وزارة التعليم العالي و البحث العلمـي

جامعة عباس لغرور–خنشلة–

كلية الحقوق والعلوم السياسية

قسم الحقوق

نيابة العمادة للدراسات وشؤون الطلبة

دور الاتفاقيات الدولية والإقليمية في مكافحة الجريمة الإلكترونية

مذكرة مكملة لنيل شهادة الماستر (ل.م.د)

تخصص: قانون جنائي و علوم جنائية

إعداد الطالبة :

- مراح ندي الريحان
- عايب وردة

إشراف الأستاذة:

الدكتورة خديجة عمراوي

لجنة المناقشة

الاسم و اللقب	الرتبة	الجامعة الأصلية	الصفة
أ.د/ بن مبارك ماية	أستاذ التعليم العالي	جامعة عباس لغرور–خنشلة–	رئيسا
د/عمراوي خديجة	أستاذ محاضر– أ–	جامعة عباس لغرور–خنشلة–	مشرفا ومقررا
د/ هباز سناء	أستاذ محاضر – أ–	جامعة عباس لغرور–خنشلة–	مناقشا

السنة الجامعية: 2023–2024

وزارة التعليم العالي و البحث العلمـي

جامعة عباس لغرور–خنشلة–

كلية الحقوق والعلوم السياسية

قسم الحقوق

نيابة العمادة للدراسات وشؤون الطلبة

دور الاتفاقيات الدولية والإقليمية في مكافحة الجريمة الإلكترونية

مذكرة مكملة لنيل شهادة الماستر (ل.م.د)

تخصص: قانون جنائي و علوم جنائية

إعداد الطالبة :

- مراح ندي الريحان
- عايب وردة

إشراف الأستاذة:

الدكتورة خديجة عمراوي

لجنة المناقشة

الاسم و اللقب	الرتبة	الجامعة الأصلية	الصفة
د/ بن مبارك ماية	أستاذ التعليم العالي	جامعة عباس لغرور–خنشلة–	رئيسا
د/عمراوي خديجة	أستاذ محاضر– أ–	جامعة عباس لغرور–خنشلة–	مشرفا ومقررا
د/ هباز سناء	أستاذ محاضر – أ–	جامعة عباس لغرور–خنشلة–	مناقشا

السنة الجامعية: 2023–2024


بسم الله الرحمن الرحيم

شكر و عرفان

الحمد لله حمدا كثيرا غير مكفى، ولا مستغنى عنه، والصلاة والسلام على خير من علمنا أدب الشكر، وعمل به سيدنا محمد وعلى آله وأصحابه، ومن اقتدى به وبعد:

حدثنا ديننا الحنيف على أن ننسب الفضل لأهله، وأن نشكر من يستحق الشكر عرفانا بالجميل

إن أحق الناس بأسمى عبارات الشكر والتقدير والامتنان الدكتورة:

عمراوي خديجة

عرفانا بفضلها وعملها وتوجيهاتها أطال الله في عمرها وسدد خطاها وأدامها ذخرا للعلم والمعرفة

نشكر كذلك كل أعضاء اللجنة التي ستناقش هذا العمل

نشكر كل من ساعدنا من قريب أو بعيد ولو بكلمة طيبة من أساتذة وطلبة

إهداء

أهدي هذا العمل إلى:

صاحب الوجه الطيب و الأفعال الحسنة، فلم يبخل علينا طيلة حياته" والدي العزيز" أطال الله في عمره

إلى من وضع المولى سبحانه وتعالى الجنة تحت قدميها ووقرها في كتابه العزيز" أمي الحبيبة" رحمها الله و أسكنها فسيح جنانه

إلى من عوضتنا حنان أمي بعد فراقها "جدتي الحبيبة" حفظها الله

إلى أختي سندي و عضدي و مشاطرة أفراحي و أحزاني" زينب"

إلى صديقتي الوفية ورفيقة دربي" عايب وردة"

إلى كل من وقف إلى جانبي وسندني

الطالبة: مراح ندي الريحان

إهداء

إلى من وهبوني الحياة و الأمل و النشأة على الشغف الاطلاع و المعرفة، ومن علموني بأن ارتقي بسلم الحياة بحكمة وصبر برا و إحسانا ووفاء إليهما: أمي الحبيبة رحمها الله، ووالدي العزيز

إلى من وهبني الله نعمة وجودهم في حياتي إلى العقد المتين من كانو لي عونا في رحلة بحثي أخي نوري و أخوتي إخلاص ، دنيا، ندى و صديقتي لمياء خليفي

إلى من كاتفتني ونحن نشق الطريق معا نحو النجاح في مسيرتنا العلمية إلى رفيقة دربي: مراح ندي الريحان

و أخيرا كل من ساعدني و كان له الدور من قريب أو بعيد في اتمام هذه الدراسة سائلة المولى عز وجل أن يجزي الجميع خير الجزاء في الدنيا والآخرة.

ثم إلى كل طالب علم سعى بعلمه ليفيد الإسلام والمسلمين بكل ما أعطاه الله من علم ومعرفة.

الطالبة: عايب وردة

مقدمة

مقدمة:

أدى التطور السريع في مجال تقنية المعلومات والاتصالات إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيء للتكنولوجيا، مما ترتب معه خلق ظاهرة إجرامية جديدة، وهي الجرائم الالكترونية، والتي تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية بغرض تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، الأمر الذي ينبه بوجود مخاطر على الصعيد الوطني والدولي إذا لم يتم تدارك هذه الظاهرة التي سوف ينشأ عنها، إذا ما تركت خسائر هائلة على المستوى العسكري والاقتصادي والاجتماعي، مما يستوجب معه إيجاد سبل للتصدي لهذه الظاهرة.

وكما فرض التطور التكنولوجي في ظل عصرنة وسائل الاتصال، ضرورة التحول من النمط التقليدي الكلاسيكي إلى النمط الإلكتروني ،حيث أصبح العالم يتحاور بلغة إلكترونية ما أدى إلى ظهور الجرائم الالكترونية كشكل جديد من أشكال الجريمة وما تتميز به هذه الجرائم من خاصية عابرة للحدود الإقليمية للدول، ما جعل بدول العالم المتقدمة منها والنامية إلى التفكير في الارتقاء بالخدمة المعلوماتية بأسلوب عقلاني يهدف إلى الحيلولة للوقوع في تلك الجرائم ، وذلك من خلال إبرام اتفاقيات وأنظمة دولية لمواجهة الجرائم والعمل على محاربتها، ونخص بالذكر اتفاقية بيرن و اتفاقية الويبو واتفاقية تريبس بودابست لمكافحة الجرائم المعلوماتية واتفاقية النموذج العربي، و نظام تسليم المتهمين، في إطار تعاون دولي مشترك.

وبناء على هذا كان عنوان مذكرتنا موسوم ب:

" **دور الاتفاقيات الدولية والإقليمية في مكافحة الجريمة الإلكترونية**".

أهمية البحث:

– إن موضوع الجرائم الإلكترونية حديث وكثير الانتشار حاليا، كما أنه من الموضوعات التي تثير جدلا فقهيا لدى فقهاء القانوني الجنائي، إضافة إلى تعلق الموضوع بالوسائل الحديثة ذلك أنه كلما تطورت الوسائل الإلكترونية كلما تطور أسلوب ارتكاب هذا النمط من الجرائم.

– إن الأساس الذي يرتكز عليه مجال مكافحة الجرائم الإلكترونية هو التعاون الدولي وتنسيق الجهود المبذولة بين كافة دول العالم عن طريق ابرام اتفاقيات دولية و إقليمية لتكون هناك نتائج مهمة يمكن الارتكاز عليها وتقويتها للحد من تلك الجرائم ذات النتائج البشعة على الدول.

إشكالية البحث:

نظرا للاستخدام المتزايد لتكنولوجيا المعلومات وانتشار الهائل للتقنيات الإلكترونية الحديثة تطورت الظاهرة الاجرامية في العصر الحديث تطورا ملحوظا واختلفت عن صورتها التقليدية سواء كان ذلك في شخصية مرتكبيها او أسلوب ارتكابها و لعل من ابرز الجرائم المستحدثة هي الجرائم الالكترونية ، التي كان لها تأثير سلبي على الاقتصاد العالمي بصفة عامة و الوطني بصفة خاصة مما جعل من الدول العالم و المنظمات عالمية الى التصدي لمثل هذه الجرائم من خلال سن مجموعة من الاتفاقات الدولية والاقليمية.

انطلاقا مما سبق تبرز إشكالية البحث الرئيسية من خلال التساؤل التالي:

ما مدى فعالية الاتفاقيات الدولية والإقليمية في مكافحة الجريمة الإلكترونية؟

وتتدرج مجموعة من الأسئلة الفرعية عن هذا السؤال الرئيسي نجملها في ما يلي:

– ما المقصود بالجريمة الإلكترونية؟.

– ما هو التعاون الدولي في مجال مكافحة الجرائم الالكترونية ؟.

– ماهي الاتفاقيات الدولية لمكافحة الجريمة الالكترونية؟.

– ماهي الاتفاقيات الإقليمية لمكافحة الجريمة الالكترونية؟.

أسباب اختيار الموضوع:

إن اختيارنا لهذا الموضوع يعود لأسباب ذاتية وأخرى موضوعية:

أ/ الأسباب الذاتية:

– الاهتمام بالقانون الجنائي والرغبة في البحث في هذا المجال.

– الميول الخاص لدراسة الاتفاقيات الدولية والإقليمية في مكافحة الجريمة الإلكترونية خاصة و أن هذا الموضوع من المواضيع المستحدثة..

– الجرائم الالكترونية أثرها وخيم على المجتمعات ولا حدود لها، وقد تكون غرضه لها في أي وقت.

ب/ الأسباب الموضوعية:

– الرغبة في إضافة مرجع لمن يرغب في الرجوع إليه.

– معرفة طريقة معالجة الاتفاقيات الدولية والإقليمية للجريمة الالكترونية.

–التعرف على المعاهدات والاتفاقيات لمكافحة الجريمة الالكترونية على المستوى الدولي والإقليمي.

أهداف الدراسة:

– إبراز ماهية الجرائم الإلكترونية و الاطلاع على حجم التطور الذي وصلت إليه.

– إبراز دور الاتفاقيات الاقليمية و الدولية لمكافحة الجرائم الالكترونية في التدخل للتصدي لهذا النوع من الجرائم.

المنهج المتبع:

إن بيان دور الاتفاقيات الدولية و الاقليمية في مجال مكافحة الجرائم الالكترونية، يتطلب الاستعانة بالمعاهدات والاتفاقيات ذات الصلة لذلك اعتمدنا في دراستنا على:

المنهج الوصفي: وهذا من خلال التطرق إلى مفهوم الجرائم الالكترونية.

كما استعنا بالتحليل كأداة من أدوات البحث العلمي الذي يقوم على جمع المعلومات وتصنيفها وتحليلها للوصول إلى حالة يمكن معها تقديم وصف وتفسير دقيقين للظاهرة محل البحث، ومن ثم سيتم توظيفه في وصف وتحليل النصوص الواردة في الاتفاقيات الدولية و الاقليمية ذات الصلة بالجرائم الالكترونية.

الدراسات السابقة:

بعدما أن أجرينا إطلاعا للمؤلفات والأبحاث والدراسات التي تناولها هذا الموضوع وجدنا دراسات تكاد تنعدم في هذه الجزئية و ما وجدناه كانت في قائمة المراجع أي في الكتب ، ونكر هذه الدراسة التي حاولنا الاستفادة منها و استدراك ما بها من نقائص من أجل تجميع الاتفاقيات الدولية والإقليمية التي تقر ضرورة مكافحة الجرائم الالكترونية:

1/ ربيعي حسين ، **اليات البحث و التحقيق في الجرائم المعلوماتية** ، أطروحة مقدمة لنيل شهادة دكتوراه علوم ، كلية الحقوق و العلوم السياسية ، جامعة باتنة 1 ، 2015، 2016.

خطة البحث:

تضمنت خطة البحث مقدمة وفصلين وخاتمة، وفي كل فصل تناولنا مبحثين، حيث أن الفصل الأول تناولنا الوسائل الاجرائية الدولية لمكافحة الجرائم الالكترونية، وجاء المبحث الأول بعنوان الإطار القانوني للجرائم الإلكترونية، إذ تطرقنا فيها إلى مفهوم الجريمة الالكترونية و أساليب ووسائل ارتكاب الجرائم الالكترونية ، وفي المبحث الثاني تعرضنا إلى التعاون الدولي في مجال مكافحة الجرائم الالكترونية، وتناولنا فيه التعاون الدولي بين أجهزة

الشرطة و التعاون القضائي الدولي في مكافحة الجرائم الالكترونية، أما الفصل الثاني فقد خصصناه للجهود الدولية والإقليمية في مكافحة الجرائم الإلكترونية، إذ جاء في المبحث الأول من هذا الفصل متضمن المعاهدات والاتفاقيات الدولية التي تناولت الجريمة الالكترونية، أما المبحث الثاني تناولنا فيه المعاهدات والاتفاقيات الإقليمية لمكافحة الجريمة الالكترونية.

وأخيرا الخاتمة تضمنت النتائج المتوصل إليها و أهم الاقتراحات.

الفصل الأول

الوسائل الإجرائية الدولية لمكافحة الجرائم الالكترونية

تمهيد:

تشكل الجريمة الالكترونية أحدث وأخطر الجرائم تواجدا على ساحة العلوم الجنائية اليوم، وذلك لما تشكله من تهديد كبير يمس الأفراد والمؤسسات ويتعداهم حتى للمساس بأمن الدول واستقرارها، وهو الأمر الذي جعل العديد من دول العالم تضع ضرورة التصدي لهذه الجريمة والعمل على كبح مخاطرها أولوية في قائمة حماية الدول ومواطنيها.

و كما تعد الجرائم الالكترونية من الجرائم المستحدثة والتي برزت نتيجة اساءة استخدام مجال تكنولوجيات الإعلام والاتصال، غير أن مكافحة هذا النوع من الجرائم يلقى صعوبات جمة نتيجة الطبيعة الخاصة لها، ويرجع السبب في ذلك من جهة إلى خصائص هذه النوع من الجرائم كونها عابرة للحدود وتتم في بيئة افتراضية يصعب اكتشافها وتتبع المجرم المعلوماتي، ومن جهة أخرى كون المعلومات هي محور ارتكاز هذا النمط من الجرائم تدخل في مجال المعالجة الإلكترونية للبيانات.

من هذا المنطلق يتم تقسيم هذا الفصل إلى مبحثين:

المبحث الأول: الإطار القانوني للجرائم الإلكترونية

المبحث الثاني: التعاون الدولي في مجال مكافحة الجرائم الالكترونية

المبحث الأول: الإطار القانوني للجرائم الإلكترونية

فرض التطور التكنولوجي في ظل عصرنة وسائل الاتصال، ضرورة التحول من النمط التقليدي الكلاسيكي إلى النمط الإلكتروني ، حيث أصبح العالم يتحاور بلغة إلكترونية ما أدى إلى ظهور الجرائم الالكترونية كشكل جديد من أشكال الجريمة و ما تتميز به هذه الجرائم من خاصية عابرة للحدود الإقليمية للدول، ما جعل بدول العالم المتقدمة منها و النامية إلى التفكير في الارتقاء بالخدمة المعلوماتية بأسلوب عقلاني يهدف إلى الحيلولة للوقوع في تلك الجرائم.

المطلب الأول: مفهوم الجريمة الإلكترونية

تعددت تعريفات الجريمة الالكترونية فقها و تشريعا و هذا راجع لكونها ظاهرة إجرامية حديثة متغيرة و متطورة و لهذا لا يوجد تعريف دقيق متفق عليه.

الفرع الأول: التعريف الفقهي

ذهب جانب من الفقه إلى تناول الجريمة الالكترونية بالتعريف على النحو الضيق بينما الجانب الاخر عرفها على النحو الواسع :

أولا- التعريف الضيق: تزعم هذا الاتجاه الفقيه "**ميروي–Merwe**" من خلال وضعه تعريفا مضمونه:" أن الجريمة الالكترونية هي ذلك الفعل الغير مشروع الذي يتورط في ارتكابه الحاسب"، كما عرفها " **روزبارت–Rosblat**" بأنها:" نشاط غير مشروع موجه لنسخ أو تغيير أو حذف الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه".[1]

2- التعريف الواسع: حاول هذا الاتجاه إعطاء تعريف موسع للجريمة الالكترونية لهدف تفادي النقص الظاهر في التعريفات السابقة فعرفت بأنها: " كل فعل أو امتناع عمدي ينشأ عن الاستخدام الغير مشروع للتقنية المعلوماتية بهدف الاعتداء عن الأموال المادية او

[1]- ربيعي حسين ، **اليات البحث و التحقيق في الجرائم المعلوماتية** ، أطروحة مقدمة لنيل شهادة دكتوراه علوم ، كلية الحقوق و العلوم السياسية ، جامعة باتنة 1 ، 2015، 2016، ص 25.

المعنوية"،[1] كما عرفت أنها:" كل سلوك سلبي كان أو ايجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأي صورة كانت".

و في تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي أنه تتحقق الجريمة في كل حالة يتم فيها تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها، و تبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على كسب اقتصادي غير مشروع له و لشخص آخر".

الفرع الثاني: خصائص الجرائم الالكترونية

نظرا للطبيعة المميزة للجريمة الالكترونية باعتبارها تمس المعلومات الشي الذي جعلها تتميز عن الجرائم التقليدية بمجموعة من الخصائص تتمثل فيما يلي :

1/ اعتمادها على الأساليب العلمية الحديثة : تتميز هده الجرائم بالاعتماد على الأساليب العلمية والابتكار الفني في التخطيط و الاعداد و كافة مراحل التنفيذ، و كيفية إخفاء كافة الاثار الدالة على ارتكابها ، بالإضافة إلى أنها ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية و أجهزة و معدات و تجهيزات الحاسب الالي.

2/ جرائم عابرة للحدود (ذات طابع دولي): أي أنها غير محددة برقعة جغرافية معينة فهذه الجريمة لا تعترف بالحدود الجغرافية للدول، فلا حدود مرئية أو ملموسة تعيق نقل المعلومات عبر الدول المختلفة بعد ظهور شبكات المعلومات، و التي استطاعت أن تربط أعدادا هائلة من الحسابات الألية عبر العالم،[2] و ذلك على خلاف الجرائم التقليدية التي تتميز بخاصيتين هما وحدة الزمان و محدودية المكان.

---

[1]– محمد أمين الشوابكة ، **جرائم الحاسوب و الانترنت الجريمة المعلوماتية**، ط4، دار الثقافة للنشر و التوزيع ، 2011 ،

[2]– مدحت محمد عبدالعزيز إبراهيم ، **الجرائم المعلوماتية الواقعة على النظام المعلوماتي (دراسة مقارنة)**، ط1، دار النهضة العربية، مصر، 2015، ص 33.

3/ تمتع المجرم بصفة الذكاء و الاحتراف: يتمتع المجرم المرتكب للجريمة الالكترونية بقدر كبير من الذكاء، حيث يستخدم الوسائل التقنية الحديثة من كمبيوتر و أجهزة الاتصال و غيرها كوسائل مساعدة لتنفيذ جريمته.

4/ أقل عنفا من الجرائم التقليدية: لا يلجا المجرم الخاص بهذا النوع من الجرائم إلى العنف في ارتكابه للجرائم، حيث أن حالات القتل و السرقة بالإكراه أو الاتلاف تعتبر نادرة نسبيا بالمقارنة بنظيرتها من الاجرام، و من ثم فلا يوجد في واقع الأمر شعور بعدم الأمان اتجاه المجرمين في مجال المعالجة الألية للمعطيات، نظرا لأن مرتكبيها ليسوا من محترفي الاجرام بصيغته المتعارف عليها.[1]

الفرع الثالث: أهداف و دوافع القيام بالجريمة الالكترونية

هناك دوافع عديدة تحرك الجناة إلى ارتكاب هذه الجرائم منها:

1/ صناعة و نشر الفيروسات: و هي أكثر الجرائم الانترنت انتشارا و تأثيرا.

2/ الاختراقات: و تتمثل في الدخول الغير مصرح به إلى أجهزة أو شبكات الحاسب الألي.

3/ **تعطيل الأجهزة:** و قد شاعت في الآونة الأخيرة مثل هذه الجرائم التي يقم من خلالها. تعطيل الأجهزة أو شبكات عن تأدية عملها بدون أن تتم عملية اختراق فعلية لتلك الأجهزة.

4/ **انتحال الشخصية:** و تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، و تتم إما لغرض الاستفادة من هوية الضحية أو إخفاء هوية شخصية المجرم لتسهيل ارتكابه لجرائم أخرى.

5-**المضايقة و الملاحقة:** تتم جرائم الملاحقة و المضايقة عادة باستخدام البريد الالكتروني و تشمل الملاحقة رسائل تهديد وتخويف.

[1]- سليم عبد الله الجبوري، **الحماية القانونية لمعلومات شبكة الانترنت**، ط 1، منشورات الحلبي الحقوقية، لبنان، 2011 ص 298.

6/ **التشهير و تشويه السمعة او المطاردة الالكترونية :** يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، و الذي قد يكون فردا أو مؤسسة تجارية لغاية تعريضهم للمضايقات الشخصية أو الاحراج العام.

7/ **النصب و الاحتيال:** في غالب الأحيان يكون الهدف من ارتكاب الجرائم الالكترونية الحصول على ربح مالي عن طريق المساومة على البرامج و المعلومات المتحصلة بطريق الاختلاس من جهاز الكمبيوتر أو عن طريق استعمال بطاقة سحب إلى مزورة .

المطلب الثاني: أساليب ووسائل ارتكاب الجرائم الالكترونية

تبعا للخصائص المتفردة للجرائم الالكترونية سواء ما تعلق بالمجرم الإلكتروني كالذكاء و الاحترافية، أو بأنواع المجنى عليهم، أو بمراحل ارتكابها أو ما تعلق بالجريمة نفسها، فهي جرائم عابرة للحدود و يصعب على المحققين اكتشافها وإثباتها، و تتم بأساليب وأدوات متنوعة، يغلب عليها الطابعان التقني والفني و هذا ما يميزها عن باقي الجرائم التقليدية،[1] و جرائم يصعب اكتشافها[2] واثباتها[3] وجرائم ناعمة[4]، فهي ترتكب بواسطة الكمبيوتر سواء كان وسيلة أو هدفا وباستعمال شبكة الإنترنت، أو بواسطة الهاتف النقال خاصة النوع الذكي الذي يستطيع الاتصال بشبكة الإنترنت، أو عن طريق اللوحة الرقمية المزودة بشريحة ذكية و غيرها من الوسائل الإلكترونية التي توفرها تكنولوجيات الاعلام و الاتصال الحديثة.

---

[1]– يقصد بذلك ربط العالم بشبكات اتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت، حيث مكن ذلك من انتشار الثقافة وتبادل المعلومات والتقارب بين الشعوب، ولكن للأسف أدي أيضا إلى عولمة الجريمة ومنها الجرائم الإلكترونية، فهي لا تعترف بالحدود الإقليمية للدول ولا بالمكان ولا بالزمان.

– محمد خليفة، **جريمة التواجد غير المشروع في الأنظمة المعلوماتية(دراسة مقارنة)**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة باجي مختار، عنابة، الجزائر، 2011، ص28.

[2]– حيث يلعب المجنى عليه في الجرائم الإلكترونية دورا سلبيا في الكشف عنها، فمن جهة يمتنع في الغالب عن التبليغ عنها لسببين الأول صعوبة تحديد هوية المجرم الإلكتروني، وثانيا التحديات التقنية لاستخلاص الدليل الإلكتروني.

[3]– حنان ريحان المبارك المضحكي، **الجرائم المعلوماتية (دراسة مقارنة)**، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014، ص39.

[4]– نهلا عبد القادر المومني، **الجرائم المعلوماتية**، ط1، دار الثقافة للنشر والتوزيع عمان، الأردن، 2008، ص58.

حيث تثير الجرائم الالكترونية في التطبيقات القضائية مسائل معقدة للقضاة نتيجة الطابع الفني و التقني و البيئة الافتراضية التي تتم فيها، حيث يتطلب من القاضي أن يكون على دراية و فهم تام للمصطلحات القانونية ذات طبيعة إلكترونية، إضافة إلى فهم الجانب التقني التي تتم فيه، وعليه وجب على الدولة إنشاء مركز وطني متخصص في التدريب على مكافحة كافة أشكال الجرائم الإلكترونية يشرف عليه متخصصون في مجال تكنولوجيات الإعلام والاتصال، من داخل الوطن وخارجه ويستفيد منه كل أعضاء الأجهزة القضائية.

الفرع الأول: الأساليب المستخدمة في الاعتداء على المكونات المعنوية للحاسوب

في هذا الشأن تتنوع هذه الأساليب تبعا للتطور التكنولوجي في مجال الحوسبة والاتصال، فكلما تطورت هذه التقنيات تطورت معها هذه الأساليب، وبصفة عامة يمكن تعريف هذه الأساليب بأنها:" برمجيات أو وسائط تقنية قابلة للتوظيف مع عتاد الحاسوب و برمجياته لتحقيق أهداف معينة كمضايقة و إنهاك مستمر لموارد النظام المعلوماتي و تدمير قواعد البيانات، و موارد البرمجيات و النظم التطبيقية و إحداث ثغرات في النظام المعلوماتي".[1]

و مما لا شك فيه أن هناك أكثر من أسلوب أو طريقة توفرها التقنية الحديثة لارتكاب هذه الجرائم، و إن أكثر ما يتم به تنفيذ هذه الاعتداءات على المكونات المنطقية للحاسوب هي البرامج الخبيثة ذات الأثر التدميري التي تستهدف محو جزء أو كل برامج وملفات الحاسوب و البيانات المخزنة، ولكل برنامج منها تسمية شائعة تستمد عن وظائفه التدميرية،[2] لذا سنحاول التطرق إلى الأساليب الشائعة في ارتكابها وذلك كالآتي:

[1]– حسن مظفر الرزو، **الأمن المعلوماتي (معالجة قانونية أولية)**، مجلة الأمن والقانون أكاديمية شرطة دبي، الإمارات العربية المتحدة، العدد 1، جانفي 2004، ص70.

[2]– هشام محمد فريد رستم، **قانون العقوبات ومخاطر تقنية المعلومات**، مكتبة الآلات الحديثة ، مصر، 1994، ص158.

1- التقاط المعلومات الموجودة بين الحاسوب والنهاية الطرفية: تتم هذه العملية بواسطة تحويلة تعمل على تكبير الذبذبات الإلكترونية وإرسالها إلى النهاية الطرفية للقيام بعملية التجسس.[1]

2- الفاحص: وهو عبارة عن برنامج تطبيقي أعد لأغراض الكشف الآلي عن مواطن الضعف في المضيفات المحلية والنائية، حيث تعمد هذه البرمجيات إلى قرع أبواب طرفيات و الخدمات المصاحبة لها، وبذلك توفر معلومات ثمينة تعتبر موردا هاما لقراصنة المعلومات مثل: الحصول على الآلاف من كلمات السر الشخصية التي تمكنهم من الدخول غير المشروع للنظام واستغلال بياناته.[2]

3- التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي: تهدف هذه العملية إلى إعادة تكوين و تغيير خصائص المعلومات، التي تبث وتنقل من خلال الأنظمة المعلوماتية، كما تحتاج هذه العملية التقنية المعقدة إلى فك شيفرة النظام.[3]

4- الفيروسات: تعتبر الفيروسات من الوسائل الأكثر استعمالا في ارتكاب الجريمة المعلوماتية من شأنها تعديل أو محو المعطيات التي يتم معالجتها آليا بما يشوه سير النظام المعلوماتي، فإذا كان بعض الفيروسات لا يتسم بالخطورة، فإن البعض الآخر منها يمكنه تخريب النظام المعلوماتي وإعاقة سيره، كما تعتبر من أهم التقنيات التي تستخدم لتدمير نظم المعلومات، فيمكن تعريفها على أنها: "برنامج يصممه بعض المتخصصين بهدف تخريبي مع إعطائه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدميره تماما"،[4] كما يعرف الفيروس أيضا على أنه:" برنامج صغير صيغ لغرض تغيير عمل برمجيات الحاسوب دون السماح للمستخدم بمعرفة هذا الأمر"،[5] فهي تكتب بواسطة

---

[1]- عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت، 2007، ص26.

[2]- حسن مظفر الرزو، المرجع السابق، ص 70.

[3]- عفيفي كامل عفيفي، المرجع السابق، ص26.

[4]- محمد علي العريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة للنشر، القاهرة، مصر، 2011، ص103.

[5]- حسن مظفر الرزو، المرجع السابق، ص77.

مبرمجين محترفين بغرض إلحاق الضرر بحاسب آخر أو السيطرة عليه أو سرقة بيانات مهمة منه و تتم كتابتها بطريقة معينة.

من جانب آخر تصنف الفيروسات إلى تصنيفات عديدة سواء حسب مبدأ عملها أو حسب التسمية التي تتخذها أو حسب الموقع الذي تصيبه بالتلف،[1] فهي عبارة عن برامج مشفرة مصممة بقدرة كبيرة على التكاثر و الانتشار من نظام إلى آخر، و من الفيروسات الشهيرة: فيروس(الحب) فيروس(ميليسا)، فيروس(الدودة)، فيروس (حصان طروادة)، القنبلة المعلوماتية، القنبلة المنطقية، القنبلة الزمنية...إلخ، و لنأخذ مثلا فيروس القنبلة الموقوتة، و هي عبارة عن برنامج مصمم بحيث تبقى ساكنة و غير فعالة و غير مكتشفة لمدة أشهر أو أعوام يحددها مؤشر زمني كتاريخ معين مثلا بحيث ينشط البرنامج عند حلوله و يؤدي مهامه الهدامة.[2]

كما تنتشر الفيروسات حينما يستقبل مستخدمي الإنترنت بواسطة البريد الإلكتروني، رسائل بريدية ملغومة بفيروسات مدمرة من مجهولين، و تنشط بمجرد فتح تلك الرسالة، و هي تعليمات غير مرخصة موضوعة في برامج بهدف إجراء عمليات غير مشروعة في وقت محدد مسبقا أو حين تتوفر شروط معينة،[3] لذلك ينصح خبراء المعلوماتية عدم فتح الرسائل الإلكترونية مجهولة المصدر، لأنها يمكن أن تشكل خطرا كبيرا على أمن المعلومات و البيانات المخزنة، و لا زالت شركات البرمجيات تعمل جاهدة على توفير برامج مضادة للفيروسات لتوفير الحماية اللازمة لمستخدمي الحاسوب و شبكة الإنترنت.

---

[1]– محمد حماد مرهج الهيتي، **الجريمة المعلوماتية(دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني)**، دار الكتب القانونية، مصر، 2014، ص475.

[2]– أمجد حسان، **الفيروسات إرهابا تهدد أنظمة المعلومات**، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، الجزائر، العدد4، 2011، ص124.

[3]– عبد الحكيم رشيد توبة، **جرائم تكنولوجيا المعلومات**، ط1، دار المستقبل للنشر والتوزيع، الأردن، 2009، ص171.

و لكن للأسف ففي كل مرة يحاول القراصنة التغلب عليها بطرح فيروسات جديدة، مما يضطر هذه الشركات إلى تحيين برامجها و إيجاد الحلول المناسبة، ويفرض عليها مزيدا من التكاليف المالية و هدرا للجهد و الوقت.

5- التدخل غير المشروع في النظام المعلوماتي: يسمح هذا الاسلوب للجاني نسخ أو تدمير البيانات، و إدخال معطيات وهمية، و التلاعب في البرامج التشغيلية و زرع الفيروسات و البرامج الوهمية و لا تتطلب العملية أكثر من جهاز حاسوب موصول بشبكة الإنترنت، مع ضرورة التعرف على كلمة السر أو شيفرة النظام.[1]

6- البرامج المعدة لأغراض محددة: تستخدم في هذه العملية برامج النظام الخاصة مثل:(super zap) المطور من قبل شركة (IBM) لاستخدامه في حالة الطوارئ قصد تجاوز قيود التحكم العادية لتنفيذ عمليات غير مشروعة.[2]

7- أسلوب الباب السحري: و هي تعليمات تعطى للحاسوب قصد السماح للمستخدم بتجاوز قيود التحكم المعتادة في النظام، و هذه التعليمات تعطى للحاسوب أثناء تطوير الأنظمة و تحذف في الغالب قبل وضع النظام أثناء مرحلة التشغيل النهائي.[3]

8- التزوير والخداع الإلكتروني: يكون التزوير حينما يستخدم شخص غير مفوض رقم هوية و كلمة السر الخاصة بمستفيد مفوض للولوج إلى النظام و القيام بعمليات غير مشروعة، أما الخداع الإلكتروني فيحدث حينما يتصل آليا شخص مخادع بمستفيد مفوض و يوهمه بأنه له حق الاستفادة من خدمات النظام.[4]

نستنتج في الأخير أن هذه الأساليب لا حصر لها ومرتبطة بالتطور التكنولوجي الحاصل في مجال المعلوماتية.

---

[1]- عفيفي كامل عفيفي، المرجع السابق، ص26.

[2]- عبد الحكيم رشيد توبة، المرجع السابق، ص171.

[3] - عفيفي كامل عفيفي، المرجع السابق، ص27.

[4]- عبد الحكيم رشيد توبة، المرجع السابق، ص172.

الفرع الثاني: الوسائل المستخدمة في الجرائم الإلكترونية

إن أساليب ارتكاب الجرائم الإلكترونية لا حصر لها فالأمر نفسه ينطبق على الأدوات المستعملة في ذلك، نتيجة التقدم الهائل الحاصل في مجال تقنية الحاسوب والاتصال. فهي من جهة توفر للمستعمل أدوات كثيرة تسهل عليه معالجة المعلومات و تخزينها واسترجاعها و إرسالها كأجهزة الحاسوب و ملحقاته و برامجه، إضافة إلى الأهمية التي تكتسيها تقنية البريد الإلكتروني الذي يمكننا من استقبال و إرسال ملفات على اختلاف أنواعها، و من جهة أخرى تعتبر تقنية الاتصالات الحديثة و الشبكات المحلية و العالمية كالهواتف النقالة و الشبكة العنكبوتية...إلخ، أدوات فعّالة تمكن المجرم المعلوماتي من ارتكاب الجرائم الإلكترونية على اختلاف أنواعها، نتطرق إلى بعض منها فيما يأتي:

1- الحاسوب وملحقاته وبرامجه: حققت التقنيات الحديثة قفزة عملاقة في مجال صناعة الحاسوب و ملحقاته، إضافة إلى التطورات الهائلة في مجال الاتصال و على رأسها شبكة الإنترنت حيث لم يعد من الممكن استغناء الإنسان في شتى مجالات حياته عن استعمال الحاسوب و الشبكة العنكبوتية، نظرا لما توفره هذه التقنية من خدمات سريعة و غير مكلفة. لكن للأسف و ككل تكنولوجيا حديثة لها سلبياتها، فقد أدى سوء استخدامها إلى اعتبار الحاسوب الأداة الأولى للجرائم الإلكترونية،[1] و ذلك لسهولة استخدامه و انتشاره بين الناس، و تنوع برامجه والاحترافية التي يتعامل بها بعض الناس و التي بدأت تزداد يوما بعد يوم، فيكفي للشخص توفر جهاز حاسوب متصل بشبكة الإنترنت، إضافة إلى معرفة بسيطة بالمعلوماتية، أن يقوم بارتكاب جريمة إلكترونية و لو كانت بسيطة مثل إرسال رسالة إلكترونية بالبريد الإلكتروني تتضمن سبا أو شتما أو قذفا أو تهديدا...إلخ.

2- البريد الإلكتروني: وفرت لنا شبكة الإنترنت أداة بالغة الأهمية بخصوص الاستعمال الشخصي لعلبة البريد الإلكتروني، حيث عّف جانب من الفقه البريد الإلكتروني على أنه:"

[1]- فايز الظفيري، **الأحكام العامة للجريمة الإلكترونية**، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر، العدد 2، 2002، ص492.

طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات"،[1] فهو يستخدم كمستودع لحفظ الأوراق والمستندات الخاصة في صندوق البريد الخاص بالمستخدم، بشرط تأمينه بطرق التأمين المعروفة كالتشفير و كلمات السر و غيرها من تقنيات الحماية.[2]

أصبحت هذه الأداة من أسرع الوسائل التي وفرتها التقنية المعلوماتية بالمجان قصد توفير خدمات الاتصال و تبادل الملفات سواء كانت صوتية أو مرئية، فالبريد الإلكتروني أصبح بديلا عن الهواتف لأنه أداة اتصال ناجزة للمصالح خاصة في المعاملات التجارية، لكنه بالمقابل يستخدمه المجرم المعلوماتي في إرسال الفيروسات على اختلاف أنواعها و أهدافها كنسخ البيانات الشخصية أو تدميرها أو تعديلها...إلخ، أو إرسال روابط لمواقع مشبوهة، كما يستخدم أيضا لترويج الشائعات و الأكاذيب و غيرها.

ومن الأمثلة على ذلك قضية فيروس البريد الإلكتروني الأكثر شهرة (Melissa) للهاكرز الأمريكي (David Smith)، حيث أحدث هذا الفيروس اضطرابا عالميا في خدمات البريد الإلكتروني، حيث يقوم باستنساخ نفسه ويسخر برمجيات البريد الإلكتروني لإرسال قائمة بعناوين مواقع جنسية إباحية ونشرها بسرعة من خلال شبكة الإنترنت، الأمر الذي أجبر العديد من الشركات على إغلاق مزودات خدمة البريد الإلكتروني لديها، مما تسبب في خسائر كبيرة لها، للإشارة تمت متابعته و حكم عليه بالسجن لمدة (40) عاما وغرامة قدرها(470)ألف دولار.[3]

3- الهاتف النقال: و يسمى أيضا الهاتف المحمول أو الخلوي أو الجوال أو المتحرك، و هو عبارة عن:" أداة اتصال لاسلكية تعمل من خلال شبكة من أبراج البث موزعة لتغطي

---

[1]- محمود محمد لطفي صالح، **المعلوماتية وانعكاساتها على الملكية الفكرية للمصنفات الرقمية(دراسة مقارنة)**، دار الكتب القانونية، مصر، 2014، ص185.

[2]- عبد الفتاح بيومي حجازي، **التزوير في جرائم الكمبيوتر والإنترنت(دراسة مقارنة)**، ط1، منشأة المعارف، القاهرة، مصر، 2010، ص66.

[3]- طارق ابراهيم الدسوقي عطية، **الامن المعلوماتي(النظام القانوني لحماية المعلوماتي)**، دار الجامعة الجديدة، الإسكندرية، 2009، ص541.

مساحة معينة ثم تترابط عبر خطوط ثابتة أو أقمار صناعية"، مع تطور هذه الأجهزة أصبحت أكثر من مجرد وسيلة اتصال صوتي فهي حاسوب محمول حجمه بكف اليد، له وظائف كثيرة كالاتصال المرئي و تنظيم المواعيد و استقبال البريد الصوتي و إرسال واستقبال ملفات الفيديو و البريد الإلكتروني، و تصفح شبكة الإنترنت و التصوير و استعمال تقنية البلوتوث... إلخ. فقد تزايد عدد مستخدمي هذه الأجهزة باستمرار خاصة بعد انتشار الهواتف النقالة الذكية، و التي أصبحت تقارب في خصائصها أجهزة الحاسوب، و صارت أداة لارتكاب كثير من الجرائم الإلكترونية مثل: جرائم الإباحية عبر الإنترنت جرائم السب و الشتم و التشهير باستعمال الصور و مقاطع الفيديو...إلخ.

4- الشبكات المحلية والعالمية: يمكن تعريف شبكة الحاسوب على أنها:" نظام لربط جهازين أو أكثر باستخدام إحدى تقنيات نظم الاتصالات من أجل تبادل المعلومات والموارد و البيانات، كما تسمح بالتواصل المباشر بين المستخدمين"،[1] إذ يمكن أن تكون أجهزة الحاسوب في الشبكة قريبة جداً من بعضها مثل: أن تكون في غرفة واحدة و تسمى الشبكة في هذه الحالة بالشبكة المحلية (LAN)، أو يمكن أن تكون مكونة من مجموعة أجهزة في أماكن بعيدة مثل: الشبكات بين المدن أو الدول وحتى القارات و تسمى بالشبكات الإقليمية (MAN)، و يتم وصل هذه الشبكات في كثير من الأحيان بالإنترنت أو بالساتل، و تسمى الشبكة حينئذ شبكة عريضة ، في مقابل ذلك هناك ما يعرف بالشبكة الشخصية و التي تربط مجموعة أجهزة قريبة من المستخدم.

من جهة أخرى تعتبر شبكة الإنترنت من أهم الشبكات، و تسمى أيضا بشبكة الشبكات، فهي تضم كافة أنواع الشبكات السابقة، فهي عبارة عن:" مجموعة من الحواسب المتصلة فيما بينها عن طريق أسلاك أو دون أسلاك، بحيث يمكن لأي منها الوصول إلى

[1]- فايز الظفيري، المرجع السابق، ص، ص 494،495.

محتوى الآخر واستخدام موارده من تطبيقات وقواعد معطيات و غيرها من المعلومات"،[1] إن الهدف الدائم من الشبكة هو التشارك في المصادر و هي تتضمن الملفات و قواعد البيانات و البرامج...إلخ.[2]

المبحث الثاني: التعاون الدولي في مجال مكافحة الجرائم الالكترونية

إزاء التطور الكبير لهذه الجرائم و التي أصبحت تلحق أضرار جسيمة بمجموعة من الدول و لم تعد تتمركز في دولة محددة، فكان لا بد على الدول أن تتكاثف جهودها من أجل وضع آليات فعالية لمكافحتها و التصدي لها، و هذا من خلال تعزيز التعاون الدولي في شتى المجالات.

المطلب الأول: التعاون الدولي بين أجهزة الشرطة

أدى التطور الكبير في وسائل المواصلات بصفة عامة و الشبكة المعلوماتية بصفة خاصة إلى انتقال المجرمين من بلد إلى آخر، و قد أدرك المجتمع الدولي أنه بات من المستحيل على أي دولة أن تقوم بالقضاء على الجرائم العابرة للحدود، ذلك أن الإجراءات العامة لأجهزة الشرطة في كل دولة لا تجعل لجهازها الأمني تعقب المجرمين و متابعتهم إذا ما عبروا حدود الدولة، و عليه فإن الحاجة إلى تعاون أجهزة الشرطة فيما بين الدول و تنسيق العمل فيما بينهم لمطاردة المجرمين، و من ابرز مظاهر التعاون أنشاء منظمة الشرطة الجنائية الدولية «الإنتربول» و ظهور العديد من صور و أشكال و وسائل التعاون بين أجهزة الشرطة، و تتمثل هذه الصور و الوسائل فيما يلي:

---

[1]– عبد الله عبد الكريم عبد الله، **جرائم المعلوماتية والإنترنت(الجرائم الإلكترونية)–دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا**، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص20.

[2]– المرجع نفسه، ص20.

الفرع الأول: شرطة الويب الدولية [1]

أنشئت هذه المنظمة في الولايات المتحدة الأمريكية عام 1986 لتلقي شكاوى مستخدمي الشبكة و ملاحقة الجناة و القراصنة إلكترونيا و البحث عن الأدلة ضدهم و تقديمهم للمحاكمة، و يضم فريق العمل بهذه المنظمة متخصصين من هيئات إنفاذ القانون و المؤسسات الحكومية و ضباط الشرطة و متطوعين فنيين من 61 دولة حول العالم، ونظرا لاتساع نشاط هذه المنظمة و ما تقوم به من إجراءات بالتعاون مع وكالات إنفاذ القانون في الدول الأعضاء فإن ذلك يسهل الأمر لفريق العمل بتتبع الأنشطة الإجرامية التي ترتكب من خلال شبكة الإنترنت على مستوى العالم، و في إطار مسألة الضوابط القانونية التي تحكم حركة مرور المعلومات عبر شبكة الإنترنت، فهناك من يرى أنه من الضروري وضع ضوابط وقواعد بحيث لا تؤدي إلى المساس بالحريات العامة في تبادل المعلومات و حقوق الإنسان من ناحية، و الا تستخدم الشبكة لأغراض إجرامية أو نشر مواد إباحية تسيء إلى المجتمع من ناحية أخرى. [2]

الفرع الثاني: مركز بلاغات احتيالات الإنترنت

تم إنشاء هذا المركز في الولايات المتحدة الأمريكية بتاريخ 2000/05/18 ليتعاون مع مكتب التحقيقات الفدرالية FBI و المركز القومي لجرائم ذوي الياقات البيضاء (National White Collier Crime Center) ، وذلك بهدف تلقي البلاغات وتتبع الجرائم والاحتيالات التي ترتكب من خلال شبكة الإنترنت بالتنسيق مع أجهزة المكافحة و الضبط المعنية داخل الولايات المتحدة الأمريكية وخارجها من خلال موقع المركز على الشبكة الدولية.

[1]– موقع المنظمة http://www.web-police.org

[2] – سليمان أحمد فضل، **المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية**، دار النهضة العربية، مصر، 2000، ص 417.

الفرع الثالث: ربط شبكات الاتصال والمعلومات

يجري الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة و بين تلك الأجهزة في الدول الأخرى عن طريق السلك الدبلوماسي، و حيث إن الاتصالات الشرطية تحتاج إلى اتصالات خاصة تحقق لها السرعة المطلوبة؛ لذا حاولت المنظمة الدولية للشرطة الجنائية «الإنتربول» وكذلك العديد من الدول تطوير نظم الاتصال وتبادل المعلومات فيما بينها، حتى يتم الوصول وتعقب المجرمين بمجرد خروجهم من الدولة التي تم ارتكاب الجريمة فيها فتقوم أجهزة شرطة الدولة المجني عليها بالاتصال السريع بالأجهزة الأمنية في الدولة المتفق معها أمنيا للقيام بملاحقة المجرمين في حدود دولتهم التي هرب إليها.[1]

الفرع الرابع: المنظمة الدولية للشرطة الجنائية (الإنتربول)

تسمي اللجنة الدولية للشرطة الجنائية ومقرها بباريس في فرنسا، و غير اسمها ليصبح المنظمة الدولية للشرطة الجنائية، و تضم في عضويتها أكثر من 182 دولة عضو،[2] و تركز المنظمة اهتمامها على ستة مجالات إجرامية أعطتها الأولوية هي الفساد، المخدرات و الإجرام المنظم، الإجرام المالي و المرتبط بالتكنولوجيا المتقدمة، المجرمون الفارون، تهديد السلامة العامة و الإرهاب، و الاتجار في البشر، و يعد الإنتربول أهم آليات التعاون الشرطي الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بصفة عامة والجريمة المعلوماتية بصفة خاصة، فمهمة الإنتربول الأساسية تفعيل التعاون بين أجهزة الشرطة التابعة للدول الأعضاء في المنظمة بتوحيد إجراءات التسليم، و من خلال تنسيق العمل الشرطي و تجميع البيانات و تبادل المعلومات لتيسير خدمات

[1]– سالم محمد سليمان الاوجلي، **أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية**، رسالة دكتوراه، كلية الحقوق ، جامعة عين شمس، 1997، ص 421.

[2] – غانم مرضي الشمري، **الجرائم المعلوماتية(ماهيتها، خصائصها، كيفية التصدي لها قانونيا)**، ط1، دار الثقافة للنشر والتوزيع، الأردن 2016، ص 96.

التحقيق لضبط و ملاحقة المجرمين الهاربين و تسلمهم إلى الدولة التي تطلب تسلمهم، و إنشاء و تطوير كل النظم القادرة على المساهمة بفاعلية في الوقاية و العقاب على جرائم القانون العام.[1]

يجمع الانتربول المعلومات من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، و يقوم بتحليلها وفحصها و يتبادلها مع جميع الدول الأعضاء، بحيث تعتبر هذه البيانات بمثابة أرشيف متكامل الوثائق يمكن الرجوع إليه عند الحاجة، و يهدف أيضا إلى تسيير التعاون الميداني بين البلدان الأعضاء من خلال إعداد لائحة بأسماء ضباط الاتصال المتيسرين على مدار الساعة للمساعدة في التحقيقات بشأن الاجرام الالكتروني، و كذلك زيادة تبادل المعلومات بين البلدان الأعضاء بشأن الأساليب الجرمية المتبعة في الإجرام الالكتروني عن طريق الفرق العاملة الإقليمية و حلقات العمل التدريبية.[2]

و يقوم الإنتربول بتعميم التحذيرات و التنبيهات المتضمنة المعلومات الاستخبارية و الاحاطات و المشورة التحليلية و الفنية عن الأخطار الإجرامية المحتملة، و يستخدم الإنتربول أدواته الخاصة كمنظومة النشرات الدولية بمختلف أنواعها و التقصي في قواعد البيانات و تقديم الخبرات و الدورات التدريبية في مجال مكافحة جرائم الإنترنت، و ذلك بالاستعانة بمجموعة من الخبراء الدوليين و المختبرات الدولية على الصعيد العالمي، و تيسير تبادل و تحليل و تخزين البيانات الجنائية حيث تقوم المنظمة بتزويد شرطة الدول الأطراف بكتيبات إرشادية حول جرائم الإنترنت و كيفية التدريب على مكافحتها والتحقيق فيها، و يعد الإجرام المالي المرتبط بالتكنولوجيا المتقدمة من الجرائم التي تركز عليها منظمة الإنتربول.[3]

---

[1]– فهد عبد الله العبيد العازمي، **الإجراءات الجنائية المعلوماتية**، دار الجامعة الجديدة، مصر، 2016، ص 651.

[2] – أحمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيات الإعلام و الاتصال في ضوء قانون رقم 09/ 04**، رسالة مكملة لنيل شهادة الماجستير، جامعة قاصدي مرباح، ورقلة، 2023، ص 59.

[3]– فهد عبد الله العبيد، المرجع السابق، ص 653.

و يمكن القول أن ملاحقة مرتكبي الجرائم وتقديمهم للعدالة يستلزم قيام القيام بإجراءات خارج حدود الدولة حيث ارتكبت، و من هذه الاجراءات معاينة مواقع الأنترنيت في الخارج و ضبط الأقراص الصلبة، و تفتيش نظم الحاسب الآلي هذا يصطدم بمشكلة السيادة، و هذا النوع من الجرائم يتطلب المساعدة الأمنية بين الدول لأن جهاز الشرطة في دولة معينة لا يمكنه تعقب المجرم و ملاحقته إلا في حدود دولته، إلى أن تم انشاء مراكز اتصالات إقليمية، و أخيرا إنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول).

و على المستوى العربي نجد أن مجلس الوزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية بهدف تأمين و تنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مكافحة الجريمة و ملاحقة المجرمين في حدود القوانين المعمول بها في كل دولة، بالإضافة إلى تقديم المساعدة لأجهزة الشرطة في الدول الأعضاء.[1]

الفرع الخامس: تبادل المعاونة لمواجهة الكوارث والأزمات

في حالة وجود أزمة وفي المواقف الحرجة، فإن عنصر الوقت يعد من الأمور الحاسمة في مواجهة تلك الأزمة أو الكارثة، الأمر الذي يحتاج معه إلى تكثيف و زيادة الجهود والخبرات والإمكانيات و هو ما لا يمكن تحقيقه إلا بتركيز الجهود الدولية في مسار واحد، فعلى سبيل المثال: مشاركة قوات الإنقاذ و الدفاع المدني للدول المنكوبة اثر الزلازل والأعاصير و الفيضانات أو المشاركة بخبراء أو تقديم معدات متطورة. كذلك المشاركة بقوات خاصة أو خبراء أو تجهيزات في تحرير رهائن محتجزين، أو مباني هامة محتلة أو طائرات أو سفن مختطفة.[2]

[1] – غانم مرضي الشمري، المرجع السابق، ص 97.

[2]– يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص 148.

الفرع السادس: القيام ببعض عمليات شرطية دولية مشتركة

تعقب مجرم الحاسب الآلي و تعقب الأدلة الرقمية وضبطها و القيام بعملية التفتيش العابر للحدود كمكونات الحاسب الآلي المنطقية و الأنظمة المعلوماتية و شبكات الاتصال، بحث عن ما تحتويه من أدلة وبراهين علي الجريمة الإلكترونية.[1]

و من أمثلة ذلك، التسليم المراقب في مجال مكافحة المخدرات، فهو يعني السماح لشحنة غير مشروعة بالمرور تحت المراقبة عبر إقليم ما، و كذلك المطاردات الساخنة و التي يقصد بها تعقب الجناة الذي يبدأ في احدى الدول و يواصل في أراضي دولة أخرى.[2]

المطلب الثاني: التعاون القضائي الدولي في مكافحة الجرائم الالكترونية

يعد التعاون القضائي الدولي من أسمى مظاهر التعاون الدولي في مكافحة الجريمة، إذ يوفق بين استقلال كل دولة في ممارسة اختصاصها الجزائي على حدود إقليمها، و بين ضرورة ممارسة حقها في العقاب و بدون هذا التعاون فلا يمكن للدولة أن تمارسه.

الفرع الأول: أسباب التعاون القضائي الدولي

أولا : تقيد سلطات الدولة بحدود إقليمها إذ لا يمكن أن تسري قوانينها العقابية أو مباشرة الإجراءات خارج حدود الإقليم الوطني للدولة لأن ذلك سيمس بسيادة الدولة الأجنبية.

ثانيا : تلازم حق الدولة في العقاب ومجال الدعوى العمومية تطبيقا لتشريعاتها الجزائية أي لابد من تطبيق قانون الإجراءات الجزائية مع قانون العقوبات، و هكذا فإن التعاون الدولي قد انحصر في التخلص من مشكلة الحدود الإقليمية بين الدول، التي تحول دون قدرتها على محاكمة الجاني طبقا لقانونها أو تنفيذ العقوبة عليه.

[1] – غانم مرضي الشمرى، المرجع السابق، ص 98.

[2] – شيخة حسين الزهراني، **التعاون الدولي في مواجهة الهجوم السبرياني**، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد1، 2020، ص 746.

و وجب الالتجاء إلى التعاون القضائي، و يتمثل هذا التعاون في مجموعة من الوسائل التي بواسطتها تقدم إحدى الدول المعاونة سلطاتها العامة أو مؤسساتها القضائية إلى سلطة التحقيق أو الحكم أو التنفيذ في دولة أخرى.[1]

كما تبرز أهمية التعاون القضائي الدولي في مكافحة الجرائم الالكترونية من خلال إلغاء الحدود الجغرافية، فهي تتحرك في فضاء شبكي يصعب معه ملاحقة المجرمين، و لهذا لابد من التعاون سواء على مستوى الإجراءات أو على مستوى التجريم و العقاب.[2]

إن فعالية التحقيق والملاحقة القضائية في الجرائم الالكترونية تتطلب تتبع أثر النشاط الإجرامي، من خلال مجموعة متنوعة من مقدمي خدمات الانترنيت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسوب الآلي بالأنترنيت، و حتي ينجح المحقق في ذلك فعليه تتبع أثر قناة الاتصالات بأجهزة الحاسوب المصدرية و الجهاز الخاص بالضحية أو بأجهزة تعمل مع مقدمي خدمات وسائط في بلدان مختلفة، و لتحديد مصدر الجريمة فيجب الاعتماد على السجلات التاريخية التي تبين متي و من أين و من قام بالتوصيلات، و وقت إجرائه، و في حالة كون مقدمو الخدمات خارج الولاية القضائية للمحقق فهنا لا بد من طلب المساعدة من المحقق في ولايته القضائية و هذا ما يسمي بالتعاون القضائي.[3]

إن التحقيقات في الجرائم الإلكترونية وملاحقة المجرم قضائيا يستلزم القيام بإجراءات خارج حدود الدولة، مثل المعاينة، سماع الشهود، ضبط الأقراص الصلبة، تفتيش الهواتف في حالة الاتصال عن بعد، القبض على المتهم كلها إجراءات تحتاج إلى ابرام اتفاقيات بين الدول و هذا لا يتحقق إلا بالمساعدة القضائية بين الدول، حيث من غير الممكن مكافحة و محاربة هذه الجريمة إلا بتظافر الجهود بين الدول.

---

[1] – حسنين صالح عبيد، **القضاء الجنائي الدولي(تاريخه، تطبيقاته، مشروعاته)**، دار النهضة العربية، القاهرة، 1977، ص، ص 99، 100.

[2] – يزيد بوحليط، **الجرائم الإلكترونية والوقاية منها في القانون الجزائري**، دار الجامعية الجديدة، الإسكندرية، 2019، ص 497.

[3] – السيد عبد الحميد أحمد، المرجع السابق، ص، ص 95، 96..

الفرع الثاني: المساعدة القضائية وصورها

تعرف المساعدة القضائية الدولية بأنها:" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخري بصدد جريمة من الجرائم"،[1] و تعتبر المساعدة القضائية المتبادلة إحدى مظاهر التعاون الدولي، فبعدما كانت تتسم في حالات بسيطة وتتخذ صور تقليدية، فأصبحت تأخذ مظاهر حديثة من أجل زيادة الفعالية في مكافحة الجريمة الالكترونية، و كذلك لتبسيط عمل الجهات القضائية التي تنظر في الدعوى العمومية الناشئة عن هذه الجريمة، خاصة مع تزايد امتداد هذه الجريمة في ظل التسهيلات التي وفرها التطور الحاصل في المجتمع.[2]

و من صور المساعدة القضائية:

أولا/ تبادل المعلومات:

يجب على الدول الموقعة على اتفاقيات مكافحة الجرائم الالكترونية، الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي اجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة، و الاتفاقيات الثنائية و مبدأ المعاملة بالمثل، فتبادل المعلومات التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت إلى رعاياها في الخارج و الإجراءات التي اتخذت ضدهم،[3] كما أن هناك مظهر آخر من مظاهر تبادل المعلومات و هو ما يتعلق بصحيفة السوابق القضائية للمتهمين و الصادرة من الجهات القضائية، من خلالها تتعرف الجهة القضائية بالتفصيل على الماضي الجنائي

[11] – سالم محمد سليمان الأوجلي، **أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية**، رسالة دكتوراه، كلية الحقوق، عين شمس، 1997، ص 425.

[2] – عباسي محمد الحبيب، **الجريمة المنظمة العابرة للحدود**، أطروحة لنيل شهادة الدكتوراه علوم، تخصص القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2016، 2017، ص 609.

[3] – المرجع نفسه، ص 105.

للفرد المحال إليها، و التي تساعد في تشديد العقوبة أو تخفيفها أو وقف تنفيذها، فهي التي تساعد في تطبيق الأحكام الخاصة بالعود و وقف تنفيذ العقوبة و عدم الأهلية.[1]

ثانيا/ نقل إجراءات الردع: يقصد به قيام دولة بناء على اتفاقية باتخاذ بنقل الاجراءات قيام الدولة بناء على اتفاق باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة وذلك إذا توافرت الشروط معينة:[2]

1- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها.

2- أن يتم الإجراء المطلوب بالشرعية، بمعنى آخر الاجراء المطلوب اتخاذه يؤدي حتما إلى الوصول للحقيقة و متخذ أيضا في الدولة المطلوب إليها عن ذات الجريمة.

4- يجوز لأي طرف متعاقد أن يطلب من أي طرف آخر أن يتخذ الإجراءات الجزائية في أي حالة من الحالات الأتية:

- إذا صدر في حق المتهم حكم يقيد حريته في الدولة الطالبة، و تكون الاجراءات مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.

- أن يحقق الاجراء المطلوب الوصول للحقيقة كأن يكون دليل الجرم متواجد على مستوى الدولة المطلوب إليها.

- أن يكون الحكم الصادر ضد الشخص يحقق له اعادة التأهيل الاجتماعي.

- أن يكون ضمان حضور المتهم أمام الدولة المطلوب إليها.

غير أنه و كاستثناء فإنه يجوز للدولة المطلوب إليها أن ترفض نقل الإجراءات في الحالات الأتية كأن تكون سبب النقل لا يدعو لهذا الإجراء أو مخالف لواجبات الدولة المطلوب إليها، إذا ثبت أن الطلب ورائه أسباب دينية أو إثنية أو قومية أو سياسية، إذا كانت الدولة المطلوب اليها قد طبقت قانونها على الجريمة قبل استلامها من الدولة

[1] - طارق إبراهيم الدسوقي، المرجع السابق، ص 569

[2] - غانم مرضي الشمري، المرجع السابق، ص 99.

الطالبة وكان الإجراء الذي سبق اتخاذه مطابقا للقانون وأخيرا إذا كانت الإجراءات المطلوبة مخالفة للمبادئ الأساسية للنظام القانوني في الدولة المطلوب اليها.

ثالثا/ الإنابة القضائية الدولية: تعد الإنابة القضائية أسلوبا هاما من أساليب التعاون الدولي في المجال الجنائي، والتي يتم من خلالها التغلب على العقبة التي تقف أمام تطبيق قانون الإجراءات الجزائية لدولة ما على جرائم ارتكبت داخل إقليم دولة أخرى – إقليمية الخصومة الجنائية –، ذلك أنه قد ينظر إليها على أنها خروج عن مقتضيات سيادة الدول،[1] ويقصد بها :"عمل بمقتضاه تفوض المحكمة (أو القاضي)، محكمة أخرى(أو قضيا آخر)، للقيام مكانها، و في دائرة اختصاصها، بأحد أو بعض إجراءات التحقيق أو الإجراءات القضائية الأخرى التي يقتضيها فصل الدعوى المرفوعة أمامها، و التي تعذر عليها مباشرتها بنفسها بسبب بعد المسافة أو أي مانع آخر".[2]

و ينصب موضوع الإنابة القضائية في الجرائم الإلكترونية على اتخاذ إجراء من إجراءات التحقيق أو الإثبات أو جمع الأدلة، حيث يتعذر على القاضي المنيب القيام بها بنفسه، وإجراءات التحقيق هي اجراءات قضائية تدخل في الخصومة الجزائية، و قد يكون محل الانابة القضائية شهادة الشهود أو اجراء التفتيش و ضبط الأشياء المتعلقة بالحاسوب، كما يمكن أن يكون محل الإنابة القضائية أي اجراء قضائي متي صدر من طرف قاضي و في أي مرحلة من مراحل الدعوى.[3]

الانابة القضائية تعتبر من أهم صور التعاون القضائي الدولي لمكافحة الجريمة الالكترونية، لأنها تهدف إلى تسهيل الإجراءات الجنائية بين الدول، و هذا لأن الجريمة الإلكترونية تتميز بسرعة التنفيذ و القيام بها في وقت واحد و من عدة دول، و الانابة تسهل

[1] – بن يحي نعيمة، **الإنابة القضائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم**، مجلة الدراسات الحقوقية، المجلد 4، العدد1، 2017، ص 11.

[2] – أحمد عبد العليم شاكر علي، **المعاهدات الدولية أمام القضاء الجنائي**، دار الكتب القانونية، مصر، 2006، ص 342.

[3] – نادية دردار، **الجهود الدولية لمكافحة الجريمة**، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص 88

اجراءات التحقيق و تقدم المتهمين للمحاكمة، و التغلب على مبدأ السيادة الذي يمنع الدول في التدخل في شؤون دولة أخرى.

رابعا/ تنفيذ الحكم الأجنبي: تم ابراهيم العديد من الاتفاقيات الدولية من أجل تنفيذ الأحكام الجزائية الأجنبية، و هذا من خلال عرض الحكم أمام جهة قضائية وطنية لمنحه الصيغة التنفيذية عندما يستوفي جميع طرق الطعن و يكون غير مخالف للنظام العام حسب قانون القاضي الآمر بالتنفيذ،[1] و هذا لمكافحة كل من تسول له نفسه ارتكاب جريمة في دولة و الهروب إلى دولة أخري.

الفرع الثالث: تسليم المجرمين في إطار مكافحة الجرائم الالكترونية

نظام تسليم المجرمين يعتبر خير مظاهر تضامن الدول، حيث تعددت المؤتمرات الدولية و تعاقبت لبحث الوسائل المتعددة لمكافحة المجرمين، لهذا بات التعاون الدولي ضرورة حتمية يفرضها الواقع الحالي، و لعل السبب في ذلك يرجع لطبيعة نظام التسليم و أثره المباشر في تحقيق أكبر قدر من الفعالية، فالتسليم هو تعبير صريح عن رغبة الدول في تحقيق هذا التعاون خاصة مع ظل التزايد المستمر للجرائم الالكترونية.

و قد يرتكب المجرم جريمة الكترونية و هو خارج البلاد سواء أكان مواطنا أم من جنسية مختلفة، و تصيب تلك الجريمة أمن و استقرار الدولة أو مركزها المالي، فيسري عليها القانون الوطني، باعتبارها من الحالات التي يمتد سريان قوانين الجزاء للدولة المتضررة لتطال مرتكبي تلك الجرائم خارج إقليمها، و لن يتأتى لها تفعيل قوانينها إلا باسترداد هؤلاء المجرمين و بمقتضي التعاون الدولي الذي تنظمه الاتفاقيات الدولية.

و يعرف نظام تسليم المجرمين:" قيام الدولة المطلوب منها التسليم بتسليم شخص موجود في إقليمها إلى الدولة طالبة التسليم بناء على طلبها بغرض محاكمته عن جريمة نسب إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمها"، ويعرف أيضا:" تخلي دولة لأخرى عن

[1] – الطيب زروتي، **القانون الدولي الخاص الجزائري مقارنا بالقوانين العربية**، مطبعة الكاهنة، الجزائر، 2000، ص 21.

شخص ارتكب جريمة لكي تحاكمه عنها، أو لتنفذ فيه الحكم الذي أصدرته عليه محاكمها، وذلك باعتبار أن الدولة طالبة التسليم هي صاحبة الاختصاص الطبيعي أو الأولى بمحاكمته وعقابه"[1]، وتسليم المجرمين هو:" أحد مظاهر التضامن الدولي لمكافحة الجريمة تقوم بموجبه دولة ما بتسليم شخص مقيم في إقليمها إلى دولة أخرى تطلبه لتحاكمه عن جريمة انتهك بها حرمة قوانينها أو لتنفيذ فيه حكما صادرا عليه من إحدى محاكمها، أي أنه تخلى دولة ما عن شخص موجود في إقليمها إلى دولة أخرى بناء على طلبها لتحاكمه عن جريمة يعاقب عليها قانونها أو لتنفذ فيه حكما صادرا عليه من إحدى محاكمها.[2]

و تخضع الجرائم الالكترونية للتسليم بمقتضي اتفاقيات دولية ذات نطاق عالمي، وهي جرائم اهتمت بها دول العالم بصفة خاصة سواء بالنظر لخطورتها الذاتية وما يترتب عليها من ضرر بالغ أو بالنظر لطريقة ارتكابها و ما تنطوي عليه من طابع دولي منظم.

و قد أخذت الاتفاقية الأوروبية للإجرام المعلوماتي بهذا الأسلوب حيث نصت في المادة 24 منها على أنه:" تطبق هذه المادة علي عملية تسليم المجرمين فيما بين الدول الأطراف بالنسبة للجرائم المنصوص عليها في المواد 2- 12 بهذه الاتفاقية بشرط أن يعاقب عليها القانون بموجب القوانين بالدولتين المعنيتين طرفي الاتفاقية بالحرمان من الحرية لفترة لا تزيد عن سنة على الأقل و بعقوبة أشد".[3]

---

[1] – إيهاب محمد يوسف، **اتفاقيات تسليم المجرمين ودورها في تحقيق التعاون الدولي لمكافحة الإرهاب**، رسالة دكتوراه في علوم الشرطة، القاهرة، 2003 ، ص 76.

[2] – جميل عبد الباقي الصغير: **الجوانب الإجرائية في تسليم المجرمين**، دار النهضة العربية، القاهرة، مصر، 1998، ص:85.

[3] – الجرائم هي:" الدخول غير مشروع(المادة2)، الاعتراض غير المشروع(المادة 3)، التدخل في البيانات(المادة 4)، التدخل غير المشروع في المنظومة(المادة 5)، إساءة استخدام الأجهزة(المادة 6)، جريمة التزوير المتعلقة بالكمبيوتر(المادة 7)، الجرائم المتعلقة بالأعمال الإباحية وصور الأطفال الفاضحة(المادة 9)، الجرائم الخاصة بالانتهاكات والنشر والحقوق المتعلقة بها(المادة 10)، الشروع والمساعدة والتحريض(المادة 11).

إذا كان نظام تسليم المجرمين يعد من أبرز صور التعاون التي تحققت للمجتمع الدولي في مكافحة الجريمة الالكترونية، والذي تنظم شروطه وأحكامه الاتفاقات الدولية المبرمة في هذا الشأن، إذ يكفل عدم إفلات المجرم من العقاب إذا التجأ إلى دولة أخرى غير تلك التي ارتكب فيها الجريمة، غير أن هذا النظام لم يبلغ بعد المرحلة التي يمكن أن تحقق معها كل الفائدة المرجوة منه، فمن المبادئ المقررة بصفة عامة : " أنه لا يجوز التسليم من أجل بعض الجرائم، كما لا يجوز تسليم رعايا الدول المطلوب منها التسليم، و لا شك أن هذه المبادئ من الممكن والجائز أن تتفق على خلافها الدول تماشيا مع ما تقتضيه روح التضامن الدولي في مكافحة الجريمة لكن ليس بصفة دائمة ومطلقة.

الفصل الثاني

الجهود الدولية والاقليمية في مكافحة الجرائم الالكترونية

تمهيد:

سعت المجتمعات إلى الحد من الجرائم الإلكترونية التي أصبحت تهدد الحياة من جميع النواحي سواء اقتصاديا و اجتماعيا و ثقافيا، فكما تصدت المجتمعات إلى الجرائم التقليدية و تم ردعها عن طريق سن القوانين و التشريعات، و سلكت نفس المسلك مع الجرائم الالكترونية، و ذلك بالتطرق إليها بالدراسة و التحليل من أجل وضعها في إطار قانوني يمكن من خلاله وضع الاتفاقيات و المعاهدات الدولية و الإقليمية لمكافحتها.

و تجسدت مكافحة هذه الجريمة من خلال نصوص المعاهدات و الاتفاقيات الإقليمية و الدولية و هذا تفاديا لإفلات الجاني منها، غير أن تطور و سرعة انتشار هذه الجريمة جعل هذه النصوص غير مواكبة لها، و بالتالي أصبحت غير مجدية في ما يخص مكافحة الجرائم الالكترونية، الأمر الذي جعل الدول المتقدمة تحاول إيجاد صيغ قانونية يمكن من خلالها الحد من هذه الجريمة المستحدثة.

و تعددت الجهود الدولية و الإقليمية لمكافحة هذه الجريمة نظرا للتهديدات الكبيرة التي جاءت بها الجرائم الإلكترونية على المستويين، و من هنا سنتطرق إليه في هذا الفص والذي قسمناه إلى:

المبحث الأول: المعاهدات والاتفاقيات الدولية التي تناولت الجريمة الالكترونية.

المبحث الثاني: المعاهدات والاتفاقيات الإقليمية لمكافحة الجريمة الالكترونية.

المبحث الأول: المعاهدات والاتفاقيات الدولية التي تناولت الجريمة الالكترونية

لا يختلف اليوم في أن الإجرام الالكتروني الدولي أخذ حجما و أبعادا لا يستهان بها، تقتضي العمل الدؤوب و التفكير الواعي و الجدي بغية الحد منه و من آثاره الهدامة، و مواجهة مثل هذه الظاهرة في نظرنا يمر عبر سلسلة من العمليات بدأ بالتوعية و الإعلام و معاينة هذا الداء و بيان آثاره السلبية، و كشف طرق تحركه و أماكن تواجده، حيث تعد الاتفاقيات الدولية و العالمية ذات الصلة بالمساعدة و التعاون القضائي، لكنها لا تجد في غالب الأحيان المجال للتطبيق العملي.

و قد تبنت مجموعة من المنظمات الدولية موضوع مكافحة الجرائم الإلكترونية، ووضعت على عاتقها مسؤولية إنشاء المعاهدات والاتفاقيات وتنفيذها بين الدول من أجل حماية شبكة الانترنيت من الاختراق.

المطلب الأول: اتفاقية برن ودورها في مكافحة الجريمة الالكترونية

بهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام اتفاقية برن الدولية في 9 سبتمبر 1886، و المكملة بباريس في ماي 1896، و المعدلة في برلين في 13 سبتمبر 1908، و المكملة ببرن في 20 مارس 1914، و المعدلة بروما في جوان 1928، و بروكسل سنة 1948، و استوكهولم في جويلية 1967، و باريس في جويلية 1971، و سميت باتفاقية برن لحماية المصنفات الأدبية و الفنية، حيث تشكل الدول الأطراف في هذه الاتفاقية اتحادا لحماية حقوق المؤلفين على مصنفاتهم الأدبية و الفنية.[1]

الفرع الأول: مبادئ اتفاقية برن

إن اتفاقية برن كأي اتفاقية دولية تعتمد على ثلاث مبادئ أساسية:

[1] – ليندة شرا بشة، **السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية**، مجلة دراسات وأبحاث، الجلفة، العدد1، 2009، ص 246.

1/ مبدأ المعاملة الوطنية: المصنفات الناشئة في إحدى الدول المتعاقدة، و هي مصنفات يكون مؤلفها من مواطني تلك الدولة أو نشرت لأول مرة في تلك الدولة، و هنا يتمتع المؤلف بنفس الحماية التي تمنحه لمواطنيها.

2/ مبدأ الحماية التلقائية: يجب أن تكون الحماية بدون شروط شكلية.

3/ مبدأ استقلال الحماية: بمعني لا تتوقف الحماية في بلد منشأ المنصف.

و بالرجوع إلى المادة الثانية الفقرة الحادي عشر من الاتفاقية نجدها وفرت الحماية لكل إنتاج في المجال الأدبي و العلمي و الفني، بأي طريقة تم التعبير عنه،[1] كما يتم حماية بعض الحقوق الاستئثارية كحق تحرير المصنفات و تحويلها،(المادة11) حق الأداء العلني للمسرحيات، حق نقلها إلى الجمهور، حق تلاوة المصنفات الأدبية علنا، حق الاستنساخ، حق استعمال مصنف ما لإنتاج مصنف سمعي بصري، و حق استنساخ هذا المصنف و توزيعه.

الفرع الثاني: الحقوق في اتفاقية برن

كما تحمل الاتفاقية مجموعة من الحقوق المعنوية كحق المطالبة بنسب المصنف لمؤلفه و حق الاعتراض عن أي تعديل أو تشويه أو تحريف قد يمس سمعة المؤلف،(المادة 6 من الاتفاقية)، و تكون مدة الحماية بعد انقضاء خمسين سنة بعد وفاة المؤلف، كما تسمح الاتفاقية كاستثناء بالانتفاع المجاني بالمصنفات المشمولة بالحماية و هذا حسب المواد 2/9 و المادة 10، المادة 10ثانيا، والمادة 11 ثانيا/3.[2]

أما الحقوق المالية فتتمثل في حق استغلال المصنف من قبل مؤلفه،(المادة 6) مقررا لهم حق استئثاري بالتصريح بعمل نسخ من مؤلفه، بأي طريقة و بأي شكل،(المادة 9) و

[1] – بن مكي نجاة، **السياسية الجنائية لمكافحة الجرائم المعلوماتية**، دار الخلدونية، الجزائر، 2017، ص92.

[2] – بن مكي نجاة، المرجع السابق، ص 94.

تعتبر هذه المادة أساس الاتفاقية، بالإضافة إلى الحق الاستئثاري في ترجمة مصنفاتهم أو تصريح بذلك طوال مدة الحماية(المادة 8).[1]

أما حول حماية البرمجيات في ظل هذه الاتفاقية فقد اعتبرتها مصنفات أدبية تخضع للحماية وفقا لقواعد اتفاقية برن للمصنفات الأدبية و الفنية، وهذه الحماية تكون على أساس معيارين:

1/ المعيار الشخصي: يستند إلى جنسية معد البرنامج أو موطنه، فاتفاقية برن تقرر اشتمال الحماية للمصنفات التي يعد مؤلفوها من رعايا إحدى دول اتحاد برن سواء كانت هذه المؤلفات منشورة أو غير منشورة.

2/ المعيار الإقليمي: يقوم على مكان أول نشر للمصنف وفقا لهذا البرنامج تتمتع البرمجيات بالحماية، إذا ما نشرت في إحدى دول الأعضاء، و هنا لا يعتد لا بجنسية المؤلف و لا محل إقامته.[2]

كما جاء في المادة 15 لمؤلفي المصنفات الأدبية و الفنية، إقامة دعاوي و مقاضاة من يتعدى على حقوقهم، كما أقرت المادة 16 منها على أن جميع النسخ المصنف غير مشروعة تكون في محل مصادرة في دول الاتحاد التي يتمتع بها المصنف الأصلي بالحماية القانونية.[3]

تعد هذه الاتفاقية أول وثيقة عالمية وضعت المبادئ العامة لحقوق الملكية الفكرية، كما تعد مرجع للاتفاقيات التي بعدها، إلا أنها لم تعالج النشر الإلكتروني عبر شبكات الأنترنيت، لأنه تم تعديلها سنة 1971أي قبل حدوث ثورة الاتصالات و المعلومات و ظهور

[1] – المواد 6، 8، و9 من باتفاقية برن لحماية المصنفات الأدبية والفنية.

[2] – بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، أطروحة دكتوراه تخصص قانون عام، جامعة يوسف بن خدة، الجزائر1، 2017، 2018،ص 09.

[3] – المواد 15، 16 من باتفاقية برن لحماية المصنفات الأدبية والفنية.

الأنترنيت بشكلها المتطور، و لهذا فهي تقدم الحلول للمشاكل المتعلقة بالمصنفات المنشورة على شبكة الأنترنت.

المطلب الثاني: اتفاقية الويبو و تريبس ودورها في مكافحة الجريمة الالكترونية.

تعد الاتفاقيتين من أهم الاتفاقيات الدولية في مكافحة الجرائم الإلكترونية وهذا ما سنتناوله في هذا المطلب بشيء من التفصيل.

الفرع الأول: اتفاقية الويبو و دورها في مكافحة الجريمة الالكترونية

منظمة الويبو هي إحدى وكالات الأمم المتحدة التي يبلغ عدد أعضائها 152 دولة، تم التوقيع عليها في ستوكهولم 1967 في السويد،[1] و ودخلت حيز التنفيذ 1970 وقعت اتفاقية ، و تفتح المنظمة العضوية لأي دولة بشروط و هي:

- أن تكون عضوية تابعة للأمم المتحدة أو عضو في أي وكالة تابعة للأمم المتحدة.
- أن توقع على النظام الأساسي لمحكمة العدل الدولية.
- أو تدعوها الجمعية العامة للويبو.

و من خلال استعراض بنود الاتفاقية فقد أكد أعضائها على حماية الملكية الفكرية في جميع أنحاء العالم، باعتبارها وسيلة لحفظ الإيداعات الإنسانية و تساهم في إثراء المجتمع، و هذا من أجل تشجيع الابتكار و تطوير ورفع كفاءة إدارة الاتحادات المنشئة في مجال حماية الملكية الصناعية و حماية المصنفات الأدبية و الفنية، كما يتعين على اتفاقية الويبو حماية حق المؤلف من خلال برامج الحاسوب أي كانت طريقة التعبير عنها أو شكلها، و قواعد البيانات أيا كان شكلها، إذا كانت تعتبر ابتكارات فنية بسبب اختيار محتوياتها أو ترتيبها.

[1] – تأسست المنظمة العالمية للملكية الفكرية" الويبو" بموجب اتفاقية تم التوقيع عليها في استكهولم في 14 يوليو 1967 تحت عنوان اتفاقية " إنشاء المنظمة العالمية للملكية الفكرية", ودخلت هذه الاتفاقية حيز التنفيذ سنة 1970، وتعتبر هذه المنظمة إحدى الوكالات المتخصصة للأمم المتحدة ابتداء من ديسمبر 1974.

و بعد تزايد الحاجة إلى نصوص قانونية لحماية البرامج شكلت المنظمة العالمية للملكية الفكرية (الويبو)مجموعة عمل تضم عدد من الخبراء من أجل حماية الحاسوب الآلي، و في 1985 و بالتعاون بين الويبو و اليونسكو في جنيف ساد الاتجاه أغلب دول العالم الثالث إلى الميل لخضوع برنامج الحاسب الآلي لقوانين حماية حق المؤلف، و منذ هذا التاريخ جل الدول غيرت تشريعاتها الداخلية الخاصة بحق المؤلف و زادت برامج الحاسب الآلي إلى المصنفات الأدبية المحمية و فقا للقانون.[1]

بادرت منظمة الويبو إلى تدعيم تدريس حماية الملكية الفكرية بفرعيها الملكية الصناعية و الملكية الأدبية والفنية في كليات الحقوق بالجامعات العربية، كما تعد المصدر الأشمل في العالم من حيث البيانات المتعلقة بنظام الملكية الفكرية، و من حيث الدراسات التجريبية و التقارير و المعلومات الواقعة و الخاصة بالملكية الفكرية، و تشجع مبادرة نشر بيانات الملكية الفكرية على الصعيد العالمي، و تدعم تبادل بيانات الملكية الفكرية بين مكاتب الملكية الفكرية الوطنية و الإقليمية و الويبو، و هناك عدة قواعد بيانات.[2]

و تتعلق الحماية الممنوحة للمؤلف بحق التوزيع و حق التأجير التجاري لنسخة أصلية أو غيرها من النسخ الثلاث للمصنفات و هي برنامج الحاسوب و المصنفات السنيمائية، و المصنفات المجسدة في تسجيلات صوتية حسب تحديدها في القانون الوطني للأطراف المتعاقدة، كذلك حق نقل المصنف للجمهور بأي طريقة سلكية أو لاسلكية، أما مدة الحماية فتكون لمدة خمسين سنة على الأقل لأي مصنف، كما تلتزم المعاهدة بتوقيع جزاءات ضد التحايل على التدابير التكنولوجية و ضد أي حذف أو تغيير في المعلومات الضرورية مثل بعض البيانات التي تعرف المصنفات أو مؤلفيها لإدارة حقوقهم.[3]

---

[1] – محمود أحمد عبابنة، **جرائم الحاسب وأبعادها الدولية**، ط1، دار الثقافة، عمان، الأردن، 2005، ص 162.

[2] – جبران خليل ناصر، **حماية الملكية الفكرية: حقوق المؤلف في ظل التشريعات الوطنية والاتفاقيات الدولية**، أطروحة دكتوراه علوم، تخصص علم المكتبات والعلوم الوثائقية، جامعة أحمد بن بلة، وهران 1، 2017، 208، ص 104.

[3] – المرجع نفسه، ص، ص 116، 117.

و نصت المعاهدة على إنشاء جمعية للأطراف المتعاقدة و مهمتها تطوير الاتفاقية، و هذا ما تم بعد توقيع اتفاقية المنظمة العالمية للملكية الفكرية في 20 ديسمبر 1996،[1] و تعتبر هذه الاتفاقية بمثابة الاطار القانوني لحماية حقوق التأليف على شبكة الأنترنيت، فقد جاءت لتصدي المشكلات الناتجة عن التكنولوجيا الرقمية.

و بعد تزايد الحاجة إلى نصوص قانونية لحماية البرامج شكلت المنظمة العالمية للملكية الفكرية (الويبو) مجموعة عمل تضم فدد من الخبراء من أجل حماية الحاسوب الآلي، و قد ساد اتجاه أغلب دول العالم الثالث إلى الميل لخضوع برنامج الحاسب الآلي لقوانين حماية حق المؤلف، و منذ هذا التاريخ جل الدول غيرت تشريعاتها الداخلية الخاصة بحق المؤلف و زادت برامج الحاسب الآلي إلى المصنفات الأدبية المحمية و فقا للقانون.[2]

جاءت اتفاقية الويبو لتوجب على الدول الأطراف ضرورة حماية حقوق التأليف على شبكة الأنترنيت، كما يمتد نطاق الحمية ليشمل برنامج الحاسوب الآلي باعتباره مصنفات أدبية، كما أكدت المادة الخامسة منه على أن نطاق الحماية جاء ليشمل قواعد البيانات أيا كان شكلها، فحماية الموقع الالكتروني يمتد ليشمل هذه القواعد باعتبارها محمية بموجب قواعد حماية حق التأليف على شبكة الأنترنيت،[3] التي تمتد بناء على المادة الثالثة عشرة من الاتفاقية إلى نهاية مدة خمسين سنة على الأقل.

أوجبت الاتفاقية على الأطراف المتعاقدة أن تنص في قوانينها على حماية مناسبة وجزاءات في حالة التحايل على التدابير التكنولوجية التي يستعملها المؤلفون لدى ممارسة

[1] – تأسست المنظمة العالمية للملكية الفكرية" الويبو" بموجب اتفاقية تم التوقيع عليها في استكهولم في 14 يوليو 1967 تحت عنوان اتفاقية "إنشاء المنظمة العالمية للملكية الفكرية", ودخلت هذه الاتفاقية حيز التنفيذ سنة 1970 ، وتعتبر هذه المنظمة إحدى الوكالات المتخصصة للأمم المتحدة ابتداء من ديسمبر 1974 وبعدها تم تعديلها سنة 1996.

[2] – محمود أحمد عبابنة، المرجع السابق، ص 162.

[3] – بقنيش عثمان، مصطفي هنشور وسيمة، **حماية الملكية الفكرية على الأنترنت في إطار المنظمة العالمية للملكية الفكرية**، مجلة البحوث في الحقوق والعلوم السياسية، العدد 02، 2015، ص، ص 367، 368.

حقوقهم على شبكة الأنترنيت، كما تمنع من مباشرة أعمال لم يصرح بها المؤلفون أو لم يسمح بها القانون والمتعلقة بمصنفاتهم و المتواجدة في المواقع الالكترونية.

كما ألزمت الاتفاقية بتوقيع عقوبات على كل من حذف أو غير بدون إذن معلومات واردة في شكل الكتروني، و أيضا لكل من يوزع ل أغراض التوزيع أو يذيع أو ينقل إلى الجمهور دون إذن، مصنفات أو نسخ عن مصنفات مع علمه بأنه قد حذفت منها أو غيرت فيها دون إذن، معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق.[1]

ود عملت المنظمة على تبني نصوص تشريعية لحماية برامج الحاسب الآلي الإلكتروني، حيث قامت بتعريفه حيث اعتبرته: "مجموعة تعليمات يمكنها إذا ما وضعت على ركيزة يستوعبها الجهاز، أن تحقق نتيجة ما بواسطة هذه الآلة القادرة على التعامل مع المعلومات"، كما قامت بإعداد نصوص نموذجية من خلال جمع عدد من الخبراء من شتى أنحاء العالم من أجل مساعدة الدول على استكمال تشريعاتها في مجال حماية البرامج أو مجرد توضيحها.[2]

و كما جاء في الاتفاقية الثانية للويبو في المادة الثامنة عشرة، توفير الحماية الازمة و توقيع الجزاء ضد التحايل على التدابير التكنولوجية التي يستغلها الفنانون فيما يخص مصنفاتهم، كما نصت على جزاءات في حالة من قام بحذف أو تغيير إذن لمعلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق، أو توزيع أو استراد لأوجه أداء مثبتة أو تسجيلات صوتية دون إذن صاحبها، كما تتطلب الاتفاقية من الدول الأطراف اتخاذ التدابير الازمة لضمان تطبيق أحكامها، كتوقيع الجزاءات العاجلة لمنع التعديات الأخرى.[3]

---

[1] – عبد الله عبد الكريم عبد الله، المرجع السابق، ص267.

[2] – محمد حسام، محمود لطفي، **الحماية القانونية لبرامج الحاسب الالكتروني**، ط1، دار الثقافة للطباعة والنشر، القاهرة، 1978، ص 161.

[3] – بقنيش عثمان، مصطفي هنشور وسيمة، المرجع السابق، ص 371.

الفرع الثاني: اتفاقية تريبس ودورها في مكافحة الجريمة الالكترونية

إن الاهتمام بحماية الملكية الصناعية كان منذ القدم، إلا أن الحماية الفعلية كانت أعقاب الثورة الصناعية و ما تبعها من تطورات و اختراعات، هذا ما جعل العديد من الدول تقر بضرورة حمايتها، من خلال الاعتراف لأصحاب الاختراع بملكيته، و أنشئت براءة الاختراع كأداة لهذا الغرض، الذي يعد سند الملكية و يتمتع صاحبه بمجموعة من الحقوق التي تخول له الاستئثار باستغلال و التصرف في اختراعه.[1]

و قد سعت جولة الأورجوان، لمنظمة التجارة العالمية عن اتفاقية تريبس التي تم التوقيع عليها من طرف الدول الأعضاء بها سنة 1994، إلى توفير نظام قانوني فعال يحمي الاختراعات و يحفظ حقوق مالكها عن طريق براءة الاختراع، و تعد الوسيلة القانونية لإضفاء الحماية القانونية على الاختراع موضوع البراءة، و هذا من خلال النص على نصوص قانونية تحمي مالكي البراءة.[2]

توسعت اتفاقية تريبس في اسباغ الحماية القانونية على ما يتم التوصل إليه من ابتكارات، و ذلك بإعطائها الحق في الحصول على البراءة عن أي اختراع، و تعتبر هذه الاتفاقية أول اتفاقية دولية لحماية حقوق الملكية الصناعية و التجارية، حيث تناولت براءات الاختراع ضمن أحكامها دون أن تورد تعريفا لها،مكتفية بتحديد مشتملاتها، فجاء فيها أن براءة الاختراع تشمل مختلف أنواع البراءات الصناعية التي تقرها تشريعات دول الاتحاد، ثم توالت الاتفاقيات إلى أن وصلت للاتفاقية المتعلقة بالتجارة، و تعتمد اتفاقية تريبس على مبدأين لمنح براءة الاختراع، أولهما مبدأ قابلية كافة الاختراعات للحصول على براءة الاختراع وهذا

[1] – سقار فايزة، **الحق الاستثماري على براءة الاختراع في اتفاقية تريبس بين مبدأ احتكار الاستغلال والقيود الواردة عليه**، مجلة دراسات وأبحاث، المجلة العربية في العلوم الإنسانية والاجتماعية ، مجلد 12، العدد 3، جويلية 2020، ص 684.

[2] – الأورجواي هي الجولة الأخيرة في سلسلة الجولات التفاوضية التي عقدت بين ممثلي دول العالم التي بدأت جولتها منذ عام 1948، بهدف تحرير التجارة وتنميتها ، وسميت بهذا الاسم نسبة إلى البلد الذي بدأت فيه منذ 20 سبتمبر 1986. – نجاة بن مكي، المرجع السابق، ص 96.

من خلال منح براءة الاختراع لكل الاختراعات سواء كانت منتجات أو عمليات صناعية، في جميع مجالات و ميادين التكنولوجيا،[1] أما المبدأ الثاني فهو عدم التمييز بين الاختراعات و هذا من خلال عدم جواز تمييز الدول الأعضاء بين الاختراعات على أساس نوع الاختراع أو مكانه أو إذا كانت مستوردة أو منتجة محليا.[2]

و كما وسعت اتفاقية تريبس نطاق الاختراعات المحمية ببراءة الاختراع ، فقد أجازت للدول الأعضاء أن تستثني مبدأ قابلية جميع الاختراعات للحصول على البراءة، و تشمل هذه الاستثناءات:

- الاختراعات التي يتعارض استغلالها مع النظام العام و الأخلاق الفاضلة.[3]
- الاختراعات المتعلقة بطرق تشخيص و العلاج و جراحة الإنسان و الحيوان.[4]
- الاختراعات المتعلقة بالحيوانات و النباتات خلاف الأحياء الدقيقة و الطرق البيولوجية. [5]

و وفقا لهذه الاتفاقية فإن البرمجيات محل للحماية سواء أكانت بلغة الألة أو المصدر، و لمؤلفها كافة الحقوق المالية و المعنوية لمصنفات حق المؤلف و هذا ما جاء في المادة 1/10، اضافة إلى حقه في اجازة أو منع تأجيرها شأنها شأن التسجيلات الصوتية و

---

[1] – المادة 27 /1 من اتفاقية تريبس:" .....تتاح إمكانية الحصول على براءات اختراع لأي اختراعات، سواء أكانت منتجات أم عمليات صناعية ، في كافة ميادين التكنولوجيا...".

[2] – المادة 1/27:"....تمنح براءات الاختراع ويتم التمتع بحقوق ملكيتها دون تمييز فيها يتعلق بمكان الاختراع أو المجال التكنولوجي أو ما إذا كانت المنتجات مستوردة أم منتجة محليا"

[3] – المادة 2/27:" يجوز للبلدان الأعضاء أن تستثني من قابلية الحصول على براءات الاختراع التي يكون منع استغلالها تجاريا في أراضيها ضروريا لحماية النظام العام أو الأخلاق الفاضلة، بما في ذلك حماية الحياة أو الصحة البشرية أو الحيوانية أو النباتية أو لتجنب الأضرار الشديدة بالبيئة، شريطة ألا يكون ذلك الاستثناء ناجما فقط عن حظر قوانينها لذلك الاستغلال

[4] – المادة 3/27(أ):" يجوز أيضا للبلدان الأعضاء أن تستثني قابلية الحصول على براءات الاختراع طرق التشخيص والعلاج والجراحة الازمة لمعالجة البشر أو الحيوانات".

[5] – المادة 3/27(ب):" يجوز أيضا للبلدان أن تستثني من قابلية الحصول على براءات اختراع النباتات أو الحيوانات، خلاف الأحياء الدقيقة والطرق البيولوجية في معظمها لإنتاج النباتات أو الحيوانات خلاف الأساليب والطرق غير البيولوجية الدقيقة، غير أنه على البلدان الأعضاء منح الحماية لأنواع النباتات إما عن طريق براءات الاختراع أو نظام فريد فذ خاص بهذه الأنواع أو بأي مزيج منهما".

المرئية(المادة 11)، و يستثنى وفق هذه المادة حالة التأجير التي لا يكون فيها البرنامج الموضوع الأساسي للتأجير، و أما مدة الحماية فهي تمتد إلى 50 عام محسوبة على أساس حياة الشخص الطبيعي، فإن لم تكن كذلك فمن نهاية السنة التي أجيز فيها النشر أو تم فيها انتاج العمل.[1]

كما تناولت الاتفاقية تحرير التجارة العالمية من مختلف مناحي النشاط التجاري على الصعيد الدولي، و لأهمية حماية الملكية الفكرية من جانب النظام التجاري العالمي، و تتوحد جميع أحكام الاتفاقية في هدف واحد و هو تحرير التجارة العالمية، مع ضرورة توفير إجراءات و تدابير لإنفاذ حقوق الملكية الفكرية دون أن تقف أمام عائقا أمام التجارة الدولية المشروعة، و أيضا العمل على تشجيع الحماية الفاعلة في مجال حقوق الملكية الفكرية بجميع فروعها.[2]

يتضح من بنود هذه الاتفاقية أنها وضعت حد أدني من الحماية القانونية في كل مجالات الملكية الفكرية، في حين نجد الدول الأعضاء فيها تضع حماية تفوق الحماية التي وضعتها الاتفاقية، و لا يمكن أن تكون أدنى منها، و عليه يجب أن تتفق بنصوص الاتفاقية مع التشريعات الداخلية للدول الأعضاء، و كان من مصلحة الدول الصناعية المتقدمة و على رأسها الولايات المتحدة الأمريكية من الانضمام للاتفاقية، وهذا بسبب الخسائر في جانب الملكية الفكرية، لأنها هي الاولي المعرضة من قرصنة الملكية الفكرية.

المبحث الثاني: المعاهدات والاتفاقيات الإقليمية لمكافحة الجريمة الالكترونية

يتم على مستوى القارة الأوروبية عمل مكثف في مجال مواجهة الإجرام الالكتروني على مختلف الأصعدة سواء في مجال البحث العلمي أم التشريعي أم الوقاية أم المكافحة، إلى درجة بروز ملامح سياسة أوروبية واضحة في ميدان مواجهة الإجرام الالكتروني، و الجريمة

[1] – أمير فرج يوسف، **الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت**، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2011، ص 407.

[2] – بدري فيصل، المرجع السابق، ص 13.

بصفة عامة تتسم بديناميكية ونشاط دؤوب لكافحتها، و الدليل علة ذلك ظهور الهيئات و الأجهزة الأوروبية الموحدة في السنوات الأخيرة، كالأوروجيست لتوحيد العمل القضائي، و الأوروبول لتنسيق العمل الشرطي، و المدعي العام الأوروبي لإزاحة العوائق القضائية في مجال تنفيذ أوامر القضاء.

و تعد الاتفاقيات و المعاهدات الاقليمية من أهم صور التعاون الدولي بصفة عامة و في مجال مكافحة الجرائم الالكترونية بصفة خاصة، و من بين المعاهدات و الاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية معاهدة بودابست لمكافحة جرائم الإنترنت، و توصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، والقانون العربي النموذجي ونبينهما فيما يلي:

المطلب الأول: معاهدة بودابيست

الفرع الأول: الاطار القانوني لمعاهدة بودابيست

تم التوقيع على معاهدة بودابيست في 23 نوفمبر 2001 و المتعلق بالإجرام الكوني من طرف مجلس أوروبا،[1] و جاءت لمكافحة الجرائم الإلكترونية و هذا بسبب التغيرات العميقة التي حدثت في الرقمنة و التقارب و العولمة المستمرة للشبكات المعلوماتية، و سميت الاتفاقية الدولية لمكافحة الإجرام عبر الأنترنيت، تمت صياغتها من طرف خبراء قانونيين في مجلس أوروبا و بمساعدة عدة دول من بينها الولايات المتحدة الأمريكية و اليابان و كندا و جنوب افريقيا، و بعد مشاورة عدة حكومات و أجهزة شرطة وقطاع كمبيوتر على مستوى العالم، تم التوقيع عليها من طرف ثلاثون دولة،[2] كما أنشأ الاتحاد الأوروبي أجهزة تساعد

[1] – معاهدة بودابيست هي معاهدة تمت بالعاصمة المجرية بودابيست في 2001 وهي أول معاهدة دولية تكافح جرائم الأنترانت وتبلور التعاون الدولي في محاربته، بعدما أصبحت عدة جرائم تهدد الأشخاص والممتلكات وبعد التوقيع عليها من طرف مسؤولين في الدول الأوروبية بالإضافة إلى أمريكا واليابان وكندا وجنوب افريقيا، بعد مشاورات ومفاوضات دامت ما يزيد عن الأربع سنوات، حتي تم التوصل للصيغة النهائية والتوقيع عليها دون أي اعتراض، ودخلت حيز النفاذ 2004.

[2] – هلالي عبد الله أحمد، **الجوانب الموضوعية والاجرامية لجرائم المعلوماتية على ضوء اتفاقية بودابيست الموقعة في 23 نوفمبر 2001**، ط1، دار النهضة العربية، القاهرة، 2003، ص 1 .

على مكافحة هذا النوع من الجرائم، من بينها جهاز اليوربول و المركز الأوروبي لمكافحة الجرائم الالكترونية و الذي افتتح في جانفي 2013.

جاءت هذه الاتفاقية اقتناعا بضرورة مباشرة سياسة عقابية مشتركة موجهة لحماية المجتمع من الاجرام في الأوساط المعلوماتية، لاسيما من خلال تبني تشريع مناسب و من خلال تطوير التعاون الدولي،[1] و وعيا بالتغيرات العميقة الناجمة عن الرقمنة و التقارب و العولمة، و انشغالا بالمخاطر الناجمة عن المخالفات الجنائية التي قد تنفذ عبر الشبكات المعلوماتية و الالكترونية، ذات الخصوصية و الصعوبة في تقفي أدلتها، و اعتقادا بضرورة التعاون الدولي بهدف المواجهة الفعالة و السريعة لتلك الجرائم.

و تتكون الاتفاقية من ديباجة و ثماني وأربعين (48) مادة و هي تعالج ثلاث محاور الأول الجرائم التي تتعرض لها شبكة الأنترنيت و الحاسب الآلي، و الثاني الجوانب الإجرائية للجرائم المعلوماتية و أخير التعاون الدولي بين الدول الأعضاء لمكافحتها، و من ضمن البنود التي تناولتها الاتفاقية هو الإرهاب الالكتروني، عمليات تزوير بطاقات الائتمان ودعارة الأطفال، لأنها تعتبر من أكثر الجرائم انتشارا على المستوى العالمي،[2] و قد جاء في التقرير التفسيري لاتفاقية الجريمة الالكترونية الصادر عن مجلس أوروبا (سلسلة المعاهدات الاوروبية رقم 185)، أنه بالإضافة إلى تدابير التعاون الدولي من خلال تسليم المجرمين و المساعدة القضائية، ينبغي معالجة مسائل القانون الموضوعي و الاجرائي بكل ما يتصل باستخدام تكنولوجيا المعلومات، و حددت المواضيع القانونية التي يجب إعادة النظر لها:

1- جرائم الفضاء الالكتروني، كالمعاملات المالية غير المشروعة، انتهاك حقوق المؤلف، تقديم خدمات غير قانونية والجرائم التي تنتهك كرامة الانسان وحماية القصر.

2- ضرورة تبني مقاربة مشتركة لأغراض التعاون الدولي.

---

[1]- وليد طه ، **التنظيم التشريعي للجرائم الالكترونية في اتفاقية بودابيست** ، مطبوعة الكترونية ، ص 14 متاحة على الموقع : http://www.lasportal.org/ar/legalnetwork/Documents/

[2] - نادية دردار، المرجع السابق، ص 165.

3- استخدام طرق قسرية كالرقابة الالكترونية و اعتراض الاتصالات على شبكات المعلومات و حتى مصادرة مواقع الانترنت وقد يمتد في البيئة الالكترونية الى تجاوز الحدود، و حماية المعلومات بالتشفير مثلا.

4- تناول مسألة الاختصاص القضائي فيما يتعلق بجرائم تكنولوجيا المعلومات لتحديد مكان ارتكاب الجريمة، و القانون الواجب التطبيق، تنازع الاختصاص الاقليمي.

إضافة إلى أن الاتفاقية تحدد أفضل الطرق الواجب إتباعها في جرائم الأنترنيت، كما تحاول إقامة توازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة، و القلق الذي عبرت عنه منظمات الدفاع عن حقوق الإنسان، حيث يتزايد القلق بزيادة الرقابة على انتهاك حقوق مستخدمي الأنترنيت.[1]

كما تهدف إلى السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوربية، كما تأكد على ضرورة التعاون الإقليمي والدولي في ميدان مكافحة الجرائم المعلوماتية، و تحقيق التوازن بين حقوق الإنسان والاجراءات المتخذة لمواجهة هذه الجرائم، و قد سعت هذه الاتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم الالكترونية في جميع أنحاء العالم من خلال التنسيق التشريعات الوطنية ببعضها البعض، و تعزيز قدرات القضاء و كذا تحسين التعاون الدولي في هذا الإطار، بالإضافة إلى تحديد و تشديد العقوبات على من يرتكب جرائم الكترونية في إطار القوانين المحلية. [2]

[1] – منير محمد الجمبيهي، ممدوح محمد الجنبيهي، **جرائم الانترنيت والحاسوب الآلي ووسائل مكافحتها** ، دار الفكر الجامعي، الإسكندرية، 2006، ص 180.

[2]– صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، شهادة الماجستير في القانون ، تخصص القانون الدولي للأعمال ، جامعة مولد معمري، تيزي وزو، 2013، ص 99.

الفرع الثاني: مواضيع الاتفاقية

تطرقت الاتفاقية إلى جرائم الكمبيوتر أو الجرائم الالكترونية تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات، و أيضا الجرائم التي تستخدم كوسيلة للهجوم على بعض المصالح القانونية، كما عالجت الاتفاقية الغش المعلوماتي و التزوير المعلوماتي و الجرائم المرتبطة بالمحتوى بمعنى الإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية، و أيضا جرائم الاعتداء على الملكية الفكرية والحقوق المرتبطة بها، و أيضا الجزاءات و الإجراءات أو التدابير و ذلك طبقا للمعايير الدولية الحديثة و مسؤولية الأشخاص المعنوية.[1]

و هكذا عرفت الاتفاقية الاوروبية:

أ: نظام الكمبيوتر: أي جهاز يتألف من أجهزة و برمجيات تم تطويرها من أجل المعالجة التلقائية للبيانات الرقمية،[2] و يمكن أن يشمل المدخلات و المخرجات، و مرافق التخزين، و يمكن أن يشتغل لوحده أو أن يكون مثلا بشبكة مع غيرها من الأجهزة المماثلة.[3]

ب: الشبكة: يمكن تعريف شبكة الحاسوب على أنها:" نظام لربط جهازين أو أكثر باستخدام إحدى تقنيات نظم الاتصالات من أجل تبادل المعلومات و الموارد و البيانات، كما تسمح بالتواصل المباشر بين المستخدمين"،[4] من جهة أخرى تعتبر شبكة الإنترنت من أهم الشبكات، و تسمى أيضا بشبكة الشبكات، فهي عبارة عن:" مجموعة من الحواسب المتصلة فيما بينها عن طريق أسلاك أو دون أسلاك، بحيث يمكن لأي منها الوصول إلى محتوى

---

[1] – حنان ريحان مبارك المضحكي، **الجرائم المعلوماتية(دراسة مقارنة)**، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014، ص 383.

[2] – دليل الأدلة الالكترونية، دليل أساسي لموظفي الشرطة، والمدعين العامين والقضاة، ، دليل مجلس أوروبا حول الأدلة الإلكترونية، النسخة ا2، قسم الجريمة الإلكترونية، المديرية العامة لحقوق الإنسان وسيادة القانون، ستراسبورغ، فرنسا، 15 ديسمبر 2014، ص 18.

[3] – هلالي عبد الله أحمد، المرجع السابق ، ص 18.

[4]– فايز الظفيري، **الأحكام العامة للجريمة الإلكترونية**، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر، العدد 2، 2002، ص 494.

الآخر واستخدام موارده من تطبيقات و قواعد معطيات وغيرها من المعلومات"، إن الهدف الدائم من الشبكة هو التشارك في المصادر و هي تتضمن الملفات و قواعد البيانات و البرامج...إلخ.[1]

ج: مقدم الخدمة: فئة واسعة من الأشخاص أو هيئات الذين يضلعون بدور خاص فيما يتعلق بالاتصال أو معالج البيانات ذات الصلة بأنظمة الكمبيوتر، (تخزين، معالجة، استضافة...).[2]

د:بيانات الحركة: فئة من بيانات الكمبيوتر الخاضعة لنظام قانوني خاص، و يتم توليدها من أجهزة الكمبيوتر إلى سلسلة الاتصالات لأجل توجيه اتصال من المصدر الاصلي الى الوجهة، تعتبر بيانات الحركة فرعية و مساعدة على الاتصال في حد ذاته .

تناولت الاتفاقية من المادة الثانية إلى المادة السادسة الجرائم ضد سرية وسلامة وإتاحة البيانات و النظم المعلوماتية، و هي جرائم الدخول غير المشروع للنظم المعلوماتية، والاعتراض غير القانوني لهذه النظم و الاعتداء على سلامة البيانات و إساءة استخدام أجهزة الحاسب، و تناولت المادتان السابعة و الثامنة التزوير و الغش المعلوماتي، كما جاء في المادة التاسعة الجرائم المتصلة بالمواد الإباحية للأطفال، و تضمنت المادة العاشرة الاعتداء على حقوق الملكية الفكرية و الحقوق المجاورة، أما المادة الحادي عشر تناولت الشروع و الاشتراك في هذه الجرائم، و قد شملت الاتفاقية مسئولية الأشخاص المعنوية عن ارتكاب هذه الجرائم، و هي مسئولية مستحدثة في التشريع الجنائي المعاصر وأيضا الجزاءات، هذه الجوانب الموضوعية للاتفاقية تهدف إلى تحسين و اصلاح وسائل منع و قمع الإجرام المعلوماتي، و هذا من خلال تحديد الحد الأدنى المشترك الذي يسمح باعتبار

---

[1]– عبد الله عبد الكريم عبد الله، **جرائم المعلوماتية والإنترنت(الجرائم الإلكترونية)–دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا**، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص20.

[2] – محمود أحمد عبابنة، المرجع السابق، ص 166.

بعض التصرفات من قبيل الجرائم الجنائية، و هذا النوع من التجانس يسنح بمكافحة هذه الجرائم سواء على المستوى الوطني أو الدولي.[1]

كما جاء في المحور الثاني من الاتفاقية الجوانب الإجرائية إذ أوصت الدول الأعضاء باتخاذ الإجراءات اللازمة و الضرورية لضبط و نسخ الأدلة المعلوماتية، و استحداث تنظيم لإجراءات هذا الضبط و تمكين سلطات التحقيق من الحصول على نسخ من الأدلة و تفتيش و ضبط البيانات المعلوماتية المخزنة آليا، و وضع نظم لمراقبة الإنترنت و التحفظ العاجل على البيانات المعلوماتية و اعتراضها.[2]

وفي المحور الأخير تناولت التعاون الدولي في مكافحة الجريمة الالكترونية، حيث نصت الاتفاقية على إمكانية التعاون الدولي في مكافحة الجرائم الإلكترونية عابرة الحدود، من خلال تسليم المجرمين و المساعدة القضائية المتبادلة، كما نصت على إجراءات طلب المساعدة القضائية المتبادلة، و تحديد مجالات هذه المساعدة في الإجراءات الوقتية العاجلة و في مجالات سلطات التحقيق، و ختاما فإن الانضمام إلى هذه الاتفاقية ذات اهمية قصوى من أجل التعاون الدولي لمكافحة الجرائم الإلكترونية خاصة مع تنامى جرائم الإرهاب على مستوى دول العالم[3].

مما سبق نلاحظ أن الاتفاقية الأوروبية حضت بتقديم بعض الحلول للتغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمكافحة الجرائم الإلكترونية، كما شجعت الاتفاقيات الدولية من أجل التعاون فيما بينها، و تدعوها لإنشاء قنوات الاتصال بين و كالاتها و دوائرها المتخصصة من أجل تبادل المعلومات، من أجل تأمين المساعدة المباشرة

---

[1] – اتفاقية بودابيست لمكافحة جرائم المعلوماتية، ص 34.

[2] – هلالي عبد الله أحمد، المرجع السابق، ص 30.

[3] –رشدي محمد علي، **الجرائم المعلوماتية دوليا خطر دولي، مواجهة جرائم الإنترنت بين اتفاقية « بودابست» والتشريعات الوطنية**، اطلع عليه في 16أوت 2021 على الساعة 12.00. على الموقع الإلكتروني:
https://gate.ahram.org.eg/daily/News/536569.aspx

للتحقيقات المتعلقة بالجرائم الالكترونية، بالإضافة إلى تحديث القوانين الجنائية منها الموضوعية و الإجرائية بما يتناسب التطور الذي تشهده تكنولوجيا الاعلام و الاتصال.

المطلب الثاني: القانون العربي النموذجي

رغم أن الجريمة الالكترونية لم تنتشر في الدول العربية مقارنة بدول العالم الأخرى، إلا أن هذا لا يمنع من اتخاذ الاجراءات اللازمة للحد من انتشارها، حيث سعت الدول العربية من خلال القوانين و المؤتمرات للحث على مكافحتها، و من أجل هذا اعتمدت القانون العربي النموذجي لمكافحة جرائم الكمبيوتر، خطوة فعالة في مجال حماية الكمبيوتر من الجرائم المعلوماتية، و كان لازما على الدول العربية إيجاد قانون لأنها ليست بمنأى عن هذه الجرائم المستحدثة.

الفرع الأول: تعريف القانون العربي النموذجي

قامت الدول العربية بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، كما أدت هذه الاتفاقية إلى ميلاد قوانين عديدة لمكافحة الجريمة الالكترونية في الدول العربية، و صارت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها، ليكتمل نصاب الدول السبع لسريانها،[1] و عرفت ديباجة الاتفاقية كل ما يتعلق بالكمبيوتر والانترنيت، و أكدت المادة الأولى منها بأن الهدف من الاتفاقية هو:" تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدولة العربية و مصالحها وسلامة مجتمعها و أفرادها".

الفرع الثاني: أنواع الجرائم الالكترونية

عددت الاتفاقية 13 جريمة الكترونية في الفصل الثاني منها و هي:[2]

[1] – حفوظة الأمير عبد القادر، غرادين حسام، **الجريمة الإلكترونية وآليات التصدي لها**، أعمال الملتقي الوطني، آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 99.

[2] – الفص الثاني من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010

1- جريمة الدخول أو البقاء غير المشروع، مع كل أو جزء من تقنية المعلومات أو الاستمرار فيه، و تشدد العقوبة حال المحو أو التعديل أو التشويه أو النسخ والنقل والتدمير للبيانات و الاجهزة و الانظمة الالكترونية وشبكات الاتصال و الحاق الضرر بالمستخدمين و المستفيدين، أو للحصول على معلومات حكومية سرية.

2- جريمة الاعتراض غير المشروع: متعمد بدون وجه حق لخط سير البيانات باي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

3- الاعتداء على سلامة البيانات: تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا و بدون وجه حق، وما لحقه من ضرر جسيم.

4- جريمة اساءة استخدام وسائل تقنية المعلومات: 1-انتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير: أ/اية أدوات او برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة الى المادة الثامنة، ب/كلمة سر نظام معلومات او شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة الى المادة الثامنة. 2-حيازة أية أدوات أو برامج مذكورة في الفقرتين اعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة الى المادة الثامنة.

5- جريمة التزوير: استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه احداث ضرر، و بنية استعمالها كبيانات صحيحة.

6- جريمة الاحتيال: التسبيب بالحاق الضرر بالمستفيدين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق: 1- ادخال أو تعديل او محو أو حجب للمعلومات والبيانات. 2-التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات او محاولة تعطيلها أو تغييرها. 3-تعطيل الأجهزة والبرامج والمواقع الالكترونية.

7- جريمة الاباحية: 1-انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد اباحية أو مخلة بالحياء بواسطة تقنية المعلومات.

2-تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال و القصر.

3-يشمل التشديد الوارد في الفقرة 2 من هذه المادة، حيازة اباحية الاطفال و القصر أو مواد مخلة بالحياء للأطفال و القصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

8- الجرائم الاخرى المرتبطة بالإباحية: المغامرة و الاستغلال الجنسي.

9- جريمة الاعتداء على حرمة الحياة الخاصة.

10- الجرائم المتعلقة بالإرهاب: و المرتكبة بواسطة تقنية المعلومات (نشر افكار... تمويل تسهيل...)

11- الجرائم المتعلقة بالجرائم المنظمة: والمرتكبة بواسطة تقنية المعلومات (سيل الاموال...، الترويج للمخدرات...الاتجار بالأشخاص، الاسلحة والاعضاء البشرية...)

12- الجرائم المتعلقة بانتهاك حقوق المؤلف والحقوق المجاورة.

13- الاستخدام غير المشروع لأدوات الدفع الالكترونية: وعليه تعتبر هذه الجرائم من الجرائم المعلوماتية التي يطبق عليها الأحكام الموضوعية والإجرائية للاتفاقية، إذا ارتبطت بواسطة تقنية المعلومات، وعرفت المادة 1/2 من الاتفاقية تقنية المعلومات:" أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة".[1]

و نظرا لخصوصية الجريمة الالكترونية التي ترتكب بواسطة تقنية المعلومات، فعلى العاملين في القضاء جمع الادلة عن هذه الجرائم بشكل الكتروني، و بالتالي الاتفاقية العربية

[1] - مرسوم رئاسي رقم 14/ 252 المؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

لمكافحة جرائم تقنية المعلومات أكدت على التزام كل دولة طرف فيها بإنشاء جهاز متخصص و متفرغ على مدار الساعة لضمان وتوفير المساعدة الفورية لغايات التحقيق أو الاجراءات المتعلقة بجرائم المعلومات أو لجمع الادلة بشكلها الالكتروني في جريمة معينة، كما نلاحظ أن هذه الاتفاقية لم تعين أي جهة تتولى الضبط القضائي في الجرائم المعلوماتية، مما يعني ترك المجال مفتوح للدول العربية من خلال إعطاء تلك السلطة لأي هيئة أو جهة تراها قادة على اكتشاف و متابعة تلك الجرائم.[1]

كما تعمل الدول الأعضاء بتبني الاجراءات الجزائية الضرورية المتعلقة بالبيانات الساكنة و المتمثلة في تمكين السلطات المختصة من اصدار الأمر، أو الحصول على الحفظ العاجل للمعلومات المخزنة، بما في ذلك تتبع المستخدمين و التي خزنت على تقنية المعلومات،[2] و خصوصا إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل، و عرفت ب:" ينطبق هذا الإجراء على البيانات المخزنة التي سبق تجميعها و الاحتفاظ بها عن طريق حائزي البيانات مثال ذلك مقدمي الخدمات، بيد أنها لا تنطبق على التجميع في الوقت الفعلي، و التحفظ المستقبلي على البيانات المتعلقة بالمرور أو الولوج في الوقت الفعلي إلى محتوى الاتصالات، إذ أن هذه المسائل تمت معالجتها، و نصت الاتفاقية

[1] – لموسخ محمد، **تنازع الاختصاص في الجرائم الإلكترونية**، مجلة دفاتر السياسة والقانون، المجلد 2، العدد 2، 2009، ص 153.

[2] – المادة 23 من الاتفاقية نصت على أنه:" 1 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد أن تلك البيانات عرضة للفقدان أو التعديل.

2– تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد. من أجل تمكين السلطات المختصة من البحث والتقصي.

2– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية المعلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي."

عن التحفظ العاجل و الكشف الجزئي لمعلومات تتبع المستخدمين،[1] كما تبنت اجراءات لتمكين السلطات المختصة من اصدار أوامر تسليم المعلومات المحازة أو المخزنة و لتقديم مزود الخدمة للخدمات،[2] و يقصد بهذا الإجراء مطالبة كل دولة سلطاتها المختصة بأن تلزم شخصا ما داخل أراضيها بتقديم بيانات معلوماتية معينة مخزنة، أو أن تلزم مقدم خدمات على أرض طرف بأن يرسل بيانات المشترك،[3] أما بالنسبة للبيانات المتحركة، فقد نصت المادتين 28 و 29 على الجمع الفوري للمعلومات والمتعلقة بالبيانات المتعلقة بالمرور والبيانات المتعلقة بالمحتوى،[4] و اعتراض معلومات المحتوى.

---

[1] – المادة 24 من الاتفاقية نصت على:" "تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يخص معلومات تتبع المستخدمين من أجل: 1 – ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات.

2– ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات."

[2] – المادة 25 من الاتفاقية نصت على: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: 1 –أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.

2– أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته."

[3] – وردة شرف الدين، **الأحكام الإجرائية لمكافحة جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات(دراسة ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010)**، مجلة الاجتهاد القضائي، العدد16، مارس 2018، ص 104.

[4] – المادة 28 من الاتفاقية:" 1 –تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من:

أ) جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف،

ب) إلزام مزود الخدمة ضمن اختصاصه الفني بأن: يجمع أو يسجل بواسطة الوسائل الفنية على إقليم الدولة الطرف، أو يتعاون أو يساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2– إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة(1–أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم."

– المادة 29 من الاتفاقية نصت:" 1 – تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يخص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من :

و أوجبت الاتفاقية كذلك إجراءات إجبارية بالنسبة الطرف الثالث مثل تفتيش الحاسوب من خلال اتباع اجراءات البحث عن الأدلة المادية و الرقمية الناتجة عن ارتكاب الجريمة الالكترونية،[1] و قد عرفت الفقه العربي التفتيش هو:" البحث في مستودع سر المتهم عن أشياء تفيد في كشف الحقيقة و نسبتها إليه، أو هو الاطلاع على محل منحه القانون حماية خاصة، باعتباره مستودع سر صاحبه، و يستوي في ذلك أن يكون المحل مسكنا أو ما هو في حكمه أو أن يكون شخصا"،[2] كما عرف المجلس الأوروبي هذا النوع من التفتيش بأنه:"

أ)الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف، أو

ب) التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2 –إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1– أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3–تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أية معلومات عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة."

[1] – المادة 1/26 من اتفاقية نصت حيث:"1– تلتزم كل دولة بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى: أ)تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.

ب)بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه."

وبخصوص التفتيش في حالة اتصال حاسبة المتهم بحاسبة أخرى أو نهاية طرفية موجودة في مكان آخر داخل الوطن نصت المادة 2/26:" – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1–أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى."

أما في حالة التفتيش في حالة اتصال حاسبة المتهم بحاسبة أخرى أو نهاية طرفية موجودة في مكان آخر خارج الوطن جاء في المادة 39 :"1– يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها بحسب المادة السابعة والثلاثين.

2–تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقا للأحكام الواردة في هذه الاتفاقية.

3–تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضه للفقدان أو التعديل".

[2] – محمد طارق عبد الرؤوف الحن، **جريمة الاحتيال عبر الإنترنت**، منشورات الحلبي الحقوقية، لبنان،2011، ص 274.

إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني"، و هكذا فإن التفتيش التحقيقي وسيلة للحصول على الدليل و ليس دليلا في حد ذاته.[1]

إن هذه الجرائم تعتمد على نظم المعلومات وقد تتجاوز إلى أنظمة أخرى غير نظام المشتبه به، وهذا الإجراء يعتمد على تمديد نطاق التفتيش على نظام غير نظام محل المشتبه به.[2]

أما ضبط البيانات فهو الوسيلة القانونية التي تضع بواسطتها السلطة المختصة يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو استعملت لاقترافها، كالأسلحة و الأشياء المسروقة، و الثياب الملوثة بالدم، و الأوراق...و غير ذلك،[3] فإنه من المهم أن تفرض هذه الدول من خلال قانونها الداخلي وسائل أخرى للتنقيب و التحري بطريقة أقل تطفلا أو تدخلا للحصول على معلومات ضرورية بالنسبة للتحقيقات أو التنقيبات الجنائية، كما لا تتوقف إجراءات الضبط على جهاز الكمبيوتر، بل تمتد من ضبط المكونات المادية

---

[1] – وردة شرف الدين، المرجع السابق، ص 108.

[2] – عبد الفتاح حجازي، **مكافحة جرائم الكمبيوتر والانترنت**، ط1، دار الفكر الجامعي، الاسكندرية، 2006، ص 14.

[3] – محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 290.

– المادة 27 من الاتفاقية نصت على:" 1– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة 1 من المادة السادسة والعشرين من هذه الاتفاقية.

هذه الإجراءات تشمل صلاحيات:

أ – ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.

ب – عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها.

ج – الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.

د – إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

3– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين ((1، 2) من المادة السادسة والعشرون من هذه الاتفاقية".

إلى مختلف أجزاء النظام محل الاشتباه، و كل الأشياء ذات الطبيعة المعنوية لأنها معرضة بسهولة للتلف والضياع.[1]

إن الجمع الفوري لمعلومات تتبع المستخدمين، اعتراض معلومات المحتوى، و اعتماد السرية في تنفيذ الاجراءات، ضمان الحفظ العاجل للمعلومات و تتبع مزودي الخدمة، و الكشف العاجل للسلطات المختصة لمقدار كاف من المعلومات للتبع المستخدمين لتحديد مزود الخدمة ومسار بث الاتصالات، التزام كل دولة طرف تبني اجراءات ضرورية لتمكين سلطاتها المختصة من التفتيش، و اجراءات الضبط و تأمين المعلومات و الحفاظ على سلامتها و أخذ نسخة منها و ازالة المنع للوصول إليها مع تبني اجراءات تسمح بتسخير الخبراء في المعلوماتية.

و أخيرا يمكن القول أن الجريمة الالكترونية لم تنتشر في الدولة العربية، إلا أن استعمال الانترنيت بشكل كبير سيؤدي حتما إلى ارتكاب الجرائم، و هذا يشكل خطرا كبيرا على البرامج و المعلومات، هذا ما جعل الدول العربية تسعي إلى إبرام اتفاقيات دولية لمكافحتها قبل أن تستفحل في المجتمع العربي.

[1] – عبد الله عبد الكريم، المرجع السابق، ص 47.

خاتمة

خاتمة:

من خلال ما سبق توصلنا إلى النتائج التالية:

– أدى سوء استخدام الفضاء الافتراضي إلى بروز نوع جديد من الجرائم المستحدثة، لم يكن للإنسان سابق عهد بها أصطلح على تسميتها: "الجرائم الإلكترونية" أو "الجرائم المعلوماتية" تتميز بخصائص فريدة من نوعها وذات طبيعة خاصة، تختلف في مفهومها وأركانها ووسائل ارتكابها ونوعية الجناة والمجنى عليهم فيها عن الجرائم التقليدية المعروفة، مما خلق صعوبات بالغة لأجهزة البحث والتحري لملاحقة المجرم الإلكتروني وتوقيع العقاب عليه.

– تبنت مجموعة من المنظمات الدولية موضوع مكافحة الجرائم الإلكترونية، ووضعت على عاتقها مسؤولية إنشاء المعاهدات والاتفاقيات وتنفيذها بين الدول من أجل حماية شبكة الانترنيت من الاختراق.

– تعد الاتفاقيات والمعاهدات الاقليمية من أهم صور التعاون الدولي بصفة عامة وفي مجال مكافحة الجرائم الالكترونية بصفة خاصة، ومن بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية معاهدة بودابست لمكافحة جرائم الإنترنت، وتوصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، والقانون العربي النموذجي.

– الجريمة الالكترونية لم تنتشر في الدولة العربية، إلا أن استعمال الانترنيت بشكل كبير سيؤدي حتما إلى ارتكاب الجرائم، وهذا يشكل خطرا كبيرا على البرامج والمعلومات، هذا ما جعل الدول العربية تسعي إلى إبرام اتفاقيات دولية لمكافحتها قبل أن تستفحل في المجتمع العربي

وبناء على ما توصلنا إليه من نتائج حول هذه الدراسة يمكن تقديم جملة من **المقترحات** نذكر منها:

–تجسدت مكافحة الجرائم الالكترونية من خلال نصوص المعاهدات والاتفاقيات الإقليمية والدولية وهذا تفاديا لإفلات الجاني منها، غير أن تطور وسرعة انتشار هذه الجريمة جعل

هذه النصوص غير مواكبة لها وبالتالي أصبحت غير مجدية، الأمر الذي يدعو الدول المتقدمة لإيجاد صيغ قانونية يمكن من خلالها الحد من هذه الجريمة المستحدثة.

– يتضح من بنود الاتفاقيات الاقليمية والدولية أنها وضعت حد أدني من الحماية القانونية في كل مجالات مكافحة الجرائم الإلكترونية، في حين نجد الدول الأعضاء فيها تضع حماية تفوق الحماية التي وضعتها الاتفاقيات ولا يمكن أن تكون أدنى منها، وعليه يجب أن تتفق بنصوص الاتفاقيات مع التشريعات الداخلية للدول الأعضاء، وكان من مصلحة الدول الصناعية المتقدمة وعلى رأسها الولايات المتحدة الأمريكية من الانضمام للاتفاقيات الدولية، لأنها هي الاولي المعرضة للجرائم الالكترونية.

قائمة المصادر

والمراجع

قائمة المصادر والمراجع:

أولا/المصادر

1/ الاتفاقيات

- اتفاقية برن الدولية في 9 سبتمبر 1886، و المكملة بباريس في ماي 1896، و المعدلة في برلين في 13 سبتمبر 1908، و المكملة ببرن في 20 مارس 1914، و المعدلة بروما في جوان 1928، و بروكسل سنة 1948، و استوكهولم في جويلية 1967، و باريس في جويلية 1971، و سميت باتفاقية برن لحماية المصنفات الأدبية و الفنية.

- اتفاقية الويبو تم التوقيع عليها في استكهولم في 14 يوليو 1967 تحت عنوان اتفاقية "إنشاء المنظمة العالمية للملكية الفكرية", ودخلت هذه الاتفاقية حيز التنفيذ سنة 1970 ، وتعتبر هذه المنظمة إحدى الوكالات المتخصصة للأمم المتحدة ابتداء من ديسمبر 1974.

- اتفاقية تريبس التي تم التوقيع عليها من طرف الدول الأعضاء بها سنة 1994،

- معاهدة بودابيست في 23 نوفمبر 2001 و المتعلق بالإجرام الكوني من طرف مجلس أوروبا.

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010.

ثانيا/ المراجع

1/الكتب:

1- الطيب زروتي، **القانون الدولي الخاص الجزائري مقارنا بالقوانين العربية**، مطبعة الكاهنة، الجزائر، 2000.

2- أحمد عبد العليم شاكر علي، **المعاهدات الدولية أمام القضاء الجنائي**، دار الكتب القانونية، مصر، 2006.

3- أمير فرج يوسف، **الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت**، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2011،

4- بن مكي نجاة، **السياسية الجنائية لمكافحة الجرائم المعلوماتية**، دار الخلدونية، الجزائر، 2017.

5- جميل عبد الباقي الصغير: **الجوانب الإجرائية في تسليم المجرمين**، دار النهضة العربية، القاهرة، مصر، 1998.

6- حنان ريحان مبارك المضحكي، **الجرائم المعلوماتية(دراسة مقارنة)**، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014.

7- حسنين صالح عبيد، **القضاء الجنائي الدولي(تاريخه، تطبيقاته، مشروعاته)**، دار النهضة العربية، القاهرة، 1977.

8- طارق ابراهيم الدسوقي عطية، **الامن المعلوماتي(النظام القانوني لحماية المعلوماتي)**، دار الجامعة الجديدة، الإسكندرية، 2009.

9- محمد أمين الشوابكة ، **جرائم الحاسوب و الانترنت الجريمة المعلوماتية**، ط4، دار الثقافة للنشر و التوزيع ، 2011 .

10- محمد حماد مرهج الهيتي، **الجريمة المعلوماتية(دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني)**، دار الكتب القانونية، مصر، 2014.

11- محمد حسام، محمود لطفي، **الحماية القانونية لبرامج الحاسب الالكتروني**، ط1، دار الثقافة للطباعة والنشر، القاهرة، 1978.

12- محمد طارق عبد الرؤوف الحن، **جريمة الاحتيال عبر الإنترنت**، منشورات الحلبي الحقوقية، لبنان،2011.

13- محمد علي العريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة للنشر، القاهرة، مصر، 2011.

14- محمود أحمد عبابنة، **جرائم الحاسب وأبعادها الدولية**، ط1، دار الثقافة، عمان، الأردن، 2005، ص 162.

15- محمود محمد لطفي صالح، **المعلوماتية وانعكاساتها على الملكية الفكرية للمصنفات الرقمية(دراسة مقارنة)**، دار الكتب القانونية، مصر، 2014.

16- مدحت محمد عبدالعزيز إبراهيم ، **الجرائم المعلوماتية الواقعة على النظام المعلوماتي (دراسة مقارنة)**، ط1، دار النهضة العربية، مصر، 2015.

17- منير محمد الجمبيهي، ممدوح محمد الجنبيهي، **جرائم الانترنيت والحاسوب الآلي ووسائل مكافحتها** ، دار الفكر الجامعي، الإسكندرية، 2006.

18- نادية دردار، **الجهود الدولية لمكافحة الجريمة**، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2017.

19- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، ط1، دار الثقافة للنشر والتوزيع عمان، الأردن، 2008.

20- عبد الحكيم رشيد توبة، **جرائم تكنولوجيا المعلومات**، ط1، دار المستقبل للنشر والتوزيع، الأردن، 2009.

21- عبد الله عبد الكريم عبد الله، **جرائم المعلوماتية والإنترنت(الجرائم الإلكترونية)-دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا**، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

22- عبد الفتاح بيومي حجازي، **التزوير في جرائم الكمبيوتر والإنترنت(دراسة مقارنة)**، ط1، منشأة المعارف، القاهرة، مصر، 2010.

23- عبد الفتاح حجازي، **مكافحة جرائم الكمبيوتر والانترنت**، ط1، دار الفكر الجامعي، الاسكندرية، 2006،

24- غانم مرضي الشمري، **الجرائم المعلوماتية(ماهيتها، خصائصها، كيفية التصدي لها قانونيا)**، ط1، دار الثقافة للنشر والتوزيع، الأردن 2016.

25- فهد عبد الله العبيد العازمي، **الإجراءات الجنائية المعلوماتية**، دار الجامعة الجديدة، مصر، 2016.

26- سليم عبد الله الجبوري، **الحماية القانونية لمعلومات شبكة الانترنت**، ط 1، منشورات الحلبي الحقوقية، لبنان، 2011.

27- هلالي عبد الله أحمد، **الجوانب الموضوعية والاجرامية لجرائم المعلوماتية على ضوء اتفاقية بودابيست الموقعة في 23 نوفمبر 2001**، ط1، دار النهضة العربية، القاهرة، 2003.

28- هشام محمد فريد رستم، **قانون العقوبات ومخاطر تقنية المعلومات**، مكتبة الآلات الحديثة ، مصر، 1994.

29- يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المركز القومي للإصدارات القانونية، القاهرة، 2011.

30- يزيد بوحليط، **الجرائم الإلكترونية والوقاية منها في القانون الجزائري**، دار الجامعية الجديدة، الإسكندرية، 2019.

2/الرسائل العلمية:

1- سالم محمد سليمان الأوجلي، **أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية**، رسالة دكتوراه، كلية الحقوق، عين شمس، 1997.

2- إيهاب محمد يوسف، **اتفاقيات تسليم المجرمين ودورها في تحقيق التعاون الدولي لمكافحة الإرهاب**، رسالة دكتوراه في علوم الشرطة، القاهرة، 2003.

3- محمد خليفة، **جريمة التواجد غير المشروع في الأنظمة المعلوماتية(دراسة مقارنة)**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة باجي مختار، عنابة، الجزائر، 2011.

4- ربيعي حسين ، **اليات البحث و التحقيق في الجرائم المعلوماتية** ، أطروحة مقدمة لنيل شهادة دكتوراه علوم ، كلية الحقوق و العلوم السياسية ، جامعة باتنة 1 ، 2015، 2016.

5- عباسي محمد الحبيب، **الجريمة المنظمة العابرة للحدود**، أطروحة لنيل شهادة الدكتوراه علوم، تخصص القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2016، 2017.

6- بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، أطروحة دكتوراه تخصص قانون عام، جامعة يوسف بن خدة، الجزائر1، 2017، 2018.

7- جبران خليل ناصر، **حماية الملكية الفكرية: حقوق المؤلف في ظل التشريعات الوطنية والاتفاقيات الدولية**، أطروحة دكتوراه علوم، تخصص علم المكتبات والعلوم الوثائقية، جامعة أحمد بن بلة، وهران 1، 2017، 2018.

8- صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، شهادة الماجستير في القانون ، تخصص القانون الدولي للأعمال ، جامعة مولد معمري، تيزي وزو، 2013.

9- أحمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيات الإعلام و الاتصال في ضوء قانون رقم 09/ 04**، رسالة مكملة لنيل شهادة الماجستير، جامعة قاصدي مرباح، ورقلة، 2023.

3/ المقالات العلمية:

1- أمجد حسان، **الفيروسات إرهابا تهدد أنظمة المعلومات**، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، الجزائر، العدد4، 2011.

2- حسن مظفر الرزو، **الأمن المعلوماتي (معالجة قانونية أولية)**، مجلة الأمن والقانون أكاديمية شرطة دبي، الإمارات العربية المتحدة، العدد 1، جانفي .2004

3- محمد لموسخ د، **تنازع الاختصاص في الجرائم الإلكترونية**، مجلة دفاتر السياسة والقانون، المجلد 2، العدد 2، 2009

4- نعيمة بن يحي ، **الإنابة القضائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم**، مجلة الدراسات الحقوقية، المجلد 4، العدد1، 2017.

5- ليندة شرا بشة، **السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية**، مجلة دراسات وأبحاث، الجلفة، العدد1، 2009.

6- عثمان بقنيش ، مصطفي هنشور وسيمة، **حماية الملكية الفكرية على الأنترنت في إطار المنظمة العالمية للملكية الفكرية**، مجلة البحوث في الحقوق والعلوم السياسية، العدد 02، 2015.

7- فايز الظفيري، **الأحكام العامة للجريمة الإلكترونية**، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر، العدد 2، 2002.

8- فايزة سقار ، **الحق الاستثماري على براءة الاختراع في اتفاقية تريبس بين مبدأ احتكار الاستغلال والقيود الواردة عليه**، مجلة دراسات وأبحاث، المجلة العربية في العلوم الإنسانية والاجتماعية ، مجلد 12، العدد 3، جويلية 2020

9- وردة شرف الدين، **الأحكام الإجرائية لمكافحة جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات(دراسة ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010)**، مجلة الاجتهاد القضائي، العدد16، مارس 2018.

الفهرس

ملخص:

بدأ الاهتمام بدراسة الجريمة الالكترونية إقليميا ودوليا في بداية الثمانينات، حيث تم اصدار قوانين حماية الحاسوب وجرمت كل اعتداء عليه ووضعت عقوبات صارمة على مرتكبيها، وأدى الانتشار الواسع للإنترنيت والكمبيوتر والتطور الهائل في عالم البرمجيات إلى إبرام اتفاقيات دولية منها اتفاقية برن واتفاقية الويبو و تريست و اتفاقيات إقليمية منها معاهدة بودابيست و القانون العربي النموذجي كلها لمكافحة الجرائم الإلكترونية.

résumé:

L'intérêt pour l'étude de ce cybercriminalité a commencé au niveau régional et international au début des années 1980, lorsque des lois sur la protection informatique ont été promulguées qui criminalisaient toute attaque contre ce crime et imposaient de strictes sanctions à ses auteurs. Le monde du logiciel a conduit à la conclusion d'accords internationaux, notamment la Convention de Berne, la Convention OMPI, les Conventions de Trieste, ainsi que des accords régionaux, dont le Traité de Budapest et la Loi type arabe pour lutter contre la cybercriminalité.

Summary:

Interest in studying this cybercrime began regionally and internationally at the beginning of the 1980s, when computer protection laws were issued that criminalized any attack on it and imposed strict penalties on its perpetrators. The widespread spread of the Internet and computers and the tremendous development in the world of software led to the conclusion of international agreements, including the Berne Convention, the WIPO Convention, the Trieste Conventions, and the Regional ones, including the Budapest Treaty and the Arab Model Law to combat cybercrime.