جامعة محمد خيضر بسكرة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة ماستر

ميدان: الحقوق والعلوم السياسية

فرع: الحقوق

تخصص: قانون دولي

رقم: .....

إعداد الطالبين:

(1) سيود دادي عبد الحق

(2) مسعودي عبد الرحمن

يوم: 12 جوان 2024

آليات التعاون الدولي لمكافحة الجريمة المعلوماتية

لجنة المناقشة:

كليبي حسن	**أستاذ محاضر –أ–**	**جامعة بسكرة**	**رئيسا**
حسن عبد الرزاق	**أستاذ التعليم العالي**	**جامعة بسكرة**	**مشرفا ومقررا**
غلابي بوزيد	**أستاذ محاضر –أ–**	**جامعة بسكرة**	**ممتحنا**

السنة الجامعية: 2023 – 2024


بسم الله الرحمن الرحيم

الإهداء

إلى أمي

أهدي إليك هذه المذكرة المتواضعة ثمرة جهدي تعبيرا عن حبي وتقديري لك،

شكرا على كل المجهودات التي قمت بها من أجلي أنت سندي القوي في هذه الحياة كنت تدعميننني وتنيرين دربي بنور حكمتك غرست في القيم والمبادئ النبيلة وأدعو الله عز وجل أن يطيل في عمرك ويحفظك

إلى أبي الحبيب في جنة الخلد السلام عليك يا أبي الغالي

أكتب إليك هذه الكلمات من أعماق قلبي حاملا إليك مشاعر الحب والاشتياق،

لقد مر على رحيلك سنوات ومازالت ذكراك حية في قلوبنا... اشتقت لوجودك معنا في مناسبات ومشاركتك فرحتنا وحبك يا أبي وذكراك ستظل خالدة في قلبي إلى الأبد، وأدعو الله عز وجل أن يغفر لك وينزل عليك رحمته الواسعة ويدخلك فسيح جنته

دادي عبد الحق

الإهداء

إلى كل من له علي فضل كل بمقامه واسمه

عبد الرحمان

شكر وتقدير

الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين سيدنا محمد وعلى آله وصحبه أجمعين

أما بعد:

إنه لمن دواعي سرورنا أنة نتقدم بالشكر وعرفان الجزيل لكل من ساهم معنا في إنجاز هذا العمل المتواضع المتمحور حول آليات التعاون الدولي في مكافحة الجريمة المعلوماتية

كما نوجه شكرنا وتقديرنا للأستاذ المشرف الدكتور حسن عبد الرزاق الذي لم يبخل علينا وأفادنا بعلمه وخبرته وساعدنا في إنجاز هذا العمل

كما نشكر أعضاء لجنة المناقشة كل باسمه ومقامه وجزاهم الله كل خير

مقدمـــة

مقدمة:

شهدت العقود الأخيرة ظهور وتطور تقنيات المعلومات، وأدت بدورها إلى التحول نحو نظام حياة جديد لم تعرفه البشرية قبلا وهو ما أرسى تحولات عميقة على البنى الاجتماعية ونظمها وأصبحت تعرف المجتمع المعلوماتي لارتباطها الوثيق بالتقنية في كافة المجالات، هذا الاخير أي المجتمع المعلوماتي لم يحدث نتيجة لطفرة شهدها المجتمع المعاصر، بل هي نتاج لسلسلة عمليات تراكمية أفرزت رسوخ النظم الالكترونية والمعلوماتية في بيئة أصبح إعتمادها الرئيسي رقميا.

إن الفترة التي نعيشها الآن هي فترة بداية مجتمع المعلومات والأكيد أن ثورة مفاهيمية قائمة في كثير من الأنساق المعرفية إنطلقت وتشكلت مع بداية هذا العصر، وفي ظل هذا الواقع الجديد لم يعد بالامكان تصور سريان نظام أي قطاع اقتصاديا كان أم تربويا أم صحيا ... الخ دون الإعتماد على تقنيات المعلومات التي وفرت القيام بالكثير من الأعمال الصعبة وإنجازها بكل سهولة ويسر، والتي جعلت من إمكانية التواصل البشري تتخطى الحدود الجغرافيا حتى أصبح العالم على شساعته يعرف بالقرية الصغيرة.

غير أن هذا الوجه المشرق المفيد لتكنولوجيا المعلومات وتطورها قابله وجه مظلم لا يخلو من المخاطر والتهديدات التي تندرج تحتها أنمط جديد للسلوك الإجرامي وهي الجريمة المعلوماتية، التي تمثل كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها، ويحدث أضرارا إقتصادية أو أجتماعية أو أمنية، والتي أخذت أبعاد تجاوزت الافراد والمؤسسات لتشكل تهديدات تمس حتى مصالح الدول.

فتحقيق مصلحة الدول لأمنها وسلامها، ومواجهتها للتحديات والجرائم المعلوماتية التي باتت تهدد أمن وسلامة المجتمع الدولي، أصبح يتطلب تعاونا دوليا بين المنظمات الحكومية والغير حكومية بشكل عام، وهو ما يمكن تطبيقه بصفة رسمية من خلال الاتفاقيات والمعاهدات أو من خلال المساعدات التقنية والفنية والتحركات المشتركة خصوصا في الآونة الأخيرة، نظرا لكثرة هذه الجرائم وتعدد أهدافها وتنوع وسائلها وطرقها، وما لوسائل الاتصالات وتكنولوجيا المعلومات من علاقة في انتشارها الواسع وما لها من آثار سلبية

هذا الواقع فرض على المجتمع الدولي التفكير في آليات التعاون الدولي لمواجهتها وتنسيق الجهود بين الدول والمنظمات واتخاذ كل الإجراءات اللازمة لذلك، خاصة أن طبيعة الجرائم المعلوماتية تتجاوز قدرة الدول منفردة مهما بلغت من قوة وتطور، بما يكفل مكافحة الجرمية المعلوماتية وتحقق أعلى مستويات الأمن في البيئة الرقمية.

أسباب إختيار الموضوع:

تنبع أسباب إختيار الموضوع أساس من رغبة وميولي شخصي لدراسة الموضوع بالاضافة الى إتصاله المباشر بمجال التخصص الدراسي، أما من الناحية الموضوعية فإن الدافع لاختيار الموضوع يرتبط بملاحظتنا لتنامي الإعتماد على تقنيات تكنولوجيات المعلومات في حياة الأفراد والمجتمعات، وما رافقه من تنامي في الجرائم المعلوماتية والتي مست الكثير من الجوانب وما تشكله من مخاطر، كما نحاول من خلال هذه الدراسة المتواضعة إلى تقديم إضافة علمية للموضوع.

أهمية الدراسة:

تعد عملية البحث عن آليات التعاون الدولي في مكافحة الجريمة الالكترونية مسألة بالغة الأهمية من الجانب العلمي والعملي خاصة مع تنامي الاعتماد على المعاملات الالكترونية في حياتنا اليومية، وبروز الحاجة إلى ضرورة خلق بيئة آمنة تبعث على الثقة والطمأنينة للمتعاملين بالتقينيات الملعوماتية على إختلاف انواعها.

أهداف الدراسة:

هي محالة سبقتها العديد من الابحاث والدراسات نهدف من خلالها إلى المساهمة ولو بالقليل في فهم طبيعة التعاون الدولية والصعوبات والعراقيل التي تقف أمام إنفاذ القانون في مثل هذه المسألة بالاضافة إلى محاولة إيجاد آليات قانونية فعالة في مكافحة الجرائم المعلوماتية بالنظر إلى حداثة وإختلاف الجرائم المعلوماتية عن الجرائم التقليدية.

إشكالية الدراسة

مما سبق تتبلور لنا الاشكالية التالية :

فيما تتمثل آليات التعاون الدولي في مكافحة الجريمة المعلوماتية ؟

منهج الدراسة:

وفيما يتعلق بالمنهج المعتمد في هذه الدراسة فقد إعتمدنا على المنهج الوصفي التحليلي فمن جهة إلى وصف آليات التعاون الدولي لمكافحة الجريمة المعلوماتية من خلال التعريف على أهم ما ورد فيها ، بالإضافة إلى التعرف على مختلف أليات التعاون الدولي في مكافحة هذه الجرائم، ومن جهة أخرى التحليل ودراسة الآليات الدولية ومدى قدرتها على تحقيق الاهداف المرجوة منها وما يعيق تحقيق ذلك وهذا ما يتم استخلاصه من تحليل الاجراءات القانونية ودراسة الجوانب الإجرائية الخاصة بها.

تقسيمات الدراسة:

وقد تم الاعتماد في دراستنا هذه على خطة ثنائية عبر تقيمها إلى فصلين حيث تمحور الفصل الأول حول آليات التعاون الدولي في مكافحة جريمة المعلوماتية وقد تم التطرق إلى إلى أهم العناصر المشكلة لهذه الآليات بالاضافة إلى التعرف على الجريمة الالكترونية من خلال المواثيق الدولية، أما في الفصل الثاني فعالجنا من خلاله الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة المعلوماتية وإبراز أهم التحديات القانونية والفنية بالاضافة إلى محاولة تبيان الآليات المقترحة لحل الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة المعلوماتية.

صعوبات الدراسة :

لقد واجهتنا في سبيل إعداد هذه الدراسة جملة من الصعوبات والمتمثلة بداية في عامل الوقت الذي كان ضيقا جدا لإعداد مثل هكذا مذكرة والإحاطة بكل جوانب الموضوع الى الحد المطلوب، بالاضافة إلى نقص المؤلفات والبحوث العلمية الأكاديمية في حدود

إطلاعنا، والتي عالجت الموضوع من نفس الزاوية بالاضافة إلى قلة المراجع القانونية والمعاهدات الدولية التي تقترن بموضوع التعاون الدولي في مكافحة الجريمة المعلوماتية.

الفصل الأول : أبرز آليات التعاون الدولي في مكافحة الجريمة المعلوماتية

تتسلل الجريمة المعلوماتية عبر حدود الدول، متجاوزةً كل الحواجز الجغرافية والمكانية، كسيل عارم من البيانات التي لا يقف في وجهها أي عائق. وتُشكل هذه الظاهرة تحديًا هائلًا، خاصةً مع تنامي ظاهرة الإجرام الدولي المنظم وارتباطه بالنشاطات المعلوماتية غير القانونية. لذلك يُعد التعاون الدولي من أهم سبل مكافحة جرائم المعلومات وملاحقة مرتكبيها، لكن تواجه هذه الجهود جملة من الصعوبات بالاضافة لضعف التنسيق بين أجهزة إنفاذ القانون، والحاجة إلى موارد مالية تقنية ضخمة، وكذا تباين في الخبرات بين الدول في التعاطي مع هذا النوع من الجرائم.

ولإبراز أهمية وخطورة الجرائم المعلوماتية فقد أفرد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين واحدة من حلقات عمله الأربع لدراسة الجرائم المتعلقة بشبكات الحاسوب والإنترنت، وقد أشير خلال المناقشات إلى أن الجرائم المعلوماتية تمثل أحد تحديات القرن الحادي والعشرين.[1]

وذلك ماسنتناوله في مبحثين اثنين:

[1]– تقرير الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، الأمم المتحدة، بانكوك، 18–25 أبريل 2005.ص 153.

المبحث الاول: آليات التعاون الثنائي في مكافحة الجريمة المعلوماتية

تظهر أهمية الجهود الإقليمية والدولية في مواجهة الجريمة المعلوماتية من خلال العمل على مكافحة هاته الجريمة، والتي رسخت في مساعي عقد وإبرام الاتفاقيات الدولية الثنائية والمتعددة الأطراف، والذي برز بدوره كعنصر فعال في مكافحة الظاهرة، خصوصا المحافظة على الثقة المتبادلة بين الدول في تقديم المساعدة الفنية والتقنية والأمنية والقضائية، الأمر الذي جعلها تضع توصيات وتبرم اتفاقيات تدرج في التشريعات الداخلية، وتعالج كل ما هو مستحدث في مجال التقدم العلمي".[1] وذلك ماسنتناوله في مطلبين اثنين:

المطلب الأول: اتفاقيات التعاون الثنائي الدولي:

يعتمد التعاون الدولي على تنسيق قوانين الجرائم المعلوماتية الوطنية، التي تجرم الجريمة المعلوماتية، والقوانين الإجرائية الوطنية للجرائم المعلوماتية التي تحدد قواعد الإثبات والإجراءات الجنائية. كما يمكن أيضًا تسهيل التعاون الدولي من خلال تنسيق الاتفاقيات الثنائية بشأن الجريمة المعلوماتية، حيثما دعت الحاجة. وهناك حاجة أيضًا إلى الانضمام إلى إتفاقيات الجريمة المعلوماتية الإقليمية والمتعددة الأطراف أو التصديق عليها لجعل هذه الاتفاقيات ملزمة قانونًا. [2]

ويتم تسهيل التعاون الدولي من خلال معاهدات الجرائم المعلوماتية الثنائية والإقليمية والمتعددة الأطراف طالما أن التجريم المزدوج موجود حيث يتطلب اعتبار السلوك المزعوم غير قانوني في البلدان المتعاونة. وبدون ازدواجية التجريم وتنسيق القوانين ، يتم إنشاء ملاذات آمنة للجرائم المعلوماتية حيث لا يمكن مقاضاة مرتكبي الجرائم المعلوماتية. ولعل أقرب مثال عن ذلك قضية فيروس Love Bug لعام 2000، والذي يعتبر أول فيروس في تاريخ الحاسوب

---

[1]– بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي أطروحة لنيل . شهادة الدكتوراه علوم تخصص، قانون عام ، كلية الحقوق، جامعة الجزائر، يوسف بن خدة، السنة الجامعية 2017–2018، ص 08

[2]– آليات التعاون الدولي الرسمية، مكتب الامم المتحدة المعني بالمخدرات والجريمة، الوحدة التعليمية7، التعاون الدولي على مكافحة الجريمة الالكترونية، يوليو 2021، اطلع عليها بتاريخ، 2024/03/26 على الموقع:
https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

مسببا مشكال كبرى حول العالم ولم يكن بالإمكان مقاضاة مرتكبها وموزعها لأن أفعاله لم تكن تعتبر جريمة في بلده الأصلي (الفلبين) وقت وقوع الحادث.[1]

غير أنه لايزال التعاون الدولي ممكنًا حتى بدون تفسير صارم لشرط ازدواجية التجريم. حيث تشير المادة 43 من اتفاقية الامم المتحدة لمكافحة الفساد والتي تضم أكثر من 184 دولة، " كلما اشترط توافر ازدواجية التجريم وجب اعتبار ذلك الشرط مستوفى بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن نفس فئة الجرائم التي تدرجه فيها الدولة الطرف الطالبة أو تستخدم في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف الطالبة، إذا كان السلوك الذي يقوم عليه الجرم الذي تُلتمس بشأنه المساعدة يعتبر فعلا إجراميا في قوانين كلتا الدولتين الطرفين".[2]

ومع ذلك، هناك استثناءات من شرط ازدواجية التجريم. وعلى سبيل المثال، لا تتطلب المادة 29 الفقرة (3) من اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية لعام 2001 تجريمًا مزدوجًا من أجل "الحفظ العاجل لبيانات الكمبيوتر المخزنة" عن طريق نظام كمبيوتر يقع داخل أراضي ذلك الطرف الآخر وتنص المادة 29 الفقرة (4) على حق الدول في رفض طلبات الحفظ إذا كانت تتطلب تجريمًا مزدوجًا للمساعدة المتبادلة في جرائم غير تلك الواردة في الاتفاقية.

وبالإضافة إلى ازدواجية التجريم، هناك شرط جوهري آخر للتعاون الدولي وهو احترام الالتزامات الدولية لحقوق الإنسان.[3] ويمكن رفض طلبات التعاون الدولي إذا كان الطلب سيؤدي إلى انتهاك الدولة المستجيبة لالتزاماتها الدولية في مجال حقوق الإنسان من خلال الاستجابة للطلب.

---

[1]– التعليم من أجل العدالة ، سلسلة الوحدات الجامعية: الجرائم الالكترونية، الوحدة السابعة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بتاريخ: 2024/03/23 على الرابط: https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

[2]– المادة 43، فقرة 02، اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 أكتوبر سنة 2003 ص، 18

[3]– مكتب الامم المتحدة المعني بالمخدرات والجريمة ، 2013، ص 205.

وتتضمن الآليات الرسمية للتعاون الدولي معاهدات ثنائية وإقليمية ومتعددة الأطراف بشأن الجرائم المعلوماتية، وتعتمد بشكل أساسي على التعاون الذي يشكل عاملا بارز في هذه المعاهدات. وعلى سبيل المثال، يتضمن اتفاق بشأن التعاون على مكافحة الجرائم في مجال المعلومات الحاسوبية لعام 2001 العديد من المواد المخصصة للتعاون الدولي (المواد 5–7)، والتي تغطي أنواع التعاون التي تغطيها هذه الاتفاقية (أي تبادل المعلومات؛ وتقديم المساعدة القانونية وفقًا للاتفاقيات الدولية؛ ومنع الجرائم الإلكترونية واكتشافها وقمعها والتحقيق فيها؛ على سبيل المثال لا الحصر)، وكذلك الطريقة التي تلتجئ إليها الدول الأعضاء لطلب المساعدة بها، والمبادئ التوجيهية للدول الأعضاء حول كيفية تنفيذ هذه الطلبات. وتتضمن المادة 8 من هذه الاتفاقية الظروف التي يمكن بموجبها رفض طلب المساعدة (أي عندما ينتهك هذا الطلب القانون الوطني للدولة) ومتطلبات الدولة الرافضة لإخطار الدولة الطالبة كتابيًا برفض الطلب وسبب (أسباب) الرفض.[1]

الفرع الاول: تبادل الخبرات والمعلومات

وتنقسم إلى الاجراءات التالية :

أولا: تبادل المعلومات:

وهو إجراء يشمل تقديم المعلومات والبيانات والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة ولهذا الإجراء سند قانوني فهو منصوص عليه بالبند "و" و "ز" من الفقرة الثانية من المادة 01 من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية.[2]

كما حث مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، المنعقد في هافانا عام 1990م في قراره المتعلق بالجرائم ذات الصلة بالحاسوب، الدول الأعضاء بكشف

[1]– آليات التعاون الدولي الرسمية، مكتب الامم المتحدة المعني بالمخدرات والجريمة، مرجع سابق.

[2]– علي حسن الطوالبة، أبحاث في جرائم تقنية المعلومات (التعاون القضائي الدولي لمكافحة الجريمة المعلوماتية)، دار الكتب والدراسات العربية، دون سنة، ص 7

جهودها لمكافحة الجرائم المعلوماتية، باتخاذ عدد من الاجراءات ، منها مضاعفة الأنشطة التي تبذلها الدول على الصعيد الدولي من أجل مكافحة جرائم المعلوماتية، بما في ذلك دخول الدول أطرافا في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل المرتبطة بجرائم المعلوماتية، وتطابق تشريعات الدول الأعضاء مع الأشكال الجديدة للإجرام. [1]

ثانيا: نقل الإجراءات:

ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جزائية بصدد جريمة ارتكبت في إقليم دولة أخرى لمصلحتها، إذا توافرت شروط معينة أهمها التجريم المزدوج بالإضافة إلى أن تؤدي الاجراءات المطلوب اتخاذها دورا مهما في الوصول إلى الحقيقة.[2]

وقد وردت هذه الصورة من صور المساعدة القضائية من خلال العديد من الاتفاقيات الدولية، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية 2000 و في المادة 21 منها، ومعاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999 وفي المادة 9 منها.[3]

ثالثا: الانابة القضائية الدولية:

تعني الإنابة القضائية مباشرة دولة ما إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمية لدولة أخرى نيابة عنها، وبناء على طلب تلك الدولة المناب عنها، ووفقا لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن، وتهدف الإنابة القضائية إلى تذليل العقبات التي تعترض سير الإجراءات الجنائية في ظل ما تشهده الظواهر الإجرامية من تطور[4].

---

[1]– عادل عبد العال ابراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، جامعة الأزهر، مصر، ص 205.

[2]– محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الاكاديمية للبحث القانوني، المجلد 14، العدد 2016/02، جامعة المجمعة، المملكة العربية السعودية، ص 54.

[3]- فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الالكترونية، مجلة البحثو في الحقوق والعلوم السياسية، المجلد 08 العدد01، لسنة 2022، ص 441

[4]– عادل عبد العال ابراهيم خراشي ، المرجع السابق، ص ص 209،210.

ومن شأن الإنابة القضائية تسهيل الاجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كإجراء التفتيش والضبط والمعاينة . وتماشيا مع سرعة الجريمة الإلكترونية، وتجنبا لطول إجراءات طلب الإنابة القضائية الدولية، فقد أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في اختصار الاجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، كالاتفاقية الأمريكية الكندية، التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال.[1]

ومن الآليات الأخرى التي تسهل التعاون الدولي في التحقيق مع مجرمي الإنترنت ومقاضاتهم، معاهدات المساعدة القانونية المتبادلة وتسليم المجرمين. ومعاهدات المساعدة القانونية المتبادلة هي اتفاقيات بين البلدان التي تنطبق على قائمة الجرائم وتحدد نوع المساعدة المقدمة من كل بلد (على سبيل المثال، الأدلة) في التحقيقات، حيث أن بعض معاهدات المساعدة القانونية المتبادلة، بدلاً من قوائم الجرائم، توافق الأطراف على التعاون في التحقيقات والملاحقات القضائية لجميع الجرائم المحظورة بموجب قوانينها الوطنية (مع استثناءات قليلة)، ويجب أن تكون طلبات المساعدة المتبادلة مكتوبة وتتضمن معلومات حول: السلطة الطالبة؛ والغرض من الطلب؛ وصف الطلب التحقيق أو إجراءات المحكمة التي يتعلق بها طلب المساعدة؛ ووصف الجريمة أو الجرائم والقوانين المنتهكة؛ وأي طلبات فيما يتعلق بالإجراءات الواجب اتباعها للحصول على الأدلة المادية والرقمية وحفظها ونقلها في نهاية المطاف إلى السلطة الطالبة؛ والمواعيد الزمنية لطلبات حفظ البيانات ولتنفيذ هذه الطلبات؛ وأي معلومات أخرى من شأنها أن تساعد الدولة التي تتلقى الطلب في تنفيذ الطلب.[2]

رابعا: التعاون الدولي من خلال تسليم المجرمين في الجرائم المعلوماتية:

يعرف تسليم المجرمين بأنه الإجراء الذي تسلم بموجبه دولة استنادا إلى معاهدة أو تأسيسا على المعاملة بالمثل عادة إلى دولة أخرى شخصا تطلبه الدولة الأخيرة لاتهامه أو لأنه محكوم عليه

[1]– محمد أحمد سليمان عيسى، المرجع السابق، ص 56.

[2]– آليات التعاون الدولي الرسمية، مكتب الامم المتحدة المعني بالمخدرات والجريمة، مرجع سابق.

لعقوبة جنائية وتشترط معظم الدول للتعليم التجريم المزدوج للسلوك الذي يطالب بالتسليم لأجله وأن يكون معاقبا عليه بموجب قوانين الدولة طالبة التسليم والدولة المطلوب إليها[1].

وتتلخص هذه الصورة من صور التعاون الدولي لمواجهة الجريمة عامة والمعلوماتية خاصة في قيام الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم العابرة للحدود، كجرائم الأنترنت، بمحاكمة هذا المتهم إذا كان تشريعها يسمح بذلك، وإلا تسليمه لدولة اخرى مختصة من أجل محاكمته، والغرض من وراء ذلك، هو الحيلولة دون إفلات المتهم من العقاب متى كان القانون الداخلي للدولة المتواجد على إقليمها لا يسمح لها بمحاكمته.

وقد كانت مسألة تسليم المجرمين في مجال مكافحة الجرائم الإلكترونية موضوع العديد من الاتفاقيات والمعاهدات الدولية، أهمها معاهدة بودابست لمكافحة جرائم الأنترنت، من خلال المواد 12 و 23 و 24 و 25 منها، وتوصيات المجلس المجلس الأوربي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجية المعلومات من خلال التوصية رقم (13/95) المؤرخة في 11 سبتمبر 1995.[2]

الفرع الثاني : المساعدة التقنية والفنية .

لتحقيق التكامل مع الاتجاه العام لرقمنة عمليات العدالة الجنائية، وتطوير المعلومات وتحليلها على الوجه الذي يخدم أهداف السياسية الجنائية الحديثة لمكافحة الإجرام عموماً والجريمة المعلوماتية بالخصوص ينبغي تبادل العناصر الإدارية، والتقانات الفنية، وتعزيز القدرات لأجهزة العدالة وتحليل ونشر البيانات والمعلومات المتاحة حول الجريمة والسبل والآليات المبتكرة لمكافحة وإبراز ماهو تقليدي وغير تقليدي منها، ويجب التركيز على الأساليب الجديدة كدعم التعاون الفني، وتقديم الخدمات الإستشارية الواسعة لتشمل كافة المجالات كتلك المتعلقة بإخفاء أثر الأموال، لمواجهة جريمة غسيل الأموال بهدف حرمان المنظمات الإجرامية من عائدات الجرائم، لأن السياسة الوقائية ستظل قاصرة، ما لم تضبط كافة عناصر السلوك الإجرامي المفترض.

[1]– محمد فاضل، التعاون الدولي في مكافحة الإجرام، جامعة دمشق، كلية الحقوق، 2012 ص 59.

[2]– عادل عبد العال ابراهيم خراشي، المرجع السابق، ص ص 216،217.

ويمكن تقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء، باستخدام التدريب وبرامج التبادل الدولي والتدريب على إنفاذ القوانين والمعاهدات المعنية بالعدالة الجنائية على الصعيد الدولي.

غير أنه في هذه الحالة يتوجب على السلطات التشريعية لأي دولة إحداث تعديل في قانون الإجراءات الجنائية، لإضفاء الشرعية على هذه الإجراءات بما يتلاءم وطبيعة الجريمة بأبعادها الجديدة المختلفة، التي تستدعي تشريعا قانونياً خاصاً للإحاطة بكافة الأوجه القانونية – الموضوعية والإجرائية – دون التقيد بالقواعد العامة التي قد تحول – أحيانا – دون أن تحقق العدالة الجنائية أغراضها.

ونصت على ذلك المادة 14 من بروتوكول مكافحة تهريب المهاجرين عن طريق البر والجو والبحر، المكمل لاتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية، بأنه يجب أن تبذل الدول الأطراف أقصى جهدها، لتوفير المواد والمعدات والنظم الحسابية وأجهزة فحص المستندات، وأن تقدم يد العون بوصفها دول منشأ أو دول عبور لتهريب المهاجرين علاوة على الكشف عن استغلال هؤلاء المهربين لعجر والضعف الإنساني لم يقعون ضحايا لهم من أجل تحقيق أغراضهم، عن طريق تقديم الرشاوى والابتزاز.[1]

المطلب الثاني: آليات التعاول الدولي الاقليمي

لقد تناولت المادة العاشرة من مشروع إتفاقية قمع الجريمة المنظمة عبر الوطنية، والمعنونة بـ " التدريب على تنفيذ القوانين" أنه : تقوم كل دولة طرف – بقدر ما تقتضيه الضرورة – باستحداث أو تطوير أو تحسين برنامج تدريبي خاص للعاملين في أجهزتها المعنية بإنفاذ القوانين ، بمن فيهم أعضاء النيابة العامة وقضاة التحقيق وغيرهم من الموظفين المكلفين بقمع الجرائم المذكورة في هذه الإتفاقية.

[1]– هاني فتحي جورجي، ورقة عمل بعنوان، "دور النيابة العامة المصرية في مكافحة الجريمة المنظمة عبر الوطنية والاتجار في الافراد، الدورة التدريبية الرابعة عشر لمنع الاتجار بالأطفال الضابط امن الموانئ بالتعاون مع وزارة الداخلية، ماي 2009 ص 96.

بالإضافة إلى ذلك، ورد في المادة 21 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية أنه : يتم رصد استيراد وتصدير الممنوعات ، من خلال تقنيات المراقبة في المناطق التجارية الحرة والموانئ الحرة، وتوظيف المعدات والتقنيات الجديدة في إنفاذ القوانين، بما في ذلك المراقبة الإلكترونية والتسليم المراقب والعمليات السرية .[1]

فتحديث القوانين الوطنية على نحو أكثر شمولية ومرونة لكي تتوائم هذه القوانين وحركة التشريع الدولية بشأن مكافحة الجريمة سبيل لتوثيق التعاون فيما بين الأجهزة التنفيذية الوطنية والأجهزة المتخصصة في مواجهة الإجرام المنظم المنشأة لهذا الغرض، ولتعدد الجرائم المعلوماتية وتطورها تزايدت صورها، مما حتم إلى ضرورة التعاون الدولي لمواجهتها، ومن ثم تكثيف الجهود الدولية وعقد الاتفاقيات والمؤتمرات الدولية لوضع استراتيجيات خاصة بمرحلتي الوقاية والمكافحة لهذ النوع من الجرائم.

الفرع الأول: تنسيق الجهود لمكافحة الجريمة المعلوماتية .

يأخذ التعاون الدولي في مجال مكافحة الجريمة المعلوماتية غالبا مظهران حيث يتعلق الأول بالسعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة في مرحلة التنفيذ، والوجه الثاني يتعلق بضرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة، والتي تعتبر إختصاصات قضائية متعددة ذات نظم قانونية مختلفة، ويتمثل في التعاون القضائي.[2]

أولا: الآليات الأمنية لمكافحة الجريمة المعلوماتية

تزداد حاجات الدول إلى الأمن والنظام من اجل ضمان الاستقرار والسلام الدائم حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول. وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، ولقد أثبت الواقع الميداني أن الدولة مهما بلغت من

[1]– لجنة منع الجريمة والعدالة الجنائية، الدورة السادسة، آراء الولايات المتحدة الأمريكية بشأن أكبر الوسائل فعالية لاجراء منع الجريمة والعدالة الجنائية، المجلس الاقتصادي والاجتماعي، نيويورك، 1997، ص ص 51، 52.

[2]– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2013/2012، ص 88.

مستويات القوة فإنها لا تستطيع بجهودها المنفردة القضاء على الجريمة خاصة وأن عالمنا المعاصر يمتاز بالتعقد الشديد والترابط في كافة مجالات الحياة داخليا وخارجيا.

ونتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوع من الجرائم المعلوماتية ، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب ، بل تعدت إلى أمن البني الأساسية الحرجة[1].

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العادلة .

ثانيا: الآليات القضائية

يبرز إختلاف القوانين السائدة من بلد إلى آخر بشكل كبير، وإذا كان بالإمكان لبلد ما أن يطبق قوانينه في إطار حدوده الجغرافية، فالأمر مختلف بالنسبة للجريمة في فضاء الإنترنت، حيث لا حدود جغرافية بين الدول.

فالولايات المتحدة الأمريكية تحظر قوانين العديد من ولاياتها ممارسة القمار عبر الشبكة، ومع ذلك تقف عاجزة إزاء انتشار هذه الظاهرة التي تنطلق من مواقع الشبكة في بلدان مجاورة لها، كما أن القانون الأمريكي يمنع الصور والأفلام الإباحية لأشخاص تقل أعمارهم عن سن الرشد، ويقرر عقوبات قاسية على هذا الفعل، ومع ذلك فالمواطنون هناك يشاهدون مثل هذه الصور والأفلام بسهولة، لأنها منتشرة في العديد من المواقع الروسية والأسبانية.[2]

---

[1]– تدابير مكافحة الجرائم المتصلة بالحواسيب – مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية المنعقد في بانكوك في الفترة 18 إلى 2005/4/25م – وثيقة رقم A/CONF.203/14

[2]– عبد الفتاح بيومي حجازي، الأحداث والانترنت دراسة معمقة عن أثر الانترنت في انحراف الأحداث، دار الكتب القانونية/ 2007، ص 314.

وللتغلب على هذه الإشكالية فإن الأمر يقتضي توحيد النظم القانونية المنظمة للأنشطة الإجرامية المتعلقة بالجرائم المعلوماتية، ولصعوبة هذا الأمر فإنه لا مناص في البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم، ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلية، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم.[1]

ويعد التعاون الدولي خطوة على طريق تدويل القانون الجنائي بقواعده الموضوعية والإجرائية، بالإضافة إلى أنه وسيلة من قبيل التدابير المانعة من ارتكاب الجريمة لإحاطة المتهمين بسياج مانعة من الإفلات من المسئولية عن الجرائم التي ارتكبوها، أو من العقوبة التي حكم عليه بها، مما يجعل المجرم يعزف عن سلوك سبيل الجريمة.[2]

الفرع الثاني: المنظمات الإقليمية المعنية بمكافحة الجريمة المعلوماتية

تتعاطى المنظمات الإقليمية مع قضايا مكافحة الجريمة المعلوماتية من خلال أطر تعاونية تهدف إلى تعزيز التعاون وتبادل المعلومات بين الدول الأعضاء. وهناك العديد من المنظمات الإقليمية التي تهتم بمكافحة الجريمة المعلوماتية، ومن بينها:

1-المنظمة الدولية للشرطة الجنائية الإنتربول.

لقد أنشأت المنظمة الدولية للشرطة الجنائية " الإنتربول" خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G8)بوضع استراتيجيات لمواجهة هذا النوع من الجرائم، من خلال إنشاء مركز اتصالات أمني عبر الشبكة، يعمل على مدار 24 ساعة و 7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف، واستخدام وسائل حديثة في تلك المكافحة كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الاطراف من خلال استخدام برنامج للتحليل

[1]- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، رسالة دكتوراه، قسم الحقوق، جامعة عين شمس، مصر ، 2007، ص 555.

[2]- محمد فتحي محمد أنور، تفتيش شبكة الانترنت، لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، مصر ، 2010، ص 54.

والمقارنة لتلك الصور، وتزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها.

ومن بين الإنجازات التي حققتها الإنتربول في ظل مواجهة الجرائم المعلوماتية، تلك العملية التي قامت بها المباحث الفيدرالية الأمريكية بالاشتراك مع الإنتربول والمتعلقة بملاحقة الشخص الذي قام بنشر دودة الحب عبر الانترنت في الفلبين، وكذا العملية التي قامت بها شرطة الإنتربول، بالاشتراك مع المباحث الفيدرالية، وكذا الشرطة الإنجليزية عام 1998 والتي أحرزت فيها إنجازات كبيرة، من خلال تفكيك منشور عليه أكثر من 75000 صورة سلبية لدعارة الأطفال، والقبض على 107 أشخاص في 12 دولة، وكذا عملية القبض على شاب ألماني، بتهمة توزيع أحد الفيروسات، وذلك بالتنسيق بين الإنتربول والمباحث الفيدرالية الأمريكية والشرطة الألمانية، وتفكيك موقع منشور للصور الإباحية في 2005/05/02، بالتنسيق مع الأوروبول[1].

وعلاوة على ذلك، تتضمن المادتان 32 و 34 من الاتفاقية العربية لجامعة الدول العربية بشأن مكافحة جرائم تقنية المعلومات لعام 2010 أحكامًا بشأن المساعدة المتبادلة وإجراءات التعاون وطلبات المساعدة المتبادلة. وعلاوة على ذلك، في اتفاقية الاتحاد الأفريقي بشأن الأمن الإلكتروني وحماية البيانات الشخصية لعام 2014، تتضمن المادة 28 أحكامًا بشأن التنسيق والمساعدة القانونية المتبادلة بشأن مسائل الجرائم الإلكترونية وتبادل المعلومات. ويدعو الحكم الأخير الدول إلى إنشاء مؤسسات يمكنها تسهيل تبادل المعلومات حول تهديدات الأمن الإلكتروني ونقاط الضعف، مثل فرق التصدي للطوارئ الحاسوبية (CERTs) أو فريق الاستجابة لحوادث أمن الفضاء الإلكتروني (CSIRT)

2-المنظمة الأوروبية لتعاون الشرطة (أوروبول):

تعمل أوروبول على تعزيز التعاون في مجال التسيير العملياتي واسع النطاق بخصوص أنظمة تكنولوجيا المعلومات في اطار سياسة "العدالة والشؤون الداخلية بين الدول الأعضاء في الاتحاد

[1]– محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 2016/02، جامعة المجمعة، المملكة العربية السعودية، ص 54.

الأوروبي[1] وتشمل جهودها مكافحة الجريمة المعلوماتية من خلال تبادل المعلومات والخبرات وتطوير القدرات.

3-المجلس الاقتصادي والاجتماعي العربي (جامعة الدول العربية):

يقوم المجلس بتعزيز التعاون بين الدول الأعضاء في العالم العربي في مختلف المجالات، بما في ذلك مكافحة الجريمة المعلوماتية من خلال تبادل المعلومات وتطوير القدرات[2].

4-المنظمة الدولية للشرطة الجنائية في آسيا والمحيط الهادئ (إينتربول-أسيان):

تهدف إينتربول-أسيان إلى تعزيز التعاون بين دول آسيا والمحيط الهادئ في مجال مكافحة الجريمة المعلوماتية، وتنظيم الأنشطة والتدريبات لتطوير القدرات.

5-المنظمة الدولية للشرطة الجنائية في أفريقيا (إنتربول-أفريقيا):

تهدف إنتربول-أفريقيا إلى تعزيز التعاون بين دول أفريقيا في مكافحة الجريمة المعلوماتية وتقديم الدعم الفني والتدريب لتعزيز القدرات.

الفرع الثالث: العمل على تطوير تشريعات وقوانين مشتركة في مكافحة الجريمة الالكترونية .

لقد عملت الكثير من الدول حول العالم على إصلاح التشريعات الإجرائية لكي تواكب المتغيرات والتطورات المتسارعة في جرائم تقنية المعلومات والتعديلات المتلاحقة في نصوص قانون العقوبات في شأنها، وتفعيل الإجراءات الجنائية وخاصة إجراءات الإثبات في مجال تقنية المعلومات.

وتميل الإصلاحات الإجرائية الحديثة إلى دمج كافة الابتكارات والتطبيقات الناتجة عن تقنية المعلومات في مجال الإجراءات الجنائية وبصفة خاصة إثبات جرائم تقنية المعلومات،

[1]- آمال جحيج، نحو قوة أورو- متوسطية للشرطة وتسيير الحدود، مجلة دفاتر السياسة والقانون، العدد الثاني عشر، جانفي 2015، ص 256.

[2]- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مشروع إعلان منتدى التعاون العربي الصيني، جامعة الدول العربية، 2010/12/21

وتستجيب النصوص المستحدثة لاحتياجات الشرطة القضائية واستغلالها بالنسبة للتحقيقات في هذا الصدد.[1]

والناظر في المواثيق الدولية الصادرة عن الأمم المتحدة يجد أنها تشجع الدول الأطراف فيها على السماح باستخدام بعض تقنيات التحقيقات الخاصة، الشئ الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعال، وقد أبرمت العديد من الاتفاقيات الدولية في مجالات التعاون الدولي، وتستهدف التقريب بين القوانين الجنائية الوطنية من أجل مكافحة الجرائم العابرة الحدود، وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ إجراءات التحقيق وجمع الأدلة والاعتراف بالأحكام الجنائية الأجنبية.[2]

وفي سبيل تحقيق ذلك يمكن الاشارة الى أن العملية التشريعية في مجال مكافحة الجريمة التقنية مرت عبر العديد من الجهود على مختلف المستويات إقليميا ودوليا وكذا عبر منظمة الأمم والمتحدة والوكالات المتخصصة وهذا لوضع نصوص عقابية وإجرائية رادعة.

فقد اهتم المجتمع الدولي بتنظيم مجال تقنية المعلومات وبذل العديد من الجهود التشريعية من أجل التصدي لظاهرت الإجرام المعلوماتي وكان من بين هذه الجهود ما قامت به الدول الآتية تباعاً:[3]

- **السويد** : حيث أصدرت عام 1973 أول قانون لها في مجال مكافحة تقنية المعلومات وهو قانون البيانات السويدي والذي اهتم بمعالجة قضايا الدخول غير المشروع للبيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها، وهي بذلك تعتبر أول دولة تقوم فعليا بإصدار تشريعات تتعلق بجرائم التقنية، لاسيما التزوير المعلوماتي.
- **الدنمارك:** والتي لحقت السويد في هذا التطور الحاصل في مجال تقنية المعلومات بإصدارها أول قانون لها يتعلق بمكافحة جرائم الحاسب الآلي والانترنت عام 1985 ،

[1]– سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، دار النهضة العربية، ط1، 1999، ص 59.

[2]– محمد فتحي أنور ، مرجع سابق، ص 55.

[3]– أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة عمل، مقدمة في المؤتمر المغارب الأول حول (المعلوماتية والقانون)، أكاديمية الدراسات العليا، طرابلس خلال الفترة 28-2009/10/29.

وكان من أهم نصوص هذا القانون ما تضمن منها فقرات خاصة بتحديد العقوبات والأفعال المجرمة التي تعد انتهاكا للحاسب الآلي كالتزوير المعلوماتي.

- **بريطانيا:** بإصدارها لقانون مكافحة التزوير والتزييف عام 1986م، وعرف أداة التزوير بأنها عبارة عن وسائط التخزين الحاسوبية المتنوعة، أو أي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى
- ألمانيا: أصدرت عام 1986م قانون خاص لمكافحة التزوير المعلوماتي والذي بموجه تكون لحقت عجلة التطور التشريعي الحاصل في مجال تقنية المعلومات.
- فرنسا: أصدرت القانون الفرنسي رقم 19 لسنة 1988م الخاص بالتصدي للتزوير المعلوماتي.
- **الولايات المتحدة الأمريكية** : أصدرت العديد من التشريعات المتعلقة مجال تقنية وتكنولوجيا المعلومات، وكان من بينها القانون رقم 474 – 99 – 100 وهو قانون تشريعي عام شمل القانون التشريعي رقم 1213 لسنة 1986 والمعدل للقانون الخاص بمواجهة جرائم الحاسوب[1].

ولم يقف الأمر عند هذا الحد بل لقد أجتمع المجلس الأوروبي عام 2001 في العاصمة المجرية بودابست في 23 نوفمبر 2001 ، للتشاور حول هذه الظاهرة الإجرامية المستحدثة وتم الاتفاق على بنود واضحة لمكافحة هذه جرائم تقنية المعلومات، وقد أبرمت الاتفاقية الأوروبية الدولية لمكافحة الجرائم السيبرانية، حيث رسمت سياسة جزائية مشتركة لمكافحة الجرائم الافتراضية، لضمان الحماية الكافية من الجرائم المعلوماتية،[2] وقد وقعت عليها 30 دولة، ثم انضم إليها العديد من الدول من خارج المجلس الأوروبي، وكان من أبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في 22 سبتمبر 2006، ودخلت حيز النفاذ في الأول من يناير 2007 ، واشتملت على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.

[1]– أبو المعالي محمد عيسى، المرجع السابق.

[2]– قطاف سليمان وبوقرين عبد الحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الاول، 2022/03/31، ص337.

المبحث الثاني: الجريمة الالكترونية في المواثيق الدولية.

تعد الجريمة الالكترونية نشاطا إجراميا تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.[1] وقبل التطرق إلى أهم الاتفاقيات الدولية المتعلقة بهذه الجريمة لا بأس وأن نشير إلى بعض أشكال هذه الجريمة من الناحية الدولية مع تبيان بعض الأمثلة عنها، وذلك ماسنتناوله في مطلبين اثنين:

المطلب الأول: نماذج عن الجريمة الالكترونية على المستوى الدولي.

تتنوع الجريمة الالكترونية وتأخذ أشكالا متعددة سوف نحاول التطرق اليها على سبيل المثال مع تدعيمها ببعض الأمثلة في دول من العالم. الفرع الأول: جرائم التجسس الالكتروني و جرائم القرصنة.

الفرع الأول: جرائم التجسس الالكتروني:

حيث يعرف هذا النوع باعتماده على تقنيات عالية التطور إذ لم يعد يقتصر التجسس على ما يتعلق بالمعلومات العسكرية أو السياسية بل تعداه إلى المجال الاقتصادي والتجاري والثقافي، و لقد برز هذا النوع من الجرائم خصوصا بعد أحداث الحادي عشر من سبتمبر التي شهدتها الولايات المتحدة الأمريكية،[2] ومن الأساليب المعتمدة أسلوب إخفاء المعلومات داخل المعلومات بحيث يتم إخفاء تلك المعلومات المهمة والمستهدفة داخل معلومات عادية في جهاز الحاسب الآلي و من ثم يتم تهريبها باستعمال أساليب متطورة لا يتم اكتشافها ولو ضبط الشخص متلبسا، و مثال ذلك: قيام شبكة دولية ضخمة للتجسس الالكتروني التي تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات في كندا وبريطانيا لرصد المكالمات الهاتفية بهدف التعامل مع الأهداف غير العسكرية، ولا يقتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية بل يشمل الاتصالات التي تجري عبر أنظمة الاتصالات العثور على مواقع الأرضية.[3]

---

[1]– عبد الفتاح بيومي حجازي، الاثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، 2007، ص 13

[2]– عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، منشأة المعارف، القاهرة، 1998، ص 382.

[3]– عبد الفتاح بيومي حجازي، المرجع السابق، ص 29.

وجدير بالذكر أن الأساليب الفنية للتجسس ألمعلوماتي هي أكثر الطرق استخداماً من قبل المجرميين الالكترونيين ، نظراً لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية، وخصوصاً العسكرية والسياسية والاقتصادية، وما يمكن ان تحقق من مكاسب مهما كانت، أوقد تستخدم هذه المعلومات إذا تعرضت للتجسس من أجل الإضرار بمصلحة المجتمع والدول.[1]

الفرع الثاني: جرائم القرصنة الالكترونية

في السنوات الأخيرة انتشرت القرصنة الإلكترونية بصورة كبيرة تنبئ بالخطر بسبب خواصها التي تميزها عن الجريمة التقليدية، ذلك أن ضحاياها يتعرضون لتعطيل وتدمير مخازن المعلومات الخاصة بهم وسرقة أموالهم والتهديد والابتزاز، مما يتسبب للاقتصاد بأضرار كبيرة. ومع تزايد نسبة الجرائم الإلكترونية وتنوع طرقها فقد أصبحت تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية، ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات، فجرائم القرصنة أصبحت تدار إلكترونيا وتوجد على الشبكة الإلكترونية لفتح قنوات تواصل جديدة بهدف استقطاب شريحة أكبر من الناس وزيادة أرباحها. مما ألحق العديد من الخسائر المادية الباهضة وهذا ما جعل الشركات المتخصصة في صناعة البرامج إلى المساهمة في تحديث تقنيات لمكافحة القرصنة الالكترونية والعمل كطرف ثالث خاصة في توفير البرمجيات والمعطيات والبيانات للجهات الخاصة بإنفاذ القانون.[2]

وأقرب مثال لذلك ما تتعرض له أنظمة التشغيل من مايكروسوفت لبرامج الكومبيوتر من عمليات قرصنة مستعملين في ذلك عامل ذكي لبرامج الكومبيوتر يمكنه التجول بحرية عبر الشبكات لالتقاط المعلومات و نقلها دون قيام المتسلل باختراق الكومبيوتر نفسه، حيث تم فتح تحقيق في هذا المجال. [3] كما يتم أيضا إرسال فيروسات لتخريب الجهاز و محتوياته حيث بمجرد كتابة كلمة أو فتح البرنامج الحامل للفيروس أو الرسالة البريدية المرسل معها الفيروس تتم إصابة الجهاز ومن ثم يقوم بمسح محتوياته أو العبث بالملفات الموجودة فيه.

[1]– محمد محمد شتا، الحماية الجنائية لبرامج الحاسوب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001، ص 94.

[2]– عبد الفتاح مراد، المرجع السابق، ص 385.

[3]– علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، ك1، 2011، ص 92-93.

الفرع الثالث: الجرائم المنظمة:

تم استغلال الإمكانيات المتاحة في وسائل الانترنت لتخطيط وتمرير وتوجه المخططات الإجرامية وتنفيذ وتوجيه العمليات غر المشروعة بكل سهولة من خلال إنشاء مواقع خاصة بها على شبكة الانترنت لمساعدتها في إدارة العمليات، والترويج بتجارة المحذرات عبر الانترنت أيضا و تعليم كيفية زراعتها وصناعتها .[1]

وكذا جرائم غسل الأموال التي تعتمد على إخفاء المصدر غير المشروع الذي تكتسب منه الأموال حيث يجد المتصفح للانترنت مواقع عديدة تتحد عن غسيل الأموال غير المشروعة التي تتميز بالسرعة وإغفال التوقيع واستعمال بطاقات مزورة شبيهة ببطاقات البنوك المستخدمة التي تساهم في تحويل الأموال عبر الانترنت مع ضمان تشفير و تأمين العملية كل ذلك ساعد على سهولة و سرعة الجريمة دون ترك الأثر.[2]

إضافة إلى العديد من الجرائم الأخرى كالجرائم الماسة بالتجارة الالكترونية من خلال الاستيلاء على بطاقات الائتمان[3]، وكذلك الجرائم الاقتصادية كسرقة خطوط الهاتف والعبث بها و إتلافها، وتحويل الأرصدة النقدية وغيرها.

وعليه بالنظر الى الطبيعة الخاصة التي تتميز بها الجريمة الالكترونية باستخدام الوسائل الالكترونية المستحدثة تمتد لتشمل البعد العالمي هذا الأخير الذي لا يتقيد بحدود دولة معينة وهذا ما يجعله ينعكس على آليات مكافحتها.

---

[1]– سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، بحث مقدم إلى مركز البحوث والدراسات، كلية الشريعة والقانون – جامعة الامارات العربية المتحدة، 2000.ص 17

[2]– أسامة حسين، الاحتيال الإلكتروني، زهران للنشر، الطبعة الأولى، الاردن، 2011.ص 28.

[3]– عماد علي الخليل، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1–3 مايو 2000م، ص4.

المطلب الثاني: الاتفاقيات الدولية الخاصة بجرائم المعلوماتية.

مع تقدم تكنولوجيا المعلومات وزيادة اهتمام الدول بمكافحة الجرائم المعلوماتية، وقعت العديد من الاتفاقيات والمعاهدات الدولية من قبل الدول التي على أعتبار الأخطار والتهديدات التي تحدثها هذه الجرائم وإتسامها بالتعقد على خلاف الجرائم التقليدية، حيث يمكن للجاني أن يكون في بلد والضحية في بلد آخر، ومقدم الخدمة في بلد ثالث، والموقع الذي تم منه الجريمة في بلد آخر. ومن هنا، تثار مسألة تطبيق القوانين الجنائية، لذلك سنحاول التطرق للمواثيق الدولية المتعلقة بجرائم الكمبيوتر والإنترنت.

الفرع الأول: قرار الأمم المتحدة الثامن لمنع الجريمة (هافانا)

يعتبر القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر. من الجهود التي بذلتها الأمم المتحدة حيث عقد هذا المؤتمر في هافانا سنة 1990 و قد حث في قراره المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء أن تكثف جهودها لمكافحة إساءة استعمال هذا الجهاز وبتجريم تلك الأفعال جنائيا و اتخاذ الإجراءات التالية متى دعت الضرورة لذلك:

- ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق و الأدلة في الإجراءات القضائية تنطبق على نحو ملائم ، وإدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك.
- النص على جرائم و جزاءات وإجراءات تتعلق بالتحقيق والأدلة حيث تدعو الضرورة للتصدي لهذا الشكل الجديد و المعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم.[1]

وقد خلص بتوصيات للدول الأعضاء بضرورة مضاعفة الأنشطة التي تبذلها على الصعيد الدولي لمكافحة الجرائم المتصلة بالكمبيوتر بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة، ونصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين

[1]– الزعبي جلال محمد والمناعسة أسامة محمد، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة، ط1، عمان، 2013،ص 44

وتبادل المساعدة في المسائل الجنائية تنطبق بكل تام على الأشكال الجديدة للإجرام مثل الجرائم الالكترونية، وأن تتخذ خطوات محددة نحو تحقيق هذا الهدف.[1]

كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة المعلوماتية بصفة عامة بضرورة وضع أو تطوير :

1-معايير دولية لأمن المعالجة الآلية للبيانات.

2-اتخاذ تدابير ملائمة لحل إشكالية الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابر للحدود أو ذات الطبيعة الدولية.

3-إبرام اتفاقيات دولية تنطوي على نصوص تنظيم و إجراءات التفتيش والضبط المباشر الواقع عبر الحدود، على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد وحرياتهم و سيادة الدول.[2]

الفرع الثاني: توصيات مؤتمر الأمم المتحدة الثاني عشر الاستراتيجيات الشاملة لمواجهة التحديات العالمية (سلفادور –البرازيل 2010)

وقد أبرز الدور المحوري للعدالة في التنمية، وأكد الحاجة إلى اتباع نهج كلي في إصلاح نظام العدالة الجنائية لتعزيز قدراتها، وضرورة استكشاف سبل كفيلة بمنع ومكافحة الأشكال المستجِدّة للجريمة على مستوى العالم، حيث نص على الأفعال المجرمة التي جرائم معلوماتية كالاحتيال، والغش المرتبط بالكمبيوتر من خلال إتلاف ومحو المعطيات، وأيضا ما يعرف بالتزوير المعلوماتي ويشمل إتلاف ومحو البرامج والبيانات و تعطيل وظائف الكمبيوتر و نظام الاتصالات (الشبكات)، أو الدخول غير المصرح به عن طريق انتهاك إجراءات الأمن.

وقد أيدت الجمعية العامة إعلان سلفادور وأوصت بلإجراء دراسة شاملة لمشكلة الجرائم السيبرانية والاستجابات لها من جانب الدول الأعضاء والمجتمع الدولي ، فيما تعلق بتبادل المعلومات وتقريب التشريعات الوطنية وأفضل الممارسات والمساعدة التقنية والتعاون الدولي،

[1]– محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية (دراسة مقارنة)، ط 1، مركز الدراسات العربيةمصر، 2016،ص56

[2]– محمد نصر محمد، المرجع نفسه، ص 57.

بهدف دراسة الخيارات المتاحة لتعزيز التعاون واقتراح استجابات قانونية وطنية ودولية جديدة لمكافحة الجريمة السيبرانية.

أما من الناحية الإجرائية فان القرار الصادر تضمن جملة من القواعد الإجرائية في بيئة الجرائم المعلوماتية تتمثل فيما يلي:[1]

6-القيام بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، و أيضا تفتيش شبكات الحاسب الآلي.

7-التعاون الفعال بين المجني عليهم والشهود و كذا مستخدمي المعلومات من أجل إتاحة استخدام المعلومات للأغراض القضائية.

8-اعتراض الاتصالات داخل نظام الحاسب الآلي ذاته وممارسة الرقابة عليها.

الفرع الثالث: اتفاقية برن الدولية لحماية المضفات الأدبية والفنية.

بهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام اتفاقية برن الدولية في 9 سبتمبر 1886، والمكملة بباريس في ماي 1896، والمعدلة في برلين في 13 سبتمبر 1908، والمكملة ببرن في 20 مارس 1914، والمعدلة بروما في جوان 1928 ، وبروكسل سنة 1948، و استوكهولم في جويلية 1967، وباريس في جويلية 1971، حيث تشكل الدول الأطراف في هذه الاتفاقية اتحادا لحماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية.[2]

وبموجب اتفاقية برن الدولية تتمتع برامج الحاسب الآلي الكمبيوتر" سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية وفقا لما جاء فيها "المتعلقة بالجوانب

[1]- الزعبي جلال محمد والمناعسة أسامة محمد، المرجع السابق، ص 76.

[2]- اتفاقية برن بشان حماية المصنفات الأدبية والفنية لسنة 1886، المنظمة العالمية للملكية الفكرية، تاريخ الاطلاع، 2024/03/28 على الرابط: https://www.wipo.int/treaties/ar/gip/berne/summary_berne.html

المتصلة بالتجارة الدولية حيث تسعى الدول إلى تشجيع الحماية الفعالة والملائمة لحقوق الملكية الفكرية من أجل تخفيف العراقيل التي تعوق التجارة الدولية.[1]

و هكذا تتميز هذه الاتفاقية بأنها لا تنظم من جوانب الملكية الفكرية إلا ما تعلق بالتجارة الدولية و دون التعارض أو الإخلال بالاتفاقيات الدولية الأخرى المخصصة لتنظيم حماية هذا النوع من أنواع الحقوق.

الفرع الرابع : اتفاقية بودابست لمقاومة جرائم المعلوماتية واتصالات 2001.

إدراكا من الدول بمدى خطورة الجريمة المعلوماتية بوصفها جريمة عابرة للحدود فقد تم التوقيع عليها من طرف ثلاثون دولة في العاصمة المجرية " بودابست" نذكر منها دول أعضاء من الاتحاد الأوروبي ، إضافة إلى كندا اليابان، جنوب إفريقيا، أمريكا، وجاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة الالكترونية وتجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها والمساعدة على الاستدلال عليهم وضبطهم كما تحدد أفضل الطرق الواجب إتباعها في التحقيق في جرائم الانترنت التي تعهد الدول الموقعة بالتعاون الوثيق من أجل محاربتها، كما فصلت الاتفاقية النصوص الجنائية الموضوعية للجريمة وأنواعها كما تشمل جوانب عديدة من جرائم الانترنت من بينها الإرهاب، عمليات تزور بطاقات الائتمان و غيرها ...

وتعتبر هذه الاتفاقية أحد محاولة وأكثرها تنوعا من أجل تنسيق قوانين جديدة في دول عديدة ضد إساءة استخدام الانترنت. كما نشير إلى أنها تأتي بعد فترة طويلة من المشاورات بين الحكومات و أجهزة الشرطة وقطاع الكمبيوتر و قد صاغ نصها عدد من الخبراء القانونين في مجلس أوروبا بمساعدة دول أخرى.

الفرع الخامس: قانون الأونستيرال النموذجي.

اقتناعا من الدول بضرورة منع هذه الجرائم و مكافحتها خاصة وأن ذلك يتطلب استجابة ديناميكية في ضوء الطابع الدولي والأبعاد الدولي لإساءة استخدام الكمبيوتر والجرائم المتعلقة

[1]– حسين جميعي، الاطار القانوني الدولي لحماية حق المؤلف والحقوق المجاورة، ندوة الويبو الوطنية عن إنفاذ حقوق الملكية الفكرية للقضاة والمدعين العامين، المنظمة العالمية للملكية الفكرية (الويبو) بالتعاون مع وزارة الاعلامن مملكة البحرين، 2004، ص13

به تم صياغة قانون الأونيسترال النموذجي بشأن التجارة الالكترونية، والآخر بشأن التوقيعات الالكترونية.

أولا: قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية.

اعتمد هذا النص في 5 جويلية 2001 و ينطبق هذا القانون حيثما تستخدم توقيعات الكترونية[1] خاصة بعدما أصبح التوقيع بمفهومه التقليدي لا يستجيب لمتطلبات السرعة، والحداثة التكنولوجية حيث أنه أمام هذه التطورات تلاشت وظيفة التوقيع التقليدي ليحل محله التوقيع الالكتروني و هو عبارة عن كود سري أو شفرة سرية يتم الحصول عليها بعد إتباع جملة من الإجراءات.

ثانيا: قانون الأونيسترال النموذجي بشأن التجارة الالكترونية.

تنطبق نصوص هذا القانون على أي نوع من المعلومات التي تكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية، بحيث يتم استلامها أو تخزينها بوسائل الكترونية، و يتم تبادل هذه البيانات من خلال نقلها الكترونيا من حاسوب إلى آخر باستخدام معيار متفق عليه مع الأخذ بعين الاعتبار تفسير هذا القانون لمصدره الدولي والضرورة توحيد تطبيقه.[2]

[1]– سليمان أحمد فضل المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، مصر، 2013، ص 111.

[2]– سليمان أحمد فضل، المرجع السابق، ص 143.

خلاصة الفصل :

نخلص في نهاية هذا الفصل إلى أن طبيعة الجرائم المعلوماتية عابرة للحدود وتمتاز بإختلافها عن الجرائم التقليدية حيث أن سمتها الابرز هو تعقد ظروفها وحيثيتها بحكم أنها تقع في بيئة إفتراضية وتعتمد على أدوات وتقنيات التكنولوجيا، مما يفرض بالضرورة تعاون دولي فعال لمكافحتها، وتتجلى آليات هذا التعاون من خلال إبرام الاتفاقيات الثنائية بين الدول لتبادل المعلومات والمساعدة القانونية المتبادلة وتسليم المجرمين بالاضافة إلى إتفاقيات الأمم المتحدة لمكافحة الجريمة المنظمة عبر الأنترنت وبروتوكولها.

الفصل الثاني:الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة المعلوماتية

التعاون الدولي بكافة صوره في مجال مكافحة ومواجهة الجريمة المعلوماتية وإن كان يعد مطلبا تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها ، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه فيها ما يتصل بطبيعة النشاط الاجرامي التي تتسم بتعدد صورها وعدم وجود نوذج واحد لها بالاضافة إلى عدم وجود إتفاق عام ومنسق بين الدول حول في شكل وطبيعة الجرائم المعلوماتية محل التجريم من عدمه، فما قد يعتبر جرما من خلال تشريعات بعض الدول قد لا تعتبره دول أخرى كذلك.

وذلك ماسنتناوله في مبحثين اثنين:

المبحث الأول: التحديات القانونية و الفنية.

أدى التقدم الكبير في استغلال الوسائل التقنية الحديثة وبخاصة شبكات المعلومات العالمية في الجرائم المعلوماتية إلى بروز تحديات وتعقيدات هائلة للجهات وهيئات إنفاذ القانون؛ فأصبح عنصر "الدولية " مضافاً أو مرادفا لمعظم الجرائم حيث أنها لا تخضع للحدود الجغرافيا وتتعدى إقليما بعينه، وهذا يعني أن الأليات البطيئة للتعاون الدولي في شأن ملاحقة الجرائم المعلوماتية والإرهابية من شأنها أن تُخرج التحقيقات عن مسارها، أو يُعيقها في حالات أخرى؛ لذلك تسعى الدول للتتفاوض فيما بينها من أجل إبرام اتفاقيات دولية علي المستوي الثنائي أو المتعدد الأطراف بغرض إرساء أطر تنظيمية تحكم مكافحة كل أشكال الجرائم المستحدثة، وخاصة منها الجرائم المعلوماتية العابرة للحدود، ثم تسلتهم منها التشريعات الوطنية الجديدة أو تُنَقح تشريعاتها الموجودة بالفعل على هدي من هذه الإتفاقيات الدولية التي تم إبرامها.[1] وذلك ماسنتناوله في مطلبين اثنين:

المطلب الأول: تباين القوانين الوطنية المتعلقة بالجرائم المعلوماتية

إن اختلاف النظم التشريعية للدول التي تطمح إلى تحقيق التعاون فيما بينها في مجال مجابهة الجرائم المعلوماتية، يشكل عقبة كبيرة تحول في معظم الحالات دون تحقيق غايات وأهداف الدول خاصة عندما لا تواكب بعض الدول التطورات الهائلة الحاصلة في نوعية هذه الجرائم المعقدة، بإصدارها التشريعات المتطورة التي تلاحق الثورة الكبيرة في مجال استخدام الحاسوب وشبكات المعلومات العالمية في ارتكاب هذه الجرائم على وجه الخصوص.

الفرع الأول: الصعوبات الإجرائية في مكافحة الجريمة المعلوماتية

تتجلى أحد أبرز الأمثلة على تعارض المصالح بين الدول وغياب التعاون القضائي في مكافحة الجرائم الإلكترونية في قضية مواطن بريطاني متهم باختراق أنظمة حاسوب الجيش الأمريكي ووكالة الفضاء الأمريكية. وعقب ملاحقات حثيثة من قبل الولايات المتحدة لتسليمه

[1]– أيمن سلامة، لماذا يصعب التعاون الدولي في مجال مكافحة الجريمة السيبرانية؟، مقال منشور على موقع سكاي نيوز، 3 يوليو 2021، اطلع عليه بتاريخ: 2024/04/18: على الرابط:
https://www.skynewsarabia.com/blog/1448837

لمحاكمته، واجهت طلبها رفضًا من المملكة المتحدة التي امتنعت عن تسليمه أو محاكمته على أراضيها. هذا ما يحيلنا الى الاستناد على جملة الصعوبات الاجرائية نوجزها فيما يلي:

- **صعوبة تبني تصور مشترك لأهداف التعاون الدولي في مجال القوانين الجنائية الموضوعية** : حيث أن هذه المسائل تخاطب مباشرة إشكالية التعريف بكل جريمة والعقوبات المناسبة لها ومسؤولية الفاعلين في الفضاء الإلكتروني، بما في ذلك مزودو خدمات الإنترنت.[1]
- **صعوبات مرتبطة بالاختصاص القضائي** : تبقى الجرائم المعلوماتية من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى الدولي وتبرز أهمية تحديد المكان الذي ارتكبت فيه الجريمة من أجل تحديد القانون الواجب تطبيقه، حيث تثار إشكالية الاختصاص على المستوى الدولي على خلفية اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المعلوماتية التي تتميز بكونها عابرة للحدود.[2] فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية ... كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى ، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.[3]

---

[1]– بن دراج علي إبراهيم، محاضرات في الجرائم المعلوماتية، تخصص القانون الجنائي والعلوم الجنائية، معهد الحقوق والعلوم السياسية، المركز الجامعي آفلو، الجزائر، 2021، ص 43.

[2]– موسى مسعود ارحومة، الاشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية،المؤتمر المغاربي الاول حول المعلوماتية والقانون، اكاديمية الدراسات العليا، طرابلس، خلال الفترة 28–2009/10/29، ص 15

[3]– جميل عبد الباقي الصعير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ط1، القاهرة، 2002، ص 82

كل هاته الإشكاليات وغيرها المرتبطة بتحديد الاختصاص القضائي ظلت ولا زالت تشكل هاجسا لدى خبراء القانون الدولي في مجال مكافحة هذا النوع من الجرائم.

الفرع الثاني: الصعوبات الفنية في مجال مكافحة الجريمة الالكترونية

تحيط بجملة التحديات والمعيقات التي تقف أمام تعزيز التعاون الدولي في مجال مكافحة الجريمة المعلوماتية أجراءت فنية مرتبطة بطيعة الفعل الاجرامي في حد ذاتة نذكر منها:

- **تفاقم وإزدياد أنواع الجرائم المتعلقة بالفضاء الإلكتروني:** وبالخصوص تلك الجرائم المرتكبة من خلال استخدام شبكات الاتصالات السلكية واللاسلكية بالاعتماد على الإنترنت والتي من أهمها المعاملات المالية غير المشروعة، أو تقديم خدمات غير قانونية، وانتهاك حقوق التأليف والنشر، علاوة على الجرائم التي تنتهك كرامة الإنسان وحماية القاصرين.[1]
- **استخدام سلطات قسرية قليلة الفعالية** : تظهر هذه الصعوبة بشكل واضح في مجال الاستخدام العابر للحدود، وقابلية تطبيقها في بيئة تكنولوجية، مثل اعتراض الاتصالات السلكية واللاسلكية والمراقبة الإلكترونية لشبكات المعلومات، لاسيما عن طريق شبكة الإنترنت، لذا يستلزم البحث في نظم معالجة المعلومات ومصادرتها ، بما في ذلك مواقع الإنترنت، مما يجعل مواد غير قانونية غير قابلة للنفاذ ويتطلب من مقدمي الخدمات الامتثال لالتزامات خاصة مع مراعاة المشاكل الناجمة عن تدابير خاصة بسلامة المعلومات، كالتشفير مثلا .
- **عدم وجود قنوات اتصال** : أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين ، الحصول على المعلومات والبيانات المتعلقة بهم ، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة ، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين. وبالتالي تنعدم الفائدة من هذا التعاون.[2]

[1]– قدوس خديجة ، عمتوت كمال، انتهاكات حقوق الانسان في ظل انتشار الجريمة الالكترونية، مجلة التدوين، المجلد 12، العدد 02، 2020، ص 173.

[2]– عبد الفتاح علي، مكافحة الجرائم الاكترونية بين نظم المعلومات والإعلام البديل، مكتبة الوفاء القانونية، الاسكندرية، ط1، 2017، ص 499.

- **الصعوبات في إطار التعاون الدولي في مجال التدريب:** يلاحظ في بعض الدول عزوف بعض القيادات الإدارية عن المشاركة في برامج التدريب، لاعتقادهم الراسخ بأنها تُعيق مسار تطوير العمل. ينبع هذا الاعتقاد من خوفهم من تطبيق ما يتعلمه المتدربون من خبرات ومهارات جديدة، ممّا قد يُشكل تهديدًا للتعاون وتناغم العمل بين أعضاء الفريق، خاصةً مع وجود فوارق فردية بين المتدربين في مستوياتهم المعرفية واكتسابهم للمهارات[1].

ويكتسي هذا التحدّي بعدا هاما بشكل خاص في مجال تكنولوجيا المعلومات والاتصالات، حيث تتفاوت مستويات الخبرة والمعرفة بين الموظفين بشكل كبير. ففي حين قد يفتقر البعض إلى أيّة معرفة تقنية، يتمتع آخرون بخبرة واسعة وثقافة عميقة في هذا المجال.

بالإضافة إلى عدم قدرة البيئة التدريبية على تمثيل الواقع العملي بشكل تام تحديًا آخر يواجه التعاون الدولي في مجال التدريب. فعندما لا تعكس البيئة التدريبية بدقة ما يدور في بيئة العمل، من وقائع وملابسات وإجراءات، ونشاطات، يواجه المتدرب صعوبة في ربط ما يتعلمه بالتطبيقات العملية، مما يُقلّل من فاعلية التدريب ويُضعف مهاراته المكتسبة.[2]

المطلب الثاني: صعوبة إثبات وجمع الأدلة الالكترونية.

إن أكثر عائق يواجه المحققين في جرائم الحاسوب هو عدم وجود دليل مرئي يمكن قراءته واستيعابه، وذلك أن البرامج والبيانات التي تقع عليها الجريمة تكون غير قابلة للإدراك الحسي، بحيث لا تخلف آثارا مادية تدل على مرتكبيها كما هو الحال في الجرائم التقليدية، فلا وجود للكسر ولا للدم ولا أيا من الآثار التقليدية للجريمة، فالجريمة المعلوماتية يتمحور نشاطها في بيئة رقمية.

الفرع الاول: صعوبة إثبات الجريمة المعلوماتية

من بين سمات الجريمة المعلوماتية التي تجعل منها جريمة صعبة وخطيرة أي يصعب متابعتها واكتشافها فهي لا تترك أثرا وهي مجرد أرقام تتغير في السجلات ، فمعظم الجرائم

[1]– سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة2013،ص 448.

[2]– المرجع نفسه، ص 450.

الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها إذ تفتقر إلى الدليل المادي التقليدي كالبصمات مثلا.

وتعود أسباب وصعوبة إثباتها إلى أن متابعتها واكتشافها من صعوبة المكان، حيث أنها لا تترك أثرا فما هي الأرقام تدور في السجلات كما أن الجرائم التي لم تكتشف هي أكثر بكثير من التي كشف عنها وتعود الصعوبة إلى الأسباب التالية.

- أنها جريمة لا تترك أثرا إلا بعد ارتكابها، وتأتي من هنا مشكلة ضبط هذه المعطيات وإحرازها في شكل إلكتروني وحجزها ووضعها في خاتم قانوني لإستغلالها في البحث، وإذا كانت بعض التجهيزات والتقنيات تسمح للباحثين بالوصول إلى هذه المعطيات التي تبقى في ذاكرة الحاسوب المستعمل، إلا أنها تتطلب خبرة عالية وإمكانيات قد لا تتوافر عادة لدى مصالح الشرطة القضائية المكلفة بالبحث .[1]
- صعوبة الاحتفاظ الفني بآثارها إن وجدت، فأغلب البيانات المخزنة والتي تتداول عبر الكمبيوتر تكون على هيئة رموز وشيفرات مخزنة على وسائط ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال الاجهزة الحاسوبية.
- تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، حيث يتطلب ذلك الاستعانة بأجهزة وادوات برمجية خاصة للإطلاع عليها أو إستخراجها في هيئة ملموسة او مادية أي تدخل متخصصين لتحويل تلك المعطيات من طبيعتها الرقمية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة. [2]
- أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها، فهي ترتكب في بيئة رقمية في الأغلب يتم إكتشاف وقوع الجريمة عن طريق المصادفة ، حيث لا يترك مرتكبها أثرا ماديا يدل عليه، كما هو الحال في الجرائم التقليدية ، فالجرائم التي ترتكب على العمليات المعلوماتية والتي تعتمد تقنيا على التشفير والأكواد السرية وإخفاء الهوية وغيرها من طرق طمس الآثار الالكترونية يصعب من خلالها أن ترك آثارا مرئية

[1]– صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجيستير ، تخصص القانون الدولي، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر 2013، ص 119.

[2]– عميمر عبد القادر، التحديات القانونية لاثبات الجريمة المعلوماتية، الناشر الجامعي الجديد، الجزائر، 2021، ص 105.

قد تكشف عنها، أو يستدل من خلالها على الجناة وبذلك يشكل هذا الدليل عائقا أمام رجال التحري والتحقيق خاصة أنهم اعتادوا على الإثبات المادي للجرائم.[1]

- يستخدم مرتكبوا الجرائم المعلوماتية الكثير من الأساليب والتقنيات تسمح لهم بإخفاء كل آثار الجريمة والتستر عنها بسهولة كبيرة، وذلك من خلال إستعمال تقنيات معدة لهذا الغرض مع الأخذ بعين الإعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي يمكن القيام بها في أزمان قياسية تقاس باللحظات والثواني، فمن خلال إدخاله لبعض التعليمات في نظام الحاسوب يتم محو البيانات بالكامل، في لمح البصر كما يمكنه وبمجرد كبسة زر خاطفة على لوحة المفاتيح أن يقوم بإلغاء الأوامر الصادرة للجهاز، [2]على إعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما أن يحس الجاني بأن أمره سينكشف حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبها أمرا في غاية الصعوبة.[3]

كما أن الفاعل في الجرائم المعلوماتية غالبا ما يتخذ الاحتياطات التي تحول دون الوصول إلى كشف الجريمة ومعرفة الفاعل، إذ بإمكانه إتلاف ادلة الادانة في ثوان بواسطة برمجيات خاصة، أو القيام بتشفير التعليمات مما يصعب الوصول إلى دليل يدينه، أو وضع كلمات السر ورموز تحول دون الوصول إلى الدليل.

وترجع صعوبة إثبات الجرائم المعلوماتية بالإضافة إلى ما سبق بيانه إلى الأسباب الآتية:

- نقص الخبرة الكافية لدى رجال الضبطية الذين اعتادوا التعامل مع الجرائم التقليدية.
- صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- صعوبة معرفة الفاعل أحيانا لاستخدامه أساليب التمويه بقصد إخفاء شخصيته، أو يستخدم موقع شخص آخر أو جهة أخرى للقيام بأفعاله الإجرامية.
- إشكالية القانون الواجب التطبيق والمحكمة المختصة.

---

[1]– اسامو حسين محي الدين، حجية الدليل الرقمي في الاثبات الجنائي للجرائم المعلوماتية– دراسة مقارنة– مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، المجلد 11، العدد 2، 2021، ص 707

[2]– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2013، ص 191.

[3]– عميمير عبد القادر، المرجع السابق، ص 109

- إحجام الكثير من المجنى عليهم في التبليغ عن هذه الجرائم، خاصة البنوك والشركات والمؤسسات الادخارية حتى لا يكشف عجزها عن تحقيق الأمان الكافي للمعلومات، وبالتالي الأموال التي تتعامل معها، وعليه تكتفي في أغلب الأحيان باتخاذ إجراءات إدارية داخلية دون الإبلاغ عما تعرضت له السلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.[1]

الفرع الثاني: صعوبة جمع الادلة الإلكترونية على الجرائم المعلوماتية

لا تتوقف صعوبة إثبات الجرائم المعلوماتية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة، بالإضافة على ذلك تمتد إلى الجناة أنفسهم لأن مرتكبي هذا النوع من الجرائم يستخدمون مختلف الوسائل الإلكترونية والبرمجيات التي تساعد على إعاقة الوصول إليهم.[2] ذلك أن مرتكبي الجرم المعلوماتي لا يقدم على أفعاله إلا وهو مؤمن على إخفاء وجوده، فيزيد من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقمنية التي تدينه، [3]

فضلا عما تقدم تواجه عملية الوصول إلى الدليل الرقمي تحديًا إضافيًا يتمثل في لجوء المجرمين إلى دس تعليمات خفية أو استخدام الرمز أو التشفير. يتم ذلك من خلال تشفير المعلومات المخزنة إلكترونيًا أو المنقولة عبر شبكات الاتصال، بحيث لا يمكن قراءتها إلا بواسطة من يملك المفتاح لفك الشفرة. وبالتالي، يصبح الدليل الرقمي مشفرًا أو مرموزًا، مما يشكل عقبة كبيرة أمام الرقابة على البيانات[4].

إذ يُعد استخدام تقنيات التشفير أحد أكبر التحديات التي تواجه جهات التحري والتحقيق والملاحقة، حيث يحد من قدرتها على قراءة البيانات المخزنة أو المنقولة عبر حدود الدولة. هذا الأمر يجعل من صون حرمة البيانات الشخصية، سواءً المخزنة في مراكز الحاسبات والشبكات

[1]- عزيزو لرقط، التعاون الدولي في مكافحة الجرائم المعلوماتية "إشكالاتها وآليات التغلب عليها" مجلة التواصل في الاقتصاد وإدارة القانون، المجلد 25، عدد 04، ديسمبر 2019، ص 4.

[2]– حجازي سهير، التهديدات الإجرامية للتجارة الالكتورنية، مركز البحوث والدراسات بإدارة شرطة دبي، الامارات العربية المتحدة، العدد09، جويلية 1999، ص 5

[3]– سعيداني نعيم، المرجع السابق، ص 192.

[4]– حجازي سهير، المرجع السابق، ص 6

أو المتعلقة بالأسرار التجارية العادية والإلكترونية أو بتدابير الأمن والدفاع، مهمة بالغة الصعوبة.[1]

الفرع الثالث: صعوبة تسليم المجرمين.

إن تسليم المجرمين يعتبر إجراء قضائي في مجال التعاون القضائي الدولي ويقصد به قيام الدولة المطلوب منها بتسليم شخص يتواجد على اقليمها إلى طرف القضائي الدولي أو لدولة الطالبة من أجل محاكمته عن جريمة اتهم بارتكابها، أو من اجل تنفيذ حكم الصادر في حقه من محاكم هذه الدولة أو المحكمة الدولية، [2] ويعتبر التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته تلك ، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية سيما وأن بعض الدول لا تجرم هذه الجرائم،[3] بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بالمعلوماتية أم لا . الأمر الذي يصعب ويعيق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول دون محاسبة مرتكبيها.

[1]– محمود مدين، فن التحقيق والإثبات في الجرائم الإلكترونية، المصرية للنشر والتوزيع، ط1، مصر، 2020، ص 64.

[2]– قارة وليد، مكافحة الجريمة المنظمة العابرة للحدود في التشريع الدولي، ط1، دار الايام للنشر والتوزيع، الاردن،ة ص 399

[3]– لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآليات مكافحتها –دراسة تحليلية مقارنة–، مجلة الميزان، المجلد04، العدد 01، جامعة العلوم الاسلامية العالمية، الاردن، 2017، ص 92.

المبحث الثاني: الآليات المقترحة لحل الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة المعلوماتية.

تتعد الاجراءات وآليات التغلب على مختلف الاشكالات التي تقف عائقا لتحقيق التعاون الدولي لمكافحة الجرائم المعلوماتية، وذلك بناءا على إختلاف الاشكالات المطروحة أمام تحقيق ذلك لذلك سنحاول من خلال هذا المبحث بيان أهم الاليات المقترحة لحل الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة المعلوماتية، في شقها المتعلق بالآليات التنظيمية والقانونية في المطلب الأول وما تعلق أيضا بالشق التقني والفني في المطلب الثاني.

المطلب الأول: الآليات التنظيمة والقانونية

يشكل التنامي الهائل والخطير للجرائم المعلوماتية ضرورة ملحة لمكافحة هذا النوع من الإجرام والذي يتصادم مع إشكالية إختلاف النظم القانونية الاجرائية ، وكذا إشكالية تنازع الاختصاص القضائي تطلب الأمر البحث عن آليات وقنوات مبتكرة وفعالة للحد من هذه الظاهرة وهو ما سنعالجه من خلال هذا المطلب.

الفرع الاول: آليات التغلب على إشكالية إختلاف النظم القانونية الاجرائية

أ- تنسيق عناصر الجرائم التي لها علاقة بالقانون الجنائي الأساسي الوطني والنصوص ذات الصلة بموضوع جرائم الكمبيوتر، ثم توفير للقانون الجنائي الإجرائي الوطني السلطات الضرورية في التحقيق وملاحقة الجرائم المعلوماتية وجرائم أخرى ترتكب بواسطة وسيلة المعلومات أو في إطار يوجد به أدلة إلكترونية[1].

ب- وضع نظام سريع وفعال للتعاون الدولي : حيث تناولت هذه الاتفاقية في قسمها الثاني وصف بعض الإجراءات التي يجب اتخاذها على الصعيد المحلي والتي تخدم التحريات الجنائية التي تجرى حول الجرائم التي ترتكب عن طريق المنظومة المعلوماتية وجمع الأدلة ذات الطابع الإلكتروني والمرتبطة بالجريمة.

[1]- لورنس سعيد الحوامدة، المرجع السابق، ص 134.

لقد ساعدة المواثيق الدولية الصادرة عن هيئة الأمم المتحدة الدول الأطراف لأجل السماح باستخدام بعض تقنيات التحقيقات الخاصة، الشيء الذي يترتب عنه تخفيفا من الاختلافات في الأنظمة القانونية الإجرائية ويفتح المجال أمام تعاون دولي فعال[1].

وعلى هذا الأساس فإن العديد من الاتفاقيات الدولية المبرمة في مجال التعاون الدولي قربت بين القوانين الجنائية الداخلية للدول لأجل مكافحة الجريمة العبارة للحدود ، ويتجسد هذا التقارب من خلال تفويض الاختصاص في اتخاذ إجراءات التحقيق وجمع الأدلة والاعتراف بالأحكام الجنائية الصادرة عن الدول الأخرى.[2]

فقد بينت إتفاقية بودالبست أن أصعب المشاكل في مجال مكافحة الجرائم في عالم الشبكات هو صعوبة تحديد هوية مرتكب الجريمة ومداها وتأثيرها، بالإضافة إلى سرعة إختفاء البيانات الإلكترونية التي يمكن تعديلها ونقلها ومحوها في ثوان معدودة وللتصدي لهذه الصعوبات أقرت هذه الاتفاقية الإجراءات التقليدية لمكافحة الجرائم المعلوماتية في المناخ التكنولوجي الحديث، كإجراء التفتيش والمصادرة، وبالمقابل وضعت إجراءات جديدة لمكافحة الجريمة المعلوماتية وهذه الإجراءات تقوم على مبادئ أساسية هامة هي التزام الدول الأطراف في الاتفاقية بإقرار الإجراءات التشريعية وإجراءات أخرى إذا استلزم الأمر بما يتناسب مع القانون الداخلي الخاص بها، وإطارها القضائي، من أجل وضع الصلاحيات والاجراءات المنصوص عليها لخدمة التحريات والاجراءات الجنائية الخاصة.[3]

ونصت الاتفاقية في المادة 31 عن إمكانية الولوج إلى البيانات والمعلومات المحفوظة في النظام المعلوماتي عن طريق السماح للدولة الطالبة للقيام بالتفتيش والدخول بطريقة مشابهة وضبط أو الحصول بطريقة مماثلة على البيانات والمعلومات المخزنة بواسطة شبكة المعلومات داخل النطاق المكاني للدولة المطلوب منها المساعدة، ويجب الاستجابة على وجه السرعة لهذا

[1]– عبد الفتاح بيومي حجازي، الدليل الجنائيي والتزوير في جرائم الكمبيوتر والانترنت، بهجات للطباعة والتجليد، مصر، 2009، ص 38.

[2]– خراشي عادل عبد العال ابراهيم ، إشكالية التعاون الدولي في مكافحة الجرائم الملعوماتية، دار الجامعة الجديدة، الاسكندرية، 2015، ص 64

[3]– طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير، تخصص: القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011–2012، ص 100.

الطلب إذا ما كانت هناك أسباب تدعو للاعتقاد بأن المعلومات والبيانات المعنية عرضة لمخاطر المحو والفقد أو التعديل، وكذلك الحالة التي توجد فيها اتفاقيات أو معاهدات تنص على التعاون الفوري. [1]

وفي الأخير فإن المادة 35 تناولت إنشاء شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة والتي يطلق عليها الشبكة 24/7 بمعنى تلك الشبكة التي تعمل على مدار 24 ساعة يوميا بمعدل سبع أيام في الأسبوع، لغرض التأكد من توفير المساعدة الفورية لإجراء التحقيقات المتعلقة بالجرائم المرتبطة بنظام وبيانات معلوماتية، أو لتجميع أدلة ذات شكل إلكتروني لجريمة ما، وهذه المساعدة يجب أن تكون مشتملة على تسهيل، وتعتبر هذه الوسائل من أفضل آليات التغلب على التحديات الكبيرة التي يفرضها عصر المعلوماتية على السلطات المناط بها تنفيذ القانون.[2]

الفرع الثاني: التعاون القضائي

إن حل إشكالية تنازع الاختصاص يكمن في اعتبار الجرائم المعلوماتية من الجرائم العالمية، أين يرجع فيها الاختصاص القضائي لكل دولة تنص قوانينها الداخلية على هذه الجرائم اعتمادا على مبدأ العالمية، الذي مفاده سريان قانون عقوبات الدولة بغض النظر عن مكان ارتكاب الجريمة أو جنسية مرتكبها، ودون النظر فيما إذا كان القانون الأجنبي يعتد بها كجريمة أم لا.

ويهدف مبدأ العالمية إلى التصدي لتنامي الظاهرة الإجرامية ذات الأبعاد الدولية، من خلال تجاوز القيود التي يفرضها مبدأ الإقليمية، كما يؤسس هذا المبدأ لفكرة التضامن بين الدول في مكافحة الجرائم المعلوماتية لأن التدخل الدولي وفقا لهذا المبدأ يحقق معاقبة الجناة وعدم إفلاتهم وضمان محاكمتهم بغض النظر عن جنسيتهم أو جنسية ضحاياهم. وفي هذا الصدد لا بد ان يقوم التعاون القضائي على:

[1]– محمود أحمد عبابنة جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الاردن، 2005، ص 176

[2]– هلالي عبد الله أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية "معلقا عليها"، ط1، دار النهضة العربية، مصر، 2007، ص 318

- **تبادل المعلومات**

ويشمل تقديم المعلومات والوثائق التي تتطلبها سلطة قضائية أو أمنية أجنبية، متى كانت بصدد جريمة ما عن الإتهامات التي وجهت الى رعاياها في الخارج، والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل أيضا السوابق القضائية للجناة، تتعرف من خلاله الجهات القضائية على الماضي الجنائي للفرد المحال اليها، لتقرير الاحكام الخاصة بالعود ووقف تنفيذ العقوبة وغيرها من الإجراءات .

- **نقل الإجراءات:**

أقرت هذه الصورة من المساعدة القضائية العديد من الإتفاقيات الدولية، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، وإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية المبرمة عام 2000 وفي المادة 21 منها ، ومعاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لعام 1999 وفي المادة 09 منها.

وتتجسد هذه الصورة بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية بصدد جريمة في إقليم دولة أخرى ولمصلحة هذه الأخيرة، وذلك بتوافر شروط معينة كالتجريم المزدوج، وأن تؤدي الإجراءات المطلوب إتخاذها دورا مهما في الوصول الى الحقيقة . 3

- **الإنابة القضائية:**

تعبر الإنابة القضائية عن قيام دولة ما عبر أجهزتها المختصة بأعمال قضائية محددة لمصلحة دولة أخرى وبطلب منها بخصوص ناشئة عن جريمة لدى الجهات القضائية للدولة الطالبة ،[1] والتغلب على عقبة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى كإجراء التفتيش والضبط والمعاينة، وتماشيا مع سرعة الجريمة الإلكترونية وتجنبا لطول إجراءات طلب الإنابة القضائية الدولية، فقد أبرمت العديد من الإتفاقيات الجديدة التي ساهمت في إختصار الإجراءات عن طريق الإتصال المباشر بين

[1]– نسيب نجيب، التعاون القانوني والقضائي الدولي في ملاحقة مرتكبي جرائم الإرهاب، مركز الكتاب الاكاديمي، الاردن ، 2020، ص 151.

السلطات المعنية بالتحقيق، كالإتفاقية الأمريكية الكندية، التي تنص على إمكانية تبادل المعلومات شفوياً في حالة الاستعجال.[1]

المطلب الثاني: الأليات التقنية والفنية

إن الصعوبات التي ترتبط بشكل وثيق بطبيعة الجرائم المعلوماتية تلك المتعلقة بالجوانب التقنية والفنية والتي تتطلب إلماما وتخصصا في كيفية التعامل مع البرمجيات الحاسوبية وفهم عميق لآليات عملها، بالاضافة إلى تكثيف تبادل الخبرات بين مختلف الاجهزة للتمكن من بناء شبكة متينة من الخحبرات التي تسهم بشكل فعال في تقوية التعاون الدولي لمكافحة الجريمة المعلوماتية.

الفرع الأول: تبادل المعلومات والخبرات بين الجهات المختصة في مختلف الدول

لابد أن تكون أجهزة العدالة على مختلف أنواعها على درجة عالية من الكفاءة والمعرفة والقدرة على كشف غموض الجرائم المعلوماتية والتعرف على مرتكبيها بسرعة ودقة متناهية، وهذا لن يتحقق إلا بالتدريب،[2] حيث لا يمكننا أن نغفل موضوع تدريب رجال العدالة، والذي يعد مظهراً من مظاهر التعاون الدولي، فنقل التجارب وإكساب رجال العدالة الخبرة الفنية عبر تدريب تخصصي يراعي فيه العناصر الشخصية للمتدربين من حيث توافر الصلاحية العلمية والقدرات الذهينة والنفسية لتلقي التدريب، ويلاحظ هنا أنه من الأسهل تدريب متخصص في تكنولوجيا المعلومات وشبكات الاتصال بدلا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلي الإدعاء العام.[3] ويذهب بعض الخبراء إلى أنه يجب أن تتوافر لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي[4]. وبالنسبة للمنهج التدريبي فيجب أن يشتمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة

[1]– عبد الحليم بوشكيوه، آليات مكافحة الجرائم الماسة بالاخلاق والآداب العامة على الانتترت، مجلة دراسات أبحاث،المجلد01، العدد01، 2009، ص 25.

[2]– هشام محمد فريد رستم، الجرائم المعلوماتية –أصول التحقيق الجنائي الفني"، حث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد 02، ط 03، 2004، ص 588.

[3]-

[4] هشام محمد فريد رستم،المرجع السابق،ص 496

المعلومات وأجهزة الحاسب الآلي مع ذكر لمفاهيم معالجة البيانات وتحديد نوعية و أنماط الجرائم المعلوماتية ، و بيان لأهم الصفات التي يتميز بها المجرم المعلوماتى ، والدوافع وراء ارتكاب الجرائم المعلوماتية.

وفيما يتعلق بمنهج التحقيق فإنه لا بد وأن يشتمل على[1]:

- إجراءات التحقيق ،
- التخطيط للتحقيق ،
- تجميع المعلومات وتحليلها،
- أساليب المواجهة والاستجواب ،
- مراجعة النظم الفنية للبيانات ،
- أساليب المخبر الجنائي.

بالإضافة إلى ذلك لا بد وأن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الكمبيوتر كأداة للمراجعة والحصول على أدلة الاتهام وما يخص الملاحقة الدولية والتعاون المشترك.[2]

وفي هذا الصدد فقد تم تخصيص عدة برامج لهذا الموضوع، فعملية التدريب تفيد المتدرب في زيادة مهاراته ومعلوماته وقدراته على التعامل مع الأجهزة الدولية الأخرى، الأمر الذي ينعكس على الجهة التي ينتمي إليها بالفائدة، ونذكر هنا تجربة الولايات المتحدة الأمريكية في هذا المجال كونها تعد من بين الدول المتقدمة في مجال مكافحة الجرائم الإلكترونية، كما أنها تعلم أن مواجهة هاته الجرائم لا يمكن أن تتم بشكل فعال دون أن يكون هنالك تعاون دولي في سبيل ذلك، لذا نجدها حريصة على تقديم المساعدة التقنية والتدريب لرفع قدرات رجال العدالة الجنائية من مسؤولي الإدعاء العام، والقضاة، وأجهزة تطبيق القانون الأمريكية، وفي سبيل ذلك قامت بتنظيم دورات تدريبية لنظيراتها من الأجهزة في البلدان الأخرى، وأنشات معاهد خاصة لتدريب العاملين بتلك الأجهزة، يتم فيها اطلاعهم على أساليب مبتكرة للتحقيق والتحري وتبادل الآراء والخبرات مع نظرائهم في مختلف الدول؛ ولتحقيق نتائج جيدة فقد أوكلت المهمة

[1] نفس المرجع،ص 497.

[2]– فراحتية خلود، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر، تخصص: قانون إعلام آلي وأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، 2022/2021، ص 20.

لعدة أجهزة، نذكر منها مكتب المساعدة والتدريب الذي يعمل على تطوير أجهزة الادعاء العام في الخارج، التابع لوزارة العدل الأمريكية، والمكلف بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى، وتعزيز إدارة القضاء في الخارج.[1]

بالاضافة للبرنامج الدولي للمساعدة والتدريب على التحقيق الجزائي(ICITAP) ، والذي يعمل على توفير مساعدات لأجهزة الشرطة في البلدان النامية في مختلف أنحاء العالم، لتعزيز القدرات التحقيقية لديها، كما تقوم الولايات المتحدة الأمريكية بتقديم المساعدة لتطوير القطاع القضائي في عدد من البلدان في إفريقيا وآسيا وأوربا الشرقية والوسطى، وأمريكا اللاتينية، وروسيا، والشرق الاوسط، ومنطقة حوض الكاريبتي[2].

ولأن معظم الدول أصبحت تعي ما للعملية التدريبية من دور في تسهيل عملية البحث عن الجرائم الإلكترونية والقبض على مرتكبيها وتقديمهم للعدالة، فقد عمدت إلى القيام بتلك الدورات التدريبية بصفة دورية في عدة قطاعات وأجهزة الأمنية منها والقضائية، منتقية منها أهم العناصر الذين تتوفر فيهم القدرات العقلية والعلمية والتقنية، وكذا تحفيز البحث والاطلاع.

الفرع الثاني: الدعوة لإنشاء محكمة جنائية دولية للجرائم المعلوماتية.

يتبين لنا من خلال ما سبق أن البعد الدولي للجرائم المعلوماتية يستدعي تنظيم تعاون دولي في سبيل مكافحتها، كالمساعدة الدولية بين أجهزة الشرطة الدولية "الانتربول" لمتابعة المجرمين والقبض عليهم،[3] إضافة إلى تنظيم تعاون على مستوى أجهزة التحقيق (النيابة العامة) وأجهزة المحاكمة، بحيث يتم الإعتداد بأعمال التحقيق والمحاكمة التي تجري في دولة معينة من الدول الأخرى في مجال هذا النوع من الجرائم، عملاً بمبدأ عالمية النص الجنائي وتفادياً لكل للعراقيل التي من شأنها عرقلة آليات التعاون الدولي. ولأجل مكافحة أفضل ومحاكمة أسرع وأوسع نطاقاً واختصاصاً، وتخفيفاً من الفوارق الموجودة بين الأنظمة العقابية الداخلية، دعا معظم رجال القانون إلى إنشاء محكمة مختصة بالجرائم المعلوماتية ذات طبيعة إليكترونية،

[1]– أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دمتوراه، تخصص: قانون خاص، جامعة محمد البشير الابراهيمي ، برج بوعريريج، الجزائر، 2020–2021، ص ص 109–111

[2]

[3]- محمد سامي عبد الحميد، أصول القانون الدولي العام، الجماعة الدولية، ج1، مؤسسة الثقافة الجامعية، الاسكندرية، 1979، ص 159

وهذا لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، كون التعاون الدولي أصبح حتمية يفرضها الواقع بالإضافة إلى خطورة هذه الجريمة[1].

فالتقاضي الإلكتروني هو تلك السلطة الممنوحة لمجموعة متخصصة من القضاة النظاميين بنظر الدعوى ومباشرة الإجراءات القضائية بوسائل إلكترونية مستحدثة، ضمن نظام أو أنظمة قضائية معلوماتية متكاملة الأطراف والوسائل، تعتمد منهج تقنية شبكة الربط الدولية (الإنترنت) وبرامج الملفات الحاسوبية الإلكترونية بنظر الدعاوى والفصل بها وتنفيذ الأحكام بغية الوصول الفصل سريع بالدعاوى والتسهيل على المتقاضين، فإنشاء محكمة رقمية (Digital Court)المحكمة التي تختص بالجرائم الرقمية Digital crime هو أمر يجب أن تسعى فيه كل الدول بمساعدة الأمم المتحدة وتحت رعايتها، حتى يتم إنشاء محكمة جنائية دولية للجرائم الإلكترونية تنظر في الجرائم الخطيرة؛ كالإرهاب الإلكتروني والحروب الإلكترونية، والجرائم المتعلقة بالفساد وغسيل الأموال المرتكبة عبر الوسائط المعلوماتية، وكذا الجرائم المرتكبة ضد الأطفال بصفتهم فئة ضعيفة تحب حمايتها وغيرها من الجرائم الخطيرة التي يحب ملاحقة مرتكبيها والعمل على عدم إفلاتهم من 5

العقاب.[2]

إن إلى إنشاء محكمة افتراضية، هي فكرة تم إرساء دعائمها في شهر مارس سنة 1996، بهدف إعطاء حلول سريعة للمنازعات المتعلقة بالإنترنت عن طريق وسيط معتمد من المركز تكون له الخبرة القانونية في الفصل في المنازعات الإلكترونية، ودراية بالقوانين الناظمة للتجارة الإلكترونية وعقودها، وقانون الإنترنت ومنازعات العلامات التجارية والملكية الفكرية، وغيرها من المواضيع المتصلة بالتجارة، حيث تفصل المحكمة الافتراضية في النزاع خلال 72 ساعة،[3] ويكون حكمها نهائياً غير قابل للاستئناف ؛ لأن موافقة الأطراف عليه هي التي تعطيه القوة القانونية، كما تم إنشاء محكمة فضائية في كلية الحقوق بجامعة مونتريال بكندا في شهر سبتمبر سنة 1996 من قبل باحثين بقسم القانون العام الكندي، والتي كانت تهدف إلى تطوير

[1]- محمد منصور الصاوي، احكام القانون الدولي المتعلقة بمكافحة الجرائم ذات الطبيعة الدولية، دار المطبوعات الجامعية، الاسكندرية، دون سنة نشر، ص 674 .

[2]- شنتير خضرة، الاليات القانونية لمكافحة الجريمة الالكترونية (دراسة مقارنة)، أطروحة دكتوراه، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية ، أدرار، 2021/2020، 240.

[3]- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية ، القاهرة 2002 ص 176.

قواعد التنظيم الذاتي الخاص بالإنترنت ومراقبة التطبيق الفعلي لهذه القواعد، وحل المنازعات التي تنشأ عن طريق شبكة الإنترنت، حيث تختص في المنازعات الناشئة عن التجارة الإلكترونية المنافسة حق المؤلف حرية التعبير، الحياة الخاصة[1].

ومن المؤكد أن مثل هذه المحاكم سوف يذلل العديد من الصعاب التي كانت تواجه المتقاضين ومنها مشكلة المحكمة المختصة، وطول الإجراءات، ولكن المحكمة التي نتمنى أن يتم إنشاؤها هي محكمة جنائية دولية متخصصة إلكترونية تكون من ضمن هياكل الأمم المتحدة وتحت إشرافها تشارك في إنشائها كل الدول المنضمة لهذه الهيئة، يخصص لها طاقم من القضاة المتخصصين في مثل هذه القضايا، خاصة وأننا نعلم أنه من بين الصعوبات التي تواجه مكافحة هذه الجريمة الخطيرة قلة القضاة المتخصصين، وكذا المحامين؛ لأن هناك اتجاه قوي بين المتخصصين ورجال القانون ينادي بضرورة عقد دورات تدريبية لرجال القانون الدراسة قانون الحاسبات وتقنيته في المعاهد المتخصصة على أن تكون هذه الدراسات نصف سنوية أو سنوية على أقصى حد.[2]

[1]- شنتير خضرة، نفس المرجع ، ص 241.
[2]- شنتير خضرة، المرجع السابق، ص 242.

خلاصة الفصل:

من خلال ما سبق يتضح أنه بالرغم من الجهود المبذولة لتعزيز التعاون الدولي في مكافحة الجريمية المعلوماتية، إلا أن هناك العديد من الصعوبات التي تعترض هذا التعاون والتي تتمحور بالاساس حول أختلاف الانظمة القانونية بين الدول وهو ما من شأنه إعاقة تبادل المساعدة القانونية المتبادلة كما أن بعض الدول تفتقر إلى الموارد والخبرات اللازمة لمكافحة الجريمة المعلوماتية بشكل فعال، وما تطرحه إشكالات التعارض مع السيادة الوطنية والاختصاص القضائي، ما يحيل التعاون الدولي إلى ضرورة البحث عن آليات أكثر فعالية بما يتجاوز الصعوبات المطروحة أما تعاون دولي لمكافحة الجريمة المعلوماتية بشكل فعال.

الخاتمــة

الخاتمــة :

نخلص في نهاية دراستنا هذه إلى أن الجرائم المعلوماتية تعتبر من أخطر الجرائم التي نشأة نتيجة التطور الهائل في تكنولوجيات المعلومات والاتصالات الحديثة، ولطبيعة هذه الجرائم الخاصة والتي تختلف عن الجرائم العادية لتعقدها ولصعوبة التعامل معها بالآليات التقليدية وهو ما شكل أعباء وتحديات بالنسبة للدول إستدعى ضرورة التعاون وتظافر الجهود الدولية لمكافحتها، كما يضح لنا أن آليات التعاون الدولي تلعب دورًا حيويًا في مكافحة الجريمة المعلوماتية. فمن خلال تبادل المعلومات والتنسيق بين الدول، يتم تعزيز قدرات الأجهزة الأمنية على التصدي لهذه الجرائم المتطورة، وتسهم الاتفاقيات الدولية والإقليمية في توحيد الجهود وتبادل الخبرات، مما يؤدي إلى تحسين كفاءة المتابعة والتحقيق.

وعلى الرغم من التحديات القائمة كاختلاف القوانين وتفاوت القدرات التقنية بين الدول، فإن التعاون الدولي يظل أداة فعالة في مواجهة التهديدات السيبرانية. لتحقيق المزيد من النجاح الأمر الذي يتطلب تعزيز هذه الشراكات وتطوير الأطر القانونية والتقنية لضمان عالم رقمي أكثر أمنا.

وقد توصلنا من خلال دراستنا إلى مجموعة من النتائج والتي كانت إجابة عن الاشكالية التي طرحناها سابقا وهي كالتالي:

- تأخذ الجريمة الالكترونية أبعادا خطيرة تتصل بأمن الافراد والمؤسسات ويمكن أن تهدد أمن الدولة كذلك كونها تعتمد على التقنيات الحديثة وتتجاوز في مداها حدود الدولة الوطنية فهي عابرة للحدود وتتميز بتعقد ظروفها وصعوبة إكتشافها وإثباتها أجرائيا.
- يعد مبدأ التعاون الدولي في العالم المعاصر من أهم المبادئ القانونية الدولية ، وقد ظهرت أهمية هذا المبدأ في مجال مكافحة الجريمة مع تعدد وتشعب التطورات التي لحقت بظاهرة الجريمة وأساليب ارتكابها.
- تعتبر الحدود الإقليمية عائقا أمام تعاون الدول في مجال مكافحة الجريمة وما يترتب عنه من إفلات لمرتكبي الجرائم ما يشجعهم على ارتكاب المزيد.

- يستحيل القضاء على ظاهرة الإجرام الالكتروني بشكل نهائي، خاصة كونها قد تحدث من بلد و تقع آثارها في بلد آخر، وهو ما يستلزم فكرة التعاون الدولي وتجاوز فكرة الحدود دون المساس بالسيادة الإقليمية.
- إن التعاون الدولي لمكافحة الجريمة الالكترونية من خلال الاتفاقيات الدولية من شأنه أن يحد من أخطار هذه الجريمة و يطوقها.
- اختلاف النظم القانونية من دولة لأخرى يحول دون التعاون الدولي في مكافحة الجريمة الالكترونية فما يجرم في بلد ما لا يكون في أخرى.

- **الاقتراحات:**

من خلال الملاحظات السابقة الذكر ارتأينا ، وبناء على كل ما استعرضناه وضع مجموعة من التوصيات التي تساهم في حل الإشكاليات والعوائق التي صادفتنا في مجال البحث ولتكون إسهاما علميا واضحا، و التي تتمثل فيما يلي:

- يجب تشجيع المساعدة المتبادلة بين سلطات الشرطة الجنائية في حدود القوانين المعمول بها.
- جمع المعلومات المتعلقة بالمجرمين و الجرائم عبر أقاليم الدول الأعضاء لتكوين قواعد بيانات مشتركة يمكن الرجوع إليها بسهولة.
- ضرورة التعاون الدولي لا يشمل المساعدة القضائية فقط و إنما يحتاج للمساعدة التقنية وتبادل الخبرات بين الدول خاصة وأن بعض الدول قطعت أشواط لابأس بها في اكتساب تقنيات البحث والتحري وغيرها من الآليات المساعدة في مكافحة الجرائم المعلوماتية.
- إنشاء دورات تكوينية للمحققين والقضاة في مجال نظم المعلوماتية والحواسيب، فدور القاضي مهم في توجيه مسار القضايا، فإذا كان القاضي غير ملم بالجوانب الفنية للتقنية الحديثة فانه لا يستطيع تقدير مدى خطورة المجرم المعلوماتي، وهذا يؤثر على الحكم عليه كان يصدر في حقه حكم غير متكافئ مع الجريمة المرتكبة.

- دور المحقق مرتبط فقط بالتحقيق في الجرائم المذكورة على سبيل الحصر في التشريعات الوطنية وكما ذكر سابقاً فالجرائم في تطور مستمر مما يجعل القوانين التقليدية غير كافية.
- إعتماد مرتكبي الجرائم المعلوماتيةبدرجة عالية على الوسائل والتقنية الحديثة ولان الإجراءات التقليدية غير كفيلة بمكافحة هذه الجرائم فينبغي على المشرع وضع إجراءات حديثة تعتمد على ذات الوسائل المستخدمة في الجريمة للكشف عنها وتتبع فاعليها.
- ينبغي على كافة الدول وضع نظام مراقبة عبر شبكة الانترنت يسمح بتتبع الملفات المدخلة والمخرجة، وتعقب الاختراقات غير المشروعة للأنظمة وتخريبها وملاحقة مرتكبيها، وهو ما من شأنه تشكيل آلية لرصد وتتبع وإثبات وقوع الجرائم المعلوماتية.
- العمل على التحسيس بخطورة الجريمة الالكترونية على الأمن العام، و أمن الأفراد وإستحداث برامج خاصة بتكوين الناشئة على الأمن السيبراني على غرار ماهو معمول به في بعض الدول المتقدمة وذلك من خلال إدراج مفهوم الجريمة المعلوماتية ضمن المقررات الدراسية.

قائمة المراجع

قائمة المراجع

أولا: النصوص القانونية:

1- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مشروع إعلان منتدى التعاون العربي الصيني، جامعة الدول العربية، 2010/12/21

2- اتفاقية برن بشان حماية المصنفات الأدبية والفنية لسنة 1886، المنظمة العالمية للملكية الفكرية، تاريخ الاطلاع، 2024/03/28 على الرابط:
https://www.wipo.int/treaties/ar/gip/berne/summary_berne.html

3- التعليم من أجل العدالة ، سلسلة الوحدات الجامعية: الجرائم الالكترونية، الوحدة السابعة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بتاريخ: 2024/03/23 على الرابط:
https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

4- اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 أكتوبر سنة 2003.

5- مكتب الامم المتحدة المعني بالمخدرات والجريمة ، 2013.

التقارير:

6- تدابير مكافحة الجرائم المتصلة بالحواسيب – مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية المنعقد في بانكوك في الفترة 18 إلى 2005/4/25م – وثيقة رقم A/CONF.203/14

7- تقرير الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، الأمم المتحدة، بانكوك، 18-25 أبريل 2005.

8- لجنة منع الجريمة والعدالة الجنائية، الدورة السادسة، آراء الولايات المتحدة الأمريكية بشأن أكبر الوسائل فعالية لاجراء منع الجريمة والعدالة الجنائية، المجلس الاقتصادي والاجتماعي، نيويورك، 1997.

ثانيا :الكتب

9- أسامة حسين، الاحتيال الإلكتروني، زهران للنشر، الطبعة الأولى، الاردن، 2011.

10- جميل عبد الباقي الصعير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ط1، القاهرة، 2002.

11- خراشي عادل عبد العال ابراهيم ، إشكالية التعاون الدولي في مكافحة الجرائم الملعوماتية، دار الجامعة الجديدة، الاسكندرية، 2015.

12- الزعبي جلال محمد والمناعسة أسامة محمد، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة، ط1، عمان، 2013.

13- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولويا المعلومات، دار النهضة العربية، ط1، 1999.

14- سليمان أحمد فضل المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهر، مصر، 2013.

15- عادل عبد العال ابراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، جامعة الأزهر، مصر، 2015.

16- عبد الفتاح بيومي حجازي، الاثبات الجنائي في جرائم الكمبيوتر والانتترت، دار الكتب القانونية، 2007،.

17- عبد الفتاح بيومي حجازي، الأحداث والانترنت دراسة معمقة عن أثر الانترنت في انحراف الأحداث، دار الكتب القانونية، 2010.

18- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية ، القاهرة 2002.

19- عبد الفتاح علي، مكافحة الجرائم الاكترونية بين نظم المعلومات والإعلام البديل، مكتبة الوفاء القانونية، الاسكندرية، ط1، 2017.

20- عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، منشأة المعارف، القاهرة، 1998.

21- علي حسن الطوالبة، أبحاث في جرائم تقنية المعلومات (التعاون القضائي الدولي لمكافحة الجريمة المعلوماتية)، دار الكتب والدراسات العربية، دون سنة،

22- علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، ط1، 2011.

23- عميمر عبد القادر، التحديات القانونية لاثبات الجريمة المعلوماتية، الناشر الجامعي الجديد، الجزائر، 2021.

24- قارة وليد، مكافحة الجريمة المنظمة العابرة للحدود في التشريع الدولي، ط1، دار الايام للنشر والتوزيع، الاردن.2013.

25- محمد سامي عبد الحميد، أصول القانون الدولي العام، الجماعة الدولية، ج1، مؤسسة الثقافة الجامعية، الاسكندرية، 1979.

26- محمد فاضل، التعاون الدولي في مكافحة الإجرام، جامعة دمشق، كلية الحقوق، 2012.

27- محمد فتحي محمد أنور، تفتيش شبكة الانترنت، لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، مصر ، 2010.

28- محمد محمد شتا، الحماية الجنائية لبرامج الحاسوب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001.

29- محمد منصور الصاوي، احكام القانون الدولي المتعلقة بمكافحة الجرائم ذات الطبيعة الدولية، دار المطبوعات الجامعية، الاسكندرية، دون سنة نشر.

30- محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية (دراسة مقارنة)، ط 1، مركز الدراسات العربيةمصر، 2016.

31- محمود أحمد عبابنة جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الاردن، 2005.

32- محمود مدين، فن التحقيق والإثبات في الجرائم الإلكترونية، المصرية للنشر والتوزيع، ط1، مصر، 2020.

33- نسيب نجيب، التعاون القانوني والقضائي الدولي في ملاحقة مرتكبي جرائم الإرهاب، مركز الكتاب الاكاديمي، الاردن ، 2020.

34- عبد الفتاح بيومي حجازي، الدليل الجنائيي والتزوير في جرائم الكمبيوتر والانترنت، بهجات للطباعة والتجليد، مصر، 2009.

35- هلالي عبد الله أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية "معلقا عليها"، ط1، دار النهضة العربية، مصر، 2007.

ثالثا: الرسائل العلمية

36- أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه، تخصص: قانون خاص، جامعة محمد البشير الابراهيمي، برج بوعريريج، الجزائر، 2020-2021.

37- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي، أطروحة دكتوراه، تخصص: قانون عام ، كلية الحقوق، جامعة الجزائر، يوسف بن خدة، السنة الجامعية 2017-2018.

38- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، أطروحة دكتوراه، قسم الحقوق، جامعة عين شمس، مصر ، 2007.

39- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2013/2012.

40- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2013.

41- شنتير خضرة، الاليات القانونية لمكافحة الجريمة الالكترونية (دراسة مقارنة)، أطروحة دكتوراه، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية ، أدرار، 2021/2020.

42- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، رسالة ماجيستير ، تخصص القانون الدولي، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر 2013.

43- طرشي نورة، مكافحة الجريمة المعلوماتية، رسالة ماجستير، تخصص: القانون الجنائي، كلية الحقوق، جامعة الجزائر1، 2011-2012.

44- فراحتية خلود، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر، تخصص: قانون إعلام آلي وأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، 2022/2021.

رابعا: المقالات العلمية

45- آمال جحيج، نحو قوة أورو- متوسطية للشرطة وتسيير الحدود، مجلة دفاتر السياسة والقانون، العدد 12، جانفي 2015.

46- أيمن سلامة، لماذا يصعب التعاون الدولي في مجال مكافحة الجريمة السيبرانية؟، مقال منشور على موقع سكاي نيوز، 3 يوليو 2021، اطلع عليه بتاريخ: 2024/04/18: على الرابط: https://www.skynewsarabia.com/blog/1448837

47- بن دراج علي إبراهيم، محاضرات في الجرائم المعلوماتية، تخصص القانون الجنائي والعلوم الجنائية، معهد الحقوق والعلوم السياسية، المركز الجامعي آفلو، الجزائر، **2021**.

48- حجازي سهير، التهديدات الإجرامية للتجارة الالكتورنية، مركز البحوث والدراسات بإدارة شرطة دبي، الامارات العربية المتحدة، العدد09، جويلية 1999.

49- سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، بحث مقدم إلى مركز البحوث والدراسات، كلية الشريعة والقانون - جامعة الامارات العربية المتحدة، 2000.

50- عبد الحليم بوشكيوه، آليات كافحة الجرائم الماسة بالاخلاق والآداب العامة على الانتنرت، مجلة دراسات أبحاث،المجلد01، العدد01، 2009.

51- قدوس خديجة ، عمتوت كمال، انتهاكات حقوق الانسان في ظل انتشار الجريمة الالكترونية، مجلة التدوين، المجلد 12، العدد 02، 2020.

52- قطاف سليمان وبوقرين عبد الحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الاول، 2022/03/31.

53- لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآليات مكافحتها –دراسة تحليلية مقارنة، مجلة الميزان، المجلد04، العدد 01، جامعة العلوم الاسلامية العالمية، الاردن، 2017.

54- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الالكتورنية، المجلة الاكاديمية للبحث القانوني، المجلد 14، العدد 2016/02.

55- محي الدين اسامة حسين ، حجية الدليل الرقمي في الاثبات الجنائي للجرائم المعلوماتية– دراسة مقارنة– مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، المجلد 11، العدد 2، 2021،

56- هشام محمد فريد رستم، الجرائم المعلوماتية –أصول التحقيق الجنائي الفني"، حث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد 02، ط 03، 2004.

بحوث مؤتمرات وندوات:

57- أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة عمل، مقدمة في المؤتمر المغارب الأول حول (المعلوماتية والقانون)، أكاديمية الدراسات العليا، طرابلس خلال الفترة 28-2009/10/29.

58- حسين جميعي، الاطار القانوني الدولي لحماية حق المؤلف والحقوق المجاورة، ندوة الويبو الوطنية عن إنفاذ حقوق الملكية الفكرية للقضاة والمدعين العامين، المنظمة العالمية للملكية الفكرية (الويبو) بالتعاون مع وزارة الاعلامن مملكة البحرين، 2004.

59- عماد علي الخليل، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3 مايو 2000.

60- موسى مسعود ارحومة، الاشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية،المؤتمر المغاربي الاول حول المعلوماتية والقانون، اكادينية الدراسات العليا، طرابلس، خلال الفترة 28-2009/10/29.

61- هاني فتحي جورجي، ورقة عمل بعنوان، "دور النيابة العامة المصرية في مكافحة الجريمة المنظمة عبر الوطنية والاتجار في الافراد، الدورة التدريبية الرابعة عشر لمنع الاتجار بالأطفال الضابط امن الموانئ بالتعاون مع وزارة الداخلية، ماي 2009.

62- آليات التعاون الدولي الرسمية، مكتب الامم المتحدة المعني بالمخدرات والجريمة، الوحدة التعليمية7، التعاون الدولي على مكافحة الجريمة الالكترونية، يوليو 2021، اطلع عليها بتاريخ، 2024/03/26 على الموقع: https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

فهرس المحتويات

ملخص الدراسة:

تأخذ مكافحة الجريمة المعلوماتية حيزا مهما ضمن إهتمامات الدول فبالنظر الى الطبيعة الخاصة للجرائم المعلوماتية التي تنشأ وتقع ضمن بيئة رقمية إفتراضية عابرة للحدود، فإن ضرورات التعاون والتنسيق الدولي في سبيل مكافحتها يجب أن تعتمد على آليات متطورة، ولها من القدرة ما يجعل إنفاذ القانون يحول دون إفلات المجريمن من العقاب، وتحقيق التوازن بين أطراف العلاقة التعاونية على المستوى الدولي، فلم يعد بإمكان الدولة بمفردها مهما كانت الوسائل التي تحوزها أن تتصدى للجريمة المعلوماتية بشكل كاف وفعال، من غير أن تعتمد على آليات التعاون الدولي.

الكلمات المفتاحية: **الجريمة المعلوماتية، التعاون الدولي، آليات مكافحة.**

Abstract:

Cybercrime has emerged as a prominent concern for nations worldwide. Owing to the unique nature of cybercrimes that originate and occur within a borderless virtual digital environment, the imperatives of international cooperation and coordination in combating them must rely on sophisticated mechanisms that empower law enforcement to prevent criminals from evading punishment and achieve balance among the parties to the cooperative relationship at the international level. A state, on its own, regardless of the means it possesses, can no longer adequately and effectively combat cybercrime without relying on international cooperation mechanisms.

Keywords: Cybercrime, International Cooperation, Anti-Cybercrime Mechanisms

.