الجمهورية الجزائرية الديمقراطية الشعبية
People’s democratic republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of higher education and scientific research
جامعـــة محمد البشيـــر الإبراهيمـــي ــ برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi-BBA
كلية الحقوق و العلوم السياسيـــة
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر في القانون

تخصص: قانون اعلام آلي وأنترنت

الموسومة بـــ :

التعاون الدولي لمكافحة الجريمة الإلكترونية

من إعداد:

- بن حسين علي
- يحياوي السعدي

إشراف الأستاذ:

د/ حسين بن داود

نوقشت وأجيزت يوم : 2025/06/18

الاسم واللقب	الرتبـــــة	الصفة
د/ رفاف لخضر	أستاذ محاضر قسم أ	رئيسا
د/ حسين بن داود	أستاذ محاضر قسم أ	مشرفا و مقررا
د/ بكيس عبد الحق	أستاذ محاضر قسم أ	ممتحنا

السنة الجامعيـــــة: 2024م/2025م

ملحق بالقرار رقم ....1082.... المؤرخ في 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): بن حسين علي الصفة: طالب، أستاذ باحث، طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: A04127591 والصادرة بتاريخ 2014 04 09

المسجل(ة) بكلية / معهد الحقوق قسم العلوم السياسية

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

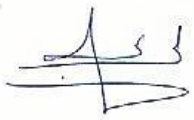
عنوانها: التعاون الدولي لمكافحة الجريمة الالكترونية

.....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 15 جوان 2025.....

توقيع المعني (ة)



ملحق بالقرار رقم ....1082.... المؤرخ في ....27 ...2020....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله.

السيد(ة): يحياوي سعدى الصفة: طالب، ~~أستاذ باحث~~ طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: 403092056 والصادرة بتاريخ 01/01/2022

المسجل(ة) بكلية / معهد: الحقوق قسم القانون العام

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: التعاون الدولي لمكافحة الجريمة الإلكترونية

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في انجاز البحث المذكور أعلاه .

التاريخ: 15 جوان 2025

توقيع المعني (ة)


بسم الله الرحمن الرحيم
١٤٢٠

شكر وعرفان

الحمد لله شكرا وامتنانا،واقرارا بفضله واحتراما بعظيم كرمه ، الحمد لله ليلا ونهارا ، سرا وجهارا، الحمد لله حين البدء والختام ، الحمد لله الذي اكرمنا ووفقنا لإكمال هذا العمل.

يشرفنا ان نتقدم بأسمى عبارات الشكر والعرفان والتقدير والمحبة إلى من مهدوا لنا طريق المعرفة والعلم

إلى جميع اساتذتنا الأفاضل أساتذة كلية الحقوق والعلوم السياسية جامعة محمد البشير الابراهيمي

ونخص بالشكر ونرفع كلمة تقدير له الدكتور الفاضل حسين بن داود حفظه الله وأطال في عمره لتفضله الكريم بالإشراف على هذه المذكرة، وتكرمه بنصحنا وتقديمه توجيهات علمية وارشادات قيمة حتى إتمام هذه المذكرة فجزاه الله كل خير

كما نتقدم بجزيل الشكر إلى أعضاء اللجنة المناقشة لقبولهم مناقشة هذه المذكرة

إهداء

من قال ان لها نالها

وأنا لها إن أبت رغم عنها أتيت بها

بكل حب أهدي ثمرة نجاحي وتخرجي :

إلى كل من سعت وضحت وشقت دربي نحو نور.

إلى من أوصاني الرحمان بها برا وإحسانا.

إلى من كان دعائها سر قوتي أمي الغالية.

إلى من علمني أن الدنيا كفاح وسلاحها العلم والمعروفة

إلى الذي لم يبخل غني بأي شئ إلى من سعى لأجل راحتي ونجاحي أبي العزيز

إلى من دمهم يجري في عروقي وبوجودهم في الحياة أكتسب القوة والمحبة لا حدود لهما أخواتي وأخي

وإلى كل من دعمني ومد لي يد العون خلال مشواري الدراسي .

بن حسين علي

الإهداء

الحمد لله الذي وفقنا لهذا ولم نكن لنصل إليه لو لا فضل الله علينا .

أهدي هذا العمل إلى الوالدين الكريمين أسئل الله تعالى لأن يبارك لهما في عمرهما وحسناتهما

و إلى أخوتي وإخوتي .

ـــ إلى كل أصدقائي قريبهم و بعيدهم ، وخاصة رفيق دربي : لوصيف صلاح إلى من كان سندي الدائم في هذا العمل.

يحياوي السعدي

مقدمـــــة

مقدمة

في عصرنا الحالي، نشهد تحولاً جذرياً في طريقة تفاعلنا وعملنا وتواصلنا، حيث أصبحت التكنولوجيا الرقمية والإنترنت جزءاً لا يتجزأ من حياتنا اليومية. هذا التطور الهائل فتح آفاقاً واسعة للتقدم والابتكار، وسهل الكثير من جوانب حياتنا. ومع ذلك، كما هو الحال مع أي ثورة، يحمل هذا العالم الرقمي في طياته تحديات ومخاطر جديدة لم نعهدها من قبل. إحدى أبرز هذه التحديات تكمن في ظهور ما يُعرف بـــ "الجريمة الإلكترونية"، وهي مجموعة واسعة من الأنشطة غير القانونية التي تستغل التقنيات الرقمية وشبكة الإنترنت لتحقيق أهداف إجرامية متنوعة.

تتسم الجريمة الإلكترونية بطبيعة عابرة للحدود، فهي لا تعترف بالقيود الجغرافية، ويمكن أن يرتكبها شخص في مكان ما ويؤثر ضحاياها في أماكن أخرى بعيدة. هذا البعد الدولي يجعل مكافحتها مهمة معقدة تتطلب تضافر الجهود على مستوى عالمي. فبينما تتطور الأدوات والتقنيات التي يستخدمها المجرمون الإلكترونيون باستمرار، يصبح التعاون بين الدول وتبادل الخبرات والمعلومات أمراً حيوياً لمواجهة هذه التهديدات بفعالية وحماية المجتمعات من آثارها المدمرة.

بالنسبة للجزائر، ومع خطواتها المتسارعة نحو تبني التحول الرقمي في مختلف القطاعات، يصبح موضوع مكافحة الجريمة الإلكترونية ذا أهمية قصوى. فكلما زاد اعتمادنا على الأنظمة الرقمية، زادت المخاطر المحتملة التي قد تهدد أمننا الاقتصادي والاجتماعي وحتى الفردي. لذا، فإن فهم آليات هذه الجرائم وكيفية التصدي لها، خاصة من خلال التعاون مع الدول الأخرى، يمثل ضرورة ملحة لحماية مكتسباتنا الرقمية وضمان بيئة إلكترونية آمنة وموثوقة لمواطنينا ومؤسساتنا.

في هذا السياق، تبرز أهمية دراسة "التعاون الدولي لمكافحة الجريمة الإلكترونية" كأحد السبل الرئيسية لمواجهة هذا التحدي العالمي. إن فهم الأطر القانونية والمؤسساتية الدولية والإقليمية، وتقييم فاعليتها، واستكشاف سبل تعزيزها، يمكن أن يساهم بشكل كبير في تعزيز قدرة الجزائر على التصدي لهذه الجرائم وحماية مصالحها ومصالح مواطنيها في الفضاء الرقمي.

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف الرئيسية التي تسهم في فهم أعمق وتناول شامل لموضوع التعاون الدولي لمكافحة الجريمة الإلكترونية، وذلك من خلال:

- ✓ تحديد الإطار النظري والمفاهيمي للجريمة الإلكترونية :بما في ذلك تعريفها، استعراض أبرز أنواعها، وتحليل الآثار السلبية المترتبة عليها على الصعد الاقتصادية، الاجتماعية، والأمنية.
- ✓ تحليل مفهوم التعاون الدولي وأهميته وأشكاله :الكشف عن ماهية التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وبيان أهميته الحيوية في ظل الطبيعة العابرة للحدود لهذه الجرائم، بالإضافة إلى استعراض مختلف الأشكال التي يمكن أن يتخذها هذا التعاون.
- ✓ تقييم الأطر القانونية والمؤسساتية الدولية والإقليمية :دراسة وتحليل الاتفاقيات والآليات القانونية والمؤسساتية المعنية بمكافحة الجريمة الإلكترونية على المستويين الدولي والإقليمي، مع تحديد موقع الجزائر ودورها ضمن هذه الأطر.
- ✓ تحديد وتحليل التحديات المعيقة للتعاون الدولي :تسليط الضوء على أبرز العقبات والتحديات القانونية، التقنية، السياسية، الاقتصادية، والاجتماعية التي

تواجه جهود التعاون الدولي في مكافحة الجريمة الإلكترونية، مع إيلاء اهتمام خاص للتحديات التي تواجه الجزائر في هذا المضمار.

- ✓ اقتراح سبل لتعزيز التعاون الدولي :تقديم توصيات عملية ومقترحات بناءة لتعزيز آليات التعاون الدولي في مكافحة الجريمة الإلكترونية، مع تحديد الأدوار المحتملة للتشريعات الوطنية، المنظمات الدولية، والقطاع الخاص في تحقيق هذا الهدف.

لقد تم اختيار موضوع "التعاون الدولي لمكافحة الجريمة الإلكترونية" لهذه المذكرة لعدة أسباب جوهرية منها مايلي:

- ➢ أولاً، الأهمية المتزايدة للجريمة الإلكترونية وتأثيراتها الخطيرة على مختلف جوانب الحياة في الجزائر والعالم.
- ➢ ثانياً، الحاجة الماسة إلى فهم معمق لآليات التعاون الدولي المتاحة والفعالة في هذا المجال، خاصة في ظل التطور السريع لهذه الجرائم وتجاوزها للحدود الوطنية.
- ➢ ثالثاً، الرغبة في تسليط الضوء على التحديات التي تواجه هذا التعاون واقتراح سبل لتعزيزه وتطويره بما يخدم المصالح الوطنية ويساهم في الجهود العالمية لمكافحة هذه الظاهرة.

تنطلق هذه الدراسة من إشكالية رئيسية مفادها ما هي الجريمة الإلكترونية وما مدى مساهمة التعاون الدولي في مكافحة الجريمة الإلكترونية؟

وللإجابة على هذه الإشكالية الرئيسية، تسعى الدراسة إلى معالجة مجموعة من الأسئلة الفرعية:

- ➢ ما هو الإطار النظري والمفاهيمي للجريمة الإلكترونية؟

- ما هو مفهوم التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وما هي أهميته وأشكاله؟
- ما هي الأطر القانونية والمؤسساتية الدولية والإقليمية المتعلقة بمكافحة الجريمة الإلكترونية؟ وما هو موقع الجزائر ضمن هذه الأطر؟
- ما هي التحديات القانونية والتقنية والسياسية والاقتصادية والاجتماعية التي تواجه التعاون الدولي في مكافحة الجريمة الإلكترونية، خاصة فيما يتعلق بالجزائر؟
- ما هي السبل الكفيلة بتعزيز التعاون الدولي لمكافحة الجريمة الإلكترونية، وما هو الدور الذي يمكن أن تلعبه التشريعات الوطنية والمنظمات الدولية والقطاع الخاص في هذا التعزيز؟

لتحقيق أهداف هذه الدراسة والإجابة على تساؤلاتها، سيتم الاعتماد على المنهج الوصفي التحليلي .سيتم من خلاله وصف وتحليل الأطر القانونية والمؤسساتية المتعلقة بالتعاون الدولي في مكافحة الجريمة الإلكترونية، مع التركيز على جهود الجزائر في هذا المجال. كما سيتم تحليل التحديات التي تواجه هذا التعاون واقتراح سبل لتجاوزها. بالإضافة إلى ذلك، سيتم الاستعانة بـــ المنهج المقارن عند استعراض التجارب الدولية في مجال التعاون لمكافحة الجريمة الإلكترونية للاستفادة منها في السياق الجزائري.

لتحقيق أهداف الدراسة والإجابة على إشكاليتها وتساؤلاتها الفرعية، سيتم تقسيم هذه المذكرة إلى ثلاثة فصول رئيسية، بالإضافة إلى مقدمة وخاتمة.

- **الفصل الأول** :سيتم تخصيصه للإطار النظري للجريمة الإلكترونية، حيث سيتم تعريفها وتحديد خصائصها وأنواعها وآثارها. كما سيتم تناول مفهوم التعاون الدولي وأهميته في هذا السياق.

- **الفصل الثاني** :سيركز على الأطر القانونية والمؤسساتية للتعاون الدولي في مكافحة الجريمة الإلكترونية، مع التركيز بشكل خاص على جهود الجزائر في هذا المجال ودور المنظمات الدولية والإقليمية ذات الصلة.كما يتناول التحديات التي تواجه التعاون الدولي في مكافحة الجريمة الإلكترونية ، بالإضافة إلى استعراض سبل تعزيز هذا التعاون وتطويره.

وأخيراً، ستتضمن **الخاتمة** أهم النتائج التي توصلت إليها الدراسة والتوصيات المقترحة.

الفصل الأول

الإطار النظري للجريمة الإلكترونية

إن الجريمة الإلكترونية، بوصفها نمطًا مستحدثًا من الأنشطة الإجرامية التي تستغل التقنيات الرقمية وشبكة الإنترنت، تمثل أحد أبرز التحديات الأمنية والقانونية في عالمنا المعاصر. تتسم هذه الجرائم بطبيعتها العابرة للحدود وصعوبة تتبع مرتكبيها، مما يستلزم فهمًا معمقًا لأبعادها المختلفة.

ولهذا الغرض، سنركز على تحليل مفهوم "الجريمة الإلكترونية" وتقديم تعريف دقيق وشامل له، مع مراعاة تطوره التقني.

وعلاوة على ذلك، سنتناول الخصائص الأساسية التي تميز الجرائم الإلكترونية، مثل طبيعتها العابرة للحدود وصعوبة تتبعها، والتي تفرض تحديات جوهرية على جهود المكافحة.

كما، سنقوم بتصنيف الجرائم الإلكترونية وفقاً لمعايير علمية، مما يساعد في فهم الأنماط الإجرامية وتوجيه جهود المكافحة بفعالية.

أخيراً، سنستعرض آثار الجرائم الإلكترونية على الأفراد والدول، مما يؤكد الأهمية القصوى للتعاون الدولي في الحد من هذه التهديدات المتزايدة.هذا مسنتناوله في المبحث الاول.

بعد وضع هذا الإطار المفاهيمي، سنتحول في المبحث الثاني لاستجلاء مفهوم "التعاون الدولي" في مكافحة هذه الجرائم، وتقديم تعريف واضح له واستعراض أشكاله المتنوعة، مع التأكيد على دوره المركزي في مواجهة طبيعتها العابرة للحدود. هذا الفهم المتعمق لأهمية التعاون الدولي سيكون أساس تحليلنا للأطر القانونية والمؤسساتية في الفصول اللاحقة.

المبحث الأول: ماهية الجريمة الإلكترونية

إن موضوع الجريمة الإلكترونية، تلك الآفة التي تستغل التطور الرقمي وتفرض تحديات جمة على النظام القانوني والأمني، يمثل صلب فهم كيفية مواجهة الأنشطة غير المشروعة في الفضاء السيبراني. ففي عالم يزداد فيه الاعتماد على التقنيات الرقمية وشبكات الاتصال، يصبح التعرف على ماهية هذه "الاعتداءات الرقمية" وأبعادها المختلفة أمرًا بالغ الأهمية لتحديد آليات مكافحتها. وعليه، فإن الغاية من هذا المبحث تتجلى في تأسيس إدراك واضح المعالم لماهية الجريمة الإلكترونية وأصنافها المتنوعة، وذلك كمنطلق لا غنى عنه لفحص سبل التعاون الدولي لمواجهة هذه الظاهرة المتنامية، وهو ما سيتم تفصيله في المباحث اللاحقة.،سنتناول مفهوم الجريمة الإلكترونية (المطلب الأول)، أنواع الجرائم الإلكترونية (المطلب الثاني)

المطلب الأول: مفهوم الجريمة الإلكترونية

في خضم التطور التكنولوجي المتسارع الذي يشهده عالمنا المعاصر، وما صاحبه من تحول جذري في أنماط التفاعل والتواصل والاعتماد المتزايد على الفضاء الرقمي، برزت الجريمة الإلكترونية كأحد أبرز التحديات الأمنية والقانونية التي تواجه المجتمعات والدول على حد سواء. إن الطبيعة المستمرة التغير لهذه الجرائم، بتطور الأدوات والأساليب المستخدمة في ارتكابها، يجعل من الضروري بشكل حتمي وضع تعريف قانوني وأكاديمي دقيق وشامل لها. هذا التعريف ليس مجرد مسألة اصطلاحية، بل يكتسب أهمية قصوى في تحديد نطاق التجريم، وتوجيه جهود المكافحة، وتسهيل التعاون الدولي، وضمان تحقيق العدالة في مواجهة هذه الأفعال غير المشروعة التي تستغل التقنيات الرقمية.

الفرع الاول: تعريف الجريمة الإلكترونية من الناحية التشريعية

تتباين التشريعات الوطنية في مختلف دول العالم في تناولها لمفهوم الجريمة الإلكترونية، وذلك تبعًا لتاريخ ظهور هذه الجرائم في كل دولة، ودرجة تطور بنيتها القانونية والتقنية، والأولويات التي تضعها في مواجهة هذا النوع من الإجرام. ففي بعض الدول، نجد تعريفات عامة وشاملة تغطي طيفًا واسعًا من الأفعال التي ترتكب باستخدام الوسائل الإلكترونية، مع التركيز على النتيجة الإجرامية أو الوسيلة المستخدمة[1].

وتعرف الجريمة الإلكترونية :يمكن تعريف الجريمة الإلكترونية بأنها أي فعل غير قانوني يتم ارتكابه باستخدام تكنولوجيا المعلومات والاتصالات، أو يستهدفها، بهدف تحقيق مكاسب مادية أو إلحاق ضرر بأفراد أو مؤسسات أو دول. يتسم هذا النوع من الجرائم بطبيعته الرقمية وقدرته على تجاوز الحدود الجغرافية، تُعرف الجريمة الإلكترونية أيضًا بأنها نشاط إجرامي يتم فيه استخدام الحاسوب أو شبكة الحاسوب كأداة أو هدف لارتكاب الجريمة. يشمل ذلك مجموعة واسعة من الأنشطة غير القانونية، من الاحتيال وسرقة الهوية إلى اختراق الأنظمة ونشر البرمجيات الخبيثة.

أما المشرع الجزائري فقد عرف الجريمة الإلكترونية بشكل غير مباشر من خلال تجريم الأفعال التي تقع على الأنظمة والمعلومات الإلكترونية أو باستخدامها، وذلك في قانون العقوبات الجزائري وتعديلاته اللاحقة، خاصة في الفصل الثالث مكرر المتعلق بـــ "الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات."لا يوجد تعريف موحد ومباشر لمصطلح "الجريمة الإلكترونية" كعنوان شامل في القانون الجزائري .بدلاً من ذلك، قام

[1] هالة الأنصاري، تطور التشريعات في مواجهة الجريمة الإلكترونية، مكتبة الأفق، البحرين، 2020، ص 115.

المشرع بتحديد وتجريم أنواع محددة من الأفعال التي تندرج ضمن مفهوم الجريمة الإلكترونية[1].

يمكن استخلاص فهم المشرع الجزائري للجريمة الإلكترونية من خلال تحليل المواد القانونية التي تتناول هذه الأفعال، حيث يركز على:

- استهداف أنظمة المعالجة الآلية للمعطيات :مثل الدخول غير المصرح به، والبقاء غير المصرح به، وتعطيل أو إتلاف الأنظمة.
- استهداف المعطيات (البيانات) المخزنة أو المعالجة :مثل إتلافها، أو تغييرها، أو تزويرها، أو الحصول عليها بطرق غير مشروعة.
- استخدام الأنظمة الإلكترونية لارتكاب جرائم أخرى :مثل الاحتيال عبر الإنترنت، والتزوير الإلكتروني، والقذف والسب، والابتزاز.

اما على الصعيد الدولي والإقليمي، سعت العديد من الاتفاقيات والمعاهدات إلى وضع إطار موحد لمكافحة الجريمة الإلكترونية، بما في ذلك تقديم تعريفات مشتركة لهذا المفهوم. تُعد "اتفاقية بودابست بشأن جرائم الإنترنت" من أبرز هذه الاتفاقيات، وعلى الرغم من أنها لا تقدم تعريفًا شاملاً للجريمة الإلكترونية كمفهوم عام، إلا أنها تحدد مجموعة واسعة من الأفعال التي تعتبر جرائم إلكترونية، مثل الدخول غير القانوني، والاعتراض غير القانوني، وإتلاف البيانات، وإساءة استخدام الأجهزة[2]. كما أن هناك جهودًا إقليمية مماثلة، حيث قد تتضمن اتفاقيات إقليمية تعريفات للأفعال المجرمة إلكترونيًا، تعكس الأولويات والتحديات الخاصة بتلك المنطقة. هذه الاتفاقيات تمثل

[1] فاطمة القاسمي، تحديد الجريمة الإلكترونية في التشريعات العربية، دار الفكر، الأردن، 2019، ص88.

[2] نوال الشرفي، تحديات التعاون الدولي في مجال الجرائم الإلكترونية، مكتبة الأفق، الكويت، 2019، ص120.

محاولة لتقريب وجهات النظر وتوحيد المفاهيم القانونية لتسهيل التعاون القضائي والأمني بين الدول.

الفرع الثاني: العناصر الأساسية المشتركة في التعاريف:

بالرغم من التباين الظاهر في التعاريف التي عرفت الجريمة الإلكترونية، يمكن استخلاص مجموعة من العناصر الأساسية المشتركة التي تتكرر في معظم هذه التعاريف:

- وجود فعل أو سلوك غير قانوني :يجب أن يشكل الفعل المرتكب انتهاكًا لقانون قائم أو قاعدة قانونية مجرمة.
- استخدام وسيلة إلكترونية أو نظام معلوماتي :يرتبط ارتكاب الفعل بشكل مباشر باستخدام جهاز كمبيوتر، أو شبكة إنترنت، أو أي نظام معلوماتي آخر. هذه الوسيلة هي الأداة التي يتم من خلالها تنفيذ الفعل الإجرامي.
- القصد الجنائي (أو ما يعادله من مسؤولية): تطلب معظم التشريعات وجود نية إجرامية لدى مرتكب الفعل، أو على الأقل درجة معينة من الإهمال أو الرعونة التي تؤدي إلى وقوع الجريمة.
- تحقيق ضرر أو إمكانية إلحاق ضرر :غالبًا ما تتطلب الجريمة الإلكترونية وقوع ضرر فعلي على الضحية (فردًا أو مؤسسة أو دولة) أو وجود خطر حقيقي لحدوث هذا الضرر نتيجة للفعل المرتكب[1].

[1] عمر الفقي، مسؤولية مرتكبي الجرائم الإلكترونية: النية والضرر، دار المعرفة، مصر، 2022، ص 110.

إن فهم هذه العناصر الأساسية المشتركة يساعد في بناء تصور أكثر وضوحًا للجريمة الإلكترونية وتحديد نطاقها، مما يسهل عملية المقارنة بين التشريعات المختلفة وتعزيز التعاون الدولي في مكافحتها.

المطلب الثاني: **خصائص الجرائم الإلكترونية:**

تنفرد الجرائم الإلكترونية بمجموعة من الخصائص المميزة التي تجعلها تختلف جوهريًا عن الجرائم التقليدية، وتُلقي بتحديات فريدة على الأنظمة القانونية وجهود المكافحة. لذلك فان فهم هذه السمات ليس مجرد تمرين أكاديمي، بل هو ضرورة عملية لتطوير استراتيجيات فعالة لمواجهة هذا النوع المتنامي من الإجرام، وتعزيز التعاون الدولي الذي يستجيب لطبيعته العابرة للحدود. وسنتناول فيما يلي ابرز هذه الخصائص:

- الطبيعة العابرة للحدود: تُعد هذه الخاصية من أبرز ما يميز الجرائم الإلكترونية، حيث يمكن ارتكابها من أي مكان في العالم وتوجيهها نحو ضحايا أو أنظمة تقع في دول أخرى. هذا البعد الدولي يجعل تطبيق القانون الوطني أمرًا صعبًا ويتطلب تعاونًا دوليًا[1] فعالًا في مجالات التحقيق وجمع الأدلة وتسليم المجرمين.
- صعوبة تحديد مكان ارتكاب الجريمة: في الجرائم التقليدية، يكون تحديد مكان وقوع الجريمة غالبًا واضحًا. أما في الجرائم الإلكترونية، فقد تتداخل مواقع ارتكاب الفعل، وتواجد الخادم، ومكان وجود الضحية، مما يجعل تحديد الولاية القضائية المختصة أمرًا معقدًا ويتطلب اتفاقيات دولية لتنظيم هذه المسألة.

[1] عز الدين القاسمي، تحديات التعاون الدولي في مواجهة الجرائم العابرة للحدود، دار المعرفة، مصر، 2022، ص 108.

- صعوبة تحديد هوية مرتكب الجريمة: يتيح الفضاء الإلكتروني للمجرمين إمكانية إخفاء هوياتهم الحقيقية أو استخدام هويات مستعارة) أسماء مستخدمين وهمية، عناوين IP متغيرة، إلخ .(هذه الخاصية تعيق جهود التعرف على الجناة وتتبعهم وتقديمهم للعدالة، وتستدعي تطوير تقنيات وأساليب تحقيق متقدمة.

- سرعة التنفيذ والانتشار الواسع: يمكن ارتكاب الجرائم الإلكترونية وتنفيذها بسرعة فائقة، كما يمكن للمواد غير القانونية (مثل البرامج الضارة أو المحتوى الإباحي للأطفال) أن تنتشر على نطاق واسع في لحظات عبر شبكة الإنترنت، مما يزيد من حجم الضرر وصعوبة احتوائه[1].

- الطبيعة غير المادية للأدلة: تعتمد الجرائم الإلكترونية بشكل كبير على الأدلة الرقمية، التي تتسم بطبيعتها غير المادية وقابليتها للتغيير أو الحذف بسهولة. يتطلب جمع هذه الأدلة والحفاظ عليها إجراءات تقنية وقانونية خاصة لضمان حجيتها في الإجراءات القضائية.

- التطور التقني المستم: يشهد عالم التقنية تطورًا مستمرًا، مما يؤدي إلى ظهور أساليب جديدة لارتكاب الجرائم الإلكترونية. هذا يستلزم متابعة دقيقة لهذه التطورات وتحديث القوانين وتطوير مهارات المحققين بشكل مستمر لمواكبة هذه التحديات.

- قلة الوعي لدى الضحايا: غالبًا ما يكون ضحايا الجرائم الإلكترونية غير مدركين لطرق الاحتيال وأساليب المجرمين، مما يجعلهم أكثر عرضة للوقوع

[1] الزهراني منى، تحديات احتواء الجرائم الإلكترونية، دار الكتاب العربي، بيروت، 2023، ص 335.

ضحايا لهذه الجرائم. يتطلب ذلك جهودًا توعوية مكثفة لرفع مستوى الوعي لدى الجمهور[1].

إن فهم هذه الخصائص المتداخلة والمعقدة للجرائم الإلكترونية يؤكد على الحاجة الماسة إلى تعزيز التعاون الدولي وتبادل الخبرات والمعلومات بين الدول لمواجهة هذه التهديدات بفعالية.

المطلب الثالث: أنواع الجرائم الإلكترونية

يشهد الفضاء الرقمي تنوعًا هائلاً في الأنشطة الإجرامية التي تُرتكب عبر وسائله، مما يستدعي تصنيف هذه الجرائم إلى أنواع محددة لتسهيل فهم طبيعة كل منها، وتطوير استراتيجيات مكافحة فعالة، وتعزيز التعاون الدولي بناءً على طبيعة التهديدات المشتركة. في هذا المطلب إلى سنستعراض أبرز التصنيفات لأنواع الجرائم الإلكترونية، مع الأخذ في الاعتبار المعايير المختلفة التي يعتمد عليها هذا التقسيم، سواء كانت تستند إلى الهدف من الجريمة، أو الوسيلة المستخدمة في ارتكابها، أو طبيعة الضحية المتأثرة بها.

الفرع الاول: الجرائم الموجهة ضد الأنظمة والبيانات

يمثل هذا الصنف من الجرائم الإلكترونية تهديدًا وجوديًا للبنية التحتية الرقمية التي يعتمد عليها عالمنا الحديث بشكل متزايد. ولعل الهدف الأساسي للمجرم في هذه الحالة ليس تحقيق مكاسب مالية مباشرة في الغالب، بل إحداث خلل أو ضرر أو السيطرة على الأنظمة والبيانات الحيوية. يمكن أن تتراوح دوافع هذه الجرائم بين التخريب

[1] الخالدي فاطمة، "تحليل دور وسائل الإعلام في رفع مستوى الوعي بمخاطر الجرائم الإلكترونية في دولة الإمارات العربية المتحدة: دراسة إحصائية"، جامعة الإمارات العربية المتحدة، 2022، ص120-135.

السياسي أو الاقتصادي، وإظهار القدرات التقنية، أو حتى مجرد الرغبة في إحداث الفوضى.

يعد الدخول غير المصرح به إلى الأنظمة (Hacking) أحد أبرز تجليات هذا النوع من الإجرام، حيث يسعى المخترقون إلى استغلال الثغرات الأمنية للوصول إلى مناطق محظورة داخل الأنظمة، مما يتيح لهم سرقة المعلومات أو زرع برامج ضارة أو التحكم في وظائف النظام. وبالمثل، فإن الاعتراض غير القانوني للبيانات، سواء أثناء نقلها عبر الشبكات أو تخزينها على الخوادم، يعرض المعلومات الحساسة للأفراد والمؤسسات لخطر الكشف والاستغلال[1].

أما الأفعال التخريبية مثل إتلاف أو تغيير أو حذف البيانات، فهي يمكن أن تتسبب في خسائر فادحة، خاصة إذا استهدفت بيانات مالية أو طبية أو حكومية هامة.

وتعطيل عمل الأنظمة أو الخدمات الإلكترونية من خلال هجمات حجب الخدمة (DDoS)يمثل سلاحًا قويًا يمكن استخدامه لابتزاز المؤسسات أو شل قدرتها على العمل. وأخيرًا، فإن نشر البرامج الضارة، كالفيروسات التي تنتشر ذاتيًا وتلحق الضرر بالملفات، والفيروسات الاخري التي تستغل الثغرات الأمنية للتكاثر والانتشار، وبرامج التجسس التي تتخفى لسرقة المعلومات الشخصية، كلها أدوات خطيرة تقع ضمن هذا التصنيف وتهدد سلامة الفضاء الرقمي[2].

[1] محل "الجرائم الرقمية"، دليل الحماية من الاختراقات الإلكترونية، 2022، https://www.digitalcrimesguide.com، تم الاطلاع عليه في 28 أبريل 2025، الساعة 14:30 بتوقيت الجزائر.

[2] الغامدي أحمد، الجرائم الإلكترونية: دراسة مقارنة، دار الكتاب الحديث، القاهرة، 2020، ص115.

الفرع الثاني: الجرائم التي تستخدم الأنظمة والبيانات كأداة

في هذا النوع من الجرائم ، يتحول العالم الرقمي من كونه هدفًا للهجوم إلى ساحة لارتكاب جرائم أخرى، حيث تُستغل الأنظمة والبيانات كأدوات لتسهيل الوصول إلى الضحايا أو تحقيق أهداف إجرامية تقليدية في سياق جديد. الدافع الأساسي هنا غالبًا ما يكون تحقيق مكاسب مالية أو إلحاق ضرر مباشر بالأفراد أو المؤسسات من خلال استغلال الثقة في المعاملات الرقمية وسهولة التواصل عبر الإنترنت.

الاحتيال عبر الإنترنت يتخذ أشكالًا متنوعة، بدءًا من التصيد الاحتيالي (Phishing) الذي يعتمد على خداع المستخدمين للكشف عن معلوماتهم السرية عبر رسائل بريد إلكتروني أو مواقع ويب مزيفة، وصولًا إلى عمليات الاحتيال المعقدة في التجارة الإلكترونية التي تستغل نقاط الضعف في أنظمة الدفع والتسليم. وسرقة الهوية عبر الإنترنت، والتي يتم فيها الحصول على معلومات شخصية حساسة واستخدامها في انتحال صفة الضحية لارتكاب جرائم مالية أو الحصول على خدمات بطرق غير مشروعة، تمثل تهديدًا خطيرًا للخصوصية والأمن الشخصي[1].

كما يُستخدم الإنترنت كمنصة لنشر المحتوى غير القانوني على نطاق واسع، بما في ذلك المواد الإباحية غير القانونية التي تستغل الأطفال، والخطابات التي تحرض على الكراهية والعنف وتؤدي إلى زعزعة الاستقرار الاجتماعي. وتتضمن الجرائم المالية الإلكترونية عمليات سرقة أرقام البطاقات الائتمانية واستخدامها في عمليات شراء غير مصرح بها، بالإضافة إلى غسيل الأموال المتحصلة من أنشطة إجرامية أخرى من خلال تحويلها عبر الأنظمة المالية الرقمية. وأخيرًا، يشمل هذا الفرع الاعتداء على الأشخاص عبر الإنترنت، والذي يتضمن أفعالًا مثل التهديد والابتزاز والمضايقة

[1] علي حسن، الاحتيال عبر الإنترنت: دراسة تحليلية في دول الشرق الأوسط، رسالة ماجستير، جامعة التكنولوجيا، 2023، الأردن، 2023، ص 150.

الإلكترونية والتنمر عبر الإنترنت، والتي تستخدم وسائل الاتصال الرقمية لإلحاق الأذى النفسي والعاطفي بالضحايا وتشويه سمعتهم[1].

المطلب الرابع: آثار الجرائم الإلكترونية على الأفراد والدول

يمثل فهم الآثار المدمرة والمتعددة الأوجه للجرائم الإلكترونية خطوة حاسمة في إدراك حجم التحدي الذي نواجهه وضرورة تضافر الجهود على المستويات كافة لمواجهته. إن هذه الجرائم لا تقتصر على إلحاق الضرر المادي فحسب، بل تمتد لتشمل الجوانب النفسية والاجتماعية والاقتصادية والأمنية للأفراد والدول على حد سواء. في هذا المطلب، سنقوم بتسليط الضوء على هذه الآثار، حيث تم تحصيص الفرع الاول الى الاثار غلى الافراد ، بينما الفرغ الثاني سنتطرق فيه الى الاثار على الدول:

الفرع الاول: الآثار على الأفراد

تترك الجرائم الإلكترونية بصمات عميقة على حياة الأفراد، تتجاوز مجرد الخسائر المالية المباشرة. إن الشعور بالانتهاك وعدم الأمان، وفقدان الثقة في البيئة الرقمية، والضغوط النفسية الناتجة عن التعرض لهذه الجرائم، كلها جوانب تستدعي اهتمامًا خاصًا. وعلي هذا الاساس يمكن ان مختلف جوانب حياتهم[2]التي تتاثر بها وهي كما يلي:

- الآثار المالية والاقتصادية :يمكن أن يتعرض الأفراد لخسائر مالية كبيرة نتيجة لجرائم مثل الاحتيال عبر الإنترنت، وسرقة الهوية واستخدامها في معاملات

[1] الهاشمي علي، *التنمر الإلكتروني: الأسباب والآثار والعلاج*، مركز الكتاب الأكاديمي، عمان، 2020، ص165.

[2] الجرائم الرقمية"، دليل الحماية من الاختراقات الإلكترونية، 2022، [https://www.digitalcrimesguide.com]، [تم الاطلاع عليه في 28 أبريل 2025، الساعة 14:30 بتوقيت الجزائر

غير مصرح بها، وسرقة أرقام بطاقات الائتمان، والابتزاز المالي عبر الإنترنت. هذه الخسائر قد تؤدي إلى ضائقة مالية كبيرةعلى الضحايا وتؤثر على مستوى معيشتهم.

- الآثار النفسية والعاطفية :يمكن أن تسبب الجرائم الإلكترونية ضررًا نفسيًا وعاطفيًا كبيرًا للضحايا. يشمل ذلك الشعور بالخوف والقلق وعدم الأمان نتيجة لجرائم مثل التهديد والابتزاز والمضايقة الإلكترونية والتنمر عبر الإنترنت وسرقة البيانات الشخصية وانتهاك الخصوصية. قد يعاني الضحايا من الاكتئاب والقلق واضطرابات النوم وصعوبة الثقة بالآخرين.
- انتهاك الخصوصية وسرقة البيانات :تعتبر سرقة البيانات الشخصية وانتهاك الخصوصية من أكثر الآثار شيوعًا للجرائم الإلكترونية. يمكن أن تشمل هذه البيانات معلومات التعريف الشخصية ، والصور ومقاطع الفيديو الخاصة، والاتصالات الشخصية، والسجلات الطبية والمالية. يمكن استخدام هذه البيانات في ارتكاب جرائم أخرى أو بيعها في السوق السوداء، مما يعرض الأفراد لمخاطر مستمرة[1].
- تأثيرات على السمعة والثقة :قد يتعرض الأفراد الذين يتم اختراق حساباتهم أو نشر معلومات كاذبة عنهم عبر الإنترنت إلى ضرر في سمعتهم وعلاقاتهم الاجتماعية والمهنية. كما أن انتشار الجرائم الإلكترونية بشكل عام قد يؤدي إلى تآكل الثقة في البيئة الرقمية والمعاملات الإلكترونية.

[1] محمود سامي، الجرائم الإلكترونية: المخاطر والحلول، دار الفكر العربي، مصر،2022، ص210.

الفرع الثاني: الآثار على الدول

إن تأثير الجرائم الإلكترونية لا يقتصر على الأفراد فحسب، بل يمتد ليشمل الدول ومؤسساتها وبنيتها التحتية الحيوية. تهدد هذه الجرائم الأمن القومي والاقتصاد والاستقرار الاجتماعي، وتفرض تحديات كبيرة على سلطات إنفاذ القانون والقضاء.وعليه سنستعرض كيف يمكن أن تؤثر الجرائم الإلكترونية على الدول ومصالحها الاستراتيجية.

- تهديد الأمن القومي :يمكن أن تستهدف الجرائم الإلكترونية البنية التحتية الحيوية للدول، مثل شبكات الطاقة والمياه والنقل والاتصالات، مما يشكل تهديدًا مباشرًا للأمن القومي. كما يمكن استخدام الفضاء الإلكتروني في أنشطة التجسس الإلكتروني والحرب السيبرانية.
- الآثار الاقتصادية :يمكن أن تلحق الجرائم الإلكترونية خسائر اقتصادية فادحة بالدول من خلال استهداف المؤسسات المالية والشركات والبنية التحتية الاقتصادية. يشمل ذلك سرقة الملكية الفكرية، وتعطيل الأعمال التجارية، والاحتيال على نطاق واسع، وفضلا عن تكاليف الاستجابة للحوادث الأمنية[1].
- تأثيرات على الاستقرار الاجتماعي والسياسي :يمكن استخدام الفضاء الإلكتروني لنشر المعلومات الكاذبة والأخبار المضللة والحملات الدعائية التي تهدف إلى التأثير على الرأي العام وزعزعة الاستقرار السياسي والاجتماعي. كما يمكن أن تستخدم التنظيمات الإرهابية الإنترنت للتخطيط وتنفيذ الهجمات.
- تحديات إنفاذ القانون والقضاء :تواجه الدول تحديات كبيرة في التحقيق في الجرائم الإلكترونية وملاحقة مرتكبيها بسبب طبيعتها العابرة للحدود وصعوبة

[1] المسعودي، هالة، *الجرائم الإلكترونية وتأثيرها على الاقتصاد العالمي*، دار العلوم، الرياض، 2022، ص 145.

تتبع الأدلة وتحديد الولاية القضائية.وهذا ما يتطلب تطوير قوانين جديدة وتعزيز التعاون الدولي في مجال إنفاذ القانون والقضاء[1].

- تكاليف مكافحة الجريمة الإلكترونية :تتحمل الدول تكاليف باهظة في سبيل تطوير القدرات الأمنية، والتقنية لمكافحة الجريمة الإلكترونية، وتدريب الكوادر المتخصصة، وتوعية الجمهور، والتعاون مع الدول الأخرى.

المبحث الثاني: مفهوم التعاون الدولي وأهميته في مكافحة الجريمة الإلكترونية

بعد أن استعرضنا في المبحث الأول الإطار النظري للجريمة الإلكترونية من حيث تعريفها وخصائصها وأنواعها وآثارها المدمرة على الأفراد والدول، ننتقل في هذا المبحث إلى مفهوم "التعاون الدولي". في عالم تتجاوز فيه الجريمة الإلكترونية الحدود الوطنية بسهولة ويسر، يصبح التعاون بين الدول ضرورة حتمية لمواجهة هذه التحديات بفعالية. سنسعى في هذا المبحث إلى استجلاء مفهوم التعاون الدولي في هذا السياق، وتحديد أشكاله المختلفة في المطلب الاول، والأهم من ذلك، تبيان الأسباب التي تجعل هذا التعاون عنصراً لا غنى عنه في التصدي لهذه الجرائم المعقدة والعابرة للقارات في المطلب الثاني. إن فهمنا العميق لأبعاد هذا التعاون وأهميته سيشكل الأساس الذي سننطلق منه في الفصول اللاحقة لتحليل الأطر القانونية والمؤسساتية التي تنظمه وتسعى إلى تفعيله.

[1] النجار فاطمة، *الجرائم الإلكترونية: المخاطر والتحديات*، دار الكتاب الجامعي، عمان، 2020، ص275

المطلب الأول: تعريف التعاون الدولي وأشكاله

إن تحديد مفهوم واضح للتعاون الدولي الخطوة الأولى والضرورية لفهم دوره وأهميته في سياق مكافحة الجريمة الإلكترونية. إن هذا المفهوم، الذي يتضمن تفاعلات وتنسيقات بين الدول، يتخذ أشكالًا متعددة تختلف باختلاف الأطراف المشاركة والأهداف المنشودة والآليات المتبعة. سنقوم بتفكيك هذا المفهوم من خلال استعراض تعاريفه الأساسية في الفرع الأول، ثم تحليل أشكاله المتنوعة التي تتجلى في الواقع العملي لمواجهة التحديات الأمنية والقانونية المشتركة في الفضاء الرقمي في الفرع الثاني.

الفرع الأول: تعريف التعاون الدولي في سياق مكافحة الجريمة الإلكترونية

يشهد مفهوم التعاون الدولي في سياق مكافحة الجريمة الإلكترونية تنوعًا في التعريفات، يعكس اختلاف وجهات نظر الدول والمنظمات حول نطاقه وآلياته. فبينما يركز البعض على تبادل المعلومات وتسليم المجرمين، يشدد آخرون على بناء القدرات المشتركة وتوحيد التشريعات لمواجهة الطبيعة العابرة للحدود لهذه الجرائم بفعالية.

أولا: التعريف القانوني الضيق :هذا التعريف يركز على الجانب الرسمي والقانوني البحت للتعاون. يعتبر التعاون الدولي بمثابة مجموعة من الإجراءات التي تتخذها الدول وفقًا لأطر قانونية ملزمة، مثل المعاهدات والاتفاقيات الثنائية أو متعددة الأطراف. على سبيل المثال، اتفاقية المساعدة القانونية المتبادلة تحدد آليات واضحة لطلب وتقديم المساعدة في جمع الأدلة أو استجواب الشهود عبر الحدود. اتفاقيات تسليم المجرمين تحدد الشروط والإجراءات القانونية لنقل شخص متهم أو مدان بجريمة إلكترونية من

دولة إلى أخرى لمحاكمته أو تنفيذ العقوبة. هذا التعريف يؤكد على أهمية الأساس القانوني المنظم للعلاقات بين الدول في هذا المجال[1].

ثانيا: التعريف الأوسع :يتجاوز هذا التعريف الإطار القانوني الرسمي ليشمل أشكالًا أخرى من التفاعل والتنسيق غير الملزمة قانونًا بشكل مباشر، ولكنه ضروري لتحقيق فعالية أكبر في مكافحة الجريمة الإلكترونية. يشمل ذلك تبادل "المعلومات الاستخباراتية" التي قد لا ترقى إلى مستوى الأدلة القانونية ولكنها حيوية لفهم التهديدات وتحديد الأنماط الإجرامية.

كما يشمل تنظيم "حملات توعية مشتركة" يعكس إدراكًا لأهمية الوقاية وتغيير سلوك المستخدمين على المستوى الدولي.واضافة الى "تطوير القدرات التقنية والقانونية" بشكل مشترك يهدف إلى رفع مستوى جاهزية الدول لمواجهة هذه الجرائم. "تبادل الخبرات وأفضل الممارسات" يسمح للدول بالتعلم من تجارب بعضها البعض وتطبيق الحلول الأكثر نجاحًا. هذا التعريف يشدد على أهمية المرونة والشمولية في التعاون.

ثالثا: التعريف العملي :يركز هذا التعريف على ما يتم تنفيذه فعليًا على أرض الواقع من خلال العمل المشترك بين الدول. "العمليات المشتركة بين أجهزة إنفاذ القانون" تمثل مثالًا حيًا على التعاون العملياتي، حيث تتشارك فرق من دول مختلفة في التحقيقات أو في تنفيذ مداهمات متزامنة ضد شبكات إجرامية عابرة للحدود. "المشاركة في المنتديات والمؤتمرات الدولية" توفر منصات لتبادل الآراء وبناء شبكات من العلاقات بين الخبراء والمختصين. "التعاون مع المنظمات الدولية المتخصصة" يبرز الدور الحيوي لهذه

[1] وسام الدين محمد العكلة، التعاون الدولي في مواجهة جرائم الإنترنت، جامعة بغداد، العراق،2012، ص13

المنظمات في تسهيل وتنسيق الجهود الدولية. هذا التعريف يؤكد على أهمية النتائج الملموسة للتعاون.[1]

يشكل التعاون الدولي لمكافحة الجريمة الإلكترونية منظومة معقدة تتأثر بعدة عوامل متداخلة. فمن جهة، تبرز الحاجة الملحة لمواجهة الطبيعة العابرة للحدود لهذه الجرائم وتطورها المستمر كقوة دافعة للتعاون. ومن جهة أخرى، تفرض الاختلافات القانونية والثقافية والسياسية بين الدول تحديات كبيرة أمام تحقيق تعاون فعال ومستدام.

- الاختلافات في الأنظمة القانونية :تباين القوانين الوطنية المتعلقة بتجريم الأفعال الإلكترونية وإجراءات التحقيق والملاحقة القضائية يمكن أن يعيق التعاون[2].
- محدودية الموارد والقدرات :قد تفتقر بعض الدول إلى الموارد التقنية والبشرية اللازمة للمشاركة بفعالية في جهود التعاون الدولي.
- الاعتبارات السياسية والأمنية :قد تؤثر الخلافات السياسية أو المخاوف الأمنية على استعداد الدول للتعاون في بعض الحالات.
- غياب الثقة المتبادلة :عدم وجود مستوى كافٍ من الثقة بين الأجهزة الأمنية والقضائية في الدول المختلفة يمكن أن يعيق تبادل المعلومات الحساسة والتعاون العملياتي.
- التحديات التقنية :الطبيعة المعقدة والمتغيرة باستمرار للتقنيات المستخدمة في ارتكاب الجرائم الإلكترونية تتطلب مستوى عالٍ من الخبرة التقنية المشتركة.

[1] االزيات، محمود، *التعاون القضائي الدولي في المسائل الجنائية*، دار النهضة العربية، القاهرة، 2023، ص 185.

[2] محمود سامي، الجرائم الإلكترونية والأنظمة القانونية: تحليل عميق، دار الفكر العربي، مصر،2022، ص 240.

يقوم التعاون الدولي الفعال في مكافحة الجريمة الإلكترونية على عدة عناصر أساسية ومتكاملة منها مايلي:

- الإرادة المشتركة للدول: هذا العنصر هو الأساس الذي يقوم عليه أي تعاون دولي. يجب أن يكون هناك اعتراف مشترك من قبل الدول بوجود تهديد مشترك يستدعي العمل الجماعي
- التنسيق في السياسات والاستراتيجيات: لا يكفي وجود إرادة للتعاون، بل يجب ترجمتها إلى سياسات واستراتيجيات متوافقة تهدف إلى تحقيق أهداف مشتركة في مكافحة الجريمة الإلكترونية[1] .
- تبادل المعلومات والخبرات: يعتبر تبادل المعلومات الحيوية حول التهديدات والاتجاهات الإجرامية والتقنيات المستخدمة أمرًا بالغ الأهمية لاتخاذ قرارات مستنيرة وتطوير استراتيجيات فعالة.
- المساعدة القانونية المتبادلة: هذه الآلية القانونية الرسمية ضرورية لتجاوز القيود الوطنية في التحقيقات العابرة للحدود وضمان إمكانية الحصول على الأدلة وتقديم المساعدة القضائية.
- تسليم المجرمين: يمثل آلية حاسمة لضمان عدم إفلات مرتكبي الجرائم الإلكترونية من العقاب بسبب قدرتهم على الاختباء في دول أخرى.
- التعاون العملياتي: العمل المشترك على الأرض من خلال فرق تحقيق مشتركة أو عمليات متزامنة يمكن أن يكون فعالًا بشكل خاص في تفكيك الشبكات الإجرامية العابرة للحدود.

[1] أحمد، طالب، استراتيجيات فعالة لمكافحة الجرائم الإلكترونية: التحديات والفرص، أطروحة دكتوراه، جامعة القاهرة، 2023، مصر، ص. 120.

- بناء القدرات: مساعدة الدول التي تفتقر إلى الموارد والخبرات يضمن مشاركة أوسع وأكثر فعالية في الجهود الدولية لمكافحة الجريمة الإلكترونية.
- التعاون مع المنظمات الدولية والإقليمية :هذه المنظمات تلعب دورًا محوريًا في تسهيل الحوار والتنسيق وتبادل المعلومات وتطوير المعايير الدولية.
- التعاون مع القطاع الخاص :نظرًا لدور الشركات التقنية ومقدمي الخدمات في البنية التحتية للإنترنت، فإن تعاونهم ضروري لتحديد التهديدات ومنع وقوع الجرائم وتقديم الأدلة.

الفرع الثاني: أشكال التعاون الدولي في مكافحة الجريمة الإلكترونية

نظرًا للطبيعة العابرة للحدود التي تتسم بها الجريمة الإلكترونية، فإن التعاون الدولي يمثل حجر الزاوية في جهود مكافحتها بفعالية. لا يقتصر هذا التعاون على شكل واحد، بل يتخذ صورًا متنوعة تتناسب مع طبيعة التهديدات والأطراف المعنية والأهداف المنشودة، وهي الصور التي سنتطرق اليها فيما يلي:

- التعاون الثنائي:يمثل هذا الشكل من التعاون تفاعلاً مباشرًا وتنسيقًا بين دولتين محددتين. غالبًا ما يتم هذا التعاون بموجب اتفاقيات ثنائية أو مذكرات تفاهم تحدد مجالات التعاون وآلياته في مكافحة الجريمة الإلكترونية[1].
- التعاون متعدد الأطراف عبر المنظمات الدولية :يتم هذا التعاون تحت مظلة منظمات دولية ذات اختصاص عالمي، مثل الأمم المتحدة والإنتربول. توفر هذه المنظمات إطارًا للتعاون بين عدد كبير من الدول وتعمل على وضع المعايير والقواعد الدولية وتسهيل تبادل المعلومات وتقديم الدعم التقني.

[1] العلوي محمد، *الاتفاقيات الثنائية في مجال حقوق الإنسان*، دار النهضة العربية، بيروت، 2021، ص 255.

- التعاون متعدد الأطراف عبر المنظمات الإقليمية : يشمل هذا النوع من التعاون التنسيق والعمل المشترك بين دول تنتمي إلى منطقة جغرافية واحدة، وذلك عبر منظمات إقليمية مثل مجلس أوروبا والاتحاد الأوروبي وجامعة الدول العربية والاتحاد الأفريقي. غالبًا ما تعكس هذه المنظمات الأولويات والتحديات الأمنية والقانونية المشتركة لدول المنطقة[1].

- التعاون غير الرسمي وشبكات الخبراء: يتضمن هذا النوع من التعاون تبادل المعلومات والخبرات والمعرفة بين الخبراء والمتخصصين في مجال مكافحة الجريمة الإلكترونية من مختلف الدول، غالبًا ما يتم ذلك بشكل غير رسمي عبر المؤتمرات وورش العمل والمنتديات المتخصصة والشبكات المهنية.[2]

- التعاون بين القطاعين العام والخاص: يشمل هذا النوع من التعاون الشراكة والتنسيق بين الحكومات وأجهزة إنفاذ القانون من جهة، والشركات التقنية ومقدمي خدمات الإنترنت والقطاع الخاص بشكل عام من جهة أخرى. نظرًا للدور الحيوي الذي يلعبه القطاع الخاص في البنية التحتية للإنترنت وتوفير الخدمات الرقمية، فإن تعاونه ضروري لتحديد التهديدات ومنع وقوع الجرائم وتقديم الأدلة والمساعدة في التحقيقات.

المطلب الثاني: أهمية التعاون الدولي في التصدي للجرائم الإلكترونية

لقد بات من الواضح، في ظل الانتشار الواسع للتقنيات الرقمية وتنامي التهديدات الإلكترونية، أن الجريمة الإلكترونية لم تعد شأنًا داخليًا يقتصر على حدود دولة بعينها.

[1] سعيد عماد، التعاون الإقليمي في مواجهة الجرائم الإلكترونية: دراسة تحليلية، أطروحة دكتوراه، جامعة الأردن، 2022، ص150.

[2] الرشيدي فهد، "دور شبكات الخبراء في تبادل المعلومات حول التهديدات السيبرانية"، *مجلة تقنية المعلومات*، العدد 21، 2022، ص 123.

فطبيعتها العابرة للحدود، وقدرة مرتكبيها على العمل من أي مكان في العالم، والسرعة الهائلة لانتشار الأنشطة الإجرامية في الفضاء الرقمي، كلها عوامل تستدعي استجابة عالمية موحدة ومنسقة. في هذا المطلب، سنقوم بإبراز الجوانب الأساسية التي تؤكد على الأهمية القصوى لتضافر الجهود الدولية في سبيل تحقيق أمن رقمي أكثر شمولية وفاعلية للجميع.

- تجاوز الطبيعة العابرة للحدود للجرائم الإلكترونية :إن قدرة المجرمين على العمل من أي مكان واستهداف ضحايا وأنظمة في دول أخرى تجعل من الصعب على أي دولة بمفردها تتبعهم وملاحقتهم قضائيًا. التعاون الدولي يسمح بتجاوز هذه القيود الجغرافية من خلال تبادل المعلومات وتقديم المساعدة القانونية المتبادلة وتسليم المجرمين[1].
- مواجهة التطور التقني السريع :يشهد عالم التقنية تطورًا مستمرًا، مما يخلق فرصًا جديدة للمجرمين الإلكترونيين. تضافر الجهود الدولية يتيح تبادل الخبرات والمعرفة حول أحدث التهديدات والتقنيات المستخدمة في ارتكاب الجرائم، وتطوير استراتيجيات مكافحة مبتكرة ومواكبة لهذا التطور.
- تنسيق القوانين والإجراءات :يؤدي تباين القوانين والإجراءات القانونية بين الدول إلى خلق ثغرات يمكن أن يستغلها المجرمون. التعاون الدولي يسعى إلى تقريب وجهات النظر وتوحيد المعايير القانونية وتسهيل التعاون القضائي والأمني بين الدول.

[1] عمر سامي، الجرائم الإلكترونية: التحديات العابرة للحدود وسبل المواجهة، دار المعرفة، مصر،2022، ص130.

- بناء القدرات وتبادل الخبرات: لا تمتلك جميع الدول نفس المستوى من القدرات التقنية والقانونية لمكافحة الجريمة الإلكترونية. الدول المتقدمة يمكن أن تقدم المساعدة التقنية والتدريب للدول النامية لمساعدتها في تطوير قوانينها وإنشاء وحدات متخصصة في مكافحة الجرائم الإلكترونية وتدريب الكوادر الأمنية والقضائية. هذا التبادل للمعرفة والخبرات يضمن مشاركة أوسع وأكثر فعالية من جميع الدول في الجهود العالمية لمكافحة هذا النوع من الإجرام[1].
- مواجهة التهديدات العالمية المشتركة :هناك أنواع من الجرائم الإلكترونية تشكل تهديدًا عالميًا، مثل الإرهاب الإلكتروني والجريمة المنظمة عبر الإنترنت والهجمات على البنية التحتية الحيوية. تتطلب هذه التهديدات استجابة دولية موحدة ومنسقة لحماية الأمن والسلم الدوليين.
- تعزيز الثقة في الفضاء الرقمي :إن وجود نظام دولي فعال لمكافحة الجريمة الإلكترونية يساهم في تعزيز ثقة الأفراد والمؤسسات في استخدام الإنترنت وإجراء المعاملات الإلكترونية بأمان، مما يدعم النمو الاقتصادي والاجتماعي الرقمي.
- تحقيق العدالة :التعاون الدولي يضمن عدم إفلات مرتكبي الجرائم الإلكترونية من العقاب بسبب قدرتهم على الاختباء في دول أخرى. إنه يسهل عملية القبض عليهم ومحاكمتهم وفقًا للقانون.

[1] منى، فريد، تطوير القوانين لمكافحة الجرائم الإلكترونية: دور الدول المتقدمة، مركز الدراسات الأمنية، 2022، ص 200.

الفصل الثانـي

الأطر القانونية والمؤسساتية للتعاون الدولـي في مكافحة الجريمة الإلكترونية

بعد أن تناولنا في الفصل الأول الإطار النظري لفهم طبيعة الجريمة الإلكترونية وأهمية التعاون الدولي في مواجهتها، ننتقل في هذا الفصل إلى استكشاف الجوانب العملية لهذا التعاون. يهدف هذا الفصل إلى تحليل الأطر القانونية والمؤسساتية التي تم وضعها على المستويين الدولي والإقليمي لتنظيم وتسهيل التعاون بين الدول في مكافحة هذه الجرائم العابرة للحدود.

إن وجود هذه الأطر يمثل اعترافًا دوليًا بأن مكافحة الجريمة الإلكترونية تتطلب جهودًا مشتركة تتجاوز القدرات الوطنية الفردية.

سنقوم في المبحث الأول بتسليط الضوء على أبرز الاتفاقيات والمعاهدات الدولية والإقليمية التي تمثل الأساس القانوني لهذا التعاون، وتحديد نطاقها وأهميتها في توحيد الجهود وتوفير آليات قانونية واضحة للتعاون في مجالات مثل تبادل المعلومات وتقديم المساعدة القانونية وتسليم المجرمين.

أما في المبحث الثاني، فسوف نتناول الدور الحيوي الذي تلعبه المنظمات والمؤسسات الدولية في تعزيز هذا التعاون، من خلال وضع المعايير والقواعد الإرشادية، وتقديم الدعم التقني وبناء القدرات للدول الأعضاء، وتسهيل تبادل المعلومات الاستخباراتية وأفضل الممارسات، وتنسيق الجهود بين الدول الأعضاء لتنفيذ استراتيجيات عالمية وإقليمية فعالة لمكافحة الجريمة الإلكترونية. اما في المبحث الثالث، فسوف نتناول تحديات وافاق التعاون الدولي في مكافحة الجريمة الإلكترونية

المبحث الأول: الاتفاقيات الدولية والاقليمية لمكافحة الجريمة الالكترونية

في سعي المجتمع الدولي لمواجهة التحدي المتنامي للجريمة الإلكترونية، برزت الاتفاقيات والمعاهدات الدولية والإقليمية كأدوات أساسية لتنظيم وتفعيل التعاون بين الدول. هذه الوثائق القانونية تمثل إرادة مشتركة لتحديد إطار قانوني موحد أو متقارب يسمح بتجاوز الحدود الوطنية في التحقيقات والملاحقات القضائية. في هذا المبحث، سنتناول أبرز هذه الاتفاقيات، بدءًا بالاتفاقية الرائدة في هذا المجال وهي اتفاقية بودابست لعام 2001، والتي تعتبر مرجعًا هامًا للعديد من الدول في سن تشريعاتها وتعزيز تعاونها الدولي. ثم سنتطرق إلى الاتفاقيات والقرارات الصادرة عن هيئة الأمم المتحدة والاتحاد الأوروبي وغيرها من المنظمات التي تساهم بشكل فعال في رسم ملامح التعاون الدولي في هذا المجال. وأخيرًا، سنناقش الدور الحاسم الذي تلعبه التشريعات الوطنية للدول في تسهيل أو إعاقة هذا التعاون الدولي المنشود. إن فهم هذه المنظومة القانونية المتشابكة يمثل خطوة ضرورية لتقييم الجهود الدولية المبذولة واستكشاف سبل تعزيزها.

إن أهمية هذه الاتفاقيات تنبع من قدرتها على توفير أساس قانوني مشترك للإجراءات التعاونية، وتحديد الالتزامات المتبادلة بين الدول الأطراف، وتسهيل تبادل المعلومات وتقديم المساعدة القانونية في التحقيقات العابرة للحدود.

كما أنها تساهم في مواءمة التشريعات الوطنية المتعلقة بتجريم الأفعال الإلكترونية، مما يقلل من الثغرات القانونية التي يمكن أن يستغلها المجرمون. بالإضافة إلى ذلك، تعمل هذه الاتفاقيات على تشجيع الدول على تطوير آليات فعالة للتعاون في مجالات مثل تسليم المجرمين وتنفيذ الأحكام القضائية في قضايا الجرائم الإلكترونية.

المطلب الاول: اتفاقية بودابست 2001

تُعد اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية، المعروفة باسم اتفاقية بودابست والموقعة في عام 2001، الوثيقة الدولية الأولى التي سعت إلى معالجة قضايا الجريمة الإلكترونية على نطاق عالمي.

لقد شكلت هذه الاتفاقية علامة فارقة في جهود التعاون الدولي لمكافحة هذا النوع من الإجرام، حيث وضعت إطارًا قانونيًا شاملاً يهدف إلى تجريم الأفعال الإلكترونية، وتوفير آليات للتحقيق والملاحقة القضائية، وتعزيز التعاون بين الدول الأطراف. في هذا المطلب، سنتناول هذه الاتفاقية بالتفصيل، بدءًا بتسليط الضوء على الأهداف الرئيسية التي سعت إلى تحقيقها وأهميتها في سياق التعاون الدولي، ثم سننتقل إلى استعراض أبرز الجوانب الموضوعية والإجرائية التي تتضمنها.

الفرع الأول: الأهداف والأهمية العامة لاتفاقية بودابست 2001

لقد نشأت الحاجة إلى اتفاقية بودابست في مطلع الألفية الثالثة مع التزايد المطرد في الأنشطة الإجرامية التي تستغل التقنيات الرقمية وشبكات الإنترنت. كانت الأهداف الرئيسية التي دفعت مجلس أوروبا إلى صياغة هذه الاتفاقية متعددة الأوجه، وفي مقدمتها توفير إطار قانوني دولي موحد أو متقارب يسمح للدول بتجريم طائفة واسعة من الأفعال التي تُعد جرائم إلكترونية. قبل اتفاقية بودابست، كانت التشريعات الوطنية في هذا المجال متفاوتة بشكل كبير، مما كان يعيق التعاون الدولي الفعال[1].

سعت الاتفاقية إلى سد هذه الفجوة القانونية من خلال تحديد قائمة بالجرائم الإلكترونية التي يتعين على الدول الأطراف تجريمها في قوانينها الداخلية، مثل الدخول غير المصرح به، وإتلاف البيانات، والاحتيال المرتبط بالكمبيوتر، وانتهاكات حقوق الملكية الفكرية عبر الإنترنت.

[1] انيا خالد، التعاون الدولي لمكافحة الجرائم الإلكترونية: اتفاقية بودابست كنموذج، جامعة الملك سعود، 2024، ص 200.

منذ دخولها حيز النفاذ، اكتسبت اتفاقية بودابست أهمية بالغة على الصعيد الدولي. فقد أصبحت معيارًا مرجعيًا للعديد من الدول، سواء كانت أطرافًا فيها أم لا، في صياغة وتحديث تشريعاتها الوطنية المتعلقة بمكافحة الجريمة الإلكترونية.

كما لعبت دورًا محوريًا في تسهيل تبادل المعلومات وتقديم المساعدة القانونية المتبادلة بين الدول في التحقيقات التي تتضمن أدلة إلكترونية أو متهمين عبر الحدود. لقد وفرت الاتفاقية آليات واضحة لطلبات المساعدة، مثل جمع الأدلة الرقمية وتجميد الأصول، مما ساهم بشكل كبير في تعزيز التعاون العملياتي بين أجهزة إنفاذ القانون في مختلف الدول.

علاوة على ذلك، كان لاتفاقية بودابست تأثير ملحوظ على تشجيع الدول غير الأطراف على تبني معايير دولية في مجال مكافحة الجريمة الإلكترونية. فقد استرشدت العديد من الدول بتوصيات الاتفاقية ومبادئها في سن قوانينها الخاصة، حتى وإن لم تصبح أطرافًا فيها بشكل رسمي.

هذا الانتشار للمعايير التي أرستها الاتفاقية ساهم في خلق أرضية مشتركة أوسع للتعاون الدولي، حتى بين الدول التي لا تربطها اتفاقية بودابست بشكل مباشر. لقد أدركت العديد من الدول أن تبني هذه المعايير يسهل عليها التعاون مع الدول الأخرى في مكافحة الجرائم الإلكترونية التي لا تعترف بالحدود[1].

الفرع الثاني: أبرز الجوانب الموضوعية والإجرائية لاتفاقية بودابست 2001

تتضمن اتفاقية بودابست مجموعة شاملة من الأحكام الموضوعية التي تحدد الأفعال التي يتعين على الدول الأطراف تجريمها في قوانينها الداخلية. في مقدمة هذه الأفعال تأتي الجرائم ضد سرية وسلامة وتوافر البيانات والنظم الحاسوبية، وتشمل الدخول غير المشروع إلى الأنظمة، والاعتراض غير القانوني للاتصالات، وإتلاف أو

[1] Smith, Robert. Democracy and Citizen Participation: A Global Perspective. Cambridge University Press, United Kingdom, 2020, p. 45.

تغيير أو حذف البيانات الحاسوبية، وإساءة استخدام الأجهزة والبرامج الضارة. هذه الأحكام تهدف إلى حماية البنية التحتية الرقمية والمعلومات الحساسة من التهديدات الإلكترونية[1].

بالإضافة إلى ذلك، تتناول الاتفاقية الجرائم المرتبطة بالكمبيوتر، حيث يكون الكمبيوتر أو النظام الإلكتروني أداة لارتكاب جريمة أخرى. ويشمل ذلك التزوير والاحتيال المرتبطين بالكمبيوتر. كما تتضمن الاتفاقية أحكامًا تتعلق بـــ جرائم المحتوى، وتحديدًا تلك المتعلقة بإنتاج وتوزيع مواد إباحية للأطفال عبر أنظمة الكمبيوتر. هذه الأحكام تعكس إدراكًا لأبعاد الجريمة الإلكترونية التي تتجاوز مجرد استهداف الأنظمة والبيانات.

وعلى صعيد الجوانب الإجرائية، أولت اتفاقية بودابست اهتمامًا خاصًا لتيسير التحقيقات العابرة للحدود وجمع الأدلة الإلكترونية التي غالبًا ما تكون موزعة عبر ولايات قضائية متعددة.

نصت الاتفاقية على إجراءات تسمح لسلطات إنفاذ القانون بتنفيذ التفتيش والحجز على أنظمة الكمبيوتر والبيانات الإلكترونية، والكشف عن بيانات حركة المرور (Traffic Data) في ظل شروط وضوابط قانونية محددة. كما تضمنت الاتفاقية آليات مفصلة للـــ تعاون الدولي في مجال المساعدة القانونية المتبادلة، تحدد كيفية تقديم طلبات المساعدة وتلبيتها فيما يتعلق بجمع الأدلة وتبادل المعلومات.

وأخيرًا، تناولت الاتفاقية مسألة تسليم المجرمين المتهمين بارتكاب جرائم إلكترونية، مما يساهم في ضمان عدم إفلات الجناة من العقاب بسبب قدرتهم على اللجوء إلى دول أخرى. هذه الجوانب الإجرائية تعتبر حيوية لتمكين الدول من التحقيق بفعالية في الجرائم الإلكترونية وملاحقة مرتكبيها عبر الحدود.

[1] علي عمر، أحكام اتفاقية بودابست ودورها في مكافحة الجرائم الإلكترونية، أطروحة دكتوراه، جامعة الإسكندرية، 2023، ص140

المطلب الثاني: الاتفاقيات ذات الصلة – هيئة الامم المتحدة- قرارات الاتحاد الاوربي-

بالإضافة إلى اتفاقية بودابست التي تعتبر حجر الزاوية في الجهود الدولية لمكافحة الجريمة الإلكترونية، هناك العديد من الاتفاقيات والمعاهدات الأخرى ذات الصلة، بالإضافة إلى القرارات والتوصيات الصادرة عن منظمات دولية وإقليمية مثل هيئة الأمم المتحدة والاتحاد الأوروبي، والتي تساهم بشكل كبير في تعزيز التعاون الدولي في هذا المجال. هذه الأدوات القانونية والسياسية، وإن لم تكن مخصصة بشكل كامل للجريمة الإلكترونية، إلا أنها تتضمن أحكامًا مهمة أو توجهات عامة تؤثر بشكل مباشر أو غير مباشر على جهود مكافحة هذه الجرائم وتعزيز التعاون بين الدول. في هذا المطلب، سنتناول أبرز هذه الاتفاقيات والقرارات الصادرة عن هاتين المنظمتين الهامتين.

الفرع الأول: دور هيئة الأمم المتحدة في تعزيز التعاون الدولي لمكافحة الجريمة الإلكترونية

تضطلع هيئة الأمم المتحدة بدور محوري في حشد الجهود الدولية لمواجهة التحدي العالمي للجريمة الإلكترونية من خلال مختلف أجهزتها وآلياتها .الجمعية العامة للأمم المتحدة أصدرت العديد من القرارات التي تؤكد على أهمية التعاون الدولي في هذا المجال، وتسلط الضوء على التهديدات المتزايدة التي تطرحها الجرائم الإلكترونية على الأمن والاستقرار والتنمية.

هذه القرارات غالبًا ما تدعو الدول الأعضاء إلى تعزيز التعاون القانوني والعملياتي، وتبادل المعلومات وأفضل الممارسات، وبناء القدرات الوطنية لمكافحة هذه الجرائم.

كما أن مجلس الأمن التابع للأمم المتحدة أولى اهتمامًا متزايدًا للجوانب المتعلقة بالجريمة الإلكترونية التي تهدد الأمن الدولي، مثل مكافحة الإرهاب الإلكتروني واستخدام الإنترنت من قبل الجماعات الإرهابية لأغراض الدعاية والتجنيد وتمويل العمليات.

وقد صدرت عن المجلس قرارات تدعو الدول الأعضاء إلى اتخاذ تدابير لمواجهة هذه التهديدات وتعزيز التعاون في هذا الصدد.

بالإضافة إلى ذلك، تعمل اللجان المتخصصة التابعة للأمم المتحدة على معالجة جوانب محددة من الجريمة الإلكترونية. على سبيل المثال، هناك جهود تبذل في إطار الأمم المتحدة لتعزيز حماية الأطفال عبر الإنترنت ومكافحة استغلالهم وإساءة معاملتهم في الفضاء الرقمي. كما يتم تناول قضايا الجريمة المنظمة عبر الإنترنت في سياق مكافحة الجريمة المنظمة عبر الوطنية[1].

وتجدر الإشارة إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (اتفاقية باليرمو) وبروتوكولاتها الإضافية، والتي تمثل إطارًا قانونيًا دوليًا هامًا للتعاون في مكافحة الجريمة المنظمة.

على الرغم من أن هذه الاتفاقية لا تركز بشكل خاص على الجريمة الإلكترونية، إلا أن أحكامها المتعلقة بالمساعدة القانونية المتبادلة وتسليم المجرمين والتعاون في التحقيقات يمكن أن تكون ذات صلة في قضايا الجرائم الإلكترونية التي ترتكبها جماعات منظمة عبر الحدود. إن جهود الأمم المتحدة تساهم بشكل كبير في وضع الأسس القانونية والسياسية للتعاون الدولي الشامل في مواجهة الجريمة الإلكترونية.

[1] أحمد سعيد، القرارات الدولية لمكافحة الجريمة الإلكترونية: تحليل شامل، أطروحة ماجستير، جامعة البحرين، 2023، ص120

الفرع الثاني: مساهمات الاتحاد الأوروبي في تطوير التعاون الإقليمي والدولي لمكافحة الجريمة الإلكترونية

يُعد الاتحاد الأوروبي نموذجًا رائدًا في تطوير أطر قانونية وسياسات متكاملة لمكافحة الجريمة الإلكترونية على المستوى الإقليمي، وله دور فاعل في تعزيز التعاون مع الدول الأخرى على الصعيد الدولي. لقد أصدر الاتحاد الأوروبي العديد من التوجيهات (Directives) التي تلزم الدول الأعضاء بتوحيد أو تقارب قوانينها في مجال تجريم الأفعال الإلكترونية، مثل تلك المتعلقة بالهجمات على نظم المعلومات، والاحتيال الإلكتروني، واستغلال الأطفال في المواد الإباحية عبر الإنترنت. تهدف هذه التوجيهات إلى ضمان وجود مستوى أساسي من الحماية القانونية في جميع أنحاء الاتحاد وتسهيل التعاون القضائي[1].

كما تبنى الاتحاد الأوروبي العديد من اللوائح (Regulations) التي لها قوة القانون المباشر في الدول الأعضاء، والتي تتناول جوانب محددة من مكافحة الجريمة الإلكترونية، مثل تلك المتعلقة بتبادل المعلومات بين أجهزة إنفاذ القانون عبر الحدود وتنسيق التحقيقات العابرة للحدود. وقد أنشأ الاتحاد آليات فعالة للتعاون القضائي، مثل الأمر الأوروبي للتحقيق (European Investigation Order) الذي يسهل جمع الأدلة في الدول الأعضاء الأخرى.

بالإضافة إلى ذلك، يلعب الاتحاد الأوروبي دورًا نشطًا في بناء القدرات داخل الدول الأعضاء وخارجها في مجال مكافحة الجريمة الإلكترونية. يقدم الاتحاد الدعم المالي والتقني لتدريب الكوادر الأمنية والقضائية وتطوير البنية التحتية اللازمة لمواجهة التهديدات الإلكترونية. كما يشارك الاتحاد في مبادرات دولية لتعزيز التعاون العالمي في هذا المجال، وتبادل الخبرات وأفضل الممارسات مع الدول الأخرى

[1] كريم، عامر، استغلال الأطفال عبر الإنترنت: التوجيهات الأوروبية كحل، أطروحة ماجستير، جامعة ليون، 2023، ص. 120.

والمنظمات الدولية. إن التزام الاتحاد الأوروبي بتطوير أطر قانونية قوية وتعزيز التعاون العملي يجعله لاعبًا رئيسيًا في الجهود الدولية لمكافحة الجريمة الإلكترونية.[1]

المطلب الثالث: دور التشريعات الوطنية في تعزيز او اعاقة التعاون الدولي

بعد استعراض الاتفاقيات الدولية والإقليمية والجهود التي تبذلها المنظمات الدولية في مجال مكافحة الجريمة الإلكترونية، ننتقل في هذا المطلب إلى مستوى آخر لا يقل أهمية، وهو دور التشريعات الوطنية للدول. إن القوانين الداخلية للدول تلعب دورًا حاسمًا في تحديد مدى قدرتها على التعاون بفعالية مع الدول الأخرى في مواجهة هذه الجرائم العابرة للحدود.

فالتشريعات الوطنية التي تتوافق مع المعايير الدولية وتوفر آليات واضحة للتعاون يمكن أن تكون محفزًا قويًا لهذا التعاون، بينما قد تشكل القوانين التي تتسم بالقصور أو تتعارض مع هذه المعايير عائقًا أمام تحقيق تعاون دولي فعال. في هذا المطلب، سنقوم بتحليل كيف يمكن للتشريعات الوطنية أن تساهم في تعزيز التعاون الدولي، وفي المقابل، كيف يمكن أن تصبح سببًا في إعاقته.

الفرع الأول: طرق التشريعات الوطنية في تعزز التعاون الدولي في مكافحة الجريمة الإلكترونية؟

تلعب القوانين الداخلية للدول دورًا محوريًا في تيسير وتدعيم التعاون الدولي في مواجهة الجريمة الإلكترونية. فعندما تتبنى الدول تعريفات متوافقة للجرائم الإلكترونية مع المعايير الدولية الواردة في اتفاقيات مثل اتفاقية بودابست، يصبح من الأسهل عليها فهم طبيعة الأفعال المجرمة في الدول الأخرى والتعاون في التحقيقات والملاحقات

[1] جمال حمد، تطوير البنية التحتية لمكافحة الجرائم الإلكترونية: دور الاتحاد الأوروبي، دار الفكر العربي، 2022، ص. 210.

القضائية المتعلقة بها. هذا التقارب في المفاهيم القانونية يقلل من العقبات التي قد تنشأ بسبب الاختلاف في توصيف الأفعال الإجرامية[1].

علاوة على ذلك، فإن توفير آليات قانونية واضحة لتقديم المساعدة القانونية المتبادلة وتبادل المعلومات مع الدول الأخرى يُعدّ عاملاً حاسمًا في تعزيز التعاون. يجب أن تتضمن التشريعات الوطنية إجراءات مُيسرة لتلقي وتنفيذ طلبات المساعدة من الدول الأجنبية فيما يتعلق بجمع الأدلة الرقمية، وتفتيش الأنظمة، وتحديد هوية المشتبه بهم.

كما أن وجود قوانين تسمح بتبادل المعلومات الاستخباراتية بين أجهزة إنفاذ القانون بشكل فعال وآمن يساهم في الكشف المبكر عن التهديدات العابرة للحدود ومنع وقوع الجرائم.

كما أن تسهيل إجراءات تسليم المجرمين المتهمين بارتكاب جرائم إلكترونية يمثل جانبًا هامًا آخر. يجب أن تتضمن التشريعات الوطنية أحكامًا واضحة وفعالة لتسليم الأشخاص المطلوبين للعدالة من قبل دول أخرى، مع مراعاة الضمانات القانونية وحقوق الإنسان.

وبالمثل، فإن السماح بالتعاون العملياتي المشترك بين أجهزة إنفاذ القانون، مثل إجراء تحقيقات مشتركة أو عمليات متزامنة بالتنسيق مع دول أخرى، يعزز القدرة على تفكيك الشبكات الإجرامية العابرة للحدود.

إن تضمين أحكام تسمح بتنفيذ طلبات التحقيق وجمع الأدلة الرقمية الواردة من دول أجنبية يُعدّ ضروريًا لمواجهة طبيعة الأدلة الإلكترونية التي غالبًا ما تكون موجودة في ولايات قضائية متعددة. يجب أن تسمح القوانين الوطنية للسلطات المحلية بتنفيذ أوامر تفتيش وحجز صادرة عن محاكم أجنبية وفقًا لإجراءات واضحة وشفافة. إن

[1] علي كمال، القوانين الداخلية ومكافحة الجرائم الإلكترونية: تحديات وآفاق، دار الفكر العربي، لبنان، 2022، ص. 190

التشريعات الوطنية التي تتسم بهذه الخصائص تعمل كحافز قوي للتعاون الدولي الفعال في مكافحة الجريمة الإلكترونية.

الفرع الثاني: دور التشريعات الوطنية في اعاقة التعاون الدولي في مكافحة الجريمة الإلكترونية؟

على النقيض من الدور المعزز للتعاون الذي يمكن أن تلعبه التشريعات الوطنية، هناك جوانب فيها قد تتحول إلى عائق حقيقي أمام تحقيق تعاون دولي فعال في مكافحة الجريمة الإلكترونية. أحد أبرز هذه العوائق يتمثل في عدم تجريم بعض الأفعال التي تعتبر جرائم إلكترونية بموجب الاتفاقيات الدولية أو في تشريعات الدول الأخرى. هذا الاختلاف في التجريم يخلق ثغرات قانونية ويجعل من الصعب على الدول التعاون في التحقيقات أو تسليم المجرمين عن أفعال لا تعتبر جرائم في قوانينهم الداخلية[1].

كما أن وجود قيود قانونية صارمة على تبادل المعلومات أو تقديم المساعدة القانونية يمكن أن يعرقل بشكل كبير الجهود الدولية. فإذا كانت القوانين الوطنية تفرض شروطًا تعجيزية أو تتطلب إجراءات طويلة ومعقدة لتبادل المعلومات مع الدول الأجنبية، أو لتقديم المساعدة في جمع الأدلة الرقمية الموجودة داخل حدودها، فإن ذلك يؤدي إلى تأخير أو حتى إفشال التحقيقات العابرة للحدود. وبالمثل، فإن القيود المبالغ فيها على السرية المصرفية أو حماية البيانات قد تعيق الحصول على معلومات حيوية ضرورية لكشف الجرائم الإلكترونية.

وجود صعوبات في إجراءات تسليم المجرمين يمثل عائقًا آخر. إذا كانت القوانين الوطنية تتضمن شروطًا معقدة أو استثناءات واسعة لتسليم المطلوبين للعدالة عن جرائم إلكترونية، فإن ذلك يوفر ملاذًا آمنًا للمجرمين ويقلل من فعالية التعاون الدولي في ملاحقتهم.

[1] سارة جاد، الاختلافات في التجريم وتأثيرها على التعاون الدولي، الأمن السيبراني: التحديات والحلول، دار المعرفة، الإمارات، 2021، ص. 210

بالإضافة إلى ذلك، فإن عدم وجود آليات واضحة للتعاون العملياتي مع الدول الأخرى، مثل إمكانية تشكيل فرق تحقيق مشتركة أو تنفيذ عمليات متزامنة بالتنسيق مع سلطات أجنبية، يحد من القدرة على مواجهة الشبكات الإجرامية العابرة للحدود بشكل فعال.

إن تشكل القوانين الوطنية التي تتعارض مع المعايير الدولية المتعلقة بحماية البيانات والخصوصية عائقًا أمام التعاون الدولي. فإذا كانت القوانين الوطنية تفرض قيودًا مبالغ فيها على جمع أو نقل البيانات الشخصية حتى في سياق التحقيقات الجنائية المشروعة، فإن ذلك قد يتعارض مع متطلبات التعاون الدولي ويؤدي إلى رفض طلبات المساعدة من الدول الأجنبية. إن تحقيق التوازن بين حماية الحقوق الفردية ومتطلبات مكافحة الجريمة الإلكترونية على المستوى الدولي يمثل تحديًا هامًا للمشرعين الوطنيين[1].

المبحث الثاني: دور المنظمات والمؤسسات الدولية في مكافحة الجريمة الالكترونية

في عالمنا المترابط، حيث تتجاوز الجريمة الإلكترونية الحدود الوطنية بسهولة، تبرز المنظمات والمؤسسات الدولية كلاعبين محوريين في تنسيق الجهود العالمية لمواجهة هذا التحدي المتنامي.

هذه الكيانات تمثل منصات حيوية للتعاون بين الدول، حيث تعمل على تيسير تبادل المعلومات، ووضع المعايير والقواعد الإرشادية، وتقديم الدعم التقني وبناء القدرات، وتنسيق العمليات المشتركة. في هذا المبحث، سنتناول الدور الهام الذي

[1] سمير طه، قيود البيانات وتأثيرها على التعاون الدولي، مكافحة الجرائم الإلكترونية: الأبعاد القانونية، دار المعرفة، الكويت، 2023، ص. 130

تضطلع به هذه المنظمات والمؤسسات في مكافحة الجريمة الإلكترونية. سنبدأ بتسليط الضوء على الدور الفريد لمنظمة الشرطة الجنائية الدولية (الإنتربول) في تسهيل التعاون الشرطي الدولي.

ثم سنتناول جهود الأمم المتحدة ومكتبها المتخصص في مكافحة الجريمة والمخدرات في وضع الأطر القانونية وتعزيز التعاون العالمي. وأخيرًا، سنتطرق إلى دور المؤسسات الإقليمية، مع التركيز على جامعة الدول العربية وجهودها في هذا السياق الإقليمي الهام. إن فهم الدور الحيوي لهذه المنظمات والمؤسسات يمثل خطوة أساسية لتقدير الجهود الدولية المبذولة وتقييم فاعليتها في مواجهة الجريمة الإلكترونية.

المطلب الأول: دور منظمة الانتربول في مكافحة الجريمة الالكترونية

تُعد منظمة الشرطة الجنائية الدولية (الإنتربول) من أبرز المنظمات الدولية التي تلعب دورًا حيويًا في تسهيل التعاون الشرطي بين الدول الأعضاء في مختلف أنحاء العالم، بما في ذلك مجال مكافحة الجريمة الإلكترونية.

بفضل بنيتها التحتية العالمية وشبكتها الواسعة من مكاتب الاتصال ونظامها المتطور لتبادل المعلومات، يمثل الإنتربول منصة فريدة لتعزيز التعاون العملياتي والاستخباراتي بين أجهزة إنفاذ القانون في مواجهة الجرائم الإلكترونية العابرة للحدود. في هذا المطلب، سنتناول الدور المتعدد الأوجه الذي تضطلع به هذه المنظمة في هذا المجال، بدءًا بتسليط الضوء على الآليات والأدوات التي يوفرها لتسهيل التعاون العملياتي، ثم سنتناول جهوده في مجال تبادل المعلومات وبناء القدرات للدول الأعضاء في مكافحة الجريمة الإلكترونية.

الفرع الأول: الآليات والأدوات التي يوفرها الإنتربول لتسهيل التعاون العملياتي في مكافحة الجريمة الإلكترونية

يُعد الإنتربول ركيزة أساسية للتعاون العملياتي الدولي في مكافحة الجريمة الإلكترونية، حيث يوفر للدول الأعضاء مجموعة من الآليات والأدوات التي تتجاوز الحواجز الجغرافية والقانونية. من أبرز هذه الأدوات نظام الإشعارات الدولي، الذي يشمل أنواعًا مختلفة من النشرات مثل النشرة الحمراء التي تهدف إلى تحديد مكان واعتقال الأشخاص المطلوبين بتهم جنائية بهدف تسليمهم، والتي يمكن استخدامها بشكل فعال في تعقب مجرمي الإنترنت العابرين للحدود[1].

كما توجد النشرة الزرقاء التي تُستخدم لجمع معلومات إضافية حول هوية شخص أو أنشطته المتعلقة بجريمة إلكترونية. هذه النشرات تُمكّن أجهزة الشرطة في جميع أنحاء العالم من التعرف على المشتبه بهم واتخاذ الإجراءات اللازمة.

أما شبكة الاتصال الآمنة24/7-I ، فتمثل بنية تحتية اتصالية عالمية تعمل على مدار الساعة، وتتيح لأجهزة الشرطة في الدول الأعضاء تبادل المعلومات الحساسة بشكل فوري وآمن.

هذه الشبكة ضرورية لتبادل البيانات المتعلقة بالتحقيقات الجارية في جرائم إلكترونية، وتحديد الروابط بين الجرائم والأفراد في مختلف الدول، وتنسيق الجهود العملياتية. كما تتيح الشبكة الوصول إلى قواعد بيانات الإنتربول التي تحتوي على معلومات حيوية حول المجرمين والجرائم الإلكترونية المعروفة.

بالإضافة إلى ذلك، يلعب الإنتربول دورًا محوريًا في تنسيق العمليات المشتركة بين الدول الأعضاء لمكافحة الجرائم الإلكترونية المنظمة والعابرة للحدود. فعندما تواجه عدة دول تهديدًا إلكترونيًا مشتركًا، يمكن للإنتربول أن يسهل التخطيط والتنفيذ

[1] رفعت ناصر، دور الإنتربول في مكافحة الجرائم العابرة للحدود، الأمن السيبراني: التحديات العالمية، مكتبة الأفق، مصر، 2023، ص. 150

لعمليات دولية متزامنة تستهدف الشبكات الإجرامية ومصادرة الأصول غير المشروعة.

يوفر الإنتربول منصة للتنسيق وتبادل المعلومات اللوجستية والاستخباراتية خلال هذه العمليات، مما يزيد من فرص النجاح في تفكيك التنظيمات الإجرامية وتقديم أعضائها للعدالة. إن هذه الآليات والأدوات تجعل من الإنتربول شريكًا لا غنى عنه في الجهود العالمية لمكافحة الجريمة الإلكترونية[1].

الفرع الثاني: دور الإنتربول في تبادل المعلومات وبناء القدرات للدول الأعضاء في مجال مكافحة الجريمة الإلكترونية

يُعد الإنتربول مركزًا حيويًا لـــ تبادل المعلومات الاستخباراتية والفنية المتعلقة بالجريمة الإلكترونية بين الدول الأعضاء. تقوم المنظمة بجهود مستمرة في جمع وتحليل البيانات الواردة من مختلف الدول حول الأنشطة الإجرامية الإلكترونية، بما في ذلك تحديد أحدث التهديدات الناشئة، وتتبع الاتجاهات الإجرامية المتغيرة، وفهم التقنيات الجديدة التي يستخدمها المجرمون في ارتكاب جرائمهم.

ثم تقوم الإنتربول بنشر هذه المعلومات القيّمة على نطاق واسع بين الدول الأعضاء من خلال قنواتها المختلفة، مما يساعد أجهزة إنفاذ القانون على فهم أفضل للمخاطر وكيفية مواجهتها بشكل استباقي.

إلى جانب تبادل المعلومات، يولي الإنتربول أهمية كبيرة لـــ بناء القدرات لدى الدول الأعضاء في مجال مكافحة الجريمة الإلكترونية. تقوم المنظمة بتنظيم الدورات التدريبية وورش العمل المتخصصة التي تستهدف العاملين في مختلف أجهزة إنفاذ

[1] جمال حمد، الآليات اللوجستية للإنتربول في مكافحة الجرائم الإلكترونية، الأمن السيبراني: المفاهيم والتطبيقات، دار الفكر العربي، لبنان، 2022، ص. 215.

القانون، بهدف تزويدهم بالمعرفة والمهارات اللازمة للتحقيق في الجرائم الإلكترونية المعقدة وملاحقة مرتكبيها[1].

تشمل هذه البرامج التدريبية موضوعات متنوعة مثل تحليل الأدلة الرقمية، وتتبع العملات المشفرة، ومكافحة الاحتيال عبر الإنترنت، والتعامل مع جرائم الإنترنت المتعلقة بالأطفال.

علاوة على ذلك، يقدم الإنتربول الدعم التقني للدول الأعضاء لمساعدتها في تطوير بنيتها التحتية لمكافحة الجريمة الإلكترونية وتعزيز قدراتها في مجال الأمن السيبراني. يمكن أن يشمل ذلك تقديم المشورة بشأن اقتناء الأدوات والتقنيات اللازمة للتحقيق في الجرائم الإلكترونية، أو المساعدة في إنشاء وحدات متخصصة في مكافحة هذا النوع من الإجرام داخل أجهزة الشرطة الوطنية.

من خلال هذه الجهود في تبادل المعلومات وبناء القدرات، يلعب الإنتربول دورًا حاسمًا في تمكين الدول الأعضاء من تعزيز دفاعاتها ومكافحة الجريمة الإلكترونية بشكل أكثر فعالية على المستويين الوطني والدولي

المطلب الثاني: دور الامم المتحدة ومكتب مكافحة الجريمة الالكترونية

تضطلع منظمة الأمم المتحدة بدور محوري في تعزيز التعاون الدولي لمكافحة مختلف أشكال الجريمة، بما في ذلك الجريمة الإلكترونية، وذلك من خلال أجهزتها المتعددة وبرامجها المتخصصة. ويعد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)الذراع الرئيسي للأمم المتحدة في هذا المجال، حيث يقوم بتطوير الأطر القانونية، وتقديم المساعدة التقنية للدول الأعضاء، وتسهيل تبادل المعلومات وتعزيز التعاون الدولي في مواجهة التهديدات الإلكترونية المتنامية.

[1] رفعت ناصر، دور الإنتربول في تدريب الكوادر الأمنية، الأمن السيبراني: التحديات العالمية، مكتبة الأفق، مصر، 2023، ص. 150.

في هذا المطلب، سنتناول الدور المتعدد الأوجه الذي تلعبه الأمم المتحدة ومكتبها المتخصص في مكافحة الجريمة الإلكترونية، بدءًا بتسليط الضوء على جهودهما في وضع الاتفاقيات والمعاهدات وتطوير الأدلة الإرشادية، ثم سنتناول دورهما في تقديم المساعدة التقنية وبناء القدرات للدول الأعضاء لتعزيز قدرتها على مواجهة هذه الجرائم.

الفرع الأول: جهود الأمم المتحدة ومكتب مكافحة الجريمة والمخدرات في وضع الأطر القانونية وتطوير الأدلة الإرشادية لمكافحة الجريمة الإلكترونية

يُعد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) قوة دافعة رئيسية في تطوير الأطر القانونية الدولية والإقليمية التي تستهدف مكافحة الجريمة الإلكترونية. يقوم المكتب بدور محوري في دعم المفاوضات بين الدول الأعضاء التي تفضي إلى تبني اتفاقيات دولية ذات صلة .

وعلى الرغم من أن بعض هذه الاتفاقيات، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (اتفاقية باليرمو) وبروتوكولاتها، لا تركز بشكل حصري على الجريمة الإلكترونية، إلا أنها تتضمن أحكامًا قابلة للتطبيق على جوانب معينة من هذه الجرائم، خاصة تلك التي ترتكبها جماعات منظمة عبر الحدود، مثل المساعدة القانونية المتبادلة وتسليم المجرمين[1].

علاوة على ذلك، يضطلع مكتب مكافحة الجريمة والمخدرات بدور هام في تطوير أدلة إرشادية ومبادئ توجيهية موجهة إلى الدول الأعضاء. تهدف هذه الأدوات إلى مساعدة الدول في سن تشريعات وطنية فعالة لمكافحة الجريمة الإلكترونية وتطبيقها على أرض الواقع.

[1] نجلاء فؤاد، "استراتيجيات تسليم المجرمين في إطار الجرائم المنظمة"، مجلة الدراسات القانونية، العدد 9، 2023.

تتضمن هذه الأدلة توصيات عملية حول كيفية تجريم مختلف أنواع الجرائم الإلكترونية بما يتماشى مع المعايير الدولية، وكيفية وضع إجراءات فعالة للتحقيق في هذه الجرائم وجمع الأدلة الرقمية، وكيفية تعزيز التعاون الدولي مع الدول الأخرى في هذا المجال. إن هذه الجهود تساهم في توحيد المفاهيم القانونية وتسهيل التعاون العملي بين الدول في مواجهة التحديات الإلكترونية.

الفرع الثاني: دور الأمم المتحدة ومكتب مكافحة الجريمة والمخدرات في تقديم المساعدة التقنية وبناء القدرات للدول الأعضاء في مجال مكافحة الجريمة الإلكترونية

يُعد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) جهة فاعلة رئيسية في تقديم المساعدة التقنية للدول الأعضاء التي تسعى لتعزيز قدراتها في ميدان مكافحة الجريمة الإلكترونية. يقوم المكتب بتوفير الخبرات والموارد اللازمة لدعم الدول في عدة جوانب حيوية. يشمل ذلك تقديم العون في تطوير التشريعات الوطنية لتكون متوافقة مع المعايير الدولية وتستجيب بشكل فعال للتحديات الإلكترونية المستجدة.

كما يركز المكتب على تدريب الكوادر الأمنية والقضائية المتخصصة من خلال تنظيم برامج تدريبية وورش عمل تهدف إلى تزويدهم بالمهارات والمعرفة الضرورية للتحقيق في الجرائم الإلكترونية المعقدة وملاحقة مرتكبيها.

ويشمل ذلك تدريبهم على جمع وتحليل الأدلة الرقمية، وتتبع الأنشطة الإجرامية عبر الإنترنت، وفهم الجوانب القانونية والإجرائية المتعلقة بهذا النوع من الجرائم. بالإضافة إلى ذلك، يساعد المكتب الدول في إنشاء وحدات متخصصة في مكافحة الجرائم الإلكترونية داخل أجهزتها الأمنية والقضائية، وتقديم الدعم اللازم لتجهيز هذه الوحدات وتفعيل دورها.

علاوة على ذلك، يضطلع مكتب مكافحة الجريمة والمخدرات بدور هام في تسهيل تبادل المعلومات وأفضل الممارسات بين الدول الأعضاء في مجال مكافحة الجريمة الإلكترونية، وذلك من خلال تنظيم المؤتمرات والمنتديات وورش العمل التي تجمع الخبراء والمتخصصين.

كما يشجع المكتب التعاون الإقليمي والدولي من خلال دعم المبادرات المشتركة وتبادل الخبرات بين الدول ذات التحديات المشتركة. إن هذه الجهود تساهم في تعزيز قدرات الدول الأعضاء على المستوى الوطني والإقليمي والدولي في مواجهة الجريمة الإلكترونية بشكل أكثر فعالية[1].

المطلب الثالث: دور المؤسسات الاقليمية جامعة الدول العربية

إلى جانب الجهود العالمية التي تبذلها الأمم المتحدة والمنظمات الدولية الأخرى، تلعب المنظمات الإقليمية دورًا لا يقل أهمية في تعزيز التعاون بين الدول الأعضاء في نطاقها الجغرافي لمواجهة تحدي الجريمة الإلكترونية. وتُعد جامعة الدول العربية إحدى هذه المنظمات الإقليمية الهامة التي تسعى إلى تضافر جهود الدول العربية في مختلف المجالات، ومن بينها مكافحة الجرائم المستحدثة التي تستغل الفضاء الرقمي.

في هذا المطلب، سنتناول الدور الذي تضطلع به جامعة الدول العربية ومؤسساتها المختلفة في سبيل تعزيز التعاون العربي لمكافحة الجريمة الإلكترونية، بدءًا باستعراض المبادرات والاتفاقيات التي تم تبنيها تحت مظلتها، ثم سنتناول جهودها في مجال تبادل الخبرات وتطوير القدرات في هذا الإطار الإقليمي.

[1] سمير، طه، استراتيجيات التعاون الإقليمي في مواجهة الجرائم الإلكترونية، دار المعرفة، الكويت، 2021، ص. 180.

الفرع الأول: المبادرات والاتفاقيات التي تبنتها جامعة الدول العربية لتعزيز التعاون في مكافحة الجريمة الإلكترونية

سعت جامعة الدول العربية، إدراكًا منها لتنامي خطر الجريمة الإلكترونية وتأثيرها على المنطقة العربية، إلى تبني العديد من المبادرات والاتفاقيات بهدف تعزيز التنسيق والتعاون بين الدول الأعضاء في هذا المجال الحيوي[1].

من أبرز هذه الجهود، المساعي الرامية إلى وضع أطر قانونية عربية مشتركة أو متقاربة للتصدي لهذه الجرائم. وقد تمثل ذلك في اقتراح نماذج لقوانين استرشادية أو صياغة اتفاقيات تهدف إلى توحيد المفاهيم القانونية وتجريم الأفعال الإلكترونية بشكل متناسق في مختلف الدول العربية.

بالإضافة إلى ذلك، أولت الجامعة اهتمامًا خاصًا للمبادرات التي تهدف إلى تبادل المعلومات والتنسيق الأمني بين الأجهزة المختصة في الدول العربية[2].

وقد تمثل ذلك في تشجيع إنشاء آليات للتواصل السريع والآمن بين وحدات مكافحة الجريمة الإلكترونية في الدول الأعضاء، وتبادل التحذيرات والمعلومات الاستخباراتية حول التهديدات الإلكترونية الناشئة والاتجاهات الإجرامية في المنطقة.

كما تم التأكيد على أهمية عقد الاجتماعات والمنتديات الدورية لتبادل الخبرات وتعزيز التنسيق العملياتي المشترك في مواجهة الجرائم الإلكترونية العابرة للحدود العربية. إن هذه المبادرات والاتفاقيات تعكس إدراكًا إقليميًا لأهمية العمل المشترك لمواجهة هذه التحديات الأمنية والقانونية.

---

[1] رفعت ناصر، "التفاعل بين التشريعات الوطنية والاتفاقيات الدولية في مكافحة الجرائم الإلكترونية"، مجلة الدراسات الأمنية، العدد 5، 2023.

[2] جمال حمد، التنسيق الأمني بين الدول العربية: دراسة تحليلية، جامعة الإسكندرية، 2023، ص. 220.

الفرع الثاني: جهود جامعة الدول العربية في تبادل الخبرات وتطوير القدرات العربية في مجال مكافحة الجريمة الإلكترونية

تضطلع جامعة الدول العربية بدور هام في تيسير تبادل الخبرات والمعرفة بين الدول الأعضاء في مجال مكافحة الجريمة الإلكترونية. وتقوم الجامعة بذلك من خلال تنظيم المؤتمرات والندوات وورش العمل التي تجمع الخبراء والمتخصصين من مختلف الدول العربية.

هذه الملتقيات تمثل منصات قيمة لمناقشة التحديات المشتركة التي تواجه المنطقة في مجال الأمن السيبراني والجريمة الإلكترونية، وتبادل أفضل الممارسات والاستراتيجيات الناجحة التي تم تطبيقها في الدول الأعضاء.

كما تسعى الجامعة إلى تطوير القدرات العربية في هذا المجال الحيوي من خلال تشجيع برامج التدريب والمساعدة التقنية .وقد تعمل الجامعة بشكل مباشر على تنظيم دورات تدريبية متخصصة للعاملين في أجهزة إنفاذ القانون والجهات القضائية في الدول الأعضاء، أو قد تشجع على التعاون الثنائي والإقليمي في تبادل المدربين والخبراء وتقديم المساعدة التقنية اللازمة لإنشاء وتطوير وحدات مكافحة الجريمة الإلكترونية الوطنية[1].

[1] فاطمة محمود، التدريب الأمني في مواجهة الجرائم الإلكترونية: المفاهيم والتطبيقات، مكتبة النهضة، مصر، 2022، ص. 175.

المبحث الثالث: تحديات وافاق التعاون الدولي في مكافحة الجريمة الإلكترونية

إن فهم العقبات التي تواجه الجهود الدولية المشتركة يمثل خطوة ضرورية لتحديد السبل الكفيلة بتجاوزها وتحقيق تعاون أكثر فعالية. لذا، سيتناول المطلب الأول أبرز التحديات التي تواجه التعاون الدولي في هذا المجال، سواء كانت قانونية تتعلق بالاختلافات في التشريعات الوطنية والإجراءات القضائية، أو تقنية ناتجة عن التطور السريع للوسائل الإجرامية وصعوبة تتبعها، أو سياسية تتعلق بالاعتبارات السيادية والخلافات بين الدول، أو حتى اقتصادية واجتماعية مرتبطة بتفاوت القدرات والموارد بين الدول وتأثير الجريمة الإلكترونية على المجتمعات. إن تحليل هذه التحديات واستكشاف سبل تجاوزها يمثل خطوة حاسمة نحو تحقيق تعاون دولي أكثر فاعلية واستدامة في مكافحة الجريمة الإلكترونية. ففي عالم يزداد فيه الاعتماد على الفضاء الرقمي، يصبح ضمان أمن هذا الفضاء مسؤولية جماعية تتطلب تضافر جهود جميع الدول والمؤسسات المعنية. أما المطلب الثاني، فسيركز على استعراض مجموعة من السبل والآليات التي يمكن من خلالها تعزيز هذا التعاون وتوسيع نطاقه لتحقيق نتائج أفضل في مواجهة التهديدات المتزايدة التي تطرحها الجريمة الإلكترونية. سنبحث في إمكانية تطوير أطر قانونية أكثر شمولية ومرونة، وتعزيز تبادل المعلومات والخبرات بين الأجهزة الأمنية والقضائية على المستوى الدولي، وتسخير التكنولوجيا المتقدمة في تعقب الجرائم الإلكترونية ومكافحتها، وأهمية بناء شراكات فعالة بين القطاعين العام والخاص في هذا الجهد المشترك.

المطلب الأول: التحديات التي تواجه التعاون الدولي في مكافحة الجريمة الإلكترونية

إن تحقيق تعاون دولي فعال في مكافحة الجريمة الإلكترونية يواجه جملة من التحديات المتنوعة التي تعيق التنسيق وتكامل الجهود بين الدول. هذه التحديات تنبع من

طبيعة الجريمة الإلكترونية نفسها، والاختلافات بين الأنظمة القانونية للدول، والتطور المستمر للتقنيات المستخدمة في ارتكاب هذه الجرائم. بالإضافة إلى ذلك، هناك تحديات سياسية واقتصادية واجتماعية يمكن أن تؤثر على مدى استعداد الدول وقدرتها على التعاون بشكل كامل وفعال في هذا المجال. إن التعقيد المتزايد للجرائم الإلكترونية، التي غالبًا ما تتضمن أطرافًا وأدلة موزعة عبر عدة ولايات قضائية، يزيد من الحاجة إلى تعاون دولي قوي ومتكامل، ولكنه في الوقت نفسه يزيد من صعوبة تحقيقه في ظل هذه التحديات.سنتناول أبرز هذه التحديات التي تعترض سبيل التعاون الدولي المنشود. سنركز في الفرع الأول على التحديات القانونية التي تنشأ عن تباين التشريعات الوطنية والإجراءات القضائية، مثل الاختلاف في تعريف الجرائم الإلكترونية، وقواعد الاختصاص القضائي، وإجراءات تبادل الأدلة وتقديم المساعدة القانونية وتسليم المجرمين.

وفي الفرع الثاني، سنتناول التحديات التقنية المرتبطة بالطبيعة المعقدة والمتغيرة باستمرار للأدلة الرقمية وصعوبة تتبعها عبر الحدود، بالإضافة إلى التحديات المتعلقة بالوصول إلى البيانات الموجودة في الخارج والتعامل مع التقنيات المشفرة. إن فهم هذه التحديات يمثل الخطوة الأولى نحو إيجاد حلول فعالة لتعزيز التعاون الدولي في هذا المجال

الفرع الأول: التحديات القانونية

يمثل الإطار القانوني حجر الزاوية في أي تعاون دولي فعال، وفي مجال مكافحة الجريمة الإلكترونية، تبرز العديد من التحديات القانونية التي تعيق هذا التعاون. تنبع هذه التحديات بشكل أساسي من الاختلافات الجوهرية بين الأنظمة القانونية للدول، سواء في تعريف الأفعال المجرمة، أو في قواعد الاختصاص القضائي، أو في الإجراءات المتعلقة بتبادل الأدلة وتقديم المساعدة القانونية وتسليم المجرمين.

إن التباين في التجريم بين الدول يمثل تحديًا هيكليًا للتعاون الدولي في مكافحة الجريمة الإلكترونية. فغياب تعريفات قانونية متسقة للأفعال الإجرامية في الفضاء الرقمي يؤدي إلى صعوبات جمة في تطبيق مبادئ أساسية للتعاون، كالتجريم المزدوج اللازم لتنفيذ طلبات المساعدة القانونية المتبادلة وتسليم المجرمين. على سبيل المثال، قد يُنظر إلى فعل معين على أنه جريمة احتيال إلكتروني خطيرة في دولة ما، بينما يُعتبر مخالفة بسيطة أو حتى فعلًا غير مجرم في دولة أخرى. هذا التباين القانوني يعيق قدرة الدول على العمل المشترك بفعالية ضد مرتكبي هذه الأفعال العابرة للحدود.

علاوة على ذلك، يتجلى تأثير اختلاف التجريم في نطاق التعاون العملياتي بين أجهزة إنفاذ القانون. فإذا لم يكن الفعل موضوع التحقيق مجرمًا في الدولة المطلوب منها التعاون، فقد تتردد أجهزتها الأمنية في تقديم الدعم اللازم أو المشاركة في عمليات مشتركة[1]. هذا النقص في التوافق القانوني يقوض الجهود الرامية إلى تفكيك الشبكات الإجرامية الإلكترونية التي غالبًا ما تنشط عبر عدة دول تستغل هذه الثغرات القانونية.

أما فيما يتعلق بـــ قواعد الاختصاص القضائي، فإن الطبيعة اللامركزية للإنترنت تجعل تطبيق المعايير الإقليمية والشخصية والنتائجية التقليدية أمرًا معقدًا. ففي الجرائم الإلكترونية، قد يكون من الصعب تحديد "مكان ارتكاب الجريمة" بشكل قاطع، حيث تبدأ الأفعال الإجرامية وتنتهي عبر شبكات عالمية. وبالمثل، قد يكون مرتكب الجريمة والضحية من جنسيات مختلفة ويقيمان في دول مختلفة، مما يثير تساؤلات حول أي قانون وطني يجب تطبيقه.

إن تضارب الاختصاص القضائي يمكن أن يؤدي إلى ازدواجية الإجراءات وتعطيل التعاون. فقد تبدأ دولتان أو أكثر تحقيقات متوازية في نفس الواقعة دون تنسيق، مما قد يؤدي إلى إهدار الموارد وتعريض الأدلة للخطر. كما قد ينشأ نزاع

[1] مروان بن عزيز .اختلاف تأثير التجريم على التعاون .دار البحث القانونية، تونس، 2023، ص 107.

حول أحقية كل دولة في محاكمة المتهم. في المقابل، فإن غياب الاختصاص القضائي يمثل مشكلة أخرى، حيث قد لا تجد أي دولة نفسها قادرة أو راغبة في ممارسة ولايتها القضائية على فعل إجرامي إلكتروني ارتكب خارج إقليمها ولم يستهدف مصالحها بشكل مباشر.

إن تفسير القوانين الوطنية المتعلقة بالجريمة الإلكترونية قد يختلف بين الدول، حتى في الحالات التي يوجد فيها تجريم مماثل للفعل. هذا الاختلاف في التفسير يمكن أن يؤثر على مدى استعداد دولة ما للتعاون في تنفيذ طلبات المساعدة القانونية أو في الاعتراف بالأحكام القضائية الصادرة من دول أخرى في قضايا الجرائم الإلكترونية. فالتضييق في تفسير النصوص القانونية قد يؤدي إلى رفض التعاون بحجة عدم تطابق الوقائع مع القانون الوطني[1].

يواجه التعاون الدولي في مكافحة الجريمة الإلكترونية تحديات جوهرية تتعلق بـــ تبادل الأدلة الرقمية وتقديم المساعدة القانونية المتبادلة، بالإضافة إلى إجراءات تسليم المجرمين .ففي قضايا الجرائم الإلكترونية، غالبًا ما تكون الأدلة ذات طبيعة رقمية وموزعة عبر خوادم وأنظمة تقع في دول مختلفة. الحصول على هذه الأدلة يتطلب تعاونًا فعالًا بين سلطات إنفاذ القانون والقضاء في الدول المعنية. إلا أن القوانين والإجراءات الوطنية المختلفة المتعلقة بجمع الأدلة الرقمية، مثل شروط إصدار أوامر التفتيش والحجز الإلكتروني، وقواعد الإثبات، وحماية البيانات الشخصية، قد تعيق عملية تبادل الأدلة أو تؤدي إلى تأخيرها.

كما أن تقديم المساعدة القانونية المتبادلة في قضايا الجرائم الإلكترونية قد يواجه صعوبات. فقد تختلف الدول في متطلباتها القانونية لتلبية طلبات المساعدة، سواء فيما يتعلق بنوع المعلومات المطلوبة، أو الإجراءات الواجب اتباعها، أو القيود المفروضة

[1] ليلى الفهيد .التعاون بين أجهزة مكافحة الجريمة .مكتبة القانون، الإمارات، 2024، ص 94.

على تقديم المساعدة. على سبيل المثال، قد تطلب دولة ما معلومات تعتبر محمية بموجب قوانين الخصوصية في دولة أخرى، مما يؤدي إلى رفض الطلب أو تأخيره.

أما فيما يتعلق بـــ تسليم المجرمين المتهمين بارتكاب جرائم إلكترونية، فتعتبر هذه العملية معقدة وتخضع لشروط وإجراءات قانونية دقيقة تختلف من دولة إلى أخرى. بالإضافة إلى شرط التجريم المزدوج الذي تم ذكره سابقًا، قد ترفض الدول تسليم مواطنيها أو في حالات تتعلق بجرائم لا تعتبرها بالغة الخطورة. كما أن الإجراءات القانونية الطويلة والمعقدة للتسليم يمكن أن تقلل من فعالية هذه الآلية في ملاحقة مجرمي الإنترنت العابرين للحدود.

الفرع الثاني: التحديات التقنية

بالإضافة إلى التحديات القانونية التي تعيق التعاون الدولي في مكافحة الجريمة الإلكترونية، تبرز مجموعة أخرى من الصعوبات ذات الطبيعة التقنية التي تزيد من تعقيد هذا التعاون. إن السرعة الهائلة للتطور التكنولوجي، والطبيعة المعقدة للأدلة الرقمية، وإمكانية إخفاء هوية مرتكبي الجرائم الإلكترونية عبر استخدام تقنيات متقدمة، كلها عوامل تجعل من تتبع هذه الجرائم والتحقيق فيها وملاحقة مرتكبيها عبر الحدود مهمة بالغة التعقيد.

تتميز الأدلة الرقمية بخصائص فريدة تجعل عملية تتبع الجرائم الإلكترونية وتحديد مصدرها عبر الحدود تحديًا بالغ التعقيد. بخلاف الأدلة التقليدية، فإن الأدلة الرقمية تتسم بـــ سهولة تغييرها وإتلافها. فبمجرد الوصول إلى نظام إلكتروني، يمكن للمجرم تعديل السجلات أو حذفها أو حتى زرع أدلة زائفة، مما يجعل الحفاظ على سلامة الأدلة ونزاهتها أمرًا صعبًا، خاصة عند التعامل مع تحقيقات تشمل ولايات

قضائية متعددة حيث تتطلب عملية الحصول على الأدلة وقتًا قد يستغله الجاني للتلاعب بها[1].

خاصية أخرى مميزة للأدلة الرقمية هي سهولة توزيعها عبر ولايات قضائية متعددة. يمكن أن تكون أجزاء من دليل واحد موجودة على خوادم في دول مختلفة، أو في حوسبة سحابية لا تخضع بشكل واضح لقانون دولة معينة. هذا التوزيع يجعل من الصعب تحديد مكان وجود الدليل بشكل قاطع والخضوع لقوانين دولة واحدة في جمعه والحفاظ عليه. يتطلب الأمر تعاونًا بين سلطات دول متعددة للحصول على صورة كاملة للدليل، وهو ما قد يعترضه الاختلاف في الإجراءات القانونية والتقنية.

بالإضافة إلى ذلك، فإن الطبيعة العابرة للحدود للشبكات الإلكترونية تعني أن مصدر الهجوم أو الفعل الإجرامي قد يكون متخفيًا في دولة بعيدة عن مكان وقوع الضرر أو وجود الضحية. تتبع مصدر الهجوم يتطلب مهارات تقنية متقدمة وتعاونًا دوليًا لتبادل المعلومات حول عناوين IP والسجلات والبيانات الأخرى التي قد تكشف عن هوية الجاني[2]، وهو ما قد يعيقه اختلاف القوانين المتعلقة بالوصول إلى هذه البيانات في الدول المختلفة.كل هذه الخصائص تجعل من تحديد مصدر الجريمة الإلكترونية وتتبع مسارها عبر الحدود تحديًا كبيرًا يواجه أجهزة إنفاذ القانون على المستوى الدولي. يتطلب الأمر تطوير أدوات تقنية مشتركة، وتبادل الخبرات، وتنسيق الإجراءات القانونية لتجاوز هذه العقبات وضمان فعالية التحقيقات العابرة للحدود.

إضافة إلى ذلك، فإن سرعة تطور التقنيات المستخدمة في ارتكاب الجرائم الإلكترونية تفوق في كثير من الأحيان سرعة تطور القدرات التقنية والقانونية لأجهزة

[1] يوسف الخليل .سلامة الأدلة الرقمية .دار الثقافة، لبنان، 2022، ص 97.

[2] عادل الفارس .تحديات الأدلة الرقمية في الفايروس .دار البحث القانونية، تونس، 2023، ص 112.

إنفاذ القانون[1]. ظهور تقنيات جديدة مثل العملات المشفرة والشبكات المظلمة يخلق تحديات جديدة في تتبع الأنشطة الإجرامية وتحديد هوية مرتكبيها عبر الحدود.

يمثل الوصول إلى البيانات المخزنة عبر الحدود تحديًا تقنيًا وقانونيًا كبيرًا في تحقيقات الجرائم الإلكترونية. غالبًا ما يتم تخزين البيانات ذات الصلة بالتحقيق على خوادم تقع في دول أخرى، تخضع لقوانين وسياسات مختلفة فيما يتعلق بالكشف عن هذه البيانات. قد تتطلب عملية الحصول على هذه البيانات اتباع إجراءات قانونية معقدة وطويلة، مثل تقديم طلبات مساعدة قانونية متبادلة، والتي قد تستغرق وقتًا طويلاً أو قد لا تؤدي دائمًا إلى النتائج المرجوة. كما أن بعض الدول قد تفرض قيودًا على نقل البيانات خارج حدودها، حتى لأغراض التحقيق الجنائي.

إن استخدام تقنيات التشفير من قبل مرتكبي الجرائم الإلكترونية يمثل عقبة تقنية كبيرة أمام جهود التعقب وكشف المحتوى الإجرامي. يمكن للتشفير القوي أن يجعل البيانات غير قابلة للقراءة بالنسبة لأجهزة إنفاذ القانون ما لم يتم الحصول على مفاتيح فك التشفير. قد يرفض المجرمون تقديم هذه المفاتيح، وقد لا تكون هناك طرق تقنية متاحة لكسر التشفير في وقت معقول. هذا يعيق القدرة على الوصول إلى الأدلة الهامة وفهم طبيعة الأنشطة الإجرامية.

إن التحدي المتعلق بـــ الولاية القضائية على مقدمي الخدمات الذين قد يكونون متواجدين في دولة أخرى غير الدولة التي يقع فيها المستخدم أو الخادم الذي يحمل البيانات المطلوبة. غالبًا ما يكون الحصول على أمر قضائي ملزم لهؤلاء المزودين بالكشف عن البيانات عملية معقدة وتستغرق وقتًا طويلاً، وتخضع للقوانين والإجراءات

[1] سمر العلي .الأدلة الرقمية والجرائم الإلكترونية .مكتبة القانون، الإمارات، 2024، ص 95.

الخاصة بالدولة التي يقع فيها المزود. هذا يعيق الوصول السريع والفعال إلى البيانات الهامة للتحقيق[1].

المطلب الثاني: سبل تعزيز التعاون الدولي لمكافحة الجريمة الإلكترونية

في ضوء التحديات التي تم استعراضها في المبحث الأول، يصبح من الضروري تحديد واستكشاف السبل والآليات الكفيلة بتعزيز التعاون الدولي وتوسيع نطاقه لتحقيق نتائج أكثر فعالية في مواجهة التهديدات المتزايدة التي تطرحها الجريمة الإلكترونية. إن تجاوز العقبات القانونية والتقنية يتطلب جهودًا متكاملة على مختلف المستويات، تشمل تطوير التشريعات، وتحسين آليات تبادل المعلومات، والاستفادة من التطورات التكنولوجية، وإقامة شراكات استراتيجية. إن الهدف النهائي هو بناء نظام دولي متين وقادر على التصدي بفاعلية لهذه الجرائم العابرة للحدود وحماية المجتمعات والفضاء الرقمي.سنركز في الفرع الأول على تطوير الأطر القانونية وتعزيز التعاون القضائي أما في الفرع الثاني، فسوف نتناول تعزيز التعاون العملياتي وتبادل الخبرات والمعلومات وتسخير التكنولوجيا .

الفرع الأول: تطوير الأطر القانونية وتعزيز التعاون القضائي

يُعد تطوير أطر قانونية دولية ووطنية أكثر شمولية ومرونة، إلى جانب تعزيز آليات التعاون القضائي بين الدول، خطوة أساسية لتجاوز التحديات القانونية التي تعيق مكافحة الجريمة الإلكترونية على المستوى الدولي. إن تحقيق قدر أكبر من الانسجام في التشريعات وتسهيل الإجراءات القضائية العابرة للحدود من شأنه أن يعزز بشكل كبير قدرة المجتمع الدولي على مواجهة هذه الجرائم بفعالية.

تُعد مواءمة التشريعات الوطنية المتعلقة بالجريمة الإلكترونية خطوة حاسمة نحو تعزيز التعاون الدولي. إن وجود اختلافات جوهرية في تعريف الأفعال المجرمة بين

[1] ليلى رمضان .عقبات الوصول إلى البيانات والمعلومات .دار المعرفة، مصر، 2023، ص 115.

الدول يخلق ثغرات قانونية ويعيق التعاون في التحقيقات والملاحقات القضائية[1]. لذا، يصبح من الضروري العمل على تقريب هذه التشريعات قدر الإمكان، وتبني تعريفات مشتركة أو متقاربة للجرائم الإلكترونية الأساسية، مثل الدخول غير المصرح به، والاحتيال الإلكتروني، وإتلاف البيانات، وإساءة استخدام الأجهزة والبرامج الضارة.

إن توحيد مفاهيم التجريم يسهم بشكل كبير في تيسير التعاون القضائي. فعندما تتفق الدول على تعريف موحد لفعل معين باعتباره جريمة إلكترونية، يصبح من الأسهل تطبيق مبدأ التجريم المزدوج في طلبات المساعدة القانونية المتبادلة وتسليم المجرمين[2]. يمكن تحقيق ذلك من خلال تبني نماذج قوانين استرشادية دولية أو إقليمية، أو من خلال إبرام اتفاقيات ثنائية ومتعددة الأطراف تحدد بشكل واضح الأفعال التي تعتبر جرائم إلكترونية وتلتزم الدول الأطراف بتجريمها في قوانينها الداخلية.

يمكن تحقيق مواءمة التشريعات من خلال تبني تعريفات واسعة وشاملة للجرائم الإلكترونية التي تغطي مختلف الأنشطة الإجرامية التي تستغل التقنيات الرقمية. بدلاً من التركيز على أفعال محددة، يمكن تبني تعريفات وظيفية تستوعب التطورات المستقبلية في أساليب ارتكاب الجرائم الإلكترونية. هذا يضمن أن تظل القوانين الوطنية ذات صلة وفعالة في مواجهة التهديدات الجديدة.

علاوة على ذلك، يجب أن تشمل جهود المواءمة القوانين الإجرائية المتعلقة بالتحقيق في الجرائم الإلكترونية وجمع الأدلة الرقمية. وجود إجراءات متقاربة في هذا المجال يسهل عملية تبادل الأدلة وتقديم المساعدة القانونية المتبادلة[3]. على سبيل المثال، يمكن العمل على توحيد متطلبات إصدار أوامر التفتيش والحجز الإلكتروني والاعتراف بها عبر الحدود.

---

[1] علي الحسن .المصطلح القانوني في التعريفات الدولية .دار الفكر، سوريا، 2023، ص 99.

[2] فهد أبو زيد .التعاون الدولي في الخارج .دار الثقافة، لبنان، 2022، ص 98.

[3] محمد السالم .الاختلافات الجديدة في تنظيم التعاون .مكتبة القانون، السعودية، 2024، ص 100.

يُعد تبسيط إجراءات المساعدة القانونية المتبادلة خطوة حيوية لتعزيز التعاون الدولي في مكافحة الجريمة الإلكترونية. إن الإجراءات المعقدة والبطيئة لتبادل الأدلة الرقمية وتقديم أشكال أخرى من المساعدة القانونية غالبًا ما تعيق التحقيقات العابرة للحدود وتؤدي إلى ضياع الفرص في ملاحقة المجرمين. لذا، يصبح من الضروري العمل على تذليل العقبات القانونية والإجرائية التي تعترض هذه العملية. يمكن تحقيق ذلك من خلال تبني قنوات اتصال مباشرة وآمنة بين السلطات المختصة في الدول المختلفة، وتوحيد نماذج طلبات المساعدة القانونية، وتقليل المتطلبات الشكلية، وتسريع وتيرة الاستجابة للطلبات.

يمكن للدول أن تلجأ إلى الاتفاقيات الثنائية والمتعددة الأطراف التي تحدد إجراءات مبسطة للمساعدة القانونية المتبادلة وتسليم المجرمين في قضايا الجرائم الإلكترونية[1]. هذه الاتفاقيات يمكن أن تتضمن أحكامًا خاصة تراعي الطبيعة العابرة للحدود لهذه الجرائم والحاجة إلى تعاون سريع وفعال.

الفرع الثاني: تعزيز التعاون العملياتي وتبادل الخبرات والمعلومات وتسخير التكنولوجيا

بالإضافة إلى تطوير الأطر القانونية، يكتسب تعزيز التعاون العملياتي وتبادل الخبرات والمعلومات، إلى جانب الاستفادة القصوى من التكنولوجيا المتاحة، أهمية قصوى في مواجهة التحديات التقنية التي تواجه مكافحة الجريمة الإلكترونية على المستوى الدولي. إن تحسين التنسيق بين أجهزة إنفاذ القانون والاستخبارات، وتبادل المعرفة حول التهديدات والأساليب الإجرامية، واستخدام الأدوات التقنية المتقدمة، كلها عناصر حيوية لتعزيز قدرة المجتمع الدولي على التصدي لهذه الجرائم بفعالية.

[1] زينب العمانية .التعاون التنظيمي في الاختلافات القانونية .دار الثقافة القانونية، عمان، 2023، ص 101.

إن تعزيز التعاون العملياتي بين أجهزة إنفاذ القانون في مختلف الدول يمثل حجر الزاوية في مكافحة الجريمة الإلكترونية العابرة للحدود. يتطلب هذا التعاون إقامة قنوات اتصال فعالة ومباشرة بين الوحدات المتخصصة في مكافحة الجرائم الإلكترونية في الدول المختلفة، مما يسهل التنسيق السريع في التحقيقات المشتركة والعمليات المتزامنة. إن القدرة على العمل المشترك بشكل منسق تزيد بشكل كبير من فرص النجاح في تفكيك الشبكات الإجرامية وتقديم أعضائها للعدالة.

ولتحقيق هذا التعاون العملياتي الفعال، من الضروري تحسين قنوات الاتصال والتنسيق بين أجهزة إنفاذ القانون والاستخبارات في مختلف الدول[1]. يمكن تحقيق ذلك من خلال إنشاء نقاط اتصال مركزية تعمل على مدار الساعة، واستخدام شبكات اتصال آمنة لتبادل المعلومات الحساسة، وعقد اجتماعات دورية بين الخبراء والمتخصصين لمناقشة التحديات المشتركة وتنسيق الجهود.

كما أن تبادل المعلومات الاستخباراتية والفنية المتعلقة بالتهديدات الإلكترونية يكتسي أهمية بالغة. يجب على الدول تبادل المعلومات حول أحدث الهجمات الإلكترونية، والجهات الفاعلة الخبيثة، والثغرات الأمنية المستغلة، والأساليب الإجرامية الجديدة. إن إنشاء فرق تحقيق مشتركة تضم محققين من دول متعددة يمكن أن يكون أداة فعالة في التعامل مع الجرائم الإلكترونية المعقدة التي تمتد آثارها عبر عدة ولايات قضائية. هذه الفرق تسهل تبادل المعلومات والخبرات بشكل مباشر وتسرع وتيرة التحقيقات[2].

إن تسخير التكنولوجيا المتقدمة يمثل عنصرًا حاسمًا في تعزيز القدرة الدولية على مكافحة الجريمة الإلكترونية بفعالية، وفي مجال تعقب الجرائم الإلكترونية، يمكن الاستفادة من تقنيات تحليل حركة مرور البيانات، وأدوات تتبع عناوينIP ، وبرامج

[1] رامي العبد .تسهيل الاتصال في التعاون .دار البحث القانونية، تونس، 2023، ص 116.

[2] سامي القحطاني .تفعيل التعاون بين المنظمات الأمنية .مركز الدراسات القانونية، قطر، 2023، ص 103.

كشف التسلل، وتقنيات الذكاء الاصطناعي لتحديد الأنماط الإجرامية والكشف عن الأنشطة المشبوهة في وقت مبكر. أما في تحليل الأدلة الرقمية، فإن استخدام أدوات تحليل الطب الشرعي الرقمي المتقدمة يصبح ضروريًا للتعامل مع الكميات الكبيرة والمتنوعة من البيانات الإلكترونية.

كما أن بناء القدرات المشتركة في مجال استخدام وتطوير هذه التقنيات أمر بالغ الأهمية. يمكن للدول التعاون في إنشاء مراكز تدريب إقليمية أو دولية متخصصة في الأمن السيبراني والتحليل الجنائي الرقمي، وتبادل الخبراء والمدربين، وتطوير مناهج تدريبية موحدة لرفع مستوى مهارات العاملين في هذا المجال على مستوى العالم[1].

[1] فهد أبو زيد .تعزيز علاقات الاتصال بين الأجهزة الأمنية .دار الثقافة، لبنان، 2022، ص 99.

الخاتمة

خاتمة:

لقد سعت هذه المذكرة إلى لقد سعت هذه الدراسة إلى تسليط الضوء على التحديات والآفاق المتعلقة بالتعاون الدولي في مكافحة الجريمة الإلكترونية، وذلك من خلال استعراض الأطر القانونية والمؤسسية القائمة، وتحليل المعوقات التي تحول دون تحقيق تعاون دولي فعال، واقتراح سبل لتعزيز هذا التعاون.

لتفعيل وتطوير التعاون الدولي لمواجهة التحديات المتزايدة التي تفرضها الجريمة الإلكترونية العابرة للحدود، يتطلب الأمر معالجة متكاملة للتحديات القانونية والتقنية والعملياتية. يستلزم ذلك مواءمة التشريعات الوطنية وتوحيد مفاهيم التجريم، وتبسيط إجراءات المساعدة القانونية المتبادلة وتسليم المجرمين، وتعزيز تبادل المعلومات والخبرات بين الأجهزة الأمنية، وتسخير التكنولوجيا المتقدمة في التعقب والتحليل وبناء القدرات. إن تجاوز هذه العقبات من خلال جهود دولية منسقة هو السبيل الأمثل لمواجهة فعالة لهذه الجرائم.

النتائج :توصلت الدراسة إلى عدة نتائج رئيسية، من أبرزها:

- وجود تباين كبير في التشريعات الوطنية المتعلقة بتجريم الجرائم الإلكترونية وقواعد الاختصاص القضائي، مما يعيق التعاون القانوني.
- الطبيعة العابرة للحدود للأدلة الرقمية واستخدام تقنيات التشفير وإخفاء الهوية يمثل تحديًا تقنيًا كبيرًا أمام التحقيقات الدولية.
- على الرغم من الجهود المبذولة من قبل منظمات دولية وإقليمية مثل الإنتربول والأمم المتحدة وجامعة الدول العربية، لا يزال التعاون العملياتي وتبادل المعلومات يواجه بعض الصعوبات.

- هناك حاجة متزايدة لتسخير التكنولوجيا المتقدمة وبناء القدرات المتخصصة لتعزيز فعالية مكافحة الجريمة الإلكترونية على المستوى الدولي.

مقترحات بناءً على النتائج التي توصلت إليها الدراسة، فإنها تقترح بما يلي:

- حث الدول على بذل مزيد من الجهود لمواءمة تشريعاتها الوطنية المتعلقة بالجريمة الإلكترونية وتوحيد مفاهيم التجريم الأساسية.
- تطوير آليات دولية أكثر فعالية وسرعة لتبادل الأدلة الرقمية وتقديم المساعدة القانونية المتبادلة.
- تعزيز التعاون العملياتي بين أجهزة إنفاذ القانون والاستخبارات من خلال قنوات اتصال مباشرة وفرق تحقيق مشتركة.
- الاستثمار في تطوير وتبادل التقنيات المتقدمة المستخدمة في تعقب الجرائم الإلكترونية وتحليل الأدلة الرقمية.
- تكثيف برامج بناء القدرات المشتركة لتدريب الكوادر المتخصصة في مكافحة الجريمة الإلكترونية على المستوى الدولي والإقليمي يتم ذلك من خلال توقيع مذكرات تفاهم واتفاقيات تعاون بين الدول والمنظمات الدولية (مثل الإنتربول، واليوروبول، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة)، والمؤسسات الأكاديمية والبحثية المتخصصة في الأمن السيبراني. هذه الشراكات تهدف إلى تحديد الاحتياجات التدريبية المشتركة وتصميم برامج متكاملة تلبيها.
- تشجيع الشراكات بين القطاعين العام والخاص لتبادل المعلومات والخبرات والمساهمة في تطوير حلول مبتكرة لمكافحة الجريمة الإلكترونية.

قائمة المصادر والمراجع

قائمة المصادر و المراجع:

قائمة المراجع

الكتب باللغة العربية:

1. هالة الأنصاري، تطور التشريعات في مواجهة الجريمة الإلكترونية، مكتبة الأفق، البحرين، 2020.
2. فاطمة القاسمي، تحديد الجريمة الإلكترونية في التشريعات العربية، دار الفكر، الأردن، 2019.
3. نوال الشرفي، تحديات التعاون الدولي في مجال الجرائم الإلكترونية، مكتبة الأفق، الكويت، 2019.
4. عمر الفقي، مسؤولية مرتكبي الجرائم الإلكترونية: النية والضرر، دار المعرفة، مصر، 2022.
5. عز الدين القاسمي، تحديات التعاون الدولي في مواجهة الجرائم العابرة للحدود، دار المعرفة، مصر، 2022.
6. الزهراني منى، تحديات احتواء الجرائم الإلكترونية، دار الكتاب العربي، بيروت، 2023.
7. الغامدي أحمد، الجرائم الإلكترونية: دراسة مقارنة، دار الكتاب الحديث، القاهرة، 2020.
8. الهاشمي علي، التنمر الإلكتروني: الأسباب والآثار والعلاج، مركز الكتاب الأكاديمي، عمان، 2020.
9. محمود سامي، الجرائم الإلكترونية: المخاطر والحلول، دار الفكر العربي، مصر،2022.

10. المسعودي هالة، الجرائم الإلكترونية وتأثيرها على الاقتصاد العالمي، دار العلوم، الرياض، 2022.

11. النجار فاطمة، الجرائم الإلكترونية: المخاطر والتحديات، دار الكتاب الجامعي، عمان، 2020.

12. وسام الدين محمد العكلة، التعاون الدولي في مواجهة جرائم الإنترنت، جامعة بغداد، العراق،2012.

13. الزيات محمود، التعاون القضائي الدولي في المسائل الجنائية، دار النهضة العربية، القاهرة، 2023.

14. محمود سامي، الجرائم الإلكترونية والأنظمة القانونية: تحليل عميق، دار الفكر العربي، مصر،2022.

15. العلوي محمد، الاتفاقيات الثنائية في مجال حقوق الإنسان، دار النهضة العربية، بيروت، 2021.

16. عمر سامي، الجرائم الإلكترونية: التحديات العابرة للحدود وسبل المواجهة، دار المعرفة، مصر،2022.

17. منى فريد، تطوير القوانين لمكافحة الجرائم الإلكترونية: دور الدول المتقدمة، مركز الدراسات الأمنية، 2022.

18. انيا خالد، التعاون الدولي لمكافحة الجرائم الإلكترونية: اتفاقية بودابست كنموذج، جامعة الملك سعود، 2024.

19. جمال حمد، تطوير البنية التحتية لمكافحة الجرائم الإلكترونية: دور الاتحاد الأوروبي، دار الفكر العربي، 2022.

20. علي كمال، القوانين الداخلية ومكافحة الجرائم الإلكترونية: تحديات وآفاق، دار الفكر العربي، لبنان، 2022.

21. سارة جاد، الاختلافات في التجريم وتأثيرها على التعاون الدولي، الأمن السيبراني: التحديات والحلول، دار المعرفة، الإمارات، 2021.

22. سمير طه، قيود البيانات وتأثيرها على التعاون الدولي، مكافحة الجرائم الإلكترونية: الأبعاد القانونية، دار المعرفة، الكويت، 2023.

23. رفعت ناصر، دور الإنتربول في مكافحة الجرائم العابرة للحدود، الأمن السيبراني: التحديات العالمية، مكتبة الأفق، مصر، 2023.

24. جمال حمد، الآليات اللوجستية للإنتربول في مكافحة الجرائم الإلكترونية، الأمن السيبراني: المفاهيم والتطبيقات، دار الفكر العربي، لبنان، 2022.

25. رفعت ناصر، دور الإنتربول في تدريب الكوادر الأمنية، الأمن السيبراني: التحديات العالمية، مكتبة الأفق، مصر، 2023.

26. سمير طه، استراتيجيات التعاون الإقليمي في مواجهة الجرائم الإلكترونية، دار المعرفة، الكويت، 2021.

27. جمال حمد، التنسيق الأمني بين الدول العربية: دراسة تحليلية، جامعة الإسكندرية، 2023.

28. فاطمة محمود، التدريب الأمني في مواجهة الجرائم الإلكترونية: المفاهيم والتطبيقات، مكتبة النهضة، مصر، 2022.

29. مروان بن عزيز. اختلاف تأثير التجريم على التعاون .دار البحث القانونية، تونس، 2023.

30. ليلى الفهيد. التعاون بين أجهزة مكافحة الجريمة .مكتبة القانون، الإمارات، 2024.

31. يوسف الخليل. سلامة الأدلة الرقمية .دار الثقافة، لبنان، 2022.

32. عادل الفارس. تحديات الأدلة الرقمية في الفايروس. دار البحث القانونية، تونس، 2023.

33. سمر العلي. الأدلة الرقمية والجرائم الإلكترونية . مكتبة القانون، الإمارات، 2024.

34. ليلى رمضان. عقبات الوصول إلى البيانات والمعلومات . دار المعرفة، مصر، 2023.

35. علي الحسن. المصطلح القانوني في التعريفات الدولية . دار الفكر، سوريا، 2023.

36. فهد أبو زيد. التعاون الدولي في الخارج .دار الثقافة، لبنان، 2022.

37. محمد السالم. الاختلافات الجديدة في تنظيم التعاون . مكتبة القانون، السعودية، 2024.

38. زينب العمانية.التعاون التنظيمي في الاختلافات القانونية . دار الثقافة القانونية، عمان، 2023.

39. رامي العبد. تسهيل الاتصال في التعاون .دار البحث القانونية، تونس، 2023.

40. سامي القحطاني.تفعيل التعاون بين المنظمات الأمنية . مركز الدراسات القانونية، قطر، 2023.

41. فهد أبو زيد. تعزيز علاقات الاتصال بين الأجهزة الأمنية . دار الثقافة، لبنان، 2022.

الكتاب باللغة الإنجليزية:

1. Smith, Robert. Democracy and Citizen Participation: A Global Perspective. Cambridge University Press, United Kingdom, 2020.

المواقع الإلكترونية:

1. "الجرائم الرقمية"، دليل الحماية من الاختراقات الإلكترونية، 2022، https://www.digitalcrimesguide.com،]تم الاطلاع عليه في 28 أبريل 2025، الساعة 14:30 بتوقيت الجزائر.

2. "الجرائم الرقمية"، دليل الحماية من الاختراقات الإلكترونية، 2022، [https://www.digitalcrimesguide.com]،[تم الاطلاع عليه في 28 أبريل 2025، الساعة 14:30 بتوقيت الجزائر

الأطروحات والرسائل الجامعية

1. الخالدي فاطمة، "تحليل دور وسائل الإعلام في رفع مستوى الوعي بمخاطر الجرائم الإلكترونية في دولة الإمارات العربية المتحدة: دراسة إحصائية"، جامعة الإمارات العربية المتحدة، 2022.

2. علي حسن، الاحتيال عبر الإنترنت: دراسة تحليلية في دول الشرق الأوسط، رسالة ماجستير، جامعة التكنولوجيا، 2023، الأردن، 2023.

3. أحمد طالب، استراتيجيات فعالة لمكافحة الجرائم الإلكترونية: التحديات والفرص، أطروحة دكتوراه، جامعة القاهرة، 2023، مصر.

4. سعيد عماد، التعاون الإقليمي في مواجهة الجرائم الإلكترونية: دراسة تحليلية، أطروحة دكتوراه، جامعة الأردن، 2022.

5. علي عمر، أحكام اتفاقية بودابست ودورها في مكافحة الجرائم الإلكترونية، أطروحة دكتوراه، جامعة الإسكندرية، 2023.

6. أحمد سعيد، القرارات الدولية لمكافحة الجريمة الإلكترونية: تحليل شامل، أطروحة ماجستير، جامعة البحرين، 2023.

7. كريم عامر، استغلال الأطفال عبر الإنترنت: التوجيهات الأوروبية كحل، أطروحة ماجستير، جامعة ليون، 2023.

المقالات في الدوريات:

1. الرشيدي فهد، "دور شبكات الخبراء في تبادل المعلومات حول التهديدات السيبرانية"، مجلة تقنية المعلومات، تونس، العدد 21، 2022.

2. نجلاء فؤاد، "استراتيجيات تسليم المجرمين في إطار الجرائم المنظمة"، مجلة الدراسات القانونية،المملكة العربية السعودية، العدد 9، 2023.

3. رفعت ناصر، "التفاعل بين التشريعات الوطنية والاتفاقيات الدولية في مكافحة الجرائم الإلكترونية"، مجلة الدراسات الأمنية،الاردن، العدد 5، 2023.

فهرس المحتويات

فهرس المحتويات

ملخص:

تُركز هذه المذكرة على تحليل التعاون الدولي لمكافحة الجريمة الإلكترونية، التي تُمثّل تحديًا عابرًا للحدود في ظل التوسع الرقمي المتسارع. تهدف الدراسة إلى استكشاف الدور الحيوي لهذا التعاون، وتحديد أبرز العقبات التي تواجهه، واقتراح آليات لتعزيز فعاليته، مع إيلاء اهتمام خاص لواقع الجزائر. تنطلق الدراسة من تساؤل محوري حول فاعلية التعاون الدولي في التصدي للجريمة الإلكترونية وتحدياته وسبل تطويره في السياق الجزائري. وللإجابة على ذلك، تتناول المذكرة محاور فرعية تشمل الإطار المفاهيمي للجريمة الإلكترونية وأنواعها، ومفهوم التعاون الدولي وأهميته وأشكاله، بالإضافة إلى تحليل الأطر القانونية والمؤسساتية الدولية والإقليمية ذات الصلة وموقع الجزائر ضمنها. كما تُسلّط الضوء على التحديات القانونية، التقنية، السياسية، والاقتصادية التي تعترض هذا التعاون، وتُقدم سبلًا لتعزيزه من خلال دور التشريعات الوطنية، المنظمات الدولية، والقطاع الخاص. تُقسّم المذكرة إلى ثلاثة فصول رئيسية: يتناول الفصل الأول الإطار النظري للجريمة الإلكترونية والتعاون الدولي، ويُخصص الفصل الثاني للأطر القانونية والمؤسساتية للتعاون الدولي مع التركيز على الحالة الجزائرية. أما الفصل الثالث، فيُعالج التحديات القائمة ويُقدم سبلًا لتعزيز هذا التعاون في سياق الجزائر. تُختتم المذكرة بمجموعة من النتائج المستخلصة والتوصيات الهادفة.

الكلمات المفتاحية: الجريمة الإلكترونية، مكافحة الجريمة الإلكترونية، التعاون الدولي.

Abstract

This dissertation focuses on analyzing **international cooperation in combating cybercrime**, a cross-border challenge amplified by rapid digital expansion. The study aims to explore the vital role of this cooperation, identify its main obstacles, and propose mechanisms to enhance its effectiveness, with a particular focus on **Algeria's context**. The study is driven by a central question regarding the effectiveness of international cooperation in addressing cybercrime, its challenges, and avenues for its development within the Algerian context. To answer this, the dissertation covers sub-topics including the conceptual framework of cybercrime and its types, the concept of international cooperation, its importance and forms, as well as an analysis of relevant international and regional legal and institutional frameworks and Algeria's position within them. It also highlights the legal, technical, political, and economic challenges hindering this cooperation and offers ways to strengthen it through the role of national legislations, international organizations, and the private sector.

The dissertation is divided into three main chapters: The first chapter addresses the theoretical framework of cybercrime and international cooperation. The second chapter is dedicated to the legal and institutional frameworks of international cooperation, with a focus on the Algerian case. The third chapter tackles existing challenges and proposes ways to enhance this cooperation within Algeria's context. The dissertation concludes with a set of findings and targeted recommendations.

Keywords: cybercrime, combating cybercrime, international cooperation.