إشكالية السيادة الوطنية في الفضاء السيبراني: بين مبدأ عدم التدخل ومسؤولية الدول

الدكتور مهدي رجائي
Mehdi.r@gmail.com
أستاذ، قسم القانون العام، جامعة قم، إيران

محمد ضياء محناوي
Mohammad.z@gmail.com
طالب دكتوراه في قسم القانون العام، جامعة قم، إيران

الكلمات المفتاحية: السيادة الوطنية، الفضاء السيبراني، مبدأ عدم التدخل، مسؤولية الدول، العناية الواجبة.

كيفية اقتباس البحث

رجائي , مهدي , محمد ضياء محناوي , إشكالية السيادة الوطنية في الفضاء السيبراني: بين مبدأ عدم التدخل ومسؤولية الدول,مجلة مركز بابل للدراسات الانسانية، آيار ٢٠٢٦, المجلد:١٦ ,العدد:٥ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

The Problem of National Sovereignty in Cyberspace: Between the Principle of Non-Intervention and State Responsibility

Dr. Mehdi Rajaei
Mehdi.r@gmail.com
Professor, Department of Public Law, University of Qom, Iran

Mohammad Zia Mahnawi
Mohammad.z@gmail.com
PhD Student in Public Law, University of Qom, Iran

Keywords : national sovereignty, cyberspace, principle of non-intervention, state responsibility, due diligence.

How To Cite This Article
Rajaei , Mehdi ,Mohammad Zia Mahnawi ,The Problem of National Sovereignty in Cyberspace: Between the Principle of Non-Intervention and State Responsibility ,Journal Of Babylon Center For Humanities Studies, May 2026,Volume:16,Issue 5.

Abstract

The problem of national sovereignty in cyberspace stems from the erosion of traditional territoriality principles, as the borderless, intangible nature of digital data and activities undermines the foundation of state jurisdiction. This issue gains critical importance with the rise of cross-border cyberattacks that exploit the legal vacuum created by the mismatch between classic international law rules (attribution, state responsibility, non-intervention) and the unique features of the digital environment. This article examines the legal basis for extending territorial sovereignty to cyberspace and the obligations of states to protect their sovereignty from cyber threats, focusing on the principle of non-intervention, the circumstances precluding wrongfulness such as consent (intervention by request of the affected state), and the right of

self-defence as an exception to the prohibition of the use of force. The research adopts a comparative analytical methodology, drawing on primary sources of public international law (UN Charter, ILC Draft Articles on State Responsibility ٢٠٠١), interpretative international documents (UNGGE reports, Tallinn Manual ٢,٠), as well as comparative Arab national legislation and regional/international instruments. Key findings include: the absence of a comprehensive binding treaty on cyber sovereignty and due diligence creates a dangerous legal vacuum exploited by technologically advanced states to launch destructive cyberattacks that remain below the "armed attack" threshold triggering self-defence; traditional attribution criteria (e.g., effective control) are hardly applicable in the context of cyber proxies, making the establishment of international responsibility almost impossible without an independent technical fact-finding mechanism; and current Arab legislative approaches focus on punitive measures while neglecting proactive oversight of private entities, thereby undermining due diligence. The article recommends a dynamic interpretation of traditional rules, the establishment of an urgent-procedure cyber chamber within the ICJ, and a binding Arab regional protocol for intervention by request of the affected state, along with objective standards for attribution and evidentiary presumptions.

الملخص

تتأسس إشكالية السيادة الوطنية في الفضاء السيبراني على تصدع البنى التقليدية لمبدأ الإقليمية، الذي يشكل الركيزة الأساسية لممارسة الدولة لاختصاصاتها السيادية، وذلك بسبب الطبيعة اللامادية العابرة للحدود للبيانات والأنشطة الرقمية. وتكتسي هذه الإشكالية أهمية بالغة في ظل ازدياد الهجمات السيبرانية العابرة للحدود، والتي تستغل الفراغ القانوني الناجم عن عدم مواءمة القواعد التقليدية للقانون الدولي – كقواعد الإسناد والمسؤولية ومبدأ عدم التدخل – مع خصوصية البيئة الرقمية. ويسعى هذا المقال إلى تحليل الأسس القانونية لامتداد السيادة الإقليمية إلى الفضاء السيبراني، وبيان التزامات الدول بحماية سيادتها من الأخطار السيبرانية، مع التركيز على مبدأ عدم التدخل، وموانع عدم المشروعية كالرضا (التدخل بطلب من الدولة المتضررة)، وحق الدفاع الشرعي كاستثناء على حظر استخدام القوة. وقد اعتمد البحث منهجاً تحليلياً مقارناً، يستند إلى المصادر الأصلية للقانون الدولي العام (كميثاق الأمم المتحدة ومشروع مواد لجنة القانون الدولي لعام ٢٠٠١)، وإلى الوثائق الدولية التفسيرية (كتقارير فريق الخبراء الحكوميين التابع للأمم المتحدة ودليل تالين ٢,٠)، بالإضافة إلى تحليل التشريعات الوطنية العربية المقارنة (كالقانون العراقي والأردني والجزائري والمصري) والاتفاقيات الإقليمية والدولية (كالاتفاقية العربية

لمكافحة جرائم تقنية المعلومات واتفاقية بودابست واتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية ٢٠٢٤). وقد خلص البحث إلى جملة من النتائج، أبرزها: أن غياب معاهدة دولية شاملة وملزمة تحدد معايير السيادة السيبرانية والعناية الواجبة يخلق فراغاً قانونياً خطيراً تستغله الدول المتقدمة تقنياً لشن هجمات سيبرانية مدمرة تبقى تحت عتبة "الهجوم المسلح" الذي يبيح الدفاع الشرعي عن النفس؛ وأن معايير الإسناد التقليدية (كالسيطرة الفعالة) ثبتت صعوبة تطبيقها في سياق التوكيل السيبراني، مما يجعل إثبات المسؤولية الدولية شبه متعذر في غياب آلية دولية مستقلة لتقصي الحقائق التقنية؛ كما أن الإجراءات التشريعية العربية الحالية تركز على النمط الردعي (العقاب بعد الجريمة) وتهمل الرقابة الاستباقية على الكيانات الخاصة، مما يضعف فعالية قاعدة العناية الواجبة. وأخيراً، أوصى البحث بضرورة تطوير تفسير ديناميكي للقواعد التقليدية يستوعب خصوصية التقنيات الرقمية، مع إنشاء آليات تنفيذ سريعة ومتخصصة، كغرفة سيبرانية تابعة لمحكمة العدل الدولية ذات اختصاص استعجالي، وإقرار بروتوكول إقليمي عربي ملزم للتدخل السيبراني بناءً على طلب الدولة المتضررة، مع وضع معايير موضوعية للإسناد والقرائن الإثباتية.

المقدمة

تعد إشكالية امتداد السيادة الوطنية إلى الفضاء السيبراني من أبرز المعضلات القانونية التي تواجه المجتمع الدولي في العصر الرقمي، ذلك أن الطبيعة اللامادية العابرة للحدود لهذا الفضاء تحدث تصدعاً في البنى التقليدية لمبدأ الإقليمية، الذي يشكل الركيزة الأساسية لممارسة الدولة لاختصاصاتها السيادية. فبموجب القانون الدولي العام، تمتد سيادة الدولة إلى إقليمها البري والبحري والجوي، إلا أن غياب رابط مادي حاسم للبيانات والأنشطة السيبرانية يثير تساؤلات جوهرية حول إمكانية إخضاع هذه الأنشطة لقاعدة الاختصاص الإقليمي. هذا الوضع يخلق فراغات قانونية خطيرة، تستغلها أطراف فاعلة دولية وغير دولية لارتكاب أفعال ضارة دون تحمل المسؤولية الجنائية أو الدولية، مما يهدد جوهر السيادة ويضعف آليات حفظ الأمن الدولي. ولذلك، يتطلب الأمر فحصاً تأصيلياً للأسس القانونية التي يمكن أن تنبني عليها السيادة الوطنية في بيئة رقمية، مع تحليل مدى قابلية تطبيق مبدأ عدم التدخل وقواعد المسؤولية الدولية على الأنشطة السيبرانية العابرة للحدود.

يرتكز الإطار القانوني المقترح لضبط العلاقة بين السيادة الوطنية والفضاء السيبراني على ثلاث ركائز مترابطة تشكل محاور هذا المقال. أولا، تحديد الأسس المعيارية لامتداد السيادة الإقليمية إلى البيئة الرقمية من خلال معايير قانونية دقيقة للولاية القضائية السيبرانية، مع بحث

أثر الطابع العابر للحدود للبيانات على تجزئة السيادة. ثانيا، تحليل نظام مسؤولية الدول عن الأفعال السيبرانية الضارة الصادرة عن إقليمها، وذلك في ضوء مبدأ عدم الإضرار وقاعدة الاجتهاد الواجب، بالإضافة إلى استعراض آليات التعويض الدبلوماسية والقضائية عن الأضرار السيبرانية. ثالثا، تفسير مبدأ عدم التدخل في الشؤون الداخلية للدول في سياقه السيبراني، وتحديد حالات الخروج المأذون به قانونا كحق الدفاع عن النفس أو التدخل بطلب من الدولة المتضررة، وذلك لضمان عدم تحول هذا المبدأ إلى عائق أمام إنفاذ القانون الدولي.

يسلط المقال الضوء على التحديات الإجرائية والتفسيرية التي تعترض تطبيق هذه القواعد التقليدية على الجرائم السيبرانية غير المتمركزة، وأبرزها صعوبة إسناد الفعل الضار إلى دولة معينة في ظل إمكانية استخدام بنية تحتية مدنية لشن الهجمات، وإشكالية إثبات نية التدخل في العمليات السيبرانية غير المباشرة. كما يناقش المقال التفاوت الكبير بين سرعة التطور التكنولوجي وبطء صياغة القواعد القانونية الدولية الموحدة، مما يفضي إلى تضارب في الاجتهادات الوطنية والدولية ويعيق تحقيق توافق حول تفسير السيادة في الفضاء السيبراني. وبناء على ذلك، يهدف هذا المقال إلى تقديم رؤية قانونية متكاملة تسهم في إعادة بناء مفهوم السيادة بما يتلاءم مع خصوصية الفضاء السيبراني، دون المساس بجوهر السيادة أو تعطيل آليات التعاون الدولي في مكافحة الجرائم العابرة للحدود.

المبحث الأول: الأسس القانونية للسيادة الوطنية في الفضاء السيبراني

يَقْتَضِي تحديدُ النطاق القانوني للسيادة الوطنية في الفضاء السيبراني إعادةَ تأصيل المبادئ الكلاسيكية للقانون الدولي العام، ولا سيما مبدأ الإقليمية والولاية القضائية، بما يتلاءم مع خصوصية البيئة الرقمية. وسيتناول هذا المبحث ثلاثة مطالب: امتداد مبدأ السيادة الإقليمية إلى البيئة الرقمية، والتزامات الدول بحماية سيادتها من الأخطار السيبرانية، وأخيراً الاتفاقيات الدولية كآلية لتكريس السيادة السيبرانية.

المطلب الأول: امتداد مبدأ السيادة الإقليمية إلى البيئة الرقمية

يُعَدُّ امتدادُ السيادة الإقليمية إلى الفضاء السيبراني إشكاليةً تأسيسيةً، إذ تتصادم الطبيعة اللامادية للبيانات مع مبدأ الإقليمية القائم على الرقعة المادية، مما يستدعي تحديد معايير واضحة للاختصاص المكاني. وسيبين هذا المطلب من خلال فرعين: إشكالية تجزئة السيادة بسبب الطابع العابر للحدود للبيانات، ومعايير الولاية القضائية السيبرانية في القانون الدولي.

الفرع الأول: إشكالية تجزئة السيادة بسبب الطابع العابر للحدود للبيانات

تطرح الطبيعة العابرة للحدود الجوهرية للبيانات في الفضاء السيبراني إشكالية قانونية جوهرية تتعلق بتفتيت مفهوم السيادة الوطنية التقليدي القائم على السيطرة الفعلية على إقليم مادي محدد. فالتدفق الآني والمستمر للمعلومات عبر الخوادم المنتشرة في بقاع متعددة من العالم، والذي يتجاوز آليات الرقابة الحدودية التقليدية، يجعل من المستحيل عملياً على الدولة فرض سيادتها الكاملة على "إقليمها الرقمي". وقد أشار الباحث "جيلالي شويرب" إلى أن مفهوم الحروب السيبرانية والأمن السيبراني برمته يتحدى النظرة الكلاسيكية للسيادة، حيث يصبح من الصعب تحديد موقع الهجوم أو مصدره بدقة، مما يخلق فجوة قانونية في تطبيق مبدأي المسؤولية الدولية وعدم التدخل. هذا الواقع يضع الدول، ومنها العراق، أمام معضلة حقيقية: فبينما تسعى لحماية بيانات مواطنيها وبنيتها التحتية الحيوية وفقاً لقوانينها الوطنية كقانون مكافحة الجرائم المعلوماتية رقم ١٠ لسنة ٢٠١١، فإن الأدلة على أي اعتداء سيبراني غالباً ما تكون موزعة عبر ولايات قضائية متعددة.[١]

لقد عمّقت ثورة المعلومات هذه الإشكالية، محولة إياها من مجرد تحدٍّ تقني إلى أزمة بنيوية في القانون الدولي. فمع كل نقلة بيانات تعبر الحدود، يتم تجاوز إرادة الدولة في المراقبة والإذن، مما يؤدي إلى "تجزئة فعلية" لممارسة السيادة. فالدولة لم تعد القادرة وحدها على حصر الجريمة الإلكترونية أو ملاحقة مرتكبيها، إذ تتداخل الاختصاصات وتتصادم القوانين الوطنية. وأوضحت "ضحى لعيبي كاظم السدخان" أن البعد الجيوسياسي للأمن السيبراني يحول دون قدرة أي دولة، مهما بلغت قوتها، على فرض نموذجها القانوني الخاص على الفضاء الرقمي، مما يستلزم بالضرورة التعاون الدولي، لكن هذا التعاون يصطدم بدوره بمخاوف الدول من انتهاك سيادتها. وفي السياق العراقي، فإن عدم التصديق على اتفاقيات دولية كاتفاقية بودابست يزيد من تعقيد هذه الإشكالية، حيث يحد من آليات التعاون القضائي المباشر للحصول على أدلة رقمية تخضع لسيادة دول أخرى.[٢]

هذا التجزيء السيادي لا يعني بالضرورة زوال السيادة، بل تحولاً في أدواتها وآلياتها، حيث تظهر الحاجة إلى نموذج جديد للسيادة "التعاونية" أو "الرقمية". فالقوانين الوطنية لم تعد كافية لحماية المصالح الحيوية للدولة في الفضاء السيبراني بمفردها، بل أصبحت عاجزة عن ملاحقة البيانات المخزنة على خوادم في دولة أخرى. وقد تطرقت "نورة شلوش" إلى أن القرصنة الإلكترونية تمثل تجسيداً خطيراً لهذه الإشكالية، حيث يستغل المخترقون الفجوات في أنظمة الرقابة الحدودية للبيانات، مما يضعف من قدرة الدولة على حماية أمنها القومي. ومن هنا، فإن أي تشريع وطني، كقانون تنظيم الاتصالات والاتصالات المعلوماتية العراقي، سيظل ناقصاً ما

لم يُستكمل بآليات فعالة للتعاون القضائي الدولي تسمح باختراق حاجز "سيادة البيانات" لدول أخرى، وهو ما يجعل مسألة الانضمام إلى الأطر الدولية المرجعية، كوثائق مجموعة الخبراء الحكوميين (GGE) التابعة للأمم المتحدة، ضرورة ملحة لإعادة تعريف معالم السيادة في هذا العصر الرقمي المتشابك.[٣]

يتضح من خلال التحليل المقارن أن الإشكالية الجوهرية لا تكمن في زوال السيادة الوطنية في الفضاء السيبراني، بل في تحولها من حق مطلق في السيطرة إلى قدرة نسبية في التنظيم والمشاركة. فالقانون الدولي التقليدي، الذي يصّر على ثنائية "الداخل/الخارج" و"الإقليم/خارجه"، يبدو غير قادر على استيعاب طبيعة الفضاء الرقمي التراكمي والموزع. إن محاولة الدول، ومنها العراق، التعامل مع هذا التحدي من خلال تشريعات وطنية صارمة ومغلقة، كتلك التي تفرض حوسبة البيانات داخل الحدود، قد تكون أشبه بـ"سباق مع الزمن" محكوم عليه بالفشل ما لم يُقرن بسياسة خارجية قانونية نشطة. يخلص التقييم القانوني إلى أن النصوص التشريعية العراقية، رغم حداثتها النسبية، تعاني من "عيب أصلي" يتمثل في افتراضها الضمني بإمكانية تطبيق السيادة على البيانات كما تطبق على الأشخاص والأشياء المادية، متجاهلة أن البيانات، بطبيعتها، "كائنات حدودية" بامتياز. الحل المقترح لا يكمن في مكافحة هذا الطابع العابر للحدود، بل في إعادة هيكلة فهمنا القانوني للسيادة لتشمل مفهوم "الولاية القضائية التراكمية" أو "السلطة التعاونية"، حيث تصبح الدولة فاعلاً رئيسياً في منظومة متعددة الأطراف تتبادل الأدلة وتنسق الردود، بدلاً من أن تكون حارساً منعزلاً لحدودها الرقمية الوهمية. إن فعالية أي قانون سيبراني عراقي ستُقاس بقدرته على التكامل مع هذا النظام العالمي، وليس بصرامته الداخلية فقط، وهو ما يضع المشرع العراقي أمام اختبار حقيقي للتخلي عن بعض مظاهر السيادة الشكلية مقابل الحصول على جوهرها في الحماية الفعلية.

الفرع الثاني: معايير الولاية القضائية السيبرانية في القانون الدولي

تستند الولاية القضائية في الفضاء السيبراني إلى مبادئ القانون الدولي التقليدية (الإقليمية، الشخصية، الحماية، العالمية)، غير أن تطبيقها العملي يثير إشكالات جوهرية تتعلق بطبيعة الأدلة الرقمية العابرة للحدود. فمبدأ الإقليمية، المُنَظَّم في المادة ٢٢(١)(أ) من اتفاقية بودابست لمكافحة الجرائم الإلكترونية لعام ٢٠٠١، يمنح الدولة ولاية قضائية على الجريمة التي تُرتكب "على أراضيها"، بيد أن تحديد "مكان وقوع" الجريمة الإلكترونية يصبح معقداً عندما تستخدم خوادم موزعة في دول متعددة. وقد سعت المحاكم الوطنية، خاصة الأمريكية، إلى تطوير معيار "الارتباط الكافي" (sufficient connection) من خلال اختبار "الأثر المتعمد" (intended

effects) في قضايا مثل United States v. Microsoft Corp.، حيث يشترط لامتداد الاختصاص أن تتجه النية إلى إحداث ضرر جوهري داخل إقليم الدولة، مع وجود صلة حقيقية بين الجاني والسلوك الإجرامي. هذا التطور يعكس محاولة قضائية لتكييف مبدأ إقليمية مرن مع طبيعة الفضاء السيبراني اللامادية، دون التخلي عن ركائز السيادة الوطنية.[٤]

أما على الصعيد العربي، فتحاول الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات (عمان، ٢٠١٠) الموازنة بين ضرورة مكافحة الجرائم الإلكترونية واحترام السيادة الوطنية، ولكنها لا تخلو من إشكاليات في صياغة معايير الاختصاص القضائي. فقد نصت المادة (٣٠) من هذه الاتفاقية على أسس الولاية القضائية (الإقليمية والشخصية)، بينما أكدت المادة (٢) على مبدأي "المساواة في السيادة الإقليمية" و"عدم التدخل في الشؤون الداخلية" كأساسين للتعاون العربي. غير أن الإشكال يبرز عند تنازع الاختصاص الإيجابي (أي عندما تطالب دولتان بمحاكمة ذات الجريمة)، حيث تكتفي المادة (٣١) بدعوة الدول الأطراف إلى "التشاور والتنسيق" دون تقديم آلية ملزمة لحل هذا التنازع. هذا النقص الإجرائي يجعل الاتفاقية، رغم كونها نافذة في معظم الدول العربية، أداة تنسيقية غير قادرة على حسم النزاعات القضائية السيبرانية، مما يترك الدول أمام خيارين غير مرضيين: إما التراخي في الملاحقة أو التوسع الأحادي في الاختصاص.[٥]

على المستوى الوطني، وبالتركيز على العراق كمثال، يلاحظ أن غياب تشريع متكامل ومُصادق عليه لمكافحة الجرائم المعلوماتية يُضعف قدرة القضاء العراقي على ممارسة الولاية القضائية السيبرانية بشكل فعال. فمشروع قانون الجرائم المعلوماتية لعام ٢٠١١ (الذي لم يُقر بعد) ظل حبيس الخلافات السياسية والتقنية، مما اضطر المحاكم العراقية إلى الاعتماد على أحكام متفرقة من قانون العقوبات رقم (١١١) لسنة ١٩٦٩، لاسيما المواد (٤٣٧) و(٤٣٨) و(٤٣٩) المتعلقة بالاعتداء على الأموال والأسرار، والتي لم تُصمم أساساً لمواجهة الجرائم العابرة للحدود. وقد أشارت دراسة ميدانية إلى أن القضاة العراقيين يواجهون صعوبة بالغة في تحديد ما إذا كان للعراق "ارتباط كافٍ" بجريمة إلكترونية مصدرها خارج حدوده، خاصة عندما تتعلق بخوادم بيانات تقع في دول أجنبية. وهذا الفراغ التشريعي يجعل العراق، رغم كونه عضواً في الأمم المتحدة وملتزماً بمبادئ ميثاقها، عاجزاً عن ممارسة اختصاصه القضائي التنفيذي في الفضاء السيبراني، ما لم تُسن قوانين واضحة تحدد معايير الولاية القضائية وتُفعّل آليات التعاون القضائي الدولي.[٦]

يخلص التقييم القانوني، بعد استعراض المعايير التقليدية والحديثة للولاية القضائية السيبرانية، إلى وجود فجوة خطيرة بين "الاختصاص التقريري" (أي حق الدولة في وضع القوانين) و"الاختصاص التنفيذي" (أي قدرتها الفعلية على إنفاذ تلك القوانين عبر حدودها المادية). فبينما توسعت الدول، ومنها العربية، في نصوصها التشريعية لتشمل مبادئ الحماية والعالمية، فإنها تظل غير قادرة على تنفيذ إجراءات ضبط أو تحقيق على خوادم تقع في أراضٍ أجنبية، إلا عبر آليات التعاون القضائي التقليدية (الإنابات القضائية) التي تثبت بطئها الشديد أمام سرعة الأدلة الرقمية. والأكثر خطورة أن هذا الجمود القانوني يخلق حالة من "السيادة الانتقائية"، حيث تمارس الدول الكبرى (التي تمتلك القدرات التقنية والتأثير الدبلوماسي) اختصاصاً تنفيذياً بحكم الأمر الواقع، بينما تظل الدول الأقل قدرة، كالعراق وبعض الدول العربية، عاجزة عن حماية سيادتها السيبرانية. من منظور نقدي، يرى الباحث أن إقرار "معيار الضرر الجسيم المتوقع" كأساس لتوسيع الولاية القضائية – دون وضع ضوابط دولية ملزمة – سيؤدي إلى مزيد من الفوضى القضائية والصراع بين الدول، لا إلى حلها. الحل المقترح لا يكمن في مزيد من التوسع التشريعي الأحادي، بل في الإسراع بإبرام معاهدة دولية متوازنة (تلافياً لعيوب مشروع اتفاقية الأمم المتحدة لعام ٢٠٢٤ غير النافذ بعد) تُلزِم الدول بتسليم الأدلة الرقمية خلال أطر زمنية محددة، مع إنشاء غرفة تمهيدية دولية تبت في نزاعات الاختصاص الإيجابي بشكل ملزم، شرط أن تقبل الدول مسبقاً بهذا الاختصاص. بدون هذه الآليات، سيبقى الفضاء السيبراني منطقة "لا قانون فيها"، حيث السيادة النظرية لا تساوي شيئاً أمام القدرات التقنية الفعلية.

المطلب الثاني: التزامات الدول بحماية سيادتها من الأخطار السيبرانية

تَقَعُ على عاتق الدول التزاماتٌ قانونيةٌ متعددةٌ بحماية سيادتها في الفضاء السيبراني، تتفاوت بين الاجتهاد الواجب في منع الضرر وسن تشريعات وطنية رادعة. ويتناول هذا المطلب في فرعين: الالتزام بالاجتهاد الواجب لمنع الضرر الصادر عن أراضيها، والموازنة بين الأمن القومي والحقوق الرقمية في التشريعات الوطنية.

الفرع الأول: الالتزام بالاجتهاد الواجب لمنع الضرر الصادر عن أراضيها

يُعد مبدأ "العناية الواجبة" (Due Diligence) أحد المبادئ الراسخة في القانون الدولي العام، وقد صاغته محكمة العدل الدولية في حكمها الشهير في قضية قناة كورفو (١٩٤٩)، حيث أقرت بأن على كل دولة "التزاماً بعدم السماح عن علم باستخدام أراضيها في أعمال تتعارض مع حقوق الدول الأخرى". وقد انتقل هذا المبدأ من مجال حماية البيئة إلى الفضاء السيبراني، ليصبح بموجبه على الدول التزاماً سلوكياً بمنع استخدام بنيتها التحتية الإلكترونية أو أراضيها في شن

هجمات سيبرانية تضر بالدول الأخرى. فالقانون الدولي العام يفرض على الدول واجباً ببذل العناية، لا واجباً بتحقيق نتيجة، مما يعني أن الدولة مطالبة باتخاذ جميع التدابير المعقولة والممكنة للحد من المخاطر السيبرانية العابرة للحدود، دون أن تكون مسؤولة عن النتائج إذا استحال المنع رغم بذل أقصى جهودها. هذا التكييف يكتسب أهمية خاصة في ضوء ازدياد الهجمات السيبرانية المنطلقة من أراضي دول غير قادرة أو غير راغبة في السيطرة على جهات فاعلة من غير الدول، مما يجعل مبدأ العناية الواجبة الإطار القانوني الأنسب لتوزيع المسؤولية الدولية في هذا المجال.[٧]

يتجسد الالتزام بالعناية الواجبة في الفضاء السيبراني في ضرورة أن تتخذ الدول تدابير فعالة لمراقبة أنظمتها الإلكترونية ومنع استغلالها في الأنشطة غير المشروعة. فإذا علمت دولة، أو كان بإمكانها أن تعلم، بأن هجمات سيبرانية تنطلق من أراضيها أو من بنيتها التحتية الإلكترونية، وكان لديها القدرة على وقفها أو التخفيف من آثارها، فإن إخفاقها في ذلك يشكل انتهاكاً للقانون الدولي. وهذا الالتزام يشمل، على سبيل المثال لا الحصر، سن تشريعات وطنية تجرم الجرائم الإلكترونية، وإنشاء وحدات وطنية للاستجابة للحوادث السيبرانية (CSIRT)، وتعزيز أمن الشبكات الحكومية والخاصة، والتعاون مع الدول المتضررة في تبادل المعلومات والأدلة. وقد أشارت تقارير فريق الخبراء الحكوميين التابع للأمم المتحدة (UNGGE) إلى أن عدم قدرة الدولة على السيطرة على جهات فاعلة من غير الدول على أراضيها لا يعفيها من المسؤولية إذا كانت قد أهملت في اتخاذ الاحتياطات المعقولة. فالمعيار هنا هو "المعرفة الفعلية أو المفترضة" (actual or constructive knowledge) للدولة بالخطر، و"القدرة على اتخاذ إجراء" (capacity to act) لمنعه أو وقفه.[٨]

يثار جدل قانوني حول ما إذا كان مبدأ العناية الواجبة يشكل قاعدة آمرة ملزمة (lex lata) في القانون الدولي للفضاء السيبراني، أم أنه لا يزال في طور التبلور كقاعدة مستحدثة (lex ferenda). فبينما تؤكد بعض الدول، مثل فرنسا وألمانيا وهولندا، على أن هذا الالتزام ينبثق من المبادئ العامة للقانون الدولي وينطبق بالضرورة على الأنشطة السيبرانية، تصر دول أخرى، مثل الولايات المتحدة والمملكة المتحدة، على أنه لا يوجد إجماع دولي حول طبيعته الملزمة، وتعتبره مجرد "قاعدة سلوك مسؤولة" طوعية. وقد عكس فريق الخبراء الحكوميين التابع للأمم المتحدة (UNGGE) هذا الغموض في تقاريره، حيث أشار إلى "ضرورة أن تمنع الدول استخدام أراضيها في أعمال سيبرانية دولية غير مشروعة" دون أن يحسم ما إذا كان ذلك التزاماً قانونياً أم سياسياً. هذا الغموض يُضعف فعالية المبدأ في الممارسة العملية، ويجعل مساءلة الدول المتقاعسة عن

منع الأضرار السيبرانية المنطلقة من أراضيها أمراً بالغ الصعوبة، خاصة في ظل غياب آلية دولية مستقلة لتقصي الحقائق وإسناد المسؤولية.[٩]

يخلص التقييم القانوني إلى أن فعالية مبدأ العناية الواجبة في حماية السيادة الوطنية من الأخطار السيبرانية تظل رهينة بحل إشكاليتين جوهريتين لم تحسمهما الممارسة الدولية بعد: الأولى، تتمثل في غياب معايير موضوعية محددة لمستوى "العناية" المطلوب، حيث تتراوح المتطلبات بين مجرد سن تشريعات وطنية إلى إنشاء أنظمة متطورة للمراقبة والردع، مما يتيح للدول الكبرى فرض معايير مرتفعة على الدول الأقل قدرة، بينما تحتج الأخيرة بمحدودية إمكاناتها لتبرير تقاعسها. والثانية، تكمن في إثبات عنصر "المعرفة" بالخطر السيبراني، إذ تستطيع الدولة المدعى عليها دائماً الادعاء بعدم علمها بالهجمات المنطلقة من أراضيها، خاصة إذا كانت الجهات الفاعلة من غير الدول تستخدم وسائل تقنية متطورة للإخفاء. ومن منظور نقدي، يرى الباحث أن استمرار هذا الغموض في صياغة المبدأ يجعله عرضة للتوظيف الانتقائي من قبل الدول الكبرى لفرض إرادتها، بدلاً من أن يكون أداة قانونية محايدة لتوزيع المسؤوليات. ولذلك، فإن الحل لا يكمن في المزيد من النقاش النظري حول طبيعة المبدأ، بل في الانتقال إلى صياغة معاهدة دولية ملزمة تحدد بدقة التدابير الدنيا التي يجب على كل دولة اتخاذها وفقاً لقدراتها، وتنشئ آلية دولية محايدة لتقييم مدى امتثال الدول لهذه المعايير، وإلا فإن مبدأ العناية الواجبة سيظل حبراً على ورق لا يحمي سيادة الضعيف ولا يردع عدوان القوي.

الفرع الثاني: الموازنة بين الأمن القومي والحقوق الرقمية في التشريعات الوطنية

تعكس الإشكالية الجوهرية في صياغة السياسة التشريعية الجنائية للجرائم الإلكترونية صعوبة الموازنة بين تعزيز متطلبات الأمن الرقمي وضمان الحقوق والحريات الأساسية للأفراد. فمع تنامي الهجمات الموجهة ضد البنى التحتية الحيوية، أصبح تعزيز الأمن السيبراني ضرورة استراتيجية لا غنى عنها، غير أن هذا التوجه قد يهدد الحقوق الدستورية للمواطنين، خاصة الحق في الخصوصية وحرية التعبير. وقد نصت المادة (٣) من مشروع قانون جرائم المعلوماتية العراقي على سريان أحكام القانون على الجرائم المرتكبة داخل العراق أو خارجه إذا كان من شأنها التأثير على أمنه القومي أو نظمه المعلوماتية، وهو ما يعد تطبيقاً ضمنياً لمبدأ الحماية، غير أن غياب تعريف دقيق لما يشكل "تهديداً للأمن القومي" سيمنح السلطات القضائية في حال إقراره سلطة تقديرية واسعة قد تؤدي إلى تقييد غير مبرر للحقوق الرقمية. وقد أشارت دراسة تحليلية إلى أن العديد من التشريعات الوطنية في المنطقة العربية، ومنها قانون الجرائم الإلكترونية الأردني رقم (١٧) لسنة ٢٠٢٣، تعاني من إشكالية النصوص الفضفاضة التي تتيح

تأويلاً موسعاً للجرائم الإلكترونية، مما يجعلها عرضة للاستخدام كأداة لقمع الأصوات الناقدة والصحفيين والمدافعين عن حقوق الإنسان، بدلاً من أن تقتصر على مكافحة الجرائم السيبرانية الحقيقية.[١٠]

يتجلى الخلل في الموازنة التشريعية بوضوح في نصوص قانون الجرائم الإلكترونية الأردني لعام ٢٠٢٣ الذي حل محل القانون السابق رقم (٢٧) لسنة ٢٠١٥، إذ وسّع هذا القانون الجديد نطاق الجرائم الجزائية بموجب أحكام جديدة تفرض قيوداً مفرطة على الحق في حرية التعبير، وتخل بالتزامات الأردن بموجب القانون الدولي لحقوق الإنسان. فالمادة (٣) منه تجرّم الدخول غير المصرح به إلى الشبكة المعلوماتية، بينما تجرّم المادة (١٥) نشر أخبار أو بيانات أو إشاعات كاذبة أو ما من شأنه المساس بشخص الأشخاص أو اعتبارهم إذا كان من شأنها إثارة الفتنة أو إلحاق الضرر بالأمن الوطني، وهي صياغة فضفاضة تتيح ملاحقة المنتقدين بذريعة "إثارة الفتنة". وقد خلصت دراسة قانونية مقارنة إلى أن القيود الواردة على حرية التعبير في قانون الجرائم الإلكترونية الأردني لم تراعِ بشكل كافٍ مبدأ التناسب بين حماية الأمن السيبراني وضمان حقوق الأفراد، إذ تفتقر النصوص إلى آليات رقابية قضائية فعالة تسبق فرض القيود أو تراقبها، مما يجعل تطبيق القانون عرضة للانتهاكات. هذا الغياب للضمانات الإجرائية يحول دون تحقيق التوازن المطلوب، ويجعل التشريع أقرب إلى أداة للرقابة الأمنية المسبقة منه إلى إطار قانوني لحماية الحقوق.[١١]

من منظور مقارن، تظهر تجارب دول عربية أخرى محاولات أكثر تقدماً للموازنة بين الأمن السيبراني والحقوق الرقمية، وإن كانت لا تخلو من إشكاليات. فقد أصدرت مصر قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، الذي أنشأ المركز الوطني لحماية البيانات الشخصية، ووضع ضوابط واضحة لجمع البيانات ومعالجتها وتخزينها، مع إلزام الجهات المعنية بالحصول على موافقة صريحة من أصحاب البيانات قبل استخدامها، وتوفير آليات للرقابة القضائية والإدارية على عمليات المراقبة الإلكترونية. وفي المملكة العربية السعودية، صدر نظام مكافحة جرائم المعلوماتية (المرسوم الملكي م/١٧ لسنة ٢٠٠٧) المعدل، ونظام حماية البيانات الشخصية (المرسوم الملكي م/١٩ لسنة ١٤٤٣هـ الموافق ٢٠٢١م)، حيث يُلزم الأخير الجهات العامة والخاصة باتخاذ التدابير التنظيمية والتقنية اللازمة لحماية البيانات الشخصية، مع إقرار مبدأ تقييم الأثر المتعلق بحماية البيانات قبل تنفيذ أي مشروع أو برنامج يتضمن معالجة للبيانات الشخصية. غير أن الملاحظ أن هذه التشريعات، رغم تقدمها النسبي، تظل محدودة الفعالية في غياب ثقافة مؤسسية راسخة لاحترام الحقوق الرقمية، واستمرار توسع السلطات التنفيذية في

تفسير مفهوم "الأمن القومي" بشكل قد يبرر استثناءات واسعة من الضمانات المقررة، وهو ما يطرح تساؤلات جدية حول مدى قدرة هذه النصوص على تحقيق التوازن المنشود في الممارسة العملية.[١٢]

من منظور نقدي يرى الباحث أن جوهر إشكالية الموازنة بين الأمن القومي والحقوق الرقمية في التشريعات الوطنية لا يكمن في النصوص القانونية وحدها، بل في غياب آليات رقابية قضائية ومجتمعية مستقلة وفعالة ترصد كيفية تطبيق هذه النصوص في الواقع العملي. فمعظم التشريعات العربية، سواء في العراق أو الأردن أو مصر أو غيرها، تتضمن صياغات مبدئية للضمانات الدستورية (كالحق في الخصوصية وحرمة المراسلات)، غير أن هذه الضمانات تظل حبراً على ورق عندما تخضع لسلطة تقديرية إدارية واسعة تفتقر إلى المساءلة الفعلية. والأخطر من ذلك أن غياب تعريف دقيق وموضوعي لمصطلح "الأمن القومي" في معظم هذه التشريعات يمنح السلطات التنفيذية والقضائية سلطة مطلقة تقريباً في تفسير السلوكيات التي تشكل "تهديداً للأمن"، مما يحول دون تحقيق أي توازن حقيقي. يخلص الباحث إلى أن الحل لا يكمن في مزيد من التعديلات التشريعية الجزئية، بل في إعادة هيكلة جذرية للمقاربة التنظيمية بأسرها، تبدأ بوضع تعريفات واضحة ومحددة للجرائم السيبرانية الحقيقية التي تهدد الأمن القومي (كالإرهاب السيبراني، والهجمات على البنى التحتية الحيوية، والتجسس الإلكتروني)، واستبعاد الجرائم البسيطة (كانتهاك حق النشر أو السب والقذف الإلكتروني) من نطاق القوانين السيبرانية العقابية، مع إخضاع أي إجراء للمراقبة الإلكترونية أو تفتيش البيانات لإذن قضائي مسبق لا يجوز تجاوزه، ووضع حد أقصى زمني له، وإلزام الجهات الأمنية بتقديم تقارير دورية وشفافة عن ممارساتها في هذا المجال، تكون متاحة للرقابة البرلمانية والمجتمع المدني. بدون هذه الإصلاحات الجوهرية، ستبقى التشريعات الوطنية أداة للقمع أكثر منها إطاراً قانونياً عادلاً.

المطلب الثالث: الاتفاقيات الدولية كآلية لتكريس السيادة السيبرانية

تُشَكِّلُ الاتفاقيات الدولية الإطارَ القانوني الأهم لتثبيت ممارسة السيادة الوطنية في الفضاء السيبراني، رغم ما تثيره من إشكاليات تتعلق بتكييف القواعد التقليدية مع الجرائم غير المتمركزة. ويناقش هذا المطلب من خلال فرعين: دور الاتفاقيات الثنائية ومتعددة الأطراف في تنظيم الاختصاص، وتحديات تكييف القواعد التقليدية مع الجرائم غير المتمركزة.

الفرع الأول: دور الاتفاقيات الثنائية ومتعددة الأطراف في تنظيم الاختصاص

تمثل الاتفاقيات الثنائية ومتعددة الأطراف الركيزة الأساسية التي تستند إليها الدول في سعيها لتسوية إشكاليات الاختصاص القضائي الناشئة عن الطبيعة العابرة للحدود للجرائم السيبرانية.

فاتفاقية بودابست لمكافحة الجريمة الإلكترونية لعام ٢٠٠١، رغم كونها صكاً إقليمياً أوروبياً في الأساس، تعتبر أول معاهدة دولية شاملة تضع إطاراً قانونياً لتنظيم مسائل الاختصاص القضائي والتعاون القضائي الدولي في هذا المجال. فقد نصت المادة (٢٢) منها على أسس متعددة للاختصاص القضائي تشمل مبادئ الإقليمية والجنسية، كما أوضحت الفقرات من (٢٣١) إلى (٢٣٩) من التقرير التفسيري للاتفاقية أن المادة سالفة الذكر تمنح الدول الأطراف سلطة تقديرية في اعتماد أسس اختصاص إضافية، مثل مبدأ حماية الدولة الضحية، دون أن تُلزمها بها إلزاماً مطلقاً. كما أوصى التقرير الدول الأطراف بتطوير آليات تنسيقية لحل تنازع الاختصاص الإيجابي وتفادي النزاعات السلبية التي قد تعيق الملاحقة الجنائية. بيد أن هذه الاتفاقية لم تحظ بإجماع عالمي، إذ انضمت إليها حتى الآن نحو سبعين دولة، معظمها من الدول الغربية، في حين ظل العديد من الدول العربية والآسيوية والأفريقية خارج إطارها، مما دفع المجتمع الدولي إلى التفكير في صك أكثر شمولاً.[١٣]

على الصعيد الإقليمي، حاولت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية عام ٢٠١٠ سد الفجوة القانونية في المنطقة العربية، وذلك من خلال تبني سياسة جنائية عربية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات. فقد نصت المادة (٣٠) من هذه الاتفاقية على أسس الولاية القضائية (الإقليمية والشخصية)، كما أوجبت المادة (٣١) على الدول العربية المتعاقدة التشاور والتنسيق لحل حالات تنازع الاختصاص الإيجابي، مع إقرار مبدأ المساعدة القضائية المتبادلة في المادة (٣٢). غير أن هذه الاتفاقية، رغم كونها ملزمة قانوناً للدول العربية المصدقة عليها، تظل محدودة الفعالية بسبب غياب آلية دولية مستقلة لحل النزاعات الإيجابية وغياب تعريف موحد للمصطلحات القانونية الأساسية، مما يترك الدول الأعضاء أمام سلطة تقديرية واسعة في تفسير النصوص وتطبيقها، وهو ما يضعف من دورها كآلية فعالة لتكريس السيادة السيبرانية في المنطقة العربية.[١٤]

شهد نهاية عام ٢٠٢٤ تطوراً تاريخياً تمثل باعتماد الجمعية العامة للأمم المتحدة لاتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، التي تعتبر أول معاهدة دولية شاملة في هذا المجال منذ عقدين من الزمن. فقد نص الفصل الثالث من الاتفاقية على أسس متعددة للاختصاص القضائي، وحددت المادة (٢٢) منها معايير الولاية القضائية التي تشمل مبادئ الإقليمية والجنسية النشطة والسلبية، كما أوجبت على الدول الأطراف التعاون في تنظيم الاختصاص بما يتفق مع مبادئ ميثاق الأمم المتحدة والقانون الدولي. وتكمن أهمية هذه الاتفاقية في كونها صادرة عن إطار دولي متوافق عليه، وتفتح باب التوقيع أمام جميع الدول الأعضاء في الأمم

المتحدة، مما يعزز فرص تحقيق قبول دولي واسع. غير أن الاتفاقية لم تدخل حيز النفاذ بعد، إذ يلزم تصديق أربعين دولة عليها حتى تدخل حيز التنفيذ، كما تثار تساؤلات حول مدى نجاحها في التوفيق بين ضرورة مكافحة الجريمة واحترام السيادة الوطنية في ظل تباين مواقف الدول الكبرى من قضايا الاختصاص التنفيذي.

يتضح من خلال التحليل المقارن أن الاتفاقيات الثنائية ومتعددة الأطراف، رغم ما حققته من تقدم في تنظيم أسس الاختصاص القضائي السيبراني، لا تزال تعاني من إشكالات بنيوية تحول دون تحقيق الأمن القانوني المنشود. فالاتفاقيات الثنائية، التي تبرم بين دولتين بهدف تسهيل تبادل الأدلة الرقمية والتعاون القضائي، تظل محدودة النطاق وغير قادرة على مواجهة الجرائم السيبرانية التي تنطوي على أكثر من دولتين، كما أنها تخلق فوضى تشريعية بسبب تباين محتواها من اتفاقية إلى أخرى. أما الاتفاقيات متعددة الأطراف، فتتميز باتساع نطاقها الجغرافي، غير أنها تظل عرضة لمعضلة التنفيذ القضائي التنفيذي، حيث تتردد الدول في السماح بتنفيذ إجراءات تحقيق قضائي أجنبي على بنيتها التحتية التقنية خوفاً من المساس بسيادتها الوطنية. يخلص الباحث إلى أن الاتفاقيات وحدها، مهما بلغت دقة صياغتها، لا يمكنها حل إشكالية الاختصاص السيبراني ما لم تصاحبها إرادة سياسية صادقة وآليات تنفيذية فعالة ومحكمة. ولعل أبرز التحديات التي تواجه الاتفاقيات الدولية في هذا المجال هي غياب آلية دولية مستقلة لتسوية النزاعات الإيجابية المتعلقة بالاختصاص، وعدم وجود تعريف قانوني موحد لمفهوم "الأمن القومي" الذي تستند إليه الدول في توسيع اختصاصها، والتفاوت الكبير في القدرات التقنية والقضائية بين الدول المتقدمة والدول النامية، مما يجعل الاتفاقيات أداة لصالح الدول الكبرى القادرة على توظيفها وفق أهدافها الاستراتيجية بدلاً من أن تكون إطاراً قانونياً عادلاً للجميع. ولذلك، يرى الباحث أن أي تقدم حقيقي في هذا المجال يتطلب الانتقال من مرحلة الاتفاقيات التنسيقية الطوعية إلى مرحلة إنشاء هيئة دولية مستقلة تتمتع بسلطة إلزامية في الفصل في منازعات الاختصاص السيبراني، أسوة بآليات تسوية المنازعات في القانون البحري أو الاستثماري الدولي.

الفرع الثاني: تحديات تكييف القواعد التقليدية مع الجرائم غير المتمركزة

تشكل القواعد التقليدية المقررة للاختصاص القضائي، وفي مقدمتها مبدأ الإقليمية الذي يحظر على القاضي الجنائي تطبيق قانون دولته خارج حدوده المكانية، عائقاً جوهرياً أمام ملاحقة الجرائم غير المتمركزة التي تنطوي على عناصر موزعة في أكثر من دولة. فإذا كان الجاني في دولة والمجني عليه في دولة ثالثة والبيانات المخزنة في خوادم موزعة على دول عدة، فإن تحديد

"مكان وقوع الجريمة" وفقاً للمعايير الإقليمية التقليدية يصبح مهمة شبه مستحيلة، مما يتيح للمجرم الإلكتروني الإفلات من العقاب. وقد سعت بعض الدول، ومنها مصر وقطر، إلى تجاوز هذه الإشكالية عبر اعتماد مبدأ "الإقليم الرقمي" (Digital Territory)، الذي يسمح بمد الإقليم المادي ليشمل الأثر الرقمي للجريمة. بيد أن هذا الحل الجزئي لا يعالج جوهر المشكلة في غياب آلية دولية موحدة لتحديد الاختصاص، ولا يحول دون تنازع الاختصاص الإيجابي بين عدة دول تطالب كل منها بمحاكمة ذات الجاني.[١٥]

تتفاقم معضلة تكييف القواعد التقليدية في ظل انتشار تقنيات الحوسبة السحابية والشبكات اللامركزية، حيث تتوزع الأدلة الرقمية (كمحتوى البريد الإلكتروني ومنشورات وسائل التواصل الاجتماعي) على خوادم تخضع لسيادة دول مختلفة، وغالباً ما تكون بعيدة عن موقع ارتكاب الفعل الإجرامي. وقد أظهرت إحدى الدراسات أن أكثر من نصف التحقيقات الجنائية في الدول الأوروبية تتضمن طلبات عابرة للحدود للوصول إلى الأدلة الإلكترونية، غير أن آليات التعاون القضائي التقليدية (كانتداءات الإنابة القضائية المتبادلة) تثبت بطءها الشديد وعدم ملاءمتها لسرعة التغير التقني. وقد تجسدت هذه الإشكالية بوضوح في قضية Microsoft Ireland، حيث رفضت شركة التكنولوجيا العملاقة الامتثال لمذكرة تفتيش أمريكية تطالبها بتسليم رسائل بريد إلكتروني مخزنة على خوادمها في أيرلندا، مستندة إلى مبدأ السيادة الإقليمية، الأمر الذي دفع الكونغرس الأمريكي إلى إقرار قانون CLOUD Act لعام ٢٠١٨، والذي يسمح للسلطات الأمريكية بالوصول إلى البيانات المخزنة خارج أراضيها متى كانت الشركة المقدمة للخدمة خاضعة لولايتها القضائية.[١٦]

لم تقف التشريعات العربية بعيداً عن هذه التحديات، إذ سعت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (٢٠١٠) إلى تقديم إطار إقليمي للتعاون القضائي، غير أن نصوصها ظلت أسيرة القواعد التقليدية في تحديد الاختصاص. فالمادة (٣٠) من الاتفاقية منحت الدول العربية أعضاءها أسساً متعددة للاختصاص (الإقليمي والشخصي)، بينما نصت المادة (٣١) على ضرورة التشاور والتنسيق لحل تنازع الاختصاص الإيجابي، دون أن تقدم آلية ملزمة لحسم النزاع. أما على الصعيد الوطني، فما زال قانون مكافحة جرائم تقنية المعلومات العراقي (الذي لم يُقر بعد) ومشاريع القوانين العربية الأخرى تعاني من إشكالية أساسية تتمثل في عجزها عن التكيف مع الجرائم غير المتمركزة، إذ تظل معايير الاختصاص فيها محصورة في الروابط التقليدية (كالجنسية والإقليمية وحماية الدولة الضحية)، مع إغفال تام لمعايير أكثر حداثة كمعيار

"الموطن الرقمي للضحية" أو "مكان التأثير الجوهري" (Substantial Effects)، وهو ما يُبقي الثغرة القانونية التي تستغلها الجماعات الإجرامية الإلكترونية مفتوحة على مصراعيها.[١٧]

من منظور نقدي يرى الباحث أن الجوهر الحقيقي للإشكالية لا يكمن في القواعد التقليدية ذاتها بقدر ما يكمن في الطريقة الجامدة التي تُفهم بها وتُطبق في السياق السيبراني. فالقانون الدولي، بطبيعته، يتسم بالمرونة والقدرة على التكيف، ومبدأ الإقليمية لم يُصمم أبداً كقاعدة جامدة تربط الاختصاص حصراً بموقع الحبر على الورق، بل هو مبدأ مرن يستند إلى مفهوم "الولاية القضائية المعقولة" التي يمكن أن تمتد لتشمل الآثار الجوهرية للفعل الإجرامي متى توافرت صلة حقيقية بين الدولة والجريمة. لكن ما يعيق هذا التكيف هو غياب إرادة سياسية دولية حقيقية تتجاوز الخطاب الإنشائي إلى صياغة ملزمة لمعيار "التأثير الجوهري المتوقع"، وليس مجرد "التأثير الفعلي"، كأساس لتوسيع الاختصاص، مع وضع ضوابط صارمة تمنع التوسع التعسفي من قبل الدول الكبرى. كما أن التحدي الأكبر الذي تواجهه الدول العربية تحديداً ليس تقنياً أو قانونياً بحتاً، بل هو تحدٍ مؤسسي يتمثل في غياب وحدات قضائية وفنية متخصصة قادرة على فهم طبيعة الأدلة الرقمية وتتبع مساراتها عبر الخوادم السحابية الموزعة. ولن يكون لأي تعديل تشريعي، مهما بلغت دقته، أي قيمة عملية ما لم يرافقه استثمار جاد في بناء قدرات تقنية وقضائية وطنية، وإنشاء آليات تعاون إقليمي سريعة ومرنة تتجاوز بطء الإجراءات الدبلوماسية التقليدية، وإلا فإن القواعد القانونية، سواء التقليدية أو المستحدثة، ستبقى حبراً على ورق أمام سرعة الابتكار التقني وجسارة الجريمة المنظمة العابرة للحدود.

المبحث الثاني: مسؤولية الدول عن الأفعال السيبرانية الضارة

تُعَدُّ مسؤوليةُ الدول عن الأفعال السيبرانية الضارة ضمانةً جوهريةً لاحترام السيادة الوطنية، غير أن إسناد الفعل الضار إلى الدولة وإثبات العلاقة السببية يثيران إشكاليات قانونية وتقنية معقدة. وسيتناول هذا المبحث ثلاثة مطالب: أساس مسؤولية الدولة عن الهجمات الصادرة عن إقليمها، والتزامات الدولة بمنع استخدام بنيتها التحتية في الهجمات، وآليات التعويض عن الأضرار السيبرانية.

المطلب الأول: أساس مسؤولية الدولة عن الهجمات الصادرة عن إقليمها

يَسْتَنِدُ أساسُ مسؤولية الدولة عن الهجمات السيبرانية الصادرة عن إقليمها إلى قواعد القانون الدولي العام، وبخاصة مبدأ عدم الإضرار، مع صعوبة إثبات الإسناد الفعلي في ظل إمكانية استخدام بنية تحتية مدنية. وسيُعالج هذا المطلب في فرعين: مبدأ عدم الإضرار كأساس لضبط الأنشطة السيبرانية، ومعايير إسناد الفعل السيبراني إلى الدولة.

الفرع الأول: مبدأ عدم الإضرار كأساس لضبط الأنشطة السيبرانية

يُعد مبدأ عدم الإضرار، المستمد من المبادئ العامة للقانون الدولي، أحد الأسس القانونية الراسخة التي تستند إليها الدول في مطالبتها بضبط الأنشطة السيبرانية المنطلقة من أراضي الدول الأخرى. وقد صاغت محكمة العدل الدولية هذا المبدأ في قضية مضيق كورفو (Corfu Channel) عام ١٩٤٩، حيث أكدت على التزام كل دولة بعدم السماح عن علم باستخدام أراضيها في أعمال تضر بحقوق الدول الأخرى، وهو ما يمثل صياغة كلاسيكية لمبدأ العناية الواجبة (Due Diligence). وقد امتد تطبيق هذا المبدأ ليشمل مجالات متعددة كالقانون الدولي للبيئة والقانون الدولي للبحار، ثم انتقل تدريجياً إلى الفضاء السيبراني، ليصبح بموجبه على كل دولة التزاماً بمنع استخدام بنيتها التحتية الإلكترونية أو أراضيها في شن هجمات سيبرانية تضر بالدول الأخرى. وتكمن أهمية هذا المبدأ في كونه يعكس التوازن الدقيق بين حق الدولة في السيادة على إقليمها والتزامها بعدم الإضرار بالغير، وهو ما يجعله الإطار الأنسب لضبط الأنشطة السيبرانية في زمن السلم. وقد أكدت الفقرة الثانية من المادة (٢) من مشروع المواد المتعلق بمسؤولية الدول عن الأفعال غير المشروعة دولياً (٢٠٠١) الصادر عن لجنة القانون الدولي على أن لكل دولة التزاماً دولياً بعدم الإضرار بحقوق الدول الأخرى، وهو ما يُسقط بالضرورة على الفضاء السيبراني.[١٨]

لا يقتصر أثر مبدأ عدم الإضرار على منع الأنشطة السيبرانية الضارة الصادرة عن الدولة ذاتها، بل يتعداه إلى إلزام الدولة ببذل العناية الواجبة لمنع الأفراد والكيانات الخاصة على أراضيها من شن هجمات سيبرانية عابرة للحدود. وقد تجسد هذا الالتزام في قاعدة (٦) من دليل تالين ٢,٠ (Tallinn Manual ٢,٠) لعام ٢٠١٧، التي تنص على أن "على الدولة بذل العناية الواجبة للتأكد من عدم استخدام الأراضي الخاضعة لسيادتها أو الأشياء أو الأشخاص الخاضعين لولايتها القضائية أو سيطرتها في أنشطة سيبرانية تؤثر سلباً على حقوق الدول الأخرى". فالدولة مطالبة باتخاذ جميع التدابير المعقولة والملائمة، وفقاً لقدراتها الوطنية، لمراقبة أنظمتها الإلكترونية ومنع استغلالها في الأنشطة غير المشروعة، سواء تعلق الأمر بهجمات القرصنة أو نشر البرمجيات الخبيثة أو الهجمات الإلكترونية الموزعة. وقد أشار فريق الخبراء الحكوميين التابع للأمم المتحدة (UNGGE) في تقريره لعام ٢٠٢١ إلى أن مبدأ العناية الواجبة المستمد من مبدأ عدم الإضرار يعتبر من المبادئ الراسخة في القانون الدولي، وينطبق بطبيعة الحال على استخدام الدول لتكنولوجيا المعلومات والاتصالات. غير أن الإشكال يبرز في تحديد مستوى العناية المطلوب، إذ يختلف باختلاف قدرات الدولة التقنية والمالية، وباختلاف درجة الخطر

المتوقعة من الأنشطة السيبرانية، مما يخلق حالة من الغموض القانوني تعيق مساءلة الدول المتقاعسة.[١٩]

من منظور مقارن، يلاحظ أن الممارسة الدولية والقضائية لا تزال متواضعة في مجال تطبيق مبدأ عدم الإضرار على الأنشطة السيبرانية، رغم الإقرار المتزايد بأهميته. ففي قضية الهجمات السيبرانية على إستونيا (٢٠٠٧)، تعذر إسناد الهجمات إلى دولة بعينها، مما حال دون تطبيق قواعد المسؤولية الدولية التقليدية القائمة على إسناد الفعل إلى الدولة. بيد أن العديد من الخبراء القانونيين اعتبروا أن روسيا، التي انطلقت منها الهجمات، كانت ملزمة بمبدأ العناية الواجبة لمنع استخدام أراضيها في الأنشطة الضارة، بغض النظر عن إسناد الفعل إلى أجهزتها الرسمية. وقد تجسدت هذه الإشكالية بشكل أكثر حدة في قضية الهجمات السيبرانية على أوكرانيا (٢٠١٥-٢٠١٧)، حيث عجزت أوكرانيا عن إثبات إخفاق روسيا في بذل العناية الواجبة بشكل قاطع، وذلك بسبب صعوبة تحديد ما إذا كانت روسيا قد توافرت لديها "المعرفة الفعلية" بالهجمات، وما إذا كانت لديها "القدرة الفعلية" على منعها. هذا الغموض في شروط تطبيق المبدأ يجعله عرضة للتوظيف الانتقائي، ويؤكد الحاجة الملحة إلى صياغة قانونية أكثر تحديداً لشروط الإخفاق في العناية الواجبة في الفضاء السيبراني، خاصة فيما يتعلق بمستوى المعرفة المطلوب ونطاق التدابير الواجب اتخاذها.[٢٠]

يتضح من خلال التحليل المقارن أن مبدأ عدم الإضرار، رغم كونه الركيزة الأساسية لضبط الأنشطة السيبرانية، يعاني من قصور جوهري في شروط تطبيقه يحد من فعاليته العملية، إذ يظل رهيناً بتحقيق شقين يصعب إثباتهما في عالم السيبرانية: أولهما "المعرفة الفعلية" للدولة بالأنشطة الضارة المنطلقة من أراضيها، وثانيهما "القدرة الفعلية" على منعها أو وقفها. فالدولة المدعى عليها تستطيع دائماً الاحتجاج بعدم علمها بالهجمات السيبرانية، خاصة إذا كانت الجهات الفاعلة تستخدم وسائل تقنية متطورة للإخفاء، كما تستطيع الاحتجاج بعدم قدرتها على منعها بسبب تعقيدات التقنية أو نقص الموارد. هذا الوضع يخلق معضلة قانونية خطيرة: فكلما زاد تعقيد الهجوم السيبراني وزادت صعوبة كشف مصدره، أصبح من الأسهل على الدولة المصدرة الادعاء بعدم المعرفة أو العجز عن المنع، وهو ما يحول دون مساءلتها قانونياً. يرى الباحث أن المخرج من هذه المعضلة لا يكمن في مزيد من النقاش النظري حول المبدأ ذاته، بل في الانتقال إلى صياغة آلية دولية مستقلة لتقصي الحقائق السيبرانية، تتولى تقييم ما إذا كانت الدولة المصدرة قد توافرت لديها "مؤشرات كافية" على وجود النشاط الضار، وما إذا كانت قد اتخذت "جميع التدابير المعقولة" المتاحة وفقاً لقدراتها الوطنية لمنعه. هذه الآلية، إذا ما أُنشئت بقرار ملزم من الجمعية

العامة للأمم المتحدة، يمكن أن تشكل حلاً عملياً لمعضلة الإثبات، وتجعل من مبدأ عدم الإضرار أداة فعالة لحماية السيادة الوطنية في الفضاء السيبراني، بدلاً من أن يظل مجرد مبدأ نظري نادر التطبيق.

الفرع الثاني: معايير إسناد الفعل السيبراني إلى الدولة

تستند قواعد إسناد السلوك إلى الدولة في القانون الدولي إلى مشروع المواد المتعلق بمسؤولية الدول عن الأفعال غير المشروعة دولياً لعام ٢٠٠١، والذي يمثل المرجعية الأساسية في هذا المجال. فقد نصت المادة (٤) من هذا المشروع على أن "سلوك أي جهاز من أجهزة الدولة يعتبر فعلاً من أفعال الدولة بمقتضى القانون الدولي"، سواء كان هذا الجهاز يتولى مهامًا تشريعية أو تنفيذية أو قضائية أو أي وظائف أخرى. كما أضافت المادة (٨) أن سلوك شخص أو مجموعة من الأشخاص يُعتبر فعلاً من أفعال الدولة إذا كانوا "يتصرفون فعلاً بمقتضى تعليمات هذه الدولة أو تحت إمرتها أو سيطرتها أثناء قيامهم بهذا السلوك". وقد أكدت محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا ضدها (١٩٨٦) على ضرورة توفر معيار "السيطرة الفعالة" (Effective Control) لإسناد سلوك الجماعات غير الحكومية إلى الدولة، وهو المعيار الذي يتطلب إثبات أن الدولة لم تكتفِ بتقديم دعم عام، بل مارست سيطرة فعلية على العمليات العسكرية المحددة. بيد أن تطبيق هذه المعايير في الفضاء السيبراني يصطدم بصعوبات إثباتية كبيرة، إذ يصعب تتبع مصدر الهجوم الإلكتروني وإثبات وجود تعليمات أو سيطرة مباشرة من قبل أجهزة الدولة على القراصنة المجهولين أو الجماعات الإرهابية الإلكترونية، وهو ما يخلق ثغرة قانونية تستغلها الدول لحماية نفسها من المساءلة.[٢١]

تتجلى الإشكالات العملية لتطبيق معايير الإسناد التقليدية في الفضاء السيبراني بشكل خاص في الحالات التي تستخدم فيها الدول جهات فاعلة من غير الدول لشن هجمات إلكترونية، إذ يتطلب إثبات "السيطرة الفعالة" أو "التوجيه المباشر" أدلة يصعب الحصول عليها. وقد سعى فريق الخبراء الدولي الذي أعد دليل تالين ٢,٠ (٢٠١٧) إلى معالجة هذه الثغرة من خلال تقديم تفسيرات موسعة لقواعد الإسناد. فقد أوضحت القاعدة (١٥) من الدليل أن سلوك جماعة غير حكومية يُعتبر فعلاً من أفعال الدولة إذا كانت الأخيرة "تمارس سيطرة شاملة" (Overall Control) على أنشطتها السيبرانية، وهو معيار أقل صرامة من "السيطرة الفعالة" التي اشترطتها محكمة العدل الدولية، وقد أُقر هذا المعيار لأول مرة في قضية Tadić أمام المحكمة الجنائية الدولية ليوغوسلافيا السابقة (١٩٩٩). غير أن هذا الدليل لا يتمتع بصفة ملزمة قانونياً، كونه مجرد رأي استشاري للخبراء، كما أنه أثار جدلاً واسعاً بين الدول بشأن المعيار الذي يجب

اعتماده، مما يُبقي الإشكالية مفتوحة دون حل قانوني ملزم. وتزداد الأمور تعقيداً في حالات الهجمات التي تنفذها جماعات إلكترونية مستقلة لا تخضع لسيطرة الدولة، إذ لا يمكن عندئذ إسناد الفعل مباشرة إلى الدولة، بل يبقى السؤال قائماً حول ما إذا كانت الدولة قد أخفقت في الوفاء بالتزامها ببذل العناية الواجبة لمنع الأنشطة الضارة المنطلقة من أراضيها.[٢٢]

على الصعيد العربي، سعت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ إلى مواكبة هذه التطورات الدولية، غير أنها لم تتضمن أحكاماً واضحة أو محددة لقواعد إسناد الفعل السيبراني إلى الدولة، مكتفية بالإشارة إلى مبادئ المسؤولية الجنائية التقليدية في المواد (٢٣) و(٢٤) و(٢٥) منها. ورغم إدراك المشرع العربي لأهمية التنسيق القضائي في هذا المجال، كما يتجلى في النص على مبدأ تسليم المجرمين والتعاون القضائي، إلا أن النصوص بقيت أسيرة القواعد التقليدية، غير قادرة على تقديم حلول مبتكرة لإشكالات الإسناد في الفضاء السيبراني. وتنطبق الإشكالية ذاتها على مشروع قانون مكافحة الجرائم المعلوماتية العراقي (غير المعتمد بعد)، الذي أهمل تماماً النص على معايير إسناد الهجمات السيبرانية التي تنفذها جهات فاعلة من غير الدول من داخل الأراضي العراقية، وهو ما يضع العراق في موقف قانوني هش أمام المجتمع الدولي، إذ سيكون عاجزاً عن الادعاء بأن أفعال القراصنة المقيمين على أراضيه لا تُسند إليه، كما سيكون عاجزاً عن تقديم أدلة تثبت عدم علمه بهذه الأنشطة أو عدم قدرته على منعها. وقد أظهرت دراسة ميدانية على عينة من القضاة والمحققين العراقيين أن الغالبية العظمى منهم ليس لديهم معرفة كافية بمفاهيم الإسناد القانوني، مما يجعل النصوص القانونية، حتى لو وجدت، غير قابلة للتطبيق الفعال في الواقع العملي.[٢٣]

من منظور نقدي، يرى الباحث أن جوهر إشكالية إسناد الفعل السيبراني إلى الدولة لا يكمن في القصور النظري لقواعد القانون الدولي، بل في استحالة تطبيق هذه القواعد عملياً في ظل غياب آلية دولية محايدة ومتخصصة لتقصي الحقائق التقنية والقانونية. فقواعد الإسناد التقليدية تفترض وجود "جهة يمكن إسناد الفعل إليها"، وهو ما ينطبق بسهولة على العالم المادي الذي تظهر فيه آثار الجريمة الملموسة، ولكنه يصطدم بصعوبات جمّة في عالم السيبرانية حيث تتقن الجهات الفاعلة استخدام تقنيات التضليل والإخفاء والتوجيه عبر الوسطاء. والأخطر من ذلك أن هذا الغياب المؤسسي يخلق حالة من "الإسناد الانتقائي"، حيث تستطيع الدول الكبرى التي تمتلك القدرات التقنية المتقدمة أن تقدم أدلة "مقنعة" تُسند بموجبها هجوماً سيبرانياً إلى دولة أخرى، بينما تظل الدول الأقل قدرة عاجزة عن دحض هذه الادعاءات أو إثبات براءتها. هذه الفجوة الهائلة بين النظريات القانونية المجردة والإمكانيات التقنية الفعلية تحول دون تحقيق العدالة الدولية في

الفضاء السيبراني. يخلص الباحث إلى أن أي إصلاح حقيقي لا يمكن أن يقتصر على مزيد من التعديلات النظرية لقواعد الإسناد، بل يجب أن يتجاوزها إلى إنشاء هيئة دولية مستقلة تتمتع بولاية قضائية تقنية وقانونية، تختص بجمع الأدلة الرقمية وتحليلها وإصدار تقارير إسناد ملزمة قانوناً، أسوة بالآليات القائمة في مجال القانون البحري أو القانون الدولي للبيئة، دون أن تحل هذه الهيئة محل القضاء الوطني، بل تكون أداة مساعدة ترفع مستوى اليقين القانوني وتحد من الانتقائية في تطبيق قواعد الإسناد.

المطلب الثاني: التزامات الدولة بمنع استخدام بنيتها التحتية في الهجمات

تُلْزِمُ قواعدُ القانون الدولي الدولَ باتخاذ التدابير اللازمة لمنع استخدام بنيتها التحتية السيبرانية في شن هجمات موجهة ضد دول أخرى، وهو ما يستدعي آليات رقابية وتشريعية فعالة. ويتضمن هذا المطلب فرعين: الرقابة على الكيانات الخاصة كامتداد للسيادة الفعالة، والإجراءات التشريعية لتجسيد الالتزام الدولي بالمنع.

الفرع الأول: الرقابة على الكيانات الخاصة كامتداد للسيادة الفعالة

تتأسس فكرة امتداد السيادة الوطنية إلى الفضاء السيبراني على مبدأ أن الدولة لا تمارس سيادتها بشكل فعال إلا إذا امتدت رقابتها إلى البنى التحتية للاتصالات وتقنية المعلومات المملوكة للكيانات الخاصة المرخص لها على إقليمها. فالمفهوم التقليدي للسيادة الإقليمية، الذي يقوم على السيطرة المادية على الحدود، لم يعد كافياً في البيئة الرقمية حيث تعبر البيانات والهجمات عبر الخوادم المملوكة لشركات خاصة. ومن هنا، تبرز الحاجة إلى إلزام تلك الكيانات بمعايير أمنية دنيا، وفرض آليات للإبلاغ عن الثغرات، وتمكين السلطات الوطنية من الوصول إلى البنى التحتية الحرجة عند الضرورة. غير أن القانون الدولي الوضعي لم يضع بعد معاهدة شاملة تحدد بدقة نطاق هذه الرقابة، مما يخل فجوة تعتمد فيها الدول على اجتهاداتها الوطنية وتفسيراتها لقاعدة العناية الواجبة المستمدة من المبادئ العرفية.[٢٤]

تستند مسؤولية الدولة عن أفعال الكيانات الخاصة في الفضاء السيبراني إلى قاعدة قانونية دولية عرفية هي "العناية الواجبة" (Due Diligence)، والتي تقتضي اتخاذ الدولة لتدابير معقولة لمنع استخدام أراضيها أو بنيتها التحتية من قبل أشخاص غير حكوميين للإضرار بدول أخرى. وقد أكدت وثائق مجموعة الخبراء الحكوميين التابعة للأمم المتحدة (GGE) في تقاريرها المتعاقبة، وخصوصاً تقرير عام ٢٠١٥، على أن الدول ملزمة بضمان أن تكون الأنشطة السيبرانية المنطلقة من أراضيها أو عبر بنيتها التحتية متوافقة مع القانون الدولي، بما في ذلك مبدأ عدم التدخل. وتتجلى هذه العناية الواجبة في صورة التزامات إجرائية: سن تشريعات تجرم

الهجمات السيبرانية، وإنشاء هيئات رقابية للإشراف على مزودي الخدمات، وتطوير آليات للاستجابة السريعة للبلاغات. إلا أن غياب آلية دولية موحدة لقياس مدى كفاية هذه التدابير يجعل تطبيق القاعدة مرهوناً بالتقدير الوطني.[٢٥]

على المستوى العربي المقارن، تتباين درجة إلزام الكيانات الخاصة بالرقابة السيبرانية تبعاً لمستوى تطور التشريعات الوطنية. ففي العراق، ركزت الدراسات القانونية على ضرورة سد الثغرات في النصوص المنظمة لعمل شركات الاتصالات ومزودي الخدمات، خصوصاً في ظل غياب قانون مستقل شامل للجرائم المعلوماتية، والاعتماد بدلاً من ذلك على أحكام متفرقة في قوانين العقوبات والاتصالات. وتشير التحليلات إلى أن معظم التشريعات العربية الحالية تكتفي بمعاقبة الجريمة بعد وقوعها (آليات ردعية) بدلاً من فرض رقابة استباقية (آليات وقائية)، مما يضعف قدرة الدول على منع الكيانات الخاصة من أن تكون أداة غير مقصودة في الهجمات السيبرانية العابرة للحدود. في المقابل، أظهرت تجارب بعض الدول كالجزائر والإمارات محاولات لتطوير أطر قانونية تفرض معايير أمنية إلزامية على القطاع الخاص، وإن بقيت هذه الأطر غير منسجمة مع معايير دولية موحدة.[٢٦]

من منظور نقدي يرى الباحث أن الإطار القانوني الحالي لرقابة الدولة على الكيانات الخاصة في الفضاء السيبراني يعاني من خلل بنيوي مزدوج: أولاً، غياب معاهدة دولية ملزمة تحدد الحد الأدنى من معايير العناية الواجبة، مما يجعل الالتزامات الحالية – المستمدة من تقارير GGE والمبادئ العرفية العامة – مجرد توصيات غير قابلة للإعمال القضائي الإلزامي في غياب محكمة دولية مختصة بالجرائم السيبرانية. ثانياً، الاعتماد المفرط في التشريعات العربية على النمط الردعي (العقاب بعد الهجوم) بدلاً من النمط الوقائي (الرقابة والترخيص والتدقيق المستمر) يُنتج وهم السيادة الفعالة، إذ تظل البنى التحتية الخاصة عرضة للاختراق والتوظيف غير المشروع لسنوات قبل أن تتحرك السلطات. كما أن عدم وجود آليات دولية لتقييم مدى كفاية الرقابة الوطنية يعني أن الدولة المتضررة من هجوم سيبراني صادر عن كيان خاص في دولة أخرى تجد نفسها أمام إثبات صعب لانتهاك قاعدة العناية الواجبة، وهو ما يفسر ندرة الدعاوى القضائية الدولية في هذا المجال. ويخلص التقييم إلى أن فعالية امتداد السيادة إلى الكيانات الخاصة تبقى رهينة بقدرة المجتمع الدولي على تجاوز النقاشات النظرية حول تطبيق القواعد التقليدية، والانتقال إلى صياغة اتفاقية دولية تلزم الدول بإنشاء هيئات وطنية مستقلة للرقابة السيبرانية على القطاع الخاص، مع تحديد جزاءات واضحة للإخلال بهذا الالتزام.

الفرع الثاني: الإجراءات التشريعية لتجسيد الالتزام الدولي بالمنع

إن ترجمة الالتزام الدولي للدولة بمنع استخدام بنيتها التحتية في الهجمات السيبرانية إلى قواعد ملزمة على أرض الواقع لا تتم إلا عبر سن إجراءات تشريعية وطنية تحدد بدقة واجبات الكيانات العامة والخاصة. وتتنوع هذه الإجراءات بين قوانين تجرم الأفعال السيبرانية الضارة، وتشريعات تلزم مزودي الخدمات بالاحتفاظ بالسجلات والتعاون مع السلطات، وقوانين تحمي البنى التحتية الحرجة. فالقانون الوطني هو الأداة التي تُحوِّل بها الدولة التزاماتها الدولية العرفية أو التعاهدية – مثل قاعدة العناية الواجبة – إلى أحكام قابلة للتنفيذ أمام القضاء الداخلي. غير أن واقع التشريعات العربية يُظهر تفاوتاً كبيراً: فبعضها يكتفي بتعديل قوانين العقوبات لتشمل بعض الجرائم المعلوماتية، بينما تذهب دول أخرى إلى إصدار قوانين مستقلة للجرائم الإلكترونية، وإن بقيت فجواتها واضحة فيما يتعلق بالرقابة الاستباقية على الكيانات الخاصة.[٢٧]

تتضمن الإجراءات التشريعية الفعالة لتجسيد الالتزام بالمنع ثلاثة مستويات متكاملة: أولاً، إصدار قانون أساسي للجرائم المعلوماتية يُعرِّف الهجمات السيبرانية ويحدد عقوباتها، مع نص صريح على مسؤولية الشخص الاعتباري (الشركات) إذا سهلت إهمالها وقوع الهجوم. ثانياً، إلزام الكيانات الخاصة المشغلة للبنية التحتية للاتصالات وتقنية المعلومات بإنشاء نظم داخلية للإبلاغ عن الثغرات، وفرض غرامات مالية رادعة على مخالفة معايير الأمن السيبراني. ثالثاً، إنشاء هيئة وطنية مستقلة للإشراف على تنفيذ هذه القوانين، مع منحها صلاحيات التفتيش الدوري وطلب البيانات. وتشير الأدبيات القانونية العربية إلى أن غياب أي من هذه المستويات يُضعف قدرة الدولة على الادعاء بأنها مارست العناية الواجبة، ويجعلها عرضة للمساءلة الدولية إذا انطلقت هجمات ضارة من أراضيها عبر كيانات خاصة لم تخضع لرقابة حقيقية.[٢٨]

عند المقارنة بين التشريعات العربية في هذا المجال، يلاحظ تباين في درجة تفصيل الإجراءات. ففي العراق، ركزت الدراسات على ضرورة استكمال النقص التشريعي بعد أن ظل الاعتماد لفترة طويلة على أحكام متفرقة في قانون العقوبات وقانون الاتصالات، دون وجود قانون شامل للجرائم المعلوماتية يلبي متطلبات العناية الواجبة الدولية. أما في الجزائر، فقد صدر الأمر رقم ٠٩-٠٤ المؤرخ ٢٠٠٩ والمتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو يمثل نموذجاً أكثر تفصيلاً في إلزام مزودي الخدمات بالتعاون القضائي والإداري. غير أن هذه النماذج تظل جميعها ناقصة من زاوية الرقابة الاستباقية، حيث تميل إلى التركيز على الجانب الزجري بعد وقوع الجريمة بدلاً من فرض التزامات دورية مستمرة على الكيانات الخاصة بتدقيق أمن نظمها والإبلاغ عن الثغرات قبل استغلالها.[٢٩]

يخلص التقييم القانوني إلى أن الإجراءات التشريعية الحالية في معظم الدول العربية – باستثناء نماذج جزئية متقدمة – تعاني من فجوة جوهرية بين النص القانوني والتطبيق العملي لالتزام العناية الواجبة. فالقوانين وإن كانت تجرّم الهجمات السيبرانية وتُلزم الكيانات الخاصة بالتعاون، إلا أنها نادراً ما تتضمن آليات رقابية وقائية حقيقية كإلزام تلك الكيانات بإجراء تدقيقات أمنية دورية مستقلة، أو الإبلاغ الفوري عن أي ثغرة مكتشفة قبل استغلالها، أو فرض تراخيص أمنية مشروطة على مشغلي البنى التحتية الحرجة. والأكثر إشكالية هو أن غياب معايير عربية أو إقليمية موحدة لقياس "كفاية" هذه الإجراءات يجعل من المستحيل تقريباً إثبات تقصير دولة ما في الوفاء بالتزامها بالمنع أمام أي محكمة دولية، إذ سيبقى التقدير متروكاً للدولة نفسها. ومن منظور نقدي، يرى الباحث أن الحل لا يكمن في مجرد إصدار قوانين جديدة، بل في إنشاء آليات إقليمية عربية للإشراف المتبادل على مدى التزام الدول بإجراءات رقابية حقيقية وفعالة، تشبه آليات التقييم الدوري الشامل في منظومة الأمم المتحدة لحقوق الإنسان، وإلا ستظل الإجراءات التشريعية مجرد واجهة شكلية لا تجسد الالتزام الدولي بالمنع جوهرياً.

المطلب الثالث: آليات التعويض عن الأضرار السيبرانية

تَمَثِّلُ آلياتُ التعويض عن الأضرار السيبرانية أحد أهم وسائل إنفاذ المسؤولية الدولية، إلا أنها تظل محدودة الفعالية بسبب صعوبة تحديد الضرر وإثبات السببية وتقدير الخسائر. ويناقش هذا المطلب من خلال فرعين: الأسس القانونية للمطالبة بالتعويض في القانون الدولي، والوسائل الدبلوماسية والقضائية لحل النزاعات دون المساس بالسيادة.

الفرع الأول: الأسس القانونية للمطالبة بالتعويض في القانون الدولي

تستند المطالبة بالتعويض عن الأضرار السيبرانية في القانون الدولي إلى قواعد قانون مسؤولية الدول عن الأفعال غير المشروعة دولياً، كما جرى تدوينها في مشروع مواد لجنة القانون الدولي (ARSIWA) لعام ٢٠٠١. فطبقاً للمادة (٢) من هذا المشروع، تتطلب مسؤولية الدولة عن هجوم سيبراني يمكن إسناده إليها توافر عنصرين: الإسناد إلى الدولة، وكون الفعل يشكل انتهاكاً لالتزام دولي. وعند توافرهما، يلتزم الطرف المعتدِي – وفقاً للمادة (٣١) التي تكرس مبدأ "الجبر الكامل" (Full Reparation) – بتعويض الدولة المتضررة عن جميع الأضرار المادية والمعنوية الناجمة. وتفصّل المواد (٣٤–٣٧) أشكال الجبر: الرد إلى الحالة السابقة (المادة ٣٥)، والتعويض المالي (المادة ٣٦)، والرضا (المادة ٣٧). وقد أكدت تقارير مجموعة الخبراء الحكوميين (GGE) التابعة للأمم المتحدة، ولا سيما التقرير A/٧٠/١٧٤ لعام ٢٠١٥، على التعقيدات الفنية لعملية الإسناد في الفضاء السيبراني، وهو ما دفع الفقه القانوني إلى الدعوة –

بالاستناد إلى ممارسات محكمة العدل الدولية في قضايا مثل نيكاراغوا (١٩٨٦) وتيمور الشرقية (١٩٩٥) – إلى تبني معايير إثبات مرنة تتناسب مع خصوصية البيئة الرقمية.[٣٠]

تتعدد الأسس القانونية التي يمكن للدولة المتضررة الاحتجاج بها عند المطالبة بالتعويض، ولكن يجب التمييز بدقة بينها. فالمادة (٤/٢) من ميثاق الأمم المتحدة تنص على "منع توسل القوة أو التهديد به"، ولا يمكن الاستناد إليها إلا إذا بلغ الهجوم السيبراني درجة من الشدة والأثر تعادل الهجوم المسلح التقليدي وفقاً لاختبار "المقياس والآثار" (Scale and Effects) الذي أقرته محكمة العدل الدولية في قضية نيكاراغوا. وفي هذا السياق، تُعد القاعدة (٧١) من دليل تالين (Tallinn Manual ٢,٠) المرجع الأساسي لتقييم ما إذا كان الهجوم السيبراني قد تجاوز عتبة استخدام القوة، بينما تُفصّل القاعدة (٧٢) متى يرقى هذا الاستخدام إلى "هجوم مسلح" يبيح الدفاع الشرعي. أما انتهاك السيادة الوطنية بمعناه الأوسع (كاختراق أنظمة حكومية دون تدمير مادي)، فيستند إلى القانون الدولي العرفي، وتنظمه القاعدة (٤) من الدليل نفسه، والتي تعتبر أي تدخل سيبراني في الأنظمة السيادية لدولة أخرى – دون إذن – انتهاكاً للسيادة. وتضاف إلى ذلك قاعدة عدم التدخل في الشؤون الداخلية، وقواعد القانون الدولي لحقوق الإنسان إذا تسبب الهجوم في حرمان السكان من خدمات أساسية.[٣١]

في الأدبيات القانونية العربية المعاصرة، بدأ الاهتمام بخصوصية الأضرار السيبرانية يتزايد مع تزايد الهجمات في المنطقة، وإن كانت الدراسات القانونية المحكّمة لا تزال محدودة. وتشير التحليلات المتخصصة إلى أن مفاهيم القانون الدولي التقليدية كالسببية المباشرة والضرر الملموس تحتاج إلى إعادة نظر عند تطبيقها على الهجمات السيبرانية التي غالباً ما تعبر ولايات قضائية متعددة وتستخدم خوادم وسيطة وقراصنة مجهولي الهوية. وقد تناولت مجلات قانونية عربية محكّمة، كمجلة الحقوق (جامعة البحرين) والمجلة الأردنية في القانون والعلوم السياسية (جامعة مؤتة)، قضايا المسؤولية الدولية عن الهجمات السيبرانية، مؤكدة على ضرورة الاستفادة من مبادئ قانون الفضاء الخارجي (معاهدة الفضاء الخارجي ١٩٦٧) وقانون البيئة الدولي (مبدأ عدم الإضرار بالغير في إعلان ستوكهولم ١٩٧٢) كأطر تحليلية مقارنة لوضع أعراف جديدة للفضاء السيبراني. غير أن هذه الدعوات لم تتبلور بعد في صكوك دولية ملزمة، ويبقى الاعتماد الأساسي على الاجتهاد الوطني والقواعد العرفية العامة مع تباين واضح في التطبيق بين الدول.

من منظور نقدي يرى الباحث أن الأسس القانونية للمطالبة بالتعويض، رغم كونها قواعد ملزمة قانوناً (normatively binding) وليست مجرد توصيات أخلاقية، تواجه تحديات إنفاذية (enforceability) حادة بسبب غياب محكمة دولية متخصصة بالفضاء السيبراني. فمحكمة

مجلة مركز بابل للدراسات الإنسانية ٢٠٢٦ المجلد ١٦/ العدد ٥

العدل الدولية لا تختص إلا بالدول التي تقبل ولايتها طواعية، وهي حالة نادرة في النزاعات السيبرانية حيث تميل الدول إلى إنكار المسؤولية أو إرجاع الهجمات إلى جهات غير حكومية. أما معايير الإثبات، فلم يستقر العرف الدولي على معيار واحد. ففي قضية مضيق كورفو (١٩٤٩)، اعتمدت المحكمة على "الاستدلال بالقرائن" (proof by inference) وليس على أدلة قاطعة. وفي قضية المنصات النفطية (٢٠٠٣)، طلبت المحكمة "أدلة واضحة ومقنعة" (clear and convincing evidence). وبالتالي، فإن المطالبة بالتعويض عن أضرار سيبرانية تظل ممكنة نظرياً لكنها صعبة عملياً، وتتطلب تعاوناً سياسياً بين الدول أكثر منه آلية قضائية صارمة. ويرى الباحث أن الدعوات إلى إنشاء محكمة سيبرانية دولية، رغم أهميتها، تظل مثالية ما لم تُرافق بتحليل واقعي لموانع السيادة الوطنية وتجارب الآليات القضائية الدولية السابقة. ويخلص التقييم إلى أن الحل المؤقت الأكثر واقعية يكمن في تطوير آليات التحكيم الإلزامي الثنائي أو الإقليمي، مع وضع معايير إثبات واضحة تراعي خصوصية البيئة الرقمية، بدلاً من انتظار إنشاء محكمة دولية شاملة قد تستغرق عقوداً.

الفرع الثاني: الوسائل الدبلوماسية والقضائية لحل النزاعات دون المساس بالسيادة

تتيح الوسائل الدبلوماسية لحل النزاعات السيبرانية مسارات متعددة تحترم سيادة الدول المعنية، وفي مقدمتها المفاوضات المباشرة والوساطة والتوفيق والتحقيق. فالمفاوضات تبقى الأداة الأكثر مرونة، إذ تسمح للدول المتنازعة بالتوصل إلى تسويات تحفظ ماء الوجه وتجنب التصعيد، دون الحاجة إلى الاعتراف بمسؤولية قانونية كاملة قد تمس السيادة الوطنية. وتلجأ الدول أحياناً إلى اللجنة الدولية للقانون الدولي أو إلى أمانة الأمم المتحدة لتوفير منصة محايدة للوساطة، خاصة في الحالات التي يكون فيها الإسناد الفني للهجوم غير حاسم. غير أن هذه الوسائل تواجه تحدياً كبيراً يتمثل في إحجام الدول غالباً عن الاعتراف بوقوع ضرر سيبراني ناجم عن إهمالها، خوفاً من التداعيات السياسية، مما يجعل نجاحها مرهوناً بحسن النية والتوازن الاستراتيجي بين الأطراف.[٣٢]

أما الوسائل القضائية، فتتمثل أساساً في التحكيم الدولي ومحكمة العدل الدولية، وهي بطبيعتها أكثر إلزاماً من الوسائل الدبلوماسية، لكنها تشترط رضا الدول المتنازعة على اختصاصها. فمحكمة العدل الدولية، وفقاً للمادة ٣٦ من نظامها الأساسي، لا تنظر في النزاع إلا إذا قبلت الدولتان ولايتها، إما بتصريح خاص أو بموجب شرط اختياري. وفي النزاعات السيبرانية، يندر حصول هذا القبول لأن الدول تخشى أن يؤدي اللجوء إلى القضاء إلى كشف نقاط ضعف في أنظمتها الدفاعية أو إلى إقرار سوابق قانونية قد تقيد حريتها مستقبلاً. أما التحكيم، فيوفر

مرونة أكبر إذ تتفق الدول على تشكيل هيئة تحكيم مؤقتة وتحديد القواعد الإجرائية والإثبات بنفسها، مما يسمح بمراعاة خصوصية الأدلة التقنية في الهجمات السيبرانية. غير أن التحكيم أيضاً يتطلب توافقاً سياسياً نادراً في نزاعات تتعلق بالأمن القومي.[٣٣]

على المستوى العربي المقارن، تظهر الدراسات أن الدول العربية تميل إلى تفضيل الوسائل الدبلوماسية على القضائية في النزاعات السيبرانية، وذلك لأسباب متعددة منها غياب آليات عربية متخصصة في التحكيم السيبراني، وضعف الثقة في المحاكم الدولية لأسباب سياسية، والرغبة في تجنب إضفاء الصبغة القانونية على نزاعات قد تُحل بتسويات سياسية غير معلنة. وقد أشارت بعض التحليلات إلى إمكانية الاستفادة من مركز التحكيم التجاري لدول مجلس التعاون الخليجي أو المركز العربي للتحكيم الدولي بالقاهرة كمنصات لتسوية نزاعات سيبرانية مدنية، لكنها لا تصلح للنزاعات المتعلقة بالأمن السيبراني والمسؤولية الدولية. كما أن ميثاق جامعة الدول العربية لا يتضمن آليات قضائية ملزمة لحل النزاعات السيبرانية، مما يخل فجوة تحتاج إلى معالجة على المستوى الإقليمي.[٣٤]

من منظور نقدي يرى الباحث أن ثنائية "الوسائل الدبلوماسية مقابل القضائية" في النزاعات السيبرانية تعكس إشكالية أعمق تتعلق بفجوة الثقة بين الدول في بيئة لا تزال قواعدها غير مستقرة. فالوسائل الدبلوماسية، رغم مرونتها واحترامها للسيادة، غالباً ما تفضي إلى تسويات غير عادلة للدولة الأضعف تقنياً، إذ تميل المفاوضات إلى عكس موازين القوى الفعلية وليس الحقائق القانونية المجردة. أما الوسائل القضائية، فعلى الرغم من أنها تقدم وعداً بالعدالة الموضوعية، فإن شروط قبول ولاية المحاكم الدولية تجعلها حكراً تقريباً على النزاعات التي ترضى فيها الدول القوية بالتقاضي، وهو أمر نادر عندما تكون طرفاً متهماً. والأكثر إشكالية هو أن غياب محكمة سيبرانية متخصصة يعني أن القضاة في محكمة العدل الدولية أو هيئات التحكيم يضطرون إلى قياس الهجمات السيبرانية على قواعد وضعت لعالم مادي مختلف، مما يؤدي إلى قرارات غير متوقعة أو غير قابلة للتطبيق عملياً. ويرى الباحث أن الحل الأمثل لا يكمن في الاختيار بين الوسائل الدبلوماسية والقضائية، بل في تطوير نموذج هجين يجمع بين المرونة الدبلوماسية والضمانات القضائية، كإنشاء لجان تحقيق دولية إلزامية للوقائع السيبرانية (على غرار آلية التحقيق في جرائم الحرب) تعقبها مرحلة تحكيم إلزامي إذا ثبت الإسناد. هذا النموذج الهجين قد يحقق التوازن المطلوب بين احترام السيادة وضمان المساءلة الفعلية.

المبحث الثالث: مبدأ عدم التدخل كقيد على الأنشطة السيبرانية الدولية

يمثل مبدأُ عدم التدخل في الشؤون الداخلية للدول ركناً أساسياً في القانون الدولي المعاصر، غير أن تطبيقه على الأنشطة السيبرانية يثير إشكاليات تتعلق بتحديد ماهية التدخل ومعايير الإكراه في بيئة لامادية. وسيتناول هذا المبحث ثلاثة مطالب: تفسير مبدأ عدم التدخل في البيئة الرقمية، والاستثناءات المسموح بها لهذا المبدأ، والتحديات الإجرائية لتطبيقه على الجرائم السيبرانية.

المطلب الأول: تفسير مبدأ عدم التدخل في البيئة الرقمية

يَقْتَضِي تفسيرُ مبدأ عدم التدخل في البيئة الرقمية إعادةَ النظر في المفاهيم التقليدية كالإكراه والتدخل المسلح، بما يتلاءم مع خصوصية العمليات السيبرانية غير المباشرة. ويُعالج هذا المطلب في فرعين: امتداد حظر التدخل المسلح إلى العمليات السيبرانية، وإشكالية تحديد معيار الإكراه في الفضاء السيبراني.

الفرع الأول: امتداد حظر التدخل المسلح إلى العمليات السيبرانية

ينطلق مبدأ حظر التدخل المسلح المنصوص عليه في المادة (٤/٢) من ميثاق الأمم المتحدة من فكرة أن الدول ملزمة بعدم استخدام القوة أو التهديد بها ضد سيادة أي دولة أخرى أو سلامتها الإقليمية. ومع تطور التهديدات في الفضاء السيبراني، برز تساؤل جوهري حول ما إذا كانت العمليات السيبرانية التي تتسبب في أضرار مادية أو بشرية تعادل في شدتها الهجمات العسكرية التقليدية، وبالتالي تدخل في نطاق هذا الحظر. وقد استقر الفقه القانوني الدولي، مستنداً إلى أحكام محكمة العدل الدولية في قضية نيكاراغوا (١٩٨٦)، على أن العبرة ليست بطبيعة الوسيلة المستخدمة بل بآثارها ومقاديرها. فالهجوم السيبراني الذي يؤدي إلى تدمير منشآت حيوية أو إصابات بشرية أو تعطيل واسع النطاق للبنية التحتية الأساسية يُعد، وفق هذا المنطق، عملاً مشمولاً بحظر استخدام القوة، بغض النظر عن كونه نابعاً من أسلحة تقليدية أو برمجيات خبيثة.[٣٥]

لمعرفة متى يرقى الهجوم السيبراني إلى مستوى "استخدام القوة" المحظور بموجب المادة (٤/٢)، طوّر الفقه الدولي والقضاء معياراً عرفياً يُعرف بـ"اختبار المقياس والآثار" (Scale and Effects). ويعني هذا الاختبار أن المحكمة أو الهيئة المختصة تنظر إلى حجم الضرر الناجم عن الهجوم السيبراني وطبيعته ومدى انتشاره، فإذا بلغت آثاره ما يعادل الآثار الناجمة عن عمل عسكري تقليدي، فإنه يُعتبر استخداماً للقوة. وقد طبق هذا المعيار في قضية نيكاراغوا عندما قارنت المحكمة بين الدعم العسكري المقدم للكونترا والتدخل العسكري المباشر. وفي السياق السيبراني، يُعتبر الهجوم الذي يؤدي إلى انفجار سد أو تعطيل مفاعل نووي أو تحطيم طائرة

مدنية عبر اختراق أنظمة التحكم، مشمولاً بالحظر. وقد تبنّى دليل تالين (Tallinn Manual ٢,٠) في قاعدته (٧١) هذا المعيار ذاته، مؤكداً أن تحديد ما إذا كان الهجوم السيبراني يشكل "استخداماً للقوة" يتوقف على آثاره ونتائجه، وليس على الأداة المستخدمة. غير أن التحدي يكمن في أن العديد من الهجمات السيبرانية لا تترك آثاراً مادية ملموسة، بل تتسبب في خسائر اقتصادية أو تعطيل خدمات رقمية، وهذه وإن كانت خطيرة إلا أنها قد لا تبلغ عتبة استخدام القوة وفق المعايير التقليدية.[٣٦]

يجب التمييز بدقة بين مفهوم "استخدام القوة" الوارد في المادة (٤/٢) وبين "الهجوم المسلح" الذي يبيح للدولة اللجوء إلى الدفاع الشرعي بموجب المادة (٥١) من الميثاق. فالهجوم المسلح هو درجة أعلى من استخدام القوة، ويتطلب آثاراً أكثر خطورة كالغزو أو القصف الواسع أو الخسائر البشرية الكبيرة. وقد كرّس دليل تالين ٢,٠ هذا التمييز في قاعدته (٧١) حيث اعتبر أن تقييم ما إذا كان العمل السيبراني يشكل "هجوماً مسلحاً" يتوقف على مقياسه وآثاره، مع الإشارة إلى أن مجرد تجاوز عتبة استخدام القوة لا يعني بالضرورة بلوغ عتبة الهجوم المسلح. وعليه، فإن العمليات السيبرانية التي تصل إلى عتبة استخدام القوة قد لا تصل بالضرورة إلى عتبة الهجوم المسلح. وهذا التفاوت يخل فجوة قانونية خطيرة تُعرف في الأدبيات المتخصصة بـ"المنطقة الرمادية" (Grey Zone): فالدولة التي تتعرض لهجوم سيبراني شديد لكنه دون عتبة الهجوم المسلح لا يحق لها قانوناً الرد بالقوة العسكرية التقليدية، بل يجب عليها الاكتفاء بإجراءات مضادة غير مسلحة كالعقوبات الاقتصادية أو الهجمات السيبرانية الانتقامية المقيدة. وتشير التقارير الدولية إلى أن معظم الهجمات السيبرانية المتبادلة بين الدول تقع في هذه المنطقة الرمادية، مما يجعل تحديد الردود المناسبة تحدياً قانونياً وسياسياً معقداً.[٣٧]

من منظور نقدي يرى الباحث أن تطبيق اختبار "المقياس والآثار" على العمليات السيبرانية، رغم كونه الإطار المعياري الوحيد المتاح حالياً – والمكرس في دليل تالين ٢,٠ وفي ممارسات دول عديدة مثل إستونيا وألمانيا والمملكة المتحدة – يعاني من قصور جوهري يعود إلى أن هذا الاختبار صُمم أصلاً لعالم مادي تترك فيه الوسائل التقليدية آثاراً ملموسة ومرئية. فالفضاء السيبراني يسمح بهجمات قد تكون ضخمة الآثار الاقتصادية أو الاجتماعية (كتعطيل شبكات مصرفية عالمية أو شل أنظمة النقل الجوي) دون أن تترك أي أثر مادي مباشر، وهو ما يجعلها، وفق التفسير الحرفي للمعيار، خارج نطاق حظر استخدام القوة، رغم أنها قد تسبب أضراراً تفوق في قيمتها بعض الهجمات المسلحة التقليدية. كما أن التمييز بين "استخدام القوة" و"الهجوم المسلح" يخلق فجوة خطيرة في نظام الردع، إذ تدرك الدول المهاجمة أنها قد تشن

هجمات سيبرانية مدمرة تقترب من عتبة الهجوم المسلح دون تجاوزها، مما يجعل الرد العسكري التقليدي غير مشروع. ويرى الباحث أن المجتمع الدولي بحاجة ماسة إلى تطوير معايير جديدة تأخذ في الاعتبار الأضرار الاقتصادية والاجتماعية الرقمية كمعادل وظيفي للأضرار المادية، أو إلى تعديل صريح للمادة (٥١) ليشمل الهجمات السيبرانية واسعة النطاق كحالة من حالات الدفاع الشرعي. وقد أشارت بعض الدراسات القانونية الحديثة إلى إمكانية الاستفادة من تجارب قانون الفضاء الخارجي في هذا المجال، لكنها تظل مقترحات نظرية لم تتبلور بعد في صكوك ملزمة. وإلى أن يحدث ذلك، ستبقى فجوة عدم التدخل المسلح في البيئة الرقمية ملاذاً آمناً للدول التي ترغب في ممارسة عدوان سيبراني دون خوف من رد عسكري تقليدي.

الفرع الثاني: إشكالية تحديد معيار الإكراه في الفضاء السيبراني

يُشكّل معيار "الإكراه" (Coercion) العنصر الجوهري في تحديد انتهاك مبدأ عدم التدخل المنصوص عليه في إعلان مبادئ القانون الدولي الصادر عن الجمعية العامة للأمم المتحدة (الإعلان ٢٦٢٥ لسنة ١٩٧٠)، والذي يُجسد قاعدة عرفية ملزمة. فلكي يُعتبر تدخل دولة ما في الشؤون الداخلية لدولة أخرى غير مشروع، يجب أن يتضمن فعلاً مقصوداً يهدف إلى إجبار تلك الدولة على سلوك معين في مجال تحفظه سيادتها، كاختيار نظامها السياسي أو الاقتصادي أو الاجتماعي. غير أن تطبيق هذا المعيار في الفضاء السيبراني يصطدم بطبيعة العمليات الرقمية التي غالباً ما تكون غير مباشرة، ومتعددة الطبقات، ويصعب فيها قياس عنصر القسر أو الإكراه. فهل يُعتبر اختراق أنظمة الانتخابات ونشر معلومات مضللة إكراهاً؟ أم أن الإكراه يتطلب تهديداً مباشراً باستخدام القوة أو أضراراً مادية جسيمة؟ هذه الإشكالية تخلق فراغاً تفسيرياً خطيراً تستغله الدول في تنفيذ عمليات تأثير دون وصولها إلى عتبة التدخل غير المشروع وفق المعايير التقليدية.[٣٨]

حاول دليل تالين ٢,٠ (القاعدة ٦٦) معالجة هذه الإشكالية بتقديم معيار أكثر تحديداً للإكراه في السياق السيبراني، حيث اعتبر أن الفعل السيبراني يُشكل تدخلاً غير مشروع إذا كان موجهاً بطبيعته إلى إجبار الدولة المستهدفة على اتخاذ قرار لا كانت لتتخذه لولا هذا الإكراه، وبشرط أن يصل الفعل إلى مستوى من الخطورة يحقق هذا القسر. غير أن هذا المعيار يظل فضفاضاً ويترك تقديره للظروف المحيطة. فعلى سبيل المثال، الهجوم السيبراني على نظام مصرفي مركزي بهدف إحداث انهيار اقتصادي قد يُعد إكراهاً إذا تسبب في شل القدرة على اتخاذ قرارات مالية سيادية. أما حملات التضليل الإعلامي الواسعة التي تهدف إلى التأثير على نتائج انتخابات، فرغم خطورتها، فإن إثبات أنها بلغت درجة "الإكراه" لا تتطلب مجرد تأثير بل حرمان المستهدفين

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

فعلياً من حرية الاختيار، وهو أمر بالغ الصعوبة في الإثبات القانوني. وتشير الدراسات إلى أن معظم العمليات السيبرانية المؤثرة تقع تحت عتبة الإكراه، مما يجعلها خارج نطاق حظر التدخل بالمعنى الدقيق.[٣٩]

على المستوى العربي، تُظهر الحالات التي تم توثيقها – كالهجمات السيبرانية التي استهدفت مؤسسات حكومية في دول عربية عدة خلال العقد الماضي – صعوبة بالغة في تطبيق معيار الإكراه، وذلك لأسباب متعددة أبرزها غياب الإرادة السياسية للتصعيد القانوني، وضعف القدرات التقنية للإسناد، وعدم وجود أحكام قضائية دولية في هذا المجال يمكن الاستناد إليها. وقد أشارت تحليلات متخصصة إلى أن الدول العربية تميل في الغالب إلى التعامل مع هذه العمليات كقضايا أمن سيبراني تقني أو كأعمال تجسس، بدلاً من مقاضاتها كانتهاكات لمبدأ عدم التدخل، مما يعكس هشاشة المعايير القانونية في مواجهة واقع عملياتي معقد. ويبقى السؤال مفتوحاً حول ما إذا كان التطور التكنولوجي سيؤدي إلى إعادة تعريف الإكراه ليشمل أشكالاً أكثر رقياً من الإجبار، كالتلاعب بالخوارزميات أو هجمات الذكاء الاصطناعي التي تستهدف أنظمة صنع القرار الآلي، أم أن القانون الدولي سيظل عاجزاً عن مواكبة هذه التطورات.[٤٠]

من منظور نقدي يرى الباحث أن إشكالية تحديد معيار الإكراه في الفضاء السيبراني تعكس أزمة أعمق في بنية القانون الدولي نفسه، الذي صُمم أصلاً لتنظيم العلاقات بين الدول في عالم مادي تقوم فيه السيادة على حدود ملموسة وقوة مادية ظاهرة. فمفهوم "الإكراه" يفترض وجود قدرة على إجبار دولة أخرى بشكل مباشر أو شبه مباشر، في حين أن معظم العمليات السيبرانية تعمل عبر التراكم والتأثير غير المباشر، وتستهدف العقول والتصورات والبيانات قبل أن تستهدف البنى المادية. وهذا يعني أن العتبة التقليدية للإكراه – التي تتطلب حرمان الدولة من خياراتها الأساسية – نادراً ما تتحقق في الفضاء السيبراني، رغم أن آثار العمليات السيبرانية قد تكون مدمرة للسيادة الوطنية بطرق أكثر دهاءً. والأكثر إشكالية هو أن بعض الدول الكبرى تتبنى تفسيراً ضيقاً لمبدأ عدم التدخل، لا يعتبر حملات التضليل الإلكتروني والتدخل في الأنظمة الانتخابية إكراهاً ما لم يصاحبها تهديد باستخدام القوة أو أضرار مادية مباشرة. وهنا يكمن الخلل: فالقانون الدولي، بتمسكه بمعيار الإكراه الجامد، يمنح الدول المتقدمة تقنياً ترخيصاً ضمنياً للتدخل في الشؤون الداخلية للدول الأخرى بوسائل رقمية، طالما أنها تتجنب تجاوز العتبة التقليدية. ويرى الباحث أن الحل لا يكمن في التخلي عن معيار الإكراه، بل في إعادة تفسيره بشكل ديناميكي يستوعب خصوصية التهديدات السيبرانية، من خلال اعتماد معيار "الإكراه الوظيفي" (Functional Coercion) الذي يقيس الأثر الفعلي على قدرة الدولة على ممارسة سيادتها،

وليس فقط وجود تهديد مادي أو قسر مباشر. كما ينبغي العمل على تطوير بروتوكول اختياري ملحق بإعلان ٢٦٢٥ يخص الفضاء السيبراني، يحدد بشكل عملي متى تصل العمليات الرقمية إلى درجة الإكراه المحظور. وإلى أن يحدث ذلك، سيبقى مبدأ عدم التدخل في البيئة الرقمية مجرد "نافذة زجاجية" يراها الجميع لكنها لا تمنع أحداً من العبور.

المطلب الثاني: الاستثناءات المسموح بها لمبدأ عدم التدخل

لا يخلو مبدأ عدم التدخل من استثناءات يجيزها القانون الدولي، أبرزها حق الدفاع عن المشروعية والتدخل بطلب من الدولة المتضررة، غير أن تطبيق هذه الاستثناءات في الفضاء السيبراني يثير إشكاليات قانونية تتعلق بالتناسب والإسناد. ويناقش هذا المطلب فرعين: حق الدفاع عن النفس السيبراني وفقاً لميثاق الأمم المتحدة، والتدخل بطلب من الدولة المتضررة كحالة إضفاء الشرعية.

الفرع الأول: حق الدفاع عن النفس السيبراني وفقاً لميثاق الأمم المتحدة

يُعد حق الدفاع عن النفس أحد الاستثناءات الجوهرية على حظر استخدام القوة المنصوص عليه في المادة (٤/٢) من ميثاق الأمم المتحدة، وقد كرسته المادة (٥١) من الميثاق باعتباره حقاً أصيلاً للدول إذا وقع "هجوم مسلح" ضدها. غير أن إعمال هذا الحق في الفضاء السيبراني يثير إشكالية قانونية كبرى تتمثل في تحديد متى يرقى الهجوم السيبراني إلى عتبة "الهجوم المسلح" التي تبرر اللجوء إلى القوة العسكرية رداً عليه. وقد استقر الرأي الفقهي الغالب، استناداً إلى معيار "المقياس والآثار" (Scale and Effects) الذي أقرته محكمة العدل الدولية في قضية نيكاراغوا (١٩٨٦)، على أن الهجمات السيبرانية لا تخول حق الدفاع عن النفس إلا إذا بلغت من الشدة والأثر ما يعادل الهجمات العسكرية التقليدية، كأن تتسبب في قتل أو إصابة أعداد من الأشخاص أو تدمير ممتلكات أو تعطيل بنى تحتية حيوية تعطيلاً واسع النطاق. وقد تبنى دليل تالين ٢,٠ في قاعدته (٧١) هذا المعيار ذاته، معتبراً أن تقييم ما إذا كان العمل السيبراني يشكل "هجوماً مسلحاً" يتوقف على مقياس آثاره ونتائجه، وليس على الوسيلة المستخدمة.[٤١]

إلى جانب معيار "المقياس والآثار"، يشترط القانون الدولي العرفي – كما كرسته محكمة العدل الدولية في قضية نيكاراغوا وقضية المنصات النفطية – شرطين أساسيين لممارسة حق الدفاع عن النفس، هما "الضرورة" و"التناسب". فالضرورة تعني أن يكون الرد المسلح هو السبيل الوحيد المتاح لمواجهة الهجوم المسلح بعد استنفاد الوسائل السلمية، أما التناسب فيقتضي ألا يتجاوز الرد ما هو ضروري لصد الهجوم وإنهائه، وأن يكون متناسباً مع شدته وحجمه. وفي

السياق السيبراني، تبرز تحديات إضافية تتمثل في سرعة الهجمات الرقمية التي قد تستغرق أجزاء من الثانية، مما يثير تساؤلات حول إمكانية تطبيق شرط الضرورة بالمعنى التقليدي الذي يفترض وجود مهلة زمنية للرد. وقد أشارت بعض الدول كأستراليا إلى إمكانية اللجوء إلى الدفاع الاستباقي عن النفس (Anticipatory Self-Defence) في مواجهة هجمات سيبرانية وشيكة ومؤكدة، شريطة أن يكون الخطر محدقاً ولا توجد وسيلة أخرى لدرئه. ويُقر دليل تالين ٢,٠ (القاعدتان ٧١ و٧٢) بهذا التوجه، مع تشديده على أن معايير الضرورة والتناسب تظل ملزمة بصرف النظر عن كون الهجوم مسلحاً تقليدياً أم سيبرانياً.[٤٢]

تتباين مواقف الدول من إمكانية تطبيق حق الدفاع عن النفس على الهجمات السيبرانية. ففي حين تؤكد وثيقة موقف ألمانيا (٢٠٢١) أن حق الدفاع عن النفس بموجب المادة (٥١) والمادة العرفية يمارس في مواجهة "هجوم مسلح" سيبراني بشرط توافر الضرورة والتناسب، تتبنى الولايات المتحدة موقفاً أكثر اتساعاً يجيز الرد بالقوة على أي استخدام غير مشروع للقوة سيبرانياً ولو لم يبلغ عتبة الهجوم المسلح، وهو موقف يعتبره الفقه الغالب رأياً شاذاً لا يعكس القانون العرفي. وتذهب دول أخرى كفرنسا وهولندا إلى تبني معيار "المقياس والآثار" نفسه مع تأكيدها على أن الرد السيبراني في إطار الدفاع عن النفس يجب أن يكون متناسباً ومحدوداً. أما على المستوى العربي، فلم تتبلور بعد مواقف رسمية واضحة ومعلنة من الدول العربية بشأن عتبة الهجوم المسلح السيبراني، وإن أشارت بعض التحليلات إلى ميل غالبية الدول العربية إلى تبني المقاربة التقليدية القائمة على الأضرار المادية، مع تحفظ على توسيع نطاق حق الدفاع عن النفس ليشمل أضراراً اقتصادية أو سياسية بحتة.[٤٣]

من منظور نقدي يرى الباحث أن إخضاع حق الدفاع عن النفس السيبراني لمعيار "الهجوم المسلح" المستمد من عالم مادي يخل فجوة خطيرة في نظام الردع الدولي، إذ تدرك الدول المهاجمة أنها قد تشن هجمات سيبرانية واسعة النطاق تسبب أضراراً اقتصادية واجتماعية هائلة (كتعطيل شبكات مصرفية عالمية أو شل أنظمة النقل الجوي) دون أن تصل إلى عتبة الهجوم المسلح بالمعنى التقليدي، مما يجعل الرد العسكري التقليدي غير مشروع والرد السيبراني المماثل عرضة للتحدي القانوني. وهذا الواقع يفسر لماذا لم تلجأ أي دولة حتى الآن إلى محكمة العدل الدولية للاحتجاج بهجوم سيبراني بوصفه مبرراً للدفاع عن النفس، واكتفت بدلاً من ذلك بردود فعل سياسية أو عقوبات اقتصادية أو هجمات سيبرانية انتقامية مصنفة ضمن إطار "الإجراءات المضادة" (Countermeasures) لا الدفاع عن النفس. والأكثر إشكالية هو أن غياب إجماع دولي حول معايير دقيقة لقياس "المقياس والآثار" في السياق السيبراني – وهل يشمل الأضرار

الاقتصادية المتراكمة أم يقتصر على الأضرار المادية الفورية – يترك الباب مفتوحاً أمام تفسيرات متباينة تسعى كل دولة إلى توظيفها لخدمة مصالحها الاستراتيجية. ويرى الباحث أن المجتمع الدولي في حاجة ماسة إلى صياغة بروتوكول اختياري ملحق بميثاق الأمم المتحدة يحدد بشكل عملي متى يرقى الهجوم السيبراني إلى "هجوم مسلح"، مع وضع معايير واضحة للإسناد والضرورة والتناسب تتناسب مع خصوصية الفضاء السيبراني، وإلا فإن المادة (٥١) ستبقى في الواقع العملي حبراً على ورق لا يردع الدول القوية تقنياً عن شن هجمات سيبرانية مدمرة تبقى بعناية تحت العتبة التي تبرر الرد العسكري.

الفرع الثاني: التدخل بطلب من الدولة المتضررة كحالة إضفاء الشرعية

يُعد تدخل دولة أو منظمة إقليمية بناءً على طلب الدولة المتضررة أحد الاستثناءات الراسخة لمبدأ عدم التدخل في الشؤون الداخلية، وقد كرسه القانون الدولي العرفي وإعلان مبادئ القانون الدولي الصادر عن الجمعية العامة للأمم المتحدة (الإعلان ٢٦٢٥ لسنة ١٩٧٠). غير أن الأساس القانوني الأكثر دقة لهذه الحالة في إطار قانون مسؤولية الدول يتمثل في المادة (٢٠) من مشروع مواد لجنة القانون الدولي (ARSIWA) لعام ٢٠٠١، والتي تنص على أن "رضا دولة ما بصورة صالحة على ارتكاب فعل معين من قبل دولة أخرى يستبعد وصف عدم المشروعية عن ذلك الفعل في علاقته بتلك الدولة، بقدر ما يبقى الفعل في حدود ذلك الرضا". وفي السياق السيبراني، يمكن للدولة المتضررة من هجوم سيبراني أن تطلب مساعدة دولة أخرى، سواء كانت مساعدة تقنية أو استخباراتية أو عسكرية، شريطة أن يكون الطلب صادراً عن السلطة الشرعية، وأن يقتصر التدخل على حدود الإذن، وألا يكون الرضا منتزعاً تحت الإكراه. غير أن تطبيق هذه القاعدة يصطدم بصعوبات عملية: كيف يمكن التحقق من صحة الرضا في ظل انقطاع الاتصالات الناجم عن الهجوم نفسه، أو في ظل اختراق أنظمة القيادة والتحكم التي قد ينطلق منها الطلب؟[٤٤]

تتعدد أشكال التدخل بطلب من الدولة المتضررة في الفضاء السيبراني، بدءاً من المساعدة الفنية البسيطة كإرسال فرق الاستجابة للحوادث السيبرانية (CERTs)، وصولاً إلى عمليات دفاع سيبراني مشترك أو حتى استخدام القوة إذا بلغ الهجوم مستوى "الهجوم المسلح" وكان الطلب موجهاً في إطار الدفاع الجماعي عن النفس بموجب المادة (٥١) من ميثاق الأمم المتحدة. وقد أقر دليل تالين ٢,٠ في قاعدته (٦٨) بأن "موافقة الدولة صاحبة الاختصاص تنفي عدم المشروعية عن أي تدخل سيبراني يكون ضمن حدود تلك الموافقة"، شريطة أن تكون الموافقة صالحة وتسبق الفعل أو تكون فورية. كما نصت القاعدة (٧٣) على أن دولة ثالثة قد تقدم

المساعدة لدولة تتعرض لهجوم مسلح سيبراني بناءً على طلبها، في إطار الدفاع الجماعي عن النفس. وتشير الدراسات الحديثة إلى أن فعالية هذا الاستثناء تتوقف على توافر آليات موضوعية للتحقق من صحة الطلب، كإخطار الأمين العام للأمم المتحدة أو هيئة إقليمية معتمدة، تحول الطلب إلى غطاء لتدخلات توسعية تحت ذريعة تقديم المساعدة.[٤٥]

على المستوى العربي، لم تُبلور بعد آليات واضحة ومعلنة للتدخل بناءً على طلب الدولة المتضررة في مواجهة الهجمات السيبرانية، رغم أن بعض الترتيبات الأمنية العربية كالاتفاقية العربية لمكافحة جرائم تقنية المعلومات (القاهرة ٢٠١٠) والاستراتيجية العربية للأمن السيبراني (٢٠١٧) تشير إلى مبدأ التعاون وتبادل المعلومات، لكنها لا تتضمن أحكاماً محددة بشأن إرسال قوات سيبرانية أو تقديم دعم عسكري بناءً على الطلب. وقد أظهرت دراسة حديثة أن الدول العربية تفضل التعاون الثنائي المحدود والمساعدات التقنية على حساب التدخلات الواسعة، خوفاً من المساس بالسيادة أو من استغلال المساعدات لأغراض تجسسية. غير أن بعض الدول المستهدفة بهجمات سيبرانية متكررة بدأت تتحول نحو توقيع اتفاقيات ثنائية للتعاون السيبراني تشمل شرط المساعدة المتبادلة عند الطلب، وإن بقيت هذه الاتفاقيات ذات طابع تقني واستخباراتي بعيداً عن البعد العسكري. ويظل التحدي الأكبر في ضمان أن الطلب صادر عن إرادة حرة وغير مفروض بفعل الإكراه السيبراني الذي قد يشل قدرة الدولة على اتخاذ القرار السيادي.[٤٦]

من منظور نقدي يرى الباحث أن إغفال معظم التحليلات العربية للمادة (٢٠) من مشروع مواد لجنة القانون الدولي عند مناقشة التدخل بطلب الدولة المتضررة يُعد فجوة منهجية خطيرة، لأن هذه المادة تمثل الإطار النظري الأكثر دقة لشروط صحة الرضا وآثاره القانونية، خاصة في بيئة سيبرانية تتسم بعدم اليقين الإسنادي. فالمادة (٢٠) تشترط أن يكون الرضا "صالاً" (validly given) ومعلناً، وأن يبقى الفعل ضمن حدود ذلك الرضا. وفي الفضاء السيبراني، تنشأ إشكالية كبرى حول معنى "الرضا الصالح" عندما يكون الطلب صادراً من حكومة ربما تكون تحت تأثير اختراق سيبراني أثر على أنظمة اتخاذ قرارها، أو عندما يكون الطلب قد تم عبر قنوات اتصال غير آمنة يُحتمل عبث جهة خارجية بها. كما أن غياب إجراءات موحدة للتحقق من الرضا – كشرط الإخطار المسبق للأمين العام للأمم المتحدة أو لهيئة إقليمية – يجعل من السهل إساءة استخدام هذا الاستثناء لتبرير تدخلات غير مشروعة، خصوصاً في النزاعات الإقليمية العربية حيث تتداخل المصالح السياسية مع الادعاءات التقنية. ويرى الباحث أن الحل لا يكمن في رفض هذه الآلية، بل في تطوير بروتوكول إقليمي عربي ملزم يحدد إجراءات صارمة للتحقق من

صحة طلب التدخل السيبراني، بما في ذلك وجوب توثيق الطلب عبر قنوات دبلوماسية متعددة ومستقلة، وإخطار جامعة الدول العربية فوراً، ووضع حد زمني أقصى للتدخل لا يمكن تجاوزه إلا بموافقة جديدة. كما ينبغي أن تتضمن الاتفاقيات الثنائية والقارية نصوصاً واضحة تحيل إلى مبادئ المادة (٢٠) من ARSIWA وتفسيرات دليل تالين ٢,٠ ذات الصلة. وإلى أن يتحقق ذلك، سيبقى التدخل بطلب الدولة المتضررة في الفضاء السيبراني استثناءً نظرياً أكثر منه أداة عملية قابلة للتطبيق الآمن، مما يدفع الدول المتضررة إما إلى تحمل الأضرار بصمت أو إلى اللجوء إلى إجراءات مضادة أحادية قد تكون أكثر خطورة على الاستقرار الإقليمي.

المطلب الثالث: التحديات الإجرائية لتطبيق المبدأ على الجرائم السيبرانية

تواجه الإجراءات القانونية الرامية إلى تطبيق مبدأ عدم التدخل على الجرائم السيبرانية عقبات كبيرة، أبرزها صعوبة إثبات نية التدخل في الأنشطة غير المباشرة، وتفوق التطور التكنولوجي على القواعد التقليدية. وسيبين هذا المطلب من خلال فرعين: صعوبة إثبات نية التدخل في الأنشطة غير المباشرة، وتضارب القواعد التقليدية مع سرعة التطور التكنولوجي.

الفرع الأول: صعوبة إثبات نية التدخل في الأنشطة غير المباشرة

يُشكل الركن المعنوي، والمتمثل في القصد الدولي إلى إكراه الدولة المستهدفة، ركناً مستقلاً لا بد من توافره – إضافة إلى الإسناد – لقيام مسؤولية الدولة عن انتهاك مبدأ عدم التدخل. وقد استقر في قضاء محكمة العدل الدولية في قضية نيكاراغوا (١٩٨٦) أن مجرد دعم قوى المعارضة لا يشكل تدخلاً غير مشروع ما لم يتوافر عنصر الإكراه المقصود، أي أن تهدف الدولة الفاعلة إلى حمل الدولة المتلقية على سلوك معين في مجال تحتفظ بولايتها عليه. غير أن صعوبة إثبات هذا الركن المعنوي في البيئة السيبرانية تتضاعف بسبب طبيعة الأنشطة غير المباشرة التي تلجأ فيها الدول إلى قراصنة مجهولي الهوية، أو مجموعات إلكترونية لا تحمل صفة رسمية، أو برمجيات خبيثة تدار من خوادم وسيطة، مما يحجب الصلة بين الإرادة الحكومية والفعل الضار. وهذا يقتضي التمييز الدقيق بين مرحلتين: الأولى إسناد الفعل مادياً إلى الدولة وفقاً للمادة الثامنة من مشروع مواد لجنة القانون الدولي لعام ألفين وواحد، والثانية إثبات أن الفعل المسند قد صدر بقصد الإكراه. وفي الفضاء السيبراني، تكمن الصعوبة الكبرى في كلا المرحلتين معاً.

في ما يخص مرحلة الإسناد المادي، تنص المادة الثامنة من مشروع مواد لجنة القانون الدولي لعام ألفين وواحد على أن سلوك شخص أو مجموعة من الأشخاص يُعتبر فعلاً منسوباً إلى الدولة إذا كان هؤلاء الأشخاص يعملون بالفعل "بتعليمات من الدولة أو بتوجيهها أو تحت

سيطرتها". وقد أقرت محكمة العدل الدولية في قضية نيكاراغوا معيار "السيطرة الفعالة" كمعيار للإسناد، وهو ما تتبعه دليل تالين في قاعدته السابعة عشرة المتعلقة بمسؤولية الدولة عن أعمال القراصنة والمجموعات الإلكترونية غير الحكومية. ويختلف هذا المعيار جوهرياً عن معيار "السيطرة الشاملة" الذي طرحته محكمة يوغوسلافيا السابقة في قضية تاديتش والذي رفضته محكمة العدل الدولية صراحة في قضية الإبادة الجماعية في البوسنة (عام ألفين وسبعة) باعتباره غير مناسب لإسناد المسؤولية للدول. وفي السياق السيبراني، يكمن التحدي في أن الدولة قد تقدم دعماً تقنياً أو مالياً أو معلوماتياً لقراصنة دون أن تصدر إليهم تعليمات محددة بكل عملية، مما يجعل إثبات "السيطرة الفعالة" بالمعنى النيكاراغوي أمراً شاقاً بل شبه متعذر، إذ يصعب الكشف عن سلسلة الأوامر الصادرة من مراكز القرار الحكومية إلى المنفذين غير الرسميين.

أما مرحلة إثبات الركن المعنوي الخاص بالتدخل (القصد إلى الإكراه)، فتستند إلى قواعد متميزة عن قواعد الإسناد، وقد حاول دليل تالين في قاعدته السادسة والستين وضع معيار وظيفي لها ينص على أن الفعل السيبراني يُعد تدخلاً غير مشروع إذا كان موجهاً بطبيعته إلى إكراه الدولة المستهدفة، ويتطلب توافر أدلة على أن الدولة الفاعلة قد قصدت هذا الإكراه، أو أن الإكراه كان نتيجة متوقعة بشكل معقول لسلوكها. غير أن هذا المعيار، رغم كونه الأداة التفسيرية المتاحة، يظل فضفاضاً من حيث آليات التطبيق القضائي. فكيف يمكن إثبات أن دولة ما قد قصدت إكراه أخرى عبر هجوم انطلق من خادم يقع على أراضيها لكنه مستأجر من شركة خاصة؟ أو عبر برمجية خبيثة صممت لتُنسب تلقائياً إلى طرف ثالث؟ تشير الدراسات القانونية إلى أن لجوء الدول إلى "التوكيل السيبراني" لا يعقد مرحلة الإسناد فحسب، بل يحجب أيضاً الأدلة على القصد، إذ يمكن للدولة أن تدعي أنها لم تقصد الإكراه بل كانت تقوم بتجارب دفاعية، أو أن المجموعة المهاجمة تصرفت بمبادرة ذاتية خارج نطاق توجيهاتها. وبذلك تتداخل صعوبتا الإسناد وإثبات القصد لتخلقا حاجزاً مرتفعاً أمام إقامة المسؤولية الدولية.[٤٧]

على الصعيد العربي المقارن، تتفاقم هذه الصعوبات بسبب محدودية القدرات التقنية للدول العربية في تتبع مسار الهجمات السيبرانية وتجميع القرائن الإسنادية، إضافة إلى ندرة اتفاقيات التعاون القضائي لتبادل الأدلة الرقمية. وتشير الرسائل الجامعية المتخصصة إلى أن غياب سوابق قضائية عربية في هذا المجال يحول دون تبلور تفسير موحد لمعيار "السيطرة الفعالة" أو لمفهوم "القصد إلى الإكراه" في السياق السيبراني، مما يخل فجوة قانونية تتيح للدول التي تنتهك مبدأ عدم التدخل الإفلات من المساءلة. كما أن الإرادة السياسية للجوء إلى آليات التسوية القضائية أو التحكيمية تكاد تكون منعدمة، إذ يُنظر إلى النزاعات السيبرانية غالباً على أنها

مسائل أمنية تُعالج بقنوات سرية، لا كمنازعات قانونية تخضع للفصل القضائي. وهذا الواقع يُضعف أي جهد لبناء ممارسة دولية عربية موحدة بشأن معايير الإسناد والركن المعنوي، ويُبقي المسألة أسيرة للتقدير السياسي الأحادي.[٤٨]

من منظور نقدي يرى الباحث أن الخلط بين الإسناد والركن المعنوي في كثير من التحليلات القانونية العربية يعكس أزمة منهجية أعمق، إذ يُفترض في القانون الدولي أن الإسناد يسبق بحث الركن المعنوي منطقياً وزمنياً، لكن في الفضاء السيبراني تنهار هذه الأولية لأن الأدلة ذاتها التي تثبت الإسناد (كالقرائن التقنية على مصدر الهجوم) قد تكون هي نفسها التي يستند إليها في استخلاص القصد. ومع ذلك، يظل الفصل بينهما ضرورياً من الناحية النظرية. والأكثر إشكالاً هو أن معيار "السيطرة الفعالة" الذي أقرته محكمة العدل الدولية – وهو المعيار الوحيد المعتمد في قانون مسؤولية الدول وفي دليل تالين – ثبتت صعوبة تطبيقه في سياق التوكيل السيبراني، حيث تكتفي الدولة بتزويد القراصنة ببرمجيات حصرية أو تمويل أو حماية دبلوماسية دون إصدار أوامر محددة بكل عملية، مما يجعل إثبات السيطرة على التفاصيل الجزئية للهجوم شبه مستحيل. وقد رفضت محكمة العدل الدولية في قضية الإبادة الجماعية في البوسنة (عام ألفين وسبعة) الانتقال إلى معيار "السيطرة الشاملة" الأقل صرامة، مؤكدة تمسكها بمعيار السيطرة الفعالة. ويرى الباحث أن هذا التمسك، رغم قيمته في حماية السيادة الوطنية، يخل فجوة خطيرة في مجال المسؤولية عن الهجمات السيبرانية غير المباشرة، إذ يوفر للدول المعتدية ملاذاً قانونياً آمناً طالما حافظت على درجة من الفصل التنظيمي بين أجهزتها الرسمية والمجموعات المهاجمة. والحل – في تقدير الباحث – لا يكمن في التخلي عن معيار السيطرة الفعالة، بل في تطوير آليات استدلالية قضائية تعتمد على القرائن الموضوعية المتراكمة (كاستمرار الهجمات من ذات البنية التحتية، أو استخدام أدوات برمجية لا تتوفر إلا للدولة المعنية) لتخفيف عبء الإثبات على الدولة المتضررة، مع بقاء عبء الإثبات الأساسي على عاتقها. كما ينبغي العمل على إنشاء سجل دولي للحوادث السيبرانية المسندة تقنياً، يُعهد إلى فريق خبراء مستقل بإصدار تقارير ترجيحية غير ملزمة تُستخدم كقرائن أمام الهيئات القضائية أو التحكيمية، دون أن تحل هذه التقارير محل الإثبات القضائي المباشر. وإلى أن يتحقق ذلك، سيظل الجمع بين صعوبة الإسناد وصعوبة إثبات القصد عقبة كأداء تحول دون إقامة المسؤولية الدولية عن انتهاك مبدأ عدم التدخل في الفضاء السيبراني.

الفرع الثاني: تضارب القواعد التقليدية مع سرعة التطور التكنولوجي

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

تتبنى القواعد التقليدية للقانون الدولي، كتلك المتعلقة بالسيادة الإقليمية والإسناد والمسؤولية، على افتراض وجود فعل مادي يمكن تتبعه إلى فاعل محدد ضمن حدود جغرافية واضحة. بيد أن العمليات السيبرانية تفتقر في الغالب إلى هذه المادية، إذ يمكن أن تنطلق الهجمات من خوادم وسيطة في عشرات الدول، باستخدام برمجيات تُغير مسارها تلقائياً، وتستهدف بنى تحتية غير ملموسة كقواعد البيانات وأنظمة التحكم عن بُعد. وقد أشارت دراسات حديثة إلى أن الطبيعة غير المادية للهجمات الرقمية، مقترنة بصعوبة إسنادها إلى دولة بعينها، أحدثت فراغاً قانونياً أضعف فعالية قواعد المسؤولية الدولية التي صُممت أصلاً لتنظيم أفعال مادية كالغزو أو القصف أو الاجتياح العسكري. فكيف يمكن تطبيق معيار "الضرر المباشر" على هجوم سيبراني تسبب في خسائر اقتصادية هائلة دون أن يترك أثراً مادياً واحداً؟ وكيف يمكن إعمال قاعدة "السببية" في بيئة تعبر فيها الحزمة الرقمية عشرات الحدود في جزء من الثانية؟[٤٩]

يتجلى أشد مظاهر التضارب في مفهوم "الهجوم المسلح" ذاته، إذ تفترض المادة (٥١) من ميثاق الأمم المتحدة وقوع "هجوم مسلح" دون أن تحدد هذا المفهوم، وهو ما فسرته محكمة العدل الدولية في قضية نيكاراغوا (١٩٨٦) بناءً على معيار "المقياس والآثار" للتمييز بين الهجوم المسلح ومجرد الحوادث الحدودية. غير أن العمليات السيبرانية قد تحدث أضراراً تعادل – بل تفوق – آثار الهجوم العسكري التقليدي، كما في حالة تعطيل شبكة كهرباء وطنية أو شل نظام مالي عالمي، مع بقائها ضمن الإطار غير المادي. وهذا الوضع يخل "منطقة رمادية" قانونية خطيرة، إذ لا تستطيع الدولة المتضررة اللجوء إلى الدفاع الشرعي عن النفس لأن الهجوم لم يبلغ – في التفسير الحرفي للقواعد التقليدية – عتبة "الهجوم المسلح"، وفي الوقت نفسه لا تجد في القواعد الوضعية ما يجرم هذا السلوك بشكل واضح. وقد ذهبت بعض الآراء الفقهية إلى أن قواعد القانون الدولي الإنساني، رغم بقائها معتبرة وملزمة، تواجه تحديات غير مسبوقة في تنفيذها في الفضاء السيبراني، إذ إن الأهداف في أي نزاع سيبراني ستكون غالباً مدنية وليست عسكرية، وسيقع ضررها على السكان أكثر مما يقع على القوات المسلحة. وهذا من شأنه أن يخل صعوبات في تطبيق مبادئ التمييز والتناسب والاحتياط التي كرستها اتفاقيات جنيف والبروتوكولات الملحقة بها.[٥٠]

تتفاقم حدة هذا التضارب حين تُقحم التقنيات المستجدة كالذكاء الاصطناعي في العمليات السيبرانية، حيث أصبحت الهجمات تُشن بواسطة خوارزميات ذاتية التعلم قادرة على تعديل مسارها وأسلوبها دون تدخل بشري، مما يطرح إشكالاً قانونياً غير مسبوق حول الإسناد: لمن تُنسب هجمة نفذها نظام ذكي تصرف بمبادرة ذاتية بعد أن زودته الدولة بالهدف العام فقط؟ كما

أن وتيرة التطور التكنولوجي المتسارعة تجعل أي محاولة لوضع قواعد قانونية جامدة محكوم عليها بالتقادم السريع، إذ تفيد الدراسات أن دورة حياة التقنية السيبرانية الهجومية قد تقل عن ثمانية عشر شهراً، بينما تستغرق عملية التفاوض على معاهدة دولية جديدة – في أحسن الأحوال – عدة سنوات. وقد خلصت تحليلات حديثة إلى وجود فراغ قانوني دولي واضح فيما يتعلق بتنظيم الفضاء السيبراني، مما أدى إلى تعدد التوجهات واختلاف التشريعات الوطنية، الأمر الذي يستدعي إنشاء هيئة دولية متخصصة تعنى بمتابعة الجرائم السيبرانية وتنظيم استخدام الذكاء الاصطناعي. غير أن مثل هذه المقترحات تظل أسيرة الخلافات السياسية بين الدول الكبرى.[٥١]

يتضح من خلال التحليل المقارن أن تضارب القواعد التقليدية مع سرعة التطور التكنولوجي ليس مجرد فجوة قانونية عابرة، بل هو أزمة بنيوية في فلسفة القانون الدولي نفسه. فالقواعد التقليدية تقوم على افتراضات ضمنية ثلاث: أولاً، أن الفعل الضار سيكون مادياً ويمكن تتبعه عبر حدود واضحة؛ ثانياً، أن ثمة مهلة زمنية كافية بين الفعل ورد الفعل لتطبيق آليات المساءلة؛ ثالثاً، أن صانع القرار القانوني والقضائي سيكون قادراً على فهم طبيعة الفعل محل النزاع. والفضاء السيبراني ينقض هذه الافتراضات الثلاثة جميعاً في آن واحد. والأكثر خطورة من الناحية العملية هو أن سرعة التطور التكنولوجي تخلق فجوة معرفية بين "من يضع القواعد" و"من يملك القدرات التقنية"، حيث تميل الدول الأكثر تقدماً في المجال السيبراني إلى الدفع بقواعد فضفاضة تترك لها مساحة واسعة للمناورة، بينما تطالب الدول الأقل تقدماً بقواعد محددة وملزمة تحميها من التهديدات التي لا تستطيع مجاراتها دفاعياً. وهذه الفجوة المعرفية تجعل عملية وضع القواعد عرضة للسيطرة من قبل الجهات صاحبة المصلحة في إبقاء الأمور غامضة، بدلاً من أن تخضع لمنطق الضبط القانوني الموضوعي. ويرى الباحث أن الحل لا يكمن في التخلي عن القواعد التقليدية واستبدالها بأخرى جديدة – فهذا سيدخل المجتمع الدولي في دوامة من عدم الاستقرار القانوني – بل في تطوير تفسير ديناميكي لتلك القواعد يستوعب خصوصية التقنيات الرقمية، مع إنشاء آليات تنفيذ سريعة ومتخصصة، كإنشاء غرفة استئناف سيبرانية تابعة لمحكمة العدل الدولية ذات اختصاص استعجالي، مع الاستعانة بخبراء تقنيين بصفة مقررين دائمين. وإلى أن يتحقق ذلك، سيظل القانون الدولي في مضمار الهجمات السيبرانية متخلفاً بخطوات عدة عن الواقع التقني الذي يفترض أنه ينظمه، وسيبقى الفضاء السيبراني بمثابة إقليم بلا قانون في كثير من جوانبه الحيوية. **النتائج**

١. تُظهر الدراسة المقارنة أن غياب معاهدة دولية شاملة وملزمة تحدد معايير السيادة السيبرانية والعناية الواجبة، إلى جانب تمسك القانون الدولي بمعيار "السيطرة الفعالة" المنصوص

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

عليه في المادة الثامنة من مشروع مواد لجنة القانون الدولي لعام ألفين وواحد والقاعدة السابعة عشرة من دليل تالين ٢,٠، يخلق فراغاً قانونياً خطيراً. فالدول المتقدمة تقنياً تستغله لشن هجمات سيبرانية مدمرة عبر ما يعرف بـ "التوكيل السيبراني"، تبقى عمداً تحت عتبة "الهجوم المسلح" المنصوص عليها في المادة الحادية والخمسين من ميثاق الأمم المتحدة والقاعدة الحادية والسبعين من دليل تالين، مما يعيق عملياً تطبيق حق الدفاع الشرعي عن النفس ويحول دون مساءلتها قانونياً.

٢. يتبين من التحليل التطبيقي أن معايير الإسناد التقليدية ثبتت صعوبة بل استحالة تطبيقها في سياق التوكيل السيبراني، إذ تكتفي الدولة بتزويد القراصنة ببرمجيات حصرية أو تمويل أو حماية دبلوماسية دون إصدار أوامر محددة بكل عملية، مما يجعل إثبات "السيطرة الفعالة" شبه متعذر. وقد رفضت محكمة العدل الدولية صراحة في قضية الإبادة الجماعية في البوسنة عام ألفين وسبعة معيار "السيطرة الشاملة" الذي أشارت إليه القاعدة الخامسة عشرة من دليل تالين ٢,٠، وأصرت على معيار السيطرة الفعالة، مما يخلق فجوة خطيرة في المسؤولية عن الهجمات السيبرانية غير المباشرة ويوفر ملاذاً قانونياً آمناً للدول المعتدية.

٣. خلصت المقارنة القانونية إلى أن الإجراءات التشريعية العربية الحالية، كقانون الجرائم الإلكترونية الأردني رقم سبعة عشر لسنة ألفين وثلاثة وعشرين ومشروع قانون الجرائم المعلوماتية العراقي غير المعتمد، تركز على النمط الردعي المتمثل في عقاب الجريمة بعد وقوعها، وتهمل الرقابة الاستباقية على الكيانات الخاصة، مما يضعف فعالية قاعدة العناية الواجبة المنصوص عليها في القاعدة السادسة من دليل تالين ٢,٠. في المقابل، أظهر الأمر الجزائري رقم تسعة وأربعة لسنة ألفين وتسعة نموذجاً أكثر تفصيلاً في إلزام مزودي الخدمات بالتعاون القضائي والإداري، لكنه يظل ناقصاً من زاوية الرقابة الوقائية الدورية المتمثلة في التدقيق المستمر والإبلاغ الفوري عن الثغرات قبل استغلالها.

٤. أثبتت الدراسة وجود تباين جوهري بين تفسير مبدأ عدم التدخل في القانون الدولي التقليدي كما ورد في إعلان مبادئ القانون الدولي الصادر عن الجمعية العامة للأمم المتحدة رقم ٢٦٢٥ لسنة ألف وتسعمائة وسبعين، والذي يشترط عنصر "الإكراه" المادي المباشر، وبين طبيعة العمليات السيبرانية التي تعمل عبر التراكم والتأثير غير المباشر على العقول والتصورات قبل أن تستهدف البنى المادية. فالقاعدة السادسة والستون من دليل تالين ٢,٠ اعتبرت الفعل السيبراني تدخلاً غير مشروع إذا كان موجهاً إلى إكراه الدولة المستهدفة، لكن معيار "الإكراه الوظيفي" لا

يزال غير مقرر في الممارسة الدولية، مما يمنح الدول المتقدمة تقنياً ترخيصاً ضمنياً للتدخل الرقمي في الشؤون الداخلية للدول الأخرى.

٥. تكشف المعالجة التشريعية والمقارنة أن غياب آلية دولية مستقلة ومتخصصة لتقصي الحقائق التقنية والقانونية يحول دون تحقيق العدالة في الفضاء السيبراني. فالدول الأقل قدرة تقنياً، كالعراق وبعض الدول العربية، تعجز عن تلبية عبء الإثبات المطلوب لإقامة المسؤولية الدولية بموجب المادتين الثانية والحادية والثلاثين من مشروع مواد لجنة القانون الدولي لعام ألفين وواحد، بينما تستطيع الدول الكبرى التي تمتلك القدرات التقنية المتقدمة أن تقدم أدلة "مقنعة" تُسند بموجبها الهجمات إلى خصومها، مما يخلق حالة من "الإسناد الانتقائي" تتعارض مع مبدأ المساواة في السيادة المنصوص عليه في المادة الثانية فقرة أولى من ميثاق الأمم المتحدة.

التوصيات

١. يوصي البحث بضرورة أن يتبنى المشرع العراقي قانوناً شاملاً للجرائم المعلوماتية، يُستكمل في إطار زمني مقترح لا يتجاوز ثمانية عشر شهراً، يُعرِّف فيه الهجمات السيبرانية ويحدد عقوباتها تصاعدياً وفقاً لجسامة الضرر، مع نص صريح على مسؤولية الشخص الاعتباري إذا سهلت إهماله الجسيم وقوع الهجوم. كما ينبغي أن يتضمن القانون آليات رقابية وقائية، على سبيل المثال: إلزام الكيانات الخاصة المشغلة للبنية التحتية الحيوية بإجراء تدقيقات أمنية دورية مستقلة كل ستة أشهر، والإبلاغ الفوري عن أي ثغرة مكتشفة خلال أربع وعشرين ساعة، وفرض تراخيص أمنية مشروطة قابلة للسحب عند الإخلال بالمعايير، مع إنشاء هيئة وطنية مستقلة للإشراف على التنفيذ، والاستفادة من التجربة الجزائرية في الأمر رقم تسعة وأربعة والتجربة الأردنية لتلافي عيوب النصوص الفضفاضة.

٢. من الضروري أن تعمل السلطات التنفيذية والدبلوماسية العراقية، بالتنسيق مع جامعة الدول العربية، على الإسراع بالتصديق على اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لعام ألفين وأربعة فور دخولها حيز النفاذ، مع تقديم تحفظات محدودة تحفظ السيادة الوطنية. كما ينبغي التفاوض على بروتوكول عربي إقليمي ملزم للتدخل السيبراني بناءً على طلب الدولة المتضررة، استناداً إلى المادة العشرين من مشروع مواد لجنة القانون الدولي والقاعدة الثامنة والستين من دليل تالين ٢,٠، يتضمن إجراءات للتحقق من صحة الطلب كإخطار الأمانة العامة لجامعة الدول العربية خلال أربع وعشرين ساعة، ووضع حد زمني أقصى للتدخل لا يتجاوز ثلاثين يوماً إلا بموافقة جديدة، وآلية رقابية قضائية إقليمية للفصل في النزاعات المتعلقة بشرعية التدخل.

٣. ينبغي على السلطات القضائية والأكاديمية العراقية العمل على بناء قدرات تقنية وقانونية متخصصة من خلال إنشاء وحدة قضائية فنية ملحقة بمجلس القضاء الأعلى، تختص بتدريب القضاة والمحققين على مفاهيم الإسناد القانوني والركن المعنوي للجرائم السيبرانية، وجمع الأدلة الرقمية وتحليلها وفق معايير دليل تالين ٢,٠ وتقرير فريق الخبراء الحكوميين، وذلك في إطار زمني مقترح لا يتجاوز ثلاثة أعوام، مع تخصيص ميزانية سنوية كافية لهذه الوحدة. كما يوصى بتوقيع اتفاقيات ثنائية متعددة مع الدول العربية والصديقة، على سبيل المثال خمس اتفاقيات خلال عامين، لتسريع تبادل الأدلة الإلكترونية والتعاون القضائي في المسائل السيبرانية، مع مراعاة الضوابط الدستورية والقانونية العراقية وبخاصة فيما يتعلق بحرمة البيانات الشخصية وحق الخصوصية.

الهوامش

[١] محمد الصغير مسيكة، ٢٠٢٢، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، بغداد، ص٤٥.

[٢] ضحى لعيبي كاظم، ٢٠٢١، البعد الجيو سياسي للأمن السيبراني، مجلة العلوم الإنسانية، بابل العراق، ص١١٢.

[٣] نورة شلوش، ٢٠١٨، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الإنسانية، بابل العراق، ص٨٩.

[4] Brenner, S. W., & Koops, B. J., ٢٠٠٤"Approaches to Cybercrime Jurisdiction" ، Journal of High Technology Law ،Suffolk University Law School ،Boston ،Volume ٤، Issue ١، p. ٣.

[٥] جامعة الدول العربية، ٢٠١٠، "الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات"، الأمانة العامة لجامعة الدول العربية – قطاع الشؤون القانونية، القاهرة، المواد (٢)، (٣٠)، (٣١).

[٦] إياد خالد عدوان، ٢٠٠٧، "مدى تقبل المواطنين للحصول على الخدمات من خلال الحكومة الإلكترونية (دراسة حالة قطاع غزة)"، الجامعة الإسلامية، غزة، ص ٤٥.

[٧] سهيل حسين الفيتلي، ٢٠٠٢، الوسيط في القانون الدولي العام، دار الفكر العربي، بيروت، ص ١٢٥.

[٨] محمد الصغير مسيكة، ٢٠٢٢، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، بغداد، ص ٤٥.

[٩] شريفة كلاع، ٢٠٢٢، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، الجزائر، ص ١١٢.

[١٠] عروس فوزية، ٢٠٢٦، "إشكالية الموازنة بين متطلبات الأمن السيبراني وضمان الحقوق الفردية"، المجلة الأكاديمية للدراسات الاجتماعية والإنسانية، الجزائر، المجلد ١٨، العدد ١، ص ٢٦٠.

[11] سارة خليل عبد الكريم سمرين، ٢٠٢٤، "القيود الواردة على حرية الرأي والتعبير في قانون الجرائم الإلكترونية (دراسة مقارنة)"، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ص ٤٥.

[12] المبيضين، عبد الرحمن عمر محمد، ٢٠٢٥، "الإطار القانوني للحقوق الرقمية: بين الحماية الدستورية والتنظيم الإداري"، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، المجلد ٦، العدد ٢، ص ١٩.

[13] مجلس أوروبا، ٢٠٠١، "التقرير التفسيري لاتفاقية الجريمة الإلكترونية"، سلسلة المعاهدات الأوروبية رقم ١٨٥، مجلس أوروبا، ستراسبورغ، الفقرات ٢٣١.

[14] جامعة الدول العربية، ٢٠١٠، "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"، الأمانة العامة لجامعة الدول العربية، القاهرة، المواد (٣٠)، (٣١)، (٣٢).

[15] خميس جمعة الشهواني، ٢٠٢٦، "إشكالية تحديد الاختصاص القضائي في الجرائم الإلكترونية"، مجلة الشرق الأوسط للدراسات القانونية والفقهية، المجلد ٦، العدد ١، ص ١٥١.

[16] Peter Swire, Jennifer Daskal, Théodore Christakis, ٢٠١٨, "The globalization of criminal evidence", IAPP, (article published online), paragraphs ١–٨.

[17] جامعة الدول العربية، ٢٠١٠، "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"، الأمانة العامة لجامعة الدول العربية، القاهرة، المواد (٣٠)، (٣١).

[18] طلال عبد الله المطيري، ٢٠٢٣، "مبدأ عدم الإضرار في القانون الدولي وتطبيقاته في الفضاء السيبراني"، مجلة الحقوق والعلوم السياسية، جامعة الكويت، المجلد ١٤، العدد ٣، ص ٤٥.

[19] Michael N. Schmitt (ed.)، ٢٠١٧، "Tallinn Manual ٢,٠on the International Law Applicable to Cyber Operations"، Cambridge University Press، Cambridge ، القاعدة ٦، الصفحات ٣٠–٣٥.

[20] حليمة الدرمكي، وائل علام، ٢٠٢٥، "المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول"، مجلة العلوم القانونية، جامعة الشارقة، المجلد ٢١، العدد ٤، الصفحات ١٨.

[21] لجنة القانون الدولي، ٢٠٠١، مشروع مواد بشأن مسؤولية الدول عن الأفعال غير المشروعة دولياً، الأمم المتحدة، نيويورك، المواد (٤)، (٨)، التعليقات.

[22] Michael N. Schmitt (ed.), ٢٠١٧, Tallinn Manual ٢,٠on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge , القاعدة ١٥، الصفحات ٨٠–٨٥.

[23] جامعة الدول العربية، ٢٠١٠، "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"، الأمانة العامة لجامعة الدول العربية، القاهرة، المواد (٢٣)، (٢٤)، (٢٥).

[24] أحمد أبو الوفا، ١٩٩٦، الوسيط في القانون الدولي العام، دار النهضة العربية، القاهرة، ص٣٨.

[25] هبة جمال الدين، ٢٠٢٣، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، بغداد، ص١٨٩.

[٢٦] مصطفى إبراهيم سلمان الشمري، ٢٠٢١، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، جامعة ديالى، العراق، ص٤٠٩.

[٢٧] علي صادق أبو هيف، ١٩٩٥، القانون الدولي العام، منشأة المعارف، الإسكندرية، ص١٠٣.

[٢٨] مصطفى إبراهيم سلمان الشمري، ٢٠٢١، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، جامعة ديالى، العراق، ص٤٠٩

[٢٩] شريفة كلاع، ٢٠٢٢، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، الجزائر، ص٢٩٢.

[30] International Law Commission, ٢٠٠١, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc A/١٠/٥٦, Articles ٢, ٣١, ..٣٧-٣٤

[31] NATO CCD COE, ٢٠١٧, Tallinn Manual ٢,٠on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge, Rules ٤, . ٧١

[٣٢]أحمد أبو الوفا، ١٩٩٦، الوسيط في القانون الدولي العام، دار النهضة العربية، القاهرة، ص٣٨ .

[٣٣] عبد القادر القادري، ١٩٨٤، القانون الدولي العام، مكتبة المعارف، الرباط، ص٩٢.

[٣٤] سعيد الركراكي، ١٩٩١، مقترب في دراسة العلاقات الدولية، المطبعة والوراقة الوطنية، مراكش، ص١١٧.

[٣٥] دخلافي سفيان، ٢٠٢٢، تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي، المجلة الأكاديمية للبحث القانوني، العدد ٢، المجلد ١٣، ص٣٠٣-٣٢٣.

[٣٦] ولهي المختار، ٢٠٢٥، القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكانياته، مجلة البحوث في الحقوق والعلوم السياسية، المجلد ١١، العدد ٢، ص٢٥٦-٢٨٢.

[37] NATO CCD COE ،٢٠١٧ ،Tallinn Manual ٢,٠on the International Law Applicable to Cyber Operations ،Cambridge University Press ،Cambridge ،Rules ٦٩، ٧١، ٧٢.

[٣٨] هبة جمال الدين، ٢٠٢٣، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، مج٢٤، ع١، ص ص. ١٨٩-٢٣٠.

[٣٩] حازم محمد خليل، ٢٠٢٣، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، مج٨، ع١٥، ص. ٢٦٦.

[٤٠] مصطفى إبراهيم سلمان الشمري، ٢٠٢١، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، جامعة ديالى، مج١٠، ع١، ص. ١٤٧.

[٤١] هبة جمال الدين، ٢٠٢٣، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٤، العدد ١، ص ص. ١٨٩-٢٣٠.

[٤٢] ضحى لعيبي كاظم السدخان، ٢٠٢١، البعد الجيو سياسي للأمن السيبراني، مجلة العلوم الإنسانية، المجلد ٥، العدد ١، ص ص. ١٨٨-٢٣٣.

[٤٣] محمد الصغير مسيكة، ٢٠٢٢، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، المجلد ٧، العدد ٤، ص ص. ٤٤٧-٤٦٢.

[٤٤] أحمد حسن الشمري، ٢٠٢٠، المسؤولية الدولية عن الهجمات السيبرانية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، ص٢١٠-٢٢٥.

[45] Michael N. Schmitt, ٢٠١٧, Tallinn Manual ٢,٠on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge., ص ٣٠٨-٣٢٠.

[٤٦] خالد وليد محمود, ٢٠٢٥, الفضاء السيبراني وتحولات القوة في العلاقات الدولية, المركز العربي للأبحاث ودراسة السياسات, الدوحة, ص ٢٥٠-٢٧٠.

[٤٧] ماجد عزيز إسكندر، ٢٠٢٣، التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ط١، ص٧٥-٩٠.

[٤٨] نورة شلوش، ٢٠١٨، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الإنسانية، بابل العراق، العدد ١٢، ص٤٥-٦٠.

[٤٩] جيهان حمية وموسى البزال، ٢٠٢٥، تحديات القانون الدولي في مواجهة التهديدات السيبرانية، المجلة العربية للنشر العلمي، العدد ٨٦، ص١٥-١٩.

[٥٠] أحمد فتحي خليفة، ٢٠٢٠، المسؤولية الدولية عن الهجمات السيبرانية: دراسة في ضوء قواعد القانون الدولي المعاصر، دار النهضة العربية، القاهرة، ص٢٤٥.

[٥١] محمد سامي عبد الصادق، ٢٠٢١، إسناد الهجمات السيبرانية في إطار قواعد مسؤولية الدولة، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد ٥٦، ص١٢٥-١٤٠.

قائمة المصادر:

١. أبو الوفا، أحمد، ١٩٩٦، الوسيط في القانون الدولي العام، دار النهضة العربية، القاهرة.
٢. أبو هيف، علي صادق، ١٩٩٥، القانون الدولي العام، منشأة المعارف، الإسكندرية.
٣. إسكندر، ماجد عزيز، ٢٠٢٣، التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ط١.
٤. جامعة الدول العربية، ٢٠١٠، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، القاهرة.
٥. حمية، جيهان، موسى البزال، ٢٠٢٥، تحديات القانون الدولي في مواجهة التهديدات السيبرانية، المجلة العربية للنشر العلمي، عمان.
٦. خليفة، أحمد فتحي، ٢٠٢٠، المسؤولية الدولية عن الهجمات السيبرانية: دراسة في ضوء قواعد القانون الدولي المعاصر، دار النهضة العربية، القاهرة.

٧. خليل، حازم محمد، ٢٠٢٣، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، الإسكندرية.
٨. دخلافي سفيان، ٢٠٢٢، تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي، المجلة الأكاديمية للبحث القانوني، الجزائر.
٩. الدرمكي، حليمة، وائل علام، ٢٠٢٥، المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول، مجلة العلوم القانونية، جامعة الشارقة، الشارقة.
١٠. الركراكي، سعيد، ١٩٩١، مقترب في دراسة العلاقات الدولية، المطبعة والوراقة الوطنية، مراكش.
١١. السدخان، ضحى لعيبي كاظم، ٢٠٢١، البعد الجيو سياسي للأمن السيبراني، مجلة العلوم الإنسانية، بابل العراق.
١٢. سمرين، سارة خليل عبد الكريم، ٢٠٢٤، القيود الواردة على حرية الرأي والتعبير في قانون الجرائم الإلكترونية (دراسة مقارنة)، جامعة الشرق الأوسط، الأردن.
١٣. شلوش، نورة، ٢٠١٨، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الإنسانية، بابل العراق.
١٤. الشمري، أحمد حسن، ٢٠٢٠، المسؤولية الدولية عن الهجمات السيبرانية، جامعة القاهرة، القاهرة.
١٥. الشمري، مصطفى إبراهيم سلمان، ٢٠٢١، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، جامعة ديالى، العراق.
١٦. الشهواني، خميس جمعة، ٢٠٢٦، إشكالية تحديد الاختصاص القضائي في الجرائم الإلكترونية، مجلة الشرق الأوسط للدراسات القانونية والفقهية، عمان.
١٧. الصغير مسيكة، محمد، ٢٠٢٢، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، بغداد.
١٨. عبد الصادق، محمد سامي، ٢٠٢١، إسناد الهجمات السيبرانية في إطار قواعد مسؤولية الدولة، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، المنصورة.
١٩. عدوان، إياد خالد، ٢٠٠٧، مدى تقبل المواطنين للحصول على الخدمات من خلال الحكومة الإلكترونية (دراسة حالة قطاع غزة)، الجامعة الإسلامية، غزة.

٢٠. فوزية، عروس، ٢٠٢٦، إشكالية الموازنة بين متطلبات الأمن السيبراني وضمان الحقوق الفردية، المجلة الأكاديمية للدراسات الاجتماعية والإنسانية، الجزائر.

٢١. الفيتلي، سهيل حسين، ٢٠٠٢، الوسيط في القانون الدولي العام، دار الفكر العربي، بيروت.

٢٢. القادري، عبد القادر، ١٩٨٤، القانون الدولي العام، مكتبة المعارف، الرباط.

٢٣. كلاع، شريفة، ٢٠٢٢، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، الجزائر.

٢٤. لجنة القانون الدولي، ٢٠٠١، مشروع مواد بشأن مسؤولية الدول عن الأفعال غير المشروعة دولياً، الأمم المتحدة، نيويورك.

٢٥. المبيضين، عبد الرحمن عمر محمد، ٢٠٢٥، الإطار القانوني للحقوق الرقمية: بين الحماية الدستورية والتنظيم الإداري، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، عمان.

٢٦. مجلس أوروبا، ٢٠٠١، التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مجلس أوروبا، ستراسبورغ.

٢٧. محمود، خالد وليد، ٢٠٢٥، الفضاء السيبراني وتحولات القوة في العلاقات الدولية، المركز العربي للأبحاث ودراسة السياسات، الدوحة.

٢٨. المختار، ولهي، ٢٠٢٥، القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكانياته، مجلة البحوث في الحقوق والعلوم السياسية، الجزائر.

٢٩. المطيري، طلال عبد الله، ٢٠٢٣، مبدأ عدم الإضرار في القانون الدولي وتطبيقاته في الفضاء السيبراني، مجلة الحقوق والعلوم السياسية، جامعة الكويت، الكويت.

٣٠. هبة جمال الدين، ٢٠٢٣، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، بغداد.

31. Brenner, S. W., Koops, B. J., ٢٠٠٤, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Boston.

32. International Law Commission, ٢٠٠١, Draft Articles on Responsibility of States for Internationally Wrongful Acts, United Nations, New York.

33. Schmitt, Michael N. (ed.), ٢٠١٧, Tallinn Manual ٢,٠on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge.

34. Swire, Peter, Jennifer Daskal, Théodore Christakis, ٢٠١٨, The globalization of criminal evidence, IAPP. ,

List of Sources:

1. Abu Al-Wafa, Ahmed, 1996, The Mediator in Public International Law, Dar Al-Nahda Al-Arabiya, Cairo.

2. Abu Heif, Ali Sadiq, 1995, Public International Law, Maaref Establishment, Alexandria.

3. Iskandar, Majid Aziz, 2023, The Political Exploitation of Cyber Attacks and Their Risks to National Security, Emirates Center for Strategic Studies and Research, Abu Dhabi, 1st ed.

4. League of Arab States, 2010, Arab Convention on Combating Information Technology Crimes, League of Arab States, Cairo.

5. Hamieh, Jihan, and Musa Al-Bazal, 2025, Challenges of International Law in the Face of Cyber Threats, Arab Journal for Scientific Publishing, Amman.

6. Khalifa, Ahmed Fathi, 2020, International Responsibility for Cyber Attacks: A Study in Light of Contemporary International Law Rules, Dar Al-Nahda Al-Arabiya, Cairo. 7. Khalil, Hazem Mohamed, 2023, Exploiting Cyberspace in Unconventional Warfare: A Study in Cyber Agencies and Cyberterrorism, Scientific Journal of the Faculty of Economics and Political Science, Alexandria.

8. Dakhlafi, Soufiane, 2022, Adapting Cyber Attacks in Light of the Provisions of International Law, Academic Journal of Legal Research, Algeria.

9. Al-Darmaki, Halima, and Wael Allam, 2025, International Responsibility for Cyber Attacks Committed by Non-State Entities, Journal of Legal Sciences, University of Sharjah, Sharjah.

10. Al-Rakrak, Said, 1991, An Approach to the Study of International Relations, National Printing and Publishing House, Marrakech.

11. Al-Sadkhan, Duha Laibi Kadhim, 2021, The Geopolitical Dimension of Cybersecurity, Journal of Humanities, Babylon, Iraq.

12. Samreen, Sarah Khalil Abdul Karim, 2024, Restrictions on Freedom of Opinion and Expression in the Cybercrime Law (A Comparative Study), Middle East University, Jordan.

13. Shloush, Noura, 2018, Cyber Piracy in Cyberspace: The Escalating Threat to State Security, Journal of the Babylon Center for Humanistic Studies, Babylon, Iraq.

14. Al-Shammari, Ahmed Hassan, 2020, International Responsibility for Cyberattacks, Cairo University, Cairo.

15. Al-Shammari, Mustafa Ibrahim Salman, 2021, Cybersecurity and its Impact on Iraqi National Security, Journal of Legal and Political Sciences, University of Diyala, Iraq.

16. Al-Shahwani, Khamis Juma, 2026, The Problem of Determining Judicial Jurisdiction in Cybercrimes, Middle East Journal of Legal and Jurisprudential Studies, Amman.

17. Al-Saghir Musayka, Muhammad, 2022, Cyberspace and the Challenges to National Security, Journal of Legal and Social Sciences, Baghdad. 18. Abdel-Sadek, Mohamed Sami, 2021, Attributing Cyber Attacks within the Framework of State Responsibility Rules, Journal of Legal and Economic Research, Mansoura University, Mansoura.

19. Adwan, Iyad Khaled, 2007, The Extent of Citizens' Acceptance of Services through E-Government (A Case Study of the Gaza Strip), Islamic University, Gaza.

20. Fawzia, Arous, 2026, The Problem of Balancing Cybersecurity Requirements and Guaranteeing Individual Rights, Academic Journal of Social and Human Studies, Algeria.

21. Al-Fitli, Suhail Hussein, 2002, The Mediator in Public International Law, Dar Al-Fikr Al-Arabi, Beirut.

22. Al-Qadri, Abdel-Qader, 1984, Public International Law, Al-Maaref Library, Rabat.

23. Kelaa, Sharifa, 2022, Cybersecurity and the Challenges of Espionage and Electronic Infiltration of States via Cyberspace, Journal of Law and Human Sciences, Algeria.

24. International Law Commission, 2001, Draft Articles on State Responsibility for Internationally Wrongful Acts, United Nations, New York.

25. Al-Mubaydeen, Abdul Rahman Omar Muhammad, 2025, The Legal Framework for Digital Rights: Between Constitutional Protection and Administrative Regulation, Al-Zaytoonah University of Jordan Journal of Legal Studies, Amman.

26. Council of Europe, 2001, Interpretive Report on the Convention on Cybercrime, Council of Europe, Strasbourg.

27. Mahmoud, Khaled Waleed, 2025, Cyberspace and Power Shifts in International Relations, Arab Center for Research and Policy Studies, Doha.

28. Al-Mukhtar, Walhi, 2025, International Humanitarian Law and Cyber Warfare: Limits and Possibilities of Application, Journal of Research in Law and Political Science, Algeria.

29. Al-Mutairi, Talal Abdullah, 2023, The Principle of Doing No Harm in International Law and its Applications in Cyberspace, Journal of Law and Political Science, Kuwait University, Kuwait.

30. Heba Jamal Al-Din, 2023, Cybersecurity and the Transformation of the International System, Journal of the College of Economics and Political Science, Baghdad.

31. Brenner, S. W., Koops, B. J., ٢٠٠٤, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Boston.
32. International Law Commission, ٢٠٠١, Draft Articles on Responsibility of States for Internationally Wrongful Acts, United Nations, New York.
33. Schmitt, Michael N. (ed.), ٢٠١٧, Tallinn Manual ٢,٠on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge.
34. Swire, Peter, Jennifer Daskal, Théodore Christakis, ٢٠١٨, The globalization of criminal evidence, IAPP. ,