Journal of Al-Quds Open University for Humanities & Social Studies - No (66) – January 2025
https: //journals.qou.edu/index.php/jrresstudy
E-ISSN: 2616-9843/ P-ISSN: 2616-9835

Digital Privacy in the Age of Artificial Intelligence:

A Reading of the Jordanian and Palestinian Legislation

Dr. Ahmad Hosni Ali Ashqar

Assistant professor, Department of Legal Sciences, Faculty of Graduate Studies, Arab American University, Ramallah, Palestine.

Oricd No: 0009-0003-9801-4151
Email: ahmad.ashgar@aaup.edu

Received:
19/ 04/ 2024

Revised:
19/ 04/ 2024

Accepted:
08/ 06/ 2024

***Corresponding Author:**
ahmad.ashgar@aaup.edu

Citation: Ashqar, A. H. A. (2025). Digital Privacy in the Age of Artificial Intelligence: A Reading of the Jordanian and Palestinian Legislation. Journal of Al-Quds Open University for Humanities and Social Studies, 7(66). https://doi.org/10.33977/0507-000-066-003

• **Open Access**

Abstract

Objectives: This research aims to demonstrate the impact of artificial intelligence on the right to digital privacy, and to scrutinize constitutional and criminal texts

Methods: The researcher followed the comparative analytical approach, where the researcher analyzed the nature of artificial intelligence and its technologies, and the relevant constitutional and international texts, in a comparative context to reach the results.

Results: The study concluded several results, the most prominent of which is that artificial intelligence systems, with their ability to access digital data, easily lead to the emergence of new types that infringe on individuals' right to privacy.

Conclusions: The study recommended issuing special criminal legislation at an advanced stage to regulate the uses of artificial intelligence and criminalize attacks on the right to digital privacy.

Keywords: Artificial Intelligence, digital privacy, cyber-crime, digital data.

الخصوصيّة الرقميّة في عصر الذَكاء الاصطناعيّ:

قراءة في التشريعين: الأردني والفلسطيني

د. أحمد حسني علي أشقر

أستاذ مساعد، قسم العلوم القانونية، كلية الدراسات العليا، الجامعة العربية الأمريكية، رام الله، فلسطين.

الملخص

الأهداف: يهدف هذا البحث إلى بيان تأثير الذَكاء الاصطناعيّ على الحقّ في الخصوصيّة الرقميّة، واستقراء النصوص الدستوريّة والجنائيّة ومدى قدرتها على توفير الحِماية القانونيّة لحقّوق الأَفراد في الخصوصيّة الرقميّة في فلسطين والأردن.

المنهجية: قام الباحث باتّباع المنهج التحليليّ المقارن، حيث عمد الباحث إلى تحليل ماهيّة الذَكاء الاصطناعيّ وتقاناته، والنصوص الدستوريّة، وكذلك الدوليّة ذات الصلة، وذلك في سياق مقارن للوصول إلى النتائج.

النتائج: خلصت الدراسة إلى نتائج عدة، أبرزها أن تميّز أنظمة الذَكاء الاصطناعيّ بقدرتها على النفاذ إلى البَيانات الرقميّة بسهولة أدت إلى نشوء تهديدات جدية على حقّ الأَفراد في الخصوصيّة.

الخلاصة: أوصت الدراسة بإصدار تشريع جنائي خاص في مرحلة متقدمة لتنظيم استخدامات الذَكاء الاصطناعيّ وتجريم الاعتداء على الحقّ في الخصوصيّة الرقميّة.

الكلمات الدالة: الذَكاء الاصطناعيّ، الخصوصيّة الرقميّة، الجرائم الإلكترونية، البَيانات الرقميّة.

المقدمة

يستند التحوّل الرقميّ الراهن على تقنيّة الذَكاء الاصطناعيّ الذي أضحى مفهوماً متداولاً جدا كأحد التطبيقات التي تهدف إلى إدراك طبيعة الذَكاء الإنسانيّ عن طريق مجموعة برمجيات وخوارزميّات تستطيع محاكاة قدرات وتصرفات الإنسان المتسم بالذَكاء، ومن ثم تكوين الآراء واتخاذ المواقف والقرارات باستقلاليّة.

ويحمل هذا التحول الكثير من الإيجابيّات لتعزيز رفاه الإنسان لكنه لا يخلو من مَخاطر وتهديدات جمّة على طائفة واسعة من حقّوق الفرد، وحرياته، ومنها: الحقّ في الخصوصيّة الفرديّة وحرمةِ الحياةِ الخاصّةِ على وجه العموم، والحقّ في الخصوصيّة الرقميّة بوجه خاص، وأمام هذه التطوّرات، بات يشعر العالم بالقلق على خصوصيّات الأَفراد، سيما الرقميّة منها، لاتصال ذلك مع تنامي قدرات الذَكاء الإصطناعيّ في هذا الإطار.

من هنا، ظهرت علاقة تضاد محقّقة بين الذَكاء الاصطناعيّ والخصوصيّة بشكل عام، ذلك أنّ صور هذا الحقّ لا تنطوي أو تقتصر على خصوصيّة الشخص المعنية بسلامة الفرد وأمانه في جوانب حياته المختلفة، أو خصوصيّة سُلوكه الفردي، بل تمتد إلى حرمة بياناته الشخصيّة في ألا تكون متوفرة بشكل تلقائيّ للجميع.

وأمام هذه التحديات، فإن الدساتير على اختلافها، وكذلك التشريعات العقابية، لم تواكب التطورات في عصر يسود فيه ما يسمى بالذَكاء الاصطناعيّ كخطر محدق على حقّ الأَفراد في الخصوصيّة الرقميّة، وفي هذا الإطار، لم تتبنى السلطتان التشريعيتان في فلسطين والأردن منهج إصدار قانون خاص ينظم استخدامات أنظمة الذَكاء الإصطناعيّ لجهة ضمان عدم مساسها بخصوصيّة الأفراد الرقميّة مثلما فعل البرلمان (الأوروبي) في مارس (2024) بإصدار قانون متخصص يتولى تنظيم الذَكاء الاصطناعيّ، والذي ستتم المباشرة في تنفيذه في مايو (أيار) 2024، بعد اجتياز الفحوصات النهائية والحصول على موافقة من المجلس الأوروبي. ثم سيتم تنفيذه على مراحل ابتداءً من عام 2025.

أولاً: أهميّة الدراسة

تربط هذه الدراسة بين الأفعال الإلكترونيّة التي جرّمها المشرعان الفلسطيني والأردني بتشريعات جزائية خاصة، واستخدام تقانات الذَكاء الإصطناعيّ التي من الممكن أن تشكل أداة جرمية معتبرة في التطبيق القضائي لهذه التشريعات بما يمكن المشتغلين بالقانون من استخدامها في التطبيق العملي أمام القضاء.

ثانياً: إشكالية الدراسة

تتمحور إشكاليّة الدراسة في عدم نجاعة التشريعات الناظمة للجرائم الإلكترونية، وكفايتها، في فلسطين، والأردن على تغطية الجوانب المتعلقة بخصوصية الجرائم الناشئة عن الاستخدام غير القانونيّ، وغير المصرح به لأنظمة الذَكاء الإصطناعيّ في ظل التخوفات المتنامية من شيوع محتمل لانتهاك حقّ الأفراد في خصوصيّة بياناتهم الرقميّة، بواسطة هذه الأنظمة التي تتمتع بقدر كبير من الاستقلالية في التصرف، واتخاذ القرار عبر جمع البَيانات الرقميّة الشخصيّة، وتحليلها، ومن ثمّ اتخاذ القرارات بشأنها بشكل تلقائي، بما يؤدي إلى انتهاك هذه الخصوصيّة، مع ما يفرزه ذلك من إشكالات تطبيقية حول مدى توافر قصد المتهمين وانصراف إراداتهم لاستخدام تطبيقات هذا الذَكاء الذي يتصرف بقدرة ذاتية مستقلة عن إرادة مستخدميه.

تناقش هذه الدراسة سؤالاً محورياً يتمثل في مدى توافر القدرة لدى النظامين القانونيّين في الأردن وفلسطين على تنظيم المسائل المتصلة بالمخاطر التي تواجه حقّ الأفراد في الخصوصيّة الرقميّة في عصر الذَكاء الاصطناعيّ، وما يتفرع عن ذلك من أسئلة حول المَخاطر المحتملة من شيوع استخدام الذَكاء الاصطناعيّ على الحقّ في الخصوصيّة الرقميّة للأفراد، ومدى إمكانية تطبيق قوانين الجرائم الإلكترونية

في فلسطين والأردن، أو القواعد العامة في القانون الجنائي على الجرائم التي تعتدي على الخصوصيّة الرقميّة للأفراد المرتكبة بإحدى أنظمة الذَكاء الاصطناعيّ.

ثالثاً- أهداف الدراسة

تستهدف الدراسة الوصول إلى ما يلي:

1. بيان تأثير الذَكاء الاصطناعيّ على الحقّ في الخصوصيّة الرقميّة.
2. استقراء النصوص الدستوريّة وغيرها من التشريعات في الأردن وفلسطين وتحليلها للتعرف إلى مدى قدرتها إسباغ الحِماية الفاعلة لحقّوق الأفراد في الخصوصيّة الرقميّة، في ضوء القانون الأوروبي للذكاء الاصطناعيّ.
3. بيان مدى إمكانيّة تطبيق قوانين الجرائم الإلكترونية على جرائم الاعتداء على الخصوصيّة الرقميّة المرتكبة بإحدى أنظمة الذَكاء الاصطناعيّ.

رابعاً- منهجيّة الدراسة

قام الباحث باتّباع المنهج التحليليّ المقارن، حيث عمد الباحث إلى تحليل ماهيّة الذَكاء الاصطناعيّ وتقاناته، والنصوص الدستوريّة، وكذلك الدوليّة ذات الصلة، وذلك في سياق مقارن للوصول إلى النتائج، وقد قام الباحث بتقسيم هذا البحث إلى مبحثين: المبحث الأول يتناول ماهية الذَكاء الاصطناعيّ ومَخاطره على الحقّ في الخصوصيّة الرقميّة، وذلك من خلال مطلبين، يقسّم كل واحد منهما إلى فرعين، في حين يتناول في المبحث الثاني الأطر التشريعية الناظمة لحماية الحقّ في الخصوصيّة الرقميّة في عصر الذَكاء الاصطناعيّ من خلال مطلبين، ويقسّم كل واحد منهما إلى فرعين أيضاً، وذلك على النحو التالي:

المبحث الأول- ماهية الذَكاء الاصطناعيّ ومَخاطره على الحقّ في الخصوصيّة الرقميّة

تتميز أنظمة الذَكاء الاصطناعيّ بخصائص متعددة، أهمها القدرة على النفاذ إلى البَيانات الرقميّة بسهولة ويسر مقارنة مع التطبيقات التكنولوجيّة الأخرى، مما يسهم في نشوء تهديدات جدية على حقّ الأفراد في الخصوصيّة الرقميّة، وبغية البحث في ماهية الذَكاء الاصطناعيّ ومَخاطره في هذا الإطار، فإننا سنتناول في المبحث دراسة ماهية الذَكاء الاصطناعيّ ومَخاطره ذات الصلة من خلال مطلبين، هما:

المطلب الأول- ماهيّة الذَكاء الاصطناعيّ وعلاقته بالخصوصيّة الرقميّة

أدى ظهور الذَكاء الاصطناعيّ بخصائصه الفريدة وقدراته على معالجة كم هائل من البَيانات إلى نشوء الحاجة إلى تحديد مفهوم دقيق للحقّ في الخصوصيّة الرقميّة، وقد ارتبطت هذه الخصوصيّة بشكل كبير مع ماهية الذَكاء الاصطناعيّ وتطور تقنياته بشكل مستمر، لذلك، سوف نعمد في هذا المطلب إلى دراسة ماهيّة الذَكاء الصناعي وعلاقته بالخصوصيّة الرقميّة من خلال الفرعين التاليين:

الفرع الأول- ماهيّة الذَكاء الاصطناعيّ

يعود الظهور الأول للذكاء الاصطناعيّ إلى العام 1963 عندما افترض العالم الإنجليزي (آلان تورنج) أن هناك آلة وهمية قادرة من تلقاء نفسها على تحديد المشكلات وحلّها، وتعتبر الولادة الحقّيقية للذكاء الاصطناعيّ بدأت في العام 1956 من قبل علماء الرياضيات الذين شاركوا في مؤتمر "دارتموت" حين قدموا ورقة عمل فريدة متعلقة بالذَكاء الاصطناعيّ (خزيمية،،2024، ص 9) لتتعاظم بعدها البحوث والمنجزات المتعلقة بالذَكاء الاصطناعيّ إلى وقتنا الراهن.

حالياً، لم يعد مصطلح الذَكاء الاصطناعيّ مصطلحاً غريباً نظراً لشيوعه في الكثير من تفاصيل حياة البشر اليومية، وقد كان يُقتصر تداول هذا المصطلح بين علماء الحاسوب والعلوم التطبيقية باعتباره فرعاً من علوم (الحاسب الآلي)، لذلك، جاءت التعريفات التي تحدد ماهية الذَكاء الاصطناعيّ منسجمة مع اعتباره علماً حاسوبياً، فهناك من عرفه بأنه ما تتسم به البرامج المحوسبة من

خصائص تقوم على محاكاة قدرات البشر وطرائق عملهم، وهو يعني أيضا ما تتمتع الآلات الحاسوبية والتكنولوجيا الرقميّة من قدرة على القيام بمهمات تتماثل وتشابه تلك القدرة التي يتصف بها البشر التي يكون منبعها التفكير العقلي، مثل القـدرة علـى التفكيـر والتعلـم التراكمي من التجار التي مرّ بها، ومـن التصرفات التـي تحتاج قدرة ذهنية وعقليـة ذكية (العجماني، 2023)، كما ذهب آخرون إلى تعريفه أيضاً بأنه نظام برمجي يعمل على أساس الخوارزميات، يعتمد على جمع البَيانات واستخدامها، ويتميز بالقدرة على التعلم بشكل جزئي أو كلي بشكل مستقل، كما يُعتبر قادرًا على اتخاذ القرارات بشكل جزئي أو كلي، وبشكل مستقل، استنادًا إلى ما تم من تدعيمه بقدرات تمكنه من تحيل البَيانات ومعالجتها مهما بلغ حجمها (Vial, 2022, p66).

وفي هذا السياق، وضعت المادة 3 في الفقرة 1 من قانون الاتحاد الأوروبي لسنة (2024) بشأن الذَكاء الاصطناعيّ تعريفاً يتماشى إلى حد بعيد مع ماهية تقنيات الذَكاء الاصطناعيّ ومن وجهة النظر التقنية، وذلك حين نصت على أنه "نظام قائم على الآلة مصمم للعمل بمستويات متفاوتة من الاستقلالية والذي قد يظهر قدرة على التكيف بعد نشره، وبناءً على أهداف محددة بشكل صريح أو ضمني، يستنتج النظام، من البَيانات التي يتلقاها، كيفية التنبؤ والتوصيات، واتخاذ القرارات التي يمكن أن تؤثر على البيئات الفيزيائية أو الافتراضية" (European Commission. (2024) Article 3 - Artificial Intelligence Ac).

ودائماً يسعى مطورو أنظمة الذَكاء الاصطناعيّ لزيادة قدرته في دعم القرار من خلال تحليل الاتجاهات وتوفير التوقعات وتحديث البَيانات، ونشأت تبعاً لذلك ثلاثة أصناف لأنظمة الذَكاء الاصطناعيّ، الأول هو الذَكاء المحدود الذي يستطيع القيام بمهمات محددة كالتعرف إلى الصوت والصورة، وهو الأكثر شيوعا من بين هذه الأنظمة، أما الصنف الثاني فهو الذَكاء الاصطناعيّ العام وهو الذي يعمد على جعل الأنظمة قادرة على ممارسة التفكير والتخطيط، بدون تدخل بشري على نحو يشابه إلى حد بعيد القدرة الإنسانية على استخدام عقله، من خلال ما يعرف بالشبكة العصبية للآلة التي تتشابه في وصفها وصفاتها مع الشبكة العصبية الإنسانية، أما الصنف الثالث فهو الذَكاء الاصطناعيّ الفائق الذي يتفوق مستوى ذكاء البشر (مهني، 2022).

ومن جهة أخرى، ارتبط الذَكاء الاصطناعيّ بمفهوم (الأمن السيبراني) الذي يعّد أمراً حيوياً لضمان التحكم الآمن في الأجهزة الذكية (Marcellin, 2024)، ما يعني وجود تهديد متنام يكمن في الإمكانية المرجّحة لقيام المجرمين السيبرانيين باستغلال تقنيات الذَكاء الاصطناعيّ لإحداث هجمات متطورة، ما يوجب تبني أدوات الذَكاء الاصطناعيّ ذاتها من جهة مقابلة، بغية التعرف المسبق إلى التهديدات، ضمن مقاربة حقّوقية تحترم مبادئ الشرعية، وأن تعمل الجهات المتخصصة ضمن ذلك في سياق دفاعي على تحليل البَيانات والمعطيات المتحصلة من السلوك المشبوه للمخالفين في المجال السيبراني، وتقصي الأنماط الشاذة، واتخاذ إجراءات فعّالة للحد من المَخاطر، وهذا يستدعي أيضاً أن يشتمل أي تعريف قانوني على قواعد إجرائية تتفق مع ماهية الذَكاء الاصطناعيّ وسبل مواجهته GoodTech. (2024). Cybersecurity (in 2024).

من الناحية القانونيّة، ونظراً لكون الذَكاء الاصطناعيّ مجالًا متطورًا ومعقدًا، فإن تحديد تعريف قانوني دقيق يستجيب لماهيّته المتغيرة له يُعتبر تحديًا جاداً للقانونين، سيما وأن التعريف التقني لماهية الذَكاء الاصطناعيّ تتطور باستمرار (European Commission. 2024. Article 3 - Artificial Intelligence Ac).

لذلك، ومع أهمية هذه التعريفات التقنية لماهيّة الذَكاء الاصطناعيّ، إلا أنها كما نرى لا تستجيب لمفهوم قانوني شامل يتناسب مع الطبيعة المتغيرة له، ذلك أنه وفي مجال يتسم بأن التطور التكنولوجي يتقدم بوتيرة أسرع بكثير من تطور القانون، فإن التعريف القانوني يجب أن يكون مُعدّاً؛ ليكون محايدًا تكنولوجيًا قدر الإمكان، وليكون قادرًا على الصمود في وجه تحديات الزمن، مع الأخذ في الاعتبار التطور السريع

لهذه التقنيات بحيث لا يكون خاضعا للمراجعة التشريعية كاستجابة لمبدأ الشرعية كقاعدة دستورية وجوبية تلزم المشرع أن تكون نصوصه واضحة وغير غامضة (European Parliament and Council. (2023). Exposition (of reasons, pt 5.2.

وأياً كان المفهوم القانوني الذي يمكن استخدامه في تعريف الذَكاء الاصطناعيّ، فإن أي تعريف يجب أن يراعي تميّز هذا التقنيات؛ ما يجعل أي مفهوم خاص به وقابل للتطبيق القانوني معضلة تشريعية تستدعي وضع تعريف جامع لا يرتهن للتطورات السريعة التي تجعل من التعريف قاصراً عن تغطية آثاره على جوانب الحياة كافة، بما فيها الجانب المتصل بالبَيانات الخاصة بالأَفراد (لخضر، معوش،2023).

وعلى ضوء ذلك، فإن المعالجة التشريعية لهذه المَخاطر والتهديدات يجب أن تنصب على التغطية القانونيّة لجوانب عدة تغطي مَخاطره في المفهوم القانوني، ومن ثم في أركان الجرائم، بحيث يشمل أي تعريف تحديد المَخاطر الناجمة عن استخدامات غير قانونية للذكاء الاصطناعيّ بما يتناسب مع ماهيته المتطورة.

الفرع الثاني- علاقة الحقّ بالخصوصيّة الرقميّة بالذَكاء الاصطناعيّ

ظهر الجدل بشأن حقّ الأَفراد في خصوصية بياناتهم الرقميّة في ستينيات القرن العشرين، نتيجة القلق المتزايد لدى الجمهور على خصوصياتهم التي ستتأثر حتما باضطراد استخدامات الذَكاء الإصطناعيّ، وشيوعها، ذلك أنّ صور هذا الحقّ لا تنطوي على خصوصية الشخص المعنية بسلامة الفرد في جسده، أو خصوصية السلوك الفردي المتصل بالجوانب السلوكية للفرد فقط، بل تمتد إلى خصوصية حقّه في حرمة بيناته الشخصيّة، ومؤدى ذلك أن لا تكون بياناته الشخصيّة والفرديّة الخاصة متوفرة بشكل تلقائي للجميع، ويتأتى ذلك من رغبة الإنسان بشكل فطري على السيطرة على تدفق بياناته ومعلوماته الشخصيّة الرقميّة، ويشمل ذلك أيضاً قدرته وتمكنه من التحكم في كيفية تداول هذه البينات والتصرف بها (مهني، 2022).

وأمام التطورات الهائلة في قدرات الذَكاء الاصطناعيّ، بات العام بالقلق يشعر على خصوصيات الأَفراد، سيما الرقميّة منها، لاتصال ذلك مع تنامي قدرات الذَكاء الاصطناعيّ في هذا الإطار، ومن هنا ظهرت علاقة تضاد محتملة بين الذَكاء الاصطناعيّ والخصوصيّة بشكل عام.

وفي الحقّيقة، فإن العلاقة بين التكنولوجيا والحقّ في الخصوصيّة الرقميّة كانت قائمة حتى قبل ظهور الذَكاء الاصطناعيّ، حيث انبثق موضوع الحقّوق المكرسة للأفراد في خصوصية بياناتهم الشخصيّة والرقميّة عن الحقّ القديم والمكرّس لخصوصية الفرد كحقّ محمي بموجب الدساتير والعديد من المواثيق الدوليّة، غير أن الفضل في صياغة هذا مفهوم الحقّ في الخصوصيّة الرقميّة كتعبير مستقل يعود للمؤلفين الأمريكيين (Milar) و(Wisten Alan)، حين أبرزا الفرق بين الحقّ القديم في الخصوصيّة والحقّ المستحدث في الخصوصيّة الرقميّة بعد ظهور الإنترنت، بينما يعود الحقّ في الخصوصيّة بوجه عام إلى حقّ الآخرين في احترام خصوصياتهم وحظر التعدي عليها (بن برغوث، 2023).

وفي هذا الجانب، وإذا كان المفهوم العام للحقّ في خصوصيّة الفرد يعني حقّه "في عدم ملاحقّة الآخرين ومتابعتهم له في حياته الخاصة (الجندي، 1993، ص 46)، وبأنها "قدرة المرء على أن يحافظ على أموره الخاصة ويمنع إفشاءها "، (الحمصاني، 1979، ص 116) فإنّ الخصوصيّة الرقميّة هي توصيف لوجوب تحقّق الحِماية الكاملة لبيانات الأَفراد، وتوافرها، وتشمل هذه الكثير من بيانات نستخدمها في المجال الإلكتروني ووسائل التواصل والاتصال، وقد انبثق عن ذلك ما يعرّف بالأمان الرقمي، وهو حاجة الانسان أن يستخدم الانترنت بشكل فعّال دون التعرض أي تهديدات تمس حقّه في الحقّ في الخصوصيّة الرقميّة وسرية المعلومات الشخصيّة (أحمد، 2021).

وعطفاً على ذلك، يمكن القول بأن ملامح العلاقة بين الذَكاء الإصطناعيّ والحقّ في الخصوصيّة الرقميّة تنطوي على مسألتين، الأولى هي حقّ الأَفراد في الحياة الخاصة، والثانية هي حقّ البشرية في الاستفادة من الجوانب الإيجابية لأنظمة الذَكاء الإصطناعيّ، إضافة إلى حقّ السلطات العامة في الاطلاع على معلومات التي تتعلق بشؤون الأَفراد، ضمن جدلية تفترض ألا يتم استخدام البَيانات الرقميّة الشخصيّة لأغراض تتنافى مع صونها واحترامها (رستم، 1992، ص 180)، وأن لا تتعارض الجوانب الإيجابية لأنظمة الذَكاء الإصطناعيّ مع خصوصية هذه البَيانات وحمايتها من أي وصول، أو استخدام غير القانوني لا يقترن بتصريح يتفق والقانون، سواء من قبل الدولة، أو الشركات الخاصة(Burgess, 2023, p. 87)

المطلب الثاني: آثار استخدام أنظمة الذَكاء الإصطناعيّ على الحقّ في الخصوصيّة الرقميّة

يترتب على استخدام الذَكاء الإصطناعيّ العديد من الآثار على حقّ الأَفراد في خصوصية بياناتهم الرقميّة نتيجة الخصائص التي تتميز بها أنظمة الذَكاء الإصطناعيّ، لذلك، سوف نعمد في هذا المطلب إلى دراسة آثار استخدام أنظمة الذَكاء الإصطناعيّ على الحقّ في الخصوصيّة الرقميّة من خلال الفرعين التاليين:

الفرع الأول: خصائص الذَكاء الإصطناعيّ وأثرها على الحقّ في الخصوصيّة الرقميّة

أسهمت القدرات الفائقة للذكاء الإصطناعيّ في تحليل البَيانات وإجراء التحليلات المعقدة في تعزيز المخاوف المتعلقة بالخصوصيّة، كما أنّ الإمكانات التي توفرها هذه التكنولوجيا لاستنباط معلومات حساسة، مثل مواقع الأشخاص وتفضيلاتهم وعاداتهم، أضحت تُشكل خطرًا على توزيع البَيانات دون إذن أو تصريح قانوني، وبالإضافة إلى ذلك، يمكن للذكاء الإصطناعيّ أن يُسهم في مَخاطر مثل سرقة الهوية والمراقبة غير المبررة، مما يُقدم تحديات فريدة تتطلب حلولًا استباقية وفورية. تُحفز هذه التطورات في مجال الذَكاء الاصطناعي على الحاجة إلى تطوير إرشادات أخلاقية وتبني أفضل الممارسات للتقليل من مَخاطر الخصوصيّة، ومن هنا، بدأ التأثير المباشر لانتشار أنظمة الذَكاء الاصطناعي على تطوير مفهوم الخصوصيّة الرقميّة للأفراد، وعلى وجوب توفير الحِماية القانونيّة لها (Sher & Benchlouch, 2023).

من جانب متصل، فإن قدرة الذَكاء الإصطناعيّ على العمل باستقلالية، مع قدرته على التنبؤ أيضاً، واتخاذ القرارات وتنفيذها بتلقائية، أدى إلى مَخاطر فقدان السيطرة عليه (مهني، 2022) بسبب مستوى الاستقلالية الذي يحظى به الأمر الذي يؤدي بالضرورة إلى إنتاج مواقف غير متوقعة ومحتملة الخطورة أثناء تشغيل هذه الأجهزة، منها احتمالية خروجها عن نطاق السيطرة البشرية، وبالتالي قيامه باتخاذ قرارات بشكل مستقل بما يدخل في نطاق الأفعال الجرمية (Parlement européen. 2020, Août 27).

كما أن التحسين المستمر لكفاءة الذَكاء الاصطناعي في معالجة وتحليل كميات هائلة من البَيانات، زاد إلى حد كبير من المخاوف المتصلة بالخصوصيّة وأمان البَيانات، (أميت، 2018) علاوة عن آلية جمع البينات بواسطة هذه التقنيات، والتي تتم غالباً من خلال ملفات تعريف الارتباط وعناوين IP دون إذن صريح من المستخدمين، (القنوبية،2024، ص590) الأمر الذي تطلب تطوير مفهوم الخصوصيّة ونقله من إطار تقليدي إلى إطار متخصص يضمن توازناً دقيقًا بين الاستفادة من إمكانيات الذَكاء الاصطناعي، وبين حماية خصوصية الأَفراد، مع ضمان استخدام البَيانات بطريقة قانونية وأخلاقية، من خلال محاولة وضع مفهوم للخصوصية الرقميّة ضمن إطار تنظيمي يحمي الأَفراد من الاستخدام غير القانوني أو غير المصرح به لبياناتهم الشخصيّة (Lucas. 2024, avril 5).

وعلى الرغم من الجوانب الإيجابية التي يمكن أن يحقّقها الذَكاء الإصطناعيّ على رفاه البشرية، إلا أن خصائصه تفرض العديد من الاعتداءات المحتملة على خصوصيات الأَفراد سيما الرقميّة منها (أميت، 2018)، وتحديداً في مجال القدرة الهائلة على تجميع البَيانات الرقميّة، ومن ثمّ تحليلها، وبعد ذلك استخدامها بأي طريقة أو بشكل غير قانوني وغير مصرح به بما قد يصل إلى حد نشرها للعموم دون

أدنى سيطرة من البشر، ذلك أن الذَكاء الإصطناعيّ يقوم بجمع البَيانات الرقميّة عبر ملفات تعريف الارتباط أو الكويكيز "Cookies"، أو عبر أو عبر بروتوكولات الانترنت "IP" address دون أن يكون هناك قيود أو أذونات ترتبط بالفرد مباشرة. (القنوبية،2024، ص590)

وعلى المستوى التشريعي، تبدو بوادر تأثر مفهوم الحقّ في الخصوصيّة الرقميّة بالخصائص المميزة للذكاء الإصطناعيّ جليّة فيما أتى به القانون الأوروبي المتعلق بالذَكاء الإصطناعيّ (2024)، وكذلك المادة 4 (1) من اللائحة رقم 2016/679 (EU)، والتي ذهبت إلى تعريف البَيانات الشخصيّة الرقميّة على أنها أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد، ويُعتبر الشخص الطبيعي قابلًا للتحديد إذا كان يُمكن تحديده، سواء بشكل مباشر أو غير مباشر، خاصةً عبر الإشارة إلى معرف مثل الاسم، رقم الهوية، بيانات الموقع، معرف عبر الإنترنت، أو عبر عامل أو أكثر محدد للهوية الجسدية، الفسيولوجية، الجينية، العقلية، الاقتصادية، الثقافية أو الاجتماعية لذلك الشخص، كما ويُبرز هذا التعريف النطاق الواسع للمعلومات التي يُمكن اعتبارها شخصية، (European Union. (2016). General Data Protection Regulation (GDPR) Article 4).

ومن جهة أخرى، يُعتبر هذا التعريف المشار له أساسيًا لفهم كيفية تطبيق اللائحة على مختلف البَيانات والسياقات، ويُساعد في تحديد الإجراءات والتدابير اللازمة لحماية البَيانات الشخصيّة، وضمان التعامل معها بطريقة قانونية وآمنة بما يتلائم مع خصائص أنظمة الذَكاء الإصطناعيّ، ويظهر هنا جلياً بأن هذه اللائحة تشدد على أهمية الشفافية والمساءلة في جميع العمليات التي تتضمن البَيانات الشخصيّة، مما يُعزز حقّوق الأَفراد ويُمكّنهم من السيطرة على معلوماتهم الشخصيّة، وهذا نشأ لضمان التوازن في العلاقة بين إيجابيات الذَكاء الإصطناعيّ وخصائصه القادرة على الوصول للبيانات الرقميّة وتحليلها والتصرف بها من جهة، وحقّ الأَفراد في الخصوصيّة الرقميّة لبياناتهم من جهة أخرى (Hoofnagle et al., 2019).

الفرع الثاني: مظاهر الاعتداء على الخصوصيّة الرقميّة باستخدام أنظمة الذَكاء الإصطناعيّ

تُعتبر التقانات المتطوّرة في مجال الذَكاء الإصطناعيّ من العوامل المؤثرة بشكل كبير في مختلف القطاعات، حيث تسهم في تحسين الكفاءة وتعزيز الابتكار، ومع ذلك، فإن هذه التقنيات تحمل في طياتها تحديات جمة، خاصةً فيما يتعلق بالجرائم الإلكترونية وحماية الخصوصيّة الرقميّة. (الدسوقي، 2021، ص 1156)، ولا تنفصل هذه المَخاطر في جوهرها عن حقّ الإنسان في الأمان على نفسه وفي حرمة حياته الخاصة، وهي تتفرع بالضرورة عن مجموعة القيم الإنسانية المتصلة بالكرامة كأساس للحقّوق الدستوريّة جمعاء.

وفي هذا الإطار، يمكن للذكاء الاصطناعي أن يُسهم في تحقّيق مَخاطر متعددة على الحقّ في الخصوصيّة الرقميّة على وجه الخصوص، مثل سرقة الهوية، والمراقبة غير المبررة، كما تتحقّق العديد من المخاوف عند مجرد التفكير بطرق تخزين بيانات الأفراد، وآليات استخدامها، وأماكن تخزينها، والأطراف التي لها حقّ الحصول عليها، الأمر الذي يدفع إلى التفكير الجدي بالحاجة إلى تطوير إرشادات أخلاقية وتبني أفضل الممارسات لتقليل التخوفات (Sher & Benchlouch, 2023).

وعليه، يمكن إجمال المظاهر المحتملة من الاعتداء على الحقّ في الخصوصيّة الرقميّة،

1. **تعقب حركة الانسان:** أمام الانتشار الواسع الأنترنت الأشياء التي جعلت البيوت والمدن ذكية، واستعمال الرجل الآلي للمساعدة في البيت أو المراقبة والحراسة، سيجعله على اتصال مباشر بالمعطيات الشخصيّة، والشيء نفسه بالنسبة للتطبيقات الذكية للهاتف الذكي والمركبات والطائرات ذاتية القيادة التي تقوم بتجميع المعلومات الشخصيّة، لوجود وحدات المعالجة أو الشريحة اللصيقة بالأشياء المتصلة بالإنترنت أو بالرجل الآلي التي ستكون مخزنا لما يتم التقاطه من صور وأصوات وتصرفات. فتلك

المعلومات سيتم تخزينها في ذاكرة الذَكاء الإصطناعيّ مكونه الأول والمسماة بالذَكاء السالب، ليتم فيما بعد تحليله، ثم معالجتها وتحليلها لاتخاذ الذَكاء عن طريق المكون الثاني وهو الاستدلال الصناعي القرار المناسب. كما يمكن تخزينها عن طريق الحوسبة السحابية بمعنى ً من المعطيات وفي مجالات عدة. ثم إرسالها لشبكة الشبكات التي تجمع عدد كبيراً من المعلومات (كريم، 2023).

2. **قرصنة واختراق شبكات المنازل الذكية والمواقع الإلكترونية:** إذ أن تزايد اتصال الأشياء بالإنترنت سيوفر بنية تحتية مثالية لمراقبة الإنسان، كما أن تلك المعلومات سوف لن تبقى ملكا لأصحابها، بل تتدخل الإنترنت فيها فمن يريد فتح باب منزله الذكي سيقوم بإرسال أمر عبرها من فتلك الأشياء هاتفه الذكي للخدمة السحابية المسؤولة عن قفل الباب لتقوم بفتحه المتصلة بالإنترنت لن تبقى مجرد أشياء عادية بل تتحول لأشياء ذكية تتحصل على معلومات عن كل ما يحيط بها وعن نشاط مستعملها واستعمالاته لها مع تجميع معلوماته الخاصة، وهو ما يمكن فيما بعد لمسيري تلك الأشياء استرجاع تلك المعلومات دون إمكانية متابعتهم باعتبارهم مسؤولين عن معالجة المعطيات ومن جهة ثانية فالهجمات الإلكترونية عبر الإنترنت يعد خطر عالمي الخاصة لإمكانية التحكم في البَيانات من الاختراق، مع التحكم أيضا في المركبات والطائرات ذاتية القيادة (كريم، 2023).
3. **نشر البَيانات وتوزيعها:** إذ يمكن لأنظمة الذَكاء الإصطناعيّ نشر الكثير من البنات الرقميّة للأفراد التي لا يرغبون بنشرها، ويكون ذلك من المسائل التي تنال من كرامتهم أيضاً، ويمكن أن يشكل أيضا تزويد البَيانات الرقميّة إلى جهات لا يرغب الفرد بتزويدها له من المسائل التي تنال من حقّه في الخصوصيّة الرقميّة.

وفي حقّيقة الأمر، تبدو المَخاطر التي تنجم عن استخدامات الذَكاء الإصطناعيّ متنوعة ومتعددة، وهي تتفاوت في درجة خطورتها عل الحقّوق بما فيها الحقّ في الخصوصيّة، لذلك، فإنّ هذه المَخاطر تخضع لمعايير وتدابير تشريعية مختلفة تبعا لهذا، فإن القانون الأوروبي للذكاء الإصطناعيّ قد ذهب إلى تصنيف أنظمة الذَكاء الإصطناعيّ إلى ثلاث فئات من المَخاطر: غير مقبولة، عالية، أو منخفضة (المادة 5 من القانون الأوروبي للذكاء الإصطناعيّ).

المبحث الثاني: الأطر التشريعية الناظمة لحماية الحقّ في الخصوصيّة الرقميّة في عصر الذَكاء الإصطناعيّ

تتعدد أطر الحِماية التشريعية لهذا الحقّ وتتنوع بين حماية دستورية وحماية دولية، وبين حماية جنائية أو تنظيمية، وفي هذا المبحث، سوف نتناول الأطر التشريعية الناظمة لحماية الحقّ في الخصوصيّة الرقميّة في عصر الذَكاء الإصطناعيّ من خلال المطلبين التاليين:

المطلب الأول: الحِماية والدستوريّة والدوليّة للحقّ في الخصوصيّة الرقميّة

يعتبر الإطار الدستوريّ الوطني هو الإطار الأول الذي يفترض فيه أن يوفّر الحِماية للحقّ في الخصوصيّة بشكل عام، والخصوصيّة الرقميّة على وجه الخصوص، باعتبارها إحدى مكونات الحقّ بالخصوصيّة وحرمةِ الحياةِ الخاصّةِ المحمية دستورياً، وتتعزز هذه الحِماية الدستوريّة بما جاءت به الحِماية الدوليّة من مواثيق وإعلانات ومبادئ توجيهية بالخصوص، وفي هذا المطلب، وبغية دراسة الحِماية والدستوريّة والدوليّة للحقّ في الخصوصيّة الرقميّة، فإننا سوف نقسمه إلى الفرعين التاليين:

الفرع الأول: الإطار الدستوريّ الناظم لحماية الحقّ في الخصوصيّة الرقميّة

إن وتيرة الاعتماد على التكنولوجيا وتحديداً تكنولوجيا الذَكاء الإصطناعيّ (AI) في ازدياد غير مسبوق، ويأتي ذلك استجابة إلى ضرورات ومقتضيات العصر الحديث؛ ذلك أنّ الاعتماد المتنامي على هذا النوع من التكنولوجيا أصبح أمرا واقعا وضرورة ملحة ينظر إليه البعض بأنه سيشكل تحولا جذريا في وجه هذه المجالات، إلى جانب وجود تحول من قبل الدول في الاعتماد على الذَكاء الإصطناعيّ في المجالات الأمنية والتي ينظر إليها كوسائل أكثر فاعلية في تكريس الحالة الأمنية داخل الدولة، وتعتمد الدول في الوقت الراهن وأكثر من أي وقت مضى على القدرات التكنولوجيّة لتحقّيق غايات ذات بعد أمني، أي في عملية السيطرة وحفظ الأمن داخل حدودها، وأحيانا خارج تلك الحدود.

في هذا الإطار، تسعى الدساتير إلى توفير حماية متكاملة للحقّوق الدستوريّة المختلفة، وينظم الإطار الدستوريّ العلاقة بين هذه الحقّوق بما يكفل التوازن بينها ويحيل إلى القوانين العادية صلاحية تنظيم هذه الحقّوق بغية إسباغ حماية فاعلة لها، وقد تكرّس الحقّ في الخصوصيّة بشكل متواتر في الإطار الدستوريّ الفلسطيني وكذلك الأردني، إلا أن الخصوصيّة الرقميّة كمفهوم مستحدث لا زال محل اجتهاد فقهي وقضائي في مدى توافر هذه الحِماية لها في مواجهة التحديات التي تفرضها استخدامات الذَكاء الإصطناعيّ وتطبيقاته.

في فلسطين، تكفّل القانون الأساسي بحماية الحقّ في حرمةِ الحياةِ الخاصّةِ وذلك طبقاً لما تنص عليه المادة (32) منه، ولم تحدد هذه المادة نطاق حرمةِ الحياةِ الخاصّةِ، تاركة للمشرّع العاديّ تحديد نطاقها والحِماية الجنائيّة الواجبة لها، وهو ما نرى أنه من المسائل الإيجابيّة التي قد تمّكن المشرع العاديّ أن يشمل بالحِماية الحقّ الخصوصيّة الرقميّة في نطاق الحِماية الدستوريّة التي وفرّتها المادة 32 المشار لها.

وعلى ذات النحو، حرص الدستور الأردني على حماية حقّ الأردنيين في حرمةِ الحياةِ الخاصّةِ، وذلك بمقتضى الفقرة (2) من المادة (7) منه، ويبدو جليّا أن هذه المادة لم تحدد نطاق الحقّ في حرمةِ الحياةِ الخاصّةِ أيضاً كما هو الحال في فلسطين، وهو ما نراه أيضاً من المسائل الإيجابيّة التي تمكّن المشرع العادي من أن يتناول بالحِماية الحقّ الخصوصيّة الرقميّة في نطاق الحِماية الدستوريّة (الدستور الأردني لسنة 1952، الأردن، 1952).

وعلى الرغم من توافر الحِماية الدستوريّة للحقّ في الخصوصيّة بوجه عام في غالب الدساتير، وعلى النحو المشار له في فلسطين والأردن، فإن الحِماية الدستوريّة للحقّ في الخصوصيّة يجب أن لا تكون قاصرة عن مواكبة التطورات التكنولوجيّة في عصر الذَكاء الإصطناعيّ، وبما يحقّق الفوائد الإيجابية من هذه التطورات، على أن لا تكون على حساب الحقّوق والحريات والعامة، وفق موازنة دستورية تقوم على إيلاء الاعتبار بالدرجة الأولى للحقّوق الدستوريّة، وبغية فرض رقابة فاعلة على تحقّق ذلك، فإن المحاكم الدستوريّة يجب أن تفرض رقابتها على مدى دستورية أي تشريع يتيح انتهاك الخصوصيّة الرقميّة، سيما في مجال محاولة السلطات العامة في الكثير من الأحيان، والشركات الخاصة أيضاً، على اتخاذ إجراءات في سياق محاولة بسط رقابتها على خصوصية الأفراد الرقميّة دون تحقّق شروط التناسب والضرورة، الأمر الذي قد يزيد من قدرتها على ذلك عبر استخدام تطبيقات الذَكاء الإصطناعيّ، وهو ما يجب أن يكون أيضا من أولويات الحِماية الدستوريّة لهذا الحقّ، ومحط اهتمام أنظمة الرقابة الدستوريّة.

وفي هذا الإطار، تناولت المحكمة الدستوريّة المصريّة وبوجه خاص أثر الأدوات العلمية الحديثة وتطوراتها على الحقّ في الخصوصيّة، وذهبت إلى ما هو أبعد من ذلك حين تحدثت عن قدرة هذه الوسائل على اختراق أدق التفاصيل اليومية للإنسان، وتحديداً ببياناتهم الشخصيّة كما ورد في صريح حكمها، الأمر الذي يلحقّ بالأفراد ضرراً فادحا وبخصوصياتهم على وجه التحديد، واعتبرت أن ذلك يشكل خرقاً للحقّ في الخصوصيّة لتعلقه بنطاق المسائل الشخصيّة التي ينبغي كتمانها، وأشارت المحكمة على نحو صريح إلى شمول ذلك بالحقّ في حرمةِ

الحياةِ الخاصّةِ على الرغم من أن هذه الدساتير بعض الوثائق الدستوريّة لا تتعترف بهذا الحقّ على نحو صريح (مصر، المحكمة الدستوريّة، دستوري رقم 23 لسنة 16 قضائية، 18، 3، 1995).

تجدر الإشارة إلى أنه وكاستجابة للحماية الدستوريّة للحقّ في الخصوصيّة الرقميّة، أصدر مجلس الوزراء الفلسطينيّ قراره رقم (3) لسنة 2019 بخصوص البَيانات الشخصيّة للمواطنين، والذي حظر بموجبه استخدام البَيانات الشخصيّة الخاصة بالمواطنين الذين يتلقون الخدمة من قبل الشركات والمؤسسات لأغراض تجارية، سواء أكان مساساً مباشر أو غير مباشر دون الحصول على إذن مسبق منهم.

ويُعد هذا القرار خطوة مهمة في تعزيز الحِماية المقرة للبَيانات الشخصيّة للمواطنين في فلسطين، غير أن هذا القرار جاء قاصراً في عدم التحديد الواضح للبيانات الشخصيّة: قد يؤدي عدم وجود تعريف دقيق لما يُعتبر "بيانات شخصية" إلى تفسيرات متباينة وربما استغلال الثغرات، وافتقر إلى آليات مراقبة وتنفيذ أكثر فعالية: قد لا تكون الإجراءات الرقابية والعقوبات المنصوص عليها كافية لضمان الامتثال الكامل للقرار.

الفرع الثاني: الحِماية الدوليّة للحقّ في الخصوصيّة الرقميّة

أسهمت المواثيق الدوليّة بشكل ملحوظ ولا زالت في تعزيز الحِماية الدستوريّة للحقّ في الخصوصيّة، فعلى سبيل المثال، تُشدد المادة (12) من الإعلان العالميّ لحقّوق الإنسان على ضرورة حماية الأَفراد من أي تدخلات غير قانونية في حياتهم الخاصة، الأسرية، أو مساكنهم. بالمثل، تُؤكد الماد (17) من العهد الدولي للحقّوق المدنية والسياسية على عدم شرعيّة التدخلات التعسفيّة في خصوصيّة الأَفراد.

وتتمتع المواثيق الدوليّة هذه بصفة ملزمة حال المصادقة عليها وإدخالها في النظام القانوني الداخلي، بما يعزز من الحِماية الدستوريّة للحقّ في الخصوصيّة، ومن أبرز أمثلة هذه القرارات هو قرار الجمعية العامة للأمم المتحدة رقم (68\167) وتقرير مكتب المفوض السامي لحقّوق الإنسان للعام 2014 أيضاً (سلمودي. ر. و ربايعة. ل. والرزي. ه. وبراهمة.ع، 2017)، وينسحب ذلك على المواثيق الإقليمية، ومن ذلك اتفاقية 108 لمجلس أوروبا، واللائحة العامة لحماية البَيانات (GDPR) في عام 2018 (Bouton, 2021 107-109)، والتي تهدف إلى ضمان سرية وأمان البَيانات الشخصيّة وحمايتها (Burgess, 2023, p. 87).

وفي العام 2015، كان مجلس حقّوق الإنسان في الأمم المتحدة قد أنشأ الولاية الأولى بشأن الخصوصيّة بموجب قراره رقم 16/28. وطلب من المقرر الخاص أن يلتمس معلومات موثوقة من الحكومات وأي طرف آخر على اطلاع على الحالات والقضايا المتعلقة بالخصوصيّة (A/HRC/RES/37/2).

إلا أن التطور الأبرز في حراك مجلس حقّوق الإنسان فيما يتعلق بحماية الحقّ في الخصوصيّة الرقميّة على وجه التحديد ظهر خلال جائحة مرض فيروس كورونا (كوفيد–19)، حيث جُمعت بيانات عن ملايين الأشخاص في جميع بلدان العالم لغاية لمكافحة الجائحة، الأمر الذي أثار أسئلة مشروعة حول مآل البَيانات الشخصيّة لملايين الأشخاص التي جمعت لمكافحة جائحة كوفيد–19، وهل سيتم حذفها أو وهل سيتم تجهيل هوية أصحابها؟ وهل من الممكن أن تستخدم لغايات أخرى غير التي جمعت من أجلها؟

ولأجل الإجابة عن هذه التساؤلات، وضعت المقررة الخاصة المعنية بالحقّ في الخصوصيّة السيدة (آنا بريان نوغريرس) تقريرها في العام (2023) البَيانات الشخصيّة التي جمعتها الكيانات العامة خلال جائحة (كوفيد19)، وقد خلص التقرير إلى أنه لا يجب أن تتم معالجة البَيانات حصراً لتحقّيق غاية محددة ومشروعة فقط، بل يجب أن تكون مقيدة بإطار زمني لازم تحقّيق الغاية المشروعة من معالجة هذه البَيانات، وأنه يتوجب بعد الانتهاء من تحقّيق الغاية المنشودة، حذف هذه البَيانات أو تجهيل أسماء أصحابها، ولا يجوز تبعا لذلك إظهار هوية أصحابها (A/HRC/52/37).

وسبق ذلك قيام الأمين العام للأمم المتحدة مذكرة إحالة حول تقرير المقررة الخاصة المعنية بالحقّ في الخصوصيّة في العام (2022) مشيراً إلى المبادئ التي تستند إليها الخصوصيّة وحماية البَيانات الشخصيّة باعتبارها جزءا هيكليا من النظم القانونيّة ذات الصلة بهذا الموضوع لأنها تؤدي وظيفة مزدوجة، وهي تفسير وإدماج الإطار التنظيمي، وباعتبارها من أكثر الوسائل قيمة وفائدة للمتحكمين في البَيانات ومعالجي البَيانات الذين يسعون إلى معالجة صحيحة للمعلومات الشخصيّة، لا سيما عند مواجهة مَخاطر إساءة استخدام تكنولوجيات المعلومات والاتصالات، كما تضمنت الإحالة تحليلاً على وجه الخصوص لمبادئ القانونيّة والشرعية والمشروعية، والموافقة، والشفافية، والغرض، والإنصاف، والتناسب، والتقليل إلى أدنى حد، والجودة، والمسؤولية، والأمن، باعتبار أن هذه المبادئ تشكل أسس النظام القانوني للخصوصية وحماية البَيانات الشخصيّة برمته، كما أجرت المذكرة المحالة دراسة مقارنة وفقا لصياغة المبادئ الواردة في سبع وثائق تنظيمية دولية، وسبل مواجهة التحديات المتمثلة في حماية الخصوصيّة والبَيانات الشخصيّة في العصر الرقمي (A/77/196).

وفي ذات الاتجاه، أصدر مكتب المفوض السامي لحقّوق الإنسان في العام 222 تقريراً حول الحقّ في الخصوصيّة في العصر الرقمي عملاً بقرار مجلس حقّوق الإنسان 4/48، وقد ناقش هذا التقرير الاتجاهات والتحديات الأخيرة المتعلقة بالحقّ في الخصوصيّة. وركز التقرير، بوجه خاص، على ما يلي: (أ) إساءة استخدام أدوات الاختراق الحاسوبي الاقتحامية؛ (ب) الدور الرئيسي للتشفير في ضمان التمتع بالحقّ في الخصوصيّة وغيره من الحقّوق؛ (ج) تفشي رصد الأماكن العامة، وسلط الضوء على خطر إنشاء نظم للمراقبة والرقابة الشاملة التي قد تقوض تنمية مجتمعات نابضة بالحياة تحترم الحقّوق(A/HRC/51/17).

ومع أهمية هذه التقارير، غير أن التطور الأهم في إطار الحِماية الدوليّة للحقّ في الخصوصيّة من مَخاطر الذَكاء الإصطناعيّ كان قد تجّسد في تقرير المقرر الخاص المعني بالحقّ في الخصوصيّة السيد (جوزيف كاناتاشي) الصادر في العام (2021)، والمتعلق بالذَكاء الإصطناعيّ والخصوصيّة، وخصوصية الأطفال، وقد تضمن هذا التقرير توصيفات دقيقة لمَخاطر الذَكاء الإصطناعيّ على الحقّ في خصوصية البَيانات، واقترح العديد من الحلول والمسؤوليات في هذا الإطار بما يشكل إطار مرجعي هام لتوفير الحِماية القانونيّة والدوليّة للحقّ في خصوصية الأفراد الرقميّة (A/HRC/46/37).

وتعتبر جميع هذه التقارير بمثابة مبادئ توجيهية للحكومات والجهات الفاعلة بغية تعزيز حماية الحقّ في الخصوصيّة بشكل عام، والخصوصيّة الرقميّة بشكل خاص، من مَخاطر استخدام تقنيات الذَكاء الإصطناعيّ.

المطلب الثاني: الحِماية الجنائيّة للحقّ في الخصوصيّة الرقميّة في الأردن وفلسطين والقانون الأوروبي

لم يصدر المشرع الفلسطيني أو الأردني تشريعات ناظمة للمسائل الجزائية المتعلقة باستخدام تقنيات الذَكاء الإصطناعيّ، في حين أصدر البرلمان الأوروبي في مارس (2024) أول قانون رئيسي لتنظيم الذَكاء الإصطناعيّ، والذي سيدخل حيز التنفيذ في نهاية الدورة التشريعية في مايو (أيار) 2024، وبغية البحث في الحِماية الجنائيّة للحقّ في الخصوصيّة الرقميّة في الأردن وفلسطين والقانون الأوروبي، فإننا سوف نقسم هذا المطلب إلى الفرعين التاليين:

الفرع الأول: الحِماية الجنائيّة في القانونين الأردني والفلسطيني

تتولى التشريعات الجزائية توفير الحِماية لسلامة الأفراد من خلال تحقّيق الردع العام والخاص، وينسحب لك على كافة الحقّوق الدستوريّة المتنوعة، فإذا كانت هذه التشريعات تحمي الحقّ في سلامة الجسد على سبيل المثال، فإنّها أيضا تحمي الحقّوق المعنوية المتصلة بحقّ الإنسان في الأمان على خصوصياته المرتبطة به وبعائلته، ومن ذلك الحقّ في الخصوصيّة على وجه العموم، والخصوصيّة الرقميّة على

نحو خاص، وقد بات من الجليّ أن التطورات الهائلة في المجال التكنولوجي في العقود الأخيرة قد دفعت نحو تغيير التفاعل الاجتماعي والمتغيرات السلوكية التفاعلية للأفراد على نحو ساهم بشكل كبير في تزايد وتصاعد جرائم الإنترنت.

وفي هذا الإطار، يشكل النمو السريع لاستخدامات تقانات الذَكاء الإصطناعيّ، وارتباط هذه الاستخدامات بشبكات الانترنت والفضاء السيبراني فرصة مواتية وجديدة وغير مسبوقة للراغبين في مخالفة القانون بواسطة هذه التقانات التي لا يستطيع الفرد العادي حماية نفسه وخصوصياته الرقميّة من آثارها، الأمر الذي بات يشكل بما يشكل تهديداً حقّيقياً وجدياً للعدالة والقانون (مصطفى، أبو عنزة، 2023)، ومن المتوقع على ضوء ذلك أن تتزايد الجرائم الإلكترونية بواسطة أنظمة الذَكاء الصناعي في ظل شيوع استخدام هذه الأنظمة في ظل القصور التشريعي على مواكبة هذا النوع من الجرائم، وتعدّ الحِماية الجنائيّة للحقّ في الخصوصيّة الرقميّة من أكثر الحمايات القانونيّة التي ينبغي أن تكون محلّ رعاية المشرع العادي لمواكبة التطورات السريعة والمتلاحقّة في أنظمة الذَكاء الإصطناعيّ التي يمكن لها أن تكون أداة طيّعة لارتكاب جرائم إلكترونية تنال من الحقّ في الخصوصيّة الرقميّة وتعتدي عليها.

فلسطينياً، لم تواكب التطورات التشريعية في مجال القانون الجنائي ما انتهت إليه الجرائم الناتجة عن استخدام التقانات والتطبيقات المختلفة للذكاء الإصطناعيّ، غير أن القرار بقانون بشأن الجرائم الإلكترونية قد ذهب إلى النص على تجريم التدخل التعسفي وغير القانوني في خصوصيات الأشخاص وفق ما أتت به المادة (22) منه، وكذلك حظرت الفقرة (2) من هذه المادة النشر بأي وسيلة إلكترونية كانت وعلى أية صورة لبيانات تؤدي بالنتيجة إلى تدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد. (قرار بقانون بشأن الجرائم الإلكترونية، فلسطين، 2018).

ويرى الباحث أن ما يمكن استقرائه من أركان جرمية لازمة لتحقّق الجريمة الإلكترونية تنطبق على استخدام تطبيقات الذَكاء الإصطناعيّ أيضاً، طالما تم اقتراف الجريمة بواسطة (الوسائل التكنولوجيّة) وكانت مرتبطة إلكترونياً بأحد أنظمة الذَكاء الإصطناعيّ، سيما وأن الذَكاء الإصطناعيّ وأنظمته تقوم بشكل محوري على استخدام كافة المعطيات الإلكترونية في الوصول للبينات الرقميّة للأفراد، وهنا تتحقّق أركان جريمة انتهاك الخصوصيّة الرقميّة للأفراد إذا تم استخدام الذَكاء الإصطناعيّ كأداة جريمة.

وفي الأردن، نجد أن قانون الجرائم الإلكترونية الأردني لم ينص صراحة على حظر الاعتداء على الخصوصيّة بواسطة الوسائل الإلكترونية كما فعل المشرع الفلسطيني، غير أن المادة 20 فقرة (أ) من هذا القانون قد جرّمت القيام (بواسطة وسيلة الكترونية) بتسجيل أو صورة أو فيديو لما يحرص الشخص على صونه، أو عدم اظهاره، وكذلك كتمانه عن العامة، الأمر الذي يعزز من انصراف قصد المشرع الأردني في هذه المادة لحماية الخصوصيّة بالإشارة إلى استخدام حرص الشخص على صون بياناته، ومعلوماته الشخصيّة الرقميّة (قانون الجرائم الإلكترونية، الأردن، 2024).

وإذا كان المشرع الفلسطيني قد ذهب على نحو صريح إلى تجريم التدخلات التعسفية وغير القانونيّة في خصوصيات الأفراد بأي وسيلة إلكترونية كانت، فإنه قد عمد أيضا إلى تجريم فعل اعتراض البَيانات أو التصنت عليها، وذلك وفق ما ذهبت إليه المادة (7) من قرار بقانون الجرائم الالكترونية، والتي يمكن أن يكون الذَكاء الإصطناعيّ وأنظمته أداة الجريمة في هذه الحالة.

وفي هذا الإطار، فإنّ المشرع الأردني كان أكثر وضوحاً من المشرع الفلسطيني في تجريم الاعتداء على البَيانات الرقميّة واعتراضها حين نصت المادة (7) من قانون الجرائم الإلكترونية الأردني 2024 حين وضع عقوبة على اعتراض خط سير البَيانات والعديد من الأفعال التي تتصل بذلك، ويلاحظ هنا أن المشرع الأردني قد وفّر حماية تشريعية جنائية للبيانات الرقميّة للأفراد.

وفي ذات السياق، يجد الباحث أن المشرع الفلسطيني قد جرّم فك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، وكذلك جرّم استعمال عناصر تشفير (شخصية) وذلك وفق ما نصت عليه المادة (8) من قرار بقانون الجرائم الإلكترونية الفلسطيني، إلا أنه يلاحظ بأن المشرع الأردني لم يعمد إلى تجريم فعل (فك تشفير البَيانات) كما ذهب إليه المشرع الفلسطيني، وإنما اكتفى بتجريم تشفير المواقع الإلكترونية كما ورد في الفقرة (ج) من المادة (3)، وهو ما يبّد قصوراً تشريعياُ في تجريم فعل فك شيفرة البَيانات باعتباره أحد أهم صور انتهاك الحقّ في الخصوصيّة الرقميّة.

وعلى الرغم من أهمية هذه الحِماية الجنائيّة التي أشرنا لها في تحليل نصوص القوانين الفلسطينية والأردنية ذات الصلة، إلا أنه تنبغي الإشارة إلى أنّ الذَكاء الإصطناعيّ يتميز بالاستقلال الوظيفي في تأدية مهامه دون تحكم بشري نشط أو حتى إشراف مباشر من قبل شخص ما، ويؤدي ذلك إلى أن تكون أفعال الذَكاء الإصطناعيّ غير قابلة للتوقع نظراً للتلقائية في تفكيره وتصرفاته، (لخضر، معوش،2023)، الأمر الذي يثير أسئلة مشروعة حول مدى توافر القصد الجنائي في الجرائم الناشئة عن الذَكاء الإصطناعيّ ومدى تأثر هذه الاستقلالية على توافر القصد المعنوي للمتهم (الإنسان) كأحد اهم أركان الجرائم القصدية، ومدى توافر المسؤولية الجنائيّة عن تصرفات الآلة التي قد تدير نفسها بشكل مستقل عن إرادة البشر، بما يؤدي يثير إشكاليات قانونية في مجال التطبيق القضائي تتعلق بمدى توافر أركان الجرائم الإلكترونية المقترفة بواسطة الذَكاء الإصطناعيّ وفقاً لمبدأ شرعية الجرائم كمبدأ دستوري.

وعلى الرغم من هذه الإشكالات القانونيّة المتوقعة في التطبيق القضائي، يرى الباحث أن الجرائم الالكترونية في الكثير من جوانبها يمكن الاعتماد عليها في تجريم الأشخاص المسؤولين عن إدارة آلة الذَكاء الإصطناعيّ، سيما تلك الآلة التي تستخدم الأنظمة التي يمكن لها أن تعتدي على الحقّ في الخصوصيّة الرقميّة، سيما وأن محل الجريمة في هذه الأحوال في الغالب قد يكون بإشراف بشري أو صنيعة بشر يتوافر لديه القصد الجنائي.

الفرع الثاني: الحِماية الجنائيّة للحقّ في الخصوصيّة الرقميّة في القانون الأوروبي للذكاء الإصطناعيّ

أصدر البرلمان الأوروبي في مارس (2024) أول قانون رئيسي لتنظيم الذَكاء الإصطناعيّ، والذي سيدخل حيز التنفيذ في نهاية الدورة التشريعية في مايو (أيار) 2024، بعد اجتياز الفحوصات النهائية والحصول على موافقة من المجلس الأوروبي، حيث سيتم تنفيذه على مراحل ابتداءً من عام 2025.

ويعتمد هذا التشريع على تقييم المَخاطر على الأمان والحقّوق الأساسية نتيجة استخدام الذَكاء الإصطناعيّ. ويصنّف تبعاً لذلك أنظمة الذَكاء الإصطناعيّ إلى ثلاث فئات من المَخاطر: غير مقبولة، عالية، أو منخفضة.

وفي هذا الإطار، تعالج المادة 5 في الفقرة 1.ب مكرر القيود المفروضة على استخدام أنظمة الذَكاء الإصطناعيّ التي تقوم بتحليل البَيانات البيومترية للأفراد بهدف تصنيفهم أو الاستدلال على خصائص شخصية حساسة مثل العرق الاثنيّ، أو الرأي السياسي، أو الانتماء النقابي، أو المعتقدات الدينيّة، أو الفلسفية، أو التوجه الجنسي (القانون الأوروبي للذكاء الإصطناعيّ، 2024)

كما تحظر المادة (5.1. ج) من هذا القانون تسويق أو تشغيل أو استخدام أنظمة الذَكاء الإصطناعيّ التي تقوم بتقييم أو تصنيف الأشخاص الطبيعيين أو مجموعات منهم على أساس سلوكهم الاجتماعي، أو خصائصهم الشخصيّة المعروفة، أو المستنتجة، أو المتوقعة على مدى فترة زمنية معينة، رغم أنها سمحت ببعض الاستثناءات في حالات الضرورة القصوى، مثل الحالات التي تتطلب تدخلًا سريعًا لحماية الأمن العام أو منع الجرائم الخطيرة. ومع ذلك، يجب أن يكون هذا الاستخدام محدودًا ومنظمًا بشكل صارم من خلال الإشراف القضائي أو الإداري، يجب أن تكون هذه الاستثناءات مدرجة بوضوح في القوانين الوطنية لضمان الشفافية والمساءلة ولتجنب الاستخدام التعسفي للتقنيات.

ويلاحظ هنا أن هذا الحظر قد اقترن بعقوبة جزائية وفقاً للمادة 71 من قانون الذَكاء الصناعي في الفقرة الثالثة والتي نصت على أنه يخضع عدم الامتثال لحظر ممارسات الذَكاء الإصطناعيّ المشار إليها في المادة 5 لغرامات إدارية تصل إلى 35.000.000 يورو، أو، إذا كان المخالف شركة، تصل إلى 7٪ من إجمالي مبيعاتها السنوية في جميع أنحاء العالم للسنة المالية السابقة أيهما أعلى."

ويرى الباحث في هذا السياق بأن هذا القانون وإن كان يتسم بالصفة التنظيمية، إلا أنه وحين أقرّ عقوبات جزائية مالية على محالفة أحكام المادة (5) منه فإنه يكون قد جنح أيضا إلى اتخاذ سمة القوانين الجنائيّة في التجريم والعقاب.

كما فرضت المادة 71 الفقرة الرابعة من هذا القانون عقوبات مالية المفروضة على عدم الامتثال للأنظمة المتعلقة بمشغلي أو الهيئات المخطرة لأنظمة الذَكاء الإصطناعيّ والتي قد تصل إلى 15 مليون يورو، وإذا كان المخالف شركة، يمكن فرض غرامة تصل إلى 3% من إجمالي الدورة المالية السنوية العالمية للشركة للسنة المالية السابقة، أيهما أعلى.

هذا يعني أن الشركات التي تخالف القواعد المتعلقة بأنظمة الذَكاء الإصطناعيّ قد تواجه عقوبات مالية كبيرة تعكس جدية القوانين في تنظيم استخدام هذه التكنولوجيا وضمان الامتثال للمعايير المحددة، ويبدو جلياً أن الهدف من هذه الغرامات هو تحفيز الشركات على الالتزام بالقوانين وتجنب الممارسات التي قد تعرض الصحة أو الأمان أو الحقّوق الأساسية للأشخاص للخطر.

أما فيما يتعلق ببعض أنظمة الذَكاء الإصطناعيّ التي تُعتبر أنها تشكل خطرًا منخفضًا أو معتدلة فقط، تخضع ببساطة لـــ "التزامات الشفافية". في هذا الإطار، يتم تحديد عدة أنظمة للذكاء الإصطناعيّ: تلك المُعدة للتفاعل مع البشر وتلك التي تولد أو تتلاعب بالصور أو المحتويات الصوتية أو الفيديو. كما تشمل الأنظمة المعنية بالتعرف على العواطف، أو تصنيف الفئات الاجتماعية. بالنسبة لهذه الأنظمة، توضح الاقتراح أنه يجب إبلاغ المستخدمين بأنهم يتفاعلون مع نظام للذكاء الإصطناعيّ. (المادة 52 من قانون الذَكاء الصناعي).

وفي هذا السياق، يبدو جلياً أن قوانين الجرائم الإلكترونية في فلسطين والأردن، لا تحقّق تلك الشرعية التي جاء بها القانون الأوروبي للذكاء الإصطناعيّ في مجال الحِماية الجنائيّة لخصوصيات الأَفراد الناشئة عن استخدام تطبيقات الذَكاء الإصطناعيّ، الأمر الذي يطرح تساؤلات حول إمكانية تبني المشرعين الفلسطيني والأردني لقانون خاص بالذَكاء الإصطناعيّ على غرار القانون الأوروبي.

خاتمة الدراسة

بدى واضحاً من خلال هذه الدراسة أن مفهوم الحقّ في الخصوصيّة الرقميّة قد انبثق عن المفهوم العام للخصوصية وحرمةِ الحياةِ الخاصّةِ بوجه عام، وقد نشأت الحاجة لهذا المفهوم المتخصص في ظل تطور استخدامات الذَكاء الإصطناعيّ، لتوفير لحماية الكاملة لبيانات الأَفراد، زفي هذا الإطار، ساهم تميز أنظمة الذَكاء الإصطناعيّ واقترانها بخصائص متعددة أهمها القدرة على النفاذ الى البَيانات الرقميّة بسهولة إلى نشوء تهديدات جدية على حقّ الأَفراد في الخصوصيّة، وفي قدرته الهائلة على جمع البَيانات الرقميّة وتحليلها استخدامها بأي طريقة أو بشكل غير قانوني، وقد توصلت هذه الدراسة في هذا الإطار إلى عدة نتائج وتوصيات نعرضها فيما يلي:

أولاً: النتائج

1. حرص الإطاران الدستوريّان في فلسطين والأردن على توفير الحِماية الدستوريّة للحقّ في الخصوصيّة وحرمةِ الحياةِ الخاصّةِ بوجه عام، ولم يتم النص بشكل صريح على الخصوصيّة الرقميّة، إلا أن النصوص الدستوريّة ذات الصلة تركت للمشرع العادي تحديد نطاق ومفهوم الحقّ في الخصوصيّة الرقميّة.
2. تتعزز الحِماية الدستوريّة للحقّ بالخصوصيّة بما جاءت بها المصادر الدوليّة من إعلانات وقرارات ومواثيق ومبادئ توجيهية.

3. وفّرت التشريعات الجزائية في فلسطين والأردن الحِماية الجنائيّة للحقّ في الخصوصيّة الرقميّة في إطار(الجرائم الإلكترونية)، إلا أنّ هذه التشريعات لم تتعرض على نحو صريح إلى الجرائم المقترفة بواسطة الذَكاء الإصطناعيّ، ومدى إمكانية انطباق أركان الجريمة الإلكترونية على تلك المرتكبة بواسطة الذَكاء الإصطناعيّ.

ثانياً: التوصيات

يوصي الباحث المشرعين الأردني والفلسطيني بما يلي:

1. تعديل النصوص الدستوريّة بالنص صراحة على توفير الحِماية الدستوريّة لحقّ الأفراد في خصوصية بيانتهم الرقميّة باعتبارها جزء أصيل من الحقّ في حرمةِ الحياةِ الخاصّةِ.
2. تعديل نصوص قوانين (الجرائم الإلكترونية) في الأردن وفلسطين بالنص صراحة على مفهوم دقيق وشامل للذكاء الإصطناعيّ واعتباره إحدى أدوات الجريمة الإلكترونية.
3. إصدار تشريع جنائي خاص في مرحلة متقدمة لتنظيم استخدامات الذَكاء الإصطناعيّ وتجريم الاعتداء على الحقّ في الخصوصيّة الرقميّة في متنها بما يتوافق مع التطورات المتسارعة في هذا الجانب.

قائمة المصادر والمراجع:

أولاً: المصادر باللغة العربية:

الوثائق الدستوريّة

- الدستور الأردني لسنة 1952، الجريدة الرسمية الأردنية، عدد (1093)، 1952/1/8.
- القانون الأساسي الفلسطيني المعدل لسنة 2003، الجريدة الرسمية الفلسطينية (الوقائع الفلسطينية)، ع (صفر)، 2003/03/19، ص 5.

القوانين والقرارات

- القانون الأوروبي للذكاء الإصطناعيّ المقرّ من قبل البرلمان الأوروبي في مارس 2024.
- قانون الجرائم الإلكترونية لسنة 2023، قانون رقم 17 لسنة 2023 (قانون الجرائم الإلكترونية لسنة 2024)، ع (5874) الجريدة الرسمية الأردنية، ع (5874)، 2023/8/13، ص3579.
- قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، ع (.)، الجريدة الرسمية الفلسطينية (الوقائع الفلسطينية)، 2018/05/03، ص 8، المعدلة تسميته إلى "قرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات بموجب المادة (1) من قرار بقانون رقم (38) لسنة 2021م بتعديل قرار بقانون رقم (10) لسنة 2018، الجريدة الرسمية الفلسطينية (الوقائع الفلسطينية)، ع (186)، 2021/12/23، ص 30.
- قرار مجلس الوزراء رقم (3) لسنة 2019 بالبَيانات الشخصيّة الخاصة بالمواطنين، ع (165)، الجريدة الرسمية، (الوقائع الفلسطينية)، 2019/6/16، ص 21.

الأحكام القضائية

- المحكمة الدستوريّة المصرية، رقم 23 لسنة 16 قضائية، 1995/3/18.

ثانياً: المراجع باللغة العربية

الكتب

- أميت. ت. (2108). الذَكاء الإصطناعيّ: نعمة أم نقمة. (ع. السلمى، مترجم). مجلة دراسات المعلومات، جمعية المكتبات والمعلومات السعودية، (21). 191 – 208، (الكتاب الأصلي نشر في العام 2016).
- الجندي، ح. (1993). ضمانات حرمةِ الحياةِ الخاصّةِ في الإسلام. ط (1). مصر: دار النهضة العربية.
- الحمصاني، ص. (1979). أركان حقّوق الإنسان، بحث مقارن في الشريعة الإسلامية والقوانين الحديثة. ط (1). لبنان: دار العلم للملايين.
- خزيمية، م. (2024). المسؤولية المدنية عن أضرار الذَكاء الإصطناعيّ. ط (1). فلسطين: الشامل للنشر والتوزيع.
- رستم، م. (1992). قانون العقوبات ومَخاطر تقنية المعلومات، ط (1). مصر: مكتبة الآلات الحديثة.

المقالات

- أحمد. أ. (2021). الحقّ في الخصوصيّة الرقميّة في إطار ثورة البَيانات وأنماط التدخلات التشريعية والدوليّة، مجلة البحوث والدراسات الإعلامية، المعهد الدولي العالي للإعلام بالشروق، (15). 9 – 48.
- بن برغوث. ل. (2023). الأمن السيبراني وحماية خصوصية البَيانات الرقميّة في الجزائر في عصر التحول الرقمي والذَكاء الإصطناعيّ: التهديدات، التقنيات، التحديات، وآليات التصدي، المجلة الدوليّة للاتصال الاجتماعي، جامعة عبد الحميد بن باديس مستغانم، كلية العلوم الإنسانية والاجتماعية، مخبر الدراسات الإعلامية والاتصالية، 10 (1). 443- 457. ص 447.
- الدسوقي، م. (2021). جرائم تقنيات الذَكاء الإصطناعيّ والشخصيّة القانونيّة الإلكترونية المستقلة. مجلة البحوث القانونيّة والاقتصادية، جامعة المنصورة، 1(1) 1140-1222.https://mjle.journals.ekb.eg/article_282445.html
- راشد، ط. ج. (2019). الحِماية القانونيّة لخصوصية البَيانات الشخصيّة في العصر الرقمي: دراسة مقارنة. مجلة القانون والاقتصاد، 92(ملحقّ خاص)، 189-314.
- سلمودي. ر. و ربايعة. ل. والرزي. ه. وبراهمة.ع. (2017). الموقف المعاصر لقواعد القانون الدولي العام من الحقّ في الخصوصيّة في العصر الرقمي، مجلة الجامعة العربية الأمريكية للبحوث، 3 (2)، 10.
- القنوبية. م. (2024، مارس، 27). تأثير الذَكاء الإصطناعيّ على خصوصية البَيانات والمستفيدين. (بحث). المؤتمر والمعرض السنوي السابع والعشرون لجمعية المكتبات المتخصصة فرع الخليج العربي: توظيف التقنيات الذكية في بيئة المكتبات المتخصصة ومؤسسات المعلومات، الدوحة: جمعية المكتبات المتخصصة، 583- 594.
- كريم، ك. (2023). حماية المعطيات الشخصيّة للشخص الطبيعي من مَخاطر الذَكاء الإصطناعيّ بموجب القانون الجزائري رقم 7 لسنة 2. مجلة جامعة الشارقة للعلوم القانونيّة، 20 (3)، (298).
- لخضر. ر، و معوش. ف. (2023). خصوصية المسؤولية المدنية عن أضرار أنظمة الذَكاء الإصطناعيّ في القانون الجزائري، مجلة طبنة للدراسات العلمية الأكاديمية، المركز الجامعي سي الحواس بريكة، 6 (1). 568 – 595.
- مصطفى. م، وأبو عنزة. أ. (2023). السياق الاجتماعي والقانوني للجريمة الإلكترونية: دراسة مقارنة بين التشريع الجزائري والأردني. مجلة "دراسات" العلوم الإنسانية والاجتماعية، الجامعة الأردنية،50(5)، 347–364.
- مهني. م. (2022). استخدام التسويق الإلكتروني لتطبيقات تكنولوجيا الذَكاء الإصطناعيّ وتحليل البَيانات الضخمة وتأثيره على الخصوصيّة في العصر الرقمي، مجلة مستقبل العلوم الاجتماعية، الجمعية العربية للتنمية والبيئية، 8 (3). 205- 264. 227.

References:

- Ahmed. A. (2021). The right to digital privacy in the context of the data revolution and patterns of legislative and international interventions, Journal of Media Research and Studies, International Higher Institute for Media in Shorouk, (in Arabic): (15). 9-48.
- Al-Desouki, M. (2021). Crimes of artificial intelligence technologies and independent electronic legal personality. Journal of Legal and Economic Research, Mansoura University, 1(1) 1140-1222. https://mjle.journals.ekb.eg/article_282445.html

- Al-Homsani, P. (1979). Modern human rights rules, compared to Islamic law and laws. I (1). Lebanon (in Arabic): House of Knowledge for Millions.
- Al-Jundi, H. (1993). Guarantees of the sanctity of private life in Islam. I (1). Egypt (in Arabic): Dar Al Nahda Al Arabiya.
- Amit. T. (2108). Artificial intelligence: a blessing or a curse? (A. Al-Salma, translator). Journal of Information Studies, (in Arabic). Saudi Public Library Association, (21). 191-208, (original book published in 2016).
- Ben Barghout. L. (2023). Cybersecurity and protecting the privacy of digital data in Algeria in the era of digital transformation and artificial intelligence: threats, technologies, challenges, and response mechanisms, International Journal of Social Communication, Abdelhamid Ben Badis University of Mostaganem, Faculty of Humanities and Social Sciences, Media and Communication Studies Laboratory, (in Arabic), 10 (1). 443- 457. p. 447.
- Bouton, J. (2021). La problématique du secret en droit du travail. In C. Baudoin, M. Boudot, & A. Gaudemet (Eds.), Le secret dans les relations de travail (pp. 121-140).
- Burgess, P. (2023). Privacy at work: Legal and ethical issues. (A. Al-Mutairi, Trans.). Riyadh, Saudi Arabia: Alukah. (Original work published 2021).
- Cabinet Resolution No. (3) of 2019 regarding personal data on citizens, Article (165), Official Gazette, (Palestinian Gazette), 6/16/2019, p. 21. (in Arabic).
- Castillo, M. (2023). The European Union: Towards Mastering Artificial Intelligence? Cahiers de la recherche sur les droits fondamentaux, (21), 99-107. https://doi.org/10.4000/crdf.8864.
- Cybercrime Law of 2023, Law No. 17 of 2023 (Cybercrime Law of 2024), Article (5874) Jordanian Official Gazette, Article (5874), 8/13/2023, p. 3579. (in Arabic).
- Decision Law No. (10) of 2018 AD regarding cybercrimes, p. (.), Palestinian Official Gazette (Palestinian Gazette), 03/05/2018, p. 8, renamed "Decision Law Concerning Cybercrimes and Communications and Information Technology Crimes in accordance with Article (1) From Decree Law No. (38) of 2021 AD amending Decree Law No. (10) of 2018, Palestinian Official Gazette (Palestinian Gazette), No. (186), 12/23/2021, p. 30. (in Arabic).
- Egyptian Constitutional Court, No. 23 of Judicial Year 16, 3/18/1995. (in Arabic).
- European Commission. (2024). Article 3 - Artificial Intelligence Act.
  Retrieved from https://artificialintelligenceact.eu/article/3/
- European Law on Artificial Intelligence approved by the European Parliament in March 2024.
- European Union. (2016). General Data Protection Regulation (GDPR), Article 4 - Definitions. Retrieved from https://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm.
- GoodTech. (2024). Cybersecurity in 2024: The New Challenges of Online Protection.
- Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union general data protection regulation: What it is and what it means. Information, Communication & Society, 22(1), 65-98.
- https://doi.org/10.1080/1369118X.2019.1573912
- https://goodtech.info/cybersecurite-en-2024-les-nouveaux-defis-de-la-protection-en-ligne/
- https://www.lemonde.fr/idees/article/2024/04/05/intelligence-artificielle-l-humain-qui-est-le-point-de-depart-de-tout-dispositif-numerique-doit-rester-le-point-d-arrivee_6226135_3232.html
- https://www.scribbr.com/apa-examples/website/
- https://www.village-justice.com/articles/encadrement-juridique-intelligence-artificielle-les-reponses-essentielles,47035.html
- Karim, K. (2023). Protecting the personal data of a natural person from the risks of artificial intelligence under Algerian Law No. 7 of 2. University of Sharjah Journal of Legal Sciences, (in Arabic): 20 (3), (298).
- Khuzaymia, M. (2024). Damage caused by industrial damage. I (1). Palestine (in Arabic): Salam Publishing and Distribution.
- Lakhdar. R., and Maoush. F. (2023). The specificity of civil liability for damages to artificial intelligence systems in Algerian law, Tabna Journal of Academic Scientific Studies, Si Hawass Barika University Center, (in Arabic): 6 (1). 568 – 595.
- Lucas, J.-F. (2024, avril 5). Intelligence artificielle: « L'humain, qui est le point de départ de tout dispositif numérique, doit rester le point d'arrivée ». Le Monde. Récupéré le [date de récupération]
- Marcellin, S. (2024). Cybersécurité et intelligence artificielle: Le paradoxe juridique. Nom du Journal ou Site Web.

- Mustafa. M, and Abu Anza. A. (2023). The social and legal context of cybercrime: a comparative study between Algerian and Jordanian legislation. Journal of Humanities and Social Sciences Studies, University of Jordan, (in Arabic): 50(5), 347–364.
- Parlement européen et du Conseil. (2023). Exposé des motifs, pt 5.2.1 de la proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle [Exposition of reasons, pt 5.2.1 of the proposed regulation establishing harmonized rules on artificial intelligence]. Journal officiel de l'Union européenne.
- Parlement européen. (2020, Août 27). Intelligence artificielle: définition et utilisation. Parlement européen. Lien vers l'article
- Professional. M. (2022). The use of electronic marketing for artificial intelligence technology applications and big data analysis and its impact on privacy in the digital age, Journal of the Future of Social Sciences, Arab Society for Development and Environment, (in Arabic): 8 (3). 205- 264. 227.
- Qanubiya. M. (2024, March 27). The impact of artificial intelligence on the privacy of data and beneficiaries. (research). The Twenty-Seventh Annual Conference and Exhibition of the Specialized Library Association, Arabian Gulf Chapter: Employing Smart Technologies in the Environment of Specialized Libraries and Information Institutions, Doha: Specialized Libraries Association, 583-594.
- Raposo, V. L. (2023). The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non‑Orwellian Draft Proposal. European Journal on Criminal Policy and Research, 29(515-533). https://doi.org/10.1007/s10610-022-09512-y.
- Rashid.T. (2019). Legal protection of personal data privacy in the digital age: a comparative study. Journal of Law and Economics, 92(Special Supplement), (in Arabic): 189-314.
- Rustom, M. (1992). Penal Code and Information Technology Risks, 1st ed. Egypt (in Arabic): Library of Modern Papers.
- Salamudi. R. And Rabaya. L. And the rice. H. And Brahmin A. (2017). The contemporary position of the rules of public international law on the right to privacy in the digital age, Arab American University Journal of Research, (in Arabic): 3 (2), 10.
- Sher, G., & Benchlouch, A. (2023, October 31). The privacy paradox with AI. AllSides. Retrieved from AllSides https://www.allsides.com/news/2023-10-31-1122/technology-privacy-paradox-ai
- The Amended Palestinian Basic Law of 2003, Palestinian Official Gazette (Palestinian Gazette), No. (Safar), 03/19/2003, p. 5. (in Arabic).
- The Jordanian Constitution of 1952, Jordanian Official Gazette, No. (1093), 1/8/1952. (in Arabic).
- United Nations document: (A/77/196). 19 – 9-2022.
- United Nations document: (A/HRC/46/37).25-2-2021.
- United Nations document: (A/HRC/51/17). 4-8-2022.
- United Nations document: (A/HRC/52/37). 27- 12- 2022.
- United Nations document: (A/HRC/RES/37/2). 6 -4-2018.
- Vial, A. (2022). Systèmes d'intelligence artificielle et responsabilité civile: Droit positif et proposition de réforme (Thèse de doctorat de droit privé et sciences criminelles). Université de Besançon.