Journal of Palestine Ahliya University for research and studies
مجلـة جامعة فلسطين الأهلية للبحوث والدراسات
ISSN: 2959-4839
Vol. 04 Issue 03 (2025)

The International Criminal Court Confronting Automated Cybercrime: Examining the Accountability of Algorithms before the ICC

Islam Albayari[1]
[1] Faculty of Law, Al Istiqlal University (Palestine)
✉ islam_albayari@pass.ps

Received:04/08/2025 Accepted:03/09/2025 Published:01/12/2025

Abstract:

The study aimed to analyze the possibility of holding algorithms responsible for committing automated cybercrimes accountable before the International Criminal Court (ICC), with a focus on the legal dimensions of these crimes, their material and mental elements, and their classification within the four international crimes stipulated in the Rome Statute. It also examined the challenges related to proving the crime and determining liability in the absence of legal personality for automated systems. The study relied on a legal analytical approach to examine the texts of the Rome Statute and relevant international agreements, a comparative method to contrast current legal frameworks with emerging technical challenges, an inductive approach to identify legislative gaps, and a descriptive method to define the nature and technical-legal dimensions of automated cybercrimes. The findings revealed that the complexity of the elements of automated cybercrime and the difficulty of classifying them within traditional crimes places responsibility on individuals or entities that develop or employ these technologies, and that the current provisions of the Rome Statute are insufficient to prosecute such crimes, necessitating urgent legislative development and the establishment of advanced technical capabilities within the Court. The recommendations included amending the Rome Statute to include clear provisions criminalizing automated cybercrimes, creating specialized technical units within the Court to analyze cyber evidence, enhancing international cooperation among states and judicial bodies, and developing training programs for judges and prosecutors to ensure the effective and reliable handling of digital crimes. The scientific contribution of the study lies in proposing a legal framework for holding algorithms accountable, bridging the gap between traditional international law and emerging technical challenges, and enhancing the ICC's effectiveness in addressing automated cybercrimes.

Keywords: *Automated Cybercrime; International Criminal Court; Rome Statute; Algorithms; International Criminal Responsibility; Artificial Intelligence; International Criminal Law.*

Journal of Palestine Ahliya University for research and studies
مجلة جامعة فلسطين الأهلية للبحوث والدراسات
ISSN: 2959-4839
Vol. 04 Issue 03 (2025)

الجنائية الدولية في مواجهة الجريمة السيبرانية الآلية: قراءة في إمكانية مساءلة الخوارزميات أمام المحكمة الجنائية الدولية

إسلام البياري[1]

[1] كلية القانون، جامعة الاستقلال (فلسطين)

islam_albayari@pass.ps

تاريخ الاستلام:2025/08/04 تاريخ القبول:2025/09/03 تاريخ النشر:2025/12/01

ملخص:

هدفت الدراسة إلى تحليل إمكانية مساءلة الخوارزميات المسؤولة عن ارتكاب الجرائم السيبرانية الآلية أمام المحكمة الجنائية الدولية، مع التركيز على الأبعاد القانونية لهذه الجرائم وأركانها المادية والمعنوية، وتصنيفها ضمن الجرائم الدولية الأربع المنصوص عليها في نظام روما الأساسي، مع دراسة التحديات المتعلقة بإثبات الجريمة وتحديد المسؤولية في ظل غياب الشخصية القانونية للأنظمة الآلية. واعتمدت الدراسة على المنهج التحليلي القانوني لتحليل نصوص نظام روما الأساسي والاتفاقيات الدولية ذات الصلة، والمنهج المقارن لمقارنة الأطر القانونية الحالية بالتحديات التقنية الحديثة، إضافةً إلى المنهج الاستقرائي لرصد أوجه القصور التشريعي والمنهج الوصفي لتحديد طبيعة الجرائم السيبرانية وأبعادها التقنية والقانونية. أظهرت النتائج أن تعقيد أركان الجريمة السيبرانية الآلية وصعوبة تصنيفها ضمن الجرائم التقليدية يجعل المسؤولية تقع على الأفراد أو الجهات المطورة أو المستفيدة من هذه التقنيات، وأن النصوص الحالية في نظام روما الأساسي غير كافية لمقاضاة هذه الجرائم، ما يستلزم تطوير تشريعي عاجل وبناء قدرات تقنية متقدمة داخل المحكمة. وتضمنت التوصيات تعديل النظام الأساسي لإدراج نصوص واضحة تُجرّم الجرائم السيبرانية الآلية، إنشاء وحدات فنية متخصصة داخل المحكمة لتحليل الأدلة السيبرانية، تعزيز التعاون الدولي بين الدول والجهات القضائية، وتطوير برامج تدريبية للقضاة والمدعين العامين لضمان قدرة القضاء على التعامل مع الجرائم الرقمية بفاعلية وموثوقية. وتتمثل الإضافة العلمية للدراسة في تقديم إطار قانوني مقترح لمساءلة الخوارزميات، مما يسهم في سد الفجوة بين القانون الدولي التقليدي والتحديات التقنية الحديثة، وتعزيز فعالية المحكمة الجنائية الدولية في مواجهة الجرائم السيبرانية الآلية.

الكلمات المفتاحية: *الجريمة السيبرانية الآلية؛ المحكمة الجنائية الدولية؛ نظام روما الأساسي؛ الخوارزميات؛ المسؤولية الجنائية الدولية؛ الذكاء الاصطناعي؛ القانون الدولي الجنائي.*

1. مقدمة:

شهد العالم في العقود الأخيرة تطورًا متسارعًا في مجال التكنولوجيا الرقمية، حيث أصبحت الخوارزميات وأنظمة الذكاء الاصطناعي جزءًا رئيسيًا من البنية التقنية العالمية. وقد صاحب هذا التطور بروز أنماط جديدة من التهديدات الإجرامية، من بينها ما يُعرف بـ"الجريمة السيبرانية الآلية"، والتي تعتمد على أدوات خوارزمية مستقلة أو شبه مستقلة لتنفيذ هجماتها. ومع تصاعد هذه المخاطر، أضحى من الضروري إعادة النظر في الإطار القانوني الدولي، لاسيما مدى قدرة المحكمة الجنائية الدولية على التصدي لهذا النوع المستحدث من الجرائم، الذي يتجاوز في طبيعته الحدود الجغرافية والسيادية التقليدية.

تتناول هذه الدراسة موضوعًا بالغ الأهمية يتمثل في: "الجنائية الدولية في مواجهة الجريمة السيبرانية الآلية: قراءة في إمكانية مساءلة الخوارزميات أمام المحكمة الجنائية الدولية"، وذلك من خلال تحليل الجوانب القانونية والواقعية المرتبطة بمساءلة الفاعلين عن هذه الجرائم، سواء أكانوا أفرادًا أم مؤسسات، أم حتى أنظمة ذكاء اصطناعي مستقلة.

1.1 مشكلة الدراسة:

تتمثل المشكلة الرئيسة للدراسة في التساؤل التالي: إلى أي مدى يمكن مساءلة الخوارزميات والأنظمة الآلية عن ارتكاب الجرائم الدولية وفق نظام روما الأساسي للمحكمة الجنائية الدولية، في ظل غياب الشخصية القانونية لتلك الكيانات وتعدد أطراف المسؤولية التقنية والبشرية؟"

وتتفرع عن هذه الإشكالية عدة تساؤلات فرعية:

- ما هو الإطار المفاهيمي والتقني للجريمة السيبرانية الآلية؟
- كيف يمكن توصيف الركنين المادي والمعنوي لهذه الجرائم؟
- هل من الممكن تصنيف الجريمة السيبرانية الآلية ضمن الجرائم الدولية الأربع؟
- ما هي التحديات القانونية التي تواجه المحكمة الجنائية الدولية في محاسبة الفاعلين التقنيين؟
- ما هي سبل تطوير نظام روما الأساسي لمواجهة هذه الجرائم؟

1.2 أهمية الدراسة

تبرز أهمية هذه الدراسة من خلال ما يلي:

- تسليط الضوء على فجوة قانونية في القانون الجنائي الدولي تتعلق بجرائم ذات طابع تقني متقدم.
- تقديم رؤية تحليلية حول ضرورة تطوير مفاهيم المسؤولية الدولية لتشمل الفواعل غير التقليدية كالخوارزميات.
- رفد الجهود الأكاديمية والقانونية المعنية بمواكبة التغيرات التكنولوجية في مجال الجريمة الدولية.

- المساهمة في إثراء الجدل الفقهي حول حدود اختصاص المحكمة الجنائية الدولية في الجرائم السيبرانية المستحدثة.

1.3 أهداف الدراسة

تهدف الدراسة إلى تحقيق ما يلي:

- توضيح الطبيعة القانونية للجريمة السيبرانية الآلية وخصائصها الفنية.
- تحليل أركان المسؤولية الجنائية في الجرائم السيبرانية ذات الطابع الآلي.
- بحث مدى توافق الجرائم السيبرانية مع التصنيفات القانونية للجرائم الدولية الأربع.
- استعراض التحديات التي تواجه المحكمة الجنائية الدولية في مساءلة مرتكبي هذه الجرائم.
- اقتراح توصيات قانونية لتطوير نظام روما الأساسي بما يتلاءم مع التهديدات السيبرانية المعاصرة.

1.4 النطاق الزماني والمكاني للدراسة:

- **النطاق الزماني:** تغطي الدراسة الفترة الممتدة من عام 2010 حتى عام 2025، وهي المرحلة التي شهدت تطورًا ملحوظًا في أنظمة الذكاء الاصطناعي وزيادة ملحوظة في الهجمات السيبرانية ذات الطابع الآلي على المستوى الدولي.
- **النطاق المكاني:** تنصب الدراسة على البيئة القانونية للمحكمة الجنائية الدولية في لاهاي، مع استعراض أمثلة من هجمات سيبرانية عالمية ذات طابع عابر للحدود.

1.5 منهجية الدراسة

تعتمد الدراسة على المنهج التحليلي القانوني من خلال تحليل نصوص نظام روما الأساسي، والاتفاقيات الدولية ذات الصلة، بالإضافة إلى المنهج المقارن لمقارنة الإطار القانوني الدولي الحالي مع التحديات التقنية الجديدة. كما يتم استخدام المنهج الاستقرائي لرصد أوجه القصور التشريعي، مع توظيف المنهج الوصفي لتحديد طبيعة الجريمة السيبرانية الآلية وأبعادها التقنية والقانونية.

2. المبحث الأول: الطبيعة القانونية للجريمة السيبرانية الآلية

مع التطور التقني المتسارع في مجال الذكاء الاصطناعي والبرمجة الرقمية، برز نوع جديد من الجرائم يُعرف بـ"الجريمة السيبرانية الآلية"، والتي تعتمد على أنظمة خوارزمية قد تعمل بصورة مستقلة لتنفيذ أفعال إجرامية دون تدخل بشري مباشر أثناء التنفيذ (Jensen, 2013). ويثير هذا النوع من الجرائم تساؤلات قانونية جوهرية حول كيفية توصيفه ضمن القواعد التقليدية للقانون الجنائي الدولي، ومدى انطباق أركان الجريمة عليه، بالإضافة إلى صعوبة تصنيفه في إطار الجرائم الدولية المعروفة (Radziwill, 2015). لذلك، يتناول هذا المبحث دراسة المفهوم

القانوني لهذه الجريمة، وأركانها المادية والمعنوية، وإمكانية تصنيفها ضمن الجرائم الدولية الأربع المنصوص عليها في نظام روما الأساسي.

2.1 المطلب الأول: مفهوم الجريمة السيبرانية الآلية وتطورها التقني

تُعد الجريمة السيبرانية فرعًا حديثًا ومتطورًا من فروع الجرائم التي تستخدم التكنولوجيا الرقمية لتنفيذ أعمال غير قانونية تستهدف أنظمة الحاسوب، الشبكات، أو البيانات. وتتخذ هذه الجرائم أشكالًا متعددة تشمل الاختراق، التدمير، الاحتيال، والتجسس، لكنها تتسم بشكل خاص بالتطور المستمر نتيجة التقدم التكنولوجي (الربيعي، 2024). أما الجريمة السيبرانية الآلية، فهي ذلك النوع من الجرائم التي تنفذ باستخدام أنظمة خوارزمية مدعومة بتقنيات الذكاء الاصطناعي، والتي تتمتع بقدرة على التصرف بشكل مستقل أو شبه مستقل دون الحاجة إلى تدخل بشري مباشر خلال تنفيذ الفعل الإجرامي (خرشف، 2021).

ويُعزى التطور النوعي للجريمة السيبرانية الآلية إلى ازدهار الذكاء الاصطناعي، الذي يعتمد على تقنيات مثل التعلم الآلي والتعلم العميق، حيث يتم تدريب الخوارزميات على تحليل كميات ضخمة من البيانات، واكتشاف نقاط الضعف الأمنية، واستغلالها بسرعة عالية وبدقة متناهية تمكنت هذه الأنظمة من تنفيذ هجمات معقدة ومتزامنة، كالهجمات الموزعة على شبكات الحاسوب (DDoS)، أو البرمجيات الخبيثة ذاتية الانتشار، مما يعكس تحولًا كبيرًا عن الأساليب التقليدية التي تعتمد على التوجيه البشري المباشر (الزنداني، 2021).

لقد أدى هذا التطور إلى ظهور تحديات قانونية وأخلاقية، أبرزها تحديد المسؤولية الجنائية عن الأفعال التي تنفذها خوارزميات ذاتية التشغيل، إذ يصعب إرجاع الفعل إلى فاعل بشري محدد، كما أن صعوبة فهم وتعقب الخوارزميات تعقد إثبات الركن المادي والمعنوي للجريمة (الحسني، 2021). وبالتالي، تتطلب معالجة الجريمة السيبرانية الآلية تطوير أطر قانونية تتناسب مع طبيعة هذه التكنولوجيا، وتحديد المسؤوليات بين المصممين والمبرمجين والمستخدمين النهائيين.

2.2 المطلب الثاني: الركن المادي والمعنوي للجريمة السيبرانية ذات الطابع الآلي

تُعد الجريمة السيبرانية ذات الطابع الآلي من الإشكاليات القانونية الحديثة التي تفرض تحديات خاصة في تحديد وتكييف أركان الجريمة، لا سيما فيما يتعلق بالركنين المادي والمعنوي. ويعود ذلك إلى الطبيعة التقنية المعقدة التي تتميز بها هذه الجرائم، حيث يتم تنفيذ الأفعال الإجرامية عبر خوارزميات مبرمجة مسبقًا أو أنظمة ذكاء اصطناعي ذاتية التشغيل.

2.2.1 الركن المادي

يتجسد الركن المادي في الأفعال الملموسة التي تقوم بها الخوارزميات، مثل اختراق الأنظمة، تعطيل الخدمات، تدمير البيانات الرقمية، نشر الفيروسات الإلكترونية، أو شن هجمات الحرمان من الخدمة ويتميز هذا الركن بغياب

التفاعل البشري المباشر أثناء التنفيذ، مما يثير جدلاً قانونيًا حول الجهة التي يمكن إسناد الفعل الجرمي إليها. وفي هذا السياق، تبرز مسألة علاقة الفعل الجرمي بفاعل بشري أو ذاتي التشغيل، حيث إنّ الخوارزمية، رغم قدرتها على اتخاذ قرارات مستقلة، تظل نتاجًا لإرادة بشرية في مراحل التصميم والبرمجة والتشغيل. وبذلك، يصبح النقاش القانوني متمحورًا حول مسؤولية المصممين والمبرمجين، أو حتى الجهات التي قامت بتفعيل النظام (فهمي، 2025).

2.2.2 الركن المعنوي

أما الركن المعنوي، فهو يمثل الجانب المتعلق بالقصد الجنائي، وهو ما يصعب إثباته في مثل هذه الجرائم نظرًا لغياب عنصر الإرادة لدى الخوارزميات التي تفتقر للوعي والإدراك. لذا يتجه الفقه الجنائي إلى تحميل المسؤولية للأشخاص الطبيعيين أو الاعتباريين الذين كانت لديهم نية الإجرام في بيئة غير بشرية، سواء عبر القصد المباشر أم القصد الاحتمالي (الحسني، 2021).

كما يُطرح التساؤل حول مدى إمكانية مساءلة الأفراد الذين كان بإمكانهم توقع النتائج الإجرامية لأفعال الأنظمة الآلية التي أطلقوها، مما يستدعي بحث أعمق في مفاهيم المسؤولية عن الإهمال أو الإخلال بواجبات الحيطة التقنية. ويبدو من مجمل التحليل أن التكييف القانوني للركنين المادي والمعنوي في الجريمة السيبرانية الآلية لا يزال بحاجة إلى تطوير نظري وتشريعي ليواكب التحولات التقنية المتسارعة في هذا المجال.

2.3 المطلب الثالث: تصنيف الجريمة السيبرانية الآلية ضمن الجرائم الدولية الأربع وفق نظام روما الأساسي

يطرح تصنيف الجريمة السيبرانية الآلية ضمن الجرائم الدولية الأربع الواردة في نظام روما الأساسي (جريمة الحرب، الجريمة ضد الإنسانية، جريمة الإبادة الجماعية، وجريمة العدوان) إشكاليات قانونية عميقة، خصوصًا في ظل غياب نصوص صريحة تغطي هذا النوع المستحدث من الجرائم. إلا أن الممارسات الدولية والاجتهادات القضائية سمحت بفتح المجال أمام إمكانية التكييف القانوني لهذه الجرائم وفق الظروف المحيطة وطبيعة الأثر الناتج (الزنداني، 2021).

2.3.1 الجريمة السيبرانية الآلية كجريمة حرب

يمكن اعتبار الجريمة السيبرانية الآلية جريمة حرب إذا ارتكبت أثناء نزاع مسلح، وكانت موجهة ضد أهداف محمية بموجب القانون الدولي الإنساني، كالبنى التحتية المدنية، المستشفيات، أو شبكات المياه والكهرباء. فعلى سبيل المثال، قد يؤدي هجوم سيبراني واسع النطاق إلى تعطيل مستشفى في منطقة نزاع، مما ينتج عنه وفاة مدنيين، وهو ما يمكن أن يُصنف كجريمة حرب طبقًا للمادة (8) من نظام روما الأساسي (الحسني، 2021).

في السياق الفلسطيني، يمكن تصور أن استخدام إسرائيل لأنظمة إلكترونية هجومية تعتمد على خوارزميات موجهة ذاتيًا لاستهداف البنى التحتية المدنية في قطاع غزة، مثل تعطيل شبكات الكهرباء أو أنظمة الاتصالات، قد يرقى إلى جريمة حرب بموجب المادة (8) من نظام روما الأساسي فالهجمات السيبرانية التي تؤدي إلى شلل في المستشفيات أو انقطاع إمدادات المياه خلال العمليات العسكرية، قد تُصنف ضمن الأفعال المحظورة التي تستهدف السكان المدنيين بشكل مباشر، و خاصة تعمد توجيه هجمات ضد المباني والمواد والوحدات الطبية ووسائل النقل والأفراد من مستعملي الشعارات المميزة المبينة في اتفاقيات جنيف طبقاً للقانون الدولي

من أبرز السوابق القضائية ذات الصلة بمهاجمة الأعيان المدنية، يمكن الاستشهاد بما ورد في قضية "قصف البنية التحتية المدنية في يوغوسلافيا" أمام المحكمة الجنائية الدولية ليوغوسلافيا السابقة، حيث أكدت المحكمة أن استهداف البنى الأساسية التي يعتمد عليها السكان المدنيون يشكل انتهاكًا جسيمًا لقوانين الحرب (المحكمة الجنائية الدولية ليوغوسلافيا السابقة، 1991).

2.3.2 الجريمة كجريمة ضد الإنسانية

إذا نفذت الجريمة السيبرانية الآلية ضمن هجوم واسع النطاق أو منهجي ضد مجموعة من السكان المدنيين، فإنها قد تقع ضمن نطاق الجرائم ضد الإنسانية وفق المادة (7) من النظام الأساسي مثال ذلك: هجوم خوارزمي يستهدف حرمان سكان منطقة كاملة من الكهرباء والمياه لفترة طويلة، مما يؤدي إلى معاناة إنسانية شديدة (رمضان، 2025).

قد تتوفر أركان الجريمة ضد الإنسانية إذا تبين أن الهجمات السيبرانية الآلية الموجهة ضد المدنيين الفلسطينيين تمت في إطار هجوم واسع النطاق أو منهجي يستهدف السكان المدنيين عمداً. على سبيل المثال، شن هجمات إلكترونية تهدف إلى تعطيل الأنظمة الصحية أو الإعلامية أو الخدمات الأساسية بشكل متكرر يمكن أن يدخل ضمن مفهوم "الهجوم الممنهج" وفق تفسير المحكمة الجنائية الدولية في قضية "أحداث كوت ديفوار" (2011)، والتي عرّفت الهجوم ضد المدنيين بأنه سلسلة من الأفعال ذات طابع منهجي وليست عرضية (المحكمة الجنائية الدولية، 2011).

2.3.3 الجريمة كجريمة إبادة جماعية

رغم أن إثبات نية الإبادة في الجرائم السيبرانية الآلية يُعد أمرًا بالغ الصعوبة، إلا أن بعض الفرضيات النظرية تتحدث عن إمكانية استخدام الخوارزميات لشن هجمات تستهدف مجموعة قومية أو إثنية معينة بهدف إلحاق ضرر جسيم بها أو القضاء عليها كليًا أو جزئيًا، وهو ما قد يرقى إلى مستوى جريمة إبادة جماعية طبقًا للمادة (6) من نظام روما الأساسي.

رغم صعوبة إثبات نية الإبادة من خلال الوسائل السيبرانية وحدها، إلا أنه في حال ثبوت وجود سياسة ممنهجة تعتمد على أدوات هجومية خوارزمية لإحداث دمار شامل يستهدف فئة محددة من السكان الفلسطينيين بقصد القضاء عليهم جزئيًا أو كليًا، فإنّ ذلك قد يفتح الباب قانونيًا لمناقشة إمكانية تصنيف هذه الأفعال كإبادة جماعية، في هذا السياق، يمكن الإشارة إلى ما ورد في حكم المحكمة الجنائية الدولية لرواندا في قضية "أكايسو" (1998)، والتي وسّعت مفهوم الإبادة ليشمل الأفعال التي تؤدي إلى تدمير جماعي حتى وإن تمت بطرق غير تقليدية (فياله، 2024).

2.3.4 الجريمة كجريمة عدوان

تقتصر جريمة العدوان وفق المادة (8 مكرر) من النظام الأساسي حاليًا على الأفعال العسكرية التقليدية، ومع ذلك فأنّ هناك اتجاهات فقهية تدعو إلى توسيع مفهوم العدوان ليشمل الهجمات السيبرانية ذات الآثار العسكرية والسياسية الفادحة. وفي هذا الإطار، قد يُطرح تساؤل حول إمكانية تصنيف هجوم إلكتروني واسع النطاق يستهدف أمن وسيادة دولة أخرى كجريمة عدوان في المستقبل (حساني، 2017). إنّ هذا التصنيف لا يزال محل جدل فقهي، ويعكس الحاجة الماسة إلى تطوير قواعد القانون الجنائي الدولي لمواكبة التطورات التقنية التي يشهدها المجال السيبراني.

فيما يتعلق بجريمة العدوان، فإنّ الهجمات السيبرانية الإسرائيلية إذا استهدفت مؤسسات الدولة الفلسطينية أو البنية السيادية للسلطة الوطنية الفلسطينية دون مبرر قانوني وبتأثير يمس سلامة أراضيها أو استقلالها السياسي، فقد تثير من الناحية الفقهية مسألة تصنيفها كعمل عدواني. وهذا يتفق مع ما ذهبت إليه اللجنة الدولية للقانون الدولي (2010) في توصياتها الأخيرة حول توسيع مفهوم العدوان ليشمل الأعمال غير التقليدية بما فيها الهجمات السيبرانية.

ورغم عدم وجود سوابق قضائية مباشرة أمام المحكمة الجنائية الدولية فيما يخص الجرائم السيبرانية، فإنّ توجهات الفقه الدولي والاجتهادات السابقة، مثل: قضايا يوغوسلافيا، رواندا، وكوت ديفوار توفر أرضية قانونية يمكن البناء عليها لإدراج الجرائم السيبرانية الآلية ضمن نطاق اختصاص المحكمة (Schabas, 2016).

أكد المدعي العام للمحكمة الجنائية الدولية، كريم خان، على أهمية إدراك التغيرات المتسارعة في الوسائل المستخدمة لارتكاب الجرائم الدولية، مشيرًا إلى أن مسار ارتكاب تلك الجرائم لم يعد يقتصر على الأدوات التقليدية مثل الأسلحة النارية والمتفجرات، بل امتد ليشمل منصات التواصل الاجتماعي، وشبكات الإنترنت، وصولًا إلى تطبيقات الذكاء الاصطناعي. وأوضح أن التوسع في استخدام الفضاء الإلكتروني من قبل الدول والجهات الفاعلة الأخرى قد يفتح المجال أمام استغلال هذه الوسائل لتنفيذ أو تسهيل ارتكاب أخطر الجرائم التي تدخل ضمن

اختصاص المحكمة الجنائية الدولية، مثل جرائم الحرب والجرائم ضد الإنسانية والإبادة الجماعية، بل وحتى أعمال العدوان بين الدول. وفي ضوء هذه المستجدات، يرى خان أن على نظام العدالة الجنائية الدولية أن يطور آلياته ويُكيف أدواته بما يتلاءم مع طبيعة التحديات التي يفرضها هذا الواقع السيبراني الجديد (مكتب المدعي العام للمحكمة الجنائية الدولية، 2025).

3. المبحث الثاني: مسؤولية الخوارزميات وإمكانية مساءلتها أمام المحكمة الجنائية الدولية

يشهد العالم تطورًا متسارعًا في استخدام التكنولوجيا الرقمية، حيث أصبحت الخوارزميات والأنظمة الذكية جزءًا مؤثرًا في مختلف مجالات الحياة، بما في ذلك المجالات ذات الصلة بالأمن والنزاعات المسلحة. هذا الواقع الجديد يطرح تساؤلات قانونية بالغة الأهمية حول مدى إمكانية مساءلة الأنظمة الخوارزمية، خاصة عندما تسهم بشكل مباشر أو غير مباشر في ارتكاب جرائم دولية خطيرة. ويأتي هذا المبحث ليسلط الضوء على الجوانب القانونية المرتبطة بمسؤولية الخوارزميات، من خلال تحليل الإطار المفاهيمي للمسؤولية الجنائية الدولية، ودراسة مدى توافقها مع طبيعة الذكاء الاصطناعي والتقنيات الرقمية، مع التركيز على التحديات التي قد تواجه المحكمة الجنائية الدولية في هذا المجال الوليد من القانون الجنائي الدولي.

3.1 المطلب الأول: التحديات القانونية في مساءلة الخوارزميات أمام المحكمة الجنائية الدولية

تعد مساءلة الخوارزميات أمام المحكمة الجنائية الدولية تحديًا قانونيًا معقدًا ينبع من طبيعة هذه الأنظمة الرقمية وغياب الشخصية القانونية لها، الأمر الذي ينعكس على مبدأ المسؤولية الجنائية التقليدية المبنية على الفاعل البشري القادر على الإدراك والنية. فالقانون الجنائي الدولي يشترط في المسؤول أن يكون كائنًا طبيعيًا أو اعتباريًا يمتلك القدرة على الإرادة والتحكم في الفعل الإجرامي، وهو ما لا ينطبق على الخوارزميات التي تمثل برامج حاسوبية ذات قدرة تنفيذية أو تعلم ذاتي، لكنها تفتقر إلى الوعي والقصد الجنائي.

3.1.1 مشكلة تحديد الجهة الفاعلة

ينشأ تحدي قانوني جوهري في تحديد من يمكن مساءلته جنائيًا في حالة ارتكاب جريمة عبر خوارزميات. فهل تُحمّل الخوارزمية ذاتها المسؤولية؟ أم المسؤول هو مطورها، أو المشغل الذي وظفها، أو الدولة التي تسمح باستخدامها؟ تكمن الصعوبة في أن الخوارزميات تعمل تلقائيًا، ولا تمتلك وعيًا أو إرادة مستقلة، مما يصعب تحميلها المسؤولية الجنائية. لذلك، تتجه الآراء القانونية إلى اعتبار الخوارزميات أدوات أو وسائل، ويجب توجيه المسؤولية إلى الأشخاص الطبيعيين أو الاعتباريين الذين يتحكمون في تصميمها أو استخدامها. هذا الإشكال يزداد تعقيدًا في ظل غياب إطار قانوني دولي موحد لتوزيع المسؤوليات بين الأطراف المختلفة (فياله، 2024).

3.1.2 غياب الشخصية القانونية للخوارزميات

تتطلب المسؤولية الجنائية وجود شخصية قانونية، سواء طبيعية أم معنوية. لكن الخوارزميات لا تحوز هذه الشخصية، ما يضعها خارج نطاق المسؤولية القانونية المباشرة. وهذا يعقد مهمة القضاء الدولي في مساءلة الأفعال المرتكبة عبرها، خاصة مع صعوبة إثبات النية أو القصد الجنائي، إذ إنّ الخوارزمية تعمل وفق برمجتها مسبقًا، ولا تملك إرادة مستقلة تؤهلها للمساءلة. بالتالي، يصبح تحميل المسؤولية متوقفًا على الأشخاص أو الكيانات المرتبطة بالخوارزمية، سواء كانوا مطورين أو مشغلين أو دولًا (Schmitt, 2017).

3.1.3 أزمة الإثبات في الجرائم السيبرانية الآلية

تُعدّ مسألة الإثبات من أبرز التحديات في سياق الجرائم السيبرانية المعتمدة على الخوارزميات، حيث يتطلب إثبات الفعل الجرمي والجهة المسؤولة عنه أدلة تقنية متقدمة وقادرة على الربط المباشر بين الأفعال الجنائية والفاعل الحقيقي وغالبًا ما يصعب تتبع مصدر الهجمات السيبرانية بسبب التعقيد التقني الكبير الذي تتسم به البنية السيبرانية، فضلًا عن صعوبة إثبات الركن المعنوي، خاصةً في الحالات التي تكون ناتجة عن أخطاء برمجية غير مقصودة. كما أن الأدلة الرقمية عرضة للتزوير والتلاعب، مما يُضعف إمكانية الاعتماد الحصري عليها كدليل إدانة. ومع ذلك، بدأت المحاكم الدولية في تطوير أدوات وإجراءات قانونية وتقنية لمعالجة هذه الأدلة، رغم أن هذه الآليات ما تزال في مراحلها الأولية من التطوير (Schmitt, 2017).

3.1.4 الإسقاط على الحالة الفلسطينية

عندما تتعرض فلسطين بشكل متكرر لهجمات سيبرانية تستهدف بنيتها التحتية الرقمية الحيوية، باستخدام تقنيات متقدمة تشمل خوارزميات الذكاء الاصطناعي. تؤثر هذه الهجمات بشكل مباشر على الخدمات الأساسية وحقوق السكان، مما يُشكّل تهديدًا حقيقيًا للأمن الوطني الفلسطيني. ويزداد الأمر تعقيدًا بسبب الاعتماد على خوارزميات تعمل بشكل شبه مستقل في تنفيذ العمليات التخريبية، الأمر الذي يعقّد من مساءلة الأطراف الفاعلة (Pretorius & Van Niekerk, 2015).

تواجه فلسطين صعوبات كبيرة في إثبات مسؤولية الفاعلين، سواء أكانوا جهات حكومية أم غير حكومية، وذلك بسبب تعقيد مسألة الإثبات في الجرائم السيبرانية وطبيعة الخوارزميات المستخدمة، فضلًا عن غياب قواعد قانونية دولية واضحة تُنظّم مسؤولية مرتكبي الجرائم السيبرانية من هذا النوع. ويبرز هذا الواقع الحاجة الملحة لتطوير آليات قانونية وتقنية تمكّن المحكمة الجنائية الدولية من قبول وتحليل الأدلة الرقمية بكفاءة، وضمان محاسبة المسؤولين، وحماية المدنيين الفلسطينيين من الأضرار الناتجة عن هذه الهجمات.

أما عن السوابق القضائية الدولية ذات الصلة على النحو الآتي:

- **قضية نيكاراغوا ضد الولايات المتحدة (1986) – محكمة العدل الدولية**

على الرغم من أن هذه القضية لم تتناول الجرائم السيبرانية بصورة مباشرة، إلا أن محكمة العدل الدولية قامت بتوسيع تفسيرها لمفهوم "استخدام القوة"، ليشمل تقديم الدعم للجماعات المسلحة، وهو ما يمكن إسقاطه قانونيًا على الهجمات السيبرانية التي تُسبب أضرارًا جسيمة عبر خوارزميات معقدة (International Court of Justice, 1986).

- **قضية لوبيانغا (ICC, 2012)**

أظهرت المحكمة الجنائية الدولية في هذه القضية استعدادها لقبول الأدلة الرقمية والتقنية، بما في ذلك الشهادات الرقمية والبيانات الإلكترونية، كأدلة رئيسة في إصدار حكم الإدانة، وقد أكدت المحكمة على أهمية تقييم مصداقية هذه الأدلة بدقة في الجرائم المعقدة (International Criminal Court, 2012).

- **مشروع تالين 2.0 (Tallinn Manual 2.0, 2017)**

يمثل مشروع تالين 2.0 مرجعًا قانونيًا دوليًا مهمًا لتفسير كيفية تطبيق القانون الدولي على العمليات السيبرانية، بما في ذلك قواعد الإثبات وتحميل المسؤولية على الجهات التي تستخدم الوسائل السيبرانية لأغراض عدوانية (Schmitt, 2017).

3.2 المطلب الثاني: أطر المسؤولية الجنائية الدولية عن الجرائم السيبرانية ذات الطابع الآلي أمام المحكمة الجنائية الدولية

3.2.1 المسؤولية الفردية(Individual Criminal Responsibility)

تنص المادة 25 من نظام روما الأساسي على أن المحكمة الجنائية الدولية تختص بمحاكمة الأفراد المسؤولين عن الجرائم الدولية، بما في ذلك جرائم الحرب والجرائم ضد الإنسانية والإبادة الجماعية وجريمة العدوان (زواقري ولخذاري، 2013).

وفي سابقة دولية مهمة، أعلنت المحكمة الجنائية الدولية في يونيو 2024 فتح تحقيق رسمي في الهجمات السيبرانية التي استهدفت البنية التحتية المدنية الأوكرانية (كالكهرباء والمياه)، معتبرةً إياها هجمات محتملة على أعيان مدنية محمية بموجب المادة (8) من النظام الأساسي (The Guardian, 2024). وقد أشارت التقارير إلى أن الاتهامات قد تُوجَّه إلى كبار القادة والمبرمجين (القراصنة) إذا ثبت توافر النية الجنائية وتعمّد استهداف المدنيين أو تعطيل الخدمات العامة.

3.2.2 مسؤولية الدول (State Responsibility Doctrine):

رغم أن المحكمة الجنائية الدولية لا تملك اختصاصًا لمحاكمة الدول، فإنّ الدول تخضع لمسؤولية قانونية بموجب قواعد القانون الدولي العام، لا سيما المادة (4/2) من ميثاق الأمم المتحدة التي تحظر استخدام القوة ضد سلامة الدول أو استقلالها السياسي (مرزق، 2021).

3.2.3 مسؤولية الشركات التقنية (Corporate Responsibility):

على الرغم من أن نظام روما الأساسي لا يشمل مساءلة الكيانات الاعتبارية مثل الشركات، إلا أن القضاء المقارن بدأ يرسخ مسؤولية الشركات عن انتهاكات حقوق الإنسان ذات الطابع الدولي. ففي سابقة قضائية كندية، أقرت المحكمة العليا في قضية شركة نيفسون للموارد المحدودة ضد أرايا (2020) إمكانية مساءلة الشركات مدنيًا داخل المحاكم الوطنية عن انتهاكات جسيمة لحقوق الإنسان في الخارج (Supreme Court of Canada, 2020).

أما في الولايات المتحدة، فقد شكلت قضية كيوبل ضد شركة رويال داتش للبترول (2013) محطة مفصلية في مسار مساءلة الشركات عن الانتهاكات الجسيمة لحقوق الإنسان. فقد قضت المحكمة العليا الأمريكية بتقييد نطاق تطبيق قانون الضرر للأجانب (Alien Tort Statute)، معتبرةً أن هذا القانون لا ينطبق عادةً على الأفعال التي وقعت خارج الأراضي الأمريكية، وهو ما حدّ من إمكانية مقاضاة الشركات الأجنبية أمام المحاكم الأمريكية. ورغم ذلك، فقد فتحت هذه القضية جدلًا واسعًا حول حدود المسؤولية الدولية للشركات في قضايا حقوق الإنسان (The Guardian, 2013). لذلك يرى الباحث لا بد من تعديل نظام روما ليتضمن مساءلة الشركات التقنية المتورطة في دعم الجرائم الدولية.

3.2.4 مسؤولية القادة والمصممين (Command and Designer Responsibility):

وفقًا للمادة (28) من نظام روما، يتحمل القادة العسكريون والمدنيون المسؤولية الجنائية عن الجرائم التي يرتكبها مرؤوسوهم متى ثبت أنهم علموا أو كان يجب أن يعلموا بها ولم يتخذوا التدابير اللازمة لمنعها أو معاقبة مرتكبيها (United Nations, 1998).

في قضية نتاغاندا (Ntaganda) أدانت المحكمة الجنائية الدولية القائد بوسكو نتاجاندا لمسؤوليته القيادية عن ارتكاب جرائم حرب وجرائم ضد الإنسانية، رغم عدم تنفيذه المباشر للجرائم (International Criminal Court, 2019). ولذلك يمكن إسقاط هذا المبدأ على الجرائم السيبرانية، لاسيما في الحالات التي يكون فيها قادة الوحدات السيبرانية أو مصممو البرمجيات الهجومية على علم بالأضرار التي قد تلحق بالمدنيين نتيجة هجماتهم.

3.3 المطلب الثالث: آفاق تطوير نظام روما الأساسي لمواجهة الجريمة السيبرانية الآلية

تواجه القوانين الدولية المعاصرة تحديًا حقيقيًا في مواكبة التطورات التقنية التي أفرزتها الجريمة السيبرانية الآلية، والتي تُشكّل تهديدًا متزايدًا على الأمن الدولي وحقوق الإنسان، إذ يُعدّ نظام روما الأساسي للمحكمة الجنائية الدولية الإطار القانوني الأهم لمحاكمة الجرائم الدولية الكبرى، إلا أنه لم يواكب بشكل كامل هذه الجرائم الجديدة، الأمر الذي يستدعي تطويره تشريعيًا وإجرائيًا لاحتواء الجريمة السيبرانية في نطاق اختصاص المحكمة.

3.3.1 التحديات التشريعية في نظام روما الأساسي لمواجهة الجرائم السيبرانية الآلية:

إنّ نظام روما الأساسي، الذي أُنشئ عام 1998، يعاني من نقص واضح في النصوص القانونية التي تتعامل مباشرة مع الجرائم السيبرانية الحديثة. فقد صيغت البنود الأصلية في سياق جرائم تقليدية كالجرائم ضد الإنسانية والجرائم الحرب، دون تصور دقيق لجرائم تكنولوجيا المعلومات المتطورة، بما فيها الهجمات السيبرانية التي تؤدي إلى أضرار جسيمة على البنية التحتية الحيوية، الخدمات الطبية، والبيانات الخاصة.

ويشير عدد من الفقهاء إلى ضرورة تعديل النظام التشريعي للمحكمة بإضافة مواد واضحة تُجرّم الاعتداءات السيبرانية ذات الأبعاد الدولية، وتوسع التعريفات لتشمل الأدوات الرقمية كوسيلة ارتكاب للجرائم الدولية (Schmitt, 2017). كما تؤكد التقارير أن عدم وجود تشريع صريح حول الجرائم السيبرانية في النظام يعوق قدرة المحكمة على التحرك بفعالية ضد هذه الجرائم (Jensen, 2013).

3.3.2 مقترحات لتعديل نصوص المحكمة الجنائية الدولية

تتطلب الجرائم السيبرانية تعديلات جوهرية على نصوص نظام روما الأساسي، خاصة فيما يتعلق بتعريفات الجرائم وأدوات الإثبات. على سبيل المثال، يمكن توسيع تعريف "الجرائم ضد الإنسانية" ليشمل الهجمات السيبرانية التي تؤدي إلى إلحاق أضرار جسيمة بالسكان المدنيين.

بالإضافة إلى ذلك، يستوجب تعديل نص المادة 8 (الجرائم الحرب) لتضمين الهجمات الإلكترونية التي تؤثر على البنية التحتية المدنية، مثل: محطات الطاقة وشبكات الاتصالات، مما يحقق فاعلية أكبر في ملاحقة مرتكبي هذه الجرائم. وتبرز أهمية إدخال مواد واضحة تحدد مسؤولية الأفراد عن استخدام الوسائل الإلكترونية كسلاح، مع تحديد الركن المادي والمعنوي المرتبط بالجريمة السيبرانية، بما يضمن تطبيق مبدأ المسؤولية الفردية الذي يرتكز عليه نظام روما.

3.3.3 أهمية إدخال الجرائم السيبرانية ضمن اختصاص المحكمة الجنائية الدولية

تُعد الجرائم السيبرانية ذات طبيعة عابرة للحدود، وتؤثر على الأمن الدولي بصورة مباشرة، مما يستدعي إدخالها ضمن اختصاص المحكمة الجنائية الدولية لتعزيز الردع والمساءلة. إذ يقتضي مبدأ "عدم الإفلات من العقاب" أن

تكون المحكمة قادرة على متابعة مرتكبي الجرائم السيبرانية التي تسبب أضرارًا واسعة على المجتمعات والدول (مرزق، 2021).

كما أن إدخال الجرائم السيبرانية يُعزّز دور المحكمة في مواجهة التحديات الجديدة، ويعطيها شرعية أوسع أمام المجتمع الدولي، ويحفز الدول الأطراف على تطوير تشريعات داخلية متوافقة مع النظام الدولي الجديد لمكافحة الجريمة السيبرانية. ويلاحظ أن هناك حالة من الفراغ القانوني الدولي فيما يخص تحديد اختصاص المحكمة على الجرائم السيبرانية، وهذا ما يزيد من أهمية تطوير النظام الأساسي ليتضمن هذه الجرائم بشكل رسمي.

3.3.4 دروس مستخلصة من ملاحقة الجرائم المستحدثة

إنّ تجارب المحاكم الدولية المختلفة، خصوصًا المحكمة الجنائية الدولية السابقة، مثل: محاكم يوغوسلافيا ورواندا، تقدم دروسًا مهمة في كيفية التعامل مع الجرائم المستحدثة. فقد كانت هذه المحاكم مرنة في تفسير النصوص القانونية لتغطية الجرائم الجديدة، ما يوضح إمكانية تطوير نظام روما الأساسي من خلال تفسيرات موسعة وتأويلات بناءة (خوجة، 2013).

كذلك، فإنّ متابعة الجرائم السيبرانية تتطلب تحديثًا مستمرًا للمعايير الفنية والقانونية، وتعاونًا دوليًا فعالًا بين الأجهزة القضائية والتقنية. إذ إنّ ملاحقة الجرائم السيبرانية لا يمكن أن تتم بمعزل عن التطور التكنولوجي، مما يحتم إنشاء وحدات فنية متخصصة داخل المحكمة أو بالتعاون معها.

4. الخاتمة

في ظل التطور التقني المتسارع الذي يشهده العالم، برزت الجريمة السيبرانية الآلية كإحدى التحديات الجديدة التي تواجه القانون الجنائي الدولي، لاسيما مع توظيف الذكاء الاصطناعي والخوارزميات في ارتكاب أفعال جرمية عبر الفضاء الإلكتروني. وتُظهر الدراسة أن الطبيعة التقنية لهذه الجرائم تعقّد من مهمة مساءلة الفاعلين، خاصة مع غياب شخصية قانونية للخوارزميات نفسها، ما يستوجب إعادة النظر في أُطر المسؤولية القائمة وفق نظام روما الأساسي. كما أن إدراج الجرائم السيبرانية ضمن اختصاص المحكمة الجنائية الدولية يمثل خطوة ضرورية لتحديث المنظومة القانونية الدولية بما يتماشى مع واقع الجريمة الحديثة. ومع ذلك، تواجه هذه المساعي تحديات قانونية وأدلة تقنية تتطلب تطوير آليات جمع الأدلة وتحليلها، فضلاً عن التنسيق الدولي الفعّال. لذلك، تُشكّل الدراسة مسعى لبلورة فهم قانوني متكامل يوازن بين التطورات التقنية ومتطلبات العدالة الجنائية الدولية.

4.1 النتائج

- إنّ تطور مفهوم الجريمة السيبرانية الآلية وتوسع استخدام الخوارزميات في تنفيذ هجمات رقمية جعل من الصعب تصنيفها ضمن الجرائم التقليدية، مما يتطلب توسيع المفاهيم القانونية.

- يتسم الركن المادي والمعنوي للجريمة السيبرانية الآلية بالتعقيد، إذ قد تنفذ الخوارزميات أفعالاً جرمية ذاتية التشغيل دون تدخل بشري مباشر، ما يطرح إشكالية تحديد المسؤولية الجنائية.
- إنّ التصنيف القانوني للجريمة السيبرانية ضمن الجرائم الدولية الأربع ما يزال محل نقاش، مع وجود مؤشرات على إمكانية إدراجها كجريمة حرب أو جريمة ضد الإنسانية، حسب تأثيرها وطبيعة استخدامها.
- إنّ غياب الشخصية القانونية للخوارزميات يحول دون مساءلتها مباشرة، ما يجعل المسؤولية تقع على الأفراد أو الجهات التي تطور أو توظف هذه التقنيات، وفق مبادئ المسؤولية الفردية والقادة.
- إنّ محدودية النصوص الحالية في نظام روما الأساسي تجعل المحكمة الجنائية الدولية تفتقر إلى أدوات قانونية واضحة لمقاضاة الجرائم السيبرانية الآلية، ما يستدعي تطوير تشريعي عاجل.
- إنّ أهمية بناء القدرات التقنية داخل المحكمة من خلال إنشاء وحدات فنية متخصصة قادرة على التعامل مع التعقيدات التقنية للأدلة السيبرانية.

4.2 التوصيات

- تعديل نظام روما الأساسي لإدخال نصوص واضحة تُجرّم استخدام الوسائل السيبرانية الآلية في ارتكاب الجرائم الدولية، مع توسيع اختصاص المحكمة ليشمل الجرائم التي تؤثر على البنية التحتية الحيوية وحماية المدنيين.
- إنشاء وحدات فنية متخصصة داخل المحكمة الجنائية الدولية لتعزيز القدرات التقنية في تحليل الأدلة السيبرانية، بما يضمن جمع الأدلة بطرق تكنولوجية حديثة وموثوقة.
- تشجيع الدول الأطراف على تحديث تشريعاتها الوطنية بما يتماشى مع التعديلات الدولية، لضمان تكامل الجهود القانونية على المستوى الدولي والوطني في مكافحة الجريمة السيبرانية.
- تعزيز التعاون الدولي وتبادل المعلومات التقنية والقانونية بين الدول والمحاكم والجهات المتخصصة، لتوحيد الاستراتيجيات وتحقيق ردع فعّال للجرائم السيبرانية الآلية.
- تطوير آليات الإثبات والأدلة التقنية عبر استحداث قواعد وإجراءات متخصصة داخل المحكمة، تعكس طبيعة الجرائم الرقمية وتعزز من قدرة القضاء على التعامل معها.
- رفع الوعي القانوني والتقني بين القضاة والمدعين العامين والمحامين بشأن الجريمة السيبرانية وآليات محاسبتها، من خلال برامج تدريبية متخصصة.

المراجع

المراجع العربية:

حساني، خالد. (2017). جريمة العدوان في ظل أحكام القانون الدولي المعاصر. *مجلة العلوم القانونية والسياسية*، 27(1)، 77-99.

الحسني، نادر. (2021). *الجرائم السيبرانية بين القانون الدولي والقانون الوطني: دراسة مقارنة*. (ط 3)، القاهرة، المركز العربي للدراسات القانونية.

خرشف، فاطمة. (2021). الإطار المفاهيمي والقانوني لمواجهة الجرائم السيبرانية. *مجلة سوسيولوجيا الجريمة للبحوث والدراسات العلمية في الظواهر الإجرامية*، 2(1)، 56-74.

خوجة، سعاد. (2013). محاكمات يوغسلافيا ورواندا ودورها في تطوير القضاء الدولي الجنائي. *مجلة الشريعة والاقتصاد*، 2(4)، 271-290.

الربيعي، نورهان. (2024). الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة). *مجلة الفارابي للعلوم الإنسانية*، 3(1)، 73-90.

رمضان، إبراهيم. (2025). مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي. *مجلة العلوم القانونية والاقتصادية*، 67(1)، 1744-1767.

الزنداني، إبراهيم. (2021). *الجرائم السيبرانية ودور السياسة الجنائية في مواجهتها والحد منها وأثرها على الأمن الدولي*. صنعاء: دار الكتب اليمنية للطباعة والنشر والتوزيع؛ مكتبة خالد بن الوليد.

زواقري، الطاهر؛ لخذاري، عبد المجيد. (2013). المسؤولية الجنائية الدولية للفرد. *مجلة العلوم الإنسانية*، العدد 32، 401-414.

فهمي، ياسر. (2025). الركن المادي في الجرائم الإلكترونية. *المجلة القانونية*، 23(2)، 905-966.

فياله، محمد. (2024). القانون الدولي والتحديات المعاصرة: الجريمة السيبرانية نموذجًا. *مجلة الحقوق للبحوث القانونية والاقتصادية*، 2(1)، 809-850.

المحكمة الجنائية الدولية ليوغوسلافيا السابقة. (1999). *قضية "الناتو – قصف يوغوسلافيا"*. المحكمة الجنائية الدولية ليوغوسلافيا السابقة.

المحكمة الجنائية الدولية. (2011). قرار ما قبل المحاكمة الأول، قضية "لوران غباغبو"، كوت ديفوار. المحكمة الجنائية الدولية.

مرزق، عبد القادر. (2021). مبدأ حظر استخدام القوة في القانون الدولي المعاصر. *مجلة الحقوق والعلوم الإنسانية*، 14(3)، 733-762.

مكتب المدعي العام للمحكمة الجنائية الدولية. (7 مارس، 2025). *مشاورة عامة حول السياسة المتعلقة بالجرائم الإلكترونية بموجب نظام روما الأساسي*. المحكمة الجنائية الدولية، متوفر على الرابط: https://www.icc-cpi.int/

المراجع العربية بنظام الرومنة:

Hsany, Khald. (2017). jrymh al'edwan fy zl ahkam alqanwn aldwly alm'easr. *mjlh al'elwm alqanwnyh walsyasyh*, 27(1), 77-99.

Alhsny, Nadr. (2021). *aljra'em alsybranyh byn alqanwn aldwly walqanwn alwtny: drash mqarnh*. (t 3), alqahrh, almrkz al'erby lldrasat alqanwnyh.

Khrshf, Fatmh. (2021). aletar almfahymy walqanwny lmwajhh aljra'em alsybranyh. *mjlh swsywlwjya aljrymh llbhwth waldrasat al'elmyh fy alzwahr alejramyh*, 2(1), 56-74.

Khwjh, S'ead. (2013). mhakmat ywghslafya wrwanda wdwrha fy ttwyr alqda' aldwly aljna'ey. *mjlh alshry'eh walaqtsad*, 2(4), 271-290.

Alrby'ey, Nwrhan. (2024). aljrymh alsybranyh walyat mkafhtha (drash mqarnh). *mjlh alfaraby ll'elwm alensanyh*, 3(1), 73-90.

Rmdan, Ebrahym. (2025). mwajhh alhjmat alsybranyh fy dw' ahkam alqanwn aldwly. *mjlh al'elwm alqanwnyh walaqtsadyh*, 67(1), 1744-1767.

Alzndany, Ebrahym. (2021). *aljra'em alsybranyh wdwr alsyash aljna'eyh fy mwajhtha walhd mnha wathrha 'ela alamn aldwly*. sn'ea': dar alktb alymnyh lltba'eh walnshr waltwzy'e؛ mktbh khald bn alwlyd.

Zwaqry, Altahr؛ Lkhdary, 'Ebd Almjyd. (2013). alms'ewlyh aljna'eyh aldwlyh llfrd. *mjlh al'elwm alensanyh*, al'edd 32, 401-414.

Fhmy, Yasr. (2025). alrkn almady fy aljra'em alelktrwnyh. *almjlh alqanwnyh*, 23(2), 905-966.

Fyalh, Mhmd. (2024). alqanwn aldwly walthdyat alm'easrh: aljrymh alsybranyh nmwdjana. *mjlh alhqwq llbhwth alqanwnyh walaqtsadyh*, 2(1), 809-850.

Almhkmh Aljna'eyh Aldwlyh Lywghwslafya Alsabqh. (1999). *qdyh "alnatw – qsf ywghwslafya"*. almhkmh aljna'eyh aldwlyh lywghwslafya alsabqh.

Almhkmh Aljna'eyh Aldwlyh. (2011). *qrar ma qbl almhakmh alawl, qdyh "lwran ghbaghbw", kwt dyfwar*. almhkmh aljna'eyh aldwlyh.

Mrzq, 'Ebd Alqadr. (2021). mbda hzr astkhdam alqwh fy alqanwn aldwly alm'easr. *mjlh alhqwq wal'elwm alensanyh*, 14(3), 733-762.

Mktb Almd'ey Al'eam Llmhkmh Aljna'eyh Aldwlyh. (7 mars, 2025). *mshawrh 'eamh hwl alsyash almt'elqh baljra'em alelktrwnyh bmwjb nzam rwma alasasy*. almhkmh aljna'eyh aldwlyh, mtwfr 'ela alrabt: https://www.icc-cpi.int/

المراجع الأجنبية:

International Court of Justice. (1986). *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua V. United States of America): Merits* (No. 70). International Court of Justice.

Jensen, E. T. (2013). Cyber attacks: Proportionality and precautions in attack. *International Law Studies, 89,* 198–217.

Radziwill, Y. (2015). *Cyber-attacks and the exploitable imperfections of international law*. Brill.

Schabas, W. A. (2016). *The International Criminal Court: A commentary on the Rome Statute* (2nd ed.). Oxford University Press.

United Nations. (1998, July 17). *Rome Statute of the International Criminal Court* (Article 28). International Criminal Court

International Criminal Court. (2012, March 14). *Prosecutor v. Thomas Lubanga Dyilo, ICC-01/04-01/06, Judgment pursuant to Article 74 of the Statute*. https://www.icc-cpi.int/court-record/icc-01/04-01/06-2842

The Guardian. (2013, April 17). *Supreme Court blocks Nigerian activists from suing Shell over alleged torture*. The Guardian. https://www.theguardian.com

Pretorius, B., & Van Niekerk, B. (2015, February). Cyber-security and governance for ICS/SCADA in South Africa. In *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 241-251).

International Criminal Court. (2019, July 8). *The Prosecutor v. Bosco Ntaganda, ICC-01/04-02/06, Judgment*. https://www.icc-cpi.int/drc/ntaganda

Supreme Court of Canada. (2020, February 28). *Nevsun Resources Ltd. v. Araya, 2020 SCC 5 (Docket No. 37919)*. https://www.scc-csc.ca/home-accueil/

The Guardian. (2024, June 25). *Russia-Ukraine war: ICC issues arrest warrants for Russian officials over attacks on Ukrainian civilian targets – as it happened*. The Guardian. https://www.theguardian.com/

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.