جامعة النجاح الوطنية
كليَّة الدّراسات العليا

إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية

إعداد
ليث علام سعيد موسى

اشراف
د. عمر بزور

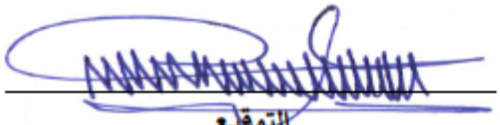
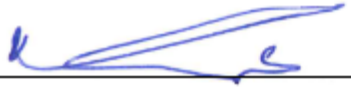
قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، من كلية الدراسات العليا في جامعة النجاح الوطنية، نابلس– فلسطين.
2025

إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية

إعداد

ليث علام سعيد موسى

نوقشت هذه الرسالة بتاريخ 2025/06/30م، وأجيزت:

د. عمر بزور	
المشرف الرئيسي	التوقيع
د. مرسي عبد الرازق	
المشرف الخارجي	التوقيع
د. عبد القادر العزة	
المشرف الداخلي	التوقيع

الإهداء

أهدي هذا العمل المتواضع إلى:

إلى من كان لي سنداً وعوناً عند الشدائد طوال عمري، إلى الرجل الأبرز في حياتي،،

أبي العزيز

إلى القلب المعطاء والصدر الحاني،،

أمي الحبيبة

إلى من شد الله بهم عضدي فكانوا خير معين،،

إخواني وأخواتي

إلى كل من ساعدني ولو بحرف في حياتي الدراسية،،

إلى زوجتي الحبيبة،،

وإبني الحبيب جواد،،

إلى هؤلاء جميعاً: أهديكم هذا العمل

الباحث

الشكر والتقدير

الحمد لله تعالى الذي أفاض عليّ من نعمته، وهداني لأســـلك طريق العلم، وأحمده حمداً كما ينبغي لجلال وجهه وعظيم سلطانه.

أمّا بعد:

أتوجّه بالشكر وعظيم الامتنان إلى كل من:

الدكتور الفاضـل **عمر بزور**؛ لتفضّـله بالاشـراف على هذه الدراسـة، وتكرّمه بنصـحي وتوجيهي حتى إتمام الدراسة.

أعضاء لجنة المناقشة السادة الدكتور **مرسي عبد الرازق** والدكتور **عبد القادر العزة**، لتفضلهم بقبول مناقشة هذه الدراسة.

ولكل من ساعد في إتمام هذه الدراسة، وقدم لي يد العون والمساعدة، فكلّ الشكر والتقدير لجامعة النجاح الوطنية متمثّلة بعمادة الدراسات العليا، التي أتاحت لي إكمال دراستي الجامعية العليا.

وكل الشكر لجميع زملائي وزميلاتي في النيابة العامة.

فجزاكم الله جميعا خير الجزاء

الباحث

الإقرار

أنا الموقع أدناه، مقدم الرسالة التي تحمل العنوان:

إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية

أقر بأن ما اشتملت عليه هذه الرسالة هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة اليه حيثما ورد، وأن هذه الرسـالة ككل أو أي جزء منها لم يقدم من قبل لنيل أية درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: **ليث علام سعيد موسى**

التوقيع:

التاريخ: **2025/06/30**

فهرس المحتويات

الإهداء ..... ج

الشكر والتقدير ..... د

الإقرار ..... هـ

فهرس المحتويات ..... و

الملخص ..... ط

الفصل الاول: مقدمة الدراسة 1

مشكلة الدراسة 2

أهداف الدراسة 3

أهمية الدراسة 3

منهج الدراسة 4

محددات الدراسة 4

الدراسات السابقة وأدبيات الدراسة 5

خطة الدراسة 5

مصطلحات الدراسة 6

الفصل الثاني: ماهية التعاون الدولي في مواجهة الجرائم الإلكترونية 7

المبحث الأول: الإطار المفاهيمي للتعاون الدولي 8

المطلب الأول: مفهوم التعاون الدولي 8

الفرع الأول: تعريف التعاون الدولي: 8

الفرع الثاني: مبررات التعاون الدولي 11

المطلب الثاني: مفهوم الجريمة الإلكترونية 12

الفرع الأول: تعريف الجريمة الإلكترونية وطبيعتها القانونية: 13

الفرع الثاني: خصائص وأركان الجريمة الإلكترونية 15

المبحث الثاني: أساليب التعاون الدولي في مواجهة الجرائم الإلكترونية 20

المطلب الأول: أوجه التعاون الدولي في مواجهة الجرائم الإلكترونية 20
الفرع الأول: التعاون الأمني في مواجهة الجرائم الإلكترونية.....20
الفرع الثاني: التعاون القضائي في مواجهة الجرائم الإلكترونية.....25
الفرع الثالث: التعاون الدولي بشأن تسليم المجرمين لمواجهة الجرائم الإلكترونية 29
المطلب الثاني: دور الهيئات والمنظمات في تفعيل التعاون الدولي.....32
الفرع الأول: الهيئات والمنظمات الدولية 32
الفرع الثاني: الاتفاقيات والمعاهدات الدولية 34
الفصل الثالث: إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية وآليات التغلب عليها 36
المبحث الأول: إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الدولي والوطني .36
المطلب الأول: إشكاليات التعاون الدولي على المستوى الدولي: 36
الفرع الأول: القصور التشريعي للدول والتعارض بين مصالحها 37
الفرع الثاني: اختلاف النظم القانونية الإجرائية وتنوعها 38
الفرع الثالث: تنازع الاختصاص القضائي الدولي 38
الفرع الرابع: الإشكاليات المتعلقة بتسليم المجرمين 39
الفرع الخامس: الإشكاليات المتعلقة بالإنابة القضائية 42
الفرع السادس: الإشكاليات المتعلقة بالتدريب في مجال مواجهة الجرائم الإلكترونية 43
المطلب الثاني: إشكاليات التعاون الدولي على المستوى الوطني.....44
الفرع الأول: عدم كفاية القوانين الجزائية الداخلية وعدم ملائمتها 45
الفرع الثاني: صعوبة اكتشاف الجرائم الإلكترونية وإثباتها 45
الفرع الثالث: تناقض القوانين المطبقة في فلسطين.....48
المبحث الثاني: آليات التغلب على إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الوطني والدولي.....49
المطلب الأول: آليات التغلب على إشكاليات التعاون الدولي على المستوى الدولي.....50
الفرع الأول: آلية التغلب على إشكالية القصور التشريعي للدول والتعارض بين مصالحها وتنوع اختلاف النظم القانونية 50

الفرع الثاني: آلية التغلب على إشكالية تنازع الإختصاص القضائي الدولي 52
الفرع الثالث: آلية التغلب على الإشكاليات المتعلقة بتسليم المجرمين.....53
الفرع الرابع: آلية التغلب على الإشكاليات المتعلقة بالإنابة القضائية 54
الفرع الخامس: آلية التغلب على الإشكالية المتعلقة بالتدريب على مواجهة الجرائم الإلكترونية 55
المطلب الثاني: آليات التغلب على إشكاليات التعاون الدولي على المستوى الوطني 56
الفرع الأول: التدابير الموضوعية كآلية للتغلب على إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية 56
الفرع الثاني: التدابير الإجرائية كآلية للتغلب على إشكالية التعاون الدولي في مواجهة الجرائم الإلكترونية57
الفصل الرابع: الخاتمة والنتائج والتوصيات 59
الخاتمة.....59
النتائج.....60
التوصيات 61
المصادر والمراجع 62
Abstract.....b

إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية

إعداد

ليث علام سعيد موسى

اشراف

د. عمر بزور

الملخص

تهدف هذه الدراسة إلى تسليط الضوء على إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية، باعتبارها جرائم عابرة للحدود تتطلب تنسيقًا دوليًا فعالًا على المستويين القانوني والتقني. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي والمهج المقارن، من خلال تحليل الإطار القانوني الدولي والوطني، واستعراض أبرز الاتفاقيات الدولية ذات الصلة، مثل اتفاقية بودابست، إلى جانب دراسة واقع التشريع الفلسطيني في هذا المجال..

توصلت الدراسة إلى أن التعاون الدولي لا يزال يواجه تحديات كبيرة، من أبرزها: تضارب التشريعات، غياب الثقة السياسية، ضعف البنية التحتية التقنية في بعض الدول، وبطء الإجراءات القضائية. عدم تفعيل الانابة القضائبة الدولية، كما كشفت الدراسة عن محدودية انخراط فلسطين في الأطر الدولية الفاعلة لمكافحة الجرائم الإلكترونية، وأوصت الدراسة بضرورة مواءمة التشريعات الوطنية مع المعايير الدولية، وتوسيع نطاق الاتفاقيات الثنائية والمتعددة الأطراف، وتعزيز القدرات الوطنية في مجال التحقيق الرقمي، إلى جانب إنشاء آليات تنسيق إقليمية فعالة.

تسهم هذه الدراسة في إثراء النقاش القانوني حول سبل تطوير التعاون الدولي لمواجهة التحديات المتزايدة التي تفرضها الجرائم الإلكترونية على الأمن الوطني والدولي.

الكلمات المفتاحية: الجريمة الإلكترونية، التعاون الدولي، التجريم المزدوج، تسليم المجرمين، اتفاقية بودابست، إنفاذ القانون عبر الحدود، التعاون القضائي الدولي، الهجوم السيبراني، بالإنابة القضائية، طلبات التسليم.

الفصل الاول

مقدمة الدراسة

إن الحمد لله نحمده ونستعينه ونستهديه ونستغفره ونعوذ بالله من شرور أنفسنا ومن سيئات أعمالنا، والصلاة والسلام على نبينا محمد ﷺ وعلى آله وصحبه أجمعين، أما بعد...

سعى الإنسان منذ وجوده إلى التطور والتقدم في جميع مجالات الحياة؛ لتلبية حاجياته، وتسهيل ممارساته اليومية سواء على المستوى الشخصي، أو على المستوى العملي، ويعد التطور التكنولوجي من أبرز التطورات التي حققها الإنسان مقارنة بالمجالات الحياتية الأخرى، حيث نجد أن أغلب القطاعات والمجالات الأخرى أصبحت تعتمد بشكل كبير ومباشر على استخدام التكنولوجيا في إتمام وتسهيل أعمالها، فقد جلب هذا التطور لحياة الإنسان العديد من المزايا، كالوصول إلى المعلومات بسهولة ويسر، وتقصير المسافات وتقليل تكاليف وأعباء الاتصال والتواصل، كونه يُقَدم للمستخدم بمقابل مادي رمزي، حيث تكاد تكون شبه مجانية، إلا أنه قد رافقه في ذات الوقت انحراف في التعامل، وإساءة استخدامه، واستغلاله في ارتكاب الأفعال التي تعد مجرمة في العالم الواقعي، فأصبحت مجالاً لحصول الانتهاكات والمخالفات، مما أدى إلى ظهور جرائم مستحدثة مرتبطة في العالم الرقمي تسمى بالجرائم الإلكترونية، حيث انتشرت في الآونة الأخيرة بمختلف أشكالها وصورها نتيجة سهولة ارتكابها، وسرعة وتيرتها.

وكون أن العالم الافتراضي لا يعترف بالحدود الجغرافية أو المسافات ما بين الدول، فقد أدى هذا إلى اتساع مسرح الجرائم الإلكترونية إلى دول متعددة، وسهولة هروب الفاعل وتخفيه وراء أجهزة التكنولوجيا، حيث ساعدت مرتكب الجريمة في تجاوز العوائق التي قد تعيقه في ارتكابه لهذه الأفعال على أرض الواقع، وقد أدى عجز الدول بمفردها على مواجهة هذه الجرائم، وقصور التشريعات الوطنية في مواجهتها، ومدى انتشارها في الآونة الأخيرة وزيادة مخاطرها إلى البحث نحو التعاون الدولي في التصدي لتلك الجرائم، كونها أصبحت تمثل خطراً يهدد الاستقرار الدولي والأمن الداخلي للدول.

ولذلك أتناول في هذه الدراســـة مواجهة الجرائم الإلكترونية وفقاً للقوانين الدولية، والتحديات التي قد تعيق تطبيق هذه المواجهة، وذلك تحت عنوان: " **إشـــكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية"**، وذلك من خلال توضيح التعاون الدولي في مواجهة هذا النوع من الجرائم، وإشكاليات تنفيذه، ومدى إمكانية إيجاد حلول مناسبة لها.

مشكلة الدراسة

نظراً لإنتشار الجرائم الإلكترونية في الآونة الأخيرة، مواكبةً للتطور التكنولوجي السريع والمستمر، وسهولة اســـتخدامه، وقلة تكلفته، وعجز الدول في مواجهة هذه الجرائم؛ لاتســـاع مكانها الجغرافي، فهي ليســـت خاضعة لحدود جغرافية أو مكانية معينة، بل هي تصل إلى العالم بأسره بسرعة الضوء؛ كما أن التشريعات الوطنية لم تواكب التطور المســـتمر لتلك التكنولوجيا، مما دفعت الحاجة إلى ضـــرورة وجود تعاون دولي لمواجهة ومكافحة الجرائم الإلكترونية، فإن مشكلة الدراسة الرئيسية تكمن في الإجابة على التساؤل التالي:

كيف تؤثر التحديات القانونية والتقنية والســـيادية على فعالية التعاون الدولي في مكافحة الجرائم الإلكترونية عابرة الحدود؟

وللإجابة على هذا التساؤل لابد من الإجابة على مجموعةٍ من التساؤلات الفرعية؛ لذا ستجيب الدراسة على التساؤلات التالية:

1. ما مدى تباين التشريعات بين الدول في تعريف وتجريم الجرائم الإلكترونية؟
2. إلى أي حد تساهم الاتفاقيات الدولية الحالية (مثل بودابست) في تعزيز التنسيق بين الأجهزة المختصة؟
3. كيف تؤثر مصالح الدول الكبرى في توجيه أو تقييد آليات التعاون؟

أهداف الدراسة

هذه الرسالة تهدف إلى تسليط الضوء على الفجوات في التنسيق الدولي، مثل اختلاف التشريعات، وصعوبة تعقّب الجناة عبر الحدود، وضـعف تبادل المعلومات بين الدول، مع تقديم رؤية نقدية وحلول ممكنة لتجاوز هذه العقبات.

لذلك تهدف هذه الدراســـة إلى تحليل أبرز الإشـــكاليات التي تواجه التعاون الدولي في مكافحة الجرائم الإلكترونية، من خلال دراسة الأبعاد القانونية والتقنية والسياسية، واقتراح آليات لتعزيز فعالية الجهود الدولية في هذا المجال.

من الأهداف الرئيسية العلمية التي تسعى هذه الرسالة تحقيقها كالتالي:

1. تحليل التحديات القانونية المرتبطة بتباين التشريعات بين الدول في مجال الجرائم الإلكترونية.
2. دراسة الإشكالات التقنية التي تعوق تبادل المعلومات والأدلة الرقمية بين الجهات المختصة دوليًا.
3. تقييم دور الاتفاقيات الدولية، مثل اتفاقية بودابست، في تعزيز أو تقويض التعاون الدولي.
4. رصد تأثير الاعتبارات السياسية والسيادية على فعالية التعاون بين الدول في مجال الأمن السيبراني.
5. اقتراح آليات عملية لتعزيز التنسيق والتعاون العابر للحدود لمواجهة الجرائم الإلكترونية.

أهمية الدراسة

يمكن تلخيص أهمية هذه الدراسة بالتركيز على جانبين على النحو التالي:

الأهمية العلمية:

تنبع أهمية الدراسة في المستوى العلمي نظراً لإرتباطها بأكثر الجرائم انتشاراً في الآونة الأخيرة، وهي الجرائم الإلكترونية، حيث أدى التطور التكنولوجي إلى تســـهيل الطريق أمام ضـــعيفي النفوس في ارتكاب الجرائم

والانتهاكات باستغلال التقنيات الحديثة، وقد أدى اتساع مسرح الجريمة الإلكترونية إلى تعزيز التعاون الدولي لمواجهة هذه الجرائم، لذا فلا بد من معرفة مدى التعاون الدولي في مجال مواجهة الجرائم الإلكترونية، ومدى تطبيق قواعد القانون الدولي في مواجهة الجرائم الإلكترونية على أرض الواقع، والإشكاليات التي قد تواجهها، وتوفير مادة بحثية للقارئ تتعلق بموضوع هذه الدراسة.

الأهمية العملية:

تنبع الأهمية العملية لموضوع هذه الدراسة في البحث حول إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية، ومحاولة إيجاد حلول مناسبة لها، من أجل ضمان مواجهة هذه الجرائم، وتقليل نسبتها بأكبر قدرٍ ممكن من خلال تطبيق القانون على مرتكبها، وتحقيق الردع العام.

منهج الدراسة

سيتبع الباحث في هذه الدراسة أُسلوب البحث العلمي القائم على المنهج الوصفي والمنهج التحليلي الاستنباطي والاستقرائي من خلال التطرق إلى المفاهيم والتعريفات للمصطلحات الأساسية في موضوع الدراسة، وتحليل نصوص القوانين الدولية المتعلقة بمواجهة الجرائم الإلكترونية، حيث يعد المنهج الوصفي التحليلي هو المنهج الأكثر ملائمة في دراسة الظواهر الإجتماعية والقانونية، ومنها مواجهة الجرائم الإلكترونية في إطار القانون الدولي، وإشكاليات تطبيقها، وكذلك سيتبع الباحث المنهج المقارن اينما لزم ذلك في سياق هذه الدراسة.

محددات الدراسة

يتحدد الإطار القانوني في القوانين الدولية، والمحلية المتعلقة بمواجهة الجرائم بشكل عام، ومواجهة الجرائم الإلكترونية بشكل خاص، كقرارات الأمم المتحدة، ومؤتمراتها، والاتفاقيات المنعقدة بين الدول التي تساعد في مواجهة هذه الجرائم، بالإضافة إلى أية قوانين أو اتفاقيات دولية قد تكون ذات صلة بموضوع الدراسة.

الدراسات السابقة وأدبيات الدراسة

1. **عاصـــف جودت النجاجرة، المواجهة القضـــائية الدولية للجرائم الإلكترونية وفقاً لأحكام التشـــريع الفلسطيني" المجلة القانونية عدد 4 2025،** والتي ركزت على فعالية التشريع الفلسطيني في تسهيل التعاون القضائي الدولي، وتسليم المجرمين، والصعوبات التي تواجه هذا التعاون.
2. **محمد باسم الخالدي، مكافحة الجريمة الإلكترونية في ظل التشريع الفلسطيني والاتفاقيات الدولية، الجامعة العربية الأمريكية، 2025، والتي ركزت على** مواءمة التشـــريع الفلســـطيني مع الاتفاقيات الدولية، الإثبات الإلكتروني، الإجراءات القانونية.
3. **التعاون الدولي في مواجهة الجريمة الإلكترونية "عمايرة طه محمد منذر (2023)، الجهة :**جامعة القدس.، **المنهج:** وصـفي تحليلي. **أبرز المحاور:** التشـريعات الفلسـطينية، الاتفاقيات الدولية، آليات التعاون الأمني والقضائي، التحديات التي تعيق التعاون.

خطة الدراسة

تم تقسيم الدراسة الى فصلين:

الفصل الأول: ماهية التعاون الدولي في مواجهة الجرائم الإلكترونية.

المبحث الأول: الإطار المفاهيمي للتعاون الدولي في مواجهة الجرائم الإلكترونية.

المطلب الأول: مفهوم التعاون الدولي.

المطلب الثاني: مفهوم الجرائم الإلكترونية.

المبحث الثاني: أساليب التعاون الدولي في مواجهة الجرائم الإلكترونية.

المطلب الأول: أوجه التعاون الدولي في مواجهة الجرائم الإلكترونية.

المطلب الثاني: دور الهيئات والمنظمات في تفعيل التعاون الدولي.

الفصل الثاني: إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية وآليات التغلب عليها.

المبحث الأول: إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الدولي والوطني.

المطلب الأول: إشكاليات التعاون الدولي على المستوى الدولي.

المطلب الثاني: إشكاليات التعاون الدولي على المستوى الوطني.

المبحث الثاني: آليات التغلب على إشـــكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الدولي والوطني.

المطلب الأول: آليات التغلب على إشكاليات التعاون الدولي على المستوى الدولي.

المطلب الثاني: آليات التغلب على إشكاليات التعاون الدولي على المستوى الوطني.

(الخاتمة) النتائج والتوصيات.

مصطلحات الدراسة

الجرائم الإلكترونية: تعرّف دولياً على أنها: أعمال متعلقة بالكمبيوتر لتحقق مكاسب شخصية أو مالية أو ضـــرر تلحقه بالغير، بما في ذلك أشـــكال الأفعال المتصـــلة بجريمة الهوية، وجرائم محتويات الكمبيوتر (البداينة، 2014).

التعاون الدولي في مواجهة الجرائم: هو ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم، وذلك من خلال تدابير وقائية تستهدف الصيغة غير الوطنية للجريمة، وتســتجمع الأدلة بمختلف الطرق، وهو ما يســتغرق وقتاً، ويتطلب إمكانيات لا تملكها ســلطات قانونية لدولة واحدة، ما لم تدعمها وتساندها جهود السلطات القانونية في الدول الأخرى، والذي يتجسد في التعاون الدولي (الأوجلي، 1997).

الفصل الثاني

ماهية التعاون الدولي في مواجهة الجرائم الإلكترونية

شهد العالم في الآونة الأخيرة قوة افتراضية لا يستهان بها عرفت بالثورة التكنولوجية، حيث انتشرت بشكل واسع بين الأفراد، وقد برزت عنها إيجابيات متعددة في جميع مجالات الحياة، فالكثير من القطاعات المختلفة اعتمدت في أداء أعمالها بشكل أساسي على استخدام الإنترنت؛ لسرعته، ودقته في جمع المعلومات عدا عن تكلفته التي تكاد تكون شبه مجانية مقارنةً بالخدمة التي يقدمها للمستخدمين، مما جعل العالم أشبه بالقرية الصغيرة حيث لا حدود بين أحيائها.

إلا أنه وبالرغم من هذه الإيجابيات لا يمكن غض الطرف عن السلبيات التي نجمت من العالم التكنولوجي شأنه شأن كافة الأمور المستحدثة التي تشكل سيف ذو حدين، ففي ظل هذه الثورة التكنولوجية المتسارعة والتوسع الهائل في استخدام الإنترنت ظهرت أنماط من الجرائم المستحدثة نتيجة سوء استخدام الأنظمة المتعلقة بتكنولوجيا المعلومات، واستغلالها في تحقيق مصالح شخصية بالإضرار بالغير، وهي ما تسمى بالجرائم الإلكترونية.

وقد أصبحت هذه الجرائم من أكبر التحديات التي تواجه المجتمع المحلي، ومن ثم المجتمع الدولي كونها لا تعترف بالحدود الجغرافية، فالآثار الناجمة عنها لا تقف عند حدود الدولة الواحدة بل تمتد؛ لتمثل عدة دول مختلفة؛ مما يجعل مكافحتها مسؤولية جماعية تتطلب تعاوناً دولياً لمواجهتها والقضاء عليها؛ لذا يتناول هذا الفصل الإطار المفاهيمي للتعاون الدولي في المبحث الأول منه، ويتناول في المبحث الثاني أساليب التعاون الدول.

المبحث الأول: الإطار المفاهيمي للتعاون الدولي

بات التعاون الدولي ضـرورة حتمية وملحة في مواجهة التحديات المسـتحدثة الناجمة عن الثورة التكنولوجية العابرة للحدود، والتي أصبحت تستخدم في جميع مجالات الحياة، وخاصة مع وجود تعقيد وكثرة في القضايا العالمية المرتبطة بهذه الثورة، فكان لا بد من تعاون دولي تبذل الدول جهودها؛ لمواجهة هذه القضـــايا، والتقييد من حدوثها بأكبر قدر ممكن؛ ولمعرفة المعنى المراد من كل من التعاون الدولي والجريمة الإلكترونية؛ لإفهام القارئ المعنى المراد منهما في سـياق هذه الدراسـة؛ لذا جاء هذا المبحث يتناول مفهوم التعاون الدولي في المطلب الأول منه، ويتناول المطلب الثاني مفهوم الجرائم الإلكترونية على النحو التالي:

المطلب الأول: مفهوم التعاون الدولي

يتناول هذا المطلب تعريف التعاون في الفرع الأول منه، ويتناول الفرع الثاني منه مبررات التعاون الدولي على النحو التالي:

الفرع الأول: تعريف التعاون الدولي:

يتناول هذا الفرع تعريف التعاون الدولي لغةً واصطلاحاً وقانوناً على النحو التالي:

أولاً: تعريف التعاون لغةً: تعاون هي: فعل من كلمة عَوْنْ وَيُقْصَـد بِها: أَنّ الْقَوْم عَاوَنَ بَعْضِـهِم بَعضَـاً، فهي تقوم على تبادل المعاونة فيما بينهم (نخبة من اللغويين بمجمع اللغة العربية، 1972).

ويقصد به: التساعد أي أن يعين الناس بعضهم بعضاً، وهو أمر واجب فيما يجب، ومستحب فيما يستحب، فقد حث الإسـلام على التعاون بين الأفراد؛ لحل المشـكلات، وتحسـين أحوالهم المختلفة، وهذا ما جاء في القرآن الكريم: قوله تعالى: ﴿ وَتَعَاوَنُواْ عَلَى ٱلۡبِرِّ وَٱلتَّقۡوَىٰۖ ﴾[المائدة: 2] (العثيمين، 2020).

وقول النبي صلى الله عليه وسلم: "والله في عون العبد ما كان العبد في عون أخيه" (أبو الحسين، 1955)، وهذا ما يوضـــح المعنى العام للتعاون والقائم على تبادل المســاعدة بين مجموعات مختلفة؛ لتحقيق أهداف

وغايات مشتركة فيما بينهم، مما يؤكد السبب الذي خلق الله تعالى الناس مختلفين؛ ليكملوا بعضهم البعض، فلا يستطيع الإنسان لوحده أن يلبي جميع احتياجاته دون الاستعانة بأحد، بل هو بحاجة إلى الآخرين لإمكانية سد حاجياته الضرورية؛ لبقائه على قيد الحياة واستمراريتها بشكل طبيعي، فالاختلاف كان رحمة من الله بسكان الأرض، فالتكامل بينهم سهّل عليهم تحقيق إعمار الأرض، والذي فرضه الله تعالى على جميع خلقه (طبنجة، 2022).

ثانياً: تعريف التعاون الدولي اصطلاحاً: إن كانت أهمية التعاون بالنسبة للفرد كبيرة، فلا شك في أن أهمية التعاون بالنسبة للدول أكثر أهمية، وأكتر فائدة، كون أن التعاون الدولي يكون من باب أولى، وذلك لأن إيجابياته تحقق النفع لأكبر عدد ممكن من الشعوب قال تعالى: ﴿ يَٰٓأَيُّهَا ٱلنَّاسُ إِنَّا خَلَقۡنَٰكُم مِّن ذَكَرٖ وَأُنثَىٰ وَجَعَلۡنَٰكُمۡ شُعُوبٗا وَقَبَآئِلَ لِتَعَارَفُوٓاْۚ ﴾[الحجرات: 13].

يعرّف التعاون الدولي على أنه: عمل مشترك ومنسق بين دولتين أو أكثر في مجال معين أي كانت طبيعته، من أجل التوصل إلى نتائج مشتركة في إطار العلاقات الدولية، فالتعاون هو ذلك القدر من المساعدة والعون الذي تبذله سلطات دولة ما لدولة أخرى بغية توقيع العقاب بالمجرمين الذين أخلوا بالأمن فوق حرم إقليمها، أي إقليم دولة أخرى (مجاهدي، 2018).

ويعرّف التعاون الدولي لمواجهة الجريمة الإلكترونية على أنه: أحد أصناف التعاون بين الدول موضوعه تبادل المساعدة والمنافع المشتركة بين سلطات أكثر من دولة، وغرضه التصدي للجرائم التي تتعدى حدود الدولة الواحدة، بما يكفل إحقاق الأمن والعدالة للأفراد والدول (ذنايب، 2010).

ثالثاً: تعريف التعاون الدولي قانوناً: فإن كانت الدولة هي الشخص القانوني الدولي للنظام السياسي والعالمي، إلا أنها ليست القوة الفاعلة الوحيدة في هذا النظام، بل أصبحت للمنظمات الدولية في وقتنا الحالي قوة ذات تأثير متزايد في المجتمع الدولي، فلم تعد الدولة هي القوة الوحيدة التي تحتكر القرارات

الدولية كما كانت في العصور السابقة، وقد عملت المنظمات الدولية على تعميق مظاهر ومجالات التعاون بين الدول وتنظيم شؤون المجتمع وحمايته من الظواهر الإجرامية (مجاهدي، 2018).

وتعد عصبة الأمم المتحدة أول منظمة قامت بتوثيق التعاون فيما بين الدول وشعوبها، حيث تعهدت الدول الموقعة على هذه العصبة بالإلتزام بالمبادئ التالية (المرعشي، 2025):

1. عدم استخدام القوة في حل القضايا الدولية.
2. احترام القانون الدولي وقواعده.
3. الالتزام بالواجبات والعهود التي تنص عليها المعاهدات الدولية.
4. إقامة العلاقات بين الدول على أساس العدل والشرف.

حيث تكرس مبدأ التعاون الدولي بعد قيام الأمم المتحدة عام 1945م من خلال قرار الجمعية العامة للأمم المتحدة الصادر في 24 أكتوبر 1970م المتعلق بمبادئ القانون الدولي المرتبطة بالعلاقات الودية والتعاون بين الدول، وقد تنوعت مجالات التعاون الدولي التي حددها ميثاق الأمم المتحدة في نصوصه، فيعتبر التعاون الدولي في مواجهة الجريمة بصفة عامة، والجرائم ذات الطابع الدولي بصفة خاصة أحد أهم هذه المجالات، وذلك بواسطة لجان متخصصة، كلجنة منع الجريمة، ولجنة العدالة الجنائية، ولجنة المخدرات (مجاهدي، 2018، صفحة 18).

ويقصد بالتعاون الدولي في مواجهة الجريمة قانوناً: تبادل العون والمساعدة وتضافر الجهود المشتركة بين دولتين أو أكثر لتحقيق مصلحة مشتركة في مجال التصدي لمخاطر وتهديدات الإجرام، وما برتبط به من مجالات أخرى، كمجالات العدالة الجزائية ومجال الأمن أو لتخطي مشكلة الحدود والسيادة التي قد تتعرض لها الجهود الوطنية في ملاحقة المجرمين، سواء كانت هذه المساعدة المتبادلة قضائية أو تشريعية

أو شـــرطية موضـــوعية أو إجرائية، وســـواء كانت بين دولتين فقط، أو كانت على نطاق إقليمي وعالمي (ذنايب، 2010، صفحة 58).

وبناءاً على ما ســـبق يمكن تعريف التعاون الدولي لمواجهة الجريمة الإلكترونية على أنه: تلك الجهود المتبادلة بين الدول المختلفة – دولتين فأكثر– التي تبذلها في مكافحة الجرائم الإلكترونية العابرة للحدود، وذلك من خلال وضع أساليب وآليات قانونية وقضائية بواسطة المؤسسات والمنظمات الدولية؛ لمحاسبة مرتكبي هذه الجرائم، وإصلاح ما قد يترتب عليه من أضرار على الفرد والمجتمع، ووضع تدابير وقائية من شأنها ردع الأفراد عن ارتكاب الجرائم الإلكترونية، والسيطرة عليها بأكبر قدر من الإمكان.

الفرع الثاني: مبررات التعاون الدولي

هنالك عدة اعتبارات أو مبررات تبرر وجود التعاون الدولي ومكافحته للجريمة بصـــورة عامة، ومن هذه المبررات ما يلي:

أولاً: التقدم التكنولوجي المستمر جعل الدولة بقوتها وصلابتها مهما بلغت لا يمكنها الاستغناء عن الدخول في العلاقات الدولية المتبادلة مع غيرها من الدول الأخرى (التعاون الدولي)، كون أن جهودها الخاصة لم تعد كافية لمواجهة الجرائم أو تقليص حجمها في ظل هذا التقدم المستمر، مما ساعد في ظهور أنماط جديدة من الجريمة، وامتداد آثارها على المستوى العالمي كالجريمة الإلكترونية، والجريمة المنظمة (خراشي، 2014).

ثانياً: في الغالب الأعم تكون الجرائم الإلكترونية جرائم غير محلية، فعادةً ما تتشـارك عدة دول مختلفة في تحقيق عناصر هذا النوع من الجرائم، مما يضع القوانين الوطنية في صعوبة مواجهة هذه الجرائم وملاحقة مرتكبيها، عدا عن صـعوبة الوصـول إلى الأدلة الثبوتية لهذه الجرائم فمن السـهل محوها وإخفائها، وهذا ما دفع المجتمع الدولي؛ لإنشاء أجهزة تعاونية تعمل على مستويات مختلفة من أجل ضمان التنسيق والمتابعة فيما يتخذ من تدابير دولية وداخلية؛ لضـمان الإلتزام بالتعاون الدولي، وضـمان تنفيذه بشـكل متكامل بما يحقق أهدافه (مبارك، 2006).

ثالثاً: تدويل القانون الجنائي، فقد دفع التعاون الدولي الفكر الدولي نحو فكرة تدويل القانون الجنائي، حيث يؤدي هذا التعاون إلى خلق نوع من التقارب بين التشريعات الحالية، مما يجعل أمر تدويل القانون الجنائي أمراً قابلاً للتحقيق، وهذا ما يهيئ وجود قانون جنائي دولي لمواجهة الجريمة المنظمة العابرة للحدود (الدسوقي، 2009).

رابعاً: تحقيق الردع، فالتعاون الدولي يعتبر من قبيل التدابير المانعة من ارتكاب الجريمة بدايةً، كون أن المجرم سوف يكتشف أنه لا يوجد مهرب من المسؤولية عن الجريمة التي ارتكبها، أو العقوبة التي حكم عليه بها، مما يجعله يمتنع عن السير في سلوك السبيل الإجرامي، فلو ارتكب جريمة وتمكن من الهروب إلى دولة أخرى، فسيكون معرّض للقبض عليه أو ترحيله إلى البلد الآخر، وهذا ما يحقق الردع الخاص للمجرم الإلكتروني، والردع العام لغيره عندما يرى أن العقوبة سبيلها التطبيق على الجريمة الإلكترونية المرتكبة بغض النظر عن موقع المجرم (خراشي، 2014؛ الدسوقي، 2009).

والتعاون الدولي في مواجهة الجريمة الإلكترونية يكون من خلال التنسيق بين تشريعات الدول المختلفة؛ لمواجهة هذه الجرائم بتطبيق كل دولة قوانينها على ما يُرتكب على أراضيها الداخلية من هذه الجرائم، وذلك فيما يتعلق بالأفعال التي تتفق التشريعات المختلفة على تجريمها والعقاب عليها، كالابتزاز من خلال الإنترنت فهو أمر مرفوض عالمياً، فلو أقدمت كل دولة على معاقبة مرتكبي أفعال الابتزاز عبر مواقع الإنترنت، فإن ذلك يساهم في تقليل تلك الأفعال الإجرامية.

المطلب الثاني: مفهوم الجريمة الإلكترونية

يتناول هذا المطلب تعريف الجريمة الإلكترونية وطبيعتها القانونية في الفرع الأول منه، ويتناول الفرع الثاني خصائص وأركان الجريمة الإلكترونية على النحو التالي:

الفرع الأول: تعريف الجريمة الإلكترونية وطبيعتها القانونية:

لمعرفة أهم ما يدور حول الجريمة الإلكترونية ومعرفة المعنى المراد منها لا بد من التطرق إلى تعريف هذه الجريمة وطبيعتها القانونية على النحو التالي:

أولاً: تعريف الجريمة الإلكترونية: لم يتفق الفقهاء فيما بينهم على تعريف مصـــطلح الجريمة الإلكترونية، في حين تعددت وجهات النظر فيما بينهم وفقاً لاختلاف النظم القانونية لكل دولة، فبعض الفقهاء عرّفها على أنها: جريمة ذات طابع مادي تتمثل في كل فعل أو سلوك غير مشروع مرتبط بأية جهة بالحاسبات، يتسبب في تكبد أو إمكانية تكبد المجني عليه خسارة، وحصول أو إمكانية حصول مرتكبه على أي مكسب ولها مسميات منها جرائم الكمبيوتر والإنترنت (فريحة، 2011، صفحة 2).

وقد عرّفها البعض على أنها: كل فعل متعمد أياً كانت صلته بالإلكترونية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل، أو هي كل سلوك غير مشروع معاقب عليه قانوناً صادر عن إرادة إجرامية محله معطيات الحاسب (فكري، 2014).

وبناءً على ما ســـبق يرى الباحث أن بعض الفقهاء وشـــراح القانون قد ارتكزوا في تعريفهم للجريمة الإلكترونية على أداة الجريمة (الحاســـوب)، في حين اتجه البعض الآخر في تعريفهم على محل الجريمة (الفعل غير المشـــروع)، كما **يمكن للباحث** أن يخرج بتعريف للجريمة الإلكترونية أقرب ما يمكن لتعريف جامع ومانع لما يدور حول مصـــطلح **الجريمة الإلكترونية**، وهو: أي أفعال غير قانونية ومعاقب عليها بموجب القانون سواء القانون الوطني أو القانون الدولي تُرتكب بواسطة استخدام أي وسيلة من الوسائل إلكترونية، كالحاسوب، أو الهواتف أو أية وسيلة أخرى يتم إنتاجها حديثاً تُمكن من استخدام الإنترنت من خلالها، وذلك بقصد الإضرار بالأفراد أو بمؤسسات الدولة؛ لتحقيق مصالح شخصية.

أما بالنسبة **للتعريف القانوني** لها نجد أن القوانين المعمول بها على الأراضـــي الفلسطينية لم تنص على تعريف الجريمة الإلكترونية فالمشرع الأردني لم يعرف الجريمة الإلكترونية في قانون العقوبات الأردني رقم

(16) لسنة 1960م المطبق على أراضي الضفة الغربية، بل ولم يتطرق في نصوصه إلى هذا النوع من الجرائم، وكذلك لم يتطرق إلى تعريفها المشرع الفلسطيني في القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته، والذي نظم موضوع الجريمة الإلكترونية.

مع الإشارة إلى أن هنالك بعض القوانين قد تطرقت إلى تعريفها في نصوصها كنظام مكافحة الجرائم الإلكترونية السعودي، حيث عرّف الجريمة الإلكترونية على أنها: أي فعل يرتكب متضمناً استخدام الحاسوب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام[1]، وغيرها من القوانين كالقانون القطري، والذي جاء تعريفه للجريمة الإلكترونية متناسقاً مع تعريف القانون السعودي، فلا يوجد فارق جوهري فيما بينهما[2].

ثانياً: الطبيعة القانونية للجريمة الإلكترونية: كما ذكرنا في تعريفنا للجريمة الإلكترونية أنها ترتبط بالوسائل الإلكترونية وتقوم عليها، مما أكسبها لوناً وطابعاً قانونياً خاصاً يميزها عن غيرها من الجرائم التقليدية، وعند الحديث عن الطبيعة القانونية للجريمة الإلكترونية فإن الحديث يتمحور حول الوضع القانوني للمعلومات والبيانات المخزنة على الأجهزة الإلكترونية، فهل لها قيمة وطابع من نوع خاص، أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم، وهذا ما أدى إلى انقسام الفقه إلى اتجاهين وهما (العجمي، 2014):

الإتجاه الأول: لا يمكن اعتبار المعلومة من قبيل القيم القابلة للاستحواذ (لها طابع خاص): اتجه أصحاب هذا الاتجاه إلى أن المعلومة لها طابع خاص، وذلك كون أن القيمة تكمن في الأشياء المادية وحدها، فالأشياء التي توصف بالقيم هي التي تقبل الاستحواذ عليها، وبالتالي وبمفهوم المخالفة تعد المعلومة ذات طبيعة معنوية، فلا يمكن اعتبارها من قبيل القيم القابلة للاستحواذ إلا فيما يتعلق بحقوق

[1] نظام مكافحة الجرائم الإلكرتونية السعودي لسنة 2007، المادة (1).

[2] قانون الجرائم الإلكترونية القطري، رقم (14) لسنة 2014م، المادة (1).

الملكية الفكرية؛ لذلك فإن هذا الاتجاه استبعد المعلومات والأفكار من مجال السرقة ما لم تكن مسجلة على اســـطوانة أو شـــريط وفي حال ســـرقتها نكون أمام واقعة ســـرقة لمال معلوماتي غير مادي، وليس مال معلوماتي ذو طبيعة مادية (الزعبي، 2021).

الإتجاه الثاني: أن المعلومة ما هي إلا مجموعة من القيم القابلة للاســـتحواذ: بينما اتجه أصـــحاب هذا الاتجاه إلى اعتبار أن المعلومة ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعّامتها المادية، وذلك كون أن المعلومات لها قيمة اقتصـادية قابلة أن تحاز حيازة غير مشروعة، وأن العلاقة التي ترتبط المعلومة بمؤلفها، كالعلاقة القانونية التي تربط المالك بالشـــيء الذي يملكه، وبمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الإقتصادية وليس على أساس كيانه المادي؛ لذلك يستحق الحماية القانونية ومعاملته معاملة المال (الزعبي، 2021).

ويرى الباحث في تحليله لفكرة الاعتداء على المعلومات وإخراجها من مجال السرقة ما لم تكن مسجلة على دعّامة معينة على اعتبار أنها ذو طبيعة معنوية ليس لها كيان مادي، إلا أن هذا غير منطقي فالمعلومة وإن كانت ليس لها كيان مادي ملموس إلا أنها عبارة عن أفكار قابلة للاســتحواذ باختلاف الطرق التي يتم الاســتحواذ بها مثل اســتخدام الأجهزة الرقمية أو من خلال الحفظ الذهني، وبما أن طبيعة المعلومات غير مادية فإن طبيعة الاستحواذ تكون غير مادية كحفظ المعلومة في عقل السـارق من خلال النظر عليها، أو إرسالها عبر وسائل التواصل الخاصة به فور حصوله عليها دون علم صاحبها، وبالتالي فقد تمكّن السارق من الاستحواذ عليها دون أن يكون هنالك شيء مادي مسجلة عليه.

الفرع الثاني: خصائص وأركان الجريمة الإلكترونية

كما ذكرنا أعلاه أن ارتباط الجريمة الإلكترونية بالوسـائل الإلكترونية أكسـبها لوناً وطابعاً خاصـاً يميزها عن غيرها من الجرائم التقليدية؛ لذلك لا بد من التطرق إلى الخصـــائص الذي يتميز بها هذا النوع من الجرائم، بالإضافة إلى الأركان التي تقوم عليها الجريمة الإلكترونية على النحو التالي:

أولاً: خصـــائص الجريمة الإلكترنية: تمتاز الجريمة الإلكترونية عن باقي الجرئم التقليدية مجموعة من الخصائص أهمها (بوشعرة و موساوي، 2018؛ سليمان، 2013):

1. الجريمة الإلكترونية جريمة عابرة للحدود: من أهم ما يميز الجريمة الإلكترونية أنها جريمة عابرة للحدود أي تتخطى الحدود الجغرافية؛ لارتباطها بالإنترنت وتقنية المعلومات، فهي جريمة عابرة لحدود الزمان والمكان، فلا تتقيد بمكان وزمان محدودين حيث مجتمع المعلومات تتلاشـــى فيه الحدود الجغرافية بين الدول؛ لارتباط العالم بشـــبكة انترنت واحدة، فأغلب الجرائم الإلكترونية المرتكبة عبر شـــبكة الإنترنت يكون فيها الجاني من دولة ما والمجني عليه من دولة أخرى، وهذا من أهم مبررات وجود تعاون دولي لمواجهة الجريمة الإلكترونية (الخراز، 2022/2021).
2. ارتكاب الجريمة في بيئة المعالجة الآلية للبينات والمعلومات: إن ارتكاب الجريمة الإلكترونية يقع عند التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي؛ لمعالجتها إلكترونياً مما يمكن المستخدم من إمكانية تصـــحيحها أو محوها أو تخزينها أو اسـترجاعها أو طباعتها، وهذه العمليات مرتبطة ارتباطاً وثيقاً بارتكاب الجريمة الإلكترونية، حيث يمكن ارتكاب الجريمة الإلكترونية في أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات في الحاسوب الآلي سواء أثناء الإدخال مثل إدخال معلومات غير صـــحيحة، أو في مرحلة المعالجة مثل التعديل على المعلومات المدخلة، أو في مرحلة الإخراج مثل التلاعب في النتائج التي يخرجها الحاســـوب بشـــأن المعلومات الصحيحة التي تم إدخالها وتمت معالجتها بطريقة صحيحة (فحصي، 2022).
3. صـعوبة إثبات الجريمة الإلكترونية واكتشـافها: فالجريمة الإلكترونية لا تترك آثاراً ملموسـة ورائها، فلا تترك شهوداً يمكن الاستدلال بأقوالهم ولا أدلة ثبوتية مادية يمكن فحصـها؛ لوقوعها في عالم افتراضـي يتم فيه نقل المعلومات وتناولها بواســطة نبضـــات إلكترونية غير مرئية، مما يصـــعب إســناد الفعل الإجرامي لشخص طبيعي، حيث يستطيع المجرم الإلكتروني إخفاء الآثار المادية للجريمة التي ارتكبها بفضـل التقنيات المعلوماتية، وإخفاء الدليل الرقمي الإلكتروني باسـتخدام عمليات التقنية الحديثة، وهذا

ما يجعل التحري عن الدليل في الجريمة الإلكترونية من قبل المختبر الجنائي الإلكتروني والخبراء المختصين أمراً في غاية الصعوبة (السلمي، 2023).

4. الجريمة الإلكترونية أقل عنفاً وجهداً في التنفيذ: فالجريمة الإلكترونية لا تتطلب جهداً في تنفيذها فهي جريمة ناعمة ونظيفة في طبيعتها على عكس الجرائم التقليدية التي تتطلب نوعاً من المجهود البدني الذي يكون في صورة ممارسة العنف والإيذاء، فهي تحتاج فقط قوة علمية وقدر من الذكاء ومهارة في توظيفهما، فلا يحتاج الجاني في ارتكابها من الوقت إلا دقائق معدودة أو حتى مجرد ثوان معدودة، ولا يحتاج من القوة العضلية سوى تحريك أصابعه على جهاز الحاسوب (فحصي، 2022؛ بوادي، 2006).

5. قلة الإبلاغ عن الجريمة الإلكترونية: يتجنب أغلب ضحايا الجرائم الإلكترونية التبليغ عنها حتى لا تتأثر سمعتهم، ولا تهتز ثقة زبائنهم فيهم، خاصة إذا كانوا من المؤسسات المالية أو مؤسسات معروفة في المجتمع، أو خوفاً من التداعيات النفسية والإجتماعية في حال كانوا أشخاصاً طبيعيين لا سيما في حالات الابتزاز والتهديد بنشر معلوماتهم أو صورهم الخاصة، مما يدل ذلك على سبب قلة القضايا الإلكترونية (السلمي، 2023).

6. تعتمد الجريمة الإلكترونية على الخداع والتضليل: فالإجرام الإلكتروني يعد إجرام الأذكياء، حيث يتميز مرتكبوها بالذكاء والدراية بالأساليب المستخدمة في أنظمة المعالجة الآلية وطريقة تشغيلها وكيفية تخزين المعلومات، مما يساعدهم في خداع المجني عليهم وتضليل الفعل الإجرامي (حشيفة، 2020).

ثانياً: أركان الجريمة الإلكترونية: للجريمة الإلكترونية أركان يجب أن تتوافر من أجل قيامها، فبالرغم من ارتكابها في العالم الإفتراضي إلا أن شأنها شأن الجريمة العادية لها ثلاثة أركان الركن الشرعي أي النصوص القانونية المجرمة للفعل المرتكب، والركن المادي وهو الفعل أو السلوك المجرّم ذاته، والركن المعنوي الذي يعبر عن إرادة ونية المجرِم الإلكتروني على النحو التالي (كيلاني، 2024؛ عقباش و مبارك، 2022):

1. **الركن الشـرعي:** إن مبدأ شـرعية الجريمة والعقوبة هو مبدأ أسـاسـي في مختلف التشـريعات الجزائية والقائل: "لا جريمة ولا عقوبة إلا بنص"؛ لذلك يعتبر الركن الشـرعي الركن الأول والأسـاسـي للجريمة الإلكترونية، كونها تتطلب وجود نص قانوني يجرّم الفعل المرتكب من قبل الشخص الجاني حتى تقوم المسـؤولية الجزائية للجريمة، وتسـتمد الجرائم الإلكترونية شـرعيتها من مختلف التشـريعات الوطنية الصـادرة بشـأن الجريمة الإلكترونية، حيث بذلت هيئة الأمم المتحدة جهوداً كبيرة إضـافة إلى جهود المجلس الأوروبي، من أجل إقناع الدول بإصـدار تشـريعات لمواجهة الجرائم الإلكترونية، وتعزيز التعاون الدولي في هذا المجال، وسـنتناول فيما بعد النصـوص القانونية الوطنية والدولية المتعلقة بالجرائم الإلكترونية (حشيفة، 2020؛ السعيد، 2011).

2. **الركن المادي:** وهو القيام بفعل أو الإمتناع عن القيام عن فعل الذي بواسـطته تكتشـف الجريمة ويكتمل جسمها، ولا توجد جريمة بدون ركن مادي، فالجريمة بغير مادياتها لا تصيب حقوق الأفراد أو الجماعة بأي اعتداء؛ لذا يعد الركن المادي أحد الاركان الأسـاسـية لارتكاب أية جريمة، وهو الفعل الإجرامي بعناصـره الثلاث (السـلوك الإجرامي، النتيجة، العلاقة السـببية بينهما)، وذلك لقيام جريمة تامة معاقب عليها (نجم، 2015).

ويقوم الركن المادي للجريمة الإلكترونية في صورتين أساسيتين وهما (حشيفة، 2020، صفحة 22):

الصـورة الأولى: الإعتداء على نظام المعالجة الآلية من خلال إما الدخول والبقاء غير المشـروع في نظام المعالجة الآلية أو الاعتداء العمدي على نظام المعالجة الآلية للمعطيات.

الصورة الثانية: الإعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي.

3. **الركن المعنوي:** يعبر الركن المعنوي عن الكيان النفسـي المقابل للكيان المادي للجريمة، فهو نص التجريم أي النصف الآخر للجريمة، ويمكن التعبير عنه بالحالة النفسية للجاني وقت ارتكاب الجريمة، حيث لا تقوم الجريمة قانوناً بدونه، فغالباً ما تقع الجريمة الإلكترونية بصورة عمدية سبقها التفكير في

الحصـــول على المعلومة أو اختراق موقع معين، فالأصـــل في الجرائم العمدية ما لم يســـتثنى بنص قانوني (السعيد، 2011، صفحة 245 وما بعدها).

ويكمن الركن المعنوي في هذا النوع من الجرائم في صـــورة القصـــد الجنائي العام بعنصـــريه العلم والإرادة، حيث تتجه إرادة الجاني إلى فعل الإعتداء، مع العلم بأن فعله يؤدي إلى ارتكاب ســـلوك يعاقب عليه القانون، ويعلم بخطورته، أو الأضـرار التي قد تنجم عنه (حشـيفة، 2020، صـفحة 26)، فالركن المعنوي في الجريمة الإلكترونية يعد أمراً هاماً من أجل تحديد طبيعة النشاط الذي يمارسه الشخص الجاني، وتحديد النصـــوص القانونية واجبة التطبيق، فإذا كان الفاعل غير مدرك لخطورة الفعل الذي ارتكبه، وكان مكره على ارتكابه أو كان غير مميز، فلا نكون أمام جريمة إلكترونية؛ لفقدانها أحد أركان الجريمة وهو الركن المعنوي، لذا يجب على الجاني مرتكب الفعل الإجرامي أن يتمتع بالوعي والإرادة الحرة؛ لمعرفة طبيعة الفعل وتكييفه تكييفاً قانونياً صحيحاً (سرور، 1981).

وبالتالي نجد أن الجريمة الإلكترونية في أركانها كالجريمة التقليدية، إلا أن الفارق بينهما أن الجريمة التقليدية تقع في عالم واقعي تقليدي، بينما الجريمة الإلكترونية تقع في عالم إفتراضـــي، حيث لاا بد من وجود نص تشـريعي يعاقب على سـلوك معين ارتكب عبر منصـات الإنترنت تطبيقاً لمبدأ شـرعية العقوبة والجريمة، وكذلك لا بد من وجود ركن مادي بعناصـــره؛ لقيام جريمة إلكترونية معاقب عليها بموجب نص القانون، وأخيراً ولقيام المســـؤولية الجزائية على عاتق مرتكبيها لا بد من توافر الركن الثالث والأخير وهو الركن المعنوي، فالجريمة الإلكترونية تحتاج إلى قصد جرمي باعتباره أنه يلعب دوراً هاماً في معرفة مرتكب الجريمة، وتكييف الجريمة تكييفاً قانونياً صحيحاً تطبيقاً للقانون.

المبحث الثاني: أساليب التعاون الدولي في مواجهة الجرائم الإلكترونية

بعد الانتهاء من توضـــيح أهم ما يدور حول مصـــطلحات التعاون الدولي والجرائم الإلكترونية، جاء هذا المبحث؛ ليتناول آليات التعاون الدولي في مواجهة الجرائم الإلكترونية من خلال معرفة أوجه التعاون الدولي، وكذلك الإجراءات القانونية لملاحقة المجرم الإلكتروني؛ لذلك يتناول هذا المبحث أوجه التعاون الدولي في مواجهة الجريمة الإلكرتونية في المطلب الأول منه، ويتناول المطلب الثاني دور الهيئات والمنظمات في تعزيز التعاون الدولي في مواجهة الجريمة الإلكترونية على النحو التالي:

المطلب الأول: أوجه التعاون الدولي في مواجهة الجرائم الإلكترونية

يأخذ التعاون الدولي في مكافحة الجريمة الإلكترونية مظهران: الأول ما يتعلق بالجانب الوقائي من الجريمة بالســـعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية قبل ارتكاب الجريمة، والتي تكفل منع ارتكابها في مرحلة التنفيذ ويتمثل في التعاون الأمني، والثاني ما يتعلق بضـــرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة، والتي تعتبر اختصـاصـات قضـائية متعددة ذات نظم قانونية مختلفة، ويتمثل في التعاون القضائي (ناشف، 2022)؛ لذا يتناول هذا المطلب التعاون الأمني في الفرع الأول منه، ويتناول الفرع الثاني التعاون القضـائي، بينما يتناول الفرع الثالث التعاون الدولي بشأن تسليم المجرمين في مواجهة الجرائم الإلكترونية على النحو التالي:

الفرع الأول: التعاون الأمني في مواجهة الجرائم الإلكترونية

يعد التعاون الأمني من أهم آليات مواجهة الجرائم الإلكترونية من خلال تمكين الدول من الحد من هذه الجرائم المستحدثة، وذلك بواسطة أجهزة تعمل بفضل تعاون الدول فيما بينها؛ لمنع أو تقليص ارتكابها.

أولاً: مفهوم التعاون الأمني وأهميته: يعرّف التعاون الأمني على أنه: تبادل العون والمســـاعدة وتضـــافر الجهود المشتركة بين طرفيين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال تصدي لمخاطر الإجرام، وما يرتبط به من مجالات أخرى مثل مجال العدالة الإجتماعية ومجال الأمن أو لتخطي

مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقد مصادر التهديد، وسواء اقتصرت على دولتين فقط أو امتدت إقليمياً أو عالمياً (أبو نمر و بوكشريدة، 2021–2022).

حيث يعد التعاون الأمني من أهم الآليات التي تساهم في منع ارتكاب هذا النوع من الجرائم، وخفض نسبة وقوعها، وهذا ما يؤكده نسبة الجرائم الإلكترونية في الآونة الأخيرة، ومجريات التحقيقات فيها، فكما ذكرنا سابقاً أن جهود الدولة وحدها لم تعد كافية بالقدر المطلوب منها في مواجهة الجرائم الإلكترونية، فمهما بلغت نسبة تطورها في القضايا الجزائية إلا أنها لا يمكن لها أن تلاحق وتعاقب المجرمين إلا في حدودها الوطنية التابعة لها، ومن هنا تبرز أهمية التعاون الأمني في مواجهة الجرائم الإلكترونية (الدسوقي، 2009، صفحة 593).

ويتضح أهمية التعاون الأمني من خلال تبني أسلوب فني متطور لإجراء التحريات والتحقيقات في مجال مكافحة الجريمة الإلكترونية، من خلال استخدام التكنولوجيا الحديثة في الاتصال مثل الدوائر التلفزيونية، والاستعانة بأساليب خاصة للتحري والمراقبة، واستحداث قنوات للاتصال، والتنسيق الأمني والقضائي بين الجهات المختصة عن طريق الأقمار الصناعية، وشبكة الإنترنت لتبادل المعلومات سريعاً، واتخاذ ما يلزم من الإجراءات للتصدي لهذه النوع من الجرائم (أبو نمر و بوكشريدة، 2021–2022؛ محمد، 2020؛ بوادي، 2006).

وهذا ما لفت انتباه الدول إلى ضرورة التعاون الدولي لمواجهة الجرائم الإلكترونية، حيث عملت الكثير من الدول على عقد اتفاقيات ثنائية؛ لتسهيل مهمة التحقيق في الجرائم الإلكترونية العابرة للحدود، ففي عام 1983م أجرت منظمة التعاون والإنماء الإقتصادي[1] دراسة حول إمكانية تطبيق القوانين الجزائية الوطنية، وتكييف نصوصها؛ لمواجهة الجرائم الإلكترونية (هروال، 2007)، وفي عام 1985م أصدرت هذه المنظمة

[1] هي منظمة التعاون الإقتصادي والتنمية (OECD) وهي منظمو دولية تركز على تعزيز السياسات الرامية إلى تحسين الرفاهية الإقتصادية والإجتماعية للناس في جميع أنحاء العالم، حيث توفر منتدى للأعضاء لتبادل المعلومات والتعاون في مختلف القضايا الإقتصادية والإجتماعية، من خلال الموقع الإلكتروني التالي: https://www.oecd.org، تاريخ آخر زيارة 2025/2/5م.

تقريراً تضمن قائمة بالحد الأدنى لعدد أفعال سوء استخدام الحاسب الآلي التي يجب على الدول أن تجرمها وتفرض عليها عقوبات في قوانينها، كالغش والتزوير في الحاسب الآلي، وسرقة الأسرار المدعمة في قواعد الحاســـب الآلي؛ لتفعيل التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وكما عالجت اتفاقية فيينا لسنة 1988م الموضوع ذاته، وشجعت العديد من الدول على عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه الجرائم، وقد لفت اللقاء التمهيدي الإقليمي لأسيا والباسفيك المنعقد في 1989م، الممهد للمؤتمر الثامن للأمم المتحدة المنعقد ســـنة 1990م في كوريا؛ للنظر إلى نتائج التطور والتقدم التكنولوجي فيما يتعلق بالجريمة الإلكترونية، واقترح تشجيع اتخاذ إجراء دولي لمواجهة هذه الجريمة، وقد ناشد المؤتمر الأخير في قراره المتعلق بالجرائم ذات صـلة بالحاسـب الآلي الدول الأطراف لضـرورة تكثيف جهودها لمواجهة الجرائم الإلكترونية (شرشر، 2021)[1].

وبالرغم من ضـــرورة التعاون الدولي وتهافت الدول إلى الســـعي وراءه؛ لتحقيق تعاون دولي يواجه الجريمة الإلكترونية ويقيدها، إلا أن الأمر لا يخلو من العقبات، فهنالك العديد من العقبات أو الصـــــعوبات التي تواجه هذا التعاون، **وسيتم تناولها في الفصل الثاني من هذه الدراسة بإذن الله تعالى.**

ثانياً: جهود الإنتربول (منظمة الشرطة الجنائية الدولية): الإنتربول هو أكبر منظمة شرطية دولية، أنشأت عام 1929م إلا أن التفكير في إنشائها راجعاً لسنة 1914م حينما اجتمع عدد من الضباط ورجال القانون والقضاء من 14 دولة في موناكو؛ ليضعوا أساس الشرطة الدولية، مقرها الرئيسي في مدينة ليون في فرنسا، وتتكون حسب دستورها الدولي من الجمعية العامة، واللجنة التنفيذية، والأمانة العامة، والمكاتب المركزية الوطنية، والمستشارون، ولجنة ضبط ملفات الإنتربول، كما كانت تسمى هذه المنظمة باللجنة الدولية للشرطة الجنائية، وتضم 182 دولة في عضويتها، وهي من قبيل المنظمات الدولية المتخصصة التي تهتم بالتعاون الدولي بين الدول الأعضاء فيها في مجال مواجهة الجرائم وتعقب المجرمين (أحمد، 2019؛ بوادي، 2006).

[1] قرار الجمعية العامة 111/53، أشار إليه: ص43، أنظر القرار 126/54، الفقرة 3.

حيث تستهدف هذه المنظمة تأكيد وتشجيع التعاون بين سلطات البوليس أو أجهزة الشرطة في الدول والأطراف، على نحو فعّال يحقق مكافحة الجريمة، وذلك من خلال تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة بواسطة المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة، وتبادل المعلومات والبيانات فيما بينها، وكذلك التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، وتزويدها بالمعلومات المتوفرة لديها على أقليمها، أي أن عضو الإنتربول لا يقوم بإجراء القبض على المجرم بنفسه، وإنما يتم من قبل جهاز الشرطة الوطنية في الدولة التي يتواجد فيها المجرم استناداً لقواعد المنظمة، وهذا ما يؤكد احترام السيادة الوطنية (الدسوقي، 2009، صفحة 594؛ عطية، 2004، صفحة 459).

لذلك من الضرورة تدعيم التعاون بين أجهزة الشرطة في الدول المختلفة بناء على اتفاقيات دولية، بحيث إذا اكتشفت الشرطة الوطنية لدولة ما أن إحدى الجرائم الإلكترونية قد تم ممارستها عبر شبكة الإنترنت ومن خلال موقع موجود خارج البلاد، أن تقوم بالإبلاغ عن هذه الجريمة إلى سلطات البوليس بالدولة التي ارتكب فيها الفعل، وهنا تكمن أهمية التعاون الدولي في مواجهة الجريمة الإلكترونية (الدسوقي، 2009).

وتعد النشرات والتعميمات الدولية التي تصدرها الأمانة العامة للمنظمة الدولية إحدى مهامها الرئيسية التي تجسد التعاون الشرطي الدولي، ويتم صدور هذه النشرات إما بمبادرة منها أو بطلب من المكاتب المركزية الوطنية أو منظمات دولية وكيانات تربطها بالإنتربول اتفاقيات خاصة، حيث من مهام الإنتربول مساعدة أجهزة الشرطة وتنفيذ القانون، وتبادل المعلومات الهامة المتعلقة بالإجرام باستخدام منظومة نشرات الإنتربول الدولية[1]، وتتضمن هذه النشرات نوعين من المعلومات تفاصيل الهوية (الهوية، الأوصاف البدنية، الصور والبصمات، والمعلومات الأخرى ذات صلة بمهنة الشخص ولغته)، وإما أن تكون معلومات قضائية (التهمة الموجهة للشخص والقانون الساري على الجريمة، والعقوبة القصوى الصادرة أو الممكنة، وفي حال صدور

[1] من خلال الموقع الإلكتروني التالي: https://www.interpol.int/ar/2/1، تاريخ آخر زيارة 2025/2/13م.

النشـرة الحمراء، رقم مذكرة التوقيف أو قرار الإدانة الصـادر عن المحكمة، وتفاصـيل البلدان التي سـيطلب منها التسليم) (أحمد، 2019، صفحة 52).

وهنالك العديد من أنواع نشرات الإنتربول منها: **النشرة الحمراء**، وهي طلب يقدم إلى أجهزة تنفيذ القانون في أرجاء العالم لتحديد مكان شـخص واعتقاله مؤقتاً في انتظار تسـليمه أو اتخاذ إجراء قانوني مماثل[1]، **النشـرة الزرقاء**، وهي لتحديد مكان إقامة الأشخاص وجمع المعلومات بشأنهم، **النشرة الخضراء**، وهي التي تستخدم للتزويد بتحذيرات ومعلومات اسـتخبار جنائية عن أشـخاص ارتكبو جرائم جنائية، **النشـرة الصـفراء**، وهي عبارة عن تنبيه عالمي من الشـرطة يتعلّق بشـخص مفقود، يتم نشـرها بشـأن ضـحايا اختطاف الوالدين، والاختطاف الجنائي (الاختطافات الابتزازية) أو الاختفاء غير المبرر[2]، **النشـرة السـوداء**، وهي التي تهدف لتبين الجثث المجهولة، وتبين الهوية الحقيقية للموتى الذين تعذر معرفة هوياتهم، **النشـــرة البرتقالية**، وهي التي تهدف لتيســير إشــعارات تحذيرية عن تهديدات إرهابية محتملة، فهي بمثابة إنذار أمني[3]، **النشـــرات الخاصـــة بالإنتربول**، وهي النشــرات التي تنبه فيها الشــرطة في العالم إلى الأفراد والكيانات الخاضــعين لجزاءات مجلس الأمن التابع للأمم المتحدة[4].

أما بالنسـبة لإنضـمام فلسـطين إلى المنظمة الدولية للشـرطة الجنائية (الإنتربول)، حيث بدأ الفلسـطينيون يســعون وراء العضــوية الكاملة بعد ســنوات عديد من التحضــير، ومع ارتفاع عدد البلدان التي تعترف بفلسطين كدولة بشكل متزايد وملحوظ من إمكانية تصويت الجمعية العامة للشرطة الدولية على عضويتها، فبحسـب لوائح الإنتربول تحتاج كل دولة للحصـول على عضـوية كاملة في المنظمة إلى ثلثي الأصـوات بالإضـافة إلى صـوت واحد من أعضـاء الجمعية العامة، ومع اعتراف أكثر من 130 دولة بفلسـطين كان

[1] من خلال الموقع الإلكتروني التالي: https://www.interpol.int/ar/2/1/3، تاريخ آخر زيارة 2025/2/13م.

[2] من خلال الموقع الإلكتروني التالي: https://www.interpol.int/ar/2/1/5، تاريخ آخر زيارة 2025/2/13م.

[3] أحمد عبد الهادي، من خلال الموقع الإلكتروني التالي، https://www.youm7.com، تاريخ آخر زيارة 2025/2/13م.

[4] من خلال الموقع الإلكتروني التالي: https://www.interpol.int/ar/2/1/4، تاريخ آخر زيارة 2025/2/13م.

الحصـــول على أغلبية الأصـــوات في متناول اليد، وفي اجتماع عقدته الجمعية العامة في بكين بتاريخ 2017/9/27م، صوتت 75 دولة من أعضاء الجمعية على انضمام فلسطين[1].

وتجدر الإشـــارة إلى أنه على نمط الإنتربول الدولي أنشـــأ المجلس الأوروبي في لكســـمبورج عام 1991م بوليس أوروبي؛ ليكون بمثابة حلقة وصل بين البوليس الوطني للدول المنضمة من ناحية، وأن يستخدم بعد ذلك للملاحقة الجزائية للجرائم العابرة للحدود من ناحية أخرى (الدسوقي، 2009، صفحة 597).

الفرع الثاني: التعاون القضائي في مواجهة الجرائم الإلكترونية

كون أن الجرائم الإلكترونية ذات طابع عالمي (عابرة للحدود) وبالتالي يمكن أن تتعدى آثارها عدة دول مختلفة، مما يجعل تنفيذ الإجراءات القضائية بحق المجرم شبه مستحيلة في ظل غياب التعاون القضائي ما بين الدول.

أولاً: تعريف التعاون القضـائي وأهميته: ويطلق عليه أيضـاً المسـاعدة القضـائية المتبادلة في المسـائل الجزائية، والذي يعد من أبرز تطبيقات التعاون الدولي في مجال مواجهة الجريمة الإلكترونية، ويعرّف على أنه: كل إجراء قضـائي تقوم به دولة من شـأنه تسـهيل مهمة المحاكمة في دولة أخرى، بصـدد جريمة من الجرائم، وتتضمن معظم الاتفاقيات الدولية لمكافحة الإرهاب نصوصاً تقتضي بضرورة اللجوء إلى المساعدة القضـــائية المتبادلة بين الدول المتعاقدة، من أجل تحقيق الفعالية و الســـرعة في إجراءات ملاحقة وعقاب جرائم الإرهاب (سليمان أ.، 2006).

ويعد التعاون القضـــائي من الآليات الفعّالة؛ لمواجهة الإجرام بوجه عام، والجريمة الإلكترونية بوجه خاص، لما للتعاون القضـائي من دور في التوفيق بين حق الدولة في ممارسـة اختصـاصـها الجنائي داخل حدودها الوطنية، وحقها في توقيع العقاب على الجاني؛ لذلك تتضـــمن معظم الاتفاقيات الخاصـــة بالجرائم التقليدية

[1] المؤسسة الفلسطينية لحقوق الإنسان من خلال الموقع الإلكرتوني التالي: https://pahrw.org/ar/، تاريخ آخر زيارة 2025/2/13م.

نصـــوصـــاً تقتضـــي بضـــرورة اللجوء إلى المســـاعدة المتبادلة، مما يحقق الســـرعة والفعالية في إجراءات الملاحقة، ومعاقبة مرتكبي الجرائم (الدسوقي، 2009، صفحة 597؛ سليمان أ.، 2006).

وقد نص المشـــرع الفلســـطيني في القرار بقانون رقم (10) لســـنة 2018م بشـــأن الجرائم الإلكترونية على التعاون الدولي في مكافحة الجرائم الإلكترونية، فقد نصت المادة (42) منه على:

1. تعمل الجهات المختصـــــة على تيســـــير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصـادق عليها، أو طبق مبدأ المعاملة بالمثل[1]، بقصـد الإسـراع في تبادل المعلومات، بما من شـــــانه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصـــــال، وتفادي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها.
2. يتوقف التعاون المشـار إليه في الفقره السـابقة على التزام الدولة الأجنبية المعنية بالحفاظ على سـرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو اســـتغلالها لأغراض أخرى غير مكافحة الجرائم المعينة بهذا القرار بقانون[2].

وعليه فإنه يمكن للســلطات المختصــة تبادل المســاعدات القضــائية الدولية؛ لمواجهة الجريمة الإلكترونية وجمع الأدلة الخاصة بها؛ للقبض على الجاني ومعاقبته.

ثانياً: صور التعاون القضائي: للتعاون القضائي في المجال الجنائي صور عديدة أبرزها:

1. **تبادل المعلومات:** وهو يشـمل تقديم المعلومات والوثائق التي تطلبها سـلطة قضـائية أجنبية بصـدد جريمة معينة، عن الاتهامات التي وجهت إلى رعاياها في الخارج، بالإضـــــافة إلى الإجراءات التي

[1] ويقصد بمبدأ المعاملة بالمثل: بأن تنص عليه اتفاقية دولية أو تشريع على أن يتعهد كل طرف بتوفير ذات المعاملة للطرف الآخر، وهو ينحصر ضمن نطاق معين أو محدد من المجالات كالمعاملة بالمثل في مركز الاجانب أو المعاملة بالمثل في العلاقات الدبلوماســـية، كما يمكن أن يتقرر هذا المبدأ بموجب العرف والممارسات الدولية، وفي هذه الحالة يكون أعمال المبدأ أكثر مرونة ولا سيما في الدول التي يحتل القانون العرفي فيها مكانة مهمة، انظر: جنان كاظم جنجر، رسالة لنيل شهادة الدكتوراة بعنوان: *مبدأ المعاملة بالمثل في القانون الدبلوماسي*، كلية القانون، جامعة كربلاء، 2022م، ص10.

[2] قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، المادة (42).

اتخذت ضدهم، فلا شك في ضرورة هذه الصورة من صور المساعدة القضائية، فنحن بصدد جريمة عابرة للحدود يكون القوام الأساسي لهذه الجريمة من المعلومات التي يمكن الحصول عليها عن المتهم الذي قام بارتكابها (الدسوقي، 2009، صفحة 598).

وقد لقيت هذه الصورة من التعاون القضائي صدى كبير في عدد من الاتفاقيات الدولية، ولا سيما المادة (1) في الفقرة (2) منها من معاهدة الأمم المتحدة النموذجية بشأن المساعدة المتبادلة في المسائل الجزائية[1]، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للأوطان، والتي تلزم الدول الأطراف بتسهيل تبادل المعلومات المتعلقة بجوانب مختلفة من النشاط الإجرامي[2]، ونصت المادة (1) من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القانونية، وصاغ اتفاق شنجن للاتحاد الاوروبي نظاماً متكاملاً لتبادل المعلومات.[3]

وبالرغم من ذلك **إلا أن الباحث يجد** أن التعاون الدولي الحالي لا يحقق المستوى المطلوب منه في مواجهة الجرائم الإلكترونية، وذلك لقلة أو محدودية الاتفاقيات الدولية المنظمة لهذا النوع من الجرائم بالذات، مع وجود بعضاً منها في المجال القضائي، عدا عن رفض بعض الدول للإنضمام والتوقيع على مثل هذه الاتفاقيات التي تساعد في مواجهة الجرائم الإلكترونية على المستوى الدولي، وسيتم تناولها في نهاية هذا المبحث بإذن الله تعالى.

2. **نقل الإجراءات:** ويقصد به قيام دولة ما بناءً على اتفاقية أو معاهدة باتخاذ إجراءات جنائية تتعلق بجريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة (الكميم،

---

[1] *معاهدة نموذجية لتبادل المساعدة في المسائل الجنائية*، المادة (2/1) قرار الجمعية العامة (117/45) بصيغته المعدلة (112/53)، صيغة المعاهدة النموذجية هي نتيجة للدمج بين المعاهدة النموذجية التي اعتمدتها في عام 1990م الجمعية العامة في قرارها (117/45) والتعديلات المدخلة عليها في عام 1998م في قرارها (112/53)، انظر: خلاصة وافية لمعايير الأمم المتحدة وقواعدها في مجال منع الجريمة والعدالة الجنائية، ص187.

[2] *اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية*، أنشئت بموجب قررا الجمعية العامة للأمم المتحدة (55/25) عام 2000م، ودخلت حيز التنفيذ في 2003م.

[3] *اتفاقية الرياض العربية للتعاون القضائي*، وافق عليها مجلس وزراء العدل العرب بموجب قرار رقم (1) بتاريخ 1983/4/6م في دورة انعقاده العادي الاولي، ودخلت حيز التنفيذ 1985م.

2017، صفحة 147)، أهمها: أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها، أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة، وأن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصـــول إلى الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب إليها (الدسوقي، 2009، صفحة 599).

وقد أقرت العديد من الاتفاقيات الدولية والإقليمية بهذه الصـورة كإحدى صـور التعاون القضـائي، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجزائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م في المادة (21) منها، والمادة (16) من النموذج الإرشـادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م.[1]

مع الإشـــارة إلى القول بأنه من حق الدولة المطلوب إليها أن ترفض نقل الإجراءات بحال عدم وجود تبرير واضـح بالطلب، وكان القصـد من الطلب سـياسـياً أو دينياً أو عنصـرياً، وإذا كانت الدولة متلقية الطلب قد طبقت قانونها على الجريمة قبل اسـتلامها من الدولة الأخرى، وكانت الإجراءات متخذة سـابقاً متوافقة مع القانون، وكذلك إذا كانت الإجراءات التي طلبتها الدولة تتعارض مع الالتزامات التي ارتكبتها الدولة متلقية الطلب ومخالفة للقانون[2].

3. **الإنابة القضـــائية:** يقصـــد بالإنابة القضـــائية طلب اتخاذ إجراء قضـــائي من إجراءات الدعوى الجزائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها؛ لضـرورة ذلك في الفصـل في مسـألة معروضـة على السلطة القضـائية في الدولة الطالبة، ويتعذر عليها القيام به بنفسـها؛ لوجوده خارج

[1] المعاهدة النموذجية بشـأن نقل الإجراءات في المسـائل الجنائية 1990م، اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م، النموذج الإرشـادي لاتفاقية التعاون القانوني والقضـائي الصـادر عن مجلس التعاون الخليجي في 2003م، أشـار إليها: خالد محمد علي الكميم، *مرجع سـابق*، ص148.

[2] الاتفاقية الأوروبية المادة (35)، أشـار إليها: ورقة عمل من إعداد الأمانة، بعنوان: *الاعتبارات العملية والممارسـات الجيدة والصـعوبات القائمة في مجال نقل الإجراءات الجنائية، بصـفته شـكلاً منفصـلاً من أشـكال التعاون الدولي في المسـائل الجنائية*، مؤتمر الأطراف في اتفاقية الأمم المتحمدة لمكافحة الجريمة المنظمة عبر الوطنية، فيينا، 2017م، ص12.

حدودها الجغرافية، وقد أقرت العديد من الاتفاقيات الدولية بالإنابة القضـــائية، كمعاهدة الأمم المتحدة النموذجية بشـــأن نقل الإجراءات في المســـائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م في المادة (21) منها (الدسوقي، 2009، صفحة 601).

ويمكن تعريفها على أنها: طلب من الســلطة القضـــائية المنيبة إلى الســلطة المنابة، قضـــائية كانت أم دبلوماسـية، أساسـه التبادل بإتخاذ اجراء من إجراءات التحقيق أو جمع الأدلة في الخارج، وكذلك أي إجراء قضـائي آخر يلزم اتخاذه؛ للفصـل في مسـألة منظورة أمام القاضـي المنيب، ليس في مقدوره القيام به في نطاق دائرة اختصاصه في الدولة التي يأتمر بأوامر مشرعها (عبد العال، 1998).

وعليه فإن الإنابة القضـائية تعمل على تسـهيل الإجراءات الجزائية بين الدول، بما يضـمن إجراء التحقيقات الضـرورية لتقديم المتهمين للمحاكمة، وتطبيق العدالة الجنائية، وكذلك التغلب على السـيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسـة بعض الإجراءات القضـائية داخل أقاليم دول أخرى، وتسـتلزم إرسـال ملف خاص بالدعوى الجزائية بمرفقاته أي محاضـر جمع الاسـتدلال والتحقيق والمسـتندات، والتي أجريت بمعرفة السلطة القضـائية في الدولة طالبة الإنابة إلى السلطة القضـائية في الدولة المطلوب اتخاذ بعض الاجراءات على إقليمها (الدسوقي، 2009).

الفرع الثالث: التعاون الدولي بشأن تسليم المجرمين لمواجهة الجرائم الإلكترونية

حيث يعد تسـليم المجرمين واحداً من أهم مجالات التعاون الدولي، إلا أنه قد يمس بأمورٍ حسـاسـة تتعلق بالسـيادة، وقد يكون في بعض الحالات موضـع جدل أسـاسـي، حيث يتناول هذا الفرع تعريف تسـليم المجرمين والشروط اللازمة لإجراء تسليم المجرمين بين الدول على النحو التالي:

أولاً: تعريف تسـليم المجرمين: هو مجموعة من الإجراءات القانونية التي تهدف إلى قيام دولة بتسـليم شـخص متهم أو محكوم عليه إلى دولة أخرى؛ لكي يحاكم بها أو ينفذ فيها الحكم الصـادر من محاكمها عليه (سليمان أ.، 2006).

ويعرّف أيضـاً: أن تتخلى الدولة عن شـخص موجود في إقليمها إلى دولة أخرى بناء على طلبها؛ لتحاكمه عن جريمة يعاقب عليها قانوناً أو لتنفيذ حكم صادر من محاكمها (سليمان أ.، 2006).

وقد عرّفت المحكمة الجنائية الدولية تسـلم المجرمين في المادة (102) من نظامها الأسـاس على أنه: "التسليم يعني نقل دولة ما شخصاً إلى دولة أخرى بموجب معاهدة أو اتفاقية أو تشريع وطني"[1].

وبناءً على ما سبق لم يعد الطابع الذي تمتاز به الجرائم الإلكترونية بأنها عابرة للحدود عائقاً أمام ملاحقة مرتكبي هذه الجرائم ومعاقبتهم؛ وذلك من خلال اتفاقيات تسـليم المجرمين التي تتيح للدولة الحصـول على المتهمين والمجرميين الفارين من العدالة؛ لمحاسـبتهم على أفعالهم، مما جعل للدول إمكانية تجاوز حدودها الإقليمية وممارسة أعمالها القضائية وفقاً لقوانينها الوطنية.

وقد كان موضـوع تسـليم المجرمين في مجال مواجهة الجرائم الإلكترونية موضـوع العديد من الاتفاقيات والمعاهدات الدولية، أهمها معاهدة بودابيسـت لمكافحة جرائم الإنترنت في المواد (25/24/23/12) منها، وكذلك توصـيات المجلس الأوروبي بشـأن مشـاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات من خلال التوصية رقم (95/13) بتاريخ 1995/9/11م[2].

[1] نظام روما الأساسي للمحكمة الجنائية الدولية، دخل حيزالنفاذ في 2002/7/1م.

[2] اتفاقية الجرائم الإلكترونية تم تبنيها من قبل مجلس أوروبا في 2001م، ودخلت حيز التنفيذ في 2004م، سـيد طنطاوي محمد سـيد، بحث بعنوان: *الجريمة المعلوماتية (الصـعوبات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها)*، المركز الديمقراطي العربي، الدراسـات الاسـتراتيجية والسـياسـية والإقتصادية، 2018م.

ثانياً: الشـروط اللازمة لإجراء تسـليم المجرمين بين الدول: إن تسـليم المجرمين لا يتم إلا بوجود بعض الشروط والضوابط الشكلية، والتي لا بد من توافرها؛ لإتمامه بالشكل القانوني (الدسوقي، 2009، صفحة 612)، ومن أهمها:

1. أن يكون الفعل المطلوب التسـليم من أجله فعل مجرم في الدولتين أي الدولة الطالبة للتسـليم، والدولة المطلوب منها التسـليم، وهذا ما يسـمى بازدواجية التجريم، واتفاقاً مع المبادئ العامة في القوانين الجزائية "لا جريمة ولا عقوبة إلا بنص".[1]

2. أن يكون الفعل المرتكب من الجرائم التي يجوز بشـأنها التسـليم، وذلك لوجود قائمة تتضـمن الجرائم التي لا يجوز التسليم فيها، كالجريمة التي تنحصر في الإخلال بواجبات عسكرية.

3. أن يكون التسـليم في الجرائم ذات الخطورة كالجنايات والجنح، بحيث لا تقل العقوبة عن الحد الأدنى الذي تحدده الاتفاقيات المنعقدة بين الدول.

4. أن لا تكون العقوبة أو الدعوى سـقطت بإحدى أسـباب السـقوط، كسـقوطها بالتقادم أو العفو العام أو الخاص، أو بموجب أي من قوانين الدولتين.

5. أن يحاكم المجرم فقط على الجريمة التي تم التسـليم من أجلها، وذلك للحيلولة دون اسـتغلال بعض الدول بهذه الاتفاقيات بإخفاء الحقيقة وراء طلب التسـليم، كون أن حسـن النية واجب في العلاقات الدولية، مما يسـتوجب الالتزام بممارسـة الإجراءات الجزائية بحق المجرم عن الوقائع التي تم الاتفاق على التسليم بشأنها فقط (العقبي، 2024).

أما فيما يتعلق بنظام تسـليم المجرمين في الأراضـي الفلسـطينية، فقد نصـت المادة (8) من قانون تسـليم المجرمين رقم (56) لسنة 1926م، النافذ في الضفة الغربية، والذي وضعته الحكومة البريطانية، جاء فيه: "الحالات التي ينطبق فيها هذا القانون على طلبات التسـليم المقدمة من أية دولة أجنبية، كل مجرم فار من

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية في المادة (16) منها.

بلاد تلك الدولة موجود في أي قسم من فلسطين أو يشتبه بوجوده في أي قسم منها يعرض نفسه للقبض عليه وتسليمه بالصورة المنصوص عليها في هذا القانون سواء ارتكب الجريمة المطلوب تسليمه من أجلها قبل العمل بهذا القانون أم بعده وسواء أكانت لأية محكمة في فلسطين صلاحية مشتركه للنظر في تلك الجريمة أم لم تكن"[1].

المطلب الثاني: دور الهيئات والمنظمات في تفعيل التعاون الدولي

يتناول هذا المطلب الهيئات الدولية التي تعمل على تفعيل التعاون الدولي لمواجهة الجرائم الإلكترونية، وذلك في الفرع الأول منه، بينما يتناول الفرع الثاني الاتفاقيات الدولية التي تناولت مواجهة الجرائم الإلكترونية في بنودها على النحو التالي:

الفرع الأول: الهيئات والمنظمات الدولية

تشكل الهيئات الدولية والمنظمات العالمية الركيزة الأساسية التي يتم من خلالها التعبير عن مختلف آراء واقتراحات أشخاص المجتمع الدولي؛ لإيجاد حلول للتصدي للجرائم الإلكترونية وتقييدها، ويتم ذلك على شكل اتفاقيات ومعاهدات بين الدول، ومن المنظمات التي كان لها دور في مواجهة الجرائم الإلكترونية:

أولاً: منظمة الأمم المتحدة: لمنظمة الأمم المتحدة جهوداً كبيرة في مواجهة الجرائم الإلكترونية، حيث توصلت المنظمة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين إلى إصدار قرار خاص يتعلق بالجرائم المعلوماتية، وفي سنة 2000م قد تبنت المنظمة الأمم المتحدة الاتفاقية الخاصة لمكافحة إساءة استعمال التكنولوجيا؛ لأغراض إجرامية، وقد أكدت على ضورة التنسيق فيما بين الدول؛ لتتبع الجرائم الإلكترونية، كما أنها عقدت سنة 2010م المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية، فقد ناقشت

[1] قانون تسليم المجرمين رقم (56) لسنة 1926م.

الدول الأعضـاء آخر التطورات في اسـتخدام التكنولوجيا الحديثة من قبل المجرمين، ومن ضـمنها الجرائم الإلكترونية حيث كان لها موقعاً بارزاً في جدول أعمال المؤتمر (العذار، 2017).

ثانياً: منظمة الشـرطة الجنائية الدولية: قد تطرقنا سـابقاً إلى جهود الإنتربول عند الحديث عن التعاون الأمني الدولي في مواجهة الجرائم الإلكترونية، وبيّنا الجهود التي بذلتها المنظمة في سـبيل مواجهة هذه الجرائم، وكان آخر أعمالها اجتماع الجمعية العامة ال26 للشـرطة الجنائية الدولية (الإنتربول) بالعاصـمية الصينية (بكين) في 2017م بمشاركة فيما يقارب 1000 من كبار قادة الشرطة والسياسيين في 156 دولة، ومن أهم الأمور التي تمت مناقشتها جرائم الإنترنت والقرصنة الإلكترونية، والمخاطر الناجمة عنها، وكيفية التصـدي لها على المسـتوى الدولي (بوشـعرة و موسـاوي، 2018، صـفحة 53؛ العذار، 2017، صـفحة 414).

ثالثاً: المجلس الأوروبي: حيث كان للمجلس الأوروبي دور واضـح في مواجهة الجرائم الإلكترونية من خلال إقراره العديد من التوصـيات الخاصـة بحماية البيانات ذات الصـبغة الشـخصـية من سوء الاسـتخدام، ومن جهود المجلس الأوروبي في مواجهة الجرائم الإلكترونية: التوقيع على الاتفاقية الخاصـة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات والتي وقعت بين المجلس الأوروبي والسوق الاشتراكية، عدا عن اتفاقية بودابسـت لمكافحة الجرائم، والتي وقعها المجلس الأوروبي، إلا أن الجهد الرئيسـي للمجلس الأوروبي لمواجهة الجرائم الإلكترونية يتمثل في إصداره الاتفاقية الأوروبية لمكافحة الجريمة عبر الإنترنت، حيث كان لهذه الاتفاقية دوراً كبيراً في مواجهة هذه الجرائم (بوشعرة و موساوي، 2018، صفحة 52).

رابعاً: الجامعة العربية: نظراً لانتشـار الجرائم الإلكترونية في الآونة الأخيرة وازدياد مخاطرها، وضـعف التشريعات الوطنية وحدها في التصدي لهذه الجرائم دفع الدول العربية إلى إيجاد طرق تشريعية لمواجهتها، ومنها القانون العربي الاسترشادي، حيث قامت جامعة الدول العربية من خلال الأمانة العامة لمجلس وزراء العدل العربي في دورة التاسـعة عشـر، باعتماد هذا القانون رقم (19-459) في 2003/10/8م، والذي

يعتبر من أهم الجهود العربية في مجال الحماية القانونية من الجرائم الإلكترونية (بوشـــعرة و موســـاوي، 2018، صفحة 55؛ العذار، 2017، صفحة 416).

الفرع الثاني: الاتفاقيات والمعاهدات الدولية

هنالك العديد من المعاهدات الدولية التي تعزز التعاون في مكافحة الجرائم الإلكترونية، وقد تطرقنا لبعضٍ منها سابقاً بشكلٍ متفرق وموجز؛ ليتناولها هذا الفرع جملةً واحدة بشيءٍ من التفصيل:

أولاً: اتفاقية المجلس الأوروبي بشأن جرائم الإنترنت: وهي الاتفاقية الأوروبية لجرائم الإنترنت، والتي تعتبر المعاهدة الدولية الأولى التي تسعى لمعالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى، فقد عملت اللجنة الأوروبية لمشاكل الجريمة بين العامين 1997 و2000م على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في 2001م، وتم التصديق عليها من قبل 30 دولة في 2010م، والتي تهدف إلى توفير الإجراءات اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونياً، وتوحيد الأحكام المتعلقة بالجرائم الإلكترونية مع عناصر القانون الجنائي المحلي، وكذلك وضع نظام سريع وفعال من أجل تحقيق التعاون الدولي (حشيفة، 2020، صفحة 31).

ثانياً: قرارات الجمعية العامة للأمم المتحدة: حيث ســـعت الأمم المتحدة من خلال قراراتها إلى حث الدول لمواجهة الجرائم الإلكترونية، وســـوء اســـتعمال تكنولوجيا المعلومات، وكان من أبرز هذه القرارات: القرار (121/45) لســـنة 1990م، والقرار (53/70) في 1998/12/4م، والقرار (49/54) في 1999/12/1م، والقرار (55/28) في 2000/11/20م، والقرار (56/19) في 2001/11/29م، والقرار (53/57) في 2002/11/22م، والقرار (32/58) في 2003/12/18م حول موضـــوع التطورات في ميدان المعلومات والاتصـــالات في سـياق الأمن الدولي (شـرشـر، 2021، صـفحة 534؛ حشـيفة، 2020، صـفحة 32؛ الجنبيهي و الجنبيهي، 2005، صـــفحة 194)، وقد أكد مؤتمر الأمم المتحدة الثالث عشـــر لمنع الجريمة والعدالة الجنائية على مكافحة الجرائم الإلكترونية، والذي انعقد في الدوحة بتاريخ 2015/4/14م، وما زالت

منظمة الأمم المتحدة تواصـــل جهودها من خلال عقد مؤتمرات ومعاهدات؛ لحماية الأنســـان ومواجهة مخاطر التكنولوجيا من خلال تعزيز التعاون بين أعضـــاء المجتمع الدولي؛ لاتخاذ الإجراءات المناســـبة (شرشر، 2021، صفحة 536).

ثالثاً: اتفاقية بودابسـت لمكافحة الجرائم المعلوماتية لسـنة 2001م: حيث وضـعت هذه الاتفاقية كم قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية وقد دخلت حيز النفاذ في 2004م، كما يمكن لأي دولة الإنضـــمام إليها، وقد بينت هذه الاتفاقية خطورة الجريمة الإلكترونية، وضـــرورة تضـــافر الجهود الدولية لمواجهتها، كما تضـــمنت مجموعة من القواعد التي تتعلق بالتعاون في ميدان مواجهة الجريمة الإلكترونية، كالقواعد الخاصـة بالاختصـاص الترابي للمحاكم في المادة (22) منها، وتسليم المجرمين في المادة (24) منها، واعتماد شبكة مفتوحة كامل الأسبوع مخصصة لبقية الأعضاء من أجل توفير المسـاعدة في الأبحاث المرتبطة بالجرائم الإلكترونية (العذار، 2017، صـفحة 416؛ الجنبيهي و الجنبيهي، 2005، صفحة 180)[1].

رابعاً: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: حيث يعد القانون العربي النموذجي لمكافحة جرائم الكمبيوتر خطة فعالة في مواجهة الجرائم الإلكترونية، حيث صـــدر هذا القانون كثمرة عمل مشـــترك بين مجلس وزراء داخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية، وذلك بعد أن قدم كلا المجلسين مشروعاً بخصـوص مكافحة الجريمة الإلكترونية، وقد تضـمن هذا القانون تعداد الجرائم التي تقع عن طريق الحاسبات الآلية والانترنت بصفة عامة، والعقوبات المقررة لها، بالإضافة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تمت الموافقة عليها في 2010/12/21م حيث تحتوي على 43 مادة تهدف إلى تدعيم التعاون بين الدول العربية في مجال مكافحة الجرائم الإلكترونية؛ للحفاظ على سلامة وأمن أفراد دول الأعضاء (حشيفة، 2020، صفحة 34)[2].

[1] اتفـاقيـة بودابيســـت من خلال الرابط الإلكتروني التـالي: https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174، تاريخ آخر زيارة 2025/3/3م.

[2] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال الرابط الإلكتروني التالي: https://fc-lc.xyz/3auel، تاريخ آخر زيارة 2025/3/3م.

الفصل الثالث

إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية وآليات التغلب عليها

أدرك المجتمع الدولي خطورة سوء استخدام التكنولوجيا، والتي ينبثق عنها ارتكاب الجرائم الإلكترونية، وقد انتشرت بشكل واسع في الآونة الأخيرة، فلا شك في ضرورة التعاون الدولي لمواجهة هذا النوع من الجرائم، واتخاذ الإجراءات اللازمة التي تهدف لمواجهتها والتقليل منها بقدر من الإمكان، وبالرغم من الجهود التي بذلتها الدول في عقد اتفاقيات ومؤتمرات في سبيل مواجهة هذه الجرائم، والتي ذكرناها سابقاً، إلا أنه لا يخلو الأمر من الإشكاليات التي تشكل عائقاً أمام تحقيق التعاون الدولي أهدافه في مواجهة الجرائم الإلكترونية؛ نظراً لاتساع عالم التكنولوجيا المتطور باستمرار؛ لذا جاء هذا الفصل يتناول الإشكاليات التي يواجهها التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الوطني والدولي؛ لبيان الإشكاليات التي تعيق التعاون الدولي، وهذا في المبحث الأول منه، بينما يتناول المبحث الثاني الحلول أو الآليات التي تمكّن الدول من التغلب على هذه الإشكاليات على النحو التالي:

المبحث الأول: إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الدولي والوطني

هنالك بعض الإشكاليات أو العوائق التي تحول دون إمكانية الدول من تحقيق أهدافها في مواجهة الجرائم الإلكترونية سواء على المستوى الوطني أو على المستوى الدولي، وهذا ما جاء به هذا المبحث، حيث يتناول في المطلب الأول منه إشكاليات التعاون الدولي على المستوى الدولي، بينما يتناول المطلب الثاني إشكاليات التعاون الدولي على المستوى الوطني على النحو التالي:

المطلب الأول: إشكاليات التعاون الدولي على المستوى الدولي:

للتعاون الدولي دوراً بارزاً في مواجهة الجرائم الإلكترونية، وبالرغم من عدم تحقيق القدر الكافي من الهدف المرجو من هذا التعاون إلا أن الجهود ما زالت مستمرة ومتزايدة في ظل القضاء على الجرائم الإلكترونية،

إلا أن هذه الجهود تواجه بعض الإشكاليات على المستوى الدولي، والتي تحول بينها وبين مواجهة الجرائم الإلكترونية يتناولها هذا المطلب في فروعه، ومن أهمها:

الفرع الأول: القصور التشريعي[1] للدول والتعارض بين مصالحها

تعد هذه الإشكالية تحدياً كبيراً يواجه التعاون الدولي في مواجهة الجرائم الإلكترونية؛ لما للقصور التشريعي من تأثير على وضع مفهوم ونظام قانوني خاص بالجرائم الإلكترونية، وما يترتب على التعارض بين مصالح الدول من مشاكل في تطبيق القانون من الناحية العملية مما يجعل تحقيق التعاون أمراً صعباً (أبو نمر و بوكشريدة، 2021–2022، صفحة 44).

وباستقراء الأنظمة القانونية النافذة في العديد من الدول نجد عدم وجود نظام قانوني موحد خاص بمواجهة الجرائم الإلكترونية، فما يكون مباح بأحد الأنظمة يكون مجرماً في نظام آخر، ويعود ذلك لعدة أسباب أهمها:

1. الاختلاف ما بين البيئات والعادات والديانات والثقافات من مجتمع لآخر، وبالتالي الاختلاف في السياسات التشريعية فيما بين الدول المختلفة.
2. كثرة المفاهيم القانونية التي تتعلق بالجرائم الإلكترونية، حيث تضع كل دولة تعريفاً حسب أنظمتها القانونية الجزائية (أكلي و عاشور، 2023–2022؛ أبو نمر و بوكشريدة، 2021–2022).

ولهذه الأسباب إنعكاساً سلبياً أثر على إجراءات التعاون الدولي في مواجهة الجرائم الإلكترونية، فانعدام النص على جميع الجرائم الإلكترونية يؤثر على مختلف مجالات الحياة، كما أن القصور التشريعي للدول في وضع نظام قانوني خاص بالجرائم الإلكترونية يؤدي إلى إفلات المجرمين من العقاب، وتهربهم من تعويض المجني عليه، بالإضافة إلى التعارض ما بين الدول، فهو بمثابة تحدي كبير يواجه التعاون الدولي في سبيل هذه المواجهة، كون أن أغلب الدول تلجأ إلى تغليب مصالحها على حساب تحقيق العدالة الجنائية.

[1] هو نقص أو عدم كفاية التشريعات الحالية مما قد يؤدي إلى عدم إمكانية تطبيق القوانين بشكل كامل أو فعّال، محمد نجم محسن، بحث بعنوان: *دور القاضي الدستوري في إصلاح القصور التشريعي*، المجلة القانونية، مجلة متخصصة في مجال البحوث القانونية، ص921.

الفرع الثاني: اختلاف النظم القانونية الإجرائية وتنوعها

هنالك بعض الاختلاف في إجراءات ضـــبط ومتابعة الجرائم من دولة إلى أخرى، فنجد أن هذه الإجراءات المتمثلة في التحري والتحقيق والمحاكمة قد تتخذها بعض الدول وتثبت فاعليتها في حين تكون في دولة أخرى عديمة الفائدة على سبيل المثال المراقبة الإلكترونية، والتسليم المراقب وغيرها من الإجراءات المماثلة (بوربابة، 2019).

وقد تعتبر طريقة معينة من طرق جمع الاستدلالات أو التحقيق على أنها قانونية في دولة معينة في حين تكون غير مشروعة في دولة أخرى، مما يجعل الدولة الطالبة في خيبة أمل من قدرتها على تنفيذ قانونها الخاص بها في الدولة الأخرى، غير أن السلطات القضائية في الدولة المطلوب منها قد لا تسمح باستخدام الأدلة التي استندت إليها الدولة الطالبة في تجريمها للفعل المرتكب، ويعود ذلك لعدم وجود تناسق بين قوانين الإجراءات الجزائية بين الدول المختلفة فيما يتعلق بمراحل الجرائم الإلكترونية، وإجراءاتها الجزائية من إثبات وتحري وتحقيق، مما يعيق التعاون الدولي في مواجهة هذا النوع من الجرائم (عبد الحفيظ، 2005).

الفرع الثالث: تنازع الاختصاص القضائي الدولي

ويقصد بالإختصاص القضائي الدولي هو: ذلك الإختصاص الذي يخص علاقة قانونية يشوبها عنصر أجنبي في الخارج إذا لم تكن له رابطة أو مبرر داخل البلاد، ويعتمد هذا الاختصـــاص على على عنصـــر النفاذ أي مدى الفائدة العملية التي يمكن الحصول عليها من الحكم الصادر، ومدى ارتباط أشخاص العلاقة بدولة المحكمة (عرموش، 2005، صفحة 243).

وكون أن الجرائم الإلكترونية ذات طابع عالمي عابرة للحدود، فإنها تعد من أكثر الجرائم التي يثار بها موضـــوع تنازع الإختصـــاص القضـــائي بين الدول؛ لاحتمالية تضـــرر أكثر من دولة من هذه الجرائم مما يخلّف تنازع في الاختصـــاص القضـــائي لكل من الدول التي أطالتها هذه الجرائم، وبالتالي يســـاهم ذلك في إفلات المجرمين من العقاب في ظل هذا التنازع في الإختصـــاص القضـــائي الدولي؛ لعدم تحديد القانون

الواجب التطبيق على هذه الجرائم، وإعاقة إجراءات التحري والتفتيش خارج إقليم الدولة الوطني (أكلي و عاشور، 2023-2022، صفحة 55).

ويولد هذا التنازع في الجرائم الإلكترونية العابرة للحدود؛ لصعوبة تحديد الاعتبار الذي يجب الأخذ به؛ لتحديد الدولة صاحبة الاختصاص في النظر في هذه الجرائم، فمثلاً عند حدوث جريمة في إقليم دولة معينة من قبل أجنبي تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استناداً لمبدأ الإقليمية، في حين يكون الاختصاص للدولة الثانية على أساس مبدأ الإختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى؛ فتدخل في اختصاصها على أساس مبدأ العينية، كما وتثار فكرة التنازع في الإختصاص القضائي في حالة تأسيس الإختصاص على مبدأ الإقليمية، فمثلاً لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها من دولة أخرى، فيثبت الاختصاص هنا وفقاً لمبدأ الإقليمية لكل دولة من الدول التي مستها (أبو نمر و بوكشريدة، 2021-2022، صفحة 46؛ عرموش، 2005، صفحة 250 وما بعدها)، ومن هنا نجد أن التنازع في الإختصاص القضائي المتعلق بالجرائم الإلكترونية يعد عائقاً وتحدياً كبيراً أمام التعاون الدولي في مواجهة هذه الجرائم.

الفرع الرابع: الإشكاليات المتعلقة بتسليم المجرمين

وإن كان تسـليم المجرمين أحد أهم المطالب التي تسـعى له أغلب الدول في ظل تعاونها مع باقي الدول الأجنبية في مواجهة الجرائم الإلكترونية إلا أن هنالك بعض التحديات التي تحول دون تحققه، ومن أهمها:

أولاً: التجريم المزدوج: ويعرّف على أنه مبدأ قانوني في تسـليم المجرمين الدوليين حيث أن الجريمة التي يطلب تسـليم شـخص بسـببها يجب أن تكون جريمة في كل من الدول الطالبة والدولة المطلوب منها التسليم[1]، حيث يعد التجريم المزدوج من أهم الشروط المتعلقة بتسليم المجرمين كإحدى آليات التعاون الدولي

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية في المادة (16) منها.

في مواجهة الجرائم الإلكترونية، وذلك تطبيقاً لمبدأ شـــرعية الجريمة، فلا عقوبة ولا جريمة إلا بنص (الزهراني، 2020؛ الدسوقي، 2009، صفحة 612).

ويتحقق هذا الشرط شرط التجريم المزدوج فيما يتعلق بتسليم المجرمين وفقاً لأحد الأسلوبين: إما أسلوب القائمة الحصرية، ويعتمد على تعداد الجرائم التي يجوز فيها التسليم واستبعاد ما عداها، وإما أسلوب الحد الأدنى للعقوبة المقررة، وتعتبر اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية من الاتفاقيات التي تأخذ كأصل عام بنظام القائمة الحصرية (بشارة، 2018؛ تدريست، 2016).

وبالرغم من أهمية هذا الشرط إلا أنه لا يخلو من التحديات التي تعيق تطبيقه في بعض الحالات مما يجعله عقبة أمام التعاون الدولي في مواجهة الجرائم الإلكترونية، ففيما يتعلق بأسلوب القائمة الحصرية فإنه يعاب عليه بمحدوديته حيث يركز على بعض الجرائم بعينها، مما يحول دون مواجهة الجرائم المستحدثة، أما فيما يتعلق بأســـلوب الحد الأدنى فيثار هنا تحديات تنشـــأ عن اختلاف التكييف الجرمي في تشـــريع الدولتين الطالبة والمطلوبة إليها الأخذ بهذا الأسلوب، عدا عن التقيد في الحد الأدنى للعقوبة يحول دون الأخذ بنظام تسليم المجرمين في حال كانت الجريمة يعاقب عليها أقل من الحد الأدنى.

بالإضـــافة إلى أن بعض الدول لا تجرم الجرائم الإلكترونية من الأســـاس، عدا عن صـــعوبة تحديد ما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم الإلكترونية أو لا تطبقها، كما قد تتوسع بعض الدول في تفسير شرط ازدواجية التجريم مما يعيق تطبيق الاتفاقيات الدولية في مجال تســـليم المجرمين، مما يحول دون اتخاذ الإجراءات القانونية اللازمة، ومحاكمة مرتكبي الجرائم الإلكترونية (بوبعاية و والي، 2021).

ثانياً: عدم وجود نظام موحد للنشاط الإجرامي: أي عدم وجود اتفاق عام مشترك بين الدول المختلفة حول النماذج المتعلقة بالجرائم الإلكترونية الواجبة التسليم بشأنها، وغياب وجود مفهوم عام حول تعريف القانون للنشـــاط الإجرامي المتعلق بهذا النوع من الجرائم، فقد تكون هذه الجرائم تقليدية في بعض الأنظمة نظراً

لاختلاف العادات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسات التشريعية فيما بينها (أبو نمر و بوكشريدة، 2021–2022، صفحة 47؛ عبد الحفيظ، 2005، صفحة 2015).

ويعد هذا عائقاً أمام التعاون الدولي في مواجهة الجرائم الإلكترونية، ومعاقبة مرتكبيها على اعتبار أن هذا الاختلاف يجعل مستخدمي الحاسب الآلي يرتكبون الجرائم الإلكترونية دون التقييد بالحدود الجغرافية، وذلك بسبب عدم الاتفاق بين الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في هذه الجرائم (واصل، 2023).

ثالثاً: التزاحم في طلبات التسليم: ويقصد به أن تتلقى دولة طلباً من المحكمة بالقبض على شخص وتسلميه إليها، وتتلقى طلباً آخر من أية دولة أخرى طرف أو غير طرف بتسليم نفس الشخص سواء عن السلوك ذاته أو عن سلوك آخر غيره (الإكيابي، 2017).

وتنتج هذه الإشكالية في مواجهة الجرائم الإلكترونية نظراً لطبيعة هذه الجرائم بأنها عابرة للحدود، وبالتالي فإن مرتكبها قد يرتكب جريمة أو أكثر من الجرائم الإلكترونية تمس بمصالح أكثر من دولة في ذات الوقت، مما يؤدي إلى تزاحم في طلبات التسليم المقدمة ضد مرتكب هذه الجرائم من قبل الدول التي مست بمصالحها.

ولاعتبار أن هنالك حالة ازدحام في طلبات التسليم يجب أن تقوم كل دولة طالبة بتقديم الأدلة التي تثبت قيام الشخص المطلوب تسليمه بارتكابه جريمة الكترونية بشكل يقيني، وليس مجرد اتهام أو ادعاء، كما يجب عليها أن تقوم بتقديم طلب فعلي، وليس الاكتفاء فقط بإبدائها لرغبتها في استلام الشخص المطلوب تسلميه، وتتحقق إشكالية الازدحام في طلبات التسليم بتعدد الطلبات إلى الدولة المطلوب إليها بغض النظر عن الفارق الزمني بين الطلبات طالما أن الشخص ما زال متواجد على أراضيها، ولم يغادر أو يسلم إلى أي دولة أخرى (حشيفة، 2020، صفحة 51).

رابعاً: عدم وجود قنوات اتصـــال: يعد الحصـــول على المعلومات والبينات المتعلقة بالمجرمين الفارين من العدالة خارج أراضـــيهم الإقليمية من أهم أهداف التعاون الدولي في مجال تســـليم المجرمين للحد من الجرائم بشـــكل عام، والجريمة الإلكترونية بشـــكل خاص، ولتحقيق هذه الهدف من التعاون كان لابد من وجود قنوات اتصـــال تســـمح للجهات القائمة بالتواصـــل مع الجهات الأجنبية من أجل جمع أدلة أو معلومات هامة تتعلق بهذه الجرائم ومرتكبيها؛ لإمكانية تطبيق الاتفاقيات المتعلقة بتســـليم المجرمين (خراشي، 2014، صفحة 137).

وغياب هذه القنوات يحول دون القدرة على الإحاطة بالأدلة اللازمة والمعلومات العملية، والتي تفيد في مواجهة الجرائم الإلكترونية ومعاقبة الجناة، مما يجعلها عائقاً يقف أمام التعاون الدولي في مواجهته للجرائم الإلكترونية، من خلال بطء تبادل المعلومات بين الدول، وتأخير مشـــاركة الأدلة والمعلومات مما يعطي الجناة وقتاً كافياً في الفرار وإخفاء أدلة الجريمة المرتكبة (خراشي، 2014، صفحة 138).

الفرع الخامس: الإشكاليات المتعلقة بالإنابة القضائية

بالرغم من أن الإنابة القضـائية تعد أسـلوباً هاماً من أسـاليب التعاون الدولي في المجال الجنائي، والتي يتم بواســـطتها التغلب على العقبة التي تعيق تطبيق قانون الإجراءات الجزائية لدولة ما على الجرائم المرتكبة داخل إقليم دولة أخرى، وأحد صـور المسـاعدة القضـائية في مجال مواجهة الجرائم الإلكترونية (بن يحيى، 2017، صـــفحة 11)، إلا أن هنالك بعض التحديات التي تتعلق بها تحول دون تحقيق التعاون الدولي أهدافه المرجوة في مواجهة الجرائم الإلكترونية ومن أهم هذه التحديات:

أولاً: فكرة السيادة: بقيت فكرة السيادة على مر العصـور محافظةً على مكانتها باعتبارها الحجر الأسـاسـي في التنظيم الدولي، إلا أنه وفي الآونة الأخيرة بدأت تتراجع تلك المكانة نتيجة المستجدات التي طرأت على الســاحة الدولية، وتعد من هذه المســتجدات الجرائم العابرة للحدود، مما نتج عنها تصــادم بين المفهوم أو المكانة المطلقة للسيادة، وما بين هذه المستجدات.

ويقصد بالسيادة: السلطة العليا للدولة حيث لا تعلوها سلطة أخرى، مما يتيح لها صلاحية ممارسة مهامها ووظائفها على رعاياها وإقليمها دون تدخل أي دولة أخرى (بن يحيى، 2017، صفحة 18).

ويعود ذلك إلى أن الجرائم الإلكترونية عندما ترتكب في إحدى الدول، وتجري محاكمة مرتكبها في دولة أخرى، فلا بد من البحث والتحري عن كافة الأدلة الثبوتية التي تتعلق بالجريمة في البلد الذي ارتكبت فيها، على اعتبار أن هذه الدولة هي مسرح الجريمة، وهذا ما يجسد فكرة التعاون القضائي الدولي، إلا أن هذا التعاون قد يصطدم بفكرة السيادة الإقليمية لكل دولة من الدول، فكل دولة ترغب في القيام بنفسها وعبر جهازها القضائي بالفصل بكافة المنازعات التي تثار على أراضيها؛ لاعتبارات تتعلق بفكرة السيادة، ومن هنا تعد السيادة تحدياً أمام التعاون القضائي بين الدول في مواجهة الجرائم العامة، ومن بينها الجرائم الإلكترونية (الشاذلي، 2018، صفحة 202).

ثانياً: إجراءات الإنابة: إن إتمام الإنابة القضائية التي تعد من أهم المساعدات القضائية على المستوى الدولي بالطرق الدوبلوماسية يجعلها تتسم بالبطء والتعقيد في التنفيذ، فيتعارض وطبيعة الإنترنت وما يتميز به من سرعة مما يعيق مواجهة الجرائم الإلكترونية (أبو نمر و بوكشريدة، 2021–2022، صفحة 49).

عدا عن التباطؤ الذي يواجه هذه الإنابة في الرد عليها، فغالباً ما تكون الدول المطلوب إليها التسليم متباطئة في الرد لسبب إما نقص في الموظفين المدربين أو نتيجة للصعوبات اللغوية، والفوارق فيما بينها في الإجراءات المتعلقة بعقد الإستجابة، وغيرها من الأسباب التي تعد عائقاً أو تحدياً كبيراً أمام التعاون الدولي في مواجهة الجرائم الإلكترونية ومعاقبة مرتكبيها (أبو نمر و بوكشريدة، 2021–2022).

الفرع السادس: الإشكاليات المتعلقة بالتدريب في مجال مواجهة الجرائم الإلكترونية

يعد التدريب في مجال مواجهة الجرائم المستحدثة وخاصة فيما يتعلق بالجرائم الإلكترونية من الأمور الهامة، والتي لا بد منها من أجل إمكانية مواجهتها على أكبر قدر ممكن، ونظراً لخاصيتها التي تحتاج إلى

قدرات وخبرات معينة؛ للتعامل معها بسـهولة وفهم اسـتخداماتها، وغياب هذا يشـكل تحدياً يقف في وجه التعاون الدولي في تحقيق أهدافه المرجوة في مواجهة الجرائم الإلكترونية.

وتتمثل هذه التحديات في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب؛ لاعتقادهم بانعدام دورها في تطوير العمل من خلال الانصياع لما تعلّمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات، كما تعد الفوارق الفردية بين المتدربين على مواجهة الجرائم الإلكترونية، وتأثيرها على اكتسابهم للمهارات المستهدفة والمرجوه من هذه الدورات التدريبية، وخاصة ما يتعلق بتكنولوجيا المعلومات وشبكات الاتصال وما يرتبط بها، فنجد بعض الأشخاص على اطلاع واهتمام بهذا المجال، ولديهم معرفة كبيرة بها، بينما نجد البعض الآخر لا يعني لهم هذا المجال شـيء، مما يعد ذلك عائقاً في مواجهة هذا النوع من الجرائم من قبلهم (الشمري، 2016، صفحة 128).

وأيضـاً من التحديات هنا التي تؤثر على عملية التدريب والتعاون الدولي في مواجهة الجرائم الإلكترونية ما يتعلق بالظروف العامة المميزة للبيئة التدريبية، ومدى قدرتها على تمثيل الواقع العلمي لبيئة العمل الطبيعية تمثيلاً دقيقاً، وما يدور حولها من وقائع وملابسـات وإجراءات، وما يتم فيها من نشـاطات، فغالباً ما تفقد الدورات التدريبية هذه القدرة حيث لا يبلغ تدريبها حد التطابق مع طبيعة المهام التي سـيؤدونها المتدربون في بيئة العمل الطبيعية على أرض الواقع (الشمري، 2016).

المطلب الثاني: إشكاليات التعاون الدولي على المستوى الوطني

إلى جانب الإشكاليات التي تعيق التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الدولي هنالك بعض الإشكاليات التي تواجه التعاون الدولي على المستوى الوطني يتناولها هذا المطلب، ومن أهمها:

الفرع الأول: عدم كفاية القوانين الجزائية الداخلية وعدم ملائمتها

بالرغم من انتشـار اسـتخدام التكنولوجيا في الآونة الأخيرة، والاسـتعانة بها في جميع مجالات الحياة، حيث أصـبح الجميع يعتمد عليها في سـائر أموره العملية والشـخصـية، ومنهم الجناة مجرمي الجرائم الإلكترونية، والذين اسـتغلوا هذا التطور في ارتكابهم للجرائم، إلا أن هذا التطور لم يقابل بذات الدرجة في النصـوص القانونية المتعلقة بالجريمة.

فإن الكثير من النصوص القانونية الجزائية لبعض الدول لا تكفي لمواجهة هذا النوع من الجرائم المستحدثة؛ لتطلّبها الصـفة المادية في محل ارتكاب الجريمة، مما يتنافى وطبيعة الجريمة الإلكترونية؛ لارتكابها في العالم الافتراضي، والذي يخرجها من نطاق التجريم والعقاب (صالح، 2023).

وبالرغم من إصدار الدول الكثير من التشريعات المتعلقة بالجرائم الإلكترونية عدا عن انضمامها للعديد من الاتفاقيات الدولية، إلا أن هذه النصوص غير كافية في مواجهة هذا النوع من الجرائم، مما يؤدي إلى تقليل جهود الشـرطة في ضـبط هذه الجرائم، وفيما يتعلق بالقواعد العامة التي في التشـريعات الداخلية المتعلقة بالجريمة التقليدية، فإن تطبيقها على الجرائم الإلكترونية أمر في غاية الصعوبة نظراً لاختلافها عن الجريمة التقليدية من حيث شروط وأركان الجريمة لغياب المادية في وقائع الجريمة الإلكترونية، مما يجعل ذلك أحد التحديات التي تواجه التعاون الدولي على المسـتوى الوطني في تحقيق أهدافة المرجوة بمواجهة الجرائم الإلكترونية، وملاحقة مرتكبيها (صالح، 2023).

الفرع الثاني: صعوبة اكتشاف الجرائم الإلكترونية وإثباتها

وتعود صعوبة اكتشاف الجرائم الإلكترونية إلى أن هذه الجرائم تتصف بالخفاء؛ لعدم وجود آثار مادية يمكن متابعتها، فهذا النوع من الجرائم ترتكب في بيئة إلكترونية يتم من خلالها نقل البيانات عبر الحسـابات الإفتراضـية الوهمية، وصـعوبة الاحتفاظ الفني بآثارها إن وجدت، فهي ليسـت أموالاً أو مجوهرات يمكن الاحتفاظ بها، بل هي مجرد أرقام تتغير في السـجلات، وهذا ما يزيد من صـعوبة عمل مأموري الضـبط

القضائي في كشف الجرائم الإلكترونية، بالإضافة إلى أنها غالباً ما تكتشف بمحض الصدفة؛ فهذه الجرائم من النادر اكتشافها أو ملاحظتها من قبل المجني عليه؛ لذلك توصف بالجرائم غير المرئية (الخراشي، 2015؛ عفيفي، 2000).

عدا عن طبيعة الجرائم الإلكترونية العابرة للحدود التي تتسم بالطابع الدولي، مما يجعل مسرح هذا النوع من الجرائم ليست محلية بل عالمية، مما يزيد في صعوبة اكتشافها، وما يزيد الأمر تعقيداً هو أن الجرائم الإلكترونية عادةً ما تتم عن بعد، حيث لا يتواجد الفاعل في مسرح الجريمة، وبالتالي تتباعد المسافات بين الفاعل والنتيجة (الخراشي، 2015؛ عفيفي، 2000).

أما بالنسبة لإثبات الجرائم الإلكترونية فهي مسألة في غاية الأهمية، فلا وجود للجريمة دون دليل قائم على إثباتها وإسنادها للمتهم، ونظراً لصعوبة إثبات هذه الجرائم نتيجةً لطبيعتها القائمة على ارتكابها عبر شبكات الإنترنت العابرة للحدود أصبح ذلك عائقاً أمام التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الوطني ويعود ذلك إلى عدة أسباب أهمها:

أولاً: الطبيعة الخاصة للدليل في الجرائم الإلكترونية: فالدليل في الجرائم الإلكتروني ليس دليلاً مرئياً يمكن فهمه بمجرد القراءة، بل هي عبارة عن بيانات غير مرئية تفصح عن شخصية معينة عادةً، وتظهر هذه الصعوبة بشكل واضح في الجرائم المرتكبة عبر الإنترنت بواسطة البريد الإلكتروني، حيث يكون من الصعب على الجهات المختصة تحديد مصدر الإرسال، والوصول إلى بياناته (الشمري، 2016، صفحة 174).

ثانياً: سهولة القيام بإخفاء معالم الجريمة: ويتمثل ذلك في عدم القدرة على تحديد مصدر مرتكب الفعل، بحيث إذا تم ارتكابها في وقت ما في حين ظهرت النتيجة بعد فترة زمنية من ارتكابه يصعب تحديد الشخص المسؤول عن الفعل المرتكب، وتحديد الظروف المحيطة بالجريمة المرتكبة، ومثال على ذلك قيام شخص ما بزرع برنامج فايروس، وقد يكتشف وجوده بعد قيامه بتحقيق آثاره التدميرية للمعلومات (عبد الحفيظ، 2005، صفحة 214).

ثالثاً: صعوبة الوصول إلى دليل في بعض الأحيان: ويقصد بالدليل: المعلومات التي قد تحاط بوسائل فنية لحمايتها، وتشكل هذه الوسائل عائقاً أمام عملية البحث والتحري والاطلاع من قبل الفريق المختص، فعادةً ما تقوم الشـــركات العالمية على الإنترنت بوضـــع حماية أمنية على بياناتها المخزنة على خوادمها؛ لمنع الوصول غير المشروع إليها من أجل تدميرها أو الاطلاع عليها أو نسخها، ومن جهة أخرى قد يقوم الجاني بزيادة صـعوبة عملية ضـبط أي دليل يدينه، وخاصـة إذا كان من الأشـخاص ذو مهارات عالية في مجال الأمن المعلوماتي (أبو نمر و بوكشريدة، 2021–2022؛ عبد الحفيظ، 2005).

رابعاً: وجود كم كبير من المعلومات يتعين فحصـــها: للوصـــول إلى أدلة الجريمة الإلكترونية يتعين على جهات الاختصـاص البحث عن جميع المعلومات التي قد تفيد في الكشـف عن هذه الجريمة مما يضـعهم أمام البحث في كم كبير من الملفات والبرامج المخزنة، والتي قد تكون غالباً على ارتباط بمعلومات خاصـة بارتكاب الجريمة، مما يشـكل صـعوبة أمام رجال الأمن في ملاحقة مرتكبي الجرائم الإلكترونية، وذلك يعود إما لطبيعة المعلومات التي يتم البحث عنها، وإما لنقص الخبرة الفنية لدى رجال الأمن في ملاحقة تلك الأدلة، مما يتطلب مع البحث اســـتغراق فترة زمنية كبيرة تعيق مواجهة هذا النوع من الجرائم، وملاحقة مرتكبيها (كيلاني، 2024؛ عبد الحفيظ، 2005).

خامساً: إحجام الكثير من الجهات عن التبليغ عن تلك الجرائم: حيث تتجنب أغلب الجهات المتضررة من الجرائم الإلكترونية عن التبليغ عن هذه الجرائم؛ لعدم الإسـاءة إلى طبيعة عمل المنشـأة، وعدم بيان عجزها عن تحقيق الأمن الكافي للمعلومات المتعلقة بالعملاء، فقد يكون لذلك مردود ســـيء لدى عملاؤها عن طريق لجوء العديد منهم لســـحب أموالهم مما يؤدي إلى إفلاس المشـــروع، وعادةً ما تكون البنوك أو المؤسسات الإدخارية والاستثمارية أكثر حرصاً من غيرها في هذه الجرائم، مما يدفعها إلى الاكتفاء بإتخاذ إجراءات إدارية داخلية دون الإبلاغ عما تعرضـت له للسـلطات المختصـة؛ للحفاظ على عملائها (كيلاني، 2024، صفحة 213؛ عبد الحفيظ، 2005، صفحة 783).

الفرع الثالث: تناقض القوانين المطبقة في فلسطين

أما بالنسبة لإشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الوطني في فلسطين، فيعد تناقض القوانين من إحدى الإشكاليات التي تواجهها، فعلى سبيل المثال جريمة تسجيل المكالمات الصوتية، والتي يمكن تعريفها على أنها انتهاكاً لحرمة الحياة الشخصية للمواطن، كأن يقوم الجاني بسرق السمع أو أن يقوم بالتسجيل دون الإذن أو أن ينقله عن طريق أي جهاز من الأجهزة التكنولوجية الحديثة، مما يحقق له مصالح شخصية، وتلحق الضرر بالغير.

إلا أن القوانين النافذة قد وضعت بعض الاستثناءات التي تسمح بارتكاب هذا الفعل ضمن ضوابط قانونية معينة؛ لتحقيق مصلحة عامة، أو في سبيل الكشف عن جريمة معينة، ففي القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية نصت المادة (34) منه على: "1. يمكن للقاضي أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسى عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توفر دلائل جدية، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمها إلى النيابة العامة. 2. وللنائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأي بيانات، بما فيها حركة الاتصالات أو معلومات إلكترونية أو بيانات مرور أو معلومات المشترك التي يراها لازمة لمصلحة التحقيقات لغايات الفقرة (1) من هذه المادة، باستعمال الوسائل الفنية المناسبة، والاستعانة بمزودي الخدمات، حسب نوع الخدمة التي يقدمها"[1].

في حين نصت المادة (51) من قانون الإجراءات الجزائية رقم (3) لسنة 2001م على: " 1. للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق والبريد الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة وشخص مرتكبها. 2. كما يجوز له بمراقبة المحادثات السلكية واللاسلكية، أو

[1] القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

إجراء تسـجيلات لأحاديث في مكان خاص بناء على إذن من قاضـي الصـلح متى كان لذلك فائدة في إظهار الحقيقة في جناية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سـنة. 3. ويجب أن يكون أمر الضبط أو إذن المراقبة أو التسجيل مسبباً، ولمدة لا تتجاوز خمسة عشر يوماً قابلة للتجديد لمرة واحدة"[1].

وبالنظر لكلا القانونين وخاصـة النصـوص المذكورة أعلاه نجد أن وإن كانت المادة (34) من القرار بقانون قد انسـجمت في مضـمون الفقرة الأولى منها مع المادة (51) من قانون الإجراءات الجزائية، إلا أنها قد خالفتها في مضمون الفقرة الثانية، وقللت من ضمانات مراقبة الاتصالات، وذلك من خلال إسقاطها لشرط الحصـول على إذن قاضـي الصـلح بالجمع والتزويد الفوري للبيانات ومنها بيانات المرور، وكذلك إسقاطها لشرط جسامة الجريمة حين اشترط بأن تكون جناية أو جنحة لا تقل عقوبتها عن الحبس لمدة سنة[2].

وعليه يرى الباحث أن التناقض بين القوانين في فلسطين يشكل تحدياً كبيراً أمام التعاون الدولي في مواجهة الجرائم الإلكترونية، ومعاقبة مرتكبيها؛ لذا لا بد من أن يقوم المشـرع الفلسـطيني بإجراء التعديلات اللازمة على القوانين التي تتعلق بالجرائم الإلكترونية بما يجعلها منسـجمة فيما بينها من جهة، وبما يؤكد على ضرورة مواجهة هذا النوع من الجرائم على المستوى الوطني والمستوى الدولي من جهة أخرى.

المبحث الثاني: آليات التغلب على إشـكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الوطني والدولي

مع انتشـار الجرائم الإلكترونية في الآونة الأخيرة بات التعاون الدولي ضـرورة حتمية في مواجهة هذه الجرائم، والقضـاء عليها، إلا أن أغلب الدول قد واجهت العديد من الإشـكاليات التي شـكلت عائقاً أمام التعاون الدولي في مواجهته للجرائم الإلكترونية، وهذا ما بيناه سـابقاً، ونظراً لهذه الإشـكاليات فقد برزت العديد من الآليات التي تهدف إلى التغلب عليها، وبالتالي تعزيز التعاون الدولي؛ ليتمكن من تحقيق أهدافه

[1] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

[2] الهيئة المستقلة لحقوق الإنسان، *مذكرة قانونية حول القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية*، رام الله، 2018م، ص4.

في مواجهة الجرائم الإلكترونية، وهذا ما جاء به هذا المبحث حيث يتناول في المطلب الأول منه آليات التغلب على إشكاليات التعاون الدولي على المستوى الدولي، بينما يتناول المطلب الثاني آليات التغلب على إشكاليات التعاون الدولي على المستوى الوطني على النحو التالي:

المطلب الأول: آليات التغلب على إشكاليات التعاون الدولي على المستوى الدولي

يتناول هذا المطلب آليات التغلب على إشـــكاليات التعاون الدولي على المســـتوى الدولي، والتي تقابل الإشكاليات التي تم ذكرها سابقا، حيث يتناول الفرع الأول منه آلية التغلب على إشكالية القصور التشريعي للدول والتعارض بين مصـــالحها وتنوع اختلاف النظم القانونية، ويتناول الفرع الثاني آلية التغلب على إشكالية تنازع الإختصاص القضائي الدولي، ويتناول الفرع الثالث آلية التغلب على الإشكاليات الخاصة بتسليم المجرمين، بينما يتناول الفرع الرابع آلية التغلب على الإشكاليات الخاصة بالإنابة القضائية، ويتناول الفرع الخامس والأخير منه آلية التغلب على الإشـــكالية المتعلقة بالتدريب على مواجهة الجرائم الإلكترونية على النحو التالي:

الفرع الأول: آلية التغلب على إشكالية القصور التشريعي للدول والتعارض بين مصالحها وتنوع اختلاف النظم القانونية

يقتضي التغلب على هذه الإشكالية توحيد النظم القانونية المتعلقة بالجرائم الإلكترونية للدول، ونظراً لصعوبة هذا الأمر فلا بد من الدول أن تبرم إتفاقيات دولية أو إقليمية؛ لمواجهة هذه الجرائم؛ للتغلب على الإشكاليات التي تعيق التعاون الدولي في مواجهة الجريمة الإلكترونية.

وأنه لا بد من التعاون الدولي في التقليل من الفوارق بين الأنظمة الجزائية الداخلية، كون أن المجرم الإلكتروني سوف يبحث عن النظام القانوني الأكثر تسامحاً؛ للإفلات من العقاب؛ لذلك يعد التعاون الدولي خطوة لتدويل القانون الجنائي بقواعده الموضـوعية والإجرائية، وهو من قبيل التدابير التي تمنع الجريمة من خلال إحاطة المجرمين بالمســـؤولية الجزائية من جميع الدول مما يضـــيق إحتمالية إفلاتهم من العقوبة

القانونية، وللتغلب على إشكالية القصور التشريعي للدول فمن الضرورة الإنضمام للإتفاقيات الدولية التي تزيد التعاون والتنسيق بين جهود الدول في مواجهة هذه الجرائم، عدا عن التنسيق بين قوانينها، كما يجب على الدول سن قوانين وتشريعات خاصة؛ لتعدل قوانينها النافذة؛ لتوفير الحماية القانونية اللازمة ضد هذا النوع من الجرائم (صالح، 2023، صفحة 117).

ولا بد من الإشارة إلى أن هنالك فجوة ما بين الدول المتقدمة والدول النامية فيما يتعلق بسن التشريعات المتعلقة بالأمور المستحدثة، فأغلب تشريعات الدول النامية تعد متأخرة في مواكبة التطورات والمستجدات التشريعية العالمية، وخاصة فيما يتعلق بجرائم الإنترنت، والهادفة إلى حماية المنظومة المعلوماتية من الجريمة الإلكترونية، وقد يعود ذلك إلى التأخر التكنولوجي لهذه الدول، في حين تجد أن خطط مواجهة الجرائم الإلكترونية في الدول المتقدمة في تزايد مستمر على عكس الدول النامية (الزيدي، 2003، صفحة 128).

ومن الجهود الإقليمية في سبيل التغلب على إشكالية القصور التشريعي اعتماد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد قانوناً نموذجياً بموجب قرار رقم 229 لسنة 1996م، وبالرجوع إلى المذكرة الإيضاحية لهذا القانون نجد أنه قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص حيث نصت المادة (191) منه على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية، وكيفية جمع المعلومات الإسمية، وكيفية الإطلاع عليها (أبو نمر و بوكشريدة، 2021-2022، صفحة 61).

أما بالنسبة لإشكالية تنوع وإختلاف النظم القانونية والإجرائية نلاحظ اتجاه الدول لإصلاح التشريعات الإجرائية؛ لتواكب التطورات في الجرائم الإلكترونية، وذلك من خلال دمج كافة التطبيقات الناتجة عن التقنية الإلكترونية في مجال الإجراءات الجنائية، وتستجيب النصوص المستحدثة؛ لاحتياجات الشرطة القضائية.

ونلاحظ أن المواثيق الدولية عملت على تشجيع الدول على استخدام بعض تقنيات التحقيق الحديثة الخاصة، مما يقلل من اختلاف النظم القانونية والإجرائية بين الدول، وبالتالي يفتح المجال أمام تعزيز

التعاون الدولي، وقد أبرمت العديد من الاتفاقيات الدولية في هذا المجال؛ للتقريب بين القوانين الجزائية الوطنية؛ لمواجهة الجرائم العابرة للحدود، ويتجسد هذا التقارب في قبول حالات تفويض الإختصاص في إتخاذ إجراءات التحري وجمع الأدلة (صالح، 2023، الصفحات 117-118).

ومثال على ذلك ما جاء في المادة (20) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000م، حيث أشارت في هذا المجال إلى التسليم المراقب، والمراقبة الإلكترونية، وغيرها من أوجه المراقبة والعمليات المستترة؛ من اجل التصدي للجماعات الإجرامية المنظمة، وذلك بسبب الصعوبات الكامنة وراء محاولة الوصول إلى عملياتها، وتجميع المعلومات وأدلة الإثبات؛ لاستخدامها في وقت لاحق في الملاحقات القضائية سواء المحلية أو الدولية في دول الأطراف تحت إطار المساعدة القانونية المتبادلة (الحسيناوي، 2009، صفحة 158).

بالإضافة إلى ضرورة تعزيز التعاون بين أجهزة الشرطة في الدول المختلفة ضمن اتفاقيات دولية، لما في ذلك أهمية ودور كبير في تسهيل عملية تعقب الجرائم الإلكترونية والقبض على مرتكبيها، وتسريع تبادل المعلومات والأدلة، وكذلك تعزيز القدرات التقنية والتدريب من خلال تبادل الخبرات فيما بينهم؛ للوصول إلى تحقيق العدالة الجنائية (أبو نمر و بوكشريدة، 2021-2022، صفحة 63).

الفرع الثاني: آلية التغلب على إشكالية تنازع الإختصاص القضائي الدولي

ويكون التغلب على هذه الإشكالية من خلال اعتبار أن جميع الجرائم الإلكترونية من الجرائم الدولية، وتدخل في الاختصاص القضائي العالمي، وبالتالي يحق لكل الدول ملاحقة ومحاكمة مرتكبي الجرائم الإلكترونية دون النظر إلى جنسية الجاني، أو مكان الجريمة، ويعني ذلك أن الجرائم الدولية يكفي أن تشكل الجريمة تهديداً على أمن وسلامة المجتمع الدولي، أي أن لا يكون لها علاقة بمبدأ الإقليمية، وقد اتجهت العديد من التشريعات للاعتراف بمبدأ العالمية في الجرائم العابرة للحدود؛ لممارسة الملاحقة الجزائية من أجل التصدي

إلى هذا النوع من الجرائم، من خلال كسر قيود مبدأ الإقليمية، ومعاقبة الجناة (صالح، 2023، صفحة 119).

وعلى سبيل المثال فقد تبنت اتفاقية جنيف للبحار العالمية سنة 1958م مبدأ الاختصاص القضائي الدولي، فعملت على تخويل دولة القبض على لصوص قراصنة البحر حق محاكمتهم ومعاقبتهم دون النظر إلى جنسيتهم، والمكان الذي ارتكبت به الجريمة، وقياساً على ذلك يمكن تطبيقها على مرتكبي الجرائم الإلكترونية كونها عابرة لحدود، وأكثر خطورةً من القراصنة البحرية أو البرية[1].

الفرع الثالث: آلية التغلب على الإشكاليات المتعلقة بتسليم المجرمين

ومن أبرز الإشكاليات المتعلقة بتسليم المجرمين إشكالية إزدواجية التجريم، وإشكالية التزاحم في طلبات التسليم، أما بالنسبة **لآلية التغلب على الإشكالية الأولى إزدواجية التجريم** فقد نصت المادة (2/23) من اتفاقية الامم المتحدة لمكافحة الفساد على أنه في مسائل التعاون الدولي كلما أشترط توافر ازدواجية التجريم يجب اعتبار هذا الشرط مستوفياً، بغض النظر عن ما إذا كانت الدولة المطلوب إليها تدرج هذا السلوك الإجرامي ضمن نفس فئة الجرائم التي تدرجها الدولة الطالبة، أو انها تستخدم ذات التسمية التي تستخدمه الدولة الطالبة، فإذا كان السلوك المرتكب يعد سلوكاً مجرماً في قانون كل من الدولتين، فيعد هذا النص مخرجاً لإشكالية الإزدواجية من خلال التزام الدول في تجريم الأفعال المنصوص عليها في الاتفاقيات، وبالتالي يتحقق شرط إزدواجية التجريم بشكل بديهي في ظل هذه الاتفاقيات[2].

بالإضافة إلى إمكانية التخفيف من التطبيق الصارم لهذا الشرط كإحدى آليات التغلب على هذه الإشكالية، ويكون ذلك من خلال إما رد الأفعال التي تتطلب أن تجرم كجرائم في قوانين الدولتين، أو السماح بالتسليم لأي سلوك تم تجريمة، ومعاقب عليه بمستوى معين من العقوبة في كل دولة، وهذا ما ركزت عليه التطورات التشريعية المتعلقة بنظام تسليم المجرمين (الشمري، 2016، صفحة 103).

[1] اتفاقية جنيف للبحار العالمية لسنة 1958م.

[2] اتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2016م، المادة (2/23).

أما فيما يتعلق **بآلية التغلب على التزاحم في طلبات التسليم** فنجد أن الاتجاه الدولي لم يستقر على تحديد التسليم في حالة التزاحم في طلبات التسليم حتى على مستوى الدولة الواحدة، ويعود ذلك لاختلاف مصالح الدول وأولوياتها، إلا أنه كان لعنصر جسامة الفعل أولوية في اتفاقية الجامعة العربية الخاصة بالتسليم، حيث نصت المادة (13) منها على: "إذا قدمت للدولة المطلوب إليها عدة طلبات من دول مختلفة بشأن تسليم متهم من أجل نفس الجريمة، فتكون الأولوية في التسليم للدولة التي أضرت الجريمة بمصالحها، ثم الدولة التي أرتكبت الجريمة على أرضها، ثم الدولة التي ينتمي إليها المطلوب تسليمه، أما إذا كانت طلبات التسليم خاصة بجرائم مختلفة فتكون الأولوية للدول التي طلبت التسليم قبل غيرها"[1].

وبناءاً على ذلك، وللتغلب على هذه الإشكالية، فلا بد من عقد اتفاقية دولية تتضمن وضع ضوابط موضوعية وآليات محددة تسري على المجتمع الدولي بعيداً عن مصالح دولة معينة، حيث تقدم المصالح العامة على المصالح الخاصة، وتكون الأولوية للدولة التي تضررت مصالحها بسبب الجريمة الإلكترونية المرتكبة، ثم الدولة التي ارتكبت الجريمة على أراضيها، ثم بعد ذلك الدولة التي ينتمي إليها المطلوب تسليمه.

بينما في حالة تعدد الجنسيات لدى الشخص الجاني تزداد صعوبة هذا الشأن وتجعله أكثر تعقيداً، حيث تثار الإشكالية هنا نظراً لاختلاف المبدأ الذي تتبناه الدولة سواء فيما يتعلق بتسليم رعاياها أو عدم تسليمهم، ولم يتم معالجة هذه الإشكالية من قبل التشريعات بل تركت الأمر لقواعد المجاملات بين الدول، ومبدأ المعاملة بالمثل، وتزداد هذه الأشكالية في حال كان الشخص المطلوب تسليمه يحمل جنسية الدولة المطلوب إليها، مما يجعل الأمر خاضعاً للعلاقات الدبلوماسية (رياض، 1986، صفحة 80).

الفرع الرابع: آلية التغلب على الإشكاليات المتعلقة بالإنابة القضائية

كما ذكرنا سابقاً تتمثل الإشكاليات المتعلقة بالإنابة القضائية في فكرة السيادة، وفي بطء إجراءات الإنابة، وللتغلب على هذه الإشكاليات التي تعيق التعاون الدولي في مواجهة الجرائم الإلكترونية هنالك بعض

[1] اتفاقية الجامعة العربية الخاصة بالتسليم لسنة 1952م، المادة (13).

الآليات التي يمكن اتباعها في سبيل ذلك، فمثلاً التغلب على **إشكالية فكرة السيادة** يكون من خلال التخلي عن فكرة الســـيادة المطلقة للدولة، وهذا ما اتجهت له العديد من الدول، حيث قبلت بوضـــع قيود على سيادتها؛ لتحقيق مصلحة المجتمع الدولي، ومواجهة الجرائم التي تهدد مصالحه؛ لذلك نجد أن فكرة السيادة المطلقة بدأت بالانحسار في مواجهة التعاون الدولي، فتعتبر الإنابة القضائية وسيلة تحقق مواجهة الجريمة دون المساس بالسيادة الوطنية للدول، من أجل التغلب على العقبات التي تواجه الدول في اتخاذ الإجراءات اللازمة للكشـف عن الجريمة وملاحقة الجاني خارج حدودها الإقليمية بواسـطة قيام دولة باتخاذ الإجراءات اللازمة نيابةً عن الدولة صاحبة الاختصاص بموجب هذه الإنابة (صالح، 2023، صفحة 120).

أما بالنسـبة **لإشـكالية البطء في إجراءات الإنابة** يمكن التغلب عليها من خلال إتمامها عن طريق اتصـال مباشر بين السلطة القضائية الطالبة والسلطة القضائية المطلوب إليها، حيث يعتبر الاتصال أكثر اختصاراً ومرونة وسرعة بما يتلائم وحالات الاستعجال والضرورة؛ لذا نجد أن أغلب التشريعات الوطنية والمعاهدات والاتفاقيات الدولية التي تعمل على تنظيم الإنابة القضـــائية اتجهت نحو إجازة اتباع هذه الطرق في حالات الضرورة والاستعجال (صالح، 2023).

الفرع الخامس: آلية التغلب على الإشكالية المتعلقة بالتدريب على مواجهة الجرائم الإلكترونية

تكمن آلية التغلب على هذه الإشكالية في إجراء الكثير من الحملات التوعوية التي تهدف إلى بيان مخاطر الجرائم الإلكترونية، والأضـــرار التي تنتج عنها، وبيان أهمية تدريب رجال العدالة الجنائية على مواجهة الجرائم الإلكترونية، والتنسيق فيما بين الأجهزة التي تقوم على البرامج التدريبية؛ لعمل برامج مشتركة تناسب جميع الفئات، وكذلك القيام بالعمليات المشـــتركة التي تعزز مهارات القائمين على مواجهة هذه الجرائم، والتقريب فيما بينهم (أكلي و عاشور، 2023-2022، صفحة 62).

المطلب الثاني: آليات التغلب على إشكاليات التعاون الدولي على المستوى الوطني

يتناول هذا المطلب آليات التغلب على إشـــكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية على المستوى الوطني، والتي تتمثل في اتخاذ بعض التدابير الموضوعية، وهذا ما يتناوله الفرع الأول منه، بينما يتناول الفرع الثاني التدابير الإجرائية على النحو التالي:

الفرع الأول: التدابير الموضـــوعية كآلية للتغلب على إشـــكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية

هنالك بعض التدابير الموضـوعية التي يجب على الدول اتخاذها؛ لتعزيز مواجهة الجرائم الإلكترونية، ومن أهم هذه التدابير:

1. يجب على كل دولة أن تقوم باتباع ســياســة تشــريعية تهدف إلى التعاون مع الدول الأخرى؛ لحماية المجتمعات من مخاطر الجرائم الإلكترونية عن طريق تبني ما يتناسب والطبيعة الخاصة لهذه الجرائم من تشـريعات قانونية؛ ليتمكنوا من مواجهة مخاطر اسـاءة اسـتعمال الإنترنت، لذلك يتعين على كل دولة أن تتبع التدابير التشريعية اللازمة للكشف المبكر عن عملية الدخول غير المشروع، وفقاً لأحكام تشريعاتها الداخلية (سرور، 1981).
2. يجب على كل دولة القيام بإدخال جميع أعمال الإتلاف أو الأضـرار أو الإعاقة أو المحو أو التعديل التي تستهدف بيانات الحاسوب في قوانينها كجريمة يعاقب عليها القانون، بالإضافة إلى الأعمال التي تعيق وظائف الشـبكة العنكبوتية والأجهزة المتصـلة بها من نقل أو إدخال أو محو أو تعديل أو إعاقة لبيانات أجهزة الحاسوب المتصلة بالإنترنت (أبو نمر و بوكشريدة، 2021-2022).
3. يجب على كل دولة أن تقوم بوضع إجراءات تشريعية يتم بواسطتها مساءلة الأشخاص المعنوية جنائياً عما يرتكب من جرائم تتعلق بالإنترنت والحاسـوب، في حال كانت الجريمة ناتجة عن قصـور الرقابة

والإشـراف من الشـخص الطبيعي الذي يتسـبب بارتكاب هذه الجرائم أو يسـهل ارتكابها (أبو نمر و بوكشريدة، 2021–2022).

4. ضـرورة القيام بإجراء تعديلات لبعض النصـوص الموضـوعية في قانون العقوبات؛ ليتم النص فيه صـراحةً على تجريم الجرائم الإلكترونية، بدلاً من إدراجها ضـمن الجرائم التقليدية القديمة، وتطبيق النصوص القانونية القديمة عليها، فهنالك حاجة ضرورية لإضافة نصوص قانونية جديدة تنص على تجريم الجرائم الإلكترونية، وما قد ينتج عنها من جرائم أخرى ناجمة عن تطور في أدوات ارتكاب هذه الجرائم (الجنبيهي و الجنبيهي، 2005).

الفرع الثاني: التدابير الإجرائية كآلية للتغلب على إشكالية التعاون الدولي في مواجهة الجرائم الإلكترونية

إلى جانب التدابير الموضـوعية هنالك بعض التدابير الإجرائية التي يجب على الدول اتخاذها في سـبيل التغلب على إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية، ومن أهمها:

1. يجب على الدول أن تتبنى التدابير التشـريعية التي تمكنها من تفتيش نظم الحاسـوب أو أجزائها، وفحص البيانات المخزنة بها، والمخزنة على مختلف وسـائط التخزين الأخرى، دون الأخذ بعين الاعتبار محل التفتيش، فسـواء كان داخل الدول أو خارجها طالما أنه يفيد التحقيق في الجريمة (عزت، 2012، صفحة 545).

2. يجب على كل دولة أن تتبنى التدابير التشريعية اللازمة لتخويل سلطاتها المعنية صلاحيات ضبط وإحضـار الأشـخاص المتورطين بالجريمة؛ ليقدموا ما يقع تحت أيديهم من بيانات مخزنة سواء أكانوا متواجدين على إقليمها أو في مكان آخر، وذلك بالطريقة التي تتطلبها السـلطات لمصـلحة التحقيق (أبو نمر و بوكشريدة، 2021–2022).

3. ضرورة قيام رجال الشرطة داخل كل دولة بدوريات لمراقبة مؤسسات انتاج الحواسيب؛ للوقاية من كافة صـور الجرائم التي تتعلق بالكمبيوتر والإنترنت، ومثال على ذلك تقليد برامج الحاسـوب الآلي بطريقة

غير مشـروعة، وإسـاءة تصـنيع مكونات الحاسـوب بطريقة تلحق مسـتخدميها بالأضـرار (عفيفي، 2000).

4. يجب على كل دولة أن تعين إدراة أمنية لمكافحة الجرائم الإلكترونية، فيوكل إليها تلقي البلاغات التي تتعلق بهذه الجرائم، وكذلك تختص في اتخاذ الإجراءات القانونية المناسـبة وفقاً للقوانين الوطنية، وتنفيذ التدابير الأمنية الواقية من تضـخم هذا الخطر المرتبط بالتقنية الحديثة (أبو نمر و بوكشـريدة، 2021-2022).

وعليه نجد أن التعاون الدولي أصـبح ضـرورة ملحة في مواجهة الجرائم الإلكترونية؛ لعجز التشـريعات الوطنية عن مواجهتها لوحدها مهما بلغت قوتها؛ لذا يجب على جميع الدول اتخاذ خطوة جدية في سـبيل تعزيز التعاون الدولي في مواجهة هذه الجرائم، وبالرغم من الإشـكاليات التي تعيق هذا التعاون إلا أن هذه الضـرورة دفعت التشـريعات الحديثة للبحث عن آليات تمكّنها من التغلب على هذه الإشكاليات وانحسـارها، فلا بد من التشريعات الوطنية مواكبة التطورات التكنولوجية، وأن تبقى على اطلاع مستمر على التشريعات الدولية وما يطرأ عليها من مسـتجدات ومواكبتها؛ لتحقيق التعاون الدولي أهدافه المرجوة منه في سـبيل مواجهة الجرائم الإلكترونية.

الفصل الرابع

الخاتمة والنتائج والتوصيات

الخاتمة

مع التطور التكنولوجي الحاصل في الآونة الأخيرة، وانتشاره بشكل واسع في جميع المجالات حيث بات الإنسان يعتمد عليه في مختلف المجالات سواء على المستوى الشخصي، أو على مستوى بيئة العمل، فكثير من الشركات أو الأشخاص أصبحوا يعتمدون بشكل أساسي عليها في تيسير أعمالهم، ونتيجةً للمميزات التي يتمتع بها استخدام هذا المجال كشبه مجانيته وسهولة استعماله يكاد يكون كل شخص لديه المعرفة الكافية التي تجعله يقدر على استخدامها، وبالرغم من هذه الميزات إلا أنه لا يخلو الأمر من بعض السلبيات التي نجمت عنه، كاستغلاله من قبل بعض الجناة في ارتكابهم لجرائمهم، وتحقيق مصالحهم بطرق غير مشروعة.

مما أدى ذلك إلى تزايد الجرائم الإلكترونية في الآونة الأخيرة، والتي تشكل تهديداً عالمياً يتجاوز الحدود الإقليمية، مما يستدعي ضرورة تكاتف الجهود الدولية لمواجهتها بفعالية، وخاصة بعد أن عجزت التشريعات الدولية الإقليمية عن مواجهة هذا النوع من الجرائم كونها عابرة للحدود، وهنا تكمن أهمية التعاون الدولي في مواجهة هذه الجرائم من خلال الاتفاقيات الدولية والمعاهدات التي تعزز دور هذا التعاون، وتحقيق غايته المنشودة بالقضاء على هذه الجرائم وملاحقة مرتكبيها.

وبالرغم من أن التعاون الدولي يعد حجر الأساس في مواجهة الجرائم الإلكترونية إلا أن هنالك إشكاليات تشكل عائقاً أمام هذا التعاون سواء على المستوى الوطني أو على المستوى الدولي، مما دفع التشريعات الدولية الحديثة للبحث حول آليات للتغلب على هذه الإشكاليات وانحسارها بقدر من الإمكان، وهذا يعني أنه يجب على جميع الدول السعي نحو تكاتف دولي للحد من الأضرار الناجمة عن الجرائم الإلكترونية بما يحقق العدالة الجنائية ما بين مرتكبيها وما بين المتضررين منها.

النتائج

1. تعد الجرائم الإلكترونية من أخطر التحديات التي تواجه الدول نظراً لخصـــائصـــها وطبيعتها العابرة للحدودة مما جعلها تقف ضعيفة (شبه عاجزة) أمام مواجهتها.

2. على الرغم من الســـعي المســـتمر من قبل الجهود الدولية في مواجهة الجرائم الإلكترونية من خلال الاتفاقيات والمعاهادت الدولية، إلا أنها ليســـت كافية بالقدر اللازم؛ لتحقيق الغرض المراد منها، كما يؤدي عدم انضمام جميع الدول إليها إلى إضعاف إلزامية بنودها مما يحد من فعاليتها.

3. إن الاختلاف القائم بين التشـريعات الوطنية المتعلقة بالجرائم الإلكترونية يولد ثغرات قانونية يسـتغلها الجناة في إفلاتهم من العقاب، مما يعرقل التعاون الدولي في مواجهتها.

4. غياب التنسيق بين الأجهزة الامنية والقضـائية على المستوى الدولي يعيق التعاون الدولي في مواجهة الجرائم الإلكترونية من خلال البطء بالإجراءات وبالتالي إفلات الجناة من العقاب.

5. وجود إشـــكاليات عديدة تعيق التعاون الدولي في مواجهته للجرائم الإلكترونية، ومنها ما هو على المستوى الدولي، ومنها ما هو على المستوى الوطني.

6. تسعى التشريعات الدولية الحديثة إلى البحث المستمر حول آليات التغلب على هذه الإشكاليات نظراً لأهمية التعاون الدولي ودوره في مواجهة الجرائم الإلكترونية.

التوصيات

1. ضرورة تشجيع الدول على الانضمام إلى الاتفاقيات الدولية والمعاهدات التي تعزز التعاون الدولي في مواجهة الجرائم الإلكترونية، والعمل على عقد اتفاقيات جديدة بما يواكب التطورات المستمرة والمستجدات التي قد تطرأ على هذا النوع من الجرائم.

2. ضرورة السعي إلى توحيد التشريعات الوطنية المتعلقة بالجرائم الإلكترونية مع الاخذ بعين الاعتبار المعايير الدولية التي تبنتها التشريعات الدولية في مواجهتها لهذه الجرائم، مما يضمن سهولة التعاون بين الدول، والتغلب على الإشكاليات التي تعيقه.

3. لا بد من إنشاء منصات دولية آمنة لتبادل المعلومات بشكل يسهل الوصول إلى المعلومات اللازمة في الكشف عن الحقيقة، وكذلك تطوير قنوات اتصال مباشرة بين الجهات المختصة في مواجهة الجرائم الإلكترونية.

4. ضرورة اخضاع الاجهزة الأمنية والقضائية لدورات تدريبية على أحدث التقنيات في مواجهة الجرائم الإلكترونية، ودعم البحث العلمي في هذا المجال، مع استمرارية عقدها بما يواكب أي تطور قد يظهر في هذا المجال.

5. العمل على دورات توعية للأفراد حول الجرائم الإلكترونية وما يدور حولها، وطرق الوقاية منها، وخاصة الجرائم التي تستهدفهم من أجل الاحتيال عليهم أو خرق معلوماتهم؛ لابتزازهم بها وتحقيق منفعة مادية أو شخصية.

المصادر والمراجع

أبو الحسين، مسلم بن الحجاج بن مسلم. (1955). *صحيح مسلم*. مطبعة عيسى البابي الحلبي وشركاه، القاهرة.

أبو نمر، سليمان، و بوكشريدة، يوسف. (2021–2022). مكافحة الجريمة المعلوماتية في إطار القانون الدولي، تخصص قانون دولي عام. رسالة لنيل شهادة الماجستير. كلية الحقوق والعلوم السياسية، جامعة محمد خيضرة، سكرة.

أحمد، معاذ زياد حمد علي. (2019). التعاون الشـــرطي الدولي ودوره في مكافحة الجريمة المنظمة في فلسطين، قسم القانون العام. رسالة لنيل شهادة الماجستير، 43. كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين.

أكلي، معتوق محمد، و عاشـــور، ســـهام. (2023–2022). التعاون الدولي في مجال مكافحة الجريمة الإلكترونية. رسالة ماجستير. جامعة محمد البشير الإبراهيمي، برج بوعريريج، تخصص قانون إعلام آلي وإنترنيت.

الإكيابي، سلوى يوسف. (2017). النظام القانوني لتقديم المتهمين الجنائية الدولية. *القانونية*، 7، 193.

الأوجلي، ســالم محمد ســليمان. (1997). أحكام المســؤولية الجنائية عن الجرائم الدولية في التشــريعات الوطنية، "دراسة مقارنة". رسالة دكتوراه، 425. مصر: جامعة عين شمس، كلية الحقوق.

البداينة، ذياب موسى. (2014). *الجرائم الإلكترونية المفهوم والأسباب*. عمان، المملكة الأردنية الهاشمية.

بشارة، عبد المالك. (2018). طبيعة الجرائم التي يجوز فيها التسليم واستثناءاتها. *مجلة العلوم الاجتماعية والإنسانية*، 15.

بن يحيى، نعيمة. (2017). *الإنابة القضـــائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم*. جامعة مولاي الطاهرة سعيدة، كلية الحقوق والعلوم السياسية.

بوادي، حســـنين المحمدى. (2006). *إرهاب الإنترنت الخطر القادم، دار الفكر الجامعي*. الإســـكندرية: الطبعة الأولى.

بوبعاية، كمال، و والي، عبد اللطيف والي. (2021). الإشـــكالات التي تعترض تنســـيق التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية. *مجلة الدراسات والبحوث القانونية*، 6(1)، 95.

بوربابة، صورية. (2019). التعاون الدولي في مكافحة الجريمة الإلكترونية. *مجلة القانون الدولي للدراسات البحثية*، العدد الأول، جويلية، 100.

بوشعرة، أمينة، و موساوي، سهام. (2018). الإطار القانوني للجريمة الإلكرتونية (دراسة مقارنة). رسالة لنيل شهادة الماجستير، 14. جامعة عبد الرحمن ميرة، كلية الحقوق والعلوم السياسية، قسم القانون الخاص.

تدريست، كريمة. (2016). معوقات نظام تسليم المجرمين كآلية للتعاون القضائي الدولي لمكافحة الجريمة المنظمة عبر الوطنية. *المجلة النقدية*، 46.

الجنبيهي، منير محمد، و الجنبيهي، ممدوح محمد. (2005). *جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها*. دار الفكر الجامعي، الاسكندرية.

الحسيناوي، علي جبار. (2009). *جرائم الحاسوب والإنترنت*. عمان: اليازوي.

حشيفة، عبد الهادي. (2020). التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، تخصص قانون جنائي وعلون جنائية. رسالة لنيل شهادة الماجستير، 18. كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة.

الخراز، مصطفى. (2022/2021). الأمن الرقمي ومكافحة الجريمة الإلكترونية في المغرب، كلية العلوم القانونية والإقتصادية والإجتماعية بتطوان. رسالة لنيل شهادة الإجازة في القانون الخاص، 15. جامعة عبد الملك السعدي.

خراشي، عادل عبد العال إبراهيم. (2014). *إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها*. القاهرة.

الخراشي، عادل عبد العال إبراهيم. (2015). *دور الضبطية الإدارية والقضائية في مكافحة جرائم بطاقات الإئتمان الإلكترونية والتعاون الأمني الدولي حيالها*، ص103،. الإسكندرية: دار الجامعة الجديدة.

الدسوقي، طارق إبراهيم عطية. (2009). الأمن المعلوماتي (النظام القانوني لحماية المعلوماتية). الإسكندرية: دار الجامعة الجديدة، بدون طبعة.

ذنايب، أسيا. (2010). الآليات الدولية لمكافحة الجريمة المنظمة عبر الوطنية. رسالة لنيل شهادة الماجستير، 59. قسنطينة: جامعة الأخوة منتوري، كلية الحقوق والعلوم السياسية.

رياض، فؤاد عبد المنعم. (1986). *الوسيط في الجنسية ومركز الأجانب*. القاهرة: دار النهضة العربية.

الزعبي، مخلد إبراهيم. (2021). فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية. *المجلة العربية للنشر العلمي*، 37، 281.

الزهراني، شيخة حسين. (2020). التعاون الدولي في مواجهة الهجوم السيبراني. *مجلة جامعة الشارقة*، 17(1)، 756.

الزيدي، وليد. (2003). *القرصنة على الإنترنت والحاسوب: التشريعات القانونية*. عمان: دار أسامة.

سرور، أحمد فتحي. (1981). *الوسيط في قانون العقوبات القسم العام*. دار النهضة العربية، القاهرة، بدون طبعة.

السعيد، كامل. (2011). *شرح الأحكام العامة في قانون العقوبات (دراسة مقارنة)*، الطبعة الثالثة. عمان: دار الثقافة للنشر والتوزيع.

السلمي، حمزة بن فهم. (2023). الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي. *مجلة الجامعة العراقية*، 59(1)، 583.

سليمان، أحمد إبراهيم مصطفى. (2006). *الإرهاب والجريمة المنظمة التجريم وسبل المواجهة*. مطبعة العشري.

سليمان، أحمد فضل. (2013). *المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)*. القاهرة: دار النهضة العربية.

الشاذلي، فتوح عبدالله. (2018). *القانون الدولي الجنائي (أوليات القانون الدولي الجنائي، النظرية العامة للجريمة الدولية)*. دار المطبوعات الجامعية.

شرشر، محمود محمد صفاء الدين علي. (2021). *الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت*. جامعة المنوفية، كلية الحقوق.

الشمري، غانم مرضى. (2016). *الجرائم المعلوماتية، ماهيتها: خصائصها، كيفية التصدي لها قانونياً*. عمان، الأردن: لدار العلمية الدولية.

صالح، فيروز عوض الكريم. (2023). دور التعاون الدولي في مكافحة الجريمة الإلكترونية. *مجلة جامعة شذى للبحوث والدراسات الشرعية والقانونية*، 9، 114.

طبنجة، عبد الرحمن. (2022). *لماذا خلق الله الناس مختلفين*. تم الاسترداد من www.mawdoo3.com

عبد الحفيظ، أيمن. (2005). *الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية*. مطابع الشرطة.

عبد العال، عكاشـــة محمد. (1998). *دراســـات في القانون الدولي الخاص في دولة الإمارات العربية المتحدة*. الإسكندرية: دار الجامعة الجديدة للنشر.

العثيمين، الشـــيخ محمد بن صـــالح. (2020). *شـــرح باب التعاون على البر والتقوى من كتاب رياض الصالحين*. تم الاسترداد من www.alukah.net

العجمي، عبدالله رغش. (2014). المشكلات العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة). رسالة لنيل شهادة الماجستير، 14. الأردن: جامعة الشرق الأوسط.

العذار، أنيس بن علي. (2017). *مكافحة الجريمة الإلكترونية (الصعوبات والحلول)*، وزارة العدل القضائية (المجلد 13).

عرموش، ممدوح عبد الكريم. (2005). *تنازع القوانين*. عمان: الطبعة الأولى، دار الثقافة للنشر والتوزيع.

عزت، محمد فتحي محمد أنور. (2012). *تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها*. القاهرة: المركز القومي للإصدارات القانونية.

عطية، ثروت عبد الصـمد محمود. (2004). السـياسـة الجنائية لمكافحة الجريمة المعلوماتية في المملكة العربية السعودية، (دراسة مقارنة). *مجلة البحوث الفقهية والقانونية*، 46.

عفيفي، عفيفي كامل. (2000). *جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)*. الإسكندرية: توزيع منشأة المعارف.

عقباش، برزة ، و مبارك، حنان. (2022). آليات مواجهة الجريمة الإلكترونية في التشـــريع الجزائري، تخصـص قانون الإعلام الآلي والإنترنت. رسـالة لنيل شـهادة الماجسـتير، 22. كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج.

العقبي، مصطفى علي. (2024). آليات التعاون الدولي في مكافحة الجرائم العابرة للحدود. *المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)*، 1343، وما بعدها.

فحصـــي، عباس. (2022). *وقائع المؤتمر العلمي الإفتراضـــي (الجرائم الإلكترونية في الفقه الإســـلامي والقانون الوضعي)*. برلين، ألمانيا: المركز الديمقراطي العربي.

فريحة، حسين. (2011). *الجرائم الإلكرتونية والإنترنت، من خلال المعلوماتية السعودية*. تم الاسترداد من http://scord.mandumah.com/Revord/122156

فكري، أيمن عبدالله. (2014). *الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية* (الإصدار 1). الرياض: مكتبة القانون والاقتصاد.

الكميم، خالد محمد علي. (2017). الخصوصية والجريمة المعلوماتية. *مجلة البحوث والدراسات القضائية والقانونية*، 8، 147.

كيلاني، حسام أحمد علي. (2024). الدليل الرقمي ومعقوات إثبات الجريمة الإلكترونية. *مجلة البحوث الفقهية والقانونية*، 47، 772.

مبارك، هشام عبد العزيز. (2006). *تسليم المجرمين بين الواقع والقانون*. القاهرة: دار النهضة العربية، الطبعة الأولى.

مجاهدي، خديجة. (2018). آليات التعاون الدولي لمكافحة الجريمة المنظمة. رسالة لنيل شهادة الدكتوراة، 16. جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية. تم الاسترداد من رسالة لنيل شهادة الدكتوراة.

محسن، محمد نجم. (2021). دور القاضي الدستوري في إصلاح القصور التشريعي. *المجلة القانونية، مجلة متخصصة في مجال البحوث القانونية*، 621.

محمد، سارة. (2020). التعاون الدولي في تسليم المجرمين في ضوء التشريعات الوطنية والاتفاقيات الدولية. *مجلة جامعة الشارقة*، 17(1)، 652.

المرعشي، فيصل براء متين. (15 1، 2025). *عصبة الأمم*. تم الاسترداد من 2017: https://fc-lc.xyz/2RTN

ناشف، فريد. (2022). آليات التعاون في مكافحة الجرائم الإلكترونية. *مجلة البحوث في الحقوق والعلوم السياسية*، 8(1)، 437.

نجم، محمد صبحي. (2015). *قانون العقوبات القسم العام*. دار الثقافة للنشر والتوزيع، عمان، الطبعة السادسة.

نخبة من اللغويين بمجمع اللغة العربية. (1972). المعجم الوسيط، مجمع اللغة العربية. القاهرة.

هروال، نبيلة هبه. (2007). *الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، (دراسة مقارنة)*. الإسكندرية: دار الفكر الجامعي.

واصـــل، ســـامي جاد عبدالرحمن. (2023). التعاون الدولي في مكافحة الجرائم الإلكترونية. *مجلة القانون والتكنولوجيا*، 3(1)، 84.

CHALLENGES OF INTERNATIONAL COOPERATION IN COMBATING CYBERCRIMES

By
Laith Allam Saeed Mousa
Supervisor
Dr. Omar Bazour

Abstract

This study seeks to elucidate the challenges associated with international cooperation in combating cybercrime, which encompasses cross-border offenses necessitating effective coordination at both legal and technical levels. The research employs a descriptive analytical and comparative methodology, analyzing both international and national legal frameworks, and reviewing pertinent international conventions, such as the Budapest Convention. Additionally, it examines the current state of Palestinian legislation in this domain. The findings indicate that international cooperation continues to encounter significant obstacles, including conflicting legal frameworks, a lack of political trust, inadequate technical infrastructure in certain nations, and protracted judicial processes. Furthermore, the study highlights Palestine's limited participation in effective international frameworks aimed at addressing cybercrime. It recommends the alignment of national legislation with international standards, the expansion of bilateral and multilateral agreements, the enhancement of national capabilities in digital investigation, and the establishment of robust regional coordination mechanisms. This research contributes to the ongoing legal discourse regarding the development of international cooperation to address the escalating challenges posed by cybercrime to both national and international security.

Keywords: international cooperation, cybercrime, legal frameworks, digital investigation, Palestine, Budapest Convention.