دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية عبر الحدود: التحديات والآفاق

The Role of International Criminal Law in Combating Cross-Border Cybercrime: Challenges and Prospects

زينب عبد الواحد عبد الوهاب

Zainab AbdUl-Wahid A.Wahhab

E-mail: zainb@uosamara.edu.iq

https://orcid.org/0009-0002-6612-8704

م.م الاء صبار احمد

Alaa Sabbar Ahmed

جامعة سامراء/ رئاسة جامعة سامراء

الكلمات المفتاحية: الجريمة السيبرانية، التحديات، الأفاق، الجنائي.

Keywords: Cybercrime, Challenges, Prospects, Criminal.

الملخص

شهد العالم في العقود الأخيرة طفرة غير مسبوقة في مجال التكنولوجيا الرقمية، مما أدى إلى تغيير جذري في طريقة تفاعل الأفراد والدول، وفي الوقت ذاته ظهرت الجرائم السيبرانية كأحد أبرز التحديات الأمنية التي تواجه المجتمعات الحديثة، تُعد الجرائم السيبرانية جرائم عابرة للحدود بطبيعتها، حيث يمكن أن يقوم المجرمون بتنفيذها من أي مكان في العالم، مما يجعل ملاحقتهم وحماية الضحايا تحدياً كبيراً للنظم القانونية التقليدية، هنا يبرز دور القانون الجنائي الدولي بوصفه الإطار القانوني الأهم للتعامل مع هذه الظاهرة من خلال وضع قواعد تنظم التعاون بين الدول وتحقيق العدالة على المستوى العالمي.

Abstract

In recent decades, the world has witnessed an unprecedented boom in the field of digital technology, which has led to a radical change in the way individuals and countries interact. At the same time, cybercrime has emerged as one of the most prominent security challenges facing modern societies.

Cybercrimes are crimes that cross borders in nature, as criminals can carry them out from anywhere in the world, which makes pursuing them and protecting victims a major challenge to traditional legal systems. Here the role of international criminal law is highlighted as the most important legal framework for dealing with this phenomenon by establishing rules regulating Cooperation between countries and achieving justice at the global level.

المقدمة

منذ انتهاء الحربين العالميتين بدأت الدول في البحث عن وسـائل جديدة للقتال تحقق لها الميزة العسكرية دون تحمل الخسائر والمخاطر التي ترافق الاشتباكات التقليدية، ففي العقد الأخير اتجهت هذه الدول نحو استخدام الجرائم السيبرانية كوسيلة فعّالة لتحقيق أهدافها العسكرية.

إذ إن الجرائم السـيبرانية تتميز بتعقيد أسـاليبها وقدرتها على اجتياز الحدود التقليدية مما يتيح للدول القدرة على تدمير البنية التحتية للخصـم بشـكل شـامل، وتسـبب آثاراً فادحة على الأهداف العسـكرية والمدنية دون الحاجة إلى مواجهة مباشـرة أو تكاليف مالية ضـخمة ترتبط بالهجمات التقليدية. وبفضل الجرائم السيبرانية، يمكن للدول تحقيق أهدافها الإستراتيجية والعسكرية بطرق جديدة وفعّالة، مما يضـع التحكم في التكنولوجيا الرقمية والأمان السـيبراني في مقدمة التحديات والأولويات العسكرية الحديثة.

وأصـبح العالم في العصـر الحديث متشـابكاً ومترابطاً بشـكل غير مسـبوق بفضـل التقدم التكنولوجي الكبير مما أدى إلى تحول الحياة اليومية للناس إلى بيئة رقمية، حيث أصـبحت الشبكات الإلكترونية ساحة أساسية للأنشطة البشرية، هذا التقدم ورغم فوائده العديدة قد جلب معه تحديات كبيرة، وأبرزها الجريمة السيبرانية.

فالجرائم السـيبرانية هي تلك الأنشـطة غير القانونية التي تُرتكب باسـتخدام تقنيات الحاسوب والشبكات الإلكترونية، وتطال الأفراد، المؤسسات، والحكومات على حد سواء مع تطور هذه الجرائم وتعقيداتها، برزت الحاجة الملحة إلى إطار قانوني دولي لمكافحة هذه الجرائم عبر الحدود، لا سيما أن العديد من الجرائم السيبرانية تتم في بيئة تتجاوز الحدود الجغرافية للدول.

يمثل القانون الجنائي الدولي أحد الركائز الأسـاسـية في التصـدي للجرائم السـيبرانية التي تنتهك السـيادة الوطنية وتهدد الأمن القومي الاقتصـادي، وإن التعامل مع هذه الجرائم يتطلب التعاون بين الدول وتنظيم التشـريعات والسـياسـات المشـتركة لمواجهة التحديات التي تطرأ على مستوى مكافحة الجرائم عبر الحدود. لكن رغم أهمية هذا الدور لا تزال هناك العديد من التحديات التي تواجه تطبيق القانون الجنائي الدولي في هذا المجال، سـواء من حيث الاتفاقيات الدولية أو التنسيق بين الجهات القانونية المختلفة، وعليه فيسعى هذا البحث إلى دراسة دور القانون الجنائي الدولي في مكافحة الجرائم السـيبرانية عبر الحدود، مع التركيز على التحديات التي تواجه هذا الدور، واستكشاف الآفاق المستقبلية لتطوير هذا المجال من خلال تعزيز التعاون الدولي.

أولاً_ أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف، أبرزها:

1. تحليل دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية العابرة للحدود.

2. تحديد التحديات القانونية والتقنية والسياسية التي تعيق التعاون الدولي في هذا المجال.
3. اقتراح حلول وآليات فعّالة لتعزيز دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية.
4. استشراف الآفاق المستقبلية لتطوير الإطار القانوني الدولي لمواجهة التحديات السيبرانية.

ثانياً_ أهمية الدراسة

تكمن أهمية هذه الدراسة في تسليط الضوء على الأدوار التي يمكن أن يلعبها القانون الجنائي الدولي في مكافحة الجرائم السيبرانية، من خلال تعزيز التعاون بين الدول وإيجاد حلول مبتكرة للحد من انتشار هذه الجرائم.

بالإضافة إلى ذلك تُبرز الدراسة أهمية معالجة القصور القانوني الحالي، خاصة في ظل تزايد الاعتماد على التكنولوجيا في مختلف مجالات الحياة، كما تسعى الدراسة إلى إبراز التحديات التي تواجه تطبيق القانون الجنائي الدولي في هذا المجال، واستشراف الآفاق المستقبلية لتطوير إطار قانوني أكثر شمولية.

ثالثاً_ إشكالية الدراسة

تكمن مشكلة الدراسة في كيفية تطبيق القانون الجنائي الدولي بشكل فعال لمكافحة الجرائم السيبرانية عبر الحدود، في ظل التحديات المعقدة التي تطرأ على هذا المجال نتيجة لتطور التكنولوجيا واختلاف التشريعات بين الدول، هذه التحديات تُؤثر سلباً على قدرة الأنظمة القانونية الدولية في التصدي للجرائم السيبرانية بشكل شامل، ومن هنا كانت الإشكالية الرئيسية التالية:

كيف يمكن للقانون الجنائي الدولي أن يلعب دوراً فعالاً في مكافحة الجرائم السيبرانية العابرة للحدود في ظل التحديات القانونية والتقنية والسياسية القائمة؟"

رابعاً_ منهج الدراسة

تعتمد هذه الدراسة على **المنهج الوصفي التحليلي**، حيث سيتم تحليل القوانين والاتفاقيات الدولية المتعلقة بمكافحة الجرائم السيبرانية، بالإضافة إلى دراسة التحديات التي تواجه تطبيق هذه القوانين عبر الحدود.

خامساً_ خطة الدراسة

من أجل معالجة الإشكالية الرئيسية قمنا بتقسيم البحث إلى مبحثين، تناولنا المبحث الأول عن **مكافحة الجرائم السيبرانية: التعريف وآليات التعاون الدولي**، من خلال بتقسيم المبحث إلى مطلبين، نتحدث في المطلب الأول عن **تعريف الجريمة السيبرانية**، أما في المطلب الثاني سوف نتحدث عن **التعاون الدولي الإجرائي في مكافحة الجرائم السيبرانية**.

أما في المبحث الثاني فقد تناولنا المبحث **الثاني التحديات والآفاق في مكافحة الجرائم السيبرانية عبر الحدود،** من خلال تقسيم المبحث إلى مطلبين، سوف نتحدث في المطلب الأول عن التحديات **في مكافحة الجرائم السيبرانية عبر الحدود،** أما في المطلب الثاني سوف نتحدث عن **آفاق مكافحة الجرائم السيبرانية عبر الحدود.**

المبحث الأول

مكافحة الجرائم السيبرانية: التعريف وآليات التعاون الدولي

تُعَدُّ مكافحة الجرائم السيبرانية من التحديات الكبرى التي تواجه الدول في العصر الرقمي، حيث تتزايد التهديدات الإلكترونية التي تستهدف البنى التحتية الحساسة، والمؤسسات المالية، والأفراد على حد سواء. تتطلب هذه الجرائم، التي تتسم بالتعقيد والعابرة للحدود، تعزيز آليات التعاون الدولي بين الحكومات والمنظمات المتخصصة لضمان التصدي الفعّال لها.

يشمل ذلك تبادل المعلومات الاستخباراتية بين الدول، وتطوير أطر قانونية موحدة تسهّل ملاحقة المجرمين السيبرانيين عبر الحدود، إضافة إلى تعزيز القدرات التقنية للأجهزة الأمنية، كما يُعتبر رفع مستوى الوعي العام حول الأمن السيبراني وتدريب الكوادر البشرية المتخصصة من العناصر الأساسية في هذه الجهود، إن تحقيق بيئة رقمية آمنة يتطلب تنسيقاً دولياً شاملاً لمواجهة هذا النوع المتنامي من الجرائم.

بناء على ذلك سوف نقوم بتقسيم المبحث إلى مطلبين، سوف نتحدث في المطلب الأول عن تعريف الجريمة السيبرانية، أما في المطلب الثاني سوف نتحدث عن التعاون الدولي الإجرائي في مكافحة الجرائم السيبرانية.

المطلب الأول

تعريف الجريمة السيبرانية

إن الجريمة السيبرانية (Cyber Crime) والتي تعرف بأنها: "هي الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو يمثل إغراءً بذلك، أو جرمة يكون الحاسب الآلي نفسه ضحيتها"(هيمان، 2010، ص108).

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(الرزاز، 2023، ص21).

فقد ترتكب لعدة أغراض كتحقيق مكاســـب مادية معينة أو لإثبات الفاعل لمهارته الفنية وقدرته على اختراق أجهزة الحاسب أو بهدف التسلية والترفيه أو لمجرد الرغبة في الإضرار بالغير، ومن أمثلة الجرائم الســيبرانية الممارســات الاحتيالية على الإنترنيت مشــاركة الصــور الإباحية للأطفال وتخزينها على الكمبيوتر والقذف والسب عبر الوسائل الإلكترونية وغيرها من النشاطات المخالفة بموجب القوانين.

تتشارك الجرائم السيبرانية مع الهجمات السيبرانية في كونها تحدث في الفضاء السيبراني، إلا أنها تختلف عنها من حيث الفاعلين والأهداف، فعادةً ما يكون مرتكبو الجرائم الســـيبرانية أفراداً، وتستهدف هذه الجرائم مؤسسات مالية أو شركات، بل وحتى أفرادًا سواء داخل الدولة أو خارجها. على عكس ذلك، فإن الهجمات الســـيبرانية غالباً ما تُنفذ من قبل دول أو مجموعات حكومية أو غير حكومية تستهدف دولًا أخرى، تتمثل الجرائم السيبرانية غالباً في تحقيق مكاسب شــخصــية، مثل ســرقة الملكية الفكرية عبر شــبكات الحاســوب، أو التســلل إلى أنظمة البنوك للتلاعب بأرقام الحسابات وتحويل الأموال.

على عكس الهجمات السيبرانية التي تستهدف الأمن القومي والسياسي للدولة، يسعى مرتكبو هذه الهجمات إلى تخريب الشــبكات التي تدير البنية التحتية الأســاســية للدولة وتدميرها بهدف إحداث الفوضـــى، وزعزعة النظام فيها لتحقيق أهداف أمنية أو عســكرية أو ســياســية، اعتمدت الجمعية العامة للأمم المتحدة تعريفًا للجرائم السيبرانية يشير إلى أنها تشمل أي جريمة تُرتكب باســتخدام نظام رقمي أو شــبكة رقمية، أو داخل نظام رقمي، وبذلك فإنها تشــمل جميع الجرائم التي يمكن أن تحدث في بيئة إلكترونية سواء كانت هذه الجرائم موجهة ضد تلك البيئة أو تمت من خلالها أو باستخدامها(إعلان فيينا بشأن الجريمة والعدالة مواجهة تحديات القرن الحادي والعشرين، 2000).

كما عرفتها الاتفاقية الأوروبية للجرائم الســـيبرانية الإطار القانوني الدولي الأول والوحيد حتى الآن لمكافحة الجرائم الســيبرانية، وقدمت تعريفاً عاماً للجريمة الســيبرانية على أنها تشــمل: "الجرائم التي تُرتكب ضـــد أو عبر أنظمة الكمبيوتر، بما في ذلك الجرائم التي تنطوي على الوصــول غير المشــروع إلى الشــبكات أو البيانات، التلاعب بالمعلومات، أو إســاءة اســتخدام الأجهزة التقنية لتحقيق أهداف غير قانونية.(اتفاقية أوروبا المتعلقة بالجريمة الإلكترونية (بودابست) ،2001).

المطلب الثاني

التعاون الدولي الاجرائي في مجال مكافحة الجريمة السيبرانية

إنّ أهمية التعاون الدولي، الأمني والقضائي، تكمن بضرورة شعور المجتمع الـدولـي بمخاطر الجرائم السيبرانية وما يمكن أن تحدثهُ من آثار سلبية على مصالح المجتمع الـدولـي المشـتركة، وإدراكه للنمو السـريع والمتزايد لهذا النمط المسـتجد والخطر من الجرائم الإرهابية الإلكترونية، حيث تمثل هذه الجرائم نقطه مشـتركة تتلاقى فيها جهود المجتمع الدولي في بذل الاهتمام لأجل اتخاذ تدابير وآليات وتدعيم سـبل التعاون الدولي في مكافحة تلك جرائم(الأسدي،2015، ص698).

حيث إنّ هذا التعاون يكون بين أجهزة الشـرطة الدولية المتخصـصـة لمكافحة الجرائم السـيبرانية عن طريق إنشـاء مكاتب متخصـصـة لجمع المعلومات عن مرتكبي هذه الجرائم وتعميمها، فينبغي أن يكون هناك تعاون بين أجهزة الشـرطة المختلفة في الدول والتنسـيق فيما بينهم لضـبط المجرمين ومكافحه هذه الجرائم التي تتجاوز حدود الدولة (الحسـيني، 2012، ص278).

إنّ من أوجه التعاون الـدولـي لمكافحة الجرائم السيبرانية أيضاً التعاون القضائي الـدولـي أو ما يسـمى بالمسـاعدة القضـائية الدولية في مكافحة الجرائم السـيبرانية والتي تعرف بأنها " أي إجراء قانوني تتخذه دولة يمكن أن يسـهم في تسـهيل عملية المحاكمة في دولة أخرى تتعلق بجريمة معينة." تتخذ المسـاعدة القضـائية الدولية في المجال الجنائي أشـكالًا متعددة، منها تبادل المعلومات، ويشمل ذلك تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضـائية أجنبية أثناء نظرها في جريمة معينة تتعلق بالاتهامات الموجهة إلى رعاياها في الخارج والإجراءات المتخذة ضـدهم. كما قد يتضـمن التبادل أيضًـا السـوابق القضـائية للجناة(حجازي، 2015، ص 102).

تشـمل العملية أيضـاً نقل الإجراءات عندما تقوم دولة ما، بناءً على اتفاقية أو معاهدة، باتخاذ إجراءات جنائية تتعلق بجريمة ارتكبت في إقليم دولة أخرى، وذلك لمصـلحة الدولة المعنية شريطة توافر شروط معينة، من أبرزها مبدأ التجريم المزدوج، ويعني هذا أن الفعل المنسوب إلى الشـخص يجب أن يُعتبر جريمة في كل من الدولة الطالبة والدولة التي يُطلب منها نقل الإجراءات، بالإضـافة إلى شـرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة، وأيضـاً من الشـروط الواجب توافرها أن تكون الإجراءات المطلوب اتخـاذها من الأهمية بحيث تؤدي دوراً مهماً في الوصول إلى الحقيقة(حجازي، 2015، ص 104).

حيث يحصـــل تدعيم التعاون بين ســـلطات البوليس في الدول المختلفة من خلال إبرام اتفاقيات دولية، بحيث إذا اكتشفت الشرطة الوطنية لدولة ما جريمة تم بها على الإنترنت من خلال موقع موجود بالخارج، فإنها تقوم بإبلاغ البوليس بالدولة التي تم فيها البث، لذلك يجب على كل دولة تعيين إدارة لتلقي هذه البلاغات، واتخاذ الإجراءات الـقـانـونية طبقاً لقوانين كل دولة، هذا ونجد إن بعض الدول تلزم مستخدم شبكة الإنترنت بتسجيل نفسه لدى مكاتب الشرطة، إنّ بوليس الإنترنت هو نوع من الإجراءات والضمانات للمحافظة على أموال الغير وأسرارهم، وبهذا فإن دور الإنتربول لا يقتصر على مجرد إرسال النشرات الـــدولـــيـــة ومتابعتها بل يمتد إلى إجراءات الملاحقة وتتبع الشخص المطلوب والتحفظ عليه.

المبحث الثاني

التحديات والآفاق في مكافحة الجرائم السيبرانية عبر الحدود

تُعد الجرائم الســـيبرانية عبر الحدود واحدة من أبرز التحديات التي تواجه المجتمعات والدول في العصـــر الرقمي، حيث تتســـم هذه الجرائم بتعقيدها وســـرعة تطورها نتيجة للتقدم التكنولوجي المتســـارع. تتجاوز هذه الجرائم الحدود الجغرافية والقانونية، مما يجعل مكافحتها تتطلب تعاونًا دوليًا فعّالًا وآليات قانونية وتقنية متقدمة من بين أبرز التحديات التي تواجه التصدي لهذه الجرائم: نقص التنسيق بين الدول، التفاوت في التشريعات الوطنية، وصعوبة تتبع المجرمين الذين يستغلون الطبيعة المجهولة للإنترنت (الموسوي، 2019، ص13).

ومع ذلك فإن هناك آفاقاً واعدة لتعزيز الجهود المبذولة في هذا المجال، مثل تعزيز تبادل المعلومات بين الدول، تطوير تقنيات الذكاء الاصـطناعي لرصـد الأنشـطة المشـبوهة، وتوحيد الإطار القانوني الدولي لمكافحة هذه الجرائم، وإن العمل المشـترك بين الحكومات والمؤسـسـات التقنية والأمنية يُعد خطوة أســـاســـية نحو بناء منظومة شـــاملة وفعّالة لحماية المجتمعات من التهديدات السيبرانية المتزايدة. **بناء على ذلك سوف نقوم بتقسيم المبحث إلى مطلبين، سوف نتحدث في المطلب الأول عن التحديات في مكافحة الجرائم الســـيبرانية عبر الحدود، أما في المطلب الثاني سوف نتحدث عن آفاق مكافحة الجرائم السيبرانية عبر الحدود.**

المطلب الأول

التحديات في مكافحة الجرائم السيبرانية عبر الحدود

تعتبر الجرائم السـيبرانية عبر الحدود تحدياً متزايداً في العصـر الرقمي، حيث تتميز هذه الجرائم بالطابع العابر للحدود الذي يجعل التصـدي لها معقدًا على المسـتويين الوطني والدولي. فيما يلي أبرز التحديات والآفاق في مكافحة هذه الجرائم:

أولاً_ التنسيق القانوني الدولي:

يعد التنسـيق القانوني الدولي حجر الزاوية في مكافحة الجرائم السـيبرانية العابرة للحدود، حيث تتطلب هذه الجرائم تعاوناً مكثفاً بين الدول لتجاوز التحديات المرتبطة بالاختلافات القانونية والسـيادية، حيث تختلف التشـريعات المتعلقة بالجرائم السـيبرانية بين الدول من حيث التعريف، العقوبات، والإجراءات القانونية، وإن بعض الدول قد لا تعتبر أنشـطة معينة جريمة (مثل بعض أنواع الهجمات الإلكترونية)، مما يجعل ملاحقة المجرمين أمراً صـعباً، فالتضـارب بين قوانين الخصـوصـية والتحقيقات مثل قوانين حماية البيانات في بعض الدول قد تعيق التحقيقات الدولية، تؤدي إلى صـعوبة الحصـول على بيانات المسـتخدمين أو الأدلة الرقمية المخزنة في دول أخرى بسبب القيود القانونية(الفيل،2012، ص 56).

فالجرائم السـيبرانية غالباً ما تحدث عبر عدة دول، مما يثير تسـاؤلات حول أي دولة لها الحق في التحقيق والمقاضـاة، مما يؤدي إلى حدوث النزاعات بين الدول حول من يملك الحق في ملاحقة المجرمين قد تؤدي إلى تأخير العدالة، وبسبب ضـعف آليات تسليم المجرمين والذي كان سببه عدم وجود اتفاقيات دولية شـاملة، يصـعب تسـليم المتهمين بين الدول، ترفض بعض الدول تسـليم مواطنيها للمحاكمة في دول أخرى، حتى في حال وجود أدلة قوية (سـليمان،2022، ص 114).

ثانياً_ صعوبة تعقب الجناة في الجرائم السيبرانية

إن تعقب الجناة في الجرائم السـيبرانية يمثل تحدياً كبيراً للجهات الأمنية بسـبب الطبيعة التقنية لهذه الجرائم والطابع العابر للحدود، يعتمد المجرمون السـيبرانيون على أدوات وتقنيات متطورة لإخفاء هويتهم ومواقعهم، مما يجعل عملية التعقب معقدة وطويلة الأمد إخفاء الهوية:

ومنها تقنيات التشـفير حيث يسـتخدم المجرمون بروتوكولات التشـفير لحماية اتصـالاتهم وإخفاء أنشـطتهم، مما يجعل من الصـعب اعتراض البيانات أو تحليلها، والشـبكات الخاصـة الافتراضـية (VPN) التي تُمكّن المجرمين من تغيير عناوين بروتوكول الإنترنت (IP) لتبدو وكأنها قادمة من مواقع جغرافية مختلفة، مما يضلل المحققين(عبد الله، 2007، ص 34).

كما إنهم يقومون باستخدام الشبكة المظلمة (Dark Web): التي توفر الشبكة المظلمة بيئة آمنة للمجرمين لبيع المعلومات المسـروقة، مثل البيانات المالية أو البرامج الضـارة، دون الكشـف عن هويته، والمجرمون غالباً ما ينفذون هجماتهم من دول تختلف عن مواقع الضـحايا، مما يؤدي إلى تعقيد عملية تحديد الموقع الجغرافي الحقيقي، حيث يمكن للمجرمين اسـتغلال الدول ذات الأنظمة القانونية الضعيفة أو التي لا تتعاون دولياً.

كما يقومون باســـتخدام بعض البرمجيات الخبيثة التي تُبرمج بحيث تُخفي أثرها أو تدمر الأدلة فور انتهاء الهجوم، فالبرمجيات الحديثة تعتمد على تقنيات مثل "التنفيذ المؤجل" أو "التشـــغيل عن بعد"، مما يزيد من صـــعوبة تتبع مصـــدر الهجوم، وإن تعقب الجناة في الجرائم الســـيبرانية يحتاج إلى مزيج من الابتكار التقني، التعاون الدولي، وتطوير الأطر القانونية المناسبة، وعلى الرغم من التحديات الكبيرة، فإن الاستثمار في الأدوات الحديثة وبناء شراكات قوية بين الدول والقطاع الخاص يمكن أن يحد من هذه الصـــعوبات ويزيد من فرص تحقيق العدالة(بغدادي،2018، ص 60).

ثالثاً_ التطور التكنولوجي السريع

يُعد التطور التكنولوجي الســـريع أحد أكبر التحديات التي تواجه جهود مكافحة الجرائم السيبرانية. ففي الوقت الذي يوفر فيه هذا التطور أدوات وتقنيات لتحسين الأمن السيبراني، فإنه يُمكّن أيضاً المجرمين السيبرانيين من تطوير أساليب جديدة ومتطورة لارتكاب الجرائم. وسنشرحها كما يلي: تأثيرات التطور التكنولوجي السريع على الجرائم السيبرانية من خلال استخدام الذكاء الاصطناعي (AI) لتطوير هجمات متقدمة مثل الهجمات التلقائية أو الموجهة، من خلال ظهور "Deepfakes" التي تُستخدم في عمليات الاحتيال أو نشر المعلومات المضللة، حيث إن تطور تقنيات التشفير يجعل من الصعب اعتراض الاتصالات بين المجرمين أو فك تشفير البيانات المسروقة (حطب، 2014، ص 25).

ويعتبر صـــعوبة مواكبة التقدم فالجهات الأمنية غالباً ما تواجه تحدياً في مواكبة الابتكارات التكنولوجية التي يستخدمها المجرمون، فمحدودية الموارد التقنية والبشرية في الدول النامية تزيد من فجوة القدرة على مواجهة الجرائم السيبرانية، كمت إن صعوبة التنبؤ بالتهديدات المستقبلية، حيث إن ظهور تقنيات جديدة، مثل الحوسبة الكمومية، قد يُحدث تحولاً جذرياً في قدرة المجرمين على فك التشفير أو تنفيذ هجمات معقدة (شلوش، 2018، ص 190).

المطلب الثاني

آفاق مكافحة الجرائم السيبرانية عبر الحدود

على الرغم من التحديات الكبيرة التي تواجه جهود مكافحة الجرائم السيبرانية عبر الحدود، فإن التطورات التقنية وتعزيز التعاون الدولي يوفران آفاقاً واعدة للتصـــدي لهذه الظاهرة، تتطلب هذه الآفاق نهجاً متعدد الجوانب يعتمد على الابتكار التقني، التعاون القانوني، وتطوير القدرات البشرية فيما يلي أهم الآفاق الممكنة:

أولاً_ تعزيز التعاون الدولي

يُعد تعزيز التعاون الدولي من الركائز الأساسية لمواجهة الجرائم السيبرانية، حيث تتجاوز هذه الجرائم الحدود الجغرافية وتستغل الثغرات في الأنظمة القانونية والتنسيق بين الدول، والتعاون الفعّال بين الحكومات، المنظمات الدولية والقطاع الخاص ضروري لتطوير استراتيجيات مشتركة وتقليل الثغرات في الأمن السـيبراني العالمي وذلك من خلال اتفاقيات الدولية(النقيب، 2022، ص141).

كتوقيع المزيد من الاتفاقيات والمعاهدات الدولية لمكافحة الجرائم السيبرانية، مثل: اتفاقية بودابسـت (2001) (اتفاقية أوروبا المتعلقة بالجريمة الإلكترونية (بودابسـت) ،2001). التي تُعتبر أول اتفاقية دولية تهدف إلى تنسيق الجهود ضد الجرائم السيبرانية، وتطوير اتفاقيات جديدة تغطي التحديات الحديثة مثل الجرائم المتعلقة بالذكاء الاصـطناعي وإنترنت الأشـياء، وإنشـاء منصـات دولية لتبادل المعلومات في الوقت الفعلي حول التهديدات والهجمات السـيبرانية، تعزيز التعاون بين الدول لتسريع تبادل الأدلة الرقمية، والعمل على إنشاء مراكز إقليمية للأمن السيبراني تعمل كحلقة وصل بين الدول لتنسيق الجهود والتدريب المشترك.

ثانياً_ الابتكار التقني

مع التطور المستمر للتكنولوجيا، أصبح الابتكار التقني أحد أهم الأدوات لمواجهة الجرائم السـيبرانية التي تتسـم بالتعقيد والتطور المسـتمر، يتيح الابتكار التقني تطوير أدوات وحلول ذكية للكشـف عن التهديدات والتصـدي لها ومنعها قبل وقوعها، حيث يُسـتخدم الذكاء الاصـطناعي لتحليل كميات هائلة من البيانات للكشـف عن الأنماط غير الطبيعية التي قد تشـير إلى نشـاط سـيبراني مشـبوه، والعمل على تطوير أنظمة قادرة على التعرف على البرمجيات الخبيثة أو الهجمات السـيبرانية في الوقت الفعلي، وتمكين الأنظمة من اتخاذ قرارات سـريعة واسـتباقية للتصدي للهجمات دون الحاجة إلى تدخل بشري(جاسم، 2023، ص11).

كما يعمل على تعزيز الأمان وتُستخدم البلوك تشين لتسجيل البيانات بطريقة آمنة وغير قابلة للتلاعب، مما يجعل من الصـعب على المهاجمين تعديل السـجلات وحماية هويات المستخدمين من السرقة أو الاحتيال باستخدام منصات بلوك تشين لتوثيق الهويات.

في النهاية يمثل الابتكار التقني أداة محورية لمواجهة الجرائم السـيبرانية عبر الحدود من خلال توظيف تقنيات الذكاء الاصـطناعي، البلوك تشين، والحوسبة الكمية، يمكن تحسين القدرة على الكشـف عن التهديدات والتصـدي لها، ومع ذلك يجب أن تتضـافر الجهود لتقليل الفجوة التقنية، تعزيز التعاون بين الدول، وضمان استخدام التقنيات الحديثة بشكل مسؤول وآمن.

ثالثاً_ بناء القدرات الوطنية والإقليمية

من خلال تطوير البنية التحتية التقنية اللازمة لمواجهة الهجمات السيبرانية المتطورة، والاستثمار في مراكز عمليات الأمن السيبراني (SOC) لرصد وتحليل التهديدات السيبرانية، والعمل على إنشاء برامج تدريبية لتأهيل المحققين والمتخصصين في الأمن السيبراني، إضافة إلى إطلاق مبادرات تعليمية لتعزيز الثقافة السيبرانية لدى الأفراد والمؤسسات، وتشجيع البحث والتطوير من خلال تمويل الأبحاث المتعلقة بتقنيات الأمن السيبراني، وتشجيع الابتكار في مجال مكافحة الجرائم السيبرانية من خلال التعاون بين الجامعات والمؤسسات التكنولوجية (القريطي، 2021، ص55).

رابعاً_ إنشاء أنظمة قضائية متخصصة

مع تزايد تعقيد الجرائم السيبرانية وانتشارها عبر الحدود، أصبح من الضروري تطوير أنظمة قضائية متخصصة قادرة على التعامل مع الطبيعة الديناميكية لهذه الجرائم، فالأنظمة القضائية التقليدية غالبًا ما تعجز عن مواكبة التطور التكنولوجي وتعقيدات التحقيقات في المجال السيبراني، لذا فإن إنشاء أنظمة قضائية متخصصة يُعتبر خطوة محورية لتعزيز العدالة وضمان محاسبة الجناة. (شلوش، 2018، ص 191).

وذلك من خلال تطوير أنظمة قضائية متخصصة للتعامل مع الجرائم السيبرانية، والعمل على تدريب القضاة والمحامين على المفاهيم التقنية المرتبطة بهذه الجرائم، إضافة إلى صياغة قوانين دولية مرنة تتكيف مع التطورات التكنولوجية، وضمان التنسيق بين القوانين الوطنية والدولية لتسهيل التحقيقات والمحاكمات العابرة للحدود.

إضافة إلى إنشاء مراكز تدريب متخصصة لتأهيل القضاة والمحامين على التعامل مع القضايا السيبرانية، وتوفير دورات تدريبية مكثفة حول الأدلة الرقمية، الجرائم السيبرانية، والتقنيات الحديثة، وذلك من أجل ضمان المحاسبة السريعة والعادلة للجناة السيبرانيين، وتقديم حماية فعالة للضحايا من خلال إجراءات قانونية متخصصة. والعمل على تسهيل التعاون بين الأنظمة القضائية المختلفة من خلال معايير موحدة للتعامل مع الأدلة الرقمية والتحقيقات، وتقليل الفجوات القانونية بين الدول فيما يتعلق بالجرائم السيبرانية، من خلال تقديم محاكمات عادلة وشفافة للجناة يساهم في تقليل الجرائم السيبرانية من خلال تعزيز الردع (الرشيدي2021، ص45).

الخاتمة

في ظل تســـارع التطورات التكنولوجية وزيادة الاعتماد على الأنظمة الرقمية في مختلف مجالات الحياة، أصـــبحت الجرائم الســـيبرانية من أخطر التحديات التي تواجه المجتمع الدولي. فهذه الجرائم، بفضـل طبيعتها العابرة للحدود، تُشـكل تهديدًا للأمن السـيبراني العالمي وتؤثر سـلبًا على الأمن الاقتصـــادي، الاجتماعي والســـياســـي للدول. وقد تناولت هذه الدراســـة دور القانون الجنائي الدولي في مكافحة الجرائم الســـيبرانية عبر الحدود، مركزة على التحديات التي تواجهه والآفاق المستقبلية لتطوير هذا المجال.

إن مواجهة الجرائم السـيبرانية تتطلب جهوداً دولية منسـقة وإرادة سـياسـية مشـتركة لتعزيز التعاون بين الدول ومع وجود تحديات كبيرة، فإن الفرص متاحـة لتطوير إطـار قـانوني جنـائي دولي قادر على التصـــــدي لهذه الجرائم وحماية المجتمع الدولي من تهديداتها، وعلى الرغم من التعقيدات فإن الالتزام الدولي بالسعي نحو تحقيق العدالة وتعزيز الأمن السيبراني يُمكن أن يُحدث فارقاً كبيراً في الحد من هذه الظاهرة المتنامية.

توصـلت الدراسـة إلى أن هناك قصـوراً واضـحاً في الإطار القانوني الدولي القائم، سـواء من حيث غياب معاهدات شـاملة تنظم هذا النوع من الجرائم، أو من حيث التباين في التشـريعات الوطنيـة، مما يُعقد عمليـة التعـاون الدولي، ومع ذلك فإن تعزيز الجهود الدوليـة وتطوير القانون الجنائي الدولي يُمكن أن يفتح آفاقاً أوسع لمواجهة هذه الظاهرة بفعالية.

وفي نهاية البحث تمكنا من التوصل إلى بعص الاستنتاجات والمقترحات التالية:

أولاً_ الاستنتاجات

1. نظراً لكون الجرائم السيبرانية عابرة للحدود بطبيعتها، فإن الجهود الوطنية وحدها غير كافية لمواجهتها، مما يستدعي تدخل القانون الجنائي الدولي.
2. هناك نقص واضح في الإطار القانوني الدولي الموحد لمكافحة الجرائم السيبرانية، سواء من حيث التشريعات أو آليات التعاون الإجرائي.
3. التعاون بين الدول في مجال تبادل الأدلة الرقمية وملاحقة الجناة لا يزال محدوداً، وهو ما يعوق فعالية الجهود الدولية لمكافحة هذه الجرائم.
4. التطور السريع في التقنيات الرقمية إلى جانب تباين المصالح السياسية بين الدول، يُمثلان عائقين كبيرين أمام تطوير إطار قانوني شامل لمواجهة الجرائم السيبرانية.
5. تطوير آليات قانونية وتقنية مبتكرة بات ضرورياً لضمان مواجهة الجرائم السيبرانية بشكل أكثر فاعلية.

ثانياً_ التوصيات

1. يجب العمل على صياغة معاهدة دولية جديدة تحت مظلة الأمم المتحدة تُعرّف الجرائم السيبرانية بشكل موحد وتضع معايير ملزمة للدول الأعضاء للتعاون في مكافحتها.
2. يُوصى بإنشاء محكمة دولية متخصصة في الجرائم السيبرانية تكون معنية بالنظر في القضايا ذات الطابع العابر للحدود.
3. يجب تحسين آليات تبادل المعلومات والأدلة بين الدول، من خلال تطوير منصات إلكترونية آمنة تسهل هذا التعاون.
4. دعم الدول النامية تقنياً وقانونياً لبناء قدراتها في مواجهة الجرائم السيبرانية مع تعزيز برامج التدريب للقضاة والمحققين الدوليين.
5. توظيف تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة للكشف المبكر عن الجرائم السيبرانية وتتبع الجناة.

قائمة المصادر والمراجع

الأسدي، هناء إسماعيل إبراهيم .(2015) .الإرهاب وغسيل الأموال كأحد مصادر تمويله: دراسة مقارنة (ط. 1). منشورات زين الحقوقية.

الأمم المتحدة .(2000) .إعلان فيينا بشأن الجريمة والعدالة مواجهة تحديات القرن الحادي والعشرين .صادر في مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا. تم الاسترجاع من http://hrlibrary.umn.edu/arab/vi2000.html

البغدادي، أدهم باسم .(2018) .وسائل البحث والتحري عن الجرائم الإلكترونية (رسالة ماجستير غير منشورة). جامعة النجاح الوطنية.

جاسم، سالم نمر .(2023) .الجرائم السيبرانية وحقوق الإنسان في القوانين الدولية والوطنية .دار النهضة العربية.

حجازي، عبد الفتاح بيومي .(2015) .الإثبات الجنائي في جرائم الكمبيوتر والإنترنت .دار النهضة العربية.

الحسيني، أحمد سعد محمد .(2012) .الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية (أطروحة دكتوراه غير منشورة). جامعة عين شمس.

حطب، ياسر محمد الكومي .(2014) .الحماية الجنائية والأمنية للتوقيع الإلكتروني .منشأة المعارف.

الرزاز، إسماعيل محمود .(2023) .الحماية القانونية من الهجمات والجرائم السيبرانية .مركز المحمود لتوزيع الكتب القانونية.

الرشيدي، هالة أحمد .(2021) .الإرهاب السيبراني: ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية .دار النهضة العربية.

سليمان، علي مروة. (2022). إسهام نظرية الأنشطة الروتينية في فهم الجرائم السيبرانية: دراسة استطلاعية. *المجلة المصرية للعلوم الاجتماعية والسلوكية، .(6)*

شلوش، نورة. (2018). القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول .مجلة مركز بابل للدراسات الإنسانية، 8.(6)

الفيل، علي عدنان .(2012) .إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية .المكتب الجامعي الحديث.

القريطي، دحان حزام .(2021) .الأمن السيبراني وحماية أمن المعلومات .دار الفكر الجامعي.

مجلس أوروبا .(2001) .اتفاقية بودابست بشأن الجريمة الإلكترونية.

الموسوي، علي محمد كاظم .(2019) .المشاركة المباشرة في الهجمات السيبرانية .المؤسسة الحديثة للكتاب.

النقيب، عدنان .(2022) .الجرائم الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين (الهجمات السيبرانية) .المركز العربي للنشر والتوزيع.

هلالي، أحمد عبد الله .(2007) .الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة 23 نوفمبر 2001 (ط. 1). دار النهضة العربية.

هيمان، ذغاري عبد الرحمن .(2010) .الحماية القانونية من جرائم المعلوماتية (أطروحة دكتوراه غير منشورة). الجامعة الإسلامية في لبنان.

References

Abd Allāh, A. H. (2007). Al-Jawānib al-Mawḍū'īyah wa al-Ijrā'īyah lil-Jarā'im al-

Ma'lūmātīyah 'alá Ḍaw' Ittifāqīyat Būdābist al-Muwaqqa'ah 23 Nūfimbir 2001 [Substantive and Procedural Aspects of Information Crimes in Light of the Budapest Convention Signed 23 November 2001] (1st ed.). Dār al-Nahḍah al-'Arabīyah.

Al-Asadi, H. I. I. (2015). Al-Irhab wa Ghasil al-Amwal ka-Ahad Masadir Tamwilihi: Dirasah Muqaranah [Terrorism and Money Laundering as One of its Funding Sources: A Comparative Study] (1st ed.). Zain Legal Publications.

Al-Baghdadi, A. B. (2018). Wasā'il al-Baḥth wa al-Taḥarrī 'an al-Jarā'im al-Iliktrūnīyah [Methods of Investigation and Detection of Electronic Crimes] (Master's thesis, An-Najah National University).

Al-Fil, A. A. (2012). Ijrā'āt al-Taḥarrī wa Jam' al-Adillah wa al-Taḥqīq al-Ibtidā'ī fī al-Jarīmah al-Ma'lūmātīyah [Investigation Procedures, Evidence Collection, and Preliminary Investigation in Information Crimes]. Al-Maktab al-Jami'ī al-Ḥadīth.

Al-Ḥusaynī, A. S. M. (2012). Al-Jawānib al-Ijrā'īyah lil-Jarā'im al-Nāshi'ah 'an Istikhdām al-Shabakāt al-Iliktrūnīyah [Procedural Aspects of Crimes Arising from the Use of Electronic Networks] (Doctoral dissertation, Ain Shams University).

Al-Mūsawī, A. M. K. (2019). Al-Mushārakah al-Mubāshirah fī al-Hajamāt al-Saybarānīyah [Direct Participation in Cyber Attacks]. Al-Mu'assasah al-Ḥadīthah lil-Kitāb.

Al-Naqīb, A. (2022). Al-Jara'im al-Iliktrūnīyah fī Ḍaw' Brūtūkūlī Sab' wa Sab'īn al-Mulḥaqayn bi-Ittifāqīyāt Jīnf al-Arba' li-Sanat Tis' wa Arba'īn (al-Hajamāt al-Saybarānīyah) [Electronic Crimes in Light of Protocols 77 Attached to the Four Geneva Conventions of '49 (Cyber Attacks)]. Al-Markaz al-'Arabī lil-Nashr wa al-Tawzī'.

Al-Qurayṭī, D. Ḥ. (2021). Al-Amn al-Saybarānī wa Ḥimāyat Amn al-Ma'lūmāt [Cyber Security and Information Security Protection]. Dār al-Fikr al-Jāmi'ī.

Al-Rashīdī, H. A. (2021). Al-Irhab al-Saybarānī: Māhiyatuhu wa Juhūd Mukafaḥatihi fī Ḍaw' al-Tashrī'āt wa al-Qawānīn al-Waṭanīyah wa al-Dawlīyah [Cyber Terrorism: Its Nature and Efforts to Combat it in Light of National and International Legislations and Laws]. Dār al-Nahḍah al-'Arabīyah.

Al-Razzaq, I. M. (2023). Al-Ḥimāyah al-Qānūnīyah min al-Hajamāt wa al-Jarā'im al-Saybarānīyah [Legal Protection from Cyber Attacks and Crimes]. Al-Maḥmūd Center for Distribution of Legal Books.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).

Ḥattab, Y. M. A. (2014). Al-Ḥimāyah al-Jinā'īyah wa al-Amnīyah lil-Tawqī' al-

Iliktrūnī [Criminal and Security Protection for Electronic Signatures]. Munshaʾat al-Maʿārif.

Haymān, D. ʿA. R. (2010). Al-Ḥimāyah al-Qānūnīyah min Jarāʾim al-Maʿlūmātīyah [Legal Protection from Information Crimes] (Doctoral dissertation, Islamic University of Lebanon).

Ḥijāzī, ʿA. F. B. (2015). Al-Ithbāt al-Jināʾī fī Jarāʾim al-Kambyūtar wa al-Intirnīt [Criminal Evidence in Computer and Internet Crimes]. Dār al-Nahḍah al-ʿArabīyah.

Jāsim, S. N. (2023). Al-Jarāʾim al-Saybarānīyah wa Ḥuqūq al-Insān fī al-Qawānīn al-Dawlīyah wa al-Waṭanīyah [Cyber Crimes and Human Rights in International and National Laws]. Dār al-Nahḍah al-ʿArabīyah.

Shalūsh, N. (2018). Al-Qarṣanah al-Iliktrūnīyah fī al-Faḍāʾ al-Saybarānī: al-Tahdīd al-Mutaṣāʿid li-Amn al-Duwal [Electronic Piracy in Cyberspace: The Escalating Threat to State Security]. Majallat Markaz Bābil lil-Dirāsāt al-Insānīyah, 8(6).

Sulaymān, A. M. (2022). Is'hām Naẓarīyat al-Anshiṭah al-Rūtīnīyah fī Fahm al-Jarāʾim al-Saybarānīyah: Dirāsah Istiṭlāʿīyah [The Contribution of Routine Activities Theory to Understanding Cybercrimes: An Exploratory Study]. Al-Majallah al-Miṣrīyah lil-ʿUlūm al-Ijtimāʿīyah wa al-Sulūkīyah, (6).

United Nations. (2000). Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century. Adopted at the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna. Retrieved from http://hrlibrary.umn.edu/arab/vi2000.html