

أساليب التعاون الدولي في القضاء على الجرائم المعلوماتية

Approaches to International Cooperation in the Elimination of Cybercrime



موسى شالي*

أستاذ تعليم ثانوي

chali.17000@gmail.com

تاريخ الاستلام: 2025/08/29 تاريخ القبول: 2025/11/22 تاريخ النشر: 2025/12/16



ملخص:

يتناول هذا البحث آليات التعاون الدولي لمكافحة الجرائم المعلوماتية، باعتبارها تهديداً عابراً للحدود يصعب التصدي له بجهود وطنية. حيث يستعرض أهم الاتفاقيات الدولية كاتفاقية بودابست، ودور المنظمات الدولية والإقليمية في تعزيز التنسيق بين الدول. كما يناقش التحديات المرتبطة بتفاوت التشريعات الوطنية، وصعوبة تتبع الجناة دولياً، ويقترح سبباً لتعزيز التعاون القانوني والتقني بين الدول لمجابهة هذا النوع من الجرائم.

الكلمات المفتاحية: الجرائم المعلوماتية، التعاون الدولي، التشريعات الوطنية، المنظمات الإقليمية والدولية، اتفاقية بودابست.

Abstract:

cross-border threat that cannot be effectively addressed through national efforts alone. It reviews key international agreements such as the Budapest Convention and highlights the role of regional and international organizations in enhancing coordination among states. The study also examines challenges such as the disparity in national legislation and the difficulty of tracking perpetrators internationally, while proposing legal and technical measures to strengthen cooperation for more efficient and effective cybercrime prevention.

key words: Cybercrime, Cross-border threat, International cooperation, Budapest Convention, Legal and technical measures

مقدمة:

أدى التطور الهائل في مجال تكنولوجيا المعلومات إلى إحداث تغييرات في طبيعة المعاملات بين الأفراد، سواء على المستوى الفردي أو المؤسسي أو الحكومي. هذا التحول الرقمي، رغم ميزاتة الإقتصادية والتنموية، ترتبت عنه تحديات جديدة تعلقت بخصوصية المستخدمين وبأمن المعلومات، حيث فتح الباب أمام أنماط جديدة من الجرائم، عُرفت بالجرائم المعلوماتية، اتسمت بقدرتها على تجاوز الحدود الجغرافية للدول، ما جعل من المنظومات القانونية التقليدية تواجه تحديات غير مسبقة من حيث الاختصاص القضائي، وصعوبة التتبع الرقمي، وكذلك ضعف التنسيق بين الدول⁽¹⁾.

لذلك ولمواجهة هذا الخطر العالمي المتنامي، برزت الحاجة إلى إرساء آليات فعّالة للتعاون الدولي من أجل الوقاية من هذا النوع من الجرائم وملاحقة مرتكبيه، سواء من خلال المعاهدات الدولية كاتفاقية بودابست المتعلقة بالجرائم المعلوماتية، أو عبر اتفاقيات التعاون الثنائي والتقني بين الدول، أو من خلال تفعيل دور المنظمات الدولية كالإنتربول، والأمم المتحدة، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة. وتعددت بذلك الأساليب المتبعة، من تنسيق للتحقيقات وتبادل للمعلومات الرقمية، إلى سنّ قوانين متقاربة أو موحّدة⁽²⁾.

إلا أنّ هذه الجهود لا تزال تعترضها جملة من الإشكاليات العملية والقانونية التي تحدّ من فعاليتها، كتضارب مفاهيم الجرائم المعلوماتية بين الدول، واختلاف النظم القانونية فيما بينها، وغياب التوافق حول مبادئ السيادة الرقمية، إضافة إلى التفاوت في المواد والإمكانات التقنية بين الدول⁽³⁾. ومن هنا، تبرز الحاجة إلى القيام بدراسة لأساليب التعاون الدولي القائمة، وتحليل أوجه القصور فيها، واستشراف سبل تطويرها بما يتماشى وطبيعة التهديدات الرقمية المتغيرة.

إشكالية الدراسة

تشكل الجرائم المعلوماتية تحديًا عالميًا يهدد أمن الأفراد والدول على حد السواء، فقد فرضت واقعًا قانونيًا جديدًا يستدعي تكييفًا سريعًا من طرف المجتمع الدولي. فرغم تعدد الاتفاقيات الدولية والمبادرات الثنائية والإقليمية، إلا أن مدى فعالية أساليب التعاون الدولي

المعتمدة في مكافحة هذه الجرائم مازال يشكّل جدلاً. فهل تجسّد الآليات الحالية إطاراً كافياً وفعالاً لمجابهة الجرائم المعلوماتية؟ وما أبرز أوجه القصور في هذه الأساليب؟ وكيف يمكن تفعيل التعاون الدولي بما يتجاوز التحديات القانونية والمؤسسية القائمة؟ هذه التساؤلات تشكل جوهر الإشكالية التي يسعى هذا المقال إلى تحليلها.

فرضيات الدراسة

ينطلق هذا المقال من مجموعة من الفرضيات تحكم مسار التحليل، تبلورت بداية في كون الجرائم المعلوماتية بما تتسم به من أخطار عابر للحدود، تجسّد تهديداً أمنياً يصعب احتواؤه من خلال الجهود الفردية للدول، مما يجعل من التعاون الدولي في هذا المجال ضرورة قصوى لا خياراً. وتتمثل الفرضية الثانية في أن الأساليب الحالية للتعاون تعاني من ثغرات قانونية وتشريعية، مترتبة عن غياب تنسيق تشريعي وغياب تعريف موحد للجرائم المعلوماتية واختلاف طرق إثباتها من بلد إلى آخر.

أما الفرضية الثالثة فتتلور في أن نجاح التعاون الدولي في مكافحة الجريمة المعلوماتية العابرة للحدود يتجسّد في إيجاد مقارنة شاملة تدمج البعد التقني بالقانوني، وتستند إلى إرادة سياسية جديّة لتجاوز الحساسيات المتواجدة والمتعلقة بالسيادة والخصوصيات القانونية.

أهداف المقال

يسعى هذا المقال إلى تحقيق عدّة أهداف علمية وعملية، في مقدمتها تحليل الإطار القانوني الدولي الذي يحكم التعاون في مجال مكافحة الجرائم المعلوماتية، من خلال دراسة الاتفاقيات الرئيسية، وعلى رأسها اتفاقية بودابست، إضافة إلى ذكر نماذج التعاون الإقليمي والثنائي. كما يهدف هذا المقال إلى تحديد التحديات التقنية والقانونية التي تعترض هذا التعاون، مع التركيز على الثغرات التشريعية، وضعف تشارك المعلومات، وغياب التنسيق الفعال بين أجهزة تطبيق القانون على المستوى الدولي.

كذلك يتطلع هذا المقال إلى طرح جملة من المقترحات العملية لتعزيز التعاون الدولي، من خلال اقتراح آليات تنسيق جديدة بين الدول، و تطوير الاتفاقيات القائمة والعمل على صياغة

اتفاقية دولية ملزمة وشاملة تتعلق بالجرائم المعلوماتية، تأخذ بعين الاعتبار التطور التكنولوجي والخصوصيات القانونية للدول، والتوازن بين حقوق الإنسان الرقمية والضرورات الأمنية.

منهج التحليل المعتمد

يعتمد هذا المقال على المنهج التحليلي القانوني المقارن، عن طريق تحليل النصوص القانونية الدولية المتعلقة بالتعاون لمكافحة الجرائم المعلوماتية، مع دراسة المعاهدات الدولية والإقليمية ذات الصلة، كاتفاقية بودابست، والمبادئ التوجيهية للأمم المتحدة، وتوصيات المنظمات الإقليمية كالاتحاد الإفريقي والاتحاد الأوروبي.

كما يعتمد المقال على المنهج المقارن من خلال دراسة تجارب بعض الدول في هذا المجال، وتحديد الفوارق في المقاربات الوطنية، ومدى تأثيرها على فعالية التعاون الدولي. كذلك، يتم توظيف المنهج الوصفي التحليلي لرصد التحديات الحالية والاتجاهات المستقبلية في التعاون الدولي لمكافحة الجرائم المعلوماتية والتصدي لها، انطلاقاً من دراسات الحالة والتقارير الدولية، مع تناول الأبعاد القانونية، السياسية والتقنية، بما يوفر رؤية شاملة ومتعددة الزوايا حول الموضوع محل الدراسة.

المبحث الأول: الإطار القانوني والمؤسسي للتعاون الدولي في مكافحة الجرائم المعلوماتية

في ظل الانتشار السريع لتقنيات المعلومات والاتصالات، أضحت الجرائم المعلوماتية تتجاوز الحدود الوطنية، مما فرض تحديات جديدة على المنظومة القانونية التقليدية. وأمام هذا الواقع المستجد، برزت الحاجة إلى تعزيز التعاون الدولي لمكافحة هذا النوع من الجرائم. لذلك حضي الإطار القانوني والمؤسسي للتعاون الدولي بأهمية بالغة كونه يشكل الركيزة التي يُبنى عليه تبادل المعلومات والتنسيق بين الدول والمساعدة القانونية المتبادلة. ويتطلب هذا التعاون تنظيمًا قانونيًا دقيقًا على المستوى الدولي، إلى جانب آليات مؤسسية فعّالة تضمن تنفيذ الاتفاقات وتسهيل الإجراءات بين الدول. لذلك، سنعمد في هذا المبحث إلى تناول الإطار القانوني الدولي الذي ينظم هذا التعاون (المطلب الأول)، ثم ننتقل إلى إبراز الأطر المؤسسية والدولية المعنية بمكافحة الجرائم المعلوماتية وتنسيق الجهود الدولية في هذا المجال (المطلب الثاني).

المطلب الأول: الإطار القانوني الدولي للتعاون في مكافحة الجرائم المعلوماتية

تعددت الجهود الدولية الهادفة إلى مواجهة الجرائم المعلوماتية، انطلاقاً من التحديات التي تفرضها طبيعتها العابرة للحدود، والنقص في الأطر القانونية الوطنية لمجابهتها. وهو ما دفع المجتمع الدولي إلى التنقيب عن حلول قانونية تتماشى مع جميع الأطراف، تنظم العلاقات بين الدول وتحدد آليات التعاون فيما بينها لمكافحة هذا النوع من الجرائم، سواء من خلال اتفاقيات دولية شاملة، أو عبر اتفاقيات ثنائية وإقليمية أكثر مرونة وخصوصية في التعامل مع هذه الظاهرة⁽⁴⁾. ومن هذا المنطلق، سنتناول هذا المطلب من خلال فرعين أساسيين، أولهما مخصص للاتفاقيات الدولية متعددة الأطراف (الفرع الأول)، وثانيهما للاتفاقيات الثنائية والإقليمية (الفرع الثاني).

الفرع الأول: الاتفاقيات الدولية متعددة الأطراف (اتفاقية بودابست نموذجاً)

اعتمدت اتفاقية بودابست المتعلقة بالجرائم المعلوماتية، من قبل مجلس أوروبا سنة 2001، وجسدت أول وثيقة قانونية دولية شاملة تهدف إلى تنظيم الجهود الدولية لمكافحة الجريمة السيبرانية. وتواجهت هذه الاتفاقية على خلفية إدراك المجتمع الدولي أنّ الجرائم المعلوماتية تتخطى الحدود الوطنية، ما يوجب وضع آليات دولية متكاملة تضمن الملاحقة القضائية الفعالة لمرتكبيها. لذلك هدفت هذه الاتفاقية إلى توحيد القواعد القانونية بين الدول، خاصة فيما يتعلق بتجريم بعض الأفعال، كالولوج غير المشروع إلى أنظمة المعلومات، واعتراض البيانات، والاحتتيال الإلكتروني، والتزوير المعلوماتي⁽⁵⁾.

تميّزت هذه الاتفاقية بتضمنها قسماً خاصاً يتعلق بتسهيل التعاون الدولي، عن طريق إقرار قواعد لتبادل المعلومات وتسليم المجرمين، والمساعدة القانونية المتبادلة، وتحديد نقاط اتصال وطنية متاحة على مدار الساعة، وهو ما يجسد نقلة نوعية في جهود التنسيق القضائي الدولي. ولم تقتصر الاتفاقية على الدول الأوروبية، وإنما فتحت أبوابها لانضمام دول غير أعضاء في مجلس أوروبا، ككندا واليابان والولايات المتحدة، ما عزز من صيغتها العالمية⁽⁶⁾.

ولمزيد فعالية إتفاقية بودابست في مجال الجرائم المعلوماتية، تم سنة 2021 اعتماد بروتوكول إضافي ثانٍ لها، يعزز أدوات التعاون العابر للحدود، من خلال التمكين من الحصول على الأدلة

الرقمية مباشرة من مقدمي خدمات المعلومات والاتصالات، ويقترح هذا البروتوكول آليات جديدة للتعاون السريع بين الدول دون العبر بالإجراءات التقليدية المعقدة. رغم أهمية هذه الاتفاقية، إلا أنها لازالت تواجه بعض التحفظات من طرف بعض الدول التي تفضل نهجاً دولياً أكثر توازناً في ما يتعلق بحماية الحقوق الرقمية، من بينها الصين وروسيا⁽⁷⁾. رغم تأكيد عدد من الفقهاء أن اتفاقية بودابست تحسّد حجر الأساس في التشريع الدولية المتعلقة بالجرائم المعلوماتية العابرة للحدود، لكن بقيت فعالية تطبيق هذه الاتفاقية متفاوتة بين الدول لارتباطها بقدرتها على تعديل تشريعاتها الداخلية وتوفير الإمكانيات المؤسسية والتقنية الكافية لذلك⁽⁸⁾.

الفرع الثاني: الاتفاقيات الثنائية والإقليمية في مجال الجرائم المعلوماتية

إضافة إلى الاتفاقيات متعددة الأطراف، برزت في السنوات الأخيرة اتفاقيات ثنائية وإقليمية جسّدت وسيلة سريعة ومرنة لتكريس التعاون العملي بين الدول لمكافحة الجرائم المعلوماتية. فقد تميزت هذه الاتفاقيات بتجاوزها للتعقيدات الدبلوماسية المصاحبة عادة للاتفاقيات العامة، من خلال إتاحتها لجملة من بنود التعاون ارتبطت مباشرة بالخصوصيات التقنية والقانونية لكل طرفين⁽⁹⁾.

فعلى مستوى التعاون الثنائي، أبرمت الولايات المتحدة اتفاقيات ثنائية مع دول أوروبية وآسيوية لتبادل المعلومات المتعلقة بالهجمات السيبرانية، وتبسيط عمليات التعقب والتسليم، ورفع مستوى الأمن المعلوماتي المشترك. وجسّدت هذه الإجراءات نموذجاً فعالاً للتعاون المبني على المصالح الأمنية المشتركة بين الدول، مع ضمان مرونة في التطبيق بما يحقق نتائج ملموسة وفورية. فهذه الاتفاقيات تعمل غالباً على إنشاء قنوات اتصال مباشرة بين السلطات القضائية المختصة والأجهزة الأمنية، لتجاوز بطء الإجراءات التقليدية للتعاون القضائي الدولي⁽¹⁰⁾.

أما على الصعيد الإقليمي، فقد شهدت العديد من التكتلات الإقليمية تطور هام في مجال الجرائم المعلوماتية. ففي القارة الإفريقية، صادقت جملة من الدول على اتفاقية الاتحاد الإفريقي للأمن السيبراني وحماية البيانات الشخصية المعروفة بـ "اتفاقية مالابو"، والتي اعتمدت سنة 2014، وقامت الدول بتنفيذها تدريجياً. وكان هدف هذه الاتفاقية توحيد الرؤية الإفريقية

للجريمة المعلوماتية، وتعزيز القدرات الوطنية للدول الأعضاء، إضافة إلى تقوية التعاون التقني والقضائي فيما بينها⁽¹¹⁾.

وفي السياق العربي، برزت جهود لتفعيل التعاون القضائي والأمني بين الدول الخليجية عبر المنظومة القانونية المشتركة لمجلس التعاون الخليجي، من خلال تبني قواعد نموذجية لمكافحة الجرائم المعلوماتية العابرة للحدود، وتبادل الخبرات الفنية والتدريبية، وتفعيل الربط بين أجهزة الأمن الإلكتروني. وتؤكد الأدبيات القانونية الحديثة على أن هذه الأطر الإقليمية، رغم محدودية تطبيقها في بعض المواقع، إلا أنها تجسّد بداية بناء منظومة تعاون رقمي متكاملة⁽¹²⁾.

المطلب الثاني: الأطر المؤسسية والدولية للتعاون في مكافحة الجرائم المعلوماتية

لا يمكن التطرق إلى فعالية التعاون الدولي في مكافحة الجرائم المعلوماتية العابرة للحدود دون التعرض إلى البنية المؤسسية التي توطر هذا التعاون. فبالإضافة إلى القواعد القانونية، فإن المؤسسات الدولية المتخصصة، سواء كانت قضائية أو أمنية، لها دور فعال وحيوي في تطبيق الاتفاقيات، وتبادل المعلومات، وكذلك دعم الدول التي تتسم بالإمكانات المحدودة. كما أن التنسيق بين السلطات الأمنية والقضائية في مختلف الدول يجسّد أحد ركائز هذا التعاون، لما له من دور فعال في تعقب الجناة، وتجميع الأدلة، وملاحقتهم قضائياً. لذلك سنتناول هذا المطلب في فرعين خصص الأول لدور المنظمات الدولية (الفرع الأول)، والثاني لآليات التنسيق القضائي والأمني (الفرع الثاني).

الفرع الأول: دور المنظمات الدولية في مكافحة الجرائم المعلوماتية

تؤدي المنظمات الدولية دوراً هاماً في تعزيز التعاون الدولي لمكافحة الجرائم المعلوماتية. فالإنترنت، باعتباره منظمة شرطية دولية، يمتلك شبكة اتصالات تربط بين الأجهزة الأمنية لما يتجاوز 190 دولة. وسعيها منه لمكافحة الجريمة المعلوماتية العابرة للحدود والحد منها، قام بإنشاء مركزاً متخصصاً للجرائم الرقمية في سنغافورة، عرف بـ"المركز العالمي للابتكار"، وظيفته تبادل المعلومات التكتيكية والفنية المتعلقة بالتهديدات الإلكترونية، إضافة إلى قيامه بتدريب الدول الأعضاء ودعمها فنياً، خاصة منها التي لتزال تعاني من نقص في الكفاءات التقنية. فمن خلال آلية الاتصال الآني الأمن الذي وفره "المركز العالمي للابتكار"، تمكنت الدول من تبادل

المعلومات الجنائية المتعلقة بالجريمة المعلوماتية بسرعة وفعالية. إضافة إلى إطلاق الإنترنت في إطار مكافحة الجريمة المعلوماتية لعمليات دولية ناجحة، كعملية "أوكس" في غرب إفريقيا، التي كانت نتيجتها تفكيك شبكات احتيال إلكتروني عابرة للحدود، واعتقال جملة من المتورطين⁽¹³⁾.

أما منظمة الأمم المتحدة، فإن دورها في التصدي للجريمة المعلوماتية فيتجلى من خلال مكتب الأمم المتحدة المعني بالمخدرات والجريمة، الذي يقوم بدعم الدول في صياغة سياسات وطنية لمكافحة الجريمة الإلكترونية، إضافة إلى توفير تقارير هامة من بينها "الدراسة الشاملة حول الجريمة السيبرانية"، التي تناولت التحديات التي تواجهها الدول النامية في تطبيق معايير التعاون الدولي⁽¹⁴⁾.

من جهة أخرى، تقوم "يوروبول"، وهي وكالة تطبيق القانون التابعة للاتحاد الأوروبي، عن طريق المركز الأوروبي للجرائم السيبرانية، بتنسيق جهود الدول الأعضاء في الاتحاد الأوروبي للتصدي ومواجهة الهجمات الإلكترونية، خاصة منها التي تستهدف البنية التحتية الحيوية. كما تدعم "يوروبول" التحقيقات من خلال تحليل البيانات الجنائية وتوفير الخبراء، وإنشاء فرق مشتركة بين الدول الأعضاء، كما هو الحال في عملية تفكيك شبكة "أموات" للبرمجيات الخبيثة، التي تمت بمشاركة العديد من الدول الأوروبية⁽¹⁵⁾.

عموماً، تؤكد هذه النماذج أن المنظمات الدولية لا تكتفي بالدور التنسيقي، وإنما أضحت عضواً فعالاً مباشراً في توفير الحلول التقنية، والتدخل الميداني، إضافة إلى إرساء ثقافة التعاون المستمر بين الدول، في منأى عن الاختلافات التشريعية أو المواقف السياسية.

الفرع الثاني: آليات التنسيق بين السلطات القضائية والأمنية للدول

لا يكتمل التعاون الدولي دون وجود آليات عملية تمكّن السلطات الأمنية والقضائية داخل الدول من التفاعل الفعال والسريع لملاحقة الجناة في الفضاء الرقمي، الذي من أبرز صفاته سرعة التغيير والتطور. وتُعدّ الإنابات القضائية، والتسليم المؤقت وطلبات المساعدة القانونية المتبادلة، من أبرز الوسائل التي تعتمد عليها الدول لتجاوز العقبات الإجرائية التي تعترض سبيل تحقيق العدالة⁽¹⁶⁾.

تُتيح الاتفاقيات الدولية، وعلى رأسها اتفاقية بودابست، آليات لتقديم المساعدة القضائية في القضايا المعلوماتية، خاصة المتعلقة بالحصول على الأدلة الرقمية، ومصادرة الأجهزة، وتجميد الحسابات الإلكترونية، والتحقيق مع الجناة على الإقليم الترابي للدولة التي ارتكبت فيها الجريمة المعلوماتية أو في إقليم بلد المتضرر. ويعزز هذه الآليات البروتوكول الإضافي الثاني للاتفاقية من خلال السماح بالتواصل المباشر مع مزودي الخدمات الرقمية خارج نطاق الإجراءات البيروقراطية التقليدية⁽¹⁷⁾.

وتبيّن بعض التجارب الناجحة أهمية التنسيق بين هيئات التحقيق والنيابات العامة في دول مختلفة، كالتعاون القضائي بين كندا وفرنسا في قضية اختراق أنظمة مصرفية، أو بين هولندا وألمانيا في جرائم الاحتيال عبر الإنترنت. وتدعم هذه التجارب مقترح إنشاء منصات إقليمية دائمة للتنسيق القضائي الإلكتروني، وهو ما تناولته يوروجست في أوروبا وشرعت في تكريسه. أما أمنياً، فالتنسيق بين هذا النوع من الأجهزة فيتبلور عن طريق تنظيم دورات تدريبية مشتركة وتبادل المعلومات الاستخباراتية الفنية، إضافة إلى إنشاء فرق أمنية متخصصة تعمل بتنسيق ميداني، كما حدث في عملية تفكيك شبكة (نو نايم) المؤيدة لروسيا، والتي تم خلالها اعتقال عناصر في عدة دول بالتنسيق مع "يوروبول"⁽¹⁸⁾.

لكن رغم التقدم في هذه الآليات، إلا أنه لزالّت توجد تحديات كبرى لعلّ في مقدّماتها تضارب السيادة القضائية، وغياب الثقة بين بعض الدول، لاسيما في ما يتعلق بتبادل المعلومات الداخلية الحساسة. وتُشير بعض الدراسات إلى أن غياب اتفاقيات التعاون القضائي الثنائي يمثل عقبة أمام 42% من طلبات المساعدة القانونية المرتبطة بالجرائم المعلوماتية. لذلك، يرى بعض الفقهاء ضرورة تطوير أدلة إجرائية موحدة للتعاون القضائي، وإنشاء شبكات إقليمية لها الإمكانية والقدرة على التدخل العاجل، إضافة إلى تعزيز الكفاءات التقنية للقضاة والمحققين للتعامل مع الأدلة الرقمية⁽¹⁹⁾.

المبحث الثاني: الأساليب التقنية والعملية للتعاون الدولي في مكافحة الجرائم المعلوماتية

في ظل الطبيعة التقنية المعقدة للجرائم المعلوماتية، لا يقتصر التعاون الدولي على الجوانب القانونية والمؤسسية فقط، وإنّما يستوجب تبني أساليب تقنية وعملية تعزز القدرة على الاستجابة

الفعّالة والسريعة للتهديدات السيبرانية. فالتطور التكنولوجي الهائل والمستمر عبر الزمن يفرض تحديات جديدة أمام الدول، يجعلها تسعى على مدار الساعة إلى تطوير آليات حديثة لتبادل المعلومات، وتعزيز القدرات الرقمية، وتنسيق الجهود بشكل ميداني مباشر. لذلك تناول هذا المبحث الأساليب التقنية والعملية المعتمدة في التعاون الدولي لمكافحة الجرائم المعلوماتية، وتطرق إلى مطلبين تجلّي الأول في تبادل البيانات والاستخبارات الرقمية (المطلب الأول)، والثاني بالتحقيقات المشتركة وبناء القدرات (المطلب الثاني).

المطلب الأول: تبادل البيانات والمعلومات الاستخباراتية الرقمية

تجسّد الاستخبارات السيبرانية والمعلومات الرقمية إحدى أهمّ الموارد لمكافحة الجرائم المعلوماتية، نظرًا لدورها الهامّ للتنبؤ بالهجمات، وتحديد الفاعلين، وتعقب مسارات الجرائم. لذلك أصبح التعاون الدولي في هذا المجال ضرورة لا غنى عنها، خصوصًا في ظل لجوء الجماعات الإجرامية إلى تقنيات التخفي وتعدد الجنسيات، ما يستوجب إحداث منصات لتبادل البيانات السيبرانية (الفرع الأول)، و تبادل الأدلة الرقمية والمحتوى الرقمي ذي الصلة (الفرع الثاني).

الفرع الأول: منصات تبادل البيانات السيبرانية الدولية

شهد التعاون الدولي في مجال الأمن السيبراني تطورًا ملموسًا حيث تمّ إنشاء منصات رقمية مشتركة تتولى تبادل المعلومات الاستخباراتية والفنية المتعلقة بالتهديدات السيبرانية. وقد أضحت هذه المنصات إحدى الأسس التي تعتمدها الدول لمكافحة الجرائم المعلوماتية والهجمات الإلكترونية المعقدة التي تتجاوز الحدود الجغرافية، حيث تُمكن بشكل فوري من تبادل مؤشرات الاختراق، ومشاركة التحليلات الفنية للبرمجيات الخبيثة، ما يعزز سرعة الاستجابة وتنسيق الجهود الأمنية بين الدول.

ولعلّ من أبرز هذه المبادرات، المنصة الدولية لمعلومات التهديدات السيبرانية التي أنشأها المنتدى العالمي لمكافحة الجرائم الإلكترونية، والتي تُعد نموذجًا حديثًا للتعاون الفني متعدد الأطراف. إذ تُتيح هذه المنصة المجال أمام الجهات الأمنية الوطنية والخبراء السيبرانيين لتبادل البيانات المتعلقة بأساليب الاختراق الجديدة، والبرمجيات الخبيثة، وكذلك البنية التحتية الرقمية

المستهدفة. وتكمن أهمية هذه المنصة في طابعها التفاعلي، فهي توفر قاعدة بيانات تحليلية محدثة باستمرار، مع واجهات تقنية تمكن المشاركين من التفاعل بشكل مباشر وسريع، مما يساهم في بناء وعي مشترك حول التهديدات السيبرانية⁽²⁰⁾.

وفي ذات التوجه، أطلقت "وكالة الأمن السيبراني وأمن البنية التحتية" في الولايات المتحدة الأمريكية، بالتعاون مع عدد من الدول والمؤسسات الدولية، منصة إلكترونية تُعرف باسم "نظام تبادل مؤشرات التهديد الآلي" بهدف تمكين الجهات الحكومية والخاصة من تبادل مؤشرات الهجمات الإلكترونية بشكل سريع وآلي، مما يُقلص هوة الزمن الفاصل بين اكتشاف التهديد وتعميمه على جميع الشركاء. ولهذه المنصة دور هام في تنسيق الجهود العالمية لاحتواء أكبر الهجمات كهجوم "سولارويندز"، الذي استهدف بنية تحتية حكومية لما يتجاوز عشر دول، من خلال استغلال تحديثات برمجية لشركة تكنولوجيا أمريكية تُستخدم في عدة قطاعات وعلى نطاق واسع.

لكن رغم أهمية هذه المبادرات، إلا أن واقع تبادل البيانات السيبرانية مازال يواجه جملة من التحديات، أبرزها إبداء بعض الدول تحفظات حول الانخراط الكامل في مثل هذه المنصات، وذلك لاعتبارات تتعلق بالسيادة الرقمية، وتخوفها من تسريب معلومات هامة وحساسة قد تمس من الأمن القومي. كما أن الاختلاف في السياسات التقنية والقانونية بين الدول قد يشكل عائقاً أمام تحقيق التكامل المطلوب. ونتيجة لذلك، دعا عدد من المتخصصين إلى تبني نظام عالمي موحد لتصنيف مؤشرات التهديدات الإلكترونية وتبادلها، مع احترام خصوصيات كل دولة وسيادتها⁽²¹⁾.

عموماً، إن تنامي الترابط الرقمي العالمي وتطور طبيعة التهديدات السيبرانية، يوجب على الدول تجاوز السياسات الانعزالية، والانخراط في آليات تبادل معلومات شاملة وفعالة. فالجرائم المعلوماتية لا تعترف بالحدود الجغرافية، بالتالي فمواجهتها يتطلب تعاوناً عابراً للأنظمة السياسية والقانونية الوطنية، وإرساء بنية تحتية مشتركة وإقرار مبدأ الثقة المتبادلة، وأخيراً الاستعداد الدائم لتبادل المعلومات والمخاطر.

الفرع الثاني: تبادل الأدلة الرقمية والمحتوى الرقمي ذي الصلة

أصبح الحصول على الأدلة الرقمية في الجرائم السيبرانية من أهمّ التحديات التي تواجه أجهزة العدالة الجنائية، خاصّة عندما تكون تلك الأدلة مخزنة خارج حدود الدولة أو لدى شركات مختصة في تزويد الخدمات الإلكترونية لا تخضع بصفة مباشرة للقانون الوطني. لذلك وفي ظل الطبيعة العابرة للحدود للجريمة المعلوماتية، أصبح تبادل الأدلة الرقمية بين مختلف الدول أداة أساسية لتيسير المحاكمات والتحقيقات وكذلك ضمان فعالية الرد القانوني على هذا النوع من الجرائم⁽²²⁾.

وفي هذا السياق، مثّلت اتفاقية بودابست لمكافحة الجرائم الإلكترونية، المعتمدة من قبل مجلس أوروبا، نقطة تحول رئيسية في ميدان التعاون القضائي الدولي الرقمي. حيث نصّت الاتفاقية وكذلك البروتوكول الإضافي الثاني على آليات مرنة وواضحة لتسهيل تبادل الأدلة الرقمية، مع إتاحة التواصل المباشر بين السلطات المختصة في الدولة الطالبة وبين مقدّمي خدمات تقنية المعلومات والاتصالات في الدول الأخرى، شرط احترام الضوابط السيادية والقانونية المعتمدة. وتعدّ هذه الخطوة نقلة نوعية هامة في سبيل تجاوز العقبات التقليدية التي كانت تعوق مسار التعاون القضائي، خاصة القضايا التي تتطلب استجابة فورية وتدخلاً عاجلاً⁽²³⁾.

إضافة إلى الأطر الاتفاقية، شهدت أوروبا مبادرات عملية لتعزيز تبادل الأدلة المخزنة على السحابة الإلكترونية. وفي هذا الإطار يبرز مشروع مجموعة أدلة السحابة الإلكترونية الذي أقره الاتحاد الأوروبي بالتعاون مع مؤسسات قضائية مختصة أبرزها الوكالة الأوروبية للتعاون القضائي الجنائي "يوروبجست". حيث هدف الاتحاد الأوروبي من هذا المشروع إلى وضع مبادئ توجيهية فعّالة وموحّدة لتبادل الأدلة الرقمية المخزّنة، بما يتوافق مع التشريعات الأوروبية لحماية الحقوق الخاصة والبيانات الشخصية. وقد تمخّض عن هذا المشروع جملة من التوصيات العملية مكّنت من صياغة نماذج قانونية موحّدة لطلبات التعاون، إضافة إلى تعزيز التدريب القانوني والفني للقضاة وأعضاء النيابة العامة في الدول الأعضاء.

وفي السياق الأكاديمي، أقرّ مركز الدراسات السيبرانية بجامعة كامبريدج في تقاريره الأخيرة على أن نجاح هذه المبادرات مرتبطة بتوفر بعض العوامل الأساسية، لعلّ أبرزها وجود قنوات اتصال مؤسسية مشقّرة وآمنة وتوفر الثقة المتبادلة بين الأطراف وضمان التوازن بين حقوق الأفراد في الخصوصية ومتطلبات الأمن العام. كما أكّدت التقارير على وجوبية أن تكون آليات تبادل الأدلة الرقمية مدعومة ببنية قانونية واضحة، تُراعي التباين في التشريعات الوطنية، وتحترم المعايير الدولية المتعلقة بمجال حماية البيانات.

لكن رغم ذلك، فلتزال بعض التحديات موجودة، لاسيما فيما يتعلق بتباين المواقف السياسية من التعاون في هذا المجال، وصعوبة إلزام بعض الشركات العالمية العملاقة، كمزوّدي خدمات البريد الإلكتروني والتخزين السحابي، بالاستجابة الفعّالة والسريعة لطلبات التعاون. ومن هنا تبرز الحاجة المؤكّدة والملحّة لتوسيع إطار الاتفاقيات الدولية، وتكثيف التنسيق بين الأجهزة القضائية، كاليابات العامة والسلطات المختصة في الأمن السيبراني، لضمان تفعيل التعاون الرقمي الجنائي بصفة آمنة وفعّالة.

عموماً، يُمكن القول بأن تبادل الأدلة الرقمية لم يضحى مجرد مسألة إجرائية أو تقنية فحسب، بل أصبح عنصراً هاماً ورئيسياً في أمن الدول واستقرارها القانوني. ومن هنا فإن العمل على تطوير آليات قانونية وتشغيلية وإرساء منصات أمر ضروري لتيسير هذا التبادل وبالتالي تجسيد خطوة استراتيجية هامة لتعزيز منظومة العدالة الجنائية في العصر الرقمي.

المطلب الثاني: التحقيقات المشتركة وبناء القدرات السيبرانية

ليس باستطاعة أيّ دولة، مهما بلغت قدراتها التكنولوجية والمعلوماتية، مواجهة التهديدات السيبرانية بمعزل عن بقية الدول. لذلك ظهرت الحاجة إلى إنشاء فرق تحقيق مشتركة (الفرع الأول)، وتكثيف جهود بناء القدرات البشرية والتقنية (الفرع الثاني)، لاسيما في الدول النامية، لتجاوز هوة التفاوت الرقمي وتعزيز الأمن السيبراني على المستوى العالمي.

الفرع الأول: التحقيقات السيبرانية المشتركة

في ظل ارتفاع نسبة الجرائم الإلكترونية واتساع نطاقها الجغرافي، أضحت تشكيل فرق تحقيق مشتركة بين الدول إحدى أهم مظاهر التعاون العملي الدولي في مكافحة الجريمة المعلوماتية

والتهديدات السيبرانية. وهذه الفرق تكتسب صبغة خاصة في القضايا التي تتعدى الحدود الوطنية، كهجمات الفدية التي تستهدف البنية التحتية الرقمية، وجرائم الابتزاز الإلكتروني، والاختراقات الماسة للأمن القومي للدول، فضلاً عن عمليات غسل الأموال الرقمية التي تتم عبر العملات المشفرة.

وتتطلع كل من الوكالة الأوروبية للتعاون في مجال إنفاذ القانون "يوروبول" والوكالة الأوروبية للتعاون القضائي الجنائي "يوروبجست" بدور هام ومحوري وفعال في تنسيق هذه التحقيقات، عن طريق إنشاء وحدات عمل مشتركة تضم ممثلين عن النيابة العامة والأجهزة الأمنية المتخصصة في مكافحة الجريمة السيبرانية من عدة دول مشاركة. ولعلّ أبرز عمليات التعاون بين الدول، عملية تفكيك شبكة "السوق المظلم" المعروفة باسم دارك ماركت، والتي نُفذت سنة 2021 بمشاركة سلطات أمنية وقضائية لأكثر من سبع دول، نتج عنها إيقاف عديد المتهمين تجاوز عددهم العشرين، ومصادرة معدات رقمية وخوادم بيانات موزعة على العديد من الدول⁽²⁴⁾.

وتعتمد هذه الفرق على جملة من أدوات التحليل الرقمية المتطورة، من بينها برمجيات الذكاء الاصطناعي التي تمكّن من تحليل كميات هائلة من البيانات الجنائية الرقمية، وكشف الأنماط المعتادة في سلوك الجناة، إضافة إلى أنظمة تتبّع العملات المشفرة، والتي تُستخدم لرصد تحركات الأموال المستخدمة في تمويل الجرائم المعلوماتية وهي أموال تكون عادة مجهولة المصدر. وقد ساهمت هذه الآليات في الكشف عن العديد من الشبكات المختصة في غسل الأموال الرقمية، ومرتكبي عمليات الفدية الإلكترونية والتي استهدفت مؤسسات مالية ومستشفيات على مستوى دولي⁽²⁵⁾.

لكن رغم هذا التطور، إلّا أنّه مازالت تتواجد العديد من العقبات التي تعيق فعالية التحقيقات المشتركة، لعلّ أهمّها تباين الإجراءات القضائية بين الدول، خاصة فيما يتعلق بجمع آليات إصدار أوامر التفتيش، والأدلة الرقمية، والضوابط القانونية لحماية المعطيات الخاصة. إضافة إلى الاختلافات اللغوية التي تشكّل أيضاً تحدياً أمام التنسيق السلس بين الفرق المشاركة،

الأمر الذي يستدعي توافر مترجمين تقنيين قانونيين مؤهلين، وكذلك فريق دعم يكون متعدد اللغات لضمان دقة المعلومات المتبادلة وسلامة إجراءات التحقيق⁽²⁶⁾.

كما تواجه بعض الفرق تحديات أخرى تعلّقت بتوزيع الاختصاص القضائي، فقد تُثار نزاعات حول الجهة التي تمتلك اختصاص محاكمة المتهمين أو تنفيذ العقوبات. لذلك أضحى من الضروري تعزيز الأطر القانونية المنظمة لعمل هذه الفرق، وتحديد اختصاصات كل دولة على حدا بشكل واضح، إضافة إلى تكثيف برامج التدريب القضائي والتقني للمحققين وأعضاء النيابة العامة في مجال الجريمة المعلوماتية.

عموماً، يُمكن القول بأن التحقيقات السيرانية المشتركة تجسّد خطوة هامة ومتقدمة نحو تحقيق عدالة جنائية فعالة وعابرة للحدود، فهي تُبيّن مدى الحاجة إلى تعاون وثيق بين الجهات الأمنية والقضائية على المستوى الدولي، لمواجهة التهديدات الرقمية المعقّدة والمتزايدة.

الفرع الثاني: بناء القدرات وتدريب الكفاءات السيرانية

في ظل انتشار التهديدات الرقمية وتعمّد أساليب الجريمة السيرانية، لم يعد التركيز على التحقيقات والردود الأمنية بمفردها كافياً، وأتّما أضحى تدريب الكفاءات البشرية وبناء القدرات المؤسسية حجر الأساس في تعزيز الأمن السيراني على المستوى الدولي. فنقص الموارد البشرية المختصة يمثّل أهمّ التحديات التي تواجه غالبية الدول، خاصّة تلك التي تواجه ضعفاً على مستوى البنية التحتية الرقمية، أو التي في طور تحديث أجهزتها الأمنية والقضائية. وتبرز هذه الفجوة خاصّة في دول إفريقيا وآسيا، حيث تشير تقارير دولية إلى محدودية عدد القضاة والمدعين العامين المختصين في الجرائم المعلوماتية، إضافة إلى ندرة الخبراء القادرين على التعامل مع الأدلة الرقمية وتحليل الهجمات السيرانية²⁷.

لذلك واستجابةً لهذا التحدي، عملت العديد من المنظمات الدولية على تطوير برامج متخصصة تهدف إلى نقل المعرفة التقنية وبناء كفاءات وطنية مستدامة. ويعد مكتب الأمم المتحدة المعني بالمخدرات والجريمة من أهمّ الجهات الفاعلة في هذا المجال، حيث أطلق المكتب برنامجاً دولياً لمكافحة الجريمة المعلوماتية تحت عنوان البرنامج العالمي للجريمة السيرانية. ويهدف هذا البرنامج إلى تدريب أعضاء النيابة العامة، والقضاة وخبراء الأمن السيراني، فيما يزيد عن

ستين دولة حول العالم، عن طريق ورش عمل ودورات تدريبية عملية ونظرية، تُراعي الخصوصيات القانونية والثقافية لكل دولة، مع التأكيد على التعاون بين الجهات القضائية والتقنية.⁽²⁸⁾

وبموازاة هذا السعي، تعمل منظمة الأمن والتعاون في أوروبا على تنظيم ورش عمل إقليمية تهدف إلى تمكين السلطات المختصة من التعامل بفعالية مع قضايا الجرائم المعلوماتية. وتشمل هذه الورش مجالات متعددة، لعلّ أهمها تحليل أنماط الهجمات الإلكترونية واسترجاع الأدلة الرقمية من الأجهزة المصادرة، واستخدام البرامج المتقدمة في إدارة مسرح الجريمة الرقمية. وقد ساهمت هذه المبادرات في دعم آسيا الوسطى ودول أوروبا الشرقية، حيث كانت هناك حاجة ماسة لتطوير قدرات وطنية مستقلة في مجال التحقيقات المتعلقة بالجرائم المعلوماتية.

كما تؤكد عدد من التقارير الصادرة عن البنك الدولي أن الاستثمار في رأس المال البشري الرقمي من أنجع السبل لمواجهة الجرائم المعلوماتية بطريقة مستمرة. ففي تقرير حديث صدر سنة 2023، بيّن البنك أن الدول التي خصّصت ميزانيات هامة وواضحة لتدريب القضاة والخبراء في هذا المجال، وأدجت الجوانب التقنية ضمن مؤسسات العدالة، سجّلت انخفاضاً هاماً بنسبة 37% في معدل الجرائم المعلوماتية التي تستهدف البنية التحتية الرقمية الحيوية، كشبكات الطاقة والمستشفيات والبنوك.

إلى جانب التدريب المباشر، دعمت هذه المبادرات إنشاء مراكز إقليمية للأمن السيبراني، تُعنى بتوفير الدعم التقني والفني للدول الأقل خبرة، وتمكينها من المشاركة في التعاون الدولي. وتعمل هذه المراكز، التي تتواجد في آسيا وإفريقيا وأمريكا اللاتينية، كحلقة وصل بين المؤسسات الأمية والدول، وتوفر بيئة لتبادل الخبرات وتنسيق الجهود في مجال مواجهة الجريمة الرقمية⁽²⁹⁾.

لكن على الرغم من هذه الجهود، فإن التحديات لا تزال متواجدة، خاصة فيما يتعلق باستمرارية البرامج التدريبية، ومحدودية الموارد المالية، والتفاوت في مستوى التعليم التقني بين الدول. ومن هنا، يبرز دور المجتمع الدولي في ضمان تمويل مستمر لتلك المبادرات، ووضع آليات لتقييم أثرها ومدى قدرتها على إحداث تحول نوعي في منظومة العدالة السيبرانية في الدول المستفيدة.

خاتمة:

كشفت هذه الدراسة عن أهمية التعاون الدولي في مواجهة الجرائم المعلوماتية، التي أضحت تجسّد تهديداً عابراً للحدود، يستهدف على السواء الأفراد والدول. وتبيّن من خلال هذا البحث أن النجاعة في مكافحة هذه الظاهرة ليست مقتصرة على تبني التشريعات الوطنية فحسب، وإنما تستوجب اعتماد مقاربات متعددة الأطراف، تشمل آليات تبادل المعلومات والأطر المؤسسية والقانونية، والتحقيقات المشتركة، وبناء القدرات الفنية والقضائية.

أولاً: النتائج

من أبرز النتائج التي توصّلت إليها الدراسة

1. تمثّل اتفاقية بودابست الإطار القانوني الدولي الأكثر شمولاً لمكافحة الجرائم المعلوماتية، لذلك كان لها دور هام في إرساء قواعد موحدة للجريمة، والتعاون القضائي الدولي، رغم تحفظ بعض الدول عليها.
2. شكّلت الاتفاقيات الثنائية والإقليمية بديلاً مرناً وسريعاً لتعزيز التعاون بين الدول التي لها نفس المصالح الأمنية، وبرزت تجارب عربية وإفريقية هامة في هذا المجال، لكنّ تأثيرها مازال محدوداً بسبب ضعف التنسيق التقني.
3. تجسّد المنظمات الدولية كالإنتربول، يوروبول، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة دوراً هاماً ومحورياً في تقديم الدعم الفني، وتبادل المعلومات، وتنسيق التحقيقات عبر الحدود، وهو ما يُعزز فعالية العمل المشترك.
4. لا يمكن تحقيق تعاون فعّال دون وجود آليات تنسيق قضائي وأمني سريعة وواضحة، لذلك تُعدّ الإنابات القضائية والمساعدة القانونية المتبادلة والتسليم المؤقت من أهمّ الوسائل المعتمدة، إلّا أن تعقيد الإجراءات ما زال يُشكل عائقاً في عدّة من القضايا.
5. تواجه الدول العربية تحديات متعدّدة في مجال مكافحة الجرائم المعلوماتية، من أبرزها غياب شبكات التعاون الإقليمي الفاعلة، وضعف البنية التشريعية والتقنية، ومحدودية الموارد البشرية المتخصصة.

ثانيًا: الاقتراحات

بناءً على ما سبق، يُقترح

1. انضمام الدول العربية إلى الاتفاقيات الدولية متعددة الأطراف، وعلى رأسها اتفاقية بودابست، مع تعديل التشريعات الوطنية لكي تتماشى مع هذه المواثيق.
2. إنشاء منصة إقليمية أو عربية لتبادل الأدلة الرقمية والمعلومات السيبرانية، تكون مستقلة ومنسجمة مع خصوصيات القوانين الوطنية، وتُسهل في تسريع آليات التنسيق القضائي.
3. تكثيف برامج التدريب القضائي والتقني لوكلاء النيابة والقضاة، وضباط الشرطة المختصين بالجرائم المعلوماتية، بالتعاون مع منظمات دولية كالإنتربول.
4. إقرار أدلة إجرائية موحدة بين الدول العربية بشأن التعاون في قضايا الجريمة الإلكترونية، تتضمن نماذج موحدة لطلبات المساعدة والإنابات القضائية.
5. تفعيل آليات التقييم المستمر والرقابة على أداء الأجهزة القضائية والأمنية في مجال مكافحة الجريمة المعلوماتية، من خلال آليات قياس الأثر والتقارير الدورية.
6. دفع الجامعات ومراكز البحوث العربية إلى تطوير دراساتها حول الجريمة المعلوماتية، بهدف إنتاج معرفة محلية لهذا النوع من الجرائم ما يساهم في صياغة السياسات العامة المبنية على الأدلة.

المراجع

- محمد أحمد علي، التعاون الدولي في مكافحة الجريمة السيبرانية: إطار قانوني وتكنولوجي، دار الشروق للطباعة والنشر، الطبعة الأولى 2022، ص. 45-67.
- أحمد يوسف عبد الله، "التحقيقات السيبرانية المشتركة بين الدول العربية: دراسة تحليلية"، مجلة الأمن السيبراني العربي، مصر، المجلد 3، العدد 1، سنة 2023، ص. 112-130.
- سارة خالد محمد، "منصات تبادل المعلومات السيبرانية والتعاون العربي: واقع وتحديات"، أطروحة ماجستير، جامعة تونس، سنة 2024، ص. 58-78.

- خالد عبد الرحمن، "آليات بناء القدرات السيبرانية المشتركة في دول الخليج"، مداخلة في المؤتمر العربي للأمن الإلكتروني، الرياض، 15-17 مايو 2023، المملكة العربية السعودية.
- خالد علي، "التبادل الإلكتروني للأدلة الجنائية في السحابة الرقمية"، 5 مارس 2024، آخر الاطلاع 20 أغسطس 2025، <https://example.com>.
- مجلس أوروبا، اتفاقية بودابست بشأن الجرائم المعلوماتية، صادرة عام 2001، نسخة مترجمة، ص. 12-35.
- الإنتربول، تقرير "المركز العالمي للابتكار في مكافحة الجرائم الرقمية"، 2022، متاح عبر <https://interpol.int>، تم الاطلاع في 15 أغسطس 2025.
- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، "الدراسة الشاملة حول الجريمة السيبرانية"، 2013، متاح عبر <https://unodc.org>، تم الاطلاع في 10 أغسطس 2025.
- يوروبول، تقرير المركز الأوروبي للجرائم السيبرانية (EC3)، 2021، متاح عبر <https://europol.europa.eu>، تم الاطلاع في 12 أغسطس 2025.
- عبد الله، أحمد يوسف، التعاون القضائي الدولي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2018، ص. 111.
- القاسمي، سعيد محمد، "التحديات التقنية في التعاون القضائي للجرائم السيبرانية"، مجلة الدراسات القانونية العربية، عمان، المجلد 10، العدد 2، 2021، ص. 65-78.
- الكبيسي، علي حسن، الجرائم المعلوماتية والتعاون الدولي: دراسة مقارنة، مكتبة النهضة، بغداد، 2019، ص. 140-155.

* المؤلف المراسل

- 1 محمد الرفاعي، الجرائم الإلكترونية والتعاون الدولي في مكافحتها، المجلة الدولية للقانون والمعلوماتية، الجزائر، المجلد 3، العدد 4، 2020، ص 85-106.
- 2 هناء عبد الله، أثر التباين التشريعي على فعالية التعاون الدولي لمكافحة الجرائم المعلوماتية، مجلة العلوم القانونية، الجزائر، المجلد 16، العدد 2، 2018، ص 92-115.
- 3 طارق الكبيسي، التعاون الدولي في مكافحة الجريمة الإلكترونية بين النظرية والتطبيق، مجلة القانون والسياسة، العراق، المجلد 10، العدد 15، 2019، ص 133-154.
- 4 إسمهان حارموش، آليات التعاون الدولي لمكافحة الجرائم السيبرانية. «المجلة الجزائرية للحقوق والعلوم السياسية، العدد 1، المجلد 9، الجزائر، 2024، ص 1758-1772.
- 5 وهيبة بلعالية، وهيبة، اتفاقية بودابست المتعلقة بالجريمة المعلوماتية: دراسة تحليلية، المجلة الجزائرية للحقوق والعلوم السياسية، الجزائر، المجلد 6، العدد 2، 2021، ص 112-129.
- 6 كامبينيا، آنا وروغريس، كارلوس، "الجريمة المعلوماتية واتفاقية بودابست التابعة لمجلس أوروبا: الوقاية، التجريم، والتعاون الدولي." في كتاب ملخصات أوراق مؤتمر زيمغا الدولي السابع للبحوث العلمية، الأناضول، تركيا، 21-23 يناير 2022، ص 112-123.
- 7 أندريا كوشيني، البروتوكول الإضافي الثاني لاتفاقية بودابست: تعزيز التعاون الدولي أم تعريض الحقوق الأساسية للخطر؟ «أرشيف القانون الدولي (Archiv des Völkerrechts)»، المجلد 61، العدد 1، 2023، ص 60-83.
- 8 محمد الرفاعي، الجرائم الإلكترونية والتعاون الدولي في مكافحتها، المجلة الدولية للقانون والمعلوماتية، الجزائر، المجلد 3، العدد 4، 2020، ص 89. ويوسف القاسمي، الجرائم المعلوماتية في القانون الدولي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2021، ص 55.
- 9 عبد الحكم سيد سامان، الجرائم المعلوماتية وآثارها: في ضوء قانون مكافحة جرائم تقنية المعلومات. المركز للدراسات العربية للنشر والتوزيع، الطبعة الأولى، مصر، 2023، ص 320.
- 10 بيان، ساي. الارتقاء الاستراتيجي: الاتجاهات الناشئة في التعاون السيبراني بين الولايات المتحدة والهند. معهد دراسات جنوب آسيا (ISAS)، الجامعة الوطنية في سنغافورة، الطبعة الأولى، سنغافورة، مايو 30، 2025، صفحات غير مرقمة.
- 11 مريم لوكال، «قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014»، مجلة الدراسات القانونية والاقتصادية، الجزائر، المجلد 4، العدد 3، 2021، ص 657-673.
- 12 هناء عبد الله، أثر التباين التشريعي على فعالية التعاون الدولي لمكافحة الجرائم المعلوماتية، المرجع السابق، ص 107. وطارق الكبيسي، التعاون الدولي في مكافحة الجريمة الإلكترونية بين النظرية والتطبيق، المرجع السابق، ص 143.
- 13 إسحق أوجيني، "عملية للإنتربول توجه ضربة قاصمة للجريمة المالية في غرب أفريقيا"، 16 يوليو 2024، تاريخ الاطلاع: 28 أغسطس 2025، رابط المقال.

https://www.interpol.int/ar/1/1/2024/16?utm_source=chatgpt.com

- 14 سانديج جون، جرينبلات سارة، موراي جيليان، الدراسة الشاملة حول الجريمة السيبرانية (مسودة)، بالتعاون مع مجموعة خبراء حكوميين، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2013، تاريخ الاطلاع: 29 أغسطس 2025.
- 15 أليساندرو ماسيلينو، عملية قاذمها "يوروبول" تحت اسم "إندغيم" تستهدف شبكات البرمجيات الخبيثة وبرامج الفدية، مجلة "إنفوسيكوريتي ماغازين"، 30 مايو 2024، تاريخ الاطلاع: 29 أغسطس 2025، <https://www.infosecurity-magazine.com/news/europol-endgame-botnet-ransomware>
- 16 يوسف برقوق، "المساعدة القضائية المتبادلة لمواجهة الجرائم الإلكترونية"، مجلة البصائر للدراسات القانونية والاقتصادية - الجزائر، المجلد 1، العدد 1، 5 مارس 2021، ص 93-103.
- 17 ل. أكسو، Second Additional Protocol to the Budapest Convention on Cybercrime: Overview (Cybercrime: Overview)، تقرير نشر في هولندا، 21 يونيو 2023، تاريخ الاطلاع: 29 أغسطس 2025، [policycommons.net](https://www.policycommons.net)
- 18 وكالة الأنباء الفرنسية، "عملية إستوود: تفكيك شبكة قراصنة موالية لروسيا"، وكالة الأنباء الفرنسية، 16 يوليو 2025، تاريخ الاطلاع: 29 أغسطس 2025، <https://www.alarabiya.net/News/world/2025/07/16/europolled-global-operation-takes-down-prorussian-cybercrime-network>.
- 19 شريف كامل، السياسة الجنائية في مواجهة الجرائم المعلوماتية، دار المنارة للنشر والتوزيع، الطبعة الأولى، القاهرة، مصر، 2022، ص 285.
- 20 محمد عبد الله الشامي، التعاون الدولي في مكافحة الجرائم الإلكترونية: المنصات الرقمية ودورها في تعزيز الأمن السيبراني، دار الفكر العربي، الطبعة الأولى، بيروت، لبنان، 2023، ص 112.
- 21 عادل حسن المزين، التحديات القانونية والأمنية في تبادل المعلومات السيبرانية الدولية، دار النهضة العربية، الطبعة الثانية، عمان، الأردن، 2024، ص 157.
- 22 سامي عبد الرحمن، الأدلة الرقمية والتحديات القانونية في مكافحة الجرائم السيبرانية، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، 2023، ص 134.
- 23 فاطمة الزهراء الحميدي، التعاون القضائي الدولي في مكافحة الجرائم الإلكترونية: دراسة في اتفاقية بودابست وآلياتها، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، 2024، ص 98.
- 24 خالد محمود علي، التعاون القضائي والأمني الأوروبي في مكافحة الجرائم السيبرانية: دراسة حالة شبكة السوق المظلم (دارك ماركت)، دار النهضة العربية، الطبعة الأولى، بيروت، لبنان، 2023، ص 143.
- 25 ليلي أحمد يوسف، التقنيات الحديثة في مكافحة الجرائم السيبرانية: الذكاء الاصطناعي والعمليات المشفرة، دار الكتب العلمية، الطبعة الأولى، القاهرة، مصر، 2024، ص 121.

- 26 محمود عبد الرحيم، التحديات القانونية والإجرائية في التعاون الدولي لمكافحة الجرائم الإلكترونية، دار الفكر الحديث، الطبعة الأولى، عمان، الأردن، 2023، ص 174.
- 27 أحمد عبد الله الشريف، تطوير القدرات البشرية في الأمن السيبراني: تحديات وفرص في الدول النامية، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، 2024، ص 210.
- 28 سامية عبد الرحمن، برامج بناء القدرات الدولية في مكافحة الجرائم السيبرانية: دور مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دار الفكر العربي، الطبعة الأولى، بيروت، لبنان، 2023، ص 165.
- البنك الدولي، الاستثمار في رأس المال البشري الرقمي وأثره على مكافحة الجرائم المعلوماتية: تقرير عام 2023، واشنطن، الولايات المتحدة الأمريكية، 2023، ص 48.
- 29نادية حسين الزهيري، المراكز الإقليمية للأمن السيبراني ودورها في دعم القدرات الوطنية لمكافحة الجريمة الرقمية، دار الصفاء للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2023، ص 132.