مجلة الحقوق والعلوم السياسية – جامعة خنشلة (RDSP)
2588-2309 : EISSN 2352-9806 : ISSN
المجلد : 11 – العدد : 01 – السنة : 2024 ص ص : 113 – 128

التعاون الدولي لمكافحة الجريمة الإلكترونية، الأشكال والإشكالات

International cooperation to combat cybercrime, forms and problems

مبروك فاطيمة *
مخبر الحقوق والعلوم السياسية
كلية الحقوق والعلوم السياسية
جامعة عمار ثليجي – الأغواط
f.mebrouk@lagh-univ.dz

ذيب محمد
مخبر الحقوق والعلوم السياسية
كلية الحقوق والعلوم السياسية
جامعة عمار ثليجي – الأغواط
Mohamedib80@gmail.com

تاريخ الإيداع: 15-11-2022 تاريخ القبول: 03-11-2023

ملخص:

نسعى من خلال هذه الدراسة إلى إبراز أهمية التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وذلك في إطار مختلف الجهود ذات الطالع الدولي والمتمثلة في الاتفاقيات والمنظمات الدولية والتي تعالج هذه الظاهرة بصفتها وسيلة قانونية مباشرة لتكاثف هذه الجهود، وأيضا في إطار مختلف أشكال هذا التعاون ومجالاته بين الدول لمنع هذه الجريمة ومجابهتها، كما نهدف من خلال هذه الدراسة إلى إبراز الإشكالات التي تعترض هذا التعاون الدولي، الأمر الذي يجعل من الصعوبة بما كانت تحقيقه على أرض الواقع، مع النظر في تذليل هذه الإشكالات وتجاوزها، وقد خلصنا في نهاية دراستنا إلى أن التعاون الدولي لمجابهة الجريمة الإلكترونية يفتقر إلى الاهتمام الدولي، وهذا ما يفسر قلة الاتفاقيات الدولية المختصة بمعالجة هذه الجريمة، مما يؤدي إلى نتيجة مفادها أن التعاون الدولي لمكافحة الجريمة الإلكترونية هو دون المستوى المطلوب، والذي يفرض على الدول إعادة النظر في جميع المعوقات التي هي سبب في عدم توحيد جهودها من أجل إعمال آليات التعاون الدولي لردع مرتكبي هذا النوع الخطير من الإجرام.

الكلمات المفتاحية: الجريمة الإلكترونية؛ التعاون الدولي؛ مكافحة؛الإشكالات

Abstract:

Through this study, we seek to highlight the importance of international cooperation in the field of combating cybercrime, Within the framework of various international efforts represented in international conventions and organizations that address this phenomenon as a direct legal means to intensify these efforts, And also within the framework of the various forms and fields of this cooperation between States to prevent and confront this crime, and we also aim through this study to highlight the problems facing this international cooperation, which makes it difficult to achieve it on the ground, while considering overcoming these problems and overcoming them, At the end of our study, we concluded that international cooperation to confront cybercrime lacks international attention, and this explains the lack of international conventions specialized in dealing with this crime, which leads to the conclusion that international cooperation to combat cybercrime is below the required level, which forces States to reconsider all obstacles that are the reason for not uniting their efforts to implement international cooperation mechanisms to deter perpetrators of this dangerous type of crime.

Keywords : cybercrime, international cooperation, combating, problems.

* مبروك فاطيمة.

مقدمة:

الجريمة الإلكترونية هي من أبرز الجرائم المستحدثة في عصر التقدم التكنولوجي والعلمي، وهي ظاهرة خطيرة تعولمت بفعل الرقمنة وتلاشي الحدود بين الدول والقارات، حيث تصنف من الجرائم العبر الوطنية، وموضوع الجريمة الإلكترونية هو محل اهتمام المجتمع الدولي ككل وبصفة عامة، وذلك نظرا لما تنطوي عليه هذه الظاهرة الإجرامية من خطورة، فكان لا بد على الدول أن تضافر جهودها من أجل إيجاد آليات مناسبة وفعالة للحد منها، وذلك بواسطة التعاون الدولي.

وإن البحث في التعاون الدولي لمكافحة الجريمة الإلكترونية يستند على أهمية كبيرة، حيث تتجلى هذه الأهمية أولا من الناحية الموضوعية، وثانيا من الناحية العملية، فتعتبر الجريمة الإلكترونية من أكبر وأخطر الجرائم التي تهدد بشكل مستمر أمن وسلامة المجتمعات بسبب تعقيداتها ودقتها اللامتناهية، كما يعتبر التعاون الدولي من أهم وسائل مكافحة هذه الجريمة فبذلت الدول والمنظمات الدولية جهودها في سبيل ذلك وفي شتى المجالات، وتزداد أهمية الجريمة الإلكترونية من خلال أهم معوقات التعاون الدولي لمكافحتها والتي لابد على المجتمع الدولي تجاوزها.

وبلك نهدف من خلال هذه الدراسة ليس فقط تبيان آليات التعاون الدولي لمكافحة الجريمة الإلكترونية، وما تعلق بها من إشكالات ومعوقات تحول بين هذا التعاون وبين تحقيق العدالة الجنائية من أجل مكافحة فعالة للجريمة الإلكترونية، وإنما أيضا لإعطاء الحلول المناسبة لتسهيل عملية التعاون الدولي وإزالة هذه الإشكالات.

والجريمة الإلكترونية هي من الجرائم الخفية التي تمتاز بالخطورة البالغة على الأفراد والدول على حد سواء ومختلف الأشخاص الاعتبارية، لدرجة أنها قد تهدد حتى مصالح الدول وأمنها الداخلي، وذلك راجع لطابعها الفني التقني وللاحتراف الكبير لمرتكبيها وحتى للقصور التشريعي في مجال نظم المعلومات، كل ذلك كان من متطلبات التعاون الدولي لمكافحة هذا النوع الخطير من الإجرام.

ومنه نطرح الإشكالية التالية:

ما مدى إعمال آلية التعاون الدولي لمكافحة الجريمة الإلكترونية؟

وتندرج تحت هذه الإشكالية عدة تساؤلات وهي:

- ما هي مجالات التعاون الدولي لمكافحة الجريمة الإلكترونية؟
- ما هي المعوقات التي تعترض تفعيل هذا التعاون الدولي لمكافحة الجريمة الإلكترونية؟

وللإجابة على هذه الإشكالية قسمنا الدراسة إلى مبحثين رئيسين، المبحث الأول بعنوان "التعاون الدولي لمكافحة الجريمة الإلكترونية،" أما المبحث الثاني بعنوان " إشكالات التعاون الدولي لمكافحة الجريمة الإلكترونية".

معتمدين في ذلك على المنهج الوصفي التحليلي من أجل البحث بشكل معمق ومكتمل في التعاون الدولي لمكافحة الجريمة الإلكترونية، والمتضمن تحديد أشكال هذا التعاون وتبيان إشكالياته، وما يمكن إستخلاصه من حلول لتذليل هذه الإشكالات.

المبحث الأول: التعاون الدولي لمكافحة الجريمة الإلكترونية

يعتبر التعاون الدولي آلية ضرورية لمكافحة الجرائم العابرة للحدود الوطنية بصفة عامة والجرائم الإلكترونية بصفة خاصة، نظرا لما تنطوي عليه هذه الجريمة المستحدثة من مميزات وخصائص يصعب معها على الدولة منفردة مكافحتها أو الحد منها ومن آثارها، وبمقتضى هذه الضرورة أصبحت الدول توحد جهودها وسياساتها من أجل الكشف عن مرتكبي هذه الجريمة الخطيرة وتوقيع الجزاء المناسب عليهم، حيث أن التعاون الدولي يتم بعدة أشكال وفي مجالات مختلفة، و سنحاول في هذا المبحث أن نبرز أشكال التعاون الدولي لمكافحة الجريمة الإلكترونية (مطلب أول)، وأيضا مجلات التعاون الدولي لمكافحة الجريمة الإلكترونية(مطلب ثان).

المطلب الأول: أشكال لتعاون الدولي لمكافحة الجريمة الإلكترونية

هناك الكثير من تصنيفات التعاون الدولي لمكافحة الجريمة الإلكترونية، لكن من خلال دراستنا هذه ميزنا بين شكلين أو نمطين لهذا التعاون، حيث يتمثل الشكل الأول في التعاون الدولي الإتفاقي (فرع أول)، أما الشكل الثاني فيكون بواسطة التعاون الدولي المؤسساتي(فرع ثان).

الفرع الأول: التعاون الدولي الإتفاقي

من أجل إيجاد الأساس القانوني للتعاون الدولي لمكافحة الجريمة الإلكترونية عقدت في سبيل ذلك مجموعة من الاتفاقيات الدولية العالمية منها والإقليمية، والتي اشتملت على مجموعة أنواع الجرائم الإلكترونية وطرق مكافحتها ومجابهتا على المستوى الدولي، ومن خلال هذا الفرع سنذكر أبرزها، أولا اتفاقية بودابست لعام 2001، ثانيا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

أولا: اتفاقية بودابست

بعد اقتناعها الكامل بالخطر القادم وقعت ثلاثون دولة أوروبية في 2001/11/23 على اتفاقية الجريمة الإلكترونية في بودابست من أجل مكافحة جرائم الإنترنت، وهي أولى الاتفاقيات التي تعاطت مع الطابع الدولي للجريمة الإلكترونية [1]، كما أنها الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم المرتكبة باستخدام أو ضد الكمبيوتر وباستخدام شبكة الإنترنت، وهي بمثابة ركيزة أساسية منذ أن دخلت حيز النفاذ في 2004/07/10، على مستوى الدول الأعضاء للاتحاد الأوروبي [2].ما يميز هذه الاتفاقية على الرغم من كومها إقليمية أنه يمكن للدول غير الأعضاء في الاتحاد الأوروبي الانضمام إليها[3].

---

[1] وسام الدين محمد العلكة، التعاون الدولي في مواجهة جرائم الإنترنت، مجلة آداب البصرة، العدد، 66، 2013، ص 371.

[2] خالد الشرقوني السموني، مكافحة الجريمة الإلكترونية على المستويين الوطني والدولي، المجلة المغربية للإدارة والتنمية، العدد 112، فيفيري 2012، ص 133.

[3] لوكال مريم، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي في ضوء قانون حماية المعطيات 18-07، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، 2019، ص 1307.

وقد جاءت هذه الاتفاقية بجوانب مهمة في الجريمة الإلكترونية الدولية، حيث تناولت التعاون الدولي وتسليم المجرمين والمساعدة المشتركة والتعاون الدولي فيما يتعلق بالتدابير الوقتية والتحفظية والتحقيقات وجمع بيانات حركة ومرور المعلومة الإلكترونية، التي من شأنها تنظيم عملية محاكمة المجرمين خارج إقليم الدولة[1].

ثانيا- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تهدف هذه الاتفاقية إلى تعزيز التعاون العربي لمكافحة الجريمة الإلكترونية، والتي تهدد أمن ومصالح وسلامة المجتمعات العربية، فأصبحت الحاجة ملحة إلى تبني سياسة عربية مشتركة لمكافحة هذه الجريمة[2] ، وقد تضمنت هذه الاتفاقية ضرورة التزام الدول الأطراف بتجريم مختلف أشكال الجرائم الإلكترونية الواردة في الاتفاقية بما يتوافق والنظم القانونية الداخلية للدول[3].

الفرع الثاني: التعاون الدولي المؤسساتي

لم تعد الاتفاقيات الدولية وحدها كافية لمجابهة الخطر الناجم أو المتوقع من الجرائم الإلكتروني، فسعت الدول لإنشاء مؤسسات وهياكل تكون مهمتها محاربة الإجرام المنظم العابر للحدود والذي يضم في أشكاله الجريمة الإلكترونية، وتعتبر المنظمة الدولية للشرطة الجنائية (الإنتربول) من أكبر الهياكل الدولية الرائدة في هذا المجال وهذا ما سنقوم أولا، إضافة إلى المنظمة العربية لمكافحة الجريمة المعلوماتية والتي هي منظمة متخصصة في الإجرام الإلكتروني، وهذا ما سنأتي على ذكره ثانيا.

أولا: المنظمة الدولية للشرطة الجنائية

من بين وظائف الإنتربول في مجال الجريمة الإلكترونية أنه يقوم بتعقب مجرمي المعلوماتية بصفة عامة وشبكة الإنترنت بصفة خاصة، وتتبع الأدلة الرقمية وضبطها وإجراء عمليات التفتيش العابرة للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال للبحث عن الأدلة والبراهين على ارتكاب الجريمة الإلكترونية التي تحتويها هذه الأنظمة المعلومات[4].

وفي مجال التعاون الدولي لمكافحة الجريمة الإلكترونية قد استحدث الإنتربول منصات لتبادل المعلومات مخصصة لأجهزة نفاذ القانون والدول الأعضاء وهي:

أ- **منصة تبادل المعارف المتصلة بالجريمة الإلكترونية:** تساهم هذه المنصة في إنشاء شبكة دولية تضم خبراء مختصين لتبادل المعرفة والخبرات في هذا المجال، حيث يمكن لأجهزة إنفاذ القانون والحكومات والمنظمات الدولية والخبراء من شركات الأمن السيبري المشاركة من أجل تبادل المعلومات الميدانية الغير شرطية والمتعلقة بالجريمة

---

[1] أيمن بن ناصر بن جماد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض ، 2015، ص 201.

[2] انظر ديباجة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1432/1/15 هـ الموافق 2010/12/21 م.

[3] انظر المادة 5 من الاتفاقية.

[4] شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية(دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2021/2020، ص 210.

الإلكترونية، فمن خلال هذه المنصة تناقش أحدث اتجاهات الجريمة الإلكترونية واستراتيجيات الوقاية منها وتقنيات الكشف عنها وأساليب التحقيق فيها.

ب- **منصة التعاون لمكافحة الجريمة الإلكترونية (العمليات)**: تنسق هذه المنصة عمليات أجهزة إنفاذ القانون على المستوى العالمي والتي ترمي إلى التصدي للجريمة الإلكترونية، فتشمل منتديات متعددة ومستقلة، تسمح للجهات الميدانية المعنية بتعميم المعلومات الاستخباراتية في إطار بيئة تفاعلية آمنة.كما تحسن هذه المنصة من كفاءة الدول الأعضاء وفعاليتها على المستوى الميداني وتمكنها من امتلاك رؤية للتهديدات والاتجاهات الإلكترونية بمجملها حتى تكون قادرة على تركيز مواردها بأفضل شكل مع تجنب ازدواجية الجهود[1].

ثانيا: المنظمة العربية لمكافحة الجريمة المعلوماتية

تم الاتفاق على إنشاء المنظمة العربية لمكافحة الجرائم المعلوماتية والإنترنت وهي منظمة عربية غير حكومية علمية ومهنية، ولها اهتمامات معينة ذات طابع قانوني واقتصادي، تعنى بتنظيم مختلف الأطر القانونية والإجرائية والمؤسسية لمكافحة الجرائم التي تتم عبر الإنترنت وكافة جرائم المعلومات، وتهدف هذه المنظمة إلى مكافحة الجرائم الإلكترونية بجميع أشكالها (الأجهزة والبرامج والشبكات والمعلومات والبيانات والأموال ووسائل الاتصال والجرائم ضد السمعة والجرائم ضد الشخصية) وأيضا تهتم بمكافحة الجرائم ضد الإنسانية وجميع أشكال الجرائم ضد الأمن القومي، وتسعى على العموم لمكافحة جميع الجرائم التي يكون أداة لارتكابها الحاسب أو الإنترنت أو يكونا أحد أهدافها[2].

المطلب الثاني: مجالات التعاون الدولي لمكافحة الجريمة الإلكترونية

تقوم الدول ببذل جهودها في مختلف المجالات من أجل تكريس فعلي للتعاون الدولي للحد من هذا النوع الخطير من الإجرام، وبهذا المعنى يشمل تكاثف الجهود الدولية لمجابهة الجريمة الإلكترونية بمختلف أنواعها التعاون الدولي القضائي الإجرائي (فرع أول)، إضافة تعاون في مجال خاص بالجريمة الإلكترونية نظرا لطبيعتها الفنية والتقنية وهو التعاون الدولي الفني (فرع ثان)، كما سنعرج على موقف المشرع الجزائري من التعاون الدولي لمكافحة الجريمة الإلكترونية(فرع ثالث).

الفرع الأول: التعاون الدولي القضائي والإجرائي

إن الطبيعة غير المادية للجريمة الإلكترونية تصعب من مهام أجهزة إنفاذ القانون متابعة وملاحقة مرتكبيها خاصة إذا كانت الجريمة الإلكترونية تعدت حدود الدولة الواحدة، ولا يمكن للدولة المتضررة أن تحصل على المعطيات والبيانات الإلكترونية الموجودة في نظام معالجة في كومبيوتر يتواجد بإقليم أو أقاليم دول أخرى، إلا يتعاون هذه الأخيرة، كما لا يمكنها الشروع أو مواصلة التحقيقات والإجراءات القضائية اللازمة في سبيل ملاحقة الجناة، والذين قد يهربون إلى دولة أخرى بعد ارتكابهم لجريمتم، أو يكونون متواجدين أصلا في إقليم دولة أخرى أثناء ارتكابهم لها، وأمام هذه المعضلات أتت الاتفاقيات الدولية من أجل تسيير الكشف عن الجريمة الإلكترونية ومعاقبة مرتكبيها، فقضت بضرورة تعاون الدول من أجل تبادل المعلومات بين الدول، وتبادل المساعدة، وتسليم المجرمين.

---

[1] انظر الموقع الإلكتروني: (https://www.interpol.int/ar/4/6/1)، تاريخ الاطلاع 2021/12/06.

[2] فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، رسالة دكتوراه، جامعة الجزائر 01- بن يوسف بن خدة- 2018/2017، ص 91.

أولا: تبادل المعلومات:

تعد الوقاية من خلال تبادل المعلومات عنصرا أساسيا، وقاعدة جوهرية لمكافحة الجريمة الإلكترونية وضمان إقامة نظام مواجهة فعال [1] ، وفي إطار قواعد اتفاقية بوادبست لمكافحة الجريمة المعلوماتية لعام 2001 يمكن للدول الأطراف أن ترسل معلومات لبعضها البعض دون طلب مسبق حيث أن الإفصاح عن هذه المعلومات من شأنه أن يساعد الطرف المتلقي في إجراءات التحقيق أو المتابعة القضائية ذات الصلة بالجرائم الإلكترونية المشمولة بهذه الاتفاقية [2]، كما يمكن للدولة الطرف أن تطلب من دولة طرف أخرى الحصول على بيانات معينة والكشف عنها مخزنة بواسطة نظام كومبيوتر داخل إقليمها، كما يجوز للدولة الطرف دون الحصول على موافقة الدولة الطرف الأخرى الحصول على المعلومات المخزنة في الكمبيوتر والتي تكون متاحة للعامة [3] .

ثانيا: المساعدة المتبادلة

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 على ضرورة تبادل الدول الأطراف المساعدة فيما بينها إلى أقصى حد ممكن في مجال الإجراءات المتعلقة بالتحقيق والكشف عن الجريمة المعلوماتية [4].

ومن جانبها أيضا تضمنت اتفاقية بودابست لعام 2001 في الفصل الثالث منها مجموعة من المبادئ العامة المتعلقة بالمساعدة المتبادلة حيث يجب على الدول أن توفر لبعضها البعض وعلى أوسع نطاق ممكن المساعدة المتبادلة لأغراض التحقيقات أو المتابعات القضائية للجرائم المشمولة بهذه الاتفاقية، كما تلتزم الدول بإصدار تشريعات داخلية وتدابير أخرى من أجل تنفيذ ما ورد في المواد من 27 إلى 35 من الاتفاقية [5] ، كما يمكن لكل دولة طرف أن تطلب المساعدة في المسائل العاجلة [6] .

ثالثا: تسليم المجرمين

عرفه المؤتمر الدولي العاشر لقانون العقوبات المنعقد بروما عام 1969 بأنه:" إجراء للتعاون القضائي بين الدول في المسائل الجنائية، والذي يرمي إلى نقل شخص يكون محلا للملاحقة الجنائية أو محكوما عليه جنائيا من نطاق السيادة القضائية لدولة إلى سيادة دولة أخرى" [7] .

ويجوز التسليم في الجرائم الإلكترونية وذلك بموجب الاتفاقيات الدولية حيث جاءت اتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 لتحث الدول على تسليم المجرمين الذين يرتكبون جرائم مشمولة بالاتفاقية، شريطة أن يكون التجريم مزدوجا للدولة الطالبة والدولة المطلوب منها التسليم [8]، وفي ذات السياق تناولت اتفاقية بودابست

---

[1] عبد الله جعفر كوفلي، العمل الأمني الناجح(دراسة نظرية-تحليلية)، دار الخليج للنشر والطباعة، عمان، 2019، ص 112.

[2] انظر الفقرة 1 من المادة 26 من اتفاقية بودبست لعام 2001.
اعتمدها مجلس أوروبا بتاريخ 2001/11/23.

[3] انظر المادتين 31، 32 من اتفاقية بودابست لعام 2001.

[4] انظر المادة الفقرة 1 من المادة 32 من الاتفاقية.

[5] انظر في ذلك الفقرتين 1، و2 من المادة 25 من الاتفاقية.

[6] انظر الفقرة 3 من ذات المادة.

[7] مجاهدي خديجة صافية، آليات التعاون الدولي لمكافحة الجريمة المنظمة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018ص 240.

[8] انظر الفقرتين 1، 2 من المادة 31 من الاتفاقية.

لعام 2001 التعاون الدولي في مجال تسليم المجرمين والذي ورد في الفصل الثاني في المادة 24 من هذه الاتفاقية حيث تناولت الأحكام والقواعد المتعلقة بالتسليم[1].

الفرع الثاني: التعاون الدولي الفني

لا يقتصر التعاون الدولي في مجال مكافحة الجريمة المعلوماتية على المساعدة القضائية المتبادلة فحسب، إذ أن المظهر الثاني لهذا التعاون هو التعاون الفني، حيث يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول، فالعناصر البشرية سواء على مستوى الأجهزة القضائية أو الأجهزة الأمنية ليست بذات الجاهزية والمستوى لمواجهة الجريمة الإلكترونية، وإنما تختلف هذه الجاهزية من دولة لأخرى بحسب تطور كل دولة. ولذلك دعت بنصوص صريحة جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة إلى وجوب التعاون الدولي في مجال التدريب ونقل الخبرات فيما بينها[2].

بينها[2]. كاتفاقية بودابست لعام 2001 حيث على الدول إنشاء هيئة تكون بمثابة نقطة اتصال على مدار الساعة واليوم والأسبوع ، وذلك من أجل ضمان المساعدة الفورية المتبادلة لغرض الإجراءات المتعلقة بالجرائم الإلكترونية من ذلك المشورة الفنية[3] ، وهذا ما تضمنته المادة 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

والتدريب من أكثر الوسائل فعالية، وذلك من خلال تكوين رجال القضاء والشرطة واكتسابهم الخبرة الفنية في مجال الجريمة الإلكترونية، على أن تراعي في هذه الخبرة المتدرب ومكونات عناصره الشخصية من حيث توافره على الصلاحية العلمية والقدرات الذهنية والنفسية من أجل تلقي التدريب بواسطة جلسات أو ورشات أو ندوات تدريبية حتى يستفيد كل الأفراد من تجارب وخبرات بعضهم البعض[4].

الفرع الثالث: موقف المشرع الجزائري من التعاون الدولي لمكافحة الجريمة الإلكترونية

تضمن القانون 09-04 الخاص بقواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على التعاون الدولي لمكافحة الجريمة الإلكترونية، حيث نص على المساعدة القضائية الدولية المتبادلة بشأن التحقيق في الجرائم المشمولة بهذا القانون وكشف مرتكبيها وجمع الأدلة الإلكترونية، وأيضا المساعدة المتعلقة بالمعلومات واتخاذ الإجراءات التحفظية.

ولما يميز الجريمة الإلكترونية من سرعة تستوجب استعجال الرد على طلبات المساعدات القضائية، فقد قضى المشرع الجزائري بالرد المستعجل على طلبات التعاون الواردة عبر البريد الإلكتروني أو الفاكس.

ومن خلال ذات القانون 09-04 أخضع المشرع الجزائري أيضا هذه المساعدة المتبادلة وفقا لشروط مبدأ المعاملة بالمثل وامتثالا لأحكام الاتفاقيات الدولية ذات الصلة[5]. كما أورد قيودا أخرى على الاستجابة لطلبات المساعدة

---

[1] انظر المادة 24 من الاتفاقية.

[2] مراد شاوش، الموقع الإلكتروني: https://www.droitetentreprise.com/، تاريخ النشر في الموقع 2018/05/22، تاريخ الاطلاع 2022/11/22..

[3] انظر البند(أ) الفقرة 1 من المادة 35 من الاتفاقية.

[4] ميرفت محمد جبايبة، مكافحة الجريمة الإلكترونية، دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري العلمية، ص 315.

[5] انظر المادتين 16 ، 17من القانون 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال..

القضائية ترتبط بالسيادة الوطنية والنظام العام، أو في حال ما إذا كانت الاستجابة مقيدة بشرط المحافظة على سرية المعلومات، أو عدم استعمال هذه المعلومات في غير ما هو موضح في الطلب[1].

أما بالنسبة للاختصاص القضائي في الجرائم الإلكترونية عندما يرتكبها أجنبيا فقد قضى المشرع الجزائري أن يكون للمحاكم الوطنية الجزائرية لما تستهدف هذه الجرائم مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني[2]، وهذا يتطلب تسليم مرتكبيها من الدول الأجنبية إلى الدولة الجزائرية، في حين قضى المشرع الجزائري في قانون الإجراءات الجزائية بعدم تسليم حاملي الجنسية الجزائرية والعبرة بوقت ارتكاب الجريمة[3]، بينما يجوز تسليم الأجانب، و الأجنبي هنا بالنسبة للدولة طالبة التسليم، مما يعني إما أن يكون حاملا للجنسية الجزائرية أو حاملا لجنسية دولة ثالثة، إذا كانت الجريمة الوارد بشأنها طلب التسليم من الجرائم التي يعاقب عليها القانون الجزائري[4].

ما يتضح لنا أن المشرع الجزائري استجاب لحتمية التعاون الدولي لمكافحة الجريمة، لكن كغيره من المشرعين ينظم هذا التعاون قواعد ومبادئ لها اعتبار في الأنظمة الوطنية ولا يمكن تجاوزها، مما يكون عائقا في إعمال قواعد التعاون الدولي، وهذا ما سنبحث فيه من خلال دراستنا في المبحث الآتي.

المبحث الثاني: معوقات التعاون الدولي لمكافحة الجريمة المعلوماتية

ذكرنا في مضى من دراستنا أهم أشكال التعاون الدولي لمكافحة الجريمة الإلكترونية ومجالاته، غير أن الواقع يثبت أن هذا التعاون يعترض تفعيله وتحقيقه عدة إشكالات، تحول بينه وبين الحد من الجريمة الإلكترونية العابرة للحدود الوطنية، مما يعوق تنفيذ أحكام ونصوص الاتفاقيات الدولية ذات الصلة، الأمر الذي يؤدي إلى إفلات المجرمين من العقاب وعدم تحقيق العدالة الجنائية، وتنقسم إشكالات التعاون الدولي لمكافحة الجريمة الإلكترونية إلى معوقات متعلقة بالأنظمة القانونية الداخلية للدول وبأشكال التعاون الدولي (مطلب أول)، والمعوقات متعلقة بالجريمة الإلكترونية ذاتها (مطلب ثان).

المطلب الأول: المعوقات المتعلقة بالأنظمة القانونية الداخلية للدول وبأشكال التعاون الدولي

رغم الضرورة الملحة للتعاون الدولي لمكافحة الجريمة الإلكترونية إلا أن السيادة المطلقة للدولة على إقليمها والتوجه الإيديولوجي لبعض الدول يؤدي حتما إلى الاختلاف في النظم القانونية الوطنية، فيختلف التجريم من دولة إلى أخرى ويتبع ذلك الاختلاف إجراءات التحقيق والمتابعة القضائية مما يؤدي إلى التنازع في الاختصاص القضائي بين الدول، إضافة إلى ذلك هناك معوقات ذات صلة مباشرة بالتعاون الدولي، ومما سبق سنقوم في هذا المطلب بتبيان المعوقات المتعلقة بالأنظمة القانونية الوطنية(فرع أول)، ومن ثم المعوقات المتعلقة بالتعاون الدولي في حد ذاتها (فرع ثان).

---

[1] انظر المادة 18 من نفس القانون.

[2] انظر المادة 15 من نفس القانون.

[3] انظر الفقرة الأولى من المادة 698 من قانون الإجراءات الجزائية الجزائري.

[4] انظر المادة 697 من نفس القانون.

الفرع الأول: معوقات الأنظمة الوطنية

يؤدي الاختلاف في النظم القانونية لمختلف الدول حتما إلى الاختلاف في مضامين النصوص القانونية خاصة في المجال الجنائي، ويرجع ذلك إلى الاختلاف في الفلسفة القانونية لكل دولة، فما قد يعتبر جريمة في نظام قانوني معين يعتبر مباح في نظام قانوني غيره، وما قد يسمح به قانون في دولة ما بإجراء معين للتحقيق أو المقاضاة يكون في نظر قانون آخر غير مشروع كالمراقبة الإلكترونية مثلا، وما يهمنا في هذا الفرع هو نتائج الاختلاف في النظم القانونية الداخلية للدول والتي تؤدي إلى عرقلة التعاون الدولي لمكافحة هذه الجريمة،ومن هنا قمنا بذكر أهم هذه النتائج والمعوقات، والمتمثلة أولا في عدم وجود نموذج تجريمي موحد بين الدول، وثانيا إشكالية ازدواجية التجريم، ثالثا إشكالية الاختصاص القضائي، ورابعا الاختلاف في النظم الإجرائية.

أولا: عدم وجود نموذج تجريمي موحد

بإلقاء نظرة متأنية للأنظمة القانونية الداخلية للعديد من الدول لمواجهة الجرائم الإلكترونية بما في ذلك تلك المتعلقة بشبكة الإنترنت يتبين لنا أنه لا يوجد اتفاق عام مشترك بين الدول حول أشكال إساءة استخدام نظم المعلومات وشبكة الإنترنت التي يجب تجريمها، فما يجوز في نظام ما قد يكون فعلا إجراميا وغير مسموح به في نظام آخر[1]، ونظرا لاختلاف مفاهيم الجرائم المعلوماتية بسبب اختلاف التقاليد والأعراف القانونية الدولية فإن ذلك يضعف نظام القانون الدولي في السيطرة على تلك الجرائم، مما يجعل الإفلات من المساءلة الجنائية سهلا بالنسبة للجناة[2].

ثانيا: اختلاف النظم القانونية الاجرائية

بسبب تنوع الأنظمة القانونية الإجرائية واختلافها نجد أن أساليب التحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما قد تكون لا فائدة منها في دولة أخرى، أو قد لا يسمح بإجرائها كما هو الحال مع المراقبة الإلكترونية[3].

ثالثا: إشكالية الاختصاص القضائي

في أغلب الأحيان تتم الجرائم الإلكترونية من خلال أفعال ترتكبها أشخاص من خارج الحدود كما يتم تنفيذها عبر شبكات وأنظمة معلومات خارج الحدود أيضا، مما يثير التساؤل حول الاختصاص القضائي بهذه الجرائم بالإضافة إلى حقيقة امتداد أنشطة الملاحقة والضبط والتحري والتفتيش خارج الحدود الوطنية أمر يتطلب تعاونا دوليا شاملا يهدف إلى تحقيق مكافحة مثل هذه الجرائم وذلك مع احترام السيادة الوطنية للدول المعنية[4].

رابعا: إشكالية إزدواجية التجريم

على الرغم من أهمية شرط إزدواجية التجريم إلا أنه غالبا ما يكون عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم الإلكترونية، خاصة وأن بعض الدول لا تتضمن نظمها القانونية تجريما لهذه الجرائم، إضافة إلى صعوبة تحديد ما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم بالإمكان تطبيقها على الجرائم

---

(1) محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، 2016، ص 60.

(2) يوسف صغير، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، 2013، ص 133.

(3) عادل عبد العال، إبراهيم الخراشي، مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة للنشر، 2015، ص 237.

(4) عبد العال الدربي، محمد صادق اسماعيل، الجرائم الإلكترونية، دراسة قضائية قانونية مقارنة مع أحدث التشريعات العربية في مجال مكافحة الجريمة المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، 2012، ص 155.

الإلكترونية أم لا، علاوة على ذلك قد تتوسع الدول في تفسير شرط ازدواج التجريم، مما يعيق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، وبالتالي يمنع جمع الأدلة وملاحقة مرتكبي الجرائم الإلكترونية ومحاكمتهم [1].

الفرع الثاني: إشكالية عدم وجود تعاون دولي

من أهم معوقات مكافحة الجريمة الإلكترونية هو عدم تكريس التعاون الدولي فعليا في هذا المجال، وهناك مسببات عديدة لذلك، وفي إطار دراستنا هذه نذكر أبرزها والمتمثلة أولا في عدم وجود اتفاقيات ومعاهدات ثنائية وجماعية تختص بشكل مباشر في التعاون الدولي لمكافحة الجريمة الإلكترونية، وثانيا صعوبة التعاون الدولي في المسائل الإجرائية والقضائية.

أولا: عدم وجود معاهدات ثنائية أو جماعية:

عدم وجود معاهدات دولية كافية [2] على نحو يسمح بالتعاون المثمر في مجال الجرائم الإلكترونية [3] ، أو عدم كفايتها إن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر وسرعة التحريات فيها [4]، فحتى في حالة وجودها فإن هذه المعاهدات قاصرة على تحقيق الحماية المطلوبة في ظل التطور السريع لنظم المعلومات وشبكة الإنترنت [5] ولا تسمح بالمعونة الثنائية أو الجماعية بين الدول [6].

ثانيا: صعوبة التعاون الدولي في المسائل القضائية والإجرائية

من الصعوبات التي يتلقاها التعاون الدولي في المسائل القضائية هي أن إجراءات المساعدة القضائية المتبادلة تتميز بالبطء والتعقيد [7] ، ومثال ذلك الإنابة القضائية الدولية والتي هي من أهم صور المساعدة القضائية، وهي تتم بواسطة الطرق الدبلوماسية، الأمر الذي يجعلها تتسم بالبطء والتعقيد والذي يتعارض مع الطبيعة المتطورة بشكل سريع للجرائم الإلكترونية، وهذا راجع إلى عدة أسباب كقلة خبرة المدرب أو الصعوبات اللغوية أو الاختلاف في الإجراءات، الأمر الذي جعل العديد من قضايا الجرائم الإلكترونية تشطب نظرا لعدم تلبية طلب المساعدة في الآجال المحددة قانونيا [8].

ويعتبر التعاون الدولي في المسائل الإجرائية هو من أهم القضايا في مكافحة الجرائم الإلكترونية، لاسيما وأن طبيعة هذه الجرائم وسرعة ارتكابها أو سهولة إخفاء أدلتها، يتطلب تكييف الإجراءات التقليدية المتبعة من طرف الأنظمة القانونية الوطنية في مجالات التحقيق والمحاكمة بما يتماشى مع تلك الطبيعة والسرعة.

---

[1] ميرفت محمد حبابية ، مرجع سابق، ص 313.

[2] عبد العال الدريبي، محمد صادق اسماعيل، مرجع سابق، ص 342.

[3] فادية محمد جاسم، التعاون الدول للحد من الجريمة المعلوماتية، المجلد 29، العدد 4، 2019، ص 375.

[4] عبد العال الدريبي، محمد صادق اسماعيل، مرجع سابق، ص 342.

[5] فادية محمد جاسم، مرجع سابق، ص 375.

[6] عبد العال الدريبي، محمد صادق اسماعيل، مرجع سابق، ص 342.

[7] برقوق يوسف، المساعدة القضائية المتبادلة لمواجهة الجرائم الإلكترونية، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 01، العد 01، 2021، ص100.

[8] ميرفت محمد حبابية ، مرجع سابق، ص 309.

ففي معظم الأحيان تختلف طرق وإجراءات التحري والتحقيق في دولة ما عن تلك الموجودة في دولة أخرى، وهذه الإجراءات حتى وإن أثبتت فعاليتها في دولة ما قد لا تكون قانونية أصلا في دولة أخرى مثل ما هو الحال بالنسبة للمراقبة الإلكترونية [1].

كما أنه من الناحية القانونية فإن انعدام وجود الأساس القانوني الذي يرخص لمأموري الضبط القضائي والإداري الحق في جمع الأدلة من دولة إلى دولة أخرى في ظل غياب وجود اتفاقيات دولية أو في حال ما إذا تعنت الدولة التي على إقليمها المجرم المعلوماتي، مما يزيد الوضع تعقيدا بالنسبة لجهات التحقيق بالنسبة لجريمة إلكترونية امتد أثرها خارج الإقليم الوطني فمسألة تعقبها والدخول إليها من أجل جمعها ونقلها إلى الدولة التي يجري فيها التحقيق تثير إشكالات تتعلق بسيادة الدولة والولاية القضائية [2].

المطلب الثاني: المعوقات المتعلقة بالجريمة الإلكترونية

الجريمة الإلكترونية هي جريمة مستحدثة، فهي نتاج مباشر للتطور التقني والتكنولوجي المستمر في العام، يرتكبها أشخاص في غاية الاحتراف والذكاء، وهي جريمة ذات طبيعة فنية تقنية، يكون محلها دائما العالم الافتراضي تمتد آثارها إلى الواقع المادي، وهي من الجرائم الأكثر تعقيدا وخطورة في العصر الحالي، كل هذه الأمور وغيرها جعلت من مهام أجهزة إنفاذ القانون بمختلف الدول جد صعبة من أجل كشفها وتقديم مرتكبيها للعدالة، فالجريمة الإلكترونية تمتاز بخصائص منفردة عن غيرها من الجرائم الأخرى التقليدية، والتي تمثل عائقا واضحا في مجال التعاون الدولي لمكافحة هذه الجريمة، ومن الخصائص نذكر البعد الدولي للجريمة الإلكترونية وصعوبة الحصول على الدليل الإلكتروني، (فرع أول)، إضافة إلى مختلف الخصائص الأخرى للجريمة الإلكترونية (فرع ثان).

الفرع الأول: البعد الدولي للجريمة الإلكترونية وصعوبة الحصول على الدليل الإلكتروني

تعتبر الجرائم الإلكترونية من الجرائم العابرة للحدود الوطنية وهذا ما يزيد من صعوبة القيام بمواصلة التحقيق في إقليم دولة أخرى إذا لزم الأمر مما يؤدي إلى صعوبة الحصول الدليل الإلكتروني الذي هو في حقيقة الأمر من أهم ما يميز الجريمة الإلكترونية سواء أكان هذا الدليل الإلكتروني داخل حدود إقليم الدولة أم خارجه، ومن خلال هذا الفرع سنتطرق أولا إلى الخاصية العبر الوطنية للجريمة الإلكترونية، وثانيا إلى الصعوبة الكامنة في الحصول على الدليل الإلكتروني.

أولا: الجريمة الإلكترونية جريمة عبروطنية

أهم ما تتميز به الجريمة المعلوماتية أنها تتجاوز الحدود الجغرافية وتكتسب صفة دولية من خلال قدرة أجهزة الكمبيوتر على نقل وتبادل المعلومات بين أنظمة تفصل بينها آلاف الأميال بسرعة هائلة [3] ، و أدى هذا التباعد إلى تشتت الجهود في مواجهة الجريمة الإلكترونية، فعلى سبيل المثال وجود الجاني في بلد والضحية في بلد آخر جعل مواجهة

---

[1] عبد الحليم بن بادة، مرجع سابق، ص 94.

[2] إبراهيم محمد، بن حمود الزنداني، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات وأحكامها في القانون اليمني والكويتي والقطري: دراسة شرعية وقانونية مقارنة، جامعة قطامي، 2019، ص 64.

[3] محمد علي سكسكر، الجريمة المعلوماتية وكيفية التصدي لها، كتاب الجمهورية، 2010، ص 42.

هذا النوع من الإجرام أمرا صعبا، وذلك لتباين الإجراءات الجنائية واختلافها أو التنازع حول القانون الواجب التطبيق [1].

ثانيا: صعوبة الحصول على الدليل الإلكتروني

تواجه سلطات التحقيق مشكلة تتعلق بمدى إمكانية تمديد إجراءات التفتيش إلى خارج إقليم الدولة التي أصدرت سلطاتها المختصة الإذن بالتفتيش والدخول في المنطقة الجغرافية لدولة أخرى. وقد اجتمع الفقه الجنائي على عدم جواز التفتيش الإلكتروني العابر للحدود في حالة غياب اتفاقية بين دولتين تسمح ذلك، أو على الأقل الحصول على إذن من الدولة الأخرى، وهذا ما يؤكد أهمية التعاون الدولي لمكافحة الجرائم الإلكترونية.

وقد أجازت المادة 32 من بودابست لمكافحة الجرائم المعلوماتية لعام 2001 [2] إمكانية الدخول في أجهزة أو شبكات تابعة لدولة أخرى دون إذنها لغرض التفتيش والضبط وذلك في الحالتين التاليتين: -كما سبق ذكره- إذا كانت المعلومات أو بيانات متعلقة بالعامة، أو إذا رضي مالك أو حائز هذه البيانات بالتفتيش [3].

الفرع الثاني: صعوبات أخرى تتعلق بالجريمة الإلكترونية

يعترض التعاون الدولي لمكافحة الجريمة الإلكترونية ليس فقط ما تم ذكره في الفرع السابق، وإنما هناك إشكالات أخرى متعددة ومختلفة لها صلة مباشرة بالجريمة الإلكترونية، ومن خلال هذه الجزئية سنذكر أولا صعوبة متابعة وإثبات الجرائم الإلكترونية، والصعوبة الثانية والمتمثلة في طبيعة محل الجرائم الإلكترونية وذاك ثانيا.

أولا: صعوبة متابعة و إثبات الجر ائم الإلكتروني

ما يميز الجرائم الإلكترونية عن الجرائم التقليدية صعوبة إثباتها، ويرجع ذلك إلى عدم وجود الآثار التقليدية للجريمة، وغياب الدليل المادي (بصمات، تخريب،شواهد مادية) مع سهولة محو وإتلاف الأدلة في زمن قصير جدا، وبالتالي يصعب الكشف عن الجرائم الإلكترونية ومتابعتها وإقامة الدليل عليها، فهي جرائم غامضة، وعولمتها أدت إلى تشتيت الجهود في مجال التحري والتنسيق الدولي لتتبع مثل هذه الجرائم،فهذه الجرائم هي شكل حقيقي من أشكال العولمة [4].

و الإجرام الإلكتروني هو إجرام من نوع خاص يتسم بالتطور المستمر فعجز التشريع عن شمول جميع أشكاله [5]، ففي بعض الحالات اتضح أن هناك أفعالا جديدة ترتبط باستخدام الكمبيوتر لا تكفي النصوص القائمة لمكافحتها [6]، ولكن هذا لا يمنع توسيع مجال التجريم والعقاب في حقل الإجرام الإلكترون[(7)]،

ثانيا: طبيعة محل الجر ائم الإلكترونية

---

[1] معاشي سميرة، ما هي الجريمة المعلوماتية، مجلة المنتدى القانوني، جامعة بسكرة، المجلد، العدد، 2010، ص 281.

[2] عبد الحليم بن بادة، إجراءات البحث والتحري عن الجريمة المعلوماتية، الخصوصية والإشكالات، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، المجلد 23، العدد ، 2015، ص 94.

[3] خالد حسن، أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2019، ص 117.

[4] صباح كزيز، أثر الجرائم الإلكترونية على أمن واستقرار الدول ، قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجا، مجلة الناقد للدراسات السياسية، العدد الثالث، اكتوبر 2018، ص 123.

[5] عبد الفتاح الطاهري، الجريمة المعلوماتية بين ثبات النص وتطور الجريمة، مجلة القانون والأعمال، جامعة الحسن الأول - كلية العلوم القانونية والاقتصادية والاجتماعية - مختبر البحث، قانون الأعمال، العدد 41، فيفري 2019، ص 45.

[6] صغير يوسف، مرجع سابق، ص 60.

[7] عبد الفتاح الطاهري، مرجع سابق، ص 45.

يتمثل موضوع ومحل الجريمة الإلكترونية في المعطيات و المصلحة المنتهكة والحق المعتدى عليه، وهو الحق في المعلومات بذاتها، وبما تمثله هذه المعلومات من أموال أو أصول أو أسرار أو بيانات شخصية، أولها قيمة بذاتها كالبرمجيات فالمعلومات الالكترونية جديرة بالحماية حتى عن المعلومات في المحتوى الورقي، فتظهر ميزة الحماية الجنائية للمعلومات المبرمجة آليا عن غيرها من المعلومات الموجودة في الملفات الورقية من ضعف النوع الأول من المعلومات ومن أهميته في الوقت نفسه، فالمعلومات المعالجة آليا في النظام الإلكتروني تكون ضعيفة داخله عن تلك الموجودة في الملفات الورقية فيمكن إخفاء هذه الأخيرة بسهولة عن المعلومات داخل النظام ،كما أن المعلومات التي يتم معالجتها آليا هي متنوعة وذات سعة كبيرة، ومنها ما له صلة بالحياة الخاصة للأفراد، كل ذلك دفع بمشرعي الكثير من البلدان إلى استحداث أشكال من التجريم من أجل حماية المعلومات داخل الكمبيوتر من الوصول إليها[1]

خاتمة

إن التعاون الدولي لمكافحة الجريمة الإلكترونية هو من متطلبات عصر الرقمنة والعولمة والأمنين الوطني والدولي، خاصة إذا كان هذا التعاون من أجل الحفاظ على أمن الأفراد والجماعات وممتلكاتهم، وذلك يقتضي أن تُبذَل مختلف الجهود الدولية لمكافحة الجريمة الإلكترونية، فالتعاون الدولي هو أهم آلية من آليات مكافحة الجرائم العابرة للحدود الوطنية عامة والجريمة الإلكترونية خاصة، كون هذه الآلية وسيلة فعالة لمنع هذه الجريمة الخطيرة والحد من آثارها، وتحقيق العدالة الجنائية وتكريس حق الدولة في العقاب، لكن بين متطلبات التعاون الدولي لمكافحة الجريمة الإلكترونية ونتائجه هناك معوقات غالبا ما تجعل من هذا التعاون أمرا يصعب تحقيقه، وهذا يسوقنا للحديث في خاتمة هذه الدراسة إلى النتائج التي توصلنا إليها، ثم إلى ما نراه مناسبا من توصيات، والتي منها ما تتعلق بالتعاون الدولي لمكافحة الجريمة الإلكترونية، ومنها ما تتعلق بالجريمة الإلكترونية.

أولا: النتائج

- يعتمد التعاون الدولي لمكافحة الجريمة الإلكترونية على عدة آليات تتمثل في الاتفاقيات الدولية وفي الهيئات الدولية، كما تتنوع مجالات هذا التعاون بين المجال الإجرائي والمجال القضائي، كما يلعب التعاون الدولي لمكافحة الجريمة الإلكترونية دورا مهما في الحد من هذه الظاهرة الإجرامية الخطيرة التي عبرت الحدود الوطنية

- إن تحقيق تعاون دولي من أجل مكافحة فعلية للجريمة الإلكترونية هو أمر في غاية الصعوبة، وذلك راجع إلى مجموعة من العراقيل أهمها عدم وجود إرادة دولية واضحة للحد من هذه الجريمة.

- إن انعدام النتيجة السابقة والمتمثلة في عدم رغبة الدول بشكل فعلي في مكافحة الجريمة الإلكترونية، يؤدي إلى رفض هذه الأخيرة إلى توحيد أنظمتها القانونية المتعلقة بمكافحة الجريمة الإلكترونية.

[1] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبي بكر بلقايد، تلمسان، 2018/2017، ص 99.

- لا يزال التعاون الدولي لمكافحة الجريمة العابرة للحدود الوطنية منها الجريمة الإلكترونية يخضع لعدة اعتبارات وأولها السيادة الوطنية، ومبدأ المعاملة بالمثل، حيث لا يزال كلا المبدأين قائم على إطلاقه، وهذا ما نجده في النصوص القانونية الجزائرية وحتى في الاتفاقيات الدولية.

- هناك نقص كبير وواضح في الاتفاقيات الدولية التي تعالج الجريمة الإلكترونية، وهذا يؤدي إلى قلة أو انعدام سبل التعاون الدولي الجماعي أو الثنائي في هذا المجال.

- يؤدي التفاوت والتباين في الأنظمة العقابية للدول والذي يتضمن شروط طلبات المساعدة القضائية إلى عرقلة الاستجابة لهذه الأخيرة، كشرط التجريم المزدوج، مما يؤدي إلى إفلات مرتكبي هذه الجريمة من العقاب.

- الجريمة الإلكترونية في تطور مستمر ، لكن التعاون الدولي لمكافحة هذه الجريمة لا يزال يتسم بالبطء والتعقيد، فالرد على طلبات المساعدة يجب أن يكون بقدر من السرعة بما يمكن الدولة الطالبة للمساعدة القضائية أن تستكمل إجراءات التحقيق والمتابعة القضائية على أكمل وجه.

ثانيا: التوصيات

- من الضرورة أن تكون هناك إرادة دولية فعلية لمكافحة الجريمة الإلكترونية حتى يتحقق معها تفعيل التعاون الدولي لمكافحة هذه الجريمة. فيتعين عقد أكبر عدد من الاتفاقيات الدولية الإقليمية والثنائية تدرج في نصوصها أحكاما ملزمة لأطرافها تبين وسائل وآليات التعاون الدولي لمكافحة الجريمة الإلكترونية.

- إن عقد اتفاقيات دولية ولو كانت من طرف منظمة الأمم المتحدة لا يكفي إنما يجب على الدول الأطراف فيها أن تلتزم بنصوصها. فمن شأن ذلك أن يجعل من التعاون الدولي وسيلة فعالة لمكافحة الجريمة الإلكترونية.

- على الدول توحيد أنظمتها القانونية المتعلقة بمكافحة الجريمة الإلكترونية خاصة ما يتعلق منها بالتجريم وإجراءات التحقيق والإجراءات القضائية مما يسهل تتبع مرتكبي الجريمة الإلكترونية خارج حدود إقليم الدولة.

- ضرورة تكثيف التعاون الدولي الفني لمكافحة الجريمة الإلكترونية في مجال التدريب بالنسبة لأجهزة إنفاذ القانون وذلك من أجل مسايرتها للتطورات المستمرة للجريمة الإلكترونية، ومن أجل تسهيل عمليات التحقيق والحصول على الدليل الإلكتروني، و سهولة القبض على مجرمي العالم الافتراضي وتقديمهم للعدالة.

- على الأنظمة القانونية الوطنية مسايرة التطور السريع والمستمر في أساليب ارتكاب الجرائم الإلكترونية وفي أنماطها، فالجمود التشريعي في بعض الأنظمة أو تأخره إما أن يؤدي إلى رفض طلبات المساعدة القضائية مباشرة، أو يجعل قبولها قائما على شروط،

- على الرغم من مبدأ السيادة ومبدأ المعاملة بالمثل هما من أهم مبادئ القانون الدولي فإن الحاجة كثيرا ما تستوجب على الدول أن نعيد النظر في هذه المبادئ، فالأمن الوطني في عالم اليوم يقتضي ألا تندرج بعض الأمور ضمن سيادة الدولة، وألا تكون المعاملة متماثلة. كتبادل المعلومات أو تقديم الأدلة التي من شأنها أن تجنب دولة ما فضائع الجرائم الإلكترونية، خاصة وأن أغلب الجرائم العابرة للحدود أصبحت ترتكب في هذا الزمن إلكترونيا.

قائمة المصادرو المراجع

أولا: المصادر

أ- الاتفاقيات الدولية

1- اتفاقية بوادبست لعام 2001،اعتمدها مجلس أوروبا يتاريخ 2001./11/23

2- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1432/1/15 هأ الموافق 2010/12/21 م.

ب- القوانين والأنظمة الوطنية:

1- القانون 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

2- قانون الإجراءات الجزائية الجزائري.

ثانيا: المراجع

أ- الكتب:

1- أيمن بن ناصر بن جماد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض ، .2015

2- عبد الله جعفر كوفلي، العمل الأمني الناجح(دراسة نظرية-تحليلية)، دار الخليج للنشر والطباعة، عمان، .2019

3- ميرفت محمد جبايبة، مكافحة الجريمة الإلكترونية، دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري العلمية، دون سنة طبع.

4- عادل عبد العال، إبراهيم الخراشي، مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة للنشر، 2015.

5- عبد العال الدريبي، محمد صادق اسماعيل، الجرائم الإلكترونية، دراسة قضائية قانونية مقارنة مع أحدث التشريعات العربية في مجال مكافحة الجريمة المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، .2012

6- إبراهيم محمد، بن حمود الزنداني، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات وأحكامها في القانون اليمني والكويتي والقطري: دراسة شرعية وقانونية مقارنة، جامعة قطامي، .2019

7- محمد علي سكسكر، الجريمة المعلوماتية وكيفية التصدي لها، كتاب الجمهورية، .2010

8- خالد حسن، أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2019.

ب- الرسائل الجامعية:

1- شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية(دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2021./2020

2- فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، رسالة دكتوراه، جامعة الجزائر 01- بن يوسف بن خدة- 2018./2017

3- مجاهدي خديجة صافية، آليات التعاون الدولي لمكافحة الجريمة المنظمة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، .2018

4- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبي بكر بلقايد، تلمسان، 2017/.2018

5- يوسف صغير، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، 2013.

ج- المجلات والمقالات العلمية:

1- وسام الدين محمد العلكة، التعاون الدولي في مواجهة جرائم الإنترنت، مجلة آداب البصرة، العدد، 66، .2013

2- خالد الشرقوني السموني، مكافحة الجريمة الإلكترونية على المستويين الوطني والدولي، المجلة المغربية للإدارة والتنمية، العدد 112، فيفيري .2012

3- لوكال مريم، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي في ضوء قانون حماية المعطيات 18-07، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، .2019

5- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، .2016

5- فادية محمد جاسم، التعاون الدول للحد من الجريمة المعلوماتية، المجلد 29، العدد 4، .2019

6- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الآكاديمية للبحث القانوني، المجلد 14، العدد02، .2016

7- برقوق يوسف، المساعدة القضائية المتبادلة لمواجهة الجرائم الإلكترونية، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 01، العد 01، .2021

8- معاشي سميرة، ما هي الجريمة المعلوماتية، مجلة المنتدى القانوني، جامعة بسكرة، المجلد، العدد، .2010

9- عبد الحليم بن بادة، إجراءات البحث والتحري عن الجريمة المعلوماتية، الخصوصية والإشكالات، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، المجلد 23، العدد ، .2015

10- صباح كزيز، أثر الجرائم الإلكترونية على أمن واستقرار الدول ، قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجا، مجلة الناقد للدراسات السياسية، العدد الثالث، اكتوبر .2018

11- عبد الفتاح الطاهري، الجريمة المعلوماتية بين ثبات النص وتطور الجريمة، مجلة القانون والأعمال، جامعة الحسن الأول - كلية العلوم القانونية والاقتصادية والاجتماعية - مختبر البحث، قانون الأعمال، العدد 41، فيفري 2019.

د- المو اقع الإلكترونية:

1- الموقع الإلكتروني: (https://www.interpol.int/ar/4/6/1)، تاريخ الاطلاع 2021./12/06

2- مراد شاوش، الموقع الإلكتروني: https://www.droitetentreprise.com/، تاريخ النشر في الموقع 2018/05/22، تاريخ الاطلاع 2022/11/22.