنولوجية وريادية، تشجع على الاستثمار في الذكاء الاصطناعي، واستثمار المنظومة الوطنية الداعمة، مثل الكوادر البشرية الأردنية المدربة، والبنية التحتية الرقمية، بهدف تعزيز الاقتصاد الوطني.

واشتملت على خمسة أهداف رئيسية تتماشى و سياسة الذكاء الاصطناعي، من خلال انشاء (68) مشروع، ولمدة خمس سنوات، وباستطلاع الاهداف الخمسة نرى ان الأهداف الأربعة الأولى، قد ركزت على تعزيز المنظومة الداعمة للذكاء الاصطناعي، من خلال تطوير القدرات الوطنية، وبناء المهارات والخبرات في هذا المجال، وتشجيع البحث العلمي والتطوير في الذكاء الاصطناعي، وتعزيز بيئة الاستثمار وريادة الأعمال فيه، بالإضافة إلى ضمان وجود بيئة تشريعية وتنظيمية، تساهم في الاستخدام الآمن لتقنيات الذكاء الاصطناعي، اما عن الهدف الخامس، فقد ركز على تطبيق أدوات الذكاء الاصطناعي، لتحسين كفاءة القطاع العام، والقطاعات ذات الأولوية.[1]

المبحث الثاني: الآليات المستحدثة لضبط استخدام الذكاء الاصطناعي وتأثيرها على الأمن السيبراني.

المطلب الأول: دور وحدة الجرائم الإلكترونية في مكافحة الجرائم السيبرانية المدعومة بالذكاء الاصطناعي.

لقد كان انشاء **وحدة الجرائم الإلكترونية** الانعكاس الأمثل لمجموعة التحديات المتزايدة، التي فرضتها التطورات التكنولوجية، واستخدام الإنترنت في مختلف جوانب الحياة، وارتفاع معدل ارتكاب الجرائم الالكترونية، واستجابة لاحتياجات ملحة في المجتمع، تتعلق بحماية بيانات الافراد والحكومات، والأمن الوطني، وضمان مواكبة التطورات التكنولوجية المتسارعة في هذا المجال، والرغبة بالوصول الى أمن رقمي.

انشئت وحدة الجرائم الالكترونية من قبل مديرية الأمن العام في إدارة البحث الجنائي عام (2008) قسم الجرائم الإلكترونية، وطورت عام 2015 باسم" وحدة مكافحة الجرائم الإلكترونية "، وفي العام

[1] موقع وزارة الاقتصاد الرقمي والريادة.

نفسه صدر قانون الجرائم الإلكترونية، وتم تعديله لأكثر من مرة، وكان آخرها صدور قانون الجرائم الإلكترونية رقم (17) لسنة 2023، ليواكب التطور الملحوظ في ارتكاب الجريمة الإلكترونية.

الفرع الأول: المهام التي تقوم بها وحدة الجرائم الإلكترونية:

لعبت وحدة الجرائم الالكترونية دورًا أساسيًا في التصدي للجرائم المرتبطة بالتكنولوجيا الحديثة والإنترنت، في ظل الارتفاع الملحوظ للجريمة الالكترونية خلال الاعوام السبعة الاخيرة، تضاعفت الاخيرة بما مقداره ستة اضعاف، وبلغت عدد القضايا المسجلة لدى وحدة الجرائم الالكترونية (2305) قضية في عام (2015)، فيما بلغت عدد القضايا المسجلة في عام 2022 (16027) قضية [1]، وهو ما القى على وحدة الجرائم الالكترونية مزيداً من المهام، لحماية الأفراد، والمؤسسات، والدولة من التهديدات الإلكترونية.

وفيما يلي أهم **المهام** التي تقوم بها الوحدة:

مكافحة الجرائم الإلكترونية :تولت الوحدة التحقيق في مختلف الجرائم الإلكترونية مثل القرصنة، الاحتيال الإلكتروني، سرقة البيانات، وغيرها، وعملت على جمع الأدلة الرقمية، وتحليلها لملاحقة المتورطين، وتقديمهم للعدالة.

- تأمين البيانات الحكومية والشخصية: **عملت الوحدة على تطوير وسائل الحماية والتشفير، لحماية البيانات الحساسة سواء كانت بيانات حكومية أو شخصية من الاختراقات والهجمات الإلكترونية، التي تستهدف أنظمة المعلومات.**
- التوعية والتثقيف: **ان كبح جماح الجرائم الإلكترونية لا ينحصر بمرحلة التنفيذ فحسب، بل يتطلب أيضًا جهودًا للتوعية والوقاية[2]، ولهذا كان من الضرورة إنشاء وحدة مختصة قادرة على نشر التوعية المجتمعية حول مخاطر الإنترنت، وكيفية تجنب الوقوع ضحية لهذه الجرائم.[3]**

كما تقوم الوحدة بتنفيذ حملات توعية للمجتمع حول مخاطر الإنترنت، وكيفية حماية أنفسهم من

[1] وكالة بوصلة للأنباء ، تقرير منشور يوم الاربعاء ، 16 اكتوبر /2024 .

[2] http://www.psd.gov.jo >ar-jo<

[3] www.almowaten.com .

الهجمات الإلكترونية، وتشمل هذه الحملات نصائح حول كيفية تأمين الحسابات الشخصية والبريد الإلكتروني، وتجنب الوقوع ضحية الاحتيال الإلكتروني.[1]

- **التحليل الرقمي:** تستخدم الوحدة تقنيات متقدمة لتحليل البيانات الرقمية، وتعقب النشاطات المشبوهة على الشبكات، ويتضمن ذلك تحليل البرامج الخبيثة، وفحص الأنظمة التي تم اختراقها، لتحديد مصدر الهجمات، وكيفية حدوثها.
- **رصد ومتابعة الأنشطة غير القانونية على الإنترنت:** تقوم الوحدة بمراقبة الإنترنت، بما في ذلك المواقع والشبكات الاجتماعية، لرصد أي نشاط مشبوه أو غير قانوني مثل تداول المواد غير المشروعة، أو استخدام الإنترنت لأغراض احتيالية.
- **ملاحقة الجرائم السيبرانية المتعلقة بالأمن الوطني:** تلعب الوحدة دورًا مهمًا في حماية الأمن القومي من الهجمات السيبرانية، التي تستهدف البنية التحتية الحيوية للدولة مثل أنظمة الطاقة، الاتصالات، والدفاع، وذلك من خلال تعقب الأنشطة المشبوهة، والاستجابة السريعة لها.
- الاستجابة السريعة للهجمات السيبرانية: **وفرت الوحدة فرقًا متخصصة للاستجابة السريعة في حال وقوع أي هجوم سيبراني، أو اختراق كبير، بحيث تعمل هذه الفرق على احتواء الهجوم، وتقليل الأضرار، ومنع تسرب البيانات، أو الوصول إلى الأنظمة الحساسة.**
- تنفيذ القوانين المتعلقة بالجرائم الإلكترونية: **تعمل الوحدة على تطبيق القوانين، واللوائح المتعلقة بالجرائم الإلكترونية، سواء من خلال التحقيقات، أو ملاحقة الجناة.**
- التعاون مع القطاع الخاص: **تتعاون الوحدة مع الشركات والمؤسسات الخاصة، لتأمين شبكاتها وأنظمتها من الهجمات الإلكترونية، وتشمل هذه المهام تقديم استشارات أمنية، ومساعدتها في تحسين إجراءات الأمان السيبراني الخاصة بها.**
- تطوير القدرات التكنولوجية: **تعمل الوحدة بشكل مستمر على تطوير قدراتها التكنولوجية، للتصدي للتهديدات الإلكترونية الحديثة، بما في ذلك استخدام أدوات متقدمة، مثل الذكاء الاصطناعي لتحليل البيانات الضخمة، والكشف عن الأنشطة السيبرانية المشبوهة.**
- **دعم التحقيقات القضائية:** تقدم الوحدة الدعم الفني والتقني للجهات القضائية في التحقيقات

[1] إطلاق مادة فيلمية للتوعية بشأن الجرائم الالكترونية/موقع الامم المتحدة.

المتعلقة بالجرائم الإلكترونية، وتوفر الأدلة الرقمية، والآليات التقنية التي تدعم المحاكمات، والإجراءات القانونية.

- **التعاون الدولي:** تعمل الوحدة للتعامل مع الجرائم الالكترونية العابرة، من خلال التعاون مع المنظمات والهيئات الدولية المتخصصة في الأمن السيبراني، وتنسيق الجهود لمكافحة الهجمات السيبرانية.[1]

الفرع الثاني: انجازات وحدة الجرائم الالكترونية:

حققت وحدة الجرائم الإلكترونية العديد من الإنجازات الهامة، التي ساهمت في تعزيز الأمن الرقمي، ومكافحة الجرائم الإلكترونية، من أبرز هذه الإنجازات:

- الكشف عن شبكات إجرامية إلكترونية :تمكنت الوحدة من كشف وتفكيك العديد من الشبكات الإجرامية المتورطة في جرائم إلكترونية، كالقرصنة، وسرقة البيانات والهوية الرقمية، وساهمت في إيقاف العديد من الممارسات غير القانونية على الإنترنت.
- حماية البيانات الحكومية :ساهمت الوحدة في تأمين الأنظمة الإلكترونية الحكومية، ومنع اختراقات كبيرة كانت تستهدف سرقة بيانات حساسة، أو تعطيل خدمات حكومية، مما أسهم في تعزيز ثقة المواطنين في الخدمات الإلكترونية الحكومية.
- الاستجابة السريعة للهجمات السيبرانية :تميزت الوحدة بالقدرة على الاستجابة السريعة لأي هجوم سيبراني كبير، يستهدف البنية التحتية الحيوية للدولة مما حد من الأضرار، ومنع تسرب معلومات حساسة، أو حدوث اختراقات مؤثرة.
- التعاون الدولي :حققت الوحدة نجاحات ملموسة في التعاون مع أجهزة أمنية[2]، ومنظمات دولية لمكافحة الجرائم الإلكترونية العابرة للحدود، وتمكنت من تقديم المجرمين السيبرانيين للعدالة في حالات تتطلب تعاونًا دوليًا.

---

[1] الرواشدة، صباح عادل عارف، 2025 ، دور انظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، المجلة الأردنية في إدارة الأعمال، المجلد 21، العدد1 ، ص4.

[2] المركز الوطني للأمن السيبراني.

- تعزيز الوعي المجتمعي: قادت الوحدة حملات توعية ناجحة للمواطنين والشركات حول كيفية حماية أنفسهم من الهجمات الإلكترونية، سواء عبر وسائل الإعلام، أو من خلال برامج توعية مجتمعية موجهة، مما ساعد في تقليل عدد الضحايا المحتملين.[1]
- تطوير التكنولوجيا المستخدمة في مكافحة الجرائم: استثمرت الوحدة في استخدام تقنيات متقدمة مثل الذكاء الاصطناعي، وتحليل البيانات الكبيرة لتعقب النشاطات غير القانونية على الإنترنت، مما جعلها أكثر فعالية في الكشف عن الجرائم قبل وقوعها.

وعلى الرغم من كل ما حققته هذه الجهود المبذولة من قبل وحدة الجرائم الالكترونية، الا انها واجهت العديد من التحديات التي عرقلت عملها، وفرضت ضغوطًا متزايدة في مواجهة التهديدات المتطورة، ومن أبرز هذه التحديات:

- التطور السريع في أساليب الجرائم الإلكترونية: تتطور أساليب المجرمين الإلكترونيين بسرعة، حيث يتم استخدام تقنيات متقدمة مثل الذكاء الاصطناعي، والبرمجيات الخبيثة المتطورة، مما يستدعي من الوحدة مواكبة تلك التطورات باستمرار، وتحديث أدواتها، وآلياتها لمكافحة الجرائم الإلكترونية.
- نقص الموارد البشرية المتخصصة: يتطلب الكشف عن الجرائم الالكترونية فرقًا مؤهلة تقنيًا، ومدربة تدريبًا عاليًا في مجالات مثل الأمن السيبراني، والتحليل الرقمي، وقد شكل نقص الكفاءات البشرية المتخصصة، تحديًا كبيرًا للوحدة وقدرتها على التعامل مع التهديدات المتزايدة بشكل فعال.
- الجرائم العابرة للحدود :ان العديد من الجرائم الإلكترونية تكون ذات طبيعة دولية، مما يجعل تتبع المجرمين والتعاون مع الدول الأخرى أمراً معقدًا، بالإضافة الى ان اختلاف القوانين والسياسات بين الدول، قد شكل عائقًا أمام محاكمة المجرمين الإلكترونيين، والحد من نشاطاتهم.
- نقص التشريعات الملائمة: تشكل القوانين المحلية المتعلقة بالجرائم الإلكترونية غير المحدثة، عائقاً للقدرة على ملاحقة المجرمين، ومعاقبتهم بالشكل المناسب.
- زيادة حجم البيانات: يعتبر حجم البيانات على الانترنت، عائقًا واضحًا أمام القدرة على تحليلها والكشف عنها بشكل مناسب وادارتها، ومعالجتها في الوقت المطلوب.
- الهجمات السيبرانية المتطورة :لقد تعرضت البنية التحتية الحيوية كأنظمة الطاقة

[1] الدعجة، بشير، مقال درع الامان الرقمي: تحية تقدير لوحدة الجرائم الالكترونية في مديرية الامن العام، نشر في صحيفة صدى الشعب اليومية، السبت ، 11 يناير 2025.

والمواصلات، والخدمات الحكومية، لهجمات سيبرانية متطورة هدفت الى تعطيل أنظمتها، أو سرقة معلوماتها.

- التحديات المالية والتقنية :تحتاج مكافحة الجرائم الإلكترونية إلى استثمارات مالية كبيرة، لتوفير أحدث التقنيات، والأدوات التي تساعد على كشف الجرائم، وتتبع المجرمين، وقد ادى ضعف الموارد المالية على قدرات الوحدة في هذا المجال.
- التوعية المجتمعية غير الكافية :رغم جهود التوعية، لا يزال الكثير من الأفراد والشركات، يفتقرون إلى الوعي الكافي بطرق حماية أنفسهم من الجرائم الإلكترونية، مما سهل استهدافهم.

تعد هذه التحديات الدليل الدامغ، والمؤكد على الحاجة إلى تعزيز القدرات التقنية، والبشرية لوحدة الجرائم الالكترونية، ووجوب تحديث التشريعات الوطنية، والمضي نحو تكثيف التعاون الدولي، لمواكبة التطورات السريعة في هذا المجال، من أجل تحقيق بيئة رقمية آمنة ومستقرة.

المطلب الثاني: دور المركز الوطني للأمن السيبراني في تعزيز الأمن الرقمي.

أنشأ المركز الوطني للأمن السيبراني في مطلع العام (2021) بموجب قانون الأمن السيبراني رقم (16) لسنة 2019، وقد منح القانون للمركز الحق بالتمتع بالشخصية الاعتبارية، ذات الاستقلال المالي والاداري، بالإضافة الى حقه بامتلاك الاموال المنقولة وغير المنقولة، والقيام بجميع التصرفات القانونية، ويرتبط المركز برئيس الوزراء[1].

لقد عني المركز الوطني للأمن السيبراني بتوفير منظومة فعالة للأمن السيبراني على مستوى الوطن، والعمل على تطويرها وتنظيمها لحماية المملكة من تهديدات الفضاء السيبراني، ومواجهتها بكفاءة وفاعلية، لضمان استدامة العمل، والحفاظ على الأمن الوطني وسلامة الأشخاص، والممتلكات والمعلومات ككل.

ولإيجاد فضاء سيبراني آمن وموثوق في الأردن، سعى المركز الوطني للأمن السيبراني إلى تنفيذ مجموعة من المبادرات والبرامج، التي تستهدف مختلف شرائح المجتمع، وقطاعات العمل.[2]

بالإضافة الى السعي الى تدريب وتأهيل الموظفين، من خلال تنظيم برامج تدريبية متخصصة لموظفي القطاعين العام والخاص، الذي اتاح لهم اكتساب المعرفة والمهارات، التي تساعدهم في

[1] نص المادة (5) من قانون الامن السيبراني رقم (16) لسنة 2019.

[2] عقد القمة الوطنية الاولى للأمن السيبراني في 2023

التصدي للمخاطر السيبرانية، وقد كان لحملات التوعية[1] والتثقيف وورش العمل المعقودة لمختلف فئات المجتمع، بما في ذلك الطلاب والشركات والأفراد، مما أسهم في نشر ثقافة الأمن السيبراني بين الجميع[2].

سعى المركز الى اتباع وتبني المعايير الدولية خلال عمله، كوسيلة لرفع كفاءة وجودة وفاعلية الحلول المقدمة من قبله، ولصد المخاطر والتهديدات السيبرانية بشكل استباقي، بالإضافة الى الاستناد الى مجموعة من القيم الجوهرية ومنها احترافية الأداء، وتداول المعرفة مع استمرار التعلم، واستشراف المستقبل في ظل مرونة مؤسسية.

الفرع الأول: الخدمات الرئيسية التي يقدمها المركز الوطني للأمن السيبراني الأردني:

يقدم مركز الامن السيبراني العديد من الخدمات التي من شأنها توفير مظلة حماية لاكبر عدد ممكن من ابناء المجتمع على الصعيدين العام والخاص، ومن الخدمات التي يوفرها المركز هي:

- ادارة العمليات السيبرانية: من خلال تعزيز الحماية السيبرانية لتحقيق الامن والثقة لبياناته واصولها، من خلال مراقبة وتحليل للشبكات والانظمة الحكومية، لرصد الحوادث الواقعة عليها، والاستجابة لها والتحقيق فيها، وتقييم الاضرار الناتجة عنها.

[1] يشرع المركز الوطني للأمن السيبراني خلال شهر أكتوبر –الذي يُعتبر عالمياً شهراً للتوعية بالأمن السيبراني– بإطلاق حملات توعوية في مجالات الأمن السيبراني بالتعاون مع جهات مختلفة، ومن أبرز الحملات التي يتم إطلاقها في شهر التوعية حملة " تلميحه رقمية" التي يتم خلالها إطلاق العديد من المنشورات الرقمية بمواضيع متعلقة بالأمن السيبراني.

[2] عقد مركز الامن السيبراني العديد من ورش العمل والمؤتمرات لمختلف الفئات العمرية ومنها:

- في عام (2024) تم تدريب طلبة الجامعات الأردنية سواء الحكومية أو الخاصة، على تحديات "**التقاط العلم**"، وهو برنامج تدريبي يعتمد على تقنيات الأمن السيبراني والتحديات المتعلقة بحماية المعلومات، و استمر التدريب لمدة ثمانية أيام لكل جامعة، وتم تقديمه عبر الإنترنت لضمان الوصول إلى أكبر عدد ممكن من الطلبة من مختلف الجامعة ، بالإضافة الى اتباع البرنامج ذاته على طلاب المدارس ، بالإضافة الى عقد المسابقات لتحفيز افراد المجتمع على المشاركة والتعرف على مفهوم الامن السيبراني ، وكيفية التعامل معه ، كعقد مسابقة محاربي السايبر للجامعات – النسخة الثالثة 17 تموز (2024) ، و معسكر النشامى في شهر تموز (2024) .

ويتم ذلك عن طريق الفريق الوطني للاستجابة لحوادث الأمن السيبراني(JOCFRT)، الذي تأسس في عام(2017) كجزء من المركز الوطني للأمن السيبراني، وقد اوكل اليه مهمة حماية المملكة من الهجمات السيبرانية، والانشطة غير المصرح بها الصادرة من الشبكات الحيوية، او البيانات والبنية التحتية الحيوية، او اي شكل من اشكال الاعتداء، بالإضافة الى تنسيق الاستجابة لحوادث الأمن السيبراني الوطنية، من خلال مجموعة من التدابير والجهات المتخصصة،، للقيام **بتنسيق الاستجابة الوطنية**، وتطوير **خطط الطوارئ السيبرانية**، وتحديث بروتوكولات الطوارئ بشكل مستمر، لضمان استمرارية عملها في حال وقوع هجمات سيبرانية، كما يعمل الفريق الوطني على **الحفاظ على العلاقات الدولية**، من خلال التعاون مع مراكز الطوارئ الشريكة الاقليمية منها والدولية، لتعزيز تبادل المعلومات حول التهديدات السيبرانية وتحليلها.

- القيام بمهمات استخباراتية، لغايات جمع المعلومات المرادة لغايات محددة، وتحليل البرمجيات الخبيثة ومراقبة البصمة الرقمية، وتقييم الجانب التقني للشبكات، والعمل على اجراء عدد من الفحوصات الامنية وفحوصات الاختراق، ليتم التحقيق بالاستناد اليها، واصدار تقارير تبين الموقف الامني، وتطلق تحذيرات امنية للحالات المشابهة.

ولأجل ذلك تم انشاء العديد من المنصات، كان اولها **منصة مكافأة الثغرات واختبارات الاختراق الأردنية**، (Bug Bounty Jo) وتعتبر الأولى من نوعها في الأردن، وتهدف إلى تمكين **الجهات الحكومية والخاصة** من إجراء اختبارات شاملة، لتحديد نقاط الضعف في منصاتها، وأصولها الرقمية، كما انها تتيح تحديد الثغرات الأمنية بشكل سريع وفعال، مع التركيز على **الاستمرارية** في مراقبة الأمان السيبراني، من خلال تمكينها **للباحثين** للمشاركة في الاختبارات، واجراء اختبارات اختراق فعالة وبأقل التكاليف، مع التركيز على عقد ورش عمل توعوية لجميع فئات المجتمع الأردني، لبيان المفاهيم الأساسية في الأمن السيبراني، وكيفية التعامل الآمن مع البريد الالكتروني، وغيرها من الموضوعات .

بالإضافة الى منصة مشاركة معلومات التهديدات السيبرانية(منصة شارك)، التي توفر بيئة آمنة وموثوقة، لتبادل المعلومات السيبرانية بين المؤسسات والوزارات المعنية بالإدارة الاستباقية، لمواجهة التهديدات والهجمات السيبرانية، حيث تعمل على تقديم بيانات وتحليلات حول الهجمات السيبرانية، الثغرات الأمنية، والتحليلات الرقمية، بالإضافة إلى المعلومات الاستخباراتية التي تكشف عن الاتجاهات، والأنماط الجديدة والمتطورة للهجمات، وبذلك فهي تضمن توفير منصة آمنة وموثوقة

لتبادل المعلومات الاستخباراتية السيبرانية، و تتيح رصد التهديدات السيبرانية الحالية والنشطة والمستقبلية، وتدعم الاستجابة السريعة والفعالة للهجمات السيبرانية، كما انها تسهم في توثيق المعلومات والتقارير الفنية، لتعزيز تبادل الخبرات والمعرفة بين الأعضاء.

- حوكمة الامن السيبراني: يهتم المركز بإيجاد اطر تشريعية، وسياسات، وتعليمات، ملزمة التنفيذ وموجبة للمساءلة، تعزز من امن الفضاء السيبراني الأردني.[1]
- بناء وتعزيز القدرات السيبرانية الوطنية: من خلال بناء القدرات الوطنية، والعمل على نشر الوعي لكافة شرائح المجتمع[2]، وبناء المهارات وتدريبها على العديد من البرامج كبرنامج ادارة التعليم(LMS)، والمنصات كمنصة (safe online)، وبناء العلاقات التعاونية التشاركية.[3]

الفرع الثاني: التشريعات الفاعلة في المركز الوطني للأمن السيبراني:

تعددت التشريعات المعمول بها في المركز الوطني للأمن السيبراني، ما بين قوانين وانظمة وتعليمات، الا ان الغاية من العمل بها واحدة، وهي توفير فضاء سيبراني آمن في المملكة قدر المستطاع، بعيداً عن المخاطر والتهديدات والاختراقات المرتكبة، لحماية البيانات والمعلومات الحكومية، في شتى الوزارات والدوائر الحكومية اثناء تناقلها بين الجهات الحكومية، او في الجهة الحكومية ذاتها .

ومن اهم التشريعات الفاعلة بالمركز، هو قانون الامن السيبراني رقم (16) لسنة 2019، وهو الإطار القانوني الذي ينظم الأمن السيبراني في الأردن، ويهدف إلى مواكبة التطورات التكنولوجية

[1] عمل المركز من خلال هذه المهمة على اصدار مسودة نظام ترخيص مقدمي خدمات الامن السيبراني لعام (2023) ومازال قيد الدراسة لدى ديوان التشريع والرأي، كما عمل على مسودة تعليمات معايير المخالفات وضوابطها والاجراءات المستحقة وهي الان في عهدة المجلس الوطني للأمن السيبراني، ليتم اقرارها.

[2] تم إطلاق حملة (وطن واع) بالتعاون مع أمانة عمان الكبرى، حيث تم خلالها اعداد العديد من مقاطع الفيديو، وتم نشرها على شاشات أمانة عمان المتواجدة في كافة أنحاء العاصمة، وامتدت هذه الحملة على مدار عام 2023، كما نفذ المركز حملة اليوم العالمي لذوي الاحتياجات الخاصة لعام (2023)، وتم تسجيل وتصميم عدد من مقاطع الفيديو بلغة الاشارة.

[3] التقرير السنوي لمركز الامن السيبراني الأردني لسنة (2023).

العالمية وتأمين الفضاء الإلكتروني في ظل تزايد الهجمات السيبرانية عالميًا، وحماية البنية التحتية الوطنية الحساسة، وتعزيز قدرات المملكة في مواجهة التهديدات السيبرانية، لتحقيق الأمن السيبراني الشامل، وتجنب الخسائر الاقتصادية، أو المعلوماتية التي قد تنجم عن الهجمات الالكترونية [1].

وقد احتوى القانون على مجموعة من الاحكام التي رتبت المفاهيم، وبينت آليات العمل في المركز، بالإضافة الى بيان المهام والمسؤوليات الموكلة الى المركز القيام بها، ومنها توليه إعداد استراتيجيات وسياسات ومعايير الأمن السيبراني، بالإضافة إلى مراقبة تطبيقها، ووضع الخطط اللازمة لتنفيذها بعد إقرارها من المجلس، وتطوير وتنفيذ عمليات الأمن السيبراني، و تحديد معايير وضوابط الأمن السيبراني، وإصدار تعليمات تحدد المعايير، وتضع تصنيفًا لحوادث الأمن السيبراني، بالإضافة الى منح التراخيص، و تبادل المعلومات والتعاون الدولي، وغيرها من المهام.[2]

كما فرض القانون على الجهات المعنية الالتزام بالإبلاغ عن أي حوادث سيبرانية قد تتعرض لها، مما يمكنها من القيام باستجابة سريعة، لحماية النظام الرقمي للدولة.[3]

ويكون المركز الوطني للأمن السيبراني، المسؤول عن إدارة وتوجيه الاستجابة للحوادث السيبرانية التي يتم تحديدها بموجب القرار الصادر عن المجلس، بناءً على توصية من رئيس مركز الأمن السيبراني، صاحب الصلاحية في تحديد مستوى خطورة الحادث السيبراني على أمن المملكة وسلامتها.

وهذا يعني أن لرئيس المركز ان يقترح أو يوصي، بأن حادثًا معينًا يشكل تهديدًا خطيرًا، ومن ثم يقوم المجلس بإصدار القرار النهائي، بشأن هذا الحادث.[4]

ولا ننكر اهمية التعاون الدولي، وهو ما نص القانون على تعزيزه مع الدول الأخرى، والمنظمات الدولية فيما يتعلق بالأمن السيبراني، مثل منظمة الاتحاد الدولي للاتصالات(ITU) ، ومنظمة

[1] صدى بودكاست، أهم التشريعات والقوانين المرتبطة بالأمن السيبراني، حكاية سيبرانية، الدكتور يعرب القضاة ، 30 نوفمبر 2023.

[2] المادة (6) من قانون الامن السيبراني لسنة 2019.

[3] نص المادة (8/أ) و(8/ب/3) من قانون الامن السيبراني لسنة 2019.

[4] المادة (9) من قانون الامن السيبراني لسنة (2019).

الأمن والتعاون في البحر الأبيض المتوسط(OSCE) ، ومنظمات أخرى معنية بأمن المعلومات[1].
حيث توفر هذه المنظمات منصات لتبادل المعلومات والتنسيق بين الدول، الذي يعزز من الفهم المشترك للتحديات السيبرانية، وطرق التعامل معها، ويسهم في تبادل الخبرات والمعلومات، وتنسيق الجهود لمواجهة التهديدات السيبرانية العابرة للحدود.[2]

وقد اتسعت دائرة تنظيم الامن السيبراني لضمان مجابهة التهديدات المتوقعة، والرد عليها بكفاءة وفعالية، وتحقيقاً لذلك، صدر نظام المركز الوطني للأمن السيبراني لسنة (2020)، لبين مهام رئيس المركز الموكول إليه، ويجعله المسؤول أمام المجلس عن إدارة المركز، ومتابعة أعماله، وهو آمر الصرف فيه.

وتعزيزا للجانب التشريعي، أصدر المركز الوطني للأمن السيبراني تعليمات (2023)، لتصنيف حوادث الأمن السيبراني وفقًا لدرجة خطورتها، وتعزيز القدرة على التصدي لتلك الحوادث بكفاءة، وبيان مدى تأثيرها على القطاعات المختلفة، سواء كانت في القطاع العام أو الخاص، لتحقيق الحماية المطلوبة من التهديدات السيبرانية.

وبالنظر الى الواقع الامني للحوادث السيبرانية، بين التقرير الامني للربع الثاني من العام (2024) للمركز ازدياد حالات سرقة المعلومات في المؤسسات الوطنية بما نسبة (39%)، مقارنة بالربع الثاني من العام الماضي، حيث بلغ عدد الحوادث السيبرانية التي استهدفا الوزارات والمؤسسات الحكومية (1582) حادثا.

الا انه وبالمقابل لوحظ انخفاض عدد الحوادث السيبرانية المكتشفة بما نسبته (23%)، مقارنة بالربع الأول من العام الماضي، ويعود السبب في ذلك الى ازدياد نسبة التزام الوزارات والمؤسسات الحكومية، بالسياسات والتدابير الأمنية. [3]

---

[1] شارك المركز على الصعيد الاقليمي في إعداد مشروع القانون العربي الاسترشادي (جامعة الدول العربية .) ، وعلى الصعيد الدولي شارك المركز في إعداد مسودة الاتفاقية الشاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، (الامم المتحدة) مازالت قيد العمل.

[2] المادة (6/ب/5) من قانون الامن السيبراني لسنة 2019.

[3] التقرير الامني للربع الثاني للعام (2024)، الصادر عن المركز الوطني للأمن السيبراني.

الخاتمة

لقد سعى التشريع الأردني جاهداً الى وضع إطار تشريعي للذكاء الاصطناعي، من خلال سنه للقوانين والسياسات، التي تعزز استخدامه بطريقة مسؤولة وآمنة، وقد حرص فيه الى خلق نوع من التوازن بين القدرة على التكيف مع التسارع الملحوظ في استخدام الذكاء الاصطناعي وتطبيقاته، وهو ردة فعل طبيعية لعالم التكنولوجيا الذي نعيشه، وبين حماية الامن السيبراني من الاختراقات التي قد تودي بحقوق مواطنيها وبياناتهم أو دولتها، أو التهديدات التي من الممكن ان تتعرض لها مستقبلاً.

وقد نجحت هذه التشريعات بالفعل في التصدي للعديد من الهجمات، والاختراقات التي تعرضت لها، مما ادى الى زيادة الثقة في التقنيات الرقمية الوطنية التي نملكها، وانعكس على ثقة المواطنين في قدرة التشريعات الوطنية، على النيل ممن يقدم على ارتكاب اي نوع من الجرائم التي تمس الحقوق، باختلاف طبيعة اقترافها.

النتائج

1. اجتهدت التشريعات الأردنية في كبح جماح مجموعة من الجرائم الالكترونية المرتكبة بالطرق الحديثة، ومنها الذكاء الاصطناعي.
2. ساهمت التشريعات الأردنية في التقليل من تأثير الجريمة الالكترونية المرتكبة بالذكاء الاصطناعي على الامن السيبراني، الا انها بحاجة الى الاستمرار في جهودها التشريعية لتشمل أكبر عدد ممكن من الصور الجرمية المقترفة.
3. ساهمت الآليات الأردنية المستحدثة كوحدة الجرائم الالكترونية، والمركز الوطني للأمن السيبراني، بمساندة التشريعات الوطنية، للعمل بشكل متناسق لمحاربة الهجمات السيبرانية المرتكبة بالذكاء الاصطناعي.
4. حقق التعاون الأردني مع الجهات الدولية، انخفاضاً في نسب الجرائم الالكترونية بشتى صورها، وزاد من قدرة الجهات المعنية على التعامل مع الادوات المستحدثة في ارتكاب هذه الجرائم، ومنها الذكاء الاصطناعي.

التوصيات

على الرغم من الجهود الوطنية للتكيف مع الواقع التكنولوجي الذي نعيشه، الا اننا نرى انه مازال هناك العديد من الامور التي نتطلع الى تحقيقها، لنتمكن من حماية امنا السيبراني من التهديدات التي يتعرض لها، ومنها:

1. المواظبة على تحديث التشريعات الوطنية، وادراج مصطلح الذكاء الاصطناعي صراحة في متنها، لحين التوصل الى تشريع خاص بالذكاء الاصطناعي.
2. عقد دورات مكثفة لجميع فئات المجتمع، للتعريف بالذكاء الاصطناعي، وكيفية التعامل معه، وأثره على الأمن السيبراني، واقترح ادخال مصطلح الذكاء الاصطناعي في المنهاج التعليمي الأردني، كإدخاله في المنهاج المدرسي (مادتي الاجتماعيات، والحاسوب) لكون اليافعين وطلبة المدارس الاكثر استخداماً للتكنولوجيا، وكذلك المنهاج الجامعي، ووضعه كمادة اجبارية توازي مادة مهارات التواصل لطلاب السنة الأولى، ومادة اختيارية او مادة حرة للسنوات اللاحقة .
3. العمل على تدريب القوى البشرية العاملة في الدوائر الحكومية ورفع كفاءتهم، من خلال عقد دورات متخصصة بشكل مكثف.
4. تعاون القطاعين العام والخاص في تبادل الخبرات، وعقد الدورات المتبادلة التي ترفع من الوعي المجتمعي.
5. التعاون ما بين الجهات الوطنية والمنظمات الدولية، وتبادل الخبرات فيما بينهم على نطاق أوسع.

قائمة المراجع والمصادر :

- **الكتب:**

1. ابراهيم، خالد، (2022)، التنظيم القانوني للذكاء الاصطناعي، دار الفكر الجامعي، الاسكندرية، مصر، ط1.
2. الراعي، أشرف، (2025)، الجرائم الالكترونية (الأحكام الموضوعية لجرائم تقنية المعلومات والذكاء الاصطناعي)، البديل للنشر والتوزيع، عمان، الأردن، ط1.
3. النوايسة، عبد الإله،"**جرائم تكنولوجيا المعلومات: شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية**، (2017)، دار وائل للنشر والتوزيع، ط1.

4. الوريكات، محمد عبد الله، (2009)، "**أصول علم الإجرام والعقاب**"، دار وائل للنشر والتوزيع، عمان، الأردن، ط1.

- **الدوريات:**

1. حداوي، أميرة هاتف، ومسلم، ضرغام علي، ومحمد، صفاء تايه،(2023) ،"**القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات: دراسة تحليلية لآراء عينة من العاملين في المصارف الأهلية في النجف الأشرف**"، مجلة العلوم الإنسانية والطبيعية.
2. الدحيات، عماد عبد الرحمن، 2020، "**نحو تنظيم قانوني للذكاء الاصطناعي في حياتنا: إشكالية العلاقة بين البشر والآلة**"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 8، العدد 5.
3. الدعجة، بشير، "**درع الأمان الرقمي: تحية تقدير لوحدة الجرائم الإلكترونية في مديرية الأمن العام**"، مقال منشور في صحيفة صدى الشعب اليومية، السبت،11 يناير 2025.
4. رجب، هبة رمضان،2024، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، مجلة العلوم المالية والاقتصادية، جامعة عين شمس، مصر.
5. الرواشدة، صباح عادل عارف،2025، دور انظمة الذكاء الاصطناعي في مكافحة الجرائم الالكترونية، المجلة الأردنية في ادارة الاعمال، المجلد 21، العدد1.

- **الرسائل:**

1. يوسف كريستيان،2019، "**المسؤولية المدنية عن فعل الذكاء الاصطناعي**"، رسالة ماجستير منشور، الجامعة اللبنانية، لبنان.

- **القوانين والتشريعات:**

1. **قانون حماية البيانات الشخصية** (2023).
2. **قانون الجرائم الإلكترونية الأردني لسنة رقم (17) لسنة 2023.**
3. **قانون الأمن السيبراني رقم (16) لسنة 2019.**
4. نظام المركز الوطني للأمن السيبراني رقم (1) لسنة 2020.

- **المواقع الإلكترونية:**

1. موقع الإسكوا http://opengov.unescwa.org/ar/node/1196 :تاريخ الزيارة: 2025/3/27
2. موقع سند الحكومي الأردني.http://sanad.gov.jo
3. موقع وزارة الاقتصاد الرقمي والريادة.
4. موقع مديرية الأمن العام الأردنيةhttp://www.psd.gov.jo.
5. موقع المركز الوطني للأمن السيبراني.
6. وكالة بوصلة للأنباء، تقرير منشور يوم الأربعاء، 16 أكتوبر 2024.
7. موقع صحيفة المواطن الإلكترونية.www.almowaten.com
8. موقع الأمم المتحدة (http://www.un.org) .

- **التقارير والبرامج:**

1. وزارة التخطيط والتعاون الدولي، تقرير صادر في ديسمبر (كانون الأول) 2021.

صدى بودكاست، "**أهم التشريعات والقوانين المرتبطة بالأمن السيبراني**"، حكاية سيبرانية، الدكتور يعرب القضاة، 30 نوفمبر 2023.