

جامعة محمد خيضر بسكرة

كلية الحقوق والعلوم السياسية

قسم الحقوق



مذكرة ماستر

ميدان: الحقوق والعلوم السياسية

فرع: الحقوق

تخصص: قانون دولي

رقم:

إعداد الطالب(ة): يعلاوي أمانة

تبينة فدوى

يوم: 2025-06-02

آليات مكافحة الجريمة الالكترونية في القانون الدولي

لجنة المناقشة:

رئيسا	جامعة بسكرة	أستاذ التعليم العالي	زوزو هدى
مشرفا	جامعة بسكرة	أستاذ محاضر ب	بولوساخ ايمان
مناقشا	جامعة بسكرة	أستاذ محاضر ب	كلاش خلود

السنة الجامعية: 2025-2024



شُكْرُكَ تَقْدِيرُكَ

الحمد لله الذي علم الإنسان ما لم يعلم والشكر لله على نعمته وعونه
في إتمام هذا عمل وما يزال الرجل عالما ما طلب
العلم فان ظن أنه قد علم فقد جهل.

أتقدم بجزيل الشكر والتقدير والاحترام والامتنان إلى أستاذتنا الفاضلة
المشرفة الأستاذة " بولوساخ ايمان " التي لم تبخل علينا بمعلوماتها القيمة
وآرائها النيرة والصائبة وتشجيعاتها المتواصلة لإخراج هذا العمل بشكله
النهائي، كما أشكرها على الوقت الذي خصصته لاطلاع على
كل كبيرة وصغيرة في انجاز هذا العمل.
كما أتقدم بجزيل الشكر والامتنان للجنة الموقرة التي خصصت لنا من وقتها
لمناقشة مذكرتنا المتواضعة
وفي أخير نشكر كل من ساهم عن قريب أو بعيد في إتمام هذا العمل.
والى كل من علمنا حرفا وأثار لنا دربا

إهداء

إلى من كانوا نور دربي، وسند قلبي، ودفء أيامي
إلى زوجي الحبيب، رفيق درب والمواقف، الذي احتمل تعبى وساندني بصبره وحبه
... فكنت خير معين بعد الله
إلى أطفالي الثلاثة الأعزاء، أتم النبض الذي منحني القوة،
والابتسامة التي أزلت عني عناء الأيام، فبكم تزهو حياتي
إلى والديّ الغاليين، نبض الدعاء وريح الجنة، من غرسا في قلبي حب العلم، وكانا لي دوماً ملاذاً وسنداً...
. جزاكم الله عني خير الجزاء
إلى مدير عملي الكريم، الذي كان يتفهم طموحي، ويمنحني الوقت والفرصة كي أتابع دراستي، فله مني خالص الشكر
والعرفان.
إلى زملائي في خزانة زريعة الوادي، أتم جزء لا يئسى من هذه الرحلة، بدعمكم وتشجيعكم كانت خطواتي أثبت
إلى أخواتي العزيزات، كنن السند الحقيقي في كل مراحل هذا الطريق، وجودكن نعمة لا تقدر بثمن
وإلى إخوتي الكرام، حضوركم في حياتي جزء من قوتي، ولكم مكانة راسخة في القلب.
إليكم جميعاً، أهدي هذا العمل المتواضع، عربون وفاء وامتنان، وذخراً أفتخر به في حضرة محبتكم.

يعلاوي أمانة

إِهْدَاء

ءإلى من غرسا فى قلبى حب العلم والأخلاق؁

إلى من تعبنا وسهرتا لأجلي؁

...إلى أمى وأبى؁ تاج رأسى ونبع عطائى

إلى إخوتى الذين كانوا دومًا السند والدعم فى كل خطوة

إلى روح أخى الغالى؁ الذى رحل عن دنيانا لكنه باقى فى قلبى وذاكرتى؁

أهديك هذا العمل؁ عسى أن يكون صدقةً جارية عن روحك الطاهرة

إلى شريك حياتى؁ زوجى العزيز؁

الذى كان لى العون والدافع فى لحظات التعب والضعف

وإلى أخوات زوجى؁

شكرًا لمودتكن ودعائكن؁ فلكنَّ من القلب كل الامتنان

إلى كل هؤلاء؁ أقدم ثمرة هذا الجهد المتواضع؁ عرفانًا وتقديرًا.

تبينة فدوى

مقدمة

عرفت الجريمة كمفهوم قانوني واجتماعي منذ نشأة المجتمعات البشرية، حيث ارتبط وجودها بوجود الإنسان على الأرض، ورافقت تطوره عبر العصور، سواء من حيث الأهداف أو الوسائل. ومع دخول البشرية في العصر الرقمي الحديث، شهدت الجريمة نقلة نوعية تمثلت في ظهور أنماط جديدة لم تكن مألوفة من قبل، أبرزها ما يُعرف بالجرائم الالكترونية، التي أضحت من أخطر التحديات التي تواجه المجتمعات والدول على حد سواء.

لقد أصبح الحاسوب والبرمجيات الحديثة، إلى جانب شبكة الإنترنت، مكونًا أساسيًا في شتى مناحي الحياة، سواء على المستوى الفردي أو المؤسسي أو الدولي، إذ تم توظيف هذه الأدوات الرقمية في المجالات الاقتصادية، والعلمية، والاجتماعية، والعسكرية وغيرها. ورغم ما توفره هذه الوسائل من مزايا وإمكانات كبيرة ساهمت في تسهيل حياة الإنسان وتقليل التكاليف والجهود، إلا أن إساءة استخدامها أدت إلى ولادة نمط مستحدث من الجرائم يتميز بخطورته، وسرعة انتشاره، وطابعه العابر للحدود.

فالجرائم الالكترونية أصبحت تتجاوز النطاق التقليدي للجريمة، إذ يتم ارتكابها بوسائل تقنية، ويصعب في كثير من الحالات تحديد مرتكبها، أو مكان وقوعها، أو حتى ضحاياها بدقة. كما أن هذه الجرائم غالبًا ما تستهدف المعطيات الحساسة، وتمس بأمن المعلومات والأنظمة المعلوماتية، ما يجعلها تهديدًا حقيقيًا للأفراد والمؤسسات والدول على حد سواء.

وقد أصبح من الواضح أن مواجهة هذا النوع من الإجرام تتطلب مقاربة قانونية جديدة، لا تقتصر على الجهود الوطنية، بل تتطلب تعاونًا دوليًا فعالًا، نظرًا للطبيعة العابرة للحدود التي تميز هذه الجرائم. وهو ما جعل المجتمع الدولي يتحرك من خلال المنظمات والهيئات المختصة، وعبر عقد الاتفاقيات الدولية التي تهدف إلى وضع إطار قانوني موحد لمكافحة هذه الجرائم، وتعزيز التعاون بين الدول في ملاحقة مرتكبيها.

ورغم هذه الجهود، فإن مكافحة الجرائم الالكترونية لا تزال تواجه عدة تحديات، أبرزها القصور التشريعي، وتعدد النظم القانونية، واختلاف المفاهيم بين الدول، إضافة إلى صعوبات الإثبات والتقنيات المعقدة التي يستخدمها الجناة.

أولاً: أسباب اختيار الموضوع

جاء اختيار هذا الموضوع نتيجة لعدة اعتبارات ذاتية وموضوعية:

1) الأسباب الذاتية

الرغبة في التعمق في فهم مدى فعالية التعاون الدولي في مكافحة الجرائم الالكترونية. الاهتمام بتقييم مدى تطبيق القواعد القانونية الدولية مقارنة بالواقع العملي. السعي للاطلاع على أهم الاتفاقيات الدولية المتعلقة بالجريمة الالكترونية.

2) الأسباب الموضوعية

تزايد الجرائم الالكترونية في ظل التطور التكنولوجي السريع، يقابله قصور في التشريعات الوطنية.

الحاجة إلى دراسة دور الاتفاقيات الدولية في الحد من هذه الظاهرة.

الأهمية المتزايدة لحماية الأمن السيبراني كجزء من الأمن القومي والدولي.

ثانياً: أهمية الموضوع

تتجلى أهمية هذا الموضوع في عدة جوانب، من أبرزها:

طبيعة الجرائم الالكترونية المستحدثة، والتي تختلف عن الجرائم التقليدية من حيث الوسائل والمجال والفاعلين.

كونها جرائم عابرة للحدود، مما يجعل التعاون الدولي ضرورة حتمية.

تطور وسائل ارتكاب هذه الجرائم، ما يستدعي تحديث الأطر القانونية باستمرار.

خطورة آثار هذه الجرائم على الأفراد والمؤسسات والدول، في ظل فجوة تشريعية واضحة. الحاجة إلى فهم الأبعاد الدولية لمكافحة هذه الجرائم وتقييم الجهود المبذولة في هذا السياق.

ثالثا: أهداف الدراسة

تهدف هذه الدراسة إلى:

- توضيح الإطار العام لمفهوم الجرائم الالكترونية وطبيعتها القانونية.
- دراسة آليات التعاون الدولي لمكافحة هذا النوع من الجرائم.
- إبراز دور المواثيق والاتفاقيات الدولية في تنظيم جهود مكافحة.
- تحليل أبرز التحديات القانونية والعملية التي تواجه هذه الجهود.
- اقتراح توصيات لتحسين فاعلية التعاون الدولي في هذا المجال.

رابعا: إشكالية الدراسة

تُطرح الدراسة ضمن الإشكالية التالية:

ما مدى مساهمة المواثيق الدولية في مكافحة الجريمة الالكترونية؟

ومن خلال الإشكالية التالية تطرقنا لاستنتاج مجموعة من الأسئلة الفرعية لدراسة

موضوعنا:

- ما هو الاطار القانوني الذي ينظم الجريمة الالكترونية في القانون الدولي؟
- ما دور الاتفاقيات الدولية والإقليمية في تعزيز التعاون الدولي؟

خامسا: المنهج المعتمد

اعتمدت هذه الدراسة على المنهج الوصفي والتحليلي، الذي يسمح بتوصيف الجريمة الالكترونية من الناحية القانونية، وتحليل المواثيق الدولية ذات الصلة، مع دراسة أبعاد التعاون الدولي، والوقوف على التحديات التي تحول دون فعالية المكافحة، وذلك من خلال الرجوع إلى المصادر القانونية، والاتفاقيات الدولية، والبحوث الأكاديمية ذات الصلة.

سادسا: صعوبات الدراسة

واجهت الدراسة عدة تحديات، من أبرزها:

ندرة المراجع التي تتناول الجريمة الالكترونية من منظور القانون الدولي.

تركيز أغلب الدراسات السابقة على الأبعاد الوطنية، مع إغفال البعد الدولي.

سابعا: خطة الدراسة

قسمت هذه الدراسة إلى فصلين رئيسيين:

الفصل الأول: تناول فيه الباحث ماهية الجريمة المعلوماتية، من خلال تعريفها، وخصائصها، وأركانها القانونية، إلى جانب استعراض النظام القانوني للتعاون الدولي ودور المنظمات الدولية في هذا السياق.

الفصل الثاني: خصص لدراسة التحديات التي تواجه التعاون الدولي في مكافحة الجريمة الالكترونية، على المستويين الوطني والدولي، مع تقديم مقترحات وحلول عملية لتحسين فعالية المكافحة.

الفصل الأول

الفصل الأول: التأصيل القانوني للجرائم الالكترونية

في ظل التطور الهائل الذي شهدته التكنولوجيا في عصرنا الحالي والتقدم المستحدث لشبكات الاتصال والحاسوب، إلا أن استخدام هذه الأخيرة بالرغم من إيجاباتها الاقتصادية والاجتماعية إلا أن ذلك لا ينفى سلبياتها المعقدة التي أصبحت تهديدا للممتلكات الوطنية والتفكير الإبداعي للأفراد، الأمر الذي أسفر عن ظهور تقنيات وجرائم مستحدثة عابر للحدود ترتكب في عالم افتراضي وتساهم في تمويل عصابات المافيا تعرف بالجرائم الالكترونية التي تتسم بطبيعة فريدة تسبب أضرار جسيمة، باتت تستخدم وتشمل كل المجالات حتى أصبحت تهدد الاستقرار الاجتماعي ومثيرة للقلق في مختلف المجالات وهذا بعد الانتشار الواسع لمواقع الذكاء الاصطناعي والهواتف النقالة والحواسيب.

ولإثبات هذا النوع من هذه الجرائم وجدت كافة الدول صعوبة في اثباتها لأنها جرائم ناعمة ترتكب بدون عنف، حيث صنفت من أخطر الجرائم المعاصرة لأنها لا تعرف مكانا محددا ولا يمكن التعرف على مرتكبيها الأمر الذي أتاح للجناة استغلال التكنولوجيا لتنفيذ مخططاتهم الخبيثة، مما استدعى ضرورة تكاتف الجهود لإيجاد حلول فعالة لمواجهة هذه الجرائم والوقاية منها، كما تجدر الإشارة أن المشرع الجزائري لم يتأخر عن سن قوانين وتشريعات لتصدي لهاته الجرائم واتخاذ الإجراءات المناسبة لاحتوائها.

وانطلاقا مما سبق حاولنا بشكل عام التعرف على الجرائم الالكترونية، لذلك تطرقنا لتبناها أكثر من خلال (مباحث الفصل الأول) المسمى بالتأصيل القانوني للجريمة الالكترونية، بحيث تطرقنا في (المبحث الأول) الى مفهوم الجرائم الالكترونية، و(المبحث الثاني) درسنا فيه النظام القانوني للتعاون الدولي ودوره المجتمع في تفعيله.

المبحث الأول: مفهوم الجرائم الالكترونية

ظهور الجريمة الإلكترونية أصبح أحد النتائج المباشرة للتقدم التكنولوجي، مثل الإدارة والتجارة الإلكترونية، فقد ساهم هذا التطور الرقمي في تحسين جودة الحياة وأصبح جزءاً أساسياً من عمل مختلف القطاعات لتقديم خدماتها بطريقة أكثر فعالية وسرعة وأقل تكلفة ومع ذلك، شهدنا أيضاً الجانب السلبي لهذا التقدم، حيث أدى الانتشار الواسع لتقنيات المعلومات وظهور الإنترنت إلى تسهيل الكثير من الأمور، ولكنه أيضاً أتاح الفرصة لظهور ممارسات غير قانونية وأفعال إجرامية ناجمة عن سوء استخدام هذه التقنيات من قبل البعض.

ولتوضيح ما يلي قسمنا هذا المبحث الى مطلبين، تضمن المطلب الأول تعريف الجريمة الالكترونية، أما المطلب الثاني تضمن خصائص الجريمة الالكترونية.

المطلب الأول: تعريف الجريمة الالكترونية

الجريمة الالكترونية، باعتبارها ظاهرة إجرامية حديثة ذات طبيعة مميزة، شكلت تحدياً كبيراً أمام الفقهاء ورجال القانون الجنائي للتوصل إلى تعريف دقيق وشامل يعكس طبيعتها المستجدة من خلال في هذا السياق، يسعى هذا المطلب إلى تناول أبرز المحاولات الفقهية التي سعت إلى تقديم تعريف واضح للجريمة الإلكترونية، إضافة إلى تسليط الضوء على أهم القوانين التي أحدثتها.

الفرع الأول: مدلول الجريمة الالكترونية

من خلال هذا الفرع سوف نتطرق الى تعريف الجريمة الالكترونية بما يأتي:

أولاً: لغة

الجريمة: " الجريمة والجرم معناها في اللغة الذنب، ومن اشتقاقها جرم وأجرم واجترام، وتجرم عليه معناها ادعى عليه ذنباً لم يفعله، وكلمة لا جرم تعني القسم والجرم هو الذنب أو الجناية"¹.

الالكترونية: " يقصد بها المعالجة الآلية للمعلومات وهي ترجمة للمصطلح الفرنسي (informatique) وهي اختصار للكلمتين الفرنسييتين (information) معلومات (automatique) ذاتيا، وصاحب هذا المصطلح هو فليب درايفوس الذي أراد أن يعني به العلم الذي يربط علم الحاسوب (compute science) والمعلومات (information) والاتصالات (communication) "².

ثانياً: اصطلاحاً

اختلف الفقه على تحديد تعريف واحد للجرائم الالكترونية، ولم يجمعوا على تعريف شامل بحيث اختلفت التسميات وذلك بسبب الاختلاف في المعايير التي تستند اليها الجريمة وكل جانب ينظر ال زاوية مختلفة من حيث مفهومها.

1. تعريف الجريمة الالكترونية حول وسيلة الجريمة:

من هذا المنطلق، تُثبت الجريمة الإلكترونية عندما يُستخدم الكمبيوتر كوسيلة أساسية لارتكابها. ويعرّف الأستاذ جون فورستر الجريمة الإلكترونية بأنها عمل إجرامي يتم تنفيذه باستخدام الكمبيوتر كأداة رئيسية، فقد ذهب الفقيه تايديمان tiedeman في تعريفه بأنه " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"³، وعرفها الدكتور عبد

¹ حبايبة ميرفت محمد، مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري

العلمية للنشر والتوزيع، عمان، 223، ص 29.

² حبايبة مرفت محمد، المرجع نفسه، ص 29.

³ رحموني محمد، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، جامعة دراية، أدرار،

الفتاح مراد على أنها " جميع الأفعال المخالفة للقانون والشرعية والتي ترتكب بواسطة الحاسوب الألي من خلال شبكة الأنترنت وهي تتطلب إماما خاصا بتقنيات الحاب الألي ونظم المعلومات سوار لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت من مواقع الأنترنت وغرف المحادثة أو البريد الإلكتروني"¹.

2. تعريف الجريمة الإلكترونية حول موضوع الجريمة:

يعتمد أنصار هذا التوجه في تعريفهم للجريمة المعلوماتية على ضرورة أن يكون الحاسوب محور ارتكاز الجريمة، بحيث يُستهدف الاعتداء مباشرةً على الجهاز ذاته أو على النظام الداخلي الخاص، نجد الفقيه ROSANBLATT عرف الجريمة بأنها " نشاط غير مشروع موجه للنسخ أو تغير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"²، كما تعرف أيضا بأنها أي تصرف إيجابي أو سلبي يؤدي إلى انتهاك البرامج أو المعلومات بهدف تحقيق استفادة بأي شكل من الأشكال يحمل في طياته العديد من التحديات، تلك السلوكيات قد تتنوع بين استغلال الأدوات التقنية لإلحاق الضرر أو لاستخلاص فوائد غير مشروعة في عالم أصبح فيه التكنولوجيا جزءًا لا يتجزأ من حياتنا اليومية، تحتاج كل جهة، سواء فردًا أو مؤسسة، إلى التفكير بعمق في سبل الحماية وتجذب الوقوع في فخ الممارسات المضللة التي قد تجعل البيانات عرضة للاعتداء أو تفتح المجال للإضرار بأنظمة حيوية.

لم يسلم هذا المقياس من النقد، إذ قصر نطاق الجريمة الإلكترونية على المصالح التي تحظى بالحماية، وتلك المصالح هي: البيانات والبرامج، والأجزاء المادية والمعنوية للحاسوب، وقد أفضى هذا المعيار إلى صياغة تعريفات عامة ومجردة، تفتقر إلى الدقة في تحديد الأفعال

¹ العنوم محمد الشبلي، جرائم التكنولوجيا المعلومات النظرية العامة للجرائم الإلكترونية، دار الثقافة للنشر والتوزيع،

عمان، الأردن، 2023، ص 19.

² معاشي سميرة، الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة الفكر، العدد 1، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2018، ص 402.

المتعلقة بجرائم الحاسوب. ونتيجة لذلك، قد تُعتبر بعض الأفعال من جرائم الحاسوب، رغم أنها في الواقع لا تصنف كذلك.

3. تعريف الجريمة الإلكترونية تعريف مستند الى معايير مختلفة:

ظهر هذا الاتجاه كاستجابة لتصحيح اللبس الذي وقعت فيه التيارات والاتجاهات السابقة حيث سعى القائمون عليه إلى تناول موضوع الجريمة الإلكترونية بمفهوم شامل يغطي جميع مكوناتها مع رفض الاعتماد على معيار أحادي في التصنيف، وبسبب عجز المحاولات السابقة عن صياغة تعريف جامع يشمل كافة أركان الجريمة الإلكترونية، لجأ أصحاب هذا الطرح إلى تقديم تعريف مبتكر يعتمد على دمج أكثر من تعريف لتحقيق رؤية أكثر تكاملاً، "هي الجريمة التي يستخدم فيها الحاسب الألي كوسيلة أو أداة لارتكابها أو يمثل اغراء بذلك، أو جريمة يكون المحاسب نفسه ضحيتها"¹، ويعرفها بعض المفكرين أيضاً بأنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الألي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"²، كما جاءت توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين المنعقد في فيينا سنة 2000 بتعريف الجرائم الحاسوب على أنه "يقصد بالجريمة الإلكترونية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"، يعد تعريف الأمم المتحدة من أبرز التعريفات الدقيقة التي تناولت مفهوم الجريمة الإلكترونية، حيث شمل جميع الأشكال الإجرامية المرتبطة بها، سواء تلك التي تستهدف النظام المعلوماتي بشكل مباشر أو التي تُنفذ باستخدامه. كما يتميز هذا التعريف

¹ سلامي لخضر، الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي - الفيسبوك نموذجا -، أطروحة دكتوراه في سوسولوجيا الاجرام، كلية العلوم الاجتماعية، قسم علم الاجتماع والأنثروبولوجيا، جامعة وهران 02، 2023/2022، ص 43.

² سيد سلمان عبد الحكيم، الجرائم المعلوماتية وأثارها في ضوء قانون مكافحة جرائم تقنية المعلومات، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى، مصر، 2023، ص 2.

بعدم تقيده بالمعايير الضيقة للجريمة، مثل أسلوب ارتكابها أو هوية مرتكبها أو الهدف والنتيجة المرجوة منها¹.

الفرع الثاني: تعريف الجريمة الإلكترونية تشريعا

أولاً: تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 04-15

بالرجوع إلى قواعد القانون 04-15² من المادة 394 مكرر إلى المادة 394 مكرر 2 نجد أنه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث حددها في المادة 394 مكرر بالآتي :

- الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.
- حذف أو تغيير المعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

تعريف الجريمة حسب المادة 394 مكرر 1 فقد أشارت إلى ما يلي - :

إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

وبالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من

الآتي:

¹ قنفود نبهية، السياسية الجنائية في مكافحة الجريمة الإلكترونية في التشريع الجزائري، أطروحة دكتوراه ل م د، شعبة الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق، قسم القانون الخاص، جامعة قسنطينة 01، الاخوة منتوري، قسنطينة، 2024، ص 12.

² القانون رقم 15/04 المؤرخ في 10 نوفمبر، يعدل ويتم الأمر 155/66 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 1، الصادر بتاريخ 2004/11/15.

تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

ثانيا: تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 104/09¹

حددت المادة (02) منه الجريمة الإلكترونية بقولها: " يقصد في مفهوم هذا القانون بما

يأتي:

- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.
- منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.
- معطيات معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

يتفق كل من التعريفين الفقهي والقانوني على أن الجريمة الإلكترونية تتمثل في فعل أو امتناع يهدف إلى إلحاق الضرر ويُرتكب باستخدام الحاسوب ويُلاحظ أن الحاسوب يُعتبر مكونًا يتضمن عناصر مادية، مثل أدواته ومستلزماته من أقراص وشاشات وغيرها، هذه العناصر المادية يمكن أن تكون هدفًا للاعتداء من خلال أفعال مثل السرقة، الكسر، أو التفجير، ولا يتطلب ذلك بالضرورة الولوج إلى شبكة الإنترنت، كما أن هذه الانتهاكات قد تنفذ

¹ القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

من قبل أفراد لا يمتلكون معرفة تقنية أو استخدامًا متخصصًا لهذه الوسائل ومع ذلك، تختلف هذه العناصر المادية عن تلك التي تُشكل موضوعًا مباشرًا للجريمة الإلكترونية، مثل البيانات، والبرمجيات، والمعلومات المخزنة داخل الحاسوب. هذه الأخيرة يمكن أن تكون هدفًا لجرائم متعددة تشمل سرقتها، تدميرها، الاطلاع غير المشروع على البيانات السرية، أو حتى استخدامها بطرق غير قانونية. كما قد تتمثل الجريمة في إرسال فيروسات عبر برامج ضارة تهدف إلى تعطيل النظام أو الإضرار بمحتوياته بشكل مباشر.

المطلب الثاني: خصائص الجريمة الإلكترونية

الجرائم المعلوماتية تحمل طابعًا فريدًا يجعلها تختلف بشكل واضح عن الجرائم التقليدية، وهو ما يمنحها مجموعة من الخصائص المميزة. هذه الخصائص لا تقتصر فقط على طبيعة الجريمة نفسها، بل تمتد أيضًا لتشمل السمات المتعلقة بمن يرتكبونها. هذا التمايز يبرز أهمية دراسة تلك الجرائم من زوايا مختلفة لفهم أبعادها ومعالجة آثارها بشكل أكثر فعالية، ومن هذا المنطلق سنتطرق من خلال الفروع الآتية إلى تبين خصائص الجريمة الالكترونية المتمثلة في:

الفرع الأول: عابرة للحدود

بالنظر إلى هذا النوع من الجرائم أنه لا يعتد بالحدود للدول ولا بين القارات وبالتالي أصبحت ساحتها للعالم أجمع، فمنه انتشار شبكة الاتصالات بين دول العالم وأقاليمه أمكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر، وهذا فالجرائم الالكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة¹.

الفرع الثاني: صعوبة اكتشافها وإثباتها

تتميز الجرائم الالكترونية بصعوبة اكتشافها، وغالبًا ما تختفي آثار مادية مما يجعل من الصعب الإمساك بمرتكبيها، بالإضافة إلى ذلك فإن الأداة المستخدمة في هذه الجرائم هي الإشارة الالكترونية سريعة الزوال بحيث يزول الدليل المادي بعد الاستخدام مباشرة، وهذا يختلف

¹ رحموني محمد، المرجع السابق، ص 441.

عن الجرائم التقليدية فهي تحدث في عالم افتراضي تقني لا يترك أي أثر ملموس وصعوبة اثباتها تعود لعدة أسباب منها الطابع التقني المعقد الذي يتطلب خبرة فنية متخصصة يصعب على المحقق العادي التعامل معها¹، ومن ناحية أخرى فإن قلة الخبرة لدى السلطات القضائية المختصة بالتحقيق في جرائم الانترنت تعيق اثباتها، مما يستلزم تدريب وتأهيل هذه السلطات في جمع الأدلة والتفتيش والمتابعة في العالم الرقمي، ونتيجة لذلك غالبا ما تفشل الشرطة في تقدير خطورة الجريمة الالكترونية فلا تبذل جهودا لحل لغزها والقبض على مرتكبيها².

الفرع الثالث: سهولة ارتكابها

تتميز هذه الجرائم بانها غالبا ما تكون مخفية ومستترة، والضحية لا يلاحظها رغم وقوعها أثناء استخدامه لشبكة الاتصالات فالمجرم يمتلك مهارات عالية تمكنه من تنفيذ جريمته بدقة، مثل ارسال الفيروسات، سرقة الأموال والبيانات، التجسس وسرقة المكالمات، بخلاف أنها تحدث في وقت قصير أغلبها لا يتم اكتشافها الا بعد فترة مثل برامج الاتلاف والتجسس أو سرقة الأموال، وما يزيد من سرعة تنفيذ الجريمة هو التطور التقني الذي أجد العديد من الأدوات والبرامج التي تسهل تنفيذ الجرائم المعلوماتية وفقا لأهداف ورغبات الجاني³.

الفرع الرابع: أسلوب ارتكابها

تتميز هذه الجرائم بطابعها الخاص الذي يظهر بوضوح في أسلوب ارتكابها وطريقتها، ففي حالة الجرائم التقليدية غالبا ما تتطلب تنفيذها جهدا جسديا ملموسا، يتجلى أحيانا في صورة الايذاء أو العنف، كما هو الحال في جرائم القتل أو الاختطاف، أو من خلال إجراءات الخلع أو الكسر أو تقليد المفاتيح كما يحدث في جرائم السرقة، أما الجرائم المعلوماتية فتتميز

¹ علي السيد محمد، الجرائم الالكترونية، ماهيتها، صورها، اثباتها، مكافحتها، دار التعليم العالي، الإسكندرية، 2024، ص 26.

² قنفود نبيلة، المرجع السابق، ص 19.

³ ياكور الطاهر، الجرائم الالكترونية الأحكام الموضوعية والاجرائية، دراسة مقارنة، دار بلقيس، دار البيضاء، الجزائر، 2024، ص 30.

بطابعها الهادئ أذ أنها لا تعتمد على العنف بل تستند الى المهارات التقنية والقدرة على التعامل مع أجهزة الحاسوب بشكل يتيح ارتكاب أفعال غير مشروعة بسهولة وفعالية¹.

ويرجع هذا الى أن هذا النوع من الجرائم يمثل بيانات ومعلومات قابلة للتغيير أو التعديل أو الحذف من السجلات المخزنة في الحواسيب، إلا أن البعض يقارنها بجرائم العنف مثل ما ذهب اليه مكتب التحقيقات الفيدرالي (FBI) وذلك بسبب تشابه دوافع المعتدين على أنظمة الحاسوب مع مرتكبي جرائم العنف².

المطلب الثالث: أركان الجريمة الإلكترونية

مثلما تعتمد الجرائم التقليدية على أركان أساسية لقيامها، فإن الجرائم الإلكترونية التي ظهرت نتيجة للتقدم التكنولوجي تحتاج أيضًا إلى توفر عناصر محددة لإثبات وقوع الجريمة . وبشكل عام، لا يمكن اعتبار أي فعل جريمة دون توافر هذه الأركان الأساسية.

الفرع الأول: الركن الشرعي

تعتبر علاقة السببية أحد العناصر الأساسية التي تساهم بشكل كبير في تكوين الركن المادي المرتبط بالجرائم التي تؤدي إلى نتيجة مادية ملموسة .يعد تحقق هذه العلاقة شرطًا جوهريًا وأساسيًا لتحمل المسؤولية الجنائية عن مثل هذه الجرائم، مما يجعلها جزءًا لا يتجزأ من مفهوم الجريمة الدولية في إطار الركن المادي .تتجلى مسؤولية الجاني في هذا السياق إما من خلال القصد الجنائي المتعمد أو نتيجة الإهمال، حيث أن وجود علاقة السببية يُعد ضروريًا أيضًا في الجرائم التي تُرتكب دون قصد، ومن الملاحظ أن هذه الجرائم غير العمدية تتميز بوجود ركن مادي يتحقق بواسطة سلوك معين يؤدي إلى نتيجة محددة، وفي الوقت نفسه يرتبط

¹ بغدادي إيمان، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة أفاق للبحوث والدراسات، العدد 04، المركز الجامعي، ايليزي، 2019، ص 188.

² داودي نعيمة، الجريمة الإلكترونية (خصائصها، مجالات استخدامها، وأهم سبل مكافحتها)، مجلة مهد اللغات، المجلد 02، العدد 01، جامعة علي لونييسي، البلدية، 2020، ص 48/49.

بهذه النتيجة بعلاقة سببية واضحة تربط بين الفعل ونتيجته، مما يضع الجاني أمام مسؤولية معينة حتى في حالة عدم وجود نية مسبقة لارتكاب الجريمة¹.

الفرع الثاني: الركن المادي

يتألف الركن المادي للجريمة من السلوك الإجرامي والنتيجة والعلاقة السببية. ومع ذلك، يمكن أن يتحقق الركن المادي حتى دون تحقيق نتيجة فعلية، كأن يتم الإبلاغ عن الجريمة قبل وقوعها على سبيل المثال، إنشاء مواقع لتشهير شخص دون أن يتم نشر الموقع على الشبكة يُشكّل كياناً ملموساً يعكس نية الفاعل بطريقة يمكن إثباتها.

أولاً: السلوك الاجرامي

يتطلب السلوك الإجرامي المتعلق بالجرائم الإلكترونية، في المقام الأول، وجود بيئة رقمية مناسبة. مما يعني ضرورة وجود جهاز حاسوب وشبكة إنترنت متاحة للاتصال، بالإضافة إلى ذلك، يجب أن يتوفر الفهم الدقيق لبداية النشاط الإجرامي والشروع فيه والنتائج المترتبة عليه. على سبيل المثال، قد يقوم الجاني بتحضير حاسوبه لتنفيذ جريمته من خلال تحميل برامج اختراق متخصصة أو قد يعتمد إلى تطوير هذه البرامج بنفسه. كما قد يشمل نشاطه إعداد صفحات تحتوي على مواد مخالفة للآداب العامة وتحميلها على الخوادم المستضيفة من ناحية أخرى، يمكن أن يتورط الجاني في إنشاء برامج فيروسية كجزء من استعداداته لارتكاب الجريمة الإلكترونية².

تبرز أهمية السلوك الإجرامي من جوانب متعددة تشكّل محوراً حيوياً في رسم حدود نفوذ المشرّع الجنائي، إذ يُعدّ الاهتمام بالسلوك كونه تصرفاً إنسانياً هو ما يشغل بال المشرّع. ومن هذا المنطلق، فإن أي واقعة تفتقر إلى عنصر السلوك لا يمكن اعتبارها موضعاً للتجريم. إضافة إلى ذلك، يتمتع السلوك الإجرامي بقيمة قانونية ذاتية، حيث يُصنّف في حد ذاته كعمل

¹ حشمان عمار، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، تخصص إدارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم علوم التسيير، جامعة قاصدي مرباح، ورقلة، 2018/2019، ص 13.

² قنفود نبيهة، المرجع السابق، ص 47.

غير مشروع، وهذا ما يبرر فرض العقوبات على مرتكبيه من قبل المشرع ومع ذلك، ظهرت بعض الآراء في الفقه التي تنكر هذه القيمة الذاتية للسلوك، حيث يفسر أصحاب هذه الآراء أن السلوك ليس سوى تعبير عابر ومظهر خارجي للشخصية الإجرامية وفقاً لهذا الفهم، يُعاقب الجاني ليس فقط على فعلٍ محدد ارتكبه، بل لأن شخصيته بحد ذاتها تعتبر خطراً على المجتمع، وللسلوك المرتكب دور في كشف هذه الخطورة، لذا فإن قيمة السلوك ليست ذاتية وإنما تُستخلص من ارتباطه بشخصية الفاعل ومدى صلاحيتها كمؤشر على خطورته المحدقة بالمجتمع¹.

ثانياً: النتيجة

يتألف الضرر الناتج عن الأفعال أو السلوكيات الإجرامية من مجموعة متنوعة، حيث تتفاوت حدته في الجرائم الإلكترونية. ففي الحالات القصوى، قد يصل الضرر إلى القتل، كما يحدث عندما يقوم طبيب عمداً باختراق قاعدة بيانات المستشفى التي يعمل بها، ويغير تركيب دواءٍ خاص بمريض محدد بقصد التسبب في وفاته. إلى جانب ذلك، يمكن أن يكون الضرر مادياً مثل الخسائر الناجمة عن إتلاف الأجهزة والبيانات، أو معنوياً كالإساءة من خلال السب والقذف وتشويه السمعة بلا مبرر باستخدام وسائل التواصل الاجتماعي².

ثالثاً: العلاقة السببية بينهما

تُعد علاقة السببية من العناصر الأساسية للركن المادي في الجرائم ذات النتيجة المادية، حيث يُعتبر تحققها شرطاً جوهرياً لتحمل المسؤولية الجنائية عن هذه الأنواع من الجرائم وبذلك، تُشكّل علاقة السببية جزءاً أساسياً من الجريمة الدولية ضمن إطار الركن المادي وتتمثل مسؤولية الجاني إما في صورة العمد أو الإهمال، إذ أن علاقة السببية تُعد ضرورة كذلك في

¹ العموري رأفت حميد ريس، أثر الجريمة المعلوماتية وتأثيرها على المجتمع، مجلة المفكر للدراسات القانونية والسياسية، المجلد 04، العدد 04، العراق، 2022، ص 138.

² هدية أحمد محمد زعتر، الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسبل مواجهتها، مجلة البحوث القانونية والاقتصادية، العدد 84، كلية إدارة الأعمال، قسم القانون، جامعة الجمعة، المملكة العربية السعودية، 2022، ص 79.

الجرائم غير العمدية. ويُلاحظ أن الجرائم غير العمدية تتسم أيضًا بوجود ركن مادي يتحقق من خلال سلوك معين، ونتيجة محددة، وعلاقة سببية تربط بينهما¹.

الفرع الثالث: الركن المعنوي

الركن المعنوي للجريمة يركز على الحالة النفسية للجاني وكيفية ارتباط عناصر الجريمة بشخصيته، يُعتبر الركن المعنوي جزءًا أساسيًا في القانون الجنائي لأنه يحدد المسؤولية الجنائية بناءً على العلم والإرادة والقصد الجرمي، وهذا الركن يوضح التفاعل بين عناصر الجريمة وشخصية الجاني، وبالتالي يشكل أساس العقاب الذي يجري تطبيقه من قبل الدولة، فيما يتعلق بالجرائم الإلكترونية، الركن المعنوي يحتفظ بنفس المبادئ الموجودة في جرائم قانون العقوبات هنا، القصد الجرمي يعتمد على معرفة الجاني بطبيعة ومخاطر تصرفاته المحظورة، ووجود إرادة لتحقيق النتيجة الضارة أو الخطرة الناتجة عن تلك التصرفات².

غالبًا ما يُعتقد أن الجرائم الإلكترونية تُرتكب عن عمد، حيث يتطلب ذلك تفكيرًا مسبقًا في كيفية الوصول إلى المعلومات أو اختراق الشبكات في الأصل، يُفترض في الجرائم أنها جرائم عمدية، ما لم يُذكر خلاف ذلك في القوانين، يشترط القانون في بعض الجرائم توفر الإرادة لارتكاب الفعل وتحقيق النتيجة، مثل الدخول غير المشروع إلى أنظمة المعلومات وتدميرها أو مسح بيانات الحاسب بعد نقل ونسخ المعلومات، بهدف محو الأدلة ومع ذلك، قد يطلب القانون في بعض الحالات توافر عنصر جنائي خاص إلى جانب القصد الجنائي العام .

¹ حبايبة ميرفت محمد، مكافحة الجريمة الإلكترونية "دراسة مقارنة" في التشريع الجزائري والفلسطيني، أطروحة دكتوراه في الحقوق، تخصص القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة عمار ثلجي، الأغواط، 2022/2021، ص 120.

² حسين محمد فلاح البرابسه، الركن المعنوي للجرائم الإلكترونية وفقا لقانون العقوبات الأردني، رسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2021، ص 76.

على سبيل المثال، قد يشترط وجود نية واضحة للاستيلاء على الأموال المسروقة ببطاقات الائتمان وتحويلها لحساب الجاني الشخصي¹.

المبحث الثاني: النظام القانوني في التعاون الدولي ودور المجتمع في تفعيله

يعمل التعاون الدولي من خلال من خلال مجموعة من المبادئ القانونية والقواعد التي تنظم العلاقات الدولية بين الدول والمنظمات الدولية وذلك لتحقيق السلم، وتعزيز التنمية الاقتصادية والاجتماعية، وحماية حقوق الإنسان، العالمية، ولا يقتصر التعاون الدولي على الحكومات والمنظمات الدولية، بل يلعب المجتمع دورا محوريا في تفعيله وهذا ما سيتم التطرق إليه من خلال دراسة هذا المبحث الى مطلبين، حيث تضمن المطلب الأول ماهية التعاون الدولي. والمطلب الثاني تضمن دور المنظمات والهيئات الدولية في تفعيل التعاون الدولي، وفي الأخير سنتطرق الى دور الاتفاقيات الدولية في مكافحة الجرائم الالكترونية في المطلب الثالث.

المطلب الأول: ماهية التعاون الدولي

يعد ميثاق الأمم المتحدة أحد أهداف الأسس القانونية للتعاون الدولي، حيث ينظم العلاقات بين الدول بناءات على مبادئ احترام السيادة، وعدم التدخل في الشؤون الداخلية، حل النزاعات بالطرق السلمية وعرف التعاون الدولي على الآتي:

الفرع الأول: تعريف التعاون الدولي

كغيره من المصطلحات تتعدد التعاريف الخاصة بالتعاون وتختلف باختلاف المجالات العلمية (سياسية، اقتصادية، اجتماعية) إلا انه سيتم الاختصار على الجانب الدولي من حيث يمكن وضع عدة تعاريف.

¹ بن عودة صليحة، الجريمة الالكترونية وأثرها على مشروعية أعمال الإدارة القانونية، مجلة دفاثر الحقوق والعلوم

السياسية، المجلد 03، العدد 1، المركز الجامعي معنية، 2023، ص 51.

ترى إكرام عبد الحميد أنه مجموعة مكثفة من التفاعلات والاتصالات في المجالات المختلفة التي تسمح بالبناء وتحقيق التقدم وتعظيم درجة الأمن بين عدة أطراف ليس بالضرورة متقاربين جغرافيا، أو منتمين إلى دين واحد أو ذي أصول عرقية واحدة.¹

كما يعرف التعاون الدولي أيضا بأنه مجموعة من علاقات تربط دول العالم بعضها بعض، وهذه العلاقات قائمة ومستندة على وحدة الطبيعة الإنسانية، وقد ساعد على ذلك تبادل المنافع والمصالح، والاحتياجات العالمية للثروات المختلفة في جميع بقاع الأرض، وإن عبارة التعاون الدولي تفرض إلزامية أساسية يقعان على عاتق جميع الدول المتعانة الأول: يتعلق بضرورة قبول المساعدة الدولية والحفاظ على التماسك الدولي. الثاني: يتصل بضرورة تقديم المساعدات من قبل الدول القادرة على تقديمها.²

وبما أن الجرائم المعلوماتية ذات طابع دولي كانت الجهود الدولية كبيرة لخدمة هذه الجرائم في هذا التعاون الدولي في مكافحتها حتى لا يجد الجاني ملاذا آمنا في إحدى الدول للقيام بتلك الأعمال غير المشروعة، الأمر الذي يكون حائلا دون انتشار الإجرام المعلوماتي، نظرا لنوافق التعاون الدولي في مجال المكافحة، ضرورة التعاون لأن تلك الجرائم هي جرائم عابرة للحدود فيقع النشاط في الدولة وتقع النتائج في أخرى.³

الفرع الثاني: مبررات لتعاون الدولي

يعد التعاون الدولي في مكافحة الجريمة تبريره في بعض الاعتبارات:

أولاً: أن أي دولة مهما بلغت درجة قوتها وصلابتها لا تستغني عن الدخول في علاقات تعاون متبادلة مع غيرها من الدول، خاصة أن جهودها الداخلية في المكافحة أو الملاحقة للجرائم لم

¹ - أنبار سليمان ، الشراكة الافروجزائرية في مجال الطاقة ومكافحة الإرهاب الطبعة الأولى ، دار المعتر للنشر والتوزيع ، الجزائر 2024 - 1445 هـ . ص 25-26

² ناجي محمد الهتاش ، صلاح حسن جاب مسعود ، التعاون الأمني في دول حوض البحر الأبيض المتوسط ، التهديدات الأمنية ظل الصراعات الإقليمية والدولية، العربي لتوزيع والنشر، 2023، ص 20 .

³ أيمن عبد الله فكري ، الجرائم المعلوماتية ، دراسة مقارنة في التشريعات العربية والأجنبية ، الطبعة الأولى . مكتبة القانون والاقتصاد ، 2014-1435 ، ص 143

تعد كافية لمنع الجريمة أو تقليصها، وذلك بسبب التقدم التكنولوجي، مما ساعد على ظهور أنماط جديدة من الجريمة، وتفاقم حجمها على المستويات الوطنية والإقليمية والعالمية، كالجريمة المنظمة، والإرهاب، وغسل الأموال، والجرائم المعلوماتية، وتزييف العملة.¹

ثانياً: حتمية التعاون الدولي في مجال التدريب على مواجهة الجرائم الإلكترونية وخاصة في المجال الأمني، وأدلة إثبات الجريمة على مرتكبيها، حيث تتسم هذه الجرائم بالحدثة في الأسلوب وسرعة التنفيذ، وسهولة إخفائها، والمقدرة على محو آثارها، حيث إن استخدام مجرمي المعلوماتية الشبكة المعلوماتية ووسائلها في ارتكاب الجرائم يشكل عبئاً ثقيلاً على عاتق جميع أجهزة العدالة الجنائية.²

ثالثاً: تعتبر عملية تنفيذ الأحكام الجنائية وخاصة في مجال الجرائم الإلكترونية أسمى صدور التعاون الدولي الهادفة إلى تحقيق العدالة يتم تجسيد منطوق الأحكام وتتحول من صياغتها النظرية القانونية إلى عادي واقعي حيث ينال المدان جزائه، ويستحق المتضرر حقه، ويقتص المجتمع برمته ممن خالفوا قواعده.³

المطلب الثاني: دور المنظمات في تفعيل التعاون الدولي لمكافحة الجريمة

إن الأمر الذي أدى الى محاولة تكثيف الجهود الدولية والإقليمية والوطنية لمكافحة الجريمة، ما هو الا ما نتج عن الجرائم الخطرة التي تهدد المجتمعات في مختلف المجالات التي انطلقت من النطاق الداخلي لدولة الى النطاق الدولي، ولتفعيل التعاون الدولي سعت تلك الأخيرة في مكافحة الجريمة الى منظمات تنظمه وتسهل عليها التعاون.

¹ عادل عبد العال إبراهيم خراش ، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها . كلية الشريعة والقانون بالقاهرة ص184 .

² جمال محمد النقبي . د سلطان محمد سالم عوض هيسان المطيعي، التعاون الوطني والدولي في الجرائم الإلكترونية، مجلة المعهد العالي للدراسات النوعية مجلة 3 عدد 16 يوليو 2023، ص 20-55.

³ محمد مدين ، الجريمة الإلكترونية وتحديات الأمن القومي، 09.03.2025 004s 12h :book .goole .dz

الفرع الأول: المنظمة الدولية للشرطة الجنائية الإنتربول

كهيئة رئيسية في مجال مكافحة الجرائم الإلكترونية، تأسست المنظمة في عام 1923 وتتخذ من مدينة ليون مقراً لها. تركز جهودها على دعم الدول في التصدي لهذا النوع من الجرائم، من خلال تقديم قوائم تضم ضباطاً متخصصين في التحقيق والبحث المرتبط بالجرائم المعلوماتية، إلى جانب توفير المعلومات المتعلقة بأساليب التحقيق. كما تنظم المنظمة فرق عمل وورش تدريبية تهدف إلى تطوير الكفاءات وتعزيز القدرات في هذا المجال¹، ومن خلال السنوات الأخيرة نظراً لتطور الجريمة العابرة للحدود قد تركزت جهود واهتمامات الإنتربول بصورة أساسية في مكافحة الجريمة وذلك من خلال اتخاذ الوسائل اللازمة للوقاية منها والقضاء عليها.

تساهم منظمة الشرطة الجنائية بشكل كبير في مكافحة الجريمة المنظمة العابرة للحدود، سواء من خلال تأسيس لجان متخصصة لمعالجة أشكال ومظاهر هذه الجرائم، أو عبر تنظيم مؤتمرات تناقش فيها آليات التصدي لهذا النوع من الجرائم والحد من انتشارها بالإضافة إلى ذلك، تقدم المنظمة دعماً كبيراً للدول عبر تزويدها بمعلومات مهمة عن الأفراد المتورطين في ارتكاب الجرائم².

ومن بين الأهداف التي عملت بها المنظمة هي، العمل على تأمين أوسع النطاقات لكافة سلطات الشرطة للمساهمة في الوقاية من جرائم القانون العام، كما تهدف إلى التخطيط

¹ رياض بركات، محمد الصغير مسيكة، تسليم المجرمين كألية لتفعيل التعاون الدولي لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، المجلد 11، العدد 01، مخبر البحث في تطوير التشريعات الاقتصادية، جامعة تيسمسيلت، 2024، ص 133.

² محمد الصغير سيليني، موسى بن تغري، قرارات منظمة الأمم المتحدة والمنظمات الدولية المتخصصة ودورها في مكافحة الجريمة المنظمة عبر الوطنية، مجلة صوت القانون، المجلد 09، العدد 02، كلية الحقوق والعلوم السياسية، جامعة يحي بن فارس، المدية، 2023، ص 744.

مع الدول للتعاون في جمع المعلومات عن الجرائم والمجرمين والقبض عليهم سواء كانت الجرائم داخل إقليم الدولة أو خارجها وتقديمهم للعدالة¹.

الفرع الثاني: دور الأمم المتحدة في مكافحة الجريمة

تظافرت جهود الدول في مواجهة الجريمة الإلكترونية وقدمت أعمال تشاركية جماعية بهدف الحد منها، ذلك من خلال المؤتمرات التي نظمتها الأمم المتحدة التي تلعب دور هام في حفظ السم والأمن ومكافحة الجريمة المنظمة التي انتشرت بسرعة وأصبحت تهدد الأمن والسم الدوليين في الدول العظيمة ليس ذلك فقط بل حتى تنامت في الدول النامية.

وللإشارة إلى منظمة الأمم المتحدة نجد أنها أنشأت من قبل معاهد "سان فرانسيسكو" في العام 1945، اشتمل ميثاقها على ديباجة و111 مادة، لها ستة أجهزة رئيسية تعمل على تنفيذ أهدافها المتمثلة في: مجلس الأمن، الجمعية العامة، المجلس الاقتصادي، مجلس الوصاية، محكمة العدل الدولية، الأمانة العامة، ومن خلال هاته الأجهزة التي نجدها تلعب دور هام مكافحة الجريمة والحفاظ على السلم، كما نجدها تصدر بعض التوصيات للدول الأطراف لاتخاذ الإجراءات المناسبة لمجابهة الوضع القائم².

في إطار جهود الأمم المتحدة لمكافحة الجريمة الإلكترونية، أسهمت مؤتمراتها بشكل كبير في صياغة السياسات الجنائية وتعزيز التعاون الدولي، كما لعبت دوراً مهماً في التصدي للمخاطر والتهديدات التي تنشأ عبر الشبكة الرقمية من بين هذه المؤتمرات، عقد المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية في البرازيل خلال الفترة من 12 إلى 19 أبريل 2010، حيث استعرضت الدول الأعضاء التطورات الحديثة في توظيف التكنولوجيا من قبل مرتكبي الجرائم والجهات المختصة بمكافحة الجريمة، بما يشمل الجرائم الإلكترونية وقد حظيت

¹ أسامة غربي، المنظمة الدولية للشرطة الجنائية (الانتربول) ودورها في مكافحة الجريمة المنظمة، دراسات وأبحاث، المجلد 03، العدد 03، جامعة يحي بن فارس، المدينة، 2011، ص 161.

² رابح نهايلي، قيرة سعاد، دور المنظمات الدولية في مكافحة الجريمة المنظمة (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجاً)، مجلة البحوث القانونية والاقتصادية، المجلد 04، العدد 02، جامعة غرداية، 2020، ص 129/128.

هذه الفئة من الجرائم بمكانة بارزة ضمن جدول أعمال المؤتمر، تأكيداً لأهميتها والتحديات التي تفرضها¹.

المطلب الثالث: دور المعاهدات والاتفاقيات الدولية في مكافحة الجرائم الالكترونية

تلعب المعاهدات والاتفاقيات الدولية دوراً أساسياً في مكافحة الجرائم الالكترونية وذلك من خلال التعاون الدولي بين الدول وهي عبارة عن "اتفاق دولي المعقود بين الدول في صيغة مكتوبة والذي ينظمه القانون الدولي، سواء تضمنته وثيقة واحدة أو وثيقتان متصلتان أو أكثر مهما كانت تسميته الخاصة"²، ومن المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الالكترونية.

الفرع الأول: معاهدة بودابست لمكافحة جرائم الانترنت

The Budapest convention on cyber crimes

شهدت العاصمة المجرية بودابست في أواخر عام 2001 ميلاد أولى المعاهدات الدولية التي تكافح الجرائم الانترنت *internet crimes* وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها لا سيما بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات³ وتحث على هذه المعاهدة 26 دولة أوروبية بالإضافة إلى كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية.

تضمنت هذه الاتفاقية 48 مادة وأكدت الاتفاقية على الحاجة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء لمكافحة الجريمة المعلوماتية واعتبرت مرجعاً لا يستهان به في ميدان محاربة الإجرام الالكتروني

¹ احمد رجدال، جهود منظمة الأمم المتحدة في سبيل مواجهة الجريمة الالكترونية، المجلة التقنية للقانون والعلوم

السياسية، المجلد 19، العدد 02، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2024، ص 686.

² المادة 2 من اتفاقية فيينا لقانون المعاهدات 1996.

³ جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، عمان، دار البداية ص 227

سواء بالنسبة لبعض الاتفاقيات اللاحقة ذات صلة أو بالنسبة للتشريعات الداخلية لبعض الدول ، لقد ركزت اتفاقية بودابست على ثلاث عناصر أساسية :¹

- العنصر الأول : يتمثل في أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية .

- العنصر الثاني : يتمثل في أهمية التدابير التشريعية الإجرامية المتلائمة مع طبيعة الجرائم الالكترونية .

العنصر الثالث: أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم والانطلاق أنتجت من جهود دولية وإقليمية في هذا المجال وكان ذلك في مواد الاتفاقية الموزعة على أربعة أبواب:

الباب الأول: الحكام العامة ، المواد من (1 - 6)

المادة 1: تحديد المصطلحات الأساسية .

المادة 2- :6 تحديد الجرائم الأساسية ، الوصول الغير القانوني للبيانات ، الاعتراض غير القانوني ، تداخل البيانات والأنظمة ، إساءة استعمال الأجهزة .

الباب الثاني :الإجراءات القانونية (المواد 7 - 22)

وقسم إلى 3 أقسام القسم الأول المواد من 7 - 13 تجريم الجرائم الالكترونية. القسم الثاني المواد 14 - 21 الإجراءات القانونية للتحقيقات. القسم الثالث المادة 22 تتعلق باختصاص المنوط.

الباب الثالث: وجاء تحت عنوان التعاون الدولي (من المادة 23 - 35)

¹ قطاف سليمان، بوقرين عبد الحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، مخبر البحث في الحقوق والعلوم السياسية، المجلد 06، العدد 01، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي، الاغواط، 2022، ص 339 .

الباب الرابع: تضمنت الأحكام الختامية المواد (36 - 48)

- جاءت هذه الاتفاقية اقتناعا بضرورة مباشرة سياسية عقابية مشتركة موجهة لحماية المجتمع من الإجرام في الأوساط الالكترونية لاسيما من خلال تبني تشريع مناسب ومن خلال تطوير التعاون الدولي ووعيا بالتغيرات العميقة الناجمة عن المخالفات الجنائية التي قد تنفذ عبر الشبكات الالكترونية ، ذات الخصوصية والصعوبة في تقفي أدلتها واعتقاد بضرورة التعاون الدولي بهدف المواجهة الفعالة والسريعة لتلك الجرائم.¹

الفرع الثاني: الاتفاقية العربية لمكافحة الجريمة الالكترونية.

لا تعتبر الجرائم الالكترونية منتشرة في الدول العربية بنفس الدرجة التي تنتشر بها في الدول الأخرى، لكن هذا لا يعني عدم اتخاذ تدابير اللازمة لمواجهتها لذلك تعمل الدول العربية على وضع قوانين وتشريعات تساعد على الحد من هذه الجرائم، فقامت الدول العربية بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 أدت هذه الاتفاقية إلى ميلاد قوانين عديدة لمكافحة الجريمة الالكترونية في الدول العربية ،وصارت سارية المفعول بعد تصديق الرئيس المصري عليها²، تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أفضاء هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها و أفرادها³ وهذا ما تضمنته المادة الأولى من الاتفاقية ،نجد في الفصل الثاني تأصيل للأفعال التي تعد مجرمة ، وذلك من خلال نص المادة 5 تشمل اتفاقية مجموعة واسعة من الجرائم الالكترونية منها :

- جريمة الدخول غير المشروع الجرائم ضد سرية وسلامة وتوافر البيانات وأنظمة المعلومات إساءة استخدام وسائل تقنية المعلومات المادة من 6 إلى 9.
- الجرائم المالية الالكترونية: جريمة التزوير، جريمة الاحتيال مثل سرقة البطاقات الائتمانية، تعطيل الأجهزة والبرامج والموقع الالكترونية المادة 10 و 11 .

ميرفت محمد حبابية، مرجع سابق، ص 265- 266.¹

ميرفت محمد حبابية، مرجع سابق ص 271 .²

المادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .³

- الجرائم المرتبطة بالمعتدي غير قانوني ، ذلك من خلال نشر مواد تحريض أو تنتهك القيم الأخلاقية ، إنتاج أو عرض أو توزيع أو توفير أو بيع أو، استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات ، المقامرة ، الاستغلال الجنسي ،المادة 12 و 13 .

انتهاك الخصوصية وسرقة البيانات الشخصية، الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات المادة 14.

التزوير الالكتروني وانتحال الهوية الرقمية، كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تحيل أو تقليد أي أداة من أدوات الدفع الالكتروني بأي وسيلة كانت، الاستخدام الغير مشروع لأدوات الدفع الالكتروني المادة 18 .

أما الفصل الثالث تم التعرض من خلاله إلى نطاق تطبيق الأحكام الجزائية، وفي الفصل الرابع نص على التعاون القانوني والقضائي أما الفصل الخامس تضمنت أحكاما ختامية.¹

¹ عماد مفلح الحسيان، عز الدين أحمد النعيمي، عدنان محمد الضمور، ياسر طالب الخزاعلة، الجرائم المستحدثة، المعلوماتية ، الالكترونية السيبرانية، الطبعة الأولى دار الخليج للنشر والتوزيع ، الأردن ، عمان 2024 ، ص 164 .

ملخص الفصل الأول

يتناول الفصل الأول الجريمة الإلكترونية باعتبارها من الجرائم المعاصرة التي فرضها التقدم الرقمي والتكنولوجي، وهي تختلف عن الجرائم التقليدية من حيث الوسيلة والمجال والأسلوب، حيث تُرتكب في بيئة افتراضية باستخدام تقنيات المعلومات الحديثة. وقد أدى غياب تعريف موحد للجريمة الإلكترونية إلى ظهور تعريفات متعددة في الفقه والقوانين الوطنية، ركزت معظمها على استخدام الحاسوب أو شبكة الإنترنت كوسيلة لتنفيذ أفعال غير مشروعة.

كما يدرس هذا الفصل الخصائص المميزة للجريمة الإلكترونية، وأهمها طابعها العابر للحدود، وصعوبة اكتشافها، وسهولة تنفيذها، وتعدد أشكالها، مما يجعلها تمثل تهديدًا واسع النطاق على الأفراد والمؤسسات والدول.

ويتطرق الفصل أيضًا إلى الأركان الثلاثة التي تقوم عليها الجريمة الإلكترونية: الركن الشرعي (النص القانوني)، الركن المادي (السلوك الإجرامي والنتيجة)، والركن المعنوي (القصد الجنائي). كما يُبرز أهمية التعاون الدولي في مواجهتها، من خلال سن التشريعات المناسبة وتفعيل الاتفاقيات والآليات القانونية الدولية، خاصة في ظل العجز الذي تعانيه الأنظمة الوطنية بمفردها في التصدي لها.

الفصل الثاني

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الإلكترونية والمعوقات التي

تواجهها

بعد أن تناول الفصل الأول الأساس النظري والقانوني للجرائم الإلكترونية، يأتي هذا الفصل ليركز على الجانب العملي والتطبيقي في مكافحة هذه الجرائم، مع إبراز أهمية التعاون الدولي كأداة فعّالة للتصدي لتحديات الأمن السيبراني، إذ لم تعد الجهود الوطنية مجدية بمفردها في مواجهة الجرائم التي تتسم بطابعها العابر للحدود وسرعة تطورها التقني، مما يستوجب تضافر جهود الدول والمنظمات الدولية عبر آليات متنوعة.

يتناول هذا الفصل أبرز أوجه التعاون الدولي في المجال الأمني والقضائي، مع التركيز على دور المنظمات الدولية مثل الإنتربول، بالإضافة إلى دراسة المساعدات القضائية وآليات تبادل المعلومات والخبرات بين الدول. كما يسلط الضوء على المعوقات والتحديات التي تعترض فاعلية هذا التعاون، مثل اختلاف النظم القانونية، التعقيدات التقنية، وصعوبة إثبات الجرائم الإلكترونية.

ويهدف الفصل إلى تقديم رؤية شاملة تساعد على فهم الواقع العملي لمكافحة الجرائم الإلكترونية، وتبيان أهمية تنسيق الجهود وتطوير الآليات الوطنية والدولية، لضمان تحقيق أمن معلوماتي فعال وحماية الحقوق في ظل التقدم الرقمي المتسارع.

المبحث الأول: أوجه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية

ينبغي على جميع الدول الأعضاء في المجتمع الدولي الالتزام بمتطلبات هذه العضوية، والتي تتضمن إقامة علاقات ثنائية تعنى بالمساعدة القضائية المتبادلة، الهدف من هذه الجهود هو تعزيز التعاون المشترك واتخاذ إجراءات فعالة للحد من الجريمة ومحاسبة مرتكبيها، نظرًا لعدم إمكانية أجهزة إنفاذ القانون تجاوز حدودها الإقليمية للتعامل مع المجرمين الفارين إلى دول أخرى ذات سيادة، يصبح التعاون الدولي ضروريًا ولذا فإن توحيد الإجراءات القضائية لضمان فعاليتها عبر الحدود الإقليمية يشكل ضرورة ملحة، ومن خلال ما يلي سوف نقوم بالتطرق في هذا المبحث إلى مطلبين، بحيث تضمن المطلب الأول التعاون القضائي، والمطلب الثاني التعاون الدولي في مجال التدريب.

المطلب الأول: التعاون القضائي

من المؤكد أن الجريمة لم تعد مجرد مسألة داخلية، وأن المقاومة المنفردة أو المحلية باتت غير فعالة، فيجب أن تتضافر جهود الدول وتتعاون لمواجهة هذه الظاهرة الإجرامية، وهذا يتطلب عدم وجود حواجز حدودية بين الدول، ومنع عرقلة السلطات العامة في تنفيذ الأحكام الجنائية الصادرة عن دول أخرى بحق الأشخاص المتواجدين داخل حدودها.

الفرع الأول: التعاون الأمني على المستوى الدولي

تتميز محاسبة المجرمين، وخاصة الجرائم الإلكترونية، بالجرائم العابرة للحدود، قد يكون المهاجمون يحملون جنسية بلد ما ولكنهم يرتكبون الجريمة على معدات في بلد آخر، مع وقوع عواقب الجريمة في بلد ثالث لذلك كان لا بد من الحاجة الملحة إلى توحيد الجهود لتبادل البيانات والمعلومات المتعلقة بالجريمة والتي يمكنها الكشف عن هوية المجرمين، إذ لا يمكن للدولة القضاء على مثل هذه الجرائم بمفردها، لأن أجهزة الشرطة لا تستطيع تعقب وملاحقة مرتكبي الجرائم خارج حدودها.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الإلكترونية والمعوقات التي تواجهها

أولاً: تعريف التعاون الأمني

يعتبر التعاون الأمني أحد أوجه التعاون الدولي المتعددة، الهدف منه ملاحقة المجرمين ومكافحة الجرائم والقضاء على أشكال الجريمة المنظمة التي تزعزع الأمن، كما يمثل مظهراً من مظاهر تشابك المصالح الدولية الذي أدى إلى سرعة وسهولة وسائل الاتصالات للتقدم العلمي¹، ومنه يرتبط الدول ببعضهم وتوطيد علاقات الصداقة ومكافحة المسائل الأمنية كما يساهم في استقرار سياسة التعايش السلمي وتسوية النزاعات بشكل سلمي.

ثانياً: أهمية التعاون الأمني

لا تقدر الدولة منفردة على التصدي لهذه الجريمة العالمية بجهاز أمني لا تتجاوز صلاحياته وسلطاته نطاق وحدود الدولة، فمتابعة فاعلي هذه الجرائم وتقديمهم للعدالة لتنفيذ العقاب يتطلب القيام بتحقيقات خارج حدود الدولة، حيث وقعت الجريمة أو جزء منها، وتشمل هذه التحقيقات فحص مواقع الإنترنت في الخارج، أو ضبط الأقراص الصلبة، أو تفتيش الحواسيب الآلية ولهذا، يصبح من الضروري مواجهة هذه الجريمة من خلال التعاون الدولي على المستوى الإجرائي الجنائي، مما يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة ويتحقق ذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم ونشرها².

وتتجلى أهمية التعاون الأمني في استخدام التقنيات المتقدمة لإجراء التحقيقات والتحريات في مجال مكافحة الجرائم الإلكترونية، واستخدام تقنيات الاتصال الحديثة مثل الدوائر التلفزيونية المغلقة، واعتماد أساليب التحقيق والمراقبة المتخصصة، وإنشاء قنوات الاتصال، والتنسيق الأمني والقضائي بين الجهات المختصة عبر الأقمار الصناعية والإنترنت، والتبادل

¹ خالد محمد نور، عبد الحميد الطباخ، التعاون الدولي في مكافحة الإرهاب، محاضر القانون الدولي بالجامعات المصرية، جامعة مدينة السادات، د س ن، ص 12.

² سميرة معاشي، آليات مكافحة الجريمة المعلوماتية دراسة مقارنة، أطروحة دكتوراه علوم في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة، 2019/2020، ص 296.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الإلكترونية والمعوقات التي تواجهها

السريع للمعلومات، وإيفاد القضاة إلى الدول المعنية لإجراء التحقيقات واتخاذ الإجراءات اللازمة¹.

ثالثاً: أساليب التعاون الأمني

إن التعاون الأمني الدولي لمكافحة هذه الأنماط الإجرامية يجب أن يعتمد على آليات متطورة تواكب تطور هذه الجرائم، ويجب أن يركز هذا التعاون الدولي على أسس ملموسة تضمن في نهاية المطاف مكافحة هذه الجرائم بطريقة بناءة ولذلك فإن التعاون الأمني الدولي في مجال مكافحة الجرائم الإلكترونية والوقاية منها يجب أن يركز على²:

يقتضي البحث العلمي في ظواهر جرائم الإنترنت تقديم معطيات وبيانات إحصائية ضرورية يجب أن تشمل هذه البيانات تفاصيل عن الجريمة نفسها، وعن المجرمين، وعن مسار النظام القضائي الجنائي، هذه المعلومات أساسية للتعامل مع هذه الجرائم بدقة وفعالية، ولتحقيق فهم شامل لأبعادها المتنوعة. لذلك، يجب إنشاء كيان دولي متخصص في جمع وتحليل هذه البيانات المتعلقة بجميع أنواع وأشكال جرائم الإنترنت.

تنسيق مختلف الأجهزة والآليات الأمنية في المجالات الأمنية الإقليمية والدولية للحد من معدل الجريمة ومنع تفاقمها وسد الثغرات في المعلومات الأمنية وجمع عناصر المعلومات من خلال التعاون للكشف في نهاية المطاف عن حجم الجريمة وخطط الإعداد الإجرامي.

تحديد سبل التعاون في مجال التدريب والتعاون التقني، وتحقيق التكامل الأمني بين الأجهزة الأمنية على المستوى الدولي.

¹ سليمان أبو نمر، يوسف بوكشيدة، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة ماستر، تخصص

قانون دولي عام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة، 2021/2020، ص 25.

² عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعية الجديدة، ط 01، الإسكندرية، 2015، ص 192.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

إعداد مدونة دولية تتضمن توحيد المعايير والأركان القانونية التي تقوم عليها هذه الجرائم، ونطاق الأفعال المؤثرة فيها، مع ضمان أن يشكل نطاق التجريم كافة جوانبها ومراحلها.

الفرع الثاني: المساعدة القضائية

تلعب المساعدة القضائية دوراً حيوياً في تعزيز فعالية النظام القانوني من خلال تبسيط المهام المرتبطة بالمحكمة وتسهيل إجراءات التعاون بين الدول المختلفة وذلك يشمل، بشكل خاص عمليات نقل وتسليم الأفراد من دولة إلى أخرى، مما يساهم في تحقيق العدالة الدولية وتعزيز الأمن القانوني عبر الحدود، هذه العملية تتطلب تنسيقاً محكماً بين السلطات القضائية في الدول المتعاونة لضمان احترام القوانين والمعايير الدولية بالإضافة إلى حماية حقوق الأفراد المعنيين.

أولاً: تعريف المساعدة القضائية

يقصد بالمساعدة القضائية الدولية "كل إجراء قضائي تقوم به السلطات المختصة في الدولة المطلوب منها بناء على طلب الدولة الطالبة من شأنه تسهيل مهمة المحاكمة وكشف الحقيقة بصدد جريمة من الجرائم، وقد اصطلح عليها في بعض الصكوك الدولية المساعدة القانونية المتبادلة شأن اتفاقية الأمم المتحدة لمكافحة الجريمة"¹.

وبالنظر الى القانون رقم 09/04 نجد في نص المادة 16 منه أنه ذكر المساعدة القضائية بقوله "في إطار التحريات أو التحقيقات القضائية الجارية لمعينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني"².

¹ جندلي وردة، التعاون الدولي لمكافحة الجريمة المعلوماتية الفاعلية والتحديات، مجلة القانون والعلوم السياسية، المجلد

10، العدد 02، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955، سكيكدة، 2024، ص 326.

² المادة 16 من القانون 09/04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

ثانياً: أساليب المساعدة القضائية

بالنظر إلى ما ورد في المادة 16 من القانون 09/04 الذي أقره المشرع الجزائري، نجد أنه في سياق التحريات والتحقيقات القضائية المتعلقة بجرائم المعلوماتية، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة المتعلقة بهذه الجرائم بشكل إلكتروني.

1. تبادل المعلومات

يُعدّ تبادل المساعدة القضائية والقانونية في القضايا الجنائية بين الدول الجانب الآخر للملاحقة القضائية في مجالات التعاون الدولي الفضائي على صعيد مكافحة جريمة الجرائم الإلكترونية، لما تحققه من تيسير للعقبات التي تعارض سير الإجراءات الجنائية كوسيلة هامة لمواجهة الإفلات من العقاب باعتبارها آلية ناجعة لمعالجة الجوانب المعقدة والخطيرة للجريمة، ولكون الحصول على البيانات والشهود من دولة لأخرى يثير العديد من التساؤلات والإشكالات القانونية المعقدة المتعلقة بالطرق التي يمكن من خلالها أن يُصاغ هذا التعاون بشكل يجعل هذه الإجراءات مُناسبة ومُيسرة لدى الدولة المطلوب منها المساعدة ومقبولة قانوناً لدى السلطة القضائية المختصة بالدولة الطالبة¹.

2. نقل الإجراءات

ويعني به قيام بلد ما بالاستناد إلى اتفاقية أو عهد باتخاذ إجراءات جنائية وهي بصدد جنحة ارتكبت في إقليم دولة أخرى والمصلحة لهذه الدولة متى ما توفرت شروط محددة من أبرزها التجريم المزدوج، وأن تكون التدابير اللازم اتخاذها ذات أهمية بالغة بحيث تؤدي دوراً مهماً في التوصل إلى الحقيقة. ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل

¹ ياكرو الطاهر، المرجع السابق، ص 177.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

الإجراءات في القضايا الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م في المادة 21 منها¹.

3. الإنابة القضائية

يعرف الفقه الإنابة القضائية بأنها "تفويض تنيب بمقتضاه سلطة قضائية بمناسبة دعوى منظورة أمام محاكمها سلطة قضائية أخرى بقصد القيام بجمع أدلة الإثبات أو الاستدلالات أو انجاز تحقيق ما يقتضيه الفصل في النزاع المعروض أمامها ويتعذر عليها القيام به بنفسها في نطاق دائرة اختصاصها"².

الهدف من الإنابة القضائية هو تسهيل الإجراءات في المسائل الجنائية لمواجهة التحديات الناتجة عن تطور الظواهر الإجرامية، والتغلب على العقبات التي تعترض سير الإجراءات الجنائية المتعلقة بقضايا ذات امتداد عالمي هذا يضمن إتمام عمليات البحث والتحقيق اللازمة للحصول على الأدلة والقرائن المطلوبة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تعيق قيام الدول الأجنبية ببعض الأعمال القضائية داخل حدود الدول الأخرى، تعبر الإنابة القضائية عن قيام دولة بأداء إجراء قضائي متعلق بدعوى جارية ضمن الحدود الإقليمية لدولة أخرى نيابة عنها، وذلك بناءً على طلب الدولة المناب عنها ووفقاً لما تحدده بنود الاتفاقية الدولية المبرمة بين الدولتين بهذا الشأن. تهدف الإنابة القضائية إلى تيسير الإجراءات الجنائية في ظل استمرار تطور الأنشطة الإجرامية، خاصة في العصر الرقمي الحديث³.

¹ سليمان عيسى محمد أحمد، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الأكاديمية للبحث القانوني، المجلد

14، العدد 02، كلية العلوم والدراسات الإنسانية بلغاط، جامعة المجمعة، المملكة العربية السعودية، 2016، ص 55.

² عبد العال محمد عكاشة، الإجراءات المدنية والتجارية وتنفيذ الأحكام الأجنبية، دار المطبوعات الجامعية، الإسكندرية، 2007، ص 239.

³ ياكور الطاهر، المرجع السابق، ص 180.

المطلب الثاني: التعاون الدولي في مجال تدريب رجال العدالة في مواجهة الجريمة

مع تزايد انتشار الجريمة الإلكترونية على المستويات الدولية أصبح من الضروري تنمية معارف ومهارات العاملين في مجال العدالة المختصين بمكافحة الجريمة الإلكترونية، من خلال الاطلاع المستمر على المفاهيم والأساليب القانونية الحديثة، ومتابعة التطورات التي طرأت على طبيعة الجريمة مع دخول عصر تكنولوجيا المعلومات والتقنيات المتقدمة.

الفرع الأول: أهمية تدريب المكافحين للجرائم الإلكترونية

يتطلب التأهيل في مجال الجرائم الرقمية امتلاك معرفة ومهارات محددة، وهو أمر لا يتحقق إلا من خلال تدريب متخصص ومستمر، والتدريب في جوهره هو عملية ممنهجة ومستمرة تهدف إلى سد الفجوة بين مستوى الأداء الحالي والمستوى المطلوب من الشخص العامل في هذا المجال ويعتمد التدريب على تحديد المهارات والكفاءات الضرورية لمن يشغلون هذه الوظائف، ثم العمل على إحداث تغييرات إيجابية في سلوك الأفراد أو المجموعات وقدراتهم لتحقيق أداء متميز¹.

وتتزايد الأهمية البالغة للتدريب في هذا العصر، وذلك بسبب التقدم التكنولوجي الهائل الذي يغمر العالم، والتدريب الذي نقصده هنا يتجاوز التدريب التقليدي، فلا يكفي لموظفي العدالة الجنائية أن يمتلكوا المعرفة القانونية الأساسية أو مبادئ العمل الشرطي؛ بل يجب تزويدهم بمهارات فنية متخصصة في مجال الجرائم المعلوماتية. هذه الخبرات الفنية لا يمكن اكتسابها إلا من خلال تدريب متخصص، يراعي فيه الجوانب الشخصية للمتدرب، مثل المؤهلات العلمية والقدرات الذهنية والنفسية الضرورية لاستيعاب التدريب. تجدر الإشارة إلى

¹ خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، بحث مقدم لاسيافاء متطلبات الحصول على درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة، د ب ن، د س ن، ص 34.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

أن تدريب متخصص في تكنولوجيا المعلومات والشبكات أسهل بكثير من تدريب العاملين في إنفاذ القانون، مثل رجال الشرطة أو أعضاء النيابة العامة¹.

الفرع الثاني: الآليات المعتمدة في مجال التعاون الدولي لتدريب رجال العدالة

تعتبر من أبرز الآليات المستخدمة في التعاون الدولي لتدريب رجال القانون هي تنظيم ندوات ومؤتمرات أو ورش عمل جماعية متخصصة في مواجهة الجرائم و تُعقد هذه الفعاليات على المستويات الدولية والإقليمية، حيث تقدم مجموعة من الأبحاث المتعلقة بالمستجدات في مجال الجرائم المستحدثة من خلالها يتم تحليل ومناقشة أبعاد هذه الجرائم بأسلوب مدروس، مما يمكن رجال القانون العاملين في الوقاية من هذه الجرائم ومكافحتها من التعرف على أساليب ارتكابها وإدراك مخاطرها، كما تساعدهم هذه الفعاليات على اكتساب معرفة بالآليات الفعالة للوقاية والمكافحة بما يفوق قدرات ووسائل مرتكبي تلك الجرائم².

وفي إطار تدريب رجال العدالة، هناك عدد من الاتفاقيات الدولية والإقليمية التي تؤكد بشكل واضح على أهمية التعاون بين الدول في مجالات التدريب وتبادل الخبرات، مثال على ذلك هو المادة 9 من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود، يمكن أن يتحقق التعاون الدولي في تدريب رجال العدالة على التعامل مع الجرائم المرتبطة بالإنترنت بين الدول وأجهزتها القضائية، في مصر مثلا تقوم النيابة العامة بتنظيم الندوات والمؤتمرات وحلقات النقاش، سواء داخل البلاد أو خارجها كما ترسل أعضاء النيابة من مختلف المستويات إلى برامج تدريبية خارجية بالتعاون مع هيئات النيابة العامة الدولية، للاستفادة من أحدث الأنظمة المتاحة عالمياً في هذا المجال، وإقامة هذه اللقاءات والندوات تساهم في تبادل الآراء والخبرات بين المشاركين، وتعزز من الحوار ومشاركة الأفكار والتصورات كما تشجع التعاون

¹ فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01، بن يوسف بن خدة، 2017/2018، ص 84.

² ادريس خوجة نضيرة، دور التعاون الدولي في مجال تدريب رجال العدالة في مواجهة الجريمة الالكترونية، مجلة القانون الدولي والتنمية، المجلد 10، العدد 01، جامعة الجبالي ليايس، سيدي بلعباس، 2022، د ص.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

بين الدول والأطراف أو المعاهدات لمكافحة الجرائم المنتشرة عبر الحدود¹، كما ينبغي على كل دولة سن قوانين تجرم وتعاقب على الأفعال التالية التي تستهدف بيانات الحاسوب المتمثل في الإضرار بها، إتلافها، محوها، تعطيلها، أو تعديلها، كما يجب أيضاً اعتبار جرائم جنائية معاقب عليها، الأفعال التي تعيق وظائف شبكة الإنترنت والحواسيب المتصلة بها ويشمل ذلك إدخال، نقل، الإضرار، محو، إتلاف، تعديل، أو تعطيل بيانات الحواسيب المتصلة بالإنترنت، سواء كانت خوادم أو أجهزة متصلة، علاوة على ذلك يتعين على كل دولة اعتماد تدابير قانونية تسمح بمحاسبة الكيانات الاعتبارية جنائياً على الجرائم المتعلقة بالحاسوب والإنترنت ويشمل ذلك حالات التقصير في الإشراف والرقابة من قبل الأشخاص الطبيعيين، مما يؤدي إلى وقوع جرائم أو يسهل ارتكابها².

المبحث الثاني: معوقات التعاون الدولي

لقد تعددت الإشكاليات التي تواجه التعاون الدولي في مكافحة الجرائم الالكترونية على جميع المستويات، ومنه تم تقسيم هذا المبحث إلى ثلاثة مطالب، حيث تضمن المطلب الأول دراسة هذه الإشكاليات على الصعيد الوطني، والمطلب الثاني على الصعيد الدولي أما بالنسبة إلى المطلب الثالث تم فيه اقتراح أهم البدائل لمكافحة الجرائم الالكترونية.

المطلب الأول: معوقات على الصعيد الوطني

على المستوى الوطني هناك مشكلتين يعيقا التعاون الدولي في مكافحة الجرائم الالكترونية وهي كالتالي:

الفرع الأول: عدم كفاية وملائمة القوانين القائمة.

إن التطور في المجال التكنولوجي سواء من ناحية الحياة العامة أو الخاصة واعتماد الجميع عليه في سائر شؤونهم، واستغلال الجناة لتلك التقنية في ارتكاب جرائمهم. هذا التطور

¹ سليمان أبو نمر، يوسف كشريدة، المرجع السابق، ص 40.

² عادل عبد العال إبراهيم خرشي، المرجع السابق، ص 251.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

في الحقيقة لا يقابل - وللأسف - تطور بذات الدرجة في النصوص القانونية¹ وذلك كون اليوم المجال الالكتروني يشهد يوميا تطورا استثنائيا، يجب على الدول أن تتبع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من مخاطر الجريمة المعلوماتية وذلك من خلال تبني التشريعات الملائمة لمواجهة المتمثلة في إمكان شبكات الكمبيوتر والمعلومات الالكترونية في ارتكاب أفعال إجرامية.²

فعلى الدول أن تتبنى قوانين ملائمة وقائمة بحد ذاتها على مواجهة هذه الجرائم والحد منها، فالكثير من النصوص القانون الجنائي لبعض الدول لا يكفي بوضعها الحالي بمواجهة هذه الجريمة. لتطلب غالبية النصوص الصفة المادية في الشيء محل ارتكاب الجريمة.³ ومنه فان طبيعة الجريمة الالكترونية أو المعلوماتية تختلف عن طبيعة الجريمة التقليدية وهذا ما يجعلها تنفي صورة التجريم والعقاب، ولقد وضع المشرع الجزائري عدة آليات تشريعية لمكافحة الجرائم الالكترونية والحد منها من خلال إضفاء تعديلات على قانون العقوبات بموجب القانون رقم 15/04 في قسم تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.⁴ وذلك لتجريد الأفعال المتعلقة بنظام الحاسوب والمعلوماتية. جاء هذا التعديل في المواد من 394 مكرر إلى 394 مكرر 7، كما قام المشرع بتعديل في 2006 في القسم السابع مكرر منه وجاء هذا التعديل مضاعفة العقوبة المقررة لهذه الجرائم.

كما قام المشرع بقانون جديد 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها. ومن الجرائم التي أقرها المشرع الجزائري في المادة 2 الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

¹ عادل عبد العال ابراهيم خراشي، المرجع نفسه، ص

² عبد العال الديربي، الجرائم الالكترونية، Almanhd, 2012 ص 346

³ قاضي خولة، جباس منال، التعاون الدولي في مكافحة الجريمة المعلوماتية، مذكر الماستر في الحقوق تخصص قانون أعمال، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 2021/2020، ص 36.

⁴ مرابط رميساء، مواجهة الجريمة الالكترونية ضمن مقتضيات تحقيق الأمن السيبراني، مجلة الحوكمة والقانون الاقتصادي، العدد 10، سنة 2010، ص 71.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

- النظام المعلوماتي.
- المعطيات المعلوماتية.
- مقدمو الخدمات.
- المعطيات المتعلقة بحركة السير.
- الاتصالات الالكترونية.

المادة 2 من القانون رقم 9-0-04 مؤرخ في 14 شعبان 1430 الموافق لـ 5 غشت 2009 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الفرع الثاني: صعوبة إثبات الجرائم الالكترونية والتحقيق فيها

إن الجريمة المعلوماتية تقسم بحدثة أساليبها وارتكابها وسرعة تنفيذها، وسهولة إخفائها، ودقة محو أثارها، وعلى هذا فان الأمر يتطلب أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها، وأساليب ارتكاب الجرائم عليها.¹

وبالتالي فان مسألة الإثبات في الجرائم الالكترونية ونظم الحاسوب والانترنت صعوبات كبيرة أمام القائمين على التحقيق، كالتخزين الالكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة. ويشكل انعدام الدليل المرئي (المفهوم) عقبة كبيرة أمام كشف الجرائم. وقد يشكل تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات الاتصال عقبة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة.

¹ خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2019 ص 94.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

كما أن سهولة محو الدليل في زمن قصير تعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب والانترنت.¹

كما أنه من المسائل التي تعيق عمليات البحث والتحقيق في الجرائم الالكترونية نقص في المعرفة التقنية الحديثة والمتجددة لدى القائمين بالبحث والتحقيق في هذه الجرائم مما يجعل منهم غير قادرين على أداء واجبهم على الوجه المطلوب إذ أن نقص الخبرة والكفاءة سواء في أجهزة الشرطة أو الادعاء يعد من الأسباب الرئيسية في الإخفاق في كشف الجرائم الالكترونية²

المطلب الثاني: معوقات على الصعيد الدولي

مع ضرورة التعاون الدولي لمكافحة الجرائم المعلوماتية ومناداة به إلا أنه ثمة معوقات تقف دون تحقيقه وهي:

الفرع الأول: القصور التشريعي للدول والتعارض بين مصالحها

إن أبرز المعوقات التي تواجه الدول لتنظيم موضوع الجرائم الالكترونية هو تفاوت الدول في تحديد مفهوم الجرائم الالكترونية وأساليب التعامل معها، وهذا راجع إلى أن كل دولة تعمل على تنظيم موضوع التقنيات الالكترونية ضمن حدود قيمتها السياسية والقانونية والأخلاقية والثقافية³، وبمنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدول يمكننا القول بعدم وجود اتفاق عام بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها، أو بمعنى آخر عدم وجود نظام قانوني لدى الدول خاص بمكافحة الجرائم المعلوماتية، فما يكون مباحا في أحد الأنظمة قد يكون مجرما في نظام آخر.⁴

¹ لؤي عبد الله نوح، مدى مشروعية المراقبة الالكترونية في الإثبات الجنائي وحجية مشروعية الدليل الالكتروني المستمد في التفتيش الجنائي وعوامل حجية الصورة والصوت في الإثبات الجنائي، الطبعة الأولى، مركز الدراسات العربية، مصر، 2018، ص 65.

² فارس العمارات، جرائم العصر من الرقمية إلى السيبرانية، الطبعة الأولى، دار الخليج للنشر والتوزيع، الأردن، 2023، ص ص 174-175.

³ عماد الحسيان، عدنان الضمور، عز الدين التميمي، ياسر الخزاعلة، الجرائم المستحدثة المعلوماتية، الالكترونية

السيبرانية، الطبعة الأولى، دار الخليج للنشر والتوزيع، الأردن: عمان، 2024، ص 93.

⁴ عادل عبد العال، ابراهيم خراشي، مرجع سابق، ص 234.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

كما أنه عندما تتعارض مصالح الدول فإن ذلك يمثل عقبة كبيرة تعترض سبل التعاون الدول، إذ تلجأ كل دولة إلى تغليب ما تفضيه مصالحها ولو تتعارض مع مصلحة دولة أخرى. وتتوقف قدرة الدول على التعاون الدولي في مسائل العدالة الجنائية وتنفيذ القوانين إلى حد ما على العلاقات السياسية القائمة بينها.¹

فتتطلب مكافحة الجريمة الالكترونية جهود مشتركة من الحكومات والقطاع الخاص والمجتمع الدولي لتطوير تشريعات فعالة وتعزيز الأمن الرقمي، وتوفير التدريب والتوعية للمستخدمين بشأن الأخطار والإجراءات الوقائية.²

الفرع الثاني: تنوع واختلاف الأنظمة القانونية والإجراءات.

بسبب تنوع النظم القانونية الإجرائية واختلافها، نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفعاليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى، أو ربما لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الالكترونية والتسليم المراقب والعمليات المستترة، وغيرها من الإجراءات.³

حيث أن الدول تختلف في مدى إمكانياتها وقدرة أجهزتها الأمنية والقضائية في التعامل مع الجرائم الالكترونية. حيث أن هناك بعض الدول لديها وحدات متخصصة في مجال هذه الجرائم بينما تفتقر دول أخرى إلى الكفاءات والخبرات اللازمة.

كما أن السلوك الإجرامي في الجريمة الالكترونية وخاصة في عالمية الشبكة يمر عبر عدة دول والذي يولد إشكالا في أي من القوانين تطبق نظرا للاختلاف بين تشريعات كل دولة، وعدم وجود اتفاقيات فيما بينها، فنجد دولة تأخذ بمبدأ إقليمية القوانين وأخرى بمبدأ شخصية القوانين في حين دولة أخرى تأخذ بمبدأ عينية القوانين.

¹ قاضي خولة، جباس منال، مرجع سابق، ص 52

² منال البلقاسي، تهديدات السيبرانية تحت المجهر الرقمي، الطبعة الأولى، المملكة العربية السعودية، الرياض، 2024، ص 99.

³ جمال محمد خلفان محمد النقبى، سلطان محمد سالم عوض هيسان المصعبي، التعاون الوطني والدولي في الجرائم الالكترونية المشكلات والحلول، مجلة المعهد العالي للدراسات النوعية، مجلد 3، عدد 16، يوليو 2023، ص 5500

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

الأمر الذي يثير تنازع القوانين فكل دولة ترى أن لها الأولوية في معاقبة الجاني.¹

الفرع الثالث: الصعوبة الخاصة بالإثبات القضائية

من الصعوبات التي تواجه التعاون الدولي في مكافحة الجرائم الالكترونية، ما يتعلق بالإثبات القضائية نجد إشكالية فكرة السيادة، إشكالية البطء في الإجراءات.

أولاً: فكرة السيادة: السيادة هي السلطة العليا التي لا تعلوها سلطة أخرى وهو ما يعني أن الدولة ذات سيادة هي التي تسن القوانين المطبقة فوق أراضيها وتتمتع بالاستقلال السياسي، والمساواة القانونية مع غيرها من الدول.²

فعندما يرتكب فرد جريمة ما من الجرائم المعلوماتية في إحدى الدول وتجرى محاكمته في دولة أخرى، فمن المنطق بل من الواجب البحث عن كافة أدلة ثبوت تلك الجريمة أو نفيها في البلد الذي وقعت فيه بحسبان أنها البلد التي كانت مسرحاً لتلك الجريمة وهذا ما يعرف بالتعاون القضائي بين الدول.³

رغم التعاون الذي بين الدول إلا أنه يكون صعباً لأنه كل دولة لها سيادتها الخاصة على أراضيها وعادة ما تفضل الدول حل القضايا القانونية بنفسها عبر نظامها القضائي دون تدخل خارجي في شؤونها، وذلك ارتباطاً بفكرة السيادة.

وبالتالي من غير المنطقي أن تطلب -مثلاً- محكمة جزائرية من دولة أخرى أجنبية أن تساعد في إجراءات التحقيق داخل أراضي تلك الدولة لأن المحكمة الجزائرية هي الجهة المسؤولة عن الفصل في القضية. وبالمثل لا يمكن لدولة أجنبية أن تطلب من الجزائر القيام بإجراءات قانونية داخل أراضيها لصالح محكمتها. وهذا يعود إلى مبدأ سيادة كل دولة على أراضيها والذي قد يشكل عائقاً أمام التعاون القضائي بين الدول في مكافحة الجرائم الالكترونية.

¹ ميرفت محمد حبابية، مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، اليازدي، 2022، ص 236.

² هارول لاسكي، محمد عفيفي، أسس السيادة، وكالة الصحافة العربية، 2021، ص 09.

³ عادل عبد العال، إبراهيم خراش، مرجع سابق، ص 243.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

ثانياً: إشكالية البطء في إجراءات الإنابة: كما نعلم أن طلبات الإنابة القضائية الدولية تسلم بطرق سلمية، وهذا يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الانترنت وما تتميز به من سرعة في التطور وهذا ينعكس على الجرائم الالكترونية.¹

كما هناك إشكالية التباطؤ في الرد وهذا بسبب قلة الخبرة المدرب أو نتيجة الصعوبة اللغوية أو الفوارق في الإجراءات.²

كما أنه لا يجوز في الإنابة القضائية أن يكون موضوعها اتخاذ إجراء من إجراءات التنفيذ كما لا يجوز أن تكون في اتخاذ إجراء ما لم يكن متعلق بحقوق الأفراد وكذا لا يجوز الفصل في الدعوى ولا تجوز أيضاً في اتخاذ إجراء يقع على عاتق الخصوم.³

المطلب الثالث: اقتراح بدائل في مجال مكافحة الجرائم الالكترونية

لقد تزايد انتشار الجرائم الالكترونية وذلك من خلال التطور الذي تشهده وسائل المعلوماتية وهنا ما أدى إلى إدراك خطورة هذه الجرائم ومدى سهولة ارتكابها وتأثيرها على المجتمع. وتهديدها للأمن بكافة مستوياته، وهذا ما جعل مكافحتها من أوليات المجتمع الدولي والحكومات.

¹ ميرفت محمد حبايبة، مرجع سابق، ص 309.

² المرجع السابق، ص 309.

³ بن الشيخ أمينة، النظام القانوني للإنابة القضائية الدولية، مذكرة ماستر أكاديمي، علاقات خاصة دولية، جامعة قاصدي مرياح ورقلة، كلية الحقوق والعلوم السياسية، 2015، ص 26.

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها

الفرع الأول: على المستوى الوطني.

أولاً: إصدار قوانين جديدة تجرم الجرائم الالكترونية في كافة أنحاء العالم بحيث يكون بينها قدراً كبيراً من التناسق: حيث اتجهت كافة الدول المتقدمة تكنولوجياً إلى استحداث نصوص قانونية جديدة تجرم الجرائم الالكترونية الجديدة على قوانينها التقليدية القديمة¹.

وضع قانون العقوبات للظواهر الإجرامية فيحدد الأفعال الجرمية ويضع العقوبات الرادعة لكل منها. وغايته إنزال العقاب بالمجرمين وحماية المجتمع من ضرورهم وردع غيرهم من الاقتداء بهم².

ثانياً: استخدام التحليل الجنائي الرقمي للتحقيق في أي جريمة تنطوي على استخدام الأجهزة الالكترونية: سواء تم استخدام هذه الأجهزة لارتكاب جريمة أو كهدف لها، يصبح امتلاك القدرة على التحاليل الجنائية الرقمية أمراً مهماً جداً³.

إضافة صفة الضبطية القضائية على العاملين في مجال المعلومات من غير رجال الشرطة، كمزودي الدخول وخدمات الانترنت فإنهم يقومون بالرقابة عبر المزود عن سير حركة العمل ومدى الخضوع للنظام من قبل العاملين والمتعاملين مع شبكة الانترنت⁴.

تطوير برامج حماية تساعد في الكشف عن المحتوى الضار والمواقع المشبوهة، تسهيل خدمة تقديم البلاغات والإجراءات القانونية للمتضررين.

الفرع الثاني: على الصعيد الولي.

التعاون الأمني من خلال جهود المنظمة الدولية للشرطة الجنائية الانترنت في مكافحة الجرائم الالكترونية، فمهمة الانترنت الأساسية تفعيل التعاون بين أجهزة الشرطة التابعة للدول

¹ جعفر حسن جاسم الطباطي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، دار البداية، عمان، ص 229.

² عماد الحسيان، عدنان الضمور، عز الدين التميمي. ياسر الخزاعلة مرجع سابق، ص 92.

³ المرجع نفسه، ص 96

⁴ عادل عبد العال، إبراهيم خراشي، مرجع سابق، ص 253 - 254

الفصل الثاني: الأهمية العملية في مكافحة الجرائم الإلكترونية والمعوقات التي تواجهها

الأعضاء في المنظمة بتوحيد إجراءات التسليم، ومن خلال تنسيق العمل الشرطي وتجميع البيانات وتبادل المعلومات لتيسير خدمات التحقيق.¹

تعاون الدول بعضها مع البعض من خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث تسليم مرتكبيها.²

كما أهاب مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين الذي عقد في هافانا في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي بالدول الأعضاء أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة استعمال الحاسب الآلي التي تستدعي تطبيق جزارات جنائية على الصعيد الوطني، بما في ذلك النظر إذا دعت الضرورة في:³

أ- تحديث الأنظمة والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضمان أن تكون الجزاءان بشأن سلطات التحقيق وقبول الأدلة على النحو الملائم.

ب- النص على جرائم وجزارات وإجراءات تتعلق بالتحقيق والأدلة، للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي.

ج- نشر ثقافة الانترنت في المجتمع أمر لا بد منه من أجل الحد أو التقليل من مخاطر تكنولوجيا المعلومات.

¹ جمال محمد خلفان محمد النقي، سلطان محمد سالم عوض هيسان المصعبي، مرجع سابق، ص 5512.

² عبد العال الديزي، مرجع سابق، ص 349.

³ مؤتمر الأمم المتحدة الحادي عشر، لمنع الجريمة والعدالة الجنائية بانكوك 10-25 نيسان أبريل 2005.

ملخص الفصل الثاني

يركّز الفصل الثاني من المذكرة على الجوانب التطبيقية في مواجهة الجرائم الإلكترونية، من خلال تحليل آليات التعاون الدولي التي تعتمد عليها الدول والمنظمات لمكافحة هذا النوع من الإجرام المتطور، خاصة في ظل طابعه العابر للحدود وصعوبة السيطرة عليه بالوسائل التقليدية.

ينطلق الفصل من التأكيد على أن الجهود الوطنية لا تكفي وحدها لمكافحة الجرائم الإلكترونية، مما يستدعي اعتماد تعاون دولي فعال على المستويين الأمني والقضائي. ويشمل ذلك تبادل المعلومات والخبرات، تنفيذ الإنابات القضائية، ونقل الإجراءات الجنائية بين الدول، بالإضافة إلى تعزيز قدرات أجهزة إنفاذ القانون.

كما يُبرز الفصل دور المنظمات الدولية المتخصصة، مثل الإنتربول، في تنسيق العمليات الأمنية ومتابعة الجناة عبر الدول، من خلال توفير قواعد بيانات مشتركة و فرق عمل متخصصة، بما يُسهم في تسريع الإجراءات وتجاوز الحواجز الجغرافية والقانونية.

في المقابل، يُناقش الفصل عددًا من التحديات والمعوقات التي تواجه هذا التعاون، من أبرزها:

- اختلاف الأنظمة القانونية بين الدول.
- تعقيد إجراءات الإثبات.
- ضعف البنية التحتية التقنية في بعض الدول.
- بطء التنسيق وتبادل المعلومات.

ويخلص الفصل إلى أن مكافحة الجرائم الإلكترونية تتطلب رؤية شاملة تقوم على التشريع الموحد، والتنسيق الأمني المستمر، وبناء القدرات البشرية والتقنية، لضمان فعالية الاستجابة القانونية في مواجهة هذه التهديدات المعاصرة.

الختمة

الخاتمة

تُعد الجرائم الإلكترونية أحد أبرز التحديات القانونية التي فرضتها الثورة الرقمية، نظرًا لسرعة تطورها، وتعقيد تقنياتها، واتساع نطاقها الجغرافي، حيث لا تعترف بحدود ولا سيادة، الأمر الذي يجعل من مكافحتها مسألة دولية تتطلب تضافر الجهود والتنسيق المستمر بين مختلف الأنظمة القانونية. وبناءً على ما سبق، فإن التعاون الدولي يُعتبر أحد المرتكزات الأساسية التي تقوم عليها سياسة مكافحة هذه الجرائم، إلا أن هذا التعاون، وعلى الرغم من أهميته، يواجه العديد من العراقيل التي تحد من فعاليته، سواء على المستوى الداخلي للدول أو في الإطار الدولي العام.

وقد هدفت هذه الدراسة إلى تسليط الضوء على الإطار القانوني المنظم للجريمة الإلكترونية، واستكشاف السبل الكفيلة بتفعيل التعاون الدولي في مواجهتها، مع بيان أبرز الصعوبات التي تقف عائقًا أمام هذا التعاون. ومن خلال ما تم عرضه وتحليله في فصول الدراسة، أمكننا الوصول إلى مجموعة من النتائج والتوصيات، نعرضها فيما يلي:

أولاً: النتائج

1. تُشكل الجرائم الإلكترونية خطرًا عالميًا حقيقيًا لا يهدد فقط الأفراد، بل يمتد ليطال المؤسسات الحيوية، ويقوض الأمن الاقتصادي والاجتماعي للدول، الأمر الذي دفع المجتمع الدولي إلى إدراجها ضمن الأولويات الأمنية والتشريعية.

2. يُعد التعاون الدولي أحد أهم المبادئ المستحدثة في القانون الدولي المعاصر، لا سيما في مجال مكافحة الإجرام العابر للحدود، وقد برزت أهميته بشكل خاص في التصدي للجرائم الإلكترونية، نظرًا لتعقيدها وتعدد أطرافها.

3. لم يتم التوصل إلى تعريف موحد وشامل لمفهوم التعاون الدولي في مجال الجرائم الإلكترونية، وذلك نظرًا لطبيعة هذا التعاون المتغيرة، واعتماده على متغيرات قانونية، تقنية، وسياسية متعددة، تختلف باختلاف الدول والأنظمة.

4. لا يمكن لأي دولة، مهما بلغت قدراتها، أن تتصدى بمفردها لظاهرة الجريمة الإلكترونية، وهو ما يفرض الانخراط الفعلي في آليات التعاون الدولي، سواء عبر الاتفاقيات الإقليمية أو عبر القنوات القضائية والأمنية الثنائية.

5. يُعتبر التنسيق الأمني بين أجهزة الشرطة المتخصصة في مكافحة الجرائم الإلكترونية وسيلة فعّالة للحد من انتشار هذه الجرائم، لا سيما من خلال تبادل المعلومات والتحقيقات الفنية، وتتبع مصادر الجريمة.

6. رغم أهمية التعاون الدولي، إلا أن هناك جملة من التحديات تعيق تنفيذه، من أبرزها:

- قصور التشريعات الوطنية عن مواكبة التطور التقني للجريمة الإلكترونية.
- التباين في الأنظمة القانونية الإجرائية.
- صعوبة الإثبات الرقمي والتقني.
- غياب الثقة المتبادلة بين بعض الدول، خاصة في مجال تبادل البيانات الحساسة.
- بطء إجراءات الإنابة القضائية، وعدم وجود آلية دولية ملزمة لتسريعها.

7. من أهم التحديات أيضًا، مشكلة تنازع الاختصاص القضائي الدولي، خصوصًا في حالات ارتكاب الجريمة في دولة، وامتداد آثارها إلى دول أخرى، مما يطرح إشكالية تحديد الجهة القضائية المختصة بالملاحقة والمحاكمة.

ثانيًا: التوصيات

استنادًا إلى ما تم التوصل إليه، ومن خلال قراءة نقدية للواقع القانوني الدولي، يمكن تقديم جملة من المقترحات العملية لتقوية آليات مكافحة الجرائم الإلكترونية، نوجزها فيما يلي:

1. على المستوى الوطني:

الخاتمة

- إدراج جميع صور الجرائم الإلكترونية ضمن التشريعات الجنائية الداخلية بشكل دقيق ومتكامل.
- منح الجهات الأمنية والقضائية صلاحيات كافية للتحقيق الفوري والفعال في الجرائم الإلكترونية.
- إشراك المختصين في مجال تكنولوجيا المعلومات ضمن فرق التحقيق، مع منحهم صفة قانونية تتيح لهم المساهمة الفعلية في الإثبات الرقمي.
- توسيع نطاق التعاون بين أجهزة الشرطة الوطنية والدولية، على أساس اتفاقيات واضحة المعالم والأهداف.

2. على المستوى الدولي:

- العمل على وضع تعريف قانوني موحد للجريمة الإلكترونية يتفق عليه في المعاهدات الدولية.
- توحيد العقوبات والإجراءات الجنائية الخاصة بالإجرام الإلكتروني، لتفادي التناقضات التي تعيق التعاون.
- إنشاء هيئة دولية خاصة بالتحقيقات السيبرانية، تكون لها صلاحيات عابرة للحدود، وتتسق بين الدول في حالات الجرائم الكبرى.
- تطوير الاتفاقيات الحالية، وتحويلها إلى أدوات تنفيذية فعالة، بدل أن تبقى مجرد نصوص غير مُفعّلة.
- تعزيز ثقة الدول في إطار التعاون، من خلال آليات لحماية البيانات السيادية وتبادل المعلومات بشكل آمن وسري.

3. فيما يتعلق بتسليم المجرمين:

- ضرورة توحيد المعايير الدولية لتحديد أولوية الطلبات في حالة تزامنها.

- اعتماد اتفاقيات تسليم مجرمين خاصة بالجرائم الإلكترونية، تتضمن إجراءات مبسطة وواضحة.

4. الإجراءات القضائية الدولية:

- اعتماد نظام اتصال مباشر وسريع بين الجهات القضائية المختصة لتجاوز بطة الإنابات.

- إضفاء الطابع الإلزامي على التعاون في مجال التحقيقات الجنائية الإلكترونية.

5. الاعتراف بالطابع الدولي للجريمة الإلكترونية:

- تصنيف الجرائم الإلكترونية ضمن الجرائم الدولية التي تخضع للاختصاص القضائي العالمي، ما يتيح ملاحقة مرتكبيها بغض النظر عن أماكن ارتكابهم للجريمة أو جنسيته.

ختامًا يبقى التصدي للجرائم الإلكترونية مسؤولية جماعية لا تقف عند حدود التشريع، بل تمتد لتشمل الإرادة السياسية، الجاهزية التقنية، والوعي المجتمعي. وإذا كانت هذه الدراسة قد حاولت الإحاطة بالجوانب القانونية والتعاونية لهذا الموضوع، فإن الطريق ما يزال مفتوحًا أمام دراسات أكثر عمقًا تتناول التحديات المستقبلية، بما يضمن تحقيق التوازن بين حماية الحريات الرقمية ومكافحة الجرائم المعلوماتية بفعالية واستدامة

قائمة المصادر

والمراجع

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولاً: المصادر

1. الاتفاقيات

- اتفاقية فيينا لقانون المعاهدات 1996.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

2. القوانين:

- القانون رقم 15/04 المؤرخ في 10 نوفمبر، يعدل ويتم الأمر 155/66 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 1، الصادر بتاريخ 2004/11/15.
- القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

ثانياً: المراجع

(1) الكتب

- البلقاسي محمد، تهديدات السيبرانية تحت المجهر الرقمي، الطبعة الأولى، المملكة العربية السعودية، الرياض، 2024.
- الحسان عماد، الضمور عماد، التميمي عماد الدين، الخزاعلة ياسر، الجرائم المستحدثة المعلوماتية، الالكترونية السيبرانية، الطبعة الأولى، دار الخليج للنشر والتوزيع، الأردن: عمان، 2024.
- الطائي جعفر حسن جاسم، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة ، عمان ، دار البداية، د س ن.
- العتوم محمد الشبلي، جرائم التكنولوجيا المعلومات النظرية العامة للجرائم الالكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2023.
- العمارات فارس، جرائم العصر من الرقمية إلى السيبرانية، الطبعة الأولى، دار الخليج للنشر والتوزيع، الاردن، 2023.

قائمة المصادر والمراجع

- الهاش ناجي محمد، صلاح حسن جاب مسعود، التعاون الأمني في دول حوض البحر الأبيض المتوسط ، التهديدات الأمنية ظل الصراعات الإقليمية والدولية ، د د ن، د ب ن، د س ن.
- أنبار سليمان، الشراكة الافروجزائرية في مجال الطاقة ومكافحة الإرهاب، الطبعة الأولى، دار المعتر للنشر والتوزيع، الجزائر 2024 - 1445 هـ .
- حبايبة ميرفت محمد، مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري العلمية للنشر والتوزيع، عمان، د س ن.
- حبايبة محمد مرفت، مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، اليازوري، 2022.
- خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2019.
- خراشي عادل عبد العال إبراهيم إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعية الجديدة، ط 01، الإسكندرية، 2015.
- خراشي عادل عبد العال إبراهيم، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، كلية الشريعة والقانون بالقاهرة، د س ن.
- سيد سلمان عبد الحكيم، الجرائم المعلوماتية وأثارها في ضوء قانون مكافحة جرائم تقنية المعلومات، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى، مصر، 2023.
- عبد العال محمد عكاشة، الإجراءات المدنية والتجارية وتنفيذ الأحكام الأجنبية، دار المطبوعات الجامعية، الإسكندرية، 2007.
- عبد الله لؤي نوح، مدى مشروعية المراقبة الالكترونية في الإثبات الجنائي وحجية مشروعية الدليل الالكتروني المستمد في التفتيش الجنائي وعوامل حجية الصورة والصوت في الإثبات الجنائي، الطبعة الأولى، مركز الدراسات العربية، مصر، 2018.
- علي السيد محمد، الجرائم الالكترونية، ماهيتها، صورها، اثباتها، مكافحتها، دار التعليم العالي، الإسكندرية، 2024.
- فكري أيمن عبد الله، الجرائد المعلوماتية ، دراسة مقارنة في التشريعات العربية والأجنبية، الطبعة الأولى . مكتبة القانون والاقتصاد ، 2014-1435.

قائمة المصادر والمراجع

- هارول لاسكي، محمد عفيفي، أسس السيادة، وكالة الصحافة العربية، 2021.
- ياكور الطاهر، الجرائم الالكترونية الأحكام الموضوعية والاجرائية، دراسة مقارنة، دار بلقيس، دار البيضاء، الجزائر، 2024.

(2) المجالات:

- ادريس خوجة نضيرة، دور التعاون الدولي في مجال تدريب رجال العدالة في مواجهة الجريمة الالكترونية، مجلة القانون الدولي والتنمية، المجلد 10، العدد 01، جامعة الجبالي ليايس، سيدي بلعباس، 2022.
- العموري رأفت حميد ريس، أثر الجريمة المعلوماتية وتأثيرها على المجتمع، مجلة المفكر للدراسات القانونية والسياسية، المجلد 04، العدد 04، العراق، 2022.
- النقيب جمال محمد خلفان محمد، هيسان المصعبي سلطان محمد سالم عوض، التعاون الوطني والدولي في الجرائم الالكترونية المشكلات والحلول، مجلة المعهد العالي للدراسات النوعية، مجلد 3، عدد 16، يوليو 2023.
- بركات رياض، مسيكة محمد الصغير، تسليم المجرمين كألية لتفعيل التعاون الدولي لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، المجلد 11، العدد 01، مخبر البحث في تطوير التشريعات الاقتصادية، جامعة تيسمسيلت، 2024.
- بغدادي إيمان، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الالكترونية، مجلة أفاق للبحوث والدراسات، العدد 04، المركز الجامعي، ايليزي، 2019.
- بن عودة صليحة، الجريمة الالكترونية وأثرها على مشروعية أعمال الإدارة القانونية، مجلة دفاتر الحقوق والعلوم السياسية، المجلد 03، العدد 1، المركز الجامعي معنية، 2023.
- جندلي وردة، التعاون الدولي لمكافحة الجريمة المعلوماتية الفاعلية والتحديات، مجلة القانون والعلوم السياسية، المجلد 10، العدد 02، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955، سكيكدة، 2024.

قائمة المصادر والمراجع

- داودي نعيمة، الجريمة الالكترونية (خصائصها، مجالات استخدامها، وأهم سبل مكافحتها)، مجلة مهد اللغات، المجلد 02، العدد 01، جامعة علي لونيبي، البلدية، 2020.
- رجدال أحمد، جهود منظمة الأمم المتحدة في سبيل مواجهة الجريمة الالكترونية، المجلة التقنية للقانون والعلوم السياسية، المجلد 19، العدد 02، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2024.
- رحموني محمد، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، جامعة دراية، أدرار، 2018.
- سليمان عيسى محمد أحمد، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، كلية العلوم والدراسات الإنسانية بلغاط، جامعة المجمعة، المملكة العربية السعودية، 2016.
- سيليني محمد الصغير، بن تغري موسى، قرارات منظمة الأمم المتحدة والمنظمات الدولية المتخصصة ودورها في مكافحة الجريمة المنظمة عبر الوطنية، مجلة صوت القانون، المجلد 09، العدد 02، كلية الحقوق والعلوم السياسية، جامعة يحي بن فارس، المدينة، 2023.
- غربي أسامة، المنظمة الدولية للشرطة الجنائية (الانتربول) ودورها في مكافحة الجريمة المنظمة، دراسات وأبحاث، المجلد 03، العدد 03، جامعة يحي بن فارس، المدينة، 2011.
- قطاف سليمان، بوقرين عبد الحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، مخبر البحث في الحقوق والعلوم السياسية، المجلد 06، العدد 01، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي، الاغواط، 2022.
- مرابط رميساء، مواجهة الجريمة الالكترونية ضمن مقتضيات تحقيق الأمن السيبراني، مجلة الحوكمة والقانون الاقتصادي، العدد 10، سنة 2010.
- معاشي سميرة، الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة الفكر، العدد 1، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2018.

قائمة المصادر والمراجع

- نهائلي رابح، قيرة سعاد، دور المنظمات الدولية في مكافحة الجريمة المنظمة (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجاً)، مجلة البحوث القانونية والاقتصادية، المجلد 04، العدد 02، جامعة غرداية، 2020.
- هدية أحمد محمد زعتر، الإشكاليات القانونية للجرائم الالكترونية العابرة للحدود وسبل مواجهتها، مجلة البحوث القانونية والاقتصادية، العدد 84، كلية إدارة الأعمال، قسم القانون، جامعة الجمعة، المملكة العربية السعودية، 2022.

(3) الرسائل العلمية

i. أطروحات الدكتوراه

- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01، بن يوسف بن خدة، 2018/2017.
- معاشي سميرة، آليات مكافحة الجريمة المعلوماتية دراسة مقارنة، أطروحة دكتوراه علوم في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة، 2020/2019.
- حبايبة ميرفت محمد، مكافحة الجريمة الالكترونية "دراسة مقارنة" في التشريع الجزائري والفلسطيني، أطروحة دكتوراه في الحقوق، تخصص القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة عمار ثليجي، الأغواط، 2022/2021.
- سلامي لخضر، الجريمة الالكترونية عبر مواقع التواصل الاجتماعي - الفيسبوك نموذجاً -، أطروحة دكتوراه في سوسيولوجيا الاجرام، كلية العلوم الاجتماعية، قسم علم الاجتماع والأنثروبولوجيا، جامعة وهران 02، 2023/2022.
- قنفود نبیة، السياسية الجنائية في مكافحة الجريمة الالكترونية في التشريع الجزائري، أطروحة دكتوراه ل م د، شعبة الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق، قسم القانون الخاص، جامعة قسنطينة 01، الاخوة منتوري، قسنطينة، 2024.

قائمة المصادر والمراجع

- خالد علي مزال الشعار، التحقيق الجنائي في الجرائم الالكترونية، بحث مقدم لاسيفاء متطلبات الحصول على درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة، د ب ن، د س ن.
- ii. رسائل الماجستير
- حسين محمد فلاح البرايسه، الركن المعنوي للجرائم الالكترونية وفقا لقانون العقوبات الأردني، رسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2021، ص 76.
- iii. مذكرات الماستر
- بن الشيخ أمينة، النظام القانوني للإنابة القضائية الدولية، مذكرة ماستر أكاديمي، علاقات خاصة دولية، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 2015.
- عمار، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، تخصص إدارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم علوم التسيير، جامعة قاصدي مرباح، ورقلة، 2018/2019.
- سليمان أبو نمره، يوسف بوكشريدة، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة ماستر، تخصص قانون دولي عام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة، 2020/2021.
- قاضي خولة، جباس منال، التعاون الدولي في مكافحة الجريمة المعلوماتية، مذكر الماستر في الحقوق تخصص قانون أعمال، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 2020/2021.

(4) المحاضرات

- خالد محمد نور، عبد الحميد الطباخ، التعاون الدولي في مكافحة الإرهاب، محاضر القانون الدولي بالجامعات المصرية، جامعة مدينة السادات، د س ن.

(5) المواقع الالكترونية

- محمد مدين، الجريمة الالكترونية وتحديات الأمن القومي، book. Google. dz

12h :004s 09.03.2025.

فهرس

المحتويات

فهرس المحتويات

Table des matières

.....	شكر وتقدير
.....	إهداء
.....	إهداء
أ.....	مقدمة
6.....	الفصل الأول: التأصيل القانوني للجرائم الالكترونية
7.....	المبحث الأول: مفهوم الجرائم الالكترونية
7.....	المطلب الأول: تعريف الجريمة الالكترونية
7.....	الفرع الأول: تعريف الجريمة الالكترونية
11.....	الفرع الثاني: تعريف الجريمة الالكترونية تشريعا
13.....	المطلب الثاني: خصائص الجريمة الإلكترونية
13.....	الفرع الأول: عابرة للحدود
13.....	الفرع الثاني: صعوبة اكتشافها وإثباتها
14.....	الفرع الثالث: سهولة ارتكابها
14.....	الفرع الرابع: أسلوب ارتكابها
15.....	المطلب الثالث: أركان الجريمة الالكترونية
15.....	الفرع الأول: الركن الشرعي
16.....	الفرع الثاني: الركن المادي
18.....	الفرع الثالث: الركن المعنوي

المبحث الثاني: النظام القانوني في التعاون الدولي ودور المجتمع في تفعيله	19.....
المطلب الأول: ماهية التعاون الدولي	19.....
الفرع الأول: تعريف التعاون الدولي	19.....
الفرع الثاني: مبررات لتعاون الدولي	20.....
المطلب الثاني: دور المنظمات في تفعيل التعاون الدولي لمكافحة الجريمة	21.....
الفرع الأول: المنظمة الدولية للشرطة الجنائية الانتربول	22.....
الفرع الثاني: دور الأمم المتحدة في مكافحة الجريمة	23.....
المطلب الثالث: دور المعاهدات والاتفاقيات الدولية في مكافحة الجرائم الالكترونية	24....
الفرع الأول: معاهدة بودابست لمكافحة جرائم الانترنت	24.....
الفرع الثاني: الاتفاقية العربية لمكافحة الجريمة الالكترونية	26.....
ملخص الفصل الأول	28.....
الفصل الثاني: الأهمية العملية في مكافحة الجرائم الالكترونية والمعوقات التي تواجهها	30
المبحث الأول: أوجه التعاون الدولي في مجال مكافحة الجرائم الالكترونية	31.....
المطلب الأول: التعاون القضائي	31.....
الفرع الأول: التعاون الأمني على المستوى الدولي	31.....
الفرع الثاني: المساعدة القضائية	34.....
المطلب الثاني: التعاون الدولي في مجال تدريب رجال العدالة في مواجهة الجريمة	37....
الفرع الأول: أهمية تدريب المكافحين للجرائم الالكترونية	37.....
الفرع الثاني: الآليات المعتمدة في مجال التعاون الدولي لتدريب رجال العدالة	38.....
المبحث الثاني: معوقات التعاون الدولي	39.....

المطلب الأول: معوقات على الصعيد الوطني	39
الفرع الأول: عدم كفاية وملائمة القوانين القائمة	39
الفرع الثاني: صعوبة إثبات الجرائم الالكترونية والتحقيق فيها	41
المطلب الثاني: معوقات على الصعيد الدولي	42
الفرع الأول: القصور التشريعي للدول والتعارض بين مصالحها	42
الفرع الثاني: تنوع واختلاف الأنظمة القانونية والإجراءات	43
الفرع الثالث: الصعوبة الخاصة بالإنبابة القضائية	44
المطلب الثالث: اقتراح بدائل في مجال مكافحة الجرائم الالكترونية	45
الفرع الأول: على المستوى الوطني	46
الفرع الثاني: على الصعيد الولي	46
ملخص الفصل الثاني	48
الخاتمة	50
قائمة المصادر والمراجع	55
فهرس المحتويات	62
الملخص	65

الملخص

شهدت الجريمة الإلكترونية نموًا مستمرًا لتصبح تحديًا عالميًا متزايدًا في ظل التقدم السريع للتكنولوجيا الرقمية، مما يشكل تهديدًا حقيقيًا لأمن المعلومات والأفراد والدول. وتؤكد هذه الدراسة أن مواجهة هذا النوع من الجرائم لا يمكن أن تعتمد على الجهود المحلية وحدها، بل تتطلب تعاونًا دوليًا فعالًا إلى جانب تنسيق قانوني وأمني مشترك.

وأشارت النتائج إلى أن الاتفاقيات الدولية والتشريعات الوطنية تحتاج باستمرار إلى التطوير والتحديث لمواكبة طبيعة هذه الجرائم المتطورة وأساليبها المتجددة لذلك، يُعدّ تعزيز التعاون الدولي، وتكامل الجهود، وتوفير التدريب اللازم والتجهيزات التقنية المتخصصة، هو النهج الأكثر فعالية للتعامل مع هذه المشكلة والحد من تداعياتها السلبية على المجتمع العالمي.

Summary:

Cybercrime has experienced continuous growth, becoming an increasingly global challenge amid the rapid advancement of digital technology. It poses a real threat to information security, individuals, and nations. This study confirms that combating such crimes cannot rely solely on local efforts but requires **effective international cooperation**, along with **coordinated legal and security measures**.

The findings indicate that **international conventions and national legislations constantly need to be updated and developed** to keep pace with the evolving nature and techniques of these crimes. Therefore, **enhancing international collaboration, integrating efforts, and providing the necessary training and specialized technical equipment** is the most effective approach to addressing this issue and minimizing its negative impact on the global community.