

جامعة عمار ثليجي الاغواط  
كلية الحقوق والعلوم السياسية  
قسم الحقوق



# الجريمة الدولية والتطور التكنولوجي

تخصص قانون دولي عام

إشراف

الاستاذ:

أ.د بن عطية

إعداد الطالب:

بوبكر علالي.

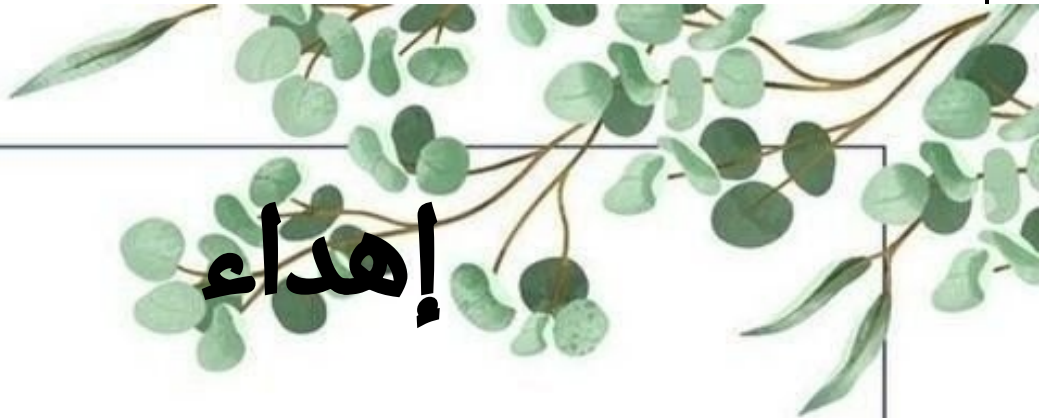
لخضر

لجنة المناقشة:

الاسم واللقب	الصفة
د. بن عرفة محمد نذير	رئيسا
أ.د بن عطية لخضر	مشرفا ومقررا
د. غريبي يحيى	عضوا مناقشا

السنة الجامعية: 2025/2026

إهداء



إلى روح والدي العزيز، رحمه الله وأسكنه فسيح جناته، الذي كان  
سندي الأول ومصدر قوتي في الحياة.

إلى والدتي الغالية، أطال الله في عمرها وأدام عليها الصحة  
والعافية، والتي كانت دعمي الدائم وسبب نجاحي بعد الله.  
إلى زوجتي وأولادي، الذين كانوا لي السند والدافع للاستمرار  
والمثابرة.

إلى إخوتي وأخواتي، الذين شاركوني مسيرة الحياة بكل حب  
ومساندة وتشجيع.

وإلى كل من كان له أثر، من قريب أو بعيد، في إنجاز هذا العمل.  
أهدي هذا العمل المتواضع، راجيًا من الله أن يكون علمًا نافعًا  
وعملًا مقبولًا



# شكر وعرّفان

الحمد لله حمداً يليق بجلاله وعظيم سلطانه، الذي بنعمته تتم الصالحات،  
وبتوفيّه أنجز هذا العمل.

نتقدم بأسمى عبارات الشكر والتقدير

إلى الأستاذ الدكتور المشرف بن عطية لخضر،

على ما أولاه من عناية علمية وتوجيهات قيمة وملاحظات دقيقة،  
كان لها الأثر البالغ في إثراء هذا البحث وإخراجه في صورته النهائية.  
كما نعبر عن خالص امتناننا إلى جميع الأساتذة الذين رافقونا خلال  
مسارنا الجامعي،

لما قدموه من علم رصين وتكوين أكاديمي ومرافقة علمية  
ساهمت في بناء رصيدنا المعرفي وصقل قدراتنا العلمية.

# مقدمة

## مقدمة

يشهد العالم في العقود الأخيرة تحولات تكنولوجية عميقة وغير مسبوقه لا تقل تأثيرا عن الثورة الصناعية الحديثة، بل يمكن وصفها بأنها ثورة رقمية شاملة تغير من طبيعة الحياة على جميع المستويات. فقد أفرز التقدم المتسارع في مجالات مثل الذكاء الاصطناعي، والأنظمة الرقمية المتصلة بالإنترنت، والفضاء السيبراني، والطائرات ذاتية التشغيل ديناميكيات جديدة في إدارة النشاطات البشرية، بما يشمل (Unmanned System) المجالات العسكرية، والاقتصادية، والاجتماعية، والإعلامية.

وعليه يعد الذكاء الاصطناعي مجرد أداة لتحسين الفعالية أو زيادة الإنتاج، وإنما أصبح جزءاً لا يتجزأ من القرارات المؤثرة في حياة الأفراد والمجتمعات، حتى في سياقات النزاعات المسلحة والأمن الدولي. هذه التكنولوجيا، التي كانت تُعد سابقاً موضوعاً للبحث العلمي والتجريب، تحوّلت اليوم إلى مكون أساسي في سلوك الأفراد والدول على حد سواء، بما يفرض إعادة النظر في جميع المفاهيم القانونية السائدة.

وقد انعكست هذه التحولات بشكل مباشر على البنى القانونية القائمة، لاسيما تلك التي صُممت في الأصل للتعامل مع واقع تقليدي للحياة الإنسانية والجرائم المرتكبة بأدوات تقليدية، ما أثار تساؤلات قانونية وفكرية جديدة حول قدرة الأنظمة القانونية الدولية على مواكبة ما أفرزته التكنولوجيا من نماذج إجرامية جديدة ومعقدة تتخطى الحدود التقليدية للدولة والزمان والمكان.

فالتطور التكنولوجي لا يضيف فقط وسائل جديدة لارتكاب الجريمة، بل يغير من جوهرها وطبيعتها إذ يمكن أن يرتكب فعل جرمي عبر شبكات رقمية معقدة، أو من خلال نظام ذكي يتخذ قراراته بشكل شبه مستقل، ما يجعله لا يزال خارج التصور القانوني الكلاسيكي للجريمة والمتطلبات التقليدية للمسؤولية الجنائية.

كما أدى هذا التحول إلى ظهور تهديدات سيبرانية متقدمة تتطلب استجابة دولية منسقة، إذ تحذر وكالات إنفاذ القانون مثل يوروبول من أن الذكاء الاصطناعي يعمل على تسريع تطور الجريمة المنظمة وجعلها أكثر دقة وتعقيداً، ما يضع منظومة القانون الدولي أمام تحديات جديدة في تنظيم العدالة الجنائية والاستجابة القانونية السريعة للتهديدات العابرة للحدود.

وبذلك، لم يعد موضوع التكنولوجيات الحديثة طموحاً علمياً فحسب، بل أصبح أحد أبرز الموضوعات التي تواجه القانون الدولي والعدالة الجنائية الدولية في عصرنا المعاصر، بما يفرض على الباحثين وصنّاع القانون معاونة التشريعات الحالية لإيجاد إطارات قانونية مرنة وفعالة تستوعب هذا التحول المتسارع وتضمن حماية حقوق الأفراد والمجتمعات من آثار هذه التحولات التقنية.

ينطلق هذا البحث من ضرورة دراسة التقاطع العميق بين الطفرة التكنولوجية ومفهوم الجريمة الدولية في إطار القانون الدولي الجنائي؛ خاصة في ظل بزوغ أنماط إجرامية عابرة للحدود تكسر القواعد التقليدية لمسرح الجريمة، إذ لم يعد حضور الجاني جسدياً شرطاً لارتكاب الفعل، كما نلمسه في الهجمات السيبرانية المنظمة والتعقيدات التقنية للأنظمة

## الذكية.

وتتضاعف أهمية هذه الدراسة بالنظر إلى ما تشكله هذه التطورات من تهديد حقيقي للسلم والأمن الدوليين؛ الأمر الذي يضع منظومة العدالة الجنائية الدولية أمام استحقاق مصيري يحتم عليها إعادة صياغة مفاهيمها الكلاسيكية، بدءاً من تكييف القصد الجنائي وقواعد إثبات المسؤولية، وصولاً إلى معايير قبول الأدلة الرقمية وفهم العلاقة المعقدة بين نصوص القانون والوسائل التقنية الحديثة

والهدف من هذه الدراسة هو تحديد الإطار القانوني الدولي الذي يمكنه تحقيق توازن فعال بين التطور التكنولوجي السريع ومفهوم الجريمة الدولية كما يحدده القانون الدولي الجنائي، من خلال تحليل التحديات القانونية التي تفرزها الأنظمة الرقمية المتقدمة، واستكشاف السبل الممكنة لتطوير آليات التحقيق والمساءلة في هذا السياق.

ويرتبط اختيار هذا الموضوع بأسباب ذاتية نبعت من شغفنا واهتمامنا بالبحث في القانون الدولي الجنائي وأسباب موضوعية تستند إلى الحاجة الملحة لاستيعاب التحولات التكنولوجية في الإطار القانوني الدولي، خاصة بعد أن أظهرت النزاعات الحديثة قصور النصوص الحالية في مواجهة هذه التحديات.

غير أن هذه الدراسة تواجه عدة صعوبات، من أبرزها غياب نصوص دولية واضحة تنظم الجرائم الرقمية في القانون الدولي الجنائي، وتشتت الاجتهادات الفقهية بين من يرى ضرورة ربط المسؤولية بالعامل البشري، وبين من يدعو إلى تطوير مبادئ قانونية جديدة تتناسب مع استدامة استقلالية الأنظمة التقنية، إضافة إلى القصور النسبي في الدراسات المحلية المنشورة مقارنة بوفرة الدراسات التقنية والعلمية.

وبناء على ما سبق، تبرز الإشكالية الأساسية لهذه الدراسة في السؤال التالي:

### **كيف يمكن للقواعد القانونية للجريمة الدولية مواكبة تأثير التطور التكنولوجي على المفهوم والمكافحة؟**

انطلاقاً من هذه الإشكالية، تعتمد هذه الدراسة على المنهج الوصفي، من خلال عرض الإطار المفاهيمي للموضوع، ثم تحليل النصوص المنظمة له في القانون الدولي الجنائي، بهدف فهم الإشكالية المطروحة وتفسير أبعادها القانونية.

وللإجابة عن الإشكالية المطروحة، تم تقسيم الدراسة إلى فصلين رئيسيين، حيث يتناول (الفصل الأول) تطور حتمي لمفهوم الجريمة الدولية وتحدياتها في ظل التطورات التكنولوجية، في حين يخصص (الفصل الثاني) لدراسة مدى قدرة القاعدة القانونية الدولية في مجال التجريم والمسؤولية على مواكبة هذا التطور التكنولوجي المتسارع.

يعكس هذا التقسيم منهجاً منظومياً وتحليلياً يربط بين التطور التكنولوجي والعدالة الجنائية الدولية، ويسعى إلى تقديم الإطار المفاهيمي المتوازن يجيب عن الإشكالية المطروحة.

## الفصل الأول:

تطور حتمي لمفهوم الجريمة الدولية وتحدياتها  
في ظل التطورات التكنولوجية

أفرز التطور المتسارع لتكنولوجيات الاتصال والمعلومات، وما صاحبه من رقمنة شاملة لمختلف مجالات النشاط الإنساني، تحولات عميقة لم تقتصر آثارها على البنى الاقتصادية والاجتماعية، بل امتدت لتطال المفاهيم القانونية الكلاسيكية، وفي مقدمتها مفهوم الجريمة الدولية فقد أسهمت البيئة الرقمية في إعادة تشكيل أنماط السلوك الإجرامي، وتوسيع مجالاته، وتعقيد وسائله، بما جعل الحدود الجغرافية والسيادية أقل قدرة على ضبط الأفعال ذات الطابع الدولي.

وفي هذا السياق لم تعد الجريمة الدولية محصورة في صورها التقليدية المرتبطة باستخدام القوة المادية أو السيطرة الإقليمية المباشرة، بل أضحت التكنولوجيا وسيطاً مركزياً في التخطيط والتنفيذ والتأثير، سواء من خلال الفضاء السيبراني، أو عبر تقنيات الذكاء الاصطناعي والطائرات المسيّرة والأنظمة المؤتمتة. وهو ما أفرز تحديات قانونية غير مسبوقة، مست جوهر الأركان المكونة للجريمة الدولية، وأعاد طرح إشكاليات المسؤولية الجنائية، وتحديد الفاعل، وإثبات القصد، في بيئة تتسم بالتعقيد واللامركزية.

وانطلاقاً من ذلك يهدف هذا الفصل إلى إبراز كيفية تفاعل مفهوم الجريمة الدولية مع التحولات التكنولوجية، من خلال تحليل التحول المفاهيمي الذي عرفته الجريمة في العصر الرقمي، واستجلاء صور الجرائم الدولية المستحدثة، (المبحث الأول) إلى جانب الوقوف عند أثر البيئة الرقمية على الركبين المادي والمعنوي للجريمة الدولية، وما تطرحه من إشكالات عملية ونظرية أمام القانون الدولي الجنائي وآلياته التقليدية. (المبحث الثاني).

## **المبحث الأول: الجريمة الدولية أمام إلزامية التطور المفاهيمي موازاة بالتطور التكنولوجي**

أدت التحولات التكنولوجية المتسارعة إلى إعادة تشكيل البنية المفاهيمية للجريمة الدولية، سواء من حيث طبيعتها، أو نطاقها، أو الوسائل المعتمدة في ارتكابها. فقد أفرزت البيئة الرقمية أنماطاً إجرامية جديدة تجاوزت الأطر التقليدية التي استقر عليها الفقه والقانون الدولي الجنائي، وأصبحت التكنولوجيا عنصراً فاعلاً في إعادة تحديد خصائص الجريمة الدولية وحدودها.

وانطلاقاً من هذا التحول، يقتضي تناول الموضوع الوقوف، أولاً، على تطور تعريف الجريمة الدولية في ظل المستجدات التكنولوجية، وما مسّ محدداتها التقليدية من إعادة

نظر، ثم الانتقال)، المطلب الأول (ثانيًا، إلى تحليل صور الجرائم الدولية التي أفرزها التطور التقني، لاسيما تلك المرتبطة بالفضاء السيبراني والتقنيات الرقمية الحديثة، وما تثيره من تحديات قانونية على المستوى الدولي). المطلب الثاني)

## **المطلب الأول: تعريف الجريمة الدولية في ضوء التطور التكنولوجي**

أفرز التطور التكنولوجي المتسارع واقعًا جديدًا فرض إعادة النظر في الإطار المفاهيمي للجريمة الدولية، بعدما أصبحت الوسائل الرقمية عنصرًا مؤثرًا في طبيعة الفعل الإجرامي ونطاقه وأثاره العابرة للحدود. ومن هذا المنطلق، يقتضي تناول الموضوع استعراض المحددات التقليدية لمفهوم الجريمة الدولية، الفرع الأول (ثم بيان التحولات التي أحدثها التطور الرقمي على خصائصها ومضمونها). الفرع الثاني)

## **الفرع الأول: المحددات التقليدية للجريمة الدولية في الفقه والقانون الدولي الجنائي**

تشكل الحماية الدولية للمصلحة المحمية أحد المحددات الأساسية المعتمدة في تصور الجريمة الدولية التقليدي، إذ تستند إلى فكرة أن الجريمة الدولية لا تقوم إلا إذا كان الاعتداء يمس مصلحة جوهرية للمجتمع الدولي ككل وتجاوز إطار المصالح الوطنية الخاصة، وهو ما يعكس الدور الذي يقوم به القانون الدولي الجنائي في حماية القيم والمصالح المشتركة للمجتمع الدولي من أخطر الانتهاكات التي تهدد السلم والأمن الدوليين.

## **أولاً: طبيعة المصلحة المحمية في الجريمة الدولية**

يشكل مفهوم المصلحة الدولية المحمية في القانون الدولي الجنائي معيارًا جوهريًا لتمييز الجريمة الدولية عن الجرائم الوطنية، إذ أن الأخير يعتمد على حماية مصالح الدولة ومواطنيها ضمن حدودها، بينما تتجاوز الجريمة الدولية هذه الحدود لتستهدف قيمًا ومصالح قانونية عالمية مشتركة تمس المجتمع الدولي بأسره ومن هذا المنطلق لا يعد مجرد ارتكاب فعل مخالف للقانون الجنائي كافيًا لتكوينه جريمة دولية، بل يستلزم أن يكون الفعل مساسًا بمصلحة محمية دولية، ويثير قلق الضمير الإنساني، ويشكل تهديدًا واضحًا للسلم والأمن الدوليين، الأمر الذي يستدعي تضافر جهود المجتمع الدولي لمساءلة مرتكبيه وضمان منع تكرار مثل هذه الانتهاكات.

ويعكس نظام روما الأساسي للمحكمة الجنائية الدولية هذا المبدأ بوضوح في ديباجته، إذ يشير إلى أن الجرائم التي تدخل ضمن اختصاص المحكمة هي أشد الجرائم التي تثير قلق المجتمع الدولي بأسره، ما يجعلها تمس مصالح وقيمًا مشتركة تستدعي حماية جماعية دولية:

{ إن الجرائم الجسيمة التي تثير قلق المجتمع الدولي بأسره يجب ألا تمر دون عقاب... }  
وأن ضمان مقاضاة مرتكبيها يسهم في منع تلك الجرائم.

وتنص المادة 5 من نظام روما الأساسي على أن اختصاص المحكمة يقتصر على الجرائم التي تمثل أشد الانتهاكات التي تثير اهتمام المجتمع الدولي بأسره، محددة بذلك

الفئات الرئيسية لتلك الجرائم، وهي الإبادة الجماعية، والجرائم ضد الإنسانية، وجرائم الحرب، وجريمة العدوان:

“The jurisdiction of the Court shall be limited to the most serious crimes of concern to the international community as a whole, namely: genocide, crimes against humanity, war crimes, and the crime of aggression.”

ويشير هذا النص إلى أن المعيار الموضوعي لتحديد الجريمة الدولية لا يقوم على وصف لغوي أو صياغة لفظية فحسب، بل يرتبط بمدى تأثير الفعل على السلم والأمن الدوليين وعلى القيم القانونية المشتركة، وبهذا المعنى، فإن القانون الدولي الجنائي يسعى لحماية مبادئ وقيم كونية وإنسانية أساسية، مثل حق الحياة، وكرامة الإنسان، ومنع الانتهاكات المنهجية التي قد تهدد استقرار النظام الدولي.

كما يتضح أن معيار المصلحة المحمية يتجاوز نطاق الحماية الوطنية المحدود، ليعكس اهتمام المجتمع الدولي بالقيم القانونية الكونية. فالالتزام الدولي الجماعي بعدم إفلات مرتكبي الجرائم الدولية من العقاب لا يقتصر على الاعتبار الفردي أو المحلي، بل يستهدف حماية نظام قانوني دولي عام قائم على المبادئ الأساسية لميثاق الأمم المتحدة وروح نظام روما الأساسي معاً، وهو ما يشكل دعامة مركزية لفهم طبيعة الجريمة الدولية في القانون الدولي الجنائي.

ومن منظور فقهي يرتبط هذا المعيار بتصور القانون الدولي الجنائي لجرائم ذات خطورة استثنائية وانتهاك جسيم للقيم القانونية المشتركة، الأمر الذي يبرر تدخل المجتمع الدولي عبر محكمة دائمة بدلاً من الاقتصار على العدالة الوطنية، ويعكس التزاماً جماعياً بالقضاء على الإفلات من العقاب، وهو الهدف الأساسي الذي يسعى إليه القانون الدولي الجنائي لضمان حماية السلم والأمن الدوليين وكرامة الإنسان على حد سواء.

ينبثق معيار المصلحة الدولية المحمية في الجريمة الدولية من فكرة أن الجرائم الدولية تنطوي على انتهاكات للقيم القانونية العالمية الأساسية وتسهم في زعزعة السلم والأمن الدوليين، وهو ما أقرته الجماعة الدولية في اتفاقياتها، مثل نظام روما الأساسي، الذي يربط اختصاص المحكمة الجنائية الدولية بالفعل الذي يثير قلق المجتمع الدولي بأسره. ويعد هذا المعيار أساساً موضوعياً في عملية التمييز بين الجرائم الدولية والجرائم الوطنية، مما يؤسس لضرورة تدخل القانون الدولي الجنائي في حماية القيم والمعايير القانونية المشتركة للجماعة الدولية.

## ثانياً: أثر تحديد المصلحة الدولية على فهم الجريمة الدولية

يتجلى أثر محدد المصلحة الدولية المحمية في قلب بنية القانون الدولي الجنائي نفسه، إذ لا يكفي أن تنشأ مخالفة لقواعد القانون الدولي العام لوحدها حتى تشكل جريمة دولية، بل يجب أن تمس انتهاكات تلك القواعد مصالح حيوية مشتركة لدي الجماعة الدولية تعد أساسية لحماية السلم والأمن وكرامة الإنسان وهذا ما يجعل تجريم الجرائم الدولية قائماً على مشروع جماعي يتجاوز إرادة الدولة المفردة ويستند إلى إرادة المجتمع الدولي المعبر

عنها في الاتفاقات الدولية مثل نظام روما الأساسي للمحكمة الجنائية الدولية، وليس مجرد قواعد جنائية وطنية أو انعكاس لمصلحة محلية ضيقة.

ويشير الفقه القانوني إلى أن الجرائم الدولية ترتكب ضد مصلحة دولية أو إنسانية تهم الجماعة الدولية بأسرها، مما يجعل القانون الدولي الجنائي وسيلة لحماية هذه المصالح العليا التي أخذها المجتمع الدولي على عاتقه بعد تجارب تاريخية دامية مثل الحربين العالميتين، وأثرى كل ذلك الحاجة إلى وضع إطار جنائي دولي لمعاقبة مثل هذه الانتهاكات.

إن هذا التصور لا يفتح فقط باب التدخل القانوني الدولي في مواجهة الانتهاكات التي تمس مصالح جماعية، بل يخلق معياراً موضوعياً لتحديد ما إذا كان الفعل قد بلغ مستوى الجريمة الدولية، وذلك بأن تكون له آثار واسعة ومعان عميقة ترتبط بالقيم القانونية المشتركة. بمعنى آخر، تجريم الفعل كجريمة دولية لا يكون بمجرد عرضه على مخالفة القواعد القانونية الدولية، بل بتأثيره في المصلحة الدولية المشتركة وبما يشكل تهديداً قائماً للسلم والأمن الدوليين أو لحقوق الإنسان الأساسية.

ولهذا السبب يرى الفقه أن التجريم الدولي لا يتوقف على مجرد النية الإجرامية أو الفعل، بل على مدى خطورته وانتهاكه لمصلحة دولية يحميها القانون الجنائي الدولي، وقد أفرز هذا التصور تطوراً في القانون الدولي الجنائي ذاته، حيث نشأت نظم مثل المحكمة الجنائية الدولية لمساءلة الأفراد الذين ترتكب أفعالهم انتهاكات جسيمة للمصالح القانونية المشتركة، بغض النظر عن موقعهم الوطني أو السياسية الداخلية للدول.

### **ثالثاً: التمييز بين الحماية الدولية والحماية الوطنية**

من الناحية المنهجية يظهر التمييز بين الحماية الدولية والحماية الوطنية من خلال طبيعة المصلحة التي تستند إليها قواعد التجريم والجزاء، فالحماية الوطنية تعنى بإرساء قواعد جنائية لحماية مصالح الدولة داخلياً مثل أمنها الداخلي وممتلكات مواطنيها ونظامها العام، ويكون ذلك من خلال التشريعات الجنائية الداخلية التي تعاقب على الأفعال المخالفة ضمن إقليم الدولة.

أما الحماية الدولية فهي ترتبط بقواعد تتبناها الجماعة الدولية ككل عبر اتفاقيات دولية وعرف دولي، تهدف إلى حماية مصالح يمكن اعتبارها ذات طابع عالمي أو مشترك؛ مثل منع الإبادة، حماية الإنسانية من الانتهاكات المنهجية، وضمان عدم الإفلات من العقاب لمن يرتكب جرائم تؤثر على السلم والأمن الدوليين، وهذا ينعكس في بنى القانون الدولي الجنائي الذي يفرض مسؤولية جنائية عن أفعال لها أثر دولي واسع ولا يمكن احتواؤها ضمن الإطار الوطني فقط، إذ تستدعي تدخلاً جماعياً من قبل المجتمع الدولي لمعالجتها بشكل فعال.

وتقديماً فإن الجرائم التي لا تتجاوز تأثيرها حدود دولة واحدة ولا تمس مصالح دولية كبرى تظل ضمن نطاق القانون الجنائي الوطني، وتكون مسؤولية منظمة داخلياً وفق القواعد التشريعية الوطنية أما تلك الانتهاكات التي ترتكب اعتداء على مصلحة دولية مشتركة، فإنها تستوجب تطبيق قواعد القانون الدولي الجنائي لأنها تمس مصالح جماعية أوسع تتطلب معالجة على مستوى المجتمع الدولي ككل.

يتبين أن مفهوم المصلحة الدولية المحمية يشكل معيارا جوهريا في القانون الدولي الجنائي لتحديد الجريمة الدولية، إذ لا يكفي مجرد مخالفة قواعد القانون الدولي العام، بل يشترط أن يكون الفعل مساسا بمصلحة تتجاوز المصالح المحلية وتهم المجتمع الدولي بأسره، بما يبرر تدخل القانون الدولي الجنائي وتطبيق تدابير.

ولذلك فإن تجريم الفعل كجريمة دولية يفترض تأثيرا دوليا واسعا يستدعي حماية جماعية وتقاضيا دوليا، بدل الاقتصار على المقاربة الوطنية، بينما تبقى الأفعال ذات التأثير المحدود ضمن نطاق القانون الجنائي الوطني وحده ما لم تمس مصالح قانونية عالمية مشتركة تستدعي حماية جماعية ومنع الإفلات من العقاب.

## **الفرع الثاني: التحولات المستحدثة إثر التطور الرقمي على مفهوم وخصائص الجريمة الدولية**

لقد أحدث التحول الرقمي طفرة نوعية في طبيعة الجريمة الدولية ومفهومها، مما شكل تحولا منهجيا في القانون الدولي الجنائي على المستويات النظرية والتطبيقية فبينما كان القانون الجنائي التقليدي يتعامل مع فعل إجرامي ذو أركان واضحة (فعل مادي محسوس، إرادة فعلية، توافر قصد جنائي)، فإن التحول الرقمي وظهور البيئة السيبرانية أضافا أبعادا جديدة لمفهوم الجريمة الدولية، مما دفع الفقه والممارسات الدولية إلى إعادة النظر في أطر المفهوم التقليدي وتكييفها لتعكس واقعا جنائيا متحولا يعبر عنه بوضوح في الأدبيات القانونية الحديثة.

### **أولا: الجريمة السيبرانية كتحوّل جوهري في مفهوم الجريمة الدولية**

ظهرت الجريمة السيبرانية كأحد أبرز مظاهر التحوّل النوعي في طبيعة الجريمة الدولية في ظل الثورة الرقمية، بحيث لم تعد الجرائم مقتصرة على الفعل المادي التقليدي المرتبط بمكان وزمان محددين، بل باتت مرتكزة على التكنولوجيا الرقمية وشبكات الإنترنت التي تسمح للمجرمين بتنفيذ أفعال تستهدف أنظمة معلومات أو بيانات أو شبكات تقنية متطورة عبر حدود الدول، دون الحاجة إلى وجود فعلي للجاني في مسرح الجريمة كما كان الحال في الجرائم التقليدية.

ويشير الفقه إلى أن جرائم تكنولوجيا المعلومات، التي تعرف أيضا بالجرائم الإلكترونية أو السيبرانية، تشمل أنشطة إجرامية متعددة مثل الاختراق غير المصرح به للأنظمة، سرقة البيانات، الاحتيال عبر الإنترنت، وحتى الهجمات على البنى التحتية الرقمية، وتستهدف في كثير من الحالات أفرادا، شركات، حكومات عبر شبكة الإنترنت العالمية دون اعتبار للحدود الجغرافية.

ومن أبرز الخصائص التي تميز الجريمة السيبرانية عن الجرائم التقليدية طابعها العابر للحدود، فهي لا تعترف بالحدود الوطنية، وقد يكون الضحية في دولة ما، والفاعل في دولة أخرى، والأدلة الرقمية في دولة ثالثة، مما يعقد تطبيق المعايير القانونية التقليدية للمسؤولية الجنائية التي تقوم أساسا على نطاقات إقليمية للولاية القضائية وتنبع هذه الصعوبة من الطبيعة الافتراضية للفضاء السيبراني الذي يمكن الجريمة من العبور الفوري واللامحدود عبر

الشبكات الرقمية، ما يخلق ثغرات قانونية وإجرائية في تطبيق القواعد الجنائية القائمة.

وتتطلب هذه الطبيعة العابرة للحدود للجرائم السيبرانية معالجات قانونية جديدة وتعاونًا دوليًا واسعًا يتجاوز حدود التشريعات الوطنية، التي في الكثير من الأحيان لا تواكب التطور التكنولوجي الحديث في تعريف الأفعال الإجرامية وأركانها فالعديد من التشريعات الوطنية تظل مرتبطة بمفاهيم الإقليم والوجود المادي للفاعل، بينما جرم الفضاء السيبراني أفعالًا ليست محصورة في إقليم بعينه، ويتطلب تنسيقًا تشريعيًا دوليًا لتوحيد التعريفات، وتسهيل التعاون في التحقيق والملاحقة ومعاينة الفاعلين عبر الدول المختلفة.

وقد كان من أولى الاستجابات الدولية للتحديات المتعلقة بالجرائم عبر الإنترنت اتفاقية بودابست لمكافحة الجريمة السيبرانية (Convention on Cybercrime)، التي أُعدت تحت إشراف مجلس أوروبا ودخلت حيز التنفيذ في 1 تموز/يوليو 2004، لتمثل أول صك دولي متعدد الأطراف يضع إطارًا قانونيًا واضحًا للتعامل مع الجرائم المعلوماتية العابرة للحدود، ويعمل على توحيد التشريعات الوطنية وتسهيل التعاون الدولي بين الدول الأطراف في مواجهة هذه الجرائم.

وتسعى هذه الاتفاقية إلى تجريم الأفعال الإلكترونية الإجرامية مثل الدخول غير المصرح به إلى الأنظمة، والتدخل في البيانات والمنظومات، والاحتياز المرتبط بالكمبيوتر، وجرائم تتعلق بالمواد الإباحية للأطفال، وغيرها من الانتهاكات التي يمكن تنفيذها عبر الشبكات الرقمية، وهو ما يعكس ضرورة موازنة القانون الجنائي مع طبيعة الجرائم الحديثة غير التقليدية.

كما تمنح الاتفاقية الدول الأطراف وسائل وإجراءات إجرائية جنائية متقدمة تشمل حفظ الأدلة الرقمية، والحصول على بيانات الاتصالات المرورية والمحتوى، وأوامر الإنتاج والمصادرة، وإجراءات المسح والضبط على النظم المعلوماتية. وتضم الاتفاقية أيضًا شبكة تعاون دولية تعمل 24/7 لتقديم المساعدة الفورية بين الدول في قضايا الأدلة الرقمية العابرة للحدود، مما يعزز قدرة الدول على متابعة الجرائم السيبرانية التي لا تعترف بالحدود الإقليمية.

ويبرز دور اتفاقية بودابست في تعزيز التعاون القضائي الدولي، إذ تشكل إطارًا لبناء الثقة بين الدول وتنسيق السياسات الجنائية، بما يسمح للدول بالتعاون في التحقيقات والملاحقات وإجراءات تبادل الأدلة والأبحاث التقنية، وهو أمر بالغ الأهمية في عالم تتوسع فيه الجرائم الرقمية بسرعة ولا يمكن لأي دولة وحدها مواجهتها بفعالية دون دعم وتنسيق دوليين.

وقد اعتبر هذا الصك رغم كونه أوروبي الأصل، مرجعًا دوليًا مهمًا لبناء تشريعات وطنية ومحاربة الجرائم السيبرانية على نطاق عالمي، وقد انضمت إليه دول خارج إطار مجلس أوروبا مثل كندا واليابان والولايات المتحدة، ما يؤكد أهميته كإطار عملي في مواجهة الجرائم المعلوماتية التي تتطلب تنسيقًا قانونيًا وعبر حدود لا يتيحها أي نص وطني بمفرده.

إلى جانب ذلك فإن الجمعية العامة للأمم المتحدة اعتمدت في أواخر 2024 اتفاقية

دولية شاملة لمكافحة الجريمة السيبرانية لتضيف إطاراً عالمياً ملزماً قانوناً، يهدف إلى تعزيز التعاون الدولي في تبادل الأدلة الإلكترونية، وتجميد العائدات الإجرامية، وحماية الضحايا، وتقديم دعم فني للدول خاصة الدول النامية، وهو تطور يعكس إدراك المجتمع الدولي للحاجة إلى إطار عالمي متكامل يتجاوز الاتفاقيات الإقليمية السابقة.

وبذلك تمثل اتفاقية بودابست وعدد من المبادرات الدولية اللاحقة خطوة تأسيسية في تطوير القانون الدولي الجنائي لمواكبة الجرائم الرقمية، حيث توفر مرجعاً قانونياً دولياً يسعى إلى دعم منظومة العدالة الجنائية العالمية في مواجهة تهديدات الفضاء السيبراني التي لم تكن موجودة في المفهوم الجنائي التقليدي، وتدفع باتجاه توحيد التشريعات وتعزيز التعاون عبر الحدود في محاكمة ومعاينة الجريمة السيبرانية.

### ثانياً: أثر الذكاء الاصطناعي والتقنيات المتقدمة على خصائص الجرائم الدولية

أضاف الذكاء الاصطناعي (AI) والتقنيات الرقمية المتقدمة مثل البلوكشين، الروبوتات، والطائرات المسيّرة طبقة من التعقيد غير المسبوقة إلى مفهوم وخصائص الجرائم الدولية، بحيث لم تعد الجرائم تقتصر على الأفعال المادية التقليدية المنسوبة مباشرة إلى الإنسان، بل باتت تشمل أفعالاً مؤتمتة أو شبه مستقلة تنفذ عبر أنظمة ذكية قادرة على التعلم، واتخاذ قرارات معقدة دون تدخل بشري مباشر. هذه الطبيعة الجديدة تمثل تحولاً جوهرياً في فهم كيفية وقوع الجرائم، وتشكل تحدياً حقيقياً للركن المادي والمعنوي في القانون الدولي الجنائي الذي يشترط عادةً وجود فعل بشري وإرادة جنائية واعية.

أظهرت الدراسات القانونية أن الذكاء الاصطناعي يغير القواعد التقليدية المرتبطة بالفاعل الإجرامي، وذلك عندما تقوم نظم أو آليات ذكية بتنفيذ أفعال قد تنتج عنها أضرار قانونية أو انتهاكات لحقوق أساسية دون أن يكون هناك فاعل بشري واضح يمكن تحميله المسؤولية، وهذا ما يطرح إشكالية في تحديد الركن المعنوي (القصد الجنائي) وأصول المسؤولية الجنائية. في بعض الحالات، يمكن أن تكون نظم الذكاء الاصطناعي قد صممت أو برمجت مسبقاً لتنفيذ سلوك ما، لكنها تتطور عبر خوارزميات التعلم الآلي بحيث يصبح تحديد الإرادة البشرية "وراء النتيجة النهائية معقداً، إن لم يكن مستحيلاً."

هذا التعقيد لا يظهر فقط في تحليل السبب المباشر وراء الفعل، بل يمتد أيضاً إلى تحديد علاقة الذكاء الاصطناعي بالضرر الناتج، حيث يمكن لأنظمة الذكاء الاصطناعي أن تخلق سلوكاً يؤثر على نطاق واسع، مثل الهجمات السيبرانية المتقدمة التي تستغل أنظمة ذكية للتكيف وتقسيم الموارد أو البيانات لأغراض احتيالية أو تدميرية. وتثير هذه الحالة تساؤلات قانونية عميقة حول ما إذا كان ينبغي تحميل المبرمج أو مطور النظام أو المشغل النهائي مسؤولية جنائية، وكيف يمكن للمعايير التقليدية للنية والقصد أن تطبق في مثل هذه الحالات.

كما يعكس هذا التطور تحديات بنيوية في الركن المادي للجريمة الدولية. ففي الجرائم التقليدية، يُنظر إلى الفعل الجرمي على أنه سلوك بشري محسوس أو استخدام أداة مادية، أما في سياق الذكاء الاصطناعي فإن الفعل يمكن أن يكون نتاج برنامج تقني يصدر عنه سلوك

غير متوقع أو غير واضح النية البشرية في سببه، مثلما تطرق إليه بعض الباحثين في الدراسات الحديثة حول الجرائم الرقمية وصعوبة تحديد الإرادة الجنائية.

وبهذا يصبح الذكاء الاصطناعي عاملاً محورياً في إعادة تشكيل الأطر القانونية الجنائية، ليس فقط بوصفه وسيلة تستخدم في ارتكاب الجريمة، بل باعتباره أطروحة جديدة حول الفعل نفسه وآليات تنفيذه. فمن ناحية، يمكن للذكاء الاصطناعي أن يعزز قدرة التحقيق الجنائي من خلال أدوات تحليل متقدمة تساعد في تتبع الأدلة الرقمية، وإجراء تحليلات معقدة للبيانات الجنائية، مما يعزز من قدرات نظم العدالة الجنائية في مواجهة الجرائم السيبرانية.

ومن ناحية أخرى فإن استخدام الذكاء الاصطناعي في تنفيذ الفعل الإجرامي يضع القانون الدولي الجنائي أمام ضرورة تطوير مفهوم الركن المادي والمعنوي ليتسق مع الواقع الرقمي الحديث، الذي قد لا يقتصر فيه الفعل الجرمي على إرادة بشرية مباشرة، بل على علاقات معقدة بين البشر والأنظمة الذكية. وهذا يستدعي إعادة نظر في مبادئ المسؤولية وإيجاد معايير قانونية جديدة تحسن التكيف مع الواقع التقني المعاصر وتضع قواعد واضحة لمسؤولية الأفراد والمؤسسات عند استخدام أو تطوير نظم الذكاء الاصطناعي التي تستخدم في ارتكاب جرائم دولية.

### **ثالثاً: إشكالات تقليص الحدود الوطنية في مواجهة الجرائم الرقمية**

من أبرز مظاهر التحول الذي أحدثته الثورة الرقمية في عالم الجريمة الدولية، أن الحدود السيادية للدول لم تعد تعكس واقع الجرائم الرقمية العابرة للحدود، إذ يمكن ارتكاب فعل إجرامي عبر شبكة الإنترنت من قارة إلى أخرى في غضون ثوان، وهو ما يفضي إلى أن الجرائم التي كانت في الماضي تتطلب وجوداً مادياً للفاعل في مكان الجريمة أصبحت اليوم تتجاوز هذا الشرط التقليدي، لتصبح الجرائم العابرة للحدود قاعدة وليس استثناء في سياق الجرائم الرقمية.

ويرى الفقه أن الطبيعة العبر-حدودية لهذه الجرائم تشكل فراغات قانونية وتشريعية، لأن التشريعات الوطنية في كثير من الأحيان لم تحدث تكييفاً مناسباً لتلك الجرائم، مما يؤدي إلى صعوبة تحديد الاختصاص القضائي، وجمع الأدلة الرقمية، وتحديد المسؤولية الجنائية بفعالية.

ولا يقتصر التحدي على مجرد عبور الحدود، بل يتفاقم بفعل تنوع وتضارب التشريعات الوطنية فيما يتعلق بتوصيف الأفعال الجرمية الرقمية ومسؤولية تنفيذها، وهو ما يحد من فاعلية الإجراءات التقليدية للمساعدة القانونية المتبادلة بين الدول، ويبيط عمليات التحقيق والملاحقة القضائية بسبب اختلاف معايير قبول الأدلة الرقمية، والقيود الإجرائية في كل نظام قانوني وفي واقع كهذا تسعى الجماعة الدولية إلى تطوير آليات قانونية دولية جديدة تسهل تبادل المعلومات والتحقيقات بين الدول، وتعالج التحديات التقنية والإجرائية بفعالية لا تقتصر على الولاية الوطنية التقليدية فقط.

### **المطلب الثاني: الجرائم الدولية الناشئة عن التكنولوجيا**

مع التطور التكنولوجي الهائل الذي يشهده العالم في العصر الرقمي، برزت أنواع جديدة من الجرائم التي تتجاوز الحدود الجغرافية وتترك أثراً عميقاً على الأمن الدولي والنظام القانوني العالمي. فقد أضحت استخدام الشبكات الرقمية والأنظمة الذكية في ارتكاب

الأفعال الإجرامية ظاهرة معقدة تتطلب فهما متداخلا بين القانون والتكنولوجيا، خاصة في ظل انتشار الجرائم السيبرانية التي يمكن أن تنفذ عن بعد وتؤثر على دول متعددة.

كما أسهمت الابتكارات الحديثة مثل الذكاء الاصطناعي، والروبوتات، والطائرات المسييرة، وتقنية البلوكشين في تغيير آليات ارتكاب الجرائم الدولية، مما خلق تحديات جديدة أمام التشريعات التقليدية لذلك أصبح من الضروري دراسة هذه الظواهر القانونية والتكنولوجية من منظور دولي لفهم طبيعتها وأبعادها القانونية. هذا المطلب يسلب الضوء أولاً على الجرائم السيبرانية العابرة للحدود كأحد أبرز أشكال الجريمة في العصر الرقمي **الفرع الأول)، ثم يتناول أثر بعض التقنيات الحديثة في تكوين وصياغة الجرائم الدولية ( المعاصرة). (الفرع الثاني).**

## **الفرع الأول: التحديات القانونية والتعاون الدولي في الجرائم السيبرانية العابرة للحدود**

تمثل الجرائم السيبرانية العابرة للحدود أحد أبرز مظاهر الجريمة في عصر الثورة الرقمية، حيث نشأت نتيجة التطور المتسارع في تكنولوجيا المعلومات والاتصالات الذي أتاح للمجرمين استغلال الفضاء الإلكتروني لارتكاب أعمال إجرامية دون تقييد بالحدود الجغرافية أو الوطنية. وتعرف هذه الجرائم على أنها أنشطة غير قانونية تنفذ عبر الشبكات الحاسوبية وتستهدف نظاماً معلوماتية وأفراداً أو مؤسسات في دول مختلفة، مما يجعلها ذات طابع دولي يتجاوز الإطار التقليدي للجريمة المحلية وتستدعي استجابات قانونية تتجاوز التشريعات الوطنية.

ومع انتشار استخدام الإنترنت وتطبيقاته في الأنشطة اليومية، أصبح بإمكان مرتكبي الجرائم استهداف ضحايا في بلدان متعددة باستخدام أساليب معقدة مثل الاحتيال الرقمي، والقرصنة، والابتزاز، وغيرها، مع صعوبة تحديد مكان الجريمة أو المجرم بصورة دقيقة، بسبب الطبيعة الافتراضية لمرتكزاتها ومنظومات تنفيذها التي لا تعترف بالحدود الوطنية. وتثير هذه الطبيعة العابرة للحدود تحديات قانونية جوهرية لا تقتصر على تحديد مكان ارتكاب الفعل الإجرامي، بل تمتد إلى تحديد الولاية القضائية، وتنازع القوانين، وإجراءات جمع الأدلة الرقمية وحجيتها أمام المحاكم الوطنية والدولية.

ورغم سبق التطرق إلى اتفاقية بودابست لمكافحة الجريمة السيبرانية في سياق بيان أثر التحول الرقمي على مفهوم الجريمة الدولية، فإن استحضارها في هذا الموضع يندرج ضمن تحليل دورها الإجرائي في معالجة إشكاليات الاختصاص والتعاون القضائي الدولي وليس مجرد عرض تعريفي، وهو ما يبرز تعدد وظائفها القانونية في مواجهة الجرائم السيبرانية العابرة للحدود.

وتعد اتفاقية بودابست إطاراً قانونياً شاملاً، يستند إليه في تطوير التشريعات الوطنية لحماية الأنظمة المعلوماتية، وتوفير آليات قانونية فعالة للتعاون الدولي تشمل تبادل المعلومات والإجراءات القضائية الفورية، وإجراءات حفظ البيانات الإلكترونية والإفصاح عنها في سياق التحقيقات الجنائية، وقد شملت بروتوكولات إضافية لهذه الاتفاقية تدابير لتعزيز التعاون الدولي والكشف عن الأدلة الرقمية بكفاءة أكبر، بما يلائم سرعة تطور الجرائم السيبرانية.

تبرز أهمية هذه الاتفاقيات الدولية في أنها لا توفر فقط أدوات للتعاون القضائي، بل تسعى أيضا إلى توحيد المفاهيم القانونية والممارسات التشريعية بين الدول، وذلك عبر تحديد نماذج قانونية للتجريم والإجراءات القانونية المرتبطة بالجرائم السيبرانية، ما يساهم في سد الفجوة التشريعية بين الأنظمة القانونية المختلفة وتسهيل عملية التحقيق والملاحقة عبر الحدود، وكذلك يساهم في حماية البنى الرقمية الحيوية وحماية حقوق الأفراد في الفضاء الإلكتروني.

ومن الأمثلة الواقعية على الجرائم السيبرانية العابرة للحدود التي تستدعي تطبيق تلك الأطر القانونية والتعاون الدولي، الهجمات السيبرانية المنظمة على أنظمة معلوماتية لمؤسسات ودول متعددة، والتي تستهدف سرقة البيانات الحساسة أو تعطيل الخدمات الحيوية، مسببة خسائر مالية وأمنية جسيمة. كما تظهر عمليات الاحتيال الإلكتروني المنظمة عبر الشبكات الرقمية، التي تستهدف الأفراد والمؤسسات في أكثر من دولة في وقت واحد، مستغلة الفجوات في التشريعات الوطنية وصعوبة تحديد هوية الجناة والملاحقة القضائية دون تعاون دولي فعال.

## **الفرع الثاني: أثر تقنيات الذكاء الاصطناعي، الروبوتات، الطائرات المسيّرة، والبلوكشين على ارتكاب الجرائم الدولية**

في ظل الثورة الرقمية والتحول التكنولوجي السريع، برزت مجموعة من التقنيات المتقدمة التي تعيد تعريف مفهوم الجريمة الدولية وطرائق ارتكابها، وتضع النظام القانوني الدولي الجنائي أمام تحديات مفاهيمية وتنظيمية لم تكن موجودة في الماضي. من أبرز هذه التقنيات الذكاء الاصطناعي (AI)، والروبوتات، والطائرات المسيّرة (Drones)، وتقنية البلوكشين، التي لم تعد أدوات تقنية فقط، بل أصبحت أحيانا وسائط تنفيذ تؤثر على الطريقة التي تقع بها الجرائم وعلى تحديد الفاعل والمساءلة القانونية.

**أولا، الذكاء الاصطناعي يمثل تقنية أصبحت قادرة على اتخاذ قرارات تلقائية وتنفيذ** عمليات معقدة دون تدخل بشري مباشر، وهو ما أثار جدالات قانونية حول مسؤولية الفعل الإجرامي وارتباطه بالإنسان. ففي حين أن القانون الجنائي التقليدي يفترض وجود إرادة بشرية ونية جنائية صريحة لقيام الجريمة، فإن تقنيات الذكاء الاصطناعي قد تؤدي أفعالا لها نتائج ضارة عبر خوارزميات معقدة يمكن أن تتجاوز سيطرة المبرمج أو المشغل، مما يثير تساؤلات حول كيفية تحميل الذكاء الاصطناعي أو من يقف وراءه المسؤولية القانونية إذا ما ارتكب انتهاكا لحقوق محمية أو أسهم في ارتكاب فعل يعد جريمة دولية هذه الإشكالية تتطلب من القانون الدولي الجنائي إعادة النظر في قواعد المسؤولية التقليدية والتميز بين الفاعل البشري والنظام الذكي.

**ثانيا، الروبوتات والطائرات المسيّرة) بما في ذلك الأنظمة ذاتية القيادة(، وخاصة في** السياقات العسكرية، تقدم مثلا صارخا على كيفية استخدام التكنولوجيا في ارتكاب أفعال قد ترقى إلى جرائم حرب أو جرائم ضد الإنسانية فالطائرات المسيّرة التي تعمل بالتحكم الذاتي أو بتوجيه من أنظمة مدعومة بالذكاء الاصطناعي تستطيع تنفيذ ضربات عبر الحدود مع قدرة أقل على التدخل البشري في لحظة اتخاذ القرار، ما يثير تساؤلات حول التمييز بين

الاستخدام المشروع وغير المشروع للأسلحة، ومسؤولية اتخاذ القرار في حالات الهجوم التي تؤدي إلى أضرار جسيمة في المدنيين أو ممتلكات غير عسكرية، فقد دعت منظمات دولية إلى وضع أطر تنظيمية دولية للحد من الاستخدام غير الخاضع للمساءلة لهذه التقنيات في سياق النزاعات المسلحة.

### **ثالثا، تقنية البلوكشين جعلت من الممكن تنفيذ معاملات مالية معقدة عبر شبكات**

لامركزية لا تعتمد على سلطة مركزية واحدة، مما يجعل تتبع الأموال غير المشروعة، وتمويل الإرهاب، وغسل الأموال عبر الحدود أكثر تعقيدا من ذي قبل هذه الخاصية تؤثر بشكل مباشر على إطار الجريمة الدولية المالي، حيث يمكن للفاعل أن يستغل هذه التقنية لتعزيز نشاطات غير قانونية بأقل إمكانية للمراقبة، مما يستلزم تطوير آليات قانونية دولية للتعامل مع الجرائم المالية الدولية وتحديد المصدر الحقيقي للأموال المتأتية من أفعال إجرامية.

وعلى صعيد الأمن السيبراني والجرائم الإلكترونية، تساهم تقنيات الذكاء الاصطناعي في زيادة قدرة المجرمين على تنفيذ هجمات معقدة مثل التزوير العميق أو الاحتيال الإلكتروني عبر تحليل كميات هائلة من البيانات لتوجيه الإغراءات أو الاستراتيجيات الخادعة، وهو ما يشكل تهديداً متزايداً للأمن القانوني والمؤسساتية على المستويين الوطني والدولي. كما أن تطور هذه الأنظمة قد يخلق مشكلات في تحديد المسؤولية القانونية لما يحدث عبر الفضاء السيبراني، حيث لا يكون الفاعل البشري حاضراً بشكل مباشر في التنفيذ.

مع كل هذه التطورات لا تزال القواعد التقليدية للركن المادي والمعنوي في الجرائم الدولية غير كافية لمعالجة هذا الواقع الجديد، لأن المفهوم التقليدي يفترض وجود فعل بشري ونية جنائية واضحة، بينما يمكن أن تنتج التقنيات الحديثة أفعالا ذات آثار جرمية دون وجود قصد بشري مباشر، ومن ثم فإن الفقه والقانون الدولي الجنائي مطالبان بتطوير أطر مفاهيمية وتنظيمية جديدة تأخذ في الحسبان طبيعة هذه التقنيات في تحديد معالم الجريمة، ومسؤولية من يقف وراءها من البشر أو المؤسسات، وكيفية تطبيق القانون على أفعال تكون الوسائط التقنية فيها وسيطا مركزيا.

يمكن القول إن التقنيات المتقدمة مثل الذكاء الاصطناعي، الروبوتات، الطائرات المسيرة، وتقنية البلوكشين لا تقتصر على كونها أدوات تنفيذ، بل تصبح عناصر فعالة في إعادة تشكيل مفهوم الجريمة الدولية وخصائصها. وهي بذلك تفرض على القانون الدولي الجنائي أن يعيد النظر في تعريفات الجرائم، في أركانها الأساسية، وفي استراتيجيات تحديد المسؤولية والمساءلة الجنائية الدولية لمواكبة هذا الواقع الجديد الذي قدمته الثورة الرقمية.

## المبحث الثاني: أركان الجريمة الدولية وتحديات اثباتها في ظل البيئة الرقمية

يطرح التحول الرقمي إشكاليات عميقة تمس البنية التقليدية للجريمة الدولية، ولا سيما ما يتعلق بركنيها المادي والمعنوي، إذ لم تعد الأفعال الإجرامية ترتكب بالوسائل المادية المباشرة وحدها، بل أصبحت تنفذ عبر أدوات تقنية معقدة ووسائل رقمية عابرة للحدود. وقد أدى هذا الواقع إلى إعادة طرح أسئلة جوهرية حول كيفية تحقق الفعل الإجرامي، وحدود نسبته إلى الفاعل، ومدى توافر القصد الجنائي في سياقات تعتمد على الذكاء الاصطناعي والهيكل التنظيمية الرقمية.

ومن ثم يهدف هذا المبحث إلى تحليل أثر التكنولوجيا على الركن المادي للجريمة الدولية (المطلب الأول)، واستجلاء التحديات التي تواجه إثبات الركن المعنوي وتحديد المسؤولية الجنائية في البيئة الرقمية المعاصرة. (المطلب الثاني).

### المطلب الأول: بطلان تطور الركن الشرعي وتوسع ماديات الجريمة الدولية

تقوم الجريمة الدولية في إطار القانون الدولي الجنائي على أركان أساسية تتمثل في الركن الشرعي، والركن المادي، والركن المعنوي، إلى جانب الركن الدولي الذي يميزها عن غيرها من الجرائم. ويُجسد الركن الشرعي مبدأ الشرعية الجنائية الدولية، من خلال حصر الجرائم التي تدخل ضمن اختصاص القضاء الجنائي الدولي، ولا سيما المحكمة الجنائية الدولية، في جرائم الإبادة الجماعية، والجرائم ضد الإنسانية، وجرائم الحرب، وجريمة العدوان.

أما الركن المادي فيتمثل في السلوك الإجرامي وما يترتب عليه من نتائج، في حين يقوم الركن المعنوي على توافر القصد الجنائي القائم على العلم والإرادة، بينما يرتبط الركن الدولي بطبيعة الجريمة من حيث مساسها بالمجتمع الدولي أو ارتكابها في إطار واسع النطاق أو منهجي.

غير أن التحولات التكنولوجية الحديثة أفرزت تحديات عميقة مست هذه الأركان، خاصة الركنين الشرعي والمادي، وهو ما يقتضي تحليل مظاهر القصور في الركن الشرعي الفرع الأول، وتبيان توسع الركن المادي بفعل الوسائل التكنولوجية (الفرع الثاني).

### الفرع الأول: قصور الركن الشرعي في استيعاب الجرائم الدولية الرقمية

يشهد الركن الشرعي للجريمة الدولية تحديات متزايدة في ظل التطور التكنولوجي، إذ أن النصوص التقليدية للقانون الدولي الجنائي، وعلى رأسها النظام الأساسي للمحكمة الجنائية الدولية، لم تتضمن تنظيمًا صريحًا للجرائم المرتكبة عبر الوسائل الرقمية أو باستخدام التقنيات الحديثة.

فرغم أن هذه النصوص جاءت شاملة لأخطر الجرائم التي تهم المجتمع الدولي، إلا أنها

صيغت في سياق تقليدي يفترض وجود أفعال مادية مباشرة، وهو ما يجعل من الصعب استيعاب بعض الأفعال المستحدثة، مثل الهجمات السيبرانية أو استخدام الذكاء الاصطناعي في تنفيذ الانتهاكات الجسيمة، ضمن الإطار القانوني القائم.

ويثير هذا الوضع إشكالية قانونية تتعلق بمدى إمكانية التوسع في تفسير النصوص الحالية لتشمل الأفعال الرقمية، أو ضرورة تدخل تشريعي دولي لتحديثها بما يتلاءم مع التحولات التكنولوجية، خاصة في ظل مبدأ الشرعية الذي يمنع القياس أو التوسع غير المشروع في التجريم.

كما أن غياب نصوص صريحة تجرم بعض الأفعال الرقمية كجرائم دولية مستقلة، يجعل من الصعب تكييفها قانونيًا، إلا في حدود إدراجها ضمن الجرائم التقليدية، وهو ما قد يؤدي إلى نوع من القصور في الحماية الجنائية الدولية، وي طرح تحديًا أمام فعالية القانون الدولي الجنائي في مواكبة الواقع الرقمي.

### **الفرع الثاني: توسع الركن المادي للجريمة الدولية بفعل الوسائل التكنولوجية**

يشهد الركن المادي للجريمة الدولية تحولًا واضحًا بفعل التطور التكنولوجي، الذي أفرز أدوات ووسائل تنفيذ غير تقليدية، بحيث لم تعد الأفعال الإجرامية محصورة في السلوك المادي المباشر، بل باتت ترتكب عبر الإنترنت والأنظمة الرقمية والبرمجيات المتقدمة، مما يسمح بارتكاب الجرائم عن بُعد ودون وجود مادي مباشر للفاعل.

### **أولاً: استخدام أدوات وتقنيات حديثة في ارتكاب جرائم الحرب والجرائم ضد الإنسانية**

يشكل استخدام الأدوات والتقنيات الحديثة في تنفيذ جرائم الحرب والجرائم ضد الإنسانية أحد التحولات الجوهرية التي فرضتها التكنولوجيا الرقمية على القانون الدولي الجنائي، إذ لم تعد الأعمال الإجرامية تقتصر على الوسائل التقليدية، بل باتت ترتكب عبر أسلحة متقدمة، أنظمة قتالية ذاتية التشغيل، وشبكات رقمية يمكن توظيفها لارتكاب انتهاكات جسيمة تخرق قواعد القانون الدولي الإنساني وتعرض المدنيين للخطر بطرق غير مسبوقة.

وفقًا للجنة الدولية للصليب الأحمر، فإن التطور في وسائل الحرب الحديثة، مثل الأسلحة ذاتية التشغيل والطائرات المسيّرة والعمليات السيبرانية، أثار "تحديات إنسانية وقانونية" في تطبيق قواعد القانون الدولي الإنساني التقليدية على هذه الوسائل بسبب خصائصها التقنية والنتائج الإنسانية المحتملة.

من أبرز الأمثلة المعاصرة على ذلك ما ورد في تقارير دولية متعددة حول استخدام الطائرات المسيّرة (الدرونز) في هجمات تستهدف المدنيين أو المنشآت المدنية في النزاعات المسلحة، حيث خلصت لجنة تحقيق مستقلة تابعة للأمم المتحدة إلى أن ضربات الطائرات المسيّرة الروسية على مناطق مدنية في أوكرانيا تعد جرائم حرب وجرائم ضد الإنسانية عندما تستخدم هذه الوسائل بشكل ممنهج لاستهداف المدنيين والبنية التحتية الحيوية بهدف إرهاب السكان أو تهجيرهم قسريًا.

كما يطرح في الممارسة الدولية الحديثة استخدام الذكاء الاصطناعي في تحديد

الأهداف العسكرية كقضية قانونية معقدة، إذ يشير تقرير وطبيعة التطبيق في بعض النزاعات إلى أن أنظمة الذكاء الاصطناعي تستعمل لتسريع عملية اختيار الأهداف وتوجيه الضربات، وهو ما أثار انتقادات قانونية لجهة احتمالية انتهاك مبادئ القانون الإنساني الدولي كالتمييز بين المدنيين والمقاتلين ومعايير التناسب، إذا لم يكن هناك إشراف بشري فعال على القرارات التي تتخذها هذه الأنظمة.

وتشكل هذه التطورات إشكالية قانونية مركزية، إذ أن القانون الدولي الجنائي التقليدي يربط قيام جرائم الحرب أو الجرائم ضد الإنسانية بفعل بشري مادي مباشر، بينما توظيف الوسائل التقنية الحديثة في السياقات العسكرية يجعل من الصعب أحيانا تحديد العلاقة السببية بين الفعل التكنولوجي والنوايا الإجرامية، مما يثير سؤالا أساسيا حول كيفية نسب المسؤولية الجنائية إلى الأفراد أو الجهات التي تتحكم في نظم متقدمة أو توظفها في عمليات قتالية.

من ناحية أخرى لا يقتصر تأثير التكنولوجيا على جانب التنفيذ فحسب، بل يشمل تطوير منظومات الإثبات والتحقيق في جرائم الحرب والجرائم ضد الإنسانية، حيث أصبحت الأدلة الرقمية – مثل صور الأقمار الصناعية، وتسجيلات الفيديو المنتشرة عبر الشبكات الاجتماعية، وبيانات الاتصالات – أدوات رئيسية لإثبات وقائع الانتهاكات ومساءلة مرتكبيها أمام المحاكم الجنائية الدولية والوطنية، مما يعكس تحولا في أدوات العمل القضائي وتحديات تتعلق بالتحقق من صحة الأدلة الرقمية وسلامتها القانونية.

وتكتسب هذه التحولات التقنية في ارتكاب جرائم الحرب والجرائم ضد الإنسانية أهمية قانونية مضاعفة عند مقارنة طبيعتها مع الإطار النصي الذي يحدده نظام روما الأساسي للمحكمة الجنائية الدولية، الذي يُعد المعيار القانوني الأسمى لمكافحة أخطر الجرائم الدولية. فالنظام يؤكد في المادة 5 على أن اختصاص المحكمة يشمل "أشد الجرائم التي تثير قلق المجتمع الدولي بأسره"، ومن بينها الجرائم ضد الإنسانية وجرائم الحرب كجزء من الآليات الدولية لمكافحة الانتهاكات الجسيمة لحقوق الإنسان والقانون الدولي الإنساني.

لذا فإن الربط بين ما يتيح النظام النصي من إطار للمساءلة وبين توظيف التكنولوجيا الحديثة في تنفيذ الأفعال الإجرامية يسلط الضوء على ضرورة تطوير فهم القانون الدولي الجنائي ليشمل طبيعة هذه الوسائط المتقدمة، وضمان عدم إفلات مرتكبي الجرائم التقنية من المساءلة بما يتوافق مع روح ومقاصد نظام روما الأساسي.

ومع توسع استخدام التكنولوجيا الرقمية في السياقات الاجتماعية والسياسية، لم تعد الوسائل التقنية تستخدم فقط كأدوات تنفيذ الأفعال الإجرامية، بل أصبحت أيضا منصات للخطاب والتحريض الذي يمكن أن يسهم في نشر الكراهية أو تمهيد الطريق لأفعال عنف وانتهاكات جسيمة، ما يستدعي فحفا قانونيا دقيقا لدور حملات المعلومات الرقمية والتحريض عبر الوسائط التقنية في تسهيل ارتكاب الجرائم الدولية والتحقيق في مدى تأثير هذا الخطاب على السلم والأمن الدوليين والنية الإجرامية.

## **ثانيا: دور حملات المعلومات الرقمية والتحريض عبر الوسائط التقنية في ارتكاب الجرائم**

في البيئة الرقمية المعاصرة لم يعد الفضاء السيبراني مجرد وسيلة لنشر المعلومات، بل

أصبح أداة تأثير مركبة يمكن توظيفها في إحداث تأثيرات قانونية واجتماعية خطيرة من خلال حملات التحريض والترهيب الرقمية.

إذ تنتشر عبر وسائل التواصل الاجتماعي والمنتديات الرقمية رسائل يمكن أن تساهم في تهيئة المناخ العقلي والاجتماعي الذي يسبق ارتكاب الجرائم الدولية، بما في ذلك جرائم الحرب والجرائم ضد الإنسانية، من خلال نشر محتوى يستهدف استقطاب العواطف واستغلال الانقسامات الاجتماعية والسياسية، ويرتبط في بعض الحالات بتحريض مباشر أو غير مباشر على العنف والكرهية.

كما تشير التحليلات القانونية إلى أن هذا النوع من المحتوى التحريضي يمكن أن يعزز إمكانيات ارتكاب الانتهاكات الجسيمة عبر الاستفادة من الانتشار الواسع للمعلومات الرقمية وسرعتها في الوصول إلى جماهير عريضة.

وتعرف الحملات الرقمية التحريضية بكونها نشر رسائل مضللة أو مؤطرة لغرض التأثير على سلوك الجمهور عبر استراتيجيات لغوية وتقنية تستهدف تضليل الرأي العام أو توجيهه نحو مسارات عنيفة أو تحريضية، مما يزيد من احتمالات تحول الخطاب إلى دافع للأفعال الإجرامية أو دعوات العنف.

هذا التحريض الرقمي لا يقتصر فقط على مضامين خاطئة، بل يسعى إلى استغلال التصورات الاجتماعية والقيم الجماعية في إشاعة العداة أو التحريض على التمييز والعنف، وهو ما يمكن أن يتضمّن دعوات صريحة أو ضمنية للعدوان.

وتشكل هذه الظاهرة إشكالية في القانون الدولي الجنائي لأنه لا يوجد حتى الآن نص دولي صادر عن الأمم المتحدة أو الصكوك الجنائية الدولية يجرم جميع أشكال التحريض عبر الوسائط الرقمية كجريمة دولية مستقلة، ويُعدّ التعامل معها غالباً في إطار المساهمة في ارتكاب الجرائم القائمة أو كدليل على إرادة الفاعل.

ومع ذلك نصوص القانون الدولي العام تبين أن التحريض المباشر على الإبادة الجماعية أو على التمييز والعنف يعد مخالفاً للالتزامات الدولية، ويستوجب مساءلة المسؤولين عن نشر هذا النوع من الخطاب فعلى سبيل المثال تناول الفقه القانوني الدولي "التحريض على الكراهية أو العنف" ضمن إطار خطاب التحريض الذي يهدد السلم والأمن الدوليين، واعتبر ذلك من صور المساهمة في الجرائم الدولية الكبرى.

على المستوى الوطني استجابت التشريعات المختلفة لهذه الظاهرة بإدراج عقوبات تحول دون التحريض عبر الوسائط التقنية، مثل تجريم نشر رسائل تحريضية أو عنصرية أو كراهية عبر الشبكات الرقمية، سواء كان ذلك عبر قوانين مكافحة جرائم تقنية المعلومات أو نصوص العقوبات الجنائية، بما في ذلك التجريم في حالات التحريض على العنف أو الكراهية أو الإبادة الجماعية عبر الإنترنت.

وأخيراً يرتبط التعامل القانوني مع التحريض الرقمي في سياق الجرائم الدولية بإشكالية أخرى تتعلق بجمع الأدلة الرقمية، وتحديد المصدر، وملاحقة المسؤولين عبر الحدود، ما يستدعي تكامل الأطر القانونية الدولية والوطنية لتوفير قواعد واضحة للإثبات، وتفعيل التعاون القضائي الدولي في ملاحقة الفاعلين الذين يستغلون الوسائط التقنية

للإسهام في وقوع انتهاكات جسيمة.

هذا التكامل يعد ضروريا لضمان عدم إفلات الأفراد الذين يستخدمون الفضاء الرقمي للتحريض على ارتكاب الجرائم الدولية من المساءلة، بما يتوافق مع مبادئ القانون الدولي الجنائي ومنع الإفلات من العقاب.

## **المطلب الثاني: تخطيط في إثبات الركن المعنوي والدولي في جرائم بمواصفات آلية**

يمثل إثبات أركان الجريمة الدولية، خاصة الركن المعنوي والركن الدولي، تحدياً جوهرياً في ظل البيئة الرقمية، حيث أدت التقنيات الحديثة، وعلى رأسها الذكاء الاصطناعي والأنظمة الرقمية المعقدة، إلى تعقيد عملية إسناد النية الإجرامية وتحديد الطابع الدولي للجريمة.

وعليه، يقتضي الأمر تحدي (الفرع الأول)، ثم التطرق إلى إشكالات إثبات الركن الدولي في الجرائم ذات الطابع الرقمي (الفرع الثاني).

### **الفرع الأول: الإشكالات القانونية في تحديد القصد الجنائي في بيئة الذكاء الاصطناعي**

يشكل الركن المعنوي أو القصد الجنائي (mens rea) حجر الزاوية في المسؤولية الجنائية التقليدية، لأنه يؤكد أن الفاعل ارتكب الفعل الإجرامي بعلم وإرادة، وهذه الآلية تستخدم في تمييز السلوك الجنائي عن السلوك غير الجنائي غير أن البيئة الرقمية الحديثة، وبالخصوص تقنية الذكاء الاصطناعي (AI)، تحدد هذا المفهوم الكلاسيكي بشكل جاد، إذ تطورت أنظمة وبرامج ذكية تتخذ قرارات وتنفيذ أفعال قد تحدث نتائج تعتبر جرائم بموجب القانون الدولي الجنائي، مما يثير تساؤلات قانونية عميقة حول مدى توافر القصد الجنائي التقليدي في مثل هذه الحالات.

### **أولاً: الإطار التقليدي للقصد الجنائي في القانون الدولي الجنائي**

أدى التطور المتسارع في تقنيات الذكاء الاصطناعي إلى إحداث تحولات عميقة في طبيعة الأفعال التي يمكن أن تشكل جرائم دولية، الأمر الذي انعكس بشكل مباشر على إمكانية تطبيق المفاهيم التقليدية للمسؤولية الجنائية، وعلى رأسها القصد الجنائي (Mens Rea) فبعد أن كان هذا الأخير يقوم على افتراض وجود إرادة بشرية واعية تتجه نحو تحقيق نتيجة إجرامية محددة، أصبح من الصعب الإبقاء على هذا التصور في بيئة رقمية تنسم بوجود أنظمة قادرة على اتخاذ قرارات شبه مستقلة دون تدخل مباشر من الإنسان..

تتميز أنظمة الذكاء الاصطناعي بقدرتها على التعلم الذاتي ومعالجة كميات هائلة من البيانات واتخاذ قرارات بناءً على خوارزميات معقدة، وهو ما يجعلها تختلف جذرياً عن الأدوات التقنية التقليدية. ففي حين يقوم الفعل الإجرامي في النموذج الكلاسيكي على تفاعل مباشر بين إرادة الإنسان والنتيجة الضارة، قد تنتج الأفعال في البيئة الرقمية عن عمليات تحليل آلي دون وجود قرار بشري مباشر في لحظة التنفيذ، مما يخلق فجوة واضحة بين السلوك المادي للجريمة والإرادة الإنسانية المفترضة وراءه

### **ثانياً: نماذج المسؤولية الجنائية في ظل الذكاء الاصطناعي**

يثير إدماج تقنيات الذكاء الاصطناعي في الأنشطة البشرية، خاصة في المجالات ذات الحساسية القانونية، إشكالا جوهريا يتعلق بكيفية إسناد المسؤولية الجنائية عن الأفعال الضارة الناتجة عنها. وفي هذا السياق، انقسم الفقه القانوني إلى اتجاهين رئيسيين يسعىان إلى تفسير موقع الذكاء الاصطناعي ضمن منظومة المسؤولية الجنائية الدولية.

هذا يرى الاتجاه الأول أن المسؤولية الجنائية يجب أن تظل مرتبطة بالعنصر البشري، باعتبار أن الذكاء الاصطناعي لا يعدو أن يكون أداة تقنية تستخدم من قبل الإنسان. ووفقا لهذا التصور، فإن المبرمج أو المصمم أو المستخدم أو الجهة التي تقرر تشغيل النظام، يظل هو المسؤول عن النتائج الضارة التي قد تترتب عن استخدام هذه التقنية، على أساس أنه صاحب القرار في تصميمها أو توجيهها أو توظيفها. ويستند هذا الاتجاه إلى القواعد التقليدية للمسؤولية الجنائية التي تربط بين الفعل والنية والنتيجة، وتفترض وجود إرادة بشرية يمكن إسناد القصد الجنائي إليها.

في المقابل، يذهب اتجاه فقهي حديث إلى ضرورة إعادة النظر في نماذج الإسناد التقليدية، في ضوء ما تتمتع به بعض أنظمة الذكاء الاصطناعي من قدرة على اتخاذ قرارات شبه مستقلة. ويدعو هذا الاتجاه إلى بحث إمكانية إضفاء نوع من الصفة القانونية الخاصة على هذه الأنظمة، بما يسمح بمساءلتها عن الأفعال التي تصدر عنها.

غير أن هذا الطرح لا يزال محل جدل واسع، في ظل غياب نصوص قانونية صريحة تمنح الذكاء الاصطناعي شخصية قانونية مستقلة، فضلا عن تعارضه مع الأسس الأخلاقية والقانونية التي يقوم عليها القانون الجنائي، والتي تفترض وجود وعي وإدراك لدى الفاعل.

### **ثالثا: الإشكالات الأساسية في تحديد القصد الجنائي في بيئة الذكاء الاصطناعي**

لا يقتصر الإشكال في هذا المجال على تحديد من يتحمل المسؤولية، بل يمتد ليشمل صعوبة إثبات القصد الجنائي ذاته، وهو ما يُعد عنصرا جوهريا في قيام المسؤولية الجنائية الدولية.

تتمثل أولى هذه الإشكالات في غياب الإرادة الذاتية والوعي القانوني لدى أنظمة الذكاء الاصطناعي، إذ إن هذه الأنظمة، رغم قدرتها على التعلم والتكيف، لا تمتلك إدراكا حقيقيا أو نية قانونية يمكن نسبتها إليها. وهو ما يجعل من الصعب تطبيق المفهوم التقليدي للقصد الجنائي الذي يفترض وجود إرادة واعية تتجه نحو تحقيق نتيجة إجرامية.

كما تتعدد المسألة بفعل تعدد الأطراف المتدخلة في تصميم وتطوير وتشغيل هذه الأنظمة، مما يثير صعوبة في تحديد الجهة التي يمكن إسناد النية الإجرامية إليها، خاصة في الحالات التي تنتج فيها الأفعال الضارة عن خلل خوارزمي أو نتائج غير متوقعة. وفي هذا السياق، برز مفهوم "فجوة المسؤولية" (Responsibility Gap)، الذي يعكس حالة عدم القدرة على تحديد فاعل بشري واضح يمكن تحميله المسؤولية الجنائية بشكل مباشر.

ويزداد هذا التعقيد في ظل اعتماد بعض الأنظمة على خوارزميات التعلم الذاتي، التي قد تؤدي إلى نتائج لا يمكن التنبؤ بها مسبقا، مما يضعف العلاقة بين الفعل المادي والإرادة

البشرية، ويجعل من إثبات القصد الجنائي عملية أكثر تعقيدًا من الناحية العملية.

ورغم هذه التحديات، يظل القصد الجنائي عنصرًا أساسيًا لا يمكن الاستغناء عنه في إطار المسؤولية الجنائية الدولية، وهو ما أكده نظام روما الأساسي للمحكمة الجنائية الدولية، التي تشترط توافر النية والمعرفة لقيام المسؤولية. غير أن تطبيق هذا المبدأ في بيئة الذكاء الاصطناعي يظل مرهونًا بإمكانية ربط الفعل الضار بإرادة بشرية يمكن إثباتها، الأمر الذي يستدعي تطوير آليات قانونية جديدة تضمن التوفيق بين متطلبات العدالة الجنائية والتطور التكنولوجي.

وتؤكد التطبيقات العملية في القانون الدولي الجنائي أن المسؤولية لا تبني على النتائج التقنية في حد ذاتها، بل على مدى ارتباطها بسلوك بشري وإع. وهو ما يبرز بوضوح في عمل المحكمة الجنائية الدولية، التي تعتمد في تقييمها على إثبات توافر النية لدى الأشخاص الطبيعيين المسؤولين عن اتخاذ القرارات التي أدت إلى ارتكاب الانتهاكات، وليس على مجرد وقوع النتيجة. وعليه، فإن التحدي الحقيقي لا يكمن فقط في تطور الوسائل التقنية، بل في قدرة القانون الدولي الجنائي على استيعاب هذه التحولات، من خلال تطوير قواعده بما يضمن عدم الإفلات من المسؤولية، مع الحفاظ في الوقت ذاته على المبادئ الأساسية التي يقوم عليها، وعلى رأسها مبدأ شخصية المسؤولية الجنائية

### **الفرع الثاني: القصور في إثبات الركن الدولي في الجرائم الرقمية**

إلى جانب الصعوبات المرتبطة بإثبات الركن المعنوي، تبرز إشكالات لا تقل أهمية تتعلق بإثبات الركن الدولي للجريمة، خاصة في ظل الطبيعة الخاصة للجرائم المرتكبة في البيئة الرقمية، والتي تتسم باللامركزية وتجاوز الحدود الجغرافية التقليدية. إذ لم يعد تحديد الطابع الدولي للجريمة أمرًا سهلًا في ظل انتشار الفضاء السيبراني واعتماده على شبكات عابرة للدول.

### **أولاً: الركن الدولي من زاوية الإثبات**

لا يكفي لقيام الجريمة الدولية مجرد إثبات وقوع فعل مجرم، بل يجب كذلك إثبات أن هذا الفعل يندرج ضمن الجرائم التي تمس المجتمع الدولي بأسره. ويتحقق ذلك عندما يكون الفعل ذا خطورة جسيمة، أو يُرتكب في إطار واسع النطاق أو منهجي، أو يكون من ضمن الجرائم التي يختص بها القضاء الجنائي الدولي.

وقد حصر نظام روما الأساسي اختصاص المحكمة الجنائية الدولية في أربع جرائم رئيسية هي: الإبادة الجماعية، الجرائم ضد الإنسانية، جرائم الحرب، وجريمة العدوان، وهو ما يجعل إثبات الطابع الدولي للجريمة أمرًا دقيقًا ومقيدًا بنطاق قانوني محدد وصارم.

### **ثانياً: صعوبة تكييف الجرائم الرقمية كجرائم دولية**

تطرح في الواقع العملي صعوبة واضحة في التمييز بين الجرائم الرقمية العادية مثل الاختراقات والاحتياال الإلكتروني، وبين الجرائم الدولية بالمعنى القانوني الدقيق. فليس كل هجوم سيبراني يعد جريمة دولية، بل يجب أن يرتبط بسياق خاص، كأن يكون جزءًا من نزاع مسلح، أو موجّهًا ضد المدنيين، أو يدخل ضمن هجوم واسع النطاق أو منهجي.

وهذا ما يجعل عملية التكييف القانوني لهذه الأفعال أمام القضاء الدولي عملية معقدة، لأنها تتطلب إثبات عناصر إضافية تتجاوز مجرد وقوع الفعل الإلكتروني.

### ثالثاً: صعوبة إثبات الطابع الدولي للجريمة الرقمية

تزداد الإشكالية تعقيداً عند محاولة إثبات أن الجريمة الرقمية ترقى إلى مستوى "الجريمة الدولية"، وذلك بسبب غياب حدود واضحة في الفضاء الرقمي، والطبيعة العابرة للحدود للأفعال الإلكترونية، إضافة إلى تداخل الاختصاص بين القضاء الوطني والقضاء الدولي.

فقد ترتكب الجريمة عبر عدة دول في وقت واحد، أو تدار من خارج الدولة التي وقع فيها الضرر، مما يجعل تحديد طبيعتها القانونية واختصاصها القضائي أمراً صعباً، ويثير إشكالات حول ما إذا كانت تدخل ضمن نطاق الجرائم الدولية أو تبقى مجرد جرائم وطنية عابرة للحدود.

### رابعاً: حدود اختصاص المحكمة الجنائية الدولية

تتجلى أهم إشكالية في أن المحكمة الجنائية الدولية لا تختص إلا بجرائم محددة على سبيل الحصر، وهي: الإبادة الجماعية، الجرائم ضد الإنسانية، جرائم الحرب، وجريمة العدوان. وبالتالي، حتى في حال خطورة الفعل الرقمي، فإنه لا يُعد جريمة دولية إلا إذا أمكن إدخاله ضمن إحدى هذه الفئات.

وعليه، فإن عبء الإثبات لا يقتصر فقط على إثبات وقوع الفعل، بل يمتد إلى إثبات انطباق الوصف القانوني الدولي عليه، وهو ما لا يتحقق في العديد من الجرائم الرقمية الحديثة، مما يحد من فعالية التكييف الجنائي الدولي في هذا المجال.

## خلاصة الفصل

يشير التحول التكنولوجي المتسارع في تكنولوجيات الاتصال والمعلومات إلى إعادة تشكيل جذري للمشهد الجنائي الدولي، إذ لم يعد تأثير التكنولوجيا مقتصرًا على الجوانب الاقتصادية والاجتماعية فحسب، بل امتد ليطل الأسس الفقهية والقانونية لمفهوم الجريمة الدولية.

ففي عصر الرقمنة تبرز أنماط إجرامية جديدة تعتمد على الوسائط الرقمية والتقنيات المتقدمة، فتتجاوز الجرائم شكلها التقليدي القائم على القوة المادية والسيطرة الإقليمية، لتشمل فعلاً عبر الفضاء السيبراني وبتوظيف أنظمة الذكاء الاصطناعي والطائرات المسيّرة والأنظمة الرقمية المؤتمتة، مما يجعل الحدود الجغرافية أقل قدرة على مواجهة هذه الظواهر.

بهذه التحولات تنشأ تحديات قانونية جوهرية تمس أركان الجريمة الدولية، وتعيد طرح إشكالات حول تحديد الفاعل، وإثبات القصد الجنائي، ومسؤولية القيادة في بيئات رقمية معقدة، بما يستلزم تطوير آليات القانون الدولي الجنائي وأطره التقليدية لمواكبة متطلبات العصر الرقمي وآثاره على الأمن الدولي والنظام القانوني العالمي

**الفصل الثاني:**  
**محاولة مواكبة القاعدة القانونية الدولية للتجريم  
والمسؤولية للتطور التكنولوجي**

في سياق التحولات العميقة التي فرضها التطور التكنولوجي المتسارع على بنية الجريمة الدولية وأنماط ارتكابها، حيث لم تعد الأفعال الإجرامية الجسيمة تقتصر على الوسائل التقليدية، بل امتدت إلى الفضاء الرقمي وتداخلت مع تقنيات حديثة كالذكاء الاصطناعي، والهجمات السيبرانية، والطائرات المسيّرة، والأنظمة المؤتمتة. وقد أفرز هذا التحول تحديات غير مسبوقة أمام قواعد القانون الدولي الجنائي، سواء على مستوى التكييف القانوني للأفعال أو من حيث آليات الملاحقة والإثبات وإسناد المسؤولية الجنائية الدولية.

ومن هذا المنطلق برزت الحاجة إلى تطوير الإطار القانوني الدولي بما يواكب هذه التحولات، من خلال إعادة قراءة النصوص المؤسسة، وعلى رأسها نظام روما الأساسي، وقياس مدى قدرته على استيعاب الجرائم ذات البعد التكنولوجي، فضلًا عن رصد جهود الأمم المتحدة والهيئات الدولية الأمنية في توصيف هذه الأفعال ومواجهتها ضمن منظومة السلم والأمن الدوليين كما أضحى من الضروري بحث إشكالات المسؤولية الجنائية الدولية في البيئة الرقمية، خاصة ما يتعلق بطبيعة الأدلة الرقمية، ومعايير قبولها أمام القضاء الدولي، فضلًا عن التحديات المرتبطة بإثبات القصد الجنائي وتحديد نطاق السيطرة الفعلية في الجرائم المرتكبة عبر أنظمة ذكية أو مؤتمتة.

وعليه يسعى هذا الفصل إلى تأصيل الإطار القانوني الدولي الناظم لمواجهة التحولات التكنولوجية في الجريمة الدولية، من خلال تحليل تطور التشريعات الجنائية الدولية، وبيان حدودها الراهنة، واستجلاء أدوار الفاعلين الدوليين في مكافحتها (المبحث الأول)، ووصولًا إلى تفكيك إشكالات المسؤولية الجنائية الدولية في البيئة الرقمية الحديثة. (المبحث الثاني).

## **المبحث الأول: تطور تشريعي ومؤسسي دولي متأخر عن تنامي أنماط الجريمة الدولية في البيئة التكنولوجية**

أدى التطور التكنولوجي إلى بروز أنماط جديدة من الجرائم ذات البعد الدولي المرتبطة بالفضاء الرقمي والتقنيات الحديثة، وقد طرح ذلك تحديات أمام قواعد القانون الدولي الجنائي التقليدية ومدى قدرتها على مواكبة هذه التحولات، الأمر الذي استدعى تعزيز الجهود الدولية لتطوير التشريعات وآليات التعاون لمواجهة الجرائم الرقمية.

وعلى هذا الأساس سنتعرض في مبحثنا هذا لتوضيح الإطار القانوني الدولي الجنائي في ظل التكنولوجيات الحديثة (المطلب الأول)، ثم نأتي لبيان الجهود الأممية والهيئات الدولية في مواجهة الجرائم الدولية ذات البعد التكنولوجي (المطلب الثاني).

### **المطلب الأول: تطور تشريعي دولي ثقيل في مواجهة الجريمة الرقمية**

أفرز التطور التكنولوجي تحديات جديدة أمام القانون الدولي الجنائي، لا سيما فيما

يتعلق بارتكاب الجرائم الدولية باستخدام الوسائل الرقمية والتقنيات الحديثة، وقد استدعى ذلك دراسة كيفية تفاعل قواعد القانون الدولي الجنائي الخاصة بالجرائم ضد الإنسانية وجرائم الحرب والإبادة والعدوان مع هذه الوسائل (الفرع الأول)، مع تسليط الضوء على حدود التشريعات الدولية الحالية، بما فيها نظام روما الأساسي، في مواجهة الجرائم الرقمية المعقدة كالذكاء الاصطناعي والطائرات المسيّرة والهجمات السيبرانية الموجهة (الفرع الثاني)، ويهدف هذا المطلب إلى استكشاف تطور هذه القواعد القانونية وحدود فعاليتها أمام التحولات التكنولوجية المعاصرة.

## **الفرع الأول: تطور قواعد القانون الدولي الجنائي لملاحقة الجرائم الدولية ذات البعد الرقمي**

يثير تطور الوسائل التكنولوجية الحديثة إشكالات قانونية جديدة أمام قواعد القانون الدولي الجنائي، خاصة فيما يتعلق بمدى قدرتها على استيعاب الجرائم الدولية المرتكبة عبر الوسائط الرقمية. ومن ثم يقتضي الأمر بحث تطور هذه القواعد وكيفية تفاعلها مع الأشكال المستحدثة للجريمة ذات البعد التكنولوجي.

## **أولاً: تفاعل قواعد الجرائم الدولية التقليدية مع الوسائل التكنولوجية الحديثة**

تطور القانون الدولي الجنائي تاريخياً لمواجهة أخطر الجرائم التي تهدد المجتمع الدولي بأسره، وفي مقدمتها جرائم الإبادة الجماعية والجرائم ضد الإنسانية وجرائم الحرب وجريمة العدوان، وهي الجرائم التي أقرها النظام الأساسي للمحكمة الجنائية الدولية باعتبارها تمثل أخطر الانتهاكات للقيم الإنسانية الأساسية.

وقد صيغت هذه القواعد في الأصل لمواجهة الجرائم المرتكبة بوسائل تقليدية في سياق النزاعات المسلحة أو السياسات القمعية للدول، غير أن التطور التكنولوجي المتسارع أدى إلى ظهور وسائل جديدة يمكن من خلالها ارتكاب هذه الجرائم أو تسهيل تنفيذها.

فمع اتساع استخدام الفضاء الرقمي والتقنيات المتقدمة، أصبح من الممكن تنفيذ أفعال قد تندرج ضمن الجرائم الدولية باستخدام أدوات تكنولوجية حديثة، مثل الهجمات السيبرانية والبرمجيات الخبيثة وأنظمة المراقبة الرقمية والطائرات المسيّرة، وقد أتاح هذا التطور للجهات الفاعلة، سواء كانت دولا أو جماعات منظمة أو حتى أفراداً، القدرة على إحداث أضرار جسيمة بالبنية التحتية الحيوية أو استهداف السكان المدنيين دون اللجوء إلى الوسائل العسكرية التقليدية فالعمليات السيبرانية قد تؤدي إلى تعطيل شبكات الكهرباء أو أنظمة الاتصالات أو الخدمات الصحية، وهو ما قد يترتب عليه آثار خطيرة تمس حياة المدنيين وأمنهم.

وفي هذا السياق برزت تساؤلات فقهية مهمة حول مدى إمكانية تكييف هذه الأفعال ضمن إطار الجرائم الدولية المعروفة فقد يرى بعض الفقه أن الهجمات السيبرانية التي تؤدي

إلى أضرار واسعة بالبنية التحتية أو خسائر بشرية قد ترقى إلى مستوى جرائم الحرب إذا ارتكبت أثناء نزاع مسلح واستهدفت أعيانا مدنية محمية بموجب القانون الدولي الإنساني، كما يمكن أن تدخل بعض الأفعال المرتكبة عبر الوسائل الرقمية ضمن الجرائم ضد الإنسانية إذا ارتبطت بهجوم واسع النطاق أو منهجي موجه ضد السكان المدنيين.

كما امتد تأثير الوسائل التقنية الحديثة إلى أساليب إدارة العمليات العسكرية، حيث أصبحت العديد من الدول تعتمد على الطائرات المسييرة والأنظمة الذكية في تنفيذ العمليات القتالية وقد أدى ذلك إلى إثارة نقاشات قانونية حول مدى توافق هذه الوسائل مع المبادئ الأساسية للقانون الدولي الإنساني، وعلى رأسها مبدأ التمييز بين الأهداف المدنية والعسكرية ومبدأ التناسب في استخدام القوة.

وعلى الرغم من أن الاتفاقيات الدولية، مثل اتفاقيات جنيف لعام 1949 والبروتوكولات الإضافية لعام 1977، لم تتناول صراحة الوسائل الرقمية الحديثة، فإن العديد من الفقهاء يرون أن المبادئ العامة للقانون الدولي الإنساني تظل قابلة للتطبيق على هذه الوسائل الجديدة.

ومن ثم يمكن القول إن التطور التكنولوجي لم يؤد إلى إلغاء القواعد التقليدية للقانون الدولي الجنائي، بل دفع نحو إعادة تفسيرها وتكييفها بما يسمح بتطبيقها على الجرائم المرتكبة باستخدام الوسائل الرقمية فالعبرة في تحديد الجريمة الدولية لا تتعلق بوسيلة ارتكابها بقدر ما تتعلق بطبيعة الفعل ونتائجه وآثاره على السلم والأمن الدوليين.

## **ثانياً: الاجتهادات الفقهية والجهود الدولية لتكييف الجرائم الرقمية في إطار القانون الدولي الجنائي**

مع تزايد التحديات التي فرضتها التكنولوجيا الحديثة، برزت جهود فقهية ومؤسسية متعددة تهدف إلى تطوير الفهم القانوني لكيفية تطبيق قواعد القانون الدولي الجنائي على الجرائم ذات البعد الرقمي، فقد أدرك المجتمع الدولي أن الفضاء السيبراني أصبح مجالاً جديداً للصراع الدولي، إلى جانب المجالات التقليدية البرية والبحرية والجوية والفضاء الخارجي، الأمر الذي يستوجب البحث عن قواعد قانونية تنظم استخدام هذا المجال وتحدد المسؤولية عن الأفعال المرتكبة فيه.

ومن أبرز المبادرات القانونية في هذا المجال ما يُعرف بـ دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية، الذي أعده مجموعة من الخبراء القانونيين الدوليين بهدف تفسير كيفية تطبيق قواعد القانون الدولي، بما في ذلك قواعد استخدام القوة والقانون الدولي الإنساني، على العمليات السيبرانية، ورغم أن هذا الدليل لا يتمتع بصفة إلزامية، فإنه يمثل محاولة علمية مهمة لتوضيح الإطار القانوني الذي يمكن من خلاله تقييم الهجمات السيبرانية وتحديد مسؤولية الدول عنها.

كما ظهرت اتجاهات فقهية ترى أن بعض العمليات السيبرانية قد تصل إلى مستوى استخدام القوة في العلاقات الدولية إذا كانت آثارها تماثل آثار الهجمات العسكرية التقليدية، مثل تدمير البنية التحتية الحيوية أو إحداث خسائر بشرية كبيرة، وفي هذه الحالة يمكن اعتبار هذه العمليات خاضعة للقواعد المنظمة لاستخدام القوة المنصوص عليها في ميثاق

الأمم المتحدة، كما قد تدرج ضمن الجرائم الدولية إذا توافرت أركانها القانونية.

إلى جانب ذلك يثير استخدام التقنيات المتقدمة مثل الذكاء الاصطناعي والأنظمة القتالية المستقلة إشكاليات قانونية معقدة تتعلق بتحديد المسؤولية الجنائية الدولية فهذه الأنظمة قد تعمل بدرجة من الاستقلالية تجعل من الصعب تحديد الشخص المسؤول عن الأفعال التي ترتكبها، خاصة عندما تعتمد على خوارزميات معقدة أو أنظمة تعلم آلي.

وعلى الرغم من هذه الجهود الفقهية والمؤسسية، فإن الإطار القانوني الدولي لا يزال يواجه صعوبات كبيرة في مواكبة التطورات التكنولوجية المتسارعة، فالقانون الدولي الجنائي ما زال يعتمد في معظمه على نصوص وضعت قبل ظهور العديد من التقنيات الحديثة، الأمر الذي يفرض على المجتمع الدولي العمل على تطوير هذه القواعد أو تبني اتفاقيات جديدة قادرة على تنظيم الجرائم الرقمية ذات الطابع الدولي ومواجهتها بفعالية أكبر.

## الفرع الثاني: حدود التشريعات الدولية الحالية أمام الجرائم الدولية الرقمية

يمثل التطور التكنولوجي المتسارع أحد أهم التحديات التي تواجه منظومة القانون الدولي الجنائي المعاصر، إذ إن العديد من القواعد القانونية الدولية التي تنظم الجرائم الدولية قد وضعت في سياق تاريخي سابق لظهور التقنيات الرقمية المتقدمة مثل الذكاء الاصطناعي والعمليات السيبرانية والطائرات المسيّرة.

وبالرغم من أن هذه القواعد تهدف إلى تجريم أخطر الأفعال التي تهدد السلم والأمن الدوليين، إلا أن طبيعة الجرائم الحديثة المرتبطة بالفضاء الرقمي تطرح إشكاليات قانونية معقدة تتعلق بمدى قدرة هذه القواعد على استيعاب هذه التحولات.

وتبرز هذه الإشكالية بشكل واضح في إطار النظام الأساسي للمحكمة الجنائية الدولية الذي لم يتناول بشكل صريح الجرائم الرقمية أو الوسائل التكنولوجية الحديثة التي يمكن أن تستخدم في ارتكاب الجرائم الدولية.

## أولاً: قصور نظام روما الأساسي في مواجهة الجرائم الدولية ذات البعد التكنولوجي

اعتمد المجتمع الدولي سنة 1998 نظام روما الأساسي للمحكمة الجنائية الدولية باعتباره الإطار القانوني الدولي الذي يحدد الجرائم الدولية الأساسية وهي جريمة الإبادة الجماعية والجرائم ضد الإنسانية وجرائم الحرب وجريمة العدوان، غير أن هذا النظام صيغ في فترة لم تكن فيها التكنولوجيا الرقمية قد بلغت المستوى الحالي من التطور، الأمر الذي جعله لا يتضمن أحكاماً واضحة تتعلق بالجرائم المرتكبة عبر الفضاء السيبراني أو باستخدام الأنظمة الذكية والوسائل التكنولوجية الحديثة.

ومن أبرز مظاهر هذا القصور أن نظام روما يركز في تعريفاته للجرائم الدولية على الأفعال المادية التقليدية مثل القتل والتعذيب والتجهير والتدمير المادي للأعيان المدنية، دون أن يضع إطاراً قانونياً واضحاً للأفعال التي قد تتحقق من خلال الوسائل الرقمية. فعلى سبيل

المثال، يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل شبكات الطاقة أو الاتصالات أو المستشفيات، وهو ما قد يترتب عليه أضرار جسيمة تمس حياة المدنيين، ومع ذلك فإن تكييف هذه الأفعال كجرائم حرب أو جرائم ضد الإنسانية يظل محل نقاش قانوني بسبب غياب نصوص صريحة تنظم هذا النوع من الجرائم، كما أن الفضاء السيبراني يتميز بخصائص فريدة، مثل صعوبة تحديد مصدر الهجوم أو الجهة المسؤولة عنه، وهو ما يعرقل إثبات المسؤولية الجنائية الدولية.

كما يثير استخدام الذكاء الاصطناعي والأنظمة القتالية المستقلة إشكاليات قانونية إضافية، خاصة فيما يتعلق بتحديد المسؤولية الجنائية عن الأفعال التي قد ترتكبها هذه الأنظمة. فالتطور المتسارع للتقنيات العسكرية القائمة على الذكاء الاصطناعي جعل من الممكن تنفيذ عمليات قتالية تعتمد بدرجة كبيرة على الخوارزميات والأنظمة الآلية، الأمر الذي يطرح تساؤلات حول من يتحمل المسؤولية القانونية عن نتائج هذه العمليات: هل هو المبرمج، أم القائد العسكري، أم الدولة التي تستخدم هذه الأنظمة؟ وقد دفعت هذه الإشكاليات العديد من الخبراء الدوليين إلى الدعوة إلى وضع قواعد قانونية جديدة لتنظيم استخدام هذه التكنولوجيا في النزاعات المسلحة.

إلى جانب ذلك يشكل استخدام الطائرات المسيّرة في النزاعات المسلحة تحدياً قانونياً آخر، إذ أصبحت هذه الوسائل تمثل أداة رئيسية في العمليات العسكرية الحديثة، لما توفره من قدرة على تنفيذ ضربات دقيقة دون تعريض القوات العسكرية للخطر.

غير أن استخدامها يثير تساؤلات حول مدى احترامها للمبادئ الأساسية للقانون الدولي الإنساني، وخاصة مبدأ التمييز بين الأهداف العسكرية والمدنية ومبدأ التناسب في استخدام القوة. كما أن الاعتماد المتزايد على هذه الوسائل قد يؤدي إلى توسيع نطاق العمليات العسكرية دون وجود ضوابط قانونية واضحة تحدد مسؤولية مرتكبي الانتهاكات المرتبطة بها.

ومن ثم يتضح أن النظام القانوني الدولي الحالي لا يزال يعاني من فجوة تشريعية واضحة فيما يتعلق بتنظيم الجرائم الدولية المرتبطة بالتكنولوجيا الحديثة، وهو ما يدفع العديد من الفقهاء إلى المطالبة بتطوير قواعد القانون الدولي الجنائي بما يتلاءم مع طبيعة الحروب الحديثة والجرائم الرقمية.

## **ثانياً: التطبيقات العملية للتكنولوجيا العسكرية الحديثة في النزاعات الدولية المعاصرة**

تكشف النزاعات الدولية المعاصرة بوضوح عن التحولات العميقة التي طرأت على طبيعة الحروب، حيث أصبحت التكنولوجيا الرقمية عنصراً أساسياً في إدارة العمليات العسكرية وتنفيذ الهجمات ويبرز هذا التحول بشكل واضح في عدد من النزاعات الحديثة، من أبرزها الحرب الروسية الأوكرانية والعمليات العسكرية في قطاع غزة.

ففي الحرب الروسية الأوكرانية لعبت العمليات السيبرانية دوراً مهماً في سياق الصراع، حيث شهدت أوكرانيا هجمات سيبرانية واسعة استهدفت المؤسسات الحكومية والبنية التحتية الرقمية، في محاولة لإضعاف قدرات الدولة وإحداث اضطراب في أنظمتها الحيوية. فقد تعرضت عدة مؤسسات حكومية أوكرانية لاختراقات إلكترونية متزامنة

استهدفت مواقع وزارات ومؤسسات حساسة، وهو ما اعتبره العديد من الباحثين جزءاً من استراتيجية عسكرية تهدف إلى إضعاف الدولة المستهدفة قبل أو أثناء العمليات العسكرية التقليدية.

كما شهدت هذه الحرب استخداماً مكثفاً للطائرات المسيّرة في تنفيذ الهجمات العسكرية، حيث استخدمت هذه الوسائل لاستهداف منشآت عسكرية ومدنية على حد سواء، الأمر الذي أثار نقاشات قانونية حول مدى توافق هذه العمليات مع قواعد القانون الدولي الإنساني.

وقد خلصت تقارير أممية إلى أن بعض الهجمات التي نفذت بواسطة الطائرات المسيّرة ضد المدنيين في أوكرانيا يمكن أن ترقى إلى مستوى جرائم حرب أو جرائم ضد الإنسانية إذا ثبت أنها استهدفت السكان المدنيين بشكل منهجي.

أما في قطاع غزة فقد تجلّى الاعتماد المتزايد على التكنولوجيا العسكرية الحديثة بصورة واضحة في العمليات العسكرية التي نفذتها قوات الاحتلال الإسرائيلي، حيث تم توظيف منظومات متطورة تعتمد على الطائرات المسيّرة وأنظمة الذكاء الاصطناعي وتحليل البيانات الضخمة في عمليات المراقبة والاستهداف العسكري.

وتعمل هذه الأنظمة على جمع كميات هائلة من المعلومات الاستخباراتية وتحليلها عبر خوارزميات رقمية بهدف تحديد الأهداف المحتملة، الأمر الذي يسمح بتنفيذ عدد كبير من الضربات العسكرية في وقت قصير.

وتشير تقارير إعلامية وبحثية إلى أن بعض الأنظمة القائمة على الذكاء الاصطناعي استخدمت لإنتاج قوائم أهداف عسكرية بسرعة كبيرة، وهو ما مكن القوات العسكرية من تنفيذ مئات الضربات في فترات زمنية متقاربة اعتماداً على تحليل البيانات الرقمية.

ويثير هذا الاستخدام المكثف للتكنولوجيا العسكرية إشكالات قانونية جديدة في إطار القانون الدولي الإنساني، خاصة فيما يتعلق بمدى احترام المبادئ الأساسية التي تحكم سير العمليات العسكرية، وعلى رأسها مبدأ التمييز بين المدنيين والمقاتلين، ومبدأ التناسب في استخدام القوة، ومبدأ الاحتياطات الواجب اتخاذها أثناء الهجوم.

فالتكنولوجيا العسكرية الحديثة، رغم ما توفره من إمكانيات تقنية متقدمة، قد تؤدي في بعض الحالات إلى الاعتماد المفرط على الأنظمة الآلية في تحديد الأهداف، وهو ما يثير تساؤلات حول مدى دقة هذه الأنظمة وقدرتها على التمييز بين الأهداف العسكرية المشروعة والأعيان المدنية، خصوصاً في البيئات الحضرية المكتظة بالسكان مثل قطاع غزة.

كما يثير توظيف أنظمة الذكاء الاصطناعي في تحليل المعلومات الاستخباراتية وتحديد الأهداف إشكالية قانونية أخرى تتعلق بمسألة المسؤولية الجنائية الدولية، إذ قد يكون من الصعب تحديد الجهة المسؤولة عن الخطأ في حال استند القرار العسكري إلى توصيات صادرة عن خوارزميات أو أنظمة تحليل بيانات آلية، ففي مثل هذه الحالات يبرز التساؤل حول ما إذا كانت المسؤولية تقع على عاتق القادة العسكريين الذين يعتمدون على هذه الأنظمة، أم على المبرمجين الذين طوروا الخوارزميات، أم على الدولة التي قامت بتشغيل هذه التكنولوجيا ضمن عملياتها العسكرية.

وقد دفع هذا الواقع العديد من المنظمات الدولية والخبراء القانونيين إلى المطالبة بوضع قواعد دولية واضحة لتنظيم استخدام الأنظمة القتالية المعتمدة على الذكاء الاصطناعي، لما قد تشكله من مخاطر على حماية المدنيين أثناء النزاعات المسلحة.

ومن ناحية أخرى فإن الطبيعة الرقمية لهذه التقنيات قد تسهم في تسريع وتيرة العمليات العسكرية بشكل غير مسبوق، حيث تسمح الأنظمة القائمة على الذكاء الاصطناعي بتوليد الأهداف وتحليلها بسرعة كبيرة مقارنة بالعمليات الاستخباراتية التقليدية، غير أن هذا التسارع في عملية اتخاذ القرار العسكري قد يؤدي إلى تقليص الوقت المتاح للتحقق من دقة المعلومات أو تقييم المخاطر الإنسانية المرتبطة بالهجمات، الأمر الذي قد يفضي إلى وقوع أخطاء تؤدي إلى استهداف المدنيين أو الأعيان المدنية، ومن هنا يبرز التحدي القانوني المتمثل في ضرورة تحقيق التوازن بين استخدام التكنولوجيا الحديثة في العمليات العسكرية وبين الالتزام الصارم بقواعد القانون الدولي الإنساني التي تهدف إلى الحد من آثار النزاعات المسلحة على السكان المدنيين.

وبناء على ذلك فإن تجربة قطاع غزة تمثل نموذجاً معاصراً يبرز بوضوح الفجوة القائمة بين التطور التكنولوجي في ميدان الحروب وبين الإطار القانوني الدولي المنظم لها، حيث إن القواعد القانونية الحالية، بما في ذلك نظام روما الأساسي للمحكمة الجنائية الدولية، لم تصمم في الأصل لمعالجة الجرائم التي قد ترتكب باستخدام الأنظمة الذكية والوسائل الرقمية المتقدمة، الأمر الذي يعزز الدعوات المتزايدة في الفقه القانوني الدولي إلى ضرورة تطوير قواعد القانون الدولي الجنائي بما يتلاءم مع التحولات التكنولوجية التي تشهدها النزاعات المسلحة في العصر الرقمي.

وتظهر هذه الأمثلة العملية بوضوح أن التكنولوجيا الحديثة أصبحت جزءاً لا يتجزأ من النزاعات المسلحة المعاصرة، وهو ما يفرض تحديات قانونية كبيرة أمام القانون الدولي الجنائي. فالقواعد القانونية الحالية، وعلى الرغم من أهميتها، لا تزال غير كافية لتنظيم جميع الأبعاد المرتبطة باستخدام التكنولوجيا في ارتكاب الجرائم الدولية. ومن ثم فإن مواجهة هذه التحديات تتطلب تطوير الإطار القانوني الدولي وتحديث قواعده بما يتلاءم مع طبيعة الحروب الحديثة والجرائم الرقمية.

## **المطلب الثاني: آليات مؤسساتية دولية تقليدية تواجه جرائم دولية متجددة تكنولوجية**

إن تنامي الجرائم الدولية المرتبطة بالتكنولوجيا الحديثة لم يعد يقتصر على نطاق التشريعات الوطنية، بل أصبح يفرض تدخلاً متزايداً من قبل المجتمع الدولي ومؤسساته المختلفة. وفي هذا الإطار برز دور الأمم المتحدة ومجلس الأمن في توصيف التهديدات الرقمية باعتبارها من المسائل المرتبطة بحفظ السلم والأمن الدوليين (الفرع الأول)، إلى جانب الدور المتنامي للمنظمات الأمنية الدولية في دعم التعاون والتحقيق في الجرائم ذات البعد التكنولوجي (الفرع الثاني).

## **الفرع الأول: دور الأمم المتحدة ومجلس الأمن في توصيف الجرائم الرقمية كتهديد للسلم الدولي**

أصبح الاعتراف الدولي بأن التهديدات المتأتية من الفضاء السيبراني والتقنيات المتقدمة لا تقل خطورة عن تهديدات الأسلحة التقليدية قضية مركزية في سياق حفظ السلم والأمن الدوليين. لذلك انخرطت الأمم المتحدة ومجلس الأمن تدريجيًا في تأسيس إطار قانوني وسياسي للتعامل مع الجرائم الرقمية باعتبارها من العناصر التي يمكن أن تعرّض السلم الدولي للخطر وتستدعي استجابات جماعية متعددة الأطراف.

## أولاً: جهود الأمم المتحدة في وضع الأطر القانونية لمواجهة الجرائم الرقمية

سعت الجمعية العامة للأمم المتحدة إلى تطوير الإطار القانوني الدولي لمكافحة الجرائم المرتبطة بالتكنولوجيا، بإقرار اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية في ديسمبر 2024. تهدف هذه المعاهدة إلى تجريم الأفعال السيبرانية وتعزيز التعاون الدولي بين الدول الأطراف، بما في ذلك تبادل المعلومات، تجميد العائدات الإجرامية من الجرائم الرقمية، حماية الضحايا، وإنشاء شبكة اتصال دولية تعمل على مدار الساعة لتسهيل التعاون الفوري في مواجهة الهجمات السيبرانية.

هذه الاتفاقية تمثل اعترافاً واضحاً من المجتمع الدولي بأهمية مكافحة الجرائم الرقمية لحفظ الأمن الدولي وتعزيز التعاون بين الدول لمواجهة التهديدات الرقمية العابرة للحدود.

إضافة إلى الأطر القانونية، اضطلعت هيئات الأمم المتحدة المختلفة دوراً في التحذير من مخاطر الاستخدام غير المنضبط للتكنولوجيا الحديثة على السلم والأمن الدوليين. ففي جلسة انعقدت في يونيو 2024، ناقش مجلس الأمن مخاطر التهديدات المتطورة في الفضاء السيبراني، حيث دعا الأمين العام إلى تعزيز التعاون الدولي واتخاذ تدابير وقائية لمواجهة هذه التهديدات. وقد جاء هذا النقاش استجابةً للتزايد الملحوظ في الهجمات السيبرانية التي تستهدف بنى تحتية حيوية للدول، مما يؤثر بشكل مباشر على الأمن القومي والاستقرار الدولي.

كما ألقى خبراء الأمم المتحدة الضوء على تأثير التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والطائرات المسيّرة على السلم والأمن الدوليين ففي إحاطة خاصة عقدها مكتب الأمم المتحدة المعني بنزع السلاح، نوقشت المخاطر الناشئة من سوء استخدام هذه التقنيات في النزاعات المسلحة، بما يشمل الخوف من سباق تسلح تكنولوجي يمكن أن يزيد من حدة النزاعات وتهديدات الأمن الدولي.

لقد بدا من هذه الجهود أن المجتمع الدولي يعترف بالمأزق القانوني الناتج عن غياب نصوص واضحة في القانون الدولي التقليدي تتعلق بالتكنولوجيات الحديثة، وهو ما دفع إلى محاولة سد هذه الفجوة عبر معاهدة دولية شاملة وتحذيرات أممية مستمرة من مخاطر التحول الرقمي على السلم العالمي.

## ثانياً: توصيف مجلس الأمن للتهديدات الرقمية كمسألة للسلم والأمن الدوليين وتطبيقاتها العملية

يلعب مجلس الأمن التابع للأمم المتحدة الدور الأساسي في صيانة السلم والأمن

الدوليين، وفقًا لأحكام ميثاق الأمم المتحدة التي توليه هذه المسؤولية. وبالتالي أصبح المجلس منفتحًا على مناقشة التهديدات الرقمية بوصفها من القضايا التي يمكن أن تؤثر على السلم العالمي، حتى ولو لم يكن ذلك في سياق النزاعات المسلحة التقليدية فقط.

من الأمثلة على ذلك، المناقشات التي عقدها المجلس في يونيو 2024 حول التهديدات المتطورة في الفضاء السيبراني، والتي أطلق خلالها الأمين العام دعوات واضحة لاتخاذ تدابير وقائية تستجيب للتطبيقات السيبرانية التي قد تستخدم لتعطيل الخدمات الحيوية للدول أو التأثير على استقرارها الداخلي.

في الحرب الروسية الأوكرانية، برز استخدام الطائرات المسيّرة والأنظمة الرقمية في العمليات العسكرية على نحو أثار اهتمام المجتمع الدولي، ومن ضمنه الأمم المتحدة، بما يعكس الحاجة إلى تنظيم قانوني دولي لهذا النوع من التقنيات، وقد دعا الرئيس الأوكراني في خطاب أمام الجمعية العامة إلى وضع قواعد دولية لتنظيم استخدام الذكاء الاصطناعي في الأسلحة، مؤكدًا أن غياب مثل هذه القواعد قد يؤدي إلى سباق تسلح تكنولوجي خطير ويشكل تهديدًا للسلم والأمن العالمي.

أما العمليات العسكرية في قطاع غزة، فقد أثارت انتقادات دولية واسعة تتعلق بآثار استخدام التكنولوجيا العسكرية المتقدمة على السكان المدنيين، وهو ما ربطته بيانات أممية بتحذيرات من استخدام مفرط وغير منظم للتقنيات الحديثة في سياق النزاع، وقد عبر الأمين العام للأمم المتحدة عن قلقه إزاء امتداد معاناة المدنيين في النزاعات وأشار إلى التحديات المرتبطة باحترام قواعد القانون الدولي أثناء العمليات العسكرية.

كل ذلك يشير إلى أن مجلس الأمن بدأ يرى في الجرائم الرقمية والهجمات السيبرانية واستخدام التكنولوجيا المتقدمة في النزاعات من القضايا المتعلقة مباشرة بالسلم والأمن الدوليين، حتى وإن لم تكن هناك قرارات ملزمة محددة تتناول الجرائم الرقمية بوجه خاص. وهذه المناقشات والمواقف تمثل خطوة نحو الاعتراف الدولي بأن التحولات التكنولوجية أصبحت تشكل أحد مصادر التوتر والصراع في النظام الدولي الحديث.

إن جهود الأمم المتحدة ومجلس الأمن في توصيف الجرائم الرقمية كتهديد للسلم الدولي تتجسد في توسيع الفهم القانوني للنظام الدولي ليشمل التحديات السيبرانية، إلى جانب السعي نحو أطر قانونية ومعاهدات جديدة لمواجهة هذه التحديات بشكل جماعي، وهو ما يعكس إدراكًا متناميًا لطبيعة التهديدات الحديثة التي تتجاوز الأسلحة والتقنيات التقليدية إلى المجال الرقمي.

## **الفرع الثاني: دور المنظمات الأمنية الدولية (الإنتربول – اليوروبول) في دعم التحقيق في الجرائم الدولية الرقمية**

مع انتشار الجرائم الرقمية على نطاق عالمي، وظهور شبكات إجرامية معقدة تعمل عبر الدول، برز دور المنظمات الأمنية الدولية كـ الإنتربول واليوروبول كمحاور رئيسية في دعم التحقيقات الجنائية الدولية. ذلك لأن هذه الجرائم لا تعترف بالحدود الوطنية، وتتطلب تعاونًا استخباراتيًا وتبادلاً فوريًا للمعلومات وخبرات تقنية متقدمة لتتبع المجرمين وملاحقتهم عبر مصادر رقمية مشتركة.

## أولاً: الإنترنت ودوره في التعاون الاستخباراتي ومكافحة الجرائم الرقمية

تعتبر المنظمة الدولية للشرطة الجنائية (الإنتربول) من أهم الآليات الدولية للتعاون بين أجهزة إنفاذ القانون في الدول الأعضاء. فهي توفر شبكة لتبادل المعلومات الفورية بين الأجهزة الأمنية على مستوى العالم، وتمتلك قواعد بيانات رقمية متقدمة تساهم في كشف وتتبع المجرمين الذين يرتكبون جرائم عبر الفضاء السيبراني. وتشمل هذه القواعد سجلات معرفات الهواتف، وعناوين الإنترنت المشبوهة، وأنماط سلوك المتهمين، ما يسهل على السلطات الوطنية تحديد مصادر الهجمات والتحقيق فيها.

وقد أثبت الإنترنت فاعليته في العديد من العمليات الدولية الاستراتيجية لمكافحة الجرائم الرقمية، حيث يقود أو ينسق حملات مشتركة تشمل دولاً عديدة تعمل معاً لمواجهة شبكات إجرامية عبر الوطنية. من الأمثلة البارزة عملية Serengeti 2.0 التي نفذت في أفريقيا بين يونيو وأغسطس 2025، وأسفرت عن القبض على 1,209 مشتبه بهم في جرائم سيبرانية متنوعة بالتعاون بين 18 دولة أفريقية والدول الشريكة، مع دعم بيانات استخباراتية من شركات أمنية مثل كاسبرسكي.

كذلك تأتي عملية Falcon 2 التي نفذت بالقارة الأفريقية بدعم تقني من الإنترنت، وأسفرت عن توقيف 318 مشتبهاً به، وتفكيك بنى إجرامية معقدة للنشاطات الرقمية مثل الاحتيال المالي والابتزاز عبر الإنترنت.

ولا تتوقف جهود الإنترنت على العمليات فحسب، بل تشمل أيضاً تقييمات تهديدات الجريمة السيبرانية التي توفر بيانات استخباراتية تستخدم في دعم التحقيقات المحلية والدولية، مما يساعد الدول الأعضاء على فهم المشهد التهديدي وتحديث استراتيجياتها القانونية والتقنية في مواجهة الجرائم الرقمية.

إضافة إلى ذلك، يعمل الإنترنت على توفير منصات آمنة لتبادل المعلومات والمعارف بين أجهزة الشرطة والشركاء العالميين، وهو أمر بالغ الأهمية في القضايا الرقمية التي تستلزم ردوداً آنية مبنية على البيانات والتحليل والتقارير التقنية.

## ثانياً: اليوروبول ودوره في دعم التحقيقات الدولية في الجرائم الرقمية

من جانب آخر، يعد المركز الأوروبي لمكافحة الجرائم السيبرانية (EC3) التابع لـ اليوروبول من أهم الكيانات الأمنية في أوروبا لدعم التحقيقات الجنائية في الجرائم الرقمية، وتنسيق تبادل المعلومات بين الدول الأعضاء في الاتحاد الأوروبي والدول الشريكة معهم.

وقد ساهم اليوروبول من خلال هذا المركز في تقديم الدعم التشغيلي والاستراتيجي والتحليل الجنائي المتخصص للسلطات المحلية، مما يساهم في تعزيز قدرات التحقيق في قضايا الاحتيال الإلكتروني والابتزاز والتصيد وبرمجيات الفدية. كما يقوم المركز بنشر تقييمات دورية للتهديدات السيبرانية (مثل تقرير IOCTA)، الذي يقدم رؤية تحليلية تهدف إلى دعم الحكومات في وضع أولويات التحقيق والمراقبة.

كما تبرز مساهمات يوروبول في عمليات مشتركة مع شركاء دوليين، إذ يشكل تعاوناً تكاملياً مع الإنترنت وأجهزة إنفاذ القانون الأخرى في حملات مكافحة الشبكات الإجرامية

العابرة للحدود، ويُستخدم تبادل البيانات المتاحة عبر قواعد البيانات الأوروبية لدعم التحقيقات في جرائم سيبرانية واسعة النطاق.

وقد أدت مثل هذه الجهود إلى تفكيك شبكات إجرامية رقمية معقدة واعتقال مشبوهين في دول متعددة، بما في ذلك عمليات هامة أدت إلى تعطيل برمجيات خبيثة وشبكات منتشرة عبر دول الاتحاد الأوروبي وشركائه.

### **ثالثاً: التعاون الاستخباراتي وقواعد البيانات الرقمية كأداة تحقيق**

يمثل التعاون الاستخباراتي الدولي بين الإنترنت واليوروبول وأجهزة الشرطة المحلية العمود الفقري للاستجابة الفاعلة للجرائم الرقمية العابرة للحدود إذ لا يمكن لأجهزة العدالة الجنائية الوطنية أن تواجه بمفردها تهديدات الجرائم الرقمية التي قد تنفذ من مواقع بعيدة جغرافياً أو عبر شبكات مشفرة وفي هذا الإطار، تعتمد التحقيقات على مبادرات منسقة لتبادل المعلومات الوقائية والاستراتيجية والتحليل الفني الذي يتم جمعه عبر قواعد البيانات الرقمية المشتركة.

وتوفر هذه القواعد المأمونة منصة لتسجيل الكيانات الإجرامية والشبكات الرقمية وعناوين IP المشبوهة والبرمجيات الخبيثة وغيرها من المؤشرات الجنائية التي تستخدم في التحليل والتتبع، ما يعزز من قدرة الأجهزة الأمنية على تحديد المشتبه بهم وتتبع أثرهم عبر الحدود الوطنية.

وقد أثبت هذا التعاون فعاليته في عمليات دولية واسعة، مثل عملية Sentinel في أفريقيا التي أسفرت عن اعتقال المئات من المشتبه بهم في عدد كبير من الدول، وتحطيم آلاف الروابط الرقمية الخبيثة، وإعادة بعض الأموال المستولى عليها، مما يبرز فاعلية التنسيق الدولي لوحدة التحقيقات الرقمية.

### **رابعاً: التحديات وأفاق العمل المشترك في مواجهة الجرائم العالمية**

رغم النجاحات التي حققتها الإنترنت واليوروبول في تنسيق التحقيقات الدولية ومكافحة الجرائم الرقمية، لا تزال هناك تحديات كبيرة تواجه هذا التعاون، منها تحديات التحقيقات عبر الحدود بسبب اختلاف الأطر القانونية الوطنية ومحدودية الموارد التكنولوجية لبعض الدول، فضلاً عن الصعوبات التقنية الناجمة عن التشفير العميق واستخدام تقنيات متقدمة من قبل المجرمين أنفسهم.

ومع ذلك يشكل التعاون الدولي في هذا المجال أحد أهم الأدوات التي يمكن للدول الاعتماد عليها في مواجهة التهديدات الرقمية العابرة للحدود، ويتطلب تعزيز هذه الآليات توحيد المعايير القانونية والتقنية، وزيادة التدريب المتخصص، وتعزيز الشراكات بين القطاع العام والخاص لتطوير قدرات التحقيق والردع الفعال للجرائم الدولية الرقمية.

يمثل الإنترنت واليوروبول عناصر مركزية في منظومة التعاون الدولي لمكافحة الجرائم الرقمية ذات الأبعاد الدولية، من خلال التعاون الاستخباراتي، قواعد البيانات الرقمية، دعم التحقيقات المشتركة، وتنسيق العمليات مع الدول الأعضاء، ما يعزز جهود العدالة الجنائية الدولية في مواجهة التحديات الناشئة في البيئة الرقمية.

## المبحث الثاني: قصور الإقرار المتكامل للمسؤولية الدولية عن الجريمة الدولية المتطورة تكنولوجيا

أثارت التحولات التكنولوجية تحديات جديدة أمام نظام المسؤولية الجنائية الدولية، خاصة مع بروز الجرائم المرتبطة بالبيئة الرقمية والتقنيات الحديثة. فقد أفرز ذلك إشكالات تتعلق بإثبات الجرائم الدولية ذات المكون الرقمي وكذا بتحديد المسؤولية الجنائية في ظل استخدام الذكاء الاصطناعي والأنظمة المؤتمتة (المطلب الأول)، ومن ثم تبرز الحاجة إلى دراسة طبيعة الأدلة الرقمية ومعايير إثباتها، إلى جانب تطور مفاهيم المسؤولية الجنائية الدولية في هذا السياق. (المطلب الثاني).

### المطلب الأول: لزوم تطوير إجرائي لإقرار المسؤولية للجريمة الدولية وأثارها

أفرزت الجرائم الدولية ذات المكون الرقمي تحديات جديدة في مجال الإثبات أمام القضاء الدولي، خاصة فيما يتعلق بطبيعة الأدلة الرقمية وحجيتها (الفرع الأول) كما تثار إشكالات تتعلق بمعايير قبول هذه الأدلة وضمان سلامتها وسلسلة حيازتها أمام المحكمة الجنائية الدولية) (الفرع الثاني).

### الفرع الأول: طبيعة الأدلة الرقمية وإشكالات أدلة الأقمار الصناعية

شهدت العدالة الجنائية الدولية تطورا نوعيا في الأعوام الأخيرة مع بروز الأدلة الرقمية كمكون أساسي في إثبات الجرائم، خاصة تلك التي لها أثر دولي أو ترتكب عبر الوسائط الرقمية المعقدة، ويفهم من الأدلة الرقمية أنها كل معلومة أو بيانات مخزنة أو مُرسلة أو منتجة في شكل إلكتروني يمكن استخدامها كدليل في الإجراءات القضائية، مثل البريد الإلكتروني والمحادثات الرقمية وسجلات المعاملات وبيانات الأجهزة الذكية وغيرها. وهذه الأدلة تختلف في طبيعتها عن الأدلة التقليدية، إذ تعتمد على تقنيات تخزين ومعالجة رقمية تتطلب فهما فنيا وقانونيا معمقا عند تقديمها أمام المحاكم الدولية.

تنشأ الأدلة الرقمية من مصادر متعددة ومتنوعة، تتراوح بين أجهزة الحواسيب والهواتف الذكية إلى الأقمار الصناعية وأنظمة المراقبة الرقمية والبصمات السيبرانية المسجلة على الشبكات. ولعل أدلة الأقمار الصناعية تعد واحدة من أكثر الأدلة الرقمية أهمية في القضايا ذات البعد الدولي، خاصة في النزاعات المسلحة أو الجرائم ضد الإنسانية، إذ يمكن أن تظهر صورا للوقائع من الجو أو مراقبة حركة القوات أو مواقع معينة ضمن أطر زمنية دقيقة.

هذه الصور تنتج كمية كبيرة من البيانات التي يمكن تقييمها لتحليل الأحداث وتوقيت وقوعها وموقعها، مما يوفر دليلاً بصرياً موثقاً يمكن للقضاء الدولي أن يستند إليه في التحقيقات.

غير أن طبيعة هذه الأدلة الرقمية تحمل معها إشكالات قانونية وتقنية معقدة تتطلب تفاعلاً ذكياً بين القانون والتقنية، فمن الناحية القانونية، يواجه القاضي الدولي صعوبة في التأكد من أصالة الأدلة الرقمية ومدى سلامتها من التلاعب أو التعديل، نظراً لأن البيانات الرقمية يمكن تغييرها أو حذفها بسهولة مقارنة بالأدلة التقليدية مثل الشهادة الحية أو الوثائق الورقية وهذا يوجب على المحاكم الدولية وضع معايير دقيقة لفحص موثوقية الأدلة الرقمية والتحقق من سلاسل الحيازة التي تضمن عدم تعرضها لأي تلاعب منذ لحظة جمعها وحتى تقديمها في الجلسات.

ومن أكبر الإشكالات المرتبطة بالأدلة الرقمية أيضاً مبدأ سلسلة الحيازة (Chain of Custody) الذي يتطلب إثباتاً قانونياً وتقنياً متسلسلاً لكل مرحلة في التعامل مع الدليل الرقمي، من وقت استرجاعه من المصدر الرقمي إلى حفظه وتحليله وتقديمه أمام المحكمة. وغالباً ما تتضمن هذه العملية تدخل خبراء في الأدلة الرقمية وتقنيات البحث الجنائي الرقمي لضمان أن التعديل أو التلاعب لم يحدث أثناء نقل أو تحليل البيانات وإلا فإن الدليل الرقمي قد يفرض من قبل القاضي لعدم وضوح سلسلة حيازته أو خضوعه لتعديل غير موثق.

علاوة على ذلك، يُشكل إدخال سجلات الأقمار الصناعية والبصمات السببرانية في الإثبات الجنائي تحدياً آخر يتمثل في ضرورة التأكد من أن هذه البيانات أو الصور تم التقاطها وتسجيلها بطريقة فنية صحيحة وموثوقة، تقوم على وسائل تكنولوجية معتمدة إذ لا يكفي أن تُقدم البيانات الرقمية ذاتها، بل يجب أن ترفق بتقارير تحليلية من خبراء مختصين يوضحون كيفية التقاطها واستخراجها وتحليلها، ويشرحون العلاقة بينها وبين الوقائع المدعاة في الدعوى وهذا ما يستلزمه القضاء الدولي ليمنح هذه الأدلة قيمة إثباتية فعلية ترقى إلى مستوى شأنها شأن الأدلة المادية التقليدية.

وعلى الرغم من هذه التحديات، فإن الأدلة الرقمية باتت تشكل جزءاً أساسياً في التحقيقات الجنائية الدولية، إذ تعتمد عليها المحاكم الدولية في عدد من الملفات الكبرى، مثل تقديم صور أقمار صناعية وشهادات رقمية في قضايا انتهاكات حقوق الإنسان أو جرائم الحرب.

ومع استمرار تطور التكنولوجيا الرقمية، يتنامى دور هذه الأدلة ويزيد تعقيدها، مما يستدعي من الهيئات القضائية تطوير معايير قانونية وإجرائية متقدمة تتعامل مع خصوصيات الطبيعة الرقمية وتضمن العدالة في الإثبات.

## **الفرع الثاني: معايير الإثبات في المحكمة الجنائية الدولية في الجرائم الرقمية المعقدة**

أصبح الإثبات في القضايا الجنائية الدولية المعاصرة أكثر تعقيداً باعتبار أن الأدلة الرقمية باتت عنصراً جوهرياً في التحقيقات، خاصة في الجرائم الدولية المرتكبة عبر الوسائل التقنية الحديثة. وعلى الرغم من أن نظام روما الأساسي لا يتضمن نصوصاً صريحة تتعلق

بالأدلة الرقمية، فإن المحكمة الجنائية الدولية تعاملت مع هذه الأدلة ضمن الإطار العام لقواعد الإثبات، مستندة إلى نصوص نظام روما الأساسي وقواعد الإجراءات والأدلة ذات الصلة، مما يستوجب تحليل معايير قبول هذه الأدلة وموثوقيتها في مختلف المراحل القضائية.

## أولاً: قبول الأدلة الرقمية أمام المحكمة الجنائية الدولية

لا يشترط نظام روما الأساسي وجود قواعد خاصة للأدلة الرقمية، لكن نصوصه العامة تبيح للمحكمة قبول أي دليل يُقدم إليها شريطة أن يكون موثقاً ومصادقاً عليه ويتسم بالملاءمة والمؤسسية القانونية، تنظر الغرف في المحكمة إلى الأدلة الرقمية بنفس المعايير التي تطبق على الأدلة المادية أو الشفوية من حيث ارتباطها بالوقائع المدعاة وقدرتها على إثبات أو دحض عناصر القضية، ويعد قبول الأدلة الرقمية ليس مسألة ما إذا كانت موجودة، ولكن ما إذا كانت تستوفي شروط الإثبات العامة كالحجية والموثوقية والارتباط الواقعي بالجرم موضوع الدعوى.

كما أن الأدلة الرقمية لا تستبعد تلقائياً فقط لأنها رقمية؛ فالمسألة ليست ما إذا كانت الأدلة رقمية أم لا، بل ما إذا كانت تستوفي متطلبات الإثبات في النظام القضائي الدولي، بما في ذلك قدرتها على إثبات الوقائع من دون شبهة تحريف أو تزوير.

## ثانياً: إشكالات سلامة الأدلة الرقمية وسلسلة الحيازة

من التحديات الأساسية في قبول الأدلة الرقمية أمام المحكمة هو تحقيق سلامتها من التلاعب وتوثيق ذلك بشكل قانوني. فالأدلة الرقمية يمكن أن تتغير بسهولة، مثل السجلات الإلكترونية أو البيانات التي تسحب من وسائل الاتصالات أو مواقع التواصل، ما يستدعي ضمان أن هذه البيانات ظلت سليمة منذ لحظة جمعها وحتى تقديمها في الجلسة.

تعد سلسلة الحيازة الرقمية (Chain of Custody) من أهم المعايير التقنية والقانونية التي تؤكد عدم التلاعب بالدليل، وذلك بتسجيل كل خطوة من خطوات جمع البيانات وتحليلها ونقلها وتخزينها، ومن هم الأشخاص الذين عالجوا تلك البيانات والوسائل التقنية المستخدمة، بما في ذلك المواقيت الزمنية (Time Stamps) وعناوين الإنترنت والبرامج المستخدمة في الاستخراج والتحليل.

تشمل إشكالات سلامة الأدلة أيضاً تحديات أخرى متعددة، فمن ناحية، يمكن أن تكون توقيعات التحقق الرقمي مثل خوارزميات التجزئة (Hash) غير كافية وحدها لإثبات الأصالة إذا كانت هناك إمكانية لتزويرها، أو إذا كانت الخوارزمية المستخدمة لم تعد مقاومة للتلاعب، مما يجعل الاعتماد عليها وحدها لإثبات سلامة الدليل أمراً غير كافٍ.

ولذلك، يتعين على محكمة الجنائية الدولية، عند فحص الأدلة الرقمية، الأخذ بعين الاعتبار كلا من مضمون البيانات التقنية والوثائق القانونية الداعمة التي تبين كيفية جمعها ومعالجتها، حتى يتمكن قاضي الإثبات من تكوين اقتناع قانوني بأنها لم تتعرض للتلاعب أو التغيير غير المصرح به.

## ثالثاً: دور قواعد الإجراءات في قبول الأدلة الرقمية

تعتمد المحكمة على قواعدها الإجرائية العامة في تحديد ما إذا كانت الأدلة الرقمية مقبولة، ومن أبرزها قاعدة الإثبات العامة التي تلزم المحاكم باستقبال الأدلة ما دامت لها صلة بالوقائع وسمتها القانونية واضحة، ما يعني أن القضاة لديهم سلطة تقديرية في تقييم مصداقية الأدلة الرقمية. وفي بعض الحالات، قد يُسمح بتقديم الأدلة الرقمية حتى لو كانت هناك شكوك، شريطة أن تُمنح الأطراف فرصة للطعن فيها أو تقديم تفسير بديل، ما يعكس تجربة القضاة في التعامل مع هذه الأدلة حتى وإن لم تكن موصوفة صراحة في نظام روما الأساسي.

إن عملية قبول الأدلة الرقمية في المحكمة لا تعد شكلية أو تلقائية، بل تتطلب تقييماً دقيقاً من القضاة يأخذ في الحسبان تقنيات جمع البيانات وكيفية حفظها، ومدى ارتباطها الوثيق بالقضية، إضافة إلى التأكد من أن عرضها وتفسيرها أمام المحكمة لا ينتهك حقوق الدفاع أو مبدأ المحاكمة العادلة.

### رابعاً: دراسة حالة تطبيقية من واقع الجرائم الرقمية

في النزاع الروسي الأوكراني، شكّلت الأدلة الرقمية جزءاً محورياً من التحقيقات الجنائية الدولية والتحقيقات الميدانية، خاصة تلك المتعلقة بحقوق الإنسان وجرائم الحرب. فقد أُحيلت حالة النزاع في أوكرانيا إلى المحكمة الجنائية الدولية منذ مارس 2022، بعد قبول أوكرانيا اختصاص المحكمة بموجب النظام الأساسي، وذلك بهدف التحقيق في الجرائم الجسيمة المزعومة المرتكبة خلال الحرب ومنذ ذلك الحين، اعتمد التحقيق على مجموعة من الأدلة الرقمية المتنوعة التي تتعلق بسلوك أطراف النزاع والوقائع المسجلة أثناء العمليات العسكرية.

من بين أنواع الأدلة الرقمية الهامة، تستخدم الصور والبيانات الملتقطة عبر الأقمار الصناعية بشكل مستمر لتوثيق حجم الأضرار التي لحقت بالمباني المدنية والبنى التحتية خلال النزاع. كما تظهر هذه الصور، التي تحلل بمساعدة تقنيات متقدمة، تغيرات في المواقع المحورية قبل وبعد الهجمات، مما يوفر منظوراً موضوعياً حول مدى الدمار وتوقيت وقوعه. وقد طور الباحثون نماذج تحليلية تعتمد على سلاسل زمنية من صور الأقمار الصناعية لتعزيز دقة تقدير حجم الأضرار على مستوى المنازل والمباني الحضرية، ما يُستخدم كأداة مساعدة في التحقيقات القانونية المستمرة.

كما ساهمت مصادر المعلومات مفتوحة المصدر (OSINT) في توثيق جوانب أخرى من النزاع، عبر تجميع وتحليل بيانات معتمدة على شبكات التواصل الاجتماعي والصور والفيديوهات الملتقطة من طرف المدنيين داخل مناطق الحرب، فقد أصبحت هذه المواد الرقمية مصدراً مثبتاً لأحداث محددة، مثل هجمات على الأحياء السكنية أو انتهاكات للقانون الدولي الإنساني، خصوصاً عندما يتم توثيقها بتواريخ ومواقع جغرافية واضحة، ويمكن للمدعين العامين في قضايا المحكمة الجنائية الدولية استخدام هذه المواد لدعم التحقيقات، شريطة التأكد من سلامة سلسلة حيازتها وعدم التلاعب بها.

إضافة إلى ذلك ساهمت أنظمة الوعي الموقعي والتقنيات الرقمية، مثل أنظمة المراقبة العسكرية والأقمار الصناعية التي تُدمج بيانات متعددة المصادر، في تحديد مواقع المعدات

العسكرية وتحركات القوات، ما يمكن الاستفادة منه في سياق إثبات أفعال قد تشكل جرائم حرب أو انتهاكات للقانون الدولي الإنساني، فالأدلة الرقمية الناتجة عن هذه الأنظمة تظهر مواقع الانتهاكات وتوقيتها، وهو ما يمثل عاملاً مهماً في تقييم مدى احترام المبادئ القانونية المتعلقة بالتمييز بين الأهداف العسكرية والمدنية.

مع ذلك لا تخلو هذه الأدلة من إشكالات قانونية بحتة، إذ يتطلب قبولها أمام المحكمة الجنائية الدولية إثباتاً دقيقاً لسلسلة الحيازة (Chain of Custody) وتأكيداً على عدم تعرضها لأي تعديل أو تلاعب خلال مراحل جمعها وتحليلها وتحويلها إلى مادة إثباتية، ويشكل هذا التوثيق ضرورياً لضمان سلامة الأدلة الرقمية، إذ أن أي ضعف في سلسلة الحيازة قد يؤدي إلى رفض الدليل أو تقليل حججه أمام القضاة، ومن هنا تظهر أهمية الاعتماد على إجراءات تقنية وقانونية محكمة في حفظ وتحليل البيانات الرقمية منذ استخراجها من مصادرها الأصلية حتى تقديمها في قاعة المحكمة.

بهذا تكون الحرب الروسية الأوكرانية نموذجاً علمياً لما تواجهه العدالة الجنائية الدولية من تحديات وفرص في استخدام الأدلة الرقمية المعقدة لتثبيت الوقائع الجنائية، ودعم التحقيقات في الجرائم الدولية، مع التأكيد على ضرورة مراعاة المعايير الصارمة للإثبات لضمان سلامة وعدالة الإجراءات القانونية.

### **المطلب الثاني: صعوبة إثبات الجرائم الدولية المرتبطة بالتطور الرقمي**

أدى التطور المتسارع في تقنيات الذكاء الاصطناعي إلى طرح تحديات جديدة أمام قواعد المسؤولية الجنائية الدولية، خاصة عندما ترتكب بعض الأفعال الضارة عبر أنظمة تقنية قادرة على اتخاذ قرارات شبه مستقلة ويثير ذلك إشكاليات قانونية معقدة تتعلق بتحديد القصد الجنائي وإسناد المسؤولية في الجرائم الدولية التي تتم عبر هياكل رقمية معقدة أو أنظمة مؤتمتة.

### **الفرع الأول: تحديات تحديد القصد الجنائي في الجرائم الدولية المرتبطة بالذكاء الاصطناعي**

إن التطور السريع في تقنيات الذكاء الاصطناعي إلى ظهور أنظمة رقمية قادرة على اتخاذ قرارات شبه مستقلة دون تدخل مباشر من الإنسان، وهو ما يثير إشكالية عميقة في إطار القانون الجنائي الدولي، خاصة فيما يتعلق بتحديد القصد الجنائي (Mens Rea) الذي يعد أحد الركائز الأساسية لقيام المسؤولية الجنائية.

فالقواعد التقليدية للمسؤولية الجنائية تقوم على فكرة أن الجريمة هي فعل إنساني صادر عن إرادة واعية تتجه نحو تحقيق نتيجة إجرامية معينة، غير أن هذا التصور يصبح أكثر تعقيداً عندما يتم تنفيذ الفعل الضار بواسطة أنظمة تقنية تعمل وفق خوارزميات معقدة وقدرة تعلم ذاتي وفي هذه الحالة يبرز التساؤل الجوهرى حول من يمكن إسناد النية إليه: هل هو المبرمج، أم المصمم، أم المستخدم، أم النظام الذكي ذاته الذي قام بالفعل؟

تتجلى الإشكالية بوضوح في الأنظمة المستقلة التي تتمتع بقدرة على تحليل البيانات واتخاذ القرارات بناءً على خوارزميات التعلم الآلي، إذ قد تنصرف هذه الأنظمة بطرق لم

يتوقعها حتى مطوروها. وفي هذه الحالات يصعب تطبيق المفاهيم التقليدية للقصد الجنائي التي تفترض وجود فاعل بشري يدرك نتائج فعله ويتوقعها، فالنظام الذكي قد يختار هدفاً معيناً أو ينفذ عملية معينة بناءً على تحليل بيانات ضخمة دون أن يكون هناك قرار مباشر من الإنسان في لحظة التنفيذ، مما يخلق فجوة بين الفعل المادي للجريمة والإرادة البشرية التي يفترض أن تقف وراءه.

ومن هنا تظهر أزمة قانونية تتعلق بإثبات عنصر النية، خاصة في الجرائم الدولية التي تتطلب إثبات قصد خاص مثل جرائم الإبادة الجماعية أو الجرائم ضد الإنسانية.

وتزداد هذه الصعوبة في سياق استخدام الذكاء الاصطناعي في المجال العسكري، مثل أنظمة الأسلحة ذاتية التشغيل التي تعتمد على خوارزميات متقدمة لتحديد الأهداف وتوجيه الضربات. ففي هذه الأنظمة قد يتم اتخاذ القرار النهائي بالهجوم بشكل آلي بعد تفعيل النظام من قبل المشغل البشري، وهو ما يطرح إشكالية تحديد المسؤولية الجنائية عندما يؤدي هذا القرار إلى انتهاك قواعد القانون الدولي الإنساني، مثل استهداف المدنيين أو الأعيان المدنية.

ففي مثل هذه الحالات يصعب إثبات أن القائد العسكري أو المشغل كان يمتلك القصد الجنائي المباشر لارتكاب الجريمة، خاصة إذا كان النظام يعمل وفق آلية ذاتية في تحديد الأهداف.

كما تثير طبيعة الذكاء الاصطناعي المعتمدة على خوارزميات التعلم الذاتي مشكلة أخرى تتمثل فيما يعرف بظاهرة "الصندوق الأسود"، حيث (Machine Learning) يصعب في كثير من الأحيان تفسير كيفية توصل النظام إلى قرار معين.

فالنظام قد يقوم بمعالجة ملايين البيانات وإنتاج نتيجة معينة دون أن يكون بالإمكان تتبع المسار المنطقي الذي أدى إلى ذلك القرار. وهذه الخاصية التقنية تجعل من الصعب إثبات العلاقة السببية بين النية البشرية والنتيجة الإجرامية، وهو ما يضع المحاكم الجنائية الدولية أمام تحدٍ كبير في إثبات القصد الجنائي في الجرائم المرتكبة عبر هذه الأنظمة الرقمية المعقدة.

إضافة إلى ذلك، أثار الفقه القانوني جدلاً واسعاً حول إمكانية منح أنظمة الذكاء الاصطناعي نوعاً من الشخصية القانونية المستقلة، بحيث يمكن مساءلتها عن الأفعال التي ترتكبها بشكل مباشر. غير أن هذا الاتجاه لا يزال محل خلاف كبير، لأن القانون الجنائي يقوم أساساً على فكرة المسؤولية الأخلاقية التي تفترض وجود وعي وإدراك لدى الفاعل، وهو ما لا يتوافر في الأنظمة التقنية الحالية. لذلك يرى أغلب الفقهاء أن المسؤولية يجب أن تبقى مرتبطة بالعنصر البشري، سواء تعلق الأمر بالمبرمجين أو المصنعين أو المستخدمين أو الجهات التي قررت نشر هذه الأنظمة في بيئات خطيرة.

وعليه، فإن تحدي تحديد القصد الجنائي في الجرائم الدولية المرتبطة بالذكاء الاصطناعي لا يتعلق فقط بمشكلة تقنية، بل يمثل تحوفاً عميقاً في طبيعة الفعل الإجرامي نفسه. فمع ازدياد استقلالية الأنظمة الرقمية، أصبح من الضروري إعادة التفكير في الأسس التقليدية للمسؤولية الجنائية الدولية، بما يسمح بملاءمتها مع الواقع التكنولوجي الجديد دون المساس بالمبادئ الأساسية للعدالة الجنائية الدولية.

يعد مبدأ السيطرة الفعالة (Effective Control) أحد أهم الأسس التي يقوم عليها نظام المسؤولية الجنائية الدولية، خاصة في إطار ما يُعرف بمسؤولية القادة والرؤساء في القانون الجنائي الدولي.

وقد كرست هذا المبدأ العديد من المحاكم الجنائية الدولية، كما تم النص عليه صراحة في المادة 28 من نظام روما الأساسي للمحكمة الجنائية الدولية، التي تقرر مسؤولية القادة العسكريين أو المدنيين عن الجرائم التي يرتكبها مرؤوسوهم إذا كانوا يملكون سلطة فعلية عليهم وكان بإمكانهم منع تلك الجرائم أو معاقبة مرتكبيها.

غير أن التطور التكنولوجي المتسارع، خاصة مع انتشار الأنظمة الرقمية المعقدة والذكاء الاصطناعي في العمليات العسكرية والأمنية، أدى إلى ظهور إشكاليات جديدة تتعلق بإمكانية تطبيق هذا المبدأ في البيئات الرقمية.

فالنموذج التقليدي لمسؤولية القيادة يقوم على وجود علاقة واضحة بين القائد والمرؤوس في إطار تسلسل هرمي محدد، حيث يمتلك القائد سلطة إصدار الأوامر ومراقبة تنفيذها، أما في الأنظمة الرقمية الحديثة، فإن الفعل الإجرامي قد يتم عبر خوارزميات أو أنظمة مستقلة نسبياً عن التدخل البشري المباشر، مما يجعل مسألة إثبات السيطرة الفعلية أكثر تعقيداً.

في السياق التقليدي، تقوم مسؤولية القائد على ثلاثة عناصر رئيسية: وجود علاقة تبعية بين القائد والمرؤوس، علم القائد أو إمكانية علمه بارتكاب الجرائم، وفشله في اتخاذ التدابير اللازمة لمنعها أو معاقبة مرتكبيها.

غير أن هذه العناصر تصبح إشكالية في البيئات الرقمية، حيث قد لا يكون النظام الذكي "مرؤوساً" بالمعنى القانوني التقليدي، بل أداة تقنية قادرة على اتخاذ قرارات مستقلة أو شبه مستقلة اعتماداً على البيانات والخوارزميات.

وهذا ما أدى إلى ظهور ما يسمى في الفقه القانوني بـ "فجوة المسؤولية" (Responsibility Gap)، حيث يصعب تحديد الفاعل الحقيقي الذي يجب تحميله المسؤولية الجنائية عندما ينتج الفعل الضار عن نظام تقني معقد.

وتزداد هذه الإشكالية وضوحاً في حالة أنظمة الأسلحة ذاتية التشغيل التي يمكنها اختيار الأهداف وتنفيذ الهجمات دون تدخل بشري مباشر بعد تفعيلها. ففي هذه الحالة قد يفقد القائد العسكري القدرة الفعلية على إيقاف النظام بعد بدء العملية، خاصة في ظل سرعة المعالجة الرقمية أو حدوث أعطال تقنية أو أخطاء برمجية غير متوقعة، وبالتالي يصبح من الصعب إثبات أن القائد كان يمتلك سيطرة فعلية على النظام وقت وقوع الجريمة، وهو الشرط الأساسي لقيام مسؤوليته وفق قواعد القانون الجنائي الدولي.

كما تبرز صعوبة أخرى تتعلق بطبيعة الأنظمة الرقمية نفسها، إذ تعتمد العديد من تطبيقات الذكاء الاصطناعي على خوارزميات التعلم الذاتي التي قد تطور سلوكيات جديدة لم تكن متوقعة عند تصميمها.

وفي هذه الحالة قد يتخذ النظام قرارات بناء على تحليل بيانات معقدة دون أن يكون

المشغل البشري قادرا على فهم أو تفسير الآلية التي أدت إلى ذلك القرار وهذا ما يضعف إمكانية إثبات عنصر العلم لدى القائد أو المسؤول، وهو عنصر جوهري في إثبات المسؤولية الجنائية الدولية.

ورغم هذه التحديات، فإن الاتجاه الغالب في الفقه القانوني الدولي يؤكد أن استخدام الأنظمة الرقمية أو الذكاء الاصطناعي لا يؤدي إلى إسقاط المسؤولية الجنائية عن القادة أو الدول. فالقانون الدولي ما يزال يقوم على مبدأ أساسي مفاده أن المسؤولية القانونية يجب أن تبقى مرتبطة بالفاعل البشري أو بالدولة التي قامت بتطوير أو نشر هذه الأنظمة وبناءا عليه، فإن أي انتهاك للقانون الدولي الإنساني يرتكب باستخدام أنظمة ذكية يُنسب في النهاية إلى الدولة التي استخدمتها وإلى القادة الذين يمتلكون سلطة تشغيلها أو الإشراف عليها.

وفي ضوء هذه التطورات، بدأ الفقه القانوني يدعو إلى إعادة تفسير مبدأ السيطرة الفعالة بما يتلاءم مع البيئة الرقمية الحديثة، فبدلا من التركيز فقط على السيطرة المباشرة لحظة تنفيذ الفعل، يقترح بعض الباحثين توسيع مفهوم السيطرة ليشمل القدرة على التصميم والبرمجة والإشراف المسبق على الأنظمة التقنية.

وبموجب هذا التصور، يمكن مساءلة القادة أو المسؤولين عن الجرائم التي ترتكبها الأنظمة الرقمية إذا ثبت أنهم سمحوا باستخدام هذه الأنظمة دون اتخاذ التدابير الكافية لضمان امتثالها لقواعد القانون الدولي الإنساني.

كما ظهرت مقترحات أخرى تدعو إلى تبني مفهوم "الإشراف البشري القعال" (Meaningful Human Control)، الذي يهدف إلى ضمان بقاء الإنسان في موقع اتخاذ القرار النهائي في العمليات العسكرية التي تستخدم الذكاء الاصطناعي.

ويهدف هذا المفهوم إلى سد الفجوة بين التطور التكنولوجي ومتطلبات المسؤولية القانونية، من خلال فرض التزام على الدول بضرورة الحفاظ على مستوى معين من التحكم البشري في الأنظمة القتالية المستقلة.

وبذلك يتضح أن التطور التكنولوجي، رغم ما يوفره من قدرات جديدة في مجال العمليات العسكرية والأمنية، يفرض في الوقت نفسه تحديات كبيرة على مفاهيم المسؤولية الجنائية الدولية، فمع تزايد اعتماد الدول على الأنظمة الرقمية والذكاء الاصطناعي، يصبح من الضروري تطوير الأطر القانونية القائمة بما يضمن عدم تحول هذه التكنولوجيا إلى وسيلة للإفلات من العقاب، مع الحفاظ في الوقت ذاته على المبادئ الأساسية التي يقوم عليها نظام العدالة الجنائية الدولية.

## خلاصة الفصل

يتناول هذا الفصل التحولات التي أحدثها التطور التكنولوجي في طبيعة الجرائم الدولية، حيث لم تعد هذه الجرائم تقتصر على الوسائل التقليدية، بل أصبحت ترتبط بالفضاء الرقمي وبالتقنيات الحديثة مثل الذكاء الاصطناعي والهجمات السيبرانية والأنظمة المؤتمتة.

وفي هذا الإطار تم التطرق إلى مدى قدرة القانون الدولي الجنائي، ولا سيما نظام روما الأساسي، على استيعاب هذه الأنماط الجديدة من الجرائم، مع إبراز دور المنظمات الدولية، وعلى رأسها الأمم المتحدة والهيئات الأمنية الدولية، في توصيف هذه الأفعال ومواجهتها ضمن منظومة السلم والأمن الدوليين.

كما تناول الفصل إشكالات المسؤولية الجنائية الدولية في البيئة الرقمية، خاصة ما يتعلق بطبيعة الأدلة الرقمية ومعايير قبولها أمام القضاء الدولي، إلى جانب التحديات المرتبطة بإثبات القصد الجنائي وتحديد نطاق السيطرة الفعلية في الجرائم المرتكبة عبر الأنظمة التكنولوجية الحديثة.

# خاتمة

## خاتمة

في ضوء التحولات التكنولوجية العميقة التي طرأت على مفهوم الجريمة الدولية، وما أفرزته من نماذج إجرامية جديدة تتجاوز المفاهيم التقليدية في القانون الدولي الجنائي، فقد أصبح من الضروري إعادة النظر في الأسس القانونية والتشريعية السائدة لتفسير هذه الظواهر الحديثة وتكييفها مع القواعد الدولية القائمة.

حيث لم يعد بإمكان المفاهيم القانونية التقليدية وحدها أن تواكب تداخل التكنولوجيا مع الجرائم ذات البعد الدولي، سواء على مستوى ارتكاب الفعل، أو إثباته، أو نسبته إلى الفاعل، أو تحميل المسؤولية الجنائية في بيئات رقمية معقدة.

كما بين التحليل القانوني أن الفجوة بين تطور التكنولوجيا ونصوص القانون الدولي الجنائي قد سهلت دخول تقنيات مثل الذكاء الاصطناعي والأنظمة المستقلة في نطاق ارتكاب أفعال يمكن أن تعد جرائم دولية، دون أن تتوفر آليات قانونية واضحة لاستيعابها في إطار المساءلة القانونية الدولية.

وفي ظل الرؤية التي تبناها هذه الجهد البحثي لفك الارتباط بين المفاهيم التقليدية والواقع التكنولوجي المتسارع، يمكننا تلخيص ما استقر لدينا من نتائج في النقاط الجوهرية الآتية:

أن التطور التكنولوجي السريع أفرز نماذج جديدة من الجرائم الدولية لا يمكن تفسيرها أو التعامل معها بالكامل عبر المفاهيم التقليدية للجريمة الدولية.

الأنظمة القانونية الدولية القائمة، بما فيها نظام روما الأساسي، تفتقر إلى نصوص واضحة لمعالجة الجرائم الرقمية المعقدة، ما يخلق فجوات قانونية تمس الكفاءة القضائية.

أن القبول العام للأدلة الرقمية وأسس إثباتها لا يزال يواجه تحديات متعددة تتعلق بسلامة الأدلة، وسلسلة الحيازة، وقابلية التفسير أمام القضاء الدولي.

أن تحديد القصد الجنائي (Mens Rea) في الجرائم المرتبطة بالذكاء الاصطناعي وأنظمة مستقلة يطرح صعوبات جوهرية، ما يضع مفهوم النية التقليدي على المحك القانوني.

أن مبدأ "السيطرة الفعالة" في الهياكل الرقمية المعقدة يحتاج لإعادة تفسير قانوني لضمان تحميل القادة والمديرين المسؤولية عند استغلال الأنظمة الرقمية في ارتكاب الجرائم.

خلصت نتائج البحث على أن التعاون الدولي بين الهيئات الأمنية والتشريعية أمر ضروري لمواجهة الجرائم الرقمية العابرة للحدود، سواء عبر الإنترنت، اليوروبول، أو تدابير الأمم المتحدة.

وعلى ضوء النتائج السابقة، تتبلور لدينا جملة من الاقتراحات التي نرى ضرورة طرحها لخدمة هذا المسار البحثي، والتي تهدف في جوهرها إلى المساهمة في تحديث السياسة الجنائية الدولية بما يواكب المتغيرات الرقمية، ولعل من أبرزها:

صياغة نصوص قانونية دولية متخصصة تكمل نظام روما الأساسي وتتناول صراحة الجرائم الرقمية الحديثة، بما في ذلك تلك المرتبطة بالذكاء الاصطناعي. وضع آليات واضحة لقبول الأدلة الرقمية في المحكمة الجنائية الدولية، تتضمن معايير سلامة وسلسلة الحيازة والإجراءات الفنية لتحليلها، مع ضمان الشفافية والحيادية.

إعادة تفسير مفهوم القصد الجنائي ليشمل حالات الجرائم التي تتفد عبر أنظمة ذكية، وحيث لا يكون التدخّل البشري مباشرًا لحظة وقوع الفعل، بما يضمن تحقيق العدالة.

تعزيز التعاون الدولي عبر تبني اتفاقيات ملزمة في مكافحة الجرائم السيبرانية، وتشجيع الدول على الانضمام إلى معاهدات مثل معاهدة الأمم المتحدة لمكافحة الجرائم السيبرانية.

تطوير برامج تدريب وتأهيل للقضاة والمحققين والمحامين في مجالات التقنيات الحديثة لضمان فهم الأدلة الرقمية وإدارتها بفاعلية في القضايا الدولية.

دعم البحوث الأكاديمية والفقهية في موضوع الجريمة الدولية والتكنولوجيا، بما في ذلك رسائل الماجستير والدكتوراه، لتوسيع قاعدة المعرفة القانونية.

تشجيع تطوير التشريعات الوطنية المتسقة مع المعايير الدولية لضمان تغطية فراغات تشريعية محلية ودعم الجهود الدولية في مواجهة الجرائم الرقمية.

قائمة المصادر  
والمراجع

## قائمة المصادر والمراجع

### أولاً: المصادر

#### 1. القوانين والاتفاقيات والمعاهدات

- 1) النظام الأساسي للمحكمة الجنائية الدولية، اعتمد في روما بتاريخ 17 يوليو 1998، ودخل حيز النفاذ في يوليو 2002.
- 2) اتفاقية بودابست بشأن الجرائم المعلوماتية، اعتمدها مجلس أوروبا في 8 نوفمبر 2001، وفتحت للتوقيع في بودابست في 23 نوفمبر 2001.
- 3) اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية (Convention on Cybercrime)، اعتمدها الجمعية العامة للأمم المتحدة بتاريخ 24 ديسمبر 2001، في إطار تعزيز التعاون الدولي لمكافحة الجرائم المرتكبة بواسطة نظم تكنولوجيا المعلومات والاتصال

#### 2. القوانين الجزائرية

1. القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر في 16 أوت 2009.

### ثانياً: المراجع

#### 1. الكتب

- 1) إسلام دسوقي عبد النبي، دور تقنيات الذكاء الاصطناعي في العلاقات الدولية والمسؤولية الدولية عن استخدامها، دار النهضة العربية، القاهرة، 2019.
- 2) حسان الباهي، الذكاء الاصطناعي وتحديات مجتمع المعرفة، دار الهدى، القاهرة، 2022.
- 3) الشاذلي فتوح عبد الله، القانون الدولي الجنائي، ديوان المطبوعات الجامعية، الإسكندرية، 2001.
- 4) عبد العال الديربي، محمد صادق إسماعيل، الجرائم الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.
- 5) محمد عادل محمد سعيد، التطهير العرقي دراسة في القانون الدولي العام والقانون الجنائي المقارن، الطبعة الأولى، دار جامعة الجديدة، الإسكندرية، 2009.
- 6) ميرفت محمد حبايية، مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري العلمية، عمان، الطبعة الأولى، 2023.
- 7) يعقوب بن سالم الحرصي، تطبيقات الثورة الصناعية الرابعة: الذكاء الاصطناعي – البيانات الضخمة – الروبوتات – تقنية النانو – إنترنت الأشياء – الأمن السيبراني، دار الوليد للنشر والتوزيع، القاهرة، 2021.

## 2. الأطروحات والرسائل الجامعية:

- 1) عبد الخالق محمد عبد المنعم، النظرية العامة للجريمة الدولية، اطروحة مقدمة لنيل شهادة دكتوراه، تخصص قانون دولي كلية عين الشمس، لقاهرة، 1988،
- 2) يوسف الصغير، الجريمة المرتكبة عبر الانترنت، رسالة مقدمة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012/2013،

## 3. المقالات العلمية

- 1) إبراهيم السيد حسنين زايد، "المسؤولية الجنائية عن أخطاء الذكاء الاصطناعي"، مجلة روح القوانين، جامعة طنطا، مصر، المجلد 35، العدد 102، مايو 2023.
- 2) إبراهيم سويسي، لخضر رابحي، "مواجهة جريمة التحريض الإلكتروني في ضوء مبدأ مسؤولية الحماية"، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي، المجلد 6، العدد 2، 2020.
- 3) أحمد عبيس الفتلاوي، "الهجمات السببرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق للعلوم القانونية والإنسانية، كلية القانون، جامعة بابل، العراق، العدد 2016، 4.
- 4) أحمد لطفي السيد مرعي، "انعكاسات تقنيات الذكاء الاصطناعي على نظرية المسؤولية الجنائية: دراسة تأصيلية مقارنة"، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، مصر، العدد 80، يونيو 2022.
- 5) خولة الكلاحي، عبد الرؤوف بزيان، "الذكاء الاصطناعي والأمن القانوني: الرهانات القانونية في المادة الانتخابية"، المركز الدولي للدراسات الاستراتيجية الأمنية والعسكرية، 2025.
- 6) رامي متولي القاضي، "نحو إقرار قواعد للمسؤولية الجنائية والعقاب على إساءة استخدام تطبيقات الذكاء الاصطناعي"، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، مصر، المجلد 4، العدد 2021، 11.
- 7) رحاب رابح القبائلي، "المسؤولية الدولية عن الأضرار الناجمة عن تقنيات الذكاء الاصطناعي"، مجلة دراسات قانونية، جامعة بنغازي، 2026.
- 8) سعيد ثاني المهيري، "التحريض في القانون الجنائي الدولي"، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الجزائر 1، المجلد 53، العدد 2016، 4.
- 9) سلوى يوسف عبد الهادي الإكيابي، "مدى انطباق القانون الدولي الإنساني على الهجمات السببرانية"، مجلة الدراسات القانونية، كلية الحقوق، جامعة الزقازيق، 2023.
- 10) صالح عبيد حسنين إبراهيم، "المصلحة في قانون العقوبات"، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، مصر، المجلد 17، العدد 1974، 2.

- 11) عبد المالك أشواق، بناني سعاد، "الذكاء الاصطناعي وأثره على المنظومة القانونية"، مجلة القانون والعلوم البيئية، جامعة زيان عاشور، الجلفة، المجلد 2، العدد 2023، 2.
- 12) عبد المؤمن الصغير، "الطبيعة الخاصة للجريمة الإلكترونية المرتكبة عبر الإنترنت في التشريع الجزائري والتشريع المقارن"، مجلة الحقوق والحريات، جامعة محمد خيضر، بسكرة، المجلد 2، العدد 2014، 2.
- 13) عشاش حمزة، خضري حمزة، "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، المجلد 6، العدد 2020، 2.
- 14) عمر محمد منيب إدلبي، "نطاق المسؤولية الجنائية الناشئة عن أخطاء الذكاء الاصطناعي"، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، إصدار خاص، 2024.
- 15) عهد محمود سليم، "الطبيعة الفريدة للجريمة الدولية وانعكاساتها على النظام القضائي الدولي"، المجلة العربية للنشر العلمي، المجلد 8، العدد 2025، 86.
- 16) قادري نور الهدى، "الجريمة السيبرانية وآليات مكافحتها: مواجهة تحديات الأمن السيبراني"، مجلة الحقوق والعلوم السياسية، جامعة أحمد بن يحيى الونشريس، تيسمسيلت، المجلد 8، العدد 2023، 1.
- 17) كواشي مراد، "المادة 5 من نظام روما الأساسي وأثرها على تطبيق القانون الدولي الإنساني وتحقيق السلم والأمن الدوليين"، مجلة الحقوق والحريات، جامعة محمد خيضر، بسكرة، المجلد 10، العدد 2022، 2.
- 18) محمود محمد سويف، "المسؤولية الجنائية لتقنيات الذكاء الاصطناعي"، مجلة البحوث القانونية والفقهية، كلية الشريعة والقانون، جامعة الأزهر، القاهرة، العدد 48، يناير 2025.
- 19) نبيل محمد عرعار، "المسؤولية الجنائية عن جرائم تقنية الذكاء الاصطناعي"، مجلة المنتدى الأكاديمي، نقابة أعضاء هيئة التدريس، الجامعة الأسمرية الإسلامية، ليبيا، المجلد 9، العدد 3، 2025.
- 20) وفاء صقر، "دور العملات الافتراضية المشفرة في جرمي غسل الأموال وتمويل الإرهاب"، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهور، جامعة الأزهر، العدد 2024، 46.
- 21) ياسر محمد اللمعي، "المسؤولية الجنائية عن أعمال الذكاء الاصطناعي ما بين الواقع والمأمول"، مجلة البحوث القانونية والاقتصادية.

#### 4. المواقع الإلكترونية

- 1) التقرير، Europol Internet Organised Crime Threat Assessment (IOCTA)، الاستراتيجي السنوي الصادر عن المركز الأوروبي لمكافحة الجرائم السيبرانية، متاح على موقع يوروبول:

<https://www.europol.europa.eu/iocta>

تم الاطلاع تاريخ 28/02/2026

- 2) International Committee of the Red Cross (ICRC), “Autonomous Weapons,” accessed 6 January 2026, at 5:00

<https://www.icrc.org/en/law-and-policy/autonomous-weapons>

- 3) International Committee of the Red Cross, Frequently Asked Questions: International humanitarian law and the use of drones in armed conflict

<https://www.icrc.org/en/article/faq-international-humanitarian-law-drones-armed-conflict>

- 4) INTERPOL, “23” الجرائم السيبرانية، “23” ديسمبر 2024، accessed January 2026, at 22:30

<https://www.interpol.int/ar/1/1/2024/39>

- 5) Lindsay Freeman, “The Rome Statute in the Digital Age: Confronting Emerging Cyber Threats,” Just Security

<https://www.justsecurity.org/118463/rome-statute-digital-age-cyber/>

- 6) The Guardian, “Russian drone attacks on civilians in Ukraine are war crimes, UN report concludes,” October 28, 2025

<https://www.theguardian.com/world/2025/oct/28/russian-drone-attacks-on-civilians-in-ukraine-are-war-crimes-un-report-concludes>

accessed 11/01/2026 at 2:40 .

- 7) الأمم المتحدة، “الجمعية العامة تعتمد اتفاقية تاريخية بشأن الجرائم الإلكترونية”، موقع الأمم المتحدة.

<https://www.ungeneva.org/ar/news-media/news/2024/12/101672/aljmyt-alamt-tmd-atfaqyt-tarykhyt-bshan-aljraym-alalktrny>

تاريخ الاطلاع 21/02/2026 بتوقيت 00:17.

- 8) الأمم المتحدة، “الاختراقات الرقمية يجب أن تُوجَّه لخدمة البشرية لا للإضرار بها: مجلس الأمن يناقش التهديدات المتطورة في الفضاء السيبراني”، وقائع اجتماع مجلس الأمن رقم 9662.

<https://press.un.org/en/2024/sc15738.doc.htm>

تم الاطلاع عليه بتاريخ 27/02/2026 بتوقيت 19:20.

- 9) الأمم المتحدة، تصريحات الأمين العام أمام مجلس الأمن حول “مواجهة التهديدات المتطورة في الفضاء السيبراني”.

<https://www.un.org/sg/en/content/sg/statement/2024-06-20/secretary-generals-remarks-the-security-councils-high-level-debate-maintenance-of-international-peace-and-security-addressing-evolving-threats-cyberspace>

- 10) الأمم المتحدة، “الأمين العام يدين استمرار سقوط المدنيين في غزة ويؤكد ضرورة احترام القانون الدولي الإنساني”، بيان صادر عن المتحدث باسم الأمين العام.

<https://www.ungeneva.org/en/news-media/news/2024/10/99404/guterres-unequivocally-condemns-continued-civilian-deaths-gaza>

تاريخ الاطلاع 01/0/2026، بتوقيت 19:29.

الجزيرة نت، «الذكاء الاصطناعي في الحروب». (11)

<https://www.aljazeera.net/blogs/2025/9/25/> الذكاء-الاصطناعي-في-الحروب

تم الاطلاع بتاريخ 28/02/2026 بتوقيت 3:00.

الجزيرة نت، «من يمتلك هذا المزيج العسكري في الحروب الحديثة سيتفوق». (12)

<https://www.aljazeera.net/politics/2025/7/10/> الحروب-الحديثة-تغيرت-ومن-يمتلك-هذا

تم الولوج اليه بتاريخ: 04/02/2026. بتوقيت 3:40.

اللجنة الدولية للصليب الأحمر، «التقنيات الجديدة والحرب». (13)

<https://www.icrc.org/ar/law-and-policy/new-technologies-and-warfare>

اللجنة الدولية للصليب الأحمر، الذكاء الاصطناعي والتعلم الآلي في النزاعات المسلحة: نهج يركز على الإنسان. (14)

<https://international-review.icrc.org/articles/ai-and-machine-learning-in-armed-conflict-a-human-centred-approach-9>

تاريخ الاطلاع 28/02/2026 بتوقيت 13:24.

المنظمة الدولية للشرطة الجنائية (الإنتربول)، «السلطات الإفريقية تفكك شبكات كبرى للجرائم السيبرانية وتوقف أكثر من 1,200 مشتبه به»، بيان صحفي صادر عن الإنتربول، 22 أغسطس 2025. (15)

<https://www.interpol.int/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions>

تاريخ الاطلاع 10/03/2026، ص 21:23.

المنظمة الدولية للشرطة الجنائية (الإنتربول)، «African authorities dismantle massive cybercrime and fraud networks, recover millions»، بيان صحفي، 22 أغسطس 2025. (16)

<https://www.interpol.int/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions>

تاريخ الاطلاع 28/02/2026، بتوقيت 20:05.

مكتب الأمم المتحدة لشؤون نزع السلاح (UNODA)، «الابتكار المسؤول في الذكاء الاصطناعي من أجل السلم والأمن الدوليين». <https://disarmament.unoda.org/responsible-innovation-a> (17)

تاريخ الاطلاع 27/02/2026 21:45.

عادل عبد الصادق، الذكاء الاصطناعي وآفاته المستقبلية، مركز الأهرام للدراسات السياسية والاستراتيجية. (18)

<https://acpss.ahram.org.eg/News/20893.aspx>

تم الاطلاع عليه بتاريخ 23/01/2026. على الساعة 21:16.

خولة الكلاحي، عبد الرؤوف بزيان، الذكاء الاصطناعي والأمن القانوني: الرهانات القانونية في المادة الانتخابية. <https://ciessm.org/2025/03/25/الذكاء-الاصطناعي-والأمن-القانوني>.

بتاريخ 10/01/2026، بتوقيت: 17:13.

## 5. المراجع الأجنبية

- 1) Abraha, Halefom H. "Regulating Law Enforcement Access to Electronic Evidence across Borders : The United States Approach." Information & Communications Technology Law.
- 2) Al Aridi, Alaa. "How Hybrid is Modern Warfare ?"SSRN Electronic Journal.
- 3) Badhan, Deepika & Jagota, Rupam. "Emerging Technologies in Warfare : Legal Challenges for International Criminal Jurisprudence." International Journal of Law.
- 4) Freeman, Lindsay. "The Rome Statute in the Digital Age : Confronting Emerging Cyber Threats." Just Security.
- 5) Gaeta, Paola. "Whose Crime Is It Anyway ? Adapting the Crime of Aggression to Grapple with AI and the Future of International Crimes." Journal of International Criminal Justice.
- 6) Hallevy, Gabriel. Liability for Crimes Involving Artificial Intelligence Systems. Springer International Publishing.
- 7) Hallevy, Gabriel. The Criminal Liability of Artificial Intelligence Entities : From Science Fiction to Legal Social Control. Akron Law Journal.
- 8) Hasan, Mohammad Tarek. "Cross-Border Cybercrimes and International Law : Challenges in Ensuring Justice in a Digitally Connected World." IJRDO Journal of Law and Cyber Crime.
- 9) McKenzie, Simon. "Cyber Operations against Civilian Data : Revisiting War Crimes against Protected Objects and Property in the Rome Statute." Journal of International Criminal Justice.
- 10) Nguyen, Chat Le & Golman, Wilfred. "Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries." Computer Law & Security Review.
- 11) Oimann, Ann-Katrien. "Why Command Responsibility May (Not) Be a Solution to Address Responsibility Gaps in LAWS." Criminal Law and Philosophy.
- 12) Schmitt, Michael N., ed. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.
- 13) Swart, Mia. "Constructing Electronic Liability for International Crimes : Transcending the Individual in International Criminal Law." German Law Journal.

14) Trahan, Jennifer. "The Criminalization of Cyber-operations Under the Rome Statute." *Journal of International Criminal Justice*.

**15)** Verbruggen, Yola. "Cyberattacks as War Crimes." *International Bar Association*.

16) Zaadi Mohamed Djelloul, *Combating Cybercrime in International Law*, *Al-Mi'yâr Journal*, Vol. 30, No. 1 2025

## فهرس المحتويات

## قائمة الفهارس والمحتويات

### مقدمة 3

### الفصل الأول : التطور الحتمي لمفهوم الجريمة الدولية وتحدياتها في ظل التطور التكنولوجي.....6

المبحث الأول: الجريمة الدولية أمام إلزامية التطور المفاهيمي موازاة بالتطور التكنولوجي 8

المطلب الأول: تعريف الجريمة الدولية في ضوء التطور التكنولوجي 8

الفرع الأول: المحددات التقليدية للجريمة الدولية في الفقه والقانون الدولي الجنائي 8

الفرع الثاني: التحولات المستحدثة أثر التطور الرقمي على مفهوم وخصائص الجريمة الدولية 13

المطلب الثاني: الجرائم الدولية الناشئة عن التكنولوجيا 19

الفرع الأول: التحديات القانونية والتعاون الدولي في الجرائم السيبرانية العابرة للحدود 20

الفرع الثاني: أثر تقنيات الذكاء الاصطناعي، الروبوتات، الطائرات المسييرة، والبلوكشين على ارتكاب الجرائم الدولية 22

المبحث الثاني: أركان الجريمة الدولية وتحديات إثباتها في ظل البيئة الرقمية 25

المطلب الأول: بطلان تطور الركن الشرعي وتوسع ماديات الجريمة الدولية 25

الفرع الأول: قصور الركن الشرعي في استبعاد الجرائم التكنولوجية 26

الفرع الثاني توسع الركن المادي للجريمة الدولية بفعل الجرائم التكنولوجية 26

المطلب الثاني: تخبط في إثبات الركن المعنوي والدولي في جرائم بمواصفات آلية 31

الفرع الأول: الإشكالات القانونية في تحديد القصد الجنائي في بيئة الذكاء الاصطناعي 31

الفرع الثاني: القصور في إثبات الركن الدولي للجرائم الرقمية.....35

خلاصة الفصل 37

### الفصل الثاني : محاولة مواكبة القاعدة القانونية الدولية للتجريم والمسؤولية التطور التكنولوجي 38

المبحث الأول: تطور تشريعي ومؤسستي دولي متأخر عن تنامي أنماط الجريمة الدولية في البيئة التكنولوجية 40

المطلب الأول: تطور تشريعي دولي ثقيل في مواجهة الجريمة الرقمية 40

الفرع الأول: تطور قواعد القانون الدولي الجنائي لملاحقة الجرائم الدولية ذات البعد الرقمي 40

الفرع الثاني: حدود التشريعات الدولية الحالية أمام الجرائم الدولية الرقمية 44

المطلب الثاني: آليات مؤسسية دولية تقليدية تواجه جرائم دولية متجددة تكنولوجيا 49

الفرع الأول: دور الأمم المتحدة ومجلس الأمن في توصيف الجرائم الرقمية كتهديد للسلم الدولي 49

الفرع الثاني: دور المنظمات الأمنية الدولية (الإنتربول – اليوروبول) في دعم التحقيق في الجرائم الدولية الرقمية 53

المبحث الثاني: قصور إقرار وتكامل المسؤولية الدولية عن الجريمة الدولية المتطورة تكنولوجيا 57

المطلب الأول: لزوم تطوير إجرائي لإقرار المسؤولية الجريمة الدولي وأثارها 57  
الفرع الأول: طبيعة الأدلة الرقمية وإشكالات أدلة الأقمار الصناعية 57

الفرع الثاني: معايير الإثبات في المحكمة الجنائية الدولية في الجرائم الرقمية المعقدة 59

المطلب الثاني: صعوبة إثبات الجرائم الدولية المرتبطة بالتطور الرقمي 63

الفرع الأول: تحديات تحديد القصد الجنائي في الجرائم الدولية المرتبطة بالذكاء

الاصطناعي 63

الفرع الثاني: إعادة تقييم مبدأ "السيطرة الفعالة" في الهياكل الرقمية المعقدة 66

70 خلاصة الفصل

71 خاتمة

74 قائمة المصادر والمراجع

83 قائمة الفهارس والمحتويات

86 ملخص المذكرة

## ملخص المذكرة

يشهد القانون الدولي الجنائي تحديات متزايدة بفعل التطورات التكنولوجية الحديثة، لا سيما الذكاء الاصطناعي، الأنظمة الرقمية، والفضاء السيبراني، التي أدت إلى ظهور نماذج إجرامية معقدة وعابرة للحدود يصعب التعامل معها عبر الأطر القانونية التقليدية.

وقد أظهر هذا التحول الحاجة إلى مراجعة المفاهيم الأساسية مثل القصد الجنائي، المسؤولية، وآليات الإثبات، خاصة في ظل الجرائم السيبرانية والهجمات الرقمية. كما برزت فجوة بين النصوص الدولية الحالية، مثل نظام روما الأساسي، ومتطلبات الملاحقة القانونية للجرائم الرقمية. وتقر الدراسة بضرورة تطوير إطار قانوني دولي متوازن يعالج هذه التحديات ويضمن فعالية العدالة الجنائية الدولية في العصر الرقمي.

### الكلمات المفتاحية:

الذكاء الاصطناعي، الجريمة الرقمية، المسؤولية الجنائية الدولية، القانون الدولي الجنائي، الإثبات السيبراني.

### Abstract

This study examines how rapid technological advances—especially in artificial intelligence, digital systems, cyber space, and autonomous weapons—have transformed the nature of international crime and challenged traditional frameworks in international criminal law.

It shows that existing legal instruments, such as the Rome Statute, lack explicit provisions to deal with complex digital crimes that transcend borders and traditional models of criminality. The research highlights difficulties in attributing criminal responsibility, proving intent, and admitting digital evidence, and underscores the need for a balanced international legal framework capable of addressing these technological challenges while preserving justice and accountability in the digital age .

### Keywords

international criminal law, digital crime, artificial intelligence, criminal responsibility, cyber evidence.

ale, preuves cybernétiques