أجيال الرقمي
نشر – طباعة – توزيع

رقم: 064 /د.أ.ر./2025

الجزائر يوم: 2025/12/21

شهادة نشر

تشهد دار النشر أجيال الرقمي أن الأستاذة: **عبد العزيز عشبة سلمى**

قد شاركت في تأليف الكتاب الجماعي المقدم لها والموسوم بـــ:

أثر التطور التكنولوجي على القانون

وقد تم طبعه خلال 2025 وهو مسجل تحت الإيداع القانوني

رقم: 978-9931-14-286-7

سلمت هاته الشهادة بطلب من المؤلفة لاستعمالها فيما يسمح به القانون.

المديـر

أجيال الرقمي AJYAL RAKMI
- نشر الكتاب -
حي سكن الريفية رقم 10 فيلا رقم 02 الطابق
الأرضي أولاد فايت الجزائر
رقم س. ت.: 20 A 4962364 - 16/00

المقر الاجتماعي: دار أجيال الرقمي، حي النجد رقم 10 أولاد فايت - الجزائر العاصمة -
الإيميل: info.ajyale@gmail.com
الهاتف: 06 57114787 / 07 75358320

استكتاب جماعي حول:

أثر التطور التكنولوجي على القانون

تأليف مجموعة من الباحثين

رئيس المشروع

د. نصرالدين العايب

أجيال الرقمي

تأليف مجموعة من الباحثين

أثر التطور التكنولوجي على القانون
استكتاب جماعي حول:

عن الكتاب

استطاع الإنسان منذ بداية الوجود تطوير الأدوات التي يستعملها ويستعين بها في مختلف مجالات حياته اليومية، بدءا من الاستعانة بالأحجار إلى اكتشاف الآلة وتطويرها، ومساعدتها له بالقيام بأعمال يصعب عليه القيام بها، ومع نهاية القرن العشرين وبداية القرن الحالي عرفت التكنولوجيا تطورا سريعا بمختلف الميادين من الحياة اليومية للإنسان؛ وعليه يجب ان يكون القانون انعكاس للواقع ويواكب التطور الحاصل في شتى الميادين وإلا كان قاصرا عن تنظيم الحياة اليومية للأفراد وتغطية متطلباتهم على مختلف الأصعدة، إذ ان العالم يشهد طفرات تقنية واسعة ولا يمر يوم الا ونسمع باختراع علمي جديد او جهاز أو تقنية جديدة، وهذه الابتكارات الجديدة والحديثة أصبحت تعمل على تغيير مفاهيم القانون وتتطلب التكييف المستمر لهذه التشريعات لمواكبة التحديات والقضايا الجديدة التي تطرحها، وكذا تطور القانون الذي يؤثر على تطور التكنولوجيا، سواء من حيث التنظيم أو معايير القانون المطبق على المنتجات أو البيئة التي تشترط التكنولوجيا؛ وبالتالي يجب ان تعمل التكنولوجيا والقانون سويا وبشكل وثيق على توفير إطار قانوني فعال لمستخدمي التكنولوجيا.

وعليه نهدف من خلال هذا الاستكتاب الجماعي دراسة التطور التكنولوجي وأثره في تحديث التشريعات، والذي سيعمل على دراسة مدى تأثير التطور التكنولوجي على القوانين المختلفة، ومدى قدرة تلك القوانين على مواكبة الطفرات الكبيرة في التطور التكنولوجي، وما هي الحلول التي يمكن اقتراحها على المشرع من اجل سد النقص التشريعي الحاصل بسبب تطور الحياة.

ISBN : 978-9931-14-286-7

9 789931 142867

أجيال الرقمي

دار أجيال الرقمي
طباعة - نشر - توزيع
حي سكن الريفية . النجد رقم 10 - أولاد فايت - الجزائر العاصمة
الهاتف : 096 999 661 (0) 213+
787 114 657 (0) 213+
البريد الالكتروني : info.ajyale@gmail.com

جامعة الشاذلي بن جديد-الطارف

كلية الحقوق والعلوم السياسية

استكتاب جماعي حول:

أثر التطور التكنولوجي على القانون

تأليف مجموعة من الباحثين

رئيس المشروع

د. نصرالدين العايب

المقالات المنشورة في الكتاب الجماعي تعبر عن أراء أصحابها
ولا يتحمل المشرفون عن الكتاب بالضرورة وجهة نظرهم

استناداً للمحضر رقم 08 المؤرخ بتاريخ 09 مارس 2025

تمت المصادقة على اعتماد الكتاب الجماعي بعنوان

أثر التطور التكنولوجي على القانون

من طرف المجلس العلمي لكلية الحقوق والعلوم السياسية جامعة الطارف

أجيال الرقمي

عنوان الكتاب:

أثر التطور التكنولوجي على القانون

تأليف جماعي

الطبعة الأولى

ردمك: **978-9931-14-286-7**

الإيداع القانوني: **ديسمبر 2025**

الحجم: 15.5x 23.5

الأفكار الواردة في هذا الكتاب مصدرها المؤلف

ولا تتبناها بالضرورة دار أجيال الرقمي

دارأجيـال الرقمـــي

حي سكن الريفية ، النجد رقم 10 - أولاد فايت - الجزائر العاصمة

الهاتف :

+213(0) 661 999 096

+213(0) 657 114 787

info.ajyale@gmail.com

محفوظة جميع الحقوق

لدار أجيال الرقمي

2025

ديباجة الاستكتاب

استطاع الإنسان منذ بداية الوجود تطوير الأدوات التي يستعملها ويستعين بها في مختلف مجالات حياته اليومية، بدءا من الاستعانة بالأحجار إلى اكتشاف الآلة وتطويرها، ومساعدتها له بالقيام بأعمال يصعب عليه القيام بها، ومع نهاية القرن العشرين وبداية القرن الحالي عرفت التكنولوجيا تطورا سريعا بمختلف الميادين من الحياة اليومية للإنسان؛ وعليه يجب ان يكون القانون انعكاس للواقع ويواكب التطور الحاصل في شتى الميادين وإلا كان قاصرا عن تنظيم الحياة اليومية للأفراد وتغطية متطلباتهم على مختلف الأصعدة، إذ ان العالم يشهد طفرات تقنية واسعة ولا يمر يوم الا ونسمع باختراع علمي جديد او جهاز أو تقنية جديدة، وهذه الابتكارات الجديدة والحديثة أصبحت تعمل على تغيير مفاهيم القانون وتتطلب التكييف المستمر لهذه التشريعات لمواكبة التحديات والقضايا الجديدة التي تطرحها، وكذا تطور القانون الذي يؤثر على تطور التكنولوجيا، سواء من حيث التنظيم أو معايير القانون المطبق على المنتجات أو البيئة التي تشترط التكنولوجيا؛ وبالتالي يجب ان تعمل التكنولوجيا والقانون سويا وبشكل وثيق على توفير إطار قانوني فعال لمستخدمي التكنولوجيا.

وعليه نهدف من خلال هذا الاستكتاب الجماعي دراسة التطور التكنولوجي وأثره في تحديث التشريعات، والذي سيعمل على دراسة مدى تأثير التطور التكنولوجي على القوانين المختلفة، ومدى قدرة تلك القوانين على مواكبة

الطفرات الكبيرة في التطور التكنولوجي، وما هي الحلول التي يمكن اقتراحها على المشرع من اجل سد النقص التشريعي الحاصل بسبب تطور الحياة.

محاور الاستكتاب

المحور الأول: الإطار المفاهيمي

- التكنولوجيا الحديثة.
- الذكاء الاصطناعي.
- المشكلات القانونية التي تنشأ من استخدام الذكاء الاصطناعي.
- الذكاء الاصطناعي في ميزان القانون "بين الحظر والإباحة.
- المسئولية المدنية الناشئة عن أضرار الذكاء الاصطناعي.
- المسئولية الجنائية الناشئة عن الجرائم المرتكبة بواسطة الذكاء الاصطناعي.
- المسئولية الدولية عن جرائم الذكاء الاصطناعي.

المحور الثاني: أثر التكنولوجيا على القانونين الموضوعي والإجرائي

- أثر التقدم التكنولوجي على الحريات الشخصية.
- أثر التكنولوجيا على القانون الجنائي.
- أثر التكنولوجيا على القانون التجاري.
- أثر التكنولوجيا على أحكام العقد والمسئولية المدنية.
- دور التكنولوجيا في تيسير إجراءات التقاضي وتنفيذ الأحكام.
- أثر استخدام التكنولوجيا على مبادئ المحاكمة العادلة
- أثر التكنولوجيا في حماية حقوق الإنسان.
- التكنولوجيا والقانون الدولي الإنساني.
- أثر التكنولوجيا في الاعتداء على حقوق الأطفال والمرأة.

- التكنولوجيا والقانون الدولي الخاص.
- تأثير تطور تكنولوجيا المعلومات على المهنيين والخبراء في مجال القانون.

المحور الثالث: التكنولوجيا وحقوق الملكية الفكرية

- أثر التكنولوجيا على الحماية القانونية للمؤلف وأصحاب الحقوق المجاورة.
- أثر التكنولوجيا في تفعيل الحماية الإجرائية لحقوق المؤلف والحقوق المجاورة.
- التطور التشريعي لقوانين الملكية الفكرية لمجابهة التطور التكنولوجي.
- أثر التكنولوجيا على الاعتداء على حقوق الملكية الفكرية.

هيئات الكتاب الجماعي

الرئيس الشرفي للكتاب: أ . د شول بن شهرة مدير جامعة الشاذلي بن جديد – الطارف.

المشرف العام للكتاب: أ. د. منية غريب عميدة كلية الحقوق والعلوم السياسية.

رئيس مشروع الكتاب: د. العايب نصرالدين

رئيس اللجنة العلمية: د. نذير قورية - د. عماد الدين بركات.

أعضاء اللجنة العلمية			
أ.د غريب منية	جامعة الطارف	د. بوعكاز أسماء	جامعة الطارف
أ.د. عبدلي نزار	جامعة الطارف	د. العايب نصر الدين	جامعة الطارف
أ.د. فؤاد خوالدية	جامعة الطارف	د. سماعيلي حسام الدين	جامعة الطارف
د. عائشة عبد الحميد	جامعة الطارف	د. رابح وهيبة	جامعة بجاية
د. حسين أحمد	جامعة الطارف	د. سهام رحال	جامعة الطارف
د. بركات عماد الدين	جامعة الطارف	د. رحماوي كمال	جامعة الطارف
د. قريمس سارة	جامعة الطارف	د. مزوزي فارس	جامعة الطارف
د. بن صالحية صابر	جامعة الطارف	د. زيد الخيل توفيق	جامعة الطارف
د. غشير صالح	جامعة الجزائر 1	د. مقدم رشا	جامعة الطارف
د. بوستة زهر الدين	جامعة الطارف	د. بلقاسم سعدون	جامعة الطارف

د. جامل صباح	جامعة الطارف	د. منصر نصر الدين	جامعة تبسة
د. بليدي دلال	جامعة الطارف	د. مزردي عبد الحق	جامعة عين تموشنت
د. هماش لمين	جامعة الطارف	د. العمري زقار مونية	جامعة الطارف
د. بويحياوي أمال	جامعة الطارف	د. عبدالوهاب بوعزيز	جامعة الطارف
د. ربعية رضوان	جامعة الطارف	د. نويري محمد الأمين	جامعة الطارف
د. بن نولي زرزور	جامعة الطارف	د. بوعون زكرياء	جامعة قسنطينة 1
د. بوشامي نجلاء	جامعة الطارف	د. ملوك نوال	جامعة الطارف
د. بوبترة طارق	جامعة قسنطينة 1	أ.د حمزة وهاب	جامعة أم البواقي
د. شعوة مهدي	جامعة قسنطينة 1	د. برابح منير	المركز الجامعي بريكة

أ.د مستاري عادل	جامعة بسكرة	د. قريمس سارة	جامعة الطارف
أ.د. شاوش حميد	جامعة قالمة	أ.د. فطناسي عبد الرحمن	جامعة قالمة
أ.د. عمراني مراد	جامعة عنابة	د. قورية نذير	جامعة الطارف
د. دغبوج تقي الدين	جامعة الطارف	برابح منير	المركز الجامعي بريكة
د. خولة غرايبية	جامعة الطارف	أ.د بوعمران عادل	جامعة سوق اهراس
د بوعقبة نعيمة	جامعة الطارف	د. علاوة حنان	جامعة بجاية

الذكاء الاصطناعي كسلاح غير تقليدي في النزاعات المسلحة واشكالية الامتثال لمبادئ القانون الدولي الإنساني

Artificial intelligence as an unconventional weapon in armed coalitions and basic models of historical international law

نعيمة بوعقبة

جامعة الشاذلي بن جديد-الطارف، bouakba-naima@univ-eltarf.dz

ملخص:

يشهد العالم اليوم تحولا غير مسبوق في طبيعة النزاعات المسلحة، حيث أصبحت الأسلحة الذاتية التشغيل، مثل الطائرات المسيرة والروبوتات القتالية المدعومة بتقنيات الذكاء الاصطناعي، جزءًا أساسيا من منظومات الحرب الحديثة.

غير أن هذا التطور بات يطرح إشكالات قانونية وأخلاقية، تتعلق بمدى توافق استخدام هذه الأسلحة -التي تمتاز بقدرتها على اتخاذ قرارات مستقلة كالتعرف على الأهداف وتقييم التهديدات وتنفيذ الهجمات ذاتيا- مع المبادئ الأساسية للقانون الدولي الانساني كمبدأ التمييز بين المدنيين والمقاتلين، والتناسب والاحتياط أثناء الهجوم، الأمر الذي بات يثير تساؤلات حول مستقبل الحروب وشرعية استخدام الذكاء الاصطناعي في النزاعات المسلحة

الكلمات المفتاحية: الذكاء الاصطناعي؛ النزاعات المسلحة؛ الأسلحة ذاتية التشغيل؛ الأسلحة غير التقليدية؛ مبادئ القانون الدولي الإنساني.

Abstract:

Today, there are massive shifts in the nature of armed conflict, as autonomous weapons, such as drones and combat robots powered by artificial intelligence technologies, have become fundamental to modern warfare systems.

These developments raise legal and ethical issues related to the extent to which the use of these weapons - which are characterized by their ability to make independent decisions such as identifying targets, assessing threats, and carrying out attacks on their own - is compatible with the basic principles of international humanitarian law, such as the principle of distinguishing between civilians and combatants, and proportionality and precaution during the attack, which raises questions about the future of wars and the legitimacy of the use of artificial intelligence in armed conflicts

Keywords: Artificial intelligence; Armed conflict; Autonomous weapons; unconventional weapons; Principles of International Humanitarian Law

مقدمة:

يشهد العالم اليوم تحولا جذريا في طبيعة النزاعات المسلحة في ظل تصاعد الاعتماد على التكنولوجيا المتقدمة في المجال العسكري، وبروز ما يعرف بحروب الجيل السادس، التي تتميز باعتمادها على الأسلحة المزودة بتقنيات الذكاء الاصطناعي لا سيما الأسلحة الذاتية التشغيل كالطائرات المسيرة (الدرونات) والروبوتات الذاتية، التي تعتمد على خوارزميات متقدمة تمكنها من اتخاذ قرارات مستقلة تشمل التعرف على الأهداف وتقييم التهديدات وتنفيذ الهجمات دون الحاجة إلى توجيه بشري مباشر خلال العمليات القتالية

على الرغم من أن الأسلحة المدعومة بالذكاء الاصطناعي بخلاف الأسلحة التقليدية تضمن دقة الضربات العسكرية على نحو يقلل من الأضرار الجانبية لكن بالمقابل يثير استخدامها العديد من الإشكالات الجوهرية المتعلقة بمدى توافقها مع قواعد القانون الدولي الإنساني، لا سيما من ناحية احترامه المبادئ الجوهرية التي

يرتكز عليها هذا القانون والمصممة لحماية المدنيين، من هنا تعالج هذه الدراسة الإشكالية الآتية:

ما مدى امتثال الأسلحة المزودة بتقنية الذكاء الاصطناعي لمبادئ القانون الدولي الإنساني؟

الإجابة على هذه الإشكالية يتطلب منا أولا التطرق إلى الأسلحة الذاتية التشغيل كتطبيق للذكاء الاصطناعي في النزاعات المسلحة (المبحث الأول)، ثم معالجة مدى امتثال الأسلحة الذاتية التشغيل كتطبيق للذكاء الاصطناعي لمبادئ القانون الدولي الإنساني (المبحث الثاني).

المبحث الأول:

الأسلحة الذاتية التشغيل كتطبيق للذكاء الاصطناعي في النزاعات المسلحة

تعتبر الأسلحة الذاتية التشغيل من أبرز تطبيقات تكنولوجيا الذكاء الاصطناعي، والتي شهدت استخداما واسعا في عدد من النزاعات المسلحة ذات الطابع الدولي منها أو غير دولي، وبأشكال ونماذج عديدة كما ترتبط ارتباطا وثيقا بقواعد القانون الدولي الانساني، لذلك سينصب تركيزنا على هذا النموذج.

المطلب الأول: استخدامات الأسلحة الذاتية التشغيل

كتطبيق للذكاء الاصطناعي في النزاعات المسلحة

نبين أولا المقصود بالأسلحة الذاتية التشغيل ثم نحاول تبيان مظاهر استخدام الأسلحة الذاتية التشغيل كتطبيق للذكاء الاصطناعي في النزاعات المسلحة.

الفرع الأول: تعريف الأسلحة الذاتية التشغيل

عرفت منظمة الأمم المتحدة الأسلحة الذاتية التشغيل كتطبيق للذكاء الاصطناعي بأنها: "منظومات سلاح آلية تستطيع في حال تشغيلها أن تختار الأهداف وتشتبك معها دون حاجة إلى تدخل إضافي من

العنصر البشري الذي يشغلها".[1]

وحسب منظمة حلف الشمال الأطلسي (الناتو) فالأسلحة الذاتية التشغيل هو: " نظام يقرر ويعمل لتحقيق الأهداف المرجوة، ضمن معايير محددة، بناءً على المعرفة المكتسبة والوعي المتطور بالوضع، باتباع مسار عمل مثالي ولكنه قد لا يمكن التنبؤ به".[2]

عرفتها اللجنة الدولية لحقوق الانسان التي أطلقت عليها تسمية الروبوتات القاتلة بأنها: " أسلحة مستقلة تماما يمكنها اختيار الأهداف والاشتباك معها دون تدخل بشري ويمكن تطويرها في غضون 20 إلى 30 عاما".[3]

وبالنظر لتأثيرها على حقوق الانسان تعرف منظمة مراقبة حقوق الانسان human Rhgits watchالأسلحة الذاتية التشغيل أو الأسلحة القاتلة المستقلة كما أطلقت وصفتها بأنها: " سلاح قادر بمجرد تشغيله على اختيار الأهداف والاشتباك بها دون تدخل بشري لاحق"، وفي هذا التعريف تركز منظمة مراقبة حقوق الانسان على

---

[1] - لمياء محمد عبد السلام جواد، ضوابط استخدام الذكاء الاصطناعي في مجال التسليح العسكري في ضوء مبادئ القانون الدولي الإنساني، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 4، ديسمبر 2024، ص 2281

[2] - Agnieszka Szpak, Artificial intelligence and international humanitarian law in the work of the parties to the Conventional Weapons Convention: lethal autonomous weapons, Artificial intelligence and international human rights law, 2024, p 280

[3] - خير الدين العايب، عبد الرحمن علي غنيم، الأسلحة الذاتية التشغيل، مجلة الدراسات الاستراتيجية والبحوث السياسية، المجلد 4، العدد 1، 2015، ص 66

مسألتين لوصف السلاح الذاتي التشغيل الأولى تركز فيها على قدرة النظام على اختيار الهدف العسكري، والثانية تركز فيها المنظمة على قدرة النظام على الاشتباك مع الهدف دون تدخل بشري لاحق.

أما اللجنة الدولية للصليب الأحمر فقد عرفت الأسلحة الذاتية التشغيل والتي أطلقت عليها تسمية الأسلحة المستقلة بأنها: " أي نظام أسلحة يتميز بالاستقلالية في وظائفه الأساسية يمكنه اختيار -أي البحث عن، كشف، تحديد، تتبع اختيار- ومهاجمة -أي استخدام القوة، إتلاف، أو تدمير- الأهداف دون تدخل بشري".[1]

يبدو من تعريف اللجنة الدولية للصليب الأحمر أن مصطلح منظومات الأسلحة الذاتية التشغيل يشمل أي نوع من منظومات الأسلحة سواء أكانت هذه الأسلحة المدعومة بالذكاء بالاصطناعي تعمل في الجو أو البر أو البحر بصورة تلقائية بتلقائية على نحو يمكنها أن تختار أي تبحث، تكشف تحدد تتعقب تختار وتهاجم أي يستخدم القوة ضد الهدف العسكري أو تعطل أو يدمر أو تلحق أضرار بالأهداف العسكرية المتوخاة دون تدخل بشري.[2]

كما يظهر من تعريف اللجنة الدولية للصليب الأحمر أن اللجنة قد ميزت بين منظومات الأسلحة التي تعمل بالبرمجة المسبقة والتي تعرف بالأتمتة، وبين منظومات الأسلحة ذاتية التشغيل بالكامل والمدعومة بالذكاء بالاصطناعي والتعلم الآلي لتكييف أداءها وخلق الحلول ذاتيا.[3]

[1] - Agnieszka Szpak, op.cit, p 280

[2] - شهلاء كمال عبد الجواد، استخدام الأسلحة الذكية في الحرب وفق القانون الدولي الإنساني، مجلة العلوم القانونية والسياسية كلية القانون، جامعة الموصل، المجلد 10، العدد 37، 2021، ص 57

[3] - خير الدين العايب، عبد الرحمن علي غنيم، المرجع السابق، ص 66

ثانيا: فئات الأسلحة الذاتية التشغيل

يعتبر العنصر البشري عنصر حاسم في تحديد فئة وطبيعة الأسلحة الذاتية التشغيل، ذلك أن مستوى تدخل الانسان في نظام هذه الأسلحة، وبعبارة أخرى أن درجة اشراف الانسان على دورة القرار القتالي لهذه الأسلحة يتحدد على 3 مستويات أو فئات

1- الاشراف داخل الحلقة In the loop

يكون للأسلحة الذاتية التي تقع ضمن هذه الفئة استقلالية محددة، حيث يكون العنصر البشري الدور البارز في إعطاء قرار أو أوامر الاستهداف والهجوم النهائي من خلال دوره، بينما يتحدد دور النظام (الأسلحة الذاتية) في باقي الوظائف العسكرية الأخرى بما فيها اختيار الأهداف دون أن تملك صلاحية تنفيذ الهجوم تلقائيا، فهذه الصلاحية يحتفظ بها المشغل البشري للسلاح الذي يملك كذلك صلاحيات التحكم وإيقاف المهاجمة في أي وقت يشاء.

2- الاشراف على الحلقة On the loop

تملك الأسلحة الذاتية التي تقع ضمن هذه الفئة القدرة على اختيار الأهداف واستعمال القوة لكن تحت مراقبة المشغل البشري الذي يملك صلاحية التحكم في منظومة السلاح في أي مرحلة بل ويملك صلاحية ايقافها وإلغاء عملها في حال فشل في تحقيق الهدف أو لمنع احداث أضرار جانبية، من أمثلتها منظومة اعتراض الصواريخ المستخدمة من إسرائيل.[1]

[1] - فاضل عبد الزهرة فاضل، المنظور الأخلاقي في استخدام الأسلحة ذاتية التشغيل، مجلة معهد العلمين للدراسات العليا، العدد 18، 2024، ص 39

3- الاشراف خارج الحلقة Out of the loop

في هذه الفئة من الأسلحة الذاتية التشغيل يكون البشر خارج دائرة القرار، وهذا ما يجعل النظام يحوز القدرة الكاملة على اختيار الأهداف المراد مهاجمتها واختيار التوقيت المناسب دون أي تدخل بشري

هذا ما يجعل استخدام أسلحة تقع ضمن هذه الفئة محل جدل قانوني وأخلاقي واسع على المستوى الدولي.[1]

الفرع الثاني: تطبيقات الذكاء الاصطناعي في الأسلحة الذاتية التشغيل

تعتمد الأسلحة الذاتية التشغيل في أداء وظائفها على تطبيقات الذكاء الاصطناعي التي تعتبر العمود الفقري لهذه الأنظمة، حيث تمكنها من اتخاذ القرار في أي مرحلة بشكل مستقل.

أولا: نماذج الأسلحة الذاتية التشغيل المدعومة بالذكاء الاصطناعي

تأخذ الأسلحة الذاتية المدعومة بالتطبيقات الذكاء الاصطناعي نماذج عديدة، ولكل نوع من هذه الأسلحة مهام عسكرية تؤديها في معركة القتال، ومن أبرز نماذج هذه الأسلحة التي تم استخدامها في بعض النزاعات المسلحة في سوريا والحرب على غزة، الحرب بين روسيا وأوكرانيا ومؤخرا الحرب بين إيران وإسرائيل والولايات المتحدة الأمريكية نجد:

[1] - دعاء جليل حاتم، الأسلحة ذاتية التشغيل في ضوء مبادئ القانون الدولي الإنساني، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، عدد خاص، 2020، ص 285

1- الطائرات المسيرة

تعرف بالدرونات العسكرية التي تكون مزودة برادار بالذكاء الاصطناعي، وتقوم بمهام عديدة في ساحة القتال منها صناعة شبكة من النيران بهدف تعطيل تحريك الطائرات المعادية[1]، كما يمكنها القيام بعمليات المناورة واخلاء الجنود وفي التجسس وحمل المتفجرات بغرض استهداف القوات والمنشئات وتنفيذ اعتداءات وهجمات عسكرية[2]، وقد كشفت الحرب الأخيرة ما بين ايران وإسرائيل عن استخدام واسع النطاق للمسيرات اما من خلال الاستعانة بها في توجيه الضربات والهجمات أو في العمليات الدفاعية، حيث استخدمت إسرائيل المسيرات المدعومة بالذكاء الاصطناعي لتعطيل الدفاعات الجوية لإيران قبل بدء الهجوم الجوي، في حين استخدمت ايران الطائرات المسيرة في شاكلة شاهد 136 التي تعتمد على التوجيه الذاتي لشن هجمات على إسرائيل، كما تمثل الحرب بين روسيا وأوكرانيا مثال آخر لاستخدام هذا النوع من الأسلحة الذاتية التشغيل حيث تشير الاحصائيات العالمية إلى الاستخدام الواسع للمسيرات في توجيه الضربات للأهداف العسكرية خاصة من قبل أوكرانيا، حيث تؤكد ذات الاحصائيات بأن ما بين 70 % إلى 80 % من الإصابات الميدانية تمت بواسطة المسيرات.[3]

[1] - زينب عبد اللطيف خالد عبد اللطيف، المسؤولية الدولية المشتركة عن استخدام الذكاء الاصطناعي في الأعمال العسكرية في ظل قواعد القانون الدولي، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، القاهرة، المجلد 66، العدد 3، 2024، ص 738

[2] - سالم نسرين، أثر توظيف تقنيات الذكاء الاصطناعي عسكريا: دراسة في متغيري الحروب والنزاعات، مجلة القانون والعلوم البيئية، المجلد 3، العدد 1، ص 870

[3] - يحي دايخ، الذكاء الاصطناعي في المجال العسكري: تطبيقات. مخاطر وتحديات قانونية وأخلاقية، مقال منشور بتاريخ 2025/9/18، تاريخ الاطلاع 2025/10/4، على الساعة 21:08، متاح على الرابط التالي:https://mnews.press/24173-2

2- الروبوتات ذاتية التحكم

يتميز هذا النوع من الأسلحة بالمهام الذاتية التي يؤديها، استنادا للبرمجة والمعلومات التي تتلقاها من أجهزة الاستشعار، حيث تكون قادرة على اختيار الأهداف واستهدافها تلقائيا وبشكل مستقل تبعا لمجموعة من الخوارزميات وبرامج تحليل البيانات، حيث تكون لها القدرة على اتخاذ قرار توجيه ضربات نحو أهداف عسكرية أو مدنية[1]، فضلا عن استخداماتها المتعددة في ساحة المعركة حيث لا يقتصر دورها على المهام الهجومية القتالية بل يمتد ليشمل كذلك مهام المعاونة والمراقبة والاستطلاع ونصب الكمائن ومراقبة الحدود والمهام اللوجستية ونقل الجرحى من ساحة الحرب وتأمين الطرق والكشف عن الألغام والعبوات الناسفة والتخلص منها[2]، ومن أبرز نماذج هذه الروبوتات نظام C-RAM المضاد للصواريخ والذي يطلق عليه تسمية " روبوت حرب النجوم الأمريكي" المزود بتقنية الذكاء الاصطناعي يمتلك هذا الروبوت القدرة على الاستشعار بوجود قذائف أو صواريخ واتخاذ القرار بإسقاطها تلقائيا[3].

كما تم استخدام الروبوتات الذاتية التشغيل في الحرب الأوكرانية الروسية حيث أورد تقرير صادر عن صحيفة التايمز البريطانية بأن أوكرانيا قد استخدمت سنة 2023 روبوت عسكري مزود بمدفع لمقاتلة جنود روس ولتنفيذ الهجمات تلقائيا، وقد كان هذا الروبوت يوازي حجم فصيلة من الجنود بالكامل.[4]

---

[1] - زينب عبد اللطيف خالد عبد اللطيف، المرجع السابق، ص 738

[2] - عبد القادر محمود محمد الأقرع، الروبوتات العسكرية في الحروب المستقبلية ومدى خضوعها لأحاكم القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق، الخرطوم، المجلد 8، العدد 3، 2020، ص 216

[3] - زينب عبد اللطيف خالد عبد اللطيف، المرجع السابق، ص 738

[4] - مستقبل الحرب يبدأ من هنا: تايمز: روبوتات أوكرانية تقاتل رجالا روسا، مقال منشور بتاريخ 2025/2/10، موقع الجزيرة، تاريخ الاطلاع 2025/7/30، على الساعة 07:09، متاح على الرابط التالي: https://www.aljazeera.net/politics/2025/2/10

من جهتها استخدمت إسرائيل في حربها على غزة هذا النوع من الروبوتات الذاتية التشغيل والتي أودت إلى قتل ألاف المدنيين وتدمير العديد من الأعيان المدنية، حيث استخدمت إسرائيل لتفادي الخسائر في صفوف جنودها روبوت باندا الذي هو عبارة عن جرافة مزودة بأجهزة استشعار متطورة تراقب الظروف المحيطة وتنقل البيانات إلى المشغلين في المواقع المحمية الذين يقومون بتمهيد المسارات لتتبع وحدات المشاة والدروع، إلى جانب هذا الروبوت استخدمت إسرائيل كذلك روبوت روني الذي أسندت له مهام التنقل في الأنفاق والأزقة وتنفيذ عمليات هندسية دقيقة وحساسة.[1]

ثانيا: مظاهر استخدام الذكاء الاصطناعي في الأسلحة الذاتية التشغيل

تتعدد استخدامات تطبيقات الذكاء الاصطناعي في المجال العسكري، ما يمكن منظومات الأسلحة الذاتية التشغيل من أداء مجموعة من الوظائف الفنية والتشغيلية المميزة، وتُختصر أبرز هذه الاستخدامات فيما يلي:

-الكشف والتعرف على الأهداف وتصنيفها: حيث توظف نماذج الرؤية الحاسوبية لاستشعار الأهداف من أفراد ومركبات ومنشآت في ظروف تشغيلية متباينة، وتقدم توصيات تكتيكية لصانع القرار (المشغل البشري)، وهذا ما يمكن أن يزيد من دقتها وفاعليتها ويقلل من الخسائر البشرية

[1] - باندا وتالون وروني. ترسانة الروبوتات التابعة للجيش الإسرائيلي، مقال منشور في موقع الجزيرة بتاريخ 2024/11/12، تاريخ الاطلاع 2025/7/30، على الساعة: 22:23، متاح على الرابط التالي:
https://www.aljazeera.net/politics/2024/11/12/%D8%A8%

-دعم واتخاذ القرار القتالي وذلك عبر أنظمة تقدم توصيات للقائد العسكري أو تقترح أهداف عسكرية محددة، إضافة إلى تقييم المخاطر وتحليلها وتقدير الأضرار المحتملة للقرارات العسكرية[1]

-تنسيق الأسراب حيث تساعد الخوارزميات على التنسيق بين مجموعات متكاملة من الطائرات المسيرة والزوارق لأداء مهام هجومية موزعة بشكل متزامن

-الملاحة والحركة الذاتية عبر خوارزميات تمكن الطائرات المسيرة والأنظمة البرية والبحرية من التنقل في بيئات معقدة.

-الاستطلاع والتحليل الاستخباراتي والمراقبة التي يمكن استخدامها لتحليل مجموعات البيانات الكبيرة بكفاءة وتسهيل كشف التهديدات، والقيام بهجمات أكثر دقة، وهذا ما من شأنه أن يؤدي إلى الحد من المخاطر على المدنيين. [2]

المطلب الثاني: مميزات الأسلحة ذاتية

التشغيل كسلاح غيرتقليدي في النزاعات المسلحة

تمتاز الأسلحة الذاتية التشغيل بالعديد من المزايا التي تجعلها تختلف جوهريا عن الأسلحة التقليدية التي يتحكم فيها الانسان بشكل كامل وفي كل مراحل العملية العسكرية.

الفرع الأول: خصائص الأسلحة الذاتية التشغيل من ناحية أداءها

[1] - مركز المستقبل للأبحاث والدراسات المتقدمة، كيف يدير الذكاء الاصطناعي دقة الحروب الحديثة، مقال منشور بتاريخ 20 مايو 2024، تم تاريخ الاطلاع 2025//10/7، على الساعة 17:45، متاح على الرابط التالي:
https://futureuae.com/ar-AE/Mainpage/Item/9281/ai-militarization

[2] - تقرير الأمين العام للأمم المتحدة، الذكاء الاصطناعي في المجال العسكري وأثاره على السلام والأمن الدوليين، 2025/6/5، الجمعية العامة، الدورة 80. البند 101، ص 4، الفقرة 7 (ألف)، A/80/78

تعتبر استقلالية الأسلحة الذاتية التشغيل وسرعتها في الأداء والتفاعل والقدرة على التعلم الذاتي من المزايا البارزة في طريقة عمل وأداء هذه الأسلحة غير التقليدية.

أولا: الاستقلالية في اتخاذ القرار

تتميز الأسلحة الذاتية بقدرتها على اتخاذ قرارات ذاتية وبشكل مستقل دون تدخل بشري مباشر وهذه الخاصية تجعلها تختلف جوهريا عن الأسلحة التقليدية التي يتوقف استخدامها على التوجيه البشري.

إن استقلالية الأسلحة الذاتية التشغيل والتي منحتها خاصية الإدارة الذاتية[1]، جعلها قادرة على اختيار الأهداف ومهاجمتها تبعا للظروف المحيطة دون تدخل من مشغلها استنادا إلى البرمجيات تم دمجها مسبقا داخل هذه الأسلحة.[2]

ثانيا: سرعة الأداء والتفاعل

تمتاز الأسلحة الذاتية التشغيل بسرعة فائقة في التعرف على المعلومات والبيانات ومعالجتها واتخاذ القرار على نحو يتجاوز القدرات البشرية، هذا ما يسمح لها بتحقيق سرعة الاستهداف وتسريع عملية اكتشاف الهدف وتعقبه، كما يسمح لها بالتفاعل مع الأحداث بسرعة ويساعدها التكيف مع المستجدات.[3]

ثالثا: القدرة على التعلم الذاتي والتكيف

تعتمد الأسلحة الذاتية التشغيل على تقنيات التعلم الآلي Machine Learning وهي تقنيات برمجية متقدمة تعتمد على الذكاء الاصطناعي تمكنها من

[1] - شهلاء كمال عبد الجواد، المرجع السابق، ص 58

[2] - لمياء محمد عبد السلام جواد، المرجع السابق، ص 2281

[3] - المرجع نفسه، ص 2282

التعلم والاستفادة من التجارب السابقة وهذا بدوره يجعلها قادرة على التكيف مع مختلف الأوضاع المستجدة وتصحيح الأخطاء دون الرجوع إلى المشغل.[1]

الفرع الثاني: خصائص الأسلحة الذاتية التشغيل المرتبطة بنتائجها

على غرار الأسلحة التقليدية، تحدث الأسلحة الذاتية التشغيل تبعات تعقب مرحلة التنفيذ، غير أن نتائج عمليات هذه الأسلحة تختلف جوهريا عما تحدثه الأسلحة التقليدية مما تجعلها عناصر مميزة لها

أولا: الفتك والتدمير

تعتبر خاصية الفتك من أهم الخصائص المميزة للأسلحة الذاتية التشغيل، ذلك أن افتقار هذا النوع من الأسلحة للأحاسيس الإنسانية في تنفيذ مهامها القتالية في ساحة الحرب هذا ما يضفي عليها وصف الفتك بالنظر لما تسببه هذه الآلات من إصابات وخسائر في سبيل تحقيق الأهداف العسكرية دون مراعاة للاعتبارات الإنسانية أو لطبيعة المستهدف فيما إذا كان هدف مشروع أم لا.[2]

بالنظر لخاصية الاستقلالية التي تتسم بها الأسلحة الذاتية التشغيل، فإن قدرة هذه الأسلحة على الفتك ستزداد لا سيما إذا كانت المهام المسندة لها هي توجيه الضربات العسكرية، لذلك توصف غالبا بالأسلحة الفتاكة الذاتية.[3]

[1] - هاني محمد خليل إبراهيم العزازي، التحديات التي تثيرها الأسلحة ذاتية التشغيل كأحد تقنيات الذكاء الاصطناعي، المجلة القانونية، جامعة القاهرة، المجلد 20، العدد 4، 2024، ص 1424

[2] - عبد القادر محمود محمد الأقرع، المرجع السابق، ص 912

[3] - هاني محمد خليل إبراهيم العزازي، المرجع السابق، ص 1426

ثانيا: التحيز الخوارزمي

تعتمد الأسلحة الذاتية التشغيل اعتمادا جوهريا على الخوارزميات التي تعد أساسا في تمكين النظام من معالجة البيانات البيئية وتحليلها (كالصور والاشارات والرادارات) واكتشاف الأهداف وتصنيفها وتقييم التهديدات واتخاذ قرار بالاستهداف أو عدم الاستهداف والتنفيذ بإطلاق الذخيرة أو تغيير مسار السلاح.[1]

إن الاعتماد الكلي على الخوارزميات بالنسبة للأسلحة الذاتية التشغيل من شأنه أن يضعها ضمن دائرة التحيز باتخاذ قرارات خاطئة أو غير عادلة، بسبب أخطاء في البيانات أو في طريقة البرمجة الخوارزمية لهذا يعتبر التحيز الخوارزمي بالنسبة للأسلحة الذاتية التشغيل ليس مجرد خطأ تقني فحسب بل كذلك ميزة سلبية تتسم بها هذه الأسلحة، ذلك أن اعتماد أنظمة الذكاء الاصطناعي على البيانات التي يتم تدريبها عليها سيؤدي بالنظام إلى تكراراها تلقائيا رغم تحيزها أو أخطاءها مما يؤدي إلى نتيجة غير عادلة كاستهداف أهداف غير مشروعة، كاعتبار جميع المدنيين أهداف مشروعة، الحافلات، المدارس، سيارات الإسعاف، أماكن العبادة...إلخ.[2]

المبحث الثاني:

مدى امتثال الأسلحة الذاتية التشغيل لمبادئ القانون الدولي الإنساني

إن الخصائص المميزة للأسلحة الذاتية التشغيل لا سيما منها المتعلقة بالاستقلالية والفتك، تجعل خضوعها وامتثالها لمبادئ القانون الدولي الإنساني أمر في غاية التعقيد والصعوبة

[1] - اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة: تجديد الالتزام بالحماية في النزاعات المسلحة بمناسبة الذكرى السبعين لاتفاقيات جنيف، 2017، ص 32

[2] - يحي دايخ، المرجع السابق

المطلب الأول:

مبادئ القانون الدولي الإنساني

يسعى القانون الدولي الإنساني أو ما يعرف بقانون النزاعات المسلحة أو قانون الحرب إلى تنظيم سير العمليات العسكرية بين أطراف النزاع وضمان الحماية للمدنيين والأعيان المدنية من أثار وأضرار هذه العمليات العسكرية، ولأجل ذلك صممت العديد من المبادئ الأساسية التي يمتثل لها أطراف النزاع أثناء سير هذه العمليات، أهمها مبدأ التمييز بين المقاتلين وغير المقاتلين، التناسب، الضرورة العسكرية، ومبدأ الالتزام بالاحتياطات أثناء الهجوم.

الفرع الأول: مبدأ التمييز والتناسب

يعتبر مبدأ التمييز بين المدنيين وغير المدنيين ومبدأ التناسب من الركائز الأساسية في القانون الدولي الإنساني، إذ يهدفان إلى حماية المدنيين والحد من أثار النزاعات المسلحة.

أولا: مبدأ التمييز بين المقاتلين وغير المقاتلين

يعتبر مبدأ التمييز بين المقاتلين وغير المقاتلين أو بين الأهداف المدنية والأهداف العسكرية من القواعد الأساسية الملزمة في القانون الدولي الإنساني، وله مكانة راسخة كقاعدة عرفية تنطبق في جميع النزاعات المسلحة الدولية وغير الدولية.

يفرض هذا المبدأ على أطراف النزاع التزام بمراعاة التمييز بين المقاتلين والمدنيين وبين الأهداف العسكرية والأعيان المدنية، وهذا ما يتطلب توجيه الهجمات ضد الأهداف العسكرية دون غيرها، وتحديدا دقيقا للأهداف لتفادي وقوع

الإصابات والأضرار بالفئات المحمية بموجب أحكام القانون الدولي الإنساني من المدنيين غير المشاركين في القتال والأعيان المدنية.[1]

لا يعتبر مبدأ التمييز بين المدنيين والمقاتلين مجرد التزام فقط بل يمثل حجر الزاوية في القانون الدولي الإنساني، حيث نجده مكرسا بشكل صريح ضمن أحكام البرتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة لعام 1977، حيث نصت المادة 48 منه على ما يلي: " تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية"[2].

نجد تأكيد غير مباشر لمبدأ التمييز كذلك ضمن مواد مختلفة من أحكام البرتوكول الإضافي الأول وأيضا في عدد من مواد البرتوكول الإضافي الثاني الملحق باتفاقيات جنيف الأربعة والمتعلق بحماية ضحايا المنازعات المسلحة غير الدولية على حماية المدنيين وتمييزهم عن المقاتلين أثناء النزاعات المسلحة، وذلك بالنظر لارتباط القواعد المتعلقة بوضع المقاتل وغير المقاتل، والقواعد المتعلقة بحماية المدنيين بمبدأ التمييز وفي هذا الصدد تنص المادة 13 فقرة 1 منه على ما يلي: " يتمتع السكان المدنيون والأشخاص المدنيون بحماية عامة من الاخطار الناجمة عن العمليات العسكرية ...".[3]

[1] - فتحي محمد فتحي الحياني، القانون الدولي الإنساني وتطبيقاته على النزاعات المسلحة في العراق، جمعية الأمل، العراق، 2022، ص 65

[2] - البرتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة المعتمدة في 1949/8/12، والمتعلق بحماية ضحايا المنازعات المسلحة الدولية، المعتمد في 1977/6/8، المؤتمر الدبلوماسي لتأكيد القانون الدولي الإنساني المنطبق على المنازعات المسلحة الدولية وتطويره، دخل حيز النفاذ في 1978/12/7، متاح على الرابط التالي: https://hrlibrary.umn.edu/arab/b094.html

[3] - البرتوكول الإضافي الثاني الملحق باتفاقيات جنيف الأربعة المعتمدة في 1949/8/12، والمتعلق بحماية ضحايا المنازعات المسلحة غير الدولية، المعتمد في 1977/6/8، المؤتمر الدبلوماسي لتأكيد القانون الدولي

من جهتها أعادت محكمة العدل الدولية في رأيها الاستشاري الصادر في 1996/7/8 حول مشروعية التهديد بالأسلحة النووية أو استخدامها التأكيد على الطابع العرفي لمبدأ التمييز بين المدنيين والمقاتلين أثناء سير العمليات العسكرية، باعتباره من المبادئ الأساسية الملزمة لجميع الدول حتى ولو لم تكن طرفا في البرتوكول الإضافي الأول لعام 1977.[1]

ثانيا: مبدأ التناسب

يفرض مبدأ التناسب على أطراف النزاع التزام بعدم شن هجمات على أهداف عسكرية من شأنها أن تؤدي إلى أضرار عرضية تصيب المدنيين أو بالأعيان المدنية، أو تؤدي لخسائر مشتركة بين المدنيين والأعيان المدنية، وبمعنى آخر فمبدأ التناسب في القانون الدولي الإنساني يستهدف الحد من الأضرار الناجمة عن العمليات العسكرية من خلال اشتراط ألا تكون آثار الوسائل والأساليب الحربية المستخدمة غير متناسبة مع الميزة العسكرية المنشودة.[2]

يرتكز تطبيق مبدأ التناسب على أساس الموازنة بين مبدأين وهما الإنسانية والضرورة العسكرية حيث يلزم مبدأ الإنسانية إلى أطراف النزاع بتوجيه هجماتهم

الإنساني المنطبق على المنازعات المسلحة الدولية وتطويره، دخل حيز النفاذ في 1978/12/7، متاح على الرابط التالي:

https://www.ohchr.org/ar/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and-0

[1] - هاني محمد خليل إبراهيم العزازي، المرجع السابق، ص 1438

[2] - Ali Zeineddine, Law Artificial intelligence in Warfare : Legal and humanitarian challenges Under International humanitarian law, p 50, Date of acces,25 /7/2025, On 23 :14, Available at the link : https:// www.fmdbpub.com/user/journals/ article_details/FTSHS/279

ضد المقاتلين وضد الأهداف العسكرية فقط، أما مبدأ الضرورة العسكرية فيعتبر مشروعية النزاع المسلح لأجل اضعاف قوة الخصم العسكرية فقط.[1]

من جهته يعتبر مبدأ التناسب ركيزة أساسية من ركائز القانون الدولي الإنساني، لهذا نجد له تكريسا ضمن العديد من الاتفاقيات الدولية منها اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية لعام 1907 حيث جاء في ديباجتها ما يلي: " وترى الأطراف السامية المتعاقدة أن هذه الأحكام التي استمدت صياغتها من الرغبة في التخفيف من الآلام الحرب، كلما سمحت بذلك المقتضيات العسكرية، وهي بمثابة قاعدة عامة للسلوك يهتدي بها المتحاربون في علاقاتهم مع بعضهم البعض ومع السكان"[2] ، كما تم إقرار مبدأ التناسب في أحكام البرتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة والبرتوكول الإضافي الأول لعام 1977 الذي فرض قيود على أساليب ووسائل القتال، حيث جاء فيه: " إن حق أطراف أي نزاع مسلح في اختيار أساليب ووسائل القتال ليس حقا لا تقيده قيود

-يحظر استخدام الأسلحة والقنابل والمواد ووسائل القتال التي من شأنها احداث إصابات أو آلام لا مبرر لها..."."[3]

[1] - ايناس أبو حميرة، الأضرار الجانبية في النزاعات المسلحة في القانون الدولي الإنساني، مجلة العلوم القانونية والشرعية العدد 6، يونيو 2015، ص 113

[2] - اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية، المعقودة في 1907/10/18، مؤتمر لاهاي الثاني للسلام متاحة على الرابط التالي:

https://maqam.najah.edu/media/uploads/2022/04/legislations/Convention__IV__respecting_the_laws_and_customs_of_war_on_land.pdf

[3] - المادة 35 من البرتوكول الإضافي الأول، المتعلق بحماية ضحايا المنازعات المسلحة الدولية، المرجع السابق

الفرع الثاني: مبدأ الاحتياط أثناء الهجوم والضرورة العسكرية

زيادة على مبدأ التمييز والتناسب تفرض قواعد القانون الدولي الإنساني على أطراف النزاع التزام بمراعاة الاحتياط أثناء الهجوم، وبمراعاة الضرورة العسكرية في استخدام القوة.

أولا: مبدأ الاحتياط أثناء الهجوم

يكتسي مبدأ الاحتياط أهمية بالغة في سياق النزاعات المسلحة نظرا لدوره المحوري في الحد من المعاناة الإنسانية، لذلك تم ادراجه ضمن أحكام البرتوكول الإضافي الأول المعني بحماية ضحايا المنازعات المسلحة الدولية الذي قرر ما يلي: " تبذل رعاية متواصلة في إدارة العمليات العسكرية من أجل تفادي السكان المدنيين والأشخاص والأعيان المدنية".[1]

يفرض البرتوكول الإضافي الأول الذي يمثل الأساس القانوني الاتفاقي لمبدأ الاحتياط أثناء الهجوم كمبدأ عرفي التزام على أطراف النزاع ببذل العناية اللازمة لتجنب أو تقليل الخسائر والأضرار في صفوف المدنيين والأعيان المدنية، وذلك من خلال اتخاذ إجراءات عملية ووقائية مثل اختيار الوسائل والأساليب التي من شأنها أن تقلل الخسائر الجانبية والتأكد من أن الهدف مشروع.[2]

وفي سبيل ضمان تجسيد مبدأ الاحتياط أثناء الهجوم يبين البرتوكول الإضافي الأول المشار إليه أعلاه جملة التدابير الوقائية واجبة الاتباع عند شن الهجوم من قبل الأطراف المتنازعة وذلك في أحكام المواد 57، 58 منه والمتمثلة في:

[1] - المادة 1/57 من البرتوكول الإضافي الأول، المتعلق بحماية ضحايا المنازعات المسلحة الدولية، المرجع السابق

[2] - لمياء محمد عبد السلام جواد، المرجع السابق، ص 2303

1.الاحتياطات الواجبة الاتباع عند التخطيط للهجوم:

- يجب على من يخطط للهجوم أن يبذل ما في وسعه عمليا للتحقق من ان الأهداف المقرر مهاجمتها ليست اشخاصا مدنيين او اعيانا مدنية وأنها غير مشمولة بحماية خاصة ولكنها اهداف عسكرية كما هي مبينة في نص المادة 52 من البرتوكول الإضافي الأول
- أن يتخذ جميع الاحتياطات المستطاعة عند تخير وسائل وأساليب الهجوم من أجل تجنب احداث خسائر في أرواح المدنيين او الحاق بحياتهم أو الإضرار بالأعيان المدنية وذلك بصفة عرضية وحصر ذلك في أضيق نطاق
- أن يمتنع عن اتخاذ قرار بشأن أي هجوم قد يتوقع منه بصفة عرضية يحدث خسائر في أرواح المدنيين أو الحاق الإصابة بهم أو الإضرار بالأعيان المدنية أو أن يحدث خليطا من هذه الخسائر والأضرار مما يفرط في تجاوز ما ينتظر أن يسفر عن ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة[1]
- على أطراف النزاع السعي جاهدة إلى نقل ما تحت سيطرتها من السكان المدنيين والافراد المدنيين والأعيان المدنية بعيد عن المناطق المجاورة للأهداف العسكرية
- تلتزم أطراف النزاع بتجنب إقامة أهداف عسكرية داخل المناطق المكتظة بالسكان أو بالقرب منها
- يتوجب على أطراف النزاع اتخاذ الاحتياطات الأخرى اللازمة لحماية ما يجب سيطرتها من سكان مدنيين وأفراد وأعيان من الأخطار الناجمة عن العمليات العسكرية.[2]

[1] - المادة 57 من البرتوكول الإضافي الأول، المتعلق بحماية ضحايا المنازعات المسلحة الدولية، المرجع السابق

[2] - المادة 58 من البرتوكول الإضافي الأول، المتعلق بحماية ضحايا المنازعات المسلحة الدولية، المرجع نفسه

2.الاحتياطات الواجبة الاتباع أثناء الهجوم:

- أن يلغي أو يعلق أي هجوم إذا تبين ان الهدف ليس هدفا عسكريا أو أنه مشمول بحماية خاصة أو أن الهجوم قد يتوقع منه أن يحدث خسائر في أرواح المدنيين أو الحاق الإصابة بهم أو الاضرار بالأعيان المدنية، أو أن يحدث خليطا من هذه الخسائر والأضرار وذلك بصفة عرضية تفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة
- يوجه انذار مسبق بوسائل مجدية في حالة الهجمات التي قد تمس السكان المدنيين ما لم تحل الظروف دون ذلك.[1]

هذا ويلتزم أطراف النزاع بمراعاة هذه الاحتياطات والتدابير الوقائية منذ بدء الهجوم وبرمجة السلاح المزود بتقنية الذكاء الاصطناعي ويستمر الالتزام بالعمل بهذه الاحتياطات طوال مدة الاشتراك في العمليات القتالية.[2]

ثانيا: مبدأ الضرورة العسكرية

يُعد مبدأ الضرورة العسكرية أحد المبادئ المكملة لمبدأ التمييز في القانون الدولي الإنساني، إذ يسعى إلى الحد من نطاق العمليات الحربية وتوجيهها نحو الأهداف العسكرية المشروعة دون المساس بالفئات المحمية بموجب القانون. ويتيح هذا المبدأ لأطراف النزاع استخدام القوة اللازمة لتحقيق الهدف الرئيسي من القتال والمتمثل في تحييد العدو سواء عن طريق القتل أو الأسر أو فقدان القدرة على القتال، أو الاستسلام.

[1] - المادة 57 من البرتوكول الإضافي الأول، المتعلق بحماية ضحايا المنازعات المسلحة الدولية، المرجع السابق

[2] - لمياء محمد عبد السلام جواد، المرجع السابق، ص 2303

وبناء عليه، فإن استمرار الأعمال العسكرية بعد تحقق هذا الهدف العسكري أو الميزة العسكرية يُعد انتهاكا صريحا لمبدأ الضرورة العسكرية لكونه يفتقر إلى مبرر قانوني يُضفي عليه المشروعية[1]، وبالتالي، فإن مبدأ الضرورة العسكرية يُقيد استخدام القوة بحدود ما يحقق ميزة عسكرية مؤكدة، دون تجاوز أو إسراف في استخدام العنف.

وقد جرى التأكيد على هذا المبدأ في عدة مواثيق دولية، من بينها لائحة لاهاي لعام 1907 بشأن قوانين وأعراف الحرب البرية، التي نصت في الفقرة الخامسة من ديباجتها على أن: "هذه الأحكام التي استُمدت صياغتها من الرغبة في التخفيف من آلام الحرب، كلما سمحت بذلك المقتضيات العسكرية، تُعد قاعدة عامة للسلوك يهتدي بها المتحاربون في علاقاتهم مع بعضهم البعض ومع السكان"، كما تم تكريس المبدأ أيضا ضمن أحكام البروتوكول الإضافي الثاني لعام 1977 لا سيما المادة 35، التي رغم عدم ذكرها الصريح لمبدأ الضرورة العسكرية، إلا مضمونها يرتبط بهذا المبدأ.[2]

المطلب الثاني: انتهاك الأسلحة الذاتية التشغيل المدعومة بالذكاء الاصطناعي لمبادئ القانون الدولي الإنساني

تثير استخدام أسلحة الذكاء الاصطناعي في النزاعات المسلحة إشكالات وتحديات للقانون الدولي الإنساني، فغياب الرقابة البشرية والقدرة في التحكم يجعل من الصعوبة بمكان امتثال هذه الأسلحة لمبادئ

القانون الدولي الإنساني لا سيما مبدأ التمييز بين المقاتلين والمدنيين ومبدأ التناسب، ومبدأ الاحتياط أثناء الهجوم، وفي هذا السياق أكدت منظمة مراقبة

[1] - تامر مصالحة، المبادئ الأساسية في القانون الدولي الإنساني، الطبعة الأولى 2009، دون دار نشر، ص 79

[2] - دعاء خليل حاتم، المرجع السابق، ص 288

حقوق الانسان هيومن رايتس ووتش Human Rights Watch في موقفها إزاء الأسلحة المبرمجة بالذكاء الاصطناعي بأن: " التنازل عن التحكم البشري للقدرات المدعومة بالذكاء الاصطناعي قد يقوض القانون الإنساني الدولي ويضعفه تدريجيا، تاركا ساحة المعركة دون رقابة قانونية والمدنيين دون حماية"، كما جاء في تقرير ذات المنظمة حول التقييم المبدئي للأسلحة ذاتية التشغيل والمعنون " فقدان الإنسانية"، بأن هذه الأسلحة تبدو غير قادرة على اتباع قواعد التمييز والتناسب وستؤدي إلى زوال الحماية للمدنيين.[1]

الفرع الأول: انتهاك الأسلحة الذاتية التشغيل لمبدأي التمييزوالتناسب

يثير استخدام الأسلحة الذاتية التشغيل تساؤلات جدية حول مدى التزامها ومراعاتها لمبدأ التمييز والتناسب خاصة في ظل غياب التقدير البشري المباشر في عمل هذه الأسلحة

أولا: انتهاك الأسلحة الذاتية التشغيل لمبدأ التمييز

إن الالتزام بمبدأ التمييز بين الأهداف العسكرية والأهداف المدنية يمثل الاشكال الأساسي التي تواجهه لأسلحة الذكاء الاصطناعي، ذلك أن افتقار هذه الأسلحة إلى الإدراك والمشاعر يجعلها غير قادرة على التمييز بين المدنيين والمقاتلين كما يميز البشر، ذلك أن تفسير النوايا والانفعالات في الحروب غير التقليدية التي غالبا ما يتعذر فيها تمييز المقاتلين إلا من خلال تفسير السلوك يشكل عائق كبير في تقييم نوايا الأشخاص، وبالتالي عدم القدرة على التفرقة بين الجريح وغير الجريح[2]، كما يصعب عليها القدرة على التمييز في الحالات التي يستسلم فيها الهدف البشري المشروع أو في الحالة التي يتخلى فيها عن سلاحه.

[1] - هاني محمد خليل إبراهيم العزازي، المرجع السابق، ص 1430

[2] - المرجع نفسه، ص 1439

أيضا يتعذر على الأسلحة المدعومة بالذكاء الاصطناعي لا سيما ذاتية التشغيل منها تحديد فيما إذا كان الهدف البشري يساهم بطريقة مباشرة في العمليات العدائية، خاصة وأن الدليل التفسيري للجنة الدولية للصليب الأحمر في هذا الصدد يتطلب فهم العلاقة السببية المباشرة بين العمل والضرر الناتج عنه، وهو شرط أساسي لاعتبار العمل مساهمة مباشرة في العمليات العدائية، وهذا ما لا يمكن لأسلحة الذكاء الاصطناعي تحديده.[1]

من جهة ثانية تزداد الصعوبة بالنسبة لهذه الأسلحة بالامتثال لمبدأ التمييز بين الأهداف المدنية والأهداف العسكرية، بسبب التحيزات الخوارزمية وهي الأخطاء أو التشوهات المنهجية التي تنشأ في مرحلة معالجة البيانات أو تطوير النماذج، أو عند استخدام النظام أو أثناء توجيه الضربات العسكرية، والتي تظهر في نتائج الخوارزميات، وعمليات البحث بسبب التحيزات الكامنة في البيانات فتنتج عنها نتائج غير صحيحة لفئات مختلفة بهدف تحقيق أهداف محددة.[2]

فالتحديد الخاطئ بسبب الاعتماد على خوارزميات ومدخلات بيانات غير دقيقة من شأنها أن تشوها عمليات صنع القرار وتقود إلى تبعات غير متوقعة منها الحاق أضرار بالمدنيين والأعيان المدنية.[3]

من جهة ثالثة ففرضية حدوث خلل تقني أو اختراق سيبراني في عمليات التنبؤ لأنظمة الذكاء الاصطناعي قد يؤدي إلى وقوع أخطاء في تقدير الأهداف العسكرية،

[1] - ماركو سوسولي، الأسلحة الذاتية التشغيل والقانون الدولي الإنساني، كتاب القانون الدولي الإنساني في النزاعات المسلحة المعاصرة، اللجنة الدولية للصليب الأحمر، دون سنة نشر، ص 155

[2] - محمود كمال الهنساوي، التوجه العسكري نحو الذكاء الاصطناعي وتأثيره على سباق التسلح التقليدي، مقال منشور في 21 ماي 2025، تاريخ الاطلاع 2025/7/28، على الساعة 22:10، متاح على الرابط التالي:

https://democraticac.de/?p=104653

[3] - Ali Zeineddine, op.cit, p 50

مما قد يؤدي بدوره إلى انتهاك مبدأ التمييز بين المدنيين والمقاتلين والأهداف العسكرية والأعيان المدنية.[1]

من أهم الأمثلة العملية على الإشكالات التي تثيرها أسلحة الذكاء الاصطناعي بخصوص مبدأ التمييز في النزاعات المسلحة، الأسلحة ذاتية التشغيل التي استخدمتها وتستخدمها إسرائيل في حربها على غزة حيث تبرز الممارسة كيف دمرت هذه الأسلحة خاصة الطائرات المسيرة العديد من المباني والمرافق العامة والمساجد والكنائس، وألحقت الخسائر في صفوف المدنيين من النساء والأطفال والشيوخ من غير المقاتلين.

ثانيا: انتهاك الأسلحة الذاتية التشغيل لمبدأ التناسب

يثير مبدأ التناسب إشكالات أخرى بالنسبة للأسلحة المدعومة بالذكاء الاصطناعي، فإذا كان مبدأ التمييز يرتبط بالمخاطر التي تهدد المدنيين والأعيان المدنية، فإن التناسب يرتبط بتقييم المزايا العسكرية المتوقعة من الهجمات العدائية[2]، والتي تعتبر عنصر أساسي في القانون الدولي الإنساني إذ يتم من خلالها تقييم ما إذا كان الهجوم على هدف عسكري مشروع أم لا.

لهذا فمبدأ التناسب يتطلب تقييما لمستوى الضرر الذي قد يلحق بالمدنيين والأعيان المدنية من جهة وتقييما مستمرا لقيمة الميزة العسكرية المكتسبة من جهة أخرى، وهذا ما لم يمكن تحقيقه بالنسبة للأسلحة المدعومة بالذكاء بالنظر لأن ساحة القتال تتغير باستمرار وفقا لخطط القائد وتطوير العمليات العسكرية على

[1] - مصطفى صلاح، دمج الذكاء الاصطناعي في المجال العسكري -الفرص والتحديات، مركز السلام للدراسات الاستراتيجية، المجلد الأول، العدد 4، 2019، ص 12

[2] - هاني محمد خليل إبراهيم العزازي، المرجع السابق، ص 1442

كلا الجانبين ومن ثم تكون عملية مقارنة الخبرة العسكرية المتوقعة مقابل الخسائر المدنية المتوقعة عملية.[1]

من جهة أخرى يتطلب امتثال الأسلحة المدعومة بالذكاء الاصطناعي لمبدأ التناسب تحديث مستمر

للمعلومات التي تحدد ما إذا كان من الجائز استهداف هدف معين أم لا وهذا يتطلب بدوره ارتباط هذه الأسلحة المستمر بالمشغل البشري، كما أن هذه الأسلحة المبرمجة بصورة مسبقة لا تملك القدرة على إلغاء أو تأجيل أو تعليق الهجوم لأن هدف ما غير مشروع.

الفرع الثاني: انتهاك الأسلحة الذاتية التشغيل لمبدأ الاحتياط أثناء الهجوم والضرورة العسكرية

من جهة ثانية تثير الأسلحة الذاتية التشغيل تساؤلات أخرى ترتبط بمدى مراعاتها لمبدأ الاحتياط أثناء الهجوم ومبدأ الضرورة العسكرية، خاصة بالنظر لما تتميز به من استقلالية في اتخاذ القرارات القتالية وغياب العنصر البشري الموجه.

أولا: انتهاك الأسلحة الذاتية التشغيل لمبدأ الاحتياط أثناء الهجوم

يمثل مبدأ الاحتياط أثناء الهجوم عقبة ثالثة في طريق استخدام الأسلحة المدعومة بالذكاء الاصطناعي في النزاعات المسلحة، حيث يثير إشكالات ليس لكون هذه الأسلحة غير قادرة على الامتثال لهذا المبدأ من مبادئ القانون الدولي الإنساني، بل لكون استخدام هذه الأسلحة يطرح العديد من التساؤلات والانشغالات أولها تلك التي تتعلق بالمدة التي يستوجب فيها على أسلحة الذكاء الاصطناعي الوفاء بهذا الالتزام فهل وجب مراعاة الاحتياطات والتدابير الوقائية عندما يتم تنشيط نظام السلاح أو عندما يكون النظام على وشك الانخراط في العمليات القتالية؟ أو يمتد

[1] - المرجع نفسه، ص 1441

التزامه طوال مدة مشاركته في هذه العمليات؟[1] وتكمن الصعوبة هنا كما ترى اللجنة الدولية للصليب الأحمر في البيئة المتغيرة التي تميز ساحة القتال.[2]

كما أنه ورغم إمكانية تقييم الخسائر المحتملة في صفوف المدنيين والأعيان المدنية في مرحلة برمجة الآلة، مما يجعل الاحتياطات والتدابير الوقائية المتخذة في هذه المرحلة فعالة، على نحو تجعل الأسلحة المدعومة بالذكاء الاصطناعي قادرة على الامتثال لمبدأ اتخاذ الاحتياط أثناء الهجوم، غير أن الاشكال الذي يطرح بالمقابل يدور حول مدى حول مصدقية هذا التقييم في ظل بيئة متغيرة. [3]

أما الاشكال الآخر الذي يثيره استخدام الأسلحة المدعومة بالذكاء الاصطناعي بالنسبة لمبدأ الاحتياط أثناء الهجوم هو الاشكال التي نهت إليه اللجنة الدولية للصليب الأحمر والمتعلق بجدوى الاحتياطات المتخذة عند استعمال هذا النوع من الأسلحة حيث ترى اللجنة في هذا الصدد بأن فاعلية الاحتياطات والتدابير الوقائية لا يرتبط بالسلاح بحد ذاته بل يتوقف على العديد من الفواعل وهم الأشخاص المسؤولون عن التخطيط للهجوم والأشخاص المكلفون باتخاذ قرار الهجوم والأشخاص المسؤولون على تنفيذ الهجوم[4] وهذا ما يجعل اعمال هذا المبدأ ضمنيا يتوقف على إبقاء الجندي البشري لغرض التحكم والاشراف.[5]

ثانيا: انتهاك الأسلحة الذاتية التشغيل لمبدأ الضرورة العسكرية

يجيز مبدأ الضرورة العسكرية استخدام القوة بالقدر اللازم لتحقيق هدف عسكري مشروع ، وبما لا يتجاوز ما تقتضيه العمليات العسكرية دون تجاوز ذلك،

[1] - دعاء جليل حاتم، المرجع السابق، ص 289

[2] - هاني محمد خليل إبراهيم العزازي، المرجع السابق، ص 1445

[3] - هاني محمد خليل إبراهيم العزازي، المرجع السابق، ص 1444

[4] - المرجع نفسه، ص 1444

[5] - دعاء جليل حاتم، المرجع السابق، ص 290

غير أن الأسلحة الذاتية التشغيل تطرح إشكالا حول مدى امتثالها لهذا المبدأ عمليا، بالنظر لما تنطوي عليه من استقلالية شبه كاملة في اتخاذ القرار باستخدام القوة دون تدخل بشري فوري، ذلك أن غياب التقدير البشري (بسبب استقلالية هذه الأسلحة) الذي يتيح تقييم التغييرات التي قد تطرأ في ساحة الحرب، وتكييف السلوك العسكري وفقا لتطور الأوضاع قد يؤدي ذلك إلى مواصلة هذه الأنظمة تنفيذ العمليات الهجومية رغم زوال الحاجة العسكرية رغم تغير الظروف مما يؤدي إلى استخدام مفرط أو غير مبرر للقوة.

وعليه فإن الاعتماد على هذه الأنظمة قد يفضي إلى خرق واضح لمبدأ الضرورة العسكرية من خلال تجاوز حدود الاستخدام المشروع للقوة وعدم مراعاة التوزان المطلوب بين الوسيلة والغاية العسكرية المرجوة.[1]

الخاتمة

في ختام هذه الدراسة نصل للقول بأن بروز الأسلحة المزودة بتقنية الذكاء الاصطناعي كالأسلحة الذاتية التشغيل التي باتت تستخدم اليوم في النزاعات المسلحة بشكل مضطرد، ورغم القدرات الفائقة التي تحوزها هذه الأسلحة وقدرتها على تحقيق أهدافها، إلا أن ذلك لا يحجب حقيقة خطورة هذه الأسلحة الفتاكة والمستقلة عن التحكم البشري في اتخاذ قراراتها، وهي الحقيقة الملموسة في ساحات القتال التي أبرزت العديد من الثغرات في الأسلحة المزودة بالذكاء الاصطناعي في مواجهة الامتثال لمبادئ القانون الدولي الإنساني حيث توصلنا على ضوء ما تقدم من الدراسة للنتائج الآتية:

-أن استخدام أنظمة الأسلحة المزودة بتقنيات الذكاء الاصطناعي خاصة الأسلحة الذاتية التشغيل تنطوي في النزاعات المسلحة محفوف بمخاطر تنبع من الميزات التي تتسم بهذه الأسلحة خاصة من ناحية استقلاليتها وقدرتها الذاتية على

[1] - ماركو ساسولي، المرجع السابق، ص 147

اتخاذ القرارات واختيار الأهداف ومهاجمتها تبعا للظروف المحيطة دون تدخل من مشغلها، وأيضا من ناحية ما تتسم به فتك بالنظر لما تسببه هذه الآلات من إصابات وخسائر في سبيل تحقيق الأهداف العسكرية دون مراعاة للاعتبارات الإنسانية أو لطبيعة المستهدف فيما إذا كان هدف مشروع أم لا

-أن استخدام الأسلحة الذاتية التشغيل في النزاعات المسلحة قد كشف عن ثغرات كبيرة في ساحات القتال في مواجهة مبادئ القانون الدولي الإنساني التي صممت لضمان الحماية للمدنيين والأعيان المدنية لا سيما مبدأ التمييز بين المقاتلين والمدنيين ومبدأ التناسب، ومبدأ الاحتياط أثناء الهجوم على نحو يقوض من تطبيق هذه المبادئ حيث أوضحت هذه الدراسة

محدودية إن لم نقل انتهاك الأسلحة المزودة بتقنية الذكاء الاصطناعي على التمييز بين المقاتلين والمدنيين وبين الأهداف العسكرية والأعيان المدنية، فضلا عما نتج عنها من مخاطر نتيجة الاستهداف العشوائي ما أدى إلى انتهاك كبير لمبدأ التناسب، وأيضا صعوبة الامتثال لمبدأ لمبد اتخاذ الاحتياطات اللازمة عند الهجوم بالنظر للبيئة المتغيرة التي تعمل وفقها هذه الأسلحة

-إن غياب الإطار القانوني المنظم لعمل الأسلحة المدعومة بالذكاء الاصطناعي من جهة، وغياب الرقابة البشرية والقدرة على التحكم في إدارة وتوجيه هذه الأسلحة عوامل تجعل من الصعوبة بمكان امتثال هذه الأسلحة لمبادئ القانون الدولي الإنساني

وعليه وبالنظر لما كشفت عنه التطبيقات العملية لهذه الأسلحة في العديد من النزاعات المسلحة التي تم فيها استخدام هذه الأسلحة، تعالت مطالبات دولية بحظر هذه الأسلحة لتعارضها مع مبادئ القانون الدولي الإنساني، رغم أن معالجة الإشكالات التي تثيرها هذه الأسلحة وضمان امتثالها لمبادئ القانون الدولي الإنساني أمر ممكن التجسيد على أرض الواقع دون الحاجة إلى حظرها، خاصة وأن الأسلحة

المزودة بتقنيات الذكاء الاصطناعي قد تكون أكثر دقة من الأسلحة التقليدية في إصابة الأهداف العسكرية، وهذا يمكن أن يتحقق عمليا انطلاقا من الاقتراحات الآتية:

-وضع إطار قانوني دولي عن طريق صياغة اتفاقيات دولية متعددة الأطراف تنظم الاستخدام الأخلاقي للأسلحة المزودة بالذكاء الاصطناعي (الأسلحة الذاتية التشغيل)، مع إمكانية حظر فئات أو نماذج محددة من هذه الأسلحة

-إعادة النظر ومراجعة الثغرات التي تنطوي عليها الأسلحة الذاتية التشغيل خاصة والتي كشفت عنها الممارسة العملية في أرض الواقع خاصة بالنسبة لمشكلة التحيز الخوارزمي وما نتج عنها عند استخدام السلاح وأثناء توجيه الضربات العسكرية.

قائمة المراجع:

أولا: المراجع باللغة العربية

1. الكتب

-تامر مصالحة، المبادئ الأساسية في القانون الدولي الإنساني، الطبعة الأولى 2009، دون دار نشر.

-فتحي محمد فتحي الحياني، القانون الدولي الإنساني وتطبيقاته على النزاعات المسلحة في العراق جمعية الأمل، العراق، 2022.

-اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة: تجديد الالتزام بالحماية في النزاعات المسلحة بمناسبة الذكرى السبعين لاتفاقيات جنيف، 2017.

- ماركو سوسولي، الأسلحة الذاتية التشغيل والقانون الدولي الإنساني، كتاب القانون الدولي الإنساني في النزاعات المسلحة المعاصرة، اللجنة الدولية للصليب الأحمر، دون سنة نشر.

2. المقالات الأكاديمية

- ايناس أبو حميرة، الأضرار الجانبية في النزاعات المسلحة في القانون الدولي الإنساني، مجلة العلوم القانونية والشرعية العدد 6، يونيو 2015

-خير الدين العايب، عبد الرحمن علي غنيم، الأسلحة الذاتية التشغيل، مجلة الدراسات الاستراتيجية والبحوث السياسية، المجلد 4، العدد 1، 2015

- دعاء جليل حاتم، الأسلحة ذاتية التشغيل في ضوء مبادئ القانون الدولي الإنساني، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، عدد خاص، 2020

-زينب عبد اللطيف خالد عبد اللطيف، المسؤولية الدولية المشتركة عن استخدام الذكاء الاصطناعي في الأعمال العسكرية في ظل قواعد القانون الدولي، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، القاهرة، المجلد 66، العدد 3، 2024

- سالم نسرين، أثر توظيف تقنيات الذكاء الاصطناعي عسكريا: دراسة في متغيري الحروب والنزاعات، مجلة القانون والعلوم البيئية، المجلد 3، العدد 1، 2024

- شهلاء كمال عبد الجواد، استخدام الأسلحة الذكية في الحرب وفق القانون الدولي الإنساني، مجلة العلوم القانونية والسياسية كلية القانون، جامعة الموصل، المجلد 10، العدد 37، 2021

- عبد القادر محمود محمد الأقرع، الروبوتات العسكرية في الحروب المستقبلية ومدى خضوعها لأحاكم القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق، الخرطوم، المجلد 8، العدد 3، 2020

- فاضل عبد الزهرة فاضل، المنظور الأخلاقي في استخدام الأسلحة ذاتية التشغيل، مجلة معهد العلمين للدراسات العليا، العدد 18، 2024

-مركز المستقبل للأبحاث والدراسات المتقدمة، كيف يدير الذكاء الاصطناعي دقة الحروب الحديثة، مقال منشور بتاريخ 20 مايو 2024، تاريخ الاطلاع 2025//1/7، على الساعة 17:45، متاح على الرابط التالي:

https://futureuae.com/ar-AE/Mainpage/Item/9281/ai-militarization

- لمياء محمد عبد السلام جواد، ضوابط استخدام الذكاء الاصطناعي في مجال التسليح العسكري في ضوء مبادئ القانون الدولي الإنساني، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 4، ديسمبر 2024

- محمود كمال البهنساوي، التوجه العسكري نحو الذكاء الاصطناعي وتأثيره على سباق التسلح التقليدي مقال منشور في 21 ماي 2025، تاريخ الاطلاع 2025/7/28، على الساعة 22:10، متاح على الرابط التالي: https://democraticac.de/?p=104653

- مصطفى صلاح، دمج الذكاء الاصطناعي في المجال العسكري -الفرص والتحديات، مركز السلام للدراسات الاستراتيجية، المجلد الأول، العدد 4، 2019

-هاني محمد خليل إبراهيم العزازي، التحديات التي تثيرها الأسلحة ذاتية التشغيل كأحد تقنيات الذكاء الاصطناعي، المجلة القانونية، جامعة القاهرة، المجلد 20، العدد 4، 2024

- يحي دايخ، الذكاء الاصطناعي في المجال العسكري: تطبيقات. مخاطر وتحديات قانونية وأخلاقية مقال منشور بتاريخ 2025/9/18، تاريخ الاطلاع: 2025/10/4، على الساعة 21:08، متاح على الرابط التالي:https://mnews.press/24173-2

3. الاتفاقيات والمواثيق الدولية

- اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية، المعقودة في 1907/10/18، مؤتمر لاهاي الثاني للسلام متاحة على الرابط التالي:

https://maqam.najah.edu/media/uploads/2022/04/legislations/Convention__IV__respecting_the_laws_and_customs_of_war_on_land.pdf

- البرتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة المعتمدة في 1949/8/12، والمتعلق بحماية ضحايا المنازعات المسلحة الدولية، المعتمد في 1977/6/8، المؤتمر الدبلوماسي لتأكيد القانون الدولي الإنساني المنطبق على المنازعات المسلحة الدولية وتطويره، النفاذ في 1978/12/7، متاح على الرابط التالي:

https://hrlibrary.umn.edu/arab/b094.html

- البرتوكول الإضافي الثاني الملحق باتفاقيات جنيف الأربعة المعتمدة في 1949/8/12، والمتعلق بحماية ضحايا المنازعات المسلحة غير الدولية، المعتمد في 1977/6/8، المؤتمر الدبلوماسي لتأكيد القانون الدولي الإنساني المنطبق على المنازعات المسلحة الدولية وتطويره، النفاذ في 1978/12/7 متاح على الرابط التالي:

https://www.ohchr.org/ar/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and-0

-تقرير الأمين العام للأمم المتحدة، الذكاء الاصطناعي في المجال العسكري وأثاره على السلام والأمن الدوليين، 2025/6/5، الجمعية العامة، الدورة 80. البند 101، ص 4، الفقرة 7 (ألف)، A/80/78

4. المقالات الصحفية

- مستقبل الحرب يبدأ من هنا: تايمز: روبوتات أوكرانية تقاتل رجالا روسا، مقال منشور بتاريخ 2025/2/10، موقع الجزيرة، تاريخ الاطلاع 2025/7/30، على الساعة 07:09، متاح على الرابط التالي:

https://www.aljazeera.net/politics/2025/2/10

- باندا وتالون وروني. ترسانة الروبوتات التابعة للجيش الإسرائيلي، مقال منشور في موقع الجزيرة بتاريخ 2024/11/12، تاريخ الاطلاع 2025/7/30، على الساعة: 22:23، متاح على الرابط التالي:

https://www.aljazeera.net/politics/2024/11/12/%D8%A8%

ثانيا: المراجع باللغة الأجنبية

- Ali Zeineddine, Law Artificial intelligence in Warfare: Legal and humanitarian challenges Under International humanitarian law, p 50, Date of acces,25 /7/2025, On 23 :14, Available at the link: https:// www.fmdbpub.com/user/journals/ article_details/FTSHS/279

-Agnieszka Szpak, Artificial intelligence and international humanitarian law in the work of the parties to the Conventional Weapons Convention: lethal autonomous weapons, Artificial intelligence and international human rights law, 2024

المسؤولية المدنية الناشئة

عن أضرار الذكاء الاصطناعي.

Civil Liability Arising

from Artificial Intelligence-Related Damages

د. سلام عبد الرحمان

جامعة وهران02 محمد بن أحمد، wahhab2308@hotmail.fr

ملخص:

تثير المسؤولية المدنية الناجمة عن الأضرار المترتبة على استعمال تقنيات الذكاء الاصطناعي إشكالية قانونية راهنة في ظل ما يشهده العالم من تطورات تكنولوجية متسارعة وتنام مستمر في الاعتماد على الأنظمة الذكية في مختلف القطاعات.

حيث يعزى جوهر هذه الإشكالية إلى محدودية قواعد المسؤولية المدنية التقليدية وعدم قدرتها على استيعاب الخصائص التقنية المعقدة والسمات الذاتية التي تميز الذكاء الاصطناعي، إذ إن هذه الأنظمة قد تحدث أضرارا يصعب إسنادها إلى شخص محدد كالمبرمج أو المنتج أو المستخدم، لا سيما في الحالات التي يعتمد فيها الذكاء الاصطناعي على اتخاذ قرارات مستقلة دون تدخل بشري مباشر، ويتفاقم التعقيد في هذا المجال عندما يمتلك الذكاء الاصطناعي القدرة على التعلم الذاتي والتكيف المستمر مع المعطيات البيئية المحيطة به، وهو ما يعقد من مهمة إثبات الخطأ، وإقامة العلاقة السببية، وتحديد الشخص المسؤول قانونا عن تعويض الضرر.

الكلمات المفتاحية: المسؤولية المدنية؛ الذكاء الإصطناعي؛ العلاقة السببية؛ الخطأ التقني؛ التعويض عن الضرر.

Abstract:

The civil liability arising from damages caused by the use of artificial intelligence (AI) technologies presents a pressing legal challenge.

This issue comes to the fore amidst rapid global technological advancements and the increasing reliance on smart systems across various sectors.

The core of this challenge lies in the limitations of traditional civil liability rules, which struggle to accommodate the complex technical characteristics and autonomous features of AI, AI systems can cause damages that are difficult to attribute to a specific individual, such as the programmer, manufacturer, or user.

This is particularly true when AI operates and makes decisions independently, without direct human intervention.

The complexity further intensifies when AI possesses the ability to self-learn and continuously adapt to its surrounding environment, this makes it significantly harder to prove fault, establish a causal link, and ultimately determine who is legally responsible for compensating the damage.

Keywords: *Civil Liability; Artificial Intelligence; Causal Link; Technical Fault; Damage Compensation*

مقدمة:

في ظل الثورة التكنولوجية المتسارعة، أصبح الذكاء الاصطناعي يمثل ركيزة أساسية في البنى الاقتصادية والاجتماعية والقانونية، مما أفرز تحديات قانونية غير مسبوقة تتعلق بمدى قدرة الأطر القانونية الحالية على مواكبة هذه التحولات الجذرية.

فمع تعقيد أنظمة الذكاء الاصطناعي وازدياد استقلاليتها في صنع القرار، تبرز إشكالية جوهرية تتمثل في عجز القواعد التقليدية للمسؤولية المدنية عن معالجة

الأضرار الناشئة عن هذه التقنيات، خاصة في حالات الضرر غير المنسوب إلى خطأ واضح من جانب شخص معين أو كيان محدد .

وعليه، يطفو على السطح تساؤل مركزي: هل يمكن للنظام القانوني القائم، بمنظومته الكلاسيكية في المسؤولية العقدية والتقصيرية، أن يقدم حلولا عادلة وفعالة لمتضرري أنظمة الذكاء الاصطناعي أم أن طبيعة هذه التقنيات تستدعي إرساء إطار تشريعي خاص، يرسم معالم المسؤولية ويوزع أعباءها بطريقة تستجيب لمتطلبات العدالة دون كبح جماح الابتكار؟ للإجابة على هاته الإشكالية سوف ندرس ذلك في مبحثين بحيث نتناول في الأول قصور قواعد المسؤولية المدنية التقليدية في مواجهة أضرار الذكاء الاصطناعي ، أما في المبحث الثاني سنتناول الموازنة بين الابتكار و حماية المتضررين.

المبحث الأول:

قصور قواعد المسؤولية المدنية التقليدية في مواجهة أضرار الذكاء الاصطناعي

يعد الذكاء الاصطناعي أحد الركائز الجوهرية في علوم الحاسب الآلي والرياضيات التطبيقية، حيث ساهم بشكل فعّال في تطوير البرمجيات والتقنيات الحديثة.

وتزداد أهمية هذا المجال في قطاعات متعددة، من بينها الطب والهندسة والزراعة وغيرها، نظرا لإمكاناته الواسعة في تقديم حلول تقنية متقدمة، لفهم أبعاد المسؤولية المدنية المرتبطة باستخدام تقنيات الذكاء الاصطناعي، من الضروري الوقوف بداية على تعريف هذا المفهوم واستعراض مراحل تطوره.

حيث ظهرت ملامح الذكاء الاصطناعي بوضوح منذ منتصف القرن العشرين، حيث برزت في عام 1946 أفكار أساسية مثل نظرية التشابك العصبي التي قدمها بيتس ووالتر ماكول وورين[1]، إلى جانب النموذج الحسابي الذي طرحه جون مكارثي في مؤتمر دارتموث عام 1956، والذي يُعتبر الانطلاقة الرسمية لمفهوم الذكاء الاصطناعي[2].

ومنذ ذلك الحين، شهد هذا المجال تطورات متسارعة جعلته قادرا على محاكاة السلوك البشري بمهارة، بما في ذلك التعلم واتخاذ القرارات المعقدة.

وفي عام 1967، أشار مارفن مينسكي إلى التحديات الكبيرة التي سيطرحها الذكاء الاصطناعي مستقبلا على العالم، ومع منتصف الثمانينات، بلغ حجم سوق برامج الذكاء الاصطناعي أكثر من مليار دولار، مما شجع الحكومات على الاستثمار بشكل موسع في هذا القطاع.

ورغم مرحلة التباطؤ التي مر بها في التسعينات، فقد استعاد الذكاء الاصطناعي زخمه لاحقا نتيجة للتطورات التكنولوجية المتلاحقة.

وتشير الدراسات المستقبلية إلى أن الذكاء الاصطناعي سيكون له أثر ثوري في مختلف جوانب الحياة البشرية، نظرًا لقدرته على معالجة وتحليل كميات ضخمة من

[1] -عبد الله موسي و أحمد بلال ،الذكاء الإصطناعي ثورة في تقنيات العصر دار الكتب المصرية ، ط1 ،القاهرة،2019،ص48.

[2] - زين عبد الهادي ،الذكاء الإصطناعي في إدارة أنشطة مؤسسة ،دراسة حالة مجموعة المؤسسات الإقتصادية،رسالة ماجيستر ،كلية العلوم الإقتصادية و العلوم التجارية،جامعة أم البواقي،الجزائر،2015/02/14،ص15و16.

البيانات وتقديم حلول مبتكرة في مجالات عدة، من بينها الطب والتشخيص والتصوير والتنبؤ بالأوبئة.

حيث يعد مشروع "روبوفيش" مثالاعلى ذلك، حيث تمكن في عام 2004 من إجراء عمليات جراحية دقيقة باستخدام تقنيات الذكاء الاصطناعي، مما يعكس الإمكانيات الكبيرة التي يحملها هذا المجال لمستقبل الإنسانية[1].

حيث هذا ما دفعنا إلى تناول هذا المبحث في مطلبين، بحيث تطرقنا في الأول إلى طبيعة قصور قواعد المسؤولية المدنية التقليدية في مواجهة أضرار الذكاء الاصطناعي، وتناولنا في المطلب الثاني إلى كيفية تعامل القوانين الحديثة مع خصائص الأضرار الناجمة عن الأنظمة الذكية

المطلب الأول: طبيعة قصور قواعد المسؤولية المدنية التقليدية في مواجهة أضرار الذكاء الاصطناعي

تبرز دراسة المسؤولية المدنية في مواجهة أضرار الذكاء الاصطناعي حجم الهوة القائمة بين القواعد التقليدية المستقرة وبين خصوصية هذه التكنولوجيا التي تعتمد على التعلم الذاتي واتخاذ القرار المستقل دون تدخل بشري مباشر.

إذ تبنى قواعد المسؤولية المدنية الكلاسيكية على ضرورة تحقق ثلاثة أركان أساسية هي الخطأ، والضرر، والعلاقة السببية بينهما، إلا أن هذه الأركان تواجه

[1] -صفات سلامة تكنولوجيا الروبوتات رؤية مستقبلية بعيون عربية المكتبة الأكاديمية، القاهرة،2006، ص45.

صعوبة بالغة في التطبيق عندما يتعلق الأمر بأضرار الذكاء الاصطناعي، سواء بسبب طبيعة النظام الذكي أو بسبب تعقيد العمليات المرتبطة بتشغيله.

فمن حيث العلاقة السببية، يصعب في كثير من الأحيان تحديد الصلة الدقيقة بين الفعل الضار والضرر الحاصل، في ظل استقلالية هذه الأنظمة في التعلم والتصرف، بل إن الغموض يزداد في حال تعدد الأطراف المتدخلة في تطوير وتشغيل النظام، من مبرمجين ومصنعين ومشغلين ومستخدمين نهائيين،هذا ما يجعل تحديد المسؤولية تحديا حقيقيا.

كما أن الغموض المرتبط بزمن ومكان تحقق الضرر يضيف بعدا إضافيا من التعقيد، حيث قد يقع الضرر بعد فترة من الفعل المسبب له، أو في أماكن متعددة، خلافا لما تفترضه القواعد التقليدية التي تنظر إلى الضرر على أنه حدث مادي مرتبط بزمن ومكان محددين وبشخص طبيعي أو اعتباري محدد.

حيث تضاف إلى هذه الإشكالات الطبيعة التقنية المعقدة للأضرار الناجمة عن الذكاء الاصطناعي، والتي غالبا ما تتطلب خبرة تقنية لفهم كيفية حدوثها، وهو ما يطرح تحديا أمام القاضي والمدعي في إثبات العلاقة بين الضرر والفعل المسبب له.

ويترتب على هذه الإشكالات، في النهاية، إضعاف مركز المتضرر الذي يجد نفسه عاجزا عن الحصول على تعويض كامل أو عادل، بسبب انعدام القدرة على تحديد المسؤول بدقة وفق الأطر القانونية التقليدية.[1]

[1] -شداد أمال عبير،المسؤولية المدنية عن الأضرار الناجمة عن الذكاء الإصطناعي ،مذكرة لنيل شهادة الماستر ،تخصص قانون خاص،جامعة غرداية،2024/06/22،ص47 إلى ص50.

حيث تنص المادة 124 من القانون المدني على أنه كل فعل أيا كان يرتكبه الشخص بخطئه، ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض[1].

المطلب الثاني: كيفية تعامل القوانين الحديثة

مع خصائص الأضرار الناجمة عن الأنظمة الذكية

لمواكبة خصوصية الأضرار الناتجة عن الأنظمة الذكية تسعى القوانين إلى ابتكار أليات علاجية تتجاوز القصور في القواعد التقليدية من خلال:

*تقتضي الضرورة القانونية ضبط نطاق المسؤولية على نحو دقيق يشمل جميع الأطراف ذات الصلة، بمن فيهم مطورو الأنظمة، والمصنّعون، والمستخدمون، وأحيانًا مزودو البيانات، مع إمكانية ترتيب المسؤولية بينهم على أساس مشترك أو تضامني بحسب طبيعة الأضرار المرتكبة. ويأتي هذا التوجه بهدف سد أي فراغ تشريعي محتمل، وضمان حماية المتضررين على نحو فعال وعادل[2].

*يعد تبني مبدأ المسؤولية الموضوعية أو ضمان الاضرار توجها عمليا في مواجهة الاضرار الناشئة عن انظمة الذكاء الاصطناعي اذ يعفى المتضرر من عبء اثبات الخطأ في سلوك النظام أو في فعل الفاعل ويكتفى بقيام الضرر الناتج عن تشغيل النظام

[1] -القانون05-10 المؤرخ في 2005/06/20 المتضمن القانون المدني المعدل و المتمم.

[2]- https://wadaq.info/%d8%a7%d9%84%d9%85%d8%b3%d8%a4%d9%88%d9%84%d9%8a%d8%a9-%d8%a7%d9%84%d9%85%d8%af%d9%86%d9%8a%d8%a9-%d9%88%d8%a7%d9%84%d8%b0%d9%83%d8%a7%d8%a1-%d8%a7%d9%84%d8%a7%d8%b5%d8%b7%d9%86%d8%a7%d8%b9%d9%8a/,20/07/2025,16h00.

ويسهم هذا التوجه في تسهيل اجراءات التعويض لا سيما في ظل التعقيد البنيوي والتقني الذي تتميز به الخوارزميات وما يرافقه من غياب

للشفافية وصعوبة التتبع مما يجعل اثبات الخطأ أمرا بالغ الصعوبة في الكثير من الحالات[1].

*ضرورة تطوير آليات تقدير الضرر لتشمل الأضرار غير المادية والمعقدة، كالانتهاكات الرقمية والإخلال بالخصوصية، إضافة إلى الأضرار المستقبلية المحتملة الناتجة عن قرارات أنظمة الذكاء الاصطناعي، مع السعي لتعزيز شفافية والتوصل مع المجتمع هذه الأنظمة بما يضمن إمكانية مراجعتها ومساءلتها، تحقيقا للعدالة وتكريسا لحق المتضرر في التعويض العادل[2].

حيث ينص الدستور المادة 47 على أن حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي[3]، و هو ما أكده المرسوم الرئاسي 20-05 المؤرخ في 2020/01/20[4] ، وكذا المرسوم الرئاسي 21-439 المؤرخ في 2021/11/07[5].

[1] -عبد الرحمن الحارثي و علي الدروبي ،تأرجح الضرر الناشيء عن الذكاء الاصطناعي بين المسؤوليتين الشخصية و الموضوعية،دراسة تحليلية نقدية،مجلة جامعة الشارقة للعلوم القانونية،مجلد 22 عدد1،سنة 2025،ص402 و 413.

[2] -لعمارة طارق زياد و ميمون سفيان،المسؤولية المدنية الناشئة عن استخدام تقنيات الذكاء الاصطناعي في التشريع الجزائري،مذكرة لنيل شهادة الماستر،جامعة محمد بوضياف مسيلة،تخصص قانون الأعمال،2024/06/01،ص41.

[3] -دستور الجزائري ،الجريدة الرسمية ،العدد 82 ،الصادرة في 2020/12/20،ص13.

[4] -مرسوم رئاسي 20-05،مؤرخ في 2020/01/20،يتضمن وضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[5] -المرسوم الرئاسي 21-439 المؤرخ في 2021/11/07 المتضمن إعادة تنظيم الهيأة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام و الاتصال و مكافحتها.

*اعتماد أنظمة تأمين خاصة ومسارات تعويض جماعي لتغطية أضرار الذكاء الاصطناعي بشكل عملي وفعّال، إضافة إلى إنشاء هيئات مختصة لمراقبة وتقييم المخاطر والتصرف في القضايا الناشئة عن هذه التكنولوجيا وتطوير تشريعات مرنة ومحدثة بشكل دوري تسمح بمراجعة القواعد مع تطور التكنولوجيا، تعكس التوازن بين تشجيع الابتكار وحماية الحقوق وضمان التعويض العادل للمتضررين[1].

بهذه الطرق يمكن للقوانين الجديدة أن تلعب دورا هاما في ضبط المسؤولية المدنية المرتبطة بالذكاء الاصطناعي، متجاوزة ضعف القواعد التقليدية، وضامنة حماية قانونية مناسبة في عصر الأنظمة الذكية.

المبحث الثاني:

أنواع المسؤولية المدنية الناشئة عن أضرار الذكاء الاصطناعي

تشهد البيئة القانونية المعاصرة تحولات نوعية عميقة في ضوء التوسع المتزايد لتطبيقات الذكاء الاصطناعي عبر طيف واسع من القطاعات الحيوية، الأمر الذي يستدعي إعادة النظر في الأسس التقليدية للمسؤولية المدنية وآليات تطبيقها في السياق التكنولوجي الراهن، إذ تطرح هذه التقنيات المبتكرة تحديات استثنائية أمام المنظومة القانونية، تتجلى في ضرورة إرساء معايير واضحة لتحديد نطاق المسؤولية والالتزامات المترتبة على الأطراف المتعددة في سلسلة تطوير واستخدام هذه الأنظمة.

[1] -حمدادو لمياء،الذكاء الاصطناعي:نموذج عن التحديات المعاصرة للمسؤولية التقصيرية،المجلة الجزائرية للقانون و العدالة ،مجلد10،عدد1، سنة2024 ،ص152 الى ص160.

حيث متى كانت أنظمة الذكاء الاصطناعي تحمل في طياتها إمكانات هائلة لارتقاء بالمجتمع البشري وتحسين جودة الحياة، فإنها في المقابل تنطوي على مخاطر محتملة قد تفضي إلى أضرار بالغة الخطورة. وهنا يبرز التحدي الأساسي المتمثل في صياغة إطار قانوني متوازن يحقق المواءمة بين تعزيز الابتكار التكنولوجي من جهة، وضمان الحماية الفعالة للحقوق الفردية والمصالح المجتمعية من جهة أخرى، بما يستدعي إعادة تقييم مدى كفاية القواعد التقليدية للمسؤولية المدنية في مواجهة هذه المستجدات، والحاجة إلى تطوير اليات تشريعية مبتكرة تتناسب مع خصوصية هذا المجال.

المطلب الأول: الأساس التعاقدي للمسؤولية المدنية الناشئة عن إخلال أنظمة الذكاء الاصطناعي

تتأسس المسؤولية المدنية الناشئة عن إخلال أنظمة الذكاء الاصطناعي بالأساس على المبادئ التقليدية للمسؤولية العقدية، حيث يشكل العقد بين الأطراف المصدر القانوني الرئيس للالتزام ومسؤولية التعويض عند الإخلال، ومع ذلك، يفرض الطابع التقني والفني للذكاء الاصطناعي خصوصيات تميزها عن الأليات أو الأداء البشري التقليدي، وهو ما يستوجب تكييف قواعد المسؤولية العقدية بما يتناسب مع طبيعة هذه الأنظمة[1].

[1] -مروان منصور نعيم السكيني،وائل عزت عبد الهادي مبارك،خصوصية المسؤولية المدنية الناشئة عن استخدام أنظمة الذكاء الاصطناعي،المجلة القانونية متخصصة في الدراسات و البحوث القانونية،المجلد23 ،العدد02،فيفري 2025 ،ص681الى ص685.

- عند وجود عقد ينظم العلاقات بين المطور أو المزود من جهة والمستخدم أو المتعاقد الاخر من جهة مقابلة، يكون الالتزام التعاقدي محددا في شروط استخدام النظام الذكي، ومدى مطابقته للمواصفات والوظائف المتفق عليها، فإذا انتفى تحقيق هذه الوظائف أو حصل عيب في الأداء، ساق ذلك ضررا لأحد الأطراف، يعد الإخلال بهذا الالتزام مبررا لإقامة دعوى المسؤولية العقدية ضد المطور أو المزود.

ففي أوروبا متى كان الروبوت غير مطابق للعقد يحق للمشتري إنهائه وتتجلى المسؤولية العقدية عند عدم قيام الروبوت بما تضمنه العقد حتى ولم ينجم أي أدى وهذا ما يلزم بالضرورة تعويض المشتري[1].

- يتميز هذا الالتزام بأشكال عدة، منها: التزام ببذل عناية (أي مراعاة معايير الحرفية والحذر في الأداء) أو التزام بتحقيق نتيجة (كالأنظمة الذكية التي تقدم نتائج محددة مثل التشخيص الطبي أو التحليل المالي)، ويترتب على ذلك أنه إذا لم تتحقق النتيجة المتفق عليها، يفهم ذلك على أنه إخلال بالعقد، ما يستوجب التعويض، والتعويض نوعان التعويض النقدي والغير النقدي، كما يعد التعويض العيني أفضل وسيلة لجبر الضرر، وهذا يتطلب في العقود التقنية دقة في صياغة نطاق الالتزامات وبيان مستوى الأداء المطلوب بوضوح[2].

[1] -نور خالد عبد الرزاق ،المسؤولية المدنية الناشئة عن استخدام الذكاء الإصطناعي،مجلة التحديات و الافاق القانونية و الاقتصادية للذكاء الاصطناعي،المجلد 66،العدد3،جانفي 2024،ص14 و ص15.

[2] https://wadaq.info/%D8%AA%D8%A3%D8%AB%D9%8A%D8%B1-%D8%A7%D9%84%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7-%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D8%AD%D9%82%D9%88%D9%82/ - 21/07/2025,11h00.

- تعقيد الذكاء الاصطناعي وقدرته على التعلم الذاتي والتطور تخلق صعوبة في إثبات علاقة السببية بين الخلل والضرر، خاصة إذا حصل تطور غير متوقع أدى إلى النتائج الضارة[1].

حيث يحتمل أن يلجأ القضاء إلى اعتماد قواعد فقهية مجربة، من بينها تفسير بنود العقد بما يحقق حماية الطرف الأضعف في العلاقة التعاقدية، أو تطبيق مبدأ ضمان العيب الخفي في حال ثبوت وجود خلل جوهري في نظام الذكاء الاصطناعي عند التسليم[2]، دون أن يكون للمستخدم علم بذلك العيب[3]، الأمر الذي يسهم في تعزيز دور الحماية القانونية للطرف المتضرر وفرض التعويض المناسب و هذا ما نصت عليه المادة 176 من القانون المدني الجزائري أنه في حالة استحالة أو تأخر تنفيد المدين للالتزام العيني حكم عليه بالتعويض و هو ما يتطابق مع المشرع المصري في المادة215 من القانون المدني المصري.

على صعيد الصياغة التعاقدية، تعد بنود تحديد المسؤولية في عقود التقنية المتصلة بأنظمة الذكاء الاصطناعي ذات أهمية بالغة، إذ تمكن الأطراف، لا سيما المطور أو المزود، من تقييد نطاق مسؤوليتهم في حالات معينة.

[1] -محمد السعيد السيد ،نحو اطار قانوني شامل للمسؤولية المدنية من أضرار نظم الذكاء الإصطناعي غير المراقب،مجلة البحوث القانونية و الإقتصادية،جامعة المنصورة،2021،ص320.

[2] - M. Assunta Cappeli, “regulation on safety and civil liability of intelligent autonomous robots: the case of smart cars”, Ph. D thesis, universita degli studidi Trento, 2014, p. 131-132.

[3] - S. Oliveira, “La responsabilité civile dans les cas de dommages causés par les robots d’assistance au Québec”, LL.M, faculté de droit, université de montréal, 2016, p.141/145.

حيث يمكن لهذه البنود أن تغطي سيناريوهات مثل التحديثات غير المراقبة التي يجريها المستخدم للنظام، أو الاستخدام غير المرخص له الذي يخرج عن الإطار التعاقدي المتفق عليه[1].

غير أن هذه النصوص لا تطلق بغير قيد، بل تخضع لرقابة قضائية صارمة في التشريع الجزائري. هذه الرقابة تهدف إلى التحقق من مشروعية هذه البنود وتناسبها مع مبدأ التوازن العقدي، الذي يضمن عدم إفراغ حق الطرف المتضرر في التعويض من مضمونه الجوهري حسب المادة 106 ، 107 و 110من القانون المدني الجزائري.

فالتشريع الجزائري يشدد على ضرورة احترام القواعد العامة للمسؤولية، التي تعنى بجبر الضرر الناجم عن الإخلال بالالتزام القانوني أو التعاقدي حسب ما نص عليه القانون المدني في المادة 119 و 122 من القانون المدني الجزائري.

وتأتي أهمية هذه الرقابة القضائية، خاصة في ظل عقود نقل التكنولوجيا والعقود الإلكترونية، لضمان ألا تستخدم هذه البنود لإعفاء أحد الأطراف كليا من المسؤولية، أو لفرض شروط تعسفية على

الطرف الأضعف في العقد و هو ما تطابقه المادة 1171 من القانون المدني الفرنسي [2] .

[1] -حويلي سلوى،المسؤولية المدنية للمستثمر في عقود نقل التكنولوجيا في التشريع الجزائري،أطروحة لنيل شهادة الدكتوراة ،تخصص قانون الإستثمار،جامعة العربي بن مهيدي ،أم البواقي،الجزائر،2022-2023،ص11-20.

[2]- https://web.lexisnexis.fr/newsletters/avocats/10_2016/dossier4.pdf,21/07/2025,13h00.

فالمشرع الجزائري يولي أهمية كبرى لضمان حسن النية في تنفيذ العقد، وهو مبدأ يمتد ليشمل مرحلة صياغة الشروط والبنود المتعلقة بالمسؤولية.

ولذلك، فإن أي بند يسعى إلى تقييد المسؤولية يجب أن يكون واضحا ومحددا، وألا يؤدي إلى إهدار مبدأ التعويض الكامل عن الأضرار الناجمة عن الإخلال بالالتزامات الأساسية للعقد.

بمعنى اخر، تسعى المنظومة القانونية الجزائرية إلى تحقيق توازن دقيق بين حرية التعاقد وضرورة حماية الحقوق، خاصة في ظل التطورات المتسارعة في مجال الذكاء الاصطناعي .

-لا بد من التأكيد على أن الذكاء الاصطناعي، بوصفه أداة تقنية، لا يكتسب أهلية التعاقد، ومن ثم لا يمكن اعتباره طرفا في العقد على نحو مستقل، وبالتالي، فإن المسؤولية الناجمة عن الإخلال بالالتزامات المتفق عليها تقع على عاتق الأشخاص الطبيعيين أو المعنويين القائمين على تصميم النظام أو تشغيله أو توريده، بحسب دور كل منهم في العلاقة التعاقدية.

حيث يقتضي ذلك ضرورة تحديد نطاق التزامات ومسؤوليات كل طرف بدقة ضمن بنود العقد، بما يحقق وضوح الأساس القانوني للمسؤولية، ويراعي الخصوصيات التقنية للنظام المستخدم، لتفادي النزاعات وتسهيل إثبات المسؤولية

حال وقوع الضرر و أن أنظمة الذكاء الاصطناعي تعتبر من قبل السلع بمفهوم المنتج في مجال حماية المستهلك [1].

المطلب الثاني: المسؤولية التقصيرية الناشئة

عن أضرار أنظمة الذكاء الإصطناعي

مع التوسع السريع في استخدام أنظمة الذكاء الاصطناعي (AI)، برزت إشكاليات قانونية معقدة، لعل أبرزها تلك المرتبطة بـ المسؤولية التقصيرية الناجمة عن الأضرار التي قد تنجم عن هذه الأنظمة. فكلما زادت قدرة هذه الأنظمة على اتخاذ القرارات بشكل مستقل وتنفيذ الأوامر دون تدخل بشري مباشر، تعاظم التساؤل حول تحديد الجهة التي تتحمل المسؤولية القانونية عند وقوع الضرر، وإزاء الطبيعة التقنية المعقدة للذكاء الاصطناعي، تبدو الأطر القانونية التقليدية عاجزة في كثير من الأحيان عن استيعاب هذه الخصوصية أو تحديد المسؤولية بشكل دقيق.

تبنى المسؤولية التقصيرية في أصلها على ضرورة إثبات خطأ أو إهمال نتج عنه ضرر، وقد تطبق في بعض السياقات وفق مبدأ المسؤولية الموضوعية التي تُغني عن إثبات الخطأ وتكتفي بتحقق الضرر. غير أن تطبيق هذه المبادئ التقليدية على الأضرار الناجمة عن أنظمة الذكاء الاصطناعي يواجه صعوبات عملية وقانونية، من أبرزها:

[1] -شبلي فضيل،بوسعيد محمد،المسؤولية المدنية عن تطبيقات الذكاء الإصطناعي في القانون الجزائري،مذكرة لنيل شهادة الماستر،تخصص قانون خاص،جامعة عين تموشنت،الجزائر،2023-2024،ص40.

-**إشكالية تحديد الفاعل**: تختلف أنظمة الذكاء الاصطناعي الحديثة، خصوصا تلك القائمة على التعلم العميق (Deep Learning)، عن الألات التقليدية في كونها قادرة على التعلم والتكيف المستمر بشكل مستقل عن برمجتها الأصلية. هذا الطابع الديناميكي لهذه الأنظمة يعقد من عملية تتبع السبب المباشر للضرر وإرجاعه إلى برمجة أو قرار بشري محدد،الأمر الذي يطرح تساؤلامحوريا: هل يُسند الخطأ إلى المبرمج الذي وضع الخوارزميات، أو إلى المصنع الذي صمم النظام، أو إلى المستخدم الذي قام بتشغيله، أم يُمكن القول بتحمل النظام ذاته للمسؤولية في حال بلوغه درجة عالية من الاستقلالية؟[1]

-غموض مفهوم الخطأ في سياق الذكاء الاصطناعي:

يشكل إثبات الخطأ أحد الأركان الجوهرية للمسؤولية التقصيرية، إذ يستلزم قيام عنصر الإهمال أو التقصير من جانب شخص طبيعي أو اعتباري يملك الإرادة والقدرة على التمييز،غير أن اعتماد أنظمة الذكاء الاصطناعي على معالجة مستقلة ومعقدة للبيانات واتخاذ قرارات ذات طابع تنبؤي، يثير إشكالية قانونية عميقة تتعلق بإمكانية إسناد الخطأ إلى إرادة بشرية محددة.

فهل يعد القرار الخاطئ الصادر عن نظام الذكاء الاصطناعي خطأ ينسب إلى الجهة المطورة للنظام باعتباره خللا في تصميم الخوارزمية؟ أم يمكن إرجاعه إلى قصور

[1] - Barfield, Woodrow, and Ugo Pagallo, eds. Research Handbook on the Law of Artificial Intelligence. Edward Elgar Publishing, 2018, pp. 125-140.

في جودة البيانات المستعملة في مراحل التعلم الآلي؟ أم أننا بصدد خطأ ذاتي صادر عن النظام نفسه خلال عمليات التعلم والتحليل التي يجريها بشكل مستقل؟

إن هذه الإشكالية تطرح تساؤلا حول مدى حاجة القانون إلى إعادة تعريف مفهوم "الخطأ" في ظل التطورات التقنية المتسارعة، على نحو يراعي خصوصية الأنظمة الذكية واستقلاليتها النسبية، وبما يضمن التوازن بين حماية المتضررين وتحفيز الابتكار التكنولوجي، مع الحفاظ على يقين النظام القانوني وعدالته[1].

تكتسب المسؤولية التقصيرية مكانة جوهرية في مجال الذكاء الاصطناعي، لإمكان نشوئها خارج نطاق العلاقة التعاقدية، مع ازدياد انتشار الأنظمة الذكية وتطور استقلالية عملها وتفرض هذه المسؤولية تحديات قانونية جديدة تستلزم تطوير القواعد التقليدية في كل من التشريع الجزائري والفرنسي، بما يواكب تعقيدات الذكاء الاصطناعي.

تعني المسؤولية التقصيرية إلزام المحدث للضرر بالتعويض بناءا على إخلال قانوني أو إهمال، دون الحاجة لعلاقة تعاقدية ومع الذكاء الاصطناعي، تبرز إشكالية تحديد مرتكب الخطأ، بسبب قدرة الأنظمة الذكية على اتخاذ قرارات ذاتية خارجة عن تصور المبرمج التقليدي، فضلاً عن صعوبة التنبؤ بتصرفاتها أو إحكام السيطرة التقنية عليها بما يرفع من احتمال وقوع أضرار غير متوقعة[2].

---

[1] -ريم خلفان سعيد راشد الكندي،النطاق الشخصي للمسؤولية الجنائية عن أخطاء الذكاء الإصطناعي،رسالة الماجستير،جامعة الشارقة،ديسمبر2024،ص02 –ص15.

[2]https://mawdoo3.com/%D8%A7%D9%84%D9%85%D8%B3%D8%A4%D9%88%D9%84%D9%8A%D8%A9_%D8%A7%D9%84%D8%AA%D9%82%D8%B5%D9%8A%D8%B1%D9%8A%D8%A9_%D9%81%D9%8A_%D8%A7%D9%84%

"يعتبر ولوج أنظمة الذكاء الإصطناعي لبيئتنا الاجتماعية تحدي حقيقي لقانون المسؤولية المدنية، إذ تبدو هذه الأخيرة غير قادرة على تغطية أضرار الذكاء الاصطناعي وفق آلياتها الكلاسيكية"[1].

1- المسؤولية عن الخطأ

في الإطار التقليدي، تقوم المسؤولية التقصيرية على إثبات الخطأ، والضرر، والعلاقة السببية بينهما، ويلزم القانون المدني الجزائري في المادة 124 كل من يرتكب فعلا سبب ضررا للغير بالتعويض، مع إلزامية إثبات ركن الخطأ والتمييز في سن محددة (16 سنة) وهذا ما دطره المشرع الفرنسي في المادة 1382 من القانون المدني الفرنسي[2].

أما في حالات الذكاء الاصطناعي، يصعب إثبات الخطأ بدقة بسبب استقلالية النظام وزيادة تعقيده، لذلك، يتجه الفقه الحديث إلى توسيع مفهوم الخطأ ليشمل الإخلال بمعايير الحذر التقنية أو الإهمال في التكوين أو البرمجة أو الرقابة على النظام الذكي[3].

D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D9%85%D8%AF%D9%86%D9%8A_%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D8%B1%D9%8A?utm_so%D8%AF%D8%AF%D8%AF,21/07/2025,16h05.

[1] -حمدادو لمياء،الذكاء الإصطناعي:نموذج عن التحديات المعاصرة للمسؤولية التقصيرية،مرجع سابق،ص137-ص139.

[2] -عبدو أحمد ،دروس في القانون المدني،الجزء الثاني،النظرية العامة للإلتزام ،ألقيت على طلبة السنة الثانية حقوق،جامعة البليدة02، 2022/2021،ص12-ص 45.

[3] -عيسى الحربي،محاولة تأطير المسؤولية التقصيرية للذكاء الإصطناعي وفقا لنظام المعاملات المدنية السعودي ،مجلة كلية الدراسات الإسلامية و العربية للبنات بالإسكندرية،المجلد40،العدد03،مارس2024،ص2476-2488.

2- المسؤولية الموضوعية

تعتمد المسؤولية الموضوعية على الضرر والعلاقة السببية فقط، دون اشتراط إثبات الخطأ،و تبرز أهميتها في الأنشطة والمنتجات عالية الخطورة أو التقنية، ومنها أنظمة الذكاء الاصطناعي، خاصة عندما يصعب تحديد الخطأ البشري أو الفني[1].

أقر التشريع الجزائري صوراً للمسؤولية الموضوعية في حالات فعل الغير أو فعل الشيء (المواد من 134 إلى 140 مدني جزائري).

أما في فرنسا، فقد توسعت المسؤولية الموضوعية لتشمل المنتجات المعيبة وكل شخص تحت سلطته الشيء الضار، كما هو مبين في التطورات الفقهية والقضائية الحديثة.

وعن جدوى المسؤولية الموضوعية في الذكاء الاصطناعي:

*توفر حماية فعالة وسريعة للمضرورين[2].

*تدفع المصنعين والموردين نحو زيادة الحذر وضبط المنتجات الذكية.

*تتناسب مع صعوبة تحديد المتسبب الحقيقي في الضرر الناتج عن النظام الذكي.

[1] -بلعباس أمال ،مدى ملاءمة قواعد المسؤولية المدنية لتعويض عن أضرار النظم الذكية،مجلة البحوث القانونية و الاقتصادية،المجلد06،العدد2023،01،ص466-ص472.

[2] -عبد الرحمان الحارثي،تأرجح الضرر الناشيء عن الذكاء الاصطناعي بين المسؤوليتين الشخصية و الموضوعية "دراسة تحليلية نقدية"،مرجع سابق،ص01.

3- المسؤولية المختلطة أو المعيارية

يتجه النقاش القانوني نحو إيجاد نظام مختلط يوفق بين العقدية والتقصيرية لاستيعاب طبيعة الأضرار الذكية، من خلال اجتهادات فقهية، أو إدراج قواعد خاصة كما في مشروع القانون الأوروبي للذكاء الاصطناعي، حيث يسمح ذلك بتوزيع الأعباء القانونية بين المصنع، المزود، المستخدم النهائي، وإلزامهم بتدابير وقائية وحلول تأمينية جماعية لضمان جبر الضرر بفعالية أكبر[1].

لا يزال القانون الجزائري يعتمد في الأساس على القواعد العامة للمسؤولية التقصيرية دون نصوص خاصة عن الذكاء الاصطناعي، مع دعوة فقهية متزايدة لتطوير التشريع ووضع أنظمة خاصة لتوزيع المسؤولية عن الأضرار الذكية[2].

التشريع الفرنسي يشهد مناقشات مستمرة وعدة مشاريع لإصلاح نظرية المسؤولية المدنية (كإصلاح 2017) تهدف للانتقال من مسؤولية الخطأ إلى تغليب ركن الضرر، مع التأكيد على تطبيق المسؤولية الموضوعية خاصة بالأضرار غير المتوقع مصدرها[3].

[1] https://ar.m.wikipedia.org/wiki/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1_%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A?,21/07/2025,16h50.

[2] -حمدادو لمياء، الذكاء الإصطناعي:نموذج عن التحديات المعاصرة للمسؤولية التقصيرية،مرجع سابق،ص157-ص159.

[3] -محمد عرفان الخطيب،الإستشراف المستقبلي لمبدأ وحدة المسؤولية المدنية في التشريع المدني الفرنسي الحديث قراءة في فلسفة مشروع قانون اصلاح نظرية المسؤولية:دراسة تحليلية معمقة،مجلة كلية القانون الكويتية العالمية ،العدد31، سبتمبر2020،ص285.

يسعى القانون الأوروبي للذكاء الاصطناعي إلى تصنيف الأنظمة حسب درجة الخطورة، ووضع التزامات صارمة لمزودي ومطوري الأنظمة، وتشديد معايير الشفافية وإدارة المخاطر، مع إمكانية تطوير آليات جديدة لجبر الضرر خارج المنطق التعاقدي التقليدي[1].

حيث تتجلى أليات تجاوز قصور القواعد التقليدية في المسؤولية التقصيرية:

-تكييف الشروط الإثباتية لتلائم تعقيدات البرهنة التقنية في الذكاء الاصطناعي.

-توزيع المسؤوليات قانونيا بين المطور والمزود والمستخدم النهائي.

-تضمين قواعد متخصصة لحصر أو الحد من المسؤولية عندما يكون الضرر بسبب استعمال غير مشروع من قبل المستخدم.

-فرض التغطية التأمينية الإلزامية لمنتجي الأنظمة الذكية.

الخاتمة:

لقد كشف التقدم المتسارع في تقنيات الذكاء الاصطناعي وتطبيقاته المتنوعة في شتى مجالات الحياة عن تحديات قانونية غير مسبوقة أمام الأطر القانونية التقليدية، ولا سيما في ميدان المسؤولية المدنية، إذ رغم ما تمنحه هذه التقنيات من

[1]https://ar.m.wikipedia.org/wiki/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1_%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A?utm,21/07/2025,17h00.

فرص للنهوض بجودة الحياة وتحقيق الكفاءة الاقتصادية، فإنها تثير إشكالات جوهرية تتعلق بتحديد المسؤولية القانونية عن الأضرار التي قد تنشأ عن استخدامها.

وقد أوضح هذا البحث أن النظريات الكلاسيكية للمسؤولية المدنية، سواء تلك القائمة على الخطأ أو على المخاطر، تواجه صعوبات عملية في استيعاب خصائص الذكاء الاصطناعي، الذي يتميز بقدرته على التعلم الذاتي واتخاذ القرار المستقل، وهو ما يؤدي إلى تعقيد مسألة إثبات العلاقة السببية والخطأ وفق التصورات التقليدية.

وفي ضوء هذه المستجدات، تبرز ضرورة تطوير إطار قانوني متوازن يتوافق مع متطلبات العصر الرقمي، إطار قادر على حماية حقوق المتضررين وضمان حقهم في التعويض، دون أن يشكل ذلك عائق أمام مسار الابتكار التقني ويستلزم هذا الإطار قدرا من المرونة القانونية التي تمكنه من مواكبة التطورات التقنية المستمرة في هذا المجال.

كما يتضح أن معالجة هذه الإشكالات لا يمكن أن تظل حبيسة الأطر القانونية الوطنية، بل يجب الانفتاح على التعاون الدولي بهدف إرساء معايير موحدة تكفل الحماية القانونية للأفراد والمجتمعات في بيئة رقمية متصلة، ولعل التجارب المقارنة تقدم نماذج عملية يمكن الاستفادة منها لصياغة إطار قانوني عربي متقدم يستجيب لمقتضيات العدالة والفعالية في ان واحد.

وهذا ما دفعنا لطرح جملة من التوصيات:

أولا: على الصعيد التشريعي

-استحداث نصوص تشريعية خاصة بالذكاء الاصطناعي تضع نظامًا تدريجيًا للمسؤولية يرتبط بدرجة استقلالية النظام ودرجة المخاطر المرتبطة باستخدامه، مع تحديد معايير واضحة لتصنيف هذه الأنظمة حسب مستويات الخطورة.

-إنشاء صندوق وطني لتعويض ضحايا أضرار الذكاء الاصطناعي، بتمويل من رسوم تفرض على المطورين والمستفيدين التجاريين، لضمان السرعة والعدالة في التعويض.

-إلزامية التأمين على المنتجات والخدمات التي تعتمد على أنظمة ذكاء اصطناعي عالية الخطورة، مع تحديد حد أدنى للتغطية التأمينية.

ثانيا: على الصعيد التنظيمي

-إنشاء هيئة وطنية متخصصة في تنظيم تقنيات الذكاء الاصطناعي، تتولى وضع معايير تقنية وأخلاقية وتشرف على تطبيقها وتقييم المخاطر المصاحبة لها.

-إرساء نظام ترخيص وإشهاد للتطبيقات عالية المخاطر، مع فرض متطلبات شفافية ومساءلة على الخوارزميات المستخدمة.

-إلزام المطورين بإنشاء أنظمة لتتبع القرارات الصادرة عن الأنظمة الذكية، مع حفظ سجلات توثيقية لفترات محددة لغايات المساءلة والتدقيق القضائي.

ثالثا: على الصعيد القضائي

-تنظيم برامج تدريبية متخصصة لتأهيل القضاة والمحامين في مجال تقنيات الذكاء الاصطناعي.

-إنشاء دوائر قضائية متخصصة في النزاعات التقنية والرقمية.

-تطوير قواعد الإثبات في قضايا الذكاء الاصطناعي، بما يشمل اعتماد الخبرة التقنية وأليات تقييم الأدلة الرقمية بصورة دقيقة.

رابعا: على الصعيد الدولي

-الانخراط الفاعل في المبادرات الدولية الهادفة إلى وضع معايير موحدة للمسؤولية عن أضرار الذكاء الاصطناعي.

-المساهمة في صياغة اتفاقيات دولية لضمان حماية حقوق الأفراد في البيئة الرقمية.

-إقامة شراكات عربية إقليمية لبناء نموذج قانوني عربي يتماشى مع الخصوصيات القانونية والاجتماعية والثقافية للمنطقة.

خامسا: على صعيد التعليم والبحث العلمي

-إدراج موضوعات الذكاء الاصطناعي والقانون في البرامج الأكاديمية لكليات الحقوق، بما يضمن إعداد أجيال قادرة على التعامل مع المستجدات التقنية قانونيا.

-تشجيع الأبحاث المشتركة بين المتخصصين في القانون وخبراء التقنية لتطوير حلول عملية تتناسب مع الإشكالات الحديثة.

-إنشاء مراكز بحثية متخصصة في الجوانب القانونية والأخلاقية للذكاء الاصطناعي، مع تخصيص موارد مالية كافية لدعم البحث العلمي في هذا المجال.

إن تحقيق هذه التوصيات يتطلب تضافر جهود كافة الأطراف المعنية، من مؤسسات الدولة والقطاع الخاص والجامعات ومنظمات المجتمع المدني، لضمان أن يكون الذكاء الاصطناعي أداة لتحقيق التنمية المستدامة وصون الكرامة الإنسانية، وأن تظل القوانين مرنة وعادلة، مستجيبة لمقتضيات العصر الرقمي دون المساس بحقوق الأفراد وحرياتهم.

قائمة المصادر والمراجع:

أولا /قائمة المصادر:

-1التشريع:

أ/الدستور:

-دستور الجزائري ،الجريدة الرسمية ،العدد 82 ،الصادرة في 2020/12/20.

ب/التشريع العادي (القانون)

-القانون05-10 المؤرخ في 2005/06/20 المتضمن القانون المدني المعدل و المتمم.

ج/المراسيم:

-مرسوم رئاسي 20-05،مؤرخ في 2020/01/20،يتضمن وضع منظومة وطنية لأمن الأنظمة المعلوماتية.

- المرسوم الرئاسي 21-439 المؤرخ في 2021/11/07 المتضمن إعادة تنظيم الهيأة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام و الاتصال و مكافحتها.

ثانيا/المراجع باللغة العربية

-1الكتب (المؤلفات)

-صفات سلامة تكنولوجيا الروبوتات رؤية مستقبلية بعيون عربية،المكتبةالأكاديمية،القاهرة،2006.

-عبد الله موسي و أحمد بلال ،الذكاء الاصطناعي ثورة في تقنيات العصر دار الكتب المصرية ، ط1 ،القاهرة،2019.

-2أطروحات الدكتوراة،رسائل الماجستير، مذكرات الماستر

أ/أطروحات الدكتوراه

-حويلي سلوى المسؤولية المدنية للمستثمر في عقود نقل التكنولوجيا في التشريع الجزائري أطروحة لنيل شهادة الدكتوراه ،تخصص قانون الإستثمار،جامعة العربي بن مهيدي ،أم البواقي،الجزائر،2022-2023.

ب/رسائل الماجستير

-ريم خلفان سعيد راشد الكندي،النطاق الشخصي للمسؤولية الجنائية عن أخطاء الذكاء الإصطناعي، رسالة الماجستير، جامعة الشارقة، ديسمبر2024.

-زين عبد الهادي ،الذكاء الاصطناعي في إدارة أنشطة مؤسسة ،دراسة حالة مجموعة المؤسسات الاقتصادية، رسالة ماجيستر ،كلية العلوم الاقتصادية والعلوم التجارية جامعة أم البواقي، الجزائر،2015/02/14

ج/مذكرات الماستر

-شبلي فضيل بوسعيد محمد المسؤولية المدنية عن تطبيقات الذكاء الاصطناعي في القانون الجزائري مذكرة لنيل شهادة الماستر تخصص قانون خاص جامعة عين تموشنت،الجزائر،2023-2024.

-شداد أمال عبير المسؤولية المدنية عن الأضرار الناجمة عن الذكاء الاصطناعي ،مذكرة لنيل شهادة الماستر ،تخصص قانون خاص جامعة غرداية،2024/06/22.

-لعمارة طارق زياد و ميمون سفيان المسؤولية المدنية الناشئة عن استخدام تقنيات الذكاء الاصطناعي في التشريع الجزائري مذكرة لنيل شهادة الماستر جامعة محمد بوضياف مسيلة تخصص قانون الأعمال،2024/06/01.

د/المقالات

-الحارثي عبد الرحمن و الدروبي علي ،تأرجح الضرر الناشئ عن الذكاء الاصطناعي بين المسؤوليتين الشخصية و الموضوعية دراسة تحليلية نقدية مجلة جامعة الشارقة للعلوم القانونية مجلد 22 عدد1،سنة 2025.

-الحربي عيسى ،محاولة تأطير المسؤولية التقصيرية للذكاء الاصطناعي وفقا لنظام المعاملات المدنية السعودي ،مجلة كلية الدراسات الإسلامية و العربية للبنات بالإسكندرية،المجلد40،العدد03،مارس2024.

-الخطيب محمد عرفان ،الاستشراف المستقبلي لمبدأ وحدة المسؤولية المدنية في التشريع المدني الفرنسي الحديث قراءة في فلسفة مشروع قانون اصلاح نظرية المسؤولية: دراسة تحليلية معمقة مجلة كلية القانون الكويتية العالمية ،العدد31، سبتمبر2020.

-السكيني مروان منصور نعيم ، مبارك وائل عزت عبد الهادي ،خصوصية المسؤولية المدنية الناشئة عن استخدام أنظمة الذكاء الاصطناعي المجلة القانونية متخصصة في الدراسات و البحوث القانونية،المجلد23 ،العدد02،فيفري 2025.

-السيد محمد السعيد ،نحو اطار قانوني شامل للمسؤولية المدنية من أضرار نظم الذكاء الإصطناعي غير المراقب،مجلة البحوث القانونية والإقتصادية،جامعة المنصورة،2021

-بلعباس أمال ،مدى ملاءمة قواعد المسؤولية المدنية لتعويض عن أضرار النظم الذكية،مجلة البحوث القانونية و الاقتصادية،المجلد06،العدد01، 2023.

-حمدادو لمياء،الذكاء الاصطناعي:نموذج عن التحديات المعاصرة للمسؤولية التقصيرية،المجلة الجزائرية للقانون و العدالة ،مجلد10،عدد1، سنة2024.

-نور خالد عبد الرزاق ،المسؤولية المدنية الناشئة عن استخدام الذكاء الإصطناعي،مجلة التحدبات و الافاق القانونية و الاقتصادية للذكاء الاصطناعي،المجلد 66،العدد3،جانفي 2024.

ه/المحاضرات

-عبدو أحمد ،دروس في القانون المدني، الجزء الثاني، النظرية العامة للإلتزام ،ألقيت على طلبة السنة الثانية حقوق، جامعة البليدة02، 2022/2021.

و/رو ابط الإنترنيت

1-
https://wadaq.info/%d8%a7%d9%84%d9%85%d8%b3%d8%a4%d9%88%d9%84%d9%8a%d8%a9-%d8%a7%d9%84%d9%85%d8%af%d9%86%d9%8a%d8%a9-%d9%88%d8%a7%d9%84%d8%b0%d9%83%d8%a7%d8%a1-%d8%a7%d9%84%d8%a7%d8%b5%d8%b7%d9%86%d8%a7%d8%b9%d9%8a/,20/07/2025,16h00

2-. https://wadaq.info/%D8%AA%D8%A3%D8%AB%D9%8A%D8%B1-%D8%A7%D9%84%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7-%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D8%AD%D9%82%D9%88%D9%82/ -21/07/2025,11h00.

3-
https://web.lexisnexis.fr/newsletters/avocats/10_2016/dossier4.pdf,21/07/2025,13h00.

4-
https://mawdoo3.com/%D8%A7%D9%84%D9%85%D8%B3%D8%A4%D9%88%D9%84%D9%8A%D8%A9_%D8%A7%D9%84%D8%AA%D9%82%D8%B5%D9%8A%D8%B1%D9%8A%D8%A9_%D9%81%D9%8A_%D8%A7%D9%84%D9

%82%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D9%85%D8%AF%D9%86%D9%8A_%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D8%B1%D9%8A?utm_so%D8%AF%D8%AF%D8%AF,21/07/2025,16h05.

5- https://ar.m.wikipedia.org/wiki/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1_%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A?,21/07/2025,16h50.

6- https://ar.m.wikipedia.org/wiki/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1_%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A?utm,21/07/2025,17h00.

ثالثا /المراجع باللغة الأجنبية

1/Ouvrage

- Barfield, Woodrow, and Ugo Pagallo, eds. Research Handbook on the Law of Artificial Intelligence. Edward Elgar Publishing, 2018.

2/These de doctorat

- M. Assunta Cappeli, "regulation on safety and civil liability of intelligent autonomous robots: the case of smart cars", Ph. D thesis, universita degli studidi Trento, 2014.

3/Memoire

- S. Oliveira, "La responsabilité civile dans les cas de dommages causés par les robots d'assistance au Québec", LL.M, faculté de droit, université de montréal, 2016.

أثر التحول الرقمي على القانون النقدي والمصرفي رقم 23-09

"رقمنة القطاع المصرفي نموذجا"

The impact of digital transformation on monetary and banking law No. 23-09

"Digitization of the banking sector as a model"

د. ڤورية نذير

جامعة الشاذلي بن جديد- الطارف

n.gorria@univ-eltarf.dz

ملخص:

تهدف هذه الورقة البحثية إلى دراسة تأثير التحول الرقمي على القانون النقدي والمصرفي رقم 23-09، يأتي ذلك في إطار اهتمام المشرع الجزائري بالاستفادة من التكنولوجيا والتقنيات الحديثة في القطاع المصرفي، حيث تم إدخال شكل جديد من العملة النقدية، الذي أتاح للعملة الوطنية بأخذ شكل رقمي، إلى جانب إنشاء البنوك الرقمية.

الكلمات المفتاحية: بنوك رقمية؛ تحول رقمي؛ عملة رقمية؛ قانون نقدي ومصرفي.

Abstract:

This research paper aims to study the impact of digital transformation on Monetary and Banking Law No. 23-09. This comes within the framework of the Algerian legislator's interest in benefiting from modern technology and techniques in the banking sector, where a new form of currency has been introduced, allowing the national currency to take a digital form, alongside the establishment of digital banks.

Keywords: keywords;

Digital banks; Digital currency; Digital transformation; monetary and banking law.

مقدمة:

منذ بداية القرن الحادي والعشرين، أدت الثورة المعلوماتية المرتبطة بالتكنولوجيا الرقمية إلى انتشار واسع لفكرة الرقمنة في مجالات متعددة، وقد أسفرت هذه الثورة عن تغييرات جذرية في التشريعات، حيث تم اعتماد الوسائط التكنولوجية كوسيلة لتعزيز مبدأ الشفافية في العلاقات والمعاملات، وأصبح التحول الرقمي تحديا ضروريا للمشرعين لتحقيق تغييرات تنظيمية تتماشى مع الاستراتيجيات والأهداف الوطنية.

وبالتالي في ظل التغيرات الاقتصادية العالمية والتحول نحو الاقتصاد الرقمي لا سيما في القطاع المالي، أصبح من الضروري أن تتماشى جميع التشريعات بما في ذلك التشريع الجزائري، مع تقنيات التحول الرقمي، وذلك نظرا لما تقدمه هذه العملية من فوائد كبيرة في تعزيز جهود مكافحة الفساد وتقليص مدة الإجراءات، وقد تجسد ذلك في صدور القانون رقم 23-09 المؤرخ في 21 يونيو 2023[1]، الذي

[1]. القانون رقم 23-09 المؤرخ في 21 يونيو 2023، يتضمن القانون النقدي والمصرفي، الجريدة الرسمية، العدد 43، المؤرخة في 27 جوان 2023.

يتضمن القانون النقدي والمصرفي، من خلال رقمنة القطاع المصرفي وإتاحة إمكانية إنشاء بنوك رقمية، وفقا لما نصت عليه المادة 90 منه، حيث يمنح المجلس النقدي والمصرفي صلاحية إنشاء هذه البنوك، بالإضافة إلى ذلك تم إدخال نوع جديد من النقد يعرف بالنقد الرقمي، الذي يتميز باستخدام تقنية البلوك تشاين.

استنادا إلى الأهمية الكبيرة التي يتمتع بها هذا الموضوع، يبرز تساؤل أساسي يتعلق **بإنعكاسات التحول الرقمي على القانون النقدي والمصرفي؟**

ويعتمد البحث على منهجين أساسيين هما المنهج التحليلي والمنهج الوصفي، حيث يتناسبان مع هدف الدراسة المتمثل في عرض المفاهيم النظرية المتعلقة بعناصر البحث، بالإضافة إلى المناقشة والتحليل، ولتسليط الضوء على إشكالية هذا الموضوع اعتمدنا خطة ثنائية الطرح، حيث نتطرق في المبحث الأول إلى التحول الرقمي من خلال إدخال الدينار الرقمي، وفي المبحث الثاني إلى التحول الرقمي من خلال إنشاء البنوك الرقمية.

المبحث الأول:

الرقمنة عبر إدخال الدينار الرقمي

تعتبر العملة الرقمية من الابتكارات الحديثة التي أحدثت تحولا في نظام الدفع الإلكتروني، في هذا الإطار يمثل الدينار الرقمي الجزائري الذي أطلقه البنك المركزي، خطوة نوعية نحو التحول الرقمي، كما يعد أداة فعالة للحد من مخاطر العملات الافتراضية، ويساهم في معالجة التحديات التي يواجهها الاقتصاد الوطني،

مثل التسرب النقدي والسوق الموازي، بالإضافة إلى ذلك يعزز ظهور أنشطة اقتصادية جديدة مثل منصات الخدمات المالية.

المطلب الأول:

مفهوم العملة الرقمية

سنحاول من خلال هذا المطلب تناول مفهوم العملة الرقمية، التي تعتبر نوعا من العملات الافتراضية تتكون من أكواد رقمية يمكن تخزينها على الأقراص الصلبة أو عبر شبكة الأنترنت، من الصعب تتبع عمليات البيع والشراء التي تتم باستخدامها، كما أنه من الصعب تحديد هوية مالكي هذه العملات، وتشمل العملات الرقمية فئات متنوعة مثل العملات الافتراضية، والعملات المشفرة، بالإضافة إلى العملات الرقمية التي تصدرها البنوك المركزية، وفي جويلية 2022 كان هناك حوالي 100 عملة رقمية قيد التطوير من قبل بنوك مركزية عالمية، بينما تم إصدار عملتين بشكل كامل، وهما عملة إي-نيرة في نيجيريا في أكتوبر 2021، والدولار الرملي في جزر البهاما في أكتوبر 2020.

الفرع الأول: تعريف العملة الرقمية (Digital currency)

تتنوع المصطلحات المستخدمة لوصف العملة الرقمية، مثل النقود الرقمية والنقدية الإلكترونية، وعلى الرغم من اختلاف هذه الاصطلاحات، إلا أنها تشير جميعها إلى مفهوم واحد هو النقود الإلكترونية، كما أن الفقهاء قد اختلفوا في تقديم تعريف موحد لها.

أولا: العملة الرقمية فقها

من التعريفات الفقهية للعملة الرقمية أنها "**مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإلكترونية أن تحل فعليا محل تبادل العملات التقليدية، وبعبارة أخرى فإن النقود الإلكترونية أو الرقمية هي المكافئ الإلكتروني للنقود التقليدية التي اعتدنا تداولها**"[1].

كما تعرف أيضا بأنها "**قيمة نقدية في شكل وحدات ائتمانية مخزونة بشكل إلكترونية أو على أداة إلكترونية يحوزها المستهلك**"[2].

ومن منظور فقهي آخر تعرف العملة الرقمية بأنها "**سلسة جزئيات صغيرة ذات قيمة مالية مكافئة لقيمة محددة بالعملة التقليدية، وتتميز بوجود رقم مرجعي متسلسل يميزها**"[3].

ثانيا: العملة الرقمية قانونا

لم يتضمن التشريع الجزائري تعريفا للعملة الرقمية أو النقود الإلكترونية، باستثناء التعريف المذكور في المادة 117 الفقرة 2، من القانون رقم 17-11 المؤرخ في

---

1. Aleksander BERENSTEN, "Monetary Policy Implications of Digital Money", *Kyklos*, n°1, 1997, p 90.

2. منير محمد الجنبيهي، ***الطبيعة القانونية للعقد الإلكتروني***، دار الفكر الجامعي، مصر، دون سنة نشر، ص 157.

3. جلال عايد الشوره، ***وسائل الدفع الإلكتروني***، دار الثقافة للنشر والتوزيع، الأردن، الطبعة الأولى، 2008، ص 57.

27 ديسمبر 2017[1]، والذي يتضمن قانون المالية لسنة 2018، حيث عرف المشرع العملة الافتراضية كأحد أنواع العملة الرقمية على النحو التالي: "**العملة الإفتراضية هي تلك التي يستعملها مستخدمو الأنترنت عبر شبكة الأنترنت، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو البطاقة البنكية**".

كما تم تعريفها في المادة الأولى من القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية لعام 2009[2]، تحت مسمى "**النقود الإلكترونية**" كالتالي: "**وحدات نقد إلكتروني يمكن حفظها إلكترونيا لمدة محددة وتصدر مقابل نقد يتم مبادلته فورا، بنفس القيمة ونفس العملة وتتيح للغير دون المصدر إتمام عملية الدفع**".

وقد عرفها المشرع الفرنسي في المادة 315-1 من القانون النقدي والمالي بأنها قيمة نقدية مخزنة إلكترونيا، بما في ذلك التخزين المغناطيسي، وتمثل هذه النقود مطالبة على الجهة المصدرة، ويتم إصدارها مقابل تحويل الأموال لغرض عمليات الدفع المحددة في المادة 133-1، والتي يتم قبولها من قبل أشخاص طبيعيين أو اعتباريين غير مصدرين للنقود الإلكترونية.

1. القانون رقم 17-11 المؤرخ في 27 ديسمبر 2017، والمتضمن قانون المالية لسنة 2018، الجريدة الرسمية، العدد 76، المؤرخة في 28 ديسمبر 2017.

2. تم اعتماد القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية بموجب قرار مجلس وزراء العدل العرب رقم 812/د 25، وذلك بتاريخ 19 نوفمبر 2009.

الفرع الثاني: أنواع العملة الرقمية

يتضمن مصطلح العملة الرقمية مجموعة واسعة من الأنواع، أبرزها العملات الرقمية اللامركزية (المشفرة) مثل البيتكوين، بالإضافة إلى العملات الرقمية الصادرة عن البنوك المركزية.

أولا: العملة الرقمية المركزية (Central digital currency)

تعمل البنوك المركزية على تطوير نظام دفع جديد يهدف إلى تقليل المشكلات المرتبطة بالعملات المشفرة، مما يجعلها الجهة المسؤولة عن هذا النظام دون إلغاء نظام الدفع التقليدي، وقد بدأت هذه البنوك في دراسة إمكانية إصدار عملاتها الخاصة، المعروفة اختصارا بـ "**CBDC**"، كنوع من الأموال التي تستخدم إلكترونيا وتكون متاحة للجمهور، هذه العملات الرقمية تصدرها البنوك المركزية، وتتميز بأن قيمتها تحددها هذه البنوك وتكون متوازية مع العملة التقليدية.

وقد تم تعريف العملة الرقمية المركزية بأنها "**أداة رقمية عالية الأمان، يصدرها البنك المركزي بموجب لوائح وقوانين بالموازاة مع الأنظمة التقليدية الأخرى للنقود، فهي تمتلك نفس صفات الأوراق النقدية، وتعتبر وسيلة للدفع ووحدة حسابية ومخزن للقيمة**"[1].

كما تعرف أيضا بأنها تلك التي تصدر عن هيئة مركزية أو منظمة رسمية، مثل العملات الرقمية التي تصدرها البنوك المركزية، كما تشمل أيضا عملات المحاكاة

1. John BARRDEAR & Michael KUMHOF, "The Macroeconomics of Central Bank Issued Digital Currencies", *staff working paper*, no 605, July 2016, p 7.

المعروفة بعملات الألعاب، وهي عملات رقمية افتراضية مركزية تصدر عن مؤسسات غير حكومية، وتستخدم غالبا في شراء وبيع ألعاب الفيديو عبر الأنترنت[1].

وبناء على ذلك فإن العملة الرقمية المركزية هي العملة التي تصدرها سلطة مالية مركزية في دولة معينة، مثل البنوك المركزية أو التجارية أو مؤسسات الائتمان المالية، تحتفظ هذه العملة بخصائصها كوسيلة للدفع نظرا لأنها صادرة عن البنك المركزي، لكنها تفتقر إلى الشكل المادي، مما يتيح لها بشكلها الرقمي الحفاظ على خصوصية المستخدم في ظل السياسات الرقابية التي يفرضها البنك المركزي.

لا شك أن إصدار البنك المركزي للعملات الرقمية المركزية يعتبر بديلا فعالا لمخاطر العملات الافتراضية، حيث تسعى الحكومات إلى التصدي لانتشار العملات الرقمية غير الرسمية، وفي هذا الإطار أصدر البنك المركزي الأردني في عام 2014 بيانا رسميا يحذر فيه المواطنين من التعامل مع العملات الرقمية التي تفتقر إلى الدعم من أي مؤسسة مالية عالمية.

ثانيا: العملة الرقمية اللامركزية (Decentralised digital currency)

تعرف العملات الرقمية اللامركزية بأنها العملات التي تفتقر إلى وجود مادي، ويمكن مقارنتها بالعملات الرسمية المتداولة حاليا مثل الدولار واليورو، يتم تداول هذه العملات عبر الأنترنت دون وجود سلطة مركزية أو بنك مركزي يتولى إصدارها[1].

---

1. جلول شرارة وليلى إسمهان بقبق، "العملات الرقمية للبنوك المركزية "تحديات ومتطلبات الدينار الرقمي الجزائري في ظل القانون النقدي والمصرفي 23-09"، ***مجلة طبنة للدراسات العلمية الأكاديمية***، المركز الجامعي بريكة، الجزائر، المجلد 06، العدد 02، ص 1093.

تعرف أيضا بأنها تمثيل رقمي لقيمة نقدية غير صادرة عن بنك مركزي أو سلطة عامة، وليست مرتبطة بالضرورة بالعملة الورقية، ومع ذلك فإنها مقبولة من قبل الأشخاص الطبيعيين والمعنويين كوسيلة للدفع، يمكن نقلها أو تخزينها أو تداولها إلكترونيا[2].

في هذا السياق اعتمد صندوق النقد الدولي تصنيف البنك المركزي الأوروبي للعملات الرقمية اللامركزية في عام 2016، معترفا بها كمجموعة فرعية من العملات الافتراضية، ومن وجهة نظره تعرف العملات الرقمية اللامركزية على أنها تمثيلات رقمية للقيمة يتم إصدارها من قبل جهات خاصة، وتمتلك وحدة حساب خاصة بها، كما يشمل هذا التعريف نطاقا واسعا من العملات الافتراضية، بما في ذلك سندات الدين البسيطة الصادرة عن جهات غير رسمية، فضلا عن العملات الافتراضية المدعومة بأصول مثل الذهب والعملات الرقمية اللامركزية على غرار البيتكوين[3].

تأسيسا على ذلك تعتبر العملات المشفرة نوعا من العملات الرقمية التي تعتمد على نظام تشفير خاص، يعتمد هذا النظام على موثوقية الخوارزميات

---

[1]- عبد الفتاح محمد أحمد صلاح، "البيتكوين عملة الكترونية مشفرة قد تسبب أزمة اقتصادية عالمية جديدة"، ***مجلة الاقتصاد الإسلامي العالمية***، مركز أبحاث فقه المعاملات الإسلامية، سوريا، العدد 33، فيفري 2015، ص 34.

[2]- عبد الله بن سليمان بن عبد العزيز الباحوث، "النقود الافتراضية مفهومها وأنواعها وآثارها الاقتصادية"، ***المجلة العلمية للاقتصاد والتجارة كلية التجارة***، جامعة عين شمس، مصر، المجلد 47، العدد 1، 2017، ص 875.

[3]- سعاد عون الله ورضوان عامري، "مخاطر وتداعيات تداول العملات المشفرة على استقرار القطاع المالي خلال الفترة 2017-2021"، ***مجلة اقتصاديات شمال إفريقيا***، جامعة حسيبة بن بوعلي شلف، الجزائر، المجلد 19، العدد 31، 2023، ص 206.

الرياضية، وهو معقد بما يكفي لضمان أمان وحماية مختلف المعاملات، يقوم النظام بتحليل البروتوكولات والخوارزميات، مما يسمح بتشفير المعلومات والبيانات بحيث لا يمكن تغييرها، ويحلل النظام البروتوكولات والخوارزميات مما يتيح تشفير المعلومات والبيانات ويمنع تعديلها، ويجعلها متاحة فقط للمتداولين المصرح لهم، كما تتميز العملات المشفرة أيضا بنظام وبروتوكول يعرف باسم سلسلة الكتل (**blockchain**) وهو سجل رقمي لامركزي، مما يعني عدم وجود طرف ثالث يتحكم في جميع الأنشطة والمعاملات والتحويلات والإرساليات على الشبكة[1].

وفي واقع الأمر هناك العديد من العملات الرقمية اللامركزية يعتمد معظمها على نموذج بيتكوين (**Bitcoin**) وتعتبر نسخا منه، عادة ما تكون الاختلافات بينها طفيفة وتتعلق غالبا بأوقات التداول، وطرق الإصدار، وخوارزميات الهامش، أو الانتشار بين المتعاملين.

المطلب الثاني:

العملة الرقمية في التشريع الجزائري

تم ذكر مصطلح "**النقود الإلكترونية**" لأول مرة في القانون الجزائري تحت مسمى "**العملة الرقمية**" و"**الدينار الرقمي الجزائري**" في القانون النقدي والمصرفي رقم 23-09، وقد أشار المشرع الجزائري إلى ضرورة وضع نظام لتحديد أحكام إصدار وتطوير العملة الرقمية، إلا أنه لم يتم حتى الآن إصدار أي نظام يتعلق بهذا الشأن.

[1]- عز الدين شرون وبوبكر مصطفى، "العملات المشفرة مستقبل المعاملات المالية "البتكوين نموذجا"، ***مجلة المنهل الإقتصادي***، كلية العلوم الإقتصادية، جامعة الوادي، الجزائر، المجلد 1، العدد 2، ديسمبر 2018، ص 37.

الفرع الأول: الدينار الرقمي الجزائري (e-DZD)

اعتمد المشرع استخدام العملة الرقمية في الجزائر للمرة الأولى من خلال القانون النقدي والمصرفي رقم 23-09، الذي أطلق عليه اسم الدينار الرقمي الجزائري، حيث أوضحت المادة 2 مكونات العملة النقدية، التي تتواجد في شكلها المادي كأوراق نقدية وقطع معدنية، وكذلك يمكن أن تكون بصورة رقمية وتسمى بالدينار الرقمي الجزائري، وتكون سلطة إصدار العملة الرقمية مختصة بالدولة، التي تفوض هذه السلطة إلى البنك المركزي -بنك الجزائر- دون غيره.

وفقا للمادة 3 من القانون رقم 23-09، يتم تحديد متطلبات إصدار وتطوير العملة الرقمية الخاصة بالبنك المركزي من خلال أنظمة تطبق تبعا لما يحدده هذا القانون، بالإضافة إلى قواعد إدارة ورقابة العملة الرقمية للبنك المركزي، أما بالنسبة للطابع القانوني للدينار الرقمي الجزائري فإنه يستند إلى ما جاء في المادة الرابعة من نفس القانون، والتي أشارت إلى أن الأوراق النقدية والقطع المعدنية بالإضافة إلى العملة الرقمية التي يصدرها بنك الجزائر فقط لها قيمة قانونية وتتمتع بقدرة إبرائية غير محدودة.

وفي هذا الإطار فرض القانون الجزائري على البنوك والمؤسسات المالية والمصالح المالية لبريد الجزائر إنشاء نظام يمكنهم من وقف تنفيذ أي عملية تتعلق بالأصول الافتراضية و/أو بمزودي الأصول الافتراضية الممنوعين وفقا للتشريع الساري، بما في ذلك تلك الموجودة في دول أخرى، وإبلاغ خلية معالجة الاستعلام المالي بذلك دون

تأخير، ولا ينطبق هذا النظام على القيم الرقمية المرتبطة بالعملات الرقمية والأوراق المالية[1].

الفرع الثاني: الدينار الرقمي الجزائري آلية لتفعيل بطاقات الدفع الإلكتروني

تعتبر بطاقات الدفع من الناحية القانونية بمثابة اتفاقية يلتزم من خلالها مصدر البطاقة بإنشاء حساب لحامل البطاقة، الذي يمكنه من خلالها تسديد ثمن مشترياته في المتاجر التي أبرمت عقدا مع مصدر البطاقة يتعهد فيه بقبول تلك المدفوعات، كما تسمح هذه البطاقات لصاحبها بسحب أو تحويل الأموال، ولها قيمة قانونية في إثبات ذلك أمام الجهات القضائية[2].

ضم المشرع الجزائري بواسطة المادة 74 من القانون رقم 23-09، العملة الرقمية ضمن الوسائل الحديثة للدفع الإلكتروني التي تعتبر وسائط مالية تمكن الأفراد من إجراء تحويلات مالية بأي طريقة كانت، بما في ذلك العملة الرقمية، وبخصوص عرض العملة الرقمية الرسمية، يتعين على البنوك المركزية اختيار الطريقة المناسبة وفقا للسياسة النقدية لحين وضع أنظمة تحدد الأحكام المتعلقة بإصدار وإدارة ورقابة تلك العملة.

---

[1]- المادة 4 من النظام رقم 24-03 المؤرخ في 24 جويلية سنة 2024، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل ومكافحتها، الجريدة الرسمية، العدد 58، المؤرخة في 22 أوت 2024.

[2]- حمود محمد غازي الحمادة، ***العلاقات التعاقدية الناشئة عن بطاقات الدفع الالكتروني***، المركز العربي للنشر والتوزيع، مصر، الطبعة الأولى، 2018، ص 41.

وبالتالي استدعت الحاجة إلى تطوير طرق دفع تتناسب مع طبيعة التجارة وشروطها، واستمرت الجهود العديدة للبحث عن وسائل إلكترونية ذات طابع حديث قادرة على التفاعل مع التطورات التي شهدتها التجارة الإلكترونية، وقد ظهرت العملات الرقمية كوسيلة قادرة على تلبية هذه المتطلبات والتوافق مع التكنولوجيا الحديثة، وهذا يعد دليلا على أهمية هذه العملة الجديدة، حيث نلاحظ في الوقت الراهن وجود منافسة بين الشركات التي تعتمد على العملات الرقمية، مما أسهم في توفير العديد من أنظمة الدفع لمعظم الشركات الكبرى[1].

تأسيسا على ذلك أنشأ المشرع الجزائري وسطاء مزودو خدمات الدفع المعتمدون قانونا[2]، حيث تكمن مسؤوليتهم في تسهيل خدمات الدفع التي توفرها المؤسسات البنكية، يقوم مقدمو خدمات الدفع بتوفير مستوى عالي من الأمان خلال تنفيذ عمليات الدفع، بسبب ارتباط أنشطتهم المباشر بتقديم هذه الخدمات للعملاء، من بين هذه الخدمات إصدار بطاقات إلكترونية وتسهيل استخدامها للعملاء، حيث تعتبر بساطة استخدام الدينار الرقمي وعدم تعقيده عاملا حاسما في تداوله[3].

[1]- الرشيد بوعافية، "دور النقود الالكترونية في تطوير التجارة الالكترونية"، ***المجلة الجزائرية للاقتصاد والمالية***، جامعة يحي فارس، المدية، العدد 02، سبتمبر 2014، ص 129.

[2]- يخضع مزودي خدمات الدفع إلى النظام رقم 25-02 المؤرخ في 14 أفريل سنة 2025، والمحدد لشروط الترخيص بتأسيس واعتماد وممارسة نشاطاتهم، الجريدة الرسمية، العدد 28، المؤرخة في 7 ماي 2025.

[3]- المادة 76 من القانون رقم 23-09، يتضمن القانون النقدي والمصرفي.

المبحث الثاني:

الانتقال الرقمي من خلال إنشاء البنوك الرقمية (Digital banking)

تؤدي البنوك دورا حيويا في تشجيع الاستثمارات ودعم الاقتصاد الوطني بشكل عام، بالإضافة إلى تقوية القطاع المصرفي بشكل خاص من خلال الخدمات المالية التي تقدمها، لذا تم إصدار القانون رقم 23-09 والذي يتضمن القانون النقدي والمصرفي كجزء من عملية الإصلاحات في القطاع المصرفي، حيث ينص هذا القانون على إنشاء ما يعرف بالبنوك الرقمية، وذلك طبقا لما هو مذكور في المادة 90 من نفس القانون.

المطلب الأول:

مفهوم البنوك الرقمية

تعد البنوك الرقمية[1] نتيجة للتحول الرقمي الذي شهده عالم المال، مما أتاح إمكانية تقديم الخدمات المصرفية التقليدية من خلال منصات رقمية وإلكترونية مثل الشبكة العنكبوتية أو من خلال تطبيقات الهواتف الذكية، كما أنها تمثل واحدة من أهم الابتكارات التي غيرت بشكل جذري أسلوب تقديم الخدمات المالية والمصرفية، حيث تعتبر هذه البنوك مركزا للابتكار والتميز في المجال المالي.

[1]. يعود أصل البنوك الرقمية إلى عام 1995، عندما أنشئ أول بنك يعمل على شبكة الأنترنت في الولايات المتحدة الأمريكية، بينما تعود أول تجربة للبنوك الرقمية عالميا إلى سنة 2015 مع بنك مونزو وبنك ريفولوت البريطانيين، اللذين ظهرا كأول بنوك ذكية بلا فروع تقليدية، لتتوسع هذه التجربة لاحقا إلى دول أخرى.

الفرع الأول: تعريف البنوك الرقمية

يعتمد تعريف البنك الرقمي على التحول الرقمي في القطاع المالي والمصرفي، لقد اتسع هذا المفهوم ليشمل المؤسسات التي لا تقدم خدمات مصرفية تقليدية، مثل المدخرات والقروض، فهي تمثل مؤسسات تقدم خدمات مالية مشابهة لتلك التي تقدمها البنوك التقليدية، لكنها تعمل من خلال الأنترنت أو التطبيقات الخاصة بالهواتف الذكية.

أولا: التعريف الفقهي

تعرف البنوك الرقمية بأنها "**تلك البنوك والمؤسسات المالية المستندة على الركائز الإلكترونية، من خلال توظيف التطورات الحديثة في مجال تكنولوجيا المعلومات والإتصالات لتقديم كافة الخدمات المصرفية بأمان وبأقل كلفة، وأسرع وقت و أقل جهد للعملاء**"[1].

وعرفت أيضا بأنها: "**النظام الذي يسمح للزبون من الدخول إلى حساباته أو أي معلومات يحتاجها، والحصول على تشكيلة متنوعة من الخدمات والمنتجات المصرفية، عبر شبكة المعلومات التي يتصل بها جهاز الكمبيوتر الخاص به أو الوسائل الإلكترونية أو الرقمية أو الآلية الأخرى**"[2].

---

[1]. ناظم محمد نوري الشمري وعبد الفتاح زهير العبداللات، ***الصيرفة الإلكترونية "الأدوات والتطبيقات ومعيقات التوسع"***، دار وائل للنشر، الأردن، الطبعة الأولى، 2008، ص 29.

[2]. عبد الهادي مسعودي، ***الأعمال المصرفية الالكترونية***، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2016، ص 20.

ذهب اتجاه آخر من الفقه إلى تعريف البنك الرقمي بأنه مؤسسة مصرفية لها وجود تام على الأنترنت، ويحتوي موقعه الإلكتروني على جميع البرمجيات والتطبيقات الضرورية للقيام بالأنشطة المصرفية، ومن خلال هذا يتيح البنك للزبون إجراء جميع معاملاته المصرفية من أي مكان يتواجد فيه، باستخدام الوسائل التي يقدمها له البنك، مما يمكنه من إتمام معاملاته البنكية دون الحاجة للذهاب إلى الفروع أو المكاتب التابعة للبنك[1].

من خلال التعريفات المذكورة سابقا للبنوك الرقمية، يمكن القول بأن هذه البنوك تقدم خدمات مصرفية مشابهة لتلك المقدمة من البنوك التقليدية، ولكن هناك اختلافات في الطرق المتبعة للوصول إلى ذلك؛ ففي حالة البنوك التقليدية تنفذ الوظائف والخدمات بشكل فعلي من خلال الفروع والمواقع الواقعية، إضافة إلى استخدام التقنيات الحديثة مثل الأنترنت، وهذا يتضمن جميع أشكال التوزيع الرقمي مثل أجهزة الصراف الآلي، ونقاط البيع الإلكترونية، والخدمات المصرفية عبر الهاتف الثابت، والبنوك عبر الهواتف المحمولة، وغيرها من وسائل التوزيع.

ثانيا: التعريف التشريعي

ورد في المادة 2 من النظام رقم 24-04[2] تعريف البنوك الرقمية بأنها: "**كل بنك يقدم خدمات ومنتوجات مصرفية حصريا عبر قنوات أو منصات أودعائم رقمية بالاعتماد على التكنولوجيات الحديثة.**"، مما يتضح من هذا التعريف أن المشرع

[1]- وسيم محمد الحداد، ***الخدمات المصرفية الالكترونية***، دار المسيرة، الأردن، الطبعة الأولى، 2012، ص6.

[2]- النظام رقم 24-04 المؤرخ في 13 أكتوبر 2024، المتعلق بالشروط الخاصة للترخيص بتأسيس واعتماد وممارسة نشاط البنك الرقمي، الجريدة الرسمية، العدد 77، المؤرخة في 19 نوفمبر 2024.

الجزائري يشترط أن تعتمد البنوك الرقمية في أنشطتها على ما تم تحقيقه من تقدم في تكنولوجيا المعلومات والاتصالات والتقنيات المالية، من خلال إمكانية إنشاء فروع بشرط أن تعمل بصورة كاملة بشكل آلي، أي أنه يجب أن تكون هذه الفروع مدفوعة بالتقنية الرقمية[1].

وفي مقابل ذلك يتسم البنك الرقمي في الجزائر بوجود فعلي، حيث فرض القانون بموجب المادة 6 من النظام رقم 24-04، ضرورة إنشاء مقر اجتماعي مخصص لأغراض إدارية وكذا للتعامل مع شكاوى الزبائن، هذا يدل على أن المشرع الجزائري لم يتبنى بما يعرف بالبنوك الرقمية الافتراضية؛ إذ أن هذه البنوك لا تمتلك وجودا ماديا في العالم الحقيقي، بل هي موجودة فقط في الفضاء الإلكتروني.

كما عرفها القانون الإنجليزي على أنها المؤسسات التي تقدم خدمات مالية بصورة حصرية عبر الشبكة، ويتم إدارتها بشكل كامل من قبل منصات إلكترونية[2].

الفرع الثاني: خصائص البنوك الرقمية

إن التنافس في مجال الخدمات المصرفية الرقمية يرتبط بجوهر الخدمة والقدرة على استقطاب الزبائن، مما يجعل البنوك الرقمية تتسم بخصائص معينة تميزها عن المؤسسات البنكية التقليدية، وذلك من خلال توفير الوقت والجهد،

---

1. المادة 7 من النظام رقم 24-04، التي نصت على أنه يمنع على البنك الرقمي فتح أي فروع سوى تلك التي تعرف بأنها "رقمية" وتعمل بالكامل من خلال الأنظمة الآلية.

2. W. Ian & H. Julia, *E-commerce Law and Practice in Europe*, Woodhead Pub, Cambridge, 2001.

بالإضافة إلى توفير خدمات مصرفية جديدة بتكاليف أقل، فضلا عن ضمان الأمان والحماية.

أولا: توفير الوقت والجهد

يسعى البنك الرقمي إلى تقليل الوقت والجهد والمسافة التي يتطلبها الزبون للوصول إلى فروع البنك التقليدي، حيث يمكنه إجراء ذلك بسهولة من خلال هاتفه الذكي أو جهاز الكمبيوتر الخاص به، مما يزيل الحاجة للذهاب إلى فروع البنك التقليدي، وبالتالي يساهم في توفير وقت وجهد كبيرين للزبائن، مما يتيح للعميل في البنك الرقمي الدخول إلى حسابه المصرفي وإجراء معاملاته في أي لحظة يرغب فيها.

ثانيا: توفير خدمات مصرفية جديدة بتكاليف أقل

بالإضافة إلى ما تقدمه البنوك الرقمية من خدمات أساسية، يمكن لهذه المؤسسات أن توفر خدمات مصرفية حديثة مثل الاستثمار، التأمين، والقروض، يرغب الزبائن في الحصول على جميع الخدمات المصرفية التقليدية المعروفة، فضلا عن أنهم يتطلعون إلى المزيد من الخدمات البنكية الجديدة عبر شبكة الأنترنت، والتي تتميز بتطورها[1]؛ فتلك الخدمات الجديدة لا يمكن لأي مصرف تقديمها لزبائنه إلا إذا كان بنكا رقميا، حيث تتميز هذه العمليات البنكية بسرعة التنفيذ، وهو أمر لا تستطيع المؤسسات المصرفية التقليدية القديمة تحقيقه[2].

---

1. Mahmood SHAH & Steve CLARKE, "E-banking Mangement Issues, solutions and strategies", *information science reference*, 2009, p 4. Mahmood & Steve

2. يوسف حسن يوسف، ***البنوك الإلكترونية***، المركز القومي للإصدارات القانونية، مصر، الطبعة الأولى، 2012، ص 16.

من بين أهم مميزات البنوك الرقمية أن تكاليفها في تقديم الخدمة أقل بكثير من تلك الخاصة بالبنوك التقليدية، ومن ثم فإن تقليل التكلفة وتحسين جودتها هي من عوامل جذب الزبون، كما أن هذه الميزة في صالح البنك نفسه، بحكم أن مصاريف التشغيل تعتبر معدومة نهائيا لإختلاف طبيعتها عن طبيعة البنوك التقليدية العادية نظرا لعدم إحتياجها إلى مقر وتأثيث وعمالة كبيرة وما إلى ذلك[1].

ثالثا: ضمان الأمان والحماية

يوفر البنك الرقمي للزبائن مستويات أمان مرتفعة لضمان حماية وسلامة معطياتهم المالية، تستخدم البنوك الرقمية بروتوكولات معقدة ومتطورة للدفاع عن أنظمتها، ولإعطاء العملاء شعورا بالأمان تجاه حساباتهم وأموالهم، يشمل ذلك على سبيل المثال حماية المعطيات والتواصل من خلال التشفير، بالإضافة إلى اعتماد المصادقة متعددة العوامل، وتنبيهات الأمان، وعمليات تسجيل الخروج التلقائي، والتي تعتبر ميزات أساسية لتأمين البنك على الأنترنت.

المطلب الثاني:

و اقع البنوك الرقمية في الجز ائروتحدياتها

تعتبر البنوك الرقمية عنصرا محوريا في عصرنة النظام البنكي، حيث تتواكب مع التحديات الحالية في عصر المعلومات؛ فقد أصبحت التجارة الإلكترونية ووسائل الدفع الإلكتروني من العوامل الأساسية التي تعزز الاقتصاد الوطني، لذلك أدرك المشرع الجزائري مدى أهمية هذه البنوك ويسعى للاستفادة منها لدعم الاقتصاد

1. منير الجنيهي وممدوح الجنيهي، ***البنوك الإلكترونية***، دار الفكر الجامعي،الإسكندرية، 2005، ص 17.

بشكل متكامل، ورغم المميزات المرتبطة بالبنوك الرقمية؛ فإن المخاطر التي تواجهها كبيرة سواء من ناحية حماية أموال هذه البنوك أو من الجوانب الاقتصادية بشكل عام.

الفرع الأول: وضع البنوك الرقمية في الجزائر

قبل صدور القانون النقدي والمصرفي رقم 23-09، لم يكن هناك بنوك رقمية قائمة بشكل كامل في الجزائر، باستثناء بنك بنكسي[1] الذي يعد بمثابة بنك محمول يمكن تحميله مجانا على الهواتف الذكية، يتيح هذا البنك إجراء المعاملات مع البنوك التقليدية بكل سهولة عن بعد، بالإضافة إلى ذلك هناك مجموعة من البنوك التقليدية التي بدأت في تقديم خدمات رقمية من خلال تطبيقاتها ومنصاتها الإلكترونية.

ومع تزايد ظهور البنوك الرقمية وتوسعها عالميا، أصبح من الضروري للبنوك في الجزائر أن تتكيف معها، بدأت هذه البنوك بوضع استراتيجيات للتحول نحو الصيرفة الرقمية بناءً على أسس متينة، وبذلت مجهودات أكبر لتلبية متطلبات الزبائن بكفاءة وفاعلية، ولتحقيق التحول الرقمي المأمول، وذلك في سبيل تقديم خدمات بنكية عبر مواقع وأدوات رقمية متنوعة.

[1]- بنك بنكسي (Banxy) أطلقته شركة نتيكسيس (Natixis) الجزائر في 23 أفريل 2018، تنتمي إلى مجموعة BPCE، ويعتبر أول بنك أوروبي تم تأسيسه في الجزائر حيث بدأ تواجده منذ عام 1999، مع وجود حوالي 800 موظف و28 وكالة منتشرة في جميع أنحاء الجزائر، توفر شركة نتيكسيس (Natixis) الجزائر مجموعة شاملة من المنتجات والخدمات المالية للشركات الكبيرة، المؤسسات الصغيرة والمتوسطة، المحترفين والأفراد.

علاوة على ذلك يعتمد الزبائن بشكل كبير على خدمات أجهزة الصراف الآلي، بالرغم من ندرتها وكونها محصورة على عدد محدود من البنوك، تليها الاعتماد على الخدمات المصرفية عبر الهواتف الذكية، من جهة أخرى، فإن استخدام نقاط الدفع الإلكترونية قليل للغاية، ويرجع ذلك إلى قلة استخدام بطاقات البنوك الذكية وعدم توفر أجهزة الدفع الإلكتروني في معظم المتاجر[1].

ومع توجه الجزائر نحو اعتماد البنوك الرقمية وفقا للقانون النقدي والمصرفي رقم 23-09؛ فإن النظام المصرفي سيواجه تغييرات كبيرة، بما في ذلك احتمال فقدان العديد من الوظائف داخل البنوك، أيضا فإن الانتقال الكامل نحو الرقمنة سيؤدي إلى تقليص عدد العاملين في هذا المجال، علاوة على ذلك سيكون بإمكان الزبائن في المستقبل الحصول على إجابات لاستفساراتهم البسيطة مباشرة من خلال استخدام خدمات الدردشة المدعومة بالذكاء الصناعي.

الفرع الثاني: مخاطر عمليات البنوك الرقمية

تحاط العمليات المصرفية التي تقوم بها البنوك الرقمية بمجموعة من المخاطر المتنوعة؛ إذ يمثل الخطر عمل المؤسسات المالية والمخاطر التي تواجهها البنوك نتيجة طبيعة عملها، مما يؤدي إلى تكبد خسائر مالية، يحدث هذا بسبب ما تتعرض له هذه البنوك من خسائر في الأصول المالية أو الأصول الشخصية نتيجة لعوامل غير متطورة على المدى الطويل أو القصير، من بين هذه المخاطر، نجد

[1]- حنان دريد وطاووس غريب، "الصيرفة الرقمية كتوجه جديد للبنوك الجزائرية (دراسة احصائية)"، ***المجلة العلمية المستقبل الاقتصادي***، جامعة محمد بوقرة، بومرداس، المجلد 10، العدد 01، ديسمبر 2022، ص 613.

المخاطر التقنية، والمخاطر القانونية، فضلا عن مجموعة متنوعة من المخاطر الأخرى.

في هذا الإطار فرضت لجنة بازل للرقابة المالية على البنوك وضع مجموعة من السياسات والإجراءات التي تسمح لها بالتعامل مع المخاطر المرتبطة بالخدمات المصرفية الرقمية، من خلال تقييمها ومراقبتها واستمرار متابعتها، وأعلنت اللجنة في مارس 1998 وماي 2001 عن مبادئ تهدف إلى التحكم في تلك المخاطر.

أولا: المخاطر التقنية

تظهر هذه المخاطر نتيجة لفرص حدوث خسائر ناتجة عن قصور في فعالية النظام أو أخطاء من قبل الزبائن، أو بسبب استخدام برنامج إلكتروني غير مناسب للمصارف والخدمات المالية الإلكترونية، كذلك قد تنشأ مشكلات بسبب تدخلات خارجية تؤدي إلى تعطيل النظام مثل إدخال برمجيات ضارة إليه[1].

وبالتالي تشمل المخاطر الفنية الأخطاء والأعطال في أنظمة تكنولوجيا المعلومات، مما يؤدي إلى عدم توافر المعلومات في الوقت المناسب وبالدقة اللازمة، وترى لجنة بازل أن المخاطر التشغيلية تمثل معاني متعددة في قطاع البنوك، ولذلك من الضروري أن تعتمد البنوك لأغراض داخلية، على تعريفها الخاص للمخاطر الفنية[2].

---

[1]- الحسين حسن شحادة، ***الجديد من أعمال المصارف من الوجهتين القانونية والاقتصادية***، الجزء الأول، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2002، ص 267.

[2]- شيرين سلطان، ***التنظيم القانوني للمعاملات المصرفية الالكترونية (في ضوء السياسة النقدية للدولة)***، دار الجامعة الجديدة، مصر، 2020، ص 304.

ثانيا: المخاطر القانونية

تظهر المخاطر القانونية عندما يفشل البنك الرقمي في الالتزام بالقوانين والأنظمة المعمول بها، أو عندما تكون الأطر القانونية غامضة أو غير محددة بالنسبة للعمليات المصرفية الحديثة، لذا تنشأ هذه المخاطر عند عدم الامتثال للقوانين أو الأنظمة المقررة، سيما فيما يخص حماية سرية المعلومات المصرفية، وانتهاك الخصوصية، أو بسبب غياب تعريف واضح للحقوق والالتزامات القانونية الناتجة عن المعاملات المصرفية الإلكترونية.

تشمل الخدمات المصرفية الرقمية مخاطر قانونية كبيرة بالنسبة للبنوك، الفكرة الأساسية المطروحة حاليا هي أن هذه الخدمات قد تساعد في تعزيز عمليات غسل الأموال وتمويل الأنشطة غير القانونية على مستوى العالم، ويرجع ذلك إلى مستوى الخصوصية الذي توفره هذه التكنولوجيا للأفراد[1].

الخاتمة:

إن الاتجاه نحو رقمنة النظام المصرفي وتعزيز البنوك الرقمية والعملات الرقمية، من المحتمل أن يحدث تحولا ملحوظا في القطاع المصرفي الجزائري في مجالات البنوك الرقمية والخدمات المصرفية عبر الأنترنت، وذلك بفضل القانون النقدي والمصرفي الجديد التي يدعم الابتكار والتقدم التكنولوجي في هذا المجال.

[1]. عصام ابراهيم الترساوي، ***غسيل الأموال***، الهيئة المصرفية العامة للكتاب، مصر، 2002، ص ص 210-209.

ومن خلال هذه الدراسة تم التوصل إلى مجموعة من النتائج التي يمكن تلخيصها على النحو التالي:

* أن جودة خدمات البنوك الرقمية تعتمد بشكل كبير على مستوى الأداء التقني، الذي يرتبط بشكل مباشر بشبكة الاتصالات، وبالتالي كلما زادت المعوقات التي قد تعرقل الأفراد من الاتصال بالشبكة، زاد التأثير السلبي على فعالية التعامل مع البنوك الرقمية.

* ساهم القانون رقم 23-09 في وضع القواعد اللازمة لتطوير البنية التحتية الرقمية في القطاع المالي والتحول إلى بنك رقمي مع تبني تكنولوجيا البلوكتشين والذكاء الاصطناعي، يتطلب هذا التحول نحو البنوك الرقمية توفر مجموعة من المزايا كالكفاءة التنافسية والقدرة على التكيف مع التغيرات في السوق.

واستنادا إلى النتائج المتوصل إليها يمكن تقديم المقترحات التالية:

* يجب وضع تشريعات وأنظمة مالية وضريبية تخص تداول العملات الرقمية، وتنظيم ذلك ضمن إطار قانوني لضمان التعامل بها من خلال المؤسسات المصرفية والبنوك المركزية والهيئات الحكومية.

* من الضروري التفكير في كيفية بناء البنية التحتية التكنولوجية المطلوبة لتحقيق التحول الرقمي في مجال البنوك، وكذلك استعراض المخاطر الجديدة التي قد تظهر نتيجة لذلك، فضلا عن كيفية التعامل معها، وخاصة من خلال ابتكار أفكار تدعم البنوك في التعرف على الفرص والتحديات الرئيسية، والتواصل من أجل وضع خطة استراتيجية لهذه البنوك.

* ضرورة تعزيز استخدام أنظمة الدفع الإلكتروني، لأنه لا يمكن إنشاء بنوك رقمية دون السعي لتعميم هذه الأنظمة.

قائمة المصادر و المراجع:

1. المؤلفات:

- الترساوي عصام ابراهيم، ***غسيل الأموال***، الهيئة المصرفية العامة للكتاب، مصر، 2002.

- الجنبيهي منير محمد، ***الطبيعة القانونية للعقد الإلكتروني***، دار الفكر الجامعي، مصر، دون سنة نشر.

- الجنيهي منير والجنيهي ممدوح، ***البنوك الإلكترونية***، دار الفكر الجامعي،الإسكندرية، 2005.

- الحداد وسيم محمد، ***الخدمات المصرفية الالكترونية***، دار المسيرة، الأردن، الطبعة الأولى، 2012.

- الحمادة حمود محمد غازي، ***العلاقات التعاقدية الناشئة عن بطاقات الدفع الالكتروني***، المركز العربي للنشر والتوزيع، مصر، الطبعة الأولى، 2018.

- الشمري ناظم محمد نوري والعبداللات عبد الفتاح زهير، ***الصيرفة الإلكترونية "الأدوات والتطبيقات ومعيقات التوسع"***، دار وائل للنشر، الأردن، الطبعة الأولى، 2008.

- الشوره جلال عايد، ***وسائل الدفع الإلكتروني***، دار الثقافة للنشر والتوزيع، الأردن، الطبعة الأولى، 2008.

- سلطان شيرين، ***التنظيم القانوني للمعاملات المصرفية الالكترونية (في ضوء السياسة النقدية للدولة)***، دار الجامعة الجديدة، مصر، 2020 .

- شحادة الحسين حسن، ***الجديد من أعمال المصارف من الوجهتين القانونية والاقتصادية***، الجزء الأول، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2002.

- مسعودي عبد الهادي، ***الأعمال المصرفية الالكترونية***، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2016.

- يوسف حسن يوسف، ***البنوك الإلكترونية***، المركز القومي للإصدارات القانونية، مصر، الطبعة الأولى، 2012.

2. المقالات العلمية:

- الرشيد بوعافية، "دور النقود الالكترونية في تطوير التجارة الالكترونية"، ***المجلة الجزائرية للاقتصاد والمالية***، جامعة يحي فارس، المدية، العدد 02، سبتمبر 2014.

- جلول شرارة وليلى إسمهان بقبق، "العملات الرقمية للبنوك المركزية "تحديات ومتطلبات الدينار الرقمي الجزائري في ظل القانون النقدي والمصرفي 23-09"، ***مجلة طبنة للدراسات العلمية الأكاديمية***، المركز الجامعي بريكة، الجزائر، المجلد 06، العدد 02.

- حنان دريد وطاووس غريب، "الصيرفة الرقمية كتوجه جديد للبنوك الجزائرية (دراسة احصائية)"، ***المجلة العلمية المستقبل الاقتصادي***، جامعة محمد بوقرة، بومرداس، المجلد 10، العدد 01، ديسمبر 2022.

- سعاد عون الله ورضوان عامري، "مخاطر وتداعيات تداول العملات المشفرة على استقرار القطاع المالي خلال الفترة 2017-2021"، ***مجلة اقتصاديات شمال إفريقيا***، جامعة حسيبة بن بوعلي شلف، الجزائر، المجلد 19، العدد 31، 2023.

- عبد الفتاح محمد أحمد صلاح، "البيتكوين عملة الكترونية مشفرة قد تسبب أزمة اقتصادية عالمية جديدة"، ***مجلة الاقتصاد الإسلامي العالمية***، مركز أبحاث فقه المعاملات الإسلامية، سوريا، العدد 33، فيفري 2015.

- عبد الله بن سليمان بن عبد العزيز الباحوث، "النقود الافتراضية مفهومها وأنواعها وآثارها الاقتصادية"، ***المجلة العلمية للاقتصاد والتجارة***، كلية التجارة، جامعة عين شمس، مصر، المجلد 47، العدد 1، 2017.

- عز الدين شرون وبوبكر مصطفى، "العملات المشفرة مستقبل المعاملات المالية "البتكوين نموذجا"، ***مجلة المنهل الإقتصادي***، كلية العلوم الإقتصادية، جامعة الوادي، الجزائر، المجلد 1، العدد 2، ديسمبر 2018.

3. القوانين:

- القانون رقم 17-11 المؤرخ في 27 ديسمبر 2017، والمتضمن قانون المالية لسنة 2018، الجريدة الرسمية، العدد 76، المؤرخة في 28 ديسمبر 2017.

- القانون رقم 23-09 المؤرخ في 21 يونيو 2023، يتضمن القانون النقدي والمصرفي، الجريدة الرسمية، العدد 43، المؤرخة في 27 يونيو 2023.

- النظام رقم 24-03 المؤرخ في 24 جويلية سنة 2024، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل ومكافحتها، الجريدة الرسمية، العدد 58، المؤرخة في 22 أوت 2024.
- النظام رقم 24-04 المؤرخ في 13 أكتوبر 2024، المتعلق بالشروط الخاصة للترخيص بتأسيس واعتماد وممارسة نشاط البنك الرقمي، الجريدة الرسمية، العدد 77، المؤرخة في 19 نوفمبر 2024.
- النظام رقم 25-02 المؤرخ في 14 أفريل سنة 2025، والمحدد لشروط الترخيص بتأسيس واعتماد وممارسة نشاطاتهم، الجريدة الرسمية، العدد 28، المؤرخة في 7 ماي 2025.
- القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية الذي تم إعتماده بتاريخ 19 نوفمبر 2009، بموجب قرار مجلس وزراء العدل العرب رقم 812/د 25.

4. **Ouvrages**:

- IAN Walden & JULIA Hörnle, *E-commerce Law and Practice in Europe*, Woodhead Pub, Cambridge, 2001.

5. **Articles**:

- BERENSTEN Aleksander, "Monetary Policy Implications of Digital Money", *Kyklos*, nº1, 1997.
- BARRDEAR John & KUMHOF Michael, "The Macroeconomics of Central Bank Issued Digital Currencies", *staff working paper*, nº 605, July 2016.
- SHAH Mahmood & CLARKE Steve, "E-banking Mangement Issues, solutions, and strategies", *information science reference*, 2009.

استخدام أدوات الذكاء الاصطناعي

في حماية حقوق المؤلف

Using artificial intelligence tools to protect copyright

د. برابح منير

المركز الجامعي سي الحواس بريكة: mounir.berrabah@cu-barika.dz

د. طويرات عبد الرحمان

المركز الجامعي سي الحواس بريكة : abderrahmane.touirat@cu-barika.dz

ملخص:

من بين أهم التطورات التي أفرزها التطور التكنولوجي والعملي ما يعرف بأدوات الذكاء الاصطناعي، حيث تم استحداث روبوتات تقوم مقام العقل البشري في التحليل وإنتاج المعلومات وتوليد الأفكار وترجمتها ...الخ، لذا فإن الأنظار كلها متجه إلى المجالات المختلفة لاستخدام هذه ولعل من بين أهم المسائل التي يمكن أن تستخدم فيها هذه الأدوات مجال الملكية الفكرية وبالضبط مجال حماية حقوق المؤلف.

الكلمات المفتاحية: حقوق، مؤلف، حماية، ذكاء، إصطناعي.

***Abstract**:*

Among the most important developments brought about by technological and practical progress are what are known as artificial intelligence tools, where robots have been created to replace human work in analyzing and producing information, generating and translating ideas, etc. Therefore, all eyes are directed towards the various fields in which these tools can be used. Perhaps among the most important issues in which these tools can be used is the field of intellectual property, specifically the field of copyright protection.

***Keywords:** Rights, author, protection, artificial intelligence.*

مقدمة:

نتج عن التطور العلمي والتكنولوجي ظهور أدوات ذكاء اصطناعي والتي عادة ما ترتبط بقاعدة بيانات أو مواقع مرتبطة بالشبكة العنكبوتية حيث تحل هذه الأدوات محل العقل البشري في كثير من الأعمال منها تحليل المعلومات، إنجاز أعمال علمية من كتب ومقالات ومذكرات، معتمدتا في ذلك على قاعدة البيانات التي ترتبط بها أو من خلال المواقع الإلكترونية التي تتصل بها ...الخ.

ولقد بدأ الناس خاصة على مستويات البحث العلمي والإنتاجات الفكرية والعلمية في استعمال واستغلال أدوات الذكاء الاصطناعي كوسيلة مساعدة على في مختلف الأعمال العلمية، بداية من البحث عن المراجع والمصادر ووصولا إلى توليد أعمال علمية كاملة من خلال استعمال هذه الأدوات.

ولقد تعددت استعمالات أدوات الذكاء الاصطناعي بين استخدامات إيجابية تصب في صميم خدمة العلم والاكتشافات والاختراعات العملية، وبين من يستخدمها في مجالات سلبية منها سرقة الأفكار والإنجازات البشرية، وهنا تظهر

أهمية أدوات الذكاء الاصطناعي كأداة مساعدة في حماية الملكية الفكرية ومن بينها حقوق المؤلف.

وتتجلى **أهمية موضوع** استخدام أدوات الذكاء الاصطناعي في حماية حقوق المؤلف في الوقوف على مدى استعمال هذا الوسيلة في إكتشاف السرقات العلمية بسهولة وببساطة ن موفرة بذلك الكثير من الجهد والوقت الذي قد تتطلبه وسائل أخرى.

أم عن **سبب اختيار موضوع** فيعود إلى الوقوف على التعامل مع وسائل الذكاء فاصطناعي باعتبارها واقع عملي وعلمي، واستخدامها بشكل إيجابي في مجال مهم من جوانب الحياة وهو حماية حقوق المؤلف.

أما عن **أهداف الدراسة** فتتمثل في إيجاد آلية واقعية عملية وقانونية لاستخدام أدوات الذكاء الاصطناعي في حماية حقوق المؤلف وتجسيدها في أرض الواقع.

وتتمثل **إشكالية الدراسة** في مايلي: كيف يمكن أن تصبح أدوات الذكاء الاصطناعي وسيلة عملية وقانونية في حماية حقوق المؤلف؟

ومن أجل معالجة هذه الإشكالية فقد ارتأينا تقسيم الدراسة إلى محورين حيث نتطرق في المحور الأول إلى نظرة عامة على حقوق المؤلف والتحديات التي تواجهها في العصر الرقمي، بينما نخصص محور ثانٍ إلى كيفية استغلال الذكاء الاصطناعي في حماية حقوق المؤلف، فيما نخصص محور ثالث لأهم التحديات التي يمكن أن تواجه مسألة استغلال أدوات الذكاء الاصطناعي في حماية حقوق المؤلف.

المبحث الأول:

نظرة عامة حول حقوق المؤلف والتحديات التي تواجهها في ظل التحول الرقمي

تعد حقوق المؤلف من القضايا الحساسة في العصر الرقمي، حيث يواجه المبدعون تحديات مستمرة في حماية أعمالهم الفكرية من التعديات والسرقات. ومع التطور التكنولوجي السريع، أصبح الذكاء الاصطناعي (AI) أحد الأدوات الفعّالة في تعزيز هذه الحماية[1]. وهو ما يجعلنا نتطرق في هذا المحور إلى نظرة عامة حول حقوق المؤلف (أولا)، ونتطرق بعدها إلى التحديات التي تواجهها في ظل التحول الرقمي (ثانيا).

المطلب الأول:

نظرة عامة حول حقوق المؤلف

حقوق المؤلف هي حقوق قانونية تمنح للمبدعين (مثل الكتاب والفنانين والموسيقيين) السيطرة على أعمالهم الأصلية. تهدف هذه الحقوق إلى حماية الإبداع الفكري وتوفير الحوافز للمبدعين للاستمرار في العمل. ومع التوسع الكبير في استخدام الإنترنت والمنصات الرقمية، أصبح من الصعب تحديد والتحقق من التعديات على حقوق المؤلف[2]، ويعتبر من أهم حقوق المؤلف تأليف كتاب علمي أو أدبي[3].

[1] Ginsburg, J. C., & Beryl, W Digital Copyright and Artificial Intelligence. Oxford University Press, 2020, p 14

[2] Ibid, p20 Ibid, p20

[3] محمد الصغير بعلي، المدخل للعلوم القانونية نظرية القانون ونظرية الحق، دار العلوم، عنابة الجزائر، 2006، ص122.

والمؤلف المقصود بالحماية هنا هو الشخص الذي قام بالإنتاج الفكري مثل مؤلف كتاب في التاريخ أو الطب، ملحن نشيد، مهند إنجازات برنامج للحاسوب[1].

ولقد عرف المشرع الجزائري المؤلف بموجب الأمر 03-05 بأنة [2]" يعتبر مؤلف أدبي أو فني في مفهوم هذا الأمر الشخص الطبيعي الذي أبدعه.

يمكن اعتبار الشخص المعنوي مؤلفا في الحالات المنصوص[2] عليها في هذا الأمر."

وكون أن المؤلف هو صاحب الإبداع الأدبي أو الفني، فإن القانون يضمن له حماية من كل وجميع الاعتداءات خاصة السرقات التي يمكن أن تطال هذه الأعمال.

ومع تطور وسائل نشر الأعمال العلمية والفنية من وسائل تقليدية متمثلة في دعائم ورقية تنشر عن طريق دور نشر وغيرها، حيث ظهرت وسائل نشر جديدة عبر المواقع الإلكترونية، وغيرها تنوعات تطورت الاعتداءات التي يمكم أن تطال حقوق المؤلف، فوجد هذا الأخير نفسه أمام تحديات في ظل العصر الرقمي.

المطلب الثاني:

التحديات التي تواجه حقوق المؤلف في العصر الرقمي

أدى التوسع الهائل في استخدام الإنترنت ووسائل التواصل الاجتماعي إلى زيادة فرص التعدي على حقوق المؤلف. من أبرز التحديات التي تواجه حماية هذه الحقوق:

---

[1] المرجع نفسه، ص123.

[2] ورد النص أعلاه في المادة 12 من الأمر المذكور أعلاه والصادر بتاريخ 19 /06/ 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية لجمهورية الديمقراطية الشعبية، العدد 44، الصادرة بتاريخ 23 /06/ 2003

1- **سهولة النسخ والانتهاك عبر الوسائط الرقمية:** أصبحت المصنفات الرقمية عرضة للنسخ والتحميل غير المشروع بسهولة بالغة، مما أضعف من قدرة المؤلفين على التحكم في استغلال أعمالهم أو الحصول على عائد مالي مناسب. تُعد قابلية النسخ اللانهائي للمصنفات الرقمية دون فقدان الجودة من أبرز التحديات التي تقوض الحماية التقليدية لحقوق المؤلف[1].

2- **صعوبة تحديد الجهة المسؤولة عن الانتهاك:** أدى استخدام الإنترنت إلى تعقيد تحديد المسؤولية، فقد يكون الانتهاك صادرًا من مستخدم مجهول الهوية أو من منصة رقمية تُستعمل كوسيط. في البيئة الرقمية، تتعدد أطراف المسؤولية بين المستخدم، والمنصة، ومقدم خدمة الإنترنت، ما يصعّب تطبيق الإجراءات القانونية الكلاسيكية[2].

3- **تنازع القوانين في المطبقة في المجال الرقمي:** يُعد البُعد العابر للحدود أحد أبرز خصائص الإنترنت، إذ يمكن انتهاك حقوق المؤلف في بلد معين من خلال خوادم موجودة في بلد آخر يخضع لتشريع مختلف.

فتنازع القوانين يشكل عائقًا حقيقيًا في وجه إنفاذ حقوق المؤلف على المستوى الدولي، ما يتطلب وجود نوع من التعاون التشريعي والقضائي عابر للحدود[3].

4- **قلة الوعي القانوني لدى المستخدمين:** يوجد الكثير من المستخدمين يجهلون أن تحميل أو مشاركة المصنفات دون إذن المؤلف أو صاحب الحق يشكل مخالفة قانونية، وهو ما يكرّس الانتهاكات اليومية.

---

[1] عبد الله محمد علي، الملكية الفكرية في البيئة الرقمية، دار النهضة العربية، القاهرة، 2018، ص 45.

[2] عبير مرزوق، الاعتداء على حقوق المؤلف في الإنترنت، مجلة الدراسات القانونية المعاصرة، العدد 12، 2020، ص 71.

[3] سليم خليل، التشريعات المقارنة لحقوق المؤلف في الفضاء الرقمي، منشورات المعرفة، بيروت، 2019، ص133.

والوضع المذكور أعلاه جعل بعض الفقه[1] يرجع ارتفاع وتيرة الاعتداءات الرقمية على حقوق المؤلف إلى ضعف الوعي القانوني بأحكام الملكية الفكرية في المجال الرقمي.

المبحث الثاني:

كيفية استغلال أدوات الذكاء الاصطناعي في حماية حقوق المؤلف

ونتطرق في هذا المحور إلى الآليات التي من خلالها يمكن توظيف واستعمال أدوات الذكاء الاصطناعي في حماية حقوق المؤلف (أولا)، ثم إلى بعض التطبيقات العملية لهذه الأخيرة في مجال حماية حقوق المؤلف (ثانيا).

المطلب الأول:

آليات توظيف أدوات الذكاء الاصطناعي في حماية حقوق المؤلف

في ظل هذه التحديات، يمكن للذكاء الاصطناعي أن يلعب دورًا محوريًا في تعزيز حماية حقوق المؤلف عبر مجموعة من التطبيقات والتقنيات المتقدمة:

1- أنظمة اكتشاف الانتهاكات: يتم استخدام تقنيات الذكاء الاصطناعي لتطوير أنظمة آلية لها القدرة على اكتشاف الانتهاكات لحقوق المؤلف. يمكن لهذه الأنظمة تحليل النصوص والصور والفيديوهات والصوتيات بشكل دقيق لمقارنة المحتوى الأصلي مع النسخ المنتشرة على الإنترنت. على سبيل المثال، تستخدم

[1] محمد الحسين، "حقوق المؤلف بين النظرية والتطبيق في الجزائر"، مجلة البحوث القانونية والاقتصادية، العدد 8، 2021، ص59.

منصات مثل يوتيوب (YouTube) وخدمات بث الموسيقى (مثل سبوتيفاي)[1]، تقنيات الذكاء الاصطناعي للكشف عن مقاطع الفيديو والموسيقى المحمية بحقوق المؤلف.

2- **التعرف على النصوص والصوروالفيديو:** تتيح تقنيات الذكاء الاصطناعي مثل التعرف على الصور (Image Recognition) والتعرف على النصوص (Text Recognition)إجراء مقارنة شاملة بين المحتوى الرقمي المتاح على الإنترنت والمواد المحمية بحقوق المؤلف. على سبيل المثال، يمكن استخدام خوارزميات الذكاء الاصطناعي لاكتشاف نسخ غير قانونية من الصور أو مقاطع الفيديو على الإنترنت.

3- **تحليل البيانات الكبيرة**: يمكن للذكاء الاصطناعي تحليل كميات ضخمة من البيانات لتحديد الاتجاهات التي تشير إلى الانتهاكات المحتملة لحقوق المؤلف. يمكن للمطورين والمبدعين تتبع أماكن نشر أعمالهم عبر الإنترنت وحمايتها باستخدام تقنيات التعلم [2].

4- **التحليل العاطفي للمحتوى**: بفضل استخدام الذكاء الاصطناعي، نستطيع تحديد ما إذا كانت النسخ المتاحة على الإنترنت هي تعدي على المحتوى الأصلي. تتضمن هذه التقنيات القدرة على تحليل الأسلوب الفني، والموضوعات المشتركة، وأنماط النصوص في الأعمال المختلفة.

لكن هناك تطبيقات عملية أثبتت استخدام أدوات الذكاء الاصطناعي في مجال حماية حقوق المؤلف أم لا؟.

[1] Finkelstein, D. Artificial Intelligence and Copyright Law: A Review of Issues and Opportunities. Journal of Intellectual Property Law, 25(1), 34, 2021, p 56.

[2] European Commission. Artificial Intelligence for Copyright Enforcement: Opportunities and Challenges. Retrieved from https://ec.europa.eu/digital-strategy, Publication date 2020 ,Viewing date 26/06/2025.

المطلب الثاني:

تطبيقات عملية للذكاء الاصطناعي في حماية حقوق المؤلف

توجد العديد من التطبيقات العملية التي استخدمت أدوات الذكاء الاصطناعي في مجال حماية حقوق المؤلف، ومن أبين أهم هذه التطبيقات نذكر مايلي:

1- **خدمة Content ID من يوتيوب:** تستخدم هذه الخدمة الذكاء الاصطناعي لمقارنة الفيديوهات التي يتم تحميلها إلى منصة يوتيوب ضد قاعدة بيانات من مقاطع الفيديو المحمية بحقوق المؤلف[1].

2- **أنظمة مكافحة القرصنة الرقمية:** تستخدم شركات مثل Spotify و Apple Music تقنيات مشابهة لحماية المحتوى الصوتي من القرصنة.

3- إدارة طلبات حماية الملكية الفكرية: تعمل العديد من المنظمات والهيئات كالمنظفة العالمية للملكية الفكرية (WIPO) على أدوات الذكاء الاصطناعي من أجل تيسير البحث عن الأعمال المشابهة وتقييم الطلبات المتعلقة بتسجيل أو طلب إزالة المحتوى[2].

[1] YouTube. Content ID and Copyright. YouTube Help Center. Retrieved from https://support.google.com/youtube. Viewing date 26/06/2025.

[2] محادثة الويبو بشأن الملكية الفكرية والذكاء الاصطناعي، الدورة الثانية، مشروع قائمة قضايا سياسات الملكية الفكرية والذكاء الاصناعي، من إعداد أمانة الويبو، بتاريخ 13 ديسمبر 2019، منشور على الموقع التالي(1)wipo-ip-ai-2-ge-20-1 ، تاريخ الإطلاع 2025/06/27

المطلب الثالث:

تحديات استخدام الذكاء الاصطناعي في حماية حقوق المؤلف

على الرغم من الفوائد العديدة لتوظيف الذكاء الاصطناعي في حماية حقوق المؤلف، إلا أن هناك بعض التحديات التي يجب معالجتها:

1- **غموض الوضع القانوني للإنتاجات الذكية:** بالنظر إلى معظم التشريعات، نجدها لا تُمنح حماية حقوق المؤلف إلا للأعمال الناتجة عن جهد إنساني. وعليه، فإن المنتجات الإبداعية الناتجة عن خوارزميات الذكاء الاصطناعي تظل خارج نطاق الحماية التقليدية، مما يخلق فراغًا قانونيًا. فعلى سبيل المثال، لم تُقر التشريعات العربية حتى الآن بأحقية الذكاء الاصطناعي في الحصول على حماية مباشرة أو غير مباشرة لمنتجاته[1].

2-**تحديات الإثبات الرقمي في بيئة الذكاء الاصطناعي:** يُصعّب الذكاء الاصطناعي مهمة إثبات الانتهاك، نظرًا إلى الطبيعة المعقدة للأنظمة الذكية والخوارزميات الغامضة. كما أن توليد المحتوى التلقائي يصعب تتبعه، مما يضعف قدرة المؤلفين الأصليين على إثبات حقوقهم أمام القضاء[2].

3-**صعوبة الموازنة بين حماية المؤلف وتشجيع الابتكار:** تفرض التكنولوجيا الحديثة واقعًا جديدًا يتطلب الموازنة بين حماية المؤلفين وتشجيع استخدام أدوات

[1] عادل عبد الغفار، "الذكاء الاصطناعي ومشكلات حماية حقوق الملكية الفكرية"، مجلة العلوم القانونية، العدد 45، 2022، ص 229.

[2] Gervais, D. AI and Copyright: Assessing the Challenge of Human-Machine Creativity, Houston Law Review, Vol. 57, (2020), p 580.

الذكاء الاصطناعي في الإبداع. إلا أن التطبيق المتشدد لقوانين حقوق المؤلف قد يحد من الابتكار، بينما التساهل المفرط يفرغ الحق من مضمونه[1].

4-الخصوصية والأمان: يجب ضمان أن استخدام الذكاء الاصطناعي لا يؤدي إلى انتهاك الخصوصية أو تسريب المعلومات الحساسة.

5- الدقة في الكشف: لا تزال بعض الأنظمة تواجه صعوبة في التمييز بين الاستخدام العادل (Fair Use) والتعدي على حقوق المؤلف.

6- الاعتراف الدولي: يتطلب تعزيز حماية حقوق المؤلف عبر الذكاء الاصطناعي التعاون بين الدول وتوحيد التشريعات الدولية.

الخاتمة:

إن الذكاء الاصطناعي يوفر إمكانيات واعدة في مجال حماية حقوق المؤلف، حيث يمكنه تحسين فعالية وكفاءة الأنظمة المستخدمة للكشف عن التعديات وحماية الإبداعات الفكرية. ولكن، مثل أي تقنية أخرى، يتطلب الأمر مراقبة دقيقة وتطوير مستمر لمواكبة التحديات القانونية والأخلاقية المرتبطة بحماية هذه الحقوق. مع التقدم المستمر في تقنيات الذكاء الاصطناعي، يمكن أن نأمل في أن تكون حماية حقوق المؤلف أكثر فعالية وأقل تكلفة في المستقبل.

ورغم انه لا يوجد نصوص قانونية تتيح اللجوء إلى تقنيات وأدوات الذكاء الاصطناعي من اجل الكشف عن الخروقات والتعديات الحاصلة على حقوق المؤلف، لا أنه لا مانع في رأينا من اللجوء إلى هذه التقنيات عند الرغبة في حماية حقوق المؤلف خاصة من خلال الكشف عن السرقات الطارئة عليها.

[1] Ricketson, S. Copyright and the Public Interest in the Age of Artificial Intelligence, Journal of Intellectual Property Law, Vol. 28, Issue 1, 2021, p 33.

ومن خلال دراستنا أعلاه نصل إلى بعض النتائج أهمها

- إن تقنيات الذكاء الاصطناعي أصبحت إلزامية في مجال حماية حقوق المؤلف ذلك أن هناك بعض الانتهاكات لا يمكن التوصل إليها إلى من خلال استخدام هذه الأدوات.

- أنه لا يوجد ما يمنع من استعمال أدوات الذكاء الاصطناعي آنيا في مجال حماية حقوق المؤلف.

- لا تزال القوانين بصفة عامة وقانون حماية حقوق المؤلف تفتقر إلى النص على ضرورة حماية حقوق المؤلف وبيان كيفية استخدامها.

- يوجد ضعف كبير في مجال مسالة التنسيق بين القوانين في مجال استخدام ادوات الذكاء الاصطناعي بصفة عامة وفي مجال حماية حقوق الملكية الفكرية وضمنها حقوق المؤلف خاصة .

ومن أجل الخروج وتجاوز العوائق التي تواجه مسألة استعمال أدوات الذكاء الاصطناعي في مجال حماية حقوق المؤلف فقد توصلنا من خلال دراستنا هذه إلى مجموعة من الحلول صغنها في شكل توصيات ومقترحات وذلك كمايلي:

1- تعديل القوانين الوطنية بما يتواكب مع التطورات العلمية ومن بينها الذكاء الاصطناعي ، ونخص بالذكر قانون حماية حقوق المؤلف والحقوق المجاورة والنص صراحة على مكانة العمال التي يقوم المؤلف بتوليدها عن طريق هذه الأدوات من جهة، ومن جهة أخرى النص على الآليات القانونية التي يمكن من خلالها استغلال أدوات الذكاء الاصطناعي في حماية حقوق المؤلف.

2- استحداث برمجيات تعمل وفقا لقواعد الذكاء لاصطناعي تمكن من الكشف عن التجاوزات الواقعة على حقوق المؤلفين ولو على المستوى الوطني في الوقت الراهن والعمل على توسيعها إلى النطاق الدولي في إطار فيما بعد.

3- العمل على توحيد الجهود الدولية من خلال إبرام اتفاقية دولية تعمل إيجاد حلول لمسالة تنازع القوانين في مجال تطبيق القواعد القانونية المرتبطة باستخدام آليات الذكاء الاصطناعي كأدوات لحماية المؤلف.

قائمة المصادر والمراجع:

أولا- القوانين:

1- الأمر 03-05 والصادر بتاريخ 19 /06/ 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية لجمهورية الديمقراطية الشعبية، العدد 44، الصادرة بتاريخ 23 /2003/06.

ثانيا- الكتب:

أ- باللغة العربية

1- سليم خليل، التشريعات المقارنة لحقوق المؤلف في الفضاء الرقمي، منشورات المعرفة، بيروت، 2019.

2- عبير مرزوق، الاعتداء على حقوق المؤلف في الإنترنت، مجلة الدراسات القانونية المعاصرة، العدد 12، 2020.

3 -عبد الله محمد علي، الملكية الفكرية في البيئة الرقمية، دار النهضة العربية، القاهرة، 2018، ص 45.

4- محمد الصغير بعلي، المدخل للعلوم القانونية نظرية القانون ونظرية الحق، دار العلوم، عنابة الجزائر، 2006، ص122.

5- محمد الحسين، "حقوق المؤلف بين النظرية والتطبيق في الجزائر"، مجلة البحوث القانونية والاقتصادية، العدد 8، 2021، ص 59.

ب- باللغة الأجنبية:

1- Ginsburg, J. C., & Beryl, W Digital Copyright and Artificial Intelligence. Oxford University Press, 2020. p 14.

ثالثا- المقالات والمجلات:

أ- باللغة العربية:

1- عادل عبد الغفار، "الذكاء الاصطناعي ومشكلات حماية حقوق الملكية الفكرية"، مجلة العلوم القانونية، العدد 45، 2022.

ب- باللغة الأجنبية:

1- Finkelstein, D. Artificial Intelligence and Copyright Law: A Review of Issues and Opportunities. Journal of Intellectual Property Law, , 25(1), 2021.

2- Gervais, D. AI and Copyright: Assessing the Challenge of Human-Machine Creativity, Houston Law Review, Vol. 57, (2020).

3- Ricketson, S. Copyright and the Public Interest in the Age of Artificial Intelligence, Journal of Intellectual Property Law, Vol. 28, Issue 1, 2021.

رابعا- المواقع الإلكترونية:

1- European Commission. Artificial Intelligence for Copyright Enforcement: Opportunities and Challenges. Retrieved from https://ec.europa.eu/digital-strategy, Publication date 2020 ,Viewing date 26/06/2025.

2- YouTube. Content ID and Copyright. YouTube Help Center. Retrieved from https://support.google.com/youtube. Viewing date 26/06/2025.

3- محادثة الويبو بشأن الملكية الفكرية والذكاء الاصطناعي، الدورة الثانية، مشروع قائمة قضايا سياسات الملكية الفكرية والذكاء الاصناعي، من إعداد أمانة الويبو، بتاريخ 13 ديسمبر 2019، منشور على الموقع التالي(1)wipo-ip-ai-2-ge-20-1 ، تاريخ الإطلاع 2025/06/27.

أثر الرقمنة والذكاء الاصطناعي

على أداء السلطة التنفيذية في الجزائر

The impact of digitalization and artificial intelligence on the performance of the executive authority in Algeria

الدكتور:توفيق مدّار

كلية الحقوق والعلوم السياسية جامعة الشاذلي بن جديد الطارف

ملخص:

يتناول هذا البحث تأثير تكنولوجيات الرقمنة ومختلف تطبيقات الذكاء الاصطناعي على أداء السلطة التنفيذية في الجزائر، حيث يركز تركيزا خاصا على تأثير هذه التقنيات على مختلف القوانين الفرعية والنظم الإدارية، ويرسم سياسات شمولية لتفادي التهميش الرقمي، ويساعد على تفعيل القدرات الرقابية والتقنية لدى الهيئات المعنية، وتعزيز الحوكمة والشفافية في مشاريع الذكاء الاصطناعي، وتطوير إطار تشريعي وأخلاقي متكامل، ولقد اعتمدت في هذا البحث على المنهج الوصفي التحليلي بوصف الرقمنة كظاهرة حديثة وتحليل مضامينها وكيفية تطبيقها على تسيير الإدارة، وفي نهاية البحث تخلص الدراسة إلى أن الرقمنة والذكاء الاصطناعي يقدمان فرصًا حقيقية لرفع كفاءة الإدارة العامة، وسرعة اتخاذ القرار وتعزيز الشفافية، لكن ذلك يحتاج إلى أطر تشريعية تنظيمية واضحة.

.**الكلمات المفتاحية**: رقمنة؛ ذكاء؛ اصطناعي؛ سلطة؛ تنفيذية.

Abstract:

This research examines the impact of digital technologies and various applications of artificial intelligence on the performance of the executive authority in Algeria. It focuses particularly on how these technologies affect different subsidiary laws and administrative systems, outlining comprehensive policies to prevent digital marginalization. The study also emphasizes enhancing the supervisory and technical capacities of relevant institutions, promoting governance and transparency in AI-related projects, and developing an integrated legislative and ethical

مقدمة:

لقد تزايد اهتمام دول العالم في السنوات الأخيرة بالإدارة الرقمية، حيث مع التدفق التكنولوجي الهائل ساعد على ضبط مجالات عدة إدارية واقتصادية، مما جعل أغلب الدول تفكر في إعادة تشكيل أنماط عمل جديدة لتسيير السلطة التنفيذية، والجزائر بدورها واكبت هذا التحول الرقمي الذي أثر في سياسات التسيير لاسيما في ظل التحولات المرتبطة بالرقمنة والذكاء الاصطناعي، حيث اعتمدت استراتيجيات وطنية طموحة الهدف منها الخروج من الطرق التقليدية في تسيير الإدارة إلى اعتماد الطرق الحديثة التي كانت نتيجة تدفق متطلبات السرعة والشفافية وجودة الأداء، وذلك عبر مختلف المنصات الرقمية وتطبيقات ذكية التي كانت من مفرزات التحول التكنولوجي .

وانطلاقا من هذا فقد أعلنت الدولة الجزائرية اعتماد استراتيجية وطنية للذكاء الاصطناعي لمواكبة التطورات في تسيير الإدارة، من خلال عمل السلطة التنفيذية التي بات من الضروري خلق بيئة عمل جديدة تعتمد في صياغة النصوص التنظيمية على منصات رقمية تترجم قدرة السلطة على استيعاب هذه التغييرات، لذلك بات من الضروري تحليل أثر هذا التحول على الإطار القانوني والمؤسسي المنظم لعمل الجهاز التنفيذي في الجزائر ،وبدأ ترجمة هذا التحول باستحداث آليات تنفيذه تتمثل أساسا في سلطتين مهمتهما رقمنة الإدارة الأولى تتعلق بـ"السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي"، وهو الجهاز الذي يقوم على ضمان الحماية للحياة الخاصة الأفراد، سرية المراسلات والاتصالات، وعدم المساس بها مهما كان الأمر، إلا بأمر قضائي، والثانية تتمثل في "المحافظة السامية للرقمنة عام 2023"[1]، وتستهدف إضفاء الشفافية والمردودية على الاقتصاد الجزائري من أجل جزائر رقمية 2030،والتي من ضمن أهدافها حوكمة الإدارة الرقمية ،هذا التطور يفتح آفاقًا لتحسين أداء السلطة التنفيذية لكنه يثير أيضًا تساؤلات حول مدى إسهام التكنولوجيا — وبشكل خاص الرقمنة والذكاء الاصطناعي — في تطوير أداء السلطة التنفيذية في الجزائر، وتأثيرها على القوانين الفرعية والتنظيمات الإدارية؟

أهمية البحث :

تبرز أهمية هذا البحث في كونه يعالج مسألة التحول الرقمي في الجزائر وتأثيره على أداء السلطة التنفيذية، ويبرز عن انتقال جذري من التسيير الإداري التقليدي إلى الإدارة الرقمية الذكية.

أهداف البحث:

- محاولة تحليل التحول الرقمي ودوره في أداء السلطة التنفيذية.

1 المرسوم الرئاسي رقم 23-314 المؤرخ في 06 سبتمبر 2023 المتضمن إنشاء محافظة سامية للرقمنة الجريدة الرسمية عدد 59 المؤرخ في 10 سبتمبر 2023.

- إبراز تأثير الرقمنة على القوانين الفرعية والممارسات التنظيمية في الجزائر.
-دراسة الانفتاح والتنسيق بين السلطة التنفيذية وباقي الهيئات عبر التكنولوجيا.

- تقييم أثر مبادرات الرقمنة على فعالية الإجراءات الإدارية وقرارات السلطة التنفيذية.

- تحليل دور استراتيجية الذكاء الاصطناعي في تحسين الخدمات العمومية وصنع القرار.

المنهج المتبع:

ولقد اعتمد البحث المنهج الوصفي التحليلي من خلال الوقوف حقيقة الرقمنة كظاهرة حديثة وتحليل مضامينها وكيفية تطبيقها على تسيير الإدارة.

المبحث الأول:
الرقمنة والذكاء الاصطناعي مع عمل السلطة التنفيذية

عرفت الإدارة العمومية في طابعها التقليدي في الجزائر أداء تراتبيا ثابتا ، يكون العمل من خلال تنفيذ القوانين الصادرة عن السلطة التشريعية ، وإصدار النصوص التنظيمية التي تساعد على تطبيق بعض المواد القانونية التي تمس الأداء الوظيفي للسلطة التنفيذية ومن خلالها الإدارة، هذا الأداء خلق بيئة روتينية نمطية في العمل مما ساهم في حدوث نوع من العمل الآلي للموظف خال من الإبداع أو التفكير ، كما ساهم فيى خلق تباطؤ كبير في الإجراءات مما ضيع كثيرا من الأوقات ، وساعد على إرهاق كاهل الخزينة العمومية بما تنفقه على تسيير المرفق العمومي، مما جعل السلطة تفكير جديا في إحداث تحوّلات عميقة تنتقل بها من هذا النموذج التقليدي (الورقي) السلّمي الهرمي، إلى نموذج حديث يسعى لتبني أدوات التحول

الرقمي وتقنيات الذكاء الاصطناعي والهدف من هذا التحول هو تسريع اتخاذ القرارات، وترسيخ مبدأ الشفافية وتحسين جودة الخدمة العمومية، و هذا التحول ليس مجرد تحديث تقني على مستوى الإدارة، بل هو تحول مؤسساتي وقانوني يمس جوهر ممارسة السلطة التنفيذية ووظائفها التنظيمية والتنفيذية على حد سواء.

المطلب الأول:

الإطار المفاهيمي للرقمنة والذكاء الاصطناعي في السياق الإداري

الفرع الأول: الرقمنة للإدارية

لقد عرف المعجم الموسوعي للمعلومات والتوثيق الرقمنة على أنها : "هي عملية إلكترونية لإنتاج رموز إلكترونية أو رقمية من خلال وثيقة أو أي شيء مادي بواسطة إشارات رقمية إلكترونية خاصة"[1].

يقصد بالرقمنة أنها تحويل الاتصال الكتابي والشفوي إلى رسائل إلكترونية يفهمها الجميع. يتم تحقيق هذا التحوّل من خلال شبكات الأعمال والشبكات اللاّسلكية. وهي التكنولوجيات الرقمية[2]. لذلك، يمكن القول أن كل شيء في العالم القديم كان يتطلب مستندًا تجاريًا مكتوبًا، في صيغته الملموسة. يتم تحويله اليوم رقميًا إلى مستندات إلكترونية بواسطة شبكات الأعمال.

1 بشير إبرير: اللغة العربية ومتغيرات الرقمنة ،مجلة المعجم الجزائري للغة العربية المجلد 19 العدد 1 لسنة 2023.

2 آمال كاب، سميرة لالوش، " الرقمنة في المكتبات الجامعية كآلية لتطوير التعليم العالي "، مجلة القانون العام الجزائري والمقارن المجلد التاسع العدد / 02 أفريل ،2024 بوقرة بومرداس- الجزائر، 2024 ، ص42.

وانظر: مليكة بوخاري و سمير يحياوي ، متطلبات تطبيق الرقمنة و دورها في تحسين أداء الإدارة المحلية دارسة حالة الشباك الإلكتروني بلدية البويرة ، دراسات اقتصادية ، 03 أكتوبر ،2022 ع16 ، م3 ، ص ص 457 - 458

إلى جانب ذلك، تشير الرقمنة في الإدارة على تحويل وتحسين نموذج العمل الإداري باستخدام العمليات الرقمية، مثل اتخاذ قرار الإدارية مع معالجتها رقميًا. وتسمح هذه التقنيات الجديدة للسلطة التنفيذية بأن تصبح أكثر كفاءة لتلبية الاحتياجات الإدارية بأقل التكاليف، مع جمع كافة القرارات والقوانين الفرعية المتخذة لتصبح البيانات التي تديرها متاحة رقميًا.

وتُسهم هذه البرامج في تبسيط الإجراءات الإدارية، وتسهيل حياة المواطنين والتخفيف من حدة أعبائهم. إلى جانب زيادة كفاءة المؤسسات والهيئات والرفع من مستوى تنافسيتها، لتنعكس كافة على جودة ومردودية النسيج الإقتصادي والإجتماعي بالبلاد.

وخلاصة القول أن الرقمنة الإدارية من المنظور الإداري تُعرَّف بأنها: " عملية إلكترونية تقوم على تسيير المرفق العمومي بأنظمة معلوماتية متطورة ومؤمّنة".

أي الانتقال من الأساليب التقليدية في تسيير المرفق العام إلى عمليات إلكترونية قائمة على أنظمة معلوماتية مؤمنة، يسمح بتسهيل الإجراءات وتعزيز قابلية تتبّع القرارات الإدارية .وهي لا تُختزل في مجرد نقل الخدمات إلى الفضاء الإلكتروني، بل تمتد إلى إعادة هندسة المسارات الإدارية.

الفرع الثاني :الذكاء الاصطناعي

عرفت لجنة الأمم المتحدة للقانون التجاري الدولي في الدورة الحادية والخمسون لعام ،2018 الذكاء الاصطناعي "...الذكاء الاصطناعي بشكل عام هو علم استنباط نظم قادر على حل المشاكل وأداء الوظائف بمحاكاة العمليات الذهنية، ويمكن تلقين الذكاء الاصطناعي كيفية حل مشكلة ما، ولكنه قادر أيضا على دراسة

المشكلة ومعرفة كيفية حلها بمفرده دون تدخل بشري ويمكن للنظم المختلفة أن تبلغ مستويات مختلفة من التشغيل الذاتي وفي مقدورها أن تتصرف باستقلالية»[1]

يُنظر إلى الذكاء الاصطناعي ع إداريًا هو :"منظومة خوارزمية قادرة على تحليل البيانات الضخمة، واستشراف السيناريوهات، ودعم اتخاذ القرار الحكومي بشكل شبه فوري، دون أن يُقصي العنصر البشري، بل يُعيد تحديد دوره من منفّذ إلى مراقب وموجّه".

وتتجلّى خصوصية هذا المفهوم في السياق الإداري من خلال ربطه باستراتيجية الدولة حول الإدارة الإلكترونية والحكومة الذكية، مما يعكس إرادة سياسية في الانتقال من مرحلة رقمنة الخدمات إلى رقمنة صناعة القرار.

يوفر الذكاء الاصطناعي العديد من التطبيقات التي أصبحت ذات أهمية كبيرة في الحياة اليومية، فعلى سبيل المثال: الهاتف الذكي الذي يحتوي على أنظمة ذكية كنظام تحديد المواقع، و الآلات الذكية التي تعمل بصورة دائمة فتقوم بالإنتاج دون النظر إلى الوقت أو الظروف المحيطة بالعمل، كذلك تستطيع أنظمة الذكاء الاصطناعي التعامل مع كم هائل من البيانات فتقوم بتخزينها ومعالجتها[2].

1 الموقع الالكتروني للأمم المتحدة https://www.un.org/ar/site تاريخ الدخول2025/10/29 التوقيت:15.00

2 سعيد سعد الله بخيت محمد، "أثر تطبيقات الذكاء الاصطناعي في تطوير خدمات المرافق العامة (الإدارة الذكية نموذجا) دراسة مقارنة، "مجلة البحوث الفقهية والقانونية، العدد،43 جامعة الأزهر، مصر ،2023 ص3424.

المطلب الثاني:

السلطة التنفيذية و أبعاد التحديث المؤسسي

الفرع الأول: التحديث المؤسسي للإدارة

تُعتبر السلطة التنفيذية الفاعل المركزي في تجسيد السياسات العمومية للدولة، إذ تجمع بين (الوظيفة التنظيمية) سن اللوائح والمراسيم التنفيذية (والوظيفة التسييرية) تطبيق القوانين وإدارة المرافق العامة .ومع التحول التكنولوجي، لم يعد المطلوب منها مجرد ضمان استمرارية الخدمة العمومية، بل الانتقال نحو نموذج إداري يقوم على السرعة، والتوقّعية، والتكامل المؤسساتي.

ويتجلّى التحديث المؤسسي في ثلاثة أبعاد رئيسية:

1.**البعد القانوني والتنظيمي**: بحيث عملت السلطة التنفيذية على إصدار مراسيم وأنظمة فرعية تنظم المنصات الرقمية والتوقيع الإلكتروني وحماية المعطيات الشخصية[1].

2.**البعد الهيكلي** :بروز وحدات حكومية جديدة مختصة في التحوّل الرقمي ومراكز بيانات.

3.**البعد الوظيفي** :الانتقال من إدارة تعتمد على ردّ الفعل إلى إدارة تعتمد على التحليل الاستباقي للمعطيات. والتسيير التنبؤي.

1 القانون رقم 18-07 المؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص في مجال معالجة المعطيات ذات الطابع الشخصي ج ر عدد 34 المؤرخة في 10 يونيو 2018 المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 جويلية 2025 ج ر عدد 48 المؤرخة في 24 جويلية 2025

هذه الأبعاد تجعل من التحديث التكنولوجي ضرورة سيادية لضمان فعالية عمل السلطة التنفيذية، بحيث يساعدها ذلك في سرعة اتخاذ القرارات المناسبة وسرعة وصولها للخاطبين بها.

المبحث الثاني:

نطاق استخدام الذكاء الاصطناعي في عمل السلطة التنفيذية

المطلب الأول:

رقمنة الهياكل التنفيذية وتعزيز الشفافية والسرعة

يساعد الذكاء الاصطناعي في تسهيل عمل السلطة التنفيذية بتوفر:

الفرع الأول: آليات تسهيل عمل السلطة التنفيذية

1-**التكنولوجيا الداعمة** : هي التي يتم استخدامها لمعاونة أشخاص السلطة التنفيذية على إنجاز مهامهم، كإنجاز المحاضر وصياغة النصوص التنظيمية، وعقد لقاءات بين السلطة التنفيذية والأشخاص ذوي الصلة بها كالتحاضر عن بعد والحضور الميداني الإلكتروني كالزيارات الميدانية إلكترونيا.

2- **حلول التكنولوجيا محل العمل البشري** :بحيث تقوم التكنولوجيا بتوجيه من المختصين بمهام السلطة التنفيذية في باب التنظيم، بحيث يحل محل بعض الأشخاص في إنجاز مهامهم كصياغة النصوص التنظيمية إلكترونيا ن وصياغة القرارات الإدارية وغيرها، لذلك سأعرض بعض التفاصيل المتعلقة بمظاهر التأثير على الأداء المؤسسي والوظيفي للسلطة التنفيذية في الجزائر.

أدت الرقمنة إلى تحويل العديد من العمليات الإدارية من إجراءات يدوية إلى عمليات إلكترونية مؤتمتة عبر منصات حكومية مركزية أو وزارية .هذا التحول أحدث تأثيرات ملموسة:

أ/ تسريع الإجراءات وتقليل البيروقراطية :: خفض زمن إنجاز المعاملات الإدارية، مما يحسّن رضا المواطن ويقلل التراكم فالتحول إلى خدمات إلكترونية يقلّل زمن المعاملة ويخفض الأخطاء الورقية..

ب/ تعزيز الشفافية ومكافحة الفساد :فالسجلات الإلكترونية قابلة للتدقيق تُسهِم في مراقبة الأداء وتقليل المساحات الرمادية، فالسجلات الرقمية والقوائم الإلكترونية تتيح تتبّع الإجراءات والحدّ من الفساد الإداري.

ج/ توحيد الإجراءات : عبر اعتماد قواعد بيانات وطنية مشتركة تقلّص التضارب بين الإدارات

د/ دعم اتخاذ القرار المستند إلى البيانات :أدوات الذكاء الاصطناعي والتحليلات الكبيرة تمكّن صانعي القرار من رؤية أنماط وقياس أثر السياسات بشكل أدق.

مع ذلك فإن هذه المكاسب مرتبطة بجودة البنية التحتية الرقمية وقدرة المستخدمين على الولوج والخبرة الرقمية.

الفرع الثاني :الذكاء الاصطناعي في دعم صياغةالنصوص التنظيمية

ان التطور الحاصل في تكنلوجيا المعلومات والثورة الصناعية الرابعة كان له تأثيرات في مختلف جوانب الحياة ، ولعل أبرز هذه التطورات استخدام قواعد البيانات والتعامل مع شبكة الأنترنت والتوجه نحو ادارة التكنلوجيا الحديثة، ومن ثم سيؤثر ذلك في الية اصدار القرارات الإدارية الخاصة بالموظف العام . إذ يعد القرار الإداري الإلكتروني أحد مظاهر تقنيات المعلومات، و من أهم الوسائل

والأدوات القانونية التي تستعملها الإدارة لممارسة الأعمال المناطة بها، و لسان حال الإدارة والمعبر عن إرادتها التي من خلالها تهدف الى تحقيق الصالح العام، و أهم الأمور الواجب توفرها في النصوص التنظيمية والقرارات الإدارية الإلكترونية هو أن تحتوي على التوقيع الإلكتروني كإجراء شكلي إلا إذا نص المشرع عليها صراحة ، فالتوقيع الإلكتروني هو مجموعة من الإجراءات الفنية التي تسمح بتحرير شخصية مصدر النص التنظيمي والقرار وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته[1].

يستخدم الذكاء الاصطناعي في الإدارة العامة في تطبيقات متعددة :تحليل بيانات الضرائب، توقع الاختلالات الاقتصادية، دعم توزيع الموارد في الصحة والتعليم، وفرز ملفات الدعم الاجتماعي .تمكن هذه التطبيقات من توفير مؤشرات أداء آنية ونماذج تنبؤية تساعد في توجيه السياسات[2].

لكن إدماج الذكاء الاصطناعي يواجه تحديات :تأمين جودة البيانات، تفادي التحيز الخوارزمي، وضمان القابلية للتفسير والمساءلة عند اتخاذ قرارات تؤثر على حقوق المواطنين.

المطلب الثالث:

أثر التكنولوجيا على القوانين الفرعية والتنظيمات الإدارية

تركز هذا المبحث على الكيفية التي تغيّرت بها القواعد التنفيذية، مراسيم، قرارات وزارية، تعليمات بفعل الرقمنة والذكاء الاصطناعي.

الفرع الأول :تطور المراسيم التنفيذية بفعل التحول الرقمي

1 عبد الوهاب ، ناجح أحمد ، التطور الحديث للقانون الإداري في ظل الحكومة الإلكترونية ، دار النهضة العربية القاهرة ، مصر ،2012،ص 288

2 المرجع نفسه.

التحول الرقمي يعتبر أحد التحولات الجوهرية المتعلقة بالمراسيم التنفيذية بحث تصبح ذات ملاحق تقنية تحدد مواصفات الأنظمة، بروتوكولات تبادل البيانات، ومتطلبات أمنية .كما أنها تصير المراسيم تتسم بالمرونة عبر تفويضات محددة تسمح بتحديث المواصفات التقنية بقرارات دورية بدلاً من تعديل النص القانوني الأساسي.

لذلك هذا التكييف مفيد من ناحية الملاءمة التقنية ولكنه يطرح مخاطر توسع سلطة التنفيذ إذا لم تفرض آليات رقابية واضحة.

الفرع الثاني :التكييف القانوني للمنصات والمنظومات الذكية

أدت الإدارة الإلكترونية الحديثة إلى تشبيك واسع وارتباطات الحدود لها بالشبكة العنكبوتية والفضاء الرقمي العالمي في عصر المعرفة وثورة تكنلوجيا المعلومات، وظهر تحول كبير نوعي في نقطة ارتكاز الفكر الإداري، إذ نلاحظ هذا اليوم التحول في التفكير في سرعة صياغة وإصدار القرارات الوزارية أو الادارية ، فلم يعد التركيز في اتخاذها على الجودة فقط وإنما تركز أيضا على ضمان سرعة الاستجابة الفورية والاستجابة في الوقت الحقيقي لتحديات البيئة الكونية للأعمال .

فالنصوص القانونية المتعلقة بالجوانب الإدارية تنجح وتفشل إذا تأخر صانعها بالنقر باللحظة المناسبة على زر الخيار المناسب فضلا عن الخصائص التي جرى ذكرها يجب توافر شروط معينة بذاتها لاتخاذ قرارات صحيحة بعيدة عن المخاطرة ومحاطة بمعلومات موثوقة.

ومن هنا أصبح من الضروري أن تتضمن القوانين الفرعية قواعد لحوكمة المنصات :شروط تشغيل الأنظمة، آليات الوصول إلى البيانات، قواعد حفظ السجلات، ومعايير الشفافية المتعلقة بعمل الخوارزميات .تتطلب المنصات الذكية

أيضًا نصوصًا تنظيمية خاصة بمراحل التجريب(sandboxes) ، وخطوات الاختبار، وشروط إنهاء التجربة أو تعميم النظام[1].

الفرع الثالث :الانفتاح والتنسيق بين الهيئات التنفيذية والمؤسسات الأخرى

تتطلب الرقمنة تنسيقًا بين وزارات متعددة وهيئات تنظيمية مستقلة لضمان تناسق السياسات وحماية الحقوق .وتتضمن آليات التوافق تبادل قواعد بيانات، بروتوكولات أمنية، واتفاقيات تعاون فني وقانوني.

أولا: التعاون الرقمي بين السلطة التنفيذية والهيئات الرقابية والقضائية

تعزيز التعاون مع هيئات حماية المعطيات، هيئات تنظيم الاتصالات، والجهات القضائية يساعد في ضبط استخدام التقنيات وتوفير آليات طعن ومراجعة فنية .يجب أن تضمن اللوائح الفرعية حق الوصول المحدود للجهات الرقابية لتنفيذ تدقيقات دون المساس بسرية البيانات.

ثانيا :التكامل مع الهيئات الاقتصادية والمالية الوطنية والدولية

يتجلى التكامل عبر اعتماد معايير فنية وقانونية موحّدة تسمح بتبادل المعلومات المالية والاقتصادية، وتحقيق تكامل السياسات الرقمية خاصة في مجالات مثل الدفع الإلكتروني والحوكمة المالية.

ورغم الفوائد الواضحة، يواجه إدماج التكنولوجيا في الأجهزة التنفيذية مخاطر متعددة:

-تفاقم التهميش الرقمي لبعض الفئات الجغرافية والاجتماعية.

-توسع نطاق التفويض التنفيذي على حساب رقابة تشريعية.

[1] رشا محمد صائم : تطبيقات الإدارة للذكاء الاصطناعي في اتخاذ القرارات الإدارية، مذكرة ماجستير قانون عام كلية الحقوق جامعة الشرق الأوسط، عمان ، الأردن،2022،ص 26.

- تحديات حماية المعطيات والخصوصية.
-صعوبات التقاضي والمساءلة في حالات قرارات آلية.

الخاتمة

تقدم الرقمنة والذكاء الاصطناعي فرصة غير مسبوقة لتحسين أداء السلطة التنفيذية في الجزائر من خلال زيادة الكفاءة، تعزيز الشفافية، ودعم اتخاذ القرار. وكذلك إن أحسن استثمارها في إطار قانوني مؤسسي متوازن .المفتاح يكمن في التوفيق بين مرونة التحديث التقني ومتطلبات الشفافية والمسائلة وحماية الحقوق لضمان تحول شامل وعادل، لكن مجرد إدخال تقنيات متقدمة لا يكفي — فدون سياسات شمولية تستهدف البنية التحتية، بناء القدرات، أطر قانونية وأخلاقية، وتصميم خدمات تراعي تنوّع المستخدمين، قد تؤدي الرقمنة إلى تعميق التهميش الاجتماعي والرقمي، وتضعف شرعية وفاعلية السلطة التنفيذية، إذن فالتحدّي الفعلي هو جعل التحوّل الرقمي أداة لنهوض شمولي ومستدام، لا مجرد تحديث تقني.وفي نهاية هذا البحث نوصي بالآتي:

1.إقرار آليات تقييم الأثر التكنولوجي والاجتماعي إلزاميًا قبل إصدار أي مرسوم أو قرار تنفيذي يتضمن نظمًا آلية.

2.حصر وتحديد حدود التفويض التشريعي بصورة واضحة مع شروط لتجديد الملاحق التقنية.

3.إدراج آليات تدقيق خوارزمي مستقل وحقوق وصول رقابي لهيئات حماية المعطيات.

4.تنفيذ سياسات شمول رقمي لتمكين المناطق الريفية والفئات الضعيفة من الولوج.

5.تبني بروتوكولات شفافية ملزمة حول عمل الخوارزميات.

6.إنشاء برامج تدريبية للمتعاملين القائمين على السلطة التنفيذية والإداريين حول التقنيات الرقمية والذكاء الاصطناعي.

قائمة المصادر و المراجع:

أولا- المراسيم:

- المرسوم الرئاسي رقم 23-314 المؤرخ في 06 سبتمبر 2023 المتضمن إنشاء محافظة سامية للرقمنة الجريدة الرسمية عدد 59 المؤرخ في 10 سبتمبر 2023.

ثانيا – القوانين:

- القانون رقم 18-07 المؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص في مجال معالجة المعطيات ذات الطابع الشخصي ج ر عدد 34 المؤرخة في 10 يونيو 2018 المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 جويلية 2025 ج ر عدد 48 المؤرخة في 24 جويلية 2025.

ثالثا: الكتب

- عبد الوهاب ، ناجح أحمد ، التطور الحديث للقانون الإداري في ظل الحكومة الإلكترونية ، دار النهضة العربية القاهرة ، مصر ،2012.

رابعا المقالات:

1- آمال كاب، سميرة لالوش، " الرقمنة في المكتبات الجامعية كآلية لتطوير التعليم العالي "، مجلة القانون العام الجزائري والمقارن المجلد التاسع العدد / 02 أفريل 2024، بوقرة بومرداس- الجزائر، 2024 .

2- بشير إبرير: اللغة العربية ومتغيرات الرقمنة ،مجلة المعجم الجزائري للغة العربية المجلد 19 العدد 1 لسنة 2023.

3- مليكة بوخاري و سمير يحياوي ، متطلبات تطبيق الرقمنة و دورها في تحسين أداء الإدارة المحلية دارسة حالة الشباك الإلكتروني بلدية البويرة ، دراسات اقتصادية ، 03 أكتوبر ،2022 عدد16 ، مجلد3 .

4- سعيد سعد الله بخيت محمد، "أثر تطبيقات الذكاء الاصطناعي في تطوير خدمات المرافق العامة (الإدارة الذكية نموذجا) دراسة مقارنة، "مجلة البحوث الفقهية والقانونية، العدد،43 جامعة الأزهر، مصر .

خامسا الرسائل الجامعية :

- رشا محمد صائم : تطبيقات الإدارة للذكاء الاصطناعي في اتخاذ القرارات الإدارية، مذكرة ماجستير قانون عام كلية الحقوق جامعة الشرق الأوسط، عمان ، الأردن،2022.

سادسا: المو اقع الالكترونية

- الموقع الالكتروني للأمم المتحدة https://www.un.org/ar/site تاريخ الدخول2025/10/29 التوقيت:15.00.

الإشكالات القانونية لاستخدامات الذكاء الاصطناعي: بين المسؤولية المدنية والجنائية والتحديات المستقبلية لحوكمة التكنولوجيا

Legal Issues in the Uses of Artificial Intelligence: Between Civil and Criminal Liability and the Future Challenges of Technology Governance)

عبد العزيز سلمى عشبة

جامعة محمد بوضياف - المسيلة، selma-achba.abdelaziz@univ-msila.dz

فريجة مروة

جامعة محمد بوضياف –المسيلة، marwa.fridja@univ-msila.dz

ملخص:

في ظل التحولات الرقمية المتسارعة، أضحى الذكاء الاصطناعي فاعلًا رئيسيًا في العديد من القطاعات الحيوية، الأمر الذي أسفر عن بروز قصور واضح في الأطر القانونية التقليدية وعجزها عن مواكبة هذا التطور التقني، سواء من حيث تحديد المسؤوليات القانونية عن الأضرار التي قد تنجم عن استخدام هذه الأنظمة، أو فيما يتعلق بوضع الضوابط الأخلاقية التي ينبغي أن تحكم توظيفها. وبناءً على ذلك، تهدف هذه الدراسة إلى تقويم مدى ملاءمة قواعد المسؤولية المدنية والجنائية القائمة لتنظيم استخدامات الذكاء الاصطناعي، خاصة في ظل ما تتمتع به هذه الأنظمة من استقلالية في اتخاذ القرارات، وما قد يترتب عن ذلك من أضرار مادية أو معنوية. وقد تم اعتماد المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية السارية، واستعراض أبرز الإشكاليات العملية التي تثيرها تطبيقات الذكاء الاصطناعي، مع الاستعانة بالنماذج التشريعية المقارنة بغرض تقييم مدى كفاءة المنظومة القانونية الحالية، والكشف عن مواضع القصور والخلل التي تعتريها.

الكلمات المفتاحية: الذكاء الاصطناعي؛ المسؤولية المدنية؛ المسؤولية الجنائية.

Abstract:

In light of the accelerating digital transformations, artificial intelligence has become a key player across various vital sectors. This development has revealed significant shortcomings in traditional legal frameworks, rendering them inadequate to keep pace with such technological advancements, whether in terms of determining legal liability for damages caused by these systems or establishing the ethical guidelines governing their use. Accordingly, this study aims to assess the extent to which existing rules of civil and criminal liability are suitable for regulating the uses of artificial intelligence, particularly given the autonomous nature of these systems and their ability to make decisions that may result in material or moral harm. The study adopts a descriptive-analytical methodology, through an in-depth analysis of prevailing legal texts and an examination of the practical issues raised by artificial intelligence applications, supplemented by a comparative review of selected legislative models, with the objective of evaluating the efficiency of the current legal system and identifying its inherent deficiencies and shortcomings

Keywords: *Artificial Intelligence; Civil Liability; Criminal Liability.*

مقدمة:

مع التطور الهائل في مجال الذكاء الاصطناعي أصبح لهذه التقنية تأثير متزايد على مختلف مجالات الحياة، حيث أصبحت تُستخدم في الصناعة، الطب، التعليم، الأمن، القضاء، وغيرها من القطاعات الحيوية، ومع تزايد ذلك برزت تحديات قانونية وأخلاقية جديدة تتطلب إعادة النظر في الإطار التشريعي التقليدي لضمان الاستخدام الآمن والمسؤول لهذه التقنيات، فمن جهة تفرض الأضرار الناجمة عن الذكاء الاصطناعي إشكالات قانونية تتعلق بالمسؤولية المدنية والجنائية، ومن جهة أخرى، أدى الانتشار الواسع لهذه التقنية إلى تحولات اجتماعية واقتصادية، مما يثير تساؤلات حول تأثيرها على سوق العمل، الخصوصية، والأمن السيبراني.

وانطلاقًا من هذه التطورات تبرز الإشكالية الرئيسية التالية: "الى أي مدى تستجيب القواعد القانونية التقليدية لتنظيم استخدام الذكاء الاصطناعي، خاصة فيما يتعلق بتحديد المسؤولية المدنية والجنائية عن الأضرار التي قد تنتج عنه؟".

لمعالجة هذه الإشكالية تم الاعتماد على المنهج الوصفي التحليلي، حيث تم استعراض وتحليل القواعد القانونية المتعلقة بالمسؤولية المدنية والجنائية، ومدى ملاءمتها لتنظيم استخدامات الذكاء الاصطناعي، بهدف تقديم رؤية متكاملة حول الحلول القانونية الممكنة لمواجهة التحديات التي يفرضها الذكاء الاصطناعي.

وللإجابة عن الإشكالية المطروحة، تم تقسيم الدراسة إلى مبحثين رئيسيين:

– **المبحث الأول**: مخاطر الذكاء الاصطناعي بين الأبعاد القانونية والأخلاقية، حيث سيتم تناول أبرز المخاطر التي يفرضها الذكاء الاصطناعي سواء على المستوى القانوني أو الاجتماعي، مع التركيز على التهديدات الأمنية، التأثير على سوق العمل، والاستخدامات العسكرية لهذه التقنية.

– **المبحث الثاني**: الإطار القانوني للمسؤولية المدنية والجنائية في مجال استخدامات الذكاء الاصطناعي، والذي سيتم فيه دراسة مدى إمكانية تطبيق قواعد المسؤولية التقليدية على الأضرار الناجمة عن الذكاء الاصطناعي سواء في إطار المسؤولية العقدية والتقصيرية، أو في نطاق المسؤولية الجنائية، مع استعراض الإشكالات المرتبطة بإسناد المسؤولية والعقوبات المترتبة على الجرائم التي قد ترتكبها الأنظمة الذكية.

– إن دراسة هذه الإشكالات القانونية باتت ضرورية في ظل التوسع المستمر لاستخدام الذكاء الاصطناعي مما يستوجب تطوير الأطر القانونية لمواكبة هذا التحول الرقمي وضمان تحقيق التوازن بين الابتكار والمسؤولية القانونية.

المبحث الأول:

مخاطر الذكاء الاصطناعي بين الأبعاد القانونية والأخلاقية

ان الاستخدام المتزايد لتطبيقات وتقنيات الذكاء الاصطناعي افضت الى بروز تهديدات رقمية وأمنية وأدت افي الوقت ذاته الى بروز العديد من التساؤلات حول مسؤولية الأطراف الفاعلة في حال وقوع أخطاء أو أضرار ناجمة عن هذه التقنية، لذا سنعالج في هذا المبحث المخاطر القانونية والاجتماعية الناجمة عن الذكاء الاصطناعي، إضافة إلى استعراض الإشكالات الأخلاقية والتشريعية التي تحيط باستخدامه.

المطلب الأول:

التداعيات القانونية والاجتماعية للذكاء الاصطناعي

مع الاستخدام المتزايد للذكاء الاصطناعي طفت الى السطح العديد من الإشكالات القانونية والاجتماعية المرتبطة باستخدامها، فمن جهة يفرض الذكاء الاصطناعي تحديات قانونية تتعلق بتحديد المسؤولية عن الأضرار الناجمة عنه، سواء في إطار العقود أو المسؤولية التقصيرية. ومن جهة أخرى، أثّر انتشار هذه

التقنية على سوق العمل، الأمن السيبراني وحتى على القيم الاجتماعية والأخلاقية،[1] وفي هذا السياق يتطلب استخدام الذكاء الاصطناعي تكييف القوانين الحالية أو استحداث تشريعات جديدة تضمن تحقيق التوازن بين الابتكار وحماية الحقوق الأساسية للأفراد والمجتمع.

الفرع الأول: المخاطر الأمنية والتهديدات السيبرانية

يمثل الذكاء الاصطناعي أداةً رئيسيةً في الجرائم الإلكترونية والهجمات السيبرانية حيث يتم استغلاله لتنفيذ عمليات احتيالية معقدة يصعب كشفها بسهولة، فقد أصبح بإمكان المتسللين استخدام تقنيات الذكاء الاصطناعي لاختراق الأنظمة، تنفيذ عمليات تزوير عبر الإنترنت، والتلاعب بالمعلومات، ومن بين أخطر التهديدات الأمنية الناجمة عن الذكاء الاصطناعي، تقنية التزييف العميق (Deepfake)،[2] التي تسمح بإنشاء مقاطع فيديو وصوت مزيفة يمكن استخدامها في التضليل الإعلامي والابتزاز.[3]

كما يمكن لأنظمة الذكاء الاصطناعي استغلال نقاط الضعف في الأنظمة الأمنية لاختراقها مما يهدد أمن البيانات الشخصية للمستخدمين ويعرضهم لسرقة

1- ايهاب خليفة، مجتمع ما بعد المعلومات- تأثير الثورة الصناعية الرابعة على الأمن القومي-، القاهرة، 2019، ص 73-74.

2- تشير هذه التقنية الى اعادة صياغة محتوى مزيف بطرق يصعب التشكيك في مصداقيتها، وللمزيد من التفاصيل أنظر: هواري صباح، الحياة الخاصة وتكنولوجيا التزييف العميق، مجلة العلوم القانونية والاجتماعية، المجلد9، العدد2، 2024.

3- أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبيرانية وسبل مواجهتها في القانون الدولي العام، مجلة القانون والشريعة، العدد35، مصر، 2020، ص410.

المعلومات والاحتيال الرقمي، إضافةً إلى ذلك هناك خطر "تسميم البيانات حيث يتم التلاعب بالبيانات المستخدمة في تدريب الأنظمة الذكية مما يؤدي إلى اتخاذ قرارات خاطئة أو غير متحيزة،[1] وقد يكون لذلك تأثير كارثي في المجالات الحساسة مثل القطاع المالي أو أنظمة العدالة الجنائية.

الفرع الثاني: التأثير على سوق العمل وارتفاع معدلات البطالة

يُعد الذكاء الاصطناعي أحد العوامل التي تؤدي إلى ارتفاع معدلات البطالة نتيجة استبدال العديد من الوظائف البشرية بالأنظمة الذكية والروبوتات. ومن هذه المجالات نذكر:[2]

- قطاع التصنيع والإنتاج حيث أصبحت الآلات الذكية قادرة على أداء المهام بكفاءة أعلى وبتكلفة أقل، مما دفع العديد من الشركات إلى تقليل الاعتماد على العمالة البشرية.

- قطاع النقل والمواصلات: فقد أدى تطوير السيارات ذاتية القيادة إلى تقليل الحاجة إلى السائقين، وهو ما يهدد مستقبل الوظائف في هذا المجال.

- القطاع المصرفي والمحاسبي: حيث أصبح الذكاء الاصطناعي قادرًا على تحليل البيانات المالية واتخاذ قرارات اقتصادية دقيقة، مما قلل الحاجة إلى المحللين الماليين التقليديين.

1- Wiliam welser, osonde osoba, the risks of artificial intelligence to security and the futur of work, RAND corporation, 2017, p-p12-22.
2- Stuart Russell And Peter Norvig, Artificial Intelligence: A Modern Approach,3rd edition, pearson editor,2020,p58.

هذه التحولات تفرض تحديات كبيرة على الحكومات التي أصبحت مطالبة بوضع سياسات جديدة مثل: إعادة تأهيل القوى العاملة من خلال برامج تدريبية متخصصة، وإصدار قوانين تحمي حقوق العمال الذين فقدوا وظائفهم بسبب التكنولوجيا الحديثة.

الفرع الثالث: الاستخدام العسكري

للذكاء الاصطناعي ومخاطر الأسلحة الذكية

في السنوات الأخيرة أصبح الذكاء الاصطناعي عنصرًا أساسيًا في تطوير الأسلحة الذكية والطائرات المسيرة مما يثير مخاوف متزايدة بشأن إمكانية استخدامه في الحروب المستقبلي، فقد تم تطوير طائرات مسيرة قتالية قادرة على تنفيذ عمليات هجومية دون تدخل بشري مباشر، مما يجعل من الصعب تحميل أي طرف مسؤولية قانونية عند وقوع أخطاء أو استهداف مدنيين.[1]

كما أن الروبوتات القتالية المستقلة أصبحت قادرة على تنفيذ عمليات عسكرية معقدة لكنها قد تتسبب في قرارات كارثية إذا لم يتم التحكم بها بشكل دقيق، في سياق متصل يزداد القلق أيضًا بشأن الحروب السيبرانية الذكية حيث يمكن استخدام الذكاء الاصطناعي في شن هجمات إلكترونية على البنية التحتية

1- Joseph s, Nye,Cyber power, Harvard Kennedy School: Belfer Center for Science and International Affairs, May 2010, pp.1-5

للدول الأخرى مما قد يؤدي إلى تعطيل الأنظمة الحيوية مثل شبكات الكهرباء والاتصالات.[1]

أمام هذه التحديات تبقى القوانين الدولية الخاصة باستخدام الذكاء الاصطناعي في المجال العسكري غير كافية، مما يزيد من احتمالية وقوع انتهاكات جسيمة لحقوق الإنسان نتيجة الاعتماد على هذه التكنولوجيا في العمليات القتالية.

المطلب الثاني: التحديات القانونية

والأخلاقية في تنظيم الذكاء الاصطناعي

مع التوسع المتسارع في استخدامات الذكاء الاصطناعي برزت تحديات قانونية وأخلاقية معقدة تتطلب تنظيمًا دقيقًا لضمان التوازن بين الابتكار وحماية الحقوق، فمن جهة يفرض الذكاء الاصطناعي إشكالات قانونية تتعلق بتحديد المسؤولية عن الأضرار التي قد تنجم عن قراراته المستقلة، ومن جهة أخرى تطرح أخلاقيات استخدام هذه التقنية تساؤلات حول مدى توافقها مع المبادئ الإنسانية مثل: العدالة، الخصوصية، وعدم التمييز، لذا أصبح من الضروري تطوير إطار قانوني وأخلاقي شامل ينظم عمل الذكاء الاصطناعي ويضمن استخدامه بشكل مسؤول وعادل.[2]

1 - ايهاب خليفة، مرجع سابق، ص 75.

2 - لغريبي آسيا، اللجنة الإقتصادية والعلمية، آفاق عالمية وتوجهات علمية، ازدهار البلدان وكرامة الإنسان، بيروت، 2019، ص14.

الفرع الأول: غياب الإطار القانوني الشامل

لتنظيم الذكاء الاصطناعي

على الرغم من التطور الكبير للذكاء الاصطناعي إلا أن معظم الدول لم تتمكن بعد من وضع إطار قانوني شامل ينظم استخدامه واحدة من أهم القضايا التي تطرحها هذه التقنية هي تحديد المسؤولية القانونية عن الأضرار التي قد تنتج عن قراراتها المستقلة، فهل تقع المسؤولية على عاتق المبرمج الذي صمم النظام، أم على الشركة المصنعة، أم على المستخدم النهائي؟ هذا السؤال يزداد تعقيدًا مع تزايد استقلالية الذكاء الاصطناعي وقدرته على اتخاذ قرارات دون تدخل بشري مباشر.[1]

بعض الاتجاهات القانونية الحديثة تقترح منح الذكاء الاصطناعي "شخصية قانونية"[2] شبيهة بالشخصية الاعتبارية التي تُمنح للشركات، بحيث يتحمل الذكاء الاصطناعي المسؤولية عن أفعاله، لكن هذه الفكرة لا تزال مثار جدل واسع ولم يتم تبنيها بشكل رسمي في أي نظام قانوني حتى الآن.

1- سهام دربال، إشكالية الإعتراف بالشخصية القانونية للروبوت الذكي، مجلة الإجتهاد القضائي، المجلد 14، العدد29، 2022، 456

2- الشخص المعنوي هو مجموع الأشخاص والأموال التي تهدف إلى تحقيق غرض معيّن، ويوجد نوعان: الشخص المعنوي العام مثل الدولة والولاية، والشخص المعنوي الخاص الذي يتكوّن من مجموعة من أفراد سواء لتحقيق غرض خاص بهم أو غرض يعود بالنفع العام، للمزيد من المعلومات انظر: محمدي فريدة، ص 105-107.

الفرع الثاني: أخلاقيات الذكاء الاصطناعي وتأثيره على القيم الإنسانية

أصبحت أخلاقيات الذكاء الاصطناعي قضية جوهرية في النقاشات حول مستقبل هذه التقنية، حيث تتزايد المخاوف بشأن التحيز في الخوارزميات، اذ تعتمد أنظمة الذكاء الاصطناعي على البيانات التي يتم تدريبها عليها وإذا كانت هذه البيانات غير متوازنة أو تعكس تحيزات مجتمعية، فإن النظام سيكرر هذه التحيزات في قراراته مما قد يؤدي إلى ممارسات غير عادلة في مجالات التوظيف، العدالة، والحصول على الخدمات العامة،[1] وأبرز مثال على ذلك ما أظهرته الدراسات العلمية الأخيرة بخصوص نظام campas المعتمد في الولايات المتحدة الامريكية لتقييم خطر اعادة الاجرام للمتهمين، حيث أكدت أنه يحتوي على تحيزات عنصرية خطيرة اذ يميل الى تصنيف المتهمين ذوي البشرة السوداء على انهم اكثر قابلية لاعادة السلوك الاجرامي من ذوي البشرة البيضاء.

بالإضافة إلى ذلك يُستخدم الذكاء الاصطناعي بشكل متزايد في المراقبة الجماعية مما يثير تساؤلات حول مدى التزام الدول بحماية الخصوصية وحقوق الأفراد، ومع قدرة الذكاء الاصطناعي على تحليل كميات هائلة من البيانات أصبح من السهل تتبع أنشطة الأفراد دون علمهم مما يشكل تهديدًا خطيرًا للحريات الشخصية.

الفرع الثالث: الحاجة إلى إطار تنظيمي شامل

لضمان الاستخدام المسؤول للذكاء الاصطناعي يجب تطوير قوانين تضمن الشفافية والمساءلة بحيث يكون المستخدمون على دراية بكيفية عمل الأنظمة

1- وسيلة سعود، الذكاء الإصطناعي وتحديات الممارسات الأخلاقية، مجلة نماء للاقتصاد والتجارة، المجلد7، العدد2، جامعة البويرة، 2023، ص 11.

الذكية واتخاذها للقرارات، كما يجب فرض قواعد صارمة لحماية البيانات الشخصية ومنع إساءة استخدامها، بالإضافة إلى وضع آليات تضمن مساءلة الشركات والمطورين عن أي أخطاء أو انتهاكات قد تنجم عن استخدام الذكاء الاصطناعي.[1]

علاوةً على ذلك ينبغي أن تلتزم هذه القوانين بالمعايير الدولية لحقوق الإنسان، بحيث يتم دمج القيم الأخلاقية في تصميم الأنظمة الذكية، لمنع استخدامها بطرق قد تنتهك الحقوق الأساسية للأفراد.

في ختام هذا المبحث فإن الذكاء الاصطناعي يمثل تقدمًا تكنولوجيًا غير مسبوق لكنه في الوقت نفسه يفرض تحديات قانونية وأخلاقية معقدة تتطلب استجابة تنظيمية سريعة، فبينما يوفر الذكاء الاصطناعي إمكانيات كبيرة لتحسين الحياة البشرية، فإنه قد يُستخدم أيضًا بطرق خطرة إذا لم يتم تنظيمه بشكل مناسب، وعليه فإن وضع أطر قانونية واضحة تضمن الاستخدام المسؤول لهذه التقنية هو أمر بالغ الأهمية لضمان الاستفادة القصوى من الذكاء الاصطناعي دون أن يصبح مصدرًا للتهديد أو الاستغلال من جهة، و لتحقيق التوازن بين الابتكار والمسؤولية القانونية ومنه ضمان مستقبل آمن وعادل في عصر الذكاء الاصطناعي.

1- أنظر دبي الذكية، (بلا تاريخ)، مبادئ وإرشادات أخلاقيات الذكاء الإصطناعي، مجلة الدراسات الكمية (01)، ص08-09.

المبحث الثاني:

الإطار القانوني للمسؤولية المدنية والجنائية

في مجال استخدامات الذكاء الاصطناعي

أدى ازدهار بعض القطاعات التي تعتمد على الذكاء الاصطناعي في نشاطها إلى زيادة الاعتماد على هذه التقنية ،والجزائر باعتبارها جزءًا من المجتمع الدولي تسعى إلى مواكبة هذا التطور لاسيما في المجال التكنولوجي، مما يستدعي تحديث منظومتها القانونية بما يتماشى مع هذه المستجدات العلمية والتقنية، وعلى الرغم من أن قضايا الأنظمة الذكية لم تُطرح بعد أمام القضاء الجزائري، إلا أن التطورات المتسارعة تشير إلى ضرورة الاستعداد لموجة جديدة من القضايا خاصة تلك المتعلقة بالأضرار الناجمة عن الذكاء الاصطناعي والتي قد تصل إلى حد الجريمة[1].

ونظرًا لأن أنظمة الذكاء الاصطناعي تعتمد على برمجيات وخوارزميات قادرة على محاكاة السلوك البشري واتخاذ القرارات بشكل مستقل، فإن استخدامها الواسع يفرض تحديات قانونية عديدة أهمها تحديد المسؤولية عن الأضرار التي قد تسببها هذه الأنظمة في ظل القواعد التقليدية للمسؤولية المدنية والجنائية، ومن هنا يبرز التساؤل حول مدى استجابة الأنظمة القانونية التقليدية لمعالجة المسؤولية المدنية والجنائية الناجمة عن استخدام تقنيات الذكاء الاصطناعي.

1- بلعباس أمال، مدى ملائمة قواعد المسؤولية للتعويض عن أضرار النظم الذكية، مجلة البحوث والعلوم القانونية والإقتصادية، المجلد06، العدد01، المركز الجامعي مغنية ،2023، ص458

المطلب الأول: المسؤولية المدنية الناتجة

عن استخدام الذكاء الاصطناعي

ترتبط المسؤولية المدنية ارتباطًا وثيقًا بحماية الحقوق في المعاملات بين الأفراد، حيث تقوم على مبدأ التعويض عن الضرر الناجم عن الخطأ،[1] غير أن التطورات التكنولوجية الحديثة بما في ذلك أنظمة الذكاء الاصطناعي تفرض تحديات جديدة على هذا المفهوم التقليدي للمسؤولية، وقد انقسم الفقه القانوني إلى اتجاهين؛ الأول يرى أن القواعد الحالية للمسؤولية المدنية، سواء التعاقدية أو التقصيرية، كافية لمعالجة الأضرار الناجمة عن الذكاء الاصطناعي، بينما يرى الاتجاه الثاني أن هذه القواعد لم تعد كافية، مما يستدعي تطوير إطار قانوني جديد يأخذ في الاعتبار المخاطر المرتبطة بهذه التقنية.

الفرع الأول: المسؤولية العقدية عن أنظمة الذكاء الاصطناعي

تستند المسؤولية العقدية إلى قاعدة "العقد شريعة المتعاقدين"، والتي تلزم أطراف العقد بتنفيذ التزاماتهم كما تم الاتفاق عليها، وعليه فإن أي إخلال بهذه الالتزامات قد يؤدي إلى مساءلة الطرف المخالف وإلزامه بتعويض المتضرر غير أن تطبيق هذا المبدأ على أنظمة الذكاء الاصطناعي يثير العديد من الإشكالات خاصة عندما يكون الذكاء الاصطناعي جزءًا من العقد، وهنا يمكن التمييز بين حالتين؛

1- محمد عبد الظاهر حسين، خطأ المضرور وأثره على المسؤولية، الطبعة الأولى، دار المعارف،القاهرة، 2014، ص13.

الأولى عندما يكون الذكاء الاصطناعي محل العقد، والثانية عندما يكون طرفًا في العقد[1].

أولًا: الذكاء الاصطناعي كمحل للعقد

قد يكون الذكاء الاصطناعي محلًا لعقود مثل البيع أو الإيجار حيث يتم الاتفاق على توفير تقنية ذكاء اصطناعي لاستخدامها في أغراض معينة، في هذه الحالة يكون البائع أو المؤجر مسؤولًا عن أي خلل أو عيب في النظام وفقًا لقواعد المسؤولية العقدية- على سبيل المثال- إذا اشترى شخص روبوتًا طبيًا وظهر فيه عيب يمنعه من أداء وظيفته فإن البائع يكون مسؤولًا بموجب ضمان العيوب الخفية وفقًا لما تنص عليه القوانين المدنية مثل القانون المدني الجزائري وقانون حماية المستهلك رقم03-09. [2]

ثانيًا: الذكاء الاصطناعي كطرف في العقد

مع تطور تقنيات الذكاء الاصطناعي أصبح من الممكن أن يتولى الذكاء الاصطناعي إبرام العقود والتفاوض بشأنها .وهنا تطرح إشكالية تحديد المسؤولية في حال أخل النظام الذكي بالتزاماته، وقد تبنى البرلمان الأوروبي مفهوم "النائب الإنساني

1- شريف طباخ، التعويض عن الإخلال بالعقد - التطبيق العملي للمسؤولية المدنية في ضوء الفقه والقضاء-، المركز القومي للإصدارات القانونية، القاهرة، 2005، ص 213

2- محمد صبري السعدي، الواضح في شرح القانون المدني النظرية العامة للإلتزامات، مصادر الإلتزام العقد والإرادة المنفردة، دار الهدى، الجزائر، 2021، ص204.

عن الروبوت"، [1]وهو شخص يُحمَّل قانونيًا مسؤولية تصرفات الذكاء الاصطناعي سواء كان المالك، المستخدم، أو المصنع.

الفرع الثاني:

المسؤولية التقصيرية عن أضرار أنظمة الذكاء الاصطناعي

تنشأ المسؤولية التقصيرية عند حدوث ضرر للغير دون وجود عقد مسبق، حيث يتحمل الفاعل مسؤولية تعويض الضرر، إلا أن تطبيق هذه القواعد على الذكاء الاصطناعي يثير صعوبات نظرًا لعدم إمكانية تحميل الروبوت أو النظام الذكي المسؤولية المباشرة نظرًا لغياب الإرادة البشرية لديه،[2] وبما أن المسؤولية التقصيرية تشمل مسؤولية الشخص عن أفعاله الشخصية وأفعال الغير والأشياء التي تحت حراسته فإن التساؤل المطروح هو :هل يمكن اعتبار الذكاء الاصطناعي "شيئًا" يخضع لنظرية الحراسة؟ في ظل استقلالية هذه الأنظمة قد يكون من الصعب تحديد الحارس الفعلي لها، مما يتطلب إعادة النظر في القواعد التقليدية للمسؤولية التقصيرية.

1- نبيلة علي خميس، محمد بن خرور المهيري، المسؤولية المدنية عن أضرار الإنسان الآلي (دراسة تحليلية)، رسالة ماجستير، جامعة الإمارات العربية،2020، ص36

2- أحمد حسن محمد علي، المسؤولية المدنية عن أضرار الروبوتات بين القواعد التقليدية والاتجاه الحديث، مجلة كلية الشريعة والقانون، العدد23، دقهلية، 2021، ص 306.

المطلب الثاني:

المسؤولية الجنائية عن استخدام الذكاء الاصطناعي

تزايدت المخاوف بشأن إمكانية ارتكاب جرائم بواسطة الأنظمة الذكية مما يستدعي بحث إمكانية مساءلتها جنائيًا، وتنشأ المسؤولية الجنائية عند ثبوت ارتكاب فعل مجرَّم بموجب القانون وتوافر العلاقة بين الجاني والجريمة، غير أن الذكاء الاصطناعي بوصفه نظامًا غير بشري يفتقر إلى الإرادة والتمييز مما يثير إشكالية تطبيق قواعد المسؤولية الجنائية عليه.

الفرع الأول: ماهية المسؤولية الجنائية.

تُعرَّف المسؤولية الجنائية بأنها: "تحمل الشخص تبعات أفعاله الإجرامية، وإخضاعه للجزاء الجنائي المقرر قانونًيا"،[1] وتقوم المسؤولية الجنائية على ثلاثة أركان أساسية[2]:

- الركن المادي: يتمثل في الفعل الإجرامي الذي قام به الجاني، والذي قد يكون سلوكًا إيجابيًا مثل: توجيه نظام ذكاء اصطناعي لتنفيذ هجوم إلكتروني، أو سلوكًا سلبيًا: مثل امتناع روبوت طبي عن تقديم المساعدة لمريض.

- الركن المعنوي: يتطلب إثبات وجود قصد جنائي لدى الفاعل، وهو ما يصعب تطبيقه على الذكاء الاصطناعي نظرًا لعدم امتلاكه إرادة مستقلة.

1- برمضان طيب، المسؤولية الجنائية في الفقه الإسلامي والقانون الجزائري، مجلة المعيار، العدد1، جامعة الجزائر1، 2021، ص89.

2- المرجع نفسه.

– العلاقة السببية :يجب أن يكون هناك رابط مباشر بين الفعل الإجرامي والنتيجة الضارة التي ترتبت عليه.

الفرع الثاني: تأثير الجرائم الناجمة عن الذكاء الاصطناعي على المسؤولية القانونية

ساهمت عدة حوادث مرتبطة باستخدام الذكاء الاصطناعي في إثارة إشكاليات قانونية حول تحديد المسؤولية المدنية والجنائية عند تسبب الأنظمة الذكية في أضرار جسيمة. ومن أبرز هذه الحوادث:

– حادثة مقتل موظف ياباني عام 1981 بواسطة روبوت صناعي، والتي طرحت لأول مرة إشكالية مسؤولية المصنعين والمبرمجين عن أخطاء الروبوتات مما ساهم في تطوير معايير السلامة الصناعي.[1].

– حادثة مقتل روبرت ويليامز عام 1979 في مصنع فورد، حيث أدى خلل في الذراع الروبوتية إلى وفاته مما دفع القضاء إلى تحميل الشركة المصنعة المسؤولية وتعويض عائلته، وأسهم ذلك في فرض تشديدات قانونية على أنظمة الأمان في الروبوتات الصناعية[2].

1- ممدوح حسين مانع العدوان، المسؤولية الجنائية عن أفعال كيانات الذكاء الإصطناعي غير المشروعة، دراسات علوم الشريعة والقانون، العدد4، الجامعة الأردنية، 2021، ص 153.

2- المرجع نفسه، ص154.

– قضية ميكا جافير جونسون عام 2016، حيث استخدمت شرطة دالاس روبوتًا مسلحًا بالمتفجرات للقضاء على مشتبه به مما أثار جدلًا واسعًا حول المسؤولية الجنائية عند استخدام الذكاء الاصطناعي في إنفاذ القانون، وأبرز الحاجة إلى إطار قانوني ينظم استخدام الروبوتات في العمليات الأمنية والعسكرية[1].

أدت هذه الحوادث إلى مراجعة القوانين التقليدية للمسؤولية، حيث أصبح من الضروري إعادة تعريف المسؤولية المدنية لتشمل مخاطر الأنظمة الذكية، ووضع معايير واضحة لتحميل المصنعين والمستخدمين والمبرمجين المسؤولية عن أضرار الذكاء الاصطناعي، كما دفعت إلى نقاشات حول ضرورة إيجاد إطار قانوني جديد لمساءلة الذكاء الاصطناعي في الجرائم الجنائية، خاصة في ظل تطور قدراته الاستقلالية واتخاذه للقرارات دون تدخل بشري مباشر.

الفرع الثالث: العقوبات القانونية الناجمة عن إساءة استخدام الذكاء الاصطناعي

تختلف العقوبات المفروضة على الجرائم المرتبطة باستخدام الذكاء الاصطناعي حسب الجهة المسؤولة عن الضرر سواء كان المصنع، المستخدم، أو أي طرف آخر متورط، ومع تزايد استقلالية هذه الأنظمة يثار التساؤل حول مدى إمكانية تحميل الذكاء الاصطناعي نفسه المسؤولية الجنائية.

1- محمد خطاب، أبرز الحالات التي قتلت على يد الروبوتات في التاريخ،آخر تحديث 2020/04/01، تاريخ الدخول 2025/04/15، على الساعة 11:57. الرابط: https:www.mp/p7UGLA-2tbd

– مسؤولية المصنع والمطور عن أضرار الذكاء الاصطناعي: يُعتبر المصنع أو المطور الطرف الأساسي المسؤول عن تصميم وبرمجة أنظمة الذكاء الاصطناعي مما يجعله ملزمًا قانونيًا بضمان امتثال هذه الأنظمة لمعايير الأمان والسلامة، وفي حال تسبب خلل في التصميم أو البرمجة في أضرار جسيمة فإنه قد يواجه[1]:

- غرامات مالية بسبب انتهاك معايير السلامة.
- إيقاف النشاط أو سحب التراخيص في حال تكرار الانتهاكات.
- مساءلة جنائية في حال تسبب الإهمال التقني في وقوع وفيات أو أضرار خطيرة.

– مسؤولية المستخدم والمالك عن إساءة استخدام الذكاء الاصطناعي: يمكن أن يكون المستخدم أو المالك مسؤولًا جنائيًا عند استغلال الذكاء الاصطناعي في أعمال غير مشروعة مثل الجرائم الإلكترونية، التجسس، أو تنفيذ هجمات إلكترونية موجهة. وقد تشمل العقوبات في هذه الحالة[2]:

- السجن في حال ثبوت تورطه في جرائم باستخدام الذكاء الاصطناعي.
- منع أو تقييد استخدامه للأنظمة الذكية في المستقبل.

1- عبد الوهاب مريم، لبيض هند، المسؤولية الجنائية عن جرائم الذكاء الإصطناعي،مجلة القانون والعلوم البيئية، المجلد 02، العدد 02، 2023، ص 690.

2- سارة أمجد عبد الهادي اطميزي، الذكاء الإصطناعي في ظل القانون الجزائي، رسالة ماجستير، جامعة الخليل، فلسطين، 2022، ص04.

- تحمل المسؤولية المشتركة مع أطراف أخرى إذا كان الفعل الإجرامي تم بالتعاون مع جهة خارجية.

– مدى إمكانية تحميل الذكاء الاصطناعي نفسه المسؤولية الجنائية: نظرًا لأن القانون الجنائي يعتمد على مبدأ الإدراك والإرادة، فإن الذكاء الاصطناعي لا يمكن تحميله المسؤولية بشكل مباشر، ومع ذلك هناك توجهات قانونية تدعو إلى إنشاء مفهوم جديد للمسؤولية الافتراضية، حيث يتم التعامل مع الأنظمة الذكية ككيانات قانونية مستقلة يمكن تحميلها المسؤولية وفقًا لإطار قانوني مستقبلي[1].

وفي ختام هذا المبحث فإن الذكاء الاصطناعي يمثل تحديًا قانونيًا غير مسبوق، إذ إن تحديد المسؤولية المدنية والجنائية عن أفعاله لا يزال محل جدل واسع، ويستلزم ذلك تطوير إطار قانوني جديد يأخذ في الاعتبار استقلالية الأنظمة الذكية مع ضمان عدم استخدامها بطرق تعرض الأفراد أو المجتمع للخطر.

خاتمة:

يعد الذكاء الاصطناعي أحد أهم الابتكارات التكنولوجية في العصر الحديث، حيث أصبح يُستخدم على نطاق واسع في مختلف المجالات مما ساهم في تحسين الإنتاجية وتطوير الخدمات، إلا أن هذا التطور التقني السريع ترافقه تحديات قانونية واجتماعية تستدعي إيجاد حلول تنظيمية فعالة لضمان الاستخدام الآمن والمسؤول لهذه التقنية.

1- المرجع نفسه، ص46.

ومن خلال الدراسة تبيّن أن الذكاء الاصطناعي يفرض إشكالات قانونية معقدة سواء من حيث تحديد المسؤولية المدنية والجنائية عن الأضرار التي قد تنتج عنه، أو من حيث تأثيره على سوق العمل والأمن السيبراني الأمر الذي يستوجب إعادة النظر في القواعد القانونية التقليدية واستحداث تشريعات تتناسب مع طبيعة هذه التكنولوجيا الحديثة.

ومن خلال هذه الدراسة توصلنا إلى جملة من النتائج:

- عدم ملاءمة القواعد التقليدية للمسؤولية المدنية لمعالجة الأضرار الناجمة عن الذكاء الاصطناعي، حيث تعتمد هذه القواعد على ضرورة وجود خطأ بشري، في حين أن الأنظمة الذكية تعمل باستقلالية مما يجعل من الصعب تحديد المسؤول عنها.

- قصور القواعد الجنائية الحالية في مواجهة الجرائم التي قد ترتكبها أنظمة الذكاء الاصطناعي نظرًا لعدم توفر الأهلية القانونية لهذه الأنظمة، مما يطرح إشكالية إسناد المسؤولية الجنائية إلى المصنع أو المستخدم أو أي طرف آخر.

- الذكاء الاصطناعي يشكل تهديدًا لسوق العمل حيث أدى إلى فقدان العديد من الوظائف التقليدية خاصة في القطاعات الصناعية والخدمية، مما يستدعي وضع سياسات جديدة لإعادة تأهيل العمالة المتأثرة.

- استغلال الذكاء الاصطناعي في الجرائم الإلكترونية مثل: التزييف العميق (Deepfake)، والقرصنة الذكية، مما يتطلب تعزيز القوانين الخاصة بالأمن السيبراني لحماية الأفراد والمؤسسات.

- تزايد استخدام الذكاء الاصطناعي في المجال العسكري يثير مخاوف قانونية وأخلاقية، حيث أصبحت الطائرات المسيّرة والأسلحة الذكية تشكل تهديدًا خطيرًا في حالة غياب ضوابط قانونية واضحة تنظم استخدامها.

- عدم وجود إطار قانوني دولي موحد لتنظيم استخدام الذكاء الاصطناعي مما يؤدي إلى اختلاف التشريعات بين الدول، ويؤثر على إمكانية محاسبة الأطراف المسؤولة عن الأضرار الناجمة عن هذه التقنية.

- ضرورة تطوير مفهوم "المسؤولية الافتراضية "كبديل عن المفاهيم التقليدية للمسؤولية، بحيث يتم تحميل الذكاء الاصطناعي نفسه المسؤولية القانونية وفق نموذج قانوني جديد.

وانطلاقا من هذه النتائج نقدم مجموعة من التوصيات:

- تعديل القوانين المدنية والجنائية بما يتناسب مع التطورات التكنولوجية، وذلك من خلال إدراج أحكام خاصة تتعلق بالمسؤولية القانونية عن الأضرار الناجمة عن أنظمة الذكاء الاصطناعي.

- استحداث تشريعات جديدة تتعلق بمساءلة الذكاء الاصطناعي بحيث يتم تحديد الجهة المسؤولة عن أخطاء هذه الأنظمة، سواء المصنع، المبرمج، أو المستخدم النهائي، وفقًا لنوع الخطأ المرتكب.

- تعزيز الأمن السيبراني من خلال سن قوانين صارمة لمكافحة الجرائم الإلكترونية التي تعتمد على الذكاء الاصطناعي مع فرض عقوبات رادعة على الجهات التي تستغل هذه التقنية بطرق غير قانونية.

- إدراج معايير أخلاقية في تصميم أنظمة الذكاء الاصطناعي بحيث يتم تقليل مخاطر التحيّز البرمجي وحماية حقوق الأفراد من القرارات غير العادلة التي قد تتخذها هذه الأنظمة.

- إطلاق برامج تدريبية لإعادة تأهيل العمال المتأثرين بالأتمتة من خلال توفير فرص تعليمية تمكنهم من اكتساب مهارات تتماشى مع التحولات التكنولوجية الجديدة.

- تطوير اتفاقيات دولية موحدة لتنظيم استخدام الذكاء الاصطناعي بحيث يتم وضع إطار قانوني عالمي يضمن الاستخدام المسؤول لهذه التقنية، خاصة في المجالات العسكرية والحكومية.

- تشجيع البحث العلمي في مجال الذكاء الاصطناعي القانوني من خلال دعم الدراسات التي تهدف إلى وضع حلول قانونية تتناسب مع تطور هذه التكنولوجيا.

- تعزيز الشفافية والمساءلة في تصميم أنظمة الذكاء الاصطناعي بحيث تكون هذه الأنظمة قابلة للفحص والمراجعة من قبل الهيئات المختصة لضمان عدم استخدامها في انتهاك حقوق الأفراد والمجتمعات.

- فرض التزامات قانونية على الشركات المطوّرة لأنظمة الذكاء الاصطناعي لضمان التزامها بالمعايير الأخلاقية والتشريعات المحلية والدولية عند تطوير واستخدام هذه الأنظمة.

- استحداث هيئات رقابية متخصصة في متابعة تطورات الذكاء الاصطناعي بحيث تتولى مراقبة مدى التزام المؤسسات باستخدام هذه التقنية بطريقة مسؤولة وتقديم توصيات بشأن تطوير القوانين المتعلقة بها.

قائمة المصادر و المراجع:

أولاً: المراجع باللغة العربية

أ- الكتب

- إيهاب خليفة، *مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*، القاهرة؛ 2019.
- محمد عبد الظاهر حسين، *خطأ المضرور وآثره على المسؤولية*، الطبعة الأولى، دار المعارف، القاهرة؛ 2014.
- شريف طباخ، *التعويض عن الإخلال بالعقد - التطبيق العملي للمسؤولية المدنية في ضوء الفقه والقضاء-*، المركز القومي للإصدارات القانونية، القاهرة؛ 2005.
- محمد صبري السعدي، *الواضح في شرح القانون المدني النظرية العامة للإلتزامات، مصادر الإلتزام العقد والإرادة المنفردة*، دار الهدى، الجزائر؛ 2021.

ب- الرسائل الجامعية

- نبيلة علي خميس، محمد بن خرور المهيري، *المسؤولية المدنية عن أضرار الإنسان الآلي (دراسة تحليلية)*، رسالة ماجستير، جامعة الإمارات العربية المتحدة؛ 2020.
- سارة أمجد عبد الهادي اطميزي، *الذكاء الاصطناعي في ظل القانون الجزائي*، رسالة ماجستير، جامعة الخليل، فلسطين؛ 2022.

ج- مقالات الصحف والمجلات العلمية

- هواري صباح، *الحياة الخاصة وتكنولوجيا التزييف العميق*، مجلة العلوم القانونية والاجتماعية، المجلد 9، العدد 2؛ 2024.

- أميرة عبد العظيم محمد عبد الجواد، *المخاطر السيبيرانية وسبل مواجهتها في القانون الدولي العام*، مجلة القانون والشريعة، العدد 35، مصر؛ 2020.

- لغريبي آسيا، *اللجنة الاقتصادية والعلمية، آفاق عالمية وتوجهات علمية، ازدهار البلدان وكرامة الإنسان*، بيروت؛ 2019.

- سهام دربال، *إشكالية الاعتراف بالشخصية القانونية للروبوت الذكي*، مجلة الاجتهاد القضائي، المجلد 14، العدد 29؛ 2022.

- وسيلة سعود، *الذكاء الاصطناعي وتحديات الممارسات الأخلاقية*، مجلة نماء للاقتصاد والتجارة، المجلد 7، العدد 2، جامعة البويرة؛ 2023.

- بلعباس أمال، *مدى ملاءمة قواعد المسؤولية للتعويض عن أضرار النظم الذكية*، مجلة البحوث والعلوم القانونية والاقتصادية، المجلد 6، العدد 1، المركز الجامعي مغنية؛ 2023.

- برمضان طيب، *المسؤولية الجنائية في الفقه الإسلامي والقانون الجزائري*، مجلة المعيار، العدد 1، جامعة الجزائر 1؛ 2021.

- ممدوح حسين مانع العدوان، *المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة*، دراسات علوم الشريعة والقانون، العدد 4، الجامعة الأردنية؛ 2021.

- عبد الوهاب مريم، لبيض هند، *المسؤولية الجنائية عن جرائم الذكاء الاصطناعي*، مجلة القانون والعلوم البيئية، المجلد 2، العدد 2؛ 2023.

د- النصوص القانونية أو الإلكترونية

- دبي الذكية، *مبادئ وإرشادات أخلاقيات الذكاء الاصطناعي*، مجلة الدراسات الكمية (01)، دون تاريخ، الرابط http://www.smartdubai.ae :تمت الاستشارة في 2025/04/15.)

- محمد خطاب، *أبرز الحالات التي قتلت على يد الروبوتات في التاريخ*، آخر تحديث 2020/04/01، تاريخ الدخول 2025/04/15، الرابط : https://www.mp/p7UGLA-2tbd.

ثانياً: المراجع باللغة الأجنبية

- William Welser and Osonde Osoba, *The Risks of Artificial Intelligence to Security and the Future of Work*, RAND Corporation; 2017.
- Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd edition, Pearson; 2020.
- Joseph S. Nye, *Cyber Power*, Harvard Kennedy School: Belfer Center for Science and International Affairs; May 2010.

مخاطر الذكاء الاصطناعي
Risks of artificial intelligence

د. محمد الأمين نويري
جامعة الشاذلي بن جديد- الطارف m.nouiri@univ-eltarf.dz
د. رشا مقدم
جامعة الشاذلي بن جديد- الطارف r.mokaddem@univ-eltarf.dz

الملخص:
إن الذكاء الاصطناعي يمثل ثورة تقنية كبرى، قادرة على إحداث تحولات عميقة في مختلف مجالات الحياة، بما في ذلك الاقتصاد والصناعة والتعليم والصحة والخدمات الحكومية، ومع ذلك فإن هذه القوة الكبيرة تنطوي على مخاطر قد تهدد الأمن الفردي والمجتمعي على حد سواء. فمن الجانب الأمني، يمكن استغلال الذكاء الاصطناعي في تنفيذ هجمات سيبرانية معقدة، وسرقة البيانات، وممارسة التجسس على الأفراد والدول، ما يضع الحكومات والمؤسسات أمام تحديات غير مسبوقة. كما أن الاستخدام غير المنضبط لهذه التكنولوجيا قد يؤدي إلى انتهاك الخصوصية الفردية، نظرًا لاعتماد العديد من الأنظمة على جمع وتحليل كميات ضخمة من البيانات الشخصية، أحيانًا دون علم أو موافقة أصحابها.
الكلمات المفتاحية: الذكاء الاصطناعي، ثورة تقنية، الجانب الأمني، هجمات سيبرانية، الخصوصية الفردية.

Abstract :

Artificial intelligence represents a major technological revolution, capable of bringing about profound transformations in various areas of life, including the economy, industry, education, health, and government services. However, this great power carries risks that may threaten both individual and societal security. On the security side, artificial intelligence can be exploited to carry out complex cyber attacks, steal data, and spy on individuals and countries, putting governments and institutions facing unprecedented challenges. Uncontrolled use of this technology may also lead to a violation of individual privacy, since many systems rely on collecting and analyzing huge amounts of personal data, sometimes without the knowledge or consent of their owners.

Keywords: *artificial intelligence, technological revolution, security aspect, cyber attacks, individual privacy.*

مقدمة:

يُعَدّ الذكاء الاصطناعي أحد أهم المحركات الرئيسة للنمو والابتكار في مختلف القطاعات الاقتصادية والعلمية، إذ يشهد العالم اليوم ثورة تكنولوجية غير مسبوقة في هذا المجال انعكست آثارها على شتى مناحي الحياة. ويُنظر إلى الذكاء الاصطناعي بوصفه أحد أبرز إنجازات الثورة الصناعية الحديثة، لما أحدثه من تحولات جوهرية في بنية المعرفة والتطبيقات العملية، حيث مثّل نقلة نوعية تمكّنت بواسطتها الحواسيب والأنظمة الذكية من محاكاة القدرات الذهنية للإنسان وتوظيفها في مهام معقدة بدقة وكفاءة عالية.

يمتاز الذكاء الاصطناعي بمجموعة من الخصائص التي تتقاطع مع برامج الحاسوب، وتُمكّنه هذه السمات من محاكاة العمليات المعرفية وأنماط السلوك البشري. وقد شكّل الذكاء الاصطناعي أداة محورية ساعدت من خلالها ثورة المعلومات والاتصالات على انتقال المجتمعات من النمط التقليدي إلى مجتمع المعرفة والمعلومات. غير أنّ تعزيز الاستثمار في المعلومات يُعدّ من أبرز التحديات

أمام تعميم المعرفة، إذ يمثل السبيل الأساس لاكتشاف معارف جديدة وتطوير حلول مبتكرة.

تبعاً لذلك نطرح الاشكال الآتي ما هي الإشكاليات والتحديات التي تواجه استخدام وتطوير تقنيات الذكاء الاصطناعي؟

المبحث الأول:

مفهوم الذكاء الاصطناعي

شهدت السنوات الأخيرة اهتماماً متزايداً بمفهوم الذكاء الاصطناعي على مستوى دول العالم، ما دفع العديد من المنظمات إلى اعتباره خياراً استراتيجياً لمواكبة التطور التكنولوجي السريع. وقد ساهمت هذه التكنولوجيا في إحداث تحولات إيجابية داخل المجتمع، حيث توفر وسيلة فعّالة لتخفيف الجهد البشري وإنجاز المهام بشكل آلي دون الحاجة إلى التدخل اليدوي. كما عملت شركات متخصصة وخبراء في المجال على تطوير هذه التقنية، الأمر الذي يبرز أهمية التعمق في دراسة ماهية الذكاء الاصطناعي وأبعاده، وهو ما سيتناول هذا المبحث.

المطلب الأول:

نشأة الذكاء الاصطناعي

يمتد الذكاء الاصطناعي بجذوره إلى الرياضيات من خلال ثلاث مجالات هي الحوسبة Computation، المنطق Logic، والنظرية الاحتمالية Probability والجبر الذي تأسس على يد العالم العربي "الخوارزمي " [1].

[1]- ياسين سعد غالب، تحليل وتصميم نظم المعلومات، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، الأردن،2011، ص19.

وقد ساعد العالم تورينج في صنع أحد أول أجهزة الكمبيوتر التقليدية في الحرب العالمية الثانية وأسس نظرية الحوسبة التقليدية عام 1936، كما تمكن وخلال الحرب العالمية الثانية من فك شفرة "إنجما" التي استخدمتها القوات الألمانية لإرسال الرسائل بشكل آمن.

وتعود فكرة الذكاء الاصطناعي لعام 1956 على يد العالم " جون ماركثي"، حيث تركزت أبحاث العلماء في ذلك الوقت على كيفية منح الآلة صفة الذكاء البشري، وكانت أول محاولة لبناء آلة ذكرة يمكنها تقليد (محاكاة) العقل البشري للعالم فرانك روز عام 1957، عندما قام بوضع نموذج مبسطة للشبكة العصبية يشبه إلى حد كبير الخلايا العصبية في الدماغ البشري[1].

رغم أن الذكاء الاصطناعي أضحى مرتبطاً بميادين علم الحوسبة والخوازماريات، إلا أن بداياته جاءت على يد مختصي الأعصاب وعلم النفس، وينطلق الذكاء الاصطناعي من مبدأ معالجة المعلومات مهما كانت طبيعتها وحجمها بطريقة آلية أو نصف آلية وبشكل مناسب ومتوافق مع هدف معين، ولقد ورد مفهوم الذكاء الاصطناعي منذ أوائل سنوات 1950، وهو تيار علمي تقني يضم الطرق والنظريات والتقنيات التي تهدف إلى إنشاء آلات قادرة على محاكاة الذكاء[2].

كما تم صياغة مصطلح الذكاء الاصطناعي في مؤتمر علمي لجامعة دارتموث في مدينة هانوفر الأمريكية من قبل البروفيسور وعالم الكمبيوتر الأمريكي جون مكارثي.

[1] - محمد مجدي صلاح طه، منهاج البحث التربوي، سلسلة العلوم التربوية الإسلامية، دار الفكر العربي للطباعة والنشر، القاهرة، مصر، 2019، ص05.

[2] - بكر عبد الجواد السيد، طه محمود إبراهيم عبد العزيز، الذكاء الاصطناعي: سياسته وبرامجه وتطبيقاته في التعليم العالي: منظور دولي، مجلة التربية، جامعة الأزهر، دون ذكر السنة، ص 373.

المطلب الثاني:

مفهوم الذكاء الاصطناعي

يطبق الذكاء الاصطناعي التحليل المتقدم والتقنيات المستندة إلى المنطق لتفسير الأحداث، ودعم قرارات أتمتها واتخاذ الإجراءات، حدثت تطورات الذكاء الاصطناعي في الغالب في التعليم الآلي، والذي يسمح بمعالجة كميات هائلة من البيانات وأشكال التعلم بناء على التعرض المتكرر للظروف التجريبية جنبا إلى جنب مع خوارزميات التعلم المعقدة، فمن الممكن تدريب البرنامج على التعرف على الصور، ترجمة اللغات، تحديد المخاطر، العثور الأنماط والاتجاهات التي يصعب على الانسان في العادة العثور عليها، ففي شكله الحالي يعتمد التعلم الذاتي على توافر كمية كبيرة من المعلومات بغض النظر عن كونها منظمة أو غبر منظمة[1].

تبعا لذاك، سنتطرق إلى تعريف الذكاء الاصطناعي، ثم التطرق إلى أبرز خصائصه:

الفرع الأول: تعريف الذكاء الاصطناعي

الذكاء الاصطناعي يتكون من كلمتين: ذكاء واصطناعي

ذكاء" Intelligence" وتعني:

أولا-الذكاء لغة :أصله تمام الشيء، ويدل على حدة في الشيء ونفاذ، والذكاء: سرعة الفطنة[2].

[1] - هشام علاق، حنان دريد، تطبيقات الذكاء الاصطناعي في المؤسسات المالية مدخل لتفعيل الشمول المالي، المجلد 05، العدد 01، مجلة الاقتصاد والتنمية المستدامة، جامعة يحي فارس، المدية، الجزائر، 2022، ص 709.

[2] - محمد بن مكرم بن على، أبو الفضل، جمال الدين ابن منظور الأنصاري الرويفعي الإفريقي، لسان العرب، دار بيروت، الطبعة الثالثة، بيروت، لبنان، دون ذكر السنة، ص 28.

وهو مصطلح شامل لتطبيقات تؤدي مهام معقدة، فالذكاء الاصطناعي هو أحد علوم الحاسب الآلي الحديثة التي تبحث عن أساليب متطورة للقيام بأعمال واستنتاجات تشابه ولو في حدود ضيقة تلك الأسباب التي تنسب لذكاء الإنسان[1].

أما الاصطناعي " Artificial فمشتق من الفعل:صنع، ومعناه في اللغة: "عمله وأنشأه، أو حوله من مادة أولية لشيء صالح للاستعمال[2]".

لغة: صنعه يصنعه صنعا، فهو مصنوع وصناع: عمله، ويقال اصطنع فلان خاتما إذا سأل رجلا أن يصنع له خاتما، وقال تعالى: «صنع الله الذي أتقن كل شيء."[3] وقوله أيضا: «واصطنعتك لنفسي"[4].

وبرز مصطلح الذكاء الاصطناعي مع ظهور الاكتشافات وتطور التكنولوجيا، ليقوم بمهام متعددة اختص بها الذكاء البشري على مر من الزمن، ليقوم تدريجيا بتسليم مهامه إلى الماكينات التي قللت من الضغط المسلط على الإنسان في إنجاز المهام.

ثانيا: تعريف الذكاء الاصطناعي اصطلاحاً:

يعرف الذكاء الاصطناعي اصطلاحاً بأنه: " فرع من فروع علوم الكمبيوتر التي تهدف إلى دراسة وتصميم الوكلاء الأذكياء، حيث يكون الوكيل الذكي النظام الذي يدرك بيئته من حوله ويتخذ الإجراءات التي تزيد من فرص النجاح، وهو يضم الطرق

[1] عبد المجيد قتيبة مازن، استخدامات الذكاء الاصطناعي في تطبيقات الهندسة الكهربائية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة ماجيستير، الأكاديمية العربية، الدنمارك، 2009، ص17 .

[2] - عبد الرزاق وهبة محمد وأحمد، المسؤولية المدنية عن أضرار الذكاء الاصطناعي، مجلة جيل الأبحاث القانونية المعمقة، المجلد 43، لبنان، 2020، ص08.

[3]-سورة النمل، الآية 88.

[4]-سورة طه، الآية 41.

والنظريات والتقنيات التي تهدف إلى إنشاء آلات وتقنيات قادرة على محاكاة الذكاء الإنساني" [1].

يعرف الذكاء الاصطناعي في الاصطلاح على أنه :"الأنظمة أو الأجهزة التي تحاك الذكاء البشري لأداء المهام والتي يمكنها أن تحسن من نفسها استناداً إلى المعلومات التي تجمعها[2]".

وعرف أيضا الذكاء الاصطناعي بأنه: " القدرة على التصرف كما لو كان الإنسان هو الذي يتصرف من خلال محاولة خداع المستجوب وإظهار كما لو إن إنساناً الأسئلة المطروحة هو الذي يقوم بالإجابة على

من قبل المستجوب"[3].

كما يعرف الذكاء الاصطناعي بأنه: "جزء من علم الحاسبات الذي يهتم بأنظمة الحاسوب الذكية، والتي تمتلك الخصائص المرتبطة بالذكاء، واتخاذ القرار والمشابهة لدرجة ما للسلوك البشري في هذا المجال فيما يخص اللغات، والتعلم، والتفكير"[4].

[1] - العاصي أحمد، تقييم خبراء الإعلام للأبعاد الأخلاقية والمهنية للذكاء الاصطناعي في الإعلام الرقمي: دراسة ميدانية، رسالة الاصطناعي في الإعلام الرقمي -دراسة ميدانية-، رسالة ماجستير، الجامعة الإسلامية، غزة، فلسطين، 2021، ص10.

[2] - عبد الرزاق وهبة محمد وأحمد، المرجع السابق، ص 10.

[3] - أعراب كيملية، مسؤولية الروبوت في ظل الذكاء الاصطناعي، عدد خاص بالملتقى الدولي المحكم حول الاستثمار المالي والصناعي في الذكاء الصناعي" التكنولوجيا المالية والثورة الصناعية الرابعة"، مركز جيل البحث العلمي، لبنان، 2022، 117.

4 - صالح، فاتن عبد الله، أثر تطبيق الذكاء الاصطناعي والذكاء العاطفي على جودة اتخاذ القرارات، رسالة ماجستير، جامعة الشرق الأوسط، 2009، ص 33.

وبصفة عامة الذكاء الاصطناعي هو ذلك الذكاء الذي يصنعه أو يصطنعه الإنسان بيده في الآلة أو الحاسوب، بمعنى أنه علم يعرف على أساس هدفه وهو جعل الآلات (منظومات الحاسوب) تعمل أشياء تحتاج ذكاء[1].

الفرع الثاني: خصائص الذكاء الاصطناعي

يتسم الذكاء الاصطناعي بمجموعة من الخصائص والمميزات والمتمثلة في[2]:

- القدرة على الاستجابة السريعة للمواقف والأوضاع الجديدة، والتعامل مع الحالات الصعبة المعقدة.
- إمكانية تمثل المعرفة، والقدرة على التصوير والإبداع.
- القدرة على استخدام الأسلوب التجريبي المتفائل عند اتخاذ القرارات وتحليلها.
- القدرة على التعامل مع الحالات الصعبة والمعقدة.
- القدرة على التعامل مع المواقف الغامضة مع غياب المعلومة.
- القدرة على تمييز الأهمية النسبية لعناصر الحالات المعروضة.
- القدرة على التصور والابداع وفهم الأمور المرئية وادراكها.

[1] -ياسين سعد غالب، أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات، دار المنهاج للنشر والتوزيع، ط 1، 2012، عمان، ص 114.

[2]- أمينة عثامنية، المفاهيم الأساسية للذكاء الاصطناعي، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين ألمانيا، 2019، ص 13.

- القدرة على تقديم المعلومة لإسناد القرارات الإدارية.
- استخدام الذكاء في حلول المشكلات مع غياب المعلومة الكاملة.
- القدرة على التفكير والإدراك، واكتساب المعرفة وتطبيقها.
- القدرة على التعلم والفهم من التجارب والخبرات السابقة، واستخدام الخبرات القديمة وتوظيفها في مواقف جديدة.
- استخدام الذكاء في حل المشاكل المعروضة مع غياب المعلومة الكاملة.
- القدرة على اكتساب المعرفة وتطبيقها.
- القدرة على التعلم والفهم من التجارب والخبرات السابقة.
- القدرة على استخدام الخبرات القديمة وتوظيفها في مواقف جديدة.
- القدرة على استخدام التجربة والخطأ لاستكشاف الأمور المختلفة.
- القدرة على الاستجابة السريعة للمواقف والظروف الجديدة.

وبناء عليه يتبين أن تطبيق الذكاء الاصطناعي لا يعتمد على خطوات متتابعة تؤدي إلى الحل الصحيح، بل يتم اختيار الطريقة التي تبدو مناسبة للحل، مع خيار تعديل إذا لزم الأمر، ومن السمات المنسوبة للذكاء الاصطناعي قدرته على اكتشاف حلول معينة على الرغم من عدم توفر المعلومات الزمنية المعينة بشكل كامل.

هذه بعض الخصائص الأساسية للذكاء الاصطناعي، وتظهر قدراته المتعددة في مجموعة متنوعة من المجالات مثل الروبوتات، والتحليل الضخم للبيانات، والطب، والتعليم، والتجارة الإلكترونية.

المبحث الثاني:

مخاطر الذكاء الاصطناعي

أصبح الذكاء الاصطناعي اليوم أحد أبرز الأدوات المستخدمة في المجالات الأمنية والاستخباراتية، نظراً لقدرته على معالجة كميات هائلة من البيانات بكفاءة عالية. إذ لم يعد الاعتماد في العمل الاستخباراتي على العنصر البشري وحده، بل أصبحت الخوارزميات الذكية قادرة على دعم جهود جمع المعلومات، التحليل، واستباق التهديدات.

إن الذكاء الاصطناعي مجال علمي سريع التطور، دخل في جميع المجالات الحيوية، ما خلق تنافس شديد بين الدول، فهو أصبح يمثل سلاحا عسكريا قويا حول ميزان القوى العالمي، ما يشكل خطرا على الأمن القومي والداخلي وعلى النظام القانوني وهو ما سنتناوله في هذا المطلب.

المطلب الأول:

المخاطر الأمنية للذكاء الاصطناعي

يسعى الذكاء الاصطناعي، باعتباره إحدى أهم ثمار الثورة التكنولوجية الحديثة، إلى محاكاة القدرات الإدراكية والسلوكية للإنسان من خلال تمكين الحواسيب والروبوتات من التفكير، التحليل، واتخاذ القرار بصورة ذاتية. ويُنظر إلى هذا التقدم باعتباره وسيلة لتعظيم الفوائد الاقتصادية عبر رفع الإنتاجية وتحقيق الأرباح، إضافة إلى دوره في تسريع الابتكارات وتقديم حلول ذكية لمختلف القطاعات. غير أنّ هذا التوسع المتسارع يثير جملة من المخاطر والتهديدات، خاصة في البعد الأمني والاستراتيجي، إذ يُخشى من إمكانية تفوق الذكاء الاصطناعي على القدرات المعرفية والعقلية للبشر، بما قد يترتب عنه تهديد لمكانة الإنسان ودوره المركزي في التحكم والسيطرة. إن ما يسمى بـ"التفوق المعرفي للآلة (Machine Cognitive) "

(Superiorityيُعد من بين أبرز التحديات المطروحة اليوم، لما يحمله من احتمالات تتعلق بفقدان السيطرة على الأنظمة الذكية، وزيادة الهشاشة في مجال الأمن السيبراني، إضافة إلى المخاطر الأخلاقية والاجتماعية المرتبطة بالاعتماد المفرط على هذه التكنولوجيا[1].

أضحى الذكاء الاصطناعي في الوقت الراهن عنصراً محورياً في ميدان الحروب الحديثة، إذ لم يعد يقتصر دوره على المهام التقنية البسيطة، بل أصبح أداة استراتيجية متقدمة تسهم في تعزيز القدرات العسكرية. فبفضل تقنيات التعلم العميق ومعالجة اللغة الطبيعية، باتت الأنظمة الذكية قادرة على تحليل معطيات ساحة المعركة بدقة متناهية، بما في ذلك جمع المعلومات وتصنيفها وتفسيرها في وقت قصير. كما يساهم الذكاء الاصطناعي في تحديد الأهداف العسكرية ورصد المسافات الأمنية، فضلاً عن تطوير قدرات التعرف البصري والحراري على الأهداف . وإلى جانب ذلك، تُستخدم خوارزمياته في تصميم أنظمة التحكم الذاتي للطائرات بدون طيار والمركبات القتالية، مما يمكّنها من اتخاذ قرارات تكتيكية ملائمة في ظروف معقدة، قد يعجز العنصر البشري عن التعامل معها بالسرعة والكفاءة المطلوبة. وبهذا المعنى، يشكل الذكاء الاصطناعي إضافة نوعية للحروب المعاصرة من حيث الدقة، والسرعة، وتقليل الأخطاء البشرية، مع ما يثيره ذلك من تحديات قانونية وأخلاقية بشأن مشروعية استخدامه في النزاعات المسلحة[2].

ومن المعروف أن الذكاء الاصطناعي قد تم استخدامه في مجالات مثل التحليل الاستخباراتي ومعالجة اللغة الطبيعية لتحليل البيانات واستخراج المعلومات منها، ومن الممكن أن يتم استخدامه أيضًا في التحقيقات والتحقيقات الأمنية للمساعدة في تحليل البيانات وتحديد الأنماط والتوجيه في التحقيقات.

[1] -Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson Education, pp. 27-30.

[2] - حيدر فالح سلمان، المرجع السابق، ص118.

كما تتعرض الأنظمة الأمنية للدول للهجمات السيبرانية ما يؤدي إلى تلف الأنظمة أو التلاعب بالمعلومات أو السرقة كونها تعتمد على برمجيات ما جعل الحكومات في تأهب دائم لتطوير أدوات الهجوم المضاد، وتأمين قوي للبيانات من عمليات الاختراق والتجسس وإيجاد بنى امنية تحتية صلبة وقوانين رادعة.

ثم إن تطبيق الذكاء الاصطناعي في جهود مكافحة الإرهاب يبشر بكثير، غير أن هناك قيودا وعقبات مختلفة يتعين معالجتها، ويتمثل أحد التحديات في توافر البيانات ونوعيتها، تعتمد أنظمة الذكاء الاصطناعي على مجموعات بيانات كبيرة ومتنوعة للتدريب والتحليل الفعالين، التحدي الآخر هو قابلية تفسير نماذج الذكاء الاصطناعي يعد فهم عملية صنع القرار في أنظمة الذكاء الاصطناعي أمرا بالغ الأهمية لبناء الثقة ومعالجة التحيزات المحتملة بالإضافة إلى ذلك، هناك اعتبارات أخلاقية وقانونية تحيط باستخدام الذكاء الاصطناعي في مكافحة الإرهاب، مثل الشواغل المتعلقة بالخصوصية واحتمال إساءة الاستخدام على الرغم من هذه التحديات فإن الذكاء الاصطناعي لديه القدرة على تعزيز جمع المعلومات الاستخبارية وتقييم التهديدات وقدرات الاستجابة في مكافحة الإرهاب[1].

الفرع الثاني: المخاطر القانونية للذكاء الاصطناعي

إنّ استخدام التكنولوجيا يمثل سلاحاً ذا حدّين، فهي من جهة وسيلة فعّالة لتسهيل الحياة اليومية وتطوير القطاعات المختلفة، ومن جهة أخرى أداة خطيرة قد تؤدي إلى انتهاك الخصوصية وتقويض الأمن المعلوماتي. إذ تقوم العديد من التطبيقات الحديثة بجمع كميات هائلة من البيانات الشخصية، سواء من خلال

[1] - Alazab, M, Broadhurst, R & Slay, J. (2018) Application of artificial intelligence to counter-terrorism: A review of limitations, impediments, and potentials. Terrorism and Political Violence, 30(5), 801-819.

موافقة المستخدم عبر الاتصال بالإنترنت، أو عن طريق أجهزة الاستشعار المدمجة في الهواتف الذكية، وغالباً ما يتم ذلك دون علم الأفراد القريبين منها[1].

ومن أبرز هذه المخاطر ما يتعلق بقدرة الأنظمة على تحديد المواقع الجغرافية للأشخاص عبر الهواتف المزودة بنظام تحديد المواقع العالمي(GPS) ، والتي غالباً ما تكون متصلة بالتطبيقات الاجتماعية أو الكاميرات الذكية، مما يشكل تهديداً مباشراً لحرمة الحياة الخاصة[2].

كما أنّ تطور خوارزميات التعرف على الوجه جعل استغلالها في أغراض غير مشروعة أمراً وارداً، مثل المراقبة دون إذن أو استخدام الصور الشخصية في سياقات مسيئة، وهو ما يمثل خطراً على الحقوق الفردية والحريات الأساسية[3].

وإلى جانب ذلك، انتشرت في السنوات الأخيرة تقنية **المقاطع الزائفة العميقة (Deepfakes)**، وهي مقاطع فيديو أو صور معدلة بالاعتماد على الذكاء الاصطناعي، بحيث يُستبدل وجه أو صوت الشخص الحقيقي بشخص آخر بطريقة يصعب كشفها. ورغم إمكانية الاستفادة من هذه التقنية في التعليم والإبداع الفني، إلا أنها تطرح مخاطر جسيمة على المستوى الأخلاقي والقانوني، إذ قد تُستغل للتشهير، أو تزوير الأخبار، أو انتهاك الحياة الخاصة[4].

واستخدام الذكاء الاصطناعي يمكن أن يُثير العديد من المخاطر القانونية إذا لم يتم التعامل معه بحذر وفقًا للقوانين المعمول بها، من بين هذه المخاطر:

---

[1] - شوشانا زوبوف، عصر رأسمالية المراقبة، ترجمة: ناصر كامل، دار نشر جداول، بيروت، 2021، ص 115.

[2] - دانيال سولوف، فهم الخصوصية، ترجمة: أحمد درويش، المنظمة العربية للترجمة، بيروت، 2015، ص 74.

[3] - وودرو هارتزوغ، مخطط الخصوصية: معركة السيطرة على تصميم التكنولوجيا، ترجمة: خالد العامري، دار جامعة حمد بن خليفة للنشر، الدوحة، 2020، ص 142.

[4] -شوشانا زوبوف، المرجع السابق، ص 120.

أولا/انتهاك الخصوصية والبيانات الشخصية:

أظهرت تقنيات الذكاء الاصطناعي إمكانات كبيرة في مكافحة الإرهاب والعنف، يمكن استخدام هذه التقنيات لتحليل كميات كبيرة من البيانات، بما في ذلك منشورات وسائل التواصل الاجتماعي والاتصالات عبر الإنترنت ولقطات المراقبة، لتحديد أنماط ومؤشرات الأنشطة الإرهابية، يمكن تدريب خوارزميات التعلم الألي على التعرف على سلوكيات أو أنماط محددة مرتبطة بالإرهاب، مما يتيح الكشف المبكر والتدخل، بالإضافة إلى ذلك يمكن للذكاء الاصطناعي أن يساعد في تحليل المعاملات والشبكات المالية والمساعدة في الكشف عن مصادر التمويل غير المشروعة وتعطيل تمويل الارهاب[1].

يُعتبر انتهاك الخصوصية من أبرز التحديات المرتبطة بالذكاء الاصطناعي، إذ تعتمد معظم تطبيقاته الحديثة على جمع وتحليل ومعالجة كميات هائلة من البيانات الشخصية للمستخدمين، سواء بشكل مباشر عبر إدخالهم لمعلوماتهم في المنصات الرقمية، أو بطرق غير مباشرة من خلال تتبع نشاطهم على الإنترنت أو عبر أجهزة الاستشعار. وغالباً ما يتم هذا الاستخدام دون موافقة صريحة أو وعي كامل من الأفراد، مما يشكل خرقاً لمبدأ حماية الحياة الخاصة الذي تضمنه القوانين الوطنية والاتفاقيات الدولية[2].

كما أن خوارزميات الذكاء الاصطناعي القائمة على البيانات الضخمة (Big Data)قد تُستغل في تحديد أنماط سلوك الأفراد، أو التنبؤ بتصرفاتهم المستقبلية، أو حتى بناء ملفات شخصية دقيقة عنهم، وهو ما قد يفتح المجال أمام ممارسات خطيرة مثل التجسس، التمييز، أو الاستغلال التجاري والسياسي .ويزداد هذا الخطر

[1]- عادل عبد السميع عوض، دور الذكاء الاصطناعي في التنبؤ بمكافحة الارهاب، مجلة متون، جامعة مولاي الطاهر، سعيدة، المجلد17، العدد01، الجزائر، 2024، ص80.

[2] - علي مصطفى، *الذكاء الاصطناعي والخصوصية: قراءة في المخاطر القانونية*، دار الجامعة الجديدة، الإسكندرية، 2022، ص. 88.

مع ضعف الشفافية في آليات عمل الأنظمة الذكية، وصعوبة ضبط الجهات المالكة لها أو محاسبتها قانونياً عند حدوث تجاوزات[1].

وعليه، فإن الحد من هذه المخاطر يستوجب وضع إطار تشريعي محكم ومتطور يواكب التقدم التكنولوجي السريع، ويعزز من حماية البيانات الشخصية للأفراد. ويتعين أن يستند هذا الإطار إلى مجموعة من المبادئ الجوهرية، أهمها : الموافقة المسبقة، بحيث لا يجوز جمع أو معالجة بيانات أي شخص إلا بعد حصول الجهة المعنية على إذن صريح منه؛ ومبدأ الشفافية، الذي يفرض على المؤسسات المالكة لتقنيات الذكاء الاصطناعي أن توضح للمستخدمين طبيعة البيانات التي يتم جمعها، وأهداف استعمالها، والجهات المستفيدة منها؛ ومبدأ التناسب، الذي يقضي بعدم التوسع في جمع المعلومات إلا في حدود ما هو ضروري لتحقيق الغرض المشروع دون إفراط أو مبالغة؛ بالإضافة إلى الحق في النسيان الرقمي، الذي يمكّن الأفراد من المطالبة بحذف بياناتهم الشخصية نهائياً متى انتفت الحاجة إليها أو متى رغبوا في ذلك. إن اعتماد هذه المبادئ وتفعيلها قانونياً من شأنه أن يضمن للأفراد قدرة فعلية على التحكم في بياناتهم الخاصة، وحمايتها من أي شكل من أشكال الاستغلال غير المشروع في بيئة الذكاء الاصطناعي[2].

ثانيا/انتهاك حقوق الملكية الفكرية:

قد يتم استخدام الذكاء الاصطناعي لانتهاك حقوق الملكية الفكرية، مثل انتهاك حقوق التأليف والنشر أو سرقة الأفكار أو براءات الاختراع، وهو ما برز مع ظهور الذكاء الاصطناعي التوليدي الذي هو تقنية من تقنيات الذكاء الاصطناعي

[1] - نسرين بوشامة، *الذكاء الاصطناعي والحقوق الأساسية للأفراد*، مجلة الفكر القانوني، جامعة الجزائر 1، العدد 3، الجزائر، 2023، ص. 102.

[2] - عبد الرزاق بن عيسى، "حماية البيانات الشخصية في ظل الثورة الرقمية"، *مجلة الدراسات القانونية*، كلية الحقوق – جامعة الجزائر 1، المجلد 15، العدد 2، الجزائر، 2021، ص. 51.

يعتمد على انتاج مجموعة مختلفة من المضامين في شكل صور أو أصوات أو فيديوهات أو بيانات بطريقة سريعة ودقيقة[1].

يعتمد الذكاء الاصطناعي التوليدي على تدريب نماذج الذكاء الاصطناعي باستخدام كميات ضخمة من البيانات، بما في ذلك النصوص والصور والموسيقى، والتي غالبًا ما تكون محمية بحقوق التأليف والنشر. إذا تم استخدام هذه المواد دون إذن من أصحاب الحقوق، فإن ذلك يشكل انتهاكًا لحقوقهم، فعلى سبيل المثال، رفعت شركة "جيتي إيمجز" دعوى قضائية ضد شركة "Stability AI" بتهمة استخدام صورها المحمية دون ترخيص لتدريب نموذج الذكاء الاصطناعي "Stable Diffusion"[2].

يُعتبر انتهاك حقوق الملكية الفكرية من خلال استخدام الذكاء الاصطناعي التوليدي دون إذن من أصحاب الحقوق، تهديدًا مباشرًا للإبداع البشري. فقد أظهرت الدراسات أن هذا الانتهاك يؤدي إلى تقويض سوق الإبداع البشري، حيث قد يتم استبدال أعمال الكُتّاب والفنانين والباحثين بمنتجات اصطناعية أقل تكلفة، مما يُضعف حقوقهم الاقتصادية ويقلل من قيمة الإبداع البشري.

على سبيل المثال، أشار تقرير لمنظمة التجارة العالمية في 17 سبتمبر 2025 إلى أن الذكاء الاصطناعي قد يؤدي إلى زيادة قيمة التجارة في السلع والخدمات بنسبة تصل إلى 40% بحلول عام 2040، مع إمكانية نمو الناتج المحلي الإجمالي العالمي بنسبة 12 إلى 13%. ومع ذلك، حذرت المنظمة من خطر تفاقم الفجوات الاقتصادية إذا لم تصاحب هذا التحول استثمارات وسياسات شاملة، موضحة أن الذكاء

[1] - مصطفى بن أمينة، الذكاء الاصطناعي التوليدي: أزمة جديدة في حقوق الملكية الفكرية، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي، المجلد07، العدد02، الجزائر، 2023، ص 792.

[2] - الشرع، أحمد إبراهيم محمد، وجاد الله، مروج ماهر أحمد، الذكاء الاصطناعي وانتهاك حق التأليف، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، المجلد 6، العدد 1، الجزائر، 2025، ص ص 86-98.

الاصطناعي قد يؤثر على الوظائف ويتطلب تعزيز التعليم وإعادة التدريب، وبالإضافة إلى ذلك، يُظهر الذكاء الاصطناعي التوليدي قدرته على إنتاج محتوى إبداعي بسرعة ودقة، مما قد يُقلل من الطلب على الأعمال الإبداعية البشرية. هذا التغير في ديناميكيات السوق قد يؤدي إلى تقليل قيمة الإبداع البشري وتقويض حقوق المبدعين في الاستفادة الاقتصادية من أعمالهم[1].

علاوة على ذلك، يُشير تقرير آخر إلى أن الذكاء الاصطناعي التوليدي لا يكتفي بإعادة استخدام المحتوى المحمي، بل يمتلك القدرة على تعزيز الإنتاجية وجودة الإبداع البشري بشكل غير مسبوق. فالأدوات المدعومة بهذه التكنولوجيا باتت تتيح للمبدعين إنتاج محتوى عالي الجودة بتكلفة زهيدة، مما يُغيّر بعمق طبيعة العمل الإبداعي وموقعه [2].

بالتالي، يُظهر الذكاء الاصطناعي التوليدي تأثيرًا مزدوجًا على الإبداع البشري: من جهة، يُسهم في تعزيز الإنتاجية وجودة المحتوى، ومن جهة أخرى، يُهدد حقوق المبدعين الاقتصادية ويُقلل من قيمة أعمالهم.

قد يؤدي استخدام الذكاء الاصطناعي إلى التمييز والتحيز في بعض الحالات بسبب اعتماد هذه الأنظمة على بيانات تاريخية قد تحمل تحيزات بشرية أو اجتماعية. على سبيل المثال، إذا تم تدريب خوارزميات التوظيف أو القروض المالية على بيانات تحتوي على تحيزات قائمة مسبقًا، فإن النظام قد يكرر هذه التحيزات ويستبعد فئات معينة بشكل غير عادل، مثل النساء أو الأقليات العرقية أو أصحاب الأعمار المختلفة. كما أن خوارزميات التعرف على الوجه أظهرت في عدة دراسات معدلات خطأ أعلى عند التعرف على وجوه الأشخاص ذوي البشرة الداكنة مقارنة

[1] - الشرع، أحمد إبراهيم محمد، وجاد الله، مروج ماهر أحمد، المرجع السابق، ص103.

[2]- لحول بن علي، وبريكي خالد، *حماية الحياة الخاصة والبيانات الشخصية في القانون المقارن*، دار الخلدونية للنشر والتوزيع، الجزائر، 2019، ص. 78.

بالأشخاص ذوي البشرة الفاتحة، مما يضعف المساواة في الوصول إلى الخدمات. هذه الانتهاكات تتعارض مع المبادئ الأساسية لحقوق الإنسان، بما في ذلك الحق في المساواة وعدم التمييز، وتخالف القوانين الوطنية والدولية المصممة لضمان المعاملة العادلة لجميع الأفراد[1].

ثالثا/ المسؤولية القانونية:

تثير مسؤولية الذكاء الاصطناعي القانونية تساؤلات معقدة في حال حدوث أخطاء أو أضرار ناتجة عن أنظمته، خاصةً في ظل غياب إطار قانوني موحد. فيما يلي تحليل مفصل لأبعاد هذه المسؤولية، بحيث تُعتبر المسؤولية المدنية من أبرز القضايا المطروحة، حيث يُسائل المتضررون عن الأضرار التي قد تنجم عن استخدام أنظمة الذكاء الاصطناعي. تختلف الآراء حول تحديد المسؤولية، فبعضها يُحمّلها للمطورين أو المستخدمين، بينما يرى آخرون أن الأنظمة ذاتها قد تكون مسؤولة. على سبيل المثال، في حالة استخدام "الروبوتات الطبية" أو "الطبيب الآلي"، قد يكون من الصعب تحديد المسؤولية المباشرة، مما يستدعي تطوير قوانين خاصة لهذا المجال، كما تقوم المسؤولية الجزائية في حال ارتكاب أفعال تُعتبر جرائم، مثل التسبب في أذى جسدي أو نفسي، قد يُثار التساؤل حول إمكانية محاكمة أنظمة الذكاء الاصطناعي. يُشير بعض الباحثين إلى ضرورة تطوير تشريعات تُمكّن من محاكمة هذه الأنظمة، خاصةً في ظل تزايد استخدامها في مجالات حساسة[2].

رابعا/ تهديدات الأمن السيبراني:

إن دمج تقنيات الذكاء الاصطناعي في البُنى التحتية السيبرانية قد يُفضي إلى تصاعد التهديدات الأمنية، بما في ذلك الهجمات الإلكترونية المتقدمة، والسرقات

[1] - عاطف عوض، "دور إدارة المعرفة وتقانتها في تحقيق التطوير التنظيمي"، *مجلة جامعة دمشق للعلوم الاقتصادية والقانونية*، عدد 01، سوريا، 2012، ص150.

[2] - عاطف عوض، المرجع السابق، ص 152.

الرقمية للبيانات الحساسة، والتجسس السيبراني المعتمد على تقنيات متطورة. على سبيل المثال، يُمكن للمهاجمين استخدام الذكاء الاصطناعي لتطوير أدوات خبيثة قادرة على التكيف مع أنظمة الدفاع، مما يجعلها أكثر قدرة على اختراق الشبكات والأنظمة المعلوماتية. بالإضافة إلى ذلك، يُمكن استغلال الذكاء الاصطناعي في تنفيذ هجمات منسقة تُصعب من اكتشافها والتصدي لها، مما يُعقد من مهمة فرق الأمن السيبراني في التصدي لهذه التهديدات المتطورة[1].

تُظهر الدراسات الحديثة أن المهاجمين يستخدمون الذكاء الاصطناعي التوليدي لإنشاء رسائل تصيد احتيالي مُخصصة، مما يزيد من فعالية الهجمات ويصعب من اكتشافها. كما أن استخدام الذكاء الاصطناعي في أتمتة الهجمات يُمكّن المهاجمين من تنفيذ عمليات معقدة بسرعة ودقة، مما يُزيد من حجم الأضرار المحتملة.

علاوة على ذلك، يُمكن أن يُسهم الذكاء الاصطناعي في تحسين تقنيات التجسس السيبراني، من خلال تحليل كميات ضخمة من البيانات واستخراج المعلومات الحساسة، مما يُعرض الأفراد والمؤسسات لمخاطر متزايدة في ظل غياب تدابير حماية فعّالة[2].

بناءً على ذلك، يُعتبر من الضروري تطوير استراتيجيات أمنية متقدمة تعتمد على الذكاء الاصطناعي لمواجهة هذه التهديدات، بالإضافة إلى تعزيز الوعي الأمني وتدريب الفرق المختصة على استخدام هذه التقنيات بشكل فعّال وآمن.

[1] - لحول بن علي، المرجع السابق، ص81.

[2] - الشرع، أحمد إبراهيم محمد، المرجع السابق، ص 121.

خاتمة:

توصلنا من خلال هذه الدراسة إلى الذكاء الاصطناعي، يمثل ثورة تقنية كبرى قادرة على إحداث تحول جذري في مختلف جوانب الحياة، بدءًا من الاقتصاد والصناعة وصولاً إلى التعليم والصحة والخدمات الحكومية. غير أن هذه القوة الهائلة لا تخلو من المخاطر التي قد تهدد الأمن الفردي والمجتمعي على حد سواء. فمن الناحية الأمنية، يمكن أن يُستغل الذكاء الاصطناعي في شن هجمات سيبرانية معقدة، وسرقة البيانات، والتجسس على الأفراد والدول، مما يضع الحكومات والمؤسسات في مواجهة تحديات غير مسبوقة. كما أن الاستخدام غير المنضبط للذكاء الاصطناعي قد يؤدي إلى انتهاك الخصوصية الفردية، إذ تعتمد العديد من الأنظمة على جمع وتحليل كميات هائلة من البيانات الشخصية، أحيانًا دون علم أو موافقة الأفراد.

إضافة إلى ذلك، قد يتسبب الذكاء الاصطناعي في تعزيز التمييز والتحيز، إذ تعتمد خوارزمياته على بيانات قد تكون غير متوازنة أو متحيزة، مما ينعكس سلبًا على القرارات في مجالات حساسة مثل التوظيف، والإقراض، والنظام القضائي. كما يمكن أن يؤدي إلى تقويض حقوق الملكية الفكرية، من خلال استخدام أعمال مبدعة دون إذن أصحابها، مما يطرح تحديات قانونية وأخلاقية جديدة.

قائمة المراجع:

أولا: القرآن الكريم

ثانيا: الكتب

1. إبراهيم عبد الله القلاف، "الروبوت: ميكانيكية الإدراك ومرئيات في الصناعات الحديثة"، المؤسسة العربية للطباعة والنشر، البحرين.
2. أعراب كيملية، مسؤولية الروبوت في ظل الذكاء الاصطناعي، عدد خاص بالملتقى الدولي المحكم حول الاستثمار المالي والصناعي في الذكاء الصناعي" التكنولوجيا المالية والثورة الصناعية الرابعة"، مركز جيل البحث العلمي، لبنان، 2022.
3. عادل عبد النور، مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عبد العزيز للعلوم التقنية، لبنان، 2012، ص18.
4. محمد مجدي صلاح طه، منهاج البحث التربوي، سلسلة العلوم التربوية الإسلامية، دار الفكر العربي للطباعة والنشر، القاهرة، مصر.
5. محمد بن مكرم بن على، أبو الفضل، جمال الدين ابن منظور الأنصاري الرويفعي الإفريقي، لسان العرب، دار بيروت، الطبعة الثالثة، بيروت، لبنان، دون ذكر السنة.
6. محمد الهادي، الذكاء الاصطناعي معالمه وتطبيقاته وتأثيراته التنموية والمجتمعية، الطبعة الأولى، الدار المصرية اللبنانية للنشر، القاهرة، مصر، 2021.
7. لحول بن علي، وبريكي خالد، حماية الحياة الخاصة والبيانات الشخصية في القانون المقارن، دار الخلدونية للنشر والتوزيع، الجزائر، 2019.
8. ياسين سعد غالب، تحليل وتصميم نظم المعلومات، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، الأردن،2011.

ثالثا: المجلات

1. إبراهيم، أسامة محمد عبد السلام، أثر بناء نظام خبير على شبكة الويب للطلاب المعلمين لتنمية مهارات حل المشكلات والقدرة على اتخاذ القرار .مجلة تكنولوجيا التعليم، المجلد25، العدد01، 2015.

2. أمينة عثامنية، المفاهيم الأساسية للذكاء الاصطناعي، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين ألمانيا، 2019.
3. الويزة خلفة ساهل، أسامة سنوسي، تطبيقات الذكاء الاصطناعي في صناعة السياحة والسفر تحول جديد في الرحلات والإقامة دراسة حالة فنادق سويسرا، مجلة القانون والعلوم البيئية، المجلد 03، العدد 01، جامعة زيان عاشور، الجلفة، الجزائر، 2024.
4. المالكي، وفاء فواز، دور تطبيقات الذكاء الاصطناعي في تعزيز الاستراتيجيات التعليمية في التعليم العالي "مراجعة الأدبيات ".مجلة العلوم التربوية والنفسية، المجلد07، العدد10، 2023.
5. اللوزي موسى، الذكاء الاصطناعي في الأعمال، بحث مقدم للمؤتمر السنوي الحادي عشر ذكاء الأعمال واقتصاد المعرفة، كلية الاقتصاد والعلوم الإدارية، جامعة الزيتونة، عمان، الأردن ،2012.
6. بليليطة أسماء، التكريس القانوني والتنظيمي للذكاء الاصطناعي في الجزائر، المجلة الدولية للذكاء الاصطناعي في التعليم والتدريب، المجلد 10، العدد 02، 2022.
7. بكر عبد الجواد السيد، طه محمود إبراهيم عبد العزيز، الذكاء الاصطناعي: سياسته وبرامجه وتطبيقاته في التعليم العالي: منظور دولي، مجلة التربية، جامعة الأزهر، دون ذكر السنة.
8. سامية شهي قمورة، باي محمد، حيزية كروش، الذكاء الاصطناعي بين الواقع والمأمول دراسة تقنية وميدانية، حوليات جامعة الجزائر، عدد خاص، ملتقى دولي، الذكاء الاصطناعي تحد جديد للقانون؟، الجزائر، 2018.
9. عبد الرزاق بن عيسى، "حماية البيانات الشخصية في ظل الثورة الرقمية"، مجلة الدراسات القانونية، كلية الحقوق – جامعة الجزائر 1، المجلد 15، العدد 2، الجزائر، 2021.
10. مصطفى بن أمينة، الذكاء الاصطناعي التوليدي: أزمة جديدة في حقوق الملكية الفكرية، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي، المجلد07، العدد02، الجزائر، 2023.

11. عبد الرزاق وهبة محمد وأحمد، المسؤولية المدنية عن أضرار الذكاء الاصطناعي، مجلة جيل الأبحاث القانونية المعمقة، المجلد 43، لبنان، 2020.
12. عاطف عوض، "دور إدارة المعرفة وتقانتها في تحقيق التطوير التنظيمي"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، عدد 01، سوريا، 2012.
13. هشام علاق، حنان دريد، تطبيقات الذكاء الاصطناعي في المؤسسات المالية مدخل لتفعيل الشمول المالي، المجلد 05، العدد 01، مجلة الاقتصاد والتنمية المستدامة، جامعة يحي فارس، المدية، الجزائر، 2022.
14. صفاء جمال جواس، أحمد جمال جواس، استخدام تطبيقات الذكاء الاصطناعي في مؤسسات التعليم العالي في اليمن (دراسة استكشافية)، المجلد 08، العدد 01، مجلة قبس للدراسات الإنسانية والاجتماعية، جامعة الشهيد حمة لخضر، الوادي، 2024.
15. هبة بنت عبد الوارث الأصبحي، مدى تأثير الذكاء الاصطناعي في بيئة التعليم الالكتروني بمدارس التعليم العام بالمملكة العربية السعودية من وجهة نظر المتعلمين، مجلة كلية التربية بالزقازيق، المجلد 39، العدد 130، الجزء الأول، مصر، 2024.

رابعا: رسائل الماجستير

1. العاصي أحمد، تقييم خبراء الإعلام للأبعاد الأخلاقية والمهنية للذكاء الاصطناعي في الإعلام الرقمي: دراسة ميدانية، رسالة الاصطناعي في الإعلام الرقمي -دراسة ميدانية-، رسالة ماجستير، الجامعة الإسلامية، غزة، فلسطين، 2021.
2. عبد المجيد قتيبة مازن، استخدامات الذكاء الاصطناعي في تطبيقات الهندسة الكهربائية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة ماجيستير، الأكاديمية العربية، الدنمارك، 2009.
3. صالح، فاتن عبد الله، أثر تطبيق الذكاء الاصطناعي والذكاء العاطفي على جودة اتخاذ القرارات، رسالة ماجستير، جامعة الشرق الأوسط، 2009.

دور الذكاء الاصطناعي

في مجال العقود والمرفق العمومي الذكي

The role of artificial intelligence in the field

of contracts and smart public services

د. بركات عماد الدين

جامعة الشاذلي بن جديد- الطارف، barkat-imadeddine@univ-eltarf.dz

د. بن صالحية صابر

جامعة الشاذلي بن جديد- الطارف، bensalhiasaber@gmail.com

ملخص:

لقد تطورت البشرية تطوراً هائلاً في الربع الأخير من القرن الماضي، وذلك منذ بداية الثورة الصناعية مروراً بإطلاق الأقمار الصناعية وصناعة الروبوتات إلى تقنية الذكاء الاصطناعي، حيث أتيح لهذا الاذكاء الاصطناعي أن يدخل في معظم المجالات والأنشطة والمهن، ويعد الذكاء الاصطناعي نظرية لتطوير الآلات لتتمكن من إتمام المهام التي تتطلب الذكاء البشري، مثل القدرة على حل المشاكل، والتفكير السليم، والإدراك الحسي والمعنوي، وذلك من خلال التعلم من التجارب والأخطاء، بحيث تتخذ القرارات التي يصعب على العقل البشري الوصول إليها بشكل سريع، وقد وصلت مجالات الذكاء الاصطناعي إلى ميدان القانون بمختلف فروعه خاصة ما تعلق بمجالي العقود وادارة المرافق العامة.

الكلمات المفتاحية: ك الذكاء الاصطناعي، العقود، المرافق العامة، التكنولوجيا، العدالة.

***Abstract**:*

Humanity has made tremendous progress in the last quarter century, from the beginning of the Industrial revolution, through the launch of satellites and the robotics industry, to artificial intelligence technology. This technology has enabled AI to enter most fields, activities, and professions. AI is a theory for developing machines to perform tasks that require human intelligence, such as problem-solving, sound reasoning, and sensory and moral perception. This is achieved by learning from experience and errors, enabling machines to quickly make decisions that are difficult for the human mind to reach. artificial intelligence has also reached the field of law in its various branches, especially those related to contracts and public utility management.
***Key words**: Artificial intelligence, contracts, public utilities, technology, justice.*

مقدمة:

أصبح الذكاء الاصطناعي جزء لا يتجزأ من صناعة التكنولوجيا الحديثة، لما له من خوارزميات وتطبيقات وتقنيات تعتمد على النظم الذكية، وله مزايا عديدة في جميع اقطاعات الاقتصادية، الاجتماعية، التعليمية والقانونية، ان القواعد القانونية مرتبطة بالتغيرات التي تطرأ في المجتمع، وهي ليست ثابتة بل متجددة حيث من خصائصها انها قاعدة اجتماعية، بمعنى أي تغير يحدث يؤثر في القواعد القانونية.

هذا ما يؤدي بتشريعات الدول في العالم للتغير لمواكبة التطور التكنولوجي السريع الحاصل، وعليه فإن للذكاء الاصطناعي تجليات عديدة خاصة في مجال العقود والقرارات.

إذ يعتبر مجال العقود من بين أهم المجالات التي ظهر فيها الذكاء الاصطناعي بوضوح وتم استخدامه فيها أولاً، كما ظهرت فكرة الحكومة الذكية بعد الحكومة

الالكترونية، وذلك من خلال قاعدة البيانات الضخمة التي يتم العمل عليها من أجل الوصول لحكومة ذكية تصدر هذه الأخيرة قرارات ذكية.

المطلب الأول :

تأثير الذكاء الاصطناعي على الأنظمة القانونية:

لما كانت التكنولوجيا في تزايد مستمر لا يمكن وقفها، مع ظهور الأنظمة الذكية التي تقوم على الذكاء الاصطناعي فإن قضية حقوق الانسان وحرياته عرفت نقاشا مهما خاصة فيما يتعلق بالمساس بحماية الحق في الخصوصية وحماية البيانات والمعطيات الشخصية وغيرها ... هذه الأخيرة التي تعتبر حق دستوري يحميه الدستور الجزائري في باب خاص اسمه الحقوق الأساسية والحريات العامة[1] .

الفرع الأول : تأثير الذكاء الاصطناعي على حقوق الانسان :

تعد حقوق الانسان من اهم الركائز التي يبنى عليها النظام القانون في دولة القانون حيث يعمل هذا الأخير على حمايتها والحد من التعسف في استخدام السلطة العامة من المساس بها ، ولعل الدستور الذي هو أسمى القوانين هو الأول في النص و تكريس حقوق الافراد حتى تكون بمعزل عن أي انتهاك لها و عدم المساس بها ، هذا على المستوى الداخلي للدول، وكذلك الأمر بالنسبة على المستوى الدولي حيث تقوم المعاهدات والاتفاقيات الدولية بالمساهمة في تنظيم حقوق الإنسان وحمايتها

[1] المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر 2020، ج.ر.ج.ج العدد 82، الصادرة بتاريخ 30 ديسمبر 2020.

مما يبعث في الافراد الاطمئنان وأن حقوقهم محمية قانون لا يمكن انتهاكها، غير أن التطور التكنولوجي الحاصل قد يطرح إشكالات في مدى انتهاكه لذه الحقوق.

أولا: اختراق الذكاء الاصطناعي للبيانات الشخصية:

إن الانتشار الواسع في استعمال التكنولوجيا أدى إلى تزايد حدة التهديدات التي يمكن ان تمس خصوصية البيانات الشخصية للأفراد في المجال الرقمي أو الافتراضي، حيث أن البيانات الشخصية لم تعد حبيسة الأوراق التقليدية بل أن كل فرد أصبح بمجرد ما يتصفح عالم الانترنت قد يقوم هذا الأخير تلقائياً بتخزين معلوماته الشخصية دون الحاجة لأخذ اذنه.

لذلك فالعالم الرقمي وتطوراته أسهم بشكل كبير في تعريض معطيات الأفراد للانتهاك سواء من خلال الإنترنت أو تطبيقات الهاتف النقال، ولا يبقى سوى جمعها وتنظيمها عبر استخدام خوارزميات ذكية تمكن من تصنيفها وتميزها لإعداد في النهاية دليل متكامل لكل فرد مع بياناته الشخصية ومراقبة تحركاته وغيرها.....

وأمام هذ الواقع اتجهت التشريعات إلى محاولة حماية حق الخصوصية في تشريعاتها مثل : التشريع الفرنسي 1978 حماية البيانات والحريات[1]، بالإضافة إلى التشريع المصري في القانون 151 لعام 2020 المتعلق بالحماية البيانات الشخصية [2] ،كما عرف الاتحاد الأوروبي البيانات الخاصة على أنها (معلومات تتعلق بشخص

[1] - La loi n°78-17 du6 /1/1978 relative a l informatique aux fichiers et aux libertes a été l une des premieres legislation en la matiere.

[2] القانون 152 لسنة 2020 المتعلق بحماية البيانات الشخصية و المنشور في ج .ر.ع 58 مكرر – سنة 63 الصادرة بتاريخ 15 يوليو 2020.

طبيعي محدد، أو يمكن تحديده بصورة مباشرة أو غير مباشرة بالرجوع إلى رقم معرف أو إلى عنصر واحد أو اكثر من عناصره التعريفية[1])، ثم صادق الاتحاد الأوروبي سنة 2016 على اللائحة العامة لحماية البيانات الشخصية للأفراد داخل الاتحاد الأوروبي (GDPR) تتضمن متطلبات قوية لرفع معايير حماية البيانات و أمنها .

غير أن الخطر بات أكبر مع كيانات الذكاء الاصطناعي حيث هذه الأخيرة التي تعتمد على قاعدة معطيات تحتوي على معلومات خاصة هائلة عن الأشخاص الذين تتعامل معهم من حيث الأسماء المهن الجنس، الحالة الصحية والتاريخ العائلي وأرقام الحسابات المصرفية[2] ...

لهذا حاول المشرع الفرنسي في قانون 78/17 في المادة الأولى منه حيث أوجب على المتعاملين مع هذه البيانات بما فيها مجال الذكاء الاصطناعي احترامه لاسيما بالنسبة للآلات الذكية ذات التخزين الرقمي خاصة في قضايا ذات الطابع التجاري، كما أن المادة السادسة منه تنص على أن معالجة المعطيات الشخصية تعتبر مشروعة إذا ما تمت بطريقة عادلة وقانونية، كاستخدامه لأغراض إحصائية أو البحث العلمي والتاريخي فهي تعتبر متوافقة مع مبدأ المشروعية، إلا أنه في المادة 7

[1]- S .L Lipovetsky et Philippe ;le droit d accès l information confronte aux données personnelles :la délicate balance des droits et libertés fondamentales .Legipresse ;2019 p 204.

[2]- محمد عرفان الخطيب، الذكاء الاصطناعي والقانون دراسة نقدية مقارنة التشريع المدني الفرنسي والقطري في ضوء القواعد الأوروبية في القانون المدني للانسآلة لعام 2017 والسياسة الصناعية الأوروبية للذكاء الاصطناعي للأنسائلات لعام 2019، مجلة الدراسات القانونية جامعة بيروت العربية، لبنان، المجلد 20، جوان 2021، ص 21

منه أكد على ضرورة أخذ موافقة المعني قبل المعالجة، ونفس الأمر بالنسبة للذكاء الاصطناعي .

إن موقف المشرع الفرنسي تم تدعيمه من قبل التوجه الحديث للتشريع الأوروبي الصادر سنة 2016 الداخل حيز التنفيذ عام 2018 المتعلق بحماية البيانات الخاصة للأشخاص الطبيعيين وتداولها، والذي يهدف إلى خلق مجموعة قواعد قانونية موحدة بين دول الاتحاد الأوروبي وتعزيز الثقة بين المواطنين والشركات في الفضاء الرقمي[1] .

فبموجبها أصبحت موافقة المستخدمين مسبقة ومكتوبة وواضحة قبل الشروع فيها، أي أن الحماية القانونية لها تتناول ثلاث محاور هي: الجمع، التحليل والتداول.

مختلف التشريعات نصت على الموافقة المسبقة بالنسبة للبيانات الشخصية لذا كان من الضرورة أن يكون الأمر نفسه بالنسبة لذكاء الاصطناعي فهو مجال حساس لابد أن تراعى فيه جانب الشفافية في الحصول على هذه البيانات والشروط المنصوص عليها قبلا (الرضا الصريح والمباشر من قبل الأفراد وتوضيح نوعية البيانات والغاية المرجوة منها وكذا طرق معالجتها وغيرها ...)[2].

[1]- بعد دخولها حيز التنفيذ 2018 قام (الناشط النمساوي ماكس سكريمس) بمتابعة شركة فايسبوك بتهمة سوء الحصول على الموافقة المسبقة للمستخدمين، كما تعرضت شركة جوجل لأول عقوبة لها سنة 2019 غرامة بـ50 مليون اورو لانتهاكها النظام الجديد لحماية المعطيات الشخصية

[2]- ظلّام عبد الكريم ، الاعتراف بالشخصية القانونية لأنظمة الذكاء الاصطناعي: ضرورة أم مغالاة؟ مجلة البحوث القانونية و الاقتصادية، المركز الجامعي لأفلو، المجلد 8, العدد 1، جانفي 2025، ص 214

وهذا رغم غياب نص قانوني خاص بها، إلا أن النصوص المذكورة سابقا كفيلة للتنظيم مجال المعطيات الشخصية بالنسبة للذكاء الاصطناعي[1].

وهذا ما أكده القرار الأوروبي المتعلق بالانسآلة 2017 ونظيره المتعلق بالسياسية الصناعية الأوروبية المتعلقة بالذكاء الاصطناعي والانسآلات 2019، حيث أكدوا على احترام مبدإ الشفافية في التعامل مع البيانات التي تستخدم في الذكاء الاصطناعي، إذ تم اقتراح العلبة السوداء التي تحتوي على جميع المعلومات المتعلقة بالبيانات المخزنة لديه ثم العمل على وضع إطار قانوني مرجعي لتعامل انترنت الأشياء مع مختلف هذه البيانات والحفاظ علي طابع السرية، بما يضمن الوصول لمنتجات آمنة ومتكيفة مع الاستخدام المقصود بها[2]، حسب القانون المدني الصادر عن الاتحاد الأوروبي 2017 يجب أن تنفذ على جميع أنواع تطبيقات الذكاء الاصطناعي معايير الخصوصية لتخزين البيانات بشكل آمن

كما أن الجزائر انتهجت نفس النهج من خلال قانون حمايات الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي رقم 07/18 الصادر بتاريخ 2018/05/10 [3] ، استنادا للمادة 4 منه فهو يطبق على كل الهيئات العمومية والخاصة التي تعنى بمعالجة المعطيات ذات الطابع الشخصي، كما نص عل انشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي من خلال المادة :22 التي

[1]- رابعي إبراهيم، الطبيعة القانونية للذكاء الاصطناعي، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 10, العدد 1,جوان 2025، ص 537

[2]- محمد عرفان الخطيب، المرجع السابق، ص 22.

[3]- القانون رقم 18-07 المؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج العدد 34، الصادرة بتاريخ 10 يونيو 2018.

تعتبر سلطة إدارية مستقلة لها الشخصية المعنوية والاستقلال المالي تخضع للوصاية المباشرة لرئيس الجمهورية مقرها الجزائر العاصمة.

ثانياً: اختراق الذكاء الاصطناعي للحق في الخصوصية:

كتب الفقيه الفرنسي ARTHUR MULLOR :أن الكومبيوتر بشراهته لجمع المعلومات على نحو لا يمكن وضع حد لها وما يتصف به من دقة ومن عدم نسيان ما يخزن فيه قد يحول حياتنا رأسا على عقب يخضع فيها الأفراد لنظام رقابة صارم ويتحول المجتمع بذلك الى عالم شفاف تصبح فيه معاملاتنا المالية وحياتنا العقلية والجسمانية عارية لأي مشاهد)، إن الحق في الخصوصية أصبح في إطار التطور التكنولوجي معرضا للاختراق والانتهاك بمعنى أن فكرة المساس بالخصوصية المادية (البيانات أو المعطيات الشخصية) قد تم تجاوزها لتمس وتستنتج بواعث وميولات الإنسان، وبالتالي تمس كيان الافراد المعنوي فيصبح انتهاك الحياة الخاصة للأفراد أكثر سهولة[1].

ولعل الحق في الخصوصية من أقدم الحقوق إلا أنه في ظل تطور الذكاء الاصطناعي وسهولة انتهاك هذا الحق أصبحت حمايته ضرورة ملحة سواء من خلال الإتفاقيات الدولية أو الإقليمية[2]، فتنامي تقنيات الذكاء الاصطناعي سيؤدي إلى

[1]- ظلّام عبد الكريم، المرجع السابق، ص 221.

[2]- المادة 12 من الإعلان العالمي لحقوق الانسان سنة 1948 التي تنص على (لا يجوز تعريض أي احد لتدخل تعسفي في حياته الخاصة او في شؤون اسرته او مسكنه او مراسلاته ولا لحملات تمس شرفه وسمعته و لكل شخص في ان يحميه القانون من مثل ذلك التدخل او تلك الحملات) ، ونفس المقتضيات أوردتها المادة 17 من العهد الدولي للحقوق المدنية والسياسية لعام 1966.

تغلغل أكثر في خصوصيات[1] الأفراد على نحو سيصبح فيه العديد من مظاهر هذه الخصوصية صيدا سهلا لغير أصحابها ،وهذا ما اتضح لنا من خلال حديثنا عن انتهاك الذكاء الاصطناعي للبيانات الشخصية الواردة أعلاه، ولا نذهب بعيد حيث يمكننا الاستدلال بانتشار فيروس كورونا المستجد المسمى COVID19، حيث سنت الدول مجموعة من التدابير الاستباقية التي تقوم بتتبع وتعقب المواطنين أينما حلوا وارتحلوا كالتطبيقات الذكية مثلا، كما قامت بتسخير انسان آلي يشخص الفيروس وحالة المصابين به من بين هذه الدول المملكة العربية السعودية من خلال الهيئة السعودية للبيانات والذكاء الاصطناعي المعروفة باختصار (SDAIA) [2]، التي تعمل على تطوير أنظمتها الأساسية للبيانات من خلال حماية خصوصية الافراد ، غير أن هذه الهيئة مع انتشار فيروس كورونا عملت على مساندة الجهود الحكومية حيث اطلقت تطبيق "تباعد"، الذي اعتمدته وزارة الصحة في اشراك الأفراد للسيطرة على تفشي الجائحة والحد من التوسع في انتشاره حيث يقوم على ارسال بيانات معروفة مموهة الى الهواتف الذكية المستخدمة للتطبيق التي سجلت خلال فترة الاختلاط[3].

[1]- مفهوم الخصوصية هو مفهوم قديم قدم الانسان يختلف باختلاف الثقافات والحضارات فنجده في الفقه الإسلامي بمفهوم "الحرمات " الذي يشير الى وجوب حفظ النفس والعرض والمال) اما الفقه الفرنسي يقصد به كل ما يتعلق بالحياة الخاصة كالعلاقة بالأبناء و الزوجة والعائلة والذمة المالية والخلوات وغيرها، وعليه هناك اعتداء على الخصوصية سواء تعلق الامر بكشف اسرار خاصة او بنشر معلومات المتعلقة برصد تحركات الفرد.

[2]- هي هيئة حكومة سعودية أنشئت بأمر ملكي مطلع 2019 ترتبط مباشرة برئيس مجلس الوزراء، يرأسها نائب رئيس مجلس الوزراء مهمتها الأساسية السهر على تطور أنظمة وحماية بيانات الأشخاص من خلال تقنيات الذكاء الاصطناعي.

[3]- رابعي إبراهيم، المرجع السابق، ص 540.

والأمر نفسه بالنسبة للدولة الامارات العربية المتحدة التي استخدمت تطبيق ذكي يسمى "الحصن"، كما عملت على إنشاء منصة افتراضية " الدكتور الافتراضي لكوفيد 19" من خلالها يمكن للأفراد تقييم الاعراض المرتبطة بالفيروس، إن اشعار المخالطين مع المصاب يؤدي إلى نفي حماية الخصوصية ويكون فيه خطورة على هذه الأخيرة إذا ما تم استغلالها في مسائل غير مشروعة[1].

وغير بعيد عن المجال الطبي نجد "خوارزميات الفيس بوك " التي تعد من بين تقنيات الذكاء الاصطناعي فكل فرد لا يستطيع استخدامها أو الدخول لها إلا بعد القيام بالاشتراك فيه، الذي يتم من خلال الإفصاح عن بعض البيانات شخصية وثيقة الصلة بخصوصية صاحبها، ومما لاشك فيه أنها لان لدى شركات الدعاية التجارية ومواقعها الالكترونية المخصصة لذلك، يمكن القول أن الحق في الخصوصية من اهم الحقوق التي لابد لكل التشريعات حمايتها من أي اختراق أو اعتداء للخصوصية في الجانب المتعلق بتقنيات الذكاء الاصطناعي، التي تعد مجالاً خصباً لذلك سواء تعلق الأمر بمعطياتهم الشخصية أو حياتهم الخاصة، وتجدر الإشارة إلى أن خوارزميات الذكاء الاصطناعي لا تنتهك فقط حقوق الانسان بل حتى حريات الافراد تلحقها انتهاكات من جراء استخدام هذه التقنيات، فرغبتنا قد تكون موجهة للقيام بعمل معين وتحقيقه لكن خوارزميات الذكاء الاصطناعي تقوم بالتصرف مكاننا دون منحنا فرصة الاختيار كما هو الشأن في ابرام العقود الذكية [2]،

[1]- ظلّام عبد الكريم، المرجع السابق، ص 220.

[2]- يطرح اشكال مهمة تتعلق بكيفية ضمان عدم التمييز بين الجنسين في برامج الذكاء الاصطناعي حيث يمكن ان تؤدي الى تفضيل جنس عن آخر أي نها قد تساهم في التميز العنصري، مما يؤدي الى خلق فوضى وتفاوتات عارمة بين مواطني نفس البلد فيحرم مجموعة من الأشخاص من هذه التقنيات الذكية فحين تستفيد مجموعة أخرى.

كما أن كيانات الذكاء لا تحتوي ضمير مما يؤدي إلى انتهاك حرية الضمير البشري فالضمير مسألة مرتبطة بقلب الانسان ولا يمكن عزلها عنه وزرعها في إنسان آلي غير عاقل يقوم بعماله بناء على برامج محوسبة ، وعليه وجب أن تكون النصوص القانونية مواجهة لكل من قام بالمساس بهذه الحقوق أو استغلالها بشكل يسيء لصاحبها[1].

ثالثاً: تأثير الذكاء الاصطناعي على مبادئ العدالة:

للذكاء الاصطناعي دور كبير في مجال العدالة الجنائية، سواء تعلق الأمر بالمساهمة في التنبؤ بالجريمة قبل ارتكابها أو القيام بمساعدة ضباط الشرطة القضائية بملاحقة المجرمين والتحقيق معهم وكذا المحاكمة الذكية، فما مدى احترام هذه الخوارزميات للمحاكمة العادلة؟ هذه الأخيرة التي تعتبر من أهم المبادئ الأساسية التي تبنى عليها دولة الحق والقانون، ومن الأهداف الكبرى التي تسعى الدول الديمقراطية لتحقيقه وبلوغه،

حيث أصبح الحق في محاكمة عادلة من أعرق حقوق الانسان وأهمها ولعل من أبرز هذه الخروقات الاعتقال التعسفي، التعذيب وانتهاك حقوق الدفاع بوجه عام، من أهم دعامات المحاكمة العادلة هي استقلالية السلطة القضائية المنصوص عليها دستوريا فضمانات المحاكمة العادلة تزرع في نفوس المحكومين نوع من الطمأنينة وتوضع ثقتهم في الجهاز القضائي العادل وهذا ما تضمنه المحاكم

[1]- قندوز فتيحة، الجوانب القانونية لاستخدام الذكاء الاصطناعي، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة .....، المجلد 09، العدد 01، 2024، ص 1175.

التقليدية، غير أن المحاكم الرقمية ونظام المحاكم عن بعد تثير الاشكال بشأن المحاكمة العادلة؟

إن المحاكمة العادلة تقوم على مبادئ أهمها: مبدأ الشرعية الجنائية: لا جريمة ولا عقوبة لا بنص، ومبدأ قرينة البراءة: المتهم بريء حتى تثبت إدانته، لكن الاشكال يطرح عند مبادئ الواردة في التنظيم القضائي وهي مبدأ الشفوية، العلنية والوجاهية:

مبدأ العلنية: لا يثار هذا الاشكال في المحاكم التقليدية حيث تمنح لكل من له اهتمام بحضور الجلسة الحق في حضورها، لكن في المحاكمة الرقمية يغيب مبدأ العلنية حيث الجهاز القضائي يكون الكتروني، والمحكمة أبوابها مغلقة والحضور غائب عن الجلسات.

مبدأ الشفوية: الذي يتأسس على المواجهة بين أطراف الخصومة الجنائية ويهدف لاحترام حقوق الدفاع والاستماع للأطراف والشهود واراء الخبراء.

مبدأ الوجاهية: بالإضافة إلى أن المحاكمة الرقمية التي مكنت من التواصل عن بعد عبر تقنية السمعي البصري من خلال امتثال المشتبه فيه أو المتهم خلف شبكة الانترنت دونما الحاجة للحضور الى قاعة المحكمة أو أمام القضاء فقد تم ضرب مبدأ الوجاهية.

للمحاكم الرقمية إيجابيات تقليص عدد الملفات المنتظرة للفصل فيها إلا أنها تنتهك مبادئ أساسية للقضاء ذكرناها سابقاً، كما أن التطور التكنولوجي أظهر لنا نوع جديد من المحاكم هو المحاكم الذكية وهي محاكم مجهزة بمعدات ذكية، كل

شيء فيها مبني على الذكاء الاصطناعي، لا وجود فيها للعنصر البشري غير أطراف الدعوى فهي عبارة عن: برمجيات وخوارزميات ذكية بما في ذلك القاضي الآلي، المحامي والنيابة العامة[1]،

برغم من عدم انتشارها في كل أنحاء العالم إلا أنه في المستقبل القريب سنشهد محاكمات تقوم على الذكاء الاصطناعي، وإذا كانت مبادئ التنظيم القضائي هي ركيزة أساسية لضمان مبدأ المحاكمة العادلة فان احترامها في مجال المحاكمة الذكية يبقى نسبيا غير أنه لا يمكن نفيها مادامت التشريعات في مختلف الدول تحاول السهر على تمتع المتهم بحقوقه[2].

لكن لابد من القول أن: المحاكم الذكية لا يمكن اعمالها في القضايا التي تمس المجتمع كالجنح والجنايات لكونها حساسة لا يمكن للإنسآلة أن يحكم فيها، لأنه لن يراعي حالاتهم ولا الضمانات المقررة له قانوناً، لذا وجب برمجت الخوارزميات بشكل يستجيب وحاجيات حقوق المتهمين، حتى لا تكون فيه انتهاكات.

رابعاً: تأثير الذكاء الاصطناعي على مستقبل العمل:

مع استخدام الذكاء الاصطناعي أكثر فأكثر في كثير من القطاعات ومعا اعتباره ثورة تكنولوجيا، وفي ظل تزايد ترابط الانسان به يرتكز القلق من الآثار السلبية المترتبة على هذا الترابط في مجال العمل من خلال تقلص فرص العمل

[1]- قندوز فتيحة، المرجع السابق، ص 1176.

[2]- د. نايف بن ناشي الغنامي، الضوابط القانونية للذكاء الاصطناعي في إبرام المعاملات القانونية، مجلة رؤى في الآداب والعلوم الإنسانية، جامعة محمد خيضر، بسكرة، المجلد 4, العدد 1، مارس 2025، ص 65.

بالنسبة للإنسان، لكون الآلة ستحل محله والقيام بمهامه أي سيتم استبدال اليد العاملة البشرية بالآلة الذكية مما يؤدي الى اختفاء بعض المهن[1] .

في الواقع سيكون قادر على القيام بالمهام المعقدة بالنسبة للإنسان، ففي القطاع المصرفي سيكون قادراً على تقديم مشورات للعملاء وفق قواعد مقررة ومحددة سلفاً، وكذا في مجال الصحة فيكون قادراً على تشخيص مجموعة من الأمراض التي يستعصي على الانسان الاقتراب منها، أو ربما يخاطر بنفسه عند الاقتراب منها "فيروس كورونا " مثلاً.

إن الذكاء الاصطناعي يستطيع أن يؤثر على الوظائف البشرية، والقيام مكانهم لأدائها لأنه يحتوي على خوارزميات لا يمتلكها الإنسان وسرعة ودقة وتكلفة أقل أيضاً؛ مما يجعل أرباب العمل يفضلون الآلة الذكية على اليد العاملة البشرية مما يساهم في زيادة نسبة البطالة، وكما اقترح" Gates Bill"مؤسس شركة "مايكرو سوفت "، أن الروبوتات لابد من أن تؤدي الضريبة التي كان يدفعها البشر كما قال عالم الاقتصاد بجامعة بيل" Robert Shiller" إن الضريبة التي ستفرض على الروبوتات حتى ولو كانت ضريبة مؤقته، فإنها قد تبطئ تطبيق التكنولوجيا وسيحدث اضطراب داخل المؤسسات كما يمكن القول أن الآلات الذكية لن تكون قادر على العمل في كل البيئات، فهي تحتاج لبيئات عمل خاصة فلا

[1]- إيهاب خليفة فرص وتهديدات الذكاء الاصطناعي السنوات العشر القادمة مقال منشور بمجلة مركز المستقبل للأبحاث والدراسات المتقدمة ع 27 لسنة 2018 ص2.

يمكن أن يعمل الروبوت فوق قمم الجبال والهضاب الصعبة وغيرها من البيئة المعقدة[1] .

كما أن الذكاء الاصطناعي يؤثر سلباً على بعض الوظائف، غير أنه بالمقابل وحسب الأستاذ " داني قزي" المتخصص في علم الأدمغة الالكترونية فإن: الذكاء الاصطناعي قد يخلق بالتأكيد فرص عمل جديدة، بمعنى أن آلية العمل وفق البرمجيات تقوم على المدخلات والمخرجات، حيث يقوم الانسان بالأولى والآلة بالثانية وفق لما يسمى بـ Outi-detect ، بناء على برمجيات معينة موجودة وعلى ما أعطيت من مدخلات وبيانات[2] .

فمن المؤكد أن فرص عمل جديدة ستظهر وهناك وظائف ستختفي لكن بالمقابل لإنسان سيبقى موجود فبالرغم من الثورة الصناعة ووجود الآلات لكن لم تلغي دور الإنسان، بل جنبته التعب والمشقة ، كذلك الأمر بالنسبة للذكاء الاصطناعي، حيث يمكن أن يكون مساعد للإنسان ولا يحل محله بل يتغير دور الإنسان مع وجود هذه الكيانات الذكية، ففي جائحة كورونا برز التعليم عن بعد لكن دور المعلم ظل على حاله لكن مكان ووسيلة التعليم هي التي تغيرت، و عليه فافي كل تطور تكنولوجي قد تتغير الأدوار لكن تظهر أدوار جديدة فالغاية الاسمى من الذكاء الاصطناعي هي الحرص على مساعدة الانسان وليس القضاء عليه[3] .

---

[1]- ضيف الله زينب . بن داود براهيم . القانون والذكاء الاصطناعي، مجلة القانون والعلوم البينية، جامعة زيان عشور الجلفة، المجلد 2, العدد 3, ديسمبر 2023، ص 371.

[2] - قندوز فتيحة، المرجع السابق، ص 1172.

[3] - ضيف الله زينب . بن داود براهيم، المرجع السابق، ص 375.

إن المجال القانوني أيضاً سيلحقه تغيرات، من جراء دخول الذكاء الاصطناعي عليه مما يؤدي الى التأثير على ترسانته القانونية والتشريعية الذي يفرض على الدول اجاد إطار قانوني لمواكبة تقنيات الذكاء الاصطناعي، بما يضمن معه احترام كافة حقوق وحريات الأفراد، وكذا وضع صيغ قانونية جديدة لتأطير تدخل الذكاء الاصطناعي في مجال العقود والقرارات الإدارية، الذي أصبح لا مفر منه في الوقت الراهن نتطرق لوجود الذكاء الاصطناعي في مجال العقود من خلال المطلب الثاني

المطلب الثاني:

دور الذكاء الاصطناعي في مجال العقود

يعد مجال العقود من اهم المجالات في حياة الانسان حيث لا يقع على عاتقه تحمل التزام غير الالتزامات العقدية أو التصرفات القانونية التي أبرمها طواعية، سواء كانت عقود مهمة أو بسيطة، كما ظهر نوع جديد من العقود هوي العقود الالكترونية.

حيث انتقلنا من العقود العادية إلى العقود الالكترونية غير أن الأمر لم يتوقف عند هذا النوع الجديد من العقود، بل بفعل التطور التكنولوجي الذي يشهده العالم أصبح لدينا كيانات ذكية تتمثل في خوارزميات وأنظمة متطورة تنافس البشر في الذكاء، تقوم بمختلف مراحل إبرام العقد وهو ما يعرف بالعقد الذكي الذي يمكن تعريفه بـ : (عقد ذاتي التنفيذ تدون فيه شروط الاتفاق بين المشتري والبائع مباشرة ضمن أسطر " الكود "، الذي يوجد بمعية الاتفاقات ضمن

شبكة موزعة و غير مركزية هي تقنية بلوك تشين[1])، التي تشبه لحد كبير العقود الالكترونية أو المبرمة عن بعد، حيث يتم إبرامها من قبل أنظمة ذكية تنتج لنا عقود متكاملة الأركان [2]

ومن هنا نتساءل عن كيفية قيامه بإبرام العقود؟ هل قواعد القانون المدني كافية للتطبيق على هذا النوع من العقود؟

الفرع الأول : ابرام العقود الذكية بواسطة الذكاء الاصطناعي

نجد أن المشرع الجزائري تطرق لتعريف العقد في المادة 54 من القانون المدني الجزائر[3] حيث نص على أنه (العقد اتفاق يلتزم بموجبه شخص او عدة اشخاص اخرين بمنح أو فعل أو عدم فعل شيء ماء) كما عرفه المشرع الفرنسي أيضا في نفس السياق، وعليه فإن أي عقد لابد من أن تتوفر فيه عنصر الإرادة والتراضي بين المتعاقدين حتى تتحقق الغاية الكبرى من ابرامه، وهو إحداث إثر قانوني معين فهل الأنظمة الذكية قادرة على إبرام العقود وزرع الثقة في العلاقات التعاقدية؟

[1]- كما يمكن ان يعرف على أنه : عقد بين طرفين ينفذ تلقائيا يقوم على فكرة الند للند " بدون وسيط" من خلال شبكة توزيع لامركزية تسمى سلسلة الكتل و يتم بالعملات المشفرة مثل البتكوين وغيرها.

[2] - نايف بن ناشي الغنامي، المرجع السابق، ص 70.

[3]- الامر رقم 75/58 المؤرخ في 1975/09/26 المتضمن القانون المدني المعدل بموجب القانون رقم 10/05 المؤرخ في 2005/07/20

إن العقد الذكي يرتبط بمنصة افتراضية يطلق عليها سلسلة الكتل[1]، وتعتمد على التكنولوجيا الرقمية في ضبط جميع المعاملات والتصرفات، كما تقوم بحفظ الاشتراطات والمفاوضات وكل العمليات التي تنعقد بين الأطراف في العالم الافتراضي سواء كان تعاقد نيابي أو بصورة ذاتية.

أولا :ابرام العقود الذكية عن طريق النيابة:

النيابة في التعاقد هي عبارة عن: نظام قانوني يطلب بواسطته شخص يسمى المنيب من شخص آخر يسمى المناب بأن يقوم بتصرف ما أو يلتزم بهذا التصرف لمصلحة شخص آخر يسمى المناب لديه.

بمعنى آخر النيابة في التعاقد: تصرف قانوني تحول آثار التصرف المناب فيه إلى الأصيل ، كما يمكن تعريفها بشكل مبسط على أنها :حلول إرادة النائب محل إرادة شخص آخر وهو الأصيل في إبرام تصرف قانوني تنصرف آثاره إلى ذمة الأصيل، غير أن تطور طبيعة التعاملات وانتقال الأشخاص من العالم المادي المحسوس إلى العالم الافتراضي، تم إيجاد برمجيات إلكترونية حاسوبية تسهل العمل في العالم الافتراضي ويكون باستطاعة المتعاملين أن يفوضوا أعمالهم وتصرفاتهم إلى هذه البرمجيات،

[1]- سلسلة الكتل عرفها قاموس المعلوماتي بانها طريقة لتسجيل البيانات ذات النشوء المستمر في شكل كتل يرتبط بعضها ببعض ضمن ترتيب زمني للتحقق منها ويكون كل من الكتلة وتسلسلها محمي ضد أي تحيز بمعنى أنها تستعمل بالدرجة الأولى في مجال العملة السيبرانية بحيث تشكل سجل عاما للعملات.

التي ستتعامل معها بشكل ذاتي ومستقل مع بيئتها المحيطة للعمل واكمال مهمتها بنجاح[1].

لا يوجد أي اشكال وغموض بخصوص حلول خوارزميات الذكاء في التعاقد بالنيابة ، بمعنى ان الأنظمة الذكية ستكون عبارة عن وكيل ذكي [2]، عن المصمم أو المالك في ابرام التصرف القانوني حيث تتصرف كوكيل عادي في شكل معاملات الكترونية، نلاحظ تكرار مصطلح الوكيل الذكي لذا لابد من التطرق لتعريفه، وهو محل جدل فقهي لم يتوصل إلى اتفاق حوله حيث هناك من يعرفه بانه: (برنامج الكتروني معد ليتصرف نيابة عن شخص معين) أو هو (برنامج من برامج الحاسوب الآلي يتميز بخصائص الاستقلالية والقدرة على التعامل مع غيره من البرامج او الأشخاص والقدرة على رد الفعل والمبادرة) .

لكن هذه التعريفات ارتكزت إما على علاقته بالمالك أو المصمم أو بناء على خصائصه المميزة له عن الوكيل العادي، لذا حاول الأستاذ Krupanski وضع تعريف شامل له: (هو عبارة عن برنامج حاسوبي يعمل على تحقيق اهداف معينة في بيئة ديناميكية، حيث يكون التغيير فيها طبيعيا نيابة عن كيانات أخرى حاسوبية أو بشرية، خلال فترة زمنية ممتدة من الزمن ودون إشراف وسيطرة مباشرة ومستمرة ،

[1]- احمد قاسم فرح، استخدام الوكيل الذكي في التجارة الالكترونية دراسة قانونية مقارنة في اطار ماهيته ونفاذ تصرفه، مجلة المفكر، جامعة محمد خيضر، بسكرة، المجلد 13، العدد 2، 2018، ص 15.

[2]- مختلف حول تسمية الوكيل الذكي فهناك من سماه الانسان الآلي ونظام المعلومات، الوكيل الذكي والالكتروني الأكثر شيوعاً.

ويظهر درجة كبيرة من المرونة وحتى الإبداعية في كيفية التي يسعى بها إلى تحويل الأهداف إلى مهمات)[1].

من خلال هذا التعريف يلاحظ أن مهمة الوكيل الذكي تنحصر في تحقيق مجموعة من الأهداف والتي تكون مبرمجة عبر برنامج حاسوبي ويقوم بالتصرف فيها بطريقة النيابة وبإبداعية واحترافية بدون أي تدخل بشري، حيث يكون مستقل بذاته، غير أن هذا التعريف أغفل هو الأخر دوراً مهما يقوم به الوكيل الذكي، والمتمثل في القدرة على الاتصال والتفاعل مع مستخدمه ومع الغير من الوكلاء الأذكياء كانوا أم بشر[2].

كما يمكن الإشارة إلى بعض التشريعات التي عرفته كالتشريع الأردني ضمن قانون المعاملات الالكترونية رقم 85 سنة 2001 والذي عرف الوسيط بأنه " برنامج الحاسوب أو أي وسيلة الكترونية أخرى تستعمل من أجل تنفيذ إجراء أو الاستجابة لإجراء بقصد إنشاء أو إرسال أو تسلم معلومات دون تدخل شخصي" ، أما المشرع الاماراتي فقد عرفه بأنه : برنامج أو نظام إلكتروني لوسيلة تقنية المعلومات التي تعمل تلقائيا بشكل مستقل دون اشراف من أي شخص طبيعي في الوقت الذي يتم فيه العمل أو الاستجابة له، هذين التشريعين في المضمون تحدثا على الوكيل الذكي لكن استخدما مصطلح الوكيل الالكتروني[3].

[1]- أحمد قاسم فرح، المرجع السابق، ص 17 .

[2]- ضيف الله زينب . بن داود براهيم، المرجع السابق، 380.

[3]- المادة 1 من القانون الاتحادي رقم 1 لسنة 2006 بشأن المعاملات والتجارة الالكترونية .

بالرجوع إلى قانون الاونيسترال النموذجي في المادة 12 منه نجده عرفه على أنه: (في العلاقة بين المنشئ والمرسل إليه تعتبر رسالة البيانات أنها صادرة عن المنشئ إذا أرسلت من نظام معلومات مبرمج على يد المنشئ أو نيابة عن العمل تلقائيا ...)، وفي هدا إشارة صريحة لنظام الوكيل الذكي.

وفي نفس الصدد ذهب المشرع الفرنسي إلى الاعتراف بالوكيل الذكي بطريقة غير مباشرة من خلال اجازته للتصرفات التي تتم عبر الوسائل والسجلات الالكترونية.[1]

بالنظر للخصائص التي يتمتع بها الوكيل الذكي يمكن القول أنه: لا مانع في ابرامه للعقود الذكية مادام أن له رؤية اجتماعية من خلال القدرة على الرد والتكييف مع بيئته وقابلية التغيير بشكل مستمر وفق لرغبات أو سلوك المستخدمين،

كما أن العلاقة المشتركة بين العقود التقليدية والالكترونية والذكية هي الايجاب والقبول، لذا فالوكيل الذكي ما هو إلا أداة لتعبير عن إرادة مستخدمه، وعليه يمكن إعمال القواعد العامة للعقد في القانون المدني خاصة ما تعلق بالوكالة في العقود، كما أن ابرام العقود الذكية لا يحتاج الاعتراف لهذه الكيانات الذكية بالشخصية القانونية لأنها لا تبرم العقود هنا بصورة مستقلة، بل تبرم باسم ولحساب شخص طبيعي أو معنوي معترف به وآثارها تؤول للموكل.

[1]- القانون المتعلق بالثقة في الاقتصاد الرقمي لسنة 2004 المواد من 1108 الى 1369 من القانون المدني الفرنسي.

ثانياً: إبرام العقود الذكية بصورة مستقلة:

إذا كانت خوارزميات الذكاء الاصطناعي يمكن أن تبرم العقود بالنيابة كما سبق التطرق لها، فليس هناك ما يمنع من أن تقوم هذه الخوارزميات بنفسها وبصورة مستقلة في ابرام العقود، مادام أن العقد ينشأ عن توافق ارادته الحرة إما بشكل صريح أو ضمني.

وحتى تقوم هذه الخوارزميات بإبرام العقود لابد من أن يتم مراعاة الأركان الأساسية للتعاقد من: رضى المحل والسبب، لأن ركني المحل والسبب يمكن اعتبارهما في مجال الذكاء الاصطناعي مثلها مثل العقود التقليدية بعد استيفاء شروطهما[1]، لكن التراضي هو ما يخلق تساؤل حول إذا ما كانت تقنيات الذكاء الاصطناعي قادرة على التعبير على ارادتها الحرة في ابرام العقود؟؟

الإجابة على هذا التساؤل تقتضي معرفة أنواع العقود التي تبرمها تقنيات الذكاء الاصطناعي والتي لا تخرج في مجملها عن كونها اما:

1-1**عقود مساومة حرة** : حيث يستدعي بالضرورة ان تدخل تقنيات الذكاء الاصطناعي في تفاوض مع الطرف الاخر، أي أن كلا الطرفين يقومان بالدخول في مناقشات ومفاوضات بشان الإتفاق على بنود العقود ليتم في الأخير ابرام العقد بشكل صحيح ، في هذه الحالة قد تشكل خطورة كبيرة لعدم معرفة هذه الانظمة لأبعاد اتخاذ القرارات، حيث لا تمتلك القدرة على التفاوض والتمييز بين ما يقع وما

[1]- يشترط في المحل ان يكون موجود او قابل للموجود في المستقبل ان يكون مشروع و قابل للتعامل فيه ، وان يكون معينا او قابل للتعين وان يكون ممكن لا مستحيل . السبب : يكون موجود حقيقي و مشروع.

يضر ، وما مجال الربح والخسارة المتوقع هنا[1] ، لذا فمجال التعبير عن ارادته محدود جداً.

2-1 **ذات النطاق الضيق** : يتضح أن الغرض من هذه الأنظمة الذكية هو أداء مهمة معينة و ليس التمتع بقدر كافي من الاستقلالية والتعبير عن ارادتها في عقود المساومة، فقد يكون وكيل ذكي ينوب فقط عن مصممه أو مالكه ، لكن الأمر مختلف في مجال الذكاء الاصطناعي الفائق فهذه الحالة بالذات تكون هذه التقنيات لها القدرة الكافية في التمتع باستقلالية ابرام العقود، والتفاوض مع الأطراف سواء كانوا آليين أو بشراً من أجل عقد من العقود ، علاوة على ذلك فقد يكون المصمم أو المبرمج برمجها بقدرات لامحدودة وبرمجيات، عالية تساعدها على انجاز مهامها دون الحاجة لتدخل بشري بعبارة أخرى انها في الأصل ستكون لها القدرة على القيام بنفس المهام التي يقوم بها الإنسان[2] .

أما في عقود الإذعان : هذه العقود فيها طرف قوي وآخر ضعيف، الأول يفرض شروط تعسفية على الثاني ، والعقد يكون معد مسبقاً، فلا يبقى على الطرف الآخر إلا التوقيع عليه أو تركه .

فإذا كانت تقنيات الذكاء الاصطناعي فائقة الذكاء: تتمتع بالقدرة على التفاوض وإبرام العقد كالإنسان، فإنه في نطاقها العام والضيق لا تمتلك هذه الميزة،

[1]- أحمد علي حسن عثمان، انعكاسات الذكاء الاصطناعي على القانون المدني دراسة مقارنة ، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 76، 2021، ص 1572.

[2]- أحمد قاسم فرح، المرجع السابق، ص 17 .

الشيء الذي يوحي تماماً إمكانية ابرامها للعقود الاذعان، لكونها لا تعتمد هنا على المناقشة والتفاوض قبل الابرام.

الأمر الذي يدل دلال صريحة على أن تقنيات الذكاء الاصطناعي سيكون لها مجال رحب وفعلي في عقود الإذعان، وهو ما يأخذنا للقول أن أنظمة الذكاء الاصطناعي هذه ستعتمد على عقود نموذجية معدة مسبقا لا يبقى معه للأطراف مجالاً لمناقشتها، بل ستقتصر فقط على التوقيع والرضى بها، من خلال ما سبق يمكن القول أن هذه التقنيات الذكية قادرة على إبرام العقود الذكية يستوي في ذلك أن تكون إما عبارة عن عقود تفاوضية، إذا ما توفرت الخوارزميات على برمجيات فائقة الذكاء، وعقود اذعان نموذجية معدة مسبقاً، غير أن ركن التراضي هنا يجد مسعاه في النوع الأول دون الثاني، لأن الأطراف المتعاقدة تكون في نفس الميزان في العلاقات التعاقدية بينهما[1].

وبالنظر للفراغ التشريعي الحالي فيمكنها ابرام العقود وفق قواعد العامة للقانون المدني الفرق يكمن فقط في الوسيلة المعتمدة.

ثالثاً: الذكاء الاصطناعي ومرحلة ما بعد الابرام:

عندما يستجمع العقد كافة العناصر اللازمة لنشوئه وفقا لما قرره القانون، فإننا نكون أمام عقد صحيح ملزم لأطرافه في حدود ما تم الاتفاق عليه في صلب العقد، وهذا ما يعرف بالقوة الملزمة للقعد.

[1]- ضيف الله زينب . بن داود براهيم، المرجع السابق، 382.

1. اسهام تقنيات الذكاء الاصطناعي في تنفيذ العقد:

اسهامات تقنيات الذكاء الاصطناعي في ابرام العقد لا تتوقف في مرحلة الابرام فقط بل تتعداه الى مرحلة التنفيذ ، خاصة في العقود الذكية لأنها محوسبة، رغم غياب النص التشريع الخاص بهذه العقود كما هو الشأن بالنسبة للعقود الالكترونية التي لم يتصورها المشرع بمعزل عن القواعد العامة، رغم أنه خصها بقواعد خاصة، تقنيات الذكاء الاصطناعي لها دور مهم في مرحلة تنفيذ العقد حيث تقوم بضمان وفاء كل طرف من الأطراف المتعاقدة بالتزامه قبل إتمام نتائج التعاقد او مبادلة القيمة المتعاقد عليها، فدورها يعزز أكثر فأكثر أثناء السهر على التنفيذ، وأن يتم تنفيذ كل ما اتفق عليه أثناء إبرام العقد، فالعقد الذكي يعد عقد ذاتي التنفيذ لان التزاماته يتم تنفيذها دون تدخل كامل من الأطراف المتعاقدة ،بالاعتماد على منصة سلسلة الكتل BLLOCKCHAINE التي تختص احدى كتلها لتسجيل وتخزين المعطيات المعلوماتية[1] ، المتعلقة بالعقد الذكي والمتضمنة لشروط التعاقد، بحيث عملية التخزين هذه تصبح بعيدة كل البعد عن التحريف أو اخلال المتعاقدين بالتزاماتهم، فبمجرد إتمام الشروط يتم تنفيذ الآداءات العقدية المتفق عليها بشكل ذاتي بواسطة العقد الذكي بطريقة الند للند[2] .

يمكن القول أن العقد الذكي بمجرد ابرامه فإن تنفيذه لا يعتمد على تدخل طرف ثالث ولا يتطلب أي موافقة، أو إجراءات إضافية بحيث يصبح ملزم للجميع.

[1]- داود منصور، عبد القادر زرقين، العقود الذكية المدمجة في البلوك تشين – بداية نهاية العقود التقليدية – المجلة الجزائرية للعلوم القانونية والسياسية،2022، جامعة الجزائر 01، مجلد 59، عدد 1، 2022، ص 535..

[2]- أحمد علي حسن عثمان، المرجع السابق، 1577.

كما تجدر الإشارة إلى أن العقد الذكي ينفذ حتى إن تم خارج تقنية "تشين" فهو يتيح إمكانية برمجة الرموز التي سيتم تنفيذها تلقائيا دون حاجة إلى وسيط، ولا تتوقف على العقد الذكي فقط بل تتعاده إلى العقد التقليدي والالكتروني، وبتالي مجال الذكاء الاصطناعي يعد مجالاً خصباً يحتوي على برامج متطورة تسهل أداء مهامه بالطريقة التي أعدها مصممه او مبرمجه.

في ظل غياب نصوص قانونية تعزز دورها الإيجابي هذا تبقى القواعد العامة لتنفيذ العقد هي المطبقة وكذا الامر بالنسبة للإخلال بالالتزام تحكمه القواعد العامة للتشريع المدني.

2. **استخدام تقنيات الذكاء الاصطناعي في مراجعة العقود:**

يتميز بالدقة والسرعة في مراجعة العقود أكثر من البشر حيث تشير دراسات نشرت على موقع " لوجيكس" إلى أن معدل المراجعة بمتوسط دقة بلغ معدله 94 % في مواجهة مجموعة من البشر المحامين الذين بلغ نتوسط دقتهم 85% لمراجعة خمس اتفاقيات في أجل شهرين، في حين كان مستوى سرعته 100% مقابل 97% أمام محامي فرد لعقد واحد، فهنا يتعذر على البشر مواكبة سرعة عمل التقنيات الذكية، لأنن مهمة مراجعة العقود تسند في الغالب للمحامي، لكن في المستقبل يمكن أن تسند لتقنيات الذكاء الاصطناعي[1].

مما تقدم يتضح دور الأنظمة الذكية في مجال العقود؛ كما يمكن لقواعد القانون المدني الحالية أن تنظمه وتطبق عليه، مادام لا توجد نصوص خاص بالذكاء

[1]- داود منصور، عبد القادر زرقين، المرجع السابق، ص 540.

الاصطناعي في هذا المجال، هذا فيما يخص العقود أما ما يتعلق بالذكاء الاصطناعي والقرار الإداري الذكي نتطرق له في المطلب الثاني.

المطلب الثالث :

القرار الإداري و الذكاء الاصطناعي

تطور الذكاء الاصطناعي يجعل منه مطلبا أساسيا للإدارة العامة خاصة فيم تعلق باختزال الوقت والجهد وتطور نشاطها، وهو الحاصل في الوقت الراهن بفضل ظهور كتل البيانات الضخمة والمعالجة الخوارزمية للمعطيات الكبرى، سمح بإدخال تطبيقات الذكاء الاصطناعي للإدارة العامة بعد الإدارة الالكترونية، أصبح لدينا الإدارة التي تعتمد على الخوارزميات في العديد من نشاطاتها مثل الإعلان الآلي للمناقصات واختيار أفضل العروض في مجال العقود الإدارية، أما في مجال الضبط الإداري فالخوارزميات تساعد بكفاءة عالية في أجهزة الضبط الوقائي، من خلال تحليل البيانات المتوفرة على الانترنيت وتقديم معلومات مبكرة عن تهديدات ممكنة للنظام العام[1] .

وعليه السؤال المطروح هنا: هل يخضع لنفس القواعد القانونية التقليدية للقرارات الإدارية؟ ام انه يستلزم تحيين للتشريعات وللنظريات ذات الصلة؟

[1]- بن صاري رضوان، تطبيقات الذكاء الاصطناعي في مجال القانون، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، المجلد 17, العدد 1, جانفي 2025، ص 30.

الفرع الأول : تعريف الإدارة العامة الذكية (الحكومة الذكية)

ظهور الإدارة العامة الذكية جاء بعد الإدارة العامة إلكترونية، حيث لا يمكن الوصول للإدارة عامة ذكية دون إدارة عامة الكترونية، هذه الأخيرة التي بنت قاعدة معطيات كبيرة يمكن من خلالها تجسيد الإدارة الذكية.

كما يمكن تعريف الإدارة العامة الذكية على أنها: تقدم خدمات للمستفيدين بالتكامل مع جهات الكترونية أخرى للحصول على البيانات اللازمة لتقديم خدمات بشكل أفضل، حيث تقوم بربط شامل لجميع خدماتها مع بعضها البعض، وذلك من خلال الاستعلام التلقائي على بيانات المستفيد بدل من طلبها منه مما يزيد في دقة المعلومات وسرعة تنفيذها[1] .

كما نجد أن الإدارة العامة الذكية (الحكومة الذكية): لها دور فعال في دفع عجلة التنمية وتعزيز الاقتصاد الوطني وزيادة الإنتاج المحلي، لكن لابد عند تطبيق الحكومة الذكية رفع درجة الأمن المعلوماتي والبرامج الامنية الخاصة بالأجهزة الذكية، وذلك لحماية البيانات من القرصنة والهجمات الالكترونية.

***التحول للإدارة عامة الذكية**: إن هذا التحول هو أمر فرض نفسه على واقع الكثير من الحكومات نتيجة سرعة التطور التكنولوجي، يقوم هذا التحول أساساً

[1]- ضيف الله العتبي، السعودية الحكومة الذكية مرحلة ما بعد الحكومة الالكترونية ، الجهة السعودية للمبرمجين، دون سنة نشر، ص 2.

على مقومات أهمها الانترنت من أجل الربط مع قناة التكامل الحكومية، كما تتطلب وجود رقمنه عبر كامل تراب أي دولة وفي كل مناطقها الحضرية والريفية[1].

الفرع الثاني : الذكاء الاصطناعي والحفاظ على النظام العام :

من بين مهام الإدارة العامة الضبط الإداري الذي يعد من أهم مجالات نشاط الإدارة العامة، فإن العملية فيها جانب هام متعلق باليقظة الالكترونية للحفاظ على النظام العام، لذا وجب على الإدارة العامة تغير مفاهيم الضبط الإداري بالانتقال من مفهومه التقليدي الى المفهوم الالكتروني، انتقالاً مدروسا يجنب الإدارة مخاطر الذكاء الاصطناعي سواء باستعماله كوسائل ضبط: (الأنظمة اليقظة أو أنظمة الاستشعار) أو استعماله من طرف المواطنين أو حتى الدول الموازية .

ممارسة الإدارة لوظيفة الضبط الإداري تنعكس على الحريات العامة للأفراد حيث هناك صلة وثيقة بين الحريات العامة والضبط الإداري، لذا وجب توخي الحذر في الاتجاه نحو الإدارة الذكية والقرارات الخوارزمية.

أولاً: مفهوم القرار الإداري الخوارزمي : لابد من تعريف الخوارزميات قبل تعريف القرار الاداري الخوارزمي

الخوارزميات هي: نوع خاص من التعليم الالي تحاكي الشبكات العصبية فيها أسلوب الدماغ البشري في الحساب والتعلم والتنبؤ، تأخذ من الناحية الهندسية شكل المصفوفة، مترابطة بشكل كثيف من خلال عدد هائل من الروابط الشبيهة

[1]- بن صاري رضوان، المرجع السابق، ص 33.

بالمشابك، يعمل التعلم العميق على ضبطها وتقويمها لتحسين أدائها ومن ثمة تدريبها على اتخاذ القرار ويطلق عليها " بيانات التدريب "[1].

كما تعرف بأنها: عبارة عن مجموعة من التعليمات المتسلسلة المصاغة بلغة رياضية والتي تستخدم إما لحل مشكل بشكل آلي، أو الحصول على نتائج ما، بهدف توظيفها العملي يتم دمج تلك التعليمات، بعد تحويلها للغة برمجة، ضمن أجهزة ذكية (الحاسوب) ذات قدرة معالجة كمية تتجاوز قدرة الانسان[2].

بناء عليه تعد الخوارزميات بمثابة ملف مشفر ناجم عن تحويل بيانات الادخال إلى مخرجات من خلال تحليل بيانات التدريب، فالخوارزميات هي التي تعمل على اكتشاف الارتباطات بين هذه البيانات باستخدام الشبكة العصبية فيها على نحو مماثل للإدراك البشري.

فالقرار يعتبر من بين الأنشطة الإدارية التي يمكن أن تستفيد من نظام الخوارزميات بما يختزل على الإدارة جهد ووقت، وذلك من خلال تفويض عملية اتخاذ القرار للكمبيوتر وفقاً لمراحل محددة تبدأ بـ:

المرحلة الأولى : تخزين كمية هائلة من المعطيات المستعملة في اتخاذ القرارات مثل: (بيانات الهوية، نتائج المسار العلمي والوظيفي، وضعه اتجاه المصالح الضريبية.....الخ)

[1]- كوثر منسل،حميد شاوش، الإشكالات القانونية لاعتماد القرار الإداري الخوارزمي، مجلة الرسالة للدراسات والبحوث الإنسانية، جامعة العربي التبسي، تبسة، المجلد 6، العدد 4، 2021، ص 808 .

[2]- آيت عودية بلخير محمد، القرار الإداري الخوارزمي مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تامنغست، المجلد 9، العدد 3 2020، ص 17.

المرحلة الثانية: تتم هندسة نظام الخوارزميات للقيام بعملية الاختيار بناء على قاعدة معطيات كبيرة ووفقا لما تقتضيه النصوص القانونية السارية المفعول.

المرحلة الثالثة: فإن البرنامج يتولى عملية اتخاذ القرار من خلال اختيار أفضل البدائل الممكنة. مثل استخدام برامج الخوارزميات في عمليات الترقية الوظيفية، حيث يستلزم الأمر تقليدياً قيام الجهة المختصة بالترقية بالمفاضلة بين أكثر من موظف من حيث درجة الكفاءة بعد دراسة ملفات كل الموظفين وتحيين الشهادات المتحصل عليها وغيرها كعدد سنوات الخبرة ، لكن باستخدام نظام الذكاء الاصطناعي في اتخاذ القرار الإداري أصبح من الممكن اختصار الجهد والزمن عبر تولي الحاسوب اتخاذ القرار الأمثل بناء على تحليل المعطيات السابقة والاختيار من بين البدائل المتوفرة، بطريقة آلية دقيقة وسريعة ، دون مؤثرات بشرية كمحسوبية والتعسف .

مما تقدم يمكن أن نعرف القرار الإداري الخوارزمي على أنه: قرار اداري متخذ بواسطة نظام معالجة خوارزمية معتمد من طرف الإدارة العامة لهذا الغرض[1].

أو نعرفه بانه[2]: آلية حسابية مبنية على قواعد ونماذج إحصائية تتخذ قرار بشكل مستقل دون تدخل بشري، فهو نتيجة لمعالجة يجريها نظام يجمع بين جمل خوارزمية وأجهزة الذكاء الاصطناعي التي تتولى اتخاذ القرار بناء على معطيات مقدمة مسبقاً.

[1]- آيت عودية بلخير محمد، المرجع السابق، ص 18.

[2]- كوثر منسل، حميد شاوش، المرجع السابق، ص 808.

كما يمكن التميز بين القرار الإداري الخوارزمي والقرار الإداري الالكتروني:

حيث يعرف هذا الأخير بأنه: (وثيقة الكترونية تعبر عن الإرادة المنفردة والملزمة للإدارة بقصد ترتيب أثر قانوني معين)، كما يعرف أيضا بأنه (تعبير الإدارة عن ارادتها بتغير مركز قانوني أو إلغائه أو إحداث مركز قانوني جديد من خلال قرار يصدر ويوقع بشكل الكتروني، كما يبلغ للمعني بطريقة الكترونية أيضا)؛ بناء على ما سبق نجد أن القرار الإداري الالكتروني يركز على[1]:

- **الجانب الشكلي والإجرائي**، خلافاً للقرار الإداري الخوارزمي الذي لا يستلزم بالضرورة أن يصدر في شكل أو ضمن إجراء معين، بل يكمن الجوهر فيه في اتخاذ نتيجة المعالجة السابق ذكرها، ويستوي أن يحمل توقيعاً يدوياً أو إلكتروني، كما يمكن أن يبلغ الطرف المعني به بطريقة الكترونية او تقليدية.

ثانياً: أركان القرار الإداري الخوارزمي : إن اعتماد أنظمة المعالجة الخوارزمية في اتخاذ القرارات الإدارية يؤدي إلى ضرورة تكييف النظام القانوني الذي يحكمها، بما يتناسب وخصوصية هذا النوع المستحدث من القرارات، بما في ذلك مسألة أركان القرار والتي تتصدر الاولوية في الاستفادة من التكييف وسنتناول هذه الجزئية بإيجاز على النحو الموالي :

1 - الأركان الشكلية: تتمثل في ركن الاختصاص، وركن الشكل والإجراءات.

[1]- كوثر منسل، حميد شاوش، المرجع نفسه، ص 809.

- **ركن الاختصاص في القرار الخوارزمي الإداري:**

إن إلتزام الإدارة باحترام قواعد الاختصاص قائم ومستمر في ظل نقل أعمالها للواقع الجديد وتطبيقها لنظام الإدارة الالكترونية، لأن فكرة الاختصاص واجبة بالنسبة للقرار أياً كان موطنه وبغض النظر عن كيفية صدوره.

بالنسبة للقرار الإداري الخوارزمي[1] : فإن الاختصاص بشأنه ينعقد للجهة المشرفة والمديرة لنظام المعالجة الخوارزمية للاتخاذ القرار، ويتحدد هذا الاشراف اما بناء على النصوص القانونية السارية بالنسبة للقرارات الإدارية التقليدية، أو بناء على نصوص جديدة تحدد الهيئة أو الشخص المنوط به الاشراف على سير نظام المعالجة، مثل قرارات التوجيه الجامعي التي تتم من خلال الأنظمة الخوارزمية، يكون الاختصاص فيها للجهة المشرفة على سير هذا النظام ، فإذا عينت القوانين أو اللوائح وزارة التعليم العالي كجهة مختصة بذلك القرار يصبح قرار التوجيه الصادر عن الجامعة معيب بسبب عدم الاختصاص[2].

- **ركن الشكل والإجراءات في إقرار الإداري الخوارزمي:**

لا يستلزم القرار الإداري الخوارزمي بطبيعته شكل الكتروني، أو توقيع للإجراءات وإلا إذا نصت القوانين واللوائح على ذلك، أو رأت الإدارة وفقاً لسلطتها التقديرية أن تعتمد شكليات أو إجراءات الكترونية ليجتمع في هذه الحالة الطابعين الخوارزمي والالكتروني في قرار إداري موحد.

[1]- آيت عودية بلخير محمد، المرجع السابق ص 20.

[2]- بن صاري رضوان، المرجع السابق، ص 34.

يمكن القول أن ركن الشكل والإجراءات :يقتضي أن تكون المراحل المتبعة في صنع القرار الإداري الخوارزمي خاضعة لمبادئ المشروعية الإدارية، لضمان ما يعرف "بالضمانات الإجرائية" أو "الانصاف الاجرائي" • والتي تقتضي شفافية كل الإجراءات، في حين يستوي أن يصدر القرار ويبلغ بطريقة الكترونية أو بالطريقة التقليدية كما سبق بيانه.

أما من الناحية التقنية فان عملية اتخاذ القرار الإداري وفقاً لنظام المعالجة الخوارزمي يستوجب إجراء تحويل الكتروني للتعليمات الخوارزمية، بالإضافة للإدخال الحاسبي للمعطيات والمعلومات اللازمة، وذلك سواء من طرف المرفق أو من طرف عون إداري مختص بذلك.

2- الأركان الموضوعية للقرار الإداري الخوارزمي: تعتبر أهم مواطن تميز القرار الإداري الخوارزمي وهي تشمل كل من: السبب، المحل والغاية، نتطرق لها كما يلي:

2-1: ركن السبب :

السبب هو: الحالة الواقعية أو القانونية السابقة على القرار والدافعة إلى تدخل الإدارة لاتخاذه[1] فإن صدور قرار الإداري وفقاً لنظام المعالجة الخوارزمية؛ يستلزم ادراج تفاصيل وشروط الحالة الواقعية أو القانونية الدافعة لإصدار القرار ضمن مدخلات الخوارزمية، وعملياتها واحتمالاتها الممكنة.

• يقصد به : أن تكون الإجراءات القانونية عادلة وغير متحيزة ونزيهة.

[1]- آيت عودية بلخير محمد، المرجع السابق ص 21.

مثل اخضاع قرار منح استفادة من مسكن اجتماعي للمعالجة الخوارزمية: فالمدخلات في هذه الحالة تكون :الشروط القانونية للاستفادة من هذا القرار المتمثلة في) :الطلب، شهادة سلبية، كشف راتب، الحالة الاجتماعية...) وتكون العملية المطلوبة هي توفر هذه الشروط مجتمعة، مع وضع كافة الاحتمالات الممكنة مثل : نقص الملف او عدم تناسب الراتب مع العتبة المحددة، والقرار المترتب عن كل حالة.

2-2 ركن المحل في القرار الإداري الخوارزمي:

محل القرار الإداري الخوارزمي هو: نتيجة المعالجة الخوارزمية والتي تكون محددة مسبقاً ضمن متغيرات المدخلات والمخرجات، أين يتم الالتزام الحرفي بالتعليمات التي صيغت بها الخوارزمية، فهي لا تملك إمكانية التفسير عندما تكون السلطة مقيدة، وبذلك يكون المبرمج للخوارزمية ملزم باحترام مقتضيات المشروعية من خلال الفهم الصحيح للنصوص القانونية[1].

أما في حالة السلطة التقديرية التي تتمتع بها الإدارة العامة في محل القرار: فإنه مالم يتم التمكن من تحويلها لاحتمالات في الجملة الخوارزمية فإنها ستظل ضمن نطاق تدخل العنصر البشري[2].

3-2 ركن الغاية في القرار الإداري الخوارزمي:

المعلوم أن تحقيق المصلحة العامة هو الهدف من اتخاذ القرار الإداري؛ والتي تتحقق بالإرادة الواعية للإنسان، فلا يمكن الحديث حالياً عن إرادة مستقلة لنظام

[1]- كوثر منسل، حميد شاوش ، المرجع السابق ص 809.

[2]- داود منصور، عبد القادر زرقين ، المرجع السابق ص 520.

المعالجة الخوارزمية، وبالتالي يمكن القول أن غاية القرار الإداري الخوارزمي تحدد في مرحلة تصميم وبرمجة نظام المعالجة من طرف العنصر البشري[1].

ثالثاً: ضوابط القرار الإداري الخوارزمي:

إن استغلال المعالجة الخوارزمية في اتخاذ القرار الإداري بالرغم مما يضفيه عليه من دقة وفعالية إلا أنه يظل بحاجة لضوابط قانونية؛ تضمن حقوق المواطن المتعامل مع الإدارة، في مقدمتها تأتي الشفافية ثم المسؤولية نتطرق لها فيما يلي:

1. الشفافية:

على عكس الأحكام القانونية التي تعد في متناول الجمهور نسبياً غالباً ما تظل خوارزميات القرارات الإدارية مخفية داخل أنظمة أجهزة الكمبيوتر، مما يجعل امر فهمها وتقييم تطابقها مع القانون أمر بالغ الصعوبة بالنسبة للمواطنين العاديين عند التعامل مع الإدارة.

من حق المواطن أن يفهم ويعلم المقومات التي تتخذ على أساسها القرارات التي تتعلق به ؛من أجل ذلك نصت القوانين على حق اعلام المواطنين بالمعلومات المتعلقة بالخوارزمية المستعملة في اتخاذ القرارات الفردية ، مثل القانون الفرنسي " قانون الجمهورية الرقمية في مادته 6 التي قضت : بتتميم قانون العلاقة بين الإدارة والمواطن بالمادة 3-1-312 L والتي جاء فيها : مع مراعاة الاسرار المحمية بموجب الفقرة الثانية من المادة 5-311 Lافانه على الإدارات ... أن تنشر عبر الانترنيت القواعد التي تحدد المعالجة الخوارزمية المستعملة في أداء مهامها عند اتخاذ

[1]- آيت عودية بلخير محمد، المرجع السابق، ص 22

القرارات الفردية، حتى لا تتحول الخوارزميات لصناديق سوداء للإدارة في المستقبل ، وهذا ما يجانب مبدأ الشفافية في العمل الإداري[1].

2. المسؤولية :

لمواكبة الإدارة العامة لتطور الذكاء الاصطناعي عموماً وللتطبيقات الخوارزمية يضع على عاتقها مسؤوليات متعددة لضمان الاستغلال الأمثل والآمن لهذه التكنولوجيا.

أول هذه المسؤوليات ضرورة الالتزام بتمكين الإدارة للأعوان والموظفين القائمين على البرامج وهذا من خلال ضمان تعليم وتكوين كاف لهم، والسماح لهم بالإشراف الفعلي على سير البرامج.

بالإضافة إلى ذلك يقع على الإدارة واجب تحمل المسؤولية الناجمة عن أضرار التطبيقات الخوارزمية في نشاطها بسبب عدم قيامها باكتشاف العيوب الظاهرة في البرامج اثناء مرحلة التجربة، أو بسبب التنفيذ الخاطئ لها.

أما العيوب الخفية والمتضمنة لمخالفات جسيمة: (نظام تمييزي، نقل سري للبيانات)، فمن شأنها إقامة المسؤولية الخاصة لمصمم ومهندس البرنامج[2].

يحتم مبدأ التكيف الذي يحكم المرفق العام ضرورة مسايرة عملية اتخاذ القرارات الإدارية لمستجدات الرقمنة والمعلوماتية في معالجة البيانات الكبرى (BIG DATA)؛ ما من شأنه أن يحسن من جودة تلك القرارات لاسيما من جهة

[1]- بلخير محمد آيت عودية، المرجع السابق، ص 23.

[2]-بلخير محمد آيت عودية ، المرجع نفسه، ص 23.

السرعة والحياد، لكن من جهة أخرى هذا يفرض على القضاء والتشريع سرعة التعامل مع آثار توظيف تقنيات الذكاء الاصطناعي على النظرية التقليدية للقرارات الإدارية، من أجل تحسين الرقابة القضائية عليها من حيث المشروعية وحماية حقوق المواطن[1].

الفرع الثالث : تطبيقات القرار الإداري الخوارزمي في القطاع العام و آثاره

توفر خوارزميات الذكاء الاصطناعي فرصة لتحسين الوضع الراهن في الحكومات؛ من خلال معالجة أوجه القصور في عمليات صنع القرار الإداري المتمثلة خاصة في توفير :الدقة، التناسب، التقليل من فرص الفساد، وكذا زيادة الكفاءة والفاعلية في الأداء إضافة الى إمكانية خلق خدمات حكومية جديدة نجد أمثلة عليه في مجال توظيف وتنمية الموارد البشرية، حيث أصبح من الشائع اتخاذ القرارات الخوارزمية في مجال التوظيف وتطوير الموارد البشرية[2]، حيث يتم صنع القرارات باستعمال الخوارزميات للتقليل من التكاليف وزيادة الموضوعية و يتم ذلك على النحو التالي :

أولاً: تطبيقات القرار الإداري الخوارزمي في مجال الإدارة العمومية

1. **توظيف الموارد البشرية :** تستخدم أدوات خوارزمية مختلفة بحسب المرحلة؛ فأدوات اختيار المرشحين للوظيفة تختلف عن التي يتم استخدامها في مرحلة الانتقاء من بين المرشحين الذين تمت الموافقة عليهم ففي مرحلة الإعلان عن الوظائف الشاغرة، والعثور على المرشحين الذين تتناسب مؤهلاتهم والوظائف

[1]- ضيف الله زينب . بن داود براهيم،. المرجع السابق، 385.

[2]-كوثر منسل وحميد شاوش، المرجع السابق، ص 810.

المعلن عنها، إذ يتم استخدام أدوات صنع القرار الخوارزمي للتوصية بالمرشحين، وهنا تستفيد أنظمة التوصية من مصادر مختلفة من المعلومات حيث تمر الخوارزميات عبر الملفات الشخصية وتقوم بفحصها للتوصل إلى المرشحين الأكثر تأهلاً ثم تقدم بناء على ذلك توصيات بشأنهم [1] .

أما مرحلة الانتقاء فإن الحاجة للمزيد من الكفاءة الحسابية يكون أكثر ، حيث تستخدم أدوات القرار الإداري الخوارزمي في فحص السيرة الذاتية للمرشحين إضافة الى توفير تقييم حسابي للمقابلات عبر الهاتف او الفيديو قبل المقابلة الشخصية، تعمل أدوات الذكاء الاصطناعي هنا على الاستشعار والتنبؤ بالسلوك البشري من خلال السلوك اللفظي وغير اللفظي (تعابير الوجه مثلاً أو لغة الجسد) والتي يتطابق معها "البرمجة اللغوية العصبية "، ومن ثم يتم معالجة كل الخوارزميات مما ينتج عنه ملف تعريف شخصي كامل لكل مرشح، والذي يلعب دوراً أساسياً في نتائج التوظيف.

2-1 **تنمية الموارد البشرية** : زاد استخدام القرارات الخوارزمية بالنسبة للمؤسسات في متابعة موظفيها بحيث يتم توثيق السجلات الشخصية وتقييم الأداء و المهارات الوظيفية في أنظمة حسابية، كما تتضمن هذه الأنظمة مؤشرات رضا الموظفين التي تشمل الراتب والمزايا المستحقة، ساعات العمل، الظروف المحيطة، المخاطر وغيرها، وهذا من أجل اتخاذ قرارات حسابية من شأنها تطوير الموارد البشرية، من خلال منح ترقيات مستحقة والوصول إلى الرضا الوظيفي من خلال تطبيق كل ما سبق بيانه.[2]

[1]- كوثر منسل، حميد شاوش، المرجع السابق ص 810.

[2]- كوثر منسل، حميد شاوش ، المرجع نفسه، ص 810.

2-1 في مجال تمويل النفقات العامة وتأمين الخدمات الاجتماعية: نقترح نموذجين من هذه الخدمات:

2-2 إدارة الضرائب (هولندا): تعتبر إدارة الضرائب الهولندية الأكثر تطور في مجال استخدام خوارزميات الذكاء الاصطناعي والبيانات الضخمة ضمن مخطط عملها، حيث تحظى بإمكانية الوصول لبيانات عدة وكالات حكومية على غرارا : البلديات ،اقسام الشرطة، وكالات الإعلانات والقروض ثم تقوم بربطها بنظامها، حيث تتضمن قواعد بيانات المواطنين الخاصة وكذا بيانات تتعلق باستخداماتهم المختلفة لمرافق الرقمية المتاحة (سلوكيات التصفح على مواقع الويب، الوقت المستغرق لإتمام الإقرار الضريبي ...)، وكل ذلك من أجل الكشف عن حالات التهرب الضريبي المحتملة والتي من خلالها يتم تعزيز درجة الفعالية في إقرار قيمة الضريبية[1]

3-2 تجربة بلدية Trelleborg السويدية : تعتبر أول بلدية سويدية تستخدم القرار الإداري الخوارزمي في مجال الخدمات الاجتماعية فمنذ عام 2015 أصبح مواطنوها قادرين على تقديم طلبات المساعدة الاجتماعية رقمياً، ثم طورت هذه العملية الرقمية من خلال دعمها بخوارزميات اتخاذ القرار وبحلول عام 2017 تم تقديم 75 % من طلبات المساعدة الاجتماعية عبر منصة "المساعدات الاجتماعية "، والمدرجة في قسم مخصص ضمن موقع ويب البلدية، بحيث يقدم المواطنين من خلاله طلباتهم باستخدام هواياتهم الالكترونية؛ أين يتم تسجيل المعلومات التي تطلبها المنصة و المتعلقة بأفراد الاسرة ودخلها، المصاريف الشخصية (كالإيجار،

[1]- بن سرية سعاد، تطبيق تقنيات الذكاء الاصطناعي في مجال القرارات الإدارية، التراث، جامعة زيان عشور، الجلفة، المجلد 14, العدد 2, جوان 2024، ص 91.

العلاج، رعاية الأطفال، التأمين على المنزل ...)، إضافة للمعلومات المتعلقة بترتيبات المعيشة وعدد افراد الاسرة مع إرفاقها بالمستندات التي تثبت ذلك، كما يقدم موظفو الخدمة مساعدات للمواطنين الذين يجدون صعوبات في التعامل مع التطبيق .

بعدها تكون المنصة قد شكلت خطة شاملة حول نشاط المواطنين وكيفية متابعته بشكل منتظم وذلك بعد دمجها بالمعلومات ذات الصلة بالوضع الاقتصادي للمواطن، والتي توفرها المنصة الوطنية الخاصة بالمزايا الاجتماعية، تأتي المرحلة الأخيرة وهي مرحلة اشراك اخصائي الحالة الاجتماعية في صنع القرار من خلال بحثهم عموما عن مدى جدية طالب المساعدة الاجتماعية، في محاولته الحصول على عمل ومدى عزمه في الاعتماد على نفسه وهنا يتساوى أن يكون الاخصائي شخصا طبيعيا او روبوت.

وعليه فالقرار النهائي بشأن الطلبات يصدر مشتركاً بين اخصائي الحالة التكنولوجيا[1]، والذي قد يكون إيجابياً أو سلبياً ليبلغ لمواطن بمجرد دخوله للمنصة، كما أدرجت المنصة ابتداء من عام 2019 وظيفة تقديم الطعون ضد القرارات السلبية، بعد أن كانت تقدم بمساعدة موظفي الخدمة المدنية.

ثانياً : الآثار السلبية للخوارزميات في الإدارة العامة أو القطاع العام:

إن اعتماد الإدارة العامة على الخوارزميات في قراراتها قد ينتج عنه إشكالات تتمثل خاصة في مسالة التقدير الرقمي وإشكالات التحيز، الأمر الذي يقتضي ضرورة أخلقة الذكاء الصناعي نتناولها كما يلي:

[1]- بن سرية سعاد ، المرجع السابق، ص 93.

1-1التقدير الرقمي وإشكالية التحيز الخوارزمي: إن الهدف من القرار الإداري الخوارزمي هو توفير الوقت والتكاليف وتعزيز الإنتاجية وزيادة الفعالية وبالتالي زيادة الموضوعية والانصاف بعيداً عن المشاعر البشرية، غير أن هناك تهديدات بشأن الانحراف في التقدير أطلق عليها "مصطلح التحيز الخوارزمي " نتطرق أولا لتحديد مفهوم التقدير الرقمي[1]، و هو التقدير الآلي أو المصطنع يحدث عندما يتم تعزيز التقدير البشري أو استبداله كلياً بالذكاء الاصطناعي الذي يوفر مدخلات في المهام التقديرية من خلال الاتمتة التي تستخدم بيانات التدريب لتحديد الأنماط بين بيانات الادخال والنتائج لتوليد نماذج تنبؤية باستخدام التفكير الاحتمالي .

كما يمكن تعريفه على أنه: مجموعة من الوظائف الرياضية التي تهدف الى ربط بيانات الادخال ببيانات الإخراج.

تجدر الإشارة إلى أن التقدير الرقمي تختلف مستوياته باختلاف المهام الموكلة له وتتراوح بين المستوى المنخفض إلى المتوسط فالعالي، فالمستوى المنخفض نجده في قرار منح الترخيص مثلاً، أما المتوسط مثل قرار تحديد وقت وكيفية استخدام الطاقة في المرافق العمومية، اما العالي فيتجسد في عمليات التوظيف.

2-1 التحيز الخوارزمي :الانحراف في السلطة:

يطلق بشكل عام على المعاملة غير المتكافئة للمراكز المختلفة والقائمة على أساس الجنس، العرق أو السن عوض النوعية ؛ هنا تنتج الخوارزميات نتائج متحيزة

[1]- كوثر منسل، حميد شاوش ، المرجع السابق ص 812.

، إذا ما تم تزويدها ببيانات غير دقيقة، أو اعتماد بيانات إدخال غير دقيقة ومتحيزة فتؤدي للقرارات متحيزة، معناه يمكن القول: إن السبب في التحيز هو بيانات الادخال، من الأمثلة على هذه الحالة: بيانات الادخال التي طبقها اخصائيو التجارة الالكترونية الامريكية "أمازون " لتوظيف مهندسي برمجيات، أين افتقرت بيانات الادخال فيها للنزاهة حيث كانت منحازة لتوظيف الذكور أكثر من الإناث، مما أدى إلى التوقف عن اتخاذ قرارات التوظيف الخوارزمية[1].

أبعد من ذلك ما حدث في استراليا حيث تم رفع الديون بشكل غير قانوني من خلال ربط بشكل خاطئ بيانات الدخل الضريبي السنوي مع بيانات دخل الضمان الاجتماعي، الأمر الذي أدى إلى خوارزميات خاطئة رفعت الديون بشكل كبير.

وعليه وجب اخضاع القرارات الإدارية الخوارزمية لمبادئ المشروعية في القرارات الإدارية التي تم تناولها مسبقاً المتمثلة في الشفافية والمساواة، وأيضاً قابلية القرار الإداري الخوارزمي للتفسير وهي فكرة قابلة لتطبيق عمليا بمعنى شرح مبررات وأسباب تقديم بيانات الادخال من جهة، وفحص النظام ومقارنة مدخلاته ومخرجاته من جهة أخرى.

إن قابلية التفسير تندرج ضمن متطلبات المسائلة الفعالة التي يلجأ لها المكلف بالقرار في حال عدم اقتناعه به وهنا تبرز مسألة خضوع الذكاء الاصطناعي

[1]- كوثر منسل، حميد شاوش، المرجع نفسه، ص 812.

المساءلة القانونية؛ والتي تلقى عادة على عاتق مطوري البرامج أو الموظف المسؤول على اعتماد أدوات الذكاء الاصطناعي داخل الإدارات بالدرجة الثانية[1].

من خلال ما تقدم عرضه يتضح جلياً أن فكرة اعمال القرار الخوارزمي في القطاع العام أضحت مطلبا من مطالب التحول نحوى إدارة ذكية، على الرغم من التحديات القانونية والتقنية التي تواجه تطبيقه وهذا ما يحتمه مبدأ التكيف الذي يتميز به المرفق العام، بما من شأنه أن يحسن من جودة القرارات لاسيما من حيث السرعة والحياد، غير أن هذا يحتم على التشريع والقضاء ضرورة التعامل السريع مع أثر توظيف كيانات الذكاء الاصطناعي على النظرية التقليدية للقرارات الإدارية من خلال تحيين واع للنظام القانوني الذي يحكم تلك القرارات، بما يضمن رقابة قضائية فعالة لمشروعيتها من جهة ، وحماية حقيقية للمتعاملين مع الادارة من جهة أخرى.

خاتمة

لقد تطورت التكنولوجية لتقلد ذكاء الإنسان بعد تقليد أدائه البدني ، وما كان مستحيلا بالأمس أصبح ممكنا اليوم عبر الذكاء الاصطناعي، إنها الثورة الصناعية الرابعة التي غيرت مجالات الطب والتعليم والنقل والأمن وساهمت في بشكل مباشر في تحسين مستوى الرعاية الصحية وتنمية الاقتصاد وتأمين خدمات جد متطورة ، وأضحى الذكاء الاصطناعي بدون أن نشعر يزاحم الإنسان في حياته بدأ بالسيارات ذاتية القيادة، الطائرة المسيرة بدون طيار، الإنسان الآلي الذكي، الأجهزة

[1]- كوثر منسل، حميد شاوش، المرجع نفسه، ص 813.

الذكية في مجال التشخيص والجراحة، الهواتف الذكية والقائمة تطول، جعل هذا التدخل الذكاء الاصطناعي محل اهتمام الحكومات والأفراد والشركات

كما يعتبر الذكاء الاصطناعي جزء لا يتجزأ من القانون بعد ان أصبح واقع مفروض على البشر إذ يتدخل في كل مجالات الحياة، حيث يعد القانون اللبنة الأساسية لحماية المجتمع وقواعده هي الكفيلة بالسهر على تنظيمه ولذلك فالأنظمة الذكية لا يمكن تصورها بمعزل عن القانون وقواعده إذ يتداخل معه في كل فروعه من المدني للجنائي فالتجاري وغيرها، وما دراستنا هذه إلا جزء يسير من بداية سيطرة الذكاء الاصطناعي على مختلف فروع القانون، وقد حاولنا من خلال دراستنا التركيز على جانبي العقود والقرارات لتدخلهم المباشر في تصرفات الإنسان.

قائمة المراجع:

أ. باللغة العربية

أولاً: المقالات:

1. أحمد علي حسن عثمان، انعكاسات الذكاء الاصطناعي على القانون المدني دراسة مقارنة ، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 76، 2021.
2. أحمد قاسم فرح، استخدام الوكيل الذكي في التجارة الالكترونية دراسة قانونية مقارنة في اطار ماهيته ونفاذ تصرفه، مجلة المفكر، جامعة محمد خيضر، بسكرة، المجلد 13، العدد 2، 2018.
3. آيت عودية بلخير محمد، القرار الإداري الخوارزمي مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تامنغست، المجلد 9، العدد 3 2020.
4. إيهاب خليفة فرص وتهديدات الذكاء الاصطناعي السنوات العشر القادمة مقال منشور بمجلة مركز المستقبل للأبحاث والدراسات المتقدمة ع 27 لسنة 2018 .
5. بن سرية سعاد، تطبيق تقنيات الذكاء الاصطناعي في مجال القرارات الإدارية، التراث، جامعة زيان عشور، الجلفة، المجلد 14, العدد 2, جوان 2024.
6. بن صاري رضوان، تطبيقات الذكاء الاصطناعي في مجال القانون، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، المجلد 17, العدد 1, جانفي 2025.
7. د. نايف بن ناشي الغنامي، الضوابط القانونية للذكاء الاصطناعي في إبرام المعاملات القانونية، مجلة رؤى في الآداب والعلوم الإنسانية، جامعة محمد خيضر، بسكرة، المجلد 4, العدد 1، مارس 2025.
8. داود منصور، عبد القادر زرقين، العقود الذكية المدمجة في البلوك تشين – بداية نهاية العقود التقليدية – المجلة الجزائرية للعلوم القانونية والسياسية،2022، جامعة الجزائر 01، مجلد 59، عدد 1، 2022.

9. رابعي إبراهيم، الطبيعة القانونية للذكاء الاصطناعي، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 10, العدد 1,جوان 2025.

10. ضيف الله العتبي، السعودية الحكومة الذكية مرحلة ما بعد الحكومة الالكترونية ، الجهة السعودية للمبرمجين، دون سنة نشر.

11. ضيف الله زينب . بن داود براهيم . القانون والذكاء الاصطناعي، مجلة القانون والعلوم البينية، جامعة زيان عشور الجلفة، المجلد 2, العدد 3, ديسمبر 2023.

12. ظلّام عبد الكريم ، الاعتراف بالشخصية القانونية لأنظمة الذكاء الاصطناعي: ضرورة أم مغالاة؟ مجلة البحوث القانونية و الاقتصادية، المركز الجامعي لأفلو، المجلد 8, العدد 1، جانفي 2025.

13. قندوز فتيحة، الجوانب القانونية لاستخدام الذكاء الاصطناعي، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة الجزائر 01، المجلد 09، العدد 01، 2024.

14. كوثر منسل، حميد شاوش، الإشكالات القانونية لاعتماد القرار الإداري الخوارزمي، مجلة الرسالة للدراسات والبحوث الإنسانية، جامعة العربي التبسي، تبسة، المجلد 6، العدد 4، 2021، ص 808 .

15. محمد عرفان الخطيب، الذكاء الاصطناعي والقانون دراسة نقدية مقارنة التشريع المدني الفرنسي والقطري في ضوء القواعد الأوروبية في القانون المدني للانسآلة لعام 2017 والسياسة الصناعية الأوروبية للذكاء الاصطناعي للأنسائلات لعام 2019، مجلة الدراسات القانونية جامعة بيروت العربية، لبنان، المجلد 20، جوان 2021.

النصوص القانونية

1. الدستور الجزائري 2020.
2. الأمر رقم 75/58 المؤرخ في 1975/09/26 المتضمن القانون المدني المعدل بموجب القانون رقم 10/05 المؤرخ في 2005/07/20

3. القانون رقم 18-07 المؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج العدد 34، الصادرة بتاريخ 10 يونيو 2018.

4. القانون الاتحادي رقم 1 لسنة 2006 بشأن المعاملات والتجارة الالكترونية .

ب. باللغة الفرنسية:

1. La loi n°78-17 du6 /1/1978 relative a l informatique aux fichiers et aux libertes a été l une des premieres legislation en la matiere.

2. S .L Lipovetsky et Philippe ;le droit d accès l information confronte aux données personnelles :la délicate balance des droits et libertés fondamentales .Legipresse ;2019 p 204.

التفاوض الإلكتروني في عقود العمل عن بُعد: قراءة قانونية في ضوء التطور التكنولوجي

Négociation électronique dans les contrats de travail à distance : une lecture juridique à la lumière du développement technologique

د. ربعية رضوان
radouane-rebaia@univ-eltarf.dz
جامعة الشاذلي بن جديد، الطارف، الجزائر
د. فارس مزوزي
mazouzi-faris@univ-eltarf.dz
جامعة الشاذلي بن جديد، الطارف، الجزائر

ملخص:
الملاحظ أن تكنولوجيا المعلومات ما ان تغلق بابا حتى تفتح أخر أكثر رحابة واتساعا، وذلك لما تتيحه من بدائل كثيرة لإعادة تشكيل مفاهيم وصياغة علاقات ونظم وبيئات مختلفة، ولقد شهد العالم في هذه السنوات القليلة سلسلة من التحولات في الفكر القانوني نتيجة تحولات تقنية في مجال الاتصال والمعلومات، من بين ما احدثته من تغير بيئة العمل التقليدية ، بظهور العمل عن بعد الذي يعد احد العقود الالكترونية والذي يثير جدل فقهي ونقاش قانوني محتدم بخصوص تطور النظام العقدي ومدى قدرة القواعد التقليدية على مسايرة واقع انعقاد عقد العمل عن، الأمر الذي سنتناول فيه مرحلة التفاوض الالكتروني على عقد العمل عن بعد من حيث بيان دلالاتها وأحكامها والتزامات طرفيها.

الكلمات المفتاحية: تكنولوجيا المعلومات، العمل عن بعد، عقد الكتروني، التفاوض الالكتروني

***Abstract**: It is noted that information technology closes one door and opens another, more spacious and broad one, due to the many alternatives it provides for reshaping concepts and formulating different relationships, systems and environments. In recent years, the world has witnessed a series of transformations in legal thought as a result of technical transformations in the field of communication and information, among which is the change in the traditional work environment. With the emergence of remote work, which is considered one of the electronic contracts, which raises a jurisprudential controversy and heated legal debate regarding the development of the contractual system and the extent to which traditional rules are able to keep pace with the reality of concluding the remote work contract, in which we will address the stage of electronic negotiation of the remote work contract in terms of explaining its implications, provisions, and obligations of its two parties.*

***Key words:** information technology, networking, electronic contract, electronic negotiation.*

مقدمة:

في ظل التغيرات الاقتصادية الراهنة والتطور التكنولوجي ، شهدت العديد من المفاهيم القانونية تحولات جذرية من الشكل التقليدي الى الشكل الإلكتروني ولعل اهم نتاج لذلك هو ولادة مفهوم جديد أطلق عليه العمل عن بعد ، بل تزايد وتنامى الاعتماد عليه مع ظهور تهديد الوباء العالمي فيروس كورونا الذي اعتبر نعمة ونقمة في نفس الوقت، اين اصبح العمل يتم انجازه بعيد عن مكان العمل بواسطة استغلال تقنيات المواصلات والمعلومات في المنزل مثلا هذا الأخير – العمل عن بعد- يعد من طائفة العقود الالكترونية التي يتم بتوافق ارادتين بوسائل الكترونية من خلال شبكة الإنترنت .

ولقد شكل العمل عن بعد بعض المشكلات القانونية بسبب خطورة الآثار المترتبة عليه خاصة بظهور التوقيعات الإلكترونية كما انه ينعقد دون حضور مادي

ملموس لطرفيه بمجلس العقد، فيكون كل طرف في مكان يختلف عن مكان الطرف الأخر ويفصل بينهما بعدا جغرافيا، ومن ثم فان مجلس العقد لا يكون مجلسا حقيقيا وإنما مجرد مجلسا حكميا او افتراضي متعاصر، الأمر الذي برر الحاجة الى وجود تشريعات تنظمه، والهدف منها خلق اتزان تعاقدي بين الأطراف، خاصة أن نظرية العقد لا تنسجم دائما في إطار العقود الالكترونية.

ويتميز عقد العمل عن بعد كغيره من العقود الالكترونية بمرحلتين مرحلة انعقاد ومرحلة سابقة على انعقاد العقد-التفاوض-هذه الاخير موضوع الدراسة.

ونظرا لتقنية وتعقيد عملية التفاوض خاصة التي تتم عبر وسيلة من وسائل الاتصال عن بعد وما تطرحه من اشكالية جدية الارادة المقابلة في الابرام والتفاوض ومدى توفر الشروط القانونية اللازمة لترتيب الآثار المرجوة من العقد ومدى التزام الطرف – العامل- بتنفيذ ما اتفق عليه ومن هنا تبرز أهمية الموضوع في تحديد المعنى الدقيق للتفاوض الالكتروني في عقد العمل بعد وأهميته القانونية وخصائصه وفق القانون الجزائري ومعرفة مدى مسايرته المشرع الجزائري للركب الحضاري في مجال التفاوض في العقود الالكترونية(عقد العمل عن بعد نموذجا).

لذا فإن الاشكالية التي يطرحها موضوع الورقة البحثية تتمثل فيما هي القواعد القانونية الخاصة التي تحكم المرحلة السابقة لإبرام عقد العمل عن بعد بوصفه عقد الكترونيا دو مجلس افتراضي؟ ومدى استجابة المشرع الجزائري في مسايرة تنظيم مثل هذه العقود؟

وسنحاول الاجابة عن هاته الاشكالية المركبة وفق الخطة التالية مع الاعتماد على المنهج الوصفي التحليلي والمقارن:

المحور الأول: ماهية التفاوض الالكتروني في عقد العمل عن بعد

المحور الثاني: أحكام التفاوض الالكتروني في عقد العمل عن بعد

المحور الأول:

ماهية التفاوض الإلكتروني في عقود العمل عن بعد

تعتبر مرحلة التفاوض من أهم المراحل التي تسبق الإبرام النهائي للعقود خاصة إذا كنا أمام عقد الكتروني يثير العديد من التساؤلات والغموض بين أطرافه، لذا وجب أن تكون هناك مرحلة تمهيدية تسبق الموافقة النهائية لتأكد من شخصية المتعاقد وطبيعة المحل وطرق التنفيذ إلى غير ذلك.

ولتحديد مفهوم التفاوض الإلكتروني في عقود العمل عن بعد سنتطرق بداية إلى تحديد مفهوم التفاوض باعتباره مرحلة سابقة وضرورية لإبرام عقد العمل الذي يتم عن بعد (المطلب الأول) ثم نتطرق إلى مفهوم عقد العمل عن بعد (المطلب الثاني)

المطلب الأول: مفهوم التفاوض الإلكتروني

لإعطاء مفهوم دقيق لتفاوض الإلكتروني سنتطرق إلى تعريفه وخصائصه (الفرع الأول) ثم نتطرق إلى الالتزامات الناتجة عنه (الفرع الثاني)

الفرع الأول :تعريف التفاوض الإلكتروني وخصائصه

أولا: تعريف التفاوض الإلكتروني

هناك العديد من التعاريف التي تناولت التفاوض الإلكتروني حيث عرف بأنه تبادل الاقتراحات والمساومات والمكاتبات والتقارير والدراسات الفنية بل والاستشارات القانونية التي يتبادلها أطراف التفاوض وليكون كل منهما على بينة

بأفضل الأشكال القانونية التي تحقق مصلحة الأطراف وللتعرف على ما قد يسفر عنه الاتفاق من حقوق والتزامات لطرفين.[1]

كما عرف بأنه قيام أطراف العلاقة العقدية المستقبلية بتبادل الاقتراحات والآراء والدراسات والتقارير الفنية والاستشارات القانونية ومناقشة ما يضعانه سوية أو ينفرد بوضعها أحدهما من اقتراحات وأراء بغية الوصول إلى أفضل النتائج التي تحقق مصالحهما ولتحديد ما يسفر عنه الاتفاق النهائي بينهما من حقوق والتزامات على كل منهم.

وعرف بأنه العرض الموجه للعامة أو لشخص محدد بهدف تبادل الآراء لإبرام العقد بحيث يحاول كل طرف من طرفي العقد تحديد مضمون ما عليه وله من حقوق والتزامات تقتضيها مصالحه مستخدما كافة الوسائل الممكنة معتمدا على براءته التجار[2].

ما تجدر الاشارة إليه أن المشرع الجزائري لم يتطرق صراحة إلى مرحلة التفاوض الإلكتروني التي تسبق مرحلة إبرام العقد ، لكنه تطرق إلى مفهوم العقد الإلكتروني في قانون التجارة الإلكترونية رقم 18-05من خلال المادة 6 ف 2 التي أحالت الى المادة 3 من القانون رقم 04 -02 الذي يحدد القواعد المطبقة على الممارسة التجارية المعدل والمتمم .حيث جاء فيها "العقد الإلكتروني : العقد بمفهوم القانون رقم 04 -02 المؤرخ في جمادى الأولى عام 1425 الموافق ل 23 يونيو سنة 2004 الذي يحدد القواعد المطبقة على الممارسات التجارية ويتم ابرامه عن بعد دون الحضور الفعلي والمتزامن لأطرافه باللجوء حصريا لتقنية الاتصال الإلكتروني " أما

[1] - أرجيليوس رحاب ، مسعودي يوسف، الإطار القانوني للتفاوض في العقد الإلكتروني ، مجلة معالم للدراسات القانونية والسياسية عدد 3 ،المركز الجامعي ، تيندوف، مارس 2018 ، ص 52 .

[2] - العلي هاشم محمود محمد، أحمد أبو شنب، الحماية المدنية للمستهلك في مرحلة ماقبل انعقاد العقد الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة عمان العربية، كلية القانون، الأردن، 2018، ص 15.

المادة 3 من القانون 04 -02 المعدل والمتمم فقد حاء فيها العقد : كل اتفاق أو اتفاقية تهدف إلى بيع سلعة أو تأدية خدمة حرر مسبقا من أحد أطراف الاتفاق مع إذعان الطرف الآخر بحيث لا يمكن هذا الأخير إحداث تغير حقيقي فيه.

وهذا على العكس بعض التشريعات العربية كالتشريع المصري والتونسي اللذان تطرقان لتفاوض الإلكتروني صراحة كمرحلة تسبق ابرام العقد الإلكتروني وهذا ما يستفاد من نص الفصل الخامس والعشرين من قانون المبادلات التجارية الإلكترونية التونسي رقم 83 لسنة 2000 بوجود مرحلة التفاوض من خلال الالتزامات التي رتبها على البائع في المعاملات الإلكترونية أن يوفر للمستهلك بطريقة واضحة ومفهومة قبل ابرام العقد المعلومات التالية : هوية وعنوان وهاتف البائع أو مسندي الخدمات وصفا كاملا لمختلف مراحل انجاز المعاملة ، طبيعة وخاصيات وسعر المنتج.

أما التشريع المصري فقد نص صراحة في المادة الأولى من قانون التجارة الإلكترونية وذلك من خلال تعريفه للعقد الإلكتروني بأنه عقد تصدر فيه ارادة الطرفين أو كليهما أو يتم التفاوض بشأنه وتبادل وثائقه كليا أو جزئيا عبر وسيط إلكتروني.

ثانيا: خصائص التفاوض الإلكتروني

1- عقد رضائي: يعد عقد التفاوض الإلكتروني من العقود التي تقوم على التراضي ، حيث يكفي فيه توافر الارادتين دون اشتراط شكل معين ويظل عقد رضائي حتى ولو كان العقد النهائي عقد شكلي وعليه يكفي الإيجاب الإلكتروني بالقبول الإلكتروني على شبكة الانترنت دون الحاجة إلى اتباع شكل معين.

2- التفاوض على العقد ثنائي الجانب: التفاوض على العقد يجب أن يتم من خلال شخصين فأكثر بالتحاور عن طريق المراسلات التي تتضمن الشروط التي يرغب

كل من الطرفين توفرها في موضوع التزامه لتحديد رغباته الأساسية من موضوع الالتزام، والذي يتم من خلال صفحة البيانات أو محركات البحث الويب المتوفرة على شاشات الأنترنت.[1]

3- تصرف إرادي: فكل طرف له الحرية الكاملة في الدخول ومباشرة المفاوضات أو الاستمرار فيها أو الانسحاب منها ولو في اللحظة الأخيرة وأساس ذلك يرجع إلى مبدأ حرية التعاقد.

4- عقد تمهيدي: يعتبر التفاوض على العقد الإلكتروني مرحلة تمهيدية لإبرامه إذ يهدف إلى الإعداد والتحضير لإبرام العقد النهائي، وإذا كان التفاوض لا يلزم الطرفين فإنه يهدف في النهاية إلى ابرام العقد بعد قيام الطرفين بالتمهيد لإبرامه بالتفاوض بعد التوصل لاتفاق يقود الطرفين في الأخير إلى بلورته إلى اتفاق نهائي[2].

5- التفاوض مرحلة ذو نتيجة احتمالية: إذ ليس كل تفاوض على العقد يؤدي بالضرورة إلى ابرام العقد وانما قد ينتهي التفاوض إلى لا شيء كون التفاوض العقدي يحكمه مبدآن الأول مبدأ حسن النية والثاني مبدأ حرية التفاوض

وعليه ومن خلال ما سبق يمكن القول أن التفاوض الإلكتروني هو مرحلة تمهيدية رضائية تتم من طرف شخصين فأكثر تهدف لتحضير لإبرام عقد نهائي، بحيث يكون لكلا الطرفان الحرية في التفاوض والحرية في قبول أو عدم قبول التعاقد.

[1] - العلي هاشم محمود محمد ، أحمد أبو شنب، المرجع السابق ، ص 19.

[2] - أرجيليوس رحاب ، مسعودي يوسف، المرجع السابق، ص 53.

الفرع الثاني: الالتزامات الناتجة عن التفاوض الإلكتروني

ينشأ عن التفاوض الإلكتروني مجموعة من الالتزامات يجب على الأطراف احترامها والتقيد بها ويؤدي عدم احترامها إلى قيام المسؤولية وهذه الالتزامات تتمثل أساسا في:

أولا: الالتزام بالإعلام: بداية يجب الاشارة أن المشرع الجزائري لم يتطرق ولم يعطي أي مفهوم للالتزام بالإعلام الإلكتروني فقط هو تناول حماية المستهلك من مخاطر الاعلان في العقود التقليدية من خلال القانون رقم 03/09 المتعلق بحماية المستهلك وقمع الغش غير أن الالتزام بالإعلام عرف بأنه التزام سابق على التعاقد يتعلق بالتزامات أحد المتعاقدين بأن يقدم للمتعاقد الآخر كافة البيانات الازمة لتولد الرضا الكامل للمتعاقد الآخر من خلال رسائل تحتوي على كافة تفصيلات العقد لظروف واعتبارات معينة تعود لطبيعة العقد أو شخص المتعاقد أو طبيعة المحل أو اي اعتبارات أخرى من المستحيل على أحد طرفي العقد أن يلتزم بتلك البيانات والشروط تبعا لهذه الاعتبارات والبيانات ،وعليه فإن الالتزام بالتفاوض الإلكتروني هو التزام قانوني يسبق العقد الإلكتروني يلتزم بموجبه أحد المتعاقدين الذي يملك معلومات جوهرية فيم يخص العقد وتقديمها بوسائط الكترونية في الوقت المناسب وبكل شفافية وأمانة للطرف الآخر الذي لا يمكنه العلم بها بوسائله الخاصة[1].

ثانيا: الالتزام بحسن النية: المقصود بها أن تتسم عملية التفاوض بالنزاهة والأمانة والثقة مع الامتناع عن كل ما من شأنه إعاقة المفاوضة أو محاولة التضليل للإضرار بالطرف الآخر .

ثالثا: الالتزام بالسرية: ان سير المفاوضات يستلزم الكشف عن العديد من الأسرار من طرف للطرف الآخر عبر الوسيلة الإلكترونية ، مما يستتبع معه امتناع

[1] - كحلول سامي ، بن طاية زوليخة ، حماية المستهلك الإلكتروني في مرحلة التفاوض ، مجلة الاجتهاد القضائي ، عدد 14 جامعة محمد خيضر ، بسكرة ، 2017 ، ص 641.

المتفاوض كلية عن افشاء هذه الأسرار أو نقلها إلى الغير سواء أثناء التفاوض أو حتى بعد فشل المفاوضات ، وأن يمتنع أيضا عن استغلالها لحسابه بدون إذن صحابها.

وتبقى للقاضي السلطة التقديرية في تحديد الأسرار بطبيعتها وهل يعد هذا الالتزام من مقتضيات حسن النية ويختلف باختلاف الظروف والأشخاص والوقائع، فما يعتبر سرا في مكان ووقت معين لا يكون سرا في وقت ومكان آخر ، فتحديد معنى السرية مسألة واقعية من وظائف القاضي.

رابعا: الالتزام بالتعاون: ان الالتزام بالتعاون في مجال التفاوض الإلكتروني هو التزام يفرضه واجب حسن النية حيث يوجب على المتفاوضين أن يلتزما بالتعاون وذلك بتحديد الهدف والغاية الأساسية من العقد الذي يسعى المتعاقدان لإبرامه بكل وضوح وليتمكن كل منهما بدراسة ظروفه وظروف الآخر ومدى قدرته على ابرام العقد[1].

المطلب الثاني :

مفهوم العمل عن بعد

لتوضيح العمل عن بعد سنتطرق إلى تعريف (الفرع الأول) ثم صوره (الفرع الثاني)

الفرع الأول : تعريف العمل عن بعد

المشرع الجزائري لم يتطرق إلى التنظيم القانوني لمسألة العمل عن البعد على الرغم من أهميتها خاصة مع التطور التكنولوجي الذي يشهده العالم في الآونة الأخيرة أين يكاد يصبح العالم عالم افتراضي كون كل المعاملات تقريبا أصبحت تؤدى عبر وسائط الاتصال الإلكتروني ، غير أن المشرع الجزائري كما أشرنا سابقا قد تناول

[1] - أرجيليوس رحاب ، مسعودي يوسف،المرجع السابق، ص 64.

وقنن مسألة العقد الإلكتروني من خلال نص المادة 6 من القانون18-05 المتعلق بالتجارة الإلكترونية، وباعتبار أن عقد العمل من بين العقود التي تفرض وجود ايجاب وقبول بين الطرفين يمكن أن تطبق عليه أحكام نص هذه المادة.

غير أن العمل عن بعد فقد عرف من طرف منظمة العمل الدولية على أنه (طريقة للعمل فيها :

أ –يؤدي العمل بعيدا عن المكتب الرئيسي أو مواقع الانتاج، حيث يكون العامل منفصلا عن الاتصال الشخصي مع العاملين الاخرين ،

ب-وتقوم التكنولوجيا الحديثة بتعويض هذا الانفصال من خلال تسهيل عملية الاتصال)[1]

وقد عرف من طرف الاتفاق النموذجي الأوروبي المؤرخ في 25 تموز 2002 بأنه العمل الذي يؤديه العامل التابع أو المستقل باستخدام وسائل الاتصال السلكية أو اللاسلكية ونظم المعلومات بصفة أساسية لهذا العمل، ويمكن أيضا إنجاز العمل داخل العمل وخارجه بشكل منتظم[2].

أما فقها فقد تعددت التعاريف التي أعطاها الفقهاء له حيث عرف العمل بأنه الاتفاق الذي يبرم ويوقع بين طرفي العقد ، لأداء المؤدى في الأماكن البديلة ووفقا للشروط التي تضعها المنشأة والتي تطبق على العاملين كما عرف بأنه العقد الذي يبرم بين عامل ما وصاحب عمل والذي يكون فيه تنفيذ العامل لعمله خارج مقر

[1] - العرايشي عمر أحمد، الطبيعة القانونية لعقد العمل عن بعد في التشريع الأردني ، المجلة الأردنية في القانون والعلوم السياسية ، مجلد 9 ، عدد 4 ، جامعة مؤتة، ص 121.

[2] - محمد عبد الحفيظ عبد الرحمان المناصير ، النظام القانوني لعقد العمل عن بعد، دراسات علوم الشريعة والقانون ، مجلد 46 ، عدد 1 ،الجامعة الأردنية ، 2019 ، ص 247

العمل المعتاد وبعيدا عن الاشراف المباشر لصاحب العمل ، وذلك عن طريق استخدام وسائل التكنولوجيا الحديثة[1].

مما سبق يتضح لنا أن عقد العمل عن بعد يشتمل على العناصر التالية:

1-الأجرة : والتي تتمثل بالمقابل الذي يتفق عليه الطرفين مقابل أداء العمل

2-العمل ويتمثل في الجهد الذي يبذله العامل في أداء العمل

3-التبعية وهي أن يعمل العامل عن بعد تحت اشراف ورقابة صاحب العمل

4-استخدام الوسائل التكنولوجيا الحديثة : وتتمثل بأداء وتنظيم العمل عن بعد من خلال استخدام الوسائل التكنولوجيا الحديثة حيث يؤدي العامل عمله في أي مكان.

الفرع الثاني: خصائص العمل عن بعد

للعمل عن بعد مجموعة من الخصائص التي جعلته يعرف تطورا وإقبالا ملحوظا في الآونة الأخيرة في شتى الميادين ومن أهم هذه الخصائص نذكر:

أولا: تميز العمل عن بعد بالموازنة بين المرونة والانتاجية في العمل: حيث أن العمل عن بعد أحدث تأثيرات ايجابية على مستوى تحسين انتاجية المؤسسات وتحسين شروط تشغيل العمال من الناحية الاقتصادية والاجتماعية، ويتحقق ذلك من خلال انخفاض تكاليف الانتاج من جهة وتوفير المرونة في التشغيل من جهة أخرى .

[1] - نجلاء توفيق نجيب فليح ، نادية محمد مصطفى قرماز ، التكييف القانوني للعمل عن بعد : دراسة مقارنة ، مجلة الزرقاء للبحوث والدراسات الإنسانية ، مجلد 18 ، عدد 1 ،2018،ص 205.

ثانيا: تحقيق التوازن في الوظائف بين المناطق الجغرافية المختلفة: مما يسمح بالمزيد من اللامركزية لأداء الأنشطة والمهام وبالتالي تخفيف الضغط على العواصم، ويؤدي إلى التقليل من استخدام السيارات مما يخفف من الازدحام المروري وبالتالي التقليل من تلوث البيئة والمساهمة في اشراك العديد من فئات المجتمع للانخراط في سوق العمل خاصة ذوي الاعاقة، مما يكون له دور ملموس في المساعدة للقضاء على البطالة[1].

ثالثا: يوفر العمل عن بعد نظاما لا مركزيا للإدارة وهو نظام يمكن أن يعلو على النظام المركزي الهرمي الذي يمثل قيودا إدارية على سلاسة العمل وسرعته والذي يحمل المنشآت رواتب جسيمة خاصة فيما يتعلق برواتب كبار الموظفين في أعلى سلم الهرم الإداري.

لكن على الرغم من الخصائص الايجابية للعمل عن بعد لا يمكن إخفاء أنه له عيوب كثيرة أهمها أن العمل عن بعد قد يؤدي إلى عزل العامل عن المجتمع وقد يؤثر هذا عليه من الناحية النفسية، كما أنه قد يؤدي الى اضمحلال الوظائف المتعلقة بالخدمات المباشرة بالعميل وإهدار حقوق العمال وذلك لغياب النقابات العملية وصعوبة معاملة المؤسسات التي تتبع أسلوب هذا العمل ضريبيا، كما يحتاج تطبيقه تكاليف تأسيسية عالية من خلال تأسيس بنية تكنولوجيا ابتداء من التدريب والاتصالات ووظائف الدعم التقني[2]

[1] - العرايشي عمر أحمد، المرجع السابق، ص 130.

[2] - محمدعبد الحفيظ المناصير، المرجع السابق ، ص251

المحور الثاني:

أحكام التفاوض الالكتروني في عقد العمل عن بعد

لما كان عقد العمل عن بعد من العقود الإلكترونية فان هذا العقد يتساوى مع بقية العقود بقيامه على مبدأ الرضائية بقصد احداث اثر قانوني معين ، بمعنى انه ينعقد بمجرد تبادل طرفي العقد التعبير عن ارادتهما وتطابقهما، ويستوي ان تكون هذه الارادة سليمة غير مشوبة بعيوب الارادة وهو ما يطلق عليه "تعبير التراضي في عقد العمل عن بعد" هذا الاخير الذي يكون تعاقدا بين حاضرين يضمهما مجلس عقد حقيقي وقد يكون اقتران القبول بالإيجاب عن بعد اي في مجلس عقد حكمي ، ونظرا لطبيعة التعاقد الالكتروني فقد اختلطت الأوراق وتعقدت الامور لدرجة ان القواعد العامة للتراضي لم تستوعب مستجدات الثورة التكنولوجية ،الامر الذي استحدثت فيه قواعد جديدة للإيجاب والقبول عبر الوسيط الالكتروني وظهرت موازين قلبت مستوى مجلس العقد. فماهي قواعد الايجاب والقبول في التعاقد الإلكتروني؟ هل تطبق على جميع صور التعاقد ام ان لعقد العمل عن بعد خصوصية؟ ماهي المميزات التي استحدثت في مجلس العقد الالكتروني؟ كل هذه لتساؤلات وغيرها سنجيب عنها ضمن هذا المحور فيما يلي:

المطلب الأول:

خصوصية التراضي الالكتروني عند ابرام عقد العمل عن بعد

ينتهي التفاوض الالكتروني على العقد قانونا في الوقت الذي يصدر فيه الايجاب اذ في هذه اللحظة الحاسمة تكون المفاوضات قد حققت الغرض الأسمى منها، وهو توصيل الطرفين المتفاوضين الى اتفاق على جميع المسائل الجوهرية او الاساسية للعقد الذي يسعيان لإبرامه، ومن تم تنتهي مرحلة المفاوضات وتبدأ مرحلة ابرام العقد ، وبالتالي يعتبر الايجاب الحد الفاصل بين مرحلة التفاوض على

عقد العمل ومرحلة ابرامه ، والملاحظ ان هذا التفاوض في هذه العقود لا يجمعها مكان فهي تنتمي الى طائفة العقود التي تتم بين غائبين حاضرين ، وينعقد عقد العمل عن بعد اذا اقترن الايجاب بالقبول المناسب يترتب عليها آثار في مواجهة الطرفين[1].

الفرع الأول: قواعد الايجاب والقبول في عقد العمل عن بعد

يجب حتى ينعقد عقد العمل عن بعد توافق ارادتين على العناصر الجوهرية للعقد صراحة او ضمنا، اضافة الى ذلك ان يكون محل التزام كل من العامل ورب العمل ممكنا ومشروعا، ويأخذ حكم المحل غير المشروع، أداء اعمال مثلا غير مرخص بها، حيث يفقد هنا هذا العامل الصفة المهنية للمزاولة.

أولا: الايجاب الإلكتروني: يعرف الايجاب بمعناه العام على انه " تعبير منفرد الجانب عن الارادة موجه الى الجمهور او الى شخص محدد بغرض ابرام العقد" ولقد نصت عليه المادة 60 من ق. م .ج على انه " التعبير عن الارادة يكون باللفظ او بالكتابة أو بالإشارة المتداولة عرفا ، كما يكون باتخاذ موقف لا يدع اي شك في دلالته على مقصود صاحبه.

ويجوز ان يكون التعبير عن الارادة ضمنيا اذا لم ينص القانون او يتفق الطرفان على ان يكون صريحا "ومصطلح الالكتروني اذا ما اضيف الى الايجاب لا يخرجه عن معناه الأصلي وفق للنظرية العامة التقليدية، فهي عبارة عن وصف لا أكثر"[2].

[1] - جمال ابو الفتوح محمد، النظام القانوني لمرحلة المفاوضات على عقد العمل: دراسة مقارنة، مجلة لبحوث القانونية والاقتصادية، عدد65، كلية الحقوق جامعة المنصورة مصر، سنة 2018 ص 599.

[2] - بوحملة صلاح الدين، خصوصية الإيجاب والقبول في العقد الالكتروني، مجلة العلوم الانسانية، جامعة منتوري قسنطينة عدد 52 سنة 2019 ص 285.

وعليه يمكن تعريف الايجاب الالكتروني بأن تعبير جازم عن الارادة يتم عن بعد عبر تقنيات الاتصال سواء كانت مسموعة أو مرئية أو كليهما وتتضمن كافة الشروط والعناصر الاساسية للعقد المراد إبرامه بحيث ينعقد به العقد إذا ما تلاقى معه القبول. وعليه فان الايجاب الصادر في عقد العمل عن بعد هو تعبير قاطع وجازم عن ارادة الراغب في التعاقد سواء أكان العامل او صاحب العمل، ويتم التعبير عنه باستخدام وسيط الكتروني يتضمن كافة الشروط والمسائل الجوهرية في عقد العمل عن بعد[1].

وعليه لا يختلف مضمون الايجاب في عقد العمل عن بعد عن مضمون الايجاب الالكتروني ويتعين محل عقد التفاوض الالكتروني يكون برسم المسار الذي يسلكه الطرفان في تفاوضهما، لذا لابد ان يشمل عقد العمل عن بعد كافة العناصر الجوهرية لعقد التفاوض الالكتروني كتحديد ما يحتاج اليه تحديدا نافيا للجهالة عن طريق تحديد المطلوب من الطرفين للوصول الى العقد النهائي، وذلك بان يحدد محل العقد ونوع العمل المطلوب وطبيعته والكمية التي يحتاج اليها والمواصفات المتطلبة فيه وكيفية تسليم المنتج ومصروفات الشحن والتسليم[2].

كما يجب ان يتناول الايجاب في عقد العمل عن بعد مسألة تحديد الأجر وملحقاته تحديدا كافيا وهل يشمل الأجر اسعار النقل والرسوم الجمركية من عدمه وبيان كيفية الدفع والعملة التي يتم السداد من خلالها والعنوان الذي ينبغي ان يتم الوفاء فيه ولا فان الايجاب يكون غير جازم. وبجانب ذلك يجب تحديد العمل المطلوب بحيث يتراضى عليه الطرفان فإذا اتجه قصد العامل الى القيام بعمل معين، واتجه قصد صاحب العمل الى القيام بعمل آخر فلا ينعقد العقد في هذه الحالة

[1] - أكسوم عيلام رشيدة، المركز القانوني للمستهلك الالكتروني، اطروحة لنيل درجة لدكتوراه الطور الثالث ال ام دي، تخصص قانون خاص داخلي، جامعة مولود معمي تيزي وزو، سنة 2018 ص 132.

[2] - محمد عبد الحفيظ عبد الرحمان، التفاوض الالكتروني في عقد العمل عن بعد: دراسة مقارنة، مجلة دراسات للعلوم الشريعة والقانون، الجامعة الاردنية، مجلد44، عدد04 سنة 2017.ص197.

لعدم التراضي على العمل لذلك ينبغي ان يكون محل العقد ممكن ومشروع طالما ان العقد النهائي المراد ابرامه مشروعا غير ممنوع قانونا. كما ان مسالة مدة التعاقد من المسائل الجوهرية التي يتوجب بيانها في الايجاب الالكتروني عكس مدة العقد التي تبقى اختيارية للأطراف[1].

ثانيا: القبول الالكتروني عن عقد العمل عن بعد

القبول هو الارادة الثانية في العقد الصادرة ممن وجه اليه الإيجاب ويجب ان يتضمن النية القاطعة في التعاقد أن يصدر منجزا بلا قيد أو شرط.

والقبول الالكتروني شأنه شأن القبول التقليدي، لا يخرج عن مضمون هذا الأخير إلا من حيث وسيلة التعبير عنه، بحيث التعبير يتم التعبير عنه بوسائل الكترونية عن طريق شبكة الاتصال الحديثة وعليه فهو يخضع لنفس القواعد والأحكام التي تنظم القبول التقليدي، إلا انه يحتفظ ببعض الخصوصية التي تعود لطبيعته الالكترونية[2].

والقبول الالكتروني في عقد العمل عن بعد لا يختلف عن القبول بصفة عامة سوى انه يتم بواسطة وسائط الكترونية من خلال شبكة الانترنت، فهو قبول عن بعد، كما يجب ان يطابق مطابقة تامة لا يجوز ان يزيد فيه او ينقص عنه وإلا اعتبر رفضا يتضمن ايجابا جديدا، ويكون صريحا كأن يبعث القابل برسالة عبر البريد الالكتروني مثلا تحتوي قبول صريحا لعرض الموجب وقد يكون ضمنيا وذلك بقيام القابل بعمل او تصرف يفيد الموافقة على القبول[3].

[1] - المرجع نفسه، ص 197-198.

[2] - مختاري اكرام، التراضي في العقود الالكترونية: اوجه الحماية والقصو التشريعي، مجلة الفقه والقانون، عدد خاص، سنة2014،ص 37.

[3] - محمدعبد الحفيظ عبد الرحمان، المرجع السابق،ص 200.

وعليه فالتعبير عن القبول الالكتروني قد يكون باستخدام الكتابة عبر البريد الإلكتروني، أو عن طريق اللفظ من خلال غرفة المحادثة، أو تنزيل عن بعد من خلال تنزيل البرامج او المنتوج عبر الانترنت وتحميله على جهاز الكمبيوتر الخاص بالقابل وغيرها من صور القبول عبر الشبكة.

وكما هو الحال من اهم الاشكالات التي يثيرها القبول الإلكتروني اشكالية مدى صلاحية السكوت للتعبير عن القبول الالكتروني فطبقا لقواعد العامة، فان السكوت، شيء سلبي، لا يمكن الأخذ به في التعبير عن الإرادة، الا انه بصورة استثنائية قد يفيد السكوت القبول- السكوت الملابس- أذا كانت طبيعة المعاملة او العرف التجاري تدل على ذلك، او كان هناك تعامل سابق بين المتعاقدين، او كان الايجاب لمصلحة من وجه اليه. وهذا طبقا لنص المادة 68 ق. م.ج.

واختلف الفقه [1] بشان صلاحية السكوت في التعبير عن القبول الالكتروني، وهذا الاختلاف جاء كنتيجة للخاصية المميزة للقبول الالكتروني، الذي يتم عن بعد عبر وسائل الاتصال الحديثة مما يجعله يختلف عن القبول التقليدي .

في حين يرى جانب اخر ان الاعتداد بالسكوت في التعاقد الالكتروني لا يجب ان يؤخذ على اطلاقه كونه توجد حالة وحيدة وهي الحالة الخاصة بوجود تعامل سابق بين المتعاقدين، بمعنى انه يشترط ان يقترن وجود التعامل السابق بظرف اخر يرجح دلالة السكوت على القبول.

الفرع الثاني: مجلس العقد في عقد العمل عن بعد

يختلف العقد الالكتروني عن العقد العادي، فهذا الاخير لا يطرح اشكال كون التعاقد يكون بين الحاضرين يلتقي فيه الايجاب بالقبول في مجلس العقد، بينما التعاقد الإلكتروني -كعقد العمل عن بعد- وخاصة الذي يتم بطريق الاتصال غير

[1] - بوحملة صلاح الدين، المرجع السابق، ص 289.

المباشر فقد يمر وقت طويل بين صدور الايجاب والقبول او بين صدور القبول ووصله الى الموجب. فالمقصود بمجلس العقد؟ وماهي الخصوصية التي يطرحها في عقد التفاوض في العمل عن بعد؟

بالنسبة لمجلس العقد يقصد به الفترة الزمنية التي تبدأ من صدور الإيجاب، والطرفان مقبلان على التعاقد دون اعتراض من أحدهما.

فالفترة الزمنية التي تمتد بين الايجاب والقبول من انشغال المتعاقدين بالعقد، دون وجود شيء يقطعه من اعراض صريح، كالإلغاء الموجب ايجابه، او عدم قبول القابل ونحوه، او اعراض ضمني، كاشتغال الموجب او القابل بأمر لا علاقة له بالعقد، هو ما يسمى بمجلس العقد[1].

وبناء على ما مضى من أن التعاقد الالكتروني الذي يتم بين المتعاقدين عبر الانترنت بالاتصال المباشر يأخذ حكم العقد بين الحاضرين من حيث الزمان وبين غائبين من حيث المكان، وان التعاقد الالكتروني الذي يتم بين المتعاقدين عبر الانترنت بالاتصال غير المباشر يأخذ حكم العقد بين الغائبين زمانا ومكانا.

فمجلس العقد في التعاقد الالكتروني المباشر يكون محدد بزمن الاتصال بين العاقدين، ما داما منشغلين بالتعاقد ولم ينصرفا الى غيره، مهما طال وقت الاتصال .

حيث يصدر الايجاب من المتصل طرف ما ويقبل القابل فورا وعندها ينعقد العقد ويصبح لازما، ا و يصدر الايجاب من الموجب وينشغلان (الموجب والقابل) بالعقد مدة، ثم يقبل الطرف المخاطب وعندها ينعقد العقد يصبح لازما .

[1] - عبد الله محمد أحمد، التعاقد الإلكتروني: دراسة فقهية اقتصادية قانونية، مجلة العلوم الشرعية، جامعة القصيم، مجلد رقمم 04 عدد02.سنة 2011، ص 519.

فلو انشغل الطرف المخاطب بما ليس له علاقة بموضوع العقد وانتهى الاتصال ففي هذه الحالة لا ينعقد العقد اذ انتهى مجلس العقد.

واما لو صدر الايجاب من الموجب وقبل القابل وانقطع الاتصال فجأة يصبح العقد لازما، لكن لو انقطع الاتصال بعد ايجاب الموجب، وقبل قبول الطرف المخاطب فان الايجاب ينتهي، فإذا اتصل القابل مرة اخرى يريد اتمام العقد يعد اتصاله وقبوله صدر من الموجب ايجابا جديدا يحتاج الى قبول اخر.

أما مجلس العقد في التعاقد الالكتروني غير المباشر فيكون مجلس وصول الرسالة عبر البريد الالكتروني اي محل بلوغ الايجاب للقابل، ويتم العقد بقبول القابل، دون اعراضه عن العقد صراحة او ضمنا.

و نظرا لان مجلس العقد في العقود الالكترونية تتم بصفة عامة في مكان افتراضي حكمي لأنه يتم في فضاء الكتروني فقد اعتبرت اغلب قوانين المعاملات الالكترونية في تحديد مكان ابرام العقد هو مكان ارسال الرسالة الالكترونية وهو المكان الذي يقع فيه مقر عمل المنشئ وأن مكان استلامها هو المكان الذي يقع فيه مقر عمل المرسل اليه ما لم يتفق المنشئ والمرسل اليه على غيره.[1]

المطلب الثاني:

مسؤولية الاخلال بعميلة التفاوض الالكتروني في عقد العمل عن بعد

نصت القواعد العامة على ضرورة تنفيذ العقود بحسن نية من قبل المتعاقدين ، وبالتالي اذا اخل أحد الأطراف بتنفيذ التزام المترتب في ذمته تحققت مسؤوليته عن هذا الاخلال وعلى هذا اذا انطوى سلوك المتفاوض على مخالفة مبادئ التفاوض فانه يكون مخطئا وتثور مسؤوليته المدنية التقصيرية.

[1] - محمد عبد الحفيظ عبد الرحمان، المرجع السابق، ص 202.

وفي مجال علاقات العمل فإنه لا يجوز اجبار صاحب العمل او المرشح للعمل عن بعد على ابرام عقد العمل، وانما التنفيذ بمقابل بطريق التعويض هو الحل الأمثل المترتب على قيام المسؤولية المدنية. في عقد العمل عن بعد لكلا طرفي هذا العقد.

الفرع الأول: اركان المسؤولية في مرحلة التفاوض الالكتروني

الاصل في التفاوض انه لا يرتب اثر قانوني ونعني بذلك انه كل طرف له الحرية الكاملة في قطع التفاوض، لكن اذا نتج عن هذا العدول خطأ، فانه يرتب مسؤولية على الطرف المسؤول عن الخطأ ، فالخطأ في مرحلة التفاوض الالكتروني تتعدد صوره وتتمثل في قطع المفاوضات دون اي مبرر مقبول، او بدون سبب جدي، بعد وصولها الى مرحلة متقدمة من النقاش في سبيل ابرام العقد المنشود او عدم تعامله بنزاهة وأمانة وشرف او اهماله التعاون والنصح والإرشاد والتحذير، وقيامه بإفشاء الاسرار والبيانات الشخصية التي يطلع عليها اثناء اجراء عملية التفاوض وانحرافه عن السلوك المألوف بالتفاوض فضلا عن قيامه بتقديم معلومات غير صحيحة او غامضة وهي لازمة للمتعاقد الأخر كونها تتعلق بالخدمة او العمل محل التعاقد او انه قدم معلومات او استعمل طرق احتيالية تظلل صاحب العمل او تخدعه وتدفعه للتعاقد، فضلا عن القيام باستفزازه بأساليب غير مسئولة[1].

وعليه الخطأ في مرحلة التفاوض الالكتروني يأخذ طابعين:

سلبي: كأن يتخذ العامل موقف المتفرج عن محل العقد جاهلا بكل تفاصيل السلعة او البضاعة او الخدمة مثلا سكت او كتم عنه معلومات وبيانات رغم علمه بها سواء كان كتمانا جزئيا او كليا.

[1] - ايناس مكي عبد، المرجع السابق، ص958.

إيجابي: قيامه بتقديم معلومات غير صحيحة فيحمل المتعاقد متوهما صدق وصحة ما بينه له المدين الطرف العامل.

وان وقوع الخطأ من جانب المدين لا يكفي وحده وانما يجب ان يرتب هذا الخطأ ضرر يصيب الأخر وقد يكون الضرر مادي او ادبي فالأول هو خسارة مالية التي تكبدها في سبيل بدء التفاوض والتواصل والمناقشة، كما يتمثل الضرر المعنوي أو الادبي في كل ما يمس المتفاوض في كرامته او سمعته او اعتباره. كما يجب ان يكون هذا الخطأ الحاصل يرتبط نتيجة للفعل بالسبب، اي لابد من توافر عناصر دعوى التعويض من خطأ وضرر وعلاقة سببية مباشرة .

الفرع الثاني: التنفيذ بمقابل او التعويض عن الضرر

يعد التنفيذ العيني هو الاصل في تنفيذ المدين لالتزاماته وفقا للقواعد العامة في القانون المدني/ ولقد اتجه اغلب الفقه الى استبعدا التنفيذ العيني في مجال التفاوض بصفة عامة، وذلك لان الاخذ به يعني الزام الأطراف بمتابعة المفاوضات وصولا الى تحقيق العقد النهائي بالقوة وهو ما يتعارض مع مبدأ الحرية التعاقدية (عقد العمل عن بعد).

لذا اتجه الفقه والقضاء الى الحكم بالتعويض في حالة الخطأ المفضي الى ضرر، ووجوب ان يغطي هذا التعويض كل الاضرار المادية والمعنوية اللاحقة بالمضرور، من جراء قطع المفاوضات بدون سبب جدي، وهي الخسارة الواقعة فعلا التي يعود تحديد مقدارها لقضاة الموضوع وهي تشمل كافة النفقات والمصاريف التي تكبدها المتفاوض المضرور في سبيل التفاوض، اعداد العقد وكذا الناجمة عن ضياع الوقت في الساعات والأيام والشهور التي استغراقها المفاوض بدون جدوى[1].

[1] - جمال ابو الفتوح محمد، المرجع السابق، ص728

وتجدر الاشارة ان نطاق التعويض في مرحلة التفاوض على العقد يصعب تحديد مداه بدقة، لصعوبة اشكالات الخطأ لتقصيري الناجم خلال الفترة الزمنية السابقة على التعاقد، فالتعويض لا يشمل التعويض عن عدم ابرام العقد النهائي ومن تم لا يشمل ايضا المزايا التي كانت ستترتب على ابرام العقد المنشود باعتبارها من الضرر الغير المباشر فهي امور احتمالية يصعب تقدير التعويض بشأنها لصعوبة تقديرها.

ومن اهم التعويضات التي يستطيع قاضي الموضوع تقديرها عند اخلال بمرحلة التفاوض القائم على خطا وضرر وعلاقة سببية بين الاطراف عقد العمل عن بعد:

- **نفقات التفاوض**: تشمل كافة النفقات والمصاريف التي تكبدها المتفاوض المضرور في سبيل التفاوض.

- **الوقت الضائع**: وتتمثل في الساعات والايام والشهور التي استغرقتها المفاوضات.

- **تفويت الفرصة**: وهو الحرمان من فرص جادة وحقيقية لتحقيق كسب احتمالي ، اذا التعويض لا ينصب على الفرصة ذاتها وانما على تفويت فرصة الابرام العقد المنشود محل التفاوض الالكتروني باعتباره ضرر محقق وجب التعويض عنه.

- **الفرصة الضائعة**: لتنفيذ عقود اخرى مع الغير بدلا من العقد المفاوض عليه والذي فشل في ابرامه او ابرام عقد بديل مع شخص اخر او عامل اخر.

الخاتمة

في ختام هذه الدراسة يمكن القول أن مرحلة التفاوض تعد من أهم المراحل في ابرام العقود الإلكترونية حيث أنها تهدف إلى الوصول إلى اتفاق لإبرام العقود ، إذ يقوم الأطراف باتخاذ كافة الاجراءات الازمة لمناقشة مختلف المسائل والنقاط محل التفاوَض ، والتي انطلاقا منها يعبر كل طرف عن ارادته في اكمال ابرام العقد أو الانسحاب منه، هذه المرحلة التي تعتبر مرحلة اختيارية حيث لا تعني الموافقة النهائية ولا يرتب على الانسحاب منها أي مسؤولية ، غير أنها تفرض في مواجهة الأطراف مجموعة من الالتزامات أهمها كتمان الأسرار أي كتمان كل ما تم الإدلاء به من معلومات خلال مرحلة التفاوض.

لكن على الرغم من أهمية هذه المرحلة نجد المشرع الجزائري لم يخصص تنظيم قانوني لها ولا حتى لعقود العمل عن بعد ، إذ تركها تخضع إلى القواعد العامة المتعلقة بالعقود التقليدية.

وعليه فإن أهم **التوصيات** التي يمكن إدراجها هي:

-1يجب على المشرع الجزائري أن ينظم مرحلة التفاوض التي تتم في عقود العمل عن بعد تنظيما خاص بها ، ذلك أن القواعد العامة غير كافية لتغطية كافة التفاصيل التي تتم الكترونيا نظرا لطبيعة الخاصة للعالم الافتراضي بصفة عامة.

قائمة المراجع

أولا: القوانين

1- قانون رقم 05-18 مؤرخ في 24 شعبان عام 1439 الموافق ل10 ماي سنة 2018 متعلق بالتجارة الإلكترونية.

2- قانون رقم 04-02 المؤرخ في 23 يونيو سنة 2004 يحدد القواعد المطبقة على الممارسات التجارية المعدل والمتمم.

ثانيا: الكتب

1- عبد الرزاق السنهوري، الوسيط في شرح القانون المدني الجديد، مج 1، نظرية الالتزام بوجه عام، مصادر الالتزام ، ط3 ، منشورات الحلبي الحقوقية ، بيروت 2000.

ثالثا: المقالات العلمية

1- أرجيليوس رحاب ، مسعودي يوسف، الإطار القانوني للتفاوض في العقد الإلكتروني ، مجلة معالم للدراسات القانونية والسياسية ،عدد 3 ، المركز الجامعي ، تيندوف، مارس 2018.

2- ايناس مكي عبد الناصر، التفاوض الإلكتروني –دراسة مقارنة في ظل بعض التشريعات العربية المعاصرة - ، ، محلة جامعة بابل للعلوم الانسانية مجلد 21 ، عدد3، 2013.

3- كحلول سامي، بن طاية زوليخة ، حماية المستهلك الإلكتروني في مرحلة التفاوض ، مجلة الاجتهاد القضائي ،عدد 14 ، جامعة محمد خيضر ، بسكرة ، 2017.

4- العرايشي عمر أحمد، الطبيعة القانونية لعقد العمل عن بعد في التشريع الأردني، المجلة الأردنية في القانون والعلوم السياسية، مجلد 9، عدد 4، جامعة مؤتة.

5- محمد عبد الحفيظ عبد الرحمان المناصير، النظام القانوني لعقد العمل عن بعد، دراسات علوم الشريعة والقانون، مجلد 46، عدد 1، الجامعة الأردنية، 2019.

6- نجلاء توفيق نجيب فليح، نادية محمد مصطفى قرماز، التكييف القانوني للعمل عن بعد: دراسة مقارنة، مجلة الزرقاء للبحوث والدراسات الإنسانية، مجلد 18، عدد 1، 2018.

7- جمال ابو الفتوح محمد، النظام القانوني لمرحلة المفاوضات على عقد العمل: دراسة مقارنة، مجلة لبحوث القانونية والاقتصادية، عدد 65، كلية الحقوق جامعة المنصورة مصر، سنة 2018.

8- مختاري اكرام، التراضي في العقود الالكترونية: اوجه الحماية والقصو التشريعي، مجلة الفقه والقانون، عدد خاص، سنة2014.

9- عبد الله محمد أحمد، التعاقد الإلكتروني: دراسة فقهية اقتصادية قانونية، مجلة العلوم الشرعية، جامعة القصيم، مجلد رقم 04 عدد02.سنة 2011.

رابعا: الرسائل العلمية

1- أكسوم عيلام رشيدة، المركز القانوني للمستهلك الالكتروني، اطروحة لنيل درجة لدكتوراه الطور الثالث ال ام دي، تخصص قانون خاص داخلي، جامعة مولود معمي تيزي وزو ، سنة 2018

2- -العلي هاشم محمود محمد ، أحمد أبو شنب ، الحماية المدنية للمستهلك في مرحلة ما قبل انعقاد العقد الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة عمان العربية ، كلية القانون ، الأردن، 2018.

إشكالية إقامة المسؤولية الجزائية عن جرائم الذكاء الاصطناعي

The problem of establishing criminal liability for artificial intelligence crimes

د.بليدي دلال أستادة محاضرة أ
جامعة الشاذلي بن جديد الطارف blidi-dallel@univ-eltarf.dz
د.خضارفايزة أستادة محاضرة ب
جامعة الشاذلي بن جديد الطارف f.kheddar@univ-eltarf.dz

ملخص:
تهدف هذه الدراسة إلى البحث عن مدى إمكانية المساءلة الجزائية للذكاء الاصطناعي عن الجرائم المترتبة عنه باعتباره آلية من الآليات المستحدثة في جميع المجالات والذي شهد استخداما كبيرا حيث واكبته جل الدول في الآونة الأخيرة.

و عليه فقد جاءت هذه الورقة البحثية لتسليط الضوء على مفهوم الذكاء الاصطناعي، ووقوفا على التكييف القانوني لإمكانية إسناد الذكاء الاصطناعي الشخصية المعنوية وبالتالي إقامة المسؤولية الجزائية له، مع إبراز موقف المشرع الجزائري من ذلك.

الكلمات المفتاحية: الذكاء الاصطناعي؛ الشخصية المعنوية ؛جرائم الذكاء الاصطناعي ؛ المسؤولية الجزائية.

Abstract:

This study aims to explore the extent to which artificial intelligence (AI) can be held criminally liable for crimes committed using it, given its status as a newly developed mechanism across all fields and its widespread adoption by most countries in recent times. Therefore, this research paper sheds light on the concept of artificial intelligence and examines the legal framework for granting AI legal personality and, consequently, establishing its criminal liability, while highlighting the position of the Algerian legislator on this matter.

Keywords: keywords; *Artificial intelligence; legal personality; AI crimes; criminal liability.*

مقدمة:

في ظل الثورة المعلوماتية واكبت جل الدول مختلف التطورات التكنولوجيا، حيث شهد العالم انفجارا رهيبا فيما يخص التطورات المعلوماتية التي تحولت إلى عصر المعرفة الذكية عن طريق الرقمنة الالكترونية، الأمر الذي أثبت أن الدول الأكثر تطورا في مجال المعلوماتية أصبحت الأكثر قوة إقتصادية وماليا لتحقيق المكانة الدولية .

وعلى إثرها انتشرت تطبيقات الذكاء الاصطناعي في معظم المجالات على سبيل المثال لا الحصر الاستشارات المالية القانونية، العلمية، الاقتصادية، العمل وغيرها من المجالات، ذلك استخدام تقنيات الذكاء الاصطناعي ترتبت عليه العديد من الإشكاليات القانونية، كتحديد الطبيعة القانونية للذكاء الاصطناعي، المساءلة القانونية له سواء المسؤولية المدنية أو الجزائية، فقد ساهم الذكاء الاصطناعي في تطوير الجرائم من الجرائم التقليدية إلى الجرائم الرقمية وصولا إلى جرائم الذكاء الاصطناعي في جميع المجالات ، الأمني الطائرات بدون طيار، الأسحلة الحربية، الروبوتات الذكية، كذلك في مجال البحث العلمي عن طريق استخدام تقنيات

الذكاء الاصطناعي في السرقة العلمية، وغيرها من الجرائم المستحدثة بتقنيات الذكاء الاصطناعي.

فقد انتشرت مؤخرا العديد من جرائم الذكاء الاصطناعي في ظل الاستخدام السيء لهذه التقنية، الأمر الذي يؤدي إلى ضرورة المساءلة الجزائية، لكن هذه المساءلة تطرح العديد من الإشكالات القانونية ، أبرزها إشكالية إسناد الشخصية المعنوية لتقنية الذكاء الاصطناعي ، خاصة في ظل الفراغ التشريعي وغياب النص القانوني الذي يفصل هذه المسألة.

وعلى ضوء ذلك يمكن طرح الإشكالية التالية: إلى أي مدى يمكن إسناد الشخصية المعنوية للذكاء الاصطناعي ومساءلته جزائية؟

وللاجابة عن هذه الإشكالية تم تقسيم الدراسة إلى مبحثين :

المبحث الأول: القواعد الموضوعية للذكاء الاصطناعي

المبحث الثاني: إسناد الشخصية المعنوية لتقنية الذكاء الاصطناعي

المبحث الأول:

القواعد الموضوعية للذكاء الاصطناعي

أصبح الذكاء الاصطناعي ضروريا في الحياة العصرية نظرا لما حققه من تسهيلات وتحولات رقمية في جميع المجالات، الأمر الذي جعله ينتشر بسرعة فائقة قبل تنظيمه بقواعد خاصة من طرف التشريع، بما فيهم المشرع الجزائري الذي واكب التطورات التكنولوجية والرقمية واستحداث تقنيات الذكاء الاصطناعي.

المطلب الأول:

تعريف الذكاء الاصطناعي

بالنسبة للمشرع الجزائري لم يعرف تقنية الذكاء الاصطناعي لقد تعددت تعريفات الذكاء الاصطناعي المقدمة من طرف الفقهاء نظرا لغياب النظام التشريعي له، فقد عرفته منظمة التعاون الاقتصادية والتنمية الاقتصادية على أنه : " نظام قائم على الألة يمكنه لمجموعة معينة من الأهداف التي يحددها الانسان وضع التنبؤات أو توصيات أو قرارات تؤثر على البيانات الحقيقية أو الافتراضية [1].

وفي مقابل ذلك هناك من اعتبر الذكاء الاصطناعي "محاولة جعل الكمبيوتر أو الالة التي تعمل بالبرمجة مثل: الإنسان سواء في تفكيره، أو تصرفاته، أو حله لمشكلاته، وممارسته لكافة نواحي الحياة اليومية، وذلك عن طريق دراسات تجرى على الإنسان وتُستخلص منها نتائج تساعد في تفسير سلوك الإنسان وبرجمة ذلك لتطبيقه على الآلة " [2].

وعرف أيضا على أنه " مجال علمي يهدف إلى بناء آلات قادرة على محاكاة القدرات الذهنية للبشر، مثل التعلم، وحل المشكلات، واتخاذ القرارات، وفهم اللغة، والإبداع. يمكن لهذه الأنظمة العمل بشكل مستقل باستخدام كميات هائلة من البيانات لتقديم تنبؤات وتوصيات، أو إنشاء محتوى جديد"[3] .

[1] - سجى احمد محمد موسى، دور كيانات الذكاء الاصطناعي في التنبؤ والكشف عن الجريمة، رسالة ماجستير، جامعة العلوم الإسلامية العلمية، 2022، ص 11.

[2] - يحي ابراهيم دهشان، المسؤولية الجنائية على جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، العدد 82، 2020، ص110 .

[3] - أنس أبو العون، المسؤولية المدنية عن أضرار الذكاء الاصطناعي، دراسة مقارنة، رسالة ماجستير، الجامعة العربية الأمريكية، جنين، 2023، ص 11.

في حين عرفته المنظمة العالمية للملكية الفكرية WIPO الذكاء الاصطناعي بأنه "تخصص في علوم الكمبيوتر يهدف إلى تطوير آلات وأنظمة قادرة على أداء المهام التي تتطلب ذكاء بشريا مع تدخل بشري محدود أو بدون تدخل بشري[1].

بالإضافة إلى ذلك فإن الذكاء الاصطناعي يعتبر أحد أهم إفرازات الثورة التكنولوجية نتيجة لما انبثق عنها من تطبيقات ذكية التي أثرت وساهمت بشكل كبير في خدمة البشرية، ونظرا لتحقيقه فوائد جد كبيرة في مختلف المجالات وباعتباره وسيلة قوية لزيادة الحيوية الاقتصادية أكدت عليه منظمة اليونسكو وألحت على أهمية ونشر تطبيقاته في التعليم بهدف تعزيز القدرات البشرية ودعم التعاون الفعال بين الإنسان والآلة في الحياة والتعلم والعمل[2].

وعليه يمكن القول إن الذكاء الاصطناعي علم يقوم على تحويل القدرات البشرية إلى قدرات ألية تكنولوجيا بهدف تعويض الذكاء البشري بالذكاء الالي ويحل محله في جل الميادين

المطلب الثاني:

مميزات الذكاء الاصطناعي

من خلال إستقراء التعاريف السابقة للذكاء الاصطناعي يتضح أن الذكاء الاصطناعي باعتباره أكثر التكنولوجيات المنتشرة في العصر الحالي يتميز بالعديد من الخصائص يمكن إجمالها فيما يلي :

[1] - أنس أبو العون، المرجع السابق، ص 11.

[2] - هبة صبحي جلال إسماعيل، توظيف تطبيقات الذكاء الاصطناعي في التعليم بمصر في ضوء تجربتي الإمارات العربية المتحدة و هونج كونج، دراسة تحليلية، مجلة جامعة مطروح للعلوم التربوية و النفسية، المجلد 04، العدد 01، 2023، ص 03.

- **يحل محل الانسان البشري**: ذلك أن الذكاء الاصطناعي أصبح يحل محل الانسان ويقوم بكل المهام المسندة إبه سواء من الناحية الفكرية، أو الجسمية، هو تقنية تحويلية تمكن الآلات من أداء مهام حل المشكلات بطريقة تشبه البشر .من التعرف على الصور وإنشاء محتوى إبداعي إلى وضع تنبؤات تعتمد على البيانات .

- **القدرة على إتخاذ القرارات** : يمكن لأنظمة الذكاء الاصطناعي إتخاذ قرارات مستقبلية استنادا إلى البيانان والفرضيات المقدمة، وذلك عن طريق تحليل الأنماط والاتجاهات.

- **التبؤ بالأحداث المستقبلية** :وذلك من خلال التنبؤ بالنتائج المستقبلية .

- **إنشاء مستوى أصلي** : يعب التميز بينه وبين الحقيقة من خلال الصور والفيدوهات التي يقوم بإعدادها [1].

المبحث الثاني:

إسناد الشخصية المعنوية للذكاء الاصطناعي

من بين سلبيات العولمة الرقمية استحداث عصر جرائم الذكاء الاصطناعي والروبوتات، بحيث تكون ظاهرةً إجراميَّةً جديدةً يقوم بارتكابها مجرمٌ من خلال أنظمة الذكاء الاصطناعيّ والروبوتات؛ فما مدى إمكانيَّة تطبيق المسئوليَّة الجنائيَّة على تلك الجرائم؟ وهل يوجد تأثيرٌ للذكاء الاصطناعيّ على تلك الجرائم؟ وهل يتم الاستفادة من تلك الأنظمة من أجل مساعدة الدول في تطوير أجهزتها لتحقيق العدالة الجنائية، ومنع هذه الجرائم، لذلك سارعت الكثير من الدول -ولا

[1] - البراء جمعان محمد الشهري، استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة، الإصدار السابع، العدد 68، حزيران، 2024، ص 79.

سيما المتقدمة – والدول العربية، لتَّصدي لتلك الظاهرة؛ وذلك بتشريع وسن القوانين التي تمنع من ارتكاب تلك الجرائم[1].

الأمر الذي أدى بالفقهاء إلى البحث عن معيار لضبط إشكالية تمتع الذكاء الاصطناعي بالشخصية المعنوية من عدمه، فقد تباينت الأراء الفقهية بين مؤيد و معارض، ذلك أن الشخصية المعنوية تعتبر أكبر عائق لإقامة المسؤولية الجزائية التي ترتكز على الشخصية القانونية له .

المطلب الأول:

الاتجاه المعارض لإسناد الشخصية المعنوية للذكاء الاصطناعي

تعد مسألة ما إذا كان الذكاء الاصطناعي له من الشخصية القانونية من عدمه مسألة فقهية أكثر ، فقد خاض فيها الفقه و رجال القانون سنوات بحثًا عن اتفاق سليم يتفق مع القواعد العامة الواردة بصدد الأشخاص، إلا أن الأمر حتى وقتنا الراهن ما زال يشكل عقبة بين الاعتراف به، وعدم الاعتراف به لا سيما وأنه لا يمكن الاعتراف بالشخصية التامة لنظم الذكاء الاصطناعي، ومن جانب آخر لا يمكن إهمال حق المضرور من الجريمة، الأمر الذي يعد بحاجة إلى تدخل تشريعي، لا سيما وأن هناك بعض نظم الذكاء الاصطناعي تملك إرادة ذاتية في اتخاذ القرار، لذلك وحتى يتم إعمال تدخل تشريعي يُمكننا القول أن نظم الذكاء الاصطناعي لها شخصية قانونية محدودة وفي نطاق ضيق [2].

[1] - منى محمد العتريس الدسوقي، جرائم تقنيات الذكاء الاصطناعي و الشخصية القانونية الالكترونية المستقلة (دراسة مقارنة)، مجلة البحوث القانونية والاقتصادية ، المجلد 12، الهدد 81، سبتمبر 2022جامعة المنصورة، ص 1147.

[2] - ريم خلفان سعيد راشد الكندي، النطاق الشخصي للمسؤولية الجنائية عن أخطاء الذكاء الاصطناعي، رسالة ماجستير، ديسمبر 2024، جامعة الشارقة، ص 13.

ويستند هذا الاتجاه على أن منح الشخصية المعنوية للذكاء الاصطناعي، لان هذه الانظمة لم تتطور الى درجة الذكاء البشري، فهي مجرد كائنات جامدة لا تتمتع بالإدراك والوعي، وبذلك لا يمكن ان تكون لها اهلية اداء، فهي لا تملك التميز بين الخطأ والصواب[1].

ذلك أن إشكالية منح الشخصية المعنوية تكمن في تطبيق أحكام المسئولية الجنائية عن أخطاء الذكاء الاصطناعي لا سيما إذا كان الخطأ صادرًا عن الشخص الاعتباري أو نظم الذكاء الاصطناعي [2].

ويعد إشارة البرلمان الأوروبي للقواعد الأوروبية المتعلقة بالروبوت سنة 2017 في القانون المدني، تلميحا إلي أن شخصا قانونيا جديدا يلوح في الأفق، و بالتالي فمن المتصور ترتيب مسئوليته وحتي إن كانت تلك المسئولية حتي الآن مدنية إلا أن القانون المدني ليس بعيدا عن نظيره الجنائي، فالمسئولية التقصيرية هي في ذاتها مسئولية جنائية، إن كان النص المخالف ذو طبيعية جنائية، طالما توافرت الشخصية القانونية [3].

ويؤسس هذا الاتجاه موقفه على أن منح الشخصية القانونية للذكاء الاصطناعي يرونا أن القانون فرق بين الاشخاص والأشياء، فالشيء أكثر التصاقا واشد ارتباطا بالحق العيني منه بالحق الشخصي، فالحق العيني سلطة قانونية مباشرة على الشيء محل الحق، ومن ثم يتصل صاحب الحق بالشيء اتصالا مباشرا دون وسيط، فالشيء هو كل ما يصلح ان يكون محلا للحقوق المالية، وعليه كل ما هو غير انساني يعتبر من الاشياء، وبالتالي لا يمكن ان تكون لها شخصية قانونية [4].

ذلك أن تعتبر المسؤولية القانونية المترتبة على استخدام الذكاء الاصطناعي و الاعتماد عليه من بين أهم الإشكالات و أكثرها تعقيدا على الإطلاق، إذ تظهر العديد

---

[1] - منى محمد العتريس الدسوقي، المرجع السابق، ص 1162.

[2] - ريم خلفاوي سعيد راشد الكندي، المرجع السابق، ص 15.

[3] - ريم خلفاوي سعيد راشد الكندي، المرجع نفسه، ص 15.

[4] - بن عثمان فريدة، لذكاء الاصطناعي (مقاربة قانونية)، مجلة دفاتر السياسة والقانون، المجلد 12، العدد 02، 2020، ص161.

من التساؤلات حول تحديد المسؤولية القانونية حال ارتكاب أخطاء ناتجة عن هذه الأنظمة الذكية و خاصة في المجال القانوني و في المهن القانونية خاصة، فاتخاذ قرار قد يؤدي إلى خسارة قضية أو نتائج في خسارة مالية، فبالرغم من تعدد المزايا للذكاء الاصطناعي المعززة و القادرة على تحليل البيانات و اتخاذ قرارات دقيقة إلا انه قد يحدث أن يتخذ قرارات غير عادلة أو غير صحيحة حتى عند تحليله و قد يحدث أن تكون البيانات التي يعتمد عليها غير مكتملة أو تحتوي على تحيزات، أو بسبب عدم قدرته على تقدير السياقات الاجتماعية أو الإنسانية كالمحامي أو القاضي البشري، مما قد يؤدي به إلى اتخاذ قرارات غير صائبة خاصة في الحالات التي تتطلب حكما أخلاقيا أو شخصيا [1].

ويستند أصحاب هذا الاتجاه إلى أن عدم إمكانية إنزال أحكام المسؤولية الجنائية إلا على أن الشخص الطبيعي فحسب على الحجج التالية:

1- الشخص الطبيعي وحده هو المخاطب بالقاعدة القانونية حيث لديه الإرادة التي أساس المسؤولية الجنائية، ذلك أن الأهلية الجنائية تستلزم صلاحية الشخص لارتكاب الجريمة وتسليط العقاب عليه، وهذا ما لا يمكن تطبيقها على كيان الذكاء الاصطناعي، لأن عدم تمتع هذا الأخير بالشخصية القانونية.

2- صعوبة توقيع العقاب على الذكاء الاصطناعي فلا يمكن توقيع العقوبات السالبة للحرية على الروبوت باعتباره ذو شخصية قانونية وبالتالي عدم تحقيق الردع العام والخاص في مكافحة الجرائم بصفة عامة و جرائم الذكاء الاصطناعي بصفة خاصة .

[1] - محمد شحادة إسماعيل، تأثير الذكاء الاصطناعي على المهن القانونية، مجلة الباحث العربي، المجلد 06، العدد 01، 2025، ص 63.

3- الفراغ التشريعي في تحدد الطبيعة القانونية للذكاء الاصطناعي ومنحه الشخصية المعنوية الأمر الذي ترك غموض في إقامة المسؤولية الجزائية و صعوبة تطبيقها مع مبدأ شرعية الجريمة والعقوبة [1].

4- أن الأشخاص المعنوية مجرد افتراض قانوني اقتضته الضرورة من أجل تحقيق مصالح معينة، الأمر الذي يحول دون إمكانية تصور إسناد الجريمة إليه.

5- التسليم بمساءلة الأشخاص المعنوية جزائيا يتنافى مع أحد أهم مبادئ القانون الجزائي، وهو **مبدأ شخصية العقوبة** [2].

وعليه يمكن القول أنه لا يمكن إسناد الشخصية المعنوية للذكاء الاصطناعي نظرا لصعوبة تحديد طبيعته القانونية هذا من جهة، ومن جهة أخرى غياب النص التشريعي الذي فتح الجدال الفقهي بين المؤيد والمعارض لإسناد الشخصية القانونية.

بل الأكثر من ذلك لا يمكن توقيع الجزاء وعقاب مرتكب جرائم الذكاء الاصطناعي لأنه يظل كيان ألي يحل محل البشر في التنفيذ والابتكار، أما المساءلة القانونية تبقى صعبة إقامتها لهيكل رقمي.

المطلب الثاني: الاتجاه المؤيد لإسناد الشخصية القانونية للذكاء الاصطناعي

حين يرى دعاة الاتجاه المؤيد للمسؤولية الجزائية للأشخاص المعنوية أن تلك الأشخاص تملك وجودا حقيقيا بسبب المصالح الخاصة التي تقوم بتحقيقها والتي

[1] - صابرين جابر محمد، اشكالية تطبيق احكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي مجلة البحوث القانونية والاقتصادية، المجلد 8، العدد 01، 2025، ص94.

[2] - محمود داوود يعقوب، ذاتية المسؤولية الجزائية للشخص المعنوي، وحدة البحث في العلوم الجزائية و الاجرام، كلية الحقوق والعلوم السياسية، جامعة المنار تونس، ص 4 .

من شأنها أن تجعل لها شخصية مستقلة ومتميزة عن شخصيات أصحاب المصلحة فيها، وفي ذلك يستندون على الحجج التالية :

- الشخصية المعنوية ذات وجود حقيقي لا جدال فيه من الناحية القانونية، ويعترف لها القانون بإرادة متميزة عن الأشخاص الطبيعيين المكونين لها ويتجسد ذلك من خلال الإقرار بوجود مصالح مستقلة للشخص المعنوي، وذمة مالية مستقلة [1].

- أن للأشخاص المعنوية وجوداً حقيقياً بسبب المصالح الخاصة التي تقوم بتحقيقها، والتي من شأنها أن تجعل لها شخصية مستقلة ومتميزة عن شخصيات أصحاب المصلحة فيها.

- قانونا يمكن للأشخاص المعنوية أن تكون لها إرادة خاصة معبر عنها بواسطة أعضائها، وهذه الإرادة مستقلة وقد لا تتماشى بالضرورة وإرادة العناصر الطبيعية التي ساهمت في بلورتها.

- ان المسؤولية في القانون لا تقوم إلا لمن يتمتع بالشخصية القانونية ان كانت طبيعية او معنوية.
- ان منح الشخصية القانونية للذكاء الاصطناعي تمكنه من اكتساب ذمة مالية مستقلة بما انه قادر على ابرام العقود من بينها عقود التامين، والتي يكون الغرض منها تعويض الضرر الناجم عنها، وهذا ما يوفر نوعا من الضمان للمتضرر[2].

فالذكاء الاصطناعي من وجهة نظر أنصار الفكر الحديث أن مساءلته حقيقة لا يمكن إنكارها أو تجاهلها، ذلك لضرورة الاعتراف بأهليته القانونية فهو ليست مجرد خيال كما يزعم الاتجاه المعارض، بل هو حقيقة وكانت لها وجودها ولها كيان الي في عالم القانون، كما أن إرادته خاصة ومستقلة عن مستخدمي تقنيات الذكاء

[1] - محمود داوود يعقوب، المرجع السابق، ص 14.

[2] - يحي ابراهيم دهشان، المرجع السابق، ص 39.

الاصطناعي أو منتجه أو مالكه فلكل منهم صفة قانونية مستقلة تتمتع بالشخصية القانونية ولها حقوق وتتحمل إلتزامات ، فحسب هذا التيار الحديث فان شخصية الذكاء الاصطناعي تتمثل في المهام والنتائج التي حققا محل الانسان وهذا ما جسده على أرض الواقع في شتى المجالات .

المطلب الثالث:

موقف المشرع الجزائري

بالنسبة لموقف المشرع الجزائري من إمكانية إسناد المسؤولية الجزائية للذكاء الاصطناعي، فكما سبق القول أن المشرع واكب عصر العولمة والرقمنة، إلا أنه في تحيين ترسانته القانونية لم يخصص للذكاء الاصطناعي تنظيم قانوني خاص في ترسانته القانونية حتى بعد إستحداثه لقانون الإجراءات الجزائية بموجب القانون رقم 25-14 [1] الذي بموجبه ألغى قانون الإجراءات الجزائية القديم ، حيث تطرق لإجراءات جدية لمساءلة الشخص المعنوي إلا أنه لم يشير ضمنها إلى الذكاء الاصطناعي .

خاتمة:

إن موضوع إسناد المسؤولية الجزائية للذكاء الاصطناعي يعتبر أكبر عائق قانوني في جل التشريعات بصفة عامة والتشريع الجزائري بصفة خاصة، سواء بتعديل الترسانة القانونية وإضافة تنظيم خاص بالذكاء الاصطناعي مثل الدول التي وضعت قواعد قانونية تنظيمية خاصة به، أو خلو الترسانة القانونية من تشريع ينظم الذكاء الاصطناعي كالمشرع الجزائري، الأمر يطرح إشكالية المساءلة الجزائية للذكاء الاصطناعي من عدمه عن الجرائم المترتبة عنه .

[1] - المؤرخ في 03 أوت 2025، المتضمن قانون الإجراءات الجزائية، العدد 54، 2025 .

وعلى إثر تم التوصل إلى جملة من النتائج أهمها :

- صعوبة تحديد الطبيعة القانونية للذكاء الاصطناعي .
- غياب نص تشريعي يجرم إساءة إستخدام الذكاء الاصطناعي .
- صعوبة توقيع الجزاء على الذكاء الاصطناعي ومساءلته جزائيا.
- إستحالة تطبيق قواعد المسؤولية الجزائية للشخص المعنوي المنصوص عليها في قانون الإجراءات الجزائية .

وعلى ضوء ذلك يمكن وضع بعض الإقتراحات :

- إلزامية تحديد المسؤول جزائيا عن جرائم الذكاء الاصطناعي لتوقيع الجزاء عليه.
- تشديد الرقابة القانونية والالكترونية على تقنيات الذكاء الاصطناعي .
- استحداث هئيات إلكترونية تعمل على رقابة استخدام الذكاء الاصطناعي خاصة الاستغلال السيء وغير القانوني له .
- ضرورة مواكبة التشريعات لمختلف التطورات التكنولوجيا في وضع الترسانة القانونية .

قائمة المصادر و المراجع:

1- القانون رقم 25-14 - المؤرخ في 03 أوت 2025، المتضمن قانون الإجراءات الجزائية، العدد 54، 2025 .

2- منى محمد العتريس الدسوقي، جرائم تقنيات الذكاء الاصطناعي و الشخصية القانونية الالكترونية المستقلة (دراسة مقارنة)، مجلة البحوث القانونية والاقتصادية ، المجلد 12، العدد 81، سبتمبر جامعة المنصورة ، 2022.

3- محمد شحادة إسماعيل، تأثير الذكاء الاصطناعي على المهن القانونية، مجلة الباحث العربي، المجلد 06، العدد 01، 2025.

4- ريم خلفان سعيد راشد الكندي، النطاق الشخصي للمسؤولية الجنائية عن أخطاء الذكاء الاصطناعي، رسالة ماجستير، ديسمبر 2024، جامعة الشارقة.

5- بن عثمان فريدة، لذكاء الاصطناعي (مقاربة قانونية)، مجلة دفاتر السياسة والقانون، المجلد 12، العدد 02، 2020، ص161.

6- أنس أبو العون، المسؤولية المدنية عن أضرار الذكاء الاصطناعي، دراسة مقارنة، رسالة ماجستير، الجامعة العربية الأمريكية، جنين، 2023.

7- صابرين جابر محمد، اشكالية تطبيق احكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي مجلة البحوث القانونية والاقتصادية، المجلد 8، العدد 01، 2025.

8- البراء جمعان محمد الشهري، استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة، الإصدار السابع، العدد 68، حزيران، 2024.

9- محمود داوود يعقوب، ذاتية المسؤولية الجزائية للشخص المعنوي، وحدة البحث في العلوم الجزائية و الاجرام، كلية الحقوق والعلوم السياسية، جامعة المنار تونس.

10-سجى احمد محمد موسى، دور كيانات الذكاء الاصطناعي في التنبؤ و الكشف عن الجريمة، رسالة ماجستير، جامعة العلوم الإسلامية العلمية، 2022.

11-يحي ابراهيم دهشان، المسؤولية الجنائية على جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، العدد 82، 2020.

12-هبة صبحي جلال إسماعيل، توظيف تطبيقات الذكاء الاصطناعي في التعليم بمصر في ضوء تجربتي الإمارات العربية المتحدة و هونج كونج، دراسة تحليلية، مجلة جامعة مطروح للعلوم التربوية و النفسية، المجلد 04، العدد 01، 2023.

الجرائم الإلكترونية الموجهة ضد الطفل في الجزائر: قراءة قانونية في صورها وآليات مكافحتها

Cybercrimes Targeting Children in Algeria: A Legal Analysis of Their Forms and Mechanisms of Combating Them

د/ قفاف فاطمة

المركز الجامعي - بريكة - fatma.gaffaf@cu-barika.dz

أ.د/ محمودي سماح

المركز الجامعي – بريكة - samah.mahmoudi@cu-barika.dz

ملخص:

يشكل تطور الفضاء الرقمي سيفًا ذا حدين، إذ أتاح فرصًا كبيرة للتعلم والتواصل، لكنه في المقابل فتح المجال أمام جرائم جديدة تمسّ فئة الأطفال بوصفهم الفئة الأكثر هشاشة في المجتمع. ومن هذا المنطلق، تهدف هذه الدراسة إلى التعرف على أبرز أنواع الجرائم الإلكترونية التي يتعرض لها الأطفال في البيئة الرقمية، وتحليل مظاهرها المختلفة مثل الاستغلال الجنسي، والابتزاز، والتجنيد الإرهابي، والاعتداء على البيانات الشخصية، مع محاولة إبراز الآليات القانونية والمؤسساتية والوقائية التي يمكن من خلالها الحد من هذه الظاهرة وحماية الطفل من مخاطرها.

لقد أظهرت الدراسة، من خلال توضيح بعض جوانب الحماية في التشريع الجزائري وبعض الآليات المطبقة في هذا المجال، أنّ حماية الطفل من الجرائم الإلكترونية ما تزال تواجه عدة تحديات تتعلق بتطور أساليب الجريمة الرقمية، وضعف الوعي المجتمعي، والحاجة إلى تنسيق أوثق بين المؤسسات المعنية بالحماية. ورغم الجهود المبذولة، فإن الإطار القانوني والمؤسساتي يحتاج إلى مزيد من التفعيل والتحديث لمواكبة التغيرات المتسارعة وضمان بيئة رقمية آمنة للأطفال.

الكلمات المفتاحية :الطفل؛ الجرائم الإلكترونية؛ الحماية القانونية؛ الانترنت؛ البيئة الرقمية.

AbstractM *The development of the digital space represents a double-edged sword: it has created vast opportunities for learning and communication, yet at the same time, it has opened the door to new forms of crime that particularly target children, who are among the most vulnerable groups in society. Accordingly, this study aims to identify the main types of cybercrimes committed against children in the digital environment, and to analyze their manifestations — including sexual exploitation, extortion, terrorist recruitment, and violations of personal data. The study also seeks to highlight the legal, institutional, and preventive mechanisms through which these crimes can be mitigated, and children can be better protected from their dangers. The findings reveal that, despite the existence of several protective measures within Algerian legislation and certain institutional mechanisms, the protection of children from cybercrimes still faces significant challenges. These challenges stem from the rapid evolution of digital criminal methods, the lack of societal awareness, and the insufficient coordination between relevant institutions. Despite the progress achieved, the legal and institutional framework remains in need of further activation and modernization to keep pace with technological changes and to ensure a safer digital environment for children.*

Keywords*: Child ; Cybercrime; Legal Protection ; Internet; Digital Environment.*

مقدمة:

يشهد العالم المعاصر تطورا متسارعًا في مجال التكنولوجيا الرقمية ووسائل الاتصال الحديثة، وهو تطور أفرز مظاهر إيجابية عديدة على مختلف المستويات الاقتصادية والاجتماعية والتربوية، غير أنّه أفرز بالمقابل تحديات خطيرة مست حياة الأفراد والمجتمعات، وفي مقدمتها فئة الأطفال باعتبارهم الشريحة الأكثر هشاشة وضعفًا في مواجهة هذه المخاطر. لقد أضحت البيئة الرقمية بيئة مزدوجة تجمع بين فرص التعلم والترفيه من جهة، ومجالًا مفتوحًا للانتهاكات والجرائم الموجهة ضد الطفل من جهة أخرى، إذ أصبحت الجرائم الإلكترونية من أبرز أشكال التهديد التي تطال الطفل في عالم اليوم، سواء تعلق الأمر بالاستغلال الجنسي عبر الإنترنت، أو الابتزاز والتهديد، أو التجنيد الإرهابي، أو حتى الاعتداء على بياناته الشخصية.

تنبع أهمية هذه الدراسة من كونها تلامس موضوعًا ذا حساسية بالغة في ظل التحولات الرقمية الراهنة، إذ لم تعد حماية الطفل تقتصر على الفضاء الواقعي فحسب، بل امتدت إلى الفضاء الافتراضي الذي يشكل اليوم جزءًا لا يتجزأ من حياته اليومية. وتبرز أهمية البحث كذلك في محاولة تسليط الضوء على بعض صور الجرائم الإلكترونية التي تستهدف الطفل في البيئة الرقمية، مع التركيز على الآليات القانونية والمؤسساتية والوقائية التي يعتمدها التشريع الجزائري لحمايته من هذه المخاطر. إن معالجة هذا الموضوع تكتسي بعدًا وقائيًا وإنسانيًا في آن واحد، ذلك أنّ حماية الطفل رقمياً تمثل في جوهرها حماية لمستقبل المجتمع، كما تساهم في إثراء النقاش القانوني حول مدى استجابة المنظومة التشريعية الوطنية للتطورات التقنية الحديثة.

وتهدف هذه الدراسة إلى إبراز الإطار القانوني الذي ينظم حماية الطفل من الجرائم الإلكترونية في الجزائر، من خلال تحليل بعض الجوانب القانونية ذات الصلة، واستعراض أهم المؤسسات والهيئات التي تضطلع بدور فعّال في الوقاية والمكافحة، مع بيان الجهود الوقائية والاجتماعية الرامية إلى تعزيز ثقافة الأمان الرقمي لدى الأطفال وأسرهم. كما تسعى الدراسة إلى تحديد أهم التحديات التي تواجه حماية الطفل في البيئة الرقمية في ظل تزايد تنوع وخطورة الجرائم الإلكترونية.

وانطلاقًا من ذلك، يمكن طرح الإشكالية المحورية التالية:

ما هي أهم صور الجرائم الإلكترونية التي تستهدف الطفل، وما هي الآليات التي يقرها التشريع الجزائري لحمايته منها؟

وللإجابة عن هذه الإشكالية اعتمدنا الدراسة المنهج الوصفي التحليلي، من خلال وصف الظاهرة الإجرامية الرقمية التي تمس الأطفال، وذلك بالتحليل القانوني الجرائم الالكترونية، ومقاربة دور المؤسسات الوطنية والجهات الوقائية في مواجهة

هذه الجرائم، مع الاستعانة ببعض المقاربات التوضيحية لإبراز أوجه القصور والتحديات القائمة.

وانسجامًا مع طبيعة الموضوع وأبعاده، تم تقسيم هذا البحث إلى مبحثين أساسيين على النحو الآتي:

المبحث الأول: بعض صور الجرائم الإلكترونية التي تستهدف الأطفال عبر وسائل الاتصال الحديثة.

المبحث الثاني: الآليات الحمائية المؤسساتية والوقائية من الجرائم الإلكترونية ضد الأطفال.

المبحث الأول: بعض صور الجرائم الإلكترونية التي تستهدف الأطفال عبر وسائل الاتصال الحديثة

أضحت وسائل الاتصال الإلكترونية ومواقع التواصل الاجتماعي فضاءً موازياً للعالم الواقعي، يتميز بخصوصياته المستحدثة ومخاطره المتعددة التي باتت تتقاطع مع واقعنا المعاش. وفي ظل هذا التحول الرقمي المتسارع، برزت الحاجة الملحة إلى حماية الفئات الهشة، وعلى رأسها الأطفال، من الانتهاكات التي قد تطالهم عبر هذه الوسائط، الأمر الذي دفع المشرّع الجزائري إلى التدخل التشريعي من خلال سن قوانين خاصة تهدف إلى الوقاية والزجر، وتحديداً القانون رقم 15-12 المتعلق

بحماية الطفل [1]، والقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[2].

تشكل الجرائم الإلكترونية تهديداً مباشراً لسلامة واستقرار الأفراد، وتزداد خطورتها حينما تستهدف الأطفال، خاصة في ظل ضعف الرقابة الأسرية وغياب التوجيه السليم، مما يجعلهم عرضة للوصول إلى محتويات غير لائقة أو الوقوع ضحية للاستغلال الجنسي من قبل الجناة المحتملين.

وقد تتخذ هذه الجرائم صوراً متعددة، من بينها المساس بالشرف والاعتبار من خلال إنتاج مواد إباحية لأغراض انتقامية، أو نشر معلومات شخصية تمس بسمعة الطفل عبر الإنترنت، أو إرسال صور ورسائل ذات طابع جنسي عبر الهواتف الذكية. وغالباً ما يعجز الأطفال، بسبب قلة نضجهم، عن إدراك حجم المخاطر المترتبة عن سلوكياتهم الإلكترونية، وما قد يترتب عنها من تداعيات خطيرة على أنفسهم وعلى الآخرين.

تتباين صور الجرائم الإلكترونية وتختلف أنواعها، فمنها ما يستهدف النظام الإلكتروني ذاته، كجرائم التزوير الإلكتروني، والاعتداء على المعلومات، والاحتيال الإلكتروني، والاعتداء على التحويلات المالية. ومنها ما يُرتكب بواسطة هذه الوسائل ويستهدف الأطفال بشكل مباشر، مثل جرائم الابتزاز، والتهديد الإلكتروني، والاتجار بالأطفال، والتجنيد الإرهابي، والانتحار الإلكتروني، والتهجير، فضلاً عما يعرف بجرائم المخدرات الإلكترونية.

[1] القانون رقم 15/ 12 المتضمن قانون الطفل؛ المؤرخ في 15 يوليو 2015 الجريدة الرسمية العدد 39؛ الصادرة بتاريخ 19 يوليو 2015.

[2] القانون رقم: 09/04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها؛ الجريدة الرسمية؛ العدد 47 الصادرة بتاريخ 16 اوت 2009 .

وتكمن خطورة هذه الجرائم في طبيعتها الخاصة، حيث تُرتكب في فضاء افتراضي غير ملموس، وتتميز بالغموض والسرية وسرعة التنفيذ، فضلاً عن صعوبة إثباتها وإمكانية ارتكابها من أي مكان في العالم.

وعليه أصبحت الجرائم الإلكترونية في العصر الرقمي تشكل تحديًا حقيقيًا أمام حماية الطفل، إذ لم تعد الاعتداءات مقتصرة على الفضاء الواقعي، بل امتدت إلى الفضاء الافتراضي الذي أتاح للمجرمين إمكانيات جديدة لارتكاب جرائمهم بوسائل يصعب رصدها أو إثباتها أحيانًا. وتعد فئة الأطفال من أكثر الفئات تعرضًا لمخاطر هذه الجرائم نظرًا لضعف إدراكهم الرقمي وقلة وعيهم القانوني، مما يجعلهم هدفًا سهلاً للاستغلال عبر الإنترنت. وفي هذا السياق، تبرز الحاجة إلى دراسة بعض صور الجرائم الإلكترونية التي تستهدف الطفل من خلال وسائل الاتصال الحديثة، لما تمثله من تهديد مباشر لسلامته الجسدية والنفسية والبيانية، ولما تثيره من إشكالات قانونية وأخلاقية معقدة تتطلب استجابات تشريعية ومؤسساتية فعّالة.

المطلب الأول: جرائم الاستغلال الجنسي للأطفال في البيئة الرقمية

تُعد جرائم الاستغلال الجنسي للأطفال من أخطر التهديدات التي تواجه الطفولة المعاصرة، ليس فقط لما تنطوي عليه من انتهاك صارخ لبراءة الطفل وكرامته، بل لأنها باتت تتخذ أشكالًا متطورة تتجاوز النمط التقليدي إلى صور إلكترونية مستحدثة بفعل الثورة التكنولوجية في الإعلام والاتصال. لقد أفرزت البيئة الرقمية نمطين رئيسيين من هذه الجرائم، يُميز كل منهما طبيعة الدور الذي يُسند للطفل داخل الجريمة.

أولًا: الطفل كمتلقٍ للاستغلال الجنسي الرقمي

في هذا النمط، لا يكون الطفل طرفًا مباشرًا في الفعل الجنسي، بل يُستهدف كمستهلك أو متلقٍ لمحتوى جنسي غير لائق، يُستخدم فيه التحريض على الانحراف

الأخلاقي والدعارة عبر وسائل متعددة مثل الصور الإباحية، المحادثات الجنسية، ومواقع البث الإباحي. وتُدار هذه العمليات غالبًا من قبل شبكات إجرامية منظمة، تتخذ من هذه الأفعال وسيلة للربح التجاري عبر توزيع المحتوى الجنسي الذي يُظهر مشاركة الأطفال فيه [1].

ثانيًا: الطفل كموضوع للاستغلال الجنسي المباشر

أما النمط الثاني، فيتجسد في إشراك الطفل بشكل فعلي في الأفعال الجنسية، سواء عبر الإيحاءات أو العروض الصريحة التي تُظهر أجزاء حساسة من جسده، ويتم توثيقها ونشرها عبر منصات إلكترونية. هذا النوع يُعد من أشد صور الانتهاك، إذ يُوظف الطفل كأداة جنسية في محتوى يُنتج ويُسوّق بشكل ممنهج[2].

ثالثا: الإطار التشريعي الجزائري لمكافحة الاستغلال الجنسي للأطفال عبر الإنترنت

في ظل التحديات المتزايدة التي تفرضها جرائم الاستغلال الجنسي للأطفال عبر شبكة الإنترنت، تباينت المواقف التشريعية بين الدول؛ إذ بادرت بعض الدول إلى سن قوانين خاصة لمعالجة هذه الظاهرة، بينما اكتفت غالبية الدول العربية بتطبيق

[1] تشير دراسة منشورة في مجلة "les cahiers du LADREN" إلى أن البيئة الرقمية أصبحت عاملاً رئيسيًا في تفشي هذه الجرائم، نظرًا لسهولة الوصول إلى المحتوى وسهولة استدراج الأطفال عبر الإنترنت. انظر :ا عبشات امينة، عماري ابراهيم: لبيئة الرقمية وعلاقتها بالجرائم الواقعة على الأطفال - الاستغلال الجنسي الالكتروني نموذجا - ، مجلة دفاتر حقوق الطفل، المجلد 13 العدد سنه 2022 ، الصفحة 135.

[2] توضح الدراسة نفسها أن هذا النوع من الجرائم يُصنف ضمن الجرائم الجنسية المباشرة، ويُعد من أخطر صور الإجرام الإلكتروني نظرًا لتأثيره النفسي والاجتماعي على الطفل. المرجع السابق، الصفحة 137.

أحكام قانون العقوبات التقليدي، إلى جانب الاستناد إلى التشريعات المتعلقة بالأخلاق والآداب العامة لمعاقبة مرتكبي هذه الجرائم[1] .

وفي هذا السياق، اتخذت الجزائر خطوات تشريعية مهمة تهدف إلى تعزيز حماية الأطفال من مخاطر الاستغلال الجنسي عبر الإنترنت، وذلك من خلال المصادقة على عدد من الاتفاقيات والمراسيم الرئاسية ذات الصلة، أبرزها:

• **المرسوم الرئاسي رقم 92-461** :الذي يتضمن التصديق بتحفظ على اتفاقية حقوق الطفل المعتمدة بتاريخ 20 نوفمبر 1989، والتي دخلت حيز التنفيذ في 2 سبتمبر 1990. وقد نصت المادة 34 من الاتفاقية على التزام الدول الأطراف بحماية الطفل من جميع أشكال الاستغلال الجنسي، بما في ذلك استخدامه في أعمال الدعارة.

• **المرسوم الرئاسي رقم 03-242** :الذي يتضمن التصديق على الميثاق الإفريقي لحقوق الطفل ورفاهيته، المعتمد بتاريخ 11 يوليو 1990، والذي يعزز الحماية القانونية للأطفال في القارة الإفريقية من مختلف أشكال الانتهاك والاستغلال.

• **المرسوم الرئاسي رقم 299** :المتعلق بالمصادقة على البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلالهم في البغاء والمواد الإباحية، والذي يمثل خطوة إضافية نحو تعزيز الإطار القانوني الوطني لمكافحة هذه الجرائم.

1 قشيوش، رحمونة: "الحماية القانونية للطفل ضحية الاستغلال الجنسي في ظل الفضاء الرقمي ".*مجلة نوميروس الأكاديمية*، المجلد 1، العدد الثاني، يونيو 2020، ص. 227.

تُظهر هذه المراسيم التزام الجزائر بتعزيز المنظومة القانونية لحماية الطفولة، وتوفير آليات فعالة للتصدي لجرائم الاستغلال الجنسي للأطفال، لا سيما تلك التي تُرتكب عبر الوسائط الرقمية.

المطلب الثاني:

جرائم الابتزاز والتهديد والتجنيد الارهابي الالكتروني للأطفال

تتخذ الجرائم الإلكترونية الموجهة ضد الأطفال أبعادًا متعددة، من بينها جرائم الابتزاز والتهديد والتجنيد الإرهابي عبر الإنترنت، حيث يسعى الجناة إلى استغلال ضعف الطفل أو جهله بالقوانين لتوريطه في ممارسات تمسّ أمنه الشخصي أو الأمن العام. ويتناول هذا المطلب أبرز ملامح هذه الجرائم وخطورتها في البيئة الرقمية.

أولا: جريمة الابتزاز والتهديد الإلكتروني للأطفال

تُعد جريمة الابتزاز والتهديد الإلكتروني للأطفال من الجرائم المستحدثة التي تنطوي على استغلال الوسائل التقنية الحديثة لاستدراج الضحية، غالباً عبر التحايل والتواصل المستمر في ظل غياب الرقابة الأسرية والمجتمعية. وتتمثل هذه الجريمة في قيام الجاني بالتجسس على الطفل أو استدراجه للحصول على معلومات أو محتوى خاص (صور أو فيديوهات)، ثم استخدام هذه المواد لاحقاً لتهديده بهدف تحقيق أغراض غير أخلاقية. وغالباً ما يرضخ الطفل لهذه التهديدات خوفاً من الفضيحة، مما قد يؤدي في بعض الحالات إلى نتائج مأساوية كالإقدام على الانتحار[1].

1 بن عمر ياسين، "الابتزاز الإلكتروني للأطفال في التشريع الجزائري"، دفاتر السياسة والقانون، المجلد 16، العدد 2، 2024 .

ثانيا: جريمة التجنيد الإرهابي الإلكتروني للأطفال

تُعد جريمة التجنيد الإرهابي الإلكتروني للأطفال من أخطر صور الجرائم الإلكترونية الحديثة، حيث يمثل الإرهاب الإلكتروني امتداد رقمياً للإرهاب التقليدي، ويعتمد على وسائل الاتصال الحديثة لنشر الأفكار المتطرفة وتجنيد الأفراد، لا سيما الأطفال والمراهقين عبر منصات التواصل الاجتماعي.

وتتم عملية التجنيد من خلال الإغراء والتقين، عبر منصات التواصل الاجتماعي. وتتم عملية التجنيد من خلال الإغراء والتضليل، وزرع مشاعر الخوف والرعب في نفوس الأطفال لدفعهم نحو تنفيذ أعمال نفوس الأطفال، لدفعهم نحو تنفيذ أعمال عدائية، غالباً عبر منتديات الإنترنت، ثم إخضاعهم لخطط قسرية تنتهي بالإكراه على المشاركة في أعمال إرهابية تحقيقاً لأهداف سياسية تهدد الأمن الدولي والسيادة الوطنية والاستقرار المجتمعي[1] .

المطلب الثالث:

جرائم الألعاب الالكترونية العنيفة

بالنظر إلى التطورات التكنولوجية المتسارعة، أصبحت الألعاب الإلكترونية جزءاً لا يتجزأ من حياة الأطفال والمراهقين، وهو ما يطرح إشكاليات قانونية وأخلاقية متزايدة، خاصة عندما تتحول هذه الألعاب من وسيلة ترفيهية إلى أدوات تهدد السلامة النفسية والجسدية للأطفال، وتدفعهم أحياناً نحو سلوكيات خطيرة قد تصل إلى حد الانتحار أو ارتكاب جرائم.

1 لمزيد من الاطلاع، غضبان نبيلة: جريمة الابتزاز والتهديد عبر الإنترنت في التشريع الجز في التشريع الجزائري"، مذكرة ماجستير، كلية الحقوق والعلوم السياسية محند أولحاج ، قسم القانون العام، 2024.

أولا: حق الطفل في اللعب بين الشرعية والمخاطر

يعد "حق اللعب" من الحقوق الأساسية التي كرستها المواثيق الدولية، وعلى رأسها اتفاقية حقوق الطفل لعام 1989[1] ، التي نصت في المادة 31 على حق الطفل في الراحة واللعب ومزاولة الأنشطة الترفيهية المناسبة لعمره. غير أن هذا الحق لا يُمارس بمعزل عن الرقابة، خاصة في ظل ظهور ألعاب إلكترونية ذات طابع عدواني أو تحريضي، مثل "الحوت الأزرق" و"مريم"، والتي أثبتت الدراسات أنها تسببت في حالات انتحار وخوف جماعي لدى الأطفال.

ثانيا: مواجهة التشريع الجزائري للمحتوى الإلكتروني الضار

أدرك المشرع الجزائري خطورة هذه الظاهرة، فتدخل عبر منظومة قانونية متعددة الأبعاد [2]، أبرزها:

- **قانون حماية الطفل رقم 15-12** المؤرخ في 15 يوليو 2015، الذي يكرّس حماية الطفل من كل أشكال الإيذاء، بما في ذلك المحتوى الرقمي الضار.

- **القانون رقم 09-04** المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والذي يجرّم نشر أو تداول محتويات إلكترونية من شأنها الإضرار بالأمن النفسي أو الجسدي للأطفال.

---

1 اتفاقيه حقوق الطفل لسنه 1989 المصادق عليها بموجب قرار الجمعية العامة للأمم المتحدة رقم 44 25، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 92 461 المتضمن المصادقة مع التصريحات التفسيرية اتفاقية حقوق الطفل التي وافقت عليها الجمعية العامة للأمم المتحدة بتاريخ 1989/12/20 الجريدة الرسمية العدد 91.

2 شتوحي يمينة، غربي ابراهيم: تدخل المشرع الجزائري لحماية الطفل من المحتوى غير المشروع، الألعاب الإلكترونية نموذجا – مجلة الفكر القانوني والسياسي، المجلد 9، العدد 1، 2025.
.رابط المقال :https://asjp.cerist.dz/en/article/266828 :

• **قانون العقوبات** الذي يتيح متابعة كل من يساهم في نشر أو ترويج ألعاب إلكترونية تحرض على العنف أو الانتحار.

تجسدت الجهود الوطنية لحماية الأطفال من مخاطر الألعاب الإلكترونية من خلال المرسوم التنفيذي رقم 05-207 الصادر بتاريخ 29 أكتوبر 2005 [1]، والذي يحدد دفتر الشروط الخاص باستغلال مؤسسات التسلية والترفيه [2]. ورغم وضوح النص القانوني في تنظيم شروط الاستغلال، إلا أن الواقع العملي يكشف عن فجوة كبيرة بين التشريع والتطبيق، حيث أن العديد من نوادي الإنترنت لا تلتزم بهذه الأحكام، وتخرج عن الإطار القانوني السليم. فقد ألزم المشرّع الجزائري أصحاب هذه النوادي بعدم تشغيل القُصّر دون سن 18 عامًا [3]، تحت طائلة سحب الرخصة، وهو إجراء صارم يعكس حرص الدولة على حماية هذه الفئة.

كما يُضاف إلى ذلك المرسوم التنفيذي رقم 97-494 المؤرخ في 21 ديسمبر1997 [4]، والذي يهدف إلى الوقاية من الأخطار الناجمة عن اللعب، حيث وضع مجموعة من المعايير الواجب اتباعها لضمان سلامة الأطفال. غير أن هذا المرسوم صدر في فترة كانت الألعاب المتوفرة تقتصر على ألعاب الفيديو التقليدية، مما يجعله غير كافٍ لمواجهة التحديات الجديدة التي فرضتها الألعاب الإلكترونية الحديثة.

---

[1] المرسوم التنفيذي رقم: 05- 207 المؤرخ في 4 يونيو سنة 2005 يحدد شروط وكيفيات فتح واستغلال مؤسسات التسلية والترفيه، الجريدة الرسمية العد 39

[2] زروقي ابراهيم: الحماية القانونية من تأثيرات الالعاب السلبية الإلكترونية، مداخلة ملقاة في الملتقى الدولي بعنوان: الحماية القانونية والاجتماعية للطفل في القانون الجزائري والقانون المقارن، جامعة محمد بن احمد، وهران، المنظم يوم 4 فيفري 2003 ص: 198

[3] المادة 24 من المرسوم 05 207 المشار اليه أعلاه.

[4] المرسوم التنفيذي رقم 97 494 :مؤرخ في 21 ديسمبر 1997 يتعلق بالوقاية من الاخطار الناجمة عن استعمال اللعب، الجريدة الرسمية رقم 85 لسنة 1997

تجدر الاشارة أنه تشير الدراسات إلى أن الألعاب ذات الطابع العنيف لها العديد من الآثار الصحية والاجتماعية التي تؤثر سلباً على الصحة الجسدية :من خلال الحركات السريعة وغير المنتظمة التي تؤثر على الجهاز العضلي والعظمي.. بالإضافة الى تأثيرها على الصحة النفسية :عبر تعزيز مشاعر القلق، العزلة، والعدوانية.

كما تؤثر سلبا على السلوك الاجتماعي حيث لوحظ ارتفاع في معدل الجرائم المرتكبة من قبل القُصّر المتأثرين بهذه الألعاب[1] .

المطلب الرابع:

جرائم الاعتداء على البيانات الشخصية للأطفال

تعدّ البيانات الشخصية من أكثر المعطيات عرضة للانتهاك في العالم الرقمي، حيث يتم جمعها أو استغلالها دون إذن، مما يشكّل مساسًا مباشرًا بحق الطفل في الخصوصية. ويتناول هذا المطلب صور الاعتداء على بيانات الأطفال وأهم الجوانب القانونية المرتبطة بحمايتها.

ومن ذلك تعد البيانات الشخصية أساسًا جوهريًا للحق في الخصوصية، غير أن التطور التكنولوجي المتسارع أصبح يشكل تهديدًا فعليًا لهذه الخصوصية، خاصة بالنسبة للأطفال، من حيث كيفية التعامل مع بياناتهم ومعالجتها عبر الوسائط الرقمية الحديثة.

وتعتبر المعالجة غير القانونية للمعطيات الشخصية الخاصة بالأطفال من أبرز صور الاعتداء على سرية المعلومات، إذ غالبًا ما يتجاهل القائمون على هذه

1 بلعموري نادية: الآليات الوقائية والعلاجية لحماية الطفل من مخاطر وسائل الاتصال الإلكترونية في التشريع الجزائري – جامعة عباس لغرور خنشلة.
الرابط الالكتروني: http://dspace.univ-khenchela.dz:4000/handle/123456789/3364

المعالجات الضوابط القانونية والأساليب المعتمدة، مما دفع العديد من التشريعات الدولية إلى إخضاع هذا النوع من المعالجة لنظام الترخيص أو التصريح المسبق من الجهات المختصة. كما اشترطت هذه التشريعات الحصول على موافقة صريحة ومسبقة من الممثل القانوني للطفل القاصر، أو عند الضرورة، إذن من القاضي المختص، قبل الشروع في أي عملية معالجة لبياناته الشخصية.

في إطار التصدي للمخاطر التي تهدد الأطفال عبر الإنترنت، تعتمد الجزائر على القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1]. هذا القانون يشكل حجر الأساس في حماية الطفل من الانتهاكات الرقمية، حيث يفرض على الجهات الفاعلة في الفضاء السيبراني احترام خصوصية الطفل وعدم جمع أو معالجة بياناته الشخصية دون موافقة واضحة ومسبقة من أوليائه. كما ينص على ضرورة اتخاذ تدابير تقنية وتنظيمية صارمة لضمان أمن هذه البيانات ومنع الوصول غير المصرح به إليها[2] .

المبحث الثاني: الآليات الحمائية المؤسساتية والوقائية من الجرائم الإلكترونية ضد الاطفال

يمثل تعدد وتداخل الجهات المعنية بحماية الطفل من الجرائم الالكترونية أحد أبرز التحديات في ظل توسّع الفضاء الإعلامي والرقمي، وارتفاع نسبة تعرض

[1] القانون رقم 18 - 07 مؤرخ في 25 رمضان عام 1439 الموافق ل 10 يونيو لسنة 2018 يتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع الشخصي الجريدة الرسمية عدد 34 مؤرخه في 10 يونيو 2018.

2 براهمي عبدالرزاق، فرحات سمير: الحماية القانونية للمعطيات الشخصية للطفل في الفضاء الرقمي، مجلة القانون العام الجزائري والمقارن، مجلد 8، العدد 2، ديسمبر 2022 . ص: 85 ومابعدها.

حيث تُشرف الدولة الجزائرية، من خلال وزارة البريد والمواصلات السلكية واللاسلكية، على تنفيذ هذا القانون عبر حملات توعية موجهة للأطفال والمربين، وتطوير منصات رقمية آمنة، مثل المنصة المتوفرة على موقع fs.mpt.gov.dz

الأطفال لمضامين خطيرة وغير ملائمة. ففي مواجهة هذه التهديدات، لم تعد الحماية القانونية كافية وحدها، بل بات من الضروري تفعيل دور مختلف الأطراف الفاعلة، سواء على المستوى المؤسسي، أو السلطات العمومية وأجهزة الرقابة، أو على المستوى المجتمعي، كالأسرة والمدرسة، ومكونات المجتمع المدني. ويندرج هذا المحور ضمن تحليل تكاملي يهدف إلى إبراز مساهمة كل طرف في إطار منظومة حماية شاملة ومتعددة المستويات، تسعى لضمان بيئة رقمية آمنة ومتوازنة للأطفال.

وعليه تمثل حماية الطفل من الجرائم الإلكترونية مسؤولية جماعية تشترك فيها مختلف الأطراف المعنية، من سلطات تشريعية وتنفيذية، ومؤسسات أمنية واجتماعية، إلى جانب الأسرة والمدرسة والمجتمع المدني. فمواجهة هذا النوع من الجرائم لا يمكن أن تقتصر على الجانب الزجري وحده، بل تستلزم منظومة متكاملة من الآليات المؤسساتية والوقائية التي تتضافر جهودها لضمان بيئة رقمية آمنة للطفل. وانطلاقًا من هذا التصور، يتناول هذا المبحث دراسة أهم الآليات القانونية والمؤسساتية التي تعنى بحماية الطفولة من الجرائم الإلكترونية، إلى جانب الآليات الوقائية العامة التي تسعى إلى الحد من هذه الظاهرة عبر نشر الوعي الرقمي وترسيخ ثقافة الحماية الذاتية لدى الأطفال وأوليائهم.

المطلب الأول:

الآليات المؤسساتية الخاصة لحماية الاطفال من الجر ائم الإلكترونية.

تضطلع المؤسسات الوطنية المختصة بحماية الطفولة بدور أساسي في الوقاية من الجرائم الإلكترونية ومكافحتها، من خلال التنسيق بين أجهزة إنفاذ القانون والهيئات الاجتماعية والإعلامية. ويهدف هذا المطلب إلى استعراض أبرز هذه المؤسسات ودورها في التصدي للاعتداءات الرقمية ضد الأطفال.

أولا: المؤسسات المختصة في حماية الطفولة والمراهقة.

تتدخل الجهات المختصة بالتحقيق العلمي في حالات تعرض الأطفال والمراهقين لمخاطر الإنترنت، وذلك بصفة آلية ومباشرة، بعد ثبوت عدم كفاية الوسائل الوقائية العامة في توفير الحماية اللازمة. ويهدف هذا التدخل إلى كشف مصادر الخطر وتحديد آليات الاستجابة المناسبة، وفقًا لمعايير السلامة الرقمية المعتمدة.

إن المؤسسات المختصة بحماية الطفولة والمراهقة تعد المؤسسات المكلفة بحماية الطفولة والمراهقة هيئات عمومية تابعة لوزارة التضامن الوطني والأسرة وقضايا المرأة، وتضطلع بمهام الرعاية الاجتماعية للأطفال والمراهقين المعرضين للخطر، أو الموضوعين تحت إشراف قضائي. وتشمل مهامها ما يلي[1] :

- ضمان التربية السليمة، والحماية الجسدية والنفسية، وإعادة الإدماج الاجتماعي والتربوي للأحداث.
- دراسة شخصية الحدث من خلال الملاحظة المباشرة لسلوكه، وتحليل قدراته واستعداداته النفسية والاجتماعية.
- إجراء التحقيقات اللازمة وتنظيم برامج تأهيلية وتقنيات تربوية ملائمة لطبيعة الفئة المستهدفة.
- مرافقة الأسرة خلال كامل مراحل التدخل، بهدف الحفاظ على الروابط الأسرية وتعزيز التكيف الأسري والاجتماعي.

1 حسيني عمار، ابي مولود عبد الفاتح: دور المؤسسات المتخصصة في حماية الطفولة، مجلة العلوم الإنسانية والاجتماعية ، العدد 30 جامعة قصدي مرباح ورقلة الجزائر سبتمبر 2017 ص: 334

• السهر على إعادة الإدماج المدرسي والمهني، وفقًا للمعايير الدولية المعتمدة في مجال حماية حقوق الطفل.

وتلتزم المؤسسات المختصة بتطبيق مجموعة من المعايير الدولية المعترف بها في مجال حماية الطفولة، وتفعيل البرامج الوقائية والتأهيلية التي تهدف إلى رعاية الأطفال المعرضين للخطر، وضمان حقوقهم في بيئة آمنة ومتكاملة.

ثانيا: الشرطة العلمية ودورها في مكافحة الجرائم الإلكترونية وحماية الطفولة

في ظل التطور المتسارع الذي يشهده العالم في مجال الاتصالات وتكنولوجيا المعلومات، أصبح من الضروري تأهيل عناصر الشرطة العلمية لمواجهة الجرائم والانتهاكات التي تُرتكب عبر الإنترنت. لم تعد الأساليب التقليدية في البحث والتحقيق كافية، بل بات من الواجب تطويرها لتواكب هذا التقدم الرقمي الهائل، بما يضمن فعالية أكبر في التصدي للمخاطر الإلكترونية.

ويقتضي ذلك دعم رجال الأمن بخبراء وتقنيات حديثة في مجال المعلوماتية، مما يُسهم في تسريع التدخل وكشف مختلف أنواع التجاوزات في الفضاء الرقمي. ومن بين المهام الحيوية التي تضطلع بها الشرطة العلمية، الكشف عن الجرائم الإلكترونية التي تستهدف الأطفال، مما يجعلها أحد أبرز الأجهزة المؤسسية المعنية بحماية الطفولة من مخاطر الإنترنت [1]..

[1] عبد الفتاح بيومي الحجازي: الاحداث والانترنت– دراسة متعمقة عن اثر الانترنت في انحراف الاحداث، دار الكتب القانونية مصر، 2007 ص: 303.

ثالثا: الادارة المركزية.

تتحمل وزارة التربية الوطنية مسؤولية جوهرية في تطوير المنظومة التعليمية، وذلك من خلال إشراك خبراء في علم النفس التربوي لضمان توافق المناهج الدراسية مع التحولات النفسية والاجتماعية التي يعيشها الطفل في العصر الحديث. هذا التوجه يهدف إلى بناء برامج تعليمية تراعي النمو المتكامل للمتعلمين وتساعدهم على التكيف مع التغيرات المتسارعة. كما أن إدراج مادة المعلوماتية في مختلف مراحل التعليم بات ضرورة ملحة، لتمكين الأطفال من فهم آليات استخدام الشبكة الرقمية، والتمييز بين مزاياها ومخاطرها. وقد تناول مقال في موقع "تربية.كوم" أهمية علم النفس التربوي في دعم العملية التعليمية، مشيراً إلى دوره في إعداد المعلم وفهم سلوك المتعلم داخل بيئة التعلم، مما يعزز فعالية التدريس ويضمن جودة التعليم [1].

وفي السياق ذاته، يمكن لوزارة التضامن الوطني أن تلعب دوراً محورياً في تعبئة المجتمع لدعم الحملات التوعوية والتحسيسية، بالتنسيق مع وزارة الاتصال التي تشرف على وسائل الإعلام. فالإعلام، بصفته مؤسسة فاعلة في التنشئة الاجتماعية، يضطلع بوظائف متعددة منها نشر القيم المجتمعية، وتوجيه السلوك، وتحقيق الضبط الاجتماعي. ومن هذا المنطلق، يمكن الاعتماد على الإعلام في توعية الأطفال بمخاطر الإنترنت وتعزيز ثقافة الاستخدام الآمن. وقد أشار مقال في "اندبندنت عربية" إلى ضرورة إعادة صياغة فلسفة التعليم في الجزائر لتتماشى مع التحولات التكنولوجية والاجتماعية، مؤكداً على أهمية إدماج التكنولوجيا والإعلام في العملية التربوية [2].

---

[1] دور علم النفس التربوي في العملية التعليمية والتدريس مقال متاح عبر الرابط الالكتروني: //https://tarbiyaa.com

[2] للاطلاع على المقال :المناهج الدراسية في الجزائر... إصلاحات جديدة وسط جدل قديم.

المطلب الثاني:

الآليات الوقائية العامة لحماية الاطفال من الجر ائم الإلكترونية

لا تقتصر الحماية من الجرائم الإلكترونية على الجانب القانوني فقط، بل تشمل كذلك الجهود التوعوية والتربوية والاجتماعية التي تساهم في بناء ثقافة رقمية آمنة لدى النشء. ويتناول هذا المطلب أهم الوسائل الوقائية العامة التي تشارك فيها الأسرة والمدرسة ووسائل الإعلام والمجتمع المدني لحماية الطفل من مخاطر البيئة الرقمية.

- أولا: الآليات المؤسساتية لحماية للطفل من مخاطر البيئة الاعلامية والرقمية.

1- <u>التزامات وسائل الإعلام والمنصات الرقمية بحماية الطفل</u>

تتحمل وسائل الإعلام والمنصات الرقمية مسؤولية قانونية وأخلاقية في حماية الأطفال من التعرض للمضامين الضارة. في الجزائر، يُلزم قانون الإعلام المؤسسات الإعلامية باحترام حقوق الطفل، ويمنع نشر أو بث مضامين قد تؤثر سلبًا على نموه.

وقد أكدت سلطة ضبط السمعي البصري على ضرورة احترام قانون الطفل رقم 15-12 الذي يكفل للطفل حقه في الحماية من كافة أشكال الضرر، داعية متعهدي الإعلام السمعي البصري ومستخدمي الإعلام البديل إلى ضرورة احترام القانون [1].

/https://www.independentarabia.com/node/631941

1 سلطة ضبط السمعي البصري تستنكر الإستغلال غير الأخلاقي للطفولة عبر وسائط التواصل الاجتماعي | وزارة الاتصال، عبر الموقع الالكتروني: "https://www.ministerecommunication.gov.dz/ar/node/9769?utm_source=chatgpt.com

على المستوى الدولي، تشجع الاتفاقيات والمعايير الدولية على التزام وسائل الإعلام والمنصات الرقمية بحماية الأطفال، من خلال تبني سياسات واضحة لحماية الخصوصية، وتوفير أدوات للرقابة الأبوية، وضمان عدم استغلال الأطفال في الإعلانات أو المحتوى التجاري[1] .

واستنادًا إلى تقرير **منظمة التعاون والتنمية الاقتصادية (OECD)** المعنون Protecting Children Online: An Overview of Recent Developments in Legal Frameworks and Policies الصادر في 2020. [2] هذا التقرير يقدم إطارًا مرجعيًا شاملًا لسياسات الدول في مجال حماية الأطفال على الإنترنت، ويسلط الضوء على مسؤوليات مختلف الفاعلين، بما في ذلك وسائل الإعلام والمنصات الرقمية.، حيث يظهر دور الإعلام والمنصات الرقمية وفقًا لتقرير الـ :OECD- تبني سياسات حماية مخصصة للأطفال حيث يشدد التقرير على أن المنصات الرقمية ووسائل الإعلام مطالبة بوضع سياسات واضحة لحماية الأطفال، تشمل آليات التحقق من العمر لمنع وصول القُصّر إلى المحتويات غير الملائمة.، وحظر أو تقنين الإعلانات الموجهة للأطفال، خاصة تلك التي تستغل ضعفهم أو تؤثر على سلوكهم الاستهلاكي.

بالاضافة الى تصميم واجهات رقمية آمنة وسهلة الاستخدام للأطفال مع الشفافية والمساءلة أين تطالب الـ OECDالمنصات الرقمية والإعلامية بالشفافية

---

[1] استغلال الأطفال إعلاميًا وآليات حمايتهم في الجزائر: قراءة في القانون الجزائري والاتفاقيات الدولية" للباحثين دبدوش الهاشمي وعبد الرحمن نشادي،
https://www.researchgate.net/publication/366356543

[2] OECD (2020), Protecting Children Online: An Overview of Recent Developments in Legal Frameworks and Policies, OECD Publishing, Paris.
[رابط التقرير بصيغة PDF]
(https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/06/protecting-children-online_0c385619/9e0e49a9-en.pdf)

فيما يتعلق بكيفية جمع واستخدام بيانات الأطفال، وتوفير تقارير دورية عن التدابير المتخذة لحمايتهم. وهذا يشمل إشعارات واضحة وسياسات خصوصية مصممة لتكون مفهومة للآباء والأطفال .وأدوات تمكن الآباء من ضبط المحتوى الذي يتعرض له أطفالهم.

ناهيك عن التعاون مع الحكومات والمجتمع المدني يؤكد التقرير أن الحماية الفعالة تتطلب تعاونًا متعدد الأطراف. على وسائل الإعلام والمنصات من خلال دعم حملات التوعية والتعليم الرقمي الآمن والإبلاغ عن أي أنشطة مشبوهة أو محتويات تشكل خطرًا على الأطفال للسلطات المختصة، اضافة الى تطوير المحتوى الإعلامي الآمن والهادف للأطفال بشكل يُوصى بأن تساهم وسائل الإعلام في إنتاج محتويات رقمية تثقيفية وترفيهية تراعي عمر الطفل وخصوصيته الثقافية والاجتماعية، وتبتعد عن العنف، الإباحية.

2- .دور السلطات العمومية المختصة

تلعب السلطات العمومية دورًا حيويًا في تنفيذ ومراقبة تطبيق القوانين المتعلقة بحماية الأطفال من المضامين الإعلامية والرقمية الضارة. في الجزائر، تُعتبر السلطة الوطنية لضبط السمعي البصري من الهيئات المسؤولة عن مراقبة المحتوى الإعلامي وضمان احترام حقوق الطفل. كما تُعنى سلطة حماية المعطيات الشخصية بحماية البيانات الخاصة بالأطفال، وضمان عدم استغلالها أو استخدامها بطرق غير قانونية.

وقد استنكرت السلطة الاستغلال غير الأخلاقي للطفولة عبر وسائط التواصل الاجتماعي، داعية إلى ضرورة احترام القانون، كما عنيت المفوضية الوطنية لحماية وترقية الطفولة بحماية البيانات الخاصة بالأطفال، وضمان عدم استغلالها أو استخدامها بطرق غير قانونية. وقد أعلنت المفوضة الوطنية لحماية الطفولة عن إنشاء خلية وطنية لليقظة لحماية الأطفال من الاستغلال عبر تكنولوجيات الإعلام

والاتصال، تتولى الكشف عن التجاوزات في حق الطفل مع التدخل في الوقت المناسب[1]

تظهر هذه الآليات القانونية التزام الجزائر والمجتمع الدولي بحماية الأطفال من المخاطر المرتبطة بالمضامين الإعلامية والرقمية. ومع ذلك، يبقى التحدي في التطبيق الفعلي لهذه القوانين، وتحديثها بما يتناسب مع التطورات التكنولوجية المستمرة.

ثانيا: دور الأسرة والمدرسة والمجتمع المدني في حماية الطفل من مخاطر البيئة الرقمية

1- التوعية الأسرية والرقابة الأبوية

تلعب الأسرة دورًا محوريًا في حماية الأطفال من مخاطر البيئة الرقمية، من خلال التوعية والرقابة الأبوية. تشير الدراسات إلى أن التوسط الأبوي في استخدام الأطفال للمواقع الإلكترونية يعزز من ثقافة المواطنة الرقمية لديهم، ويقلل من تعرضهم للمحتويات الضارة [2].

[1] إطلاق خلية يقظة لحماية الأطفال من الجرائم السيبرانية والاستعمال الآمن للأنترنت، أنظر الموقع: https://www.aps.dz/ar/societe/162913-2024-05-28-13-05-45?utm_source=chatgpt.com

[2] محمود محمد عبد الحليم: اتوسط الابوي في استخدام الاطفال المواقع الالكترونية وعلاقته بتعزيز ثقافة المواطنة الرقمية لديهم. المجلة المصرية للبحوث الراي العام المجلد 21 العدد الرابع؛ الجزء الاول اكتوبر/ديسمبر 2022.ص: 525.

-امال علال: حماية الطفل في مجال الاعلام. المجلة المتوسطية للقانون والاقتصاد؛ المجلد 2 العدد 2؛ ص: 131

كما أن الرقابة الأسرية تساهم في توجيه استخدام الأطفال للوسائل الرقمية بشكل إيجابي وتحد من تأثيراتها السلبية [1].

لقد أصبح الاطفال في العصر الرقمي متواصلين مع بيانات افتراضية واشخاص مجهولين قد يؤثرون سلبا على حياتهم وعلى المجتمع ككل وهويته وسلامته خاصه في ظل استخدام الاطفال المفرد لمواقع التواصل الاجتماعي، وفي الآونة الأخيرة تزايد اساءة استخدام الاطفال للتكنولوجيا والتي شملت استخدام مواقع ويب للتخويف او التهديد والكثير من الاشياء غير القانونية.. ومع انتشار الاستخدام السيء للتطبيقات الرقمية تأثرت شخصية الافراد خاصة الاطفال وتكوينهم الاخلاقي، وفي ظل مجتمع رقمي خال في اغلب الاحيان من القواعد المرتبطة بسلوكيات المواطن الرقمي الايجابي يظهر دور السلطة الأبوية في توعية الابناء من المخاطر المحتملة جراء تحميل الوسائط المختلفة كالصور والفيديوهات من مصادر غير معروفه او الرد على رسائل او منشورات او اعلانات مجهولة الهوية او التواصل مع اشخاص غرباء عبر التطبيقات التواصل الاجتماعي [2].

وعليه لابد من تفعيل اختيار الرقابة الأبوية وضوابط الامن المتاح بأغلب التطبيقات والمتصفحات في البيئة الالكترونية ووضع ميثاق مع الابناء يتضمن قواعد الاستخدام الامن للأنترنت كمده الاتصال والمواقع المسموح بزيارتها.

2- <u>التربية الإعلامية والرقمية في المدارس</u>

التربية الإعلامية والرقمية تشير إلى مجموعة من المعارف والمهارات التي تُعلَّم للمتعلمين بهدف تمكينهم من استخدام وسائل الإعلام والتقنيات الرقمية بشكل فعّال، آمن، وناقد. وهي تتيح للطلاب فهم كيفية إنتاج المحتوى الإعلامي، وتحليله،

[1] لتفاصيل اكثر حول الموضوع راجع: عبد سليم؛ شويني خالد: الرقابة الاسرية ودورها في توجيه استخدام الاطفال للوسائل الرقمية- مقاربة نظرية- مجلة اقلام المجلد 4؛ العدد1؛ 2025.

[2] محمود محمد عبد الحليم: المرجع السابق، ص: 523.

والتفاعل معه، بالإضافة إلى تعزيز التفكير النقدي والمسؤولية الرقمية في بيئة معلوماتية معقدة [1].

تعد التربية الإعلامية والرقمية في المدارس أداة فعالة لتمكين الأطفال من التعامل الآمن والواعي مع الوسائط الرقمية. تؤكد الدراسات على أهمية إدخال التربية الإعلامية والرقمية كمناهج ثابتة في المدارس والجامعات، لتزويد الطلاب بالمهارات اللازمة للتعامل مع المعلومات الرقمية بشكل نقدي و آمن.

كما أن التربية الإعلامية الرقمية تعزز من وعي الطلاب بالأخبار الزائفة، وتساعدهم على التمييز بين المعلومات الصحيحة والمضللة [2] .

لقد ورد في تقرير منظمة الأمم المتحدة للطفولة (اليونيسف) لعام 2017 بعنوان: "أطفال في عالم رقمي" إلى أهمية إدماج التربية الإعلامية والرقمية في المدارس لتزويد الأطفال بالمهارات اللازمة لاستخدام التكنولوجيا بوعي وأمان، خاصة في ظل تزايد تعرضهم للمخاطر الرقمية مثل التنمر الإلكتروني والمعلومات المضللة. ويؤكد التقرير على ضرورة تدريب المعلمين، وتوفير مناهج تعليمية تساعد الطلاب على التفكير النقدي، وحماية أنفسهم رقميًا، والمشاركة الإيجابية في الفضاء الإلكتروني[3] .

[1] اليونسكو – التربية الإعلامية والمعلوماتية: Media and Information Literacy: Curriculum for Teachers
عبر الرابط: https://unesdoc.unesco.org/ark:/48223/pf0000192971

[2] طارق محمد الصعيدي: التربية الإعلامية بالمدارس المصرية ودورها في التوعية بالأخبار الزائفة، المجلة العلمية للبحوث الصحافة: العدد 26 الجزء الثاني يوليو 2023 .مقال عبر الرابط الالكتروني: https://sjsj.journals.ekb.eg/article_337692

[3] UNICEF (2017), The State of the World's Children 2017: Children in a Digital World. https://www.unicef.org/reports/state-worlds-children-2017

3- مبادرات الجمعيات لحماية الأطفال

تلعب الجمعيات والمجتمع المدني دورًا مهمًا في حماية الأطفال من المخاطر الرقمية، من خلال إطلاق مبادرات وبرامج توعوية. على سبيل المثال، تعمل بعض الجمعيات على توفير بيئة رقمية دامجة توفر الحماية للأطفال، من خلال برامج ومبادرات إرادية تهدف إلى تعزيز الوعي الرقمي لدى الأطفال وأسرهم.

كما أن مبادرة حماية الأطفال على الإنترنت، التي أطلقتها الأمم المتحدة، تهدف إلى تعزيز الوعي بسلامة الأطفال في العالم الإلكتروني، وتطوير أدوات عملية لحمايتهم[1].

تلعب الجمعيات والمنظمات غير الحكومية دورًا مهمًا في التصدي للمخاطر التي يواجهها الأطفال في البيئة الإعلامية والرقمية، مثل التعرض للمحتوى العنيف أو الإباحي، التنمر الإلكتروني، اختراق الخصوصية، والإدمان على الشاشات .وتتمثل أبرز أدوار الجمعيات في التوعية والتثقيف لأنها تنظم ورشات عمل للأهالي والأطفال حول الاستخدام الآمن للتقنيات، وتقدم دلائل إرشادية للحد من المخاطر الرقمية [2].

[1] سلامة الأطفال والشباب على الإنترنت | الأمم المتحدة، "the United Nations -
https://www.un.org/ar/global-issues/child-and-youth-safety-online?utm_source=chatgpt.com "

[2] - كتاب اليونيسكو – حماية الأطفال في البيئة الرقمية ـ Guidelines for Industry on Child Online Protection
يصدر بالتعاون بين اليونسكو والاتحاد الدولي للاتصالات (ITU) ويوضح أدوار المنظمات والمجتمع المدني.
- أمثلة من العالم العربي حول مساهمة الجمعيات في التوعية وحملات الحماية الرقمية.
دور الجمعيات الأهلية في حماية الطفل من مخاطر الفضاء الرقمي، مقال علمي في مجلة المعرفة – وزارة التعليم السعودي ، رابط المقال:
https://www.almarifa.com.sa/article/1313304](https://www.almarifa.com.sa/article/1313304)

بالإضافة الى تقديم الدعم النفسي والاجتماعي حيث توفر بعض الجمعيات خطوط مساعدة ودعم نفسي للأطفال الذين تعرضوا لصدمات رقمية، والمناصرة وتغيير السياسات حيث تضغط الجمعيات على الحكومات لوضع قوانين تحمي الأطفال من الاستغلال الرقمي، وتراقب التزام الشركات الرقمية بحقوق الطفل.

كما تعمل بعض المبادرات على إنتاج محتوى بديل وآمن بإنتاج تطبيقات ومحتويات إعلامية موجهة للأطفال تراعي قيم الحماية والخصوصية والأخلاق الرقمية.

أخيرا ومن خلال هذا المحور يمكننا القول أن الأدوار المتكاملة للأسرة والمدرسة والمجتمع المدني، يمكن تحقيق حماية فعالة للأطفال من المخاطر المرتبطة بالبيئة الإعلامية والرقمية.

ويتضح أن حماية الطفل من المخاطر المتزايدة للبيئة الإعلامية والرقمية لا يمكن أن تتحقق فقط من خلال التشريعات القانونية، بل تتطلب تضافر جهود مختلف الفاعلين في المجتمع. فالأسرة تمثل خط الدفاع الأول عبر التوعية والرقابة، بينما تضطلع المدرسة بدور تربوي محوري في غرس قيم الاستخدام الآمن والمسؤول للتكنولوجيا من خلال التربية الإعلامية والرقمية .كما يشكل المجتمع المدني فاعلًا تكميليًا هامًا، عبر المبادرات التوعوية والمرافقة والدعوة إلى تطوير السياسات العامة.

إن تفعيل هذه الأدوار بشكل متكامل يساهم في بناء بيئة رقمية آمنة تُمكّن الطفل من الاستفادة من مزايا التكنولوجيا دون التعرض لمخاطرها، مما يفرض على الدول دعم هذه الآليات عبر استراتيجيات وطنية واضحة، وتوفير موارد بشرية ومادية لضمان استدامتها.

الخاتمة:

تمثل الجرائم الإلكترونية التي تستهدف الأطفال أحد أخطر مظاهر الجريمة المعاصرة في ظل التطور التكنولوجي المتسارع، إذ باتت البيئة الرقمية، رغم مزاياها العديدة، فضاءً مفتوحًا للانتهاكات التي تمس القيم والمبادئ الإنسانية، وتعرّض الطفل لمخاطر متعددة تمس سلامته الجسدية والنفسية والبيانية. ومن خلال تحليل عناصر هذه الدراسة، تبيّن أنّ التشريع الجزائري خطا خطوات معتبرة في مجال حماية الطفل من هذه الجرائم، غير أنّه لا يزال بحاجة إلى مزيد من التكييف والتحديث لمواكبة التطور التقني المتسارع وتعقّد صور الجريمة الرقمية.

يمكن القول إن حماية الطفل من الجرائم الإلكترونية في الجزائر ما تزال تتأرجح بين الجهد التشريعي والمؤسسي القائم والحاجة إلى تعزيز البعد الوقائي والتوعوي، فالقوانين الحالية وضعت أسسًا قانونية لحماية الطفل في الفضاء الرقمي، لكن التطبيق العملي وتكامل الأدوار بين المؤسسات المعنية لا يزال يتطلب المزيد من التنسيق والتطوير لضمان حماية فعلية وشاملة للطفولة في البيئة الإلكترونية.

إن أهم صور الجرائم الإلكترونية الموجهة ضد الأطفال تتنوع بين الاستغلال الجنسي والابتزاز والتهديد والتجنيد الإرهابي، فضلًا عن الجرائم الناشئة عن الألعاب الإلكترونية العنيفة والاعتداء على البيانات الشخصية.

يتضح أن أخطر هذه الجرائم هي تلك التي تُمارس خفية عبر الإنترنت، مما يصعّب رصدها أو الإبلاغ عنها، خصوصًا في ظل ضعف الوعي الرقمي لدى الأطفال.

لا يزال الإطار القانوني الجزائري، رغم تطوره، بحاجة إلى نصوص أكثر تحديدًا تتناول صور هذه الجرائم بشكل دقيق، خاصة ما يتعلق بحماية البيانات الشخصية للأطفال والمحتوى الرقمي الموجَّه لهم.

تبين أن المؤسسات الوطنية المعنية بالطفولة، إلى جانب أجهزة إنفاذ القانون، تلعب دورًا محوريًا في مكافحة الجرائم الإلكترونية ضد الأطفال، إلا أن هذا الدور يحتاج إلى مزيد من التنسيق والتخصص في الجوانب التقنية.

أما من الناحية الوقائية، فإن دور الأسرة والمدرسة والمجتمع المدني يظل حجر الزاوية في ترسيخ ثقافة الاستخدام الآمن للتكنولوجيا.

رغم وجود بعض المبادرات الإعلامية والتوعوية، إلا أنها ما تزال محدودة من حيث الانتشار والتأثير، مما يستدعي إستراتيجية وطنية متكاملة للوقاية من الجرائم الرقمية الماسة بالطفولة.

المقترحات :

1 .تطوير التشريع الجزائري ليشمل نصوصًا أكثر تحديدًا ودقة تعالج مختلف صور الجرائم الإلكترونية ضد الأطفال، مع تضمين عقوبات رادعة للجناة.

2 إنشاء هيئة وطنية مختصة بحماية الطفل في الفضاء الرقمي تكون مهمتها التنسيق بين مختلف القطاعات (العدالة، التربية، الإعلام، الاتصالات).

3 تعزيز قدرات الشرطة العلمية ووحدات مكافحة الجريمة الإلكترونية** في مجال تتبع الجرائم الموجهة ضد القُصّر، وتوفير تكوينات متخصصة للكوادر العاملة في هذا المجال.

4 إدراج التربية الرقمية ضمن المناهج التعليمية بهدف ترسيخ ثقافة الوعي الرقمي والمسؤولية الإلكترونية لدى التلاميذ منذ المراحل الأولى.

5 تفعيل دور الإعلام في التوعية بمخاطر الجرائم الإلكترونية ونشر برامج هادفة موجهة للأسر والأطفال حول أساليب الحماية الرقمية.

6 تشجيع الأسرة على المراقبة الإيجابية لاستخدام الطفل للتكنولوجيا، وتعزيز التواصل الأسري حول سلوكياته الرقمية.

7 إطلاق حملات وطنية مشتركة بين الدولة والمجتمع المدني لتعزيز ثقافة "الأمان الرقمي للطفل" تشمل المدارس والمنصات الإلكترونية.

في الختام إن حماية الطفل من الجرائم الإلكترونية ليست مجرد التزام قانوني، بل هي واجب وطني وأخلاقي يستدعي تضافر الجهود على جميع المستويات القانونية، المؤسسية، والتربوية. فالمجتمع الذي يصون طفولته هو المجتمع الذي يصون مستقبله، والوعي الرقمي هو حجر الأساس لبناء جيل آمن ومسؤول في عالم تحكمه التكنولوجيا.

قائمة المصادر و المراجع:

1-المصادر

أ- الاتفاقيات الدولية

اتفاقية حقوق الطفل سنة 1989 المصادق عليها بموجب قرار الجمعية العامة للأمم المتحدة رقم 25/44، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 461/92 المتضمن المصادقة مع التصريحات التفسيرية.

ب- القوانين

1) المرسوم التنفيذي رقم 97: 494 مؤرخ في 21 ديسمبر 1997 **يتعلق بالوقاية من الأخطار الناجمة عن استعمال اللعب**، الجريدة الرسمية رقم 85 لسنة 1997.
2) المرسوم التنفيذي رقم: 05- 207 المؤرخ في 4 يونيو سنة 2005 **يحدد شروط وكيفيات فتح واستغلال مؤسسات التسلية والترفيه**، الجريدة الرسمية العد 39.
3) القانون رقم: 04/09 **المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**؛ الجريدة الرسمية؛ العدد 47 الصادرة بتاريخ 16 أوت 2009.
4) القانون رقم 15/ 12 **المتضمن قانون الطفل**؛ المؤرخ في 15 يوليو 2015 الجريدة الرسمية العدد 39؛ الصادرة بتاريخ 19 يوليو 2015.
5) القانون رقم 18 - 07 مؤرخ في 25 رمضان عام 1439 الموافق ل 10 يونيو سنة 2018 **يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع شخصي**، الجريدة الرسمية عدد 34 مؤرخه في 10 يونيو 2018.

3- المراجع

أ- المقالات

1) أمال علال: "**حماية الطفل في مجال الإعلام**"، المجلة المتوسطية للقانون والاقتصاد، المجلد 2 العدد 2.
2) براهمي عبد الرزاق، فرحات سمير: "**الحماية القانونية للمعطيات الشخصية للطفل في الفضاء الرقمي**"، مجلة القانون العام الجزائري والمقارن، مجلد 8، العدد 2، ديسمبر 2022.
3) بن عمر ياسين، "**الابتزاز الإلكتروني للأطفال في التشريع الجزائري**"، دفاتر السياسة والقانون، المجلد 16، العدد 2، 2024.
4) حسيني عمار، أبي مولود عبد الفاتح: "**دور المؤسسات المتخصصة في حماية الطفولة**"، مجلة العلوم الإنسانية والاجتماعية، العدد 30، جامعة قصدي مرباح ورقلة الجزائر، سبتمبر 2017.
5) شتوحي يمينة، غربي إبراهيم: "**تدخل المشرع الجزائري لحماية الطفل من المحتوى غير المشروع، الألعاب الإلكترونية نموذجا**"، مجلة الفكر القانوني والسياسي، المجلد 9، العدد 1، 2025.
6) طارق محمد الصعيدي: "**التربية الإعلامية بالمدارس المصرية ودورها في التوعية بالأخبار الزائفة**"، المجلة العلمية للبحوث الصحافة، العدد 26 الجزء الثاني، يوليو 2023، مقال عبر الرابط الالكتروني: https://sjsj.journals.ekb.eg/article_337692
7) عبد الفتاح بيومي الحجازي: "**الأحداث والإنترنت - دراسة متعمقة عن أثر الإنترنت في انحراف الأحداث**"، دار الكتب القانونية، مصر، 2007.
8) عبد سليم، شويني خالد: "**الرقابة الأسرية ودورها في توجيه استخدام الأطفال للوسائل الرقمية - مقاربة نظرية**"، مجلة أقلام، المجلد 4، العدد 1، 2025.
9) عيشات أمينة، عماري إبراهيم: "**البيئة الرقمية وعلاقتها بالجرائم الواقعة على الأطفال - الاستغلال الجنسي الإلكتروني نموذجا**"، مجلة دفاتر حقوق الطفل، المجلد 13 العدد سنة 2022.

10) قشيوش، رحمونة: "**الحماية القانونية للطفل ضحية الاستغلال الجنسي في ظل الفضاء الرقمي**"، مجلة نوميروس الأكاديمية، المجلد 1، العدد الثاني، يونيو 2020.

11) محمود محمد عبد الحليم: "**التوسط الأبوي في استخدام الأطفال المواقع الإلكترونية وعلاقته بتعزيز ثقافة المواطنة الرقمية لديهم**"، المجلة المصرية للبحوث الرأي العام، المجلد 21 العدد الرابع، الجزء الأول، أكتوبر/ديسمبر 2022.

ب- الكتب

1) كتاب اليونيسكو – **حماية الأطفال في البيئة الرقمية ـ Guidelines for Industry on Child Online Protection**، يصدر بالتعاون بين اليونسكو والاتحاد الدولي للاتصالات (ITU) ويوضح أدوار المنظمات والمجتمع المدني.

ج - المداخلات والمذكرات

1) زروقي إبراهيم: "**الحماية القانونية من تأثيرات الألعاب السلبية الإلكترونية**"، **مداخلة ملقاة في الملتقى الدولي بعنوان**: "الحماية القانونية والاجتماعية للطفل في القانون الجزائري والقانون المقارن"، جامعة محمد بن أحمد، وهران، 4 فيفري 2003.

2) بلعموري نادية: "**الآليات الوقائية والعلاجية لحماية الطفل من مخاطر وسائل الاتصال الإلكترونية في التشريع الجزائري**"، جامعة عباس لغرور خنشلة.

د- المراجع والمواقع الالكترونية

1) OECD (2020), Protecting Children Online: An Overview of Recent Developments in Legal Frameworks and Policies, OECD Publishing, Paris. Availabel at : https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/06/protecting-children-online_0c385619/9e0e49a9-en.pdf

2) UNICEF (2017), The State of the World's Children 2017: Children in a Digital World. https://www.unicef.org/reports/state-worlds-children-2017

3) استغلال الأطفال إعلاميًا وآليات حمايتهم في الجزائر: قراءة في القانون الجزائري والاتفاقيات الدولية" للباحثين دبدوش الهاشمي وعبد الرحمن نشادي، https://www.researchgate.net/publication/366356543

4) إطلاق خلية يقظة لحماية الأطفال من الجرائم السيبرانية والاستعمال الآمن للأنترنت، أنظر الموقع45-05-28-13-05-2024-162913/societe/ar/dz.aps.www://https :

5) دور الجمعيات الأهلية في حماية الطفل من مخاطر الفضاء الرقمي، مقال علمي في مجلة المعرفة – وزارة التعليم السعودي

6) رابط المقال:

https://www.almarifa.com.sa/article/1313304](https://www.almarifa.com.sa/article/1313304

7) سلامة الأطفال والشباب على الإنترنت | الأمم المتحدة، - the United Nations"https://www.un.org/ar/global-issues/child-and-youth-safety-online " سلطة ضبط السمعي البصري تستنكر الإستغلال غير الأخلاقي للطفولة عبر وسائط التواصل الاجتماعي | وزارة الاتصال، عبر الموقع الالكتروني: https://www.ministerecommunication.gov.dz/ar/node/9769?utm

عقد التأمين الإلكتروني بين متطلبات البيئة الرقمية وخصوصيات التنظيم القانوني في الجزائر

The Electronic Insurance Contract Between the Requirements of the Digital Environment and the Specificities of Legal Regulation in Algeria

د. تقي الدين دغبوج

كلية الحقوق والعلوم السياسية، جامعة الشاذلي بن جديد (الطارف)

د. فؤاد مخربش

كلية الحقوق والعلوم السياسية، جامعة الشهيد الأخوة منتوري (قسنطينة)

ملخص:

يعد التأمين من أهم الأنشطة الاقتصادية في العالم، لارتباطه المباشر بالتنمية الاقتصادية من خلال دعمه لمختلف الأنشطة التجارية، كأعمال الاستثمار والمقاولات وعقود النقل وغيرها من الأنشطة الأخرى. ويؤثر التأمين إيجابا في هذه الأنشطة، كما يسهم في تمويل الاستثمارات المنتجة التي تعد ركيزة أساسية للتقدم. ومن ثم، تبرز ضرورة تبسيط إجراءات التأمين وإزالة التعقيدات الإدارية التي تثني المستهلكين عن الاستفادة من خدماته. ولمواكبة التطور التكنولوجي الهائل، اتجهت معظم الدول إلى ربط خدمات التأمين بالتجارة الإلكترونية، باعتبار شركات التأمين مؤسسات تجارية تهدف إلى تحقيق مزايا عديدة للمستهلكين وتشجيعهم على الحصول على خدمات التأمين بوسائل إلكترونية.

الكلمات المفتاحية: التأمين الإلكتروني؛ العقود الإلكترونية؛ البيئة الرقمية؛ التجارة الإلكترونية؛ التنمية الاقتصادية.

Abstract

Insurance is considered one of the most important economic activities worldwide, due to its direct connection with economic development through its support of various commercial activities such as investment, contracting, and transportation, among others. Insurance positively influences these activities and contributes to financing productive investments, which are regarded as a fundamental pillar of progress. Therefore, it is essential to simplify insurance procedures and eliminate administrative complexities that discourage consumers from benefiting from its services. In response to the rapid technological advancements, most countries have moved towards integrating insurance services with electronic commerce, given that insurance companies are commercial entities aiming to provide numerous advantages to consumers and to encourage them to access insurance services through electronic means.

Keywords: *Electronic insurance; Electronic Contracts; Digital environment; Electronic commerce; Economic development.*

مقدمة

تعد صناعة التأمين عنصرا حيويا في الاقتصاد الوطني، إذ لا يمكن لهذا الأخير أن ينمو ويتطور بمعزل عن الاقتصاد العالمي. وهذا يستلزم أن تواكب عمليات التأمين التطورات الحديثة من خلال تقديم خدمات التأمين إلكترونيا، والابتعاد عن الأساليب التقليدية في إبرام عقود التأمين، لما يتيحه ذلك من مزايا تتماشى مع السرعة والمرونة التي تميز المعاملات التجارية. ولأن استخدام شبكات الإنترنت في تقديم خدمات التأمين يعد فكرة جديدة نسبيا في الجزائر، فإن الأمر يتطلب وعيا وإدراكا لأهمية التجارة الإلكترونية في دفع عجلة التنمية الاقتصادية وتحقيق أهداف شركات التأمين.

وبناء على ذلك، فإن بيان التنظيم القانوني للتأمين الإلكتروني أصبح ضرورة تمليها طبيعة الحياة التجارية المعاصرة المليئة بالمخاطر، خاصة بالنسبة لأصحاب

المشاريع الاستثمارية الذين يسعون إلى إبرام عقود تأمين على استثماراتهم بعيدا عن التعقيدات الإدارية التي قد تعيق جذب الاستثمارات. كما يقتضي اعتماد التأمين الإلكتروني من الدول تهيئة البنية التقنية الحديثة ونشر الثقافة الإلكترونية لدى كل من المستهلكين وموظفي شركات التأمين، لتمكينهم من التعامل مع الشبكة المعلوماتية في تسويق خدمات التأمين إلكترونيا.

وتكمن صعوبة هذا الموضوع في أن أغلب دول العالم لم تخصص بعد قانونا مستقلا ينظم التأمين الإلكتروني، رغم أن بعض الدول تبنت تطبيقاته على أرض الواقع استنادا إلى قوانين التجارة الإلكترونية والتوقيع الإلكتروني، التي عرفت العقد الإلكتروني وآليات إبرامه وتنفيذه عن بعد. أما في الجزائر، فعلى الرغم من صدور قانون التوقيع والتصديق الإلكترونيين وقانون التجارة الإلكترونية، لا يزال التأمين يمارس وفق الأساليب التقليدية، كما لمسنا ذلك عمليا لدى شركات التأمين الوطنية. وقد دفعنا إلى اختيار هذا الموضوع عدة أسباب، من أبرزها:

1 . إن فكرة التأمين الإلكتروني، التي ظهرت نتيجة انتشار المعاملات التجارية عبر الإنترنت، لا تزال شبه مجهولة في ظل غياب تنظيم قانوني خاص بها، وندرة الإشارات إليها في كتابات الفقهاء وأحكام القضاء، مما يستدعي وضع قواعد قانونية خاصة بهذا النوع من التأمين، استنادا إلى أحكام التجارة الإلكترونية والقواعد العامة لإبرام العقود إلكترونيا.

2 . بروز تطبيقات التأمين الإلكتروني، خصوصا في المجال التجاري، بصورة متزايدة وقوية، دفع بعض الدول إلى إصدار قرارات تنظم هذا المجال، من أبرزها القرار رقم (2) لسنة 2012 بشأن استخدام النظام الإلكتروني الفلسطيني للتأمين على المركبات وتنظيم آلية عمله وفقا لأحكام قانون التأمين رقم (20) لسنة 2005.

3 . قصور القواعد العامة المنظمة للتأمين التقليدي عن مواجهة النتائج القانونية والعملية التي تترتب على إبرام وتنفيذ التأمين إلكترونيا.

ومما تقد تطرح إشكالية مفادها **في ظل التحوّل نحو بيئة رقمية حتمية، ما هو واقع التنظيم التشريعي للتأمين الإلكتروني في الجزائر، وعلاقته بالإطار القانوني للعقود الإلكترونية؟**

وللإجابة على هذا الإشكال ارتأينا تقسم الموضوع لمبحثين سنتطرق أولا لمفهوم التأمين الإلكتروني ثم سنعرج ثانيا على أثار هذا العقد بالنسبة للمستهلك والمورد الإلكترونيين

المبحث الأول:

مفهوم التأمين الإلكتروني

يعد التأمين من أهم الأنشطة الاقتصادية في العالم، لارتباطه المباشر بالتنمية الاقتصادية، إذ يسهم في دعم مختلف الأنشطة التجارية مثل الاستثمار، وأعمال المقاولات، وعقود النقل، وغيرها من الأنشطة المرتبطة بالحركة الاقتصادية. كما يؤثر التأمين إيجابا في هذه الأنشطة، ويسهم في تمويل الاستثمارات المنتجة التي تعد ركيزة أساسية للتقدم. ومن ثم، تبرز ضرورة تبسيط إجراءات التأمين وإزالة التعقيدات الإدارية التي قد تثني المستهلكين عن الاستفادة من خدماته. وقد حققت الدول المتقدمة في مجال التأمين تطورا ملحوظا بإنشاء شبكات معلومات ضخمة على المستوى الدولي، وتوظيف كفاءات ذات خبرة عالية، إلى جانب دعمها بمؤسسات مالية قوية.

وانطلاقا من هذا التطور، أصبح من الضروري فهم كيفية إجراء التأمين بوسائل إلكترونية حديثة، الأمر الذي يستدعي بداية توضيح مفهوم التأمين الإلكتروني وبيان خصائصه المميزة. وبناء عليه، سنقسم هذا المبحث إلى مطلبين:

نتناول في المطلب الأول تعريف التأمين الإلكتروني، بينما نخصص المطلب الثاني لبيان خصائصه وذاتيته.

المطلب الأول:

تعريف التأمين الإلكتروني

تعد فكرة تقديم خدمات التأمين إلكترونيا حديثة نسبيا في معظم الدول، وخاصة النامية منها، إذ تتطلب توفر بنية مادية وفنية متطورة تمكن من الانتقال من النمط التقليدي للتأمين إلى النمط الرقمي الحديث. ولهذا، يلاحظ أن الفقه القانوني لم يفرد تعريفا مستقلا للتأمين الإلكتروني، انسجاما مع غياب تنظيم قانوني خاص به، في حين اقتصر على تعريف التأمين بصورته التقليدية بأنه: «اتفاق يلتزم بموجبه المؤمن، مقابل قسط معين، بأن يؤدي إلى المؤمن له أو إلى الغير المستفيد مبلغا من المال أو إيرادا أو أي أداء آخر، في حال تحقق الخطر المتفق عليه في العقد»[1]. كما ذهب جانب من الفقه إلى اعتباره «عقدا وعملية فنية في آن واحد؛ فهو يحتوي على جانب قانوني يتمثل في العلاقة التعاقدية بين الطرفين، وجانب فني يقوم على التعاون بين مجموعة من الأشخاص لتوزيع نتائج الكوارث والخسائر بينهم»[2].

ويستفاد من هذه التعريفات أن التأمين، باعتباره عقدا تجاريا احتماليا، يقوم على جانبين متكاملين: جانب قانوني يرتكز على التزام المؤمن بدفع تعويض مناسب للمؤمن له عند تحقق الخطر المؤمن ضده، وجانب فني يقوم على مبدأ التعاون وتقاسم الخسائر داخل الجماعة المؤمنة.

[1] عصام أنور سليم، أصول عقد التأمين، منشأة المعارف، الإسكندرية، 2008، ص11.

[2] احمد شرف الدين، أحكام التأمين –دراسة في القانون والقضاء المقارنين، مطبعة نادي القضاة، ط3، 1991، ص12.

أما في الجزائر، فلم يحدد المشرع بعد تعريفا للتأمين الإلكتروني، واكتفى بتعريف التأمين التقليدي في المادة (2) من الأمر رقم 95-07 المتعلق بالتأمينات بأنه: «عقد يلتزم المؤمن بمقتضاه بأن يؤدي إلى المؤمن له أو الغير المستفيد الذي اشترط التأمين لصالحه مبلغا من المال أو إيرادا أو أي أداء مالي آخر، في حالة تحقق الخطر المبين في العقد، وذلك في مقابل أقساط أو أي دفعة مالية أخرى»[1].

وعلى الرغم من صدور القانون رقم 15-04 لسنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين، فإن التأمين لا يزال يمارس بالأسلوب التقليدي، ولم يتطرق القانون المذكور إلى تنظيم التأمين الإلكتروني ضمن أحكامه.

غير أن تبني التأمين الإلكتروني في الجزائر ممكن بالاستناد إلى القواعد العامة الواردة في قانون التجارة الإلكترونية، الذي عرف العقد الإلكتروني بأنه: «العقد الذي يتم إبرامه عن بعد، دون الحضور الفعلي والمتزامن لأطرافه، باللجوء حصريا إلى تقنيات الاتصال الإلكتروني»[2]. ومن ثم، فإن عقد التأمين يمكن أن يبرم إلكترونيا من خلال تقديم الطلبات والمستندات والتفاوض وإبرام العقد عبر وسائل إلكترونية، بعيدا عن التعقيدات الإدارية التقليدية.

وتجدر الإشارة إلى أن كثيرا من دول العالم لم تخصص بعد قانونا مستقلا للتأمين الإلكتروني، لكنها سمحت به ضمنيا من خلال تشريعات التجارة الإلكترونية والتوقيع الإلكتروني، بل إن بعضها أصدر قرارات خاصة لتقنينه، مثل القرار رقم

[1] المادة 2 من الأمر رقم 95-07 المتعلق بالتأمينات المؤرخ في 25 يناير سنة 1995، جريدة رسمية عدد 13 الصادرة بتاريخ 8 مارس سنة 1995.

[2] قانون رقم 18-05 المؤرخ في 10 مايو 2018، يتعلق بالتجارة الإلكترونية، جريدة رسمية عدد 28 الصادرة بتاريخ 16 مايو سنة 2018.

(2) لسنة 2012 بشأن استخدام النظام الإلكتروني الفلسطيني للتأمين على المركبات[1].

وبالاستناد إلى ما سبق، يمكن اقتراح تعريف للتأمين الإلكتروني بأنه: «عقد يلتزم بموجبه المؤمن بتقديم التغطيات التأمينية والتعاون والتعاقد عبر الإنترنت، مقابل أقساط أو دفعات مالية يؤديها المؤمن له باستخدام وسائل الدفع الإلكتروني».

المطلب الثاني:

خصائص التأمين الإلكتروني

يتميز التأمين الإلكتروني بجملة من الخصائص التي تعكس طبيعته الخاصة وتميزه عن غيره من العقود، ويمكن تلخيصها فيما يلي:

أولا: التأمين الإلكتروني عقد يبرم عن بعد

يبرم عقد التأمين الإلكتروني من خلال شبكات الإنترنت، حيث تتم عملية بيع وشراء خدمات التأمين دون حضور فعلي ومتزامن للأطراف في مجلس عقد واحد. وبذلك يعد العقد مبرما بين غائبين من حيث المكان، وإن كان يبرم بين حاضرين من حيث الزمان، كما تنفذ التزامات أطرافه بوسائل إلكترونية[2].

ويمر هذا العقد بعدة مراحل، تبدأ بالإعلان عن خدمات التأمين على الموقع الإلكتروني لشركة التأمين، ثم قيام المستهلك بالاختيار والتقديم، يلي ذلك مرحلة

[1] يوسف حسن يوسف، التسويق الالكتروني، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012، ص27.

[2] محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية، عمان، 2006، ص28.

التفاوض وتبادل المعلومات إلكترونيا، لتنتهي بإبرام العقد وتنفيذه وفقا للشروط المحددة فيه.

ثانيا: التأمين الإلكتروني من عقود الإذعان

يعد عقد التأمين الإلكتروني من عقود الإذعان، لأن المستهلك لا يملك سوى الموافقة أو الرفض لشروط موضوعة مسبقا من طرف شركة التأمين على موقعها الإلكتروني، ولا يتاح له مناقشة تلك الشروط أو تعديلها[1].

ولهذا يستحسن أن تضع شركات التأمين الإلكترونية وسطاء إلكترونيين أو أدوات تفاعلية للرد على استفسارات المستهلكين وتوضيح الشروط قبل إبرام العقد، بما يعزز الثقة ويشجع على الإقبال على التأمين الإلكتروني بدلا من الاكتفاء بالنماذج الجامدة التي قد تنفر بعض المتعاملين.

ثالثا: التأمين الإلكتروني من عقود حسن النية

يقوم عقد التأمين الإلكتروني، كغيره من عقود التأمين، على مبدأ حسن النية، إذ يعتمد المؤمن (شركة التأمين) على البيانات التي يصرح بها طالب التأمين عبر نموذج إلكتروني مخصص، ومن خلالها يقيم درجة الخطر ويحدد قيمة القسط التأميني المناسب.

وفي حال تحقق الخطر المؤمن ضده، تتحقق الشركة من صحة البيانات المصرح بها، فإذا ثبت عدم صحتها جاز لها رفض التعويض. لذلك يتعين على الطرفين الالتزام بمبدأ حسن النية في جميع مراحل التعاقد: التفاوض، والإفصاح عن

[1] عمر حسن الموفي، التوقيع الالكتروني وقانون التجارة الالكترونية، عمان، 2003، ص35-36.

البيانات والتنفيذ[1]، وهو ما يعزز الثقة ويحقق التوازن العقدي رغم أن العقد يبرم عن بعد. ويعد هذا الالتزام قيدا على كل من المستهلك وشركة التأمين، ويستمد أساسه من مبدأي سلطان الإرادة و«العقد شريعة المتعاقدين»[2].

المبحث الثاني:

آثارعقد التأمين الإلكتروني

أشرنا في المبحث المتقدم أن من خصائص التأمين الالكتروني أنه عقد الكتروني، وحيث أن آثار أي عقد تتمثل بالحقوق والالتزامات التي تترتب على عاتق كل من طرفيه، وطالما إن الأمر كذلك، لذا سنبحث الالتزامات فقط لأنها تمثل حقوقا للطرف الأخر. لهذا سنقسم هذا المبحث على مطلبين، نتناول في المطلب الأول التزامات المؤمن له (المستهلك الإلكتروني)، أما المطلب الثاني فسنعقده لالتزامات المؤمن (المورد الإلكتروني).

[1] ينظر في ذلك نص الفقرة (1) من المادة 107 من القانون المدني الجزائري على انه "يجب تنفيذ العقد طبقا لما اشتمل علية و بحسن النية". وكذلك أشارت اتفاقية الأمم المتحدة للبيع الدولي للبضائع لسنة 1980 إلى مبدأ حسن النية في نص المادة (7) على انه "1- يراعى في تفسير هذه الاتفاقية صفتها الدولية وضرورة تحقيق التوحيد في تطبيقها، كما يراعى ضمان احترام حسن النية في التجارة الدولي" كذلك نجد إن مبادئ اليونيدرموا المتعلقة بالعقود التجارية الدولية لسنة 2010 قد نصت على مبدأ حسن النية في نص المادة (1-7) "على ضرورة التزام الأطراف بأن يتعرفوا وفقا لما يقتضيه مبدأ حسن النية وأمانة التعامل في التجارة الدولية:.

[2] احمد شرف الدين، أحكام التأمين، مرجع سابق، ص80.

المطلب الأول:

التزامات المستهلك (المؤمن له)

يلتزم المؤمن له (المستهلك الإلكتروني) بمقتضى عقد التأمين الإلكتروني بعدة التزامات أساسية تمكن شركة التأمين من تقييم المخاطر بدقة وتنفيذ التزاماتها، أبرزها: الإفصاح عن البيانات، أداء قسط التأمين، وإشعار الشركة بتحقق الخطر المؤمن ضده، كما يلي:

الفرع الأول: الالتزام بالإفصاح عن البيانات المتعلقة بالخطر

يمثل الخطر حجر الزاوية التي يقوم عليها التأمين الالكتروني، فالمقصود من هذا الأخير هو تفادي أو تخفيف أثر الخطر[1]، فالمؤمن يحرص على معرفة اكبر قدر من المعلومات عن الخطر[2].

يعد الإفصاح عن البيانات من أهم التزامات المؤمن له، إذ يمكن شركة التأمين من تقييم الخطر محل العقد. وقد نصت الفقرة (ب) من المادة (986) من القانون المدني العراقي على أن المؤمن له يلتزم عند إبرام العقد بالإفصاح عن جميع الظروف المعلومة له والتي تهم المؤمن معرفتها لتقدير المخاطر التي يتحملها.

وبالقياس على عقود التأمين الإلكتروني، يتعين على طالب التأمين ملء نموذج بيانات إلكتروني يتضمن معلومات دقيقة عن محل التأمين والظروف المحيطة بالخطر، كما يلتزم بإخطار الشركة بأي تغييرات قد تؤدي إلى زيادة احتمالات وقوع

[1] محمد حسن قاسم، القانون المدني، العقود المسماة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص556.

[2] عبد الهادي السيد محمد تقي الحكيم، عقد التأمين، حقيقته ومشروعيته، منشورات الحلبي الحقوقية، بيروت، ط1، 2003، ص99.

الخطر أثناء سريان العقد[1]. ويعد هذا الالتزام جوهريا نظرا لاعتماد المعاملات الإلكترونية على الثقة المتبادلة بين الأطراف.

الفرع الثاني: الالتزام بأداء قسط التأمين إلكترونيا

يعد الالتزام بأداء قسط التأمين من ابرز الالتزامات على عاتق المؤمن له (المستهلك الإلكتروني)، لأنه يعد المقابل الذي يدفعه نظير التزام شركة التأمين بضمان الخطر، والواقع إن هذه الأقساط تكون لشركات التأمين الالكترونية سلطة في تقديرها حسب نوع الخطر المؤمن ضده وبناء على البيانات التي تم الحصول عليها من قبل المؤمن له[2].

فدفع القسط التأميني المقابل الأساسي لالتزام شركة التأمين بتحمل الخطر، وتحتفظ الشركة بسلطة تقدير قيمة القسط بناء على درجة الخطر المصرح بها[3]. ويتميز التأمين الإلكتروني بأن دفع الأقساط يتم عبر وسائل الدفع الإلكتروني، كالبطاقات البنكية وبطاقات الائتمان والتحويلات المصرفية الرقمية، بدل الطرق التقليدية[4].

[1] تنص الفقرة (3) من المادة (15) من قانون التأمينات على انه "يلزم المؤمن له: 3- بالتصريح الدقيق بتغيير الخطر أو تفاقمه إذا كان خارج عن إرادة المؤمن له ..."

[2] مصطفى محمد الجمال، أصول التأمين، مرجع سابق، ص305.

[3] حسين عبد الله الرضا، الوفاء الالكتروني كوسيلة لتنفيذ الالتزام – دراسة قانونية، بحث منشور في مجلة كلية الحقوق، جامعة النهرين، المجلد 14، العدد 3، 2012، ص11.

[4] محمود السيد عبد المعطي خيال، الانترنت وبعض الجوانب القانونية، دار النهضة العربية، القاهرة، 1998، ص145.

وقد أجاز المشرع الجزائري التعامل بالوسائل الإلكترونية لتحويل الأموال، ما يسهل تنفيذ هذا الالتزام ويحقق السرعة وتقليل التكاليف، شريطة تطوير البنية المصرفية لتدعيم أدوات الدفع الإلكتروني وضمان أمانها[1].

الفرع الثالث: الالتزام بإشعار الشركة بتحقق الخطر المؤمن ضده

عند تحقق الخطر المؤمن ضده، لا تنشأ مسؤولية شركة التأمين تلقائيا، بل يجب على المؤمن له إشعار الشركة بذلك فورا، لتمكينها من اتخاذ التدابير اللازمة لتقليل الأضرار والتحقق من أسباب وقوع الخطر[2]. وفي إطار التأمين الإلكتروني، يتم هذا الإشعار عادة عبر البريد الإلكتروني أو بوابات مخصصة على موقع الشركة، على أن ترد الشركة بتأكيد استلام الإشعار[3].

ويفضل أن يرفق المؤمن له تقريرا إلكترونيا موثقا يتضمن وصفا للأضرار الحاصلة، إذ إن التأخر في الإشعار أو تقديم بيانات غير دقيقة قد يؤدي إلى سقوط

---

[1] تنص المادة (27) من قانون التجارة الالكترونية على انه "يتم الدفع في المعاملات التجارية الإلكترونية إما عن بعد أو عند تسليم المنتج، عن طريق وسائل الدفع المرخص بها، وفقا للتشريع المعمول به.
عندما يكون الدفع إلكترونيا، فإنه يتم من خلال منصات دفع مخصصة لهذا الغرض، منشأة ومستغلة حصريا من طرف البنوك المعتمدة من قبل بنك الجزائر وبريد الجزائر وموصولة بأي نوع من أنواع محطات الدفع الإلكتروني عبر شبكة المتعامل العمومي للمواصلات السلكية واللاسلكية.
يتم الدفع في المعاملات التجارية العابرة للحدود، حصريا عن بعد، عبر الاتصالات الإلكترونية."

[2] توفيق حسن فرج، أحكام التأمين، القواعد العامة للتأمين، مؤسسة الثقافة الجامعية، الإسكندرية، ط2، 1996، ص56.

[3] بشار محمود دودين، الإطار القانون للعقد المبرم عبر شبكة الانترنت، دار الثقافة والنشر والتوزيع، عمان، ط1، 2010، ص200.

حقه في التعويض. ولهذا أنشأت بعض الشركات منصات إلكترونية (Extranet)[1] للتفاعل مع وكلائها وعملائها وتلقي الإشعارات إلكترونيا بشكل فوري وموثوق.

وتعد هذه الالتزامات الثلاثة أساس العلاقة التعاقدية في التأمين الإلكتروني، ويؤدي الإخلال بها إلى إعفاء شركة التأمين من التزاماتها أو تقليص مسؤوليتها طبقا لشروط العقد.

المطلب الثاني:

التزامات المؤمن (المورد الإلكتروني)

يلتزم المؤمن (المورد الإلكتروني) بعدة التزامات جوهرية بموجب عقد التأمين الإلكتروني، تهدف إلى ضمان حماية حقوق المؤمن له وتحقيق التوازن العقدي، وأبرزها:

الفرع الأول: الالتزام بدفع مبلغ التأمين عند تحقق الخطر المؤمن ضده

يعد هذا الالتزام من أهم التزامات شركة التأمين الإلكترونية، إذ يتعين عليها دفع مبلغ التأمين أو التعويض المتفق عليه بمجرد تحقق الخطر المؤمن ضده، أو عند حلول الأجل إذا كان التزامها مضافا إلى أجل معين.

ولا ينشأ هذا الالتزام إلا إذا كان المؤمن له قد أوفى بجميع التزاماته المنصوص عليها في العقد، كالإفصاح عن البيانات وسداد الأقساط، ويعد ذلك شرطا سابقا لاستحقاق التعويض[1].

[1] يعرف الاكسترانت بأنه "شبكة مكونة من مجموعة شبكات انترانت ترتبط ببعضها عن طريق الانترنت وتحافظ على خصوصية كل شبكة انترانت مع منح أحقية الشراكة على بعض الخدمات والملفات فيما بينها".

الفرع الثاني: الالتزام بآلية تسوية المطالبات إلكترونيا

تلتزم شركة التأمين بتوفير منصة إلكترونية تمكن المؤمن له من تقديم طلبات التعويض إلكترونيا عبر نماذج مخصصة، مرفقة بالمستندات والأدلة التي تثبت صحة المطالبة.

كما يجب عليها التأكيد على استلام الطلبات وإخطار المؤمن له بمراحل معالجتها إلكترونيا، بما يضمن الشفافية والسرعة في تسوية التعويضات[2].

الفرع الثالث: الالتزام بالحفاظ على سرية البيانات

تتحمل شركات التأمين الإلكترونية مسؤولية قانونية بالحفاظ على سرية بيانات العملاء وعدم إفشائها أو استغلالها دون إذن. ويشمل ذلك التزامها بفرض السرية على جميع موظفيها ووكلائها والبنوك المتعاملة معها، تحت طائلة المسؤولية التضامنية عند الإخلال.

وتعد حماية البيانات الشخصية من أبرز التحديات في البيئة الرقمية، لذا تلزم الهيئات الرقابية شركات التأمين بإبرام اتفاقيات سرية معلومات (Confidentiality Agreements) كجزء من نظام التأمين الإلكتروني[3].

---

[1] عصام أنور سليم، مرجع سابق، ص250 .

[2] ينظر في ذلك نص المادة (4) من قرار رقم (2) لسنة 2012 بشأن استخدام النظام الالكتروني الفلسطيني للتأمين على المركبات وتنظيم آلية عمله بمقتضى أحكام قانون التأمين رقم 20 لسنة 2005 التي نصت على انه: "تلتزم جميع الأطراف المستخدمة للنظام بالسرية التامة وعدم استخدام الشبكة بينها وبين أي طرف أخر لأي أغراض أخرى غير المخصصة لها...2- تلتزم جميع الجهات المستخدمة للنظام بالتوقيع على نموذج سرية المعلومات الذي يعتبر جزءا لا يتجزأ من هذه الآلية".

[3] احمد شرف الدين، مرجع سابق، ص383.

وبالإضافة إلى هذه الالتزامات، يخضع عقد التأمين الإلكتروني في النهاية إلى القواعد العامة لانقضاء العقود، فينتهي بانقضاء مدته، أو بتحقق الخطر ودفع التعويض، أو بفسخه أو انحلاله لأي سبب قانوني آخر، غير أن ذلك لا يعد من التزامات المؤمن بل من الآثار اللاحقة للعقد.

الخاتمة

توصلت هذه الدراسة حول عقد التأمين الإلكتروني بين متطلبات البيئة الرقمية وخصوصيات التنظيم القانوني في الجزائر إلى أن هذا النمط من العقود أصبح ضرورة حتمية تفرضها التحولات التكنولوجية في المعاملات الحديثة، إذ يوفر آلية سريعة وفعالة لإبرام وتنفيذ عقود التأمين عبر الوسائط الرقمية.

ورغم أن التشريع الجزائري لم ينص صراحة على عقد التأمين الإلكتروني، إلا أنه يمكن إخضاعه للقواعد العامة لعقود التأمين التقليدية، طالما لا تتعارض مع طبيعته الرقمية، على أن يستكمل ذلك بأحكام قانون التجارة الإلكترونية والتوقيع الإلكتروني وحرية الإثبات في المادة التجارية.

وقد بينت الدراسة أهم الآثار القانونية لعقد التأمين الإلكتروني، والمتمثلة في التزامات كل من المؤمن له (المستهلك الإلكتروني) من جهة، والمؤمن (المورد الإلكتروني) من جهة أخرى، وكيفية تنفيذها في بيئة إلكترونية وفق ضوابط قانونية وتقنية تضمن حماية حقوق الطرفين.

أهم التوصيات:

1. ضرورة تدخل المشرع الجزائري لإصدار نصوص قانونية خاصة تنظم عقد التأمين الإلكتروني بشكل صريح ومستقل.

2. سن تشريعات حديثة لحماية المستهلك الإلكتروني في مجال التأمين عبر الإنترنت، خاصة فيما يخص حماية البيانات الشخصية وحق العدول.

3. تأهيل وتكوين الموارد البشرية العاملة في قطاع التأمين لاستخدام الوسائل التكنولوجية الحديثة في مختلف مراحل التعاقد الإلكتروني.

4. وضع قواعد قانونية واضحة تحدد وسائل إثبات عقد التأمين الإلكتروني وطرق حفظه وأرشفته رقميا بما يضمن سلامته القانونية.

5. استحداث آليات فعالة للرقابة على نشاط شركات التأمين الإلكترونية وضمان التزامها بمعايير الأمان المعلوماتي وحماية بيانات العملاء.

وبهذا، فإن تنظيم عقد التأمين الإلكتروني تشريعيا ورقميا أصبح شرطا أساسيا لمواكبة التحول الرقمي في قطاع الخدمات المالية والتأمينية وضمان حماية المستهلك وثقة المتعاملين.

قائمة المراجع

1- النصوص القانونية

- قانون الاونسيترال النموذجي بشأن التجارة الالكترونية لسنة 1996.
- اتفاقية الأمم المتحدة للبيع الدولي للبضائع لسنة 1980.
- مبادئ اليونيدروا المتعلقة بالعقود التجارية الدولية لسنة2010.
- اتفاقية الأمم المتحدة للبيع الدولي للبضائع لسنة 1980.
- القانون رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم بالقانون رقم 05-10، المؤرخ في 20 جوان 2005، جريدة رسمية عدد 44، لسنة 2005.
- الأمر رقم 95-07 المتعلق بالتأمينات المؤرخ في 23 شعبان عام 1415 الموافق 25 يناير سنة 1995، جريدة رسمية عدد 13 الصادرة بتاريخ 7شوال عام 1415 الموافق 8 مارس سنة 1995.
- قانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو 2018، يتعلق بالتجارة الإلكترونية، جريدة رسمية عدد 28 الصادرة بتاريخ 30 شعبان عام 1439 الموافق 16 مايو سنة 2018.
- قرار رقم (2) لسنة 2010 بشأن استخدام النظام الالكتروني الفلسطيني للتأمين على المركبات وتنظيم الية عمله بمقتضى أحكام قانون التأمين رقم 20 لسنة 2005.

2- المؤلفات

- عصام أنور سليم، أصول عقد التأمين، منشأة المعارف، الإسكندرية، 2008.
- احمد شرف الدين، أحكام التأمين –دراسة في القانون والقضاء المقارنين، مطبعة نادي القضاة، ط3، 1991.

- يوسف حسن يوسف، التسويق الالكتروني، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012.
- محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية، عمان، 2006.
- عمر حسن الموفي، التوقيع الالكتروني وقانون التجارة الالكترونية، عمان، 2003.
- محمد حسن قاسم، القانون المدني، العقود المسماة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.
- عبد الهادي السيد محمد تقي الحكيم، عقد التأمين، حقيقته ومشروعيته، منشورات الحلبي الحقوقية، بيروت، ط1، 2003.
- مصطفى محمد الجمال، أصول عقد التأمين (عقد الضمان)، منشورات الحلبي الحقوقية، لبنان، ط1، 1999.
- محمود السيد عبد المعطي خيال، الانترنت وبعض الجوانب القانونية، دار النهضة العربية، القاهرة، 1998.
- توفيق حسن فرج، أحكام التأمين، القواعد العامة للتأمين، مؤسسة الثقافة الجامعية، الإسكندرية، ط2، 1996.
- بشار محمود دودين، الإطار القانون للع3قد المبرم عبر شبكة الانترنت، دار الثقافة والنشر والتوزيع، عمان.

3- المقالات العلمية

- حسين عبد الله الرضا، الوفاء الالكتروني كوسيلة لتنفيذ الالتزام – دراسة قانونية، بحث منشور في مجلة كلية الحقوق، جامعة النهرين، المجلد 14، العدد 3، 2012.

التحول الرقمي لقانون الأعمال في الجزائر

Digital transformation of business law in Algeria.

د / بوستة زهر الدين.

جامعة الشاذلي بن جديد - الطارف، boucetta-zahr-edine@univ-eltarf.dz

د / بوعشة كمال.

جامعة الشاذلي بن جديد - الطارف، إيميل الباحث الثاني الخط: bouacha-kamel@univ-eltarf.dz

ملخص:

عرفت الجزائر نقلة تكنولوجية و معلوماتية نوعية كان لها الأثر على جملة من المجالات ذات الارتباط المباشر بالقانون في مقدمتها الأنشطة الاقتصادية ، إذ تجلت هذه الاصلاحات ضمن التعاملات الرقمية ، التجارة الالكترونية و الدفع الالكتروني و المؤسسات و الشركات الرقمية و هي أجزاء لا تتجزأ من بيئة الأعمال في محاولة لإعادة تكييف هذا القانون مع التوجه الجديد للدولة.

إن ارتباط هذه الإصلاحات بالتنمية الوطنية الاقتصادية الشاملة ، دفع إلى إعادة النظر من جديد في عدة محاور منها الاستثمار و التجارة و وسائل الدفع ...إلخ، بهدف تسهيل الإجراءات و تحسين الشفافية و استحداث بيئة رقمية مختلفة عن البيئة التقليدية التي لم تحقق النتائج التنموية المرجوة منها ، بذلك كان للرقمنة آثارًا على طبيعة قانون الأعمال.

الكلمات المفتاحية: تحول ؛قانون الأعمال ؛ رقمنة ، اقتصاد رقمي.

***Abstract**:*
Algeria has witnessed a qualitative technological and informational shift that has had an impact on a number of areas related to the law, most notably economic activities. These reforms have been evident in digital transactions, e-commerce, e-payment, and digital institutions and companies, which are integral parts of the business environment, in an attempt to re-adapt this law to the state's new direction.
The connection between these reforms and comprehensive national economic development has prompted a renewed review of several aspects, including investment, trade, and payment methods, etc., with the aim of facilitating procedures, improving transparency, and creating a digital environment distinct from the traditional environment, which has not achieved the desired developmental outcomes. Thus, digitization has had an impact on the nature of business law.
***Keywords:** Transformation; Business Law; Digitization ;Digital economy.*

مقدمة:

عرف العالم في السنوات العقود الأخيرة تحولات جدرية بفعل النقلة التكنولوجية التي مست مختلف مجالات الحياة سواء الاقتصادية أو الاجتماعية و حتى القانونية، إذ أضحت الاستخدامات الرقمية حتمية ضرورية بالنسبة للأنشطة الإدارية و التجارية و بذلك تم استحداث فضاءات الكترونية لإدارة الأعمال بالاعتماد على التقنيات الحديثة كالذكاء الاصطناعي.

إن هذه التحولات فرضت نفسها في الجزائر على الأنظمة القانونية ، فبرزت عدة مسائل قانونية ذات ارتباط باستخدام الرقمة ، حول ملاءمة القواعد التقليدية لتنظيم هذه المعاملات أو حول مسألة ضمان حماية المعاملات في البيئة الرقمية ...إلخ ، و بما أن الرقمنة ليست مجرد تحديث تقني فقط بل هي تغيير في المفاهيم و الأحكام و القواعد القانونية التي تؤطر شأناً قانونياً معيناً و منه إعادة النظر في القواعد و المبادئ التقليدية التي تشكل التنظيم القانوني للعلاقات التجارية ، من خلال رسم معالم جديدة للعلاقة بين القانون و الاقتصاد عبر التحفيز على الابتكار من جهة و ضمان سبل الحماية القانونية للاقتصاد و المجتمع ، منه برزت الإشكالية

التي تتمحور حول مدى ساهم الطريق الرقمي في تغيير قواعد قانون الأعمال في الجزائر؟

المبحث الأول:

اعتماد الرقمنة في التشريعات الجزائرية :

تبنت الجزائر مسار إصلاحياً للرقمنة الشاملة عبر محاور رئيسة تعمل على تطويرها من بينها الحوكمة الرقمية و الاقتصاد الرقمي و المجتمع الرقمي ، إذ تم اعتماد استراتيجية وطنية للتحول الرقمي تمس كل القطاعات ، و بذلك لابد من إبراز الأهمية القانونية للرقمنة (المطلب الأول) و التي كانت السبب في هذا التحول ، ثم توضيح أهم مظاهر هذا التحوّل في جانب قانون الأعمال (المطلب الثاني) .

المطلب الأول:

الأهمية القانونية للرقمنة:

تبرز الأهمية العامة للتحوّل الرقمي فيما يمكنه تقديمه لوضع حلول للمشكلات البشرية من جهة و تحقيق التوازن مع التنمية وتعزيز استدامتها من جهة أخرى ، و هو يشمل جميع الجوانب الاقتصادية الاجتماعية ، البيئية و الثقافية و لاسيما القانونية[1]. و للرقمنة أهمية بالغة من الزاوية القانونية من باب كوّنها دعامة أساسية للدولة الحديثة – دولة القانون - حيث تساهم التحولات الرقمية في إرساء قواعد جديدة لتنظيم المعاملات القانونية و الإدارية .

[1] عبد الله عبد الرحيم محمد مجرشي : دور إدارة التحول الرقمي في تطوير أداء المؤسسات ، دراسة ميدانية على مديرية الأحوال المدنية بمدينة تبوك في المملكة العربية السعودية، رسالة ماجستير، جامعة تبوك، المملكة العربية السعودية، 2023، ص 17.

إن تحديث المنظومة القانونية و التحول نحو إدارة عصرية من خلال اعتماد الطريق الرقمي لتبسيط الإجراءات الإدارية و القضائية و بذلك نكون قد ضمنا سرعة الوصول للمعلومات القانونية و كذا تداولها بكل شفافية بين مختلف المؤسسات و الهيئات .

كما تبرز كذلك الأهمية القانونية للرقمنة من خلال تعزيز مبدأ الامن القانوني و الذي نلمسه ضمن توثيق المعاملات الالكترونية و السجلات الرقمية، وبالتالي القضاء على أهم آفة تواجهها الدولة اليوم و هي التزوير، دون أن ننسى المساهمة الفعالة للرقمنة في ضمان تحسين أداء مرفق العدالة الذي يعتمد على أنظمة معلوماتية للتقاضي عن بعد [1] و تمكين المتقاضين من الأحكام بنفس الطريق و حتى الوثائق الصادرة على هذه الأجهزة على غرار وثيقة الجنسية، بذلك المساواة في الوصول إلى العدالة.

إن هذه المبررات هي التي تحفز الدولة على تكييف النظم القانونية مع البيئة الرقمية وتعزيز الثقة في الاقتصاد الرقمي الوطني.

المطلب الثاني:

أبرز الإصلاحات الرقمية ضمن قانون الأعمال:

شهد العالم خلال العقود الأخيرة ثورة رقمية غيرت ملامح الاقتصاد العالمي وأنماط التفاعل التجاري والإداري، بالتالي كان لهذه الإصلاحات انعكاس على مختلف فروع القانون، و كان قانون الأعمال أكثر هذه القوانين تأثرًا بالرقمنة لارتباطه بعدة

[1] بوعمرة عقبة : رقمنة الإجراءات القضائية و سرعة المحاكمة الجزائية أي علاقة؟، مجلة القانون والعلوم البيئية ، المجلد 03 ، العدد 03 جامعة الجلفة ، الجزائر، 2024 ، ص 142.

مسائل تتعلق بتطويره ، و بالتالي يمكن أن نلخص أهم القوانين التي صدرت في هذا السياق:

أولاً :النسبة للقانون النقدي و المصرفي: تبنت الجزائر مراجعة للنشاط النقدي و المصرفي، بموجب القانون رقم 23-09 المؤرخ في 21 يونيو2023 [1] ،إذ بمقتضى هذا القانون الجديد الذي ألغى الأمر رقم 03-11 المؤرخ في 26 أوت 2003[2]، المتعلق بالنقد والقرض، و من جملة الإصلاحات التي وردت ضمن مساعي رقمنة القطاع البنكي ، يمكن أن نذكر ما يلي :

1- **التوجه نحو اعتماد البنوك الرقمية** : نص المشرع الجزائري على اعتماد النوك الرقمية بموجب النظام رقم 24-04 المؤرخ في 13 أكتوبر 2024، المتعلق بالشروط الخاصة للترخيص بتأسيس و اعتماد و ممارسة نشاط البنك الرقمي ، و هو كل بنك يقدم خدمات و منتوجات مصرفية حصريا عبر قنوات أو منصات و دعائم رقمية باستخدام التكنولوجيات الحديثة في إطار ممارسة النشاط. و يشترط في ذلك أن يتمتع البنك بخبرة كافية في مجال الخدمات البنكية عبر الأنترنت و بالمقابل يقدم كافة العمليات و المنتجات البنكية التي تقدمها البنوك التقلدية و الإسلامية ، و تتوجه بالدرجة الأولى لفائدة أصحاب المشاريع الصغيرة و المتوسطة[3].

و تبين المادة الثانية الفقرة الثانية من النظام رقم 24- 04 ، أن التكنولوجيات المقصودة هي تلك المرتبطة بالإعلام و الاتصال و التكنولوجيا المالية.

[1] القانون رقم 23- 09 المؤرخ في 21 يونيو 2023، يتضمن القانون النقدي و المصرفي، ج ر عدد 43، المؤرخة في 27 يونيو 2023.

[2] الأمر رقم 03-11 المؤرخ في 26 أوت 2003[2]، المتعلق بالنقد والقرض، ج ر عدد 52، المؤرخة في 27 أوت 2003

[3] المادة 108 الفقرة 02 من القانون رقم 23-12.

2- استحداث **الدينار الرقمي** : من خلال القانون رقم 23-09 المتعلق بالقانون النقدي و المصرفي استحدث المشرع ضمن مسارات التحول الرقمي لأول مرة الدينار الرقمي و هي الشكل الرقمي لعملة البنك المركزي الجزائري.[1].

ثانيا : بالنسبة لقانون التجارة الالكترونية: سنت الجزائر لتنظيم المعاملات الإلكترونية القانون رقم 05-18 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، والذي وضع الأسس القانونية للعقود الإلكترونية، والتزامات المورد والمستهلك، و آليات الدفع الإلكتروني [2] .

ثالثا :بالنسبة للتصديق الالكتروني: كما نص القانون رقم 15-04 ، المؤرخ في 01 فيفري 2015، المتعلق بالتوقيع والتصديق الإلكترونيين على الاعتراف القانوني بالوثائق الإلكترونية، مما مكّن المؤسسات من تبادل المستندات و المعاملات عن بعد بشكل رسمي [3].

رابعاً : بالنسبة لقانون الصفقات العمومية: جاء في القانون رقم 23-12 المؤرخ في 05 أوت2023 ، الذي يحدد القواعد العامة المتعلقة بالصفقات العمومية[4]، جملة من الإجراءات التي ترمي إلى رقمنة هذه العقود الإدارية ، و إن كان موضوع رقمنة الصفقات العمومية يرجع إلى المرسوم الرئاسي رقم 10-236 ، المؤرخ في 17 أكتوبر 2010 ، المتعلق بتنظيم الصفقات العمومية [5] ، ليؤكد المرسوم الرئاسي 15 -

[1] المادة 02 الفقرة 02 من القانون رقم 23-09.

[2] القانون رقم 18- 05، المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية ، ج ر عدد28، المؤرخة في 16 ماي2018.

[3] القانون رقم 15-04 ، المؤرخ في 01 فيفري 2015، المتعلق بالتوقيع والتصديق الإلكترونيين ، ج ر عدد 06، المؤرخة في 10 فبراير 2015.

[4] المادة 12 الفقرة ب من النظام رقم 24-04 السابق الذكر.

[5] المرسوم الرئاسي رقم 10-236 ، المؤرخ في 17 أكتوبر 2010 ، المتعلق بتنظيم الصفقات العمومية ، ج ر عدد 58، المؤرخة في 07 أكتوبر 2010. (الملغى)

247 ، المتعلق بتنظيم الصفقات العمومية و تفويضات المرفق العام [1] حتمية التوجه الرقمي نتاج مؤشرات ترتبط برقمنة العمل الإداري لإضفاء أكبر قدر من الشفافية على هذه الأعمال.

بذلك كان المرسوم الرئاسي 10-236 الملغى، أول نص قانوني متعلق بالصفقات العمومية يتضمن تقنيات الإعلام [2]،تجسدت فيما يلي:

-**إجبارية نشر الصفقات العمومية إلكترونياً :** ورد في المادة 119 الفقرة 03 من المرسوم الرئاسي رقم 10 - 236 ،أنه يتعين النشر الإجباري للمعلومات المتعلقة بالصفقة العمومية في النشرة الرسمية لصفقات المتعامل العمومي و / أو في الموقع الإلكتروني للمصلحة المتعاقدة.

- **التواصل بين مختلف فواعل الصفقة بالطريق الالكترونية :** جاء في المادة 173 منه ،على استحداث البوابة الالكترونية للصفقات العمومية توضع تحت وصاية الوزير المكلف بالمالية ، و يحدد محتواها و كيفية سيرها بموجب قرار من وزير المالية.

- **إمكانية تبادل المعلومات المتعلقة بالصفقة بالطريق الالكترونية :** نصت المادة 174 منه ،على أنه يمكن للمصلحة المتعاقدة تمكين المترشحين أو متعهدي الصفقة العمومية ، من الوثائق المتعلقة بالدعوة للمنافسة ، كما يمكن أن يتم الرد بنفس الطريقة و ارتبط ذلك بقرار يصدر عن وزير المالية لكنه لم يصدر .

[1] النظام رقم 24- 04 المؤرخ في 13 أكتوبر 2024، المتعلق بالشروط الخاصة للترخيص بتأسيس و اعتماد و ممارسة نشاط البنك الرقمي ، ج ر العدد 77، المؤرخة في 19 نوفمبر 2024.

[2] بن جلول محمد ، زعرورة فاطمة : رقمنة الصفقات العمومية في التشريع الجزائري بين الواقع و المأمول على ضوء القانون الجديد 23- 12 مجلة البحوث القانونية و الاقتصادية ، المركز الجامعي أفلو ، المجلد 07 ، العدد 01 ، الجزائر ، 2024 ، ص 65.

أما بالنسبة للمرسوم الرئاسي 15 – 247، المؤرخ في 16 سبتمبر 2015 ، المتعلق بتنظيم الصفقات العمومية و تفويضات المرفق العام ، فقد أكد هو الآخر على ضرورة ادماج الرقمنة في جانب الصفقات العمومية و تجلى ذلك من خلال :

- **العمل على تكييف إجراءات إبرام الصفقة بالتحول من الطريق الورقي إلى الإلكتروني:** أحال المرسوم الرئاسي عدة مسائل تتعلق بالصفقات العمومية لصدور نصوص تنظيمية، وهي التي لم ترى النور و كانت السبب في عدم نجاعة هذه القواعد القانونية .

- **تحول طبيعة البوابة الخاصة بالصفقات العمومية و التأكيد عليها:** اصبحت هذه البوابة تمثل قاعدة بيانات و أرشيفا الكتروني يمكن من خلالها طلب الوثائق المتعلقة بالصفقات إلكترونيا و بالتالي استخدام المعلومات و بالتالي يعفى المتعهد من الملف الورقي.

- **مواصلة التوجه نحو النشر الإلكتروني للصفقات العمومية :** نص المرسوم الرئاسي السالف الذكر على أنه يجب على المصلحة المتعاقدة عند انطلاق كل سنة مالية إعداد قائمة بكل الصفقات العمومية التي تم إبرامها بعنوان السنة السابقة و تبيان أسماء المؤسسات التي حازت عليها بحسب ما ورد ضمن المادة 158 فقرة 01 منه، و بالنسبة للصفقات الجديدة فيتم إعداد برنامج تقديري للمشاريع قابل للتعديل و يتم النشر إجباريا إما في النشرة الرسمية لصفقات المتعامل العمومي و / أو في الموقع الإلكتروني للمصلحة المتعاقدة ، و للحفاظ على خصوصية المعلومات فإنه يمكن للمصلحة المتعاقدة الاستغناء عن هذا الإجراء.

و بصدور القانون 23-12 ، المؤرخ في 05 أوت 2023، الذي يحدد القواعد العامة المتعلقة بالصفقات العمومية الجديد الذي تخلى عن جانب تفويضات المرفق العام ، و صل المشرع نفس التوجه لرقمنة إجراءات الصفقة العمومية و خص

الفصل الثاني من الباب السادس تحت عنوان الرقمنة في مجال الصفقات العمومية و مظاهر تتلخص في :

- مواصلة الاعتماد على البوابة الإلكترونية للصفقات العمومية :

جاء في المادة 105 من القانون المستحدث أنه تتولى الوزارة المكلفة بالمالية تسيير البوابة الالكترونية للصفقات العمومية، يمكن استخدام المعلومات و الوثائق التي تمر عبرها كقاعدة بيانات ، ومن تم تحفظ ملفات المترشحين للمتعهدين بهدف استعمالها فيما يتبقى من الإجراءات[1].

- تبادل المعلومات بالطريقة الالكترونية : حاوت الجزائر مواكبة التحولات ، إذ تبنت سياسة تهدف إلى رقمنة مختلف القطاعات ، حيث جاءت الرقمنة لمواكبة التطورات و ضمان تنافسية الاقتصاد الوطني [2]. بذلك يجب على المصالح المتعاقدة وضع وثائق الدعوة للمنافسة و تمكين المترشحين للصفقات العمومية أو المتعهدين منها عبر الوسائط الالكترونية ، وذلك من خلال جدول زمني يحدد الوزير المكلف بالمالية بموجب قرار ، لكن الملاحظ أن ها القرار لم يرى النور . وبالمقابل يتم التعامل و الرد على الدعوة من جانب المترشحين بنفس الطريق ، و قد تكيف الإجراءات الورقية مع الإجراءات الرقمية .

- الإحصاء الاقتصادي في مجال الصفقات العمومية : وهو عملية إحصائية سنوية من طرف الوزارة المكلفة بالمالية للصفقات العمومية ، و بالمقابل يتوجب على

[1] المادة 106 من القانون رقم 23-12.

[2] بيصار عبد الحكيم ، بوتيارة عنتر "التحول الرقمي و الحوكمة الرقمية و مقاربات تحقيق التنمية المستدامة" مداخلة مقدمة ضمن فعاليات الملتقى الدولي : التحول الرقمي كآلية لتحقيق التنمية المستدامة بين التشريع الجزائري و التشريعات المقارنة المنعقد بالمركز الجامعي بريكة يوم 07 ماي 2024، ص 16.

المصالح المتعاقدة المساهمة في هذا المسعى عبر تقديم المعلومات اللازمة و في الوقت المناسب حتى تتمكن المصالح المعنية من إنجاز الإحصاء[1].

إذن، هي إصلاحات باشرتها الجزائر من خلال القانون 23-12 ضمن سياسة شاملة و استراتيجية وطنية للشفافية و الحد من الفساد و التحفيز على تطوير الأداة الانتاجية الوطنية و تشجيع المؤسسات الوطنية لاسيما الصغيرة و المتوسطة و المؤسسات الناشئة و دفع قطاع المقاولاتية ، لكن يبقى أهم عائق أمام هذا القانون تأخر صدور النصوص التنظيمية المتعلقة بتطبيقه.

خامساً: بالنسبة لقواعد الشركات التجارية :

ضمن التحفيز على بعث المؤسسات الناشئة و هي مؤسسات تعمل ضمن مجال التكنولوجيا و دعم الابتكار تم تعديل قواعد القانون التجاري الجزائري لاسيما المواد من 715 مكرر133 إلى غاية المادة 715 مكرر 143 منه بمقتضى القانون رقم 22-09 [2] المؤرخ في 05 ماي 2022، و هي شركة تجارية بشكلها و مهما يكن موضوعها ، عرفت على أنها شركة ينقسم رأسمالها إلى أسهم تضم شركاء لا يتحملون الخسائر إلا في حدود ما قدموا من حصص.

و بالرجوع إلى الفقرة الثانية من المادة 715 مكرر 133 من القانون التجاري المستحدثة تتأسس شركة المساهمة البسيطة من شخص واحد إلى عدة أشخاص طبيعيين و / أو معنويين ، حيث أنه إذا ضمت شخصا واحدًا فهي "شركة المساهمة البسيطة ذات الشخص الوحيد". يحدد رأسمال في القانون الأساسي و يحظر عليها اللجوء العلني للادخار أو طرح أسهمها للبورصة على الرغم من خضوعها للأحكام التي

[1] المادة 108 الفقرة 02 من القانون رقم 23-12.

[2] القانون رقم 22-09 ، المؤرخ في 05 ماي 2022 ، يعدل و يتمم الأمر رقم 75-59 ، المؤرخ في 26 سبتمبر 1975 و المتضمن القانون التجاري ج ر عدد 32، المؤرخة في 14 ماي 2022.

تتعلق بشركات المساهمة مثلما قضت المادة 715 مكرر 135 ، و هي القواعد التي استحدثت ضمن بعث مؤسسات مجالها التكنولوجيا و الابتكار .

إن هذه الأمثلة عن تطبيقات الرقمنة في مجال قانون الأعمال وهي ليست على سبيل الحصر ، بل أننا شهدنا مثلا العقد الإلكتروني الذي تبقى عديد القواعد القانونية المتعلقة به تحتاج إلى مزيد الرعاية و التوضيح في ظل خصوصيته بالمقارنة مع القواعد التقليدية للعقود المقررة بموجب أحكام القانون المدني.

المبحث الثاني:

انعكاسات التحول الرقمي على طبيعة قانون الأعمال

خلف التوجه الرقمي الجديد الذي انتهجته الجزائر ضمن قانون الأعمال تغيير في القواعد الإجرائية التي تتعلق بإنشاء و تسيير الشركات و المؤسسات ضمن مختلف القوانين ذات الصلة (المطلب الأول) ، و امتد التغيير إلى بعض الآثار المرتبطة بنمط المسؤولية في ظل حلول الذكاء الاصطناعي محل الانسان في معالجة الملفات و المعطيات ذات البعد الاقتصادي (المطلب الثاني).

المطلب الأول:

من حيث الإجراءات المتعلقة بإنشاء المؤسسات وتسييرها

في جانب رقمنة إجراءات إنشاء المؤسسات ، تم تبني أنظمة لرقمنة تقديم ومعالجة هذه الملفات و محاولة لتسهيل الإجراءات و تخفيفها و القضاء على كافة العراقيل التي تقف أمام تحقيق الهدف التنموي، لذلك فقد تم إنشاء " البوابة الالكترونية المخصصة لإنشاء المؤسسات " بموجب المرسوم التنفيذي 23-169

المؤرخ في 24أفريل 2023 و حدد كيفيات تسيير و سيرها[1].تم إنشاء البوابة الالكترونية المخصصة لإنشاء المؤسسات، يتم تسييرها من طرف المركز الوطني للسجل التجاري ، بالتنسيق مع كل من إدارة الضرائب و الصندوق الوطني للضمان الاجتماعي لغير الأجراء (CASNOS) و كذا الصندوق الوطني للضمان الاجتماعي للعمال الأجراء (CANAS) ، فضلاً عن الديوان الوطني للإحصائيات.

تعد البوابة هي الألية الوحيدة لتسجيل المؤسسة بعد مصادقة المركز الوطني للسجل التجاري و التأكيد من الإدارات السالفة الذكر. وظيفة البوابة الالكترونية تمثل الأسلوب الوحيد لدى الإدارة المكلفة بالسجل التجاري ، عليه يلزم المعني بعد تسجيل الطلب بالتنقل و تقديم وثائق ثبوتية ،ثم ترسل الوثائق المطلوبة لإنشاء المؤسسة عبر البريد الالكتروني مرفقة بالاستمارة الالكترونية التي تمثل طلب التسجيل محرر و موقع. حيث يمكن لمصالح المركز الوطني للسجل التجاري التحقق من صحة المعلومات و التعرف على مقدم الطلب عبر السجل الوطني للحالة المدنية.

في حين أنه بعد عملية التسجيل الالكتروني يتلقى مقدم الطلب اشعارًا بذلك عبر البوابة يتضمن الموافقة على طلبه ، و في الجهة المقابلة فيتعين على هذا الأخير أن يرسل ما يلي:

- مستخرج السجل التجاري.

- رقم التعريف الجبائي.

- رقم التعريف الإحصائي.

[1] المرسوم التنفيذي رقم 23 -169، المؤرخ في 24 أفريل 2023، يحدد كيفيات تسيير و سير البوابة الالكترونية المخصصة لإنشاء المؤسسات و كيفيات التسجيل و التحويل و استلام الوثائق الإلكترونية و منح رقم التعريف المشترك ، جريدة رسمية عدد 29 ، المؤرخة في 02 ماي 2023.

- الانتساب لدى الصندوق الوطني للضمان الاجتماعي الخاص بغير الأجراء أو الانتساب للصندوق الوطني للضمان الاجتماعي للعمال الأجراء، إلا أن هذا الانتساب يرتبط بفترة العطلة التي يتحصل عليها طالب إنشاء المؤسسة.

- رقم التعريف المشترك.

بعد انتهاء عملية التسجيل يمنح مقدم الطلب رقم التعريف المشترك الذي يعد مرجع تعريفي له لدى كل من مصالح الضرائب ، الصندوق الوطني للضمان الاجتماعي الخاص بغير الأجراء و الصندوق الوطني للضمان الاجتماعي للعمال الأجراء و الديوان الوطني للإحصائيات.

و في جانب الإجرائي دائما ، فقد اعتمدت عدة قطاعات طرق جديدة لتسييرها و من بينها القطاع الضريبي فقد تم اتخاذ بعض الإجراءات الرامية لرقمنة كل ما يتعلق بسيرورة المؤسسات ، فقد تم إطلاق النظام المعلوماتي الجبائي " جبايتك " وتم إطلاقه بصفة أولية على مستوى ولاية الجزائر [1] . و هذا الإجراء نحو الاعتماد على قواعد فحص ضريبية الكترونية تسعى السلطات الدولة لتعميمها على الشركات والمؤسسات كنظام للمحاسبة و الفوترة الالكترونية [2].

المطلب الثاني:

من حيث الآثار التي يخلفها التحول الرقمي :

سبق الذكر أن التحوّل الرقمي في مجال الأعمال يرتبط بتحديث في كيفيات الانتاج و التسيير وحتى تقديم الخدمات في إطار الحوكمة الرقمية، مما ترتب عنه آثارًا قانونية مرتبطة بالمسؤولية ، إذ تغيرت طبيعة العلاقات بين مختلف الفاعلين

[1] موقع المديرية العامة للضرائب : www .mfdgi.gov.dz ، تاريخ الإطلاع : 2025/10/20.

[2] قوادري محمد : رقمنة النظام الضريبي و دوره في دعم الرقابة الجبائية في الجزائر ، مجلة المنتدى للدراسات و الأبحاث الاقتصادية المجلد 06 ، العدد 02 ، جامعة الجلفة ، الجزائر، 2022 ، ص 239.

الاقتصاديين على اعتبار أن التعامل يتم في بيئة إلكترونية تستخدم أنظمة الرقمنة والذكاء الاصطناعي و بالتالي البحث عن من سيتحمل المسؤولية عند وقوع الضرر بين الشخص الطبيعي أو المعنوي أو حتى الروبوت و تحديد المسؤولية بالنسبة للقرارات الآلية.

كما نجد أن من بين الآثار التي يثيرها التعامل بالرقمنة في قانون الأعمال ، تلك المتعلقة بالتعامل في بيانات شخصية و سبل تأمين الأنظمة المعلوماتية بالنسبة للمؤسسات و مكافحة الاعتداء عليها لاسيما ضد أي احتمال للاختراق أو التسريب [1] ، و منه كل إخلال و تقصير في هذا الجانب قد ينتج عنه مسؤولية لمقدمي الخدمات الرقمية و بالتالي إمكانية المطالبة بالتعويض خاصة في ظل البرمجيات و المنصات الإلكترونية [2].

بناءً على ما سبق، فإن التحوّل الرقمي في قانون الأعمال لم يستبعد قواعد المسؤولية القانونية المكرسة بموجب القواعد العامة ، و إنما دفع لك إلى توسعة في نطاق هذه القواعد مما يفرض ضرورة إعادة صياغتها بما ينسجم مع البيئة الرقمية و يحقق التوازن بين التحفيز على الابتكار و ضمان الحماية القانونية للمعطيات الشخصية و الأطراف المتعاملة.

[1] فرقاق معمر ، بلحمزي فهيمة : البيئة الإلكترونية و الأمن القانوني ، مجلة البحوث في الحقوق و العلوم السياسية ، المجلد 03 ، العدد 02 ، كلية الحقوق و العلوم السياسية ، جامعة تيارت ،الجزائر ، 2017 ، ص 85.

[2] عبد القادر بكر ، طارق جاسم زياد : مسؤولية مزودي خدمات شبكة الأنترنت المدنية عن المحتوى المضلل و المحتوى غير المشروع – دراسة مقارنة ، مجلة الدراسات حول فعلية القاعدة القانونية ، المجلد 04 ، العدد 02 ، كلية الحقوق و العلوم السياسية ، جامعة بجاية ، الجزائر ، 2020 ، ص 186.

الخاتمة:

ختاماً، لما سبق بيانه، يمكن القول أن التحوّل الرقمي في قواعد قانون الأعمال يمثل نقلة نوعية في تطوير البيئة القانونية و الاقتصادية على حد سواء ، فقد أدى إدماج التكنولوجيا في مجالات القانون و المعاملات خاصةً التجارية منها إلى تحسين كفاءة الأداء القانوني و الاقتصادي و تسهيل الإجراءات الإدارية و القضائية و إرساء الشفافية و الحوكمة الرقمية.

إن مظاهر التحول الرقمي في القانون عمومًا و في قانون الأعمال على وجه الخصوص عديدة ، وقد ساهمت في تجسيد أكثر فعالية اقتصادية و سرعة في المعاملات التجارية مما قد يوفر بيئة ملاءمة للاستثمار ، و قد أفرز التحول في هذه القواعد آثارًا قانونية تتعلق بالإجراءات المتبعة ، المسؤولية و الحماية.

من بين أهم النتائج التي توصلنا إليها من خلال هذه الورقة البحثية نذكر :

- التأخر في إصدار النصوص التطبيقية ذات الصلة بقانون الصفقات العمومية الجديد رقم 23-12.

- التحوّل الرقمي في قانون الأعمال لم يستبعد قواعد المسؤولية القانونية المكرسة بموجب القواعد العامة ، و إنما دفع ذلك إلى توسعة في نطاق هذه القواعد

- قصور القواعد التقليدية للعقود المقررة ضمن القانون المدني لتنظيم العقود الإلكترونية و العقود الذكية لاسيما مع خصوصية الأركان و الآثار هذا النوع من العقود.

بناء على ما سلف ذكره، يمكن أن نتوصل إلى المتقرحات التالية :

- ضرورة الإسراع في إصدار النصوص التنظيمية المتعلقة بتطبيق القانون الخاص بالصفقات العمومية الجديد.

- ضرورة إعادة النظر في القواعد المتعلقة بالعقد بما يضمن تأطير العقود الإلكترونية و العقود الذكية لاسيما من حيث خصوصية الأركان و الآثار فيها.

- ضرورة تحديد المسؤولية القانونية بما ينسجم مع البيئة الرقمية و يحقق التوازن بين التحفيز على الابتكار و ضمان الحماية القانونية للمعطيات الشخصية والأطراف المتعاملة ، الأمر الذي يعزز الثقة الرقمية.

قائمة المصادر و المراجع:

1/ نصوص قانونية

أ - قوانين :

1. القانون رقم 15-04 ، المؤرخ في 01 فيفري 2015، المتعلق بالتوقيع والتصديق الإلكترونيين ، ج ر عدد 06، المؤرخة في 10 فبراير 2015.
2. القانون رقم 18- 05، المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية ، ج ر عدد28، المؤرخة في 16 ماي2018.
3. القانون رقم 22-09 ، المؤرخ في 05 ماي 2022 ، يعدل و يتمم الأمر رقم 75-59 ، المؤرخ في 26 سبتمبر 1975 و المتضمن القانون التجاري ج ر عدد 32، المؤرخة في 14 ماي 2022.
4. القانون رقم 23- 09 المؤرخ في 21 يونيو 2023، يتضمن القانون النقدي و المصرفي، ج ر عدد 43، المؤرخة في 27 يونيو 2023.

ب - أوامر:

- الأمر رقم 03-11 المؤرخ في 26 أوت 2003[1]، المتعلق بالنقد والقرض، ج ر عدد 52، المؤرخة في 27 أوت 2003

ج - مراسيم:

1. المرسوم الرئاسي رقم 10-236 ، المؤرخ في 17 أكتوبر 2010 ، المتعلق بتنظيم الصفقات العمومية ، ج ر عدد 58، المؤرخة في 07 أكتوبر 2010. (الملغى)
2. المرسوم التنفيذي رقم 23 -169، المؤرخ في 24 أفريل 2023، يحدد كيفيات تسيير و سير البوابة الالكترونية المخصصة لإنشاء المؤسسات و كيفيات التسجيل و التحويل و استلام الوثائق الإلكترونية و منح رقم التعريف المشترك ، جريدة رسمية عدد 29 ، المؤرخة في 02 ماي 2023.

د - أنظمة :

- النظام رقم 24- 04 المؤرخ في 13 أكتوبر 2024، المتعلق بالشروط الخاصة للترخيص بتأسيس و اعتماد و ممارسة نشاط البنك الرقمي ، ج ر العدد 77، المؤرخة في 19 نوفمبر 2024.

2/ المذكرات

- عبد الله عبد الرحيم محمد مجرشي : دور إدارة التحول الرقمي في تطوير أداء المؤسسات، دراسة ميدانية على مديرية الأحوال المدنية بمدينة تبوك في المملكة العربية السعودية، رسالة ماجستير، جامعة تبوك، المملكة العربية السعودية، 2023.

3/ المقالات:

1. بن جلول محمد ، زعرورة فاطمة : رقمنة الصفقات العمومية في التشريع الجزائري بين الواقع و المأمول على ضوء القانون الجديد 23- 12 مجلة البحوث القانونية و الاقتصادية ، المركز الجامعي أفلو ، المجلد 07 ، العدد 01 ، الجزائر ، 2024.
2. بوعمرة عقبة : رقمنة الإجراءات القضائية و سرعة المحاكمة الجزائية أي علاقة؟، مجلة القانون و العلوم البيئية ، المجلد 03 ، العدد 03 جامعة الجلفة ، الجزائر، 2024.
3. بيصار عبد الحكيم ، بوتيارة عنتر "التحول الرقمي و الحوكمة الرقمية و مقاربات تحقيق التنمية المستدامة" مداخلة مقدمة ضمن فعاليات الملتقي الدولي : التحول الرقمي كآلية لتحقيق التنمية المستدامة بين التشريع الجزائري و التشريعات المقارنة المنعقد بالمركز الجامعي بريكة يوم 07 ماي 2024.
4. - عبد القادر بكر ، طارق جاسم زياد : مسؤولية مزودي خدمات شبكة الأنترنت المدنية عن المحتوى المضلل و المحتوى غير المشروع – دراسة مقارنة ، مجلة

الدراسات حول فعلية القاعدة القانونية المجلد 04 ، العدد 02 ، كلية الحقوق و العلوم السياسية ، جامعة بجاية ، الجزائر ، 2020.

5. فرقاق معمر ، بلحمزي فهيمة : البيئة الإلكترونية و الأمن القانوني ، مجلة البحوث في الحقوق و العلوم السياسية ، المجلد 03 ، العدد 02 ، كلية الحقوق و العلوم السياسية ، جامعة تيارت ،الجزائر ، 2017.

6. - قوادري محمد : رقمنة النظام الضريبي و دوره في دعم الرقابة الجبائية في الجزائر ، مجلة المنتدى للدراسات و الأبحاث الاقتصادية المجلد 06 ، العدد 02 ، جامعة الجلفة ، الجزائر، 2022.

4/ المو اقع الإلكترونية :

- موقع المديرية العامة للضرائب : www .mfdgi.gov.dz.

الذكاء الاصطناعي والأمن السيبراني

Artificial intelligence and cybersecurity

بوعكاز أسماء
جامعة الشاذلي بن جديد الطارف
a.bouakkaz@univ-eltarf.dz
غرايبية خولة
جامعة الشاذلي بن جديد الطارف
drgheraibia.khaoula1992@gmail.com

ملخص:
يعد الذكاء الاصطناعي والأمن السيبراني من أبرز أشكال التطور التكنولوجي الكبير الذي نشهده منذ سنوات، وقد حظي هذان المجالان بانتشار واسع في عالم التكنولوجيا الحديثة نظراً لدورهما الجوهري في صياغة العالم الرقمي ، وحرصت المؤسسات على استخدام أدوات وأنظمة الأمن السيبراني المدعومة بالذكاء الاصطناعي بهدف اكتشاف التهديدات والتعامل معها بفعالية وسرعة أكبر.

الكلمات المفتاحية: الامن السيبراني ؛الفضاء السيبراني ؛الذكاء الاصطناعي ؛الذكاء البشري .

***Abstract**:*
Artificial intelligence (AI) and cybersecurity are among the most significant technological advancements of recent years. These two fields have gained popularity in the modern technology world due to their essential role in shaping the digital world. Organizations are looking to use AI-powered cybersecurity tools and systems to detect and respond to threats more effectively and quickly.

***Keywords:** Cybersecurity **;** cyberspacea**;** rtificial intelligence**;** human intelligence.*

مقدمة:

مع تصاعد الهجمات الإلكترونية التي استهدفت المؤسسات والشركات خلال السنوات الأخيرة، أصبح جليًا أن الأساليب الحالية للأمن السيبراني تشهد ضعفًا مستمرًا في التصدي للتهديدات الرقمية المتنامية، وما زاد الوضع تعقيدًا هو نجاح قراصنة روس في اختراق مجموعة من الوكالات الحكومية الأمريكية مؤخرًا، مما دفع العديد من الخبراء الأمنيين إلى الدعوة لإجراء تحولات جذرية في استراتيجيات كشف ومعالجة التهديدات الإلكترونية .

وتركز هذه الدعوات على استبدال الأساليب التقليدية المعتمدة على قواعد بيانات ثابتة بنماذج ذكاء اصطناعي أكثر تطورًا، تمتاز بمرونتها وقدرتها على تحليل وفهم السلوك الطبيعي وغير الطبيعي للموظفين.

وفي هذا السياق، أشارت رئيسة قسم الأمن في شركة IBM" إلى أن تزايد استخدام الأجهزة المحمولة داخل بيئات العمل، إلى جانب التحول المتزايد نحو تقنيات الحوسبة السحابية، قد أوجد عددًا لا يُحصى من المسارات التي يمكن أن تُستغل لاختراق مساحات العمل الافتراضية، مما ساهم بدوره في زيادة احتمالات التعرض للهجمات الرقمية.

ويُعد الذكاء الاصطناعي أحد الإنجازات البارزة في الثورة الصناعية الرابعة، بالنظر إلى تطبيقاته الواسعة في مختلف مجالات الحياة .فقد استُخدمت هذه التكنولوجيا في الاقتصاد، والصناعة، والخدمات، فضلًا عن القطاعين العسكري والسياسي، حيث أثبتت كفاءتها الكبيرة في العديد من السياقات، إلى جانب ذلك يمثل الذكاء الاصطناعي أداة حيوية لتطوير وتعزيز الأمن السيبراني، ما يمنحه أهمية متزايدة في مواجهة التهديدات الإلكترونية المعقدة.

***الاشكالية محل الدراسة** : مدى فعالية الذكاء الاصطناعي في تعزيز الامن السيبراني ؟

***اهداف البحث :** يهدف هذا البحث الى تحقيق ما يلي :

- التعرف على مفهوم الذكاء الاصطناعي واهم مجالاته .
- الوقوف على تطبيقات الذكاء الاصطناعي في تحسين وتطوير الامن السيبراني .
- تحديد التحديات التي تعترض الذكاء الاصطناعي في الامن السيبراني .

***منهجية الدراسة** : لدراسة هذا الموضوع اعتمدنا المنهج الوصفي من خلال وصف تقنية الذكاء الاصطناعي ومجالاته و المفاهيم المرتبطة بالامن الاصطناعي والدور الذي يلعبه في تطوير الامن السيبراني وتحقيق اهدافه .

المبحث الاول :

الاطار المفاهيمي للذكاء الاصطناعي والامن السيبراني :

شهد العالم في السنوات السابقة تطورا سريعا في مجال التكنولوجيا خصوصا في مجال الامن السيبراني والذكاء الاصطناعي باعتبارهما تقنيات اثرت بشكل كبير في التعامل مع البيانات والمعلومات عبر شبكة الانترنت .

المطلب الاول :

مفهوم الذكاء الاصطناعي

الفرع الاول : تعريف الذكاء الاصطناعي

قبل التطرق لماهية الذكاء الاصطناعي لا بد من الاشارة الى مفهوم الذكاء البشري باعتباره المقدرة والمهارة على وضع ايجاد الحلول للمشكلات باستخدام الرموز وطرق البحث المختلفة للمشكلات والقدرة على استخدام الخبرة المكتسبة في اشتقاق معلومات ومعارف جديدة ، تؤدي الى وضع الحلول لمشاكل ما في مجال معي ويتفاوت الذكاء من شخص الى اخر كما يعتبر الذكاء البشري هو المسؤول عن التطور والابداع في نمو الحضارات المختلفة ونظرا لأهمية الذكاء البشري ، فان الانسان كان ولا يزال دائم البحث عن طبيعة هذا الذكاء وكيف يمكن قياسه ووضع الخطوات المحاكاة اساليبه في شكل برامج باستخدام الحاسبات [1].

اما الذكاء الاصطناعي فيعرف بانه فرع من فروع علم الحاسوب يركز على تصميم تقنيات وادوات متقدمة تعتمد على القدرات الحسابية العالية للحواسيب وتكنولوجيا المعلومات لإنشاء نماذج تتفاعل وتتعلم وتتخذ قرارات بشكل مشابه

[1] : انظر فايز النجار ، نظم المعلومات الادارية ، منظور اداري ، ط4، دار الحامد للنشر والتوزيع ، الاردن، 2010، ص169.

للبشر ، وتشمل فروع الذكاء الاصطناعي تصنيف الصور والاصوات والترجمة الالية وكذلك التخطيط والاستنساخ .[1]

وذهب البعض لتعريفه بانه "احد فروع الكمبيوتر المعنية بكيفية محاكاة الآلات لسلوك البشر فهو علم انشاء اجهزة وبرامج كمبيوتر قادرة على التفكير بالطريقة نفسها التي يعمل لها الدماغ البشري ، تتعلم مثلما نتعلم وتقرر كما نقرر ، وتتصرف ما نتصرف".[2]

وبذلك فهو التقنية التي تبديها الآلات والبرامج بما يحاكي القدرات الذهنية البشرية وانماط عملها ، مثل القدرة على التعلم والاستنتاج ورد الفعل على اوضاع لم تبرمج في الالة ، وهو كذلك اسم لمجال اكاديمي يعنى بكيفية صنع حواسيب وبرامج قادرة على اتخاذ سلوك ذكي[3].

أما مجلس صناعة المعلومات " ITI "فعرفه بانه مجموعة من التقنيات القادرة على التعلم واستخدام المنطق والتكيف واداء المهام بطرق مستوحاة من العقل البشري ، [4] وعرفته منظمة التعاون الاقتصادي نظام الذكاء الاصطناعي دون تعريف الذكاء الاصطناعي بقولها انه نظام قائم على الالة يمكنه لمجموعة معينة من الاهداف التي يحددها الانسان تقديم تنبؤات او توصيات او قرارات تؤثر على

[1] : حسين نايف مبارك الحجرف ، دور الذكاء الاصطناعي في تعزيز الامن السيبراني ، رؤى نظرية ، مجلة الدراسات الجامعية للبحوث الشاملة ، مجلد 32، عدد5 ،2024 ، ص14075.

[2] : احمد ابراهيم محمد ابراهيم ، المسؤولية الجنائية الناتجة عن اخطاء الذكاء الاصطناعي في التشريع الاماراتي – دراسة مقارنة – اطروحة مقدمة للحصول على درجة الدكتوراه ، جامعة عين شمس ، مصر ، السنة الجامعية 2020/2019، ص34.

[3] : عبد الحميد بسيوني ، الذكاء الاصطناعي والوكيل الذكي ،دط، البيطاش سنتر للنشر والتوزيع ، الاسكندرية ، 2005، ص41.

[4] : حسن بن محمد حسن العمري ، الذكاء الاصطناعي ودوره في العلاقات الدولية ، المجلة العربية للنشر العلمي ، عدد23، 2021، ص309

البيئات الحقيقية او الافتراضية وتم تصميم انظمة الذكاء الاصطناعي للعمل بمستويات متفاوتة من الاستقلالية ".[1]

و نجد المشرع المصري قد اصدر ضمن القرار رقم 2889 لسنة 2019 المتعلق بإنشاء مجلس وطني للذكاء الاصطناعي، هذا وعملت الامارات العربية المتحدة على تطوير قوانينها ووضعت العديد من المبادئ بخصوص الذكاء الاصطناعي في اكتوبر 2017، اما المشرع الجزائري فنجده لم يعرف الذكاء الاصطناعي على الرغم من ابداء اهتمامه به و العزم على انشاء مراكز للذكاء الاصطناعي انشاء المدرسة العليا للذكاء الاصطناعي.

وبذلك نخلص للقول ان الذكاء الاصطناعي يهدف الى فهم طبيعة الذكاء الانساني من خلال عمل برامج للحاسب الالي يكون باستطاعتها ان تحاكي السلوك البشري الذي يتميز بالذكاء فهو يشير الى قدرة برنامج الحاسب على حل مسالة ما او اتخاذ قرار في ظرف معين بناء على وصف الموقف ويجد البرنامج الطريقة بنفسه والتي يجب ان يتم اتباعها لإيجاد الحل.[2]

الفرع الثاني: تصنيف الذكاء الاصطناعي

من خلال التعاريف السابق ذكرها يمكن القول ان الذكاء الاصطناعي انواع تتمثل في ما يلي :

- **الذكاء الاصطناعي الضيق :** وهو مستوى برنامج الكمبيوتر الذي يحقق اداء يفوق اداء الانسان في مهمة محددة وضيقة اي يرتبط هذا النوع بتطبيقات وانظمة ذكية للقيام ومعالجة المهام النمطية اليومية والمتكررة

[1] : بن ازواو ليلى ، الذكاء الاصطناعي في مهنة التدقيق : نحو اطار حوكمي للممارسات الاخلاقية ، مجلة المنتدى ، المجلد9، عدد1، 2025، ص31.

[2] : وسيلة سعود ، الذكاء الاصطناعي وتحديات الممارسة الاخلاقية ، مجلة نماء للاقتصاد والتجارة ، مجلد 7، عدد2، ديسمبر 2023، ص4

وتعتبر معظم انظمة الذكاء الاصطناعي الحالية ذكاء اصطناعي ضيقا حيث ينمو عدد هذه البرامج بسرعة بسبب نجاح التعلم الالي والشبكات العصبية وتستخدم السيارات ذاتية القيادة مثلا جيدا للذكاء الاصطناعي الضيق .

- **الذكاء الاصطناعي العام :** وهو الذكاء الاعلى مستوى من الذكاء البشري في العديد من المجالات فعلى سبيل المثال من المحتمل ان يكون هناك تواصل باللغة الطبيعية وفهم سياق معظم المواقف فضلا عن اداء معظم المهام الفكرية التي يستطيع البشر القيام بها ، كما ان القدرة على تحسين الذات هي نتيجة واضحة لهذا المستوى من تطوير الذكاء الاصطناعي ونتيجة لذلك ووفقا" **لنيك بوستروم** "فإن عصر الذكاء الاصطناعي على مستوى الانسان سيكون قصيرا حيث سيتطور الذكاء الاصطناعي العام مع قدرات تحسين الذات الى ذكاء خارق قريبا .
- **الذكاء الاصطناعي الفائق :** وهو حالة افتراضية في المستقبل ويمثل المستوى الذي يستفوق فيه الذكاء الاصطناعي على البشر في جميع الجوانب ويتفوق على ذكاء الحضارة الانسانية بأكملها ، اذ سيكون قادرات على اجراء الاكتشافات العلمية وانشاء محاكاة دقيقة للماضي البشري.[1]

الفرع الثالث: مجالات الذكاء الاصطناعي :

يمكننا القول ان الذكاء الاصطناعي له العديد من التطبيقات في مختلف المجالات فنجد انها تستخدم في القطاعات العسكرية والمالية والخدمية والصناعية كما يمكن استخدامها في مجال التعليم من خلال المنصات التعليمية والتطبيقات الرقمية المبرمجة كما يقدم الذكاء الاصطناعي العديد من المزايا ففي مجال الطب يمكن ان يساعد الذكاء الاصطناعي الاطباء في تشخيص الامراض وتوجيه العلاج

[1] : انظر حسن بن محمد حسن العمري ،المرجع السابق ، ص310

بشكل اكثر دقة وفي مجال التصنيع يمكن للذكاء الاصطناعي تحسين عمليات الانتاج وزيادة الكفاءة حيث يمكن للروبوتات المجهزة بتقنيات الذكاء الاصطناعي اداء المهام الروتينية بدقة عالية وسرعة عالية ومع ذلك يواجه الذكاء الاصطناعي ايضا بعض التحديات والقيود في بعض المجالات التي تتطلب التفكير الابداعي والحدس البشري.

ومسالة الخوض في تحديد مجالات الذكاء الاصطناعي تتحدد بتحديد انواعه بالنظر لمجال تطبيقه او التخصص وتشمل ما يلي :

1-انواع الذكاء الاصطناعي وفقا لمجال التطبيق :

* **تعلم الالة** : يقصد به العلم الذي يمكن الالة من اكتساب القدرة على ترجمة وتنفيذ والتحقق من البيانات عن طريق خوارزميات مطورة بقدرات رياضية معقدة ثم ترميزها الى لغة تستطيع الالة فهمها وذلك من اجل مساعدة الانسان على حل بعض المشكلات التي تواجهه .

* **الشبكة العصبية** : يتم في اطارها دمج العلوم الادراكية والآلات وذلك من اجل تأدية مهام محددة بناءا وانطلاقا من محاكاة الية وطريقة عمل الجهاز العصبي للمخ ، فهي تشير الى نوع ونمط من تطبيقات الذكاء الاصطناعي التي تيم فيها الدمج بين كل من علم الاعصاب والذكاء الاصطناعي للآلة سعيا الى ايجاد الحلول للقيام ببعض المهام التي تتميز بالتعقيد .

* **الروبوتات** : تعتمد وتقوم هذه التطبيقات على الدمج ما بين العديد من التخصصات منها العلوم ، الهندسة الميكانيكية ، الهندسة الكهربائية ، علوم الحاسب الالي، وغيرها من العلوم والتخصصات .

***البرمجة اللغوية العصبية** : تتعلق بتطوير اساليب متقدمة تتيح عملية تواصل وتعامل الآلات مع مختلف اللغات البشرية بسهولة كاللغة الانجليزية بما فيها الترجمة والتعرف على فهم النصوص المتنوعة والتمكن من تحليل محتواها وفهمه .[1]

2- مجالات الذكاء الاصطناعي بالنظر للتخصص :

- **في الرعاية الصحية :** يعمل الذكاء الاصطناعي في تحسين نتائج المرضى وتقليص التكاليف ، اذ يستعمل التعلم الالي من اجل اجراء التشخيصات بشكل افضل واسرع مما يقوم به البشر فيستخرج النظام بيانات المرضى ومصادر البيانات الاخرى المتاحة لتشكيل فرضية وفقا لذلك وتشتمل على استخدام مساعدين صحيين افتراضيين عن طريق الانترنت وتستخدم روبوتات الدردشة لمساعدة المرضى وعملاء الرعاية الصحية من خلال تقديم وتوفير المعلومات الطبية التي يحتاجونها وجدولة المواعيد اضافة الى القيام بعمليات الفوترة واستكمال العمليات الادارية الروتينية الاخرى، كما يتم استخدام الذكاء الاصطناعي في التنبؤ بالأوبئة وفهمها ومكافحتها.

- **في التعليم والترجمة:** يتم من خلال الذكاء الاصطناعي تقييم الطلاب والتكيف مع احتياجاتهم ومساعدتهم في العمل بناء على سرعتهم الخاصة ما يتيح امكانية تقديم دعم اضافي للطلاب كما يساهم الذكاء الاصطناعي في تعزيز اساليب التجربة وتقليص ونسبة الخطأ فيها اين تقوم كبريات الشركات في العامل باستخدام هذه التطبيقات من اجل تقديم خدمات ترجمة فورية وصحيحة وامنة خلافا لما كانت تواجهه من قبل من صعوبات في ايصال الترجمة الصحيحة .

- **في ريادة الاعمال:** يتم استخدامه في دمج الخوارزميات الخاصة بالتعلم الالي ففي الانظمة الاساسية للتحليلات وفي انظمة ادارة علاقات العملاء

[1] : وسيلة سعود ، المرجع السابق ، ص5.

وهو ما يسمح بالتعرف وتحديد المعلومات اللازمة عن افضل طريقة لخدمة العملاء كما تم ايضا في هذا المجال دمج روبوتات الدردشة في العديد من مواقع الويب للشركات المختلفة والذي يسمح بتقديم خدمة فورية للعملاء مع انتشار اتمتة العديد من المناصب الوظيفية .

- **في العمليات القانونية :** يساعد الذكاء الاصطناعي على اتمتة العمليات القانونية بما يوفر الوقت ويحسن الخدمات المقدمة كما تلجا شركات المحاماة الى تقنيات التعلم الالي من اجل وصف البيانات والتنبؤ بالنتائج وتصنيف واستخراج المعلومات من الوثائق من طرف الكمبيوتر وغيرها .

- **في العمليات البنكية :** يتم توظيف روبوتات المحادثة من قبل البنوك لتوعية عملاءها بالخدمات والعروض المقدمة وللقيام بالمعاملات التي لا تستلزم تدخلا بشريا كما يتم ايضا الاستعانة بالمساعدين الافتراضيين من اجل تحسين وتخفيض تكاليف الامتثال للوائح المصرفية وكذا يستخدم الذكاء الاصطناعي في تحسين اتخاذ القرارات بخصوص القروض وحدود الائتمان وفرص الاستثمار .[1]

- **في العمليات العسكرية :** يمكن استخدام هذه التقنيات في الطائرات بدون طيار وغيرها من الاسلحة التي تؤدي الى الدمار ولكن تكمن المشكلة ان تطوير مثل هذه التقنيات اصبح سهلا ومتوفرا وقد ينتج عنه توفرها في ايد غير مضمونة في اماكن مختلقة في العالم حيث لا توجد اتفاقيات دولية تحد من هذه التقنية مما يشكل خطرا على المدنيين وعلى الدول ، وقد

[1] : وسيلة سعود ، المرجع السابق ص8.

اشار البعض ان العلماء في شركة قوقل قد وقعوا اتفاقية تمنع استخدام الذكاء الاصطناعي لاغراض عسكرية.[1]

المطلب الثاني

مفهوم الامن السيبراني و ابعاده :

يشير مصطلح الامن السيبراني الى الممارسات والادوات والتقنيات التي تهدف الى حماية الانظمة والشبكات والبيانات من التهديدات السيبرانية وللوقوف على تحديد مفهوم الامن السيبراني لا بد من تعريفه، وتعريف المصطلحات التي ترافقه خصوصا منها الفضاء السيبراني والجريمة السيبرانية .

الفرع الأول: مفهوم الامن السيبراني :

-أ- تعريف الامن السيبراني :

لفظة cyber هي كلمة يونانية تعني الشخص الذي يدير دفة السفينة وهناك من يرجع اصل اللفظة الى منتصف القرن 20 مع عالم الرياضيات الامريكي wieners narbert الذي استخدمها للتعبير عن التحكم الالي ، حيث عرف السيبرنيتيقية على انها " التجكم والتواصل عند الحيوان والالة "، وذكر في الكتاب ذاته انها " علم نقل الرسائل بين الانسان والالة او بين الالة والالة "، ومن هنا تبلورت السيبرانية وتم توظيفها للتعبير عن العمليات الالية والعلاقات بين الاجهزة الإلكترونية والانسان .

وبذلك فالأمن السيبراني هو النشاط الذي يضمن حماية الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات ويضمن القدرة على التعافي من

[1] : اضاءات ، الذكاء الاصطناعي ، منشرة توعوية يصدرها معهد الدراسات المصرفية ، الكويت مارس2021، سلسلة 13، عدد4، ص10

الخسائر والاضرار الناتجة عن مخاطر وتهديدات محتملة مما يسمح بإعادة الوضع الطبيعي في اسرع وقت ممكن .[1]

وذهب البعض للقول بانه الوسائل التي من شانها الحد من خطر الهجوم على البرمجيات او اجهزة الحاسوب او الشبكات ومنها الوسائل المستخدمة في مواجهة القرصنة وكشف الفيروسات .[2]

وبالرجوع لأهدافه يمكن تعريفه بانه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن امكانات الحد من الخسائر والاضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح اعادة الوضع الى ما كان عليه باسرع وقت ممكن ، بحيث لا تتوقف عجلة الانتاج وبحيث لا تتحول الاضرار الى خسائر دائمة .[3]

و يعد كذلك مجالا يهتم بحماية الانظمة الحاسوبية والشبكات والمعلومات الرقمية من التهديدات الالكترونية والهجمات السيبرانية، وذلك بتامين البيانات ومنع كشف واستجابة للانتهاكات الامنية والهجمات الالكترونية التي تستهدف الافراد والمؤسسات ويتضمن هذا المجال تحليل المخاطر وتصميم وتنفيذ اجراءات الامان الضرورية لحماية البيانات والشبكات والتعامل الفعال مع حوادث الامن والتحقيق فيها للتعلم والتحسين المستمر .[4]

هذا وذهب البعض للقول بانه مجموع الاجراءات الواجب اتخاذها من قبل الاجهزة الامنية او الاخرى غيرها ذات العلاقة للمحافظة على سرية المعلومات

[1] : حسين نايف مبارك الحجرف ، دور الذكاء الاصطناعي في تعزيز الامن السيبراني ، رؤ نظرية ، مجلة الدراسات الجامعية للبحوث الشاملة ، مجلد 32، عدد5 ،2024 ص1081.

[2] : amoroso,e,g ,cyber security.(s,press,ed,2007) ,p1

[3] : بارة سمير ، الامن السيبراني في الجزائر السياسات والمؤسسات ، المجلة الجزائرية للامن الانساني ، عدد4، جويلية 2017.ص257.

[4] : حسين نايف مبارك الحجرف ،المرجع السابق ، ص14075.

الالكترونية ومنع الاختراقات الفيروسية من اجل ضمان وصول المعلومات الحاسوبية الى الجهات المختصة في الوقت المناسب وضمان عدم وقوعها في ايدي الاعداء او الاصدقاء على حد سواء خصوصا بعد الثورة الهائلة في عالم الاتصالات والتداولات الالكترونية حيث شكل هذا النوع من الامن هاجسا استراتيجيا للقوى العالمية والمتمثلة في الولايات المتحدة الامريكية والصين وروسيا اذ تدور في وقتنا الخالي حرب الكترونية بين هذه القوى من اجل اختراق المعلومات والتأثير على اسعار البورصة والعملات وغيرها من المنشأة .[1]

وفي هذا الشأن قدمت وزارة الدفاع الامريكية تعريفا دقيقا لمصطلح الامن السيبراني بأنه " جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها الاكترونية والمادية من مختلف الجرائم والهجمات والتخريب والتجسس والحوادث .[2]

-ب- **الفضاء السيبراني :** يعرف بانه المنطقة العالمية داخل بيئة المعلومات التي تتكون من شبكات مترابطة من البنية التحتية للبيانات وتكنولوجيا المعلومات مثل الانترنت وشبكات الاتصالات والحوسبة والمعالجة والتحكم ، وتخدم شبكات المعلومات حوسبة عالم الفضاء السيبراني .

وشبكات المعلومات هي حجم رقمي للمعلومات التي لا تعتمد كليا على البيئة التي تم انشاؤها فيها ولكن مفرداتها تغطي مجموعة واسعة من المعالجات بالإضافة

[1] : علي زياد علي ، الصراع والامن الجيوسيبراني في الساحة الدولية – دراسة في استراتيجيات الاشتباك الرقمي ،دط، دار امجد للنشر والتوزيع ، عمان ، ص56.

[2] :خالد ظاهر المطيري ، دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي ، مجلة البحوث الفقهية والقانونية ، عدد 38،2022، ص996.

الى سرعات نقل البيانات والوصول الى الشبكة وما الى ذلك وبيئة الفضاء الالكتروني تتعامل مع البيانات اثناء تدفقها.[1]

وبذلك فالفضاء السيبراني هو بيئة انسانية وتكنولوجية جديدة للتعبير والمعلومات والتبادل ، وهو يشمل المعلومات المتوفرة الكترونيا والتي يتم تبادلها وتشكيلها في مجموعات بناء على استخدامها ويعمل الفضاء الالكتروني تحت ظروف مادية غير تقليدية حيث يكون وسيطا عبر العمل من خلال اجهزة الكمبيوتر وشبكات الاتصال .[2]

-ج- **الجريمة السيبرانية :** هي الجرائم التي ترتكب ضد الافراد او مجموعات من الافراد بدافع الجريمة وبقصد ايذاء سمعة الضحية او الحاق اي اذى مادي او عقلي للضحية سواء كان بشكل مباشر او غير مباشر باستخدام شبكات الاتصالات كالانترنت وغرفة الدردشة والبريد الالكترونية ،

فهي الجريمة التي تعبر عن كل سلوك غير مشروع او غير اخلاقي او غير مصرح به يتعلق بالمعالجة الالية للبيانات او نقلها .[3]

وتشكل الجرائم الالكترونية تحدي كبير للبيئة التي تركب فيها اذ يمكن لمجرمي الانترت العمل من اي مكان في العالم واستهداف اعداد كبيرة من الناس او الشركات عبر الحدود الدولية وتزداد التحديات التي تفرضها استنادا الى نطاق وحجم الجرائم والتعقيد التقني لتحديد هوية الجناة وكذلك ضرورة العمل على الصعيد الدولي

[1] : عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني ، مكتبة الاسكندرية وحدة الدراسات المستقبلية ، الاسكندرية ، 2016، ص11

[2] : قاسيمي صافية ، الفضاء السيبراني والاغوار الالكترونية اشكالية خلق فضاء الكتروني افتراضي حسب المنظور الهابر ماسي ، مجلة الحكمة للدراسات الفلسفية ، الجزائر ،عدد7، 2016، ص67.

[3] : ذياب البداينة ، الجريمة الافتراضية ، ورقة مقدمة في الملتقى الدولي التنظيم القانوني للأنترنت والجريمة الالكترونية جامعة عاشور زيان الجلفة ، الجزائر ، 2009، ص5

لتقديمهم الى العدالة، فالانترنت تفتح فرصا جديدة لمجرميها على اساس الاعتقاد بان انفاذ القانون لا يعمل في عالم الانترنت .

الفرع الثاني -عناصر الامن السبراني

لتحقيق الامن السيبراني تحتاج الدولة الى تنسيق جهودها في جميع انحاء نظام المعلومات الخاص بها وتشمل هذه الجهود عناصر الامن السيبراني المتمثلة في ما يلي :

- أمن الشبكة : وهي اجراءات تستخدمها الشركات والافراد لحماية شبكة المؤسسات من الاختراق
- أمن التطبيقات : وهي وضع تدابير لحماية البرامج من الفيروسات الضارة وعدم سرقة المعلومات السرية
- امن المعلومات : وهي عبارة عن الضوابط التي تضمن خصوصية المعلومات وحمايتها والوصول بسهولة لها عند الحاجة سواء نقلها او تخزينها
- الامن التشغيلي : وهي عمليات لحماية المعلومات ومعالجتها وتخزين البيانات
- التعافي من الكوارث : مجموعة خطوات تستخدمها الشركات للحد من التهديدات او فقدان المعلومات
- استمرارية العمل : خطة تتبعها الشركات لمواصلة العمل اثناء خرق المعلومات رغم الموارد المتاثرة .

الفرع الثالث- ابعاد الامن السيبراني

أ-البعد العسكري : يهدف الى الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية مما يتيح تبادل وتدفق المعلومات والاوامر وانها فكرة لانشاء ونشر شبكة للانترنت والاهداف البعيدة ولكنها ايضا نقطة ضعف خاصة اذا كانت غير امنة ، ويمكن ان يؤدي قواعد البيانات العسكرية او المساومة عليها الى تعطيل الاتصالات بين وحدات القيادة والوحدات العسكرية فضلا عن امكانية التحكم وفقدان السيطرة على بعض الاسلحة مثل الطائرات بدون طيار والصواريخ الموجهة والاقمار الصناعية.

وتسهم تكنولوجيا الاعلام والاتصال في تقديم ابحاث تخدم القدرات العسكرية وتطورها والانجازات العلمي التي تسهم في تفوق بلد على اخر حيث كان اهمها تطوير الاسلحة النووية وفي هذا الشان وجه خبراء امريكيون خطابا مفتوحا للرئيس الامريكية جورج بوس في سنة 2007 محذرين اياه من خطر الهجمات السيبرانية على البنية التحتية الامريكية التي تضم الى الدفاع امدادات الطاقة الكهربائية والمياه والاتصالات السلكية واللاسلكية والخدمات الصحية والنقل والانترنت.[1]

ب-البعد الاقتصادي : نظرا لاستخدام اجهزة الكمبيوتر لتشغيل الصناعات وتنميتها ودفع الاقتصاد ستصبح الانترنت اساس التجارة والتمويل والمعاملات المالية وكلها مرتبطة ببعضها البعض من خلال شبكات الكمبيوتر لتحقيق الامن السيبراني خصوصا ما تعلق بالقطاع المالي ،و اصبح الفضاء الالكتروني جاذبا لقطاعات المجتمع كافة وباتت المعرفة محرك الانتاج والنمو الاقتصادي كما ايقن الجميع ان مبدا التركيز على المعلومات و التكنولوجيا ي عد عاملا من العوامل الاساسية للنهوض بالاقتصاد وهو ما دفع بالدول في الاونة الاخير الى زيادة استثمارها في المعرفة

[1] :منى الاشقر ، الامن السيبراني التحديات ومستلزمات المواجهة اللقاء السنوي الاول للمختصين في امن وسلامة الفضاء السيبراني ، بيروت ، 28/27 اغسطس 2012 ، القاهرة جامعة الدول العربية ، المركز العربي للبحوث القانونية والقضائية ، ص15.

واصبحت عصرنة الاقتصاد مرتبطة بالتحكم في الاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين كما ان استخدام الحاسوب وشبكة الانترنت في تطوير الصناعات وتحريك الاقتصاد ومعالجة كل المعاملات الاقتصادية والمالية زاد من اهمية ضرورة توفير الامن السيبراني لضمان حماية هذه المعلومات .

ج-**البعد السياسي:** بعيدا عن تسريبات الوثائق السرية والامتيازات التي غالبا ما تؤدي الى ازمات دبلوماسية بين الدول فان التدخل السيبراني لروسيا في الانتخابات الامريكية هو اهم دليل على الحاجة الى الامن السيبراني واهميته في البعد السياسي.

د-**البعد القانوني:** يتطلب التطور التكنولوجي السريع الامتثال للقوانين القانونية من خلال تطوير الاطر والقوانين للأنشطة القانونية وغير القانونية في الفضاء السيبراني وان الجرائم الإلكترونية هي في الغالب جرائم سيبرانية وبعض البلدان ليس لها اطار قانوني صارم للتعامل معها .[1]

هـ-**البعد الاجتماعي:** ينبغي التشديد على واجب الامن والمسؤولية الفردية والتدابير الرادعة وكذلك التداعيات المحتملة في اطار القانون الجنائي التي تترتب على عدم احترام الالتزامات التي يوجبها الامن وبصورة اكثر عمومية وليس فقط على الامن والتدابير الرادعة اذ يجب للثقافة الامنية ان تغرس داخل ثقافة تكنولوجيا المعلومات .[2]

[1] : محمد دحماني ، الذكاء الاصطناعي كالية لتعزيز الامن السيبراني ، مجلة الفكر القانوني والسياسي ، المجلد7، عدد2، 2023، ص605 ،ص606.

[2] : الاتحاد الاوروبي للاتصالات ، دليل الامن السيبراني للبلدان النامية ، جنيف ، الاتحاد الدولي للاتصالات ،2006، ص16.17.

المبحث الثاني :

الذكاء الاصطناعي وعلاقته بالامن السيبراني

يوفر العنصر الرقمي مزايا وفرص كبيرة لمواجهة التحديات الامنية السيبراني، الا انه في نفس الوقت يفتح بابا ايضا للاعتداءات وظهور مخاطر امنية جديدة تواجه كل من الافراد والشركات والمؤسسات في ظل التهديدات الاجرامية الالكترونية الامر الذي يستدعي توظيف التقنيات الحديثة خصوصا منها الذكاء الاصطناعي لحماية الانظمة والبيانات الرقمية .

المطلب الأول:

تطبيقات الذكاء الاصطناعي في الامن السيبراني

تتجسد تطبيقات الذكاء الاصطناعي في تحقيق متطلبات الامن السيبراني في ما يلي :

* **توفير البيانات** : يعد الذكاء الاصطناعي الخيار الافضل لاكتشاف التهديدات التي قد تهدد امن وسلامة المجتمع من خلال مراقبة البيانات التي تتم بين العملاء والمنشات ومراقبة حركة المرور تلقائيا وتحليل نشاط الخادم بدقة وتحديد المخاطر المحتملة في حركة مرور البيانات .

***توفير الوقت** : يمكن للذكاء الاصطناعي فحص كميات كبيرة من البيانات في وقت واحد لاكتشاف التهديدات السيبرانية وبالتالي تسهيل الامن ، وافادت التقارير ان 56 بالمئة من المؤسسات انها غارقة في ملف تعريف التهديد الذي يواجه المحللين السيبرانيين وان ما يقارب 23 بالمئة منهم بانهم غير قادرين على التحقق بشكل فعال من التهديدات المحددة .

***توقع التهديدات المستقبلية** : ان كمية البيانات التي تمر عبر محللي الامن السيبراني تجعل من الصعب التنبؤ بالتهديدات المستقبلية لكن الذكاء الاصطناعي يمنع معالجة كميات كبيرة من البيانات في وقت واحد مما يتيح الكشف المبكر عن الانشطة الضارة ويمكن ان يؤدي تحديد الاجراءات الوقائية والتهديدات المحتملة الى تقليل الوقت الضائع واداء الموظفين ويساعد على البقاء يقظا من خلال اتخاذ خطوات لحماية المؤسسة.[1]

***تحليل البيانات** : يستخدم الذكاء الاصطناعي تقنيات التعلم العميق والتحليل المتقدم لفهم البيانات السيبرانية وتحديد الانماط والانحرافات التي قد تشير الى هجمات .

***تحسين الامن الشبكي والمعلوماتي** : يمكن للذكاء الاصطناعي تحسين تصنيف البيانات وتشفيرها ورصد تسريبات البيانات وتعزيز الامان الشبكي بشكل عام .

المطلب الثاني:

تحديات الذكاء الاصطناعي في الامن السيبراني

على الرغم من ان دمج الذكاء الاصطناعي في الامن السيبراني امر ضروري الا ان العوائق الرئيسية التي تحول دون اعتماده ونموه هي احتياجات اكتساب المواهب وتعقيد البيانات واستخدام ادوات الذكاء الاصطناعي المناسبة ، اذ انه وبالرجوع لتقرير شركة IBM بانه هذا العائق يبطئ تبني الذكاء الاصطناعي وتطويره حيث تكافح حوالي37 بالمئة من المؤسسات للعثور على اشخاص يتمتعون بالمستوى المناسب من الخبرة والمعرفة في هذا المجال فان تطوير الذكاء يؤدي الى نقص

[1] : محمد دحماني ، المرجع السابق ، ص605.

اصطناعي في الانسان وهو امر مهم جدا للمؤسسات التي بدات في تطوير الذكاء الاصطناعي .

ويزيد استخدام الذكاء الاصطناعي في هذه التقنية من دقة وفعالية الهجمات مما يخلق تهديدات مدمرة ويمكن ايضا استخدام الذكاء الاصطناعي في هجمات التصيد الاحتيالي .

هذا و تلتزم المنظمات التي تدمج الذكاء الاصطناعي في انظمة الامن السيبراني الخاصة بها بلوائح محددة وغالبا ما تحد من نطاق استخدامها ومن ناحية اخرى يتمتع مجرمو الانترنت بملعب لا حدود له مما يسهل عليهم استغلال التكنولوجيا .[1]

واهم التحديات التي تعيق الذكاء الاصطناعي في تحقيق الامن السيبراني تتمثل في:

***الخصوصية وحماية البيانات :** يعتمد الذكاء الاصطناعي على كميات هائلة من البيانات الشخصية لتحليلها وتقديم التوقعات او التوصيات ويمكن ان يؤدي هذا الى انتهاك خصوصية الافراد اذا تم جمع البيانات واستخدامها دون موافقتهم وعليه وجب ضمان حماية البيانات الشخصية من سوء الاستخدام او التعرض للهجمات السيبرانية ، ووضع قوانين صارمة لضمان الامتثال.[2]

***الشفافية والمساءلة :** تعتمد معظم خوارزميات الذكاء الاصطناعي على تقنيات معقدة تجعل من الصعب على المستخدمين العاديين فهم كيفية اتخاذ القرارات وهذا يؤدي الى تحدي في تحديد المسؤولية اذا حدث خطا او كان هناك قرار غير عادل حيث تظهر الحاجة الى الذكاء الاصطناعي القابل للتفسير الذي يسمح بفهم الية اتخاذ القرارات وتحديد الجهات المسؤولة عند حدوث الخطا .

[1] : محمد دحماني ، المرجع السابق ، ص606.

[2] : رضوان بن صاري، تطبيقات الذكاء الاصطناعي في مجال القانون ، مجلة دفاتر السياسة والقانون ، مجلد 17، عدد 1، 2025، ص30

***التاثير على العلاقات الاجتماعية :** يؤدي استخدام الذكاء الاصطناعي في الحياة اليومية الى تغيير طبيعة التفاعل البشري ويمكن للناس الاعتماد بشكل مفرط على التكنولوجيا مما يؤدي الى صعوبة الحفاظ على التواصل البشري والاجتماعي وتجنب الانعزال الناتج عن الاعتماد على التكنولوجيا في العلاقات .[1]

***استخدام الذكاء الاصطناعي في تطبيق القانون :** يمكن ان يؤدي استخدام الذكاء الاصطناعي في تطبيق القانون ان يؤدي الى مشكلات تتعلق بالخصوصية والتمييز ومثال ذلك انظمة التعرف على الوجوه قد تكون غير دقيقة وتستهدف فئات معينة بشكل غير عادل ، وعليه وجب ضمان ان يكون استخدام الذكاء الاصطناعي في تطبيق القانون متوافقا مع مبادئ حقوق الانسان ولا يؤدي الى انتهاك الخصوصية او التمييز .[2]

المطلب الثاني:

الافاق المستقبلية للذكاء الاصطناعي في مجال الامن السيبراني

الفرع الأول: استخدامات محتملة للذكاء الاصطناعي في تعزيز الامن السيبراني

مع التقدم المتسارع للتكنولوجيا يزداد التهديد السيبراني بشكل مستمر ولذلك فان استخدام الذكاء الاصطناعي في مجال الامن السيبراني ينعكس على العديد من الفوائد والاستخدامات المحتملة واستخدامات الذكاء الاصطناعي في تعزيز الامن السيبراني يمكن ان يكزن له تاثير كبير في مجالات عدة منها " اكتشاف

[1] : معتز ابو زيد ، الذكاء الاصطناعي بين القانون والاخلاق (تنظيم اخلاقيات استخدام الذكاء الاصطناعي) ، مجلة العلوم القانونية والاقتصادية ، كلية الحقوق جامعة عين شمس ، المجلد 66، عدد3، 2023، ص965.

[2] : رضوان بن صاري، تطبيقات الذكاء الاصطناعي في مجال القانون ، مجلة دفاتر السياسة والقانون ، مجلد 17، عدد 1، 2025، ص31.

منع التهديدات ، الاستجابة الفورية للهجمات ، تحليل سلوك المستخدمين ، التشخيص التلقائي للثغرات ".

الفرع الثاني- تطوير التقنيات المستقبلية للذكاء الاصطناعي في مجال الامن السيبراني

مع استمرار التطور التكنولوجي تزداد ايضا امكانيات الذكاء الاصطناعي في مجال الامن السيبراني خصوصا منها ما يتعلق به " تعلم الالة المعزز ، التحليل التنبؤي والتصنيف التلقائي ، الشبكات العصبية العميقة، التفكير الذاتي واتخاذ القرارت".[1]

الخاتمة

وفي الختام، يمكننا القول بأن الذكاء الاصطناعي يمثل خطوة نوعية وبارزة في مجال تكنولوجيا الإعلام والاتصال، حيث يوفر فوائد كبيرة وتطبيقات واسعة النطاق .ومع ذلك، فإن الاستخدام المسؤول لهذه التكنولوجيا يظل ضرورة ملحة،

[1] : انظر محمد جمعه محمد السيد، الذكاء الاصطناعي وتكنولوجيا الامن السيبراني ، مقال متاح على الموقع الالكتروني التالي :
https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.bsu.edu.eg/Backend/Uploads/PDF/Conference/%25D8%25A7%25D9%2584%25D8%25B0%25D9%2583%25D8%25A7%25D8%25A1%2520%25D8%25A7%25D9%2584%25D8%25A5%25D8%25B5%25D8%25B7%25D9%2586%25D8%25A7%25D8%25B9%25D9%258A%2520%25D9%2588%25D8%25AA%25D9%2583%25D9%2586%25D9%2588%25D9%2584%25D9%2588%25D8%25AC%25D9%258A%25D8%25A7%2520%25D8%25A7%25D9%2584%25D8%25A3%25D9%2585%25D9%2586%2520%25D8%25A7%25D9%2584%25D8%25B3%25D9%258A%25D8%25A8%25D8%25B1%25D8%25A7%25D9%2586%25D9%258A.pdf&ved=2ahUKEwij1MzWmbiQAxXShv0HHeSOAbkQFnoECCIQAQ&usg=AOvVaw0DjW5qpMwtto3z8qfXeS0v ، تم الاطلاع بتاريخ 2025/6/10 على الساعة 22.25، ص8

ويتطلب الالتزام بالقوانين والتشريعات المنظمة بالإضافة إلى مراعاة الأبعاد الأخلاقية اذ ينبغي تخصيص جهود واضحة لحماية الخصوصية الفردية وتجنب الآثار السلبية المحتملة الناتجة عن توظيف التكنولوجيا الحديثة، وذلك بهدف جعل الذكاء الاصطناعي أداة فعّالة لتعزيز أمن المعلومات والحماية السيبرانية.

وفي سبيل تحقيق توازن مستدام بين التطور التكنولوجي وأهمية القيم الإنسانية، هناك حاجة لتناول أعمق للموضوعات المرتبطة بالذكاء الاصطناعي وأمن المعلومات، كما يجب تسخير الإمكانات التي تقدمها هذه التقنيات لحماية البيانات الشخصية للمستخدمين وضمان أمانها في ظل التحول الرقمي المتسارع.

التوصيات المقدمة :

*على المؤسسات والمنظمات الاستثمار في تحسين البنية التحتية السيبرانية لتمكين تطبيق التقنيات المتقدمة خصوصا منها الذكاء الاصطناعي .

*تشجيع الوصول الى البيانات بشكل اكثر للباحثين دون المساس بالخصوصية الشخصية للمستخدمين باعتماد تقنيات الذكاء الاصطناعي .

* تعزيز انظمة التشفير للبيانات بأحدث الوسائل الوسائل وتوعية المتعاملين بتطبيقات الذكاء الاصطناعي بأخذ الحيطة والحذر عند التعامل الالكتروني.

قائمة المصادر و المراجع:

1. -عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني ، مكتبة الاسكندرية وحدة الدراسات المستقبلية ، الاسكندرية ، 2016،
2. -عبد الحميد بسيوني ، الذكاء الاصطناعي والوكيل الذكي ،دط، البيطاش سنتر للنشر والتوزيع ، الاسكندرية ، 2005،
3. -علي زياد علي ، الصراع والامن الجيوسيبراني في الساحة الدولية – دراسة في استراتيجيات الاشتباك الرقمي ،دط، دار امجد للنشر والتوزيع ، عمان ،
4. -فايز النجار ، نظم المعلومات الادارية ، منظور اداري ، ط4، دار الحامد للنشر والتوزيع ، الاردن، 2010،
5. -منى الاشقر ، الامن السيبراني التحديات ومستلزمات المواجهة اللقاء السنوي الاول للمختصين في امن وسلامة الفضاء السيبراني ، بيروت ، 28/27 اغسطس 2012 ، القاهرة جامعة الدول العربية ، المركز العربي للبحوث القانونية والقضائية ،
6. -بارة سمير ، الامن السيبراني في الجزائر السياسات والمؤسسات ، المجلة الجزائرية للامن الانساني ، عدد4، جويلية 2017.
7. -بن ازواو ليلى ، الذكاء الاصطناعي في مهنة التدقيق : نحو اطار حوكمي للممارسات الاخلاقية ، مجلة المنتدى ، المجلد9، عدد1، 2025،
8. -حسن بن محمد حسن العمري ، الذكاء الاصطناعي ودوره في العلاقات الدولية ، المجلة العربية للنشر العلمي ، عدد23، 2021،
9. -حسين نايف مبارك الحجرف ، دور الذكاء الاصطناعي في تعزيز الامن السيبراني ، رؤى نظرية ، مجلة الدراسات الجامعية للبحوث الشاملة ، مجلد 32، عدد5 ،2024.
10. -خالد ظاهر المطيري ، دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي ، مجلة البحوث الفقهية والقانونية ، عدد 2022،38،
11. -رضوان بن صاري، تطبيقات الذكاء الاصطناعي في مجال القانون ، مجلة دفاتر السياسة والقانون ، مجلد 17، عدد 1، 2025.

12. -رضوان بن صاري، تطبيقات الذكاء الاصطناعي في مجال القانون ، مجلة دفاتر السياسة والقانون ، مجلد 17، عدد 1، 2025،
13. -قاسيمي صافية ، الفضاء السيبراني والاغوار الالكترونية اشكالية خلق فضاء الكتروني افتراضي حسب المنظور الهابر ماسي ، مجلة الحكمة للدراسات الفلسفية ، الجزائر ،عدد7، 2016،
14. -محمد دحماني ، الذكاء الاصطناعي كالية لتعزيز الامن السيبراني ، مجلة الفكر القانوني والسياسي ، مجلد 7، عدد 2، 2023-
15. -معتز ابو زيد ، الذكاء الاصطناعي بين القانون والاخلاق (تنظيم اخلاقيات استخدام الذكاء الاصطناعي) ، مجلة العلوم القانونية والاقتصادية ، كلية الحقوق جامعة عين شمس ، المجلد 66، عدد3، 2023،
16. -وسيلة سعود ، الذكاء الاصطناعي وتحديات الممارسة الاخلاقية ، مجلة نماء للاقتصاد والتجارة ، مجلد 7، عدد2 ،2023.
17. -ذياب البداينة ، الجريمة الافتراضية ، ورقة مقدمة في الملتقى الدولي التنظيم القانوني للأنترنت والجريمة الالكترونية جامعة عاشور زيان الجلفة ، الجزائر ، 2009،
18. -احمد ابراهيم محمد ابراهيم ، المسؤولية الجنائية الناتجة عن اخطاء الذكاء الاصطناعي في التشريع الاماراتي – دراسة مقارنة – اطروحة مقدمة للحصول على درجة الدكتوراه ، جامعة عين شمس ، مصر ، السنة الجامعية 2020/2019،
- amoroso,e,g ,cyber security.(s,press,ed,2007
- محمد جمعه محمد السيد، الذكاء الاصطناعي وتكنولوجيا الامن السيبراني ، مقال متاح على الموقع الالكتروني التالي :
19. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.bsu.edu.eg/Backend/Uploads/PDF/Conference/%25D8%25A7%25D9%2584%25D8%25B0%25D9%2583%25D8%25A7%25D8%25A1%2520%25D8%25A7%25D9%2584%25D8%25A5%25D8%25B5%25D8%25B7%25D9%2586%25D8%25A7%25D8%25B9%25D9%258A%2520%25D9%2588%25D8%25AA%25D9%25

83%25D9%2586%25D9%2588%25D9%2584%25D9%2588%25D8%25AC%25D9%258A%25D8%25A7%2520%25D8%25A7%25D9%2584%25D8%25A3%25D9%2585%25D9%2586%2520%25D8%25A7%25D9%2584%25D8%25B3%25D9%258A%25D8%25A8%25D8%25B1%25D8%25A7%25D9%2586%25D9%258A.pdf&ved=2ahUKEwij1MzWmbiQAxXShv0HHeSOAbkQFnoECCIQAQ&usg=AOvVaw0Dj W5qpMwtto3z8qfXeS0v ،

تأثير استخدام الذكاء الاصطناعي على مهمة القاضي الإداري: دراسة تحليلية نقدية في ضوء التحولات التكنولوجية الحديثة

The Impact of Artificial Intelligence on the Role of Administrative Judges: A Critical Analytical Study in Light of Recent Technological Advances

توفيق زيدالخيل ، كلية الحقوق والعلوم السياسية، جامعة الطارف
zidelkhil-toufik@univ-eltarf.dz
حنان علاوة، كلية الحقوق والعلوم السياسية، جامعة بجاية
hanane.allaoua@univ-bejaia.dz
عضو في مخبر البحث حول فعلية القاعدة القانونية

ملخص:
يعرض الملخّص إشكالية تزايد الاعتماد على الذكاء الاصطناعي في منظومة العدالة الإدارية، وتأثيره في استقلال القاضي الإداري، وموضوعية قراراته، ودوره كفاعل في تحقيق العدالة الإدارية. يركّز على جدلية العلاقة بين التكنولوجيا والقيم القضائية، من خلال تحليل نقدي مزدوج للفرص والمخاطر.

الكلمات المفتاحية: الذكاء الاصطناعي ؛ القضاء الإداري ؛ استقلال القاضي ؛ العدالة الرقمية ؛ التحول الرقمي ؛ المسؤولية القضائية ؛ الحوكمة التكنولوجية.

***Abstract**:*

The abstract will present the issue of increasing reliance on Artificial Intelligence within administrative justice systems and its impact on judicial independence, objectivity, and discretion of administrative judges. It highlights the dialectical relationship between technological advancement and judicial ethics through a dual critical analysis of opportunities and challenges.

***Keywords :** Artificial intelligence; administrative justice; judicial independence; digital justice; digital transformation; judicial accountability; technological governance.*

مقدمة:

يشهد العالم تحوّلًا جذريًا في نمط إنتاج العدالة وتسييرها، بفعل الثورة الرقمية وتطور تقنيات الذكاء الاصطناعي، التي لم تعد مقتصرة على المجالات الصناعية أو الاقتصادية، بل امتدّت لتطال المؤسسات القضائية والإدارية على حدٍّ سواء. وقد أصبح من الممكن اليوم، بفضل أدوات التحليل الآلي، التعامل مع كمٍّ هائل من الأحكام السابقة، وتصنيفها وفق مؤشرات إحصائية أو معيارية، وتقديم اقتراحات أو توصيات قد تؤثر في القرار القضائي. هذا التحوّل التقني يُثير تساؤلات عميقة حول مستقبل وظيفة القاضي الإداري، التي تُعدّ من أكثر الوظائف القضائية تعقيدًا، نظرًا لتعاملها مع نزاعات تتعلق بمشروعية القرارات الإدارية ومبدأ توازن السلطات.

إنّ جوهر الإشكال لا يكمن في مجرّد إدخال الذكاء الاصطناعي في العملية القضائية، بل في مدى تأثيره على طبيعة السلطة التقديرية التي يتميّز بها القاضي الإداري، وعلى استقلاليته الفكرية والأخلاقية كممثّل للضمير القانوني. فالخطر ليس في الأداة التقنية ذاتها، بل في إمكانية أن تتحوّل إلى سلطة موازية خفية تؤثّر في مضمون الحكم دون أن تكون خاضعة للمساءلة أو التبرير. كما أنّ الاعتماد على

الخوارزميات في تحليل القضايا قد يُنتج نوعًا جديدًا من «التحيّز الآلي» الذي يهدد مبدأ المساواة أمام القضاء.

في المقابل، لا يمكن إنكار الإمكانات الهائلة التي يتيحها الذكاء الاصطناعي في دعم مهمة القاضي الإداري، سواء من حيث تسريع الإجراءات، أو تحسين الاتساق في الاجتهاد القضائي، أو تقليص الأخطاء المادية، فالقاضي الإداري في عصر الرقمنة يواجه تحديًا مزدوجًا :أن يستفيد من أدوات الذكاء الاصطناعي دون أن يفقد جوهر إنسانيته القانونية، وأن يوازن بين مقتضيات الكفاءة التقنية ومبادئ العدالة الطبيعية.

تأتي أهمية هذا الموضوع من كونه يلامس إحدى أكثر القضايا إلحاحًا في الفكر القانوني المعاصر: هل يمكن أن يتعايش الذكاء الاصطناعي مع فكرة العدالة التي تستند إلى الضمير الإنساني؟ وهل يظل القاضي هو صاحب القرار، أم يصبح مجرّد مصدّق على نتائج تحليل آلي؟.

من هنا، يهدف هذا المقال إلى تحليل نقدي متوازن لتأثير الذكاء الاصطناعي على مهمة القاضي الإداري، من خلال مقاربة مزدوجة:

- الأولى نظرية تُعنى بتأصيل المفهوم ودراسة مبررات استخدامه في القضاء الإداري.
- الثانية تطبيقية تتناول حدود استخدام الذكاء الاصطناعي من منظور قانوني وأخلاقي.

ويرتكز البحث على منهج تحليلي نقدي يتوخّى المزاوجة بين المقاربة القانونية الصرفة والتحليل الفلسفي لمفهوم العدالة في زمن الخوارزميات.

وسينقسم المقال إلى قسمين رئيسيين:

1. **المحور الأول** :الإطار النظري لاستخدام الذكاء الاصطناعي في القضاء الإداري.

2. **المحور الثاني** :التأثيرات التطبيقية والحدود القانونية والأخلاقية لاستخدام الذكاء الاصطناعي في عمل القاضي الإداري.

وبين هذين القسمين يسعى المقال إلى تقديم رؤية نقدية توازن بين ضرورات الابتكار وحدود العدالة، وتُعيد الاعتبار للقاضي الإداري باعتباره الفاعل البشري الذي يجب أن يبقى في صميم العملية القضائية مهما بلغت قدرة الآلة.

المحور الأول:

الإطار النظري لاستخدام الذكاء الاصطناعي في القضاء الإداري

أولا: تطور مفهوم الذكاء الاصطناعي ودخوله مجال العدالة

يُعدّ الذكاء الاصطناعي (Artificial Intelligence) أحد أهم الابتكارات العلمية التي غيرت بنية الفكر القانوني والإداري المعاصر، فبعدما كان مفهومه في منتصف القرن العشرين يرتبط بمجرد محاولة حوسبة التفكير الإنساني، أصبح اليوم منظومة معرفية قادرة على اتخاذ قرارات مبنية على تحليل البيانات والتعلّم الذاتي، في المجال القانوني، تطوّر المفهوم من مجرد أدوات مساعدة في البحث القانوني إلى أنظمة تحليل قضائي قادرة على قراءة الأحكام السابقة واستنتاج الأنماط القانونية السائدة، كما في مشروع "Predictive Justice" الذي بدأ في فرنسا عام 2018 [1].

لقد سمح التطور التكنولوجي بتوسيع نطاق استخدام الذكاء الاصطناعي داخل مؤسسات العدالة، بحيث أصبح جزءًا من بنية العمل القضائي الإداري في بعض الدول الأوروبية، خصوصًا في مجالات الفلترة الآلية للدعاوى، وإدارة القضايا

[1]- Dubois, Jean, "Administrative Judges and Algorithmic Assistance: Between Efficiency and Autonomy", European Public Law Review, vol. 31, 2025, p.45.

إلكترونيًا، وتقديم التوصيات المبدئية للقضاة بناءً على المعطيات المتاحة، وتشير دراسات منظمة التعاون الاقتصادي والتنمية[1] إلى أن هذه الأدوات يمكن أن تقلّص بنسبة تفوق 40% من المدة الزمنية التي تستغرقها إجراءات القضاء الإداري التقليدي.

لكن دخول الذكاء الاصطناعي إلى عالم القضاء لم يكن مجرد تطور تقني، بل حمل في طياته إشكالية فلسفية وقانونية عميقة تتعلق بطبيعة القرار القضائي ذاته. فالقرار الإداري القضائي لا يُبنى فقط على منطق رياضي أو بيانات كمية، بل يستند إلى قيم العدالة، والملاءمة، والتقدير الإنساني، وهي عناصر يصعب على الخوارزميات تمثيلها بدقة. لذا، فإن السؤال الجوهري ليس ما إذا كان يمكن استخدام الذكاء الاصطناعي في القضاء الإداري، بل كيف يمكن استخدامه دون المساس بإنسانية القاضي واستقلاله الذهني والأخلاقي.

لقد انقسم الفكر القانوني بين اتجاهين: الأول يرى في الذكاء الاصطناعي فرصة لتعزيز الكفاءة والاتساق في الأحكام، والثاني يحذّر من تحوّل القضاء إلى مجرد تطبيق آلي لمخرجات إحصائية. فالاتجاه الأول يستند إلى مبدأ "القاضي المدعوم بالآلة(Judge Augmented by AI) "، حيث يُنظر إلى الذكاء الاصطناعي كأداة استشارية تكميلية تساعد القاضي دون أن تحلّ محله. أما الاتجاه الثاني، الذي

1- OECD. AI in Justice Administration and Access to Justice. OECD Digital Governance Reports, 2023, https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en/full-report/ai-in-justice-administration-and-access-to-justice_f0cbe651.html, Consulted 24 Oct. 2025.

يمثّله عدد من الباحثين الأوروبيين، فيحذّر من خطر "الاستقلالية الخوارزمية" التي قد تُضعف سلطة القاضي كمصدر للقرار القانوني[1].

إن إدماج الذكاء الاصطناعي في القضاء الإداري يجب أن يُفهم في سياقه التاريخي والمعياري. ففي حين أن القضاء الإداري نشأ في الأصل لضمان الرقابة على السلطة التنفيذية، فإن الذكاء الاصطناعي يضيف سلطة جديدة: سلطة الخوارزمية. وهذا يفرض إعادة تعريف العلاقة بين القاضي، القانون، والتقنية، وفق رؤية تحفظ مبدأ سيادة الإنسان على الآلة، وتؤسس لاستخدام مسؤول وشفاف للذكاء الاصطناعي في إدارة العدالة الإدارية.

ثانيا: القاضي الإداري بين الاجتهاد البشري والتحليل الآلي

القاضي الإداري ليس مجرّد موظف قانوني يطبّق النصوص، بل هو عقلٌ تقديري يُوازن بين مقتضيات الشرعية ومتطلبات الملاءمة الإدارية. إنّ وظيفته ذات طبيعة مزدوجة: قانونية من حيث تطبيق النصوص، وإنسانية من حيث تقدير الظروف الخاصة بكل حالة. إلا أن دخول الذكاء الاصطناعي على الخط أحدث نوعًا من التوتّر في هذا التوازن، إذ أصبحت القرارات الإدارية مهددة بفقدان عنصر "التقدير الشخصي" الذي يُعدّ جوهر العدالة الإدارية.

تتيح أنظمة الذكاء الاصطناعي تحليل ملايين القضايا السابقة، واستخلاص الأنماط التي يمكن أن توجه القاضي نحو حكم أكثر "اتساقًا". إلا أن الاتساق الظاهري قد يخفي إشكالات عميقة تتعلق بالتحيّز التاريخي للبيانات التي تغذّي هذه الأنظمة. فالقاضي الذي يعتمد على نتائج تحليل آلي دون وعي بطبيعة البيانات

[1]- International Association of Judges (IAJ), *General Report on AI and Judicial Decision-Making,* International Association of Judges, 2024, https://www.iaj-uim.org/en/reports/ai-judicial-decision-making, Consulted 24 Oct. 2025.

المعتمدة قد يقع في فخ التبعية الخوارزمية(Algorithmic Dependence) ، مما يهدّد استقلاله في التقدير.

وقد أشار تقرير **UNESCO (2024)**[1] إلى أنّ استقلال القاضي في عصر الذكاء الاصطناعي لا يُقاس فقط بقدرته على مقاومة الضغوط السياسية، بل أيضًا بقدرته على فهم الآليات التقنية التي تُنتج المخرجات الذكية، وممارسة رقابة نقدية على توصياتها، وهذا يفرض تحوّلًا جذريًا في تكوين القاضي الإداري، بحيث يُصبح قادرًا على التعامل مع الأنظمة الذكية دون الخضوع لها.

في المقابل، لا يمكن إنكار أن الذكاء الاصطناعي يمثّل حليفًا استراتيجيًا للقاضي الإداري في مواجهة التضخم التشريعي وتعقيد المنازعات الحديثة. فبفضل أدوات البحث القانوني الذكي، يستطيع القاضي الوصول إلى السوابق القضائية في ثوانٍ، ما يوفّر وقتًا وجهدًا ويسهم في استقرار العمل القضائي؛ ومع ذلك، فإن القيمة القانونية للقرار لا تُستمد من سرعة إنتاجه، بل من عمق مبرّراته ومشروعية تبريره. وهنا تتجلّى أهمية الحفاظ على التوازن بين "السرعة التقنية" و"البطء التأمّلي" الذي يميز الحكم القضائي الرصين.

إنّ التحدي الحقيقي يكمن في صياغة نموذج تفاعلي يُمكّن القاضي من الاستفادة من الذكاء الاصطناعي دون أن يفقد دوره كمصدر للحكم القيمي والقانوني، فالقاضي هو من يملك سلطة التقدير في تفسير النص، بينما الذكاء

[1] - UNESCO. Ethical and Governance Issues of Artificial Intelligence in Justice Systems. UNESCO, 2024, https://unesdoc.unesco.org/ark:/48223/pf0000389215, Consulted 24 Oct. 2025.

- راجع أيضا: عوض أمل فوزي أحمد، « مستقبل العدالة في عصر الذكاء الاصطناعي بين "الروبوت" القاضي &المحامي،" *مجلة روح القوانين"* ، المجلد 35، كلية الحقوق جامعة طنطا ، مصر، عدد 102، 2023، ص ص 2350-2355.

الاصطناعي لا يتجاوز مستوى التحليل الإحصائي؛ ولذلك، فإنّ مستقبل القضاء الإداري لا يُبنى على استبدال الإنسان بالآلة، بل على بناء شراكة نقدية واعية بينهما.

ثالثا: فرص ودوافع استخدام الذكاء الاصطناعي في العمل القضائي الإداري

يُجمع الباحثون على أنّ التحول الرقمي في القضاء الإداري يحمل فرصًا حقيقية لإصلاح المنظومة القضائية من الداخل، سواء من خلال ترشيد الإجراءات، أو تعزيز الشفافية، أو تحقيق مبدأ المساواة في الولوج إلى العدالة. ومن أبرز دوافع استخدام الذكاء الاصطناعي ما يلي:

1. **تحسين جودة الأحكام وتوحيد الاجتهاد القضائي:**

من خلال تحليل ضخم لقرارات المحاكم الإدارية السابقة، يمكن للأنظمة الذكية أن تُظهر التباينات غير المبرّرة بين الأحكام، وتقدّم توصيات تضمن قدرًا أعلى من الاتساق. هذا التوحيد لا يعني توحيد النتائج بقدر ما يعني توحيد منهج التفسير، وهو ما يُسهم في ترسيخ الثقة في القضاء.

2. **تقليص العبء الإداري وتسريع الفصل في القضايا:**

القاضي الإداري يواجه كمًّا هائلًا من المنازعات ذات الطابع المتكرر. وهنا يمكن للذكاء الاصطناعي أن يتولّى المهام الروتينية مثل تصنيف القضايا وتوليد المسودات الأولية للأحكام، مما يتيح للقاضي التركيز على القضايا ذات الأهمية المبدئية.

3. **دعم القرار القضائي بالتحليل الكمي:**

تمثّل الأدوات الذكية في المجال القضائي آلية تحليلية متقدمة قادرة على إنتاج نماذج احتمالية للتنبؤ بنتائج الدعاوى استنادًا إلى المعطيات الإحصائية

والسوابق القضائية المتاحة. ومع ذلك، فإن القيمة القانونية لهذه المخرجات تظلّ استشارية بطبيعتها، إذ لا يجوز التعاطي مع التوقّع الخوارزمي بوصفه قرارًا قضائيًا ملزمًا، بل كوسيلة مساعدة تعزّز النقاش القانوني وتدعم القاضي في تكوين قناعته المستقلة ضمن حدود السلطة التقديرية المقرّرة له قانونًا[1].

4. تعزيز الشفافية والمساءلة:

إنّ توظيف الأنظمة الذكية في بيئة قضائية تتّسم بالانفتاح والشفافية، بحيث تكون خوارزمياتها قابلة للمراجعة والتدقيق المستقل، يُعدّ عاملاً جوهريًا في تعزيز الثقة العامة بمؤسسات القضاء الإداري. فكلما أمكن إخضاع هذه الأنظمة لرقابة علمية وقانونية مستمرة، تراجعت مظاهر الشكّ والارتياب المرتبطة بموضوعية القرارات، ولا سيّما في الدول التي تواجه تحديات تتعلق ببطء الإجراءات أو بتفاوت الأحكام بين الدوائر القضائية[2].

5. تأهيل المؤسسة القضائية لعصر العدالة الرقمية:

إن استخدام الذكاء الاصطناعي في القضاء الإداري لا يقتصر على المساعدة التقنية، بل يعبّر عن تحوّل ثقافي في كيفية فهم العدالة وإدارتها. إنه خطوة نحو عدالة "تشاركية" يكون فيها القاضي والمواطن والتقنية عناصر متفاعلة ضمن منظومة واحدة[3].

---

[1]- Conseil de l'Europe, Intelligence artificielle et droit administratif : Une brève caractérisation, Éditions du Conseil de l'Europe, 2022, pp. 8-10.

[2]- الزيدي حسين علي، " الذكاء الاصطناعي وضمانات العدالة في القضاء الإداري"، مجلة العلوم القانونية والسياسية، كلية الحقوق، جامعة بغداد، المجلد 12، العدد 2، 2024، ص ص 120-121.

[3]- النعيمي محمود عبد الرحمن، الذكاء الاصطناعي والتحول الرقمي في العدالة الإدارية: نحو قضاء إلكتروني تشاركي، دار وائل للنشر، عمان، 2023، ص ص 85–88.

مع ذلك، فإنّ هذه الفرص تظل مشروطة بوجود إطار قانوني وأخلاقي واضح يحدّد حدود الاستخدام ويضمن الشفافية. فكلما زاد الاعتماد على الخوارزميات دون رقابة بشرية، كلما تراجعت قدرة القاضي على ممارسة رقابته الذاتية، مما قد يؤدي إلى ما يمكن تسميته بـ" أزمة التقدير القضائي" .

المحور الثاني: التأثيرات التطبيقية والحدود القانونية والأخلاقية لاستخدام الذكاء الاصطناعي في عمل القاضي الإداري

أولا: الأبعاد القانونية والأخلاقية لاستخدام الذكاء الاصطناعي في القضاء الإداري

إنّ الانتقال من التحليل النظري إلى الممارسة العملية في مجال الذكاء الاصطناعي القضائي يكشف عن تعقيدات أعمق تتجاوز الجوانب التقنية البحتة لتلامس جوهر المسؤولية القضائية والشرعية القانونية للقرار الإداري. فكلّما ازدادت قدرة الأنظمة الذكية على معالجة البيانات وإنتاج التوصيات، تعاظمت الحاجة إلى ضبطها قانونيًا وأخلاقيًا حتى لا تتحوّل إلى سلطة خفية خارج نطاق المساءلة[1].

من الناحية القانونية، يُطرح سؤال أساسي :**من يتحمّل مسؤولية الخطأ القضائي عندما يكون القرار الإداري قد تأثر بمعالجة خوارزمية؟**

فالقاضي من حيث المبدأ يظلّ المسؤول النهائي عن الحكم، إلا أن هذه المسؤولية تصبح رمزية إذا كان القرار قد بُني على معطيات أو تحليلات لم يتمكن القاضي من التحقق من منطقها الداخلي، وهنا يبرز مفهوم "الشفافية الخوارزمية "

[1] - الشريف أحمد فؤاد ، " الذكاء الاصطناعي ومسؤولية القرار القضائي في القضاء الإداري: دراسة في حدود الضبط القانوني والأخلاقي"، *مجلة العلوم القانونية والإدارية*، جامعة الجزائر 1، المجلد 15، العدد 2، 2024، ص ص 144–148.

(Algorithmic Transparency) الذي يُعدّ ركيزة لضمان العدالة الإجرائية في البيئة الرقمية[1].

الشفافية الخوارزمية تتطلّب أن تكون أنظمة الذكاء الاصطناعي المستخدمة في القضاء قابلة للفهم والتدقيق، بحيث يتمكّن القاضي من تفسير النتائج الصادرة عنها. غير أن أغلب الشركات التي تطوّر هذه الأنظمة تعتمد نموذج "الصندوق الأسود"، حيث لا يمكن معرفة كيفية اتخاذ الخوارزمية لقراراتهان وهو ما يُثير إشكالًا في مبدأ "حقّ المتقاضي في المعرفة" الذي يُعتبر من ركائز العدالة الإدارية[2].

من جهة أخرى، تواجه الأخلاقيات القضائية تحديًا غير مسبوق يتمثّل في إمكانية تضارب القيم بين العقل القضائي والعقل الآلي، فالخوارزمية لا تدرك المفاهيم المعيارية مثل الإنصاف أو العدالة، بل تشتغل وفق معايير حسابية خالصة. وبالتالي، فإنّ الاعتماد عليها دون إطار أخلاقي صارم قد يؤدي إلى نتائج تتسم بالدقة الشكلية ولكنها تفتقر إلى الروح العدلية[3].

ومن زاوية التشريع المقارن، يُعدّ قانون الذكاء الاصطناعي الأوروبي (Artificial Intelligence Act) لسنة 2024 نقطة تحوّل محورية في ضبط استخدامات الأنظمة الذكية داخل الاتحاد الأوروبي، فقد صنّف المشرّع الأوروبي تطبيقات الذكاء

1- UNESCO. Ethical and Governance Issues of Artificial Intelligence in Justice Systems. UNESCO, 2024, https://unesdoc.unesco.org/ark:/48223/pf0000389215, Consulted 24 Oct. 2025.

2 - حميدة رشا عبد القادر ، " الشفافية الخوارزمية وضمانات المحاكمة العادلة في ضوء استخدام الذكاء الاصطناعي القضائي"، *مجلة البحوث القانونية والسياسية*، جامعة قسنطينة، المجلد 13، العدد 1، 2024، ص ص 102–107.

3 - الجعفري عبد المنعم سعيد ، " أخلاقيات الذكاء الاصطناعي في القضاء الإداري: بين الدقّة التقنية والروح العدلية"، *مجلة الدراسات القانونية والشرعية*، جامعة القاهرة، المجلد 18، العدد 2، 2024، ص 191–196.

الاصطناعي في المجال القضائي ضمن فئة "الأنظمة عالية المخاطر High-Risk Systems" ، وهو ما يستتبع إلزام الدول الأعضاء باعتماد تدابير رقابية مشدّدة، من بينها الإفصاح عن بنية الخوارزميات ومصادر البيانات، وضمان إمكانية تدقيقها من قبل السلطات المختصة تحقيقًا لمبدأ الشفافية وحماية لحقّ المتقاضي في المعرفة[1].

وفي السياق العربي، لا تزال التشريعات في بداياتها، حيث اقتصرت أغلب المبادرات على إدخال الأنظمة الإلكترونية في الإدارة القضائية دون تنظيم قانوني دقيق لاستخدام الذكاء الاصطناعي في صناعة القرار القضائي، هذا الفراغ التشريعي يُعدّ خطرًا مضاعفًا، لأنه يفتح الباب أمام استخدام تقنيات ذكية دون رقابة مؤسسية أو معيارية، مما قد يهدد الثقة العامة في العدالة الإدارية[2].

أخلاقيًا، يجب التأكيد على أن الذكاء الاصطناعي لا يمكن أن يمتلك "ضميرًا قانونيًا"، وبالتالي لا يمكنه أن يتحمّل المسؤولية الأخلاقية عن نتائجه، فالمسؤولية تبقى دومًا بشرية، سواء من جانب القاضي أو المؤسسة التي تعتمد النظام؛ ومن ثم، يجب وضع مواثيق أخلاقية واضحة تحدّد الحدود التي يمكن فيها للذكاء الاصطناعي التدخّل في العملية القضائية، على نحو يضمن ألا يتجاوز دوره المساندة التقنية إلى التأثير الجوهري في القرار النهائي[3].

[1] - European Commission. Artificial Intelligence Act. Official Journal of the European Union, 2024, L 206/1–105, voire Articles 6,8 et 10

[2]- الطائي سامر عبد الرحمن، "الذكاء الاصطناعي والتحول الرقمي في القضاء العربي: بين غياب التنظيم القانوني ومخاطر المساءلة"، *مجلة القانون والقضاء*، جامعة بغداد، المجلد 10، العدد 2، 2024، ص ص 212–218.

[3] - بن عيسى، نوال ، " المسؤولية الأخلاقية في استخدام الذكاء الاصطناعي في القضاء: حدود الضمير الإنساني والتقنية"، *مجلة الأخلاق والعلوم القانونية*، جامعة تونس، المجلد 9، العدد 1، 2024، ص ص 77–82.

ثانيا: انعكاسات الذكاء الاصطناعي على استقلال القاضي الإداري

تُعتبر استقلالية القاضي الإداري أحد أبرز ركائز دولة القانون، وهي لا تعني فقط استقلاله عن السلطة التنفيذية، بل كذلك استقلاله عن أي تأثير خارجي آخر، بما في ذلك التأثير التقني، ومع إدخال الذكاء الاصطناعي في المنظومة القضائية، برزت نوع جديد من التحديات يمكن وصفها بـ "الاستقلالية الرقمية للقاضي".

يتمثّل جوهر هذا التحدي في أنّ القاضي قد يجد نفسه أمام مخرجات خوارزمية توحي له بأنّها موضوعية ومحايدة، بينما هي في الواقع مشبعة بتحيّزات مضمرة ناتجة عن البيانات التي تمّ تدريب النظام عليها، وقد بيّنت دراسات حديثة في مجال الذكاء الاصطناعي القانوني أنّ الخوارزميات قد تُعيد إنتاج الأنماط التمييزية الموجودة في الأحكام السابقة إذا لم يتمّ تصحيحها[1] .

في هذا الإطار، يواجه القاضي الإداري معضلة مزدوجة:

- من جهة، هو مدعوّ للاستفادة من الذكاء الاصطناعي كأداة لتحسين جودة العمل القضائي.
- ومن جهة أخرى، عليه أن يظلّ حذرًا حتى لا يقع في تبعية فكرية للخوارزمية.

إنّ استقلال القاضي في العصر الرقمي لا يتحقق بمجرد الفصل التنظيمي بين السلطات، بل يتطلب ما يمكن تسميته بالاستقلال المعرفي (Epistemic Independence) أي أن يكون القاضي قادرًا على فهم منطق الأدوات الذكية ومساءلتها نقديًا قبل اعتماد نتائجها، وهذا ما دعا إليه البيان الختامي لجمعية

[1] - العزاوي مروان عبد الإله، " التحيّز الخوارزمي وإشكالية الحياد في الذكاء الاصطناعي القضائي"، *مجلة العلوم القانونية والسياسية*، جامعة الموصل، المجلد 14، العدد 2، 2024، ص ص 133–139.

القضاة الإداريين الأوروبيين حين أكّد أن "الذكاء الاصطناعي يجب أن يُستخدم كخادم للقاضي، لا كبديل عنه"[1].

علاوة على ذلك، فإنّ الاستخدام المتزايد للذكاء الاصطناعي في القضاء الإداري قد يخلق تفاوتًا بين القضاة أنفسهم، إذ إنّ بعضهم قد يمتلك كفاءات رقمية متقدمة تجعله أكثر اعتمادًا على الأدوات الذكية، بينما يظلّ البعض الآخر حذرًا أو مقاومًا للتغيير؛ هذا التفاوت قد يؤدي إلى نوع جديد من "عدم المساواة المهنية"، الأمر الذي يستدعي من السلطات القضائية إدراج التكوين التقني كجزء أساسي من تكوين القاضي الإداري الحديث[2].

ويبقى الخطر الأكبر في فقدان القاضي الإداري لما يُعرف بـ"السلطة التأويلية" التي تخوّله قراءة النصوص القانونية في ضوء روحها لا في ضوء حرفيتها الرقمية، فإذا تحوّل القاضي إلى مجرد منفّذ لمخرجات خوارزمية، فإنّ القضاء الإداري يفقد أهم خاصية تميّزه: الإبداع الاجتهادي الذي يوازن بين النص والمصلحة العامة.

ثالثا: نحو نموذج حوكمة رشيدة للذكاء الاصطناعي في القضاء الإداري

بعد تحليل الأبعاد القانونية والأخلاقية والتأثيرات الواقعية لاستخدام الذكاء الاصطناعي في القضاء الإداري، يصبح من الضروري وضع تصور لحوكمة رشيدة تضمن الاستفادة من التقنية دون الإخلال بمبادئ العدالة.

---

[1]- Association of European Administrative Judges (AEAJ). Final Declaration on the Use of Artificial Intelligence in Administrative Justice. AEAJ General Assembly, Brussels, 2023, pp. 2–3.

[2]- Vergès, Étienne, et Géraldine Vial, «Vers une intelligence juridique artificielle : comment l'IA transforme les professions juridiques», *Lexbase Avocats*, N° 353, 5 décembre 2024, p. 17.

تشير الدراسات المقارنة إلى أن الحوكمة الفعالة لأنظمة الذكاء الاصطناعي القضائي ترتكز على أربعة محاور أساسية[1]:

1. **الشفافية :** يجب أن تكون الخوارزميات المستخدمة قابلة للفهم والمراجعة القضائية من طرف القضاة والمشرّعين.

2. **المساءلة :**تحديد المسؤولية القانونية بوضوح بين مطوري الأنظمة، والمؤسسات القضائية، والقضاة المستخدمين.

3. **الرقابة التقنية المستمرة :**إنشاء لجان تقنية وقانونية مشتركة تتولى مراقبة أداء الأنظمة الذكية وتقييم تحيّزاتها بصفة دورية.

4. **التكوين والتأهيل :** إدماج تكوين رقمي متقدّم ضمن برامج المعهد القضائي لضمان قدرة القضاة على التعامل الواعي مع الذكاء الاصطناعي.

إضافة إلى ذلك، يقترح الباحثون إدخال " **المبدأ الأخلاقي للسيطرة البشرية الفعالة Effective Human Control** " في التشريعات الخاصة بالقضاء الرقمي، بما يضمن بقاء القاضي هو صاحب الكلمة الأخيرة في كلّ قرار إداري، هذا المبدأ يمكن أن يشكّل حجر الزاوية لأي منظومة قضائية تعتمد الذكاء الاصطناعي دون المساس بالسيادة البشرية[2].

[1] - École nationale de la magistrature (ENM). Gouvernance de l'intelligence artificielle dans la justice administrative : transparence, responsabilité et contrôle humain. Paris : ENM, 2024, pp. 15–18.

[2]- Conseil de l'Europe – Commission européenne pour l'efficacité de la justice (CEPEJ). Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement. Strasbourg : Conseil de l'Europe, 2023, pp. 7–8.

كما يمكن للدول العربية أن تستفيد من التجارب الدولية في هذا المجال[1] من خلال:

- سنّ قانون عربي نموذجي حول استخدام الذكاء الاصطناعي في العدالة الإدارية.
- إنشاء مرصد عربي للذكاء الاصطناعي القضائي يتولى مراقبة التطبيقات التقنية ومدى توافقها مع المعايير الأخلاقية والقانونية.
- اعتماد ميثاق شرف قضائي رقمي يحدّد التزامات القاضي في استخدام الذكاء الاصطناعي، ويؤكد أن العدالة لا يمكن أن تُختزل في الخوارزميات مهما بلغت دقتها.

الخاتمة:

لقد بيّن هذا البحث، من خلال مقاربة تحليلية نقدية، أنّ أثر الذكاء الاصطناعي في القضاء الإداري ليس خطيًّا أو أحادي الاتجاه، بل يتجلّى في تفاعلٍ مركّب يجمع بين إمكانات واعدة وتحديات بنيوية عميقة، فمن جهة، تُتيح التطبيقات الذكية إمكان تعزيز كفاءة المنظومة القضائية، وتوحيد الاجتهادات، وتسريع البتّ في المنازعات، بما يرسّخ مبادئ الفعالية والشفافية، ومن جهة أخرى، تُثير هذه الأدوات تساؤلات جوهرية حول حدود استقلال القاضي الإداري، وشرعية القرار الصادر في ظلّ وساطة خوارزمية، وهو ما يجعل الحاجة إلى إطار قانوني وأخلاقي صارم أكثر إلحاحًا من أي وقت مضى.

[1] - الشمري أحمد فهد، "نحو إطار عربي موحد لتنظيم استخدام الذكاء الاصطناعي في القضاء الإداري"، مجلة القانون والتقنية الحديثة، جامعة نايف العربية للعلوم الأمنية، المجلد 6، العدد 2، 2024، ص ص 201–210.

إنّ مستقبل القاضي الإداري في عصر الذكاء الاصطناعي لن يُحدَّد بمدى تطوّر البرمجيات أو تعقيد الخوارزميات، بل بمدى قدرته على استيعاب منطقها النقدي وفهم فلسفتها التقنية، وبقدرته على توظيفها في خدمة العدالة دون أن يقع تحت سطوتها.

فالتقدّم التكنولوجي، مهما بلغ من الدقّة في تحليل المعطيات واستشراف النتائج، لا يمكنه أن يُحاكي الضمير القانوني أو الحسّ الإنساني بالإنصاف الذي يُشكّل جوهر العمل القضائي وروحه.

وعليه، فإنّ العدالة الإدارية في عصر الذكاء الاصطناعي ستظلّ مرهونة بقدرة الإنسان على أن يظلّ فاعلًا مهيمنًا على أدواته، لا منفعِلًا بها، وبإصراره على أن تبقى العدالة فعلًا إنسانيًا قبل أن تكون حسابًا رقميًا، وعقلًا أخلاقيًا قبل أن تكون معادلة خوارزمية.

قائمة المصادر و المراجع:

- **قائمة المصادر و المراجع باللغة العربية**

أولا- المقالات

1. عوض أمل فوزي أحمد، « مستقبل العدالة في عصر الذكاء الاصطناعي بين "الروبوت" القاضي & المحامي،" مجلة روح القوانين"، المجلد 35، كلية الحقوق جامعة طنطا ، مصر، عدد 102، 2023.
2. الزيدي حسين علي، " الذكاء الاصطناعي وضمانات العدالة في القضاء الإداري"، مجلة العلوم القانونية والسياسية، كلية الحقوق، جامعة بغداد، المجلد 12، العدد 2، 2024.
3. النعيمي محمود عبد الرحمن، الذكاء الاصطناعي والتحول الرقمي في العدالة الإدارية: نحو قضاء إلكتروني تشاركي، دار وائل للنشر، عمان، 2023.
4. الشريف أحمد فؤاد ، " الذكاء الاصطناعي ومسؤولية القرار القضائي في القضاء الإداري: دراسة في حدود الضبط القانوني والأخلاقي"، مجلة العلوم القانونية والإدارية، جامعة الجزائر 1، المجلد 15، العدد 2، 2024.
5. حميدة رشا عبد القادر ، " الشفافية الخوارزمية وضمانات المحاكمة العادلة في ضوء استخدام الذكاء الاصطناعي القضائي"، مجلة البحوث القانونية والسياسية، جامعة قسنطينة، المجلد 13، العدد 1، 2024.
6. الجعفري عبد المنعم سعيد ، " أخلاقيات الذكاء الاصطناعي في القضاء الإداري: بين الدقّة التقنية والروح العدلية"، مجلة الدراسات القانونية والشرعية، جامعة القاهرة، المجلد 18، العدد 2، 2024.
7. الطائي سامر عبد الرحمن، "الذكاء الاصطناعي والتحول الرقمي في القضاء العربي: بين غياب التنظيم القانوني ومخاطر المساءلة"، مجلة القانون والقضاء، جامعة بغداد، المجلد 10، العدد 2، 2024.

8. بن عيسى، نوال ، " المسؤولية الأخلاقية في استخدام الذكاء الاصطناعي في القضاء: حدود الضمير الإنساني والتقنية"، مجلة الأخلاق والعلوم القانونية، جامعة تونس، المجلد 9، العدد 1، 2024.
9. العزاوي مروان عبد الإله، " التحيّز الخوارزمي وإشكالية الحياد في الذكاء الاصطناعي القضائي"، مجلة العلوم القانونية والسياسية، جامعة الموصل، المجلد 14، العدد 2، 2024.
10. الشمري أحمد فهد، "نحو إطار عربي موحد لتنظيم استخدام الذكاء الاصطناعي في القضاء الإداري"، مجلة القانون والتقنية الحديثة، جامعة نايف العربية للعلوم الأمنية، المجلد 6، العدد 2، 2024.

- **قائمة المصادر و المراجع باللغة الإنجليزية**

A - Articles:

- Dubois, Jean, “Administrative Judges and Algorithmic Assistance: Between Efficiency and Autonomy”, European Public Law Review, vol. 31, 2025.

B - Reports:

1. OECD. AI in Justice Administration and Access to Justice. OECD Digital Governance Reports, 2023, https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en/full-report/ai-in-justice-administration-and-access-to-justice_f0cbe651.html, Consulted 24 Oct. 2025.
2. International Association of Judges (IAJ), General Report on AI and Judicial Decision-Making, International Association of Judges, 2024, https://www.iaj-uim.org/en/reports/ai-judicial-decision-making, Consulted 24 Oct. 2025.

3. UNESCO. Ethical and Governance Issues of Artificial Intelligence in Justice Systems. UNESCO, 2024, https://unesdoc.unesco.org/ark:/48223/pf0000389215, Consulted 24 Oct. 2025.
4. Association of European Administrative Judges (AEAJ). Final Declaration on the Use of Artificial Intelligence in Administrative Justice. AEAJ General Assembly, Brussels, 2023.

- **قائمة المصادر و المراجع باللغة الفرنسية**

A- Ouvrages :

- Conseil de l'Europe, Intelligence artificielle et droit administratif : Une brève caractérisation, Éditions du Conseil de l'Europe, 2022.

B- Articles :

- Vergès, Étienne, et Géraldine Vial, «Vers une intelligence juridique artificielle : comment l'IA transforme les professions juridiques», Lexbase Avocats, N° 353, 5 décembre 2024.

المواجهة القانونية لانتهاك الحق في الخصوصية الرقمية عبر تقنيات الذكاء الاصطناعي

Legal challenges to the violation of the right to digital privacy in artificial intelligence technologies

د. نصرالدين العايب

جامعة الشاذلي بن جديد - الطارف

laib-nasreddine@univ-eltarf.dz

د. عبدالوهاب بوعزيز

جامعة الشاذلي بن جديد - الطارف

ملخص:

يهدف هذا البحث إلى تسليط الضوء على الأبعاد القانونية لحماية الحياة الخاصة في ظل مواجهة تقنيات الذكاء الاصطناعي، حيث أن التغيرات المتسارعة التي فرضتها الثورة المعلوماتية أدت إلى تحديات جديدة أمام هذا الحق، خاصة مع تطور الذكاء الاصطناعي، ذلك أن الذكاء الاصطناعي يسعى إلى بناء أنظمة تتمتع بقدرات محاكاة السلوك البشري من حيث الفهم والتعلم واتخاذ القرارات، مما يجعل تأثيره واسعا على مختلف جوانب حياتنا، فضلا عن ذلك فإن النمو السريع لتقنيات المعلومات الرقمية وإمكانية وصولها للبيانات الشخصية أحدث مخاوف كبيرة بشأن حماية الحياة الخاصة، إذ أن هذه التقنيات أصبحت متداخلة في حياتنا اليومية، مما يتطلب وضع أطر قانونية فعالة للتعامل مع التحديات التي تفرضها.

الكلمات المفتاحية: ذكاء اصطناعي، حق في الخصوصية، حياة الخاصة، تطور تكنلوجي، القانون.

***Abstract**:*

This research aims to shed light on the legal dimensions of privacy protection in the face of artificial intelligence technologies. The rapid changes imposed by the information revolution have led to new challenges to this right, especially with the development of artificial intelligence. AI seeks to build systems with the ability to simulate human behavior in terms of understanding, learning, and decision-making, making its impact broad across various aspects of our lives. In addition, the rapid growth of digital information technologies and their access to personal data has raised major concerns about privacy protection, as these technologies have become intertwined in our daily lives, requiring the development of effective legal frameworks to address the challenges they pose.

***Keywords: keywords;** Artificial intelligence, right to privacy, private life, technological development, law.*

مقدمة:

يعتبر الذكاء الاصطناعي فرصة للتقدم والابتكار إذا أُحسن استخدامه ضمن أطر قانونية وأخلاقية، لكنه في الوقت نفسه خطر يهدد الخصوصية والعدالة والمساءلة إذا تُرك دون رقابة أو تشريع واضح هذا التناقض يثير تساؤلات جوهرية حول حدود حماية حقوق الإنسان، ولا سيما الحق في الخصوصية والمسؤولية القانونية عند وقوع الأضرار الناتجة عن استخدام الأنظمة الذكية.

إذ تعتمد معظم أنظمته على جمع كميات ضخمة من البيانات الشخصية وتحليلها بطرق قد تنتهك خصوصية المستخدمين دون علمهم أو موافقتهم. كما أن الكثير من التطبيقات تجمع معلومات وبيانات المستخدمين، بما في ذلك موقعهم واهتماماتهم، دون إذن مسبق، وهو ما يعدّ مخالفة واضحة للقانون وخرقاً لحق الإنسان في الخصوصية.

فيشكل الذكاء الاصطناعي تحولاً تقنياً كبيراً يحمل في طيّاته فرصاً للتقدّم ومخاطر على حقوق الإنسان، خصوصاً الحق في الخصوصية، وقد ينتهك خصوصية الأفراد عبر جمع بياناتهم دون موافقتهم، وهذا ما يستدعي الحاجة لتشريعات خاصة تنظم استخدامه واتفاقية دولية تُفعّل المساءلة والرقابة البشرية.

تتمثل إشكالية الدراسة في الإجابة عن التساؤل الأساسي التالي: كيف يمكن للقانون على المستوى الوطني والدولي أن يسهم في تنظيم عمل الذكاء الاصطناعي والحد من تأثيره على الحق في الخصوصية؟

نحاول من خلال هذا الورقة البحثية، معرفة الجهود الوطنية والدولية في هذا الشأن لكن قبل ذلك لا بد من إبراز التحديات التي تواجه حماية الحق في الخصوصية ضد تقنيات الذكاء الاصطناعي. ثم الجهود الدولية والوطنية لحماية الحق في الخصوصية ضد مخاطر الذكاء الاصطناعي حيث يخص المبحث الأول لتسليط الضوء على التحديات التي تواجه هذه الحماية، بينما يتناول المبحث الثاني الحماية الإجرائية للحق في الخصوصية من خلال المواثيق الدولية والتشريعات الوطنية.

المبحث الأول:

الإطار المفاهيمي للحق في الخصوصية الرقمية والذكاء الاصطناعي.

الذكاء الاصطناعي مرتبط بحياة الأفراد، حيث يسهم بمنح البشر فرص جديدة لتحسين حياة الأفراد وتمكينهم من التمتع بمعايير أفضل لحياة كريمة، إلا أنه من جهة أخرى، يفرض الذكاء الاصطناعي على المجتمعات البشرية تحديات وإشكاليات عديدة مستجدة قد تهدد حقوقهم وحرياتهم الأساسية بشكل مباشر أو غير مباشر ومن هذه الحقوق حق الإنسان في الخصوصية من الانتهاك والاعتداء

عليها. ولابد لنا من التعرف على ماهية الحق في الخصوصية الرقمية في المطلب الأول، ثم مفهوم الذكاء الاصطناعي وعلاقته بالخصوصية الرقمية في المطلب الثاني.

المطلب الأول:

ماهية الحق في الخصوصية الرقمية

تقتضي دراسة مفهوم الحق في خصوصية المعلومات محاولة تعريفه من خلال الفرع الأول؛ ثم بيان عناصره الفرع الثاني.

الفرع الأول: تعريف الحق في الخصوصية الرقمية

يجد الحق في الخصوصية بصفة عامة صعوبة كبيرة في تحديد تعريف كامل وشامل له، وي رجع ذلك لديناميكية المفهوم، والتطور المستمر لعناصره التي تشمل العديد من الجوانب المتصلة بحياة الأفراد؛ سواء كانت بمفهومها التقليدي المتمثلة في الجسد والمسكن والم ا رسلات...الخ، أو الخصوصية بمفهومها الحديث المرتبط بالتكنولوجيا والمتمثلة في البيانات أو المعلومات الرقمية. وقد أثيرت فكرة خصوصية المعلومات لأول مرة على يد المؤلفين الأمريكيين :الأول آلان ويستون وذلك في كتابه : الخصوصية والحرية، والثاني ميلير ضمن كتابه :الاعتداء على الخصوصية، وبعد الانتشار الواسع لإنشاء بنوك المعلومات وعمليات المعالجة الآلية للبيانات، ووفقا للفقيه ويستن تعد خصوصية المعلومات: حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم ، بينما يعرفها: ميلير على أنها: قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم[1].

1 بولين أنطونيوس أيوب، الحماية القانونية للحياة الخاصة في مجال المعلوماتية دراسة مقارنة، الطبعة1، منشورات الحلبي الحقوقية، لبنان، 2009، ص 59.

وفي هذا السياق يمكن تقسيم الخصوصية إلى عدة مفاهيم ترتبط م ع ا في الوقت ذاته وهي:

1.خصوصية المعلومات والتي تتضمن القواعد التي تحكم جميع إدارارت البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية.

2.الخصوصية الجسدية أو المادية والتي تتعلق بالحماية الجسدية للأفراد ضد أي إجراءات ماسة بالنواحي المادية كفحص المخدرات.

3.خصوصية الاتصالات والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الإلكترون وغيرها من الاتصالات.

4. الخصوصية الإقليمية والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الإلكترونية.

إذن الخصوصية، وبصفة عامة، هي مقياس غير موضوعي، أي يختلف تعريفها وحدودها من بيئة إلى أخرى، بيد أن الصفة المشتركة في جميع هذه التعريفات هي منظور أن الخصوصية إحدى حقوق الإنسان في حياته، ولكنها تعتمد بشكلٍ أساسي على البيئة والسياق .وبنا ء عليه فمفهوم خصوصية المعلومات متوقف على حق الفرد في حفظ سرية معلوماته أثناء المعالجة الآلية للمعطيات الشخصية المتعلقة به، وتقييد استخدامها وفقا للأحكام القانونية المعمول بها، فكلما استطاع الفرد التحكم في خصوصية معلوماته كلما نجح في حمايتها من الانتهاكات التي تقع عليها.

الفرع الثاني: عناصر الحق في الخصوصية الرقمية

مع ظهور التقنيات الذكية، الذكاء الاصطناعي، وتحليل البيانات الضخمة، أصبح مفهوم الخصوصية أكثر تعقيدا من أي وقت مضى .فبعدما كانت المعلومات

الشخصية والأسرار محمية بطبيعتها من الوصول غير المصرح به، باتت اليوم تجمع وتخزن وتنقل عبر الشبكات الرقمية بسرعة وسهولة، مما زاد من التحديات المتعلقة بحمايتها.

يحدد الخبراء عدة عناصر أساسية تشكل الحق في الخصوصية[1]، وهي:

الخصوصية الجسدية: تشمل حق الفرد في حماية جسده مطن أي تدخل غير قانوني، مثل الإجراءات الطبية القسرية، أو المراقبة البيو مترية دون موافقته.

خصوصية السلوك الشخصي: تعني حق الفرد في التصرف بحرية دون التعرض للمراقبة أو التدخل غير المرغوب فيه، سواء في حياته اليومية أو في ممارساته الدينية، السياسية، والاجتماعية.

خصوصية الاتصالات الشخصية: تتعلق بحماية جمي أشكال الاتصالات الخاصة، سواء كانت مراسلات إلكترونية، مكالمات هاتفية، أو بيانات رسائل التطبيقات الحديثة، من التجسس والمراقبة غير القانونية.

خصوصية البيانات الشخصية: تعرف أيضا بخصوصية المعلومات، وتتعلق بحق الفرد في التحكم في كيفية جمع بياناته، وتخزينها، واستخدامها، ومشاركتها.

وفقا للقانون الأوروبي لحماية البيانات (GDPR) ، تشمل البيانات الشخصية أي معلومات يمكن أن تستخدم للتعرف على شخ معين بشكل مباشر أو غير مباشر، مثل:

1 أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات" دراسة مقارنة"، الطبعة 3، دار النهضة العربية، القاهرة،2004 ، ص 35.

الاسم والعنوان.

الصور والمقاط الصوتية.

البيانات الصحية والمعتقدات الدينية.

مع التحولات التكنولوجية، أصبح من الضروري التمييز بين:

- الخصوصية التقليدية التي تتعلق بحماية المسكن، الجسد، والمراسلات الورقية.
- الخصوصية الرقمية التي تركز على حماية البيانات الشخصية المخزنة إلكترونيا، وعمليات تتبع المستخدمين عبر الإنترنت.

ففي العصر الرقمي، تعددت الطرق التي يمكن من خلالها انتهاك الخصوصية، بدءا من المراقبة الجماعية، اختراق البيانات، تتبطط المواقع الجغرافية، وانتهاك سياسات الخصوصية من قبل الشركات الكبرى. يمثل الحق في خصوصية المعلومات أحد أهم الحقوق الأساسية التي تواجه تحديات كبيرة في ظل الثورة الرقمية .فبينما توفر التكنولوجيا الحديثة فرصا هائلة للاستفادة من البيانات، فإنه يعترض الأفراد أي لمخاطر انتهاك الخصوصية وتسريب المعلومات الشخصية .لذا، فإن حماية الخصوصية تتطلب تطوير قوانين حديثة، تعزيز الشفافية، وإيجاد توازن بطين الابتكار التكنولوجي واحترام الحقوق الفردية.

المطلب الثاني:

ماهية الذكاء الاصطناعي وعلاقته بالخصوصية الرقمية

نتناول تعريف الذكاء الاصطناعي في الفرع الأول أما الفرع الثاني نخصصه العلاقة بين الذكاء الاصطناعي والخصوصية الرقمية

الفرع الأول: تعريف الذكاء الاصطناعي

على الرغم من أهمية الذكاء الاصطناعي في عالم التكنولوجيا إلا أنه لا يوجد تعريف جامع مانع متفق عليه للذكاء الاصطناعي، إذ تتعدد التعريفات للذكاء الاصطناعي، فقد عرف البعض الذكاء الاصطناعي على أنه "علم وهندسة صنع الآلات الذكية، وخاصة برامج الحاسب الذكية. إنه مرتبط بالمهمة المماثلة والمتمثلة في استخدام أجهزة الكمبيوتر لفهم الذكاء البشري، غير أن الذكاء الاصطناعي لا يجب أن يقتصر على الأساليب التي يمكن ملاحظتها بيولوجيًا، بينما عرفه البعض الآخر على أنه "قدرة كمبيوتر أو روبوت مدعم بكمبيوتر على معالجة المعلومات والوصول إلى نتائج بطريقة مماثلة لعملية التفكير لدى البشر في التعلم واتخاذ القرارات وحل المشاكل[1] .

وعرف الذكاء الاصطناعي هو عملية محاكاة الذكاء البشري من خلال أنظمة الكمبيوتر، ومحاولة تقليد السلوك البشري، وأساليب التفكير، وأساليب اتخاذ القرار، من خلال دراسة السلوك البشري تجريبيا يحاول محاكاة التفكير البشري من خلال سلوكه، ووضعه في مواقف محددة، ومراقبة ردود الفعل، وأساليب التفكير، والتعامل مع المواقف، وأنظمة الكمبيوتر القوية[2].

[1] غفران محمد إبراهيم هلال، يسرا محمد محمود شعبان، أمال محمد منور نجاح، حوكمة الذكاء الاصطناعي ضمن أحكام القانون الدولي لحقوق الإنسان، مجلة علوم الشريعة والقانون، المجلّد 49، عدد 4، 2022، ص 128.

2 إيهاب خليفة، مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي، ط 1، العربي للنشر والتوزيع ، القاهرة 2019 ، ص 41.

كما يعرف على أنه كيفية إنشاء جهاز كمبيوتر أو روبوت يتحكم فيه جهاز كمبيوتر، أو برنامج، يفكر بذكاء كما يفكر الإنسان الذكي، أو الذكاء الاصطناعي، هو علم إنشاء آلات تقوم بما هو مطلوب[1].

ومع تعدد التعريفات للذكاء الاصطناعي يتم اللجوء إلى تقسيم الذكاء الاصطناعي وفقا لأهدافه الأربعة الأساسية، وذلك في سبيل حصر التعريفات تبعاً لهذه الأهداف. تميّزت هذه الأهداف بين أنواع الذكاء الاصطناعي المبني على أنظمة الكمبيوتر على أساس العقلانية والتفكير مقابل التصرف ويتم تقسيمها إلى النهج البشري والذي ينقسم بدوره إلى الأنظمة التي تفكر مثل البشر والأنظمة التي تتصرف مثل البشر، والنهج المثالي والذي ينقسم إلى الأنظمة التي تفكر بعقلانية والأنظمة التي تعمل بعقلانية[2].

الفرع الثاني: العلاقة بين الذكاء الاصطناعي والخصوصية الرقمية

تعتمد أنظمة الذكاء الاصطناعي، خاصة تلك القائمة على "التعلم الآلي، على البيانات كوقود لتعلم الأنماط واتخاذ القرارات. كلما زادت كمية البيانات وجودتها، زادت دقة النموذج في التنبؤ أو التصنيف أو التفاعل. غير أن جزءا كبيرا من هذه البيانات يتضمن معلومات شخصية وحساسة، مثل البيانات الصحية أو البيو مترية أو سلوكيات المستخدمين على الإنترنت، مما يثير مخاوف جدية تتعلق بحماية الخصوصية وحقوق الأفراد والجهات، إلى جانب قضايا حقوق النشر والملكية الفكرية.

1 عبد الله موسى و احمد حبيب، بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، ط1 ، المجموعة العربية للتدريب والنشر، القاهرة 2019 ، ص 02.

2 غفران محمد إبراهيم هلال، يسرا محمد محمود شعبان، أمال محمد منور نجاح، المرجع السابق، ص 129.

ففي ظل تسارع التطورات التقنية، لم تعد المنافسة في الذكاء الاصطناعي مجرد سباق بين الشركات الكبرى، بل أصبحت ساحة لتنافس استراتيجي شامل بين الدول. هذا التنافس يتقاطع مع أبعاد اقتصادية، وأمنية، وسياسية واجتماعية، حيث تسعى كل دولة إلى ترسيخ نموذجها في كيفية إدارة البيانات والتحكم في التكنولوجيا الحديثة.

في هذا السياق، باتت الدول الرائدة في مجال الذكاء الاصطناعي تدرك أهمية تطوير تشريعات واضحة تنظم استخدام البيانات وتحمي الخصوصية وأن غياب الأطر القانونية الواضحة يشكّل تهديدا مزدوجا. من جهة، قد يؤدي هذا الغياب إلى انتهاكات جسيمة للخصوصية وحقوق الأفراد، ومن جهة أخرى، قد يهدد أمنها القومي وقدراتها علي التنافسية.

وتتضاعف أهمية هذه القوانين في ظل اعتماد تقنيات الذكاء الاصطناعي على كميات هائلة من البيانات الشخصية والسلوكية، مما يجعلها من "التقنيات المزدوجة الاستخدام(Dual-Use Technologies) "، التي يمكن استخدامها لتعزيز التنمية والابتكار، أو في المقابل، لتقويض الأمن القومي إذا استُخدمت بطرق عدائية أو دون رقابة، لذلك، فإن تقنين استخدام الذكاء الاصطناعي لم يعد خيارا تشريعيا فقط، بل ضرورة استراتيجية لحماية الأمن والسيادة الرقمية[1].

[1]https://www.aljazeera.net/tech/2025/5/4/%D9%82%D9%88%D8%A7%D9%86%D9%8A%D9%86-%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9-%D9%88%D8%AD%D9%88%D9%83%D9%85%D8%A9-%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%B3%D8%A7%D8%AD%D8%A9 تاريخ الاطلاع: 10.10. 2025

المبحث الثاني: الجهود المبذولة لحماية الحق في الخصوصية الرقمية من مخاطر الذكاء الاصطناعي

لقد كرست العديد مطط المواثيق الدولية والإقليمية، وكذلك القوانين الوطنية، حماية الحق في الخصوصية بمفهومه التقليدي والمعلوماتي .وتعتبر هذه النصوص القانونية هي الأساس الذي تبنى عليه أي جهود لمواجهة التحديات الجديدة التي يطرحها الذكاء الاصطناعي .يستعرض هذا المبحث هذه الحماية من خلال مطلبين، يتناول الأول الجهود الدولية والإقليمية، ويتناول المطلب الثاني نماذج من التشريعات الوطنية.

المطلب الأول: الجهود الدولية لحماية الحق في الخصوصية من مخاطر الذكاء الاصطناعي

أثارت مسألة حماية الخصوصية المعلوماتية اهتمام مختلف المنظمات الدولية والإقليمية، التي سعت إلى وضع معايير مشتركة لتحقيق التوازن بين حرية تدفق المعلومات وحماية حقوق الأفراد.

أولاً :منظمة التعاون الاقتصادي والتنمية(OECD)

تعتبر المبادئ التوجيهية التي أصدرتها المنظمة في عام 1980 بشأن حماية الخصوصية وتدفق البيانات عبر الحدود، من أقدم وأهم النصوص في هذا المجال . وعلى الرغم مطن أنها غير ملزمة، إلا أنها شكلت الأساس للعديد من التشريعات الوطنية اللاحقة، وهدفت إلى تحقيق توازن بين حماية حق الخصوصية وتشجع التدفق الحر للبيانات الضروري للتجارة الدولية.

ثانيا: المجلس الأوروبي

لعب المجلس الأوروبي دورا رائدا في هذا المجال .فقد أصدر الاتفاقية رقم 108لسنة 1981 ، والتي تعتبر أول صك قانوني دولي ملزم بشأن حماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطاب الشخصي .تهدف هذه الاتفاقية إلى حماية كرامة وحقوق الأفراد، بغض الن ر عن جنسيتهم أو مكان إقامتهم، فيما يتعلق بمعالجة بياناتهم الشخصية 2 وقد تم تحديث هذه الاتفاقية مؤخرا بموجب البروتوكول المعروف باسم Convention 108+ لمواكبة التحديات الجديدة التي يطرحها العصر الرقمي، بما في ذلك الذكاء الاصطناعي والبيانات الضخمة.

ثالثا: منظمة الأمم المتحدة

أكدت الجمعية العامة للأمم المتحدة مرارا على أن الحقوق التي يتمت بها الأفراد خارج الإنترنت يجب أن تحمى أيضاق داخله .وفي هذا السياق، أصدرت قرارات مهمة، منها:

القرار 68_-167 (2013) هو أول قرار يعالج، بشكل مباشر" الحق في الخصوصية فطي العصر الرقمي"، حيث أعرب عن القلق العميق إزاء انتشار الآثار السلبية للمراقبة الرقمية وجمع البيانات الشخصية على حقوق الإنسان

القرار 73-178 (2018) عزز هذا القرار الحماية، ووسط نطاق الخصوصية ليشمل" البيانات المستنتجة "التي يتم جمعها وتحليلها بواسطة الخوارزميات، ونبه إلى أن مجرد المراقبة السرية لبيانات الأفراد الشخصية قد يشكل انتهاكاك لحقهم في الخصوصية.

رابعا: اتفاقية بودابست للجرائم السيبرانية (2001)

على الرغم من أن تركيزها الأساسي هو مكافحة الجرائم الإلكترونية، إلا أن هذه الاتفاقية، التي أبرمت برعاية المجلس الأوروبي، تضمنت أحكاما مهمة تتعلق بالإجراءات الجنائية في البيئة الرقمية، من التأكيد على ضرورة الموازنة بين احتياجات إنفاذ القانون وحماية الحقوق الأساسية، بما في ذلك الحق في الخصوصية .وتهدف إلى تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية عبر سياسات مشتركة[1] .

خامسا :الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010)

أبرمت هذه الاتفاقية في القاهرة عام 2010 بهدف تعزيز التعاون بين الدول العربية فطي مجال مكافحة الجرائم المعلوماتية .وقد سارت على نه، المن مات الدولية في التأكيد على احترام حقوق الأفراد وحرياتهم الأساسية، بما في ذلك الحق في الخصوصية، أثناء إجراءات التحقيق والملاحقة في هذا النوع من الجرائم[2]. تشتكل هذه المواثيق الدولية والإقليمية إطارا مرجعيا مهما، وتضبط التزامات على الدول لسن تشريعات وطنية تضمن حماية فعالة للخصوصية في العصر الرقمي.

المطلب الأول: الجهود الوطنية لحماية الحق

في الخصوصية من مخاطر الذكاء الاصطناعي

التزاما بالمواثيق الدولية، وتلبية للحاجة الملحة لحماية مواطنيها فطي الفضاء الرقمي، سنت العديد من الدول تشريعات وطنية متخصصة في حماية

1 اتفاقية بودابست بشأن جرائم الفضاء الإلكتروني، 2001.

2 الاتفاقية العربية لمحاربة جرائم تقنيات المعلومات، المحررة في القاهرة 2010.

البيانات الشخصية في بداية الأمر ثم تشريعات خاصة بالذكاء الإصطناعي[1]؛ وسوف نستعرض موقف المشرع الفرنسي والتشريعات العربية وأخيرا موقف المشرع الجزائري

أولاً : التشريع الجزائري

عمد المشرع الجزائري على سن قوانين خاصة لمكافحة الجرائم الإلكترونية، مثل:

الأمر رقم 15-04 يحدد قواعد حماية البيانات الشخصية والتوقيع الإلكتروني[2] ، كذلك القانون رقم 18 - 07 لعام 2018 يعزز حماية الأفراد ضد الجرائم الرقمية وسرقة البيانات[3].

التشريع الفرنسي

يعتبر المشرع الفرنسي من الرواد في هذا المجال، حيث أصدر القانون المتعلق بالمعلوماتية والملفات والحريات[4]، وقد تم تعديل هذا القانون عدة مرات لمواكبة

1 منذ إنشاء مركز الذكاء الاصطناعي والروبوتات لدى الأمم المتحدة اتجه عدد من الدول إلى تبني سياساتها وخططها الاستراتيجية على المستوى الداخلي لتنظيم تطوير الذكاء الاصطناعي. فبالرجوع إلى الجدول الزمني للوثائق الاستراتيجية لحوكمة وتنظيم الذكاء الاصطناعي نجد أن بعض الدول، مثل كندا وفنلندا، طورت استراتيجياتها الوطنية للذكاء الاصطناعي في وقت مبكر منذ عام 2017، وتبعتها عن كثب اليابان وفرنسا وألمانيا والمملكة المتحدة في عام 2018، ومن ثم تم اعتماد استراتيجية وطنية للذكاء الاصطناعي من قبل دول أخرى، مثل البرازيل والمجر وبولندا وإسبانيا.

2 قانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 01 فبراير سنة 2015. يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

3 قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018. يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

4 القانون رقم 17- 78 لسنة 1978 المتعلق بالمعلوماتية والملفات والحريات الفرنسي.

التطورات التكنولوجية، ويهدف إلى حماية بيانات الأفراد الشخصية فطدي سياق المعالجة الآلية .وقد وضع القانون مجموعة مطتن المبادئ الأساسية لجمع البيانات ومعالجتها، مثل مبدأ الشرعية والنزاهة والشفافية، وأنشأ هيئة مستقلة للإشراف على تطبيق القانون.

ثانيا: التشريعات العربية

سعت العديد من الدول العربية إلى تحديث أطرها القانونية لمواجهة تحديات العصر الرقمي .ومطن أبرز الأمثلة:

المشرع التونسي : أصدر القانون رقم 63 لسنة 2004 المتعلق بحماية المعطيات الشخصية[1]، والذي يعتبر من القوانين المتقدمة في المنطقة.

المشرع الإماراتي :أصدر المرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، وهو قانون شامل وحديث يتماشى م أفضل الممارسات الدولية[2].

الخاتمة:

الذكاء الاصطناعي هو الشكل الجديد للحضارة الإنسانية، فإذا ما اعتبرنا أن التوجه الرسمي لتطوير تقنيات الذكاء الاصطناعي لا تستهدف استبدال الذكاء البشري، وإنما تسخير العلم والطبيعة لخدمة المجتمع البشري، فإنه لابد من أن نتأكد من تطويره من خلال نهج إنساني قائم على القيم الأخلاقية واحترام حقوق

1 قانون أساسي عدد 63 لسنة 2004 مؤرخ في 27 جويلية 2004 يتعلق بحماية المعطيات الشخصي التونسي.

2 مرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصي الاماراتي.

الإنسان منها الحق في الخصوصية. وقد قيمنا في سياق دراستنا هذه أهم الفرص والمخاطر التي يشكلها الذكاء الاصطناعي على الحق في الخصوصية.

بناء على ما تقدم سابقا، خلصنا إلى التأكيد على أهمية وجوب تطوير تقنيات الذكاء الاصطناعي من خلال نهج قائم على قيم أخلاقية راسخة ومبادئ احترام الحق في الخصوصية.

قائمة المراجع:

الاتفاقيات الدولية:

1- الاتفاقية العربية لمحاربة جرائم تقنيات المعلومات، المحررة في القاهرة 2010.

2- اتفاقية بودابست بشأن جرائم الفضاء الإلكتروني، 2001.

القوانين:

1- قانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 01 فبراير سنة 2015. يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

2- قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018. يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

3- القانون رقم 78 -17 لسنة 1978 المتعلق بالمعلوماتية والملفات والحريات الفرنسي.

4- قانون أساسي عدد 63 لسنة 2004 مؤرخ في 27 جويلية 2004 يتعلق بحماية المعطيات الشخصي، التونسي.

5- مرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصي الاماراتي.

الكتب:

1- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات "دراسة مقارنة"، الطبعة 3، دار النهضة العربية، القاهرة، 2004.

2- إيهاب خليفة، مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي، ط1 ، العربي للنشر والتوزيع ، القاهرة 2019 .

3- بولين أنطونيوس أيوب، الحماية القانونية للحياة الخاصة في مجال المعلوماتية دراسة مقارنة، الطبعة 1، منشورات الحلبي الحقوقية، لبنان، 2009.

4- عبد الله موسى و احمد حبيب، بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، ط 1، المجموعة العربية للتدريب والنشر، القاهرة، 2019 .

المقالات العلمية:

1- غفران محمد إبراهيم هلال، يسرا محمد محمود شعبان، أمال محمد منور نجاح، حوكمة الذكاء الاصطناعي ضمن أحكام القانون الدولي لحقوق الإنسان، مجلة علوم الشريعة والقانون، المجلّد 49، عدد 4، 2022.

مو اقع الانترنت:

1- https://www.aljazeera.net/tech/2025/5/4/%D9%82%D9%88%D8%A7%D9%86%D9%8A%D9%86-%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9-%D9%88%D8%AD%D9%88%D9%83%D9%85%D8%A9-%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%B3%D8%A7%D8%AD%D8%A9

مكافحة الجريمة الالكترونية في الجزائر: بين التأصل القانوني والتنظيم الاجرائي

Combating Cybercrime in Algeria: Between Legal Foundation and Procedural Organization

بوهنتالة ياسين/ مخبر افاق الحوكمة للتنمية المحلية المستدامة، المركز الجامعي الشهيد سي الحواس بريكة، الجزائر معهد الحقوق والعلوم الاقتصادية المركز الجامعي سي الحواس بريكة.

yacine.bouhentala@cu-barika.dz

زيبار الشاذلي/ مخبر افاق الحوكمة للتنمية المحلية المستدامة، المركز الجامعي الشهيد سي الحواس بريكة، الجزائر معهد الحقوق والعلوم الاقتصادية المركز الجامعي سي الحواس بريكة.

chadli.zibar@cu-barika.dz

ملخص:

نسلط الضوء من خلال هذه الدراسة على الاطار القانوني والاجرائي لمكافحة الجريمة الالكترونية في الجزائر، من خلال تحليل الأسس التشريعية التي تقوم عليها، وتحديد الجهات الأمنية وعير الأمنية المتدخلة في في مكافحتها، وكذا ابراز فعالية هذه المنظومة في مواجهة هذا النوع المستحدث من الجرائم، خاصة من حيث وضوح التجريم، وتوزيع الاختصاصات، والتنسيق بين الجهات المعنية.

الكلمات المفتاحية: الجريمة الالكترونية، الجريمة المعلوماتية، تكنولوجيا الاعلام والاتصال

Abstract:

This study sheds light on the legal and procedural framework for combating cybercrime in Algeria, through an analysis of its underlying legislative foundations and the identification of both security and non-security bodies involved in the fight against it. It also aims to highlight the effectiveness of this system in addressing this emerging type of crime, particularly in terms of the clarity of criminalization, the distribution of responsibilities, and coordination among the relevant authorities

key words: *Cybercrime, Computer Crime, Information and Communication Technology*

مقدمة:

اظهر التطور السريع لتنكولوجيا المعلومات والاتصالات أنماط جديدة للسلوك الاجرامي تجاوزت الحدود الجغرافية، واكتسبت طابع غير تقليدي، وهو ما يسمى بالجريمة الالكترونية، هذه الظاهرة الاجرامية التي أصبحت تشكل خطر مباشر على الدول والافراد، ما جعلها من بين أكبر التحديات التي تواجه المنظومة القانونية والأمنية، نظرا للخصائص التي تميزها من حيث طبيعة الشخص الجاني المرتكب لها أو من حيث اثارها واضرارها وبصورة خاصة البيئة الرقمية التي ترتكب فيها.

والجزائر كغيرها من الدول المهددة بخطر الجرائم الالكترونية، سارعت الى إرساء إطار قانوني يساير هذه الجريمة المستحدثة من خلال تجريم الأفعال الالكترونية بصورة دقيقة، وتحديد اليات المتابعة والتحقيق من خلال تعديل قانون العقوبات، وإصدار قوانين خاصة، كما ان طبيعة الجريمة الالكترونية وخصوصيتها من حيث وسيلة ارتكابها وصعوبة اثباتها وتعقب مرتكبها شكل تحديا مضاعفا على الأجهزة المختصة، ما يقتضي وجود تنسيق فعال بين الأجهزة الأمنية وغير الأمنية على أساس قانوني مؤسساتي شامل.

ومن هنا تبرز أهمية الموضوع كونه يعالج مسألتين جوهريتين في محاربة الجريمة الالكترونية الأولى وهي وجود إطار قانوني يحدد هذه الجريمة ويبين طبيعتها واهم خصائصها هذا من جهة، ويحدد الأفعال التي تدخل في دائرة التجريم والعقوبات المقررة لها، والثانية هي الجانب الاجرائي سواء من حيث تحديد الجهات التي توكل اليها مهمة معالجة وحماية المعطيات الشخصية وكذا البحث والتحري في هذه الجرائم.

ومن هنا تطرح هذه الدراسة الإشكالية الاتية: هل يحقق الإطار القانوني والاجرائي في التشريع الجزائري الفعالية والكفاية في مواجهة الجريمة الالكترونية؟

للإجابة على هذه الإشكالية نتبع المنهج الوصفي التحليلي، من حيث تحليل الإطار القانوني المنظم للجريمة الالكترونية ودراسة الجوانب الإجرائية والمؤسساتية المرتبطة بها.

للإجابة على هذه الإشكالية قسمنا هذه الدراسة الى مبحثين:

المبحث الأول: الأساس القانوني للجريمة الالكترونية.

المبحث الثاني: الجوانب الإجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري.

المبحث الأول:

الأساس القانوني للجريمة الالكترونية

لقد افرزت الثورة التكنولوجية وما ينبثق عنه من ثورة رقمية في العقود الأخيرة جملة من التحديات في مختلف المجالات، بما في ذلك المجال القانوني، ومن أبرز هذه التحديات الجريمة الالكترونية التي يتخذ من الفضاء الرقمي بيئة له، وهو ما جعلها تختلف عن الجرائم التقليدية سواء من حيث الأفعال المكونة لها او من حيث الضرر الناتج عنها أو من حيث الجاني المرتكب لها.

المطلب الأول:

ماهية الجريمة الالكترونية:

قبل التطرق الى القواعد الموضوعية التي تحكم الجرائم الالكترونية، يتوجب علينا أولا ان بين المقصود بها واهم الخصائص التي تميزها.

الفرع الأول: تعريف الجريمة الالكترونية:

لم يتفق الفقه على وضع تسمية موحدة للجريمة الالكترونية، فمنهم من يطلق عليها الجريمة المعلوماتية، ومنهم من يطلق عليها تسمية الجرائم الالكترونية ومنهم من يطلق عليها جرائم إساءة استعمال تكنولوجيا المعلومات والاتصال، ومنهم من أطلق عليها جرائم السيبر أو جرائم الانترنت.

ويرجع سبب الاختلاف في التسمية للاجتهادات الفقهية فمنهم من نظر الى هذه الجرائم من زاوية تقنية ومنهم من نظر اليها من زاوية قانونية وعليه ظهرت عده اتجاهات فقهية مختلفة حول المعيار الذي يمكن اعتماده لوضع تعريف محدد للجريمة[1].

أولا: التعريف الضيق للجريمة الالكترونية

يركز الجانب الذي تبنى التعريف الضيق على الجرائم التي ترتكب باستخدام الوسائل المعلوماتية كأداة رئيسية لتنفيذ الفعل الاجرامي، ويستند الى معايير مختلفة أهمها:

[1] - مرفت محمد حبايبة، مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري للنشر والتوزيع، الأردن، د.ط، 2022، ص 30.

- **معيار الوسيلة المستعملة في ارتكاب الجريمة**

حيث عرفت " الجريمة الالكترونية هي كل شكل من اشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"[1].

وعرفها "MEREWE" بأنها " الفعل غير المشروع يتورط في ارتكابه الحاسب الالي"[2].

كما يعرفها الفقيه الألماني تاديمان "Tiedemann" على انها:" كل اشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب"[3].

- **معيار معرفة الجاني بتكنولوجيا المعلوماتية**

وهو معيار شخصي يربط بين شخص الجاني ومدى تحكمه ومعرفته بتقنية المعلوماتية كون ان هذا النوع من الجرائم يتطلب المام بمجال الحاسوب والمعلوماتية.

من بين الذين اخذوا بهذا المعيار الفقيه البلجيكي سيتن ستشيولبيرج "Stein Schiollberg" الذي عرفها بأنها:" أي فعل غير مشروع تكون المعرفة بتقنية الكومبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا"[4].

---

[1] زهراء عادل سلبي، الابتزاز الالكتروني (دراسة مقارنة)، دار الأكاديميون للنشر والتوزيع، الأردن، د.ط، 2021، ص28.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، ط 02، 2010، ص48.

[3] محمود مدين، فن التحقيق والاثبات في الجرائم الالكترونية، المصرية للنشر والتوزيع، القاهرة، ط01، 2020، ص27.

[4] مرفت محمد حبايبة، المرجع السابق، ص 33.

كما عرفها الدكتور هشام فريد بأنها:" فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لارتكابه"[1]

كما تعرف أيضا بأنها:" الجرائم التي يتطلب الماما خاصا بتقنيات الحاسب ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها"[2]

- **معيار موضوع الجريمة أو محل الجريمة:**

والذي هو الحاسوب او النظام المعلوماتي.

ومن بين أهم هذه التعريفات:" لي ستانس وفيفانت ' Le Staince and vivant" حيث عرفا الجريمة الالكترونية على أنها: " مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن ان تكون جديرة بالعقاب"[3].

ويعرفها أيضا "Rosenblatt" على أنها نشاط: غير مشروع موجه لنسخ او تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[4]

[1] مختارية بوزيدي، ماهية الجريمة الالكترونية، اعمال الملتقى الوطني: اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 29 مارس 2017، الجزائر العاصمة، منشورة من قبل مركز جيل البحث العلمي، 2017، ص09.

[2] ايمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ط 01، 2014، ص

[3] مرفت محمد حبايبة ، المرجع السابق، ص32.

[4] شريف حسين محمد، القانون الواجب التطبيق على الجريمة الالكترونية، المصرية للنشر والتوزيع، القاهرة، د.ط، 2021، ص 21.

ثانيا: التعريف الموسع

في ظل عدم إمكانية حصر نطاق الجرائم الالكترونية اعتمادا على التعريف الضيق خاصة وان الحاسوب الذي استند اليه العديد من الفقهاء كمعيار لتعريف الجريمة الالكترونية لم يعد كذلك في ظل ظهور وسائل الاتصال الحديثة مثل الهواتف الذكية، ما جعل العديد من الفقهاء يتجهون نحو اعتماد تعريف موسع،[1] حيث ذهب الفقيهان (Michel&Credo) الى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة الى الى الولوج غير المصر به الى الأجهزة و البيانات كما تشمل الاعتداءات على الأجهزة المادية مثل بطاقات الائتمان والتلاعب في ماكينات الحسابات الالية، وتزوير مكونات الحاسب، وكذلك سرقة الحاسب او مكوناته[2].

كما عرفت الجريمة الالكترونية بأنها " كل فعل يرتكب من شخص كامل الاهلية باستخدام الحاسب الالي أو شبكة الانترنت يلحق الضرر والأذى بالغير، وان يقع على الحاسب الالي نفسه ويكون هذا الفعل معاقبا عليه بالقانون"[3]

وتعرف أيضا:" كل سلوك إيجابي او سلبي يقترف بوسيلة معلوماتية لاعتداء على حق او مصلحة يحميها القانون، اما بغية احداث الضرر على مكونات الوسيلة المعلوماتية أو مضمونها"[1].

[1] دمان ذبيح عماد، بهلول سمية، الاليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد 13، جانفي 2021، ص140.

[2] عبد العال الدريبي، الجرائم الالكترونية دراسة قانونية قضائية مع أحدث التشريعات العربية في مجال مكافحة الجريمة المعلوماتية والانترنت، المصدر القومي للإصدارات القانونية، القاهرة، ط 01، 2012، ص41.

[3] مرفت محمد حبايبة ، المرجع السابق، ص36.

ونرى لوضع تعريف جامع وشاكل للجريمة الالكترونية يراعي في ذلك الابعاد القانونية والتقنية ويأخذ بعين الاعتبار الاختلافات الفقهية فانه يمكننا تعريفها على أنها كل سلوك غير مشروع معاقب عليه قانونا يرتكب باستخدام أي وسيلة تكنولوجية رقمية كالحاسوب أو شبكة الانترنت أو أي نظام معلومات، او كانت هذه الأجهزة وسيلة لتنفيذ هذه الجريمة، وهو الامر الذي يتطلب في الغالب ان يكون القائم بهذه الأفعال ملما بتقنيات المعلوماتية.

ثالثا: تعريف المشرع الجزائري للجريمة الالكترونية:

أطلق المشرع الجزائري على الجريمة الالكترونية تسمية المساس بأنظمة المعالجة الالية للمعطيات وعرفها بموجب المادة 02 من القانون 09-04 على أنها" جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أز يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية". ما يلاحظ على هذا التعريف ان المشرع الجزائري[2]:

- جمع من خلاله بين عدة معايير أولها معيار الوسيلة المتمثل في نظام الاتصالات الالكترونية ومعيار موضوع الجريمة المتمثل في المساس بأنظمة المعالجة الالية للمعطيات، وأخيرا معيار توافر الركن الشرعي للجريمة.

[1] هيثم عبد الرحمان البقلي، الجرائم الالكترونية الواقعة على العرض بين الشريعة والقانون المقارن، دار العلوم للنشر والتوزيع، مصر، د.ط، 2010، ص15.

[2] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، كلية الحقوق والعلوم السياسية، جامعة المسيلة، العدد 11، 2018، ص353.

- حدد نطاق الجريمة الالكترونية حيث نص على انها كل جريمة ترتكب او يسهل ارتكابها في نظام معلوماتي موسعا بذلك من نطاق مجال ارتكاب الجرائم الالكترونية.

الفرع الثاني: السمات المميزة للجريمة الالكترونية

تعتبر الجريمة الالكترونية من الجرائم المستحدثة والتي لها خصوصية تميزها عن الجرائم التقليدية، ويمكن اجمال اهم هذه الخصائص فيما يلي:

أولا: الطابع العابر للحدود للجريمة الالكترونية

يستخدم الجاني في ارتكابه للجريمة الالكترونية وسائل تقنية، ما يمكنه من ارتكاب جريمته من أي مكان في العالم، مما يصعب من عملية تتبعه والتحقيق معه، فالشبكة المعلوماتية تتيح للجاني عبور الحدود الوطنية للدول والقارات دون قيود جغرافية، مما يخلق تحديات قانونية في مجال المكافحة الدولية لهذه الجرائم سواء من حيث الدولة صاحبة الاختصاص او من حيث القانون الواجب التطبيق او من إجراءات المتابعة والتحقيق، وفي ظل الاضرار التي تخلفها هذه الجرائم تعالت الأصوات للمناداة بضرورة التعاون الدولي من اجل مكافحة هذه الجريمة عن طريق ابرام اتفاقيات ومعاهدات دولية. و في هذا الصدد صادقت الجزائر على الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية والتي نصت في المادة 21 منها على تجريم ارتكاب او المشاركة في ارتكاب الأفعال التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لتغطية أنظمة المعلومات[1].

[1] مرفت محمد حبايبة، المرجع السابق، ص 42.

ثانيا: صعوبة ملاحقة الجاني والتأكد من هويته (صعوبة الاثبات)

ان معرفة الجاني بتقنية المعلومات يجعله يستخدم وسائل جد متطورة لإخفاء هويتهم، مثل الشبكات الخاصة الافتراضية (VPN)، وتقنية إخفاء العناوين الرقمية (IP SPOOFING) و أداوت التشفير، مما يجعل تجعل تعقبهم اشد تعقيدا مقارنة بالمجرمين التقليديين اذ لا تخلف الجرائم الالكترونية ادلة مادية واضحة كالحمض النووي أو البصمات أو الشهود، الامر الذي يزيد من صعوبة اثباتها[1].

ثالثا: المجرم الالكتروني يختلف عن الصورة التقليدية للجاني

حيث اصبح المجرم على درجة عالية من الذكاء، نتيجة المامه بالجوانب التقنية ومواكبته لتطور التكنولوجي، وما يميز الجاني هنا انه قلما يكون محترفا للإجرام او عائدا، حتى أنه لا ينظر اليه كمجرم بالمعنى المتعارف عليه في صورته التقليدية، وذلك لاختلاف الأسباب والعوامل التي تقف وراء ارتكاب هذه الجريمة[2].

رابعا: وقوع الجريمة في بيئة المعالجة الالية للبيانات والمعلومات

يشترط لقيام الجريمة الالكترونية التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي وذلك من اجل معالجتها الكترونيا بما يسمح للمستخدم إمكانية كتابتها من خلال العمليات المتبعة والتي يتوافر فيها إمكانية تصحيحها او تعديلها او محوها او تخزينها او استرجاعها او طباعتها[3].

---

[1] دعاء عبد العال، خالد عبد الحق، الجرائم الالكترونية والتحقيقات الجنائية، دار اليازوري للنشر والتوزيع، الأردن، د.ط، 2025، ص18.

[2] بونعارة ياسمينة، الجريمة الالكترونية، مجلة المعيار، كلية أصول الدين، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، العدد 39، 2015، ص282.

[3] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العراق، العدد07، 2008، ص115

خامسا: جسامة الضرر المترتب على الجريمة الالكترونية

اكدت الشركة العالمية المتخصصة في تقنيات حماية أمن المعلومات، أن قطاعات الاعمال العالمية تتكبد خسائر سنوية تصل الى 400 مليار دولار امريكي، كما أوضحت الشركة ان الهجمات الالكترونية أصبحت تشكل اقتصادا متناميا قائما بذاته تبلغ قيمته ما بين 2 الى 3 تريليون دولار سنويا[1].

فالجاني يمكنه الوصول الى البيانات الخاصة بالشركات والبنوك والمؤسسات المالية الوطنية او العالمية والمساس بها اما بتحويل أموال او الحاق اضرار بقواعد البيانات الخاصة بها مما يكبد هذه المؤسسات خسائر مالية ضخمة.

سادسا: قلة التبليغ عن الجرائم الالكترونية

في العديد من الجرائم الالكترونية لا يتم التبليغ عنها لعدة أسباب منها الأسباب النفسية والاجتماعية المتمثلة في الحرج والخوف من الفضيحة مثلما هو الامر في جرائم الابتزاز الجنسي أو الولوج الى الحسابات الشخصية، او لأسباب قانونية مثل طول الإجراءات القضائية وتعقيدها، واما لأسباب تقنية كعدم ادراك الضحية بوقوع الجريمة مثل التجسس الالكتروني[2].

[1] بونعارة ياسمينة، المرجع السابق، ص282.

[2] هشام بشير، الاليات الدولية لمكافحة الجريمة الالكترونية، المركز الدولي للدراسات المستقبلية والاستراتيجية، القاهرة، د.ط، 2012، ص11.

المطلب الثاني: الإطار القانوني لتجريم الأفعال الالكترونية في التشريع الجزائري

في سبيل مكافحة الجرائم المستحدثة وبصفة خاصة تلك الناتجة عن التطور التكنولوجي، اتجه المشرع الجزائري الى سن نصوص قانونية تجرم الأفعال الالكترونية لسد الفراغ التشريعي في هذا المجال سواء من خلال نصوص قانون العقوبات او في القوانين الخاصة ذات الصلة.

الفرع الأول: الاحكام الواردة في قانون العقوبات الجزائري

جرم المشرع الجزائري الجريمة الالكترونية في قانون العقوبات بموجب القانون 15/04 المؤرخ في 10 نوفمبر2004[1]، حيث أضاف القسم السابع بعنوان"المساس بأنظمة المعالجة الالية للمعطيات" والذي تضمن ثمانية مواد من المادة 394 مكرر الى المادة 394 مكرر8، والذي كان محل تعديل بموجب القانون 24-06 المؤرخ في 28 أفريل 2024 [2]أين شدد المشرع من خلاله العقوبات المقررة لهذه الجرائم.

وقد تضمن قانون العقوبات بموجب هذه المواد الجرائم الاتية[3]:

- الغش او الشروع فيه، في كل او جزء من المنظومة للمعالجة الالية للمعطيات.

[1] القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر 155/66، المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج.ر، العدد 71، 2004.

[2] القانون 24-06 المؤرخ في 28 افريل 2024 المعدل و المتمم للامر 155/66، المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج.ر، العدد 30، 2024.

[3] راضية عميمور، الجريمة الاكترونية واليات مكافحتها في التشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، العدد01، 2022، ص ص: 96-97.

- حذف أو تغيير لمعطيات المنظمة
- ادخال او تعديل في نظام المعطيات.
- تصميم او بحث او تجميع او توفير او نشر او الاتجار.
- حيازة او افشاء او نشر أو استعمال المعطيات.
- تكوين جماعة اشرار.

إضافة الى جريمة تجنيد الأشخاص لصالح إرهابي أو منظومة إرهابية باستخدام وسائل تكنولوجيا الاعلام والاتصال والتي تعتبر جناية استحدثها المشرع بموجب القانون 16-02 المتضمن تعديل قانون العقوبات.

الفرع الثاني: الاحكام الواردة في القوانين الخاصة

نظرا لخصوصية الجريمة الالكترونية وتشعبها بحيث ان استخدام التكنولوجيا كوسيلة لارتكاب الجريمة ليس محصور في نوع او مجال محدد، لذلك حاول المشرع الجزائري افراد قانون خاص بالجريمة الالكترونية، كما نجد العديد من النصوص الخاصة في القوانين الخاصة الأخرى.

أولا: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

تضمن القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها مجموعة من القواعد تجمع بين القواعد الإجرائية

المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية للوقوف دون وقوع هذه الجريمة والكشف عن مركبيها[1].

ومن بين ما تضمنه القانون 09-04، السالف الذكر، التزام مقدمي الخدمات بالتعاون مع السلطات القضائية في جمع وتسجيل بيانات الاتصالات، وحفظ معلومات حركة السير لتمكين تلك السلطات من استخدامها في التحريات وعدم الالتزام بهذه المسؤوليات يعرض الافراد والشركات للمسؤولية الجنائية، فيعاقب الشخص الطبيعي بالحبس من ستة (6) اشهر الى خمس (5) سنوات، وغرامة من 50.000دج الى 500.000 دج ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات[2].

ثانيا: قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي رقم 18-07

سعى المشرع الجزائري من خلال القانون 18-07 الى ضمان حماية الحقوق والحريات الفردية عند جمع ومعالجة المعطيات ذات الطابع الشخصي، حيث يتم ذلك وفق وفقا إجراءات قانونية، وضمن الأغراض المرخص لها، في اطار المدة المحددة قانونا، ويعد أي تجاوز لهذه الضوابط، سواء في الجمع او المعالجة أو الحفظ، جريمة يعاقب عليها القانون، كما يلزم المسؤولون عن معالجة هذه

[1] رمزي حوحو، منيرة بلورغي، مواجهة الجريمة المعلوماتية في الجزائر، مجلة الحقوق والحريات، كلية الحقوق والعلوم السياسية جامعة بسكرة، العدد 02، 2014، ص58.

[2] بن مالك أحمد، خصوصية الجريمة المعلوماتية وسيل مكافحتها في التشريع الجزائري، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة تسمسيلت، العدد 02ن2023، ص953.

المعطيات بالتقيد بالاستخدام المشروع لها، واي انحراف عن ذلك يعد فعلا مجرما قانونا ومن اهم الجرائم التي نص عليها القانون 18-07 في هذا الخصوص[1]:

- الجرائم المرتبطة بطريقة جمع المعطيات ذات الطابع الشخصي او بطبيعتها ومن صورها الجريمة المرتبطة بطريقة جمع هذه المعطيات، حيث جرم المشرع الجزائري الأساليب غير المشروعة في جمع المعطيات الشخصية بموجب نص المادة 59 كم القانون 18-07، اين قرر عقوبة الحبس بين سنة (01) الى ثلاث (03) سنوات وغرامة من 100.00 الى 300.00 كل من يقوم بجمع المعطيات ذات الطابع الشخصي بطريقة تدليسية او غير نزيهة او غير مشروعة. ومن بين صورها أيضا الجريمة المرتبطة بطبيعة المعطيات ذات الطابع الشخصي محل الجمع حيث عاقب المشرع الجزائري بموجب المادة 68 كل من يقوم في غير الحالات المنصوص عليها قانونا بوضع او حفظ في الذاكرة الالية المعطيات ذات الطابع الشخصي بخصوص او جرائم او ادانات او تدابير امن بعقوبة من ستة (06) أشهر الى ثلاث (03) سنوات وبغرامة من 60.000 الى 300.000 دج.

- جرائم المساس بشروط التصريح المرتبطة بالمعطيات الشخصية والمتمثلة في جريمة استعمال المعالجة لأغراض غير مصرح بها والتي جرمها المشرع بموجب نص المادة 58 من القانون 18-07 حيث عاقب كل من يقوم بإنجاز او استعمال معطيات لأغراض أخرى غير تلك المصرح بها او المرخص بها بعقوبة الحبس من ستة (06) أشهر الى سنة (01) وبغرامة من 60.000دج الى 100.000 دج أو بإحدى هاتين العقوبتين. وكذا جريمة الاحتفاظ بالمعطيات الشخصية خارج المدة المحددة المعاقب عليها وفقا لنص المادة 65

[1] مليايي عبد الوهاب، الجرائم الماسة بالمعطيات الشخصية على ضوء القانون رقم 18-07، مجلة البحوث القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، العدد 01، 2023، ص-ص: 279-280.

الفقرة الثانية حيث يعاقب كل من يقوم بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها قانونا.

- جريمة المساس بالسر المهني المرتبطة بالمعطيات الشخصية والتي تأخذ صورة جريمة السماح لغير المؤهلين بالولوج الى المعطيات الشخصية المجرمة بنص المادة 60 من القانون 18-07 والتي تعاقب على ذلك بعقوبة الحبس من سنتين (02) الى خمس (05) سنوات وغرامة من 200.000 الى 500.00. و الصورة الثانية هي جريمة افشاء معلومات المجرمة بنص المادة 62 من القانون 18-07 اين عاقب المشرع الجزائري بموجبها كل من افشى معلومات محمية بموجب هذا القانون بالعقوبات المنصوص عليها في المادة 301 من قانون العقوبات، أما الصورة الثالثة فهي جريمة التسبب او التسهيل للاستعمال التعسفي أو التدليسي للمعطيات الشخصية حيث يعاقب كل مسؤول عن معالجة وكل معالج من الباطن وكل شخص مكلف، بالنظر الى مهامه، بمعالجة معطيات ذات طابع شخصي يتسبب او يسهل ، ولو عن اهمال، الاستعمال التعسفي او التدليسي للمعطيات المعالجة او المستلمة او يوصلها الى غير المؤهلين لذلك.

ثالثا: القانون المتعلق بالتوقيع والتصديق الالكترونيين

صدر القانون رقم 15-04 المحدد للقواعد المتعلقة بالتوقيع والتصديق الالكترونيين بتاريخ 1 فبراير 2015، حيث يتعلق التصديق والتوقيع الالكتروني بمجموعة من البيانات والمعلومات ذات الطابع الشخصي، التي يشكل الاعتداء عليها جريمة يعاقب عليها قانونا، ومن اهم صور هذه الاعتداءات:

- افشاء البيانات الشخصية أو إساءة استعمالها حيث انه بموجب المادة 68 من القانون 15-04 فانه يعاقب كل من يقوم بحيازة أو افشاء أو استعمال بيانات انشاء توقيع الكتروني موصوف خاص بالغير بالحبس من ثلاث (03)

اشهر الى ثلاث (03) سنوات وبغرامة من 1.000.000دج الى 5.000.000 دج او بإحدى هاتين العقوبتين، كما نصت المادة 73 من ذات القانون على معاقبة كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها اثناء قيامه بالتدقيق بالحبس من ثلاث (03) اشهر الى سنتين (02) وبغرامة من 20.000 دج الى 200.000 دج او بإحدى هاتين العقوبتين.

- جريمة الاخلال بسرية البيانات بحيث انه في حالة اخلال مؤدي خدمات التصديق الالكتروني بواجب الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكترونية الممنوحة وفقا لما نصت عليه المادة 42 توقع عليهم العقوبة المنصوص عليها في المادة 70 وهي الحبس من ثلاث (03) أشهر الى سنتين (02) وبغرامة من 200.000دج الى 1.000.000 دج او بإحدى هاتين العقوبتين.

رابعا: القانون الخاص بحماية حقوق المؤلف والحقوق المجاورة

اعترف القانون الخاص بحماية حقوق المؤلف والحقوق المجاورة بأن المواقع الالكترونية تعد " مصنفات متعددة الأغراض" حيث يمكن استخدامها من قبل الشركات كعلامات تجارية لتمييز منتجاتها او كأسماء تجارية لجذب الجمهور ان حتى كمصنفات أدبية وفنية لعرض الاعمال، وبمجرد تسجيل الموقع يحصل على حماية قانونية بموجب قانون حماية الملكية الفكرية، تحول دون أي انتهاك لحقوق الافراد مثل استخدام أسمائهم وصورهم دون اذن. حيث ان المواقع الالكترونية التي تعرض المصنفات الأدبية او الفنية تكون محمية بموجب قانون حماية المؤلف والذي يشمل حقوق المؤلف الأدبية والمالية، كما يحضر استغلال هذه المصنفات بطرق تؤثر على

الحياة الخاصة للأفراد او تعرض معلوماتهم الشخصية دون اذن منهم، وهنا نشير الى ان حماية المصنفات في المواقع الالكترونية مرتبطة بحماية الموقع نفسه[1].

وبذلك اعترف المشرع الجزائري بوصف المصنف الفكري لمعطيات الحاسب الالي، واحاطه بحماية جزائية بموجب القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، حيث اعتبر ان الاعتداء على الحق المالي والادبي لمؤلف البيانات يندرج ضمن أفعال التقليد المنصوص عليها في المادة 161 من هذا القانون والمعاقب عليها بموجب المواد 153، 154، 156، 158[2].

رابعا: قانون التأمينات الاجتماعية

قام المشرع الجزائري من خلال قانون التأمينات بتنظيم احكام الحريمة الالكترونية من خلال هيئات الضمان الاجتماعي من خلال نصوص تخص البطاقة الالكترونية من خلال تقرير جزاءات في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل او نسخ او حذف كلي او جزئي للمعطيات التقنية او الإدارية المقيدة في البطاقة الالكترونية للمؤمن له اجتماعيا او في المفتاح الالكتروني لهيكل العلاج او في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 93 مكرر[3].

[1] حسين نوارة، اليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة الكترونيا، اعمال الملتقى الوطني: اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 09 مارس 2017، ص121..

[2] بن مالك أحمد، المرجع السابق، ص953.

[3] بوضياف اسمهان، المرجع السابق، ص 367.

خامسا: قانون الاعلام

جرم المشرع في اطار ممارسة النشاط الإعلامي مجموعة من الأفعال التي يترتب عنها قيام جرائم الكترونية وهذا من خلال المواد 119 الى 121 و"المتمثلة في نشر او بث بأحد وسائل الاعلام المنصوص عليها في قانون الاعلام ، أي خبر او وثيقة تلحق ضررا بسير التحقيق الابتدائي، او فحوى مناقشة الجهات القضائية التي تصدر الحكم اذا كانت جلساتها سرية او تقارير عن المرافعات التي تتعلق بحالة الأشخاص او الإجهاض او نشر او بث بإحدى الوسائل الإعلامية صورا او رسوما او بيانات توضيحية أخرى تعييد تمثيل كل او جزء من ظروف الجنايات او الجنح المذكورة في المواد من 255 الى 263 مكرر ومن 333 الى 342 من قانون العقوبات"[1].

المبحث الثاني: الجوانب الإجرائية

لمكافحة الجريمة الالكترونية في التشريع الجزائري

تتضمن الجوانب الإجرائية لمكافحة الجرائم الالكترونية، تحديد الجهات المختصة والموكلة اليها مهمة التصدي، لهذا النوع من الجرائم فضلا عن التطرق الى الإجراءات الخاصة والمستحدثة لمتابعة هذه الجرائم.

المطلب الأول:

الجهات المختصة بمكافحة الجريمة الالكترونية

في سبيل محاربة الجريمة الالكترونية وما يتطلبه ذلك من تكاثف للجهود قام المشرع الجزائري باستحداث عدد من الهيئات غير الأمنية تعمل الى جانب

[1] بن مالك أحمد، المرجع السابق، ص954

الجهات الأمنية حيث تتقاطع الأدوار وتتكامل فيما بينهما لرصد هذه الجرائم والتحقيق فيها.

الفرع الأول: الجهات غير الأمنية المختصة بمكافحة الجريمة الالكترونية

تتمثل الجهات غير الأمنية التي استحدثها المشرع الجزائري في:

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها

استحدثها المشرع بموجب المادة 13 القانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها[1]، والتي حدد تشكيلها وتنظيمها وكيفيات سيرها بموجب المرسوم الرئاسي رقم 15-261[2].

وهي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل مقرها الجزائر العاصمة[3]. تناط بهذه الهيئة العديد من المهام يمكن ايرادها فيمايلي[4]:

[1] القانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر، العدد 47، المؤرخة في 16اوت 2009.

[2] المرسوم الرئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، المحدد تشكيلها وتنظيمها وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها (ج.ر، العدد 53 مؤرخة في 08 أكتوبر 2015.

[3] انظر المواد 02،03 من المرسوم الرئاسي رقم 15-261.

[4] انظر المادة 14 من القانون 09-04، المرجع السابق، والمادة 04 من المرسوم الرئاسي 15-261، المرجع السابق.

- تنسيق الوقاية ومكافحة الجرائم الالكترونية وذلك عن طريق تنشيط وتحسين التنسيق في مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.

- دعم التحريات القضائية وذلك عن طريق مساعدة السلطات القضائية والشرطة في التحقيق في الجرائم الالكترونية وجمع المعلومات.

- التعاون الدولي من حيث تبادل المعلومات مع الدول الأجنبية لتحديد مرتكبي الجرائم وتحديد أماكنهم، وكذا تنفيذ طلبات المساعدة في إطار تعزيز التعاون الدولي.

- التنسيق والتعاون الوطني وهذا مع السلطات والهيئات المختصة بمكافحة الجرائم الالكترونية.

- تدريب المحققين وهذا فيما يتعلق بالبحث والتحري التقني في مجال الجرائم الالكترونية

- اقتراح استراتيجيات الوقاية من خلال وضع استراتيجيات وطنية للوقاية من الجرائم الالكترونية.

- مراقبة الاتصالات الالكترونية للكشف عن الجرائم الإرهابية والتخريبية، تحت اشراف القضاء.

- جمع وتسجيل المعلومات الرقمية لاستخدامها في الإجراءات القضائية.

- تحديث المعايير القانونية من حيث المساهمة في تحديث القوانين ذات الصلة بالجرائم الالكترونية.

ثانيا: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تعتبر الهيئة سلطة إدارية مستقلة تتمتع بالاستقلال المالي والإداري والمعنوي، كما نصت على ذلك المادة 22 من القانون18-07، وتتكون من رئيس يعينه رئيس الجمهورية، وثلاثة قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة، بالإضافة الى أعضاء ممثلين عن البرلمان ومجموعة من الوزراء المختصين، وهم وزير الدفاع، وزير الشؤون الخارجية، الوزير المكلف بالداخلية، وزير العدل، الوزير المكلف بالبريد والتكنولوجيات، وزير الصحة، وزير العمل والتشغيل والضمان الاجتماعي، ويمكن للهيئة ان تستعين بأي شخصية مؤهلة من شانها مساعدتها في اعمالها لمدة 5 سنوات قابلة للتجديد لكل أعضاء الهيئة، كما انه تلزم هذه الشخصيات بأداء اليمين[1].

وتتمحور مهامها بصورة رئيسية حول[2]:

- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي

- اعلام الأشخاص المعنيين. والمسؤولين عن المعالجة بحقوقهم وواجباتهم.

[1] صليع سعد. اليات مكافحة الجريمة الالكترونية في التشريع الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث، تخصص قانون جنائي، معهد الحقوق والعلوم السياسية المركز الجامعي تيبازة، 2025/2024، ص213.

[2] المادة 25 من القانون 18-07.

- تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي الى مثل هذه المعالجة.

- تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي واعلام أصحابها بمالها.

- الترخيص بنقل المعلومات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون.

- الامر بتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.

- الامر بإغلاق معطيات او سحبها او اتلافها.

- تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.

- نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني.

- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.

- اصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون

- وضع معايير في مجال المعطيات ذات الطابع الشخصي.

- وضع قواعد السلوك والاخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

إذا ترأى لها اثناء ممارسة مهامها وجود أفعال تأخذ وصف جزائي، تقوم فورا بإعلام النائب العام، كما تقوم بإعداد تقرير سنوي حول نشاطها يرفع الى رئيس الجمهورية.

ثالثا: المنظومة الوطنية لأمن الأنظمة المعلوماتية

قام المشرع بموجب المرسوم الرئاسي رقم 20-05 باستحداث منظومة وطنية لأمن الأنظمة المعلوماتية، والتي تتكون من مجلس وطني ووكالة لأمن الأنظمة المعلوماتية، تعني بالأنظمة المعلوماتية من خلال تحضير واعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، من خلال المهام المسندة لكل من المجلس الوطني لأمن الأنظمة المعلوماتية أو من خلال وكالة أمن الأنظمة المعلوماتية[1].

1- المجلس الوطني لأمن الأنظمة المعلوماتية

يتشكل المجلس الوطني لأمن الانظمة المعلوماتية بحسب المادة 05 من المرسوم الرئاسي 20-05 رئيسا يتمثل في وزير الدفاع الوطني او ممثلا له، ويتكون المجلس من تشكيلة تضم: ممثل عن رئاسة الجمهورية، ممثل عن الوزير الأول، الوزير المكلف بالعدل، الوزير المكلف بالمالية، الوزير المكلف بالطاقة، الوزير المكلف بالاتصالات، الوزير المكلف بالتعليم العالي، كما يمكن للمجلس الاستعانة بأي شخص او مؤسسة من شانه تنويره في اعماله. وتولي المجلس القيام بالمهام الاتية:

[1] صليع سعد، المرجع السابق، ص 219

- البت في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.

- دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليهما.

- دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها.

- الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في جمال أمن الأنظمة المعلوماتية.

- الموافقة على تصنيف الأنظمة المعلوماتية.

- اقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتي عند الحاجة.

ويبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية.

2- وكالة أمن الأنظمة المعلوماتية

تعتبر الوكالة مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلالية المالية، مقرها مدينة الجزائر.

تعمل الوكالة على حماية الفضاء السيبراني الوطني وضمان استقراره، وفي هذا الاطار تتمحور مهامها على وجه الخصوص في وضع استراتيجية وطنية للأمن السيبراني، وتامين الأنظمة المعلوماتية وحمايتها من المخاطر، وكذا مراقبة وتقييم

مستوى الامن السيبراني في المؤسسات، كما تعمل بالتنسيق مع الجهات المعنية في حالة وجود جرائم سيبرانية، تقوم أيضا بمهام التكوين والتوعية في مجال الامن السيبراني، وكذا التعاون الدولي في هذا المجال، كما تقوم بإجراء التفتيش والمراجعة للتأكد من الالتزام بالمعايير الأمنية، إضافة الى تقديم المشورة والاشراف على تطبيق السياسات الأمنية.[1]

الفرع الثاني: الجهات الأمنية المختصة بمكافحة الجريمة المعلوماتية

إضافة الى الأجهزة غير الأمنية تلعب الأجهزة الأمنية دور فعال في الحد من الجرائم المعلوماتية حيث تعتمد هذه الأجهزة على التكنولوجيا الحديثة في الكشف عن هذه الجرائم، وتتمثل هذه الأجهزة في جهاز الدرك الوطنين وجهاز الامن الوطني.

أولا: جهاز الدرك الوطني

جهاز الدرك الوطني يتبع لوزارة الدفاع الوطني ومن بين المهام الموكلة في مجال الشرطة العمل على محاربة الاجرام، والاجرام المنظم وهذا بالاعتماد على التقنيات الحديثة القضائية من خلال مختلف اجهزته المتمثلة أساسا في:

- مديرة الامن العمومي والاستغلال وهي التي تتولى عملية التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم الالكترونية.

بالإضافة الى المصلحة المركزية للتحريات والجنائية وهي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الاعلام والاتصال.

[1] للاطلاع على مهام الوكالة انظر المادة 18 من المرسوم الرئاسي 20-05.

- مركز الوقاية من جرائم الاعلام الالي والجرائم الالكترونية: تم استحداثه سنة 2008 أيضا ويعد احد الأجهزة المركزية التي تعمل على مكافحة الجريمة الالكترونية فهو يساعد في المساعدة التقنية للمحققين.[1]

- المعهد للأدلة الجنائية من اهم الجهات التي تقدم الدعم في مكافحة الجريمة بجميع اشكالها وذلك بإدراج العلوم في العدالة الجزائية من خلال التكوين والتعليم وتقديم المساعدات التقنية، فهو يتكون من احدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن انجاز الخبرة، ومن بينها دائرة الاعلام الالي والالكتروني التي تختص بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، إضافة الى تقديم المساعدة التقنية للمحققين في المعاينات[2].

ثانيا: جهاز الامن الوطني

يعمل جهاز الامن الوطني على مكافحة الجريمة الالكترونية من خلال ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي:

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية قسنطينة.
- المخبر الجهوي للشرطة العلمية بوهران.

ومن اطار السياسة المنتهجة للحد من الجريمة الإلكترونية قامت المديرية العامة للأمن الوطني سنة 2010 باستحداث حوالي 23 خلية لمكافحة هذا النوع من الجرائم على مستوى 08 خلايا على مستوى الوسط و 8 خلايا على مستوى ولايات

[1] صليع سعد، المرجع السابق، ص ص: 227-228.

[2] بوضياف اسمهان، المرجع السابق، ص370.

الوسط، و6 خلايا على مستوى ولايات الغرب، وخلية واحدة على مستوى ولايات الجنوب، لتقوم فيما بعد بتعميم الخلايا على مصالح أمن ولاية الوطن[1].

المطلب الثاني:

خصوصية إجراءات المتابعة في الجرائم الالكترونية

في ظل تزايد الجرائم الالكترونية وتعقيدها، ادخل المشرع الجزائري العديد من التعديلات القانونية التي تتماشى وخصوصية هذه الجرائم التي تتطلب اللجوء الى اليات تقنية حديثة وفق إجراءات خاصة للكشف عنها ومتابعة مرتكبيها.

الفرع الأول: إجراءات البحث التحري وجمع المعلومات في الجرائم الالكترونية

أولا الإجراءات المنصوص عليها في قانون الإجراءات الجزائية

في اطار مكافحة الجريمة الالكترونية ادخل المشرع الجزائري العديد من التعديلات التي تتماشى وهذا النوع من الجرائم المستحدثة ومن بين اهم التعديلات في هذا الخصوص هو تمديد الاختصاص للضباط الشرطة القضائية الى كامل التراب الوطني في بعض الجرائم ومنها الجرائم الماسة بأنظمة المعالجة الالية للمعطيات، وهذا وفقا لما تنص عليه الفقرة 07 من المادة 24 قانون الإجراءات الجزائية[2] .

[1] سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة قسنطينة، العدد 52، 2019، ص 54، انظر كذلك: حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للامن الوطني في مكافحة الجرائم الالكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية والعلوم السياسية، جامعة بسكرة، يومي 16-17 نوفمبر 2015ن ص08.

[2] القانون رقم 25-14 مؤرخ في 3 غشت سنة 2015 المتضمن قانون الإجراءات الجزائية، ج.ر، عدد54، الصادرة بتاريخ 13 غشت 2025

ومن بين الإجراءات الخاصة التي تضمنها قانون الإجراءات الجزائية هو إمكانية اللجوء تمديد التوقيف للنظر من قبل ضابط الشرطة القضائية ثلاث مرات (المادة83 من قانون الإجراءات الجزائية)، إضافة الى إمكانية اللجوء الى أساليب البحث والتحري الخاصة كاعتراض المراسلات وتسجيل الأصوات والتقاط الصور التي نص عليها المشرع في المواد 114 الى 119، والتسرب 120 الى 127 من قانون الإجراءات الجزائية.

كما أجاز المشرع خلافا للقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية بموجب المادة 78 فقرة 03 دخول المساكن وتفتيشها في أي وقت من الليل والنهار دون التقييد بالميقات القانوني المنصوص عليه في المادة 78 فقرة 01، كما لم يشترط بموجب نص المادة 97 من ق.ا.ج توافر رضاء صريح من المعني، حيث تتم عملية التفتيش وفقا للاستثناءات المنصوص عليها في المادة 78 فقرة 03 من قانون الإجراءات الجزائية، اما في مرحلة التحقيق فوفقا للمواد 158 و 159 ق.ا.ج فيخضع التفتيش في الجرائم الماسة بأنظمة المعالجة الالية للمعطيات للضوابط المنصوص عليها في المادة78 من قانون الإجراءات الجزائية وهي الموافقة المسبقة لوكيل الجمهورية او قاضي التحقيق وبحضور شاهدين مسخرين، او بحضور ممثل يعينه صاحب المسكن محل التفتيش[1].

ثانيا: الإجراءات المنصوص عليها في القانون 09-04

جاء القانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها بجملة من الإجراءات لمكافحة الجريمة الالكترونية أهمها[2]:

[1] بن مالك احمد، المرجع السابق، ص954.

[2] المرجع نفسه، ص959.

- **مر اقبة الاتصالات الالكترونية (المادة04):** تتم بناء على اذن من السلطات المختصة حيث تسمح بمراقبة الاتصالات الالكترونية (علامات، إشارات، أصوات) في حالات معينة مثل:

  - الوقاية من الجرائم الإرهابية أو تلك التي تمس بالأمن الوطني.
  - عند صعوبة الوصول الى نتائج التحقيقات.
  - في إطار تنفيذ المساعدة القضائية الدولية.

- **تفتيش المنظومات المعلوماتية:** حيث يجوز التفتيش بناء على اذن من الهيئة الوطنية ويمكن ان يتم ذلك عن بعد في بعض الحالات مثل:

  - الوقاية من الجرائم الإرهابية او تلك التي تمس بالأمن الوطني
  - عند صعوبة الوصول الى نتائج من خلال التحقيق.
  - وجود تهديد للنظام العام او مؤسسات الدولة
  - في إطار تنفيذ المساعدة القضائية الدولية.

- **جمع وتسجيل بيانات محتوى الاتصالات (المادة 10)** حيث يقع على عاتق مقدمي خدمات الأنترانت مساعدة السلطات القضائية المكلفة بالتحري في جمع وتسجيل بيانات محتوى الاتصالات في حينها، كما يتوجب عليهم سحب أي محتوى مخالف للقانون فورا، مع الحفاظ على السرية العمليات التي يقومون بإنجازها بطلب من المحققين تحت طائلة العقوبات المقررة لإفشاء اسرار التحري والتحقيق....

الفرع الثاني: القطب الجزائي الوطني المستحدث لمكافحة الجريمة الإلكترونية

[1]في ظل تزايد الجريمة الالكترونية، ومن اجل الحد من هذه الظاهرة توجه المشرع الجزائري الى استحداث قطب جزائي وطني توكل اليه مهمة بمهمة التحقيق والفصل في هذه الجرائم وهذا بموجب الامر 21-11 [2] المتعلق بإنشاء القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المتمم لقانون الإجراءات الجزائية من خلال المواد من335 الى 342 ق.ا.ج.

حيث نصت المادة على أنه يوجد على مستوى محكمة مقر مجلس قضاء الجزائر قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والجرائم المرتبطة بها. كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا.

وعلى هذا الأساس يعتبر القطب الجزائي " هيئة نوعية تنشأ على مستوى محكمة مقر مجلس قضاء الجزائر يختص بالنظر في قضايا تتميز بنوع من التعقيد وجرائم محددة حصرا والمرتبطة بتكنولوجيا الاعلام والاتصال والجرائم المرتبطة بها"[3].

1

[2] الامر 21-11 المؤرخ في 25 غشت 2021 المتمم للامر 66-155 المؤرخ في 08 يونيو 1966 والمتضمن قانون الإجراءات الجزائية (الملغي)، ج.ر، عدد 65 المؤرخة في 26 غشت 2021 والمتضمن استحداث قطب وطني للتحري عن الجرائم المتصلة بتكنولوجيات الاعلام والانصال.

[3] عون فاطمة الزهراء، الإجراءات التشريعية المستحدثة في مواجهة الجريمة الالكترونية في القانون الجزائري- القطب الجزائي نموذجا-، مجلة حقوق الانسان والحريات العامة، جامعة مستغانم، العدد 02،2002، ص557

يختص القطب الجزائي الوطني بحسب المادة 337 ق.ا.ج نوعيا بجرائم تكنولوجيا الاعلام والاتصال المبينة ادناه والجرائم المرتبطة بها:"

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.
- جرائم نشر وترويج اخبار كاذبة بين الجمهور من شانها المساس بالأمن والسكينة العامة او استقرار المجتمع.
- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والامن العمومين ذات الطابع المنظم أو العابر للحدود الوطنية.
- جرائم المساس بأنظمة المعالجة الالية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.
- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية او تهريب المهاجرين
- جرائم التمييز وخطاب الكراهية".

و يختص القطب الجزائي الوطني بجرائم تكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها، ويقصد بالجرائم الأكثر تعقيدا هنا، الجرائم التي "بالنظر الى تعدد الفاعلين او الشركاء او المتضررين او بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة او جسامة اثارها او الاضرار المترتبة عليها او لطابعها المنظم او العابر للحدود الوطنية او لمساسها بالنظام و الامن العموميين تتطلب استعمال ووسائل تحري خاصة او خبرة فنية متخصصة او اللجوء الى تعاون قضاء دولي(المادة 338ق.ا.ج)

ونظرا لخصوصية هذا النوع من الجرائم بالنظر الى اثارها والضرر الناتج عنها والذي يمكن ان يمس امن الدولة واستقرارها خاصة اذا تعلق بالمؤسسات المالية والبنوك، فقد جعل من اختصاص القطب الجزائي الوطني بعدما كانت تدخل ضمن الاختصاص الموسع للأقطاب الجزائية، كما يعتبر الاختصاص النوعي للقطب الجزائي الوطني من النظام العام لا يمكن ان تفصل أي جهة قضائية أخرى في هذه الجرائم .

الخاتمة:

يشكل تطور الجريمة الالكترونية تديا فعليا امام المنظومات القانونية في كافة الدول، ومن بينها المنظومة القانونية الجزائرية التي سع من خلالها المشرع جاهدا الى مسايرة هذا التطور من خلال بناء إطار تشريعي يجمع بين التجريم والعقاب من جهة، وضمان نجاعة الأجهزة الإجرائية من جهة أخرى عليه يمكن نجد أن:

- المشرع الجزائري تبنى مقاربة متعددة الابعاد لمعالجة هذا النوع من الجرائم، بداية بوضع تعريف للجريمة الالكترونية وتوسيع نطاقها لتشمل الاعتداء على النظم المعلوماتية والمعطيات الشخصية وسرية الاتصالات مستندا الى جملة من القوانين المتخصصة والمكملة لما جاء في قانون العقوبات كالقانون 09-04 وقانون 18-07.

- كما يلاحظ ان الاليات الإجرائية لمكافحة هذه الظاهرة شهدت تطورا واضحا، من خلال منح سلطات موسعة واستثنائية للجهات القضائية والشبه قضائية إضافة الى استحداث قطب جزائي وطني متخصص.

التوصيات:

- ان طبيعة الجريمة الالكترونية وتطورها يستدعي بالضرورة اجراء مراجعة مستمرة للتشريعات الخاصة بهذه الجرائم لتتلاءم مع المستجدات التكنولوجية وأساليب الاجرام الحديثة.

- تعزيز التكوين والتدريب لضباط الشرطة القضائية والقضاة في مجالات التحري الرقمي وتحليل الأدلة الالكترونية

- توسيع صلاحيات التعاون الدولي، وتفعيل الاتفاقيات المبرمة في هذا المجال لتسهيل تتبع الجناة خارج الحدود الوطنية.

- توعية الافراد والمؤسسات حول مخاطر الجريمة الالكترونية وسبل الوقاية منها والتبليغ عليها.

قائمة المصادر والمراجع:

- **المصادر:**

1- القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 155/66، المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج.ر، العدد 71، 2004.

2- القانون 24-06 المؤرخ في 28 افريل 2024 المعدل والمتمم للأمر 155/66، المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج.ر، العدد 30، 2024.

3- القانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر، العدد 47، المؤرخة في 16اوت 2009.

4- المرسوم الرئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، المحدد تشكيلها وتنظيمها وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها (ج.ر)، العدد 53 مؤرخة في 08 أكتوبر 2015

5- الامر 21-11 المؤرخ في 25 غشت 2021 المتمم للأمر 66-155 المؤرخ في 08 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر، عدد 65 المؤرخة في 26 غشت 2021 والمتضمن استحداث قطب وطني للتحري عن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

- **المراجع**

أولا: الكتب

1- ايمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ط 01، 2014.

2- دعاء عبد العال، خالد عبد الحق، الجرائم الالكترونية والتحقيقات الجنائية، دار اليازوري للنشر والتوزيع، الأردن، د.ط، 2025.

3- زهراء عادل سلبي، الابتزاز الالكتروني (دراسة مقارنة)، دار الأكاديميون للنشر والتوزيع، الأردن، د.ط، 2021.
4- شريف حسين محمد، القانون الواجب التطبيق على الجريمة الالكترونية، المصرية للنشر والتوزيع، القاهرة، د.ط، 2021.
5- عبد العال الدريبي، الجرائم الالكترونية دراسة قانونية قضائية مع احدث التشريعات العربية في مجال مكافحة الجريمة المعلوماتية و الانترنت، المصدر القومي للإصدارات القانونية، القاهرة، ط 01، 2012.
6- محمود مدين، فن التحقيق والاثبات في الجرائم الالكترونية، المصرية للنشر والتوزيع، القاهرة، ط01، 2020.
7- مرفت محمد حبايبة، مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري للنشر والتوزيع، الأردن، د.ط، 2022.
8- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، ط 02، 2010.
9- هشام بشير، الاليات الدولية لمكافحة الجريمة الالكترونية، المركز الدولي للدراسات المستقبلية والاستراتيجية، القاهرة، د.ط، 2012.
10- هيثم عبد الرحمان البقلي، الجرائم الالكترونية الواقعة على العرض بين الشريعة والقانون المقارن، دار العلوم للنشر والتوزيع، مصر، د.ط، 2010.

ثانيا: المقالات

1- بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، كلية الحقوق والعلوم السياسية، جامعة المسيلة، العدد 11، 2018.
2- دمان ذبيح عماد، بهلول سمية، الاليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد 13، جانفي 2021.
3- بونعارة ياسمينة، الجريمة الالكترونية، مجلة المعيار، كلية أصول الدين، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، العدد 39، 2015.

4- عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العراق، العدد07، 2008.
5- راضية عميمور، الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، العدد01، 2022.
6- رمزي حوحو، منيرة بلورغي، مواجهة الجريمة المعلوماتية في الجزائر، مجلة الحقوق والحريات، كلية الحقوق والعلوم السياسية جامعة بسكرة، العدد 02، 2014.
7- بن مالك أحمد، خصوصية الجريمة المعلوماتية وسيل مكافحتها في التشريع الجزائري، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة تسمسيلت، العدد 2، 2023.
8- مليانى عبد الوهاب، الجرائم الماسة بالمعطيات الشخصية على ضوء القانون رقم 18-07، مجلة البحوث القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، العدد 01، 2023.
9- سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة قسنطينة، العدد 52، 2019.
10- عون فاطمة الزهراء، الإجراءات التشريعية المستحدثة في مواجهة الجريمة الالكترونية في القانون الجزائري- القطب الجزائي نموذجا-، مجلة حقوق الانسان والحريات العامة، جامعة مستغانم، العدد 02،2022.

ثالثا: الرسائل الجامعية

- صليع سعد. اليات مكافحة الجريمة الالكترونية في التشريع الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث، تخصص قانون جنائي، معهد الحقوق والعلوم السياسية المركز الجامعي تيبازة، 2025/2024.

رابعا: اعمال الملتقيات

1- حسين نوارة، اليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة الكترونيا، اعمال الملتقى الوطني: اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 09 مارس 2017.

2- حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للامن الوطني في مكافحة الجرائم الالكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية والعلوم السياسية، جامعة بسكرة، يومي 16-17 نوفمبر 2015.

3- مختارية بوزيدي، ماهية الجريمة الالكترونية، اعمال الملتقى الوطني: اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 29 مارس 2017، الجزائر العاصمة، منشورة من قبل مركز جيل البحث العلمي، 2017.

فهرس المحتويات

الرقم	الموضوع والمؤلفين	الصفحة
.1	الذكاء الاصطناعي كسلاح غير تقليدي في النزاعات المسلحة واشكالية الامتثال لمبادئ القانون الدولي الإنساني د. بوعقبة نعيمة	9
.2	المسؤولية المدنية الناشئة عن أضرار الذكاء الاصطناعي. د. عبد الرحمان سلام	43
.3	أثر التحول الرقمي على القانون النقدي والمصرفي رقم 23-09 "رقمنة القطاع المصرفي نموذجا" د. نذير قورية	73
.4	استخدام أدوات الذكاء الاصطناعي في حماية حقوق المؤلف د. منير بر ابح طويرات عبد الرحمان	101
.5	أثر الرقمنة والذكاء الاصطناعي على أداء السلطة التنفيذية في الجزائر د. مدار توفيق	116
.6	الإشكالات القانونية لاستخدامات الذكاء الاصطناعي: بين المسؤولية المدنية والجنائية والتحديات المستقبلية لحوكمة التكنولوجيا د. عبدالعزيز عشبة سلمى د. مروة فريجة	133
.7	مخاطر الذكاء الاصطناعي د. نويري محمد الأمين د. رشا مقدم	160
.8	دور الذكاء الاصطناعي في مجال العقود و المرفق العمومي الذكي د. عماد الدين بركات د. صابر بن صالحية	183

.9	التفاوض الإلكتروني في عقود العمل عن بُعد: قراءة قانونية في ضوء التطور التكنولوجي د. رضوان ربعية د. مزوزي فارس	231
.10	إشكالية إقامة المسؤولية الجزائية عن جرائم الذكاء الاصطناعي د. دلال بليدي د. فايزة خضار	256
.11	الجرائم الإلكترونية الموجهة ضد الطفل في الجزائر: قراءة قانونية في صورها وآليات مكافحتها د. سامية قفاف د. سماح محمودي	271
.12	عقد التأمين الإلكتروني بين متطلبات البيئة الرقمية وخصوصيات التنظيم القانوني في الجزائر د. تقي الدين دغبوج د. فؤاد مخبرش	304
.13	التحول الرقمي لقانون الأعمال في الجزائر. د. زهر الدين بوستة د. كمال بوعشة	322
.14	الذكاء الاصطناعي والأمن السيبراني د. أسماء بوعكاز د. خولة غرايبية	341
.15	تأثير استخدام الذكاء الاصطناعي على مهمة القاضي الإداري: دراسة تحليلية نقدية في ضوء التحولات التكنولوجية الحديثة د. حنان علاوة د. زيد الخيل توفيق	367
.16	المواجهة القانونية لانتهاك الحق في الخصوصية الرقمية عبر تقنيات الذكاء الاصطناعي د. نصرالدين العايب د. عبد الوهاب بوعزيز	387

.17	مكافحة الجريمة الالكترونية في الجزائر: بين التأصل القانوني والتنظيم الاجرائي د. ياسين بوهنتالة د. زبيار الشاذلي	405