

المسؤولية الدولية عن الأضرار الناجمة عن استخدامات الذكاء الاصطناعي في العلاقات الدولية

دراسة تحليلية في تحديات التنظيم القانوني الدولي

امل عبد الكريم مفتاح الفاندي

المعهد العالي للعلوم والتقنية بئر معتوق .

amlabdulkarimmofth@gmail.com

الملخص بالعربية

يتناول البحث المسؤولية الدولية عن أضرار الذكاء الاصطناعي بوصفه تهديداً ناشئاً للأمن والسلام الدوليين، في ظل عجز قواعد المسؤولية التقليدية عن استيعاب "الغموض الخوارزمي" والاستقلالية الذاتية لتلك الأنظمة، ويحلل البحث الأضرار السيبرانية والعسكرية والحقوقية العابرة للحدود الناتجة عن تداخل أدوار الدول والشركات مع استعراض قصور المبادرات الدولية القائمة، وخلص البحث إلى اقتراح إطار قانوني دولي مرن يتضمن اتفاقية خاصة تركز على الشفافية الخوارزمية وتحديث معايير الإسناد وجبر الضرر؛ وذلك بهدف تحقيق التوازن بين تشجيع الابتكار من جهة، وحماية حقوق الإنسان وضمان المساءلة الدولية من جهة أخرى.

الكلمات المفتاحية بالعربية: المسؤولية الدولية، الذكاء الاصطناعي، القانون الدولي العام، الأضرار العابرة للحدود، الإسناد القانوني، الأنظمة الذكية، الأسلحة ذاتية التشغيل، الأمن السيبراني، حقوق الإنسان، الخصوصية الرقمية.

Abstract

This study examines international responsibility for AI-driven harms, highlighting how autonomous decision-making challenges traditional public international law. It addresses risks across cyber, military, and human rights domains, where actor multiplicity complicates liability and accountability. The analysis critiques fragmented international initiatives, recommending a comprehensive framework focused on algorithmic transparency, updated attribution standards, and multi-actor responsibility to prevent a regulatory vacuum. Ultimately, it seeks to balance technological innovation with the preservation of international peace.

Keywords in English: International responsibility, artificial intelligence, public international law, transboundary harm, legal attribution, autonomous systems, autonomous weapons, cybersecurity, human rights, digital privacy.

مقدمة البحث

أحدث الذكاء الاصطناعي، باعتباره أبرز ملامح الثورة الصناعية الرابعة، تحولاً استراتيجياً في العلاقات الدولية العسكرية والسياسية، وقد فرض هذا التطور المتسارع تحديات قانونية معقدة؛ إذ عجزت قواعد القانون الدولي التقليدية عن تأطير تقنياته، أو مواجهة أضراره العابرة للحدود والتي تمس مصالح المجتمع الدولي بشكل مباشر.

إشكالية البحث

تتمحور الإشكالية حول مدى كفاية قواعد المسؤولية الدولية التقليدية في معالجة أضرار الذكاء الاصطناعي وإمكانية تطوير إطار تنظيمي يستوعب تعقيداته، وتتفرع عن هذه الإشكالية تساؤلات حول التكيف القانوني ومعايير الإسناد في ظل الاستقلالية الرقمية، وحدود المساءلة وفاعلية آليات التقاضي، وتحقيق التوازن بين تشجيع الابتكار وضمان الامتثال للقوانين.

أهمية البحث

تكمن الأهمية الجوهرية للمسؤولية الدولية عن أضرار الذكاء الاصطناعي في قصور القوانين التقليدية وضيق نطاقها؛ فبينما صُممت هذه القواعد لضبط السلوك الإنساني، فإنها تقف اليوم عاجزة أمام الطبيعة المستقلة للأنظمة الرقمية، وما يرافقها من تداخل معقد في الأدوار والمسؤوليات بين المبرمجين والمستخدمين والدول المشرفة عليها.

اهداف البحث

يهدف البحث إلى تحليل الأسس القانونية للمسؤولية الدولية، وتبيان قصور قواعدها التقليدية، مع استشراف أطر تنظيمية وآليات حديثة للتعامل مع استقلالية الأنظمة الذكية وما قد تسببه من أضرارٍ عابرة للحدود.

فرضيات البحث

ينطلق هذا البحث من فرضية مفادها عجز قواعد المسؤولية الدولية التقليدية عن مواجهة الأضرار الناجمة عن الذكاء الاصطناعي، ويناقش عدداً من الفرضيات الفرعية، أبرزها: صعوبة إسناد المسؤولية نظراً لاستقلالية هذه الأنظمة، وتنامي دور الفاعلين غير الدوليين، وضرورة صياغة إطار قانوني جديد يركز على تقييم المخاطر والوقاية منها.

المنهجية

اعتمد البحث المناهج الوصفية والتحليلية والنقدية والمقارنة؛ لتوصيف أبعاد الظاهرة القانونية، وتقييم قصور القواعد القائمة، واستشراف سبل تطويرها تشريعياً.

نطاق البحث

يستعرض هذا البحث المسؤولية الدولية للدول والشركات التقنية عن الأضرار الناجمة عن الذكاء الاصطناعي متولاً معايير الإسناد، وقواعد الإثبات وآليات التعويض، والأبعاد العابرة للحدود في ظل المعطيات الراهنة.

المبحث الأول: الإطار المفاهيمي والقانوني للذكاء الاصطناعي والمسؤولية الدولية

بات الذكاء الاصطناعي عنصراً استراتيجياً في العلاقات الدولية، فإرضاً لتحديات قانونية تتعلق بعجز القواعد الدولية التقليدية عن ضبط أضراره العابرة للحدود؛ الأمر الذي يستدعي مراجعة إطاره المفاهيمي، وبحث مدى إمكانية تطبيق تلك القواعد على قراراته المستقلة.

المطلب الأول: ماهية الذكاء الاصطناعي واستخداماته في العلاقات الدولية

يستعرض هذا المبحث مفهوم الذكاء الاصطناعي، وأنواعه، وخصائصه، مبيناً تطبيقاته في مجالات الأمن والدبلوماسية وصنع القرار، بالإضافة إلى دوره في صياغة التفاعلات الدولية المعاصرة.

الفرع الأول: مفهوم الذكاء الاصطناعي وخصائصه القانونية

أولاً: تعريف الذكاء الاصطناعي.

ظهر هذا المصطلح لأول مرة في مؤتمر "دارتموث" عام 1956 على يد العالم الأمريكي جون مكارثي الذي عرّفه بأنه: "علم وهندسة صناعة الآلات الذكية القادرة على محاكاة التفكير البشري".⁽¹⁾ كما عرفه الاتحاد الأوروبي في مشروع قانون الذكاء الاصطناعي لسنة 2021 بأنه "منظومة آلية مستقلة ومرنة تستنبط طرق معالجة المدخلات لتحقيق أهداف محددة، وتؤثر مخرجاتها - سواء كانت تنبؤات أو قرارات - في البيئتين المادية والافتراضية".⁽²⁾

ثانياً: خصائص الذكاء الاصطناعي.

تتمثل أبرز خصائص الذكاء الاصطناعي المعقدة التي تعيق المساءلة التقليدية في:

1. الاستقلالية التقنية. 2. عدم الشفافية الخوارزمية. 3. الطابع العابر للحدود.⁽³⁾

ثالثاً: أنواع الذكاء الاصطناعي.

يمكن تقسيم الذكاء الاصطناعي حسب اختلاف درجة الاستقلالية والقدرات التقنية إلى:

1. الذكاء الاصطناعي الضيق: وهو نظامٌ مُصمم لأداء مهمةٍ محددةٍ بدقةٍ عاليةٍ، يتفوق فيه على البشر، لكنه يفتقر إلى الوعي الذاتي والقدرة على نقل خبراته إلى مجالات أخرى؛ إذ يعمل تحت تحكم الإنسان تماماً كآلة الحاسبة والهواتف المحمولة. (4)

2. الذكاء الاصطناعي العام: هو نظامٌ قادرٌ على فهم أو تعلّم أي مهمة فكرية يؤديها الإنسان أو غيره من الكائنات، ويتميز بقدرته على توظيف المعارف والمهارات المكتسبة في إنجاز مهام جديدة ضمن سياقات مختلفة دون الحاجة إلى تدريب بشري إضافي، ومن أمثلته الحواسيب والسيارات ذاتية القيادة. (5)

3. الذكاء الاصطناعي الفائق: وهو نظامٌ يتمتع بقدراتٍ ذهنية خارقة تتفوق على أذكى العقول البشرية في شتى المجالات، كالإبداع والفهم والتحليل واتخاذ القرار؛ وهو مشروعٌ افتراضي لم يتحقق بعد. (6)

الفرع الثاني: استخدامات الذكاء الاصطناعي في العلاقات الدولية

أعاد الذكاء الاصطناعي تشكيل موازين القوى في العلاقات الدولية، بعدما وظّفته الدول كأداة محورية في التفاعل والصراع والتعاون في مجالات شتى، لعل من أبرزها:

1. المجال العسكري: حيث تعتمد دول عديدة على الأنظمة الذكية في تطوير أسلحة ذاتية التشغيل، مثل الطائرات المسيّرة، وأنظمة الدفاع الصاروخي، وتقنيات التحليل الاستخباراتي. وقد أشار تقرير معهد ستوكهولم الدولي لأبحاث السلام إلى أن الذكاء الاصطناعي بات ركيزةً أساسية في سباق التسلح العالمي المعاصر. (7)

2. مجال الأمن السيبراني: تعتمد الدول على الخوارزميات الذكية لاكتشاف الهجمات الإلكترونية، وتحليل التهديدات الرقمية، وحماية البنى التحتية الحيوية، وفي المقابل، تُستخدم هذه التقنيات في شن هجمات سيبرانية متطورة تستهدف الأنظمة الحكومية والاقتصادية والعسكرية للدول الأخرى.

3. المجال الاقتصادي: إذ تعتمد الشركات الكبرى على الخوارزميات الذكية في إدارة الأسواق، وتحليل البيانات، وضبط سلاسل الإنتاج والتجارة الدولية، ما أدى إلى تعاظم نفوذ الشركات التكنولوجية العملاقة وتحولها إلى فاعلٍ مؤثرٍ في العلاقات الدولية، مثيراً بذلك تحدياتٍ تتعلق بالسيادة الاقتصادية والأمن الرقمي للدول.

4. المجال السياسي والدبلوماسي: يُستخدم الذكاء الاصطناعي في تحليل البيانات السياسية والتنبؤ بالأزمات الدولية، بالإضافة إلى توجيه الرأي العام عبر تقنيات تحليل السلوك الرقمي ومعالجة المعلومات. وقد كشفت تقارير دولية (8*) عديدة عن توظيف هذه التقنيات للتدخل في العمليات الانتخابية، ونشر الأخبار المضللة، وزعزعة الاستقرار السياسي؛ مما يبرز الأثر العميق الذي تتركه هذه التكنولوجيا في العلاقات الدولية. (9)

المطلب الثاني: الأساس القانوني للمسؤولية الدولية

تستند المسؤولية الدولية إلى حتمية جبر الضرر الناشئ عن الأفعال غير المشروعة، وتكتسب هذه القواعد أهمية متزايدة في مواجهة التحديات القانونية التي فرضتها الطفرة التكنولوجية.

الفرع الأول: مفهوم المسؤولية الدولية وأركانها

أولاً: التعريف بالمسؤولية الدولية.

تطور مفهوم المسؤولية الدولية فقهيًا وتشريعيًا من "التعويض الميكانيكي" إلى "الالتزام الشامل بجبر الضرر". فبينما ركّز المنظور الكلاسيكي لـ "شارل روسو" على ثنائية الفعل والتعويض، مُعرِّفًا إياها بأنها: «نظام قانوني يترتب بموجبه على الدولة التي ارتكبت عملاً يحرمه القانون الدولي، التعويض عن الضرر الذي لحق بالدولة المتضررة» (10)، جاء تقنين لجنة القانون الدولي بالأمم المتحدة عام 2001 ليرسخ هذا المبدأ؛ فلم تعد المسؤولية مجرد آلية لإصلاح الضرر، بل التزاماً قانونياً تلقائياً بموجب م 1 التي نصت على أن: «كل فعل غير مشروع دولياً تقوم به دولة ما يستتبع مسؤوليتها الدولية»؛ وبذلك تضافرت الرؤية الفقهية والتشريعية لتكريس المسؤولية كعاقبة قانونية حتمية. (11)

ثانياً: أركان المسؤولية الدولية: للمسؤولية الدولية ركنين رئيسيين:

1. الركن الأساسي "الفعل غير المشروع دولياً":

هو سلوك (إيجابي أو امتناع) يصدر عن شخص دولي ويُشكّل خرقاً لالتزام دولي، بصرف النظر عن وجود قصد أو خطأ، ويقوم على عنصرين:

أ- عنصر الإسناد (السلوك المنسوب للدولة). ب - عنصر الخرق (مخالفة التزام دولي). (12)

2. الركن المتمم ويتمثل في:

أ - الضرر: وهو خسارة محققة تقع على المتضرر، سواء كانت مادية كخسارة الأموال، أو معنوية كالمساس بكرامة الدولة.

ب - العلاقة السببية: وجود رابطة مباشرة ومؤكدة تثبت أن الضرر هو نتيجة مباشرة للفعل غير المشروع، سواء كان ناشئاً عن فعل إيجابي، أو عن امتناع عن عمل كان يتعين القيام به. (13)

الفرع الثاني: صور المسؤولية الدولية في القانون الدولي العام

تتخذ المسؤولية الدولية عموماً صوراً متعددة ومتداخلة، ويمكن تصنيفها وفق المعايير الآتية:

أولاً: من حيث طبيعة المسؤولية:

1. المسؤولية الأدبية (السياسية): تترتب عند ارتكاب عمل غير مشروع يمس كرامة دولة ما، ودون إلحاق ضرر مادي مباشر بها، وتتم تسويتها عادة عبر ترضية دبلوماسية أو اعتذار رسمي.

2. المسؤولية القانونية: وتنقسم إلى صورتين:

أ - المسؤولية المدنية: تهدف إلى محو آثار العمل غير المشروع وجبر الضرر، وتتخذ أحد الشكلين التاليين: إما التعويض العيني (إعادة الحال إلى ما كان عليه) - أو التعويض المالي. (14)

ب - المسؤولية الجنائية: تقع على عاتق الكيانات أو الأفراد عند ارتكاب جرائم دولية جسيمة، كالإبادة الجماعية وجرائم الحرب، وتترتب عليها عقوبات زجرية دولية. (15)

ثانياً: من حيث الشخص المسؤول: وتنقسم إلى:

1. مسؤولية الدولة. (16) 2. مسؤولية المنظمات الدولية (17) 3. مسؤولية الفرد (الجنائية الدولية). (18)

ثالثاً: من حيث الإسناد: وتنقسم إلى:

1. المسؤولية المباشرة: وهي تلك التي تتحملها الدولة عن الانتهاكات الصادرة مباشرة عن سلطاتها الثلاث (التشريعية، والتنفيذية، والقضائية) أو أحد موظفيها الرسميين. (19)

2. المسؤولية غير المباشرة: هي المسؤولية التي تتحملها الدولة عن الأفعال غير المشروعة التي ترتكبها كيانات تقع تحت سيادتها أو توجيهها، كالدول الاتحادية أو الدول الخاضعة للوصاية. (20)

رابعاً: من حيث أساس المسؤولية: وتنقسم إلى:

1. المسؤولية على أساس الخطأ: وهي التي تتطلب توافر الركن المعنوي (العمد أو الإهمال) من جانب الدولة أو أجهزتها لإثبات مخالفة الالتزام. (21)

2. المسؤولية الموضوعية (المطلقة/المخاطر): تتحقق بمجرد وقوع ضرر ناتج عن أنشطة خطيرة وإن كانت مشروعة، دون اشتراط إثبات خطأ الدولة. (22)

الفرع الثالث: تطور قواعد المسؤولية الدولية في ظل التطور التكنولوجي

يواجه القانون الدولي تحديات هيكلية في ظل الذكاء الاصطناعي والأنظمة الذاتية، ونظراً لعجز القواعد التقليدية القائمة على "الخطأ والسببية" عن استيعابها، أصبح تبني مقاربات جديدة لسد "فجوة المسؤولية" أمراً ضرورياً.

أولاً: قصور القواعد التقليدية: ويرجع ذلك إلى:

1. صعوبة إثبات الخطأ: يغدو إثبات الخطأ الدولي في الأنظمة ذاتية الاستقلالية أمراً بالغ الصعوبة؛ نظراً لافتقارها إلى الأهلية والإدراك، ولأن قراراتها تُتخذ دون إرادة بشرية آثمة أو إهمالٍ واعٍ، مما يُضعف رابطة السببية بين الفعل البشري والضرر الناتج. (23)

2. انقطاع علاقة السببية: تؤدي طبيعة اتخاذ القرار في هذه الأنظمة إلى قطع سلسلة السببية التقليدية بين الفعل البشري والنتيجة الضارة، ما يخلق "فجوة مسؤولية" يصعب سدّها بموجب قواعد القانون الدولي الراهنة. (24)

3. الطابع العابر للحدود للفعل الرقمي: تتسم الأفعال الرقمية بطبيعة لا مادية وعابرة للحدود، مما يجعل معايير الاختصاص القضائي وقواعد تنازع القوانين التقليدية التي تستند إلى أسس مادية - كمكان وقوع الضرر - غير كافية، بل ومقوّضة لأسسها.

ثانياً: الاتجاهات الحديثة لتطوير قواعد المسؤولية الدولية:

1. التحول نحو المسؤولية الموضوعية: إذ تقترح الأدبيات المعاصرة الانتقال من نموذج "إثبات الخطأ" إلى نموذج "المسؤولية الموضوعية" (المخاطر) لمواجهة تحديات التكنولوجيا؛ بحيث يُسأل المطور أو المشغل أو المتحكم في الأنظمة عالية الخطورة عن الأضرار الناجمة عنها دون الحاجة إلى إثبات وقوع خطأ.

2. اعتماد آليات تكميلية لتعويض الأضرار: تُجمع الدراسات على أهمية استحداث تأمين إلزامي وصناديق تعويض خاصة؛ لضمان جبر أضرار الضحايا بفعالية، دون انتظار تطوير قواعد المساءلة الجوهرية.

3. الدعوة إلى اتفاقيات دولية متخصصة: نظراً إلى محدودية التشريعات الوطنية تدعو الدراسات لعقد اتفاقية دولية عاجلة؛ لصياغة أطر موحدة تنظم مسؤولية الفاعلين في مجال الذكاء الاصطناعي وتوزيعها، وآليات التقاضي والاختصاص القضائي، لسد الثغرات ومواجهة المخاطر عابرة الحدود. (25)

المبحث الثاني: المسؤولية الدولية عن الأضرار الناشئة عن استخدامات الذكاء الاصطناعي

أحدث الذكاء الاصطناعي تحولاً في موازين القوى الدولية، وفرض تحديات قانونية معقدة بسبب استقلاليته؛ مما يستوجب إعادة النظر في أسس المسؤولية الدولية عن أضراره.

الفرع الأول: إسناد المسؤولية الدولية عن أضرار الذكاء الاصطناعي

يشكل التطور المتسارع للذكاء الاصطناعي تحدياً قانونياً مستحدثاً، يفرض ضرورة البحث في آليات توزيع التبعات القانونية وتحديد الجهة الدولية المسؤولة عن التعويض، وهو ما يقودنا إلى:

أولاً: مسؤولية الدولة عن الأنظمة الذكية

تلتزم الدولة بضبط وتوجيه هذه التقنيات داخل إقليمها، مما يجعلها في مواجهة مباشرة مع التزاماتها الدولية عند حدوث أي خرق رقمي؛ وهو ما يستدعي تأصيل هذا الالتزام من خلال معرفة:

1. الأساس القانوني لمسؤولية الدولة الدولية.

تقوم المسؤولية الدولية على خرق الدولة لالتزام مفروضٍ عليها، مما يوجب جبر الضرر كاملاً (وفقاً لقضية مصنع تشورزوف) ويتطلب قيام هذه المسؤولية توافر عنصرين: إسناد الفعل غير المشروع للدولة، وخرق الالتزام الدولي.⁽²⁶⁾

2. تطبيق المسؤولية على استخدامات الذكاء الاصطناعي.

إن اعتماد الدولة على أنظمة الذكاء الاصطناعي كأداة تنفيذية في مجالات الدفاع والأمن السيبراني لا يعفيها من مسؤوليتها القانونية الدولية عن الأضرار الناجمة عنها؛ فالعبرة في القانون الدولي تكمن في الصلة الوظيفية والسيطرة الفعلية للدولة على هذه الأدوات، وهو ما يمنعها من التصل من التزاماتها عند استخدام الأسلحة ذاتية التشغيل أو تنفيذ العمليات السيبرانية، وذلك وفقاً لقواعد القانون الدولي الإنساني ودليل تالين 2.0.⁽²⁷⁾

3. حدود القواعد التقليدية أمام استقلالية الأنظمة الذكية

يواجه تطبيق المسؤولية الدولية على أنظمة الذكاء الاصطناعي صعوبات عملية؛ نظراً لاستقلاليته وما تتخذه من قرارات غير متوقعة ناتجة عن التعلم الآلي، وتزيد هذه العوامل من تعقيد تحديد مصدر القرار وإثبات العلاقة السببية بينه وبين الضرر، مقارنةً بالأنظمة التقليدية التي تعتمد على فاعل بشري مباشر، ومع ذلك، لا تعفي صعوبات السيطرة على الأنظمة الذكية الدولة من مسؤوليتها الدولية، بل تفرض اعتماد معايير إسناد مرنة تتناسب طردياً مع غياب الضوابط الكافية للأنشطة عالية الخطورة.⁽²⁸⁾

ثانيا: مسؤولية الشركات والفاعلين من غير الدول.

تكمن أهمية دراسة مسؤولية الفاعلين من غير الدول في تنامي دور شركات التكنولوجيا، ما يثير تساؤلات جوهرية حول مركزها القانوني ومدى خضوعها للمسؤولية الدولية.

1. المركز القانوني للشركات التكنولوجية في النظام الدولي.

تحولت كبرى شركات التكنولوجيا إلى قوى دولية مؤثرة بفضل سيطرتها على البيانات والبنى التحتية الرقمية، مما وسّع نفوذها العابر للحدود رغم احتفاظ الدولة بوضعها القانوني التقليدي، ولم تعد مسؤولية هذه الشركات محصورة في إطار القانون الخاص، بل امتدت لتشمل التزامها بمعايير حقوق الإنسان الدولية⁽²⁹⁾ وفقاً للمبادئ التوجيهية للأمم المتحدة التي تُلزمها بتجنب أي انتهاكات، وهو ما يضع أساساً لتقييم سلوكها في تطوير واستخدام تقنيات الذكاء الاصطناعي.

2. صور مسؤولية الشركات عن أضرار الذكاء الاصطناعي.

تتحمل الشركات التكنولوجية المسؤولية عند تطويرها أنظمة معيبة، أو طرح خوارزميات غير آمنة أو تصميم تطبيقات تنتهك الخصوصية للتأثير في الرأي العام،⁽³⁰⁾ ويتسع نطاق هذه المسؤولية عند استخدام تقنيات المراقبة والتعرف على الوجوه الماسة بالحقوق الأساسية دون قيود وقائية، حيث يُلزمها معيار العناية الواجبة والمبادئ التوجيهية للأمم المتحدة لعام 2011 باتخاذ تدابير لمنع الأضرار واحترام حقوق الإنسان.⁽³¹⁾

ثالثا: إشكالية استقلالية الذكاء الاصطناعي وأثرها على الإسناد القانوني.

تثير أنظمة الذكاء الاصطناعي باستقلاليتهما وقدرتها على التعلم الذاتي إشكاليات قانونية تضعف مفاهيم المسؤولية التقليدية القائمة على الإرادة البشرية، ما يجعل تحديد المسؤول عن أضرارها أمراً معقداً، وانقسم الفقه القانوني في معالجة هذه المعضلة إلى اتجاهين: **يتمسك الأول** بالقواعد التقليدية التي تُحمل الإنسان أو الشركة أو الدولة المسؤولية لانتفاء الإرادة لدى الآلة، بينما **يدعو الثاني** إلى منح الأنظمة المتقدمة "شخصية قانونية إلكترونية" على غرار مقترح البرلمان الأوروبي عام 2017⁽³²⁾، غير أن هذا المقترح يواجه انتقادات واسعة؛ خوفاً من استغلاله كذريعة لتتصل الشركات والدول من مسؤولياتها، ولأن الشخصية القانونية ترتبط جوهرياً بالوعي والإدراك الأخلاقي وهما عنصران تفتقر إليهما التقنية، ولمواجهة ذلك، اقترح الفقه تبني "المسؤولية عن المخاطر التقنية"؛ بحيث تتحمل الجهة المشغلة المسؤولية بمجرد تشغيل نظام عالي الخطورة⁽³³⁾ إلى جانب فرض التزام بـ "الشفافية الخوارزمية".

الفرع الثاني: صور الأضرار الدولية الناتجة عن الذكاء الاصطناعي

لا شك ان للذكاء الاصطناعي أضرار عالمية متعددة الأبعاد، تهدد الاستقرار والأمن البشري، لعل من أبرزها:

أولاً: الأضرار السيبرانية والأمنية: وتتنوع أشكالها لتشمل:

1. الهجمات السيبرانية المعززة بالذكاء الاصطناعي: تُستخدم أنظمة الذكاء الاصطناعي في تطوير هجمات سيبرانية أكثر تطوراً وفاعلية، إذ تتيح هذه الأنظمة اكتشاف الثغرات الأمنية تلقائياً واستغلالها (تكييف أساليب الهجوم وفقاً لنظام الهدف - تنفيذ هجمات متعددة في وقت واحد دون تدخل بشري).⁽³⁴⁾
2. استهداف البنى التحتية الحيوية: تُوظف أنظمة الذكاء الاصطناعي في شن هجمات سيبرانية تستهدف البنية التحتية الحيوية للدول، ومن أمثلتها: أنظمة الطاقة الكهربائية⁽³⁵⁾ - أنظمة المياه والصرف الصحي - أنظمة النقل والمواصلات - الأنظمة المالية والمصرفية.

3. الهجمات على الأنظمة المالية: تُستخدم تقنيات الذكاء الاصطناعي في تنفيذ هجمات سيبرانية تستهدف الأنظمة المالية، ومن أبرز صورها: اختراق البنوك والشركات المالية - سرقة البيانات المالية للأفراد.⁽³⁶⁾ كما تُلحق الهجمات السيبرانية وعمليات الابتزاز أيضاً أضراراً مادية ونفسية بالأفراد، وتُقوض سمعة المؤسسات وتُزعزع ثقة عملائها، كما تهدد استقرار المجتمع عبر تعطيل الخدمات الحكومية، وتسريب البيانات السيادية الحساسة التي تمس الأمن القومي.

ثانياً: الأضرار العسكرية الناجمة عن الأسلحة الذاتية التشغيل:

1. انتهاك مبدأ التمييز: حيث تُشكل الأسلحة ذاتية التشغيل تحدياً لمبدأ التمييز في القانون الدولي الإنساني، نظراً لعجزها عن محاكاة التفكير البشري في الفصل بين المدنيين والمقاتلين، ويبرز التحدي في ثلاثة أبعاد مترابطة:

أ- قصور التقدير السياقي: إذ تعجز الخوارزميات عن فهم السلوكيات البشرية المركبة كالتفريق بين جندي يستسلم ومدني يحمل أداة عادية، مما يحول القرارات الميدانية إلى أحكام ميكانيكية جامدة.

ب - إشكالية البيانات والمستشعرات: حيث تعتمد هذه الأنظمة على مدخلات رقمية قد تكون ناقصة أو متحيزة، كما تتأثر مستشعراتها بالعوامل الطبيعية كالغبار، مما يزود الآلة بمعلومات مضللة تؤدي إلى استهداف خاطئ.⁽³⁷⁾

ج - غياب الوازع الأخلاقي: إذ تفتقر الآلات إلى الضمير الإنساني الذي يمنع إطلاق النار في

المواقف الملتبسة ما يرفع احتمالية وقوع كوارث وخسائر فادحة في صفوف المدنيين.⁽³⁸⁾

2. انتهاك مبدأ التناسب: ويُقصد به الموازنة بين الضرر المتوقع إلحاقه بالخصم والمكاسب العسكرية

المرجوة من استخدام القوة، وتثير الأسلحة ذاتية التشغيل إشكاليةً في هذا الصدد للأسباب الآتية:

أ- العجز عن تقدير التناسب بدقة: وذلك لأسباب ثلاثة:

• الاختزال الرقمي للقيم الإنسانية. - غياب التقدير المتبصر. - الجمود أمام المتغيرات.⁽³⁹⁾

ب - قصور معايير تقييم الضرر: يفتقر الذكاء الاصطناعي إلى "الحس الإنساني"، إذ يعتمد في تقييم

المواقف على خوارزميات مجردة، مما يؤدي إلى النتائج التالية:

• الاعتماد على بيانات مضللة. - الركون إلى الأنماط لا اليقين. - إهمال المتغيرات اللحظية.⁽⁴⁰⁾

ج - اتخاذ قرارات تتجاوز الضرورة العسكرية ويتجلى ذلك في:

• المعادلات الرقمية غير المتكافئة: برمجة النظام لقبول تدمير بناية سكنية تضم عشرات المدنيين

لتحديد تهديد محتمل لشخص واحد ضئيل الأهمية عسكرياً.

• تأثير "انحياز التأكيد": الثقة العمياء للقادة العسكريين في دقة الآلة تدفعهم للموافقة على قرارات

قصف مبالغ فيها، إيماناً منهم بأنها "لا تخطئ" وأن الهدف يبرر حجم الدمار.

• تخفيض قيمة الحياة البشرية: تحويل أرواح المدنيين إلى مجرد "أرقام هاشمية" أو أضرار جانبية

مقبولة ضمن خوارزميات السلاح، مما يؤدي إلى اتساع نطاق الدمار العشوائي.⁽⁴¹⁾

د - الأضرار البشرية الجسيمة: وتتمثل في الآتي:

انتهاك الحق في الحياة - إصابة الأشخاص بعاهات دائمة - تدمير الممتلكات المدنية على نطاق واسع.⁽⁴²⁾

ثالثاً: انتهاكات حقوق الإنسان والخصوصية الرقمية

تتعدد الممارسات التقنية التي تمس الحقوق الأساسية للإنسان، وتتمثل أبرز صورها في:

1. المراقبة الجماعية غير المشروعة: وتشمل:

أ - الجمع القسري للبيانات. ب - التنميط السلوكي الآلي. ج - التتبع الجغرافي المستمر والانتهاك المكاني.⁽⁴³⁾

2. انتهاك الحق في الخصوصية: حيث تُشكّل أنظمة الذكاء الاصطناعي تحدياً لحرمة الحياة

الخاصة، إذ تتجاوز ممارساتها التشريعات التقليدية لحماية البيانات وذلك عن طريق:

أ - الجمع الموسع للبيانات الشخصية. ب - التحليل الدقيق والتميط الشامل للهوية الرقمية. ج - التخزين الأبدي ومخاطر الاستخدام المستقبلي.

3. التمييز الخوارزمي: تتعدد أشكال التمييز الخوارزمي في البيئة الرقمية، وتُصنّف قانونياً وتقنياً إلى نمطين رئيسيين تندرج تحتها تطبيقات وممارسات تمس الحقوق الأساسية:

أ - التمييز الخوارزمي المباشر: ويحدث عند إدراج الخوارزمية لمعايير تمييزية محظورة قانوناً بشكل صريح في معادلاتها البرمجية لاتخاذ القرار، ومن أبرز أشكاله: التمييز على أساس الجنس (44) - التمييز على أساس السن.

ب - التمييز الخوارزمي غير المباشر: يُعدّ هذا النوع الأكثر خطورة وتعقيداً؛ إذ لا تُشير الخوارزمية إلى "المعايير المحظورة" (كالعرق أو الدين) صراحة، بل تعتمد على "مؤشرات بديلة تُفسي إحصائياً إلى النتيجة التمييزية ذاتها ومن أبرز أشكاله:

التمييز الجغرافي (الرمز البريدي) - التمييز السلوكي والاستهلاكي (45) - التمييز القائم على التحيز الإحصائي.

4. التأثير الهيكلي على الحق في حرية التعبير:

يهيمن الذكاء الاصطناعي على الفضاء الرقمي، متحكماً بحرية التعبير والسلوك البشري من خلال آليات تقنية مترابطة تنتهك الحقوق الأساسية للمستخدمين وفق الآتي:

أ - حجب المحتوى بشكل غير موضوعي. ب - توجيه المستخدمين نحو محتوى محدد. ج - مراقبة التعليقات والمنشورات. (46)

المبحث الثالث: تحديات التنظيم القانوني الدولي للذكاء الاصطناعي وآفاق تطوير

المطلب الأول: تحديات التنظيم القانوني الدولي للذكاء الاصطناعي

يمكن تقسيم تحديات التنظيم القانوني إلى قسمين رئيسيين:

الفرع الأول: التحديات الإجرائية.

تتمثل أبرز التحديات في آليات صياغة القوانين وتطبيقها والتنسيق الدولي بشأنها ويمكن اختزالها في الآتي:

1. الفجوة الزمنية: وتتمثل في التباين الكبير بين التطور المتسارع للذكاء الاصطناعي، وببطء الدورة التشريعية نظراً لطول أمد المفاوضات الدبلوماسية اللازمة لإقرار القوانين والاتفاقيات، وهو ما يضع المشرع الدولي في حالة عجز مستمر عن المواكبة. (47)

2. **التفتت التشريعي الدولي:** غياب معايير عالمية موحدة وانقسام العالم إلى تكتلات قانونية متنافسة: أوروبي صارم يركز على تقييم المخاطر، وأمريكي مرن يعزز الابتكار ويقلل القيود، وصيني يكرّس السيادة الرقمية. (48)

3. **تجاوز الحدود وتنازع الاختصاص:** يُصعّب التداخل في منازعات الذكاء الاصطناعي تحديد المحكمة المختصة إقليمياً؛ نظراً لطبيعة نشاطه غير المادية التي تمتد عبر دولٍ عدة، مما يجعل حصر مكان النزاع أمراً بالغ التعقيد.

4. **صراع الابتكار والتقنين:** التخوف من أن تؤدي القواعد الصارمة إلى كبح الإبداع التكنولوجي، مما قد يدفع بالاستثمارات والشركات الناشئة إلى المغادرة.

الفرع الثاني: التحديات الموضوعية (الذاتية المرتبطة بطبيعة التقنية).

تتمثل في العقبات التقنية الفريدة للذكاء الاصطناعي والتي تعجز القوانين التقليدية عن استيعابها ولعل من أبرزها:

1. **معضلة "الصندوق الأسود":** تكمن المشكلة في غموض آليات اتخاذ القرار بالأنظمة الذكية وصعوبة تحديد المسؤولية، ويزداد الأمر تعقيداً برفض مطوريها الكشف عن شيفراتها المصدرية حماية لأسرارهم التجارية، مما يعيق عمليات الفحص الفني القضائي والرقابي. (49)

2. **أزمة المسؤولية القانونية:** حيث تنشبت المسؤولية القانونية عن أنظمة الأسلحة الذكية بين المطور والمبرمج والشركة المصنعة والقائد؛ وذلك لاستحالة مساءلة النظام جنائياً لانتهاء الإرادة لديه، وصعوبة إثبات القصد الجنائي لدى الأطراف البشرية المعنية. (50)

3. **التحيز الخوارزمي:** إعادة إنتاج الآلة للتحيزات البشرية، كالعرقية والجنسية، الموجودة في بيانات التدريب التاريخية.

4. **انتهاك الخصوصية والملكية الفكرية:** استخدام بيانات ومصنفات محمية في تدريب النماذج دون الحصول على إذن أصحابها.

ثالثاً- أزمة الضمير الإنساني (شرط مارتنز) (51*): يفرض القانون الدولي مراعاة "مقتضيات الضمير العام"، ويُعد تفويض الآلة في اتخاذ قرار سلب الحياة البشرية إهداراً لهذا الضمير، واختزالاً للكائن البشري في مجرد بيانات ضمن مصفوفة برمجية. (52)

المطلب الثاني: الجهود الدولية والإقليمية لتنظيم الذكاء الاصطناعي (دراسة مقارنة)

انقسم المجتمع الدولي بين مقارباتٍ تشريعيةٍ صارمةٍ تتبناها التكتلات الإقليمية، ومبادراتٍ مرنةٍ تقودها المنظمات الأممية.

الفرع الأول: المبادرات الدولية

أولاً: المقاربة الأوروبية وقانون الذكاء الاصطناعي:

1. الفلسفة التشريعية القائمة على تصنيف المخاطر: يُمثل قانون الذكاء الاصطناعي الأوروبي أول إطار قانوني شامل وملزم عالمياً لتنظيم التكنولوجيا، وتستند فلسفته إلى فرز الأنظمة وفق أربعة مستويات من المخاطر:

أ- المخاطر غير المقبولة (المحظورة تماماً): وتشمل أنظمة الذكاء الاصطناعي التي تُشكل تهديداً صريحاً لسلامة الأفراد وحقوقهم وسبل عيشهم، ويحظر قانون الذكاء الاصطناعي ثماني ممارسات، هي: استخدام الأساليب اللاواعية أو التلاعبية أو الخادعة - استغلال نقاط الضعف لدى الأفراد - أنظمة "التقييم الاجتماعي" - "تقييم المخاطر الجنائية للأفراد بناءً على التمييز فقط" - استخراج البيانات غير الموجه لقواعد بيانات التعرف على الوجوه - تقنيات التعرف على المشاعر في أماكن العمل والمؤسسات التعليمية - التصنيف البيومترى لاستنتاج خصائص محمية - التعرف البيومترى عن بُعد في الوقت الفعلي لأغراض إنفاذ القانون في الأماكن العامة (مع استثناءات أمنية).⁽⁵³⁾

ب - المخاطر العالية: تخضع أنظمة الذكاء الاصطناعي عالية المخاطر لرقابة تشريعية صارمة بموجب المادة (6) والملحق الثالث من قانون الذكاء الاصطناعي الأوروبي، نظراً لما تشكله من تهديدات محتملة على السلامة والحقوق الأساسية. وتتوزع مجالات استخدامها على النحو الآتي:

❖ مجالات الاستخدام عالي المخاطر.

الأمن والبنية التحتية - السيادة والعدالة - الحقوق المدنية والاجتماعية.

❖ التزامات الامتثال القانوني: تُلزم اللائحة الجهات المطورة باستيفاء سبعة معايير موضوعية

قبل طرح هذه الأنظمة في السوق:

- إدارة المخاطر: وضع نظم دورية وشاملة لتقييم المخاطر والتخفيف من آثارها.
- حوكمة البيانات: ضمان جودة وموثوقية البيانات المدخلة للحد من النتائج التمييزية والانحياز الفني.

- التوثيق الفني: إعداد وثائق مفصلة تُمكن السلطات الرقابية من تقييم مدى الامتثال.
- الشفافية الإجرائية: تسجيل الأنشطة إلكترونياً لضمان تتبع المخرجات، مع توفير إرشادات واضحة للمستخدمين.
- الرقابة البشرية: إدماج آليات رقابة بشرية دائمة وفعالة أثناء تشغيل النظام.
- الحصانة التقنية: تحقيق مستويات متقدمة من المتانة والدقة والأمن السيبراني. (54)
- ج - **المخاطر المحدودة:** تشير إلى التقنيات التي لا تهدد السلامة، لكنها قد تضلل المستخدم؛ لذا يفرض القانون عليها التزامات بالشفافية، كإبلاغ المستخدمين بأنهم يتعاملون مع آلة، ووسم المحتوى المؤلّد آلياً. (55)
- د - **المخاطر الدنيا أو المنعدمة:** لا يفرض قانون الذكاء الاصطناعي قيوداً إضافية على الأنظمة ذات "المخاطر الضئيلة"، كالألعاب وفلاتر البريد الإلكتروني؛ وذلك تشجيعاً للابتكار واكتفاء بالتشريعات القائمة لكونها لا تهدد حقوق الأفراد. (56)

2. مدى تأثير القواعد الأوروبية كمعيار قانوني عالمي (أثر بروكسل)

- يمتد قانون الذكاء الاصطناعي الأوروبي ليصبح معياراً تنظيمياً عالمياً بفضل "أثر بروكسل"، الذي يمكن الاتحاد الأوروبي من توجيه الأسواق الدولية بشكل غير مباشر عبر آليتين:
- أ - **امتداد النطاق الجغرافي العابر للحدود:** إذ لا يُطبّق قانون الذكاء الاصطناعي للاتحاد الأوروبي داخل نطاقه فقط بل يمتد ليشمل الشركات العالمية متى ما أُتيحت مخرجات أنظمتها داخل الاتحاد.
 - ب - **تصدير المعايير بحكم الأمر الواقع:** يُجبر التشريع الشركات العالمية على موافقة معاييرها مع الاشتراطات الأوروبية تقادياً للغرامات الباهظة، مما يعزز مكانة النموذج الأوروبي كمعيار دولي حاكم للذكاء الاصطناعي. ومع ذلك، يؤثر التوسع التنظيمي الأوروبي خارج الحدود على الحقوق الرقمية وسياقات استخدام التكنولوجيا عالمياً، مما يرسخ "أثر بروكسل" كأداة لإعادة صياغة الحوكمة الرقمية الدولية. (57)

الفرع الثاني: المبادرات الأممية والدولية غير الملزمة

أولاً: التوصيات الصادرة عن اليونسكو ومجلس حقوق الإنسان

1. **أخلاقيات الذكاء الاصطناعي (اليونسكو):** اعتمدت اليونسكو عام 2021 وثيقةً لحوكمة الذكاء الاصطناعي أخلاقياً؛ بهدف تعزيز الشمول، وحظر المراقبة الجماعية، وحماية الأقليات، ومع ذلك، فإن الطبيعة غير الملزمة للوثيقة أتاحت لبعض الدول الموقعة، مثل الصين، الاستمرار في ممارساتها المنتهكة لهذه المبادئ. (58)

2. تقارير مجلس حقوق الإنسان:

تحدّر قرارات مجلس حقوق الإنسان من مخاطر التوسع غير المنضبط للذكاء الاصطناعي في مجال المراقبة الرقمية على الحريات الأساسية، وتؤكد أن حوكمته باتت ضرورة ملحة لحماية الحقوق المدنية.⁽⁵⁹⁾ وفي هذا السياق، دعت الأمم المتحدة إلى فرض حظر مؤقت⁽⁶⁰⁾ على تقنيات التعرّف على الوجوه في الأماكن العامة، إلى حين ضمان التزامها بالمعايير القانونية والأخلاقية الصارمة وفق الشروط الآتية:

أ - إثبات الامتثال الحقوقي: إلزام الدول والشركات المطورة بتقديم أدلة دامغة تثبت أن هذه التقنيات لا تنتهك الحق في الخصوصية وحرمة الحياة الشخصية للأفراد.

ب - حماية الحق في التجمع السلمي: ضمان عدم استخدام هذه الأدوات لترهيب المتظاهرين أو تعقب المشاركين السلميين، نقادياً لخلق "تأثير مروع" يقيد حرية التعبير والتظاهر.

ج - تقييم الأثر المسبق: إخضاع أي نظام ذكاء اصطناعي مخصص للمراقبة لتقييمات أثر شاملة ومستقلة تشرف عليها جهات حقوقية وقضائية قبل السماح بتداوله.

د - معالجة التحيز الخوارزمي: تطوير معايير تقنية تضمن خلو هذه البرمجيات من عيوب التمييز حسب العرق والجنس، والتي أثبتت التقارير أنها تؤدي إلى اعتقالات خاطئة واستهداف غير عادل للأقليات.⁽⁶¹⁾ وعليه، تعكس صياغة القرارات الأممية إدراكاً متزايداً لأهمية حماية حقوق الإنسان، والتمييز بين الاستخدام المشروع للتكنولوجيا وبين ممارسات المراقبة الشاملة.

ثانياً: دور مدونات السلوك وأثر القوانين المرنة.

1. مرونة التشريع التقني: يلجأ المجتمع الدولي إلى «القانون المرن»، والإعلانات السياسية، ومدونات السلوك الطوعية للشركات؛ لتجاوز بطء إجراءات المعاهدات الدولية التقليدية.

2. محدودية الفعالية: رغم مرونة هذه الأدوات وسرعتها، فإن افتقارها إلى الإلزام والجزاء يجعلها عاجزة عن ردع الدول والشركات متى تعارضت مع مصالحها.

الفرع الثالث: التنافس الجيوسياسي وأثره على صياغة الاتفاقيات الدولية

أولاً: الصراع التكنولوجي بين القوى الكبرى (الولايات المتحدة والصين)

يفرض الصراع البنيوي بين أمريكا والصين حول الذكاء الاصطناعي، بوصفه أداة لتشكيل النظام الدولي، عوائق جوهريّة أمام التوصل إلى معاهدات دولية موحدة لتنظيمه.

1. المقاربة الأمريكية (حمائية الابتكار القائمة على السوق الحر): تُفضّل واشنطن الاعتماد على التشريعات المرنة والأوامر التنفيذية لتعزيز ابتكار شركاتها؛ ضماناً لهيمنتها العالمية وقطعاً للطريق أمام أي تفوق تكنولوجي خارجي.

2. المقاربة الصينية (سيادة الدولة والرقابة المجتمعية والأمن القومي): على النقيض تماماً، تنظر بكين إلى الذكاء الاصطناعي بوصفه أداة سيادية للأمن والرقابة، لذا تفرض قيوداً صارمة على الخوارزميات والمحتوى لضمان الاستقرار السياسي.

هذا الانقسام الإيديولوجي العميق بين "النموذج الليبرالي الابتكاري" و"النموذج السلطوي الموجه" يخلق فجوة تنظيمية يستحيل معها صياغة قانون دولي شامل وموحد.⁽⁶²⁾

ثانياً: استغلال الذكاء الاصطناعي عسكرياً والأنظمة الفتاكة ذاتية التشغيل. أفرز دمج الذكاء الاصطناعي في المنظومات العسكرية المعاصرة، عوضاً عن الآلات التقليدية، تحديات استراتيجية وأخلاقية غير مسبقة في تاريخ النزاعات.

1. معضلة نزع السلاح الرقمي: حيث تعاني الدبلوماسية الدولية من حالة شلل تجاه حظر استخدام الذكاء الاصطناعي في الأغراض العسكرية، نتيجة رفض القوى الكبرى تقييد خوارزمياتها الدفاعية خشية فقدان تفوقها الاستراتيجي، وهو ما أوجع سباق تسلح رقمياً معقداً.

2. تهديد قواعد القانون الدولي الإنساني: إذ يُثير النشر الميداني للأنظمة الفتاكة ذاتية التشغيل أزمة أخلاقية وقانونية؛ نظراً لعجزها البنيوي عن الامتثال للمبادئ الأساسية لقوانين الحرب، وتحديداً: أ - مبدأ التمييز: إذ تفتقر الآلة والبرمجيات الرياضية إلى القدرة الإنسانية والوعي السياقي اللازمين للفصل الدقيق بين المقاتلين العسكريين والمدنيين، لاسيما في حروب المدن والنزاعات غير المتناظرة. ب - مبدأ التناسب في استخدام القوة: تعجز الخوارزميات عن تقدير حجم الأضرار الجانبية التي تلحق بالمدنيين مقارنة بالميزة العسكرية المباشرة المرجوة؛ فهذا التقدير يتطلب حساً إنسانياً وقيماً تفتقر إليه الأسطر البرمجية.⁽⁶³⁾

وعليه، يهدّد هذا الخلل بانهيار اتفاقيات جنيف وتبديد المسؤولية الجنائية عند ارتكاب الآلة مجازر، إذ تضيع المحاسبة بين القائد والمبرمج والمصنّع، مما يجعل حروب المستقبل بلا رادع.

المطلب الثالث: الآفاق المستقبلية والآليات المقترحة لتطوير التنظيم الدولي

تتطلب مواجهة تحديات الذكاء الاصطناعي آليات دولية مرنة تُعزز السيادة الإنسانية المشتركة وذلك من خلال:

الفرع الأول: تدويل الرقابة وإنشاء وكالة عالمية للذكاء الاصطناعي.

أولاً: مقترحات تأسيس منظمة أممية متخصصة لمراقبة وتفتيش الأنظمة الفائقة

1. النموذج التنظيمي المستوحى: حيث يُطالب الفقه الدولي بإنشاء "وكالة دولية للذكاء الاصطناعي"

على غرار الوكالة الدولية للطاقة الذرية؛ نظراً لمخاطره الوجودية التي تضاهي تهديدات الأسلحة النووية.

2. المهام الرقابية والتفتيشية: تُمنح الوكالة المقترحة صلاحيات التفتيش على مراكز البيانات،

ومراقبة أنظمة الحوسبة، ومنع تطوير الخوارزميات الخطرة على المستوى الدولي.⁽⁶⁴⁾

ثانياً: وضع معايير دولية موحدة لمنح تراخيص التشغيل للأنظمة عالية الخطورة.

1. نظام التراخيص العالمي: تهدف هذه الآلية إلى منع ظهور "ملاذات آمنة للذكاء الاصطناعي"،

حيث قد تلجأ الشركات إلى الدول ذات الرقابة الضعيفة لتطوير أنظمتها هرباً من القوانين الصارمة.

2. شروط منح الترخيص: يُحظر إطلاق الذكاء الاصطناعي الفائق قبل خضوعه لاختبارات أمان

دولية تضمن حصانته ضد الاختراق، وخلوه من التحيز، ووجود بروتوكول للحظر التلقائي في حال

فقدان السيطرة عليه.⁽⁶⁵⁾

الفرع الثاني: تبني التشريعات المرنة ومبدأ "الرقابة البشرية الدائمة"

أولاً: صياغة أطر قانونية قابلة للتحديث المستمر لمواكبة قفزات التكنولوجيا.

1. التشريع الديناميكي: استبدال القوانين الجامدة بأطر مرنة تمنح الهيئات التنظيمية صلاحية التحديث

الدوري لمواكبة القفزات التكنولوجية المتسارعة، مثل تقنيات الوكلاء المستقلين.

2. المختبرات التنظيمية: التوسع في توفير بيانات تجريبية آمنة لاختبار تطبيقات الذكاء الاصطناعي

تحت إشراف قانوني؛ لتقييم آثارها الحقوقية والاجتماعية قبل طرحها للجمهور.⁽⁶⁶⁾

ثانياً: إلزامية وجود العنصر البشري في القرارات الحساسة.

1. مفهوم التدخل البشري الحتمي: يمثل هذا المبدأ حجر الزاوية في آفاق التطوير القانوني، حيث

يُحظر قانوناً وعالمياً ترك القرار النهائي والقطعي للآلة في المجالات السيادية والحيوية التي تمس

حياة الإنسان وحرية.

2. مجالات التطبيق الإلزامية:

- **المجال العسكري:** حظر تفويض قرار القتل للأنظمة المستقلة، وحصر تحديد الأهداف وإطلاق النار بالقائد البشري.
- **المجال القضائي والأمني:** حظر إصدار أحكام الإدانة أو أوامر التوقيف بناءً على توصيات خوارزمية دون مراجعة وتدقيق قضائي بشري كامل.
- **المجال الطبي:** الإبقاء على التشخيص الخوارزمي كأداة استشارية مساعدة فقط، مع تحميل الطبيب البشري المسؤولية القانونية النهائية عن القرار العلاجي. (67)

الفرع الثالث: صياغة معاهدة دولية شاملة لحماية حقوق الإنسان الرقمية.

أولاً: سبل توفير الحماية القانونية ضد التحيز الخوارزمي والتزييف العميق عالمياً.

1. **سد الفراغ التشريعي الدولي:** إبرام "معاهدة الحقوق الرقمية والأمان الخوارزمي" الملزمة، لتجريم تقنيات التزييف العميق التي تستهدف الاستقرار السياسي، أو تُستخدم في التشهير والابتزاز.

2. **مكافحة التمييز الرقمي:** إلزام الشركات والجهات الحكومية بمراجعة دورية لأكواد أنظمتها لضمان حياديتها، مع فرض عقوبات رادعة على أي نظام يثبت ممارسته للتمييز العرقي أو الاجتماعي الممنهج.

ثانياً: تفعيل آليات المسؤولية الدولية للدول التي تسيء استخدام الذكاء الاصطناعي

يتطلب المشهد التكنولوجي المعاصر تفعيل آليات المسؤولية الدولية للدول التي تسيء استخدام الذكاء الاصطناعي وذلك عبر مسارين متكاملين:

1. تأصيل المسؤولية عن الأفعال السيبرانية والخوارزمية:

يستوجب التطور الرقمي إقرار المسؤولية الدولية الشاملة للدول عن أضرار الذكاء الاصطناعي العابرة للحدود استناداً إلى توصيات اليونسكو، مع إلزامها بمبدأ "العناية الواجبة" لضمان عدم اتخاذ لامركزية الخوارزميات ذريعةً للتوصل من التزاماتها.

2. **تفعيل القضاء الدولي وتكييف الهجمات كعدوان مسلح:** يتطلب إرساء العدالة الرقمية تفعيل دور القضاء الدولي، وتمكين محكمة العدل الدولية من النظر في النزاعات الناجمة عن الانتهاكات الخوارزمية الجسيمة عابرة الحدود.

وفي هذا السياق، يتعين سد الفراغ التشريعي الدولي عبر إعادة تفسير المادة الثانية (الفقرة الرابعة) من ميثاق الأمم المتحدة لتستوعب الأنماط المستحدثة لاستخدام القوة؛ بحيث تُصنّف الهجمات السيبرانية التي تُنفَّذ عبر أنظمة الذكاء الاصطناعي التوليدي والتي تستهدف شلّ المنظومات

الاقتصادية أو تدمير البنى التحتية الحيوية والمرافق الاستراتيجية بوصفها "عدواناً إلكترونياً صريحاً" وعملاً من أعمال القوة المحظورة، مما يترتب المسؤولية الدولية الموجبة للتعويض، ويُشرعن فرض العقوبات الدولية على الدول المُسهلة لهذه الهجمات.

الخاتمة

تخلص هذه الدراسة، بناءً على التحديات القانونية والأمنية والأخلاقية التي تثيرها تطبيقات الذكاء الاصطناعي إلى النتائج والتوصيات الآتية:

أولاً: النتائج

1. قصور القواعد التقليدية: عجز قواعد المسؤولية الدولية الكلاسيكية عن استيعاب التحولات البنيوية التي أحدثها الذكاء الاصطناعي في العلاقات الدولية.
2. تحديات الإسناد والسببية: صعوبة تحديد الفاعل المسؤول وإثبات العلاقة السببية في المخالفات الدولية، نتيجة استقلالية الآلة وغموض الخوارزميات.
3. تعدد الفاعلين والفراغ التشريعي: تظل الدولة مسؤولة عن الأنظمة الخاضعة لسيطرتها، بيد أن تنامي دور الشركات التكنولوجية يكرس فراغاً تشريعياً عابراً للحدود في ظل غياب أطر دولية ملزمة.
4. سباق التسلح الرقمي: تحول الفضاء الرقمي العسكري إلى ساحة مواجهة محمومة ومستترة، في ظل امتناع القوى العظمى عن حظر الأنظمة ذاتية التشغيل خشية التأثير على توازناتها الاستراتيجية.

ثانياً: التوصيات المقترحة

1. تقنين المسؤولية الموضوعية: وذلك عبر تبني نهج فقهي وتشريعي يعتمد نظام المسؤولية الدولية الموضوعية القائمة على المخاطر التقنية بدلاً من معيار الخطأ التقليدي.
2. إبرام معاهدة دولية: من خلال صياغة اتفاقية دولية شاملة لتنظيم الذكاء الاصطناعي وتحديد معايير إسناد المسؤولية بدقة.
3. تأسيس وكالة رقابية دولية: من خلال التعجيل بإنشاء "الوكالة الدولية للذكاء الاصطناعي"، ومنحها صلاحيات التفتيش التقني على مراكز البيانات الكبرى والحوسبة الفائقة.
4. عصرنه القضاء الدولي: وذلك بتفعيل دور محكمة العدل الدولية في النزاعات الخوارزمية، وتحديث قواعد الإثبات باعتماد الأدلة الرقمية، واستحداث لجان تحكيم فنية متخصصة.

قائمة المراجع

المراجع العربية

أولاً: الكتب

1. إبراهيم محمد بن حمود الزنداني. *النكاء الاصطناعي في مسطرة التشريعات والمعاهدات الدولية*. ط. 1. بيروت، لبنان: المركز العربي للأبحاث ودراسة السياسات، 2026.
2. شارل روسو. *القانون الدولي العام*. ترجمة شكر الله خليفة وعبد المحسن سعد. بيروت: الأهلية للنشر والتوزيع، 1987.
3. علي عبد القادر القهوجي. *القانون الدولي الجنائي: أهم الجرائم والمحاكم الدولية*. بيروت: منشورات الحلبي الحقوقية، 2012.
4. صورية بوربابة وخديجة لحلو. «الإطار القانوني للنكاء الاصطناعي بين متطلبات الابتكار وضمانات المسؤولية القانونية». في *أشغال المؤتمر الدولي: التحديات القانونية لتكنولوجيا المعلومات في عصر النكاء الاصطناعي والتحول الرقمي*. برلين: المركز الديمقراطي العربي، 2024.
- ثانياً: الرسائل العلمية
1. إسحاق العشعاش. *منظومات الأسلحة الفتاكة ذاتية التشغيل في القانون الدولي*. أطروحة دكتوراه، جامعة الجزائر، الجزائر، 2024.
2. أسعد كاظم وحيش الصالحي. *التنظيم الدولي لإبرام الاتفاقيات الدولية لدى الدولة الاتحادية*. رسالة ماجستير غير منشورة، جامعة بابل، العراق، 2013.
3. هاجر عمور، *النكاء الاصطناعي والقانون* رسالة ماجستير غير منشورة، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2025.
- ثالثاً: المقالات المنشورة في المجلات
1. أزرو محمد رضا، «المسؤولية عن أضرار السيارات ذاتية القيادة»، مجلة القانون العام الجزائري والمقارن، المجلد 11، العدد 3، 2023.
2. إسماعيل سلطاني، «الأسلحة ذاتية التشغيل من منظور القانون الدولي الإنساني: بين مشروعية الاستخدام وحتمية الامتثال»، مجلة أبحاث قانونية وسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحيى (جيجل)، الجزائر، المجلد 10، العدد 1، 2025.
3. خالد ناصر المازمي. «الأطر القانونية للنكاء الاصطناعي في القانون الدولي». *مجلة جامعة الشارقة للعلوم القانونية*، الإمارات، المجلد 23، العدد 1، 2026.
4. رنا صفوت الكجك. «النكاء الاصطناعي وتأثيره في الحرب». *مجلة القرار للبحوث العلمية المحكمة*، المجلد 7، العدد 21، 2025.
5. رسل علاء داود العكيدي وحيدر أدهم الطائي. «أثر شرط مارتينز في التفسير التطوري للتكنولوجيا العسكرية الحديثة: دراسة تحليلية». *المجلة الأكاديمية للبحث القانوني*، المجلد 14، العدد 1، 2023.
6. زينب بنور، المسؤولية القانونية عن أخطاء أنظمة الذكاء الاصطناعي. «مجلة القانون الدولي للدراسات البحثية»، المجلد 7، العدد 21، 2026.
7. عبد المجيد علي أحمد عثمان. «قواعد المسؤولية الدولية». *مجلة القرطاس للعلوم التربوية والإنسانية*، ليبيا، العدد 11، 2020.

8. عبير سالم عبد إله». الذكاء الاصطناعي بين حداثة المفاهيم وتقليدية قواعد المسؤولية. «مجلة العلوم والدراسات الإنسانية، كلية الآداب والعلوم، المرج، جامعة بنغازي، العدد 85، 2025.
 9. فاتن علي بشينة». المسؤولية الدولية عن أضرار استخدام الأسلحة المدعمة بتقنيات الذكاء الاصطناعي. «مجلة المنتدى الأكاديمي، الأكاديمية الليبية للدراسات العليا، المجلد 9، العدد 3، 2025.
 10. محمد إبراهيم عبد الفتاح يس». المسؤولية الموضوعية عن المخاطر المستحدثة. «مجلة بنها للعلوم الإنسانية، جامعة بنها، مصر، المجلد 1، العدد 1، الجزء 2، 2022.
 11. محمد جمال عزاز أبو رحاب، المسؤولية المدنية الدولية الناشئة عن قرارات الذكاء الاصطناعي: إشكالية الفعل الضار العابر للحدود، مجلة البحوث القانونية والاقتصادية، جامعة بني سويف، مصر، المجلد 37، العدد 2، 2025.
 12. محمد عبد القادر مصباح الشقلاف، فعالية شرط مارتينز في سد الثغرات التي تحدث في قواعد القانون الدولي الإنساني، مجلة الأصاله، الجمعية الليبية للعلوم التربوية والإنسانية، المجلد 7، العدد 12، 2025.
- رابعاً: التقارير والوثائق القانونية الدولية
1. اتفاقية المسؤولية الدولية عن الأضرار التي تسببها الأجسام الفضائية، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم A/RES/2777(XXVI) في 29 ديسمبر 1971 (دخلت حيز النفاذ عام 1972).
 2. الأمم المتحدة، حوكمة الذكاء الاصطناعي من أجل الإنسانية: التقرير النهائي. نيويورك: الأمم المتحدة، 2024.
 3. الأمم المتحدة. المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة «الحماية والاحترام والانتصاف»، 201.
 4. اللجنة الدولية للصليب الأحمر. موقف اللجنة الدولية للصليب الأحمر من منظومات الأسلحة ذاتية التشغيل. جنيف: اللجنة الدولية للصليب الأحمر، 2021.
 5. لجنة القانون الدولي، تقرير لجنة القانون الدولي عن أعمال دورتها الثامنة والخمسين». الفصل الخامس: المسؤولية الدولية عن النتائج الضارة الناجمة عن أنشطة لا يحظرها القانون الدولي. وثيقة الأمم المتحدة رقم A/61/10، 2006.
 6. لجنة القانون الدولي، مشروع المواد بشأن مسؤولية المنظمات الدولية، في تقرير لجنة القانون الدولي عن أعمال دورتها الثالثة والستين، قرار الجمعية العامة للأمم المتحدة رقم A/RES/66/100، 2011.
 7. لجنة القانون الدولي». مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً». الفصل الرابع: مسؤولية دولة عن فعل دولة أخرى. في تقرير لجنة القانون الدولي عن أعمال دورتها الثالثة والخمسين. وثيقة الأمم المتحدة رقم A/56/10، 2001.
 8. مجلس حقوق الإنسان، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، الدورة الحادية والأربعون، 24 يونيو-12 يوليو 2019. وثيقة الأمم المتحدة رقم A/HRC/41/35، البند 3 من جدول الأعمال.
 9. مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي: تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، وثيقة رقم A/HRC/51/17، 4 أغسطس 2022.
 10. مركز العودة الفلسطيني. Algorithms of Death: How AI Fuels Mass Killings in Gaza. تقرير سياسات. لندن: مركز العودة الفلسطيني، 2025.
 11. منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)، التوصية الخاصة بأخلاقيات الذكاء الاصطناعي، باريس: اليونسكو، 2021. unesco.org.
 12. نظام روما الأساسي للمحكمة الجنائية الدولية، اعتمد في 17 يوليو 1998، مجموعة معاهدات الأمم المتحدة، المجلد 2187، 25.

المراجع الأجنبية

أولاً: الكتب

1. Crawford, James. *State Responsibility: The General Part*. Cambridge: Cambridge University Press, 2013.
2. McCarthy, John. *Programs with Common Sense*. Stanford: Stanford University Press, 1960.
- Pasquale, Frank. *The Black Box Society*. Harvard: Harvard University Press, 2015.
3. Russell, Stuart J., and Peter Norvig. *Artificial Intelligence: A Modern Approach*. 3rd ed. New Jersey: Prentice Hall, 2010.
4. Woolley, Samuel. *The Reality Game: How the Next Wave of Technology Will Break the Truth*. New York: Public Affairs, 2020.

ثانياً: المقالات والدراسات الأكاديمية

1. Chung, Jason, and Amanda Zink. "Hey Watson—Can I Sue You for Malpractice? Examining the Liability of Artificial Intelligence in Medicine." *Asia Pacific Journal of Health Law & Ethics* 11, no. 2 (2018).
2. Lancieri, Filippo, Laura Edelson, and Stefan Bechtold. "AI Regulation: Competition, Arbitrage & Regulatory Capture." *Theoretical Inquiries in Law* 26, no. 1 (2025). <https://doi.org/>.
3. Robinson, Mark. "The Establishment of an International AI Agency: An Applied Solution to Global AI Governance." *International Affairs* 101, no. 4 (2025).

ثالثاً: التقارير والأوراق المؤسسية والبحثية

1. Bo, Marta, Laura Bruun, and Vincent Boulanin. "Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems: On Accountability for Violations of International Humanitarian Law Involving AWS." Stockholm International Peace Research Institute (SIPRI), 2023.
2. Clark, Michael. "Prohibited AI Practices Under Article 5 of the EU AI Act: Scope, Enforcement, and Compliance Methodology." Research Paper, Standard Intelligence Limited, June 2026. *SSRN Electronic Journal*.
3. CrowdStrike. "2026 CrowdStrike Global Threat Report: AI Accelerates Adversaries and Reshapes the Attack Surface." News release, February 24, 2026.
4. Dastin, Jeffrey. "Insight - Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women." *Reuters*, October 10, 2018.
5. European Commission. *Liability for Artificial Intelligence and Other Emerging Digital Technologies*. Expert Group on Liability and New Technologies, 2019.
6. European Parliament and Council of the European Union. "Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." *Official Journal of the European Union*, L series, July 12, 2024.
7. European Parliament. "Resolution on Civil Law Rules on Robotics." 2017.
8. European Parliamentary Research Service (EPRS). *The Global Reach of the EU's Approach to Digital Transformation*. Briefing. Brussels: European Parliament, 2024.
9. *Factory at Chorzów (Merits)*. Judgment, September 13, 1928. PCIJ, Series A, No. 17.
10. Human Rights Watch. *Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook*. New York: Human Rights Watch, 2023.
11. Lee, Robert M., Michael J. Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid." White paper, SANS Industrial Control Systems and E-ISAC, March 18, 2016.
12. Madiega, Tambiama. *Artificial Intelligence Act*. Briefing. European Parliamentary Research Service (EPRS), September 2024.

13. New York State Department of Financial Services. *Report on Apple Card Investigation*. New York: NYSDFS, March 2021.
14. Shaik, Ali Sadhik. "Sandboxes, Safe Harbors, and Sunset Clauses: Designing Adaptive Regulation for AI That Doesn't Become Obsolete on Arrival." Working Paper, Golden Gate University, 2024.
15. Siegmann, Charlotte, and Markus Anderljung. *The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market*. Centre for the Governance of AI, 2022.
16. SIPRI. *Artificial Intelligence and International Security*. Stockholm: Stockholm International Peace Research Institute, 2020.
17. Stango, Antonio. "The Geopolitical Competition Between China and the U.S. in New Technologies." *SOG Working Paper Series*, no. SOG-WP12/2024. Rome: Luiss School of Government, May 2024.
18. U.S. House of Representatives. *The Equifax Data Breach*. Committee on Oversight and Government Reform. Washington, DC: U.S. GPO, December 2018.
19. *United States of America v. Meta Platforms, Inc.* No. 1:22-cv-05187 (S.D.N.Y. June 21, 2022) [Complaint and Settlement Agreement].

الهوامش

- ¹ انظر John McCarthy, *Programs with Common Sense*, Stanford University Press, 1960, p. 12.
- ² انظر European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 of 13 June 2024 laying down Harmonised rules on artificial intelligence (Artificial Intelligence Act)" *Official Journal of the European Union*, L series, recital 3 p 46.
- ³ انظر Frank Pasquale, *The Black Box Society*, Harvard University Press, 2015, p. 18.
- ⁴ انظر فاتن علي بشينة، المسؤولية الدولية عن اضرار استخدام الأسلحة المدعمة بتقنيات الذكاء الاصطناعي، مجلة المنتدى الأكاديمي، الأكاديمية الليبية للدراسات العليا، المجلد 9، العدد 3، 2025، ص 5.
- ⁵ انظر هاجر عمور، الذكاء الاصطناعي والقانون، رسالة ماجستير غير منشورة، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2025، ص 9.
- ⁶ انظر Russell, Stuart J., and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed., Prentice Hall, New Jersey, 2010, p. 27–32.
- ⁷ SIPRI Report, *Artificial Intelligence and International Security*, Stockholm, 2020, p. 41.
- ⁸ تقرير وكالة الإنذار المشترك - (DSA) مايو 2023 الذكاء الاصطناعي يعتبر "الخطر الأكبر" على الانتخابات في الأعوام القادمة، أيضا تقرير اليونسكو "Freedom of expression, artificial intelligence and elections" - (2025) ركز على استغلال الذكاء الاصطناعي للتضليل في الحملات الانتخابية والتأثير على العمليات الديمقراطية، كذلك تقرير شبكة BOOM الهندية لتدقيق الحقائق (2025) إحصائية صارخة: ارتفعت نسبة المحتوى المُنتج بالذكاء الاصطناعي ضمن الأخبار المفبركة من 8.35% عام 2024 إلى 20.5% عام 2025.
- ⁹ انظر Samuel Woolley, *The Reality Game: How the Next Wave of Technology Will Break the Truth*, Public Affairs, 2020, p. 73.
- ¹⁰ انظر شارل روسو القانون الدولي العام ترجمة شكر الله خليفة، عبد المحسن سعد، الاهلية للنشر والتوزيع بيروت 1987 ص 106
- ¹¹ انظر لجنة القانون الدولي، "تقرير لجنة القانون الدولي عن أعمال دورتها الثامنة والخمسين (2006)"، الفصل الخامس: المسؤولية الدولية عن النتائج الضارة الناجمة عن أنشطة لا يحظرها القانون الدولي، الأمم المتحدة، وثيقة رقم A/61/10، 2006، ص. 90-100
- ¹² انظر اسعد كاظم وحيش الصالحي، التنظيم الدولي لابرار الاتفاقيات الدولية لدى الدولة الاتحادية، رسالة ماجستير غير منشورة جامعة بابل العراق 2013، ص 189: 190
- ¹³ انظر عبد المجيد علي أحمد عثمان، قواعد المسؤولية الدولية، مجلة القرطاس للعلوم التربوية والإنسانية، ليبيا، العدد 11، 2020، ص 66

- ¹⁴ انظر لجنة القانون الدولي، "مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً"، المادتان 34، 35، في تقرير لجنة القانون الدولي عن أعمال دورتها الثالثة والخمسين، وثيقة الأمم المتحدة رقم. A/56/10 (2001)
- ¹⁵ انظر علي عبد القادر القهوجي، القانون الدولي الجنائي: أهم الجرائم والمحاكم الدولية، منشورات الحلبي الحقوقية، بيروت، 2012، ص 89
- ¹⁶ لجنة القانون الدولي، المرجع السابق، م 2
- ¹⁷ لجنة القانون الدولي، "مشروع المواد بشأن مسؤولية المنظمات الدولية"، في تقرير لجنة القانون الدولي عن أعمال دورتها الثالثة والستين، قرار الجمعية العامة للأمم المتحدة رقم (2011) A/RES/66/100، المادة 3
- ¹⁸ نظام روما الأساسي للمحكمة الجنائية الدولية، اعتمد في 17 يوليو 1998، مجموعة معاهدات الأمم المتحدة، المجلد 2187، المادة 25.
- ¹⁹ لجنة القانون الدولي، المرجع نفسه، المواد 4، 5، 6.
- ²⁰ لجنة القانون الدولي، "مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً"، الفصل الرابع: مسؤولية دولة عن فعل دولة أخرى، مرجع سبق ذكره، المواد 16، 17، 18
- ²¹ انظر James Crawford, *State Responsibility: The General Part* (Cambridge: Cambridge University Press, 2013), 142-145
- ²² اتفاقية المسؤولية الدولية عن الأضرار التي تسببها الأجسام الفضائية، اعتمدت في 29 ديسمبر 1971 (ودخلت حيز النفاذ عام 1972)، وثيقة الأمم المتحدة رقم A/RES/2777(XXVI)، المادة الثانية
- ²³ محمد جمال عزاز أبو رحاب، "المسؤولية المدنية الدولية الناشئة عن قرارات الذكاء الاصطناعي" إشكالية الفعل الضار العابر للحدود"، مجلة البحوث القانونية والاقتصادية، جامعة بني سويف مصر، المجلد 37، العدد 2، 2025، ص. 350، 351
- ²⁴ انظر European Commission, Expert Group on Liability and New Technologies – New Technologies Formation, *Liability for Artificial Intelligence and Other Emerging Digital Technologies* (2019) p. 20
- ²⁵ انظر محمد جمال عزاز أبو رحاب، مرجع سبق ذكره، ص 360: 363.
- ²⁶ انظر Factory at Chorzów (Merits) Judgment, 13 September 1928, PCIJ, Series A, No. 17, p. 61
- ²⁷ انظر خالد ناصر المازمي، الأطر القانونية للذكاء الاصطناعي في القانون الدولي، بحث منشور في مجلة جامعة الشارقة للعلوم القانونية، الإمارات، المجلد 23، العدد 1، يناير/مارس 2026، ص 351 وما بعدها.
- ²⁸ انظر في ذات المعنى عبير سالم عبد إله، الذكاء الاصطناعي بين حداثة المفاهيم وتقليدية قواعد المسؤولية، مجلة العلوم والدراسات الإنسانية، كلية الآداب والعلوم المرج، جامعة بنغازي، العدد 85 ص 23: 26.
- ²⁹ انظر في ذات المعنى خالد المازمي، مرجع سبق ذكره، ص 350 وما بعدها الأخطاء الطبية التي سببت أضراراً للمرضى، انظر Jason Chung and Amanda Zink, "Hey Watson — Can I Sue You for Malpractice? Examining the Liability of Artificial Intelligence in Medicine," *Asia Pacific Journal of Health Law & Ethics* 11, no. 2 (2018) p. 73 and following.
- ب - المسؤولية عن الأضرار المادية والجسدية للمركبات ذاتية القيادة: تسببت أنظمة القيادة الذاتية في سيارات "أوبر" و"تسلا" في وقوع حوادث سير مميتة للمشاة والركاب؛ بسبب عجز المستشعرات عن تمييز الأجسام في ظروف معينة، مما يُرتب على الشركات مسؤولية مدنية وجنائية ناتجة عن عيوب التصنيع والبرمجة. انظر في ذات المعنى ازرو محمد رضا، "المسؤولية عن أضرار السيارات ذاتية القيادة"، *مجلة القانون العام الجزائري والمقارن*، المجلد 11، العدد 3، 2025، ص 76-77. ج - المسؤولية القانونية عن انتهاك الخصوصية وحماية البيانات: التحيز والتمييز الخوارزمي: واجهت شركة "أمازون" انتقادات قانونية إثر تطويرها خوارزمية للتوظيف أثبتت تحيزاً ضد النساء واستبعاداً تلقائياً لطلباتهن، مما رتب على الشركة مسؤولية قانونية لمخالفتها مبادئ العدالة وتكافؤ الفرص، وتسببها في أضرار معنوية ومهنية انظر. Jeffrey Dastin, "Insight – Amazon scraps secret AI recruiting tool that showed bias against women," *Reuters*, October 10, 2018

³⁰ من هذه الصور أ. المسؤولية العقدية والتقصيرية عن الأخطاء الطبية: أدى اعتماد نظام الذكاء الاصطناعي "واتسون (Watson)" التابع لشركة IBM على بيانات طبية افتراضية -بدلاً من الواقعية- إلى تقديم توصيات علاجية خاطئة وخطيرة لمرضى السرطان، وهو ما يُرتب مسؤولية الشركة عن

³¹ انظر الأمم المتحدة، المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة «الحماية والاحترام والانتصاف»، 2011، ص 14.

³² انظر European Parliament Resolution on Civil Law Rules on Robotics, 2017, p. 17

³³ انظر في ذات المعنى محمد إبراهيم عبد الفتاح يسن، المسؤولية الموضوعية عن المخاطر المستحدثة، مجلة بنها للعلوم الإنسانية العدد 1، الجزء 2، 2022، ص 68 وما بعدها.

³⁴ نشرت مجموعة FANCY BEAR، المرتبطة بروسيا، برمجية خبيثة مدعومة بتقنية (LAMEHUG) LLM لأتمتة عمليات الاستطلاع وجمع الوثائق، الجريمة الإلكترونية استخدمت مجموعة PUNK SPIDER، وهي مجموعة فاعلة مرتبطة بكوريا الشمالية، نصوصاً مؤلفة بالذكاء الاصطناعي لتسريع تسريب بيانات الاعتماد ومحو الأدلة الجنائية الرقمية، كذلك استغلت مجموعة FAMOUS CHOLLIMA المرتبطة بكوريا الشمالية، شخصيات مؤلفة بالذكاء الاصطناعي لتوسيع نطاق عملياتها الداخلية. انظر CrowdStrike. 2026. "2026 CrowdStrike Global Threat Report: AI Accelerates Adversaries and Reshapes the Attack Surface." News release, February 24. crowdstrike.com.

³⁵ يُعد هجوم شبكة الكهرباء الأوكرانية (2015-2016) نموذجاً بارزاً للهجمات السيبرانية التي نفذتها مجموعة "Sandworm" المدعومة من روسيا؛ إذ نجحت في اختراق أنظمة التحكم الصناعية (SCADA)، مما أدى إلى انقطاع التيار الكهربائي عن ربع مليون مواطن. وقد اتسم الهجوم بتعطيل مراكز الاتصال عبر هجمات حجب الخدمة الهاتفية (DDoS)؛ بهدف منع المشغلين من تلقي بلاغات الطوارئ وتأخير عمليات استعادة الطاقة. انظر Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid" (white paper, SANS Industrial Control Systems and E-ISAC, March 18, 2016, sans.org. P1.2.

³⁶ تعد حادثة شركة "Equifax" الأمريكية عام 2017 من أبرز وقائع انتهاك البيانات المالية؛ إذ استغل المهاجمون ثغرة أمنية غير معالجة لاختراق قواعد بيانات الشركة، مما أسفر عن تسريب المعلومات الشخصية والائتمانية لنحو 147 مليون شخص، بما في ذلك الأسماء، وأرقام الضمان الاجتماعي، والعناوين، وبيانات بطاقات الائتمان وقد انتهت القضية بتسوية مع السلطات الأمريكية بلغت قيمتها نحو 700 مليون دولار، لتصبح الحادثة مرجعاً رئيسياً في قضايا المسؤولية القانونية عن اختراقات البيانات والأمن السيبراني، انظر U.S. House of Representatives, Committee on Oversight and Government Reform, *The Equifax Data Breach* (Washington, DC: U.S. Government Publishing Office, December 2018, P 2

³⁷ كشف تقرير صحفي عن استخدام الجيش الإسرائيلي منظومتي الذكاء الاصطناعي "لافندر" و"أين أبي؟" في قطاع غزة لتحديد واستهداف 37 ألف شخص آلياً؛ وهو ما أدى، نتيجة الاعتماد على بيانات ومستشعرات متحيزة، إلى مقتل عائلات بأكملها وتسجيل ارتفاع قياسي في أعداد الضحايا المدنيين. مجلة 972+ بالتعاون مع Local Call، 3 أبريل 2024. <https://www.972mag.com/lavender-ai-israeli-army-gaza/>

³⁸ انظر سماعيل سلطاني، "الأسلحة ذاتية التشغيل من منظور القانون الدولي الإنساني: بين مشروعية الاستخدام وحتمية الامتثال، مجلة أبحاث قانونية وسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحيى (جيجل)، الجزائر، المجلد 10، عدد 1، 2025، ص 87-88.

³⁹ (3) انظر في ذات السياق إسحاق العشعاش، منظومات الأسلحة الفتاكة ذاتية التشغيل في القانون الدولي، أطروحة دكتوراة جامعة الجزائر 2023-2024 ص 67-69

⁴⁰ يعتمد الكيان الإسرائيلي في غزة على منظومة "غوسبل" المؤتمتة لتوليد أهداف عسكرية احتمالية بمراجعة بشرية صورية، وهو ما ينتهك مبدأ التناسب الدولي، ويعكس استراتيجية استهداف ممنهجة قد ترقى قانونياً إلى نية الإبادة الجماعية. انظر مركز العودة الفلسطيني، *Algorithms of Death: How AI Fuels Mass Killings in Gaza*، تقرير سياسات (لندن: مركز العودة الفلسطيني، 2025، ص 3-4.

⁴¹ انظر سماعيل سلطاني ص 88-89

- ⁴² وظف الاحتلال في غزة (2023-2024) منظومتي "حبسورا" و"لافندر" لتوليد قوائم اغتيال مؤتمتة، مستخدماً قنابل غير موجهة تسببت في مجازر واسعة، ودمار هائل، وبتّر أطراف آلاف المدنيين، في ذات السياق انظر رنا صفوت الكجك، الذكاء الاصطناعي وتأثيره في الحرب، مجلة القرار للبحوث العلمية المحكمة، المجلد السابع، العدد 21، السنة الثانية، 2025، ص 555-556.
- ⁴³ تُعد فضيحة "كامبريدج أناليتيكا" وفيسبوك عام 2018 نموذجاً صارخاً لانتهاك الخصوصية؛ إذ جُمعت بيانات 87 مليون مستخدم للتلاعب بالرأي العام في الانتخابات الأمريكية وتصويت "البريكست" عبر الإعلانات المضللة والتتبع الجغرافي. وأدى ذلك إلى إفلاس "كامبريدج أناليتيكا"، وفرض غرامات تاريخية على فيسبوك بلغت 5 مليارات دولار من لجنة التجارة الفيدرالية الأمريكية، و500 ألف جنيه إسترليني من السلطات البريطانية. انظر İsmihan İlker Atik, *Investigation of "Facebook-Cambridge Analytica Data Privacy Scandal" Case in Terms of Ethics and Law* (Instituto Politécnico do Cávado e do Ave, 2020) p 3-9
- ⁴⁴ أثارت "بطاقة أبل" (2019) جدلاً واسعاً حول الانحياز الخوارزمي، بعد أن منحت زوجات رواد أعمال حدوداً ائتمانية أقل بكثير من أزواجهن رغم تفوقهن المالي. مارست الآلة حينها ما يُعرف بـ "التمييز بالوكالة" عبر تحليل عادات الإنفاق وبيانات تاريخية مشوهة. ورغم أن التحقيقات الرسمية (2021) برأت البنك من تعمد التمييز، إلا أن القضية أصبحت درساً قانونياً يثبت أن مجرد حجب بيانات الجنس لا يضمن حياد الخوارزميات التي تُغذّي ببيانات بشرية متحيزة. انظر New York State Department of Financial Services, *Report on Apple Card Investigation* (New York: NYSDFS, March 2021) p 1-2, https://www.dfs.ny.gov/system/files/documents/2021/03/rpt_202103_apple_card_investigation.pdf.
- ⁴⁵ تُعد قضية "الولايات المتحدة ضد ميتا" (2022) نموذجاً بارزاً للتمييز الخوارزمي غير المباشر، حيث واجهت الشركة دعوى فيدرالية لاستخدام خوارزمياتها "مؤشرات بديلة" كرموز بريدية وأنماط استهلاك، مما أدى تقنياً إلى حجب إعلانات السكن والعمل عن الأقليات والنساء، انتهت القضية بتسوية تاريخية ألزمت "ميتا" بإلغاء أدوات الاستهداف الحساسة، لتظل دليلاً على خطورة خوارزميات "الصندوق الأسود" في تعميق التمييز. انظر Complaint at 1, *United States of America v. Meta Platforms, Inc.*, No. 1:22-cv-05187 (S.D.N.Y. June 21, 2022), ECF, p 1-39
- ⁴⁶ حُجبت خوارزميات "ميتا" تعليقات ومنشورات فلسطينية وإخبارية بذريعة مكافحة الإرهاب و"غموض النية"، وقيدت وصول المحتوى وحظرت حسابات صحفيين. وأسفر هذا الاعتماد على الرقابة الآلية، المفترقة للسياق الثقافي والسياسي، عن فرض قيود تعسفية عززت اتجاهاً فكرياً أحادياً، مما دفع المستخدمين لممارسة الرقابة الذاتية خوفاً من فقدان حساباتهم. للمزيد انظر Human Rights Watch, *Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook*, (New York: Human Rights Watch, 2023) p 25-26 <https://racismandtechnology.center>.
- ⁴⁷ انظر في ذات السياق صورية بوربابة وخديجة لحلو، "الإطار القانوني للذكاء الاصطناعي بين متطلبات الابتكار وضمانات المسؤولية القانونية"، في كتاب أشغال المؤتمر الدولي: التحديات القانونية لتكنولوجيا المعلومات في عصر الذكاء الاصطناعي والتحول الرقمي، إشراف وتنسيق صورية بوربابة (برلين: المركز الديمقراطي العربي، 2024)، ص 143
- ⁴⁸ انظر في ذات السياق إبراهيم محمد بن حمود الزندان، الذكاء الاصطناعي في مسطرة التشريعات والمعاهدات الدولية، ط 1، المركز العربي للأبحاث ودراسة السياسات، بيروت - لبنان، 2026، ص 19-21
- ⁴⁹ انظر Filippo Lancieri, Laura Edelson, and Stefan Bechtold, "AI Regulation: Competition, Arbitrage & Regulatory Capture," *Theoretical Inquiries in Law* 26, no. 1 (2025) p 242-246, doi.org.
- ⁵⁰ لتفاصيل أكثر انظر Marta Bo, Laura Bruun, and Vincent Boulanin, "Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems: On Accountability for Violations of International Humanitarian Law Involving AWS," *Stockholm International Peace Research Institute (SIPRI)*, 2023, p 23-34
- ⁵¹ (*) ظهر هذا الشرط لأول مرة في ديباجة اتفاقية لاهاي الثانية لعام 1899، واقترحه الدبلوماسي والقانوني الروسي "فيدور مارتنز"، وصار جزءاً لا يتجزأ من اتفاقيات جنيف لعام 1949 والبروتوكولات الإضافية لها ويقصد به "أنه في حال غياب نصوص قانونية أو اتفاقيات صريحة تحكم بيئة حرب معينة، فإن المدنيين والمقاتلين يظلون تحت حماية ومظلة المبادئ الإنسانية وما يمليه الضمير العام."

- انظر محمد عبد القادر مصباح الشقلاف، فعالية شرط مارتينز في سد الثغرات التي تحدث في قواعد القانون الدولي الإنساني، مجلة الاصلية، الجمعية الليبية للعلوم التربوية والإنسانية، المجلد 7، العدد 12، 2025، ص 53-55.
- ⁵² انظر رسل علاء داود العكدي، حيدر أدهم الطائي، "أثر شرط مارتنز في التفسير التطوري للتكنولوجيا العسكرية الحديثة" دراسة تحليلية"، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 01، السنة 2023، ص 97
- ⁵³ انظر، 51.p 51, "Artificial Intelligence Act," chapter II, Article 5, European Parliament, "Artificial Intelligence Act," chapter II, Article 5, and Michael Clark. "Prohibited AI Practices Under Article 5 of the EU AI Act: Scope, Enforcement, and Compliance Methodology." Research Paper, Standard Intelligence, Limited (Manchester, England), June 2026. SSRN Electronic Journal., p2-4.
- ⁵⁴ انظر عفاف أبروجي، قانون الاتحاد الأوروبي لتنظيم الذكاء الاصطناعي وآثاره على الحقوق الرقمية للفلسطينيين والفلسطينيات (حيفا: حملة - المركز العربي لتطوير الإعلام الاجتماعي، ٢٠٢٤، ص 6-7
- ⁵⁵ انظر زينب بنور المسؤولية القانونية عن اخطاء أنظمة الذكاء الاصطناعي، مجلة القانون الدولي للدراسات البحثية، المجلد 7، العدد 21، 2026 ص 110
- ⁵⁶ انظر Tambiana Madiaga, *Artificial intelligence act*, Briefing (European Parliamentary Research Service, September 2024) p 7-8
- ⁵⁷ انظر Siegmann, Charlotte, and Markus Anderljung. The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. Centre for the Governance of AI, 2022.p 18- 22
- ⁵⁸ انظر European Parliamentary Research Service (EPRS), The global reach of the EU's approach to digital transformation, Briefing (Brussels: European Parliament, 2024) p 6.
- ⁵⁹ انظر الأمم المتحدة، *حوكمة الذكاء الاصطناعي من أجل الإنسانية: التقرير النهائي* (نيويورك: الأمم المتحدة، 2024 ص 39
- ⁶⁰ انظر *مفوضية الأمم المتحدة السامية لحقوق الإنسان*، "الحق في الخصوصية في العصر الرقمي: تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان"، *A/HRC/51/17* (4 آب/أغسطس 2022)، ص 20.
- ⁶¹ انظر مجلس حقوق الإنسان، "تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير"، الدورة الحادية والأربعون (24 يونيو - 12 تموز/يوليو 2019)، وثيقة الأمم المتحدة رقم *A/HRC/41/35*، البند 3 من جدول الأعمال، ص 23 وما بعدها
- ⁶² انظر Antonio Stango, "The Geopolitical Competition between China and the U.S. in New Technologies," *SOG Working Paper Series*, no. SOG-WP12/2024 (Rome: Luiss School of Government, May 2024) p 9-18
- ⁶³ انظر اللجنة الدولية للصليب الأحمر، موقف اللجنة الدولية للصليب الأحمر من منظومات الأسلحة ذاتية التشغيل (جنيف: اللجنة الدولية للصليب الأحمر، 2021)، ص 7 وما بعدها.
- ⁶⁴ انظر Mark Robinson, "The establishment of an international AI agency: an applied solution to global AI governance," *International Affairs* 101, no. 4 (2025) p 1485- 1486
- ⁶⁵ انظر Ali Sathik Shaik, "Sandboxes, Safe Harbors, and Sunset Clauses: Designing Adaptive Regulation for AI That Doesn't Become Obsolete on Arrival" (Working Paper, Golden Gate University, 2024) p 16-19
- ⁶⁶ انظر European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 of 13 June 2024 laying down Harmonised rules on artificial intelligence," *Official Journal of the European Union* L (July 12, 2024) art. 14 (Human oversight).
- ⁶⁷ منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)، *التوصية الخاصة بأخلاقيات الذكاء الاصطناعي* باريس: اليونسكو، 2021 https://unesdoc.unesco.org/ark:/48223/pf0000380455_ara.