آفاق إصلاح القانون الدولي الإنساني في ظل التحديات الرقمية والعولمة الأمنية

Prospects for Reforming International Humanitarian Law in Light of Digital Challenges and Security Globalization

د. هشام بولنوار
أستاذ القانون الدولي بالكلية متعددة التخصصات بآسفي
جامعة القاضي عياض – المغرب

ملخص

يأتي هذا البحث في سياق التحولات العميقة التي يمر بها العالم تحت تأثير الثورة الرقمية والعولمة الأمنية، حيث لم تعد النزاعات المسلحة تقتصر على المواجهات التقليدية، بل انفتحت على مسارح جديدة تقودها التكنولوجيا الجديدة والفضاءات السيبرانية. حيال هذا الواقع المتغير تتسع الحاجة لإعادة النظر في قواعد القانون الدولي الإنساني، فالمخاطر الرقمية وطبيعة الفاعلين الجدد من شركات تكنولوجيا ومجموعات قرصنة عابرة للحدود، تفرض تحديات نوعية لم تكن في حسبان واضعي النصوص القانونية التقليدية.

يحلل البحث أثر التطور التقني المتسارع على بيئة النزاع المعاصر، فيبرز كيف أسهم الذكاء الاصطناعي، والطائرات المسيرة، والهجمات السيبرانية في تقويض الحدود بين الميدانين المدني والعسكري، وتعقيد مهمة حماية الضحايا وتطبيق مبادئ التمييز والحيطة والتناسب. كما يتناول الإشكالات القانونية المستجدة على صعيد الامتثال والمساءلة ومحدودية الأدوات التقليدية في ضبط استخدام القوة الرقمية، ويبحث في مصير القواعد الكلاسيكية أمام عجزها الواضح عن استيعاب التعقيد التشريعي والتقني للنزاعات الراهنة.

الكلمات المفتاحية: القانون الدولي الإنساني _ العولمة الأمنية_ الهجمات السيبرانية_ النزاعات الرقمية_ الإصلاح التشريعي.

Abstract : This research comes in the context of the profound transformations the world is experiencing under the impact of the digital revolution and security globalization, where armed conflicts are no longer limited to traditional confrontations but have expanded into new arenas driven by technology and cyberspace. In light of this changing reality, the need to

reconsider the rules of international humanitarian law is intensifying, as digital risks and the nature of new actors—such as technology companies and transnational hacking groups—pose qualitative challenges unforeseen by the drafters of traditional legal texts.

The study analyzes the effect of rapid technological advancement on the contemporary conflict environment, highlighting how artificial intelligence, drones, and cyber-attacks have undermined the boundaries between civilian and military domains, complicated the task of protecting victims, and challenged the application of principles such as distinction, precaution, and proportionality. It also addresses emerging legal problems regarding compliance, accountability, and the limitations of traditional tools in regulating digital force, and examines the fate of classical legal rules in the face of their evident inability to accommodate the legislative and technical complexity of current conflicts.

Keywords: International Humanitarian Law- Security Globalization- Cyber Attacks- Digital Conflicts- Legislative Reform

مقدمة

يشهد العالم في العقود الأخيرة تسارعا غير مسبوق في مجالات التكنولوجيا الرقمية، تواكبها تحديات أمنية وسياسية تتطلب مقاربات جديدة في فهم النزاعات المسلحة وضبط أدواتها. فلم تعد الحروب مجرد نزاع بين جيوش نظامية تلتزم بقواعد الاشتباك التقليدية، بل تجاوزت حدود المكان والزمان، لتنتقل إلى فضاءات رقمية لا تعترف بالحدود الجغرافية ولا تعترف بالسيادة الوطنية بمعناها التقليدي. في ظل هذا الوضع المضطرب والمتغير، يطرح موضوع إصلاح القانون الدولي الإنساني نفسه كقضية محورية لبناء نظام عالمي أكثر عدالة وإنسانية، قادر على حماية الضحايا من آثار النزاعات الرقمية المعاصرة ورصد التطورات العميقة في هيكلية الحرب وتكنولوجيتها وأبعادها الأخلاقية والقانونية.

السياق العام للموضوع:

برزت ثورة الاتصالات والمعلومات في نهاية القرن العشرين وبداية القرن الحادي والعشرين كعامل رئيسي في إعادة تشكيل مفهوم الأمن الجماعي والدولي، و لم يتوقف تأثير هذه الثورة عند تحسين البنية التحتية للمعرفة والاتصال فحسب، بل وصل إلى قلب الصراعات المسلحة، بحيث باتت الحرب السيبرانية والهجمات الرقمية على المرافق الحيوية جزءا لا يتجزأ من أدوات القوة الحديثة. هذا الواقع العالمي، الذي يجمع بين العولمة الأمنية والتطور التكنولوجي العابر للحدود، يعقد من مهمة التشريع الدولي ويضاعف من الحاجة إلى إصلاح منظومة الحماية القائمة وإعادة تفسيرها لتستجيب لمتطلبات العصر.

السياق الخاص للموضوع:

تتبلور الأهمية الخاصة لهذا الموضوع في ضوء ما يشهده العالم من أزمات متجددة وصراعات تأخذ طابعا مركبا بين التقليدي والحديث. فقد باتت الصراعات المحلية والإقليمية لا تدار فقط بالوسائل العسكرية الكلاسيكية، وإنما أضحت الساحات الرقمية منصات لتبادل الهجمات، وبث التضليل، واستهداف البنى المدنية والسياسية. ويبرز القلق متصاعدا من هشاشة البنية التشريعية الدولية، الوطنية والإقليمية أمام طوفان الابتكارات التكنولوجية، ما يستدعي مراجعة شاملة لأدوات الحماية القانونية وإيجاد منظومة قادرة على الربط بين الآليات الوطنية والاتفاقيات الدولية ضمن إطار تكاملي يكفل أمان الأفراد والمجتمعات.

أهمية الموضوع:

تتأتى أهمية هذا البحث من كونه يتناول واحدة من أكثر الإشكاليات إلحاحا وضرورة في الفكر القانوني والسياسي المعاصر، وهي علاقة القانون الدولي الإنساني بالسياقات الرقمية الجديدة في ظل العولمة الأمنية، حيث تتضاعف هذه الأهمية عند النظر إلى ضعف الإجراءات الرادعة إزاء الهجمات الرقمية، مما يهدد منظومة الحماية الإنسانية برمتها. كما يعكس الموضوع

رهانا جوهريا على قدرة المجتمع الدولي على صياغة تشريعات مرنة قادرة على التكيف مع متغيرات البيئة الأمنية الرقمية والتعامل مع الفاعلين الجدد، سواء كانوا دولا أو كيانات خاصة أو مجموعات غير حكومية، في ساحة معقدة تعيد باستمرار رسم حدود الأخلاق والقانون والسياسة.

أهداف البحث:

ينطلق هذا العمل من جملة أهداف مركزية، أبرزها:

- تحليل السياق الدولي والإقليمي الراهن وبيان أثر العولمة الأمنية والتحول الرقمي على طبيعة النزاعات المسلحة؛
- رصد أهم التحديات التي تواجه القانون الدولي الإنساني في ضوء التطورات التكنولوجية الحديثة؛
- دراسة نقاط القوة والقصور في النظام القانوني الحالي والمعايير المنظمة لحماية الضحايا في النزاعات المعاصرة؛
- تقديم تصورات واقعية حول آليات الإصلاح والتطوير التشريعي، مع إبراز ضرورة التعاون الدولي والتكامل بين المؤسسات القانونية والتقنية؛
- البحث في دور الفاعلين الجدد –منظمات المجتمع المدني، الشركات الرقمية، الهيئات والمنظمات الحقوقية – في صياغة ملامح تشريع مستقبلي أكثر فعالية وإنسانية.

إشكالية البحث:

تكمن الإشكالية الأساسية في مدى قدرة قواعد القانون الدولي الإنساني الراسخة في اتفاقيات جنيف والبروتوكولات الملحقة بها على مواكبة المتغيرات التي فرضتها النزاعات الرقمية. كما تتضح الحاجة إلى تقييم مدى فعالية هذه القواعد في توفير الحماية القانونية الكافية في ظل العولمة الأمنية وتطور أدوات الحرب السيبرانية. هذا الواقع الجديد يستدعي دراسة إمكانية

تعديل أو تحديث النصوص القانونية لتلبية متطلبات الحماية المتجددة. كما يتطلب تصعيد الأطر التشريعية الحالية استجابة للتحديات التقنية والتهديدات العابرة للحدود التي تؤثر في المسارات التقليدية للنزاعات المسلحة. بالتالي، تبرز أهمية بناء منظومة قانونية قادرة على التكيف مع المستجدات دون التفريط في المبادئ الأساسية للقانون الدولي الإنساني.

وينبثق من هذا الإشكال المركزي مجموعة تساؤلات فرعية تتعلق بمدى قدرة النصوص القانونية على استيعاب التقنيات الحديثة وأساليب الهجوم السيبراني، وتوزيع المسؤولية بين الفاعلين التقليديين والجدد، وفعالية إجراءات المحاسبة الدولية وضمان الإنصاف للضحايا، ومدى إمكانية إعادة إنتاج منهجية تشريعية تجمع بين الثبات القيمي والاستجابة العملية للتغيرات التقنية ذات الطابع المتسارع.

أمام هذا التحدي الهيكلي، يقف المجتمع الدولي على مفترق طرق، حيث باتت خيارات الإصلاح إما بالانغلاق ضمن صيغ تقليدية صارت عاجزة عن احتواء الوقائع الجديدة، أو بالانفتاح على ديناميكيات تشريعية مبتكرة تنهض على شراكة وطنية وإقليمية ودولية في إطار استدامة حماية كرامة الإنسان، مهما اختلفت الأدوات واختلفت مسارح النزاع. وبذلك يغدو البحث في آليات الإصلاح والتطوير التشريعي للقانون الدولي الإنساني في عصر العولمة الأمنية والثورة الرقمية ليس مجرد مسألة أكاديمية، بل مسؤولية أخلاقية واستراتيجية لصيانة الأمن الإنساني العالمي بصورة أكثر فعالية وعدلا ومرونة.

المطلب الأول: التحديات الرقمية أمام القانون الدولي الإنساني

شهدت العقود الأخيرة تغيرات جذرية في طبيعة النزاعات المسلحة، بفعل الطفرة التكنولوجية المتسارعة التي طالت مختلف جوانب الحياة، بما في ذلك ميادين القتال ووسائل النزاع. فقد أدى تزايد الاعتماد على الفضاء الرقمي والتكنولوجيا المتقدمة إلى ظهور نماذج جديدة من الحروب، تتجاوز الأشكال التقليدية وتطرح تحديات غير مسبوقة أمام منظومة القانون الدولي

الإنساني. فلم تعد النزاعات تدور فقط في ميادين القتال البرية أو البحرية أو الجوية فحسب، بل امتدت إلى مجالات غير مادية كالهجمات السيبرانية، والذكاء الاصطناعي، والطائرات المسيرة، مما أفرز صعوبات في التمييز بين المدنيين والمقاتلين، وفي تحديد المسؤوليات القانونية عن الأفعال المرتكبة.

وفي هذا الصدد، أصبح من الضروري إعادة التفكير في قدرة القواعد الحالية للقانون الدولي الإنساني على الاستجابة للتعقيدات الرقمية، وعلى حماية الضحايا وضمان احترام المبادئ الإنسانية في ظل واقع تقني متحول. وعليه، يتناول هذا المطلب أبرز التحديات التي تواجه هذا القانون نتيجة الثورة الرقمية، من خلال تحليل أثر التطورات التكنولوجية على بيئة النزاعات (الفقرة الأولى)، وبيان الإشكالات القانونية المرتبطة بالامتثال القانوني في الفضاء الرقمي (الفقرة الثانية).

الفقرة الأولى: أثر التطورات التكنولوجية على بيئة النزاعات المسلحة

شهدت العلاقات الدولية والتحولات الجيوسياسية خلال العقود الأخيرة طفرة تكنولوجية غير مسبوقة، انعكست بعمق على طبيعة النزاعات المسلحة ومحدداتها وأدواتها. إذ لم تعد الحروب الحديثة تندرج ضمن نموذج المواجهة التقليدية بين جيوش نظامية في ميادين واضحة للقتال، إنما تحولت إلى منظومة ديناميكية شديدة التعقيد تغزو الحدود الافتراضية والمادية معا وتعيد رسم سياق الصراع وفق متغيرات رقمية متسارعة. و هكذا فإن فهم ماهية النزاع المعاصر أصبح رهينا بمواكبة أثر الثورة الرقمية على إطار العمليات العسكرية، وكيفية إدارة مخاطرها، وإعادة تفسير مكانة الضحية والأطراف الفاعلة، وعلاقة ذلك كله بمنظومة القانون الدولي الإنساني التي لم تكن قوانينها التقليدية معدة لمثل هذا التغير العميق والمتعدد الأوجه.

الثورة الرقمية وتوسع ميدان النزاع

أفضت الطفرات المتلاحقة في تكنولوجيا المعلومات والاتصالات إلى انفتاح جبهات النزاع على الفضاء السيبراني[307]، فلم تعد الحرب تقتصر على البر والبحر والجو، بل باتت تدور رحاها كذلك على الإنترنت ومنصات البرمجيات الرقمية وشبكات الحوسبة السحابية. فقد أصبح التخطيط العسكري وتنفيذ العمليات الهجومية والدفاعية يعتمد بشكل متزايد على البيانات الضخمة، والذكاء الاصطناعي، ومحاكاة الأحداث، والتلاعب بمعايير التشفير وتدفق المعلومات. كل ذلك أفرز ذلك نوعا جديدا من النزاعات يسمى بالحروب السيبرانية، حيث أصبح ممكنا مهاجمة البنية التحتية الأساسية للدول — الطاقة، الاتصالات، البنوك، المواصلات والمرافق الصحية — دون تحريك جندي واحد فعليا في الميدان[308].

من هذه الزاوية الجديدة، يصبح تحديد مسرح العمليات وضبط المشاركين الفعليين وتشخيص أثر الهجمات أكثر تعقيدا وأوسع نطاقا، وهو ما يضع القانون الدولي الإنساني أمام تحديات مفصلية في تعريف دائرة الحماية القانونية وإثبات الصفة المدنية أو العسكرية للأهداف، خاصة حين يتعذر التمييز بين الاستخدام المدني والعسكري للمنشآت الرقمية في ظل ما يعرف بازدواجية التكنولوجيا الحديثة[309].

الذكاء الاصطناعي وإعادة تعريف القرار العسكري

لم يكن للخيال البشري أن يتوقع خلال سنين معدودة تسليم زمام القرارات القتالية إلى أنظمة برمجية قادرة على التعلم والتطور ذاتيا؛ أنظمة تتخذ قرارات القتل أو التدمير خلال أجزاء من

---

307 الفضاء السيبراني يعرف بأنه الوسط أو المجال الافتراضي الذي تتواجد فيه شبكات الحاسوب ويتم من خلاله التواصل الإلكتروني ومختلف الأنشطة الرقمية. يشمل هذا المجال كل ما يتعلق بالأنظمة الحاسوبية مثل أجهزة الكمبيوتر، شبكات الاتصالات، البرمجيات، البيانات المخزنة والمتبادلة، ومستخدمي هذه التكنولوجيا، ويستخدم لتسهيل التفاعل ونقل المعلومات بين الأفراد والمؤسسات عبر شبكة الإنترنت وغيرها من الوسائل الإلكترونية.

308 العذبة فهد حمد، "استشراف أثر التطور التكنولوجي في الحروب الحديثة والقوة العسكرية للدول الصغرى"، **استشراف للدراسات المستقبلية**، المركز العربي للأبحاث ودراسة السياسات، العدد السابع، ديسمبر 2022، ص: 217

309 الخفاجي خالد علي و آخرون، "القانون الدولي الإنساني والتحديات المعاصرة"، **المجلة المغربية للإدارة المحلية والتنمية**، العدد 158، 2021، ص: 223

الثانية بعيدا عن التدخل البشري المباشر. ففي الحروب الحديثة، بات الذكاء الاصطناعي يشكل عصبا محوريا لآليات جمع وتحليل البيانات الميدانية، وتقدير حجم ونوعية التهديدات، وتطوير أنظمة الدفاع والهجوم الإلكتروني بشكل لم يسبق له مثيل.

هذا التحول أعاد طرح أسئلة في غاية الأهمية حول مدى إمكان التزام الأنظمة الذكية بـ"مبادئ التمييز" و"التناسب" و"الاحتراز" المنصوص عليها في اتفاقيات جنيف والقانون الدولي الإنساني.[310] فهل تستطيع أنظمة الذكاء الاصطناعي التمييز حقا، في ظروف الحرب الحقيقية، بين مقاتلين ومدنيين أو بين الأهداف العسكرية والمستشفيات؟ هل تأخذ هذه الأنظمة القرارات وفق القيم الإنسانية أم وفق خوارزميات تستند إلى معايير الإحصاء المجرد، بغض النظر عن البعد الأخلاقي؟ حتى اللحظة، لا يملك الذكاء الاصطناعي الحس الأخلاقي الذي يمتلكه الإنسان، ولا يقدر على تقدير جملة الظروف الإنسانية المحيطة بالهدف المستهدف.

الهجمات السيبرانية وعدم وضوح الخطوط الحمر

من أخطر مظاهر تأثير التكنولوجيا على النزاعات المسلحة يبرز تصاعد عمليات الاختراق والاعتداء على المنظومات الرقمية للدول والمؤسسات، في ما يصطلح على تسميته بالحرب السيبرانية. فقد أصبحت هذه الهجمات وسيلة فعالة لإلحاق ضرر استراتيجي بالعدو، سواء عبر تعطيل أنظمة الدفاع والمراقبة أو شل شبكات الطاقة والنقل أو حتى السيطرة على بيانات الدولة ونشرها والإضرار بسمعتها وتعطيل قطاعات كاملة من الاقتصاد الوطني[311].

لذلك، فقد امتلأ سجل النزاعات الحديثة بحوادث الهجمات السيبرانية التي استهدفت محطات الكهرباء ومصادر المياه والمستشفيات، وأحيانا مراكز الأبحاث النووية أو الأنظمة المصرفية للدول مما أدى إلى شلل اجتماعي أو اقتصادي مؤقت بل وأحيانا كارثي. فخطورة هذه الهجمات

---

[310] أبو حصوة باهي شريف، "التنظيم القانوني للذكاء الاصطناعي وفقا لأحكام القانون الدولي بشأن حقوق الإنسان"، **مجلة البحوث القانونية والاقتصادية**، العدد الرابع، المجلد 60، أكتوبر 2024، ص: 139

[311] سعود يحيى ياسين، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، **المجلة القانونية**، العدد الرابع، 2018، ص: 88

لا تكمن في مدى التدمير المادي فقط، بل في فشل الأنظمة التقليدية للقوانين في رصد الفاعل أو تحميله المسؤولية، إذ غالبا ما يكون المهاجم مجموعة مجهولة الهوية، أو جهة غير حكومية بعيدة جغرافيا عن مسرح الأحداث، أو حتى مجموعات قرصنة تدير عملياتها من خارج الحدود الوطنية للخصمين[312].

هذا الواقع ألحق بالبيئة القانونية الحربية ضبابية شديدة، جعلت من التحقيق في أسباب الانهيار التقني أو تعطل البنى الأساسية أمرا بالغ الصعوبة، وزادت من التكلفة الإنسانية على المدنيين الذين أصبحوا فجأة في قلب العاصفة الإلكترونية حتى دون قصدهم أو تخطيطهم لذلك.[313]

الطائرات بدون طيار: تحولات في قواعد اللعبة

شكل ظهور الطائرات المسيرة (الدرونز) علامة بارزة في نقل الصراع من أرض الواقع إلى سماء التقنية الرقمية، فقد استخدمت هذه الطائرات بكثافة في النزاعات المعاصرة لما تمنحه من قدرة على المراقبة الدقيقة وشن الضربات محددة الأهداف مع تقليص المخاطر البشرية للقوات المهاجمة. لكن هذه الميزة التقنية حملت معها أيضا إشكاليات قانونية وأخلاقية بالغة التعقيد[314].

وغالبا ما تعتمد عمليات الطائرات المسيرة على تحاليل بيانات ضخمة وجمع معلومات استخبارية من الفضاء الرقمي، وقد تؤدي الأخطاء في المعطيات المستخدمة أو عدم اكتمالها

---

312 السعيد عادل عبد الله، "الهجمات السيبرانية وأثرها على الأمن القومي... دراسة تحليلية في ضوء القانون الدولي"، مجلة الحقوق والعلوم الإنسانية، جامعة نايف العربية للعلوم الأمنية، عدد 41 ،2020، ص: 163

313 في 28 أبريل 2025، وقع انقطاع كهرباء ضخم شمل شبه الجزيرة الإيبيرية (إسبانيا والبرتغال)، واستمر لنحو عشر ساعات في معظم المناطق، وتسبب في تعطيل الخدمات الحيوية بشكل كبير. انقطع التيار الكهربائي عن ملايين الأشخاص، وتوقفت إشارات المرور، وتعطلت شبكات الهاتف المحمول، واضطرت مستشفيات إلى العمل بمولدات احتياطية، كما أشارت تقارير إلى وفاة ما لا يقل عن سبعة أشخاص بسبب حوادث مرتبطة بالانقطاع

314 المشاقبة محمد صلاح الدين، "أثر التطور التكنولوجي العسكري على النزاعات الدولية"، **اتجاهات سياسية**، المركز الديمقراطي العربي، العدد الثالث و العشرون، يونيو 2023، ص: 267

إلى استهداف مدنيين أو بنى تحتية غير عسكرية بمبررات "استخباراتية". ومن هنا، يتضح أن الاعتماد المكثف على البيانات الاستخباراتية، مع ما قد يشوبه من قصور أو أخطاء، يقود بدوره إلى توسع دائرة الاستهداف الجغرافي، فالأهداف لم تعد محصورة في مسرح عمليات تقليدي، بل قد تستهدف غارة بطائرة مسيرة شخصا أو منشأة في بلد لم يدخل في نزاع مسلح مباشر، مما يثير إشكاليات سيادية وقانونية عميقة.

تآكل خطوط التمايز بين المدني والعسكري

دخلت تكنولوجيا المعلومات والاتصال في هيكلية كل مناحي الحياة اليومية، من التعليم إلى الصحة، ومن الخدمات المصرفية إلى البنية التحتية. هذا التشابك عزز من صعوبة التمييز بين الأهداف المدنية والعسكرية ولاسيما عند استخدام تقنيات مزدوجة الغرض توظف للسلام والحرب معا. فلم يعد من الممكن أحيانا تحديد متى يتحول النظام الرقمي من أداة خدمية تخدم المواطن إلى هدف عسكري شرعي في نظر الأطراف المتصارعة[315].

ويظهر الإشكال جليا عند الهجوم على مؤسسات اتصالات أو مزود خدمة إنترنت يمتلك قاعدة عملاء مدنيين لكنه يقدم دعما لوجستيا أو استخباراتيا للقوات المسلحة. في تلك الحالة يكون الضرر غير مباشر وواسع النطاق، ويسفر غالبا عن معاناة آلاف المدنيين وفقدانهم مقومات الحياة اليومية – وهي معاناة يصعب تبريرها أخلاقيا وقانونيا.

الإعلام الرقمي والتأثير على ديمومة النزاع

دخل الإعلام الرقمي، ووسائل التواصل الاجتماعي خصوصا، كعنصر محوري في النزاعات المسلحة الراهنة. يوظف هذا الفضاء في شحن الرأي العام، والتلاعب بالعواطف والمعلومات، وترويج سرديات متضادة عن مجريات النزاع. وتتحول الأخبار والصور والفيديوهات أحيانا إلى أداة للحرب النفسية، أو ذريعة لتبرير انتهاكات وتجاوزات ضد القواعد الإنسانية.

315 العذبة فهد حمد، "استشراف أثر التطور التكنولوجي في الحروب الحديثة والقوة العسكرية للدول الصغرى"، مرجع سابق، ص: 229

فقد أصبحت عمليات التضليل الإعلامي والتلاعب بالحقائق أو فبركة الأدلة بأنظمة الذكاء الاصطناعي، آلية جديدة للتأثير على سير العمليات ولتشتيت الرأي العالمي أو نزع الشرعية عن خصم ما. هذه البيئة الإعلامية المتوترة تقوض ثقة الشعوب بالقانون الدولي الإنساني وتضعف من مكانته كمرشد أخلاقي وحقوقي أثناء النزاعات[316].

كل هذه التغيرات التقنية فرضت على القانون الدولي الإنساني مراجعة دائمة للمفاهيم الجوهرية التي يستند إليها، إذ باتت المعايير الكلاسيكية مثل التمييز، والتناسب، والمسؤولية، والضرر الجانبي، بحاجة لتفسير موسع يتلاءم مع التعقيد الرقمي والحرب الفضائية. فلم لم يعد تحديد المسؤولية القانونية عن جرم حرب معلوماتية مسألة يسهل الحسم بها، لذلك قد يكون الفاعل دولة أو جهة غير حكومية، أو حتى مجموعة من الأفراد المنتشرين على عدة قارات[317].

و ترد في هذا السياق مشكلات الإثبات القانوني: كيف يمكن البرهنة على نية استخدام برنامج ضار أو تثبيت مسؤولية المسؤول العسكري أو المبرمج إذا انتهكت حقوق الإنسان بواسطة نظام ذاتي التشغيل؟ كيف يمكن مساءلة التحالفات العسكرية الرقمية غير المعلنة؟ هذه التساؤلات وغيرها تفتح المجال أمام اجتهادات قضائية وتشريعية متنوعة في النظم القانونية والعرف الدولي، وتعيد تسليط الضوء على أهمية تعاون جميع الفاعلين القانونيين والمبرمجين والخبراء وصانعي القرار لوضع قواعد جديدة تلائم هذا التطور الكبير.

الفقرة الثانية: إشكالات الامتثال القانوني في الفضاء الرقمي

شهد الفضاء الرقمي في العقدين الأخيرين تحولات عميقة طالت معظم مناحي الحياة الإنسانية، وامتدت آثارها إلى ميادين النزاع والقانون الدولي الإنساني. إذ يعكس التفاعل القانوني مع البيئة

316 أبوزيد حنان أحمد الفويل. "تحديات التضليل الرقمي للقانون الدولي الإنساني"، **مجلة روح القوانين**، العدد 106، أبريل 2024، ص: 207

317 العيسى طلال ياسين وعدي محمد عناب، "المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، **مجلة الزرقاء للبحوث والدراسات الإنسانية**، المجلد 19، العدد الأول، 2019، ص:87

الرقمية تداخلا معقدا بين قوى تقنية صاعدة، وفاعلين جدد في مشهد الصراع، وقواعد قانونية تم تصميمها لبيئات حربية مادية تقليدية. فقد أصبح الامتثال القانوني في مواجهة النزاعات الرقمية أمرا إشكاليا يطرح مسائل عميقة تتعلق بحدود التعريف والسيطرة، وإثبات النية والمسؤولية، والشفافية والمحاسبة، فضلا عن قدرة المجتمع الدولي على مواكبة السرعات التي تمليها روح العصر.

تعددية الفاعلين وحدود التنظيم القانوني

يمثل اتساع الفضاء السيبراني من الناحية الجغرافية والانسيابية الرقمية تحديا محوريا للامتثال القانوني. فالنزاعات المعاصرة باتت تضم أطرافا فاعلة غير تقليدية مثل مجموعات القرصنة الإلكترونية، والشركات العسكرية الخاصة، وتنظيمات إرهابية عالمية، إضافة إلى الدول الفاعلة نفسها. ويتمتع هؤلاء اللاعبون بمستوى عال من المرونة والتخفي، ما يجعل رصد سلوكهم ومساءلتهم عملية مشوبة بالصعوبات.

ويطرح ذلك سؤالا حول مدى انطباق قواعد القانون الدولي الإنساني على هذه الأطراف، حيث أن العديد منها لا تعترف أصلا بالاتفاقيات الدولية أو لا تخضع لسلطة الدول الوطنية. ومع غياب سلطة مركزية أو منظومة رقابية فعالة في الفضاء الرقمي، كثيرا ما تبقى الانتهاكات خارج نطاق المحاسبة، في غياب آليات توثيق فعالة أو إجماع على معايير الإثبات المطلوبة[318].

غموض المفاهيم القانونية في البيئة الرقمية

لم تأت قواعد القانون الدولي الإنساني على ذكر مصطلحات مثل "الهجمات السيبرانية"، أو "الرموز البرمجية الخبيثة"، أو "الذكاء الاصطناعي القتالي"، وهو ما يفرض حالة من الغموض الدلالي جعلت من تفسير هذه الوقائع تحديا لمجتمع القانونيين والقضاة. فكيف يمكن تكييف

318 عبدالغني أمل عمرو، "القانون الدولي الإنساني والحرب السيبرانية في النزاعات المسلحة غير الدولية: الأطر القانونية والتحديات"، **مجلة الحقوق والمنظومات القانونية**، المجلد 35، العدد 44، 2023، ص: 560

واقعة اختراق نظام تشغيل المستشفى الوطني خلال أزمة نزاع مسلح بناء على قواعد وضعت للعمليات العسكرية الكلاسيكية؟

إن غياب تعريفات موحدة وواضحة يجعل من الصعب تصنيف الأفعال الرقمية ضمن جرائم الحرب، أو حتى تحديد متى تبدأ الحرب السيبرانية ومتى تنتهي. ففي حين تعتبر بعض الدول الهجمات الرقمية وسيلة من وسائل الصراع دون الحاجة إلى إعلان حرب تقليدية، ترى أخرى أنها أعمال عدائية موجبة لتطبيق القانون الدولي الإنساني بكامل نصوصه. هذا التناقض يدفع إلى أزمة في معايير الإعلان عن النزاع وتفاصيل الحقوق والواجبات الناشئة عنه[319].

التعقيدات التقنية والمساءلة القانونية

تستغل بعض الجهات التقدم التقني لتحقيق مستوى عال من التخفي والتمويه، سواء عبر استخدام الشبكات المظلمة، أو تقنيات إخفاء الهوية، أو توجيه الهجمات من منصات جغرافية متعددة. هذا الواقع يضع المجتمع الدولي أمام معضلة في تحديد الجهة المسؤولة عن الهجوم، إذ يمكن ارتكاب جريمة رقمية من عدة أطراف تتوزع مسؤوليتها القانونية في أكثر من إطار قضائي وسيادي، وقد يشترك فيها أفراد من دول لا تربطهم علاقة مباشرة بالنزاع الأصلي[320]. وتكمن صعوبة أخرى في إثبات النية الجنائية وراء الفعل الرقمي، فمثلا قد يهاجم نظام برمجيات ضار مؤسسة صحية، لكن إثبات أن الفاعل استهدف المدنيين عمدا أو عرف مسبقا بنتائج الهجوم على السكان يظل صعبا في غياب أدلة رقمية دامغة. هذا يجعل من بناء القضايا في المحاكم الدولية أمرا معقدا ويقلل من فاعلية آليات الردع القائمة.

---

319 اللجنة الدولية للصليب الأحمر، "بعد عشرين عاما: القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية أثناء النزاعات المسلحة، **المجلة الدولية للصليب الأحمر**، العدد 913، مارس 2021، على الرابط (تاريخ التصفح: 26 يوليوز 205):
https://international-review.icrc.org/ar/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber?utm_source=chatgpt.com

320 رمضان شريف عبد الحميد، "الحرب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني"، مجلة **جامعة الطائف للعلوم الشرعية والقانونية**، المجلد 23، العدد 4، يونيو 2021، ص. 3070

هشاشة آليات الرصد والتحقيق

تقليديا، تعتمد آليات التحقيق في جرائم الحرب على شهود العيان، وتقارير المراقبين الميدانيين، والأدلة الملموسة. إلا أن الفضاء الرقمي خلق بيئة سرية تتحلل فيها الأدلة بسرعة، وتستخدم فيها أدوات تدمير الذات البرمجي، مما يجعل بعض البصمات والتقارير الرقمية زائلة أو غير قابلة للاحتفاظ بها. حتى عندما تكتشف الأدلة قد تواجه تحديات قانونية في قبولها بالمحاكم بسبب احتمالية التلاعب أو التشكيك في مصدرها الرقمي[321].

كما أن تعدد المواقع الجغرافية للخوادم والبيانات يجعل من ممارسة السلطات القضائية ومذكرات التتبع والتحري مسألة أكثر تعقيدا في ظل اختلاف القوانين الوطنية حول الخصوصية، المعطيات الرقمية وحرية المعلومات. ينعكس ذلك على الثقة في نتائج التحقيق ويمنح المهاجمين حصانة مؤقتة تعود عليهم بالفائدة في غياب تعاون دولي وثيق ومنظومة مشتركة لمكافحة الجرائم الرقمية[322].

إشكالية الهويات الرقمية والفاعلين غير المعروفين

في النزاعات الرقمية، يتخذ كثير من الفاعلين هويات زائفة أو يعملون ضمن مجموعات غير مركزية تشبه الشبكات الفوضوية، يصعب تصنيف أعضائها قانونيا أو حتى فهم منهجيات عملها وأهدافها السيادية أو السياسية. يؤدي هذا التشتت البنيوي إلى حالة من سيولة المسؤولية، إذ لا يمكن الركون إلى القوالب التقليدية المتعارف عليها مثل الدولة، الجهة المانحة، أو القائد العسكري[323].

---

321 طلبية بسام، **"إثبات الجريمة المعلوماتية أمام القضاء"، مجلة الشريعة والقانون**، جامعة الإمارات، عدد 75، 2019، ص: 470

322 Margaret L. Satterthwaite, "Digital Evidence and the Prosecution of Human Rights Abuses," **Journal of International Criminal Justice** , no, 3, 2016,P: 528

323 Michael N. Schmitt, ed., **Tallinn Manual on the International Law Applicable to Cyber Warfare ,** Cambridge University Press, 2013,P : 26

وغالبا ما تستهدف الهجمات الرقمية بنى تحتية مشتركة تخدم المدنيين والعسكريين معا، ما يعقد من توصيف الانتهاكات وإثبات طبيعتها غير المشروعة بحكم القانون الدولي الإنساني. وفي هذا السياق، يطفو النقاش الدولي حول ضرورة تطوير معايير جديدة لتحديد المسؤولية الجماعية والفردية في الفضاء الرقمي، وكيفية فرض الجزاء وفرض قواعد الحماية الإنسانية خارج الأطر التقليدية للسيادة والدولة الوطنية.

الهجمات الرقمية على الأهداف المدنية

مثلت الهجمات السيبرانية على المستشفيات والمنشآت الطبية، ومحطات الطاقة، وشبكات المياه والدعم اللوجستي الإنساني مثالا صارخا على التحديات التي يواجهها القانون في الفضاء الرقمي.[324] وغالبا ما تبدأ تلك الهجمات كنتيجة جانبية أو "ضرر جانبي" للحملات العسكرية الرقمية، ما يعيد طرح قضية مبدأ التناسب والتمييز التي يستوجبها القانون الدولي الإنساني. فكيف يمكن تقدير الأضرار المدنية المستقبلية جراء نشاط برمجي قد يظل خامدا أو ينتشر بعد شهور من إطلاقه الأصلي؟

في هذا السياق، تتفاقم مسؤولية الأطراف العسكرية للحفاظ على أرواح المدنيين، كما يتسع الجدل حول مدى شرعية استهداف بنى تحتية تخدم السكان خلال النزاع، بغض النظر عن علاقاتها العسكرية، خاصة إذا كان العنصر الرقمي أساسيا في تشغيلها واستدامتها.

حدود القانون في مواجهة التقنيات سريعة التطور

تتميز صناعة تقنية المعلومات بسرعة فاقت جميع المجالات الأخرى، لا سيما في أساليب تطوير البرمجيات الخبيثة، وأدوات التسلل والتضليل، ومنهجيات التشفير، ومزايا الذكاء الاصطناعي المتقدم. هذه الوتيرة المتسارعة جعلت من التشريع والتحديث القانوني سباقا غير متكافئ مع الواقع التقني. فغالبا ما تكون التعديلات التشريعية بطيئة، صعبة التنفيذ، أو غير قادرة على استشراف المخاطر المستقبلية، مما يخلق فراغا في الحماية القانونية.

---

324 ميساء الفضلي وخالد المحمود، "تحديات حماية البنية التحتية المدنية أثناء النزاعات السيبرانية"، **مجلة الحقوق**، جامعة الكويت، مجلد 45، العدد الثاني، 2021، ص: 217

علاوة على ذلك، يواجه واضعوا القوانين تحديات تتعلق بكيفية المواءمة بين التطورات التقنية ومتطلبات الشفافية والخصوصية، وضمان عدم التحول إلى تشديد رقابي مفرط ينتقص من حرية الاتصال الرقمي المشروعة أو يفتح الباب لانتهاكات خصوصية المستخدمين[325].

السياسات الدفاعية والشرعية الاستباقية

تحت ذريعة "الدفاع الرقمي الاستباقي"، بررت بعض الحكومات استخدام عمليات رقابية أو هجومية مسبقة ضد أهداف رقمية داخل وخارج حدودها. ويشكل ذلك جدلا حول مدى إباحة الأعمال الاستباقية ومدى توافقها مع القانون الدولي والقيود الأخلاقية. كما تطرح عمليات الحجب والهجمات الوقائية مسألة ما إذا كانت تلك الردود مبررة قانونيا أو تعد انتهاكا لحقوق وسيادة الدول والأفراد المستهدفين[326]. أضف إلى ذلك، أن بعض الدول تستخدم مبدأ "القدرة على الردع السيبراني" كتكتيك دبلوماسي أو سياسي، ما يتسبب في تصاعد السباق الرقمي العسكري ويخلق توترات إضافية في العلاقات الدولية.

المطلب الثاني: آفاق تطوير القانون الدولي الإنساني في ظل العولمة الأمنية

لم تعد النزاعات المسلحة اليوم محصورة في الميدان العسكري التقليدي، بل باتت تعكس منظومة متشابكة من التهديدات الرقمية والمخاطر العابرة للحدود، في سياق أوسع يعرف بـ"العولمة الأمنية". هذا التحول العميق في طبيعة النزاعات، وتزايد الاعتماد على التكنولوجيا والفضاء السيبراني، كشف عن حدود القواعد الكلاسيكية التي تأسس عليها القانون الدولي الإنساني، وأظهر الحاجة الملحة إلى مراجعة شاملة لمفاهيمه وآلياته بما يستجيب للواقع المتغير.

إزاء هذا الوضع، برزت أسئلة جديدة تتعلق بمدى ملاءمة القواعد القائمة لحماية الإنسان، وضمان المساءلة القانونية في زمن الرقمنة، الذي يشهد تآكلا في وضوح المسؤولية القانونية وتوسعا في الفاعلين غير الحكوميين، إضافة إلى صعوبة الإثبات في الجرائم الرقمية.

---

325 الدغيثر عبد العزيز بن سعد، **الحماية القانونية ضد الجرائم الإلكترونية**، مكتبة العبيكان، الرياض، 2020، ص: 141

326 عودة إياد، **"مبدأ الدفاع الشرعي في الفضاء السيبراني: رؤية قانونية"، مجلة العلوم القانونية والاقتصادية**، جامعة عين شمس، عدد 47، 2021، ص: 64

وعليه، يناقش هذا المطلب آفاق إصلاح القانون الدولي الإنساني عبر محورين أساسيين: أولهما مراجعة القواعد والمعايير القانونية الحالية ومدى استجابتها لتحولات الواقع الأمني والتقني (الفقرة الأولى)، وثانيهما استكشاف إمكانيات التعاون الدولي وآليات التحديث التشريعي الكفيلة بجعل نصوص القانون الدولي الإنساني أكثر فعالية وقدرة على مواجهة التحديات الرقمية (الفقرة الثانية).

الفقرة الأولى: مراجعة القواعد والمعايير القانونية الحالية

شهد القانون الدولي الإنساني منذ نشأته مراحل تحول متلاحقة واستجابات متعددة لتعقيدات الواقع السياسي والتكنولوجي الجديد، والتي فرضت تطويرا مستمرا لقواعده ومعاييره. وقد كان من بين أبرز هذه التحولات تنامي ظاهرة العولمة الأمنية، وما نتج عنها من تحديات غير مسبوقة تمس جوهر حماية الإنسان وتحديد المسؤولية القانونية في النزاعات المعاصرة. وبدا أن الرقمنة والذكاء الاصطناعي والجريمة السيبرانية ليست مجرد إضافات على مشهد الصراع التقليدي، بل مكونات جوهرية تستدعي مراجعة جذرية شاملة لكل منظومة الحماية القانونية على المستوى الدولي[327].

منذ أن تأسست اتفاقيات جنيف عام 1949 وما تبعها من بروتوكولات، رسم القانون الدولي الإنساني صورة معيارية لحماية المدنيين خلال النزاعات المسلحة، مستندا إلى وضوح نسبي في تصنيف الفاعلين والتمييز الدقيق بين المدنيين والمقاتلين، وارتباط الأعيان المدنية والعسكرية بجغرافيا النزاع وزمنه. غير أن العقود الأخيرة شهدت تحولات جذرية غيرت ليس فقط في طبيعة النزاعات المسلحة، بل في ماهية التهديد ذاته، وأدواته، ووسائطه، الأمر الذي فرض إعادة النظر في مدى انسجام القواعد القائمة مع التحديات بما يكفل الحفاظ على الإنسان كقيمة مركزية عند اشتداد النزاع[328].

---

327 فياله محمود، **"القانون الدولي والتحديات المعاصرة: الجريمة السيبرانية نموذجا"، مجلة الإسكندرية للدراسات القانونية**، العدد 12، 2024، ص 150

328 Reda El Mawy, *'*The Changing Nature of Armed Conflict and International Humanitarian Law," **International Review of the Red Cross**, *101 (2019),*

ولا يمكن تقييم مدى ملاءمة القانون الإنساني للراهن الدولي إلا بفهم تعقيد المشهد الأمني المستجد، حيث تصاعدت الحروب السيبرانية والهجمات المعلوماتية، وأضحى الذكاء الاصطناعي فاعلا حقيقيا يشارك في اتخاذ القرارات الهجومية.[329] بل لم يعد مسرح الحرب مقتصرا على خطوط الاشتباك التقليدية، فقد امتد إلى الفضاء الرقمي الذي يعجز عن إدراك حدوده الزمنية والجغرافية أي إطار قانوني كلاسيكي، وأفرز هذا التغير انتقال أمن الأفراد والمجتمعات من المفهوم الدفاعي التقليدي إلى ضرورة الحماية في فضاء غير مادي، سريع التحول، يختلط فيه المدني بالعسكري، وتغيب فيه أحيانا الرؤية حول طبيعة الفاعلين، وهويتهم ومسؤولياتهم القانونية.

برزت، على هذا الأساس، معضلات فكرية وتطبيقية حول جوهر قواعد القانون الدولي الإنساني، وأهمها التمييز بين المدني والمقاتل، والتناسب في استخدام القوة، وتوزيع المسؤولية عن الأضرار. فالمنشآت الطبية والتعليمية والمصرفية التي شكلت لعقود ممتلكات محمية بموجب نصوص الحماية الإنسانية أضحت اليوم بنى تحتية مزدوجة الاستخدام؛ يقدم اختراقها الرقمي خدمة مباشرة للقدرات العسكرية، ما يخلق حالة من التشابك بين الضرورة العسكرية وقيمة الحماية الإنسانية، وزاد من فجوة الحماية عجز الأجهزة القانونية عن إثبات النية أو كشف الفاعل الحقيقي في العمليات الرقمية، إذ تتوزع الأدوار بين الدولة، والجهات الخاصة، وقراصنة مستقلين، وشبكات غير حكومية، يضاف لذلك تفوق الفضاء السيبراني في ملاحقة الضحايا عبر الحدود، وإخفاء هوية المعتدي[330].

---

p: 1053.
https://international-review.icrc.org/articles/changing-nature-armed-conflict-and-international-humanitarian-law-irrc-no-913 (27.07.2025)

329 Dapo Akande and Emanuela Gillard, "Cyber Operations and the Use of Force in International Law," **International Law Studies**, Vol. 97, (2021), P: 310

330 Peart, Isabelle. “Digital Safe Havens: Shelter Civilians from Military Cyber Operations.” **Humanitarian Law & Policy Blog**. International Committee of the Red Cross. July 1, 2021. https://blogs.icrc.org/law-

ويفرض الواقع الرقمي كذلك إشكاليات على بناء أساس المسؤولية الجنائية الدولية، حيث تتعذر ملاحقة الجناة أحيانا بسبب غياب اتفاقيات ملزمة للتعاون العابر للحدود، وتباين القوانين الوطنية بشأن الجريمة السيبرانية، ووجود مناطق رمادية يستحيل فيها الجزم بالمخالفات القانونية وفق نصوص اتفاقيات جنيف والبروتوكولات المكملة لها. وزادت حدة الأمر مع بروز ظواهر التضليل الرقمي، وحملات التشويش المعلوماتي، واستغلال منصات التواصل الاجتماعي لتبرير انتهاكات القانون الدولي الإنساني أو التغطية عليها، بل وأحيانا تحويل الرواية عن مسار الانتهاكات لصالح المعتدي[331].

بالإضافة إلى التهديدات التكنولوجية، أفرزت العولمة الأمنية اختلالات هيكلية في مفهومي السيادة وحدود المسؤولية، إذ لم تعد الحروب الحديثة تنحصر داخل حدود الدولة بل غدت مناطق الصراع عابرة للحدود ومطبوع عليها الطابع الدولي، حتى وإن ظلت غير معلنة رسميا. وقد أدى هذا التغير إلى تجاوز الرقابة القانونية المفروضة على النزاع التقليدي، وأصبح التصدي للهجمات الرقمية أو الردع الاستباقي ساحة مفتوحة للاجتهادات الوطنية، في غياب معايير دولية محددة تجتهد في ضبط القيد الأمني وتوازناته مع كفالة الحماية الإنسانية[332].

و على هذا النحو، تتجلى أزمة القواعد التقليدية حين تتعرض لمحيط النزاعات الرقمية التي لا يسهل فيها تصنيف العمل العدائي، ولا حتى تعريف الأطراف المسؤولة بسهولة، خصوصا في ظل اتساع استخدام الذكاء الاصطناعي في نظم الأسلحة والقيادة، وتوزع الأدوار بين الأنظمة البرمجية والمستخدم النهائي وصانع القرار العسكري. يظهر السؤال الحيوي هنا: من يتحمل

---

and-policy/2021/07/01/civilians-military-cyber-operations (28/07/2025)

[331] أبو المجد عبد الرحمن، **الجريمة السيبرانية وتحديات الإثبات الرقمي**، دار الفكر الجامعي، القاهرة، 2022، ص: 222

[332] Assaf Alaa**n,** "Violations of Sovereignty in 'Cyberspace' Under the United Nations Charter"**, HSE University Journal of International Law 10,** no. 1 (2023), p :22

المسؤولية القانونية؛ مطور البرنامج، أم الدولة، أم المستخدم العسكري؟ وتزداد إشكالية النية الجنائية عندما تتخذ القرارات على أساس عتبات خوارزمية أو تعليمات مسبقة البرمجة قد لا يمكن تتبعها بعد التنفيذ.

تشير بعض الدراسات الأكاديمية إلى أن التطور التقني الذي اكتسح المجال العسكري والمدني لم يواكبه تعديل في قواعد القانون الدولي الإنساني بذات السرعة أو العمق المطلوبين، بل اقتصر غالبا على اجتهادات من هيئات خبراء أو نصوص إرشادية تفتقد لطابع الإلزام والقبول الدولي الواسع. وأسهم هذا البطء في سد الثغرات بتزايد الاعتماد على التشريعات الوطنية في اتخاذ التدابير الاستباقية تحت مظلة "الدفاع السيبراني"، واستخدام ذلك أحيانا ذريعة لشرعنة أعمال تتعدى على مبادئ العدالة الدولية[333].

وتبرز إشكاليات الإثبات الرقمي بالغة الحدة عند محاولة رصد الجرائم الرقمية أو جمع الأدلة وتقديمها أمام المحاكم الدولية. إذ تفتقر معظم النظم القضائية الوطنية فضلا عن الدولية للكوادر الفنية المؤهلة لرصد الدليل الرقمي، وفهم برمجيات التضليل، وضمان نزاهة جمع الأدلة وحفظها وصولا لاستخدامها في المحاكمة العادلة. كما تمتد الأزمة إلى معايير قبول الأدلة، ووزنها، وتكيفها مع أصول المحاكمة وضمانات الدفاع، ما قد يحرم الضحايا من الوصول إلى الإنصاف، ويمنح المعتدين ملاذات عدة للإفلات من المساءلة[334].

وقد أبرزت التحولات الرقمية أيضا أزمة التداخل بين المصالح الوطنية والنزاعات المسلحة، وإمكانية استغلال ضعف القوانين لتبرير أعمال عدائية، أو رفض القبول بالأدلة الرقمية بحجة عدم توافر ضمانات العدالة. هذا الوضع يعكس الحاجة إلى تطوير معايير قبول موحدة للأدلة الرقمية، وإلى بناء قدرات تحقيق وطنية ودولية ذات كفاءة عالية في التتبع الرقمي والتحليل السيبراني، وآليات تعزز التعاون الدولي السريع لمواجهة الجرائم العابرة للحدود.

---

[333] اللجنة الدولية للصليب الأحمر، **"تقرير خبراء حول القانون الدولي الإنساني والتحديات السيبرانية"**، جنيف، 2021، ص: 26

[334] بن عوض فايز، **التحقيق في الجرائم العابرة للحدود في الفضاء الرقمي**، دار الفكر العربي، الرياض، 2021، ص: 181

وفي سياق المراجعة الشاملة، يجمع معظم الباحثين على لزوم تطوير قواعد مكملة أو بروتوكولات إضافية لاتفاقيات جنيف، يكون من شأنها الآتي:

- تعريف الهجمات الرقمية زمن النزاع وتوصيفها الدقيق ضمن الإطار القانوني؛
- وضع ضوابط واضحة لمسؤولية الأعمال المنفذة عبر أنظمة الذكاء الاصطناعي، وضمان عدم الإفلات من العدالة تحت ستار البرمجيات أو الشبكات المستترة؛
- سن معايير واضحة للتمييز بين الاستخدام المدني والعسكري للبنية التحتية الرقمية ومن ثم حظر أي هجوم قد يؤدي إلى آثار عشوائية على المدنيين أو يخترق قاعدة التناسب؛
- تحديد شروط وآليات جبر الضرر والتعويض للضحايا، ودعم أنظمة إنذار مبكر رقمية تتيح توثيق الانتهاكات ورصدها وحفظها من التعديل أو التلاعب؛
- تعزيز حماية البيانات الشخصية ونظم المعلومات في زمن النزاعات، خاصة لمنع تسرب معلومات المدنيين واستخدامها لأهداف عسكرية أو إجرامية.[335]

ويتطلب بناء منظومة الحماية الرقمية تعاونا عابرا للقطاعات، يجمع بين الدول والمنظمات الحقوقية الدولية، والشركات التقنية الكبرى، ومراكز الأبحاث، والخبراء القانونيين والتقنيين. فالتوافق على لجنة دائمة أممية لتحديث قواعد القانون الإنساني رقميا قد يشكل فرصة لمتابعة التطورات، وملء الفجوات، وتقديم توصيات محدثة تكون موضع نقاش دائم وفي خدمة العدالة الإنسانية .كما يجب أن يتوازى ذلك مع دعم دور المنظمات الدولية في وضع بروتوكولات وقائية وأخلاقيات لاستخدام الفضاء الرقمي والذكاء الاصطناعي في العمليات العسكرية[336].

---

[335] حمد جلال عبد العال، **القانون الدولي الإنساني في ضوء تحديات الحرب السيبرانية**، دار النهضة العربية، القاهرة، 2023، ص: 160

[336] الشربيني حنان، **"تطوير الدور الدولي للصليب الأحمر في زمن الحرب السيبرانية"، مجلة القانون الدولي الإنساني**، جامعة القاهرة، العدد 17، 2022، ص: 109

ولا يمكن لأي مراجعة قانونية أن تتجاهل تعزيز مكانة الضحايا في منظومة الحماية، إذ يتعين إعمال برامج دعم نفسي وقانوني للمتضررين من الجرائم الرقمية، وتيسير وصولهم إلى نظم الشكوى الإلكترونية والمنصات الذكية التي تمكن من التوثيق السريع للأضرار، مما يعزز فعالية الرصد والمساءلة ويعطي القانون الدولي الإنساني بعدا واقعيا في ظل تحولات العولمة والرقمنة.

الخلاصة التي تتولد عن هذا النقاش تشير إلى أن مستقبل القانون الدولي الإنساني، في مواجهة التحديات الرقمية والأمنية المعولمة، لا يتوقف على حماية النصوص فقط، بل على الانتقال نحو منظومة ديناميكية تمتلك مقومات المرونة والتحديث المستمر والصرامة في إنفاذ مبادئها. ويتطلب ذلك جميعا إعادة تعريف لأطر السيادة والحدود، وابتكار نماذج تنظيم جديد تربط بين أخلاقيات الفعل العسكري ومقتضيات الأمن الجماعي والكرامة الإنسانية. فلا سبيل إلى ضمان فعالية القانون وحمايته سوى بحلول مبتكرة تراعي التطور التكنولوجي، وتحقق شراكة واسعة تدمج الحقوقيين بالتقنيين وصانعي السياسات على المستوى العالمي. ولا شك أن استثمار هذه الجهود سيكون بمثابة نقطة الانطلاق لضمان حماية الإنسان من أخطار عالم متغير تتداخل فيه الجغرافيا الرقمية مع حدود الفعل القانوني، وتتعقد معه سبل تحقيق العدالة وإعلاء القيم الإنسانية.

الفقرة الثانية: إمكانيات التعاون الدولي وآليات التحديث التشريعي

أضحى التعاون الدولي، في ظل التحولات الرقمية والعولمة الأمنية، ركيزة أساسية لأي مسعى جاد وفعال لتحديث قواعد القانون الدولي الإنساني، فالتحديات الراهنة تجاوزت تماما قدرات الدول أو المؤسسات منفردة في مواكبة التعقيدات التي فرضتها تيارات الرقمنة المتسارعة واندماج التهديدات. إذ لم يعد المشهد مقصورا على الحروب الكلاسيكية بل أصبح الفضاء السيبراني مسرحا لعمليات عابرة للحدود تحمل طابع التكامل والتشابك بين مخاطر سياسية وتقنية وتجارية ونفسية واجتماعية، ومن ثم أضحى النجاح في تطوير القواعد القانونية الإنسانية مرهونا باتساع دائرة التشاركية وترحيل المقاربة المحلية أو الثنائية لصالح رؤية جماعية شاملة.

لقد أفرزت العولمة الأمنية، المقترنة بالثورة التكنولوجية، أنماطا جديدة من الفاعلين لم تكن مأخوذة في الحسبان عند وضع اتفاقيات جنيف ومحاكمات نورمبرغ الأولى. فاليوم، الفواعل ليست حكرا على الدول أو الجيوش النظامية، بل برزت شركات متعددة الجنسيات تطور الأدوات الرقمية والأسلحة الذكية، ومجموعات قرصنة ومنظمات عابرة للحدود، وباحثون في الذكاء الاصطناعي،[337] وصارت مصالح الأمن الجماعي والاقتصاد والبنية التحتية مرتبطة جميعها، وتحت رحمة التهديدات الرقمية الدقيقة الموجهة بتقنيات الذكاء المعمق وخوارزميات تحليل البيانات الضخمة. إن مواجهة هذه الهياكل المعقدة لا يمكن أن تتحقق إلا من خلال تظافر جهود الدول والمنظمات الأممية، والشركات الخاصة، وهيئات المجتمع المدني، ليعمل الجميع ضمن نهج تشاركي يتيح الرصد المبكر والتدخل السريع وصياغة التشريعات المناسبة لنطاق الفعل الجديد[338].

لذلك، فقد أسهمت تطورات العقدين الماضيين في تعرية محدودية الآليات الوطنية والقضائية، حيث بات تبادل المعلومات حول طبيعة الهجمات السيبرانية، أو مصادر البرمجيات الخبيثة، أو الإجراءات الوقائية، شرطا لا مفر منه لاستباق الكارثة، والإحاطة بمسرح النزاع الرقمي المتغير بسرعة. ولا شك أن تدشين قواعد البيانات المشتركة، ومنصات التحليل الاستخباراتي عبر الحدود، عزز من قدرة الأجهزة الدولية على رسم خرائط للهجمات والمخططات العدائية، ووفر مجالا لتعاون أكثر كثافة بين أجهزة إنفاذ القانون، ما شكل قاعدة مشتركة تحسن فرص التحقيق الفعال والمحاسبة حتى في القضايا الأشد تعقيدا.[339]

---

337 يحيى سعود. "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، **المجلة القانونية**، المجلد 4، العدد 4، ص: 94

338 الفار محمد صبحي و عبد الغني أمل، " القانون الدولي الإنساني و الحرب السيبرانية في النزاعات المسلحة غير الدولية"، **المجلة القانونية الاقتصادية**، كلية الحقوق جامعة الزقازيق، العدد 44، 2023، ص: 540

339 أبو النور مصطفى عبد السلام وآخرون، "مواجهة الحرب السيبرانية أثناء النزاعات المسلحة في ضوء القانون الدولي الإنساني"، **مجلة كلية الشريعة والقانون**، العدد 29، ديسمبر 2024، ص: 3027

كذلك أصبح دور المنظمات الدولية – وعلى رأسها الأمم المتحدة واللجنة الدولية للصليب الأحمر – محوريا في دعم وسائل التنسيق والدفع نحو توحيد الأطر التشريعية الخاصة بمجال الحرب الرقمية. و قد ارتبط ذلك بتنظيم المؤتمرات التقنية العالمية، وإدارة حلقات عمل مشتركة بين الوفود القانونية وخبراء البرمجة وأمن الشبكات، تمخض عنها إعلان مبادئ وملاحظات تفسيرية ملهمة لعمليات التحديث. وكانت مثل هذه المنتديات المقدمة الطبيعية لفكرة أن القانون الجديد ليس إطارا نظريا فحسب، بل منظومة متكاملة من الأدوات التشريعية والآليات التقنية والإجماع الأخلاقي[340].

من جهة أخرى، برزت الحاجة الملحة لإدماج القطاع الخاص، خصوصا شركات البرمجيات العملاقة وشركات الذكاء الاصطناعي والاتصالات، وذلك من خلال تشكيل لجان مشتركة لصياغة معايير جديدة للسلوك الرقمي وضبط استخدام الأدوات ذات الاستخدام المزدوج. فقد أصبح الطريق إلى التشريع يمر عبر صياغة كود أخلاقي دولي لاستعمال التقنيات الحديثة، وتنظيم العمل البحثي والصناعي بحيث تحترم قواعد القانون الدولي الإنساني كجزء من منظومة المساءلة الاجتماعية للشركات، وهذا ما دفع جهات فاعلة متعددة للانخراط طواعية في مبادرات الشفافية الإيجابية، مثل نشر تقارير دورية عن التأثيرات الإنسانية والاجتماعية للبرمجيات والتي يتم تطويرها للأغراض الدفاعية[341].

بالإضافة إلى ذلك، لم يعد تحديث التشريعات مسألة تعود للحكومات المركزية فقط، بل يمتد إلى ضرورة التكامل مع الجهاز الأكاديمي والمراكز البحثية، التي تتيح إنتاج فقه جديد قادر على استكشاف الثغرات القانونية ومحاولة سدها بناء على مستجدات الرقمنة. وقد لعبت الجامعات ومعاهد هندسة البرمجيات والأمن السيبراني الدور الأكبر في تقديم حلول عملية

340 عبد العال محمد جلال، **القانون الدولي الإنساني في ضوء تحديات الحرب السيبرانية**، مرجع سابق، ص: 90

341 بوزلماط عز الدين، "دور المؤسسات الخاصة للتصدي للجريمة السيبرانية على الصعيدين الدولي والوطني"، **مجلة القانون والأعمال الدولية**، الإصدار 53، غشت – شتنبر 2024، ص: 23

للتحديات المستجدة؛ منها إعداد أطر عمل للبروتوكولات الجديدة، ونماذج للمحاكم الرقمية المتخصصة، واقتراح ضمانات توثيق الأدلة الرقمية وسلاسل حفظها منذ لحظة جمع البيانات إلى التوظيف القضائي، ما عزز من مصداقية الأدلة وحصانتها أمام ساحة القضاء[342].

أما على مستوى التشريع المحلي، فقد ثبت أن فعالية الإصلاح رهينة بمدى سرعة النظم الوطنية في مواءمة تشريعاتها مع الالتزامات الدولية الناشئة من التوافقات الجماعية. وتبين أنه لا بد من لجان تشريعية دائمة في البرلمانات الوطنية تجتمع مع الجهات الرقابية وخبراء التقنية والقضاء والأمن والدفاع، بغرض تحليل المشهد الدولي وتقديم توصيات عملية تدمج قواعد الحرب السيبرانية والذكاء الاصطناعي ضمن القوانين الجنائية والعسكرية للدول الأعضاء في المنظومة الأممية. فقد ساعدت برامج التدريب المشتركة والمنح الدراسية في بناء كوادر جديدة من المشرعين الأقدر على فهم التداخل بين التقنية والقانون، ما أدى إلى وضع أطر تنظيمية واضحة تصنف الهجمات الرقمية والجرائم العابرة للفضاءات، وتضبط درجات العلنية والسرية في مداولات القضايا السيبرانية.

كما ينعكس تحديث التشريعات أيضا على السلطة القضائية، حيث تبرز الحاجة إلى محاكم متخصصة تملك تفويضا واضحا للنظر في انتهاكات القانون الإنساني ذات الطابع الرقمي، وفي الوقت ذاته تشرك خبرة فنية وتقنية قادرة على دراسة أنماط الجرائم الجديدة. لذلك فقد تعالت أصوات تطالب بإنشاء جهات تحقيق دولية دائمة تعنى بتجميع وتحليل الأدلة السيبرانية وتقديم التوصيات الاستشارية للمحاكم المحلية والدولية، كما ظهرت في بعض البلدان وحدات تحقيق مختصة بالجرائم الرقمية المرتبطة بالنزاعات المسلحة، غايتها سد الفجوة بين الأدلة التقنية والتكييف القضائي والحقوقي[343].

---

[342] دخلافي سفيان، "العدوان في القانون الدولي والهجمات السيبرانية بين الدول"، **مجلة العلوم القانونية والسياسية**، العدد الثاني، شتنبر 2023، ص: 90

[343] شويرب الجيلالي ومراد فايزة، "الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية"، **مجلة الدراسات القانونية والسياسية**، العدد الثاني، يونيو 2023، ص: 161

أيضا كان الرهان على الأطر الإقليمية فعالا في تعزيز فرص الإصلاح والابتكار القانوني، إذ أثبتت الاتفاقيات الإقليمية مثل الاتفاقيات الأوروبية لحماية البيانات، أو شبكات الإنذار المبكر للدفاع السيبراني في آسيا وأفريقيا، أنها أكثر مرونة وسرعة في التجاوب مع متطلبات بيئة النزاع المتغيرة، وأنها تشجع تبادل الحلول المستجدة بطريقة تحترم التباينات الثقافية والقانونية ضمن الوحدة الإقليمية نفسها. كذلك فإن اللجوء إلى الوساطات الإقليمية في حل النزاعات التقنية قدم نموذجا واعدا لحل الاختلافات دون تصعيد الأوضاع أو تدويل النزاعات[344].

أما على الصعيد التشاركي، فقد بات المجتمع المدني لاعبا رئيسيا في جهود مراقبة وتوثيق الانتهاكات الرقمية وتقديم رؤى تجديدية للتشريع. حيث اعتمدت المنظمات غير الحكومية استراتيجية "الشبكة القانونية المفتوحة"، التي تسمح للمواطنين بالإبلاغ عن الجرائم الرقمية وضحايا الحرب السيبرانية، ومهدت الطريق أمام حملات مناصرة قوية تدعو إلى اعتماد معايير الحد الأدنى من الحماية الرقمية لكل إنسان. وتكرست هذه الأدوار عبر المراقبة المستقلة وتقديم الخبرة التقنية للمحاكم والمؤسسات التشريعية، وبالعون في صياغة مدونات السلوك العالمية وتوصيات الممارسات الفضلى[345].

يمثل كل ذلك أساسا لمنظومة إصلاحية تتطلع إلى خلق جسور تواصل وتشاور شاملة لا تتوقف عند حدود التطور التشريعي الآني، بل تؤسس لمسارات مراجعة دورية تدمج إنجازات المستقبل مع تحديات اللحظة الراهنة. إذ يدرك المجتمع الدولي اليوم أن ضمان أمن الإنسان وسلامته في العصر الرقمي يتوقف على مرونة ومصداقية التشريع الجماعي، وحيوية التعاون بين الفاعلين القانونيين والتقنيين والمنظمات الدولية والإقليمية، وديمومة الابتكار الذي يسبق التهديدات أو يتواكب معها، ويتجنب سقوط الضحايا في الفراغ القانوني أو التشظي المؤسساتي.

---

344 فولي فولي وأحمد حسن، "الانتهاكات السيبرانية للقانون الدولي وتحديات مواجهته"، **مجلة العلوم القانونية**، جامعة المدينة عجمان، المجلد 35، العدد الثاني، يوليوز 2023، ص:15

345 علوي مولاي رشيد والراجي الخدير، "الديمقراطية الرقمية: العلاقة بين المشاركة المدنية وانفتاح الدولة الرقمية"، **مجلة الدراسات المندمجة في العلوم الاقتصادية و القانونية و التقنية و التواصل**، المجلد الأول، العدد الأول، 2024، ص: 5

ومما لا شك فيه أن استدامة هذا الجهد تستدعي وعيا سياسيا عالي المستوى، يعترف بقيمة التشارك واستثمار رأس المال البشري وتكثيف الشراكة العابرة للدول والقطاعات، ويضمن ألا يصبح التحديث التشريعي حبيس النخبة بل ثمرة مساهمة الجميع، من المتخصصين وصانعي القرار، وصولا إلى المتضررين أنفسهم. فالقانون الدولي الإنساني، في نهاية المطاف، نظام حي يتطور باستمرار ليستجيب لنداءات كرامة الإنسان في مواجهة عنف متغير الوسائط، ومعولم الأبعاد، متجدد الأدوات، وتظل فاعليته رهن ما يبذل لإحيائه من تضامن وتعاون وتطوير مجتمعي لا ينقطع مع تسارع الزمن الرقمي وتحدياته المستجدة.

الخاتمة

مع بلوغ هذا البحث نهايته، يتأكد حجم التحولات العميقة التي فرضتها الثورة الرقمية والعولمة الأمنية على منظومة القانون الدولي الإنساني. لقد أفرزت هذه المتغيرات واقعا جديدا لم يعد فيه الصراع مقتصرا على جيوش تتقاتل ضمن ميادين محددة أو على مفهوم تقليدي للعدو والحماية، بل صار النزاع يمتد إلى فضاءات افتراضية غير مرئية، حيث تدار المعارك الرقمية بلا قيود للزمان أو المكان، وتتصاعد المخاطر على المدنيين، والبنى التحتية الاجتماعية والاقتصادية، ومجمل النظام الإنساني الذي صمم تاريخيا لحالات النزاع الكلاسيكي.

إن استعراضنا للتحديات التقنية المصاحبة لنشوء الذكاء الاصطناعي، والطائرات المسيرة، وتوسع الهجمات السيبرانية، أظهر أن هناك فجوة متسعة بين الواقع الميداني وأطر القانون الدولي الإنساني كما رسختها نصوص اتفاقيات جنيف وبروتوكولاتها. وقد أبرز هذا التباعد الحاجة العاجلة إلى مراجعة المفاهيم والمسارات التشريعية، بحيث يصبح هذا القانون أكثر قدرة على الاستجابة لمتطلبات الحماية في بيئة لم تعد فيها حدود واضحة بين المدني والعسكري أو المادي والرقمي.

كما تبينت، من خلال البحث، الإشكاليات البنيوية التي تعترض عملية الامتثال القانوني في الفضاء الرقمي، سواء على مستوى صعوبة تحديد الجهات المسؤولة عن الأفعال العدائية الرقمية، أو في عوائق الإثبات وتجميع الأدلة أمام القضاء الدولي، أو حتى في غموض وتداخل

التصنيفات القانونية بين الأعمال العدائية التقليدية وأشكال الضرر الرقمي الحديثة. وقد أفضت هذه الإشكاليات إلى مظاهر جديدة من الإفلات من العقاب، وهددت بتقويض الثقة في النظام القانوني الإنساني، خاصة في ظل اندماج قوى جديدة – كالشركات التقنية الكبرى ومجموعات القرصنة العابرة للحدود – في هندسة مسارات الصراع وصناعة القرار الحربي أو التأثير عليه. في هذا السياق المتلاحق التغير، يصبح إصلاح القانون الدولي الإنساني ضرورة إستراتيجية وليس مجرد خيار سياسي أو قانوني عابر. فالواقع الجديد يتطلب منظومة تشريعية أكثر انفتاحا ومرونة، قادرة على إدماج القيم الإنسانية الراسخة في بنية أدوات ذكية ومتجددة تتسم بالتعقيد وسرعة التطوير. ولم يعد ممكنا الركون إلى اجتهادات تفسيرية أو مبادرات متفرقة، بل يجب إطلاق مشروعات متعددة المستويات، تبدأ بمراجعة شاملة للمفاهيم المركزية (كالتمييز، والحماية، والتناسب، والمسؤولية)، وتؤسس لمجموعة بروتوكولات مكملة وصياغة أدوات تنفيذية تشمل الضبط البرمجي، وتطوير تقنيات التحقق والتحقيق، وتأمين قاعدة بيانات مشتركة للضحايا والانتهاكات.

لقد شدد البحث على أن تحقيق إصلاح حقيقي لقواعد القانون الدولي الإنساني لا بد أن يسير ضمن مسارات تعاون دولي فعالة؛ إذ بات من غير الممكن لأي دولة أن تنفرد بضبط الحماية القانونية ضد تهديدات رقمية عابرة للحدود أو توجيه ذكاء اصطناعي يمكنه التأثير على أمن المجتمع الدولي ككل. إن الشراكة بين الدول، والمنظمات الأممية والإقليمية، والقطاع الخاص، والمجتمع المدني والمراكز البحثية، تشكل جميعها شبكة التوازن المطلوبة للجمع بين حيوية التطوير التشريعي وضمان الالتزام بالحد الأدنى من المعايير الإنسانية الجامعة. كما أن إشراك الشركات التقنية ليس ترفا ولا خيارا تكميليا، بل هو سبيل إلزامي لمنع تسليع الذكاء الاصطناعي وتوجيهه إلى الاستخدامات غير الأخلاقية أو المدمرة للإنسانية.

تبين، من خلال البحث، أن الحلول والتوصيات لا ترتبط غالبا بوفرة النصوص أو صرامة العقوبات فحسب، بل بمدى قدرة المنظومة القانونية على التكييف المستمر والتعلم من الواقع وتجاوز منطق الردة التشريعية. إذ أن عصر العولمة الأمنية والرقمنة يشهد اشتباكا متناميا بين

التطلعات الإنسانية والمخاطر التكنولوجية، ما يستدعي بناء نظام ردع وحماية مشترك، تنصهر فيه جهود الإصلاح، الابتكار، وتبادل الخبرات مع إرادة سياسية جماعية لا تساوم على القيم الإنسانية لصالح موازين قوى متغيرة أو اعتبارات مصلحية معيارية.

وأخيرا، يبقى السؤال المركزي الذي يطرحه هذا البحث أمام المجتمع الدولي مفتوحا: كيف نحافظ على جوهر القانون الدولي الإنساني – أي صيانة كرامة الإنسان أثناء الحروب – في نظام عالمي تلفه العولمة الأمنية وتتسارع فيه شمولية الأدوات والتهديدات الرقمية؟ الجواب، الذي حاول البحث أن يرسم معالمه، رهين بإرادة الجميع في تجاوز القصورات وإعلاء التعاون كمبدأ، واعتماد المرونة التشريعية كإستراتيجية، والتعجيل بالابتكار القانوني والتقني كأساس لاستمرار عهد العدالة الإنسانية. بهذا فقط يمكن أن يستعيد القانون الدولي الإنساني مكانته الضابطة لمسارات الصراع في عصر الثورة الرقمية، ويبقى حارسا حقيقيا لقيم الإنسان والعالم في الزمن الجديد.