



الولاية الجنائية الدولية على الجرائم المرتكبة في الفضاء السيبراني وتنازع الاختصاص القضائي

الولاية الجنائية الدولية على الجرائم المرتكبة في الفضاء السيبراني وتنازع الاختصاص القضائي

م.م مهند ياس خضير

مديرية تربية بغداد الرصافة الثانية / قسم تربية المدائن - الشعبة القانونية

البريد الإلكتروني Email : legalmohnd@gmail.com

الكلمات المفتاحية: الولاية الجنائية الدولية، الجريمة السيبرانية، تنازع الاختصاص، اتفاقية الأمم المتحدة ٢٠٢٤، السيادة الرقمية، المحكمة الجنائية الدولية.

كيفية اقتباس البحث

خضير، مهند ياس ، الولاية الجنائية الدولية على الجرائم المرتكبة في الفضاء السيبراني وتنازع الاختصاص القضائي، مجلة مركز بابل للدراسات الانسانية، تشرين الأول ٢٠٢٦، المجلد: ١٦، العدد: ١٠ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مسجلة في
ROAD

مفهرسة في
IASJ

International Criminal Jurisdiction over Crimes Committed in Cyberspace and the Conflict of Jurisdiction

Assistant Lecturer: Muhannad Yass Khudair

Baghdad Al-Rusafa II Education Directorate / Al-Madain Education
Department - Legal Division

Keywords : International criminal jurisdiction, cybercrime, jurisdictional disputes, 2024 United Nations Convention, digital sovereignty, International Criminal Court.

How To Cite This Article

Khudair, Muhannad Yass, International Criminal Jurisdiction over Crimes Committed in Cyberspace and the Conflict of Jurisdiction, Journal Of Babylon Center For Humanities Studies, October 2026, Volume:16, Issue 10.



This is an open access article under the CC BY-NC-ND license
(<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

[This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.](http://creativecommons.org/licenses/by-nc-nd/4.0/)

Abstract:

This study discusses the complex legal issues that cyberspace poses to the traditional rules of international criminal jurisdiction, as cybercrime is characterized by its transnational nature, which transcends the concept of physical territorial sovereignty. The research aims to analyze the adequacy of the traditional principles of jurisdiction (territorial, personal, protective, and universal) in addressing digital crimes, with a focus on studying the conflict of jurisdiction in its positive and negative forms. The study also highlights newly developed international instruments, most notably the United Nations Comprehensive Convention on Cybercrime adopted in December 2024, and the International Criminal Court Prosecutor's new policy for 2024 on the prosecution of international crimes committed through cyber means. The study concludes that it is necessary to move from the concept of physical sovereignty to flexible digital sovereignty to ensure that perpetrators do not escape punishment.



This research aims to analyze the principles of jurisdiction regarding cybercrimes, evaluate the effectiveness of the principle of universality as a last resort for justice, assess the emerging role of the International Criminal Court in prosecuting cyberattacks that rise to the level of international crimes, and explore the future of international cooperation under the 2024 UN Convention, while identifying the challenges developing nations face in its implementation.

The research problem is addressed through the following central question: To what extent have international law and recent international agreements succeeded in formulating a unified legal framework for criminal jurisdiction?

المستخلص :

تحاول هذه الدراسة مناقشة الإشكاليات القانونية المعقدة التي قد يفرضها الفضاء السيبراني على القواعد التقليدية القانونية للولاية الجنائية الدولية ، إذ تنسم الجريمة السيبرانية بطابع عابر للحدود متجاوزاً مفهوم السيادة الإقليمية المادية ، وإذ يهدف البحث إلى تحليل مدى كفاية مبادئ الاختصاص التقليدية (الإقليمية، الشخصية، الحماية، والعالمية) في استيعاب هذه الجرائم الرقمية ، من خلال التركيز على دراسة تنازع الاختصاص بنوعيه الإيجابي والسلبي ، كما وتسلط الدراسة الضوء على الصكوك القانونية الدولية المستحدثة ، وفي مقدمتها اتفاقية الأمم المتحدة الشاملة لمكافحة الجريمة السيبرانية المعتمدة في ديسمبر من العام ٢٠٢٤ ، والسياسة الجديدة للمدعي العام للمحكمة الجنائية الدولية من العام ٢٠٢٤ بشأن الملاحقة القضائية للجرائم الدولية المرتكبة بوسائل سيبرانية ، وتلخص هذه الدراسة إلى ضرورة الانتقال من مفهوم السيادة المادية إلى مفهوم السيادة الرقمية المرنة لضمان عدم إفلات المجرمين من العقاب.

تتمثل مشكلة البحث من خلال التساؤل الرئيس الآتي : إلى أي مدى تمكن القانون الدولي والاتفاقيات الدولية المستحدثة من صياغة إطار قانوني موحد للولاية الجنائية

تهدف البحث الى تحليل مبادئ الاختصاص القضائي في الجرائم السيبرانية وتقييم فاعلية مبدأ العالمية كملاذ أخير للعدالة ، و تقييم الدور المستحدث للمحكمة الجنائية الدولية في ملاحقة الهجمات السيبرانية التي ترقى لمستوى الجرائم الدولية ، و استشراف مستقبل التعاون الدولي في ظل اتفاقية الأمم المتحدة ٢٠٢٤ ، وتحديد التحديات التي تواجه الدول النامية في تنفيذها



المقدمة :

شهد المجتمع الدولي في مطلع العقد الثالث من القرن الحادي والعشرين تحولاً جذرياً ومهماً في طبيعة السلوك الإجرامي، إذ أفرزت الثورة الرقمية فضاءً افتراضياً متجاوزاً المفاهيم التقليدية للسيادة الوطنية والحدود الجغرافية ، وإن هذا التحول لم يقتصر على الجوانب التقنية فحسب ، بل يمتد ليزعزع الأركان المستقرة للقانون العام وعلى وجه الخصوص في شقه الجنائي الدولي ، إذ أصبحت الجريمة السيبرانية تمثل التحدي الأكبر للولاية القضائية للدول وللنظام القضائي العالمي وتكمن الإشكالية القانونية في أن القواعد التقليدية للاختصاص القضائي، والتي تأسست على مبدأ الإقليمية المادي أصبحت عاجزة عن استيعاب جرائم تُرتكب في اللا-مكان وتستهدف ضحايا في أقاليم متعددة في آن واحد من العالم ، مما يولد نزاعات إيجابية وسلبية حول الاختصاص القضائي مما يتطلب معالجة هذه الظاهرة بصورة مقارنة قانونية شاملة تفحص مدى قدرة الولاية الجنائية الدولية على بسط سيادتها على الفضاء السيبراني فضلاً عن تحلل آليات فض تنازع الاختصاص في ظل الاتفاقيات الدولية المعاصرة أمثال اتفاقية بودابست لعام ٢٠٠١ واتفاقية الأمم المتحدة الشاملة لمكافحة الجريمة السيبرانية لعام ٢٠٢٤ ، وإن هذه الدراسة تسعى إلى تأصيل مفاهيم السيادة الرقمية والولاية الافتراضية من خلال التركيز على السياسات القضائية المستحدثة للمحكمة الجنائية الدولية والتشريعات الوطنية المقارنة.

أهمية الموضوع

تنبثق أهمية هذا البحث من التحول الجذري في طبيعة النزاعات الدولية والجريمة المنظمة، إذ أصبح الفضاء السيبراني مسرحاً لهجمات تستهدف البنى التحتية الحيوية للدول، مما يهدد السلم والأمن الدوليين، وتبرز الأهمية القانونية في محاولة سد الفجوة بين جمود النصوص القانونية التقليدية التي تعتمد على المكان المادي، وبين ديناميكية الجريمة السيبرانية التي تُرتكب في فضاء افتراضي لا يعترف بالحدود كما تكمن الأهمية في مواكبة أحدث التوجهات القضائية الدولية التي بدأت تدرج الهجمات السيبرانية ضمن جرائم الحرب والجرائم ضد الإنسانية

أسباب اختيار الموضوع

- ١.تفاقمت التهديدات السيبرانية مؤخراً من خلال ازدياد الهجمات الرقمية على وتيرة عالية وعابرة للحدود والتي تضع الدول في مواجهة تنازع واجبات قانونية وتشريعية.
- ٢.الحدثة التشريعية الخاصة بالتهديدات السيبرانية وصدور اتفاقية الأمم المتحدة الشاملة لمكافحة الجريمة السيبرانية في نهاية عام ٢٠٢٤، مما استوجب دراستها وتحليل أثرها على السيادة الوطنية

٣. تطور دور القضاء الدولي عبر إعلان المحكمة الجنائية الدولية في العام ٢٠٢٤ عن قدرتها على ملاحقة الجرائم الميسرة رقمياً ، مما مثل منعطفاً تاريخياً مهماً في القانون الجنائي الدولي.

٤. تعقد في إشكالية الاختصاص عبر الحاجة الملحة من أجل إيجاد معايير دولية لفض التنازع بين الولايات القضائية المتعددة والتي تدعي جميعها الحق في المحاكمة بناءً على معايير مختلفة

مشكلة البحث

تتمثل مشكلة البحث من خلال التساؤل الرئيس الآتي : إلى أي مدى تمكن القانون الدولي والاتفاقيات الدولية المستحدثة من صياغة إطار قانوني موحد للولاية الجنائية قد ينهي أزمة تنازع الاختصاص القضائي في الفضاء السيبراني دون المساس بالسيادة الوطنية وحقوق الإنسان؟. ويتفرع عن هذا التساؤل مجموعة من التساؤلات الآتية :

١. هل يمكن تكييف مبدأ الإقليمية مع جريمة لا يوجد لها مسرح مادي محدد على الأرض؟.
٢. هل هناك آليات لفض التنازع الإيجابي للاختصاص عندما تدعي أكثر من دولة ولايتها على المجرم السيبراني؟.
٣. هل بالإمكان توفر الاتفاقيات الدولية (بوابست ٢٠٠١ والأمم المتحدة ٢٠٢٤) ضمانات دولية كافية لحماية الخصوصية عند جمع الأدلة العابرة للحدود؟.

هدف البحث

١. تحليل مبادئ الاختصاص القضائي في الجرائم السيبرانية وتقييم فاعلية مبدأ العالمية كملاذ أخير للعدالة.
٢. تقييم الدور المستحدث للمحكمة الجنائية الدولية في ملاحقة الهجمات السيبرانية التي ترقى لمستوى الجرائم الدولية
٣. استشراف مستقبل التعاون الدولي في ظل اتفاقية الأمم المتحدة ٢٠٢٤ ، وتحديد التحديات التي تواجه الدول النامية في تنفيذها

المبحث الأول: ماهية الجريمة السيبرانية وتكييفها في القانون الدولي العام

تعتبر الجريمة السيبرانية ظاهرة إجرامية مستحدثة تنتم بالتعقيد الفني والغموض القانوني، وهي تختلف جوهرياً عن الجرائم التقليدية من إذ طبيعة الركن المادي ومسرح الجريمة إن فهم الولاية القضائية يبدأ بالضرورة من تحديد طبيعة الفعل الجرمي الذي يراد بسط السلطة عليه (١)

المطلب الاول : تعريف الجريمة السيبرانية

تعرف الجريمة السيبرانية بأنها : هي الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك، أو جريمة يكون الحاسب الآلي نفسه ضحيتها ، إن الجريمة

السيبرانية لا تشمل فقط الجرائم التي ترتكب عن طريق الكمبيوتر ، بل تشمل أيضا أية جريمة تتضمن استخدام أو استهداف الكمبيوتر وتأكيدا على ذلك ما جاء في إرشادات الإسكوا (ESCWA) للتشريعات السيبرانية في بيان مفهوم الجريمة السيبرانية إذ ذهب إلى: إن الجريمة السيبرانية تنقسم على نوعين أساسيين: النوع الأول هو الذي يكون فيه الحاسوب أداة تنفذ بواسطتها الجريمة والنوع الثاني هو الذي يكون فيه جهاز الحاسوب وشبكات الحواسيب وبرامجها موضوعاً للجريمة، أي إن الفعل الجرمي ارتكب على هذا الجهاز فقد ترتكب لعدة أغراض كتحقيق مكاسب مادية معينة أو لإثبات الفاعل مهارته الفنية وقدرته على اختراق أجهزة الحاسب أو بهدف التسلية والترفيه أو لمجرد الرغبة في الإضرار بالغير، ومن أمثلة الجرائم السيبرانية الممارسات الاحتيالية على الإنترنت مشاركة الصور الإباحية للأطفال وتخزينها على الكمبيوتر والقفز والسب عبر الوسائل الإلكترونية وغيرها من النشاطات المخالفة بموجب القوانين وتشارك الجرائم السيبرانية مع الهجمات السيبرانية في كونها تحدث في الفضاء السيبراني إلا أنها تختلف عنها من إذ الفاعلين والأهداف، فعادة ما يكون مرتكبو الجرائم السيبرانية أفراداً، وتستهدف هذه الجرائم مؤسسات مالية أو شركات، بل وحتى أفرادا سواء داخل الدولة أو خارجها، على عكس ذلك، فإن الهجمات السيبرانية غالباً ما تنفذ من قبل دول أو مجموعات حكومية أو غير حكومية تستهدف دولاً أخرى، تتمثل الجرائم السيبرانية غالباً في تحقيق مكاسب شخصية، مثل سرقة الملكية الفكرية عبر شبكات الحاسوب، أو التسلل إلى أنظمة البنوك للتلاعب بأرقام الحسابات وتحويل الأموال على عكس الهجمات السيبرانية التي تستهدف الأمن القومي والسياسي للدولة، يسعى مرتكبو هذه الهجمات إلى تخريب الشبكات التي تدير البنية التحتية الأساسية للدولة وتدميرها بهدف إحداث الفوضى، وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية ، كما عرفتھا الاتفاقية الأوروبية للجرائم السيبرانية الإطار القانوني الدولي الأول والوحيد حتى الآن لمكافحة الجرائم السيبرانية، وقدمت تعريفاً عاماً للجريمة السيبرانية على أنها تشمل: الجرائم التي ترتكب ضد أو عبر أنظمة الكمبيوتر، بما في ذلك الجرائم التي تنطوي على الوصول غير المشروع إلى الشبكات أو البيانات، التلاعب بالمعلومات، أو إساءة استخدام الأجهزة التقنية لتحقيق أهداف غير قانونية(٢)

المطلب الثاني : الخصائص الفنية ذات الأثر القانوني

تتميز الجريمة السيبرانية بخصائص تجعل من الإقليمية قيداً معيقاً للعدالة بدلاً من أن تكون ضابطاً لها فالطابع العابر للحدود يعني أن النشاط الإجرامي يتوزع بين عدة دول، فالفاعل قد يكون في الدولة (أ)، والخادم في الدولة (ب)، والنتيجة الإجرامية في الدولة (ج) هذا التباعد

المكاني يثير تساؤلات حول مكان وقوع الجريمة، وهل هو مكان الفعل أم مكان النتيجة؟ فضلاً عن ذلك، تتسم هذه الجرائم باللامادية، إذ إن محل الاعتداء هو بيانات وبرامج غير ملموسة، مما يصعب من عملية الضبط والتفتيش القضائي التقليدي الذي يتطلب وجود أشياء مادية كما أن سرعة محو الأدلة الرقمية تفرض على سلطات التحقيق ضرورة التحرك العابر للحدود بسرعة فائقة، وهو ما يصطدم غالباً بإجراءات المساعدة القانونية المتبادلة البطيئة (٣)

المبحث الثاني: أسس الولاية الجنائية في الفضاء السيبراني

تعتمد الدول في بسط ولايتها الجنائية على مجموعة من المبادئ المستقرة في القانون الدولي العام، غير أن تطبيق هذه المبادئ في الفضاء السيبراني يتطلب تكييفاً افتراضياً يتماشى مع طبيعة التدفقات الرقمية (٤)

أولاً: مبدأ الإقليمية والسيادة الرقمية

يعد مبدأ الإقليمية الأساس التقليدي للاختصاص، إذ تختص الدولة بالجرائم التي تقع داخل إقليمها المادي وفي سياق الجرائم السيبرانية، تم التوسع في تفسير هذا المبدأ ليشمل الإقليم الافتراضي، أي البنية التحتية الرقمية والخواص الموجودة تحت سيادة الدولة، وتعد الجريمة مرتكبة في إقليم الدولة إذا تحقق فيها أحد ركنيها (الفعل أو النتيجة)، وهو ما يُعرف بنظرية مكان وقوع الجريمة الموسعة، تبرز إشكالية السيادة الرقمية عندما تطلب دولة ما النفاذ إلى بيانات مخزنة في خواص تقع في دولة أخرى، وبالتالي يثور النزاع بين حق الدولة في ملاحقة الجريمة التي أضرت بمصالحها، وبين حق الدولة الأخرى في حماية سيادتها على إقليمها الرقمي وخصوصية البيانات المخزنة فيه

ثانياً: مبادئ الجنسية والحماية والعالمية

في الحالات التي لا يكفي فيها مبدأ الإقليمية، تلجأ الدول إلى مبادئ أخرى لترسيخ ولايتها: ١. تمنح الدولة الحق في محاكمة مواطنيها الذين يشاركون في ارتكاب جرائم سيبرانية في الخارج وقد نصت اتفاقية الأمم المتحدة ٢٠٢٤ في المادة (٢٢) على ترسيخ الولاية بناءً على جنسية الجاني أو محل إقامته المعتاد (٥) ٢. يخول الدولة ملاحقة الجرائم التي تمس أمنها القومي أو مصالحها الحيوية (مثل التجسس الإلكتروني أو الهجمات على الأنظمة الحكومية) بغض النظر عن مكان وقوعها أو جنسية فاعلها

الولاية الجنائية الدولية على الجرائم المرتكبة في الفضاء السيبراني وتنازع الاختصاص القضائي

٣. يمثل قمة التعاون الجنائي الدولي، إذ يحق لأي دولة محاكمة مرتكبي جرائم دولية معينة (مثل الاستغلال الجنسي للأطفال أو الإرهاب السيبراني) لمنع إفلاتهم من العقاب ويُقترح حالياً ضم الجرائم السيبرانية الخطيرة إلى نطاق هذا المبدأ للتغلب على عقبات الاختصاص

مبدأ الاختصاص	معيار التطبيق في الفضاء السيبراني	الأساس القانوني (مثال)
الإقليمية	مكان وجود النظام المخترق أو وقوع الضرر	المادة ٦ من قانون العقوبات العراقي
الشخصية النشطة	جنسية الجاني (المخترق)	المادة ١٠ من قانون العقوبات العراقي
الحماية	المساس بأمن الدولة أو بنية المعلومات الحيوية	المادة ٢٢ (٢-ب) من اتفاقية الأمم المتحدة ٢٠٢٤
العالمية	خطورة الجريمة على الضمير الإنساني العالمي	المادة ٢٤ من اتفاقية الأمم المتحدة ٢٠٢٤

المبحث الثالث: إشكاليات تنازع الاختصاص القضائي وفض النزاعات

يعد تنازع الاختصاص القضائي في الجرائم السيبرانية من أعقد المسائل في القانون الدولي العام، إذ يتأرجح بين التنازع الإيجابي الذي قد يؤدي إلى محاكمة الشخص مرتين، والتنازع السلبي الذي يؤدي إلى ضياع حقوق الضحايا

أولاً: التنازع الإيجابي ومعايير الأولوية

يحدث التنازع الإيجابي عندما تدعي أكثر من دولة ولايتها على الجريمة ذاتها بناءً على مبادئ مختلفة (مثل دولة الجنسية ودولة الإقليم) لحل هذا النزاع، تتبع الاتفاقيات الدولية منهجية التشاور والتنسيق فالمادة (٢٢) من اتفاقية الأمم المتحدة ٢٠٢٤ تلزم الدول الأطراف بالسعي للتشاور بهدف تنسيق الإجراءات الجنائية وتحديد الدولة الأنسب للملاحقة، وتبرز في الفقه معايير لتفضيل اختصاص دولة على أخرى، منها (٦):

١. معيار الدولة الأكثر تضرراً: إذ تُعطى الأولوية للدولة التي وقع فيها الضرر الأكبر أو التي استهدفت بنيتها التحتية الحيوية
٢. معيار مكان وجود الجاني: لتسهيل عملية المحاكمة وتنفيذ العقوبة ومنع الحاجة لإجراءات التسليم المعقدة

٣. معيار سهولة جمع الأدلة: إذ يُفضل اختصاص الدولة التي توجد بها الأدلة الرقمية الأساسية لضمان سير العدالة

ثانياً: التنازع السلبي ومخاطر الملاذ الآمن

يمثل التنازع السلبي ثغرة قانونية يستغلها المجرمون السيبرانيون من خلال ارتكاب أفعالهم انطلاقاً من دول لا تجرم هذه الأفعال أو لا تمتلك القدرة التقنية على ملاحقتها إن مبدأ الشرعية الجنائية (لا جريمة ولا عقوبة إلا بنص) يمنع الدول من الملاحقة إذا لم يكن الفعل مجرمًا في قانونها الداخلي، وهو ما يؤكد على أهمية ازدواجية التجريم في الاتفاقيات الدولية ، وتهدف المعاهدات الحديثة إلى تجفيف الملاذ الآمن من خلال إلزام الدول بتجريم باقية موحدة من الأفعال السيبرانية لضمان إمكانية التسليم والملاحقة في أي مكان

المبحث الرابع: الآليات الدولية والإقليمية لمواجهة الجرائم السيبرانية

لقد أدرك المجتمع الدولي أن الولاية الوطنية القاصرة تتطلب دعماً من صكوك دولية ملزمة تنظم الاختصاص وتسهل التعاون العابر للحدود

المطلب الاول : الاتفاقيات الدولية والإقليمية

أولاً: اتفاقية بودابست ٢٠٠١ والبروتوكولات الملحقه (٧)

تُعد اتفاقية بودابست حجر الزاوية في السياسة الجنائية الدولية لمكافحة جرائم المعلوماتية وقد أرست هذه الاتفاقية قواعد مهمة للاختصاص في المادة (٢٢)، إذ ألزمت الدول بترسيخ ولايتها على الجرائم المرتكبة في أقاليمها أو بواسطة سفنها وطائراتها أو رعاياها ، أما الابتكار الأكبر فقد جاء في المادة (٣٢) التي نظمت الوصول العابر للحدود إلى البيانات، إذ سمحت للسلطات بالوصول إلى البيانات المخزنة في الخارج في حالتين:

١. إذا كانت البيانات متاحة للعموم (مثل المواقع الإلكترونية العامة)

٢. إذا حصلت السلطات على موافقة قانونية وطوعية من الشخص الذي يملك السلطة القانونية للإفصاح عن البيانات

هذا المبدأ يمثل استثناءً جزئياً لمبدأ الإقليمية ، ويهدف لتجاوز بطء إجراءات الإنابة القضائية الدولية ، فقد تم تعزيز هذه الآليات بالبروتوكول الإضافي الثاني (٢٠٢٢) الذي وضع شروطاً وضمانات أكثر صرامة لحماية حقوق الإنسان والخصوصية عند جمع الأدلة الإلكترونية العابرة للحدود.

ثانياً: اتفاقية الأمم المتحدة الشاملة ٢٠٢٤ (٨)

تعد هذه الاتفاقية أول صك عالمي يجمع بين الدول المتقدمة والنامية لمكافحة الجريمة السيبرانية وتتميز بمواد إجرائية وموضوعية دقيقة تهدف لتعزيز الولاية الجنائية الدولية:

١. المادة ٣: حددت نطاق التطبيق ليشمل منع الجرائم والتحقيق فيها وجمع الأدلة الإلكترونية لأغراض الملاحقة القضائية

٢. المادة ٢١: ألزمت الدول بفرض عقوبات فعالة ومتناسبة، مع مراعاة جسامة الجرائم التي تستهدف البنى التحتية الحيوية

٣. المادة ٤٨: نظمت حالات تعدد الولايات القضائية، مؤكدة على ضرورة التنسيق لضمان كفاءة الملاحقة واحترام السيادة الوطنية

إن هذه الاتفاقية تسد الفراغ الذي تركته اتفاقية بودابست ذات الطابع الأوروبي، وتوفر منصة عالمية لتبادل الأدلة وتسليم المجرمين واسترداد عائدات الجريمة

المطلب الثاني: التحديات الإجرائية وجمع الأدلة الرقمية عابرة الحدود

لا تتوقف إشكالية الولاية عند حدود الاختصاص القضائي، بل تمتد لتشمل السلطات الإجرائية في جمع الأدلة الرقمية التي تتسم بالديناميكية والتقلب

أولاً: التفتيش والضبط في البيئة الافتراضية

يشير التفتيش على أنظمة الحاسب تساؤلات حول حرمة المسكن الافتراضي وحقوق الأفراد في الخصوصية وتتطلب الإجراءات الجنائية الحديثة سلطات خاصة تتيح للمحققين (٩):

١. حجز أنظمة تكنولوجيا المعلومات أو واسطة تخزين البيانات

٢. عمل نسخ رقمية من البيانات مع صون سلامتها وضمان عدم العبث بها

٣. إلزام مقدمي الخدمات بـ الحفاظ العاجل للبيانات لمنع مسحها قبل صدور الأوامر القضائية

وفي الحالات التي تكون فيها البيانات مشفرة، تبرز معضلة قانونية حول مدى جواز إجبار المتهم أو مقدم الخدمة على فك التشفير، وهو ما يثير صراعاً بين حق الدولة في الوصول للحقيقة وحق المتهم في عدم تقديم دليل ضد نفسه

ثانياً: الصراع القضائي بين الولايات المتحدة والاتحاد الأوروبي (Cloud Act vs)

(GDPR) يمثل التنازع بين القانون الأمريكي والقانون الأوروبي نموذجاً تطبيقياً لتحديات الولاية العابرة للحدود

١. قانون Cloud Act الأمريكي (٢٠١٨): يمنح السلطات الأمريكية ولاية عابرة للحدود

لإجبار شركات التقنية الأمريكية على تسليم بيانات مخزنة في أي مكان في العالم (١٠)

٢.لائحة حماية البيانات الأوروبية (GDPR) وتنظيم E-Evidence: يضع قيوداً صارمة على نقل البيانات الشخصية خارج الاتحاد الأوروبي، ويشترط وجود ضمانات كافية لحماية الخصوصية(١١)

هذا الصراع التشريعي يضع شركات التقنية في مواجهة تنازع واجبات، إذ قد يؤدي الامتثال للقانون الأمريكي إلى انتهاك القانون الأوروبي والعكس صحيح ولحل هذا الإشكال، بدأت مفاوضات لإبرام اتفاقيات ثنائية (مثل الاتفاق بين الولايات المتحدة والاتحاد الأوروبي بشأن الأدلة الإلكترونية) تهدف لوضع معايير مشتركة للنفاد القانوني للبيانات مع احترام معايير الخصوصية.

المطلب الثالث: سياسة المحكمة الجنائية الدولية تجاه الجرائم السيبرانية ٢٠٢٤

لم تعد الجرائم السيبرانية مقتصرة على الاحتيال والابتزاز، بل أصبحت أداة في النزاعات المسلحة والجرائم الدولية الكبرى

أولاً: توسيع نطاق نظام روما الأساسي

أطلق مكتب المدعي العام للمحكمة الجنائية الدولية في عام ٢٠٢٤ سياسة رسمية تؤكد أن نظام روما الأساسي ينطبق على الجرائم المرتكبة عبر الوسائل السيبرانية ، وأن المحكمة هي الوسيلة (سواء كانت رصاصة أو كود برمجي) لا تغير من طبيعة الجريمة إذا كانت النتائج تقع ضمن اختصاص المحكمة(١٢)

ثانياً: الهجمات السيبرانية كجرائم حرب وجرائم ضد الإنسانية

يمكن ملاحقة الهجمات السيبرانية وفقاً للاتفاقيات الحديثة في الحالات التالية(١٣):

١.استهداف البنى التحتية المدنية والتي تتمثل بـ(شبكات المياه، الكهرباء، المستشفيات) والذي يؤدي إلى معاناة شديدة أو خسائر في الأرواح ويصنف كجريمة حرب.

٢.المساهمة في نشر الكراهية المنهجية أو التحريض على الإبادة الجماعية أو التطهير العرقي من خلال استخدام منصات التواصل الاجتماعي.

٣.المساهمة في تعطيل الأنظمة الحيوية لغرض تجويع المدنيين أو تهجيرهم قسراً.

وتؤكد هذه السياسة على ضرورة مواكبة القانون للتكنولوجيا ، وقد يبرز دور المحكمة الدولية كملاذ أخير للعدالة عندما تعجز المحاكم الوطنية من ملاحقة الجناة السيبرانيين بسبب حصاناتهم أو هروبهم العابر للحدود.

المطلب الرابع : الولاية القضائية في التشريع العراقي: دراسة حالة

ان واقع القانوني في العراق يعكس التحديات التي قد تواجهها الدول النامية في قوانينها التقليدية مع التقدم في العصر الرقمي.

أولاً: الأساس القانوني الحالي والقصور التشريعي (١٤)

أفتقار العراق حتى هذه اللحظة إلى قانون متكامل لمكافحة الجرائم السيبرانية ، وما زال يعتمد القضاء على تكييف نصوص قانون العقوبات رقم ١١١ لسنة ١٩٦٩ لمواجهة الجرائم الرقمية وبالرغم من أن المادة (٦) من قانون العقوبات تتبنى مبدأ الإقليمية الموسع ، لكن هناك قصوراً واضحاً في ملاحقة الجرائم والتي تقع جميعها في الخارج وتصيب المصالح العراقية ، من خلال عدم إدراج الجرائم السيبرانية ضمن الجرائم المشمولة بمبدأ العالمية في المادة (١٣)

ثانياً: مسودة قانون الجرائم المعلوماتية والعقوبات الدستورية

فقد شهدت السنوات الأخيرة محاولات عديدة من أجل أقرار قانون خاص ولكن مسودة العام ٢٠٢٢ قد واجهت انتقادات كبيرة وحادة ويرجع سبب ذلك الى صياغات غامضة قد تستخدم لتقييد من حرية التعبير ومن الناحية الإجرائية ، فقد تضمنت المسودة نصوصاً لإنشاء محاكم مختصة فضلاً عن تدريب قضاة ومحققين متخصصين في الجريمة السيبرانية ، وهو توجه إيجابي يهدف لتعزيز كفاءة الولاية القضائية الوطنية في العراق ، كما ويقترح الباحثون العراقيون الى ضرورة تعديل القوانين الإجرائية من اجل شمول قواعد خاصة بالتفتيش الرقمي وقبول الأدلة الإلكترونية بصورة كاملة في الإثبات الجنائي ، فضلاً عن ضرورة تفعيل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادق عليها العراق (١٥).

المطلب الخامس: آليات التعاون الدولي وفرض تنازع الاختصاص

إن فاعلية الولاية الجنائية الدولية قد تعتمد في المقام الأول على التعاون مع الدول وليس التصادم بين السيادة الوطنية (١٦)

أولاً: المساعدة القانونية وتسليم المجرمين : تتطلب ملاحقة المجرم السيبراني تعاوناً أمنياً وقضائياً وثيقاً يشمل:

١. تبادل المعلومات الاستخباراتية حول التهديدات السيبرانية
٢. الإنابة القضائية لتنفيذ إجراءات التحقيق في دولة أخرى
٣. تسليم المجرمين، وهو أمر يصطدم غالباً بمبدأ عدم تسليم المواطنين، مما يفرض على الدولة التي ترفض التسليم واجب الملاحقة القضائية نيابة عن المجتمع الدولي.

ثانياً: الموازنة بين الحقوق الأساسية وإنفاذ القانون

يجب أن تخضع كافة إجراءات جمع الأدلة والولاية العابرة للحدود لضمانات حقوق الإنسان ويشمل ذلك الحق في الخصوصية، وحرمة المراسلات، والحق في محاكمة عادلة وتؤكد الاتفاقيات الدولية أن مكافحة الجريمة السيبرانية لا يجب أن تكون ذريعة لقمح الحريات الرقمية أو الرقابة غير المشروعة

الاستنتاجات

١. أثبتت الدراسة أن الولاية الجنائية الدولية على الجرائم السيبرانية تمر بمرحلة انتقالية من السيادة المادية الصلبة إلى السيادة الرقمية المرنة إن الفضاء السيبراني، بطبيعته اللامركزية، يفرض على القانون العام تبني مفاهيم الولاية الافتراضية والاختصاص المبني على التأثير بدلاً من الاختصاص المبني على الموقع الفيزيائي للجاني

٢. تعد اتفاقية الأمم المتحدة ٢٠٢٤ بارقة أمل لتوحيد الجهود الدولية، إذ تضع إطاراً ملزماً لفض تنازع الاختصاص وتؤسس لتعاون جنائي عالمي يتجاوز الانقسامات الإقليمية كما أن انخراط المحكمة الجنائية الدولية في هذا المجال يبعث برسالة قوية بأن الفضاء الرقمي لن يكون ثقباً أسود للعدالة الدولية

٣. على صعيد التشريعات الوطنية، وخاصة في العراق، تبرز الحاجة الملحة لإقرار قانون عصري للجرائم السيبرانية يوازن بين متطلبات الأمن القومي وحماية الحريات العامة، مع ضرورة الانضمام للاتفاقيات الدولية لضمان عدم تحول الإقليم الوطني إلى ملاذ آمن للمجرمين الرقميين نتيجة القصور التشريعي إن مواجهة الجريمة السيبرانية تتطلب ذكاءً قانونياً يوازي ذكاء المجرمين، وتعاوناً دولياً يسبق سرعة تدفق البيانات عبر الألياف الضوئية

٤. تعد مسألة الولاية الجنائية الدولية في الفضاء السيبراني من أعقد التحديات القانونية المعاصرة، وذلك للطبيعة العابرة للحدود التي تتسم بها الجريمة الإلكترونية، إذ يمكن للمجرم أن يتواجد في دولة، ويستخدم خادماً (Server) في دولة ثانية، لضرب هدف في دولة ثالثة

٥. المبدأ التقليدي للسيادة المرتبط بالحدود الجغرافية لم يعد كافياً فالفضاء السيبراني بيئة لا مكانية، مما يجعل تطبيق مبدأ إقليمية القوانين أمراً صعباً عند تحديد مكان وقوع الجريمة

٦. ينشأ تنازع الاختصاص القضائي (Jurisdictional Conflict) بسبب تبني الدول لمعايير مختلفة (مبدأ الجنسية، مبدأ حماية المصالح الحيوية، أو مبدأ مكان وقوع الضرر)، مما قد يؤدي إما إلى ازدواجية الملاحقة أو الإفلات من العقاب

الولاية الجنائية الدولية على الجرائم المرتكبة في الفضاء السيبراني وتنازع الاختصاص القضائي

٧. رغم وجود اتفاقية بودابست لجرائم تقنية المعلومات، إلا أنها لا تضم كافة دول العالم، وهناك فجوة تشريعية بين الدول المتقدمة تقنياً والدول النامية في تعريف وتوصيف الجرائم السيبرانية الدولية

٨. الأدلة الجنائية السيبرانية سريعة الزوال وسهلة التعديل، والحصول عليها يتطلب تعاوناً دولياً فورياً، وهو ما يعطله بطء إجراءات الإنابة القضائية التقليدية

التوصيات

١. العمل تحت مظلة الأمم المتحدة من أجل صياغة معاهدة دولية ملزمة لتوحيد جميع تعريفات الجرائم السيبرانية مع وضع قواعد واضحة من أجل فض تنازع الاختصاص.

٢. تكون الأولوية بالجرائم السيبرانية في الاختصاص القضائي للدولة التي قد تعرضت مصالحها الحيوية أو أمنها القومي للضرر الأكبر، بغض النظر عن مكان انطلاق الهجوم ووقته.

٣. إيقاف المراسلات الورقية التقليدية واستبدالها بمنصات رقمية تكون مؤمنة من أجل تبادل الأدلة الجنائية بين الدول من أجل ضمان سرعة التحفظ على البيانات قبل القيام بحذفها.

٤. العمل على إنشاء آلية قضائية دولية تكون متخصصة من أجل الفصل في النزاعات السيبرانية التي تعجز الدول عن حلها وعلى وجه الخصوص تلك التي تمس السلم والأمن الدوليين.

٥. يجب ان يكون تعاون في العمل فعلى الدول المتقدمة القيام بتقديم المساعدة للدول النامية من أجل بناء منظومات دفاعية وقانونية لسد الملاذات السيبرانية الآمنة التي يستغلها المجرمون.

٦. المساهمة بدعم المكاتب الدولية التي تكون متخصصة في مكافحة الجريمة السيبرانية المنظمة لتعمل كحلقة وصل سريعة بين أجهزة النيابة العامة والقضاء عالمياً.

٧. هناك تطور كبير في الفضاء السيبراني بشكل أسرع من القانون لذا فإن المرونة القانونية يجب ان تكون هي المفتاح لحماية الحقوق في العصر الرقمي.

الهوامش

١. هيمان، ذغاري عبد الرحمن (٢٠١٠)، الحماية القانونية من جرائم المعلوماتية (اطروحة دكتوراه غير منشورة)، الجامعة الإسلامية، لبنان، ص ١٠٨

٢. الرزاز، اسماعيل محمود (٢٠٢٣)، الحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، ص ٢١

٣. الحسيني، احمد سعد محمد (٢٠١٢)، الجوانب الاجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية (اطروحة دكتوراه غير منشورة)، جامعة عين شمس، ص ٢٧٨



٤. عبد الوهاب ، زينب عبد الواحد ، دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية عبر الحدود : التحديات والآفاق ، مجلة سر من رأى للدراسات الانسانية ، المجلد الحادي والعشرون / العدد الرابع والثمانون ، السنة العشرون ، حزيران ، ٢٠٢٥ ، ص ٣٣٩
٥. المادة (٢٢) اتفاقية الأمم المتحدة ٢٠٢٤
٦. المادة (٢٢) من اتفاقية الأمم المتحدة ٢٠٢٤
٧. اتفاقية بودابست ٢٠٠١ والبروتوكولات الملحق
٨. اتفاقية الأمم المتحدة الشاملة ٢٠٢٤
٩. الرشدي ، هالة احمد (٢٠٢١)، الارهاب السيبراني : ما هيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية ، دار النهضة العربية ، ص ٦
١٠. قانون CLOUD Act الأمريكي (٢٠١٨)
١١. لائحة حماية البيانات الأوروبية (GDPR) وتنظيم E-Evidence
١٢. الجرائم السيبرانية الارشاد الخامس رابط الورقة البحثية :

https://archiveunesco.org/sites/wwwunesco.org/files/page_attachments/dir-5-cybercrimespdf/08

13. REGNER SABILLON, JEIMY CANO, VICTOR CAVALLER, JORDI SERRA, Cybercrime and Cybercriminals: A Comprehensive Study, R Sabillon et al / International Journal of Computer Networks and Communications Security, (6 4), June 2016, p 165

١٤. المادة (٦) والمادة (١٣) من قانون العقوبات رقم ١١١ لسنة ١٩٦٩
١٥. عبد الوهاب ، زينب عبد الواحد ، دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية عبر الحدود : التحديات والآفاق ، مجلة سر من رأى للدراسات الانسانية ، المجلد الحادي والعشرون / العدد الرابع والثمانون ، السنة العشرون ، حزيران ، ٢٠٢٥ ، ص ٣٣٩
١٦. عبد الوهاب ، زينب عبد الواحد ، دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية عبر الحدود : التحديات والآفاق ، مجلة سر من رأى للدراسات الانسانية ، المجلد الحادي والعشرون / العدد الرابع والثمانون ، السنة العشرون ، حزيران ، ٢٠٢٥ ، ص ٣٤٠

المصادر

١. اتفاقية بودابست ٢٠٠١ والبروتوكولات الملحق
٢. الحسيني، احمد سعد محمد (٢٠١٢)، الجوانب الاجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية (اطروحة دكتوراه غير منشورة)، جامعة عين شمس
٣. الرزاز، اسماعيل محمود (٢٠٢٣)، الحماية القانونية من الهجمات والجرائم السيبرانية ، مركز محمود لتوزيع الكتب القانونية
٤. الرشدي ، هالة احمد (٢٠٢١)، الارهاب السيبراني : ما هيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية ، دار النهضة العربية

٥. عبد الوهاب ، زينب عبد الواحد ، دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية عبر الحدود : التحديات والآفاق ، مجلة سر من رأى للدراسات الانسانية ، المجلد الحادي والعشرون / العدد الرابع والثمانون ، السنة العشرون ، حزيران ، ٢٠٢٥
٦. قانون CLOUD الأمريكي (٢٠١٨)
- ٧.لائحة حماية البيانات الأوروبية (GDPR) وتنظيم E-Evidence
- ٨.المادة (٢٢) اتفاقية الأمم المتحدة ٢٠٢٤
- ٩.المادة (٦) والمادة (١٣) من قانون العقوبات رقم ١١١ لسنة ١٩٦٩
- ١٠.المادة (٢٢) من اتفاقية الأمم المتحدة ٢٠٢٤
- ١١.هيمن، ذغاري عبد الرحمن (٢٠١٠)، الحماية القانونية من جرائم المعلوماتية (اطروحة دكتوراه غير منشورة)، الجامعة الاسلامية ، لبنان
- ١٢.الجرائم السيبرانية الارشاد الخامس رابط الورقة البحثية :

https://archiveunesco.org/sites/www.unesco.org/files/page_attachments/dir-5-cybercrimespdf/08 :

13.REGNER SABILLON, JEIMY CANO, VICTOR CAVALIER, JORDI SERRA, Cybercrime and Cybercriminals: A Comprehensive Study, R Sabillon et al / International Journal of Computer Networks and Communications Security, (6 4), June 2016

Sources

1. Budapest Convention (2001) and Additional Protocols
2. Al-Husseini, Ahmed Saad Mohamed (2012), *Procedural Aspects of Crimes Arising from the Use of Electronic Networks* (Unpublished PhD thesis), Ain Shams University
3. Al-Razzaz, Ismail Mahmoud (2023), *Legal Protection Against Cyberattacks and Cybercrimes*, Al-Mahmoud Center for Legal Book Distribution
4. Al-Rashidi, Hala Ahmed (2021), *Cyberterrorism: Its Nature and Counter-Efforts in Light of National and International Legislation and Laws*, Dar Al-Nahda Al-Arabiya
5. Abdel-Wahab, Zainab Abdel-Wahed, "The Role of International Criminal Law in Combating Transborder Cybercrimes: Challenges and Prospects," *Sur Man Ra'a Journal for Humanities Studies*, Vol. 21 / Issue 84, Year 20, June 2025
6. US CLOUD Act (2018)
7. European General Data Protection Regulation (GDPR) and E-Evidence Regulation
8. Article (22) of the UN Convention (2024)
9. Article (6) and Article (13) of Penal Code No. 111 of 1969
10. Article (22) of the UN Convention (2024)
11. Hayman, Daghari Abdel-Rahman (2010), *Legal Protection Against Information Technology Crimes* (Unpublished PhD thesis), Islamic University, Lebanon
12. Cybercrimes – Guideline 5 (Research Paper Link): https://archive.unescwa.org/sites/www.unescwa.org/files/page_attachments/dir-5-cybercrimes.pdf
13. Regner Sabillon, Jeimy Cano, Victor Cavaller, Jordi SERRA, Cybercrime and Cybercriminals: A Comprehensive Study, R Sabillon et al / International Journal of Computer Networks and Communications Security, (6 4), June 2016