وزارة التعليم العالي و البحث العلمي
جامعة عباس لغرور خنشلة
كلية الحقوق و العلوم السياسية

مذكرة مكملة لنيل شهادة الماستر في شعبة حقوق

تخصص : قانون جنائي و علوم جنائية

عنــوان المذكـرة

التعاون الدولي في مكافحة الجرائم السيبرانية

- **إعداد الطلبة**

قتوم عبد اللطيف

طلاطة رضا

إشراف الدكتور :

زمورة داود

أعضاء لجنة المناقشة

الاسم و اللقب	الرتبة العلمية	الجامعة الأصلية	الصفة
بن مكي نجاة	أستاذ التعليم العالي	جامعة عباس لغرور– خنشلة	رئيـــسًا
كواشي نجوى	أستاذ محاضر–أ –	جامعة عباس لغرور– خنشلة	عضوًا ممتحنًا
زمورة داود	أستاذ محاضر –أ–	جامعة عباس لغرور– خنشلة	مشرف و مقررًا

السنــة الجامعيــة :

2025/2024


بسم الله الرحمن الرحيم

و قل ربي زدني علمًا

الله نُور السَّمَاوَاتِ وَ الأَرْض مَثَلُ نُورِهِ كَمِشْكَاةٍ فِهَا

مِصْبَاحٌ الْمِصْبَاُحُ فِي زُجَاجَةِ الزُجَاجَةً كَأَنَّها كَوْكَبٌ

دُرِّيٌّ يُوقَدُ مِن شَجَرةٍ مُباركةٍ زَيْتُنَةٍ لاَّ شَرْقية ولا غربية

يَكَادُ زَيْتُهَا يُضِيءُ وَلَوْ لَمْ تَمْسَسهُ نَارٌ نُّورٌ عَلى نُورٍ

يهْدِي الله لنُورِهِ مَن يَشاءُ و يضْربُ الله الأمْثَال للنّاس

والله بِكُلِّ شيئ عليمٌ

صدق الله العظيم

بعد بسم الله الرحمان الرحيم نهدي هذا العمل الى والديا الكريمين حفظهما الله كذلك اهدي هذا العمل الى اخوتي واصدقائي و إلى السادة المشرفين الأفاضل الذين مدوا لي يد العون، وذللوا لي كل عسير، وأخذوا بيدي بينما أخطوا خطواتي الأولى في هذا الميدان الصعب.

والله العظيم أسأل أن يجزيهم بإحسانهم إحساناً وأن ينفع ببحثي هذا البلاد والعباد.

عبد اللطيف قتوم

رضا طلاطة

كلمة شكر

الحمد لله الذي تتم بنعمته الصالحات و الذي وفقنا في انجاز هذا العمل المتواضع ومن يقتضي مني واجب الشكر والاعتراف بالفضل أن أتقدم للدكتور "**زمورة داود**" الذي اشرف على هذه المذكرة ولم يبخل علينا صبرنا ولو بكلمة وتقديم نصائح وتوجيهات و ارشادات و صبره معنا طوال مسارنا لانجاز هذا البحث قيمة كما اتقدم بالشكر الى لجنة المناقشة على قبولهم مناقشة مذكرتنا و شرفونا بتكريس جزء من وقتهم لدراسة هذا البحث كما نتقدم بالشكر الى الأسرة الجامعية بكلية الحقوق و العلوم السياسية من أساتذة و اداريين ونتقدم بالشكر لكل من ساهم من قريب او بعيد ولو بكلمة في هذا العمل الى كل هؤلاء نقدم شكرنا

قتوم عبد اللطيف طلاطة رضا

المقدمة

مقدمــة

المقدمة

إن الجريمة ظاهرة اجتماعية قديمة، عرفت المجتمعات البشرية ملامحها منذ فجر التاريخ، حيث قامت الجماعات البدائية بوضع قواعد وقوانين عرفية لضبط سلوك الأفراد حفاظًا على الأمن والاستقرار، وتدرجت عبر الزمن من أنظمة بدائية بسيطة إلى نظم قانونية معقدة في ظل ظهور الدولة، حيث تبنت بنفسها سلطة التجريم والعقاب، فأصدرت قوانين موضوعية تحدد الأفعال المجرّمة وعقوباتها، وإجراءات إجرائية تنظم كيفية ملاحقة الجناة، إلى جانب الشريعة الإسلامية التي وضعت مقاصد سامية لحماية ضرورات الحياة، وهي الدين والنفس والعقل والنسل والمال.

غير أن تطور المجتمعات البشرية في شتى الميادين، خاصة في المجال التكنولوجي، أدى إلى بروز طائفة جديدة من الجرائم لم تكن معروفة من قبل، مرتبطة بثورة المعلومات والاتصالات، حيث ظهر الحاسوب وشبكة الإنترنت وانتشرت بشكل مذهل في جميع أنحاء العالم، مما أسفر عن نشوء ما يُعرف بالجرائم السيبرانية، التي تمثل الانعكاس السلبي لهذا التطور العلمي.

وفي هذا السياق، تُعرف الجريمة السيبرانية بحسب دراسة منشورة في مجلة الفارابي الإنسانية بأنها "كل نشاط إجرامي يُرتكب باستخدام الوسائل التقنية الحديثة عبر شبكة الإنترنت ضد أفراد أو مؤسسات أو نظم إلكترونية"، لتشمل بذلك الاعتداء على المعلومات، انتهاك الخصوصية، قرصنة البرمجيات، والاعتداءات المالية والاقتصادية عبر الفضاء الرقمي.

اهمية اختيار الموضوع:

وقد اكتسبت هذه الظاهرة أهمية متزايدة بالنظر إلى طبيعتها العابرة للحدود، وسهولة ارتكابها، وصعوبة تتبع مرتكبيها، مما جعلها تشكل خطرًا حقيقيًا يهدد الأفراد، المؤسسات، والدول على حد سواء، وهو ما يبرز ضرورة التصدي لها عبر تطوير الإطار القانوني والمؤسساتي الملائم.

أهداف الدراسة:

تهدف هذه الدراسة بشكل أساسي إلى تسليض الضوء على مختلف أبعاد الجريمة السيبيرانية، من ناحية مفهومها والمصطلحات المتداخلة معها و أهم صورها، كما تسعى الد ارسة إلى تحليل اليات التعاون الدولي في مكافحة هذه الجريمة وذلك في محاولة الالمام الشامل بمكافحة جوانب هذا الموضوع الهام.

اسباب اختيار الموضوع :

أما عن دوافع اختيار هذا الموضوع فتعود الى أسباب ذاتية و أخرى موضوعية ، اذ أن الغموض الذي يكتنف الجرائم السيبيرانية و طبيعتها المعقدة ، و ما تطرحه من اشكاليات قانونية و فنية ، جعلني أجد فيه مجالا خصبا للتحليل و البحث ، كما أن الأهمية البالغة لهذا الموضوع و ارتباطه المباشر بتطور المجتمعات الحديثة و توجهها نحو الادارة و الحكومة الالكترونية ، فرضت نفسها بقوة على الساحة القانونية و الأكاديمية .

و من الأسباب الذاتية: التي دفعتني للكتابة في هذا الموضوع هو أن مجرد طرح اشكاليتها يبعث في نفسنا حالة من الغموض خصوصا في أهميتها و اطار مكافحتها ، فتجعل العقل يفكر في شكل الجريمة و طريقة التفتيش و غيرها من الاجراءات ، هذا ما دفعني للبحث في طيات الموضوع و الوصول الى حقيقة الموضوع .

أما الأسباب الموضوعية: فقد تم اختيار الموضوع على التطور الملحوظ للجريمة الالكترونية فقد أصبحت واقع معاش و ليست شيء وهمي ، اذ أنها تمس كل المجالات.

الاشكالية:

و الاشكال الذي يطرح نفسه في هذا الصدد هو :ما مدى كفاية التعاون الدولي و الاقليمي لمكافحة الجرائم السيبيرانية ؟

ماهي الوسائل والطرق للتعاون الدولي في مواجهة الجريمة السيبيرانية ؟ و هل هي كافية ؟

المنهج المتبع :

وللاجابة عن هاته الاشكالية الجوهرية اتبعنا المنهج الوصفي من خلال ابراز التساؤلات التي تتفرع عنها و التي من بينها ماهية الجريمة الالكترونية ؟ أنواعها و خصائصها ؟ آليات و استراتيجيات مكافحتها ,, كما يتخلله المنهج المقارن من خلال تمييز التعاون الدولي في مكافحة الجارئمالسيبيرانية.

الدراسات السابقة :

لقد تطرقت عدة دراسات لموضوع الجريمة السيبيرانية وبصفة خاصة الجريمة الالكترونية نذكر منها :

نايري عائشة لالجريمة الالكترونية في التشريع الجزائري للحصول على مذكرة نيل شهادة الماستر في القانون الاداري جامعة احمد دراية ادرار لسنة 2016 2017

تطرقت هذه الدراسة الى ماهية الجريمة الالكترونية ومكافحة الجريمة الالكترونية في القانون الجزائري .

وما يميز دراستنا عن هذه الدراسة هو تطرقنا في كيفية التعاون الدولي في مكافحة الجرائم السيبيرانية.

مقدمــة

الخطة:

ولقد إعتمدنا في دراستنا لموضوع التعاون الدولي في مكافحة الجرائم السيبرانيةخطة ثنائية حيث تطرقنا إلى الاطار المفاهيميللجرائم السيبيرانية في الفصل الاول ففي المبحث الاول تمت دراسة مفهوم الجريمةالسيبيرانيةأما المبحث الثاني صور الجرائم السيبيرانيةأما اليات وإستراتيجيات التعاون الدولي في مكافحة الجرائم االسيبيرانية تطرقنا إليها في الفصل الثاني ففي المبحث الاول تمت دراسة اليات و تحديات التعاون الدولي في مكافحة الجرائم السيبرانيةأما المبحث الثاني تمت دراسة المكافحة الدولية للجريمة السيبيرانية .

الفصل الاول :الاطار المفاهيمي للجرائم السيبيرانية

الفصل الأول : الاطار المفاهيمي للجرائم السيبيرانية

شهد العالم في الآونة الأخيرة تطورا ملحوظا في مجال التكنولوجيا ، مما سمح باستخدام الحاسوب و الانترنت في جميع مجالات الحياة ، الا أن هذا التطور رافقه ظهور أنماط جديدة من الجرائم التي ترتكب عبر الوسائل التقنية الحديثة، و تعرف عموما بالجرائم الالكترونية ، هذه الجرائم ليست لها أي صلة بعلاقة تقليدية مع الجيل المعهود من الجرائم ، بل تعتمد على وسائل افتراضية ترتبط بالأنظمة المعلوماتية . و قد أظهر هذا الواقع مصطلح "الجريمة السيبيرانية " و هي جريمة حديثة النشأة تتطلب تعريفا قانونيا دقيقا و نظرة شاملة لمكوناتها و أنواعها و دوافعها ، و من هنا جاء هذا الفصل لتقديم اطار مفاهيمي حول هذا النوع من الجرائم من خلال توضيح ماهيته و أهيمته.

المبحث الأول : مفهوم الجريمة السيبيرانية

سيخصص هذا المبحث لعرض الاطار المفاهيمي للجريمة السيبيرانية من خلال التعرض لمفهومها العام و تبيان خصائصها ، مع الوقوف على أهميتها و خطورة تأثيرها على الأفراد و الدول .

المطلب الأول: تعريف الجرائم السيبيرانية

لم يتم التوصل إلى تعريف موحد للجريمة السيبيرانية في الفقه الجنائي، إذ تُطلق عليها تسميات متعددة مثل: الجريمة المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، جرائم الحاسوب والإنترنت، الجرائم المستحدثة، الجريمة الناعمة، أو جرائم ذوي الياقات البيضاء[1].

[1] – عادل يوسف عبد النبي الشكري، بحث بعنوان الجريمة المعلوماتية و أزمة الشرعية الجزائية، جامعة الكوفة 221–222.

من المهم التمييز بين مجال جرائم الحاسوب ومجال جرائم الإنترنت؛ فالأولى تتعلق بالاعتداء على مكونات الحاسوب وبرمجياته والمعلومات المحفوظة فيه، بينما الثانية تُرتكب من خلال تبادل البيانات عبر خطوط الهاتف أو الشبكات الفضائية. غير أن تطور التكنولوجيا واندماج مجالي الحوسبة والاتصالات أدى إلى ظهور مفهوم شامل هو "الجريمة السيبرانية.(Cybercrime) "

وقد انقسم الفقهاء إلى اتجاهين في تعريف الجريمة السيبيرانية : أحدهما يضيق نطاقها، والآخر يوسع مفهومها. كما أن لهذه الجريمة أركانًا أساسية يجب توافرها حتى تُعد الجريمة قائمة، وسأتناول في هذا المطلب تعريف الجريمة الإلكترونية.

مفهوم الجريمة الإلكترونية

اختلفت آراء الفقهاء حول تقديم تعريف موحد للجريمة السيبيرانية، ويعود هذا الاختلاف إلى تباين وجهات النظر بشأن نطاقها، بين من يراها من منظور ضيق ومن يعتمد مفهوماً أوسع. وفيما يلي عرض لأبرز التوجهات الفقهية:

<u>الفرع الأول: الاتجاه الضيق لتعريف الجريمة السيبيرانية</u>

يرى أنصار هذا الاتجاه أن الجريمة السيبيرانية هي "كل فعل غير مشروع يتطلب قدراً كبيراً من المعرفة بتكنولوجيا الحاسوب لارتكابه والتحقيق فيه.[1]" ويفيد هذا التعريف بأن الجريمة لا تُعد إلكترونية إلا إذا كان مرتكبها يمتلك مهارات تقنية عالية، وينطبق ذلك أيضًا على من يلاحق الجريمة من قضاة وضباط شرطة.

[1] – مفتاح بوبكر المطرودي، الجريمة الإلكترونية و التغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث إلى رؤساء المحاكم العليا في الدول العربية من جمهورية السودان ، المنعقد في عام 2008. ص 214.

كما يوجد من يعرفها بأنها: "فعل إجرامي يتضمن استخدام الحاسوب كأداة رئيسية." ويذهبTredmannإلى اعتبار أن الجريمة المعلوماتية تشمل كل الجرائم المرتبطة بالمعالجة الآلية للبيانات. في حين يرى Rosenblatt أن الجريمة الإلكترونية تتعلق بأي نشاط غير مشروع يستهدف نسخ أو تعديل أو حذف أو تحويل البيانات من خلال الحاسوب.

أما Parker فيصفها بأنها: "كل فعل إجرامي متعمد يتعلق بتقنية المعلومات، وينتج عنه ضرر للمجني عليه أو منفعة للفاعل".

الفرع الثاني: الاتجاه الموسع لتعريف الجريمة الإلكترونية

يرى أصحاب هذا التوجه أن الجريمة الإلكترونية تشمل أي فعل جرمي يُرتكب باستخدام وسائل إلكترونية كالحاسوب والإنترنت، سواء من خلال غرف الدردشة، أو اختراق البريد الإلكتروني، أو عبر منصات التواصل الاجتماعي، بهدف إلحاق الضرر بفرد أو جهة أو حتى دولة، وقد يكون الهدف سياسيًا أو اقتصاديًا أو دعائيًا، كالتسريب أو التشهير[1].

وقد اعتمد المجلس الأوروبي هذا التوجه، حيث اعتبر أن الجريمة تقع متى حدث أي تغيير أو حذف أو تعديل أو معالجة غير مشروعة للبيانات، ونتج عنها ضرر اقتصادي أو مكسب غير مشروع.

كما يُعرف هذا النوع من الجرائم بأنه: "أي فعل ضار يُرتكب باستخدام نظام حاسوبي أو شبكة معلوماتية بهدف نسخ أو تخريب أو تزوير أو تعطيل البيانات أو البرامج، أو حتى

[1] – حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي ، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة، نقلاً عن قورة نائلة، جرائم الحاسب الإقتصادية ،القاهرة 2011. ص 115.

حيازتها وتوزيعها بصورة غير قانونية." وهناك من يرى أنها: "أي نشاط إجرامي تُستخدم فيه التكنولوجيا الرقمية بشكل مباشر أو غير مباشر كوسيلة لتنفيذ الفعل الإجرامي".

ومع ذلك، فإن هذا التعريف الواسع قد لا يكون دقيقًا دائمًا، إذ لا يمكن اعتبار كل جريمة ارتُكبت باستخدام الحاسوب جريمة إلكترونية، مثل سرقة الحاسوب نفسه أو استخدامه في التنسيق لجرائم تقليدية.

التعريف القانوني للجريمة الإلكترونية في الجزائر:

في القانون الجزائري، استخدم المشرّع مصطلح "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، ووفق المادة 02 من القانون رقم 04-09، تُعرّف هذه الجرائم بأنها: "كل مساس بأنظمة المعالجة الآلية للمعطيات كما حددها قانون العقوبات، إضافة إلى أي جريمة تُرتكب أو تُسهل عبر منظومة معلوماتية أو نظام اتصالات إلكترونية".

ومن هذا التعريف، يتبين أن المشرّع الجزائري ركز على دور النظام المعلوماتي في الجريمة، كما حددها ضمن المواد 394 مكرر إلى 394 مكرر 07 من قانون العقوبات، وفتح المجال أمام أنواع جديدة من الجرائم التي تُرتكب أو تُسهل عبر الوسائل التقنية[1].

ومن الأمثلة الواقعية على الجرائم الإلكترونية في الجزائر: تسريب أسئلة البكالوريا عام 2016، والاختراقات البنكية العالمية التي قام بها القرصان الجزائري "حمزة بن دلاج."

[1] – مليكة عطوي الجريمة المعلوماتية حوليات جامعة الجزائر ، مجلة علمية 2017 العدد 85 ص.159.

المطلب الثاني: أركان الجرائم السيبيرانية

كل الجرائم تتكوّن من أركان ثلاثة هي: الركن الشرعي، الركن المادي، والركن المعنوي، غير أنّ الجريمة المعلوماتية تمتاز بإضافة ركن رابع يتمثّل في الركن الافتراضي، وتشكّل هذه الأركان مجتمعة أساس دراستنا في هذا المبحث.

الفرع الاول: الركن الافتراضي للجريمة المعلوماتية

لقيام الجريمة المعلوماتية، لا بدّ من توفر نظام المعالجة الآلية للمعطيات، وهنا يُطرح التساؤل حول ماهية هذا النظام؟

اولا: تعريف نظام المعالجة الآلية للمعطيات

يُعرفه بعض الفقهاء على أنه منظومة تقنية وإجرائية منظمة تُستخدم في جمع وتصنيف وتحليل البيانات، وتحويلها إلى معلومات قابلة للاسترجاع عند الحاجة، بهدف تمكين الإنسان من اتخاذ القرارات، أداء المهام أو إنجاز الأعمال، بالاعتماد على المعرفة المستخرجة من هذه المعلومات[1].

ومن هذا التعريف تبرز إشكالية تعدد مكونات هذا النظام، وتُثار التساؤلات بشأن ما إذا كان الاعتداء على أحد عناصره الفردية يُعد اعتداءً على النظام برمته؟ وهنا يرى فقهاء القانون أنه يجب العودة إلى علاقة الجزء المستهدف بالنظام، فإن كان هذا الجزء مستقلاً عنه، فلا تقوم الجريمة المعلوماتية، كما في حالة الاعتداء على برامج تُعرض للبيع أو أجهزة حاسوب لم تدخل حيز الخدمة بعد، أو تلك التي تكون في مرحلة التجربة أو توقفت عن العمل.

[1] – سعيداني نعيم آليات البحث و التحري عن الجريمة المعلوماتية، القانون الجزائري ،مذكرة ماجستير في العلوم القانونية تخصص علوم جنائية ، جامعة الحاج لخضر باتنة، الجزائر 2013 ص 42.

ولم يُقدّم المشرّع الجزائري في تعديله لقانون العقوبات سنة 2004 (الذي أضاف القسم 7 مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات") تعريفًا دقيقًا لهذا النظام، بل ترك الأمر للاجتهاد القضائي والفقهي، على غرار نظيره الفرنسي، الذي تخلى كذلك عن هذه المهمة بعد رفض الجمعية الوطنية مقترح مجلس الشيوخ بهذا الخصوص.

واستنادًا إلى تعريف مجلس الشيوخ الفرنسي، فإن نظام المعالجة الآلية للمعطيات هو "مجموعة تتألف من وحدة أو أكثر من وحدات المعالجة، والتي تحتوي على الذاكرة، البرامج، المعطيات، أجهزة الإدخال والإخراج، وأجهزة الربط، وتتكامل هذه المكونات من خلال علاقات وظيفية تسمح بتحقيق معالجة البيانات، شريطة خضوع هذا النظام لحماية فنية."

ويُلاحظ أن هذا التعريف أكثر دقة وشمولاً، إذ لا يكتفي بتحديد مكونات النظام بل يشترط أيضًا توفر حماية فنية للمعطيات، وغياب هذه الحماية يمنع توصيف الجريمة على أنها معلوماتية.

ومن هنا يمكن القول بأن إغفال المشرع لتعريف هذا النظام يعكس إدراكًا لطبيعة تطوره المستمر بسبب اعتماده على عناصر تقنية متجددة، لذا فإن ترك مهمة التعريف للفقه والقضاء يُعدّ مقاربة وجيهة، كما يرى بعض الفقهاء.

ثانيا: الحماية الفنية للنظام المعلوماتي كشرط لقيام المسؤولية الجزائية

تباينت آراء الفقهاء حول ما إذا كانت الحماية الأمنية لنظام المعالجة الآلية تُعد شرطًا جوهريًا لتمتعه بالحماية الجزائية. فقد اعتبر بعض الفقه الفرنسي أن الحماية الفنية ليست ضرورية لقيام الجريمة المعلوماتية، معتبرين أن دور هذه الحماية يظل إيجابيًا، بينما يتحقق الركن المعنوي من خلال إثبات سوء نية الجاني ودخوله غير المشروع إلى النظام.

في المقابل، ذهب اتجاه فقهي آخر إلى ضرورة توفر حماية أمنية، وقسّم الأنظمة المعلوماتية إلى ثلاث فئات:

1.أنظمة مفتوحة أمام العموم.

2.أنظمة مقيدة على فئة من المستخدمين، ولكن دون حماية فنية.

3.أنظمة مقيدة ومحاطة بحماية فنية.

ويؤمن هذا الاتجاه بأن الفئة الثالثة فقط تستحق الحماية الجنائية، معتبرين أن القانون لا يحمي إلا من أبدى حرصًا على حماية بياناته، حتى ولو كان ذلك بوسائل بسيطة.

ورغم ذلك، يُطرح تساؤل حول إمكانية وجود نظام معلوماتي دون أدنى حماية فنية، وهو ما يبدو غير منطقي من الناحية العملية، إذ إن توفر الحماية يُسهم في تحديد القصد الجنائي للجاني، ما يجعل اشتراط الحماية أمرًا مقبولاً في الفترة الأخيرة.

الفرع الثاني: الأركان العامة للجريمة المعلوماتية

تخضع الجريمة المعلوماتية، شأنها شأن الجرائم التقليدية، إلى ثلاثة أركان: الشرعي، المادي، والمعنوي.

اولا : الركن الشرعي للجريمة المعلوماتية

بعد توفر الركن الافتراضي كشرط أساسي للجريمة المعلوماتية، يبرز الركن الشرعي الذي يتمثل في وجود نصوص قانونية تُجرّم الأفعال المرتبطة بالاعتداء على أنظمة المعلومات.

ففي الولايات المتحدة، ينص القانون الفيدرالي على مكافحة هذه الجرائم، إلى جانب أغلب قوانين الولايات. أما في كندا، فقد أُدرجت ضمن قانون العقوبات، بينما خصصت فرنسا قانونًا مستقلًا لها هو القانون رقم 78/17 الصادر بتاريخ 16 جانفي 1978 والمعروف باسم "قانون الإعلام الآلي والحريات."

وفي الجزائر، نص المشرّع على تجريم هذه الأفعال ضمن تعديل قانون العقوبات لسنة 2004، بإضافة القسم 7 مكرر المعنون بـ "المساس بأنظمة المعالجة الآلية للمعطيات"، كما سبق بيانه.

وتُركز هذه النصوص على حماية المال المعلوماتي، وهو ما أكد عليه الاجتهاد القضائي والفقهي كأولوية تشريعية.

ثانيا: الركن المادي للجريمة المعلوماتية

يُعرّف الركن المادي على أنه أي فعل يؤدي إلى تعطيل نظام المعالجة الآلية للمعطيات عن أدائه الطبيعي. ورغم الجدل حول مدى شمول النظام لكل مكوناته، يتفق أغلب الفقهاء على عدم ضرورة إلحاق الضرر بالنظام بأكمله، بل يكفي استهداف أحد عناصره، مثل الحاسوب، الشبكة، البرنامج، أو البيانات[1].

[1] – قارة أمال الجريمة المعلوماتية ماجستير تخصص قانون جنائي و العلوم الجنائية كلية الحقوق بجامعة الجزائر ، 2005ص01

وتتحقق الجريمة أيضًا بالدخول أو البقاء غير المشروع في النظام، أو بحذف أو تعديل المعطيات، إضافة إلى التخريب أو الإتلاف في أنظمة التشغيل، وفقًا للمادة 394 مكرر من قانون العقوبات الجزائري.

وتشمل الأفعال المادية كذلك إدخال معلومات في النظام أو حذفها، مما يوفر الركن المادي للجريمة المعلوماتية.

ثالثا: الركن المعنوي للجريمة المعلوماتية

يتجلى الركن المعنوي في القصد الجنائي، وهو عنصر ضروري لقيام المسؤولية الجزائية. ونظرًا لخصوصية الجرائم المعلوماتية، فقد تناولها الفقه كلٌّ على حدة لتحديد مدى توفر القصد.

يرى اتجاه فقهي أن القضاء الأمريكي لم يستقر في بعض الحالات على تحديد ما إذا كانت الجرائم المعلوماتية تتطلب قصدًا عامًا أم خاصًا. ففي بعض الحالات، يكفي القصد العام، وهو علم الجاني بكون فعله غير مشروع، واقترانه بالإرادة[2].

ومثال ذلك حكم لمحكمة النقض الفرنسية، التي اعتبرت أنّ نية التملك المؤقت كافية لقيام جريمة سرقة معلومات من جهاز حاسوب، إذا تم الاستيلاء عليها ولو لفترة مؤقتة بدون إذن صاحبها.

[2] – لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها و آلية مكافحتها ، دراسة تحليلية مقارنة، مجلة الميزان ، المجلد 04 العدد 1 جامعة العلوم الإسلامية العالمية ، الأردن 2017 ص 189.

وفي جريمة التزوير المعلوماتي، يُفترض وجود نية إضافية لدى الجاني لاستخدام المستند المزوّر، حتى وإن لم يتم استخدامه فعليًا، مما يشير إلى قيام القصد الاحتمالي بمجرد علم الجاني بإمكانية حدوث ضرر.

وبالتالي، فإن إثبات القصد الجنائي الخاص يبقى صعبًا، مما يعقّد إثبات الركن المعنوي، وهو أحد أبرز الخصائص التي سبق ذكرها.

المبحث الثاني: صور الجريمة الإلكترونية في القانون الجزائري

بعد أن تم تناول أركان الجريمة الإلكترونية وشروط قيامها وفقًا للقانون الجزائري، يتناول هذا المبحث الجوانب التي تميز هذا النوع من الجرائم عن غيره، من حيث الخصائص التي تتصف بها، سواء على مستوى الجريمة نفسها أو على مستوى مرتكبيها، بالإضافة إلى التصنيفات المختلفة التي تندرج تحتها الجريمة الإلكترونية. وسنقوم بدراسة هذه العناصر من خلال المطلبين الآتيين:

المطلب الأول: خصائص الجريمة الإلكترونية

كون الجريمة الإلكترونية وليدة التقدم العلمي والتكنولوجي، فقد نشأت في بيئة مغايرة تمامًا عن البيئة التي تنشأ فيها الجرائم التقليدية، مما منحها خصائص فريدة من نوعها تميزها عن باقي الجرائم الأخرى. ويمكن رصد أبرز هذه السمات من خلال ما يلي:

الفرع الاول: السمات المرتبطة بالجريمة الإلكترونية

الخفاء وسرعة التنفيذ: تتميز الجريمة الإلكترونية بقدرتها على التخفي، إذ غالبًا ما تحدث دون أن يشعر بها الضحية، رغم وقوعها أحيانًا أثناء تواجده الفعلي على الشبكة. كما أنها تنفذ بسرعة فائقة تصل أحيانًا إلى جزء من الثانية، ويستعمل فيها الجاني أدوات رقمية مثل البرمجيات والأجهزة المعلوماتية[1].

ارتكابها من طرف أشخاص ذوي كفاءات خاصة: تتطلب هذه الجرائم مهارات تقنية متقدمة ومعرفة علمية متخصصة، إذ يعتمد مرتكبوها على أدوات معرفية وأساليب احترافية عالية.

صعوبة الإثبات: نظرًا لطبيعتها الرقمية، فإن الجرائم الإلكترونية تفتقر غالبًا إلى الأدلة المادية التقليدية، مما يصعّب من مهمة إثباتها قانونيًا، خاصة إذا تم ارتكابها من داخل المؤسسات من قبل موظفين محل ثقة.

ضرورة الاعتماد على تقنيات حديثة للتحري: تتطلب هذه الجرائم تدخل خبراء في الأمن السيبراني ورجال شرطة ومحققين مؤهلين في المجال الرقمي من أجل تحليل الأدلة الرقمية وملاحقة الجناة.

الطابع العابر للحدود: لا تعترف الجريمة الإلكترونية بالحدود الجغرافية، إذ يمكن تنفيذها من أي مكان في العالم واستهداف أي ضحية في موقع آخر، بفضل الوسائط الرقمية.

قلة الإبلاغ عنها: يعزف الضحايا، خصوصًا الشركات، عن التبليغ عن هذه الجرائم خوفًا من التأثير على سمعتها أو زعزعة ثقة عملائها، كما حدث مع بنك "سيتي بانك مارشنت" في بريطانيا.

[1] –صغير يوسف ، الجريمة المرتكبة عبر الأنترنت ، مذكرة لنيل شهادة الماجستير في القانون ، تخصص القانون الدولي للأعمال ، جامعة مولود معمري تيزي وزو 2016 ص45 .

فداحة الأضرار المترتبة عنها: غالبًا ما تكون الخسائر التي تخلفها هذه الجرائم جسيمة من الناحية المادية والمعنوية.

أسلوب التنفيذ الذاتي: تختلف طريقة ارتكاب الجريمة الإلكترونية عن الجرائم التقليدية، فهي لا تتطلب عنفًا جسديًا بل تعتمد على التلاعب الرقمي بالشبكات والنظم.

التنظيم والتعاون بين الجناة: غالبًا ما تُرتكب هذه الجرائم بتنسيق بين عدة أشخاص، يتوزعون الأدوار بين من يملك الكفاءة الفنية ومن يتولى إخفاء الأدلة والاستفادة من المكاسب غير المشروعة.

الفرع الثاني : السمات المتعلقة بالمجرم الإلكتروني

الذكاء والمهارة: يتمتع المجرم الإلكتروني بقدرات تحليلية وتقنية عالية، تسمح له بفهم بيئة الجريمة واستغلالها لصالحه، كما يخطط بدقة لتفادي الفشل أو الوقوع في قبضة القانون.

تبرير الفعل الإجرامي: غالبًا ما لا يرى المجرم الإلكتروني أن أفعاله تشكل جريمة، خصوصًا عندما تكون موجهة ضد مؤسسات وليس أفراد، ويبرر فعله بأنه تحدٍ لأنظمة الحماية دون نية للإضرار المباشر[1].

الخوف من كشف أمره: رغم الحذر الشديد الذي يتسم به المجرمون الرقميون، إلا أن القلق الدائم من انكشاف هويتهم يلازمهم، خصوصًا أن ذلك قد يؤدي لفقدان الوظيفة أو الإضرار بسمعتهم.

[1] – سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية ، مذكرة مكملة لمتطلبات نيل شهادة الماستر في الحقوق تخصص قانون جنائي جامعة محمد خيضر بسكرة 2018 ص 111.

نزعة التقليد: يتأثر بعض المجرمين الإلكترونيين بأقرانهم ويحاولون تقليدهم تقنيًا، ما يؤدي بهم إلى ارتكاب الجرائم بدافع الفضول أو الانبهار.

التخطيط والتنظيم: نادرًا ما يرتكب المجرم الإلكتروني جرائمه بشكل عشوائي، بل غالبًا ما تكون هناك خطط دقيقة، ويُوزع العمل بين أفراد الشبكة الإجرامية وفق أدوار محددة.

الاندماج الاجتماعي: لا يعيش المجرم الإلكتروني في عزلة، بل هو جزء من المجتمع وقد يمارس وظائف عادية، وهذا يسهل عليه إخفاء نشاطه الإجرامي.

التطور الإجرامي: بمرور الوقت، يكتسب المجرم مهارات إضافية تُمكنه من الارتقاء في مدارج الجريمة، وقد ينتقل من دور مساعد إلى المخطط الرئيسي.

الفرع الثالث : أنواع المجرمين الإلكترونيين

انطلاقًا من تنوع المهارات والدوافع، يمكن تصنيف المجرمين الإلكترونيين إلى عدة فئات، من أبرزها:

1المتسللون (Hackers) : يشملون فئات متعددة مثل أصحاب "القبعة البيضاء" (الأخلاقيون)، و"القبعة السوداء" (المخربون)، و"القبعة الرمادية" (الذين يمزجون بين الاثنين). وغالبًا ما يكونون شبابًا يتمتعون بذكاء فائق وشغف بالتكنولوجيا.

2المقتحمون (Crackers) :هم من يملكون خبرة عالية، وغالبًا ما يشغلون مناصب مرموقة في المجتمع، ويستخدمون معرفتهم التقنية في اقتحام الأنظمة عن قصد لإحداث أضرار.

3المجرمون المحترفون: يهدفون إلى تحقيق مكاسب مالية من خلال أنشطة إجرامية منظمة ومدروسة، وتُعد هذه الفئة من أخطر المجرمين نظرًا لمهاراتهم العالية.

4المنتقمون: يسعون للانتقام من مؤسسات أو أفراد، سواء كانوا من موظفي المؤسسة أو غرباء يكنّون لها العداء، ويعتمدون في ذلك على أدوات مثل الفيروسات والبرمجيات الخبيثة.

5صغار السن: يطلق عليهم "صغار نوابغ المعلوماتية"، وهم مراهقون أو حتى أطفال يملكون فضولًا تقنيًا عاليًا، وقد ينجرفون إلى عالم الجريمة بدافع التحدي أو التسلية.

6المجرمون ذوو الدوافع السياسية: يستهدفون أنظمة تحتوي على معلومات سرية تتعلق بالأمن والدفاع بدافع أيديولوجي أو سياسي، ويشكلون خطرًا كبيرًا على الأمن القومي.

وتُجمع هذه الفئات على صفات مشتركة، أبرزها: الفئة العمرية التي تتراوح بين 18 و45 سنة، والتمكن الكبير من تكنولوجيا المعلومات، والثقة الزائدة بالنفس، والقدرة على تفادي الأخطاء التي قد تُفشل مخططاتهم[1].

المطلب الثاني: أنواع الجرائم الإلكترونية في القانون الجزائري

تُصنّف الجرائم التقليدية من حيث خطورتها إلى ثلاث فئات: الجنايات، وهي الأشد خطورة، والجنح ذات الخطورة المتوسطة، ثم المخالفات التي تُعدّ الأقل من حيث الخطورة. كما يمكن تصنيفها من حيث طبيعتها إلى: جرائم عادية، جرائم سياسية، جرائم عسكرية،

[1] مزغيش سمية مصدر سابق ص116 .

وجرائم إرهابية. غير أن الجريمة الإلكترونية تختلف من حيث التقسيم، نظراً لتباين مفاهيمها وتعدد معايير تصنيفها، حيث اعتمد كل اتجاه معياراً معيناً؛ فهناك من صنفها حسب الوسائل المستخدمة في ارتكابها، وآخرون اعتمدوا على الدوافع، في حين لجأ البعض إلى تصنيفها تبعاً لمحل الاعتداء وتعدد الحقوق المعتدى عليها.

أما فيما يخص المشرع الجزائري، فقد ميّز بين نوعين من الجرائم الإلكترونية:
الأول، جرائم تُرتكب باستخدام النظام المعلوماتي، وقد أشار إليها بشكل عام دون تحديد دقيق، لتشمل بذلك جميع الأفعال الإجرامية التي تُنفذ بواسطة وسائل تكنولوجيا الإعلام والاتصال.

أما النوع الثاني، فهو الجرائم التي تستهدف النظام المعلوماتي نفسه، وقد تم النص عليها صراحة ضمن قانون العقوبات. وسنتناول هذين الصنفين في الفرعين الآتيين[1].

الفرع الأول: الجريمة الإلكترونية المرتكبة باستخدام النظام المعلوماتي

يشمل هذا التصنيف أبرز أنواع الجرائم المرتبطة بمجال المعلوماتية، حيث يُستخدم الحاسوب كأداة تسهّل تنفيذ الجريمة وتُضخم من آثارها، وتنقسم إلى ثلاثة أنواع رئيسية: جرائم تمس الأفراد، وجرائم تستهدف أنظمة معلوماتية أخرى، وجرائم تمس بالأسرار. وسنوضح هذه الأنواع فيما يلي:

أولا: الجريمة الإلكترونية الماسة بالأشخاص الطبيعيين

تنقسم هذه الفئة إلى:

[1] – أحسن بوسقيعة الوجيز في القانون الجزائي العام ، الديوان الوطني للأشغال التربوية 2020 ط02 ص 113.

.1**الجرائم المتعلقة بحقوق الملكية الفكرية:** في هذا النوع من الجرائم، يُستخدم النظام المعلوماتي كوسيلة للاعتداء على الحقوق الفكرية، مثل التعدي على بنوك المعلومات باستخدامها أو تخزينها دون موافقة أصحابها، مما يُعتبر انتهاكاً للحقوق الأدبية والمادية. كما تندرج براءات الاختراع ضمن هذه الفئة، باعتبارها تمثل ابتكارات فكرية محمية قانوناً. وقد نظم المشرع هذه الحقوق بموجب الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 الخاص ببراءات الاختراع، الصادرين سنة 2003.

.2**الجرائم المتعلقة بحرمة الحياة الخاصة:** حَرص الدستور الجزائري على حماية خصوصية الأفراد، غير أن الحاسوب، بقدرته الكبيرة على تخزين البيانات، بات أداة تهدد هذه الخصوصية. فعلى سبيل المثال، قد يقوم موظف بجمع معلومات شخصية عن شخص آخر دون علمه، أو يقوم بمشاركة تلك المعلومات مع الغير دون إذن، أو أن يتم اختراق الأجهزة للحصول على مذكرات شخصية أو ملفات سرية.

ثانيا: الجريمة الإلكترونية الماسة بأنظمة معلوماتية أخرى

تتحقق هذه الجريمة إما من خلال الدخول المادي إلى مراكز المعالجة المعلوماتية، أو عبر أدوات إلكترونية تتيح التقاط البيانات والتجسس عليها، كما تشمل سوء استخدام البطاقات البنكية.

في الحالة الأولى، يتمكن الجاني من الوصول إلى المعلومات من خلال أدوات مثل شاشات النظام أو الطابعات أو مكبرات الصوت.

أما الحالة الثانية، فتتعلق باستخدام غير قانوني لبطاقات الائتمان، كاستعمال بطاقة منتهية الصلاحية أو ملغاة.

في الحالة الثالثة، قد يُقدم السارق على استخدام بطاقة شخص آخر للحصول على خدمات أو سلع دون وجه حق.

ثالثا: الجريمة الإلكترونية الماسة بالأسرار

تتمثل هذه الجريمة في استخدام النظام المعلوماتي لإفشاء الأسرار، سواء كانت خاصة أو عامة، وتتخذ صورتين:

1الجرائم ضد أسرار الدولة: تُمكّن الإنترنت بعض الدول من التجسس على غيرها، من خلال الحصول على معلومات حساسة كالأسرار العسكرية أو الاقتصادية، خاصة في حالات النزاع.

2الجرائم ضد الأسرار المهنية: يكون الهدف من هذه الجرائم عادة التشهير أو الابتزاز، أو حتى بيع المعلومات لأطراف مهتمة بها. وقد حرص المشرع على حماية هذه الأسرار ضمن مواد قانون العقوبات من المادة 61 إلى المادة 96 مكرر، إضافة إلى المادة 394 مكرر 03 التي تنص على تشديد العقوبات في حال استهداف الدفاع الوطني أو مؤسسات عامة.

الفرع الثاني: الجريمة الإلكترونية الماسة بالنظام المعلوماتي

سدّاً للفراغ التشريعي، أُدرجت أحكام جديدة بموجب القانون رقم 04-15 الصادر بتاريخ 10 نوفمبر 2004، الذي أدخل تعديلات على قانون العقوبات، من خلال القسم السابع مكرر بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وذلك في المواد من 394 مكرر إلى 394 مكرر 07، حيث تم التطرق إلى صورتين أساسيتين: الدخول والبقاء غير

المشروعين في النظام، والتعدي على مكوناته، إضافة إلى صور أخرى من الغش المعلوماتي.

أولا: الدخول والبقاء غير المشروع في النظام المعلوماتي

بحسب المادة 394 مكرر، يُعاقب كل من يدخل أو يبقى داخل نظام معلوماتي باستعمال وسائل احتيالية، ولو كان جزئياً. وتُضاعف العقوبة في حال نتج عن هذا الفعل تخريب أو تعديل للبيانات.

الدخول غير المشروع: لا يُقصد به الدخول المادي، بل هو فعل معنوي يشير إلى النفاذ غير المصرح به إلى عمليات النظام. وتُعتبر الجريمة قائمة حتى دون تحقق أي نتائج مادية، ولا يُشترط امتلاك الجاني المهارات الفنية، إذ يكفي تحقق الدخول بطريقة غير قانونية.

البقاء غير المشروع: يتحقق عندما يظل الشخص داخل النظام ضد إرادة من يملك حق السيطرة عليه، حتى وإن كان دخوله في البداية مشروعاً، كأن يدخل بالخطأ ولا يغادر، أو يسيء استخدام الصلاحيات الممنوحة له، كاستخدام معلومات يُسمح له بالاطلاع عليها فقط دون نسخها.

ثانيا: المساس بمنظومة معلوماتية

نصت المادة 394 مكرر 01 على تجريم إدخال أو حذف أو تعديل البيانات داخل النظام باستعمال الغش. ويتحقق الركن المادي من خلال واحدة فقط من هذه الأفعال الثلاثة،

مثل إدخال بيانات زائفة أو حذف بيانات صحيحة أو تعديلها بشكل غير قانوني، ما يُعد تخريباً مقصوداً للمعطيات، كزرع فيروسات لإتلاف البرامج.

ثالثا: أفعال إجرامية أخرى

أشارت المادة 394 مكرر 02 إلى تجريم تصميم أو جمع أو توفير أو تداول معطيات قابلة لاستخدامها في جرائم إلكترونية، ويُقصد بها مثلاً فيروسات الحواسيب أو برامج الاختراق. كما جرّمت المادة ذاتها حيازة أو نشر أو استخدام بيانات تم الحصول عليها من جرائم إلكترونية سابقة لأي غرض كان.

من خلال ما سبق، يتضح أن الجريمة الإلكترونية تملك طبيعة خاصة، فهي تُرتكب بسهولة بالغة ودون احتكاك مباشر بين الجاني والمجني عليه، مما يُصعّب من مكافحتها. ويُسجل على المشرع الجزائري اقتصاره على تجريم بعض الأفعال دون تقديم تعريف جامع أو تحديد دقيق لخصائص الجريمة الإلكترونية، وهو ما يستدعي مزيداً من التأصيل والتحديث لمواكبة التطورات المتسارعة في هذا المجال.

ملخص الفصل:

الجريمة السيبرانية هي أي نشاط غير قانوني أو غير أخلاقي يتم باستخدام التكنولوجيا الحديثة، مثل الإنترنت والحواسيب والشبكات. تشمل أنواع الجرائم السيبرانية الاختراق،

القرصنة، الاحتيال الإلكتروني، الابتزاز الإلكتروني، وجرائم الدفع الإلكتروني. تهدف هذه الجرائم إلى جمع المعلومات الشخصية، الابتزاز المالي، والتخريب. تواجه مكافحة الجرائم السيبرانية تحديات مثل التطور السريع للتكنولوجيا والتهديدات العالمية وصعوبة تحديد الجناة. استراتيجيات الوقاية تشمل استخدام كلمات مرور قوية، تثبيت برامج مكافحة الفيروسات، توعية المستخدمين، وتطبيق سياسات أمنية صارمة.

الفصل الثاني

آليات واستراتيجيات التعاون الدولي لمكافحة الجرائم السيبيرانية

الفصل الثاني: آليات واستراتيجيات التعاون الدولي في مكافحة الجرائم السيبيرانية

في ظل الثورة الرقمية المتسارعة، أضحت الجرائم السيبيرانية واحدة من أخطر التحديات التي تواجه الأمن الدولي، لما لها من قدرة على تجاوز الحدود الجغرافية واختراق البنى التحتية للدول والمؤسسات والأفراد على حدٍّ سواء. وقد أدى هذا الطابع العابر للحدود إلى إظهار محدودية الجهود الوطنية المنفردة في التصدي لتلك الجرائم، ما استدعى ضرورة تطوير آليات فعّالة للتعاون الدولي في المجال السيبراني، سواء على المستوى الثنائي أو متعدد الأطراف.

إن تنامي التهديدات الإلكترونية وتنوعها، من الجرائم المالية والقرصنة الرقمية إلى الإرهاب السيبراني والهجمات الموجهة على البنية التحتية الحيوية، يفرض على الدول تبني استراتيجيات شاملة تتكامل فيها الأبعاد القانونية، والتقنية، والمؤسسية، والدبلوماسية. ولم تعد الاتفاقيات الدولية والمؤتمرات المتخصصة ترفًا دبلوماسيًا، بل أصبحت أدوات ضرورية لتنظيم هذا الفضاء السيبراني الذي لا يخضع لسلطة دولة بعينها.

يهدف هذا الفصل إلى تسليط الضوء على أبرز آليات واستراتيجيات التعاون الدولي في مجال مكافحة الجرائم السيبيرانية، من خلال استعراض الإطار القانوني الدولي، ودور المنظمات الإقليمية والدولية، إضافة إلى التحديات التي تعترض هذا التعاون، مع إبراز بعض النماذج والمبادرات الناجحة.

ويُراد من هذا العرض بناء فهم أعمق للكيفية التي يمكن من خلالها تعزيز العمل المشترك بين الدول لحماية الفضاء السيبراني وتحقيق الأمن الرقمي العالمي.

المبحث الأول :آليات و تحديات التعاون الدولي في مكافحة الجرائم السيبيرانية

أحدث التطور المتسارع في تكنولوجيا المعلومات والاتصالات نقلة نوعية في شتى مجالات الحياة، لكنه في الوقت ذاته أفرز أشكالاً جديدة من التهديدات، يأتي في مقدمتها ما يُعرف بالجرائم السيبيرانية.

وتمثل هذه الجرائم، بما تتسم به من طابع معقد وعابر للحدود، تحدياً متزايداً أمام أجهزة إنفاذ القانون الوطنية، ما جعل التعاون الدولي ضرورة ملحة لا خيارًا.

إن فعالية التصدي للجرائم السيبرانية تعتمد بشكل كبير على مدى توافر آليات تنسيقية بين الدول، تشمل تبادل المعلومات، والمساعدة القانونية المتبادلة، والتدريب والتأهيل، فضلاً عن اعتماد اتفاقيات ومعايير قانونية موحدة تسهل التحقيق والملاحقة القضائية.

غير أن هذا التعاون يواجه تحديات جوهرية، من بينها تباين التشريعات الوطنية، واختلاف المفاهيم القانونية، وضعف الثقة المتبادلة، إضافة إلى المعوقات التقنية والسياسية المرتبطة بسيادة الدول على فضائها الرقمي.

يستعرض هذا الفصل أبرز الآليات المتاحة للتعاون الدولي في مكافحة الجرائم السيبيرانية، ويناقش العقبات التي تحول دون تحقيق تعاون فعّال ومستدام، مع الإشارة إلى بعض المبادرات الدولية والإقليمية الرائدة في هذا المجال. ويهدف الطرح إلى توضيح أوجه النقص ومجالات التحسين الممكنة لبناء نظام تعاون دولي أكثر تكاملاً ومرونة في مواجهة هذا التهديد العالمي المتنامي.

المطلب الأول :آليات التعاون الدولي في مكافحة الجرائم السيبيرانية

سنتطرق في هذا المطلب إلى جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية وبعض المنظمات الدولية كمنظمة التعاون الاقتصادي والتنمية والاتحاد الدولي للاتصالات

الفرع الأول: دور الأمم المتحدة في مكافحة الجريمة السيبرانية

أوصى المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة بأن تتولى المنظمة دورا رئيسيا في صياغة سياسة منع الجريمة وإرساء العدالة الجنائية الدولية، وقد تحقق ذلك عندما وافقت الجمعية العامة للأمم المتحدة على هذه التوصية في عام1950 مما أدى إلى إنشاء اللجنة الاستشارية لمنع الجريمة ومعاملة المجرمين التي تضطلع بمكافحة الجريمة وتقديم المشورة للأمين العام بالإضافة إلى وضع برامج ورسم سياسات للتدابير الدولية في هذا المجال[1] .

كما تجدر الإشارة إلى أن مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي عقد في ميلانو بإيطاليا عام 1985 أسفر عن مجموعة من القواعد التوجيهية والتي صيغت في الجلسات الإقليمية التحضيرية للمؤتمر الثامن الذي تبنى هذه المبادئ وعقد في هافانا بكوبا عاما1990.

كما أكد المؤتمر على ضرورة تطبيق التطورات الجديدة في العلم والتكنولوجيا في جميع الأماكن لصالح الجمهور وبالتالي منع الجريمة بفعالية، كما أكد على أن التكنولوجيا بما أنها سلاح ذو حدين ، فانه من المهم اتخاذ تدابير مناسبة لمنع إساءة استخدامها، وإقرار نظم كفيلة بوصول الأفراد إلى البيانات وتصحيح الأخطاء فيها،ويمكن إجمال توصيات مؤتمر هافانا 1990 في المبادئ التالية:

- تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية.
- تعزيز أمن الكمبيوتر والضوابط الوقائية.

---

[11] قطاف سليمان، بوقرين عبد الحليم: مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد، العدد 02 ، 2022 ،ص 73.

- توفير تدريب كافي للموظفين والهيئات المسؤولة عن منع الجرائم الاقتصادية وجرائم الحاسب الآلي والتحري والادعاء فيها .
- تضمين آداب الحاسب الآلي ضمن مقررات الاتصال والمعلومات وتبني سياسات لمعالجة القضايا المتعلقة بالضحايا في هذه الجرائم.
- تعزيز التعاون الدولي لمكافحة هذه الجرائم بشكل فعال.

كما عقد المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين بإشراف الأمم المتحدة في القاهرة عام 1990، حيث شدد على ضرورة حماية خصوصية الإنسان وحقوقه الفكرية من المخاطر المتزايدة للتكنولوجيا وأكد على أهمية التنسيق والتعاون المثمر بين مؤسسات وأفراد المجتمع الدولي لاتخاذ التدابير المناسبة للحد من هذه المخاطر.

ضف إلى ذلك أن أفضل إستراتيجية طويلة الأجل لمكافحة الجريمة السيبرانية هي من خلال الإتفاقيات الدولية أي التعاون في تقديم مرتكبي جرائم الكمبيوتر إلى العدالة نظرا للانتشار العالمي للانترنت[1].

الفرع الثاني: دور المنظمات الدولية في مكافحة الجريمة السيبرانية

اتخذت العديد من المبادرات بواسطة منظمات متعددة مثل الاتحاد الدولي للاتصالات منظمة التعاون الاقتصادي والتنمية، مؤسسة الأنترنت للأسماء والأرقام المخصصة، المنظمة الدولية لتوحيد المقاييس، اللجنة الكهروتقنية الدولية، بالإضافة إلى فرق عمل هندسة الانترنت ومنظمة التعاون الاقتصادي للمحيط الهادئ وآسيا ومنظمة الدول الأمريكية ورابطة دول جنوبشرق آسيا وجامعة الدول العربية والاتحاد الإفريقي وفي دراستنا هذه سوف نركز على عمل منظمتين كمثال.

- منظمة التعاون الاقتصادي والتنمية (OECD)

[1] المرجع نفسه ص 73 .

تركز هذه المنظمة على تحقيق أعلى مستويات النمو الاقتصادي وتحقيق التوازن بين التطور الاقتصادي والتنمية الاجتماعية، منذ عام 1978، بدأت المنظمة في التركيز على الجريمة السيبرانية من خلال وضع أدلة وقواعد توجيهية تتعلق بتقنية المعلومات، و كانمن أوائل الأدلة التي اعتمدها مجلس المنظمة في عام 1980 هو الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات مع توصية الأعضاء بالالتزام به،في عام 1983 أصدرت المنظمة تقريرا بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية استعرض السياسة الجنائية الحالية وقدم مقترحات خاصة بعدة دول أعضاء، وتضمن التقرير الحد الأدنى من الأفعال المتعلقة بإساءة استخدام الحاسوب التي على الدول تجريمها وتشمل هذه الأفعال:

- الاستخدام أو الدخول غير المصرح به إلى أنظمة وموارد الحاسوب.
- الإفشاء غير المصرح به للمعلومات المعالجة آليا والنسخ والإتلاف أو التخريب وما يتعلق بذلك من بيانات وبرامجوالتعطيل غير المشروع لموارد الحاسوب بهدف منع استخدام برامجه أو البيانات المخزنة فيه.[1]

– الاتحاد الدولي للاتصالات (ITU)

أصدر المؤتمر العالمي لتنمية الاتصالات عام 2006 القرار رقم 45 الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع حول الأمن المعلوماتي ومكافحة الرسائل غير المرغوب فيها وتقديم تقرير يتضمن نتائج الاجتماع إلى مؤتمر المندوبين المفوضين التي عقد في نفس السنة، وتمخض عنه تبني مجموعة من التوصيات في مجالي الأمن المعلوماتي والرسائل الاقتحامية، في عام 2007 أطلق الأمين العام جدول أعمال الأمن المعلوماتي العالمي الذي يهدف إلى وضع إطار كفيل بمواجهة الخطورة المتزايدة لأمن

[1]عبد العزيز بن فهد بن محمد بن داود:، الجرائم السيبرانية– دراسة صيلية مقارنة، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**،المجلد09 ،العدد 03
2020. ص149 ، .

الانترنت، والبحث عن حلول لتعزيز الأمن في مجتمع المعلومات، وفي أكتوبر 2007 أنشأ فريق من الخبراء رفيع المستوى يتكون من أكثر من مائة خبير قدموا تقاريرهم وتوصياتهم عام 2008، حيث نشرت الإستراتيجية العالمية في 12/11/2008 واشتملت على عدة مجالات التدابير القانونية والإجرائية الهياكل التنظيمية وبناء القدراتوالتعاون الدولي.[1]

الفرع الثالث: اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

دعا المجلس الدول العربية المصدقة على الاتفاقية إلى إبلاغ الأمانة الفنية للمجلس بالإجراءات التي اتخذتها من أجل موائمة تشريعاتها مع أحكام الاتفاقية وتجريم أشكال الجرائم الالكترونية المستحدثة لمنع الإرهابيين من استخدام الانترنت، كما دعا إلى تعزيز التعاون مع لمنظمات الدولية والإقليمية المعنية بمحاربة كافة أشكال جرائم الإرهاب الالكتروني،كما شجع المجلس الدول العربية على التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات والأنترنت بهدف التحريض على دعم أنشطتهم الإرهابية وتمويلها والتخطيط والإعداد لها،بالرغم من كل هذه الجهود الدولية سواء على مستوى الأمم المتحدة والمنظمات الدولية أو على المستوى الإقليمي وخاصة اتفاقية بودابست التي تعتبر بمثابة دعوة للدول لإعادة النظر في تشريعاتها الداخلية والدعوة إلى التعاون الدولي لأجل مكافحة الجرائم السيبرانية التي لا تعترف بالحدود الجغرافية إلا أن هناك صعوبات تواجه هذه الجهود تتمثل في:

- غياب نموذج موحد فيما يتعلق بالنشاط الإجرامي بالإضافة إلى افتقاد تعريف متفق عليه للأفعال التي ينبغياعتبارها جرائم.
- عدم وجود معاهدات ثنائية أو جماعية بين الدول يسهم في تعطيل التعاون المثمر في مكافحة هذه الجرائم، وحتى المعاهدات القائمة فإنها لاتزال غير قادرة على توفير

[1] قطاف سليمان، بوقرين عبد الحليم: مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد،العدد 02، 2022 . ص 77 ،

الحماية المطلوبة بسبب التطور السريع في أنظمة وبرامج الحاسب الآلي وشبكة الانترنت.

- تفتقر الدول فيما بينها إلى التنسيق في الإجراءات الجنائية المتعلقة بالجريمة المعلوماتية خاصة فيما يتعلق بالتحقيق وجمع الأدلة مشكلة الاختصاص في الجرائم الالكترونية تشكل عقبة كبيرة أمام الحصول على الأدلة نتيجة التداخل والترابط بين شبكات المعلومات، حيث يمكن أن تقع الجريمة في مكان معين وتنتج آثارها في مكان آخر"[1]

المطلب الثاني :تحديات التعاون الدولي في مكافحة الجريمة السيبرانية

رغم إدراك المجتمع الدولي لأهمية التعاون في مواجهة الجرائم السيبرانية، فإن هذا التعاون لا يزال يواجه جملة من التحديات المعقدة التي تحدّ من فاعليته. ويُعزى ذلك في المقام الأول إلى الطابع العابر للحدود الذي تتسم به هذه الجرائم، مما يصعّب تحديد الاختصاص القضائي ويطرح إشكاليات تتعلق بالسيادة الوطنية والاختلاف في الأنظمة القانونية.

الفرع الأول: القصور التشريعي للدول [2]

إن اختلاف الدول في موروثها الثقافي و الاجتماعي و مستواها السياسي أثر بشكل مباشر على السياسة التشريعية لكل دولة، و هذا ما جعل بعض الأنظمة القانونية تشكل عائقا كبيرا أمام التعاون الدولي، إذ إن هناك من الدول من تستشعر خطورة بعض الأفعال فتجرمها في قوانينها الداخلية، في حين أن دولاً أخرى لم تجرم هذه الأفعال مما يجعلها أفعالا مباحة تطبيقا لمبدأ الشرعية ، و هو ما ينطبق على الجرائم المعلو ماتية، إذ من الدول من لم تدرج نصوصا قانو نية لمو اجهة الآثار السلبية على هذه التقنية الحديثة و الناتجة عن

[1] عبد العزيز بن فهد بن محمد بن داود:، الجرائم السيبرانية– دراسة تفصيلية مقارنة، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، المجلد، العدد 03 ،2020 09، ص149.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر2008، ص102، .

الاعتداءات التي تلحق المعلو مات خاصة المخزنة في النظام المعلو ماتي، كما أن الاطلاع على الأنظمة القانونية القائمة في العديد من الدول لمكافحة الجرائم المعلوماتية يتضح عدم و جود اتفاق بين الدول على نماذج إساءة استخدام الأنظمة المعلوماتية و شبكة الأنترنت الو اجب تجريمها، أو بعبارة أخرى عدم وجود نظام قانوني موحد بين الدول خاص بمكافحة الجرائم المعلو ماتية، و العلة في ذلك هو كثرة التعاريف و المفاهيم القانونية المتعلقة بالجريمة المعلوماتية[1]

الفرع الثاني: اختلاف الأنظمة القانو نية الإجرائية

و يتجلى هذا العائق في اختلاف الأنظمة القانونيةالإجرائية بين الدول، ذلك أن طرق التحري و التحقيق و المحاكمة قد تثبت فعاليتها في دو لة ما إلا أنها تكو ن عكس ذلك في دو لة أخرى، أو لا يسمح بإجرائها لعدم مشروعيتها في هذه الدو لة، كما أن الدليل المتحصل عليه بالطرق غير المشروعة حسب قانون دولة ما لا يمكنها اعتماده كدليل إثبات حتى و ان كان قد تم الحصول عليه في اختصاص قضائي و بشكل مشروع حسب قانون الدولة الأخرى، و نذكر على سبيل المثال في هذا المجال إجراء المراقبة الالكترونية الذي تعتد به بعض الدول، في حين أن دولا أخرى ترى فيه مساسا بالحياة الخاصة مما يتعين استبعاده.

الفرع الثالث: تنازع الاختصاص القضائي الدولي

يقصد بتنازع الاختصاص القضائي بين الدول تقديم دعوى عن ذات الجريمة أو عدة جرائم مرتبطة إلى جهتين أو أكثر من جهات التحقيق أو الحكم، و تمسّك كل جهة باختصاصها بالنظر أو التحقيق في الدعوى و هو ما يعرف بتنازع الاختصاص الإيجابي، أو رفض كل دولة النظر في الدعوى على أساس عدم ختصاصها و هو ما يسمى بتنازع الاختصاص السلبي، و عليه يتحقق تنازع الاختصاص الدو لي في الجريمة المعلو ماتية في الحالة التي

[1] رشيدة بو كر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأو لى، منشو رات الحلبي الحقو قية،لبنان، 2012، ص86.

إلى [1]نظام معلو ماتي لأحد أجهزة دو لة ما غير التي يقيم بها، فيقو م فيها مثلا أجنبي بإرسال فيروس فيقوم بتدميروالاتلاف المعلومات المو جودة به، و هنا يقوم الاختصاص للدو لة التي ارتكب على إقليمها الجريمة اعتمادا على مبدأ الإقليمية، كما يقوم الاختصاص أيضا للدولة التابع لها الأجنبي مرتكب الجريمة استنادا لمبدأ الشخصية، و في الأخير يقوم الاختصاص أيضا للدولة التي هدد أمنها و سلامة مصالحها الجوهرية بغض النظر عن مكان ارتكاب الجريمة أو جنسية الجاني و هو ما يطلق عليه مبدأ العيني، و عليه يكو ن التساؤل عن الدولة المختصة هل هي الدو لة التي ارتكب على إقليمها الفعل الإجرامي؟ أم الدو لة التي حدثت نتيجة الفعل فيها؟ أو بعبارة أخرى الدو لة التي لحق الضرر مصالحها الأساسية؟ أم الدو لة التي يحمل المجرم المعلوماتي جنسيتها و عالج المشرع الجزائري هذه المسألة من خلال القانون 09/04 المتضمن القو اعد الخاصة للوقاية من الجرائم المتصلة بتكنو لوجيات الإعلام و الاتصال و مكافحتها إذ أكد في المادة 15 منه على مبدأ العينية بالإضافة إلى مبدأ الإقليمية و مبدأ الشخصية، و عليه تنص المادة 15 على أنه "زيادة على قو اعد الاختصاص المنصوص عيها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا و تستهدف مؤسسات الدو لة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني"

الفرع الرابع: الإشكالات الخاصة بالإنابة القضائية

يثير التعاون القضائي الدولي لمكافحة الجرائم المعلوماتية عن طريق الإنابة القضائية إشكاليات تتمثل في فكرة السيادة، وكذلك إشكالية البطء في الإجراءات .

أ- إشكالية فكرة السيادة:

يقصد بالسيادة: "استئثار جهة الحكم في الدو لة بكافة اختصاصات السلطة و مظاهرها، دون أن تخضع في ذلك لأي جهة أعلى، و دو ن أن تشارك معها في ذلك سلطة أو جهة مماثلة و تثور إشكالية فكرة السيادة في الحالة التي يرتكب فيها الجاني جرما على إقليم دو لة ما و تجري محاكمته في دو لة أخرى، فحتى تقام محاكمة عادلة لابد من جمع الأدلة التي تثبت الجريمة و يتم نسبتها للجاني، و هذا لا يتحقق إلا على إقليم الدولة التي كانت مسرحا للجريمة و هو ما يعرف بالتعاون القضائي الدولي، إلا أن هذا التعاون يصطدم مع فكرة السيادة التي تتمسك بها الدو لة على إقليمها، و من ثم لا تسمح لدو لة أخرى القيام بالإجراءات على إقليمها، و انما تقوم بها عن طريق أجهزتها القضائية باعتبارها صاحبة الاختصاص بالفصل في كافة الجرائم المرتكبة على إقليمها اعتمادا على فكرة السيادة[1].

ب- إشكالية البطء في إجراءات الإنابة القضائية:

إن إرسال طلبات الإنابة القضائية بالطريق الدبلو ماسي يجعلها تتسم بالبطء و التعقيد الذي يتعارض مع طبيعة و خصائص الجريمة المعلو ماتية التي تتميز بالسرعة، إذ يمكن تدمير أدلة الإثبات، و هو ما انعكس سلبا على فكرة التعاو ن الدو لي. في مكافحة هذا النو ع المستحدث من الجرائم، تفعيل كما أن التباطؤ في الرد بسبب نقص المو ظفين، أو الصعو بات اللغو ية، أو الاختلاف في الأنظمة الإجرائية يحول دون تفعيل التعاون الدولي.

<u>الفرع الخامس: الإشكاليات الخاصة بتسليم المجرمين</u>

من بين الإشكاليات التي يثيرها تسليم المجرمين نجد إشكاليتي ازدواجية التجريم و التزاحم في طلبات التسليم:

أ- ازدو اجية التجريم :

[1] جميل عبد الباقي الصغير، الجو انب الإجرائية للجرائم المتعلقة بالأنترنت، دار الفكر العربي، مصر، 2001، ص72.

إن التجريم المزدو ج من أهم الشروط الخاصة بنظام تسلي المجرمين، إلا أنه بالرغم من أهميته فإنه يشكل عقبة أمام التعاو ن القضائي في مجال تسليم المجرمين بشأن الجرائم المعلوماتية، خاصة و أن معظم التشريعات قد أغفلت النص على هذا النو ع من الجرائم، بالإضافة إلى ثبو ت عجز مواكبة النصو ص التقليدية لهذا النو ع المستحدث من التجريم، و هو الأمر الذي يشكل عائقا أمام تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، و يحو ل دو ن جمع الأدلة لإدانة مرتكبي الجرائم المعلوماتية[1] .

ب- التزاحم في طلبات التسليم

يقصد بالتزاحم في طلبات التسليم قيام دو لتين أو عدة دول بتقديم طلب تسليم عن نفس الشخص، سواء كان الطلب متعلقا بذات الجريمة أو بجرائم مختلفة، و تتحقق هذه الإشكالية في الجرائم المعلو ماتية عندما يرتكب الجاني الفعل الإجرامي الذي يمس في ذات الو قت مصالح أساسية لأكثر من دولة، و عليه فكل دو لة لحقها ضرر جراء النشاط الإجرامي الذي قام به الجاني يمكنها تقديم طلب التسليم إلى الدولة المطلوب منها.

و الجدير بالذكر أن طلب التسليم لابد أن يكو ن مبنيا على أدلة تثبت قيام الجاني بالأفعال المنسوبة إليه، و ليس مجرد ادعاء من الدو لة الطالبة، كما يشترط أن يكو ن إرسال الطلب بصو رة فعلية و ليس مجرد تصريحات شفوية ، أو إبداء الرغبة في استلام الشخص .

لا يشترط أن تكو ن طلبات التسليم قد و ردت إلى الدو لة المطلو ب منها في ذات الوقت، بل يكفي أن تكو ن طلبات التسليم قد و ردت إلى الدو لة المطلو ب منها تسليم شخص في الو قت الذي مازال فيه المطلو ب على إقليمها، و لم يتم تسليمه بعد لأي دولة من الدو ل التي تطالب به .

المبحث الثاني:المكافحة الدولية للجريمة السيبرانية.

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

في ظل التحول الرقمي الذي يشهده العالم، أصبحت الجريمة السيبرانية تمثل تهديدًا حقيقيًا ومتناميًا لأمن الأفراد والدول على حد سواء، وذلك لما تتميز به من طابع تقني معقد، وحدود جغرافية مفتوحة، وأساليب متجددة يصعب تتبعها أو الحد منها بوسائل تقليدية. وبفعل هذا التهديد المتصاعد، لم يعد من الممكن الاقتصار على المعالجات الوطنية لمواجهته، بل بات من الضروري تفعيل أطر التعاون الدولي، وإرساء قواعد قانونية موحّدة تتيح للدول تبادل المعلومات، وتنسيق الجهود، وتطوير وسائل التصدي الفعّالومن هذا المنطلق، يتناول هذا المحور دراسة أوجه المكافحة الدولية والوطنية للجريمة السيبرانية، من خلال تحليل الاتفاقيات الدولية ذات الصلة، واستعراض الجهود الوطنية المبذولة، مع بيان التحديات التي تواجه هذه المنظومة.

المطلب الأول : التعاون الدولي في مكافحة الجريمة السيبرانية

الفرع أول: أهمية التعاون الدولي في المجال السيبراني

تُعد الجريمة السيبرانية من أكثر التهديدات تعقيدًا في العصر الرقمي، نظرًا لطبيعتها العابرة للحدود. فالجاني قد يتواجد في دولة، والضحية في دولة أخرى، مما يجعل التحقيق والملاحقة القضائية أمرًا معقدًا لا يمكن مواجهته بشكل فردي. لذلك، أضحى التعاون الدولي ضرورة حتمية لضمان فعالية التصدي لهذه الجريمة، سواء من حيث تبادل المعلومات أو ملاحقة المجرمين أو توحيد التشريعات.

يشمل هذا التعاون:

تبادل البيانات والمعلومات حول الجرائم الإلكترونية والجهات المشتبه بها.

تقديم المساعدة القانونية المتبادلة في التحقيقات والملاحقات القضائية.

تدريب الكوادر الأمنية والقضائية على أحدث الأساليب التكنولوجية للكشف عن الجرائم الرقمية.

الفرع ثاني: صور التعاون الدولي في مكافحة الجريمة السيبرانية

1. التعاون الأمني عبر المنظمات الدولية:

تلعب منظمة الإنتربول دورًا رئيسيًا من خلال "المركز العالمي للابتكار" الذي يدعم الدول الأعضاء في مواجهة التهديدات السيبرانية عبر تبادل التحذيرات الأمنية وتحليل الأدلة الرقمية.

كما يساهم مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) في بناء قدرات الدول النامية، خاصة في مجال تطوير استراتيجيات الأمن السيبراني والتشريعات الوطنية.

2. الاتفاقيات الدولية والإقليمية:

اتفاقية بودابست (2001) الخاصة بمكافحة الجريمة السيبرانية، والتي أرست نموذجًا دوليًا للتعاون في التحقيقات الجنائية الإلكترونية.[1]

اتفاقية مالابو الإفريقية (2014) التي تهدف إلى تعزيز أمن الفضاء السيبراني داخل الدول الإفريقية.

جهود الاتحاد الأوروبي عبر وحدة "يوروبول" المتخصصة في الجرائم الرقمية.

3. الشراكات الثنائية والمتعددة الأطراف:

كثير من الدول وقعت اتفاقيات ثنائية لتبادل المعلومات والتعاون في التحقيقات المتعلقة بالجريمة السيبرانية، مثل التعاون بين الولايات المتحدة ودول آسيا.

[1] – لأمم المتحدة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، مكافحة الجريمة السيبرانية: دليل الممارسات الجيدة، فيينا، 2013. ص 55

المنتديات العالمية مثل منتدى حوكمة الإنترنت IGF تتيح تبادل الخبرات وتنسيق الجهود.

ثالثًا: التحديات التي تواجه التعاون الدولي

رغم التقدم المحرز، لا يزال التعاون الدولي يواجه عدة عوائق، منها:

الاختلاف في تعريف الجريمة السيبرانية بين الدول، ما يُصعب التعاون القضائي.

غياب الثقة بين بعض الدول خاصة في القضايا ذات الطابع السيادي أو الأمني.

التقدم التكنولوجي السريع الذي يفوق قدرة التشريعات الدولية على المواكبة.

صعوبات تسليم المجرمين لاعتبارات قانونية أو سياسية.

المطلب الثاني : التشريعات الدولية المتعلقة بالجرائم السيبرانية

نظرًا للطبيعة العابرة للحدود التي تتميز بها الجرائم السيبرانية، أصبح من الواضح أن مواجهتها لا يمكن أن تتم بشكل فعال من خلال الجهود الوطنية المنفردة فقط، بل تتطلب تنسيقًا وتعاونًا دوليًا شاملاً. فهذه الجرائم، التي تُرتكب في فضاء إلكتروني لا تعترف حدوده بالسيادة التقليدية للدول، تمثل تهديدًا مشتركًا للمجتمع الدولي، ما دفع بالعديد من الدول والمنظمات إلى البحث عن أطر قانونية وآليات تعاون تسمح بملاحقة الجناة وتبادل المعلومات والأدلة الرقمية بصورة تتجاوز العوائق القضائية والحدود الإقليمية[1].

وفي هذا السياق، برزت الاتفاقيات الدولية كوسيلة أساسية لتوحيد المفاهيم القانونية وتسهيل التعاون القضائي والتقني بين الدول، حيث تم التوصل إلى عدد من الصكوك القانونية الدولية التي تُعد اليوم المرجع الأساسي في هذا المجال، وعلى رأسها "اتفاقية بودابست لمكافحة الجريمة السيبرانية" التي أقرها مجلس أوروبا عام 2001، والتي شكلت أول اتفاقية دولية مخصصة لهذا النوع من الجرائم .

[1] المرجع السابق ،ص 370

ويهدف هذا الجزء من البحث إلى تسليط الضوء على أبرز هذه الاتفاقيات، من حيث مضمونها، وأهدافها، وآليات تنفيذها، ومدى فعاليتها في تعزيز الجهود الدولية لمكافحة الجريمة السيبرانية، إلى جانب الإشارة إلى أوجه القصور التي ما زالت تحد من فاعلية هذه الاتفاقيات في ظل التغير المستمر في أساليب وتقنيات ارتكاب الجرائم الإلكترونية.

الفرع الأول: مكافحة الجريمة السيبرانية دوليا

في مجال مكافحة الجرائم السيبرانية بصفة عامة عقدت المعاهدات والاتفاقيات التي تعمل على تكريسالتعاون الدولي في مجال مكافحة الجرائم الإلكترونية نذكر منها معاهدة بودابست لمكافحة جرائم الإنترنت ، توصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، كما ننوه بمساعي الجمعية العامة للأمم المتحدة لدراسة الوضع بشأن الجريمة السيبرانية ونبينهما فيما يلي:

أولا: معاهدة بودابست لمكافحة جرائم الإنترنت

تعد معاهدة بودابست لمكافحة جرائم الإنترنت أولى المعاهدات المتعلقة بتلك الجرائم والتي تمت في العاصمة المجرية بودابست في 2001/11/23، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت، وقد وقعت على تلك المعاهدة 26 دولة أوروبية بالإضافة إلى كندا واليابان وجنوب أفريقيا، والولايات المتحدة الأمريكية، وتوفر المعاهدة أسس الأمن العام وتتضمن 48 مادة مقسمة على أربعة فصول.

وتهدف الاتفاقية إلى :

1-توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

2-توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيا بواسطة الكمبيوتر.

3-تعيين نظام سريع وفعال للتعاون الدولي.

4-الحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

5-جمع معلومات عن حركة البيانات وعن إمكان وجود تدخل في محتواها.[1]

نرى من خلال مبادئ معاهدة بودابست حرصها على التعاون الدولي من خلال القوانين الجزائية الوطنية المتعلقةبهذا النوع من الجرائم بإعتبار كل دولة تحاول الحفاظ على أمنها القومي وإقتصادها وإستقرار نظامها السياسي منخلال العمل على أمنها السيبراني أي حماية قاعدة بياناتها، ولما كانت الجريم السيبرانية عابرة للحدود فمن المنطقي أن تنطلق في دولة وتنتهي في أخرى، مما جعل التعاون لمكافتحها وملاحقة المجرمين ضرورة لا مفر منها .

ثانيا :مكافحة الجريمة الإلكترونية من خلال هيئة الأمم المتحدة

طلبت الجمعية العامة، في قرارها 65-230 من لجنة منع الجريمة والعدالة الجنائية أن تنشئ، وفقا للفقرة 42 من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية:

نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير من خلال تكوين فريق خبراء حكومي دولي مفتوح العضوية من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبيرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية وأفضل الممارسات والمساعدة الفنيةأنوالتعاون الدولي، بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من

[1]- عبد الله أحمد هلالي، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست (2001 دارالنهضة العربية، ط 2001، ص 30.

التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجرائم السيبرانية وإقتراح تدابير جديدة في هذا الشأنأحاطت الجمعية العامة علما في قرارها 18967 بعمل فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية، وشجعته على تحسين الجهود التي يبذلها من أجل إنجاز أعماله و عرض نتائج الدراسة في الوقت المناسب على لجنة منع الجريمة والعدالة الجنائية.

وعقدت الدورة الأولى لفريق الخبراء في فيينا في الفترة الممتدة من 17 الى 21 جانفي 2011 وقام خلالها فريق الخبراء باستعراض واعتماد مجموعة من المواضيع وكذلك منهجية للدارسة تضمنت مجموعة المواضيع المطروحة للنظر فيها ضمن إطار الدراسة الشاملة للجريمة السيبرانية، مشكلة الجريمة السيبرانية، وتدابير التصدي القانونية للجريمة السيبرانية، وقدرات منع الجريمة والعدالة الجنائية وتدابير التصدي الأخرى للجريمة السيبرانية، والمنظمات الدولية، والمساعدة الفنية . ثم قسمت هذه الموضوعات الى 12 موضوعا فرعيا تناول هذه الموضوعات في سياق هذه الدراسة في ثمانية فصول. وفي إطار منهجية الدراسة؛ كلف مكتب الأمم المتحدة المعني بالمخدرات والجريمة بإعداد الدراسة، بما في ذلك إعداد استبيان بهدف جمع المعلومات، وجمع البيانات وتحليلها، وإعداد مشروع لنص الدراسة.[1]

وتقرر في إطار جمع المعلومات وفقا لمنهجية الدراسة التي أعدها مكتب الأمم المتحدة المعني بالمخدرات والجريمة، توزيع استبيان على الدول الأعضاء والمنظمات الحكومية الدولية وممثلين عن القطاع الخاص والمؤسسات الأكاديمية من شهر فيفري 2012 الى غاية جويلية 2012 وقد وردت إلى مكتب الأمم المتحدة المعني بالمخدرات والجريمة معلومات من 69 دولة عضوا. واستعرضت الأمانة أيضا أكثر من 500 وثيقة من مصادر مفتوحة . ويتضمن الملحق الخامس بهذه الدراسة مزيدا من التفاصيل بشأن المنهجية.

[1]– نفس المرجع السابق , ص31.

تناولت الدراسة مشكلة الجريمة السيبرانية من خلال منظور الحكومات، والقطاع الخاص، والأوساط الأكاديمية،والمنظمات الدولية، وقد تم طرح النتائج في ثمانية فصول تناولت الموص ولية الخاصة بشبكة الإنترنت والجريمة السيبرانية والصورة العالمية للجريمة السيبرانية وأطر وتشريعات مكافحة الجريمة السيبرانية، وتحريم الجريمة السيبرانية، وإنفاذ القانون والتحقيقات في الجريمة السيبرانية والأدلة الإلكترونية والعدالة الجنائية والتعاون الدولي في المسائل الجنائية التي تنطوي على جريمة سيبرانية، والوقاية الجريمة السيبرانية.[1]

الفرع الثاني: الآليات القانونية الإقليمية لمكافحة الجريمة السيبرانية

يأخذ التعاون الدولي شكلا دوليا أو إقليميا داخل تحالفات مثل ما هو عليه الإتحاد الأوروبي والذي عمل على مكافحة الجريمة السيبرانية على المستوى الإقليمي وأصدر توصيات في هذا الشأن من خلال المجلس الأوروبي بإعتبارهاهيئة إستراتيجية توجه السياسات العامة للإتحاد الأوروبي هذه التوصيات التي سنتناولها في النقاط التالية :

أولا:توصيات المجلس الأوروبي

أدى التطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجزائية في هذا المجال إلى إصدار المجلس الأوروبي التوصية رقم 95/13 المؤرخ في 1995/09/11 في شأن مشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، وحث الدول الأعضاء بمراجعة قوانين الإجراءات الجزائية الوطنية لكي تتلاءم من التطور في هذا المجال، ومن أهم ما ورد بتوصية المجلس الأوروبي ما يلي:

1-أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.

[1]- دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فينا، 2013، ص 13

2-أن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محلا للتفتيشمع بيان المعلومات التي تم ضبطها، ويسمح بإتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش.

3-أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع إحترام الضمانات المقررة بعد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة إختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط ان يكون هذا الإجراء ضروريا.

4-أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.

5-تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية والإحترام للمعلومات التي يفرض القانون لها حماية خاصة.

6-يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.

7-يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء كانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.[1]

8-يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحتويه من معلومات باتخاذ الازم للسماح لرجال التحقيق بالاطلاع عليها، وأن تخول سلطات التحقيق

[1]- مدحت رمضان جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط 2000 ، ص 80

بإصدار أوامر مماثلة لأي شخص لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.

9-يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع ادله معينة ويتعين عندئذ ان تسمح السلطة الأخيرة بإجراءات التفتيش والضبط ويتعينكذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها ولذلك يتعين تطوير اتفاقيات التعاون الدولي القائمة.

ثانيا : إتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

أقرت جامعة الدول العربية قانونا استرشاديا لمكافحة جرائم الفضاء السيبيراني، وقد سعت الدول العربية لتقنين وتحريم الأعمال الغير مشروعة المرتكبة من خلال إستخدام الفضاء السيبيراني بالتوقيع على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات من أجل تعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبيرانية والحفاظ على أمنها وسلامة مجتمعاتها، حيث دعا المجلس، إلى موافاة الأمانة الفنية للمجلس ما إتخذته من إجراءات لموائمة تشريعاتها مع أحكام الإتفاقية وتحريم الصور المستحدثة من الجرائم الإلكترونية لمنع الإرهابيين من إستخدام الإنترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال جرائم الإرهاب الإلكترونية.

كما دعا المجلس الى تفعيل التعاون لمنع المجرمين من استغلال تكنولوجيا المعلومات والاتصالات والإنترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها، وأكد المجلس على أهمية تعزيز التعاون المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، ودعم أمن المطارات والموانئ والحدود.

بالرغم من كل هذه الجهود الدولية سواء على مستوى الأمم المتحدة والمنظمات الدوليه أو على المستوى الإقليمي وخاصة إتفاقية بودابست التي تعتبر بمثابة دعوة للدول لإعادة النظر في تشريعاتها الداخلية والدعوة إلى التعاون الدولي لأجل مكافحة الجرائم السيبرانية التي لا تعرف الحدود الجغرافية .[1]

خلاصة الفصل

لقد أظهرت الدراسة أن الجرائم السيبرانية تمثّل أحد أبرز التحديات المعاصرة التي تواجه المجتمع الدولي، حيث تتخطى هذه الجرائم حدود السيادة الوطنية وتطال الأفراد والمؤسسات والبنى التحتية الحيوية على مستوى عالمي. وفي مواجهة هذه التهديدات، باتت الحاجة ملحة إلى بناء نظام قانوني دولي متكامل ومرن، يستجيب لتطورات الفضاء الرقمي ويواكب أنماط الجريمة المتجددة.

[1]– نفس المرجع السابق ، ص 81.

تشكل الاتفاقيات الدولية مثل إتفاقية بودابست واتفاقية مالابو، إضافة إلى المبادرات الأممية الجارية، محاولات مهمة لرسم ملامح تعاون قانوني دولي، إلا أن نجاح هذه الجهود لا يكمن فقط في النصوص القانونية، بل في الآليات العملية للتنفيذ والتعاون الميداني بين الدول. ويبرز في هذا السياق دور آليات تبادل المعلومات، والمساعدةالقانونية المتبادلة، والتدريب، والتحقيقات المشتركة، بوصفها أدوات أساسية لتعزيز الفعالية في مواجهة الجرائم السيبرانية.

غير أن هذه الآليات تواجه العديد من التحديات، أبرزها التفاوت في البنية التحتية الرقمية بين الدول، وتباين الرؤى السياسية والقانونية حول مفاهيم مثل حرية التعبير، السيادة الرقمية، والخصوصية، إضافة إلى غياب الثقة بين بعض الدول، ما يعيق تبادل المعلومات الحساسّة.

في المحصلة لا يمكن لأي دولة بمفردها أن تواجه التهديدات السيبرانية المعقدة والمتغيرة باستمرار فالمعركة ضد الجرائم السيبرانية هي مسؤولية جماعية تتطلب تضامنًا دوليًا، وتنسيقًا متواصلًا، وتحديثًا تشريعيًا مرنًا يستند إلى احترام سيادة القانون وحقوق الإنسان. ويبقى الاستثمار في بناء الثقة الدولية، وتطوير القدرات المؤسسية، وتفعيل الاتفاقيات القائمة، هو السبيل الأمثل نحو فضاء سيبراني أكثر أمنًا وتعاونًا واستدامة.

الخاتمة

خاتمـــة

الخاتمة:

مع ختام هذه الدراسة ،يمكننا التأكيد على أن الجرائم السيبرانية أصبحت من أبرزالتحديات التي تواجه المنظومة القانونية و الأمنية في العصر الحديث، نظرًا لطابعها المستحدث، وطبيعتها المتغيرة ،واتساع نطاقها عبرالفضاء الرقمي. لقد تناولنا منخلال هذه المذكرة الإطار المفاهيمي للجرائم السيبرانية، وعرّفنا بأشكالها وخصائصها، ثم انتقلنا إلى دراسة آليات واستراتيجيات التعاون الدولي في مواجهتها، مع تحليل أبرز الاتفاقيات والتجارب الدولية.

أولًا: النتائج المتوصل إليها

1. تُعدالجرائم السيبرانية جرائم معقدة تتطلب مقاربة شاملة، نظرًا لتعدد أطرافها و تداخل حدودها الجغرافية.

2.هناك تفاوت كبير في التشريعات الوطنية بشأن تعريف و تجريم الجرائم السيبرانية، مما يُضعف من فعالية التعاون الدولي.

3. تظل اتفاقية بودابست لعام 2001من أبرز أدوات التعاون الدولي، لكنها لم تحظ بالإجماع الدولي، مما يحد من فعاليتها.

4.يشكل نقص الكوادر المتخصصة والتجهيزات التقنية عقبة أمام الكثير من الدول، لا سيما النامية، في التصدي لهذا النوع من الجرائم.

5.التعاون بين الدول في هذا المجال ما يزال هشًّا، ويواجه عقبات سياسية و قانونية و تقنية تحول دون الاستجابة السريعة و المشتركة.

ثانيًا: التوصيات

خاتمــة

1.ضرورة توحيد الإطار القانوني الدولي لمكافحة الجرائم السيبرانية، من خلال العمل على إعداد اتفاقية دولية شاملة تحظى بإجماع واسع.

2.تفعيل مذكرات التعاون القضائي والفني بين الدول، لتسهيل تبادل المعلومات والمساعدة القانونية المتبادلة في زمن قياسي.

3. تعزيزقدرات الدول النامية في مجال الأمن السيبراني عبر برامج تكوين وتدريب ودعم تقني منتظم.

4.اعتماد استراتيجية وطنية شاملة للأمن السيبراني في كل دولة، تشمل الجوانب القانونية، التقنية، التوعوية ، والوقائية.

5.توسيع التعاون مع القطاع الخاص، خاصة الشركات التكنولوجية و مزودي خدمات الإنترنت، لكونهم يملكون المعطيات والأدوات اللازمة للكشف المبكرعن الجرائم.

6.تشجيع البحث العلمي في مجال الجريمة الرقمية و القانون السيبراني، وربط الجامعات ومراكز الدراسات بمراكز اتخاذ القرار.

ختامًا

إنّ مكافحة الجريمة السيبرانية ليست مسؤولية دولة واحدة ،بل هي مسؤولية جماعية تتطلب تضافر الجهود الدولية وتجاوز الخلافات السياسية من أجل بناء فضاء إلكتروني آمن وعادل. كما أن المستقبل الرقمي لا يمكن أن يكون آمنًا ما لم يُدعّم بمنظومة قانونية عادلة، متطورة، وفعّالة.

قائمة المصادر و المراجع

فهرس المحتويات

قائمة المصادر و المراجــع:

[1] – عادل يوسف عبد النبي الشكري، بحث بعنوان الجريمة المعلوماتية و أزمة الشرعية الجزائية، جامعة الكوفة 221–222.

[1] – مفتاح بوبكر المطرودي، الجريمة الإلكترونية و التغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث إلى رؤساء المحاكم العليا في الدول العربية من جمهورية السودان ، المنعقد في عام 2008. ص 214.

[1] – حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي ، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة، نقلاً عن قورة نائلة، جرائم الحاسب الإقتصادية ،القاهرة 2011. ص 115.

[1] – مليكة عطوي الجريمة المعلوماتية حوليات جامعة الجزائر ، مجلة علمية 2017 العدد 85 ص.159.

[1] – سعيداني نعيم آليات البحث و التحري عن الجريمة المعلوماتية، القانون الجزائري ،مذكرة ماجستير في العلوم القانونية تخصص علوم جنائية ، جامعة الحاج لخضر باتنة، الجزائر 2013 ص 42.

[1] – قارة أمال الجريمة المعلوماتية ماجستير تخصص قانون جنائي و العلوم الجنائية كلية الحقوق بجامعة الجزائر ، 2005ص01

[2] – لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها و آلية مكافحتها ، دراسة تحليلية مقارنة، مجلة الميزان ، المجلد 04 العدد 1 جامعة العلوم الإسلامية العالمية ، الأردن 2017 ص 189.

[1] –صغير يوسف ، الجريمة المرتكبة عبر الأنترنت ، مذكرة لنيل شهادة الماجستير في القانون ، تخصص القانون الدولي للأعمال ، جامعة مولود معمري تيزي وزو 2016 ص45 .

[1] – سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية ، مذكرة مكملة لمتطلبات نيل شهادة الماستر في الحقوق تخصص قانون جنائي جامعة محمد خيضر بسكرة 2018 ص 111.

[1] مزغيش سمية مصدر سابق ص116 .

قطاف سليمان، بوقرين عبد الحليم: مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد، العدد 02 ، 2022 ،ص 73.

المرجع نفسه ص 73 .

عبد العزيز بن فهد بن محمد بن داود:، الجرائم السيبرانية– دراسة صيلية مقارنة، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**،المجلد09 ،العدد 03
2020. ص149 ، .

فهرس المحتويات

قطاف سليمان، بوقرين عبد الحليم: مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد،العدد 02، 2022 . ص 77 ،

عبد العزيز بن فهد بن محمد بن داود:، الجرائم السيبرانية– دراسة تفصيلية مقارنة، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، المجلد، العدد 03 ،2020 09، ص149.

عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر2008، ص102،

رشيدة بو كر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأو لى، منشو رات الحلبي الحقو قية،لبنان، 2012، ص86.

جميل عبد الباقي الصغير، الجو انب الإجرائية للجرائم المتعلقة بالأنترنت، دار الفكر العربي، مصر، 2001، ص72.

عزيزة لرقط ،التعاون الدولي في مكافحة الجرائم المعلوماتية إشكالاتها وآليات التغلب عليها ،مجلة التواصل في الاقتصاد وإدارة القانون المجلد 25-عدد 04 -ديسمبر 2019

[1] – لأمم المتحدة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، مكافحة الجريمة السيبرانية: دليل الممارسات الجيدة، فيينا، 2013. ص 55

المرجع السابق ،ص 370

– عبد الله أحمد هلالي، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست (2001 دارالنهضة العربية، ط 2001، ص 30.

– دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فينا، 2013، ص 13

– مدحت رمضان جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط 2000 ، ص 80

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

ملخص :

التعاون الدولي في مكافحة الجريمة السيبرانية ضروري لمواجهة التحديات المتزايدة في هذا المجال، حيث يسهل تبادل المعلومات وتنسيق الجهود بين الدول، وتطوير القدرات، ووضع السياسات. تشمل الأمثلة على هذا التعاون الاتفاقيات الدولية مثل اتفاقية بودابست، والمنظمات الدولية مثل الاتحاد الدولي للاتصالات والإنتربول، والتعاون الثنائي والمتعدد الأطراف بين الدول، مما يعزز الأمن السيبراني العالمي ويقلل من تأثير الجرائم السيبرانية.

SUMMARY

International cooperation in combating cybercrime is essential to address the growing challenges in this field, facilitating information sharing, coordination of efforts among countries, capacity development, and policy formulation. Examples of this cooperation include international agreements such as the Budapest Convention, international organizations like the International Telecommunication Union and Interpol, and bilateral and multilateral cooperation among countries, which enhances global cybersecurity and reduces the impact of cybercrime.