جامعة الشهيد العربي تبسي –تبسة –الجزائر

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر

تخصص: قانون جنائي وعلوم جنائية

بعنوان

التعاون الشرطي في مكافحة الجريمة الإلكترونية

من إعداد الطالبة: إشراف الدكتورة:

شرفي إيمان احمد بومعزة نبيلة

الاسم واللقب	الرتبة العلمية	الصفة في البحث
أ.د دلول الطاهر	أستاذ التعليم العالي	رئيسا
د. أحمد بومعزة نبيلة	أستاذ محاضر أ	مشرفا ومقررا
د. اموسى عائشة	أستاذ محاضر أ	ممتحنا

السنة الجامعية 2023-2024

الكلية لا تتحمل أي أراء حول هذه المذكرة

كلمة شكر

بداية الشكر لله عز وجل الذي وفقنا لإتمام هذا العمل المتواضع

كما أشكر الأستاذة المؤطرة " بومعزة نبيلة " والتي ساعدتني كثيرا في إعداد مذكرتي، جعلها الله في ميزان حسناته يوم لا ظل إلا ظله.

كما أتقدم بالشكر الجزيل إلى أعضاء لجنة المناقشة الذين تشرفت بقبولهم مناقشة هذه المذكرة.

والشكر موصول لجميع أساتذة كلية الحقوق والعلوم السياسية من درسني ومن لم يدرسني

وختاما أشكر كل من ساهم معي وساعدني في إنجاز هذا العمل من بعيد أو قريب ولو بالكلمة الطيبة والدعم المعنوي

شرفي إيمان

إهداء

الحمد لله حبا وشكرا وامتنان على البدء والنام

﴿ وآخر دعواهم أن الحمد لله رب العالمين ﴾

من قال أنا لها نالها وأنا لها وإن أبت رغما عنها أتيت بها

نلتها اليوم وعانقت فرحتي نجوم السماء وكسرت وجوها استهزئت بدروب العلم لم تكن الرحلة قصيرة

ولا ينبغي لها أن تكون لم يكن الحلم قريبا ولا الطريق محفوفا بالتسهيلات لكنني فعلتها .

أهدي ثمرة جهدي هذه:

إلى جدي الغالي ﴿ السعيد ﴾ وروحه الطاهرة

إلى من أحمل اسمه بكل فخر إلى مصدر قوة العائلة الوالد الكريم

إلى من كان دعاؤها سر نجاحي وحنانها بلسم جراحي إلى سندي وعوضي وداعمتي الأولى وسر قوتي

شكرا على كل شيء يا أعظم أم أمي الحبيبة أمدها الله بالصحة والعافية

إلى أرضي الصلبة وجداري المتين إلى من شد الله بهم عضدي

إلى من أزاحوا عن طريقي المتاعب ﴿ إخوتي وأخواتي ﴾

إلى الإضافات الجميلة إلى عائلتي زوجات إخوتي وأولادهم

إلى رفقاء الروح إلى من تتعالى معهم الضحكات من شاركوني هذا الطريق بحلوه ومره

وفي الختام أهدي نجاحي هذا إلى زملائي في فلسطين إلى من منعتهم الحرب أن يكونوا مكاني

شرفي إيمان

قائمة المختصرات

قائمة المختصرات

ق.إ.ج: قانون الإجراءات الجزائية

ق.ع.ج : قانون العقوبات الجزائري

ق.م: قانون المدني

ج.ر: الجريدة الرسمية

ط: طبعة

د.ط: دون طبعة

ص: صفحة

ص ص: صفحة من إلى

مقدمة

مقدمة

مقدمة:

نتيجة التطور التكنولوجي الرهيب في مجال المعلوماتية نشأت أنماط مستحدثة من الجرائم التي تسمى بالجريمة الإلكترونية أو الرقمية، والتي تعتبر من أكبر التحديات التي تواجه العدالة الجنائية بصفة عامة وأجهزة الشرطة بصفة خاصة نظرا للتطور المستمر والمتسارع لشبكة الإنترنت حيث أن هذه الأخيرة مكنت للعديد من المجرمين والجماعات الإجرامية من القيام بالعديد من الأفعال الغير مشروعة مستغلين التسهيلات التي تقدمها هذه الشبكة.

وإن ما يميز مرتكبي هذه الجرائم ذكائهم ونفوذهم وتحكمهم الكبير في هذه الشبكة وهذا ما أدى إلى صعوبة إثبات هذه الجريمة ويعيق تحديد هوياتهم والقبض عليهم، مما نتج عن هذا اجتماع عربي وإقليمي ودولي من خلال خلق واستحداث أجهزة وتكاثف جهود في مواجهتها في مجال التعاون الشرطي نظرا لدور الفعال الذي يلعبه هذا الأخير في ردع ومواجهة الجريمة الإلكترونية، كذلك إيجاد جملة من الكيانات التي تتعاون من خلالها أجهزة الشرطة في دول مختلفة منها ما هو ذات طابع عربي كالمكتب العربي للشرطة الجنائية، ومنها ما هو ذات طابع إقليمي كمنظمة الشرطة الإفريقية(الأفريبول) أو كمكتب الأوروبي للشرطة (اليوروبول)، ومنها ما هو ذات طابع دولي كالمنظمة الدولية للشرطة الجنائية.

تكمن **أهمية دراسة** التعاون الشرطي في مكافحة الجريمة الإلكترونية كالتالي:

من الناحية العلمية:

- بروز الجريمة الإلكترونية كنوع مستحدث من الجرائم لا بد من التطرق أليه.

أما من الناحية الأكاديمية:

- تكمن في معرفة مدى أهمية التعاون الشرطي ودوره الفعال لردع وتصدي للجريمة الإلكترونية، وكذا معرفة الكيانات التي تتعاون بها أجهزة الشرطة.
- إن انتشار هذا النوع من الجرائم في مختلف المجتمعات أصبح يهدد الأمن الإلكتروني.

بالنسبة **لأهداف الدراسة** تتجسد في:

- فهم طبيعة الجرائم الإلكترونية وأساليب ارتكابها.
- تعزيز التعاون الشرطي العربي والإقليمي والدولي، وتسليط الضوء أكثر على أهمية هذا التعاون، والدور الفعال الذي يلعبه.
- تطوير القدرات الشرطية حيث يمكن لدراسة هذا الموضوع توجيه الجهود نحو تحسين القدرات التقنية والتدريب الشرطي لمكافحة الجرائم الإلكترونية.

بالنسبة **لأسباب اختيار الموضوع:**

فلم تكن هناك دوافع شخصية لاختيار الموضوع كونه موضوع مد لنا من اللجنة العلمية، إلا أنه موضوع مميز ومستحدث.

أما عن **الدوافع الموضوعية** فتتمثل في:

- الانتشار الرهيب لمثل هذه الجرائم يؤدي إلى ضرورة معرفة الأسباب ومحاولة معرفة مدى نجاعة الأجهزة الشرطية تكون رادعا قويا يحول بين الأشخاص وتلك الأفعال.

وتبعا لهذا نطرح الإشكالية التالية:

كيف يساهم التعاون الشرطي في مكافحة الجريمة الإلكترونية؟

وللإجابة عن هذه الإشكالية تم اعتماد على المنهج الوصفي التحليلي، فالمنهج الوصفي استخدمناه لوصف هذه الجريمة والمفاهيم المتعلقة بالموضوع وإعطائها دلالات علمية، وكذلك من خلال وصف الكيانات التي تتعاون بها الشرطة لمكافحة الجريمة الإلكترونية، أما المنهج التحليلي اعتمدناه في تحليل البيانات والمعلومات المتاحة لفهم طبيعة الجرائم الإلكترونية وتحليل الاتجاهات وتطوير الاستراتيجيات فعالة لمكافحتها.

بالنسبة **للدراسات السابقة** في هذا الموضوع قليلة جدا، باستثناء بعض الجزئيات كالتركيز على الأحكام الموضوعية للجريمة الإلكترونية فقط، كما أن طبيعة الموضوع تجعله دائما مجالا للدراسة.

خلال إنجازي لهذه المذكرة تعرضت لمجموعة من الصعوبات، تمثلت في قلة المراجع المتخصصة في موضوع البحث، بالرغم من كثرة المراجع المتعلقة بالجريمة الإلكترونية، إلا أنها

اكتفت بدراسة المفاهيم والقوانين والاتفاقيات ولم تسلط الضوء على مجال التعاون الشرطي وأجهزته.

وللإحاطة بكل جوانب الموضوع وللإجابة عن الإشكالية المطروحة، ارتئينا أن نقسم الموضوع إلى فصلين، الفصل الأول منه بعنوان: **الأحكام الموضوعية للجريمة الإلكترونية،** الذي اندرج ضمنه مبحثين، المبحث الأول كان بعنوان ماهية الجريمة الإلكترونية، والمبحث الثاني تضمن أركان الجريمة الإلكترونية، أما الفصل الثانين فكان معنونا ب:**التعاون الشرطي لمكافحة الجريمة الإلكترونية،** قسمنا هذا الأخير إلى مبحثين، المبحث الأول معنون ب: التعاون الشرطي العربي والإقليمي، والمبحث الثاني معنون ب: دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة الإلكترونية.

الفصل الأول

الأحكام الموضوعية للجرائم الإلكترونية

الفصل الأول: الأحكام الموضوعية للجريمة الإلكترونية

أصبح تحدي مكافحة الجريمة الإلكترونية في عصرنا الحالي أكثر أهمية مع تزايد التكنولوجيا وتطورها، وبالأمر الذي جعل لا تكون الحماية القانونية محصورة في مجالات معينة، ونظرا لطبيعتها العابرة للحدود كان لزاما تطوير القانون الجنائي والعلوم الجنائية لمواجهة هذه التحديات.

يتفاوت تعريف الجريمة الإلكترونية وفقا لتخصص كل باحث، يمكن للمختصين في الأمن السيبراني التركيز على الجوانب التقنية والأمنية، بينما يمكن للمختصين في القانون التركيز على الجوانب القانونية والتشريعية.

من الواضح أن الجريمة الإلكترونية هي جريمة حديثة، حيث أن العالم الرقمي لم يكن موضوعًا رئيسيًا للتشريعات الجنائية في الماضي، ومن هنا، ينبغي على النظام القانوني تطوير آليات قانونية فعالة لمواجهة هذا التحدي، بما في ذلك تعريف دقيق لجريمة الاعتداء الإلكتروني وتحديد المسؤوليات.

بالإضافة إلى ذلك، يجب أن نسلط الضوء على الجوانب المختلفة للجريمة الإلكترونية، سواء كانت ذلك الجوانب الدافعة للارتكابها الشخصية منها أو الموضوعية، وباختصار تواجه مكافحة الجريمة الإلكترونية تحديات متنوعة تتطلب استجابة شاملة من النظام القانوني والعلوم الجنائية لضمان تحقيق العدالة والأمن في البيئة الرقمية.

وعلى ما سبق ذكره نقسم هذا الفصل إلى مبحثين، تناول المبحث الأول ماهية الجريمة الإلكترونية واختص المبحث الثاني بالحديث عن أركان الجريمة الإلكترونية.

المبحث الأول: ماهية الجريمة الإلكترونية

الجريمة المعلوماتية نوع جديد ينشأ نتيجة التطور التكنولوجي السريع في عصرنا الحالي، ترتبط هذه الجرائم بشكل أساسي بالتقنيات الحديثة، مثل أجهزة الكمبيوتر، وشبكات الإنترنت، والمواقع الإلكترونية. تعد شبكة الإنترنت واحدة من أهم البيئات التي تسهل وتشجع ارتكاب الجرائم المعلوماتية، حيث تمثل وسيلة للاتصال وتبادل المعلومات بين أجهزة الكمبيوتر.

تتباين التشريعات في تعريف الجرائم المعلوماتية؛ فبعضها يعرفها بشكل غير مباشر، بينما لم تتعرض بعض التشريعات لتعريف واضح للجرائم المعلوماتية. ومن مهام المشرع تجريم الأفعال التي تشكل الجرائم المعلوماتية وتحديد العقوبات المناسبة لها.

سوف نستعرض في هذا المبحث مفهوم الجرائم الإلكترونية في المطلب الأول من خلال التطرق أولا إلى تعريف الجريمة الإلكترونية من الناحية الفقهية والقانونية في الفرع الأول مرورا بالتطرق للطبيعة القانونية للجريمة الإلكترونية.

ثم نستعرض في الفرع الثاني خصائص الجريمة الإلكترونية وصولا في الأخير إلى أنواع الجرائم الإلكترونية ودوافع ارتكابها في المطلب الثاني.

المطلب الأول: تعريف الجريمة الإلكترونية وخصائصها

تعتبر الجريمة المعلوماتية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية "بإساءة استخدام الكمبيوتر"، ثم "احتيال الكمبيوتر"، "فالجريمة المعلوماتية، بعدها "جرائم" الكمبيوتر"، و"الجريمة المرتبطة بالكمبيوتر"، ثم "جرائم التقنية العالية"، إلى "جرائم" الهاكرز، فجرائم" الانترنت"، وأخيرا "السيبر كرايم[1].

وقد حاولت العديد من الأعمال الأكاديمية "تعريف" الجريمة الإلكترونية"، ومع ذلك فلا تبدو التشريعات الوطنية مهتمة بتعريف دقيق للمصطلح، فمن أصل حوالي 200 مكون منبثقة من التشريعات الوطنية التي استشهدت بها البلدان في الرد على الاستبيان الدولي في تحديد معنى الجريمة الإلكترونية، استخدم أقل من خمسة في المائة كلمة "الجرائم الإلكترونية" في العنوان أو في السياق التشريعي وبدلا من ذلك فالاستخدام الأكثر شيوعا في التشريعات هو مصطلح "جرائم الكمبيوتر"، و" الاتصالات الإلكترونية"، و"تكنولوجيا المعلومات"، أو "الجريمة ذات التقنية العالية" وفي الممارسة العملية فإن العديد من هذه المفردات من التشريعات التي تم إنشاؤها للجرائم الجنائية والتي هي المدرجة في مفهوم الجريمة الإلكترونية، مثل الدخول غير المصرح به لنظام الكمبيوتر أو التدخل في نظام الكمبيوتر أو البيانات، حيث لم تستخدم التشريعات الوطنية على وجه التحديد مصطلح "الجريمة الإلكترونية في عنوان فعل أو قانون مثل: " قانون الجرائم الإلكترونية[2]".

[1] – ياسمينة بونعارة، «الجريمة الإلكترونية»، مجلة المعيار، المجلد20، العدد39، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، الجزائر، 2015، ص276.

[2] – المرجع نفسه، ص276

الفرع الأول: التعريف الفقهي والقانوني للجريمة الإلكترونية

إزاء المساعي الموجهة نحو التصدي لظاهرة الإجرام المعلوماتي، فإن المصطلحات التي تناولت هذه الظاهرة قد اختلفت فيما بينها، حيث لم يتفق الفقه الجنائي على تسمية موحدة للجريمة المعلوماتية، فالبعض أطلق عليها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات والبعض يسميها جرائم الكمبيوتر والأنترنت، وهناك من يطلق عليها الجرائم المستحدثة؛ إضافة إلى عدم الاتفاق على تعريف تشريعي شامل لهذا النوع من الجرائم[1].

البند الأول: التعريف الفقهي للجريمة الإلكترونية

وقد ذهب الفقهاء في تعريف الجريمة الإلكترونية مذاهبا مختلفة، ونتيجة للتطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، فإن ذلك حال دون وضع تعريف فقهي جامع وشامل، إذ تباينت في هذا السياق الاتجاهات الفقهية بين موسع لمفهوم الجريمة الإلكترونية، وبين مضيق لمفهومه، وسنحاول إبراز هذين الاتجاهين.

أولا: الاتجاه الضيق لمفهوم الجريمة الإلكترونية

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وفقا لمعايير متعددة، سواء كانت وفقا لمعيار شخصي من حيث توفر المعرفة والدراية بالتقنية، أو وفقا لمعيار موضوع الجريمة والمعايير المتعلقة بالبيئة المرتكب فيها الجريمة، وسنسرد في هذا الإطار بعض التعريفات الفقهاء القانون الجنائي، فقد عرفتها الدكتور هدى قشقوش بأنها:" كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الألية للبيانات أو نقل البيانات"؛ وعرفها الأستاذ Rosen Blat بأنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحوّل عن طريقه[2] .

[1] – مقلاتي مونة، راضية مشري، «الجريمة الإلكترونية، دلالة المفهوم وفعالية المعالجة القانونية»، مجلة أبحاث قانونية وسياسية، المجلد 06، العدد 01، كلية الحقوق والعلوم السياسية، جامعة جيجل، الجزائر، 2021، ص 493.

[2] – المرجع نفسه، ص 493.

يعاب على هذا التعريف أنه يخرج من نطاق الجريمة الإلكترونية، عدد كبير من الأفعال غير المشروعة، والتي يستخدم فيها الحاسب الآلي، كأداة لارتكابها كالاحتيال المعلوماتي، وقد أخذت وزارة العدل الأمريكية بتعريف للجريمة الالكترونية في تقرير صادر عنها عام 1989 المتعلق بجرائم المعلوماتية بكونها: كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الألية بقدر كبير لازم لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى، يتبين لنا من خلال هذا التعريف أنه لا يكف فقط أن تتوافر معرفة تكنولوجيا الحاسبات الألية، بدرجة كبيرة من أجل ارتكاب الجريمة الإلكترونية، ولكن أيضا من أجل ملاحقتها ومتابعتها والتحقيق فيها، بمعنى لابد من توافر قدر كبير من العلم بهذه التكنولوجيا، لدى الجناة والقائمين على معاينة وملاحقة مرتكبيها[1].

ثانيا: الاتجاه الموسع لمفهوم الجريمة الإلكترونية

على عكس الاتجاه السابق يرى فريق أخر من الفقهاء، ضرورة التوسع في مفهوم الجريمة الإلكترونية أو المعلوماتية، وعدم حصرها في الحاسوب وحده، أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية؛ فيعرفونها بأنها كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل"؛ كما عرفتها منظمة التعاون الاقتصادي والتنمية بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ، أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، فقد تبنى التعريف التالي للجريمة الإلكترونية : " هي أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[2].

[1] – مقلاتي مونة، راضية مشري، المرجع السابق، ص 494.

[2] –مرجع نفسه، ص494.

نحن من جانبنا نتفق مع هذا التعريف، إذ أنه التعريف الذي استطاع الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة الإلكترونية سواء التي قد تقع بواسطة النظام المعلوماتي، أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما يشمل التعريف الجرائم التي من الممكن أن تقع في بيئة إلكترونية، فهذا التعريف لم يركز على فاعل الجريمة ومقدراته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة الإلكترونية، بل إنه حاول عدم حصر الجريمة الإلكترونية في نطاق ضيق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب[1].

البند الثاني: المفهوم القانوني للجريمة المعلوماتية

نظراً لما تتسم به الجرائم المعلوماتية من سهولة وخطورة، اهتمت بعض التشريعات بتعريفها في المواد الأولى من النظام الذي يعالج هذا النوع من الجرائم، ففي المملكة العربية السعودية تم سن تشريع خاص بمكافحة الجرائم المعلوماتية أطلق عليه ما يسمى بـ" نظام مكافحة جرائم المعلوماتية " الصادر وفقا لقرار مجلس الوزراء رقم (79) وتاريخ 1428/03/07هـ والذي عرف الجريمة المعلوماتية في المادة الأولى (8) بأنها: أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام، أما المشرع القطري فقد عرفها بأنها : " أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي، أو الشبكة المعلوماتية، بطريقة غير مشروعة بما يخالف أحكام القانون ، ويتشابه هذا التعريف مع ما ورد بالمادة الأولى من قانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي الذي عرفها كما يلي: " في تطبيق أحكام هذا القانون يقصد بالمصطلحات التالية المعنى الموضح قرين لكل منها : الجريمة المعلوماتية: كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة الحكام هذا القانون"[2]، وفي المقابل خلت

[1] – مقلاتي مونة، راضية مشري، المرجع سابق، ص 495.

[2] – حمزة بن فهم السليمي، الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي، مجلة الجامعة العربية، العدد59، جامعة العراق، العراق، 2023، ص580

التشريعات الجنائية لبعض الدول من كل تعريف للجريمة المعلوماتية، ومنها قانون الجرائم المعلوماتية السوداني لسنة 2007، وقانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012 ، وقانون جرائم تقنية المعلومات البحريني رقم 60 لسنة 2014، وأيضا قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015 ، ويتضح بذلك أن المشرعين السعودي والكويتي متقدمين على العديد من الأنظمة الأخرى حيث عرفا الجريمة المعلوماتية، وهي مسألة. مهمة جدا نظراً وأن الجريمة المعلوماتية تقتضي تحديد مفهومها وتعريفها صلب النصوص القانونية[1].

وعرف المشرع الجزائري الجريمة الإلكترونية في المادة الثانية من القانون 09-04 والتي سماها" الجرائم المتصلة بتكنولوجيا الإعلام والاتصال" بأنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[2]".

الملاحظ من خلال قراءة المادة سالفة الذكر هو أن المشرع الجزائري اعتمد في تعريف الجريمة الإلكترونية على معيارين هما: معيار موضوع الجريمة، ومعيار وسيلة ارتكاب الجريمة والتي نستعرضها فيما يلي:

أولا: التعريف على أساس موضوع الجريمة

اعتمد المشرع الجزائري موضوع أو محل الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات كأساس لتحديد الجريمة المعلوماتية[3]، وهي المحددة في الفصل السابع مكرر من قانون العقوبات الجزائري تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات" والتي تحكمها المواد من 394 مكرر إلى 394 مكرر7 من هذا القانون.

---

[1] – حمزة بن فهم السليمي، المرجع السابق، ص580.

[2] –المادة 02 من قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5غشت سنة2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] –عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، ط01، النشر الجامعي الجديد، تلمسان، الجزائر، 2021، ص18.

ثانيا: التعريف على أساس معيار وسيلة ارتكاب الجريمة

بالإضافة إلى الاستناد في تحديد الجريمة المعلوماتية على موضوع الجريمة أضاف المشرع الجزائري معيارا آخر لتحديد الجريمة المعلوماتية وهو وسيلة ارتكاب الجريمة وهي المنظومة المعلوماتية أو نظام الاتصالات الالكترونية، بالقول:" .... وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية" فوسيلة ارتكاب الجريمة أو تسهيل ارتكابها في هذا التعريف هي محل اعتبار في تكييف الجريمة، وهنا يمكن القول إن الجريمة المعلوماتية حسب المشرع الجزائري تنقسم إلى طائفتين، تضم الطائفة الأولى الجرائم التي ترتكب ضد نظام المعالجة الآلية للمعطيات وتستهدف المساس الكلي أو الجزئي بهذه المنظومة وهي الجرائم المنصوص عليها في الفصل السابع مكرر من قانون العقوبات تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات[1]".

فيما تتضمن الطائفة الثانية كل الجرائم الأخرى المنصوص عليها في قانون العقوبات أو في القوانين الخاصة التي يتم ارتكابها أو يتم تسهيل ارتكابها باستخدام منظومة معلوماتية أو أي نظام للاتصالات، وعرفت الجريمة المعلوماتية في التشريع الأمريكي وزارة العدل في الولايات المتحدة الأمريكية الجريمة عبر الانترنت بأنها" أي جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابه"، أما مكتب تقييم التقنية في الولايات المتحدة الأمريكية فقد عرف الجريمة المعلوماتية بأنها:" الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا[2]".

[1] – عميمر عبد القادر، المرجع السابق، ص 19.

[2] –المرجع نفسه، ص22.

البند الثالث: الطبيعة القانونية للجريمة الإلكترونية

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى ارتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعهم إلى ربط حواسهم بالشبكة، على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة كما قد ترتكب هذه الجرائم في مجال معالجة النصوص، وصعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة، بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات ومتابعة مرتكبها وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة[1].

الفرع الثاني: خصائص الجريمة المعلوماتية

تتسم الجريمة الالكترونية بدرجة من الخطورة البالغة، والحجم الكبير للأضرار التي تنشأ عنها، وهي بذلك تشترك مع بعض الجرائم كالإرهاب والإتجار بالمخدرات، ومن هذه الخصائص يمكن تفصيل ما يلي:

البند الأول: خصائص الذاتية للجريمة الإلكترونية

أولا: خطورة الجريمة الإلكترونية

إن ما يتميز به عمل الكمبيوتر والوظائف التي يقوم بها من سرعة في العمل، وطاقة كبيرة الاستيعاب المعلومات، جعلت منه يشكل خطورة على حياة الأفراد وأسرار حياتهم الشخصية، وكذلك اقتصاديات المؤسسات، وأمن البلاد وسياستها واقتصادها، والخطر يتحقق إذا طال المعلومات[2] وهذا من خلال أسلوب تسجيلها، ففي فرنسا مثلا وفي عام 1986 ووفقا لإحصاء

[1] – بوضياف اسمهان، «الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر»، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف، مسيلة، الجزائر، 2018، ص353.

[2] – معاشي سميرة، «الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)»، مجلة المفكر، المجلد 13، العدد 17، كلية الحقوق والعلوم السياسية –بسكرة، الجزائر، 2018، ص 410.

الجمعية العمومية لشركات التأمين ضد الحرائق والمخاطر المختلفة فقد خسرت هاته الشركات حوالي 7.3 مليار فرنك فرنسي، و أكدت الإحصاءات ارتفاع حجم الخسائر الناشئة عن التحايل حيث قدرت في هذا المجال بما يقارب من المليار و سبعة من عشره ، كما تضاعفت الخسائر الناتجة عن سرقة المال المعلوماتي المعنوي ذو النمط الواحد في الفترة بين عامي 1984 و1985 لتصل إلى المليار و اثني عشرة من مئة وشكلت جريمة السرقة للمال المعلوماتي المعنوي، الذي يتعلق بالكيانات المنطقية ذو النمط الواحد كبرامج التصميم وإدارة البيانات والأمن وصيانتها نسبة قدرت بثلاث و أربعون بالمائة من الخسائر، أما في بريطانيا والتي يرى الدارسون أنها من المجتمعات التي تعتمد بشكل ملحوظ على أنظمة المعالجة الآلية للبيانات، فتختلف التقديرات من 500 مليون جنيه إلى 2 بليون جنيه في السنة، ووجدت دراسة تبنتها الحكومة في 1986 أن 40% من شركات المملكة قد عانت على الأقل مرة من نصب رئيسي في الحاسوب خلال السنوات العشرة الأخيرة[1].

وفي الولايات المتحدة الأمريكية أعلن معهد المعلومات تقرير نتائج عام 2001 وهو التقرير السادس حول جرائم الكمبيوتر ودراسة أمن المعلومات المسحية ، وهذه الدراسة يتم إجراؤها سنويا من قبل المعهد بالتعاون مع مكتب التحقيقات الفيدرالي الأمريكي، حيث أظهرت الدراسة تزايد خطر هذه الجرائم و ارتفاع حجم الخسائر الناجمة عنها ، فقد تبين أن 85 بالمائة من المشاركين في الدراسة و تحديدا المؤسسات الحكومية الكبرى كانت ضحية اختراقات للكمبيوتر خلال السنة السابقة و أن 64 بالمائة منهم لحقتهم خسائر مادية بلغت 378 مليون دولار بالمقارنة مع خسائر سنة 2000 التي قدرت بحدود 120 مليون دولار، وتشير الإحصاءات إلى أن جميع الأنشطة التي تستخدم الحاسب الآلي تكون عرضة لخطر الجريمة المعلوماتية، ويلاحظ أن الاتجاه الأساسي للجريمة المعلوماتية يستهدف البنوك في حدود 19 % ويستهدف خاصة المنشآت المالية التي تهيمن على الأقل على القيم الرأسمالية ثم تأتي بعد ذلك النقود وهناك السوق السوداء للمعلومات بجانب السوق الشرعي للمعلومات والتي يتم بمقتضاه مقايضة وبيع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين[2].

[1] – معاشي سميرة، نفس المرجع، ص 410.

[2] – مرجع نفسه، ص411.

كما أن هذا النوع من الجريمة يرتبط بالجزء الأعظم للأنشطة الاقتصادية والاجتماعية للمجتمع ويخص المعلومات التالية:

- ❖ المعلومات المالية
- ❖ المعلومات التجارية والصناعية
- ❖ المعلومات الشخصية
- ❖ المعلومات العسكرية

ثانيا: الجريمة الإلكترونية عابرة للحدود

:بسبب عصر العولمة و الانتشار الكبير لاستعمال الانترنت الذي ربط كافة دول العالم، انتشرت الجريمة المعلوماتية التي لا تعرف بحدود الدول و القارات اتسمت بطابع عالمي و ذلك من خلال النظام المعلوماتي و الرقمي للشبكة العنكبوتية و الذي يسهل ارتكاب مثل هذا النوع من الجرائم المستحدثة[1].

أي أنها جريمة غير مقيدة بحدود ولا مرتبطة بمنطقة جغرافية معينة، يمكن ارتكابها بدون أخذ بعين الاعتبار قرب أو بعد المسافات بين الفاعل والمفعول به أو المفعول فيه أو المفعول عليه، يمكن ارتكابها من دولة في دولة أخرى فقط باستعمال الحاسوب والشبكة.

إن كان ارتكاب الجرائم التقليدية يتطلب حضور المجرم وموضوع اجرامه في مسرح الجريمة، فإن مرتكب الجريمة المعلوماتية لا يشترط تواجده في مكان ارتكابها مع موضوع اجرامه عند قيام شخص ما بارتكاب جريمة سرقة تقليدية كسرقة أموال من بنك مثلا، كان الأمر يتطلب انتقاله إلى البنك للقيام بالركن المادي للجريمة، بينما اليوم، يمكن للسارق القيام بجريمته من بيته، حيث يكفيه استعمال الكمبيوتر والشبكة العنكبوتية وهو جالس في بيته (في استراليا مثلا) لسرقة أموال من بنك موجودة في بلد آخر (روسيا مثلا[2]).

[1] –لطروش فيروز، بن عزوز حاتم، «الجريمة الإلكترونية في الجزائر: من جريمة فردية إلى جريمة منظمة»، مجلة الآفاق للعلوم، المجلد 01، العدد01، جامعة الجلفة، الجزائر، 2016، ص 325.

[2] – عليوة سليم، «الجريمة المعلوماتية»، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 06، العدد01، كلية الحقوق والعلوم السياسية، مسيلة، الجزائر، 2021، ص 1215.

ثالثا: صعوبة إثبات الجريمة الالكترونية

فالجرائم المعلوماتية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، وهي خطيرة وصعبة الاكتشاف أو هي صعبة في تحديد مكان وقوعها ومكان التعامل معها بسبب اتساع نطاقها المكاني وضخامة البيانات، وترجع صعوبة إثبات الجريمة الالكترونية إلى عدة أمور أهمها:

- ❖ تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية غير المرئية وبدون مستندات ورقية ولا تترك آثار مادية.
- ❖ صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية.
- ❖ تحتاج الى خبرة فنية والذكاء في ارتكابها، ويصعب على المحقق التقليدي التعامل معها.
- ❖ تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها، وما يساعد من ازدياد عدم التعرف على مرتكبي الجرائم الالكترونية إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم معلوماتية تجنبا للإساءة لسمعتها وهز ثقة العملاء فيها، وكذلك إخفاء أسلوب ارتكاب الجريمة خوفا من قيام آخرين بتقليد هذا الأسلوب[1].

رابعا: صعوبة اكتشاف الجريمة الإلكترونية

يصعب اكتشاف الجريمة الإلكترونية فهي لا تترك أثرا لمتابعتها وملاحظتها بل وقد يستخدم الجاني برامج تقنية من خلالها تعرقل الوصول إليه أو معرفة التقنية للجريمة المرتكبة أيا كان نوعها كما أن المجني عليه لا يكتشفها مباشرة ولا يشعر بها أما لضعف قدرته الفنية على ذلك بالمقارنة بالمرتكب الجريمة أو للمهارات الفنان التي استخدمها الجاني عند ارتكابه للجريمة[2].

[1] –سي حميدي عبد المومن، قيرة سعاد، «الجريمة الإلكترونية وآليات التصدي لها في قانون الجزائري»، مجلة البيبان للدراسات القانونية والسياسية، المجلد 07، العدد01، كلية الحقوق والعلوم السياسية، جامعة برج بوعريريج، الجزائر، 2022، ص 62.

[2] – عفاف بعون، نسيمة أولاد سالم، «الجريمة الإلكترونية –قراءة سوسيوتاريخية في النشأة والآثار»، مجلة القبس للدراسات النفسية والاجتماعية، المجلد 05، العدد 20، جامعة المدية الجزائر، 2023، ص 89.

البند الثاني: خصائص وسيمات المجرم الإلكتروني

حتى تحقق العقوبة أهدافها، يجب أن نضع في الاعتبار شخصية المجرم، وذلك لإعادة تأهيله اجتماعيا حتى يعود مواطنا صالحا مرة أخرى ويندمج مع المجتمع، وينطبق هذا القول على المجرم المعلوماتي مثلما ينطبق على المجرم التقليدي. ويمكن القول بأن المجرم المعلوماتي يتمتع بقدر كبير من الذكاء يميزه عن غيره من المجرمين واتصافه بسمات معينة جعلت منه محلا للعديد من الأبحاث والدراسات[1].

أولا: المجرم المعلوماتي كانسان يتمتع بالمهارة والمعرفة والذكاء

تحفظ البعض من الفقه حيال رسم صورة عامة للمجرم المعلوماتي متسمة بصفة الذكاء، وذلك على سند من القول إن بعض أنماط الجريمة المعلوماتية مثل إتلاف الحاسوب الآلي أو تدميره كليا أو جزئيا، أو سرقة المعلومات المخزنة داخل الحاسب الآلي، لا تحتاج في مرتكبها أن يكون على قدر كبير من الذكاء، والواقع أنه لا يمكن وصف كل جريمة تتصل بالحاسب الآلي بأنها نمط من أنماط الجريمة المعلوماتية، حيث أن المقصود بالإجرام المعلوماتي بالمعنى الدقيق هو الإجرام الذي ينشا عن تقنيات التدمير الناعمة التي تتمثل في التلاعب بالمعلومات والكيانات المنطقية (البرامج) فلكي ينشأ هذا النوع من الإجرام فانه يلزم استخدام تقنية خاصة تتعامل مباشرة مع البرامج أو البيانات، وهو بذلك يتميز عن الإجرام العنيف الموجود ضد النظام المعلوماتي.

ولهذا يتميز المجرم المعلوماتي غالبا بالذكاء، حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة، خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة تلحق بالمجني عليه ، فالمجرم المعلوماتي يستخدم مقدرته العقلية ولا يلجا إلى استخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء، فالإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم المعلوماتي يسعى بشغف إلى معرفة طرق جديدة[2] مبتكرة

[1] – حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة ماجستير في العلوم القانونية، تخصص علم الاجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2011 –2012، ص29.

[2] – المرجع نفسه، ص 29.

لا يعرفها أحد سواه، وذلك من أجل اختراق الحواجز الأمنية في البيئة الالكترونية، ومن ثم تحقيق مراده.

ثانيا: المجرم الالكتروني يتمتع بالخبرة والمهارة

يتصف مرتكب الجرائم الالكترونية بأنه على قدر عالي من الخبرة والمهارة في استخدام التقنية المعلوماتية، ذلك لأن مستوى الخبرة والمهارة التي يكون عليها هي التي تحدد الأسلوب الذي يرتكب به تلك الجرائم ، فهو يتمتع بالمهارة و المعرفة الكافيتين لاختراق المواقع الالكترونية وكسر حواجز الشفرة ، بعكس المجرم العادي في الجرائم التقليدية و الذي غالبا ما يتميز بالقوة العضلية ونادرا ما يميز بعضهم بالذكاء، فالمجرم المعلوماتي يجب أن يكون على معرفة فنية علمية بجهاز الحاسوب والانترنت و كيفية التعامل مع البيانات و تخزينها و معالجتها وحذفها حتى يتمكن من إتمام الجريمة، وبناء على ذلك فانه لا يستطيع أي شخص أن يرتكب الجرائم المعلوماتية دون المعرفة التامة بكيفية التعامل مع جهاز الحاسوب و الانترنت والبيانات و المعلومات بشكل منهجي و دقيق[1].

ثالثا: خوف المجرم المعلوماتي من كشف جريمته

يعرف عن مجرمو المعلوماتية خوفهم من انكشاف جرائمهم وانفضاح أفعالهم، بالرغم من أن هذا الخوف يصاحب المجرمين على اختلاف أنماطهم، إلا أنها تميز المجرمون المعلوماتيون بصفة خاصة لما يترتب عن كشف أمرهم من فقدان لمراكزهم ،و يساعدهم على الحفاظ على سرية أفعالهم و طبيعة الأنظمة المعلوماتية نفسها، وذلك أن أكثر ما يعرض المجرم إلى اكتشاف أمره هو أن يستجد أو يطرأ أثناء تنفيذه لجريمته مجموعة من العوامل غير المتوقعة والتي لا يمكن التنبؤ بها ، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحواسيب إنما تؤدي عملها غالبا بطريقة آلية، بحيث لا تتغير المراحل المختلفة التي نمر بها، فخوف المجرم المعلوماتي من انكشاف فعله يعود إلى انتمائه في الغالب الأعم إلى وسط اجتماعي متميز سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل[2].

[1] – غريبي بشرى، «خصوصية المجرم المعلوماتي ودوافعه»، مجلة نوميروس الأكاديمية، المجلد 02، العدد 02، مركز الجامعي مغنية، تلمسان الجزائر، 2021، ص 105.

[2] – المرجع نفسه، ص105.

رابعا: المجرم الإلكتروني شخص سوي والاجتماعي

يتميز بأنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو بغاية إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيله بها، أو بدافع الحصول على الأموال، أو بهدف الانتقام[1].

خامسا: المجرم الالكتروني يتميز بقوة التحمل والصبر

يحتاج المجرم المعلوماتي إلى القدرة على التحمل والصبر، فقد يستغرق أمر اختراق إلكتروني، أو تحويل أموال ساعات طوال أو أياما لأجل تجسيده، ولذلك فإن قوة التحمل والمثابرة من السمات التي تساعد المجرم، المعلوماتي على نيل مبتغاه ورفع وتنمية قدراته ومهاراته فتكرار المحاولات يستغرق وقتا طويلا يحتم عليه التمتع بالصبر[2].

سادسا: المجرم المعلوماتي يتمتع بالسلطة

يقصد بالسلطة في هذا المجال، جملة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير منهم لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وتتمثل عادة في امتلاك شفرة الدخول إلى النظام المعلوماتي، وإجراء المعاملات، وقد تكون هذه السلطة أحيانا غير مشروعة في حال سرقة شفرة الدخول.

وقد يستغل المجرم المعلوماتي المزايا التي توفرها تكنولوجيا المعلومات وسلطته عليها فيدون بيانات وهمية، وغير صحيحيه ويطلب الحاسوب اعتمادها عند إجراء بعض العمليات ومثالها الموظف المشرف على الموظفين على مصالح المحاسبة وصرف الأجور الذي يمكن أن يدرج أسماء بعض الموظفين الوهميين ضمن قائمة الموظفين، ثم يمرر عملية صرف الرواتب[3]

---

[1] – رحموني محمد، «خصائص الجريمة الإلكترونية ومجالات استخدامها»، مجلة الحقيقة، المجلد 16، العدد41، جامعة ادرار، الجزائر، 2018، ص 444.

[2] – ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة للنيل شهادة الدكتوراه في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة01، 2015–2016، ص37.

[3] – المرجع نفسه، ص37.

ويتولى إيداع رواتب الموظفين الوهميين في حسابه الخاص، ولذلك فان المهتمين بمجال المعلوماتية عادة ما ينبهون أصحاب المؤسسات الى الأخذ الاحتياطات اللازمة عند اختيار المشرفين على ذلك[1].

المطلب الثاني: أنواع ودوافع الجريمة الإلكترونية

سنحاول من خلال هذا المطلب التطرق لكل من دوافع الجريمة الالكترونية الشخصية منها والموضوعية في الفرع الأول، ثم الى توضيح أنواعها من خلال الفرع الثاني.

الفرع الأول: دوافع الجريمة الإلكترونية

إن إقدام الشخص على ارتكاب الجريمة الإلكترونية لا يكون بدون سبب معين، بل إن هناك العديد من الدوافع والأسباب التي تتحكم فيه، وتدفعه لارتكاب هذا الفعل، وإن تنوعت الدوافع المؤدية للجريمة الإلكترونية بين دوافع شخصية والأخرى موضوعية ، فإن هذه الدوافع باطنها الأساسي هو نفسي محض على اعتبار أن قيام مرتكب الجريمة الإلكترونية تختلف دوافعه عن الجريمة التقليدية خاصة ما تعلق منها بحب البروز والظهور والشهر وغيرها من الدوافع النفسية الكثيرة التي نحاول الإلمام بها في هذا المقام سنقوم بالإشارة إليها من خلال الاتي ذكره[2].

البند الأول: الدوافع الشخصية

ويمكن رد الدوافع الشخصية لدى المجرم الالكتروني إلى دوافع مادية وأخرى ذهنية.

أولا: الدوافع الشخصية

الرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم، من أجل تحقيق المكاسب المالية هذه يتم اللجوء إلى ارتكاب الجريمة المعلوماتية، أما عن طريق المساومة على البرامج[3] أو

[1] – ربيعي حسين، المرجع السابق، ص37.

[2] – صابر بحري، منى خرموش، «أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية»، مجلة دراسات في سيكولوجية الانحراف، المجلد06، العدد 01، جامعة سطيف، الجزائر، 2021، ص 47.

[3] – نهلا عبد القادر المومني، الجرائم المعلوماتية، ط02، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 90.

المعلومات المتحصلة بطريق الاختلاس من جهاز الحاسوب أو عن طريق استعمال بطاقة سحب الي مزورة أو منتهية الصلاحية وغير ذلك الكثير، ولقد أشارت مجلة (Securite informatiqne) وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال و 23 من أجل سرقة معلومات و 19 افعال إتلاف و 15% سرقة وقت الآلة أي الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية[1]).

تجدر الإشارة إلى أنه في حال نجاح المجرم في ارتكاب جريمته المعلوماتية فإن ذلك قد يدر عليه أرباحا تكون هائلة في زمن قياسي، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة لاقترافه هذا النوع من الإجرام من خلال ما يرويه أحد هؤلاء المجرمين المحترفين في سجن كاليفورنيا بقوله: لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكاني أن أكرر ذلك في أي وقت لقد كان شيئا سهلاً فأنا أعرف أسلوب عمل جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني[2].

ثانيا: الدوافع الذهنية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبو جرائم نظم المعلومات إلى إظهار تفوقهم ومستوي ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبو هذه الجرائم لديهم شغف الآلة يحاولون إيجاد وغالباً ما يجدون الوسيلة إلى تحطيمها بل والتفوق عليها[3].

ويتزايد شيوع هذا الدافع لدي فئات صغار السن من مرتكبي جرائم الكمبيوتر الذين يمضون وقتاً طويلاً أما حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات[4]

---

[1] – نهلا عبد القادر المومني، المرجع السابق، ص 90.

[2] – المرجع نفسه، ص90.

[3] –-عبد العال الديربي، محمد صادق اسماعيل، الجرائم الإلكترونية –دراسة قانونية قضائية مقارنة، ط01، المركز القومي للإصدارات القانونية، 2012، ص 52.

[4] – المرجع نفسه، ص52.

المعلومات وإظهار تفوقهم على وســـائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مســـاءلة مرتكبي جرائم الحاســـب الآلي الذي يتمثل باعثهم في إظهار تفوقهم، واعتبار أعمالهم غير منطوية على نوايا آثمة، وقد أمكن الكشـــف في بعض الأحوال عن أن مجرد إظهار شعور جنون العظمة وهو الدافع لارتكاب فعل الجريمة المعلوماتية وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي وهو مفتاح ســـر كل نظام قد ينتابه إحســـاس بالإهمال وبالنقص داخل المنشأة التي يعمل بها[1].

فهؤلاء لا يقومون الأشخاص بارتكاب الجرائم المعلوماتية بغرض تحقيق مكاسب مالية وإنما يقومون بذلك إرضاء لغرورهم من أجل إثبات قدرتهم على تحقيق النتيجة بغض النظر عن الأضرار اللاحقة بالغير من جراء هذا التصرف، وهو نوع من التفاخر والتعالي الذي يدفع إليه في بعض الأحيان التحدي أو الرغبة في تحقيق المتعة، كما أن الشعور بالنقص يمكن أن يكون كذلك دافعا لارتكاب الجريمة المعلوماتية ليثبت هذا الشخص أن النقص النفسي أو الفسيولوجي الذي يعاني منه لا يعيقه عن التفوق في مجالات أخرى[2]

البند الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية

قد يكون باعث الجرمي للجريمة الالكترونية ليس له دخل في حب المال وكذا التفوق على أنظمة بل يكون بدافع الانتقام والتواطؤ.

أولا: دافع الانتقام

يعد دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب جريمة، لأن دافع الانتقام غالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها و غالبا ما يكون أحد موظفيها الذي يقوم بارتكاب الجريمة المعلوماتية بدافع الانتقام نتيجة إما لفصله من عمله أو تخطيه في الحوافز أو الترقية وابرز مثال على ذلك: حادثة شركة اوميغا[3]

[1] –عبد العال الدريبي، محمد صادق اسماعيل، المرجع السابق، ص ص52.

[2] –عميمر عبد القادر، المرجع السابق، ص 50.

[3] – غريبي بشرى، المرجع السابق، ص ص110

التي ترجع وقائعها في أن مصمم ومبرمج شبكات كمبيوتر و رئيس سابق لشركة OMEGA من مدينة Delaware ويدعى Timothy Allen Lioyd الذي تم اعتقاله في : 17 فيفري 1998 بسبب إطلاقه لقنبلة الكترونية في عام 1996 وذلك بعد 20 يوما من فصله من العمل، كما أنها استطاعت أن تلغي كافة التصاميم و برامج الإنتاج لإحدى كبرى مصانع التقنية العالمية في نيوجرسي و التي تؤثر على نظم تحكم مستخدمة في NASA والبحرية الأمريكية، ملحقا خسائر بلغت 10 ملايين دولار وتعتبر هذه الحادثة مثالا حيا على مخاطر جرائم التخريب في بيئة الانترنت بل اعتبرت أنها من أكثر و اخطر الجرائم التخريبية للكمبيوتر منذ بروز هذه الظاهرة[1].

ثانيا: دافع التعاون والتواطؤ على الأضرار

هذا النوع كثير التكرار في الجرائم المعلوماتية وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية يقوم بالجانب الفني من المشروع وآخر من المحيط أو خارج المؤسسة المجني عليها لتغطية التلاعب وتمويل المكاسب المادية وعادة ما يمارسون التلصص على الأنظمة[2].

الفرع الثاني: أنواع الجريمة الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة، والتي اختلف الفقه في تصنيفها إلى عدة مسميات، ولم تراع أغلب التقسيمات خصائص الجرائم الإلكترونية وموضوعها، وإن أهم ما يميز الجرائم الإلكترونية عن غيرها هو أن هذه الجرائم تستهدف الكيانات المعنوية للحاسب الآلي، وترتكب بواسطة جهاز إلكتروني، أما ما يستهدف الكيانات المادية للحاسب الآلي فيندرج تحت صور الجرائم التقليدية، واختلاف الفقه في تقسيم الجرائم الإلكترونية هو نتيجة ظهور جرائم جديدة من حين لأخر، حيث أن الجرائم الإلكترونية لا حصر لها، ولا يمكننا أن نجملها بكل أصنافها وأشكالها، فهي متغيرة ومتجددة، فكلما ظهرت وسيلة جديدة لاستخدام الحاسب الآلي والأنترنت ظهرت معه جريمة جديدة[3].

---

[1] –غريبي بشرى، المرجع السابق، ص111.

[2] – بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، مجلد 14، العدد04، جامعة قسنطينة02، الجزائر، 2021، ص54.

[3] –– بوضياف اسمهان، المرجع السابق، ص 357.

إذ لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم الإلكترونية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو على أساس محل الجريمة، وعلى هذا الأساس يمكن تقسيمها إلى:

البند الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

بعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة، وتنقسم هذه الجرائم بدورها إلى:

أولا: الجرائم الواقعة على الأشخاص

ان للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الخاصة بشخص ما أو تسجيل مكالمات أو فيديو أو مراقبته[1].

ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسلوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالأداب العامة، ويقوم بنشرها عبر الأنترنت[2]، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإرادة على ذلك إن جمع معلومات حول شخص، المعالجة المعلوماتية للمعلومات التي جمعها، تحويل المعلومات الاسمية عن مقصدها، إنما هو مساس بحقوق الأشخاص[3].

[1] – بوضياف اسمهان، المرجع السابق، ص357.

[2] – المرجع نفسه، ص357

[3] –أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، د ط، النشر الجامعي الجديد، تلمسان، الجزائر، 2022، ص 489.

ثانيا: الجرائم الواقعة على الأموال

الحقوق المالية منها ما يقع على أشياء مادية كحق الملكية وحق الانتفاع وحق الارتفاق ومنها ما يرد على شيء غير مادي كحقوق المؤلف وهو ما يعرف بالملكية الأدبية والفنية والملكية الصناعية والتجارية الى غير ذلك من أنواع التي تظهر مع تطور المجتمعات ومنها ما يرد على الحقوق غير المادية لا تدرك بالحس ويطلق عليها الأشياء الذهنية أو الحقوق الذهنية ومنها حق المؤلف والمخترع وحقوق التجارية، ويذهب اتجاه من الفقه إلى أنه ذلك النوع من الحقوق التي ترد على أشياء معنوية وغير محسوسة من خلق الذهن ونتاج الفكر، كما يمكن أن تقع كانه صورة الاعتداء على المال بطريقة تقليدية باستخدام الحاسب الالي[1].

يمكن أن النظام المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية والأدبية ، ومثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج نظام معلوماتي آخر ، أو حالة تخزين، واستخدام هذه المعلومات أو التفريط فيها دون إذن صاحبها، ذلك أن استخدام معلومة معينة دون إذن صاحبها يتضمن اعتداء على حق من الحقوق المعنوية، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي و آخر مالي للمخترع[2] .

وقد نص المشرع الجزائري على حقوق الملكية الفكرية وبراءات الاختراع من خلال عدة نصوص قانونية نذكر من بينها المادة 38 من الدستور الجزائري[3]، والأمر 03/05 المؤرخ في

---

[1] –محمد نصر محمد، الوسيط في الجريم المعلوماتية، ط 01، مركز الدراسات العربية للنشر والتوزيع، مصر، 2010، ص140.

[2] – سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، تلمسان،2010 ،2011، ص 34.

[3] -تنص المادة 38 من الدستور الجزائري التي تنص على أن "حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن.

–حقوق المؤلف يحميها القانون

–لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي".

2003.07.19 المتعلق بحقوق المؤلف والحقوق المحـاورة، والأمر 03/07 المؤرخ في 2003.07.19 المتعلق ببراءات الاختراع[1].

ثالثا: الجرائم المعلوماتية الواقعة على أسرار الدولة

إن أغلب التشريعات قد وضعت ترسانة قانونية عقابية في مواجهة كل ما من شأنه المساس بأمن وسـلامة مواطنيها ومؤسـساتها الحيوية، وقبل التطرق إلى ذلك يمكن الإشـارة إلى مفهوم الجرائم المعلوماتية الماســـة بالنظام العام من خلال ما أوردته المادة 15 و16 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية بشأن نوع هذه الجرائم وحصرتها فيما يلي:

أولا: نشر أفكار ومبادئ الجماعات الإرهابية والدعوة لها.

ثانيا: تمويل العمليات الإرهابية والتدريب عليها وتســـهيل الاتصـــالات بين المنظمات الإرهابية.

ثالثا: نشر طرق صناعة المتفجرات .

رابعا: نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

خامسا: القيام بعمليات غسل الأموال أو نشر طرق غسل الأموال[2].

البند الثاني: الجرائم الواقعة على نظام المعلوماتي

هناك نوع آخر من الجرائم المعلوماتية بالاعتماد على التصـــنيف الذي يقوم على محل الجريمة المعلوماتية يتمثل في الجرائم الواقعة على النظام المعلوماتي التي قد تســـتهدف إما المكونات المادية للنظام المعلوماتي والمكونات المنطقية والمعلومات المدرجة بالنظام المعلوماتي[3].

[1] – سوير سفيان، المرجع السابق، ص 35

[2] –ربيعي حسين، المرجع السابق، ص91.

[3] –سوير سفيان، المرجع السابق، ص39.

المبحث الثاني: أركان الجريمة الإلكترونية

من الناحية القانونية، تتمتع هذه الجرائم بطابع فريد، حيث لا تستهدف القوانين التقليدية هذا النوع الجديد من الجرائم بشكل محدد، وبالتالي، فإن استخدام الأنظمة التقليدية للقضاء على الجرائم المعلوماتية سيواجه تحديات عديدة، منها صعوبة العثور على الأدلة المادية التي تدين المتهم.
ومن الملحوظ أن التشريع الجزائري لم يصل إلى اتفاق واضح حيال هذا الأمر، حيث اعتمد تعريفات مختلفة بين القوانين الجنائية والتشريعات الفرعية في مجال الجريمة، حيث وصفت في قانون 04-15 باسم " المساس بأنظمة المعالجة الألية للمعطيات "، بينما وصفت في قانون 09-04 باسم " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال "، وعلى الرغم من هذا التباين، تهدف جميع التسميات إلى محاربة الجرائم المعلوماتية.
والجريمة الالكترونية تقوم على نفس أركان الجريمة العادية والمتمثلة في الركن الشرعي والمادي والمعنوي والركن المفترض.

المطلب الأول: الركن الشرعي والمادي للجريمة الإلكترونية

سنحاول من هذا المطلب التطرق للركن الشرعي والمادي للجريمة الإلكترونية من خلال الفرعين التاليين:

الفرع الأول: الركن الشرعي للجريمة الإلكترونية

تتحقق الجريمة بالفعل الصادر عن الأنسان فيتخذ صورة مادية معينة، تختلف الأفعال المادية باختلاف نشاطات الانسان وهذا ما يجعل المشرع يتدخل لتحديد فئة من الأفعال الضارة أو الخطرة على سلامة أفراد المجتمع فينهي عنها بموجب نص قانوني جزائي يجرم هذه الأفعال ويحدد عقوبة من يأتي على ارتكابها[1].

وما عدا ذلك يبقى الإنسان حرا في تصرفه شرط ألا يلحق الضرر بالغير فالنص القانوني هو إذا مصدر التجريم وهو المعيار الفاصل بين ما هو مباح وما هو منهي عنه تحت طائلة الجزاء[2].

---

[1] – أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دط، النشر الجامعي الجديد، تلمسان، الجزائر، 2022، ص ص 64، 65.

[2] –المرجع نفسه، ص64.

يفهم من المادة الأولى[1] من قانون العقوبات الجزائري حصر مصادر التجريم والعقاب في نطاق نصوص قانونية مكتوبة[2]، ومعنى ذلك، اعتراف المشرع والنص على تجريم الفعل المرتكب من خلال المادة سالفة ذكر بالنسبة للتشريع الجزائري فقد أحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث خاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعا لجة الآلية للمعطيات[3]، وهو القسم السابع مكرر بمحتوى المادة 394 مكرر إلى 394 مكرر 7 بمقتضى القانون رقم : 04-15 المؤرخ في 10 نوفمبر 2004 ولم يكتف المشرع الجزائري لذلك فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 والذي مس المادة 303 واقراره بالمادة 303 مكرر 3 وهذا تصديا للاستخدام السيئ لوسائل التكنولوجيا الحديثة ، فهذا يعني أن المشرع نص على تجريم الفعل المرتكب ، والمشرع الفرنسي فصل بين جرائم الاعتداء على نظام المعالجة الآلية للمعطيات وبين جريمتي تزوير المستندات المعالجة آليا واستعمالها ، كذلك تجريم كل الاعتداءات على نظام المعالجة آليا واستعمالها[4] .

وتجدر الإشارة أنه ثار اختلاف حول إدماج النصوص القانونية الجديدة الخاصة بالجريمة الإلكترونية في قانون العقوبات أو في قانون خاص ، فظهر هناك من ادمجها في جرائم الأموال باعتبار أنه يمكن إضفاء صفة المال على الكيانات المادية و المعنوية للحاسوب ، والبعض الآخر يفضل ادماجها في إطار الجزء الخاص بالجرائم ضد الملكية باعتبار الكيان المادي[5] للحاسوب عناصر مادية قابلة للتملك كما أن الكيان المعنوي يدخل في إطار الملكية الفكرية، وهناك من يرى إضافة جزء آخر بالجرائم المعلوماتية مستقل عن الأجزاء التقليدية باعتبار أن هاته الجرائم تتعلق بقيمة اقتصادية جديدة لها طابع خاص ، والاتجاه الثالث يرى أنه لابد من

[1] –تنص المادة الأولى من ق ع ج: لا جريمة ولا عقوبة أو تدبير أمن بغير قانون.

[2] –عبد أوهابية، شرح قانون العقوبات الجزائري–القسم العام، دط، موفم للنشر، الجزائر، 2015، ص 99.

[3] – لامية طالة، كهينة سلام «الجريمة الإلكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي»، مجلة الرواق للدراسات لاجتماعية والإنسانية، المجلد 06، العدد02، المركز الجامعي غليزان، 2020، ص69.

[4] – إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة الآفاق للبحوث والدراسات، العدد04، المركز الجامعي إليزي، الجزائر، 2019، ص188.

[5] – المرجع نفسه، ص188.

الحاق كل جريمة معلوماتية بما يقابلها في قانون العقوبات التقليدي مثل : وضع جريمة التزوير المعلوماتي في باب المحررات ، الاعتداء على المعطيات يلحق بالإتلاف[1].

الفرع الثاني: الركن المادي للجريمة الإلكترونية

لا يعاقب قانون العقوبات على الأفكار رغم قباحتها ولا على النوايا السيئة ما لم تظهر إلى الوجود الخارجي بفعل أو عمل[2].

ويشكل الفعل أو العمل الخارجي الذي يعبر عن النية الجنائية أو الخطأ الجزائي ما يسمى بالركن المادي للجريمة، فعلى سبيل المثال يتمثل الركن المادي في جريمة القتل في الطلقة النارية أو الطعن بالخنجر، ويتمثل بالطعن بالخنجر في جريمة السرقة، وإذا كان القانون يوجب دائما فعلا ماديا في الجريمة، فإنه لا يشترط أن يترك هذا الفعل آثارا مادية أو أنه يتسبب في نتائج ضارة، فحتى إذا لم ينتج الفعل آثاره الجرمية فانه يشكل ركنا ماديا للجريمة كما في حالتي الشروع والجريمة الخائبة، لا بد من فعل أو امتناع يمكن إثباته إذ لا عبرة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل[3].

وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر ، وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها، وهذا ما يدعو للتدخل التشريعي"[4].

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها،

[1] -إيمان بغدادي، المرجع السابق، ص188.

[2] – أحسن بوسقيعة، المرجع السابق، ص114.

[3] – المرجع نفسه، ص 115.

[4] – بوضياف اسمهان، المرجع السابق، ص354.

(مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل[1]).

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب (مثلا: جريمة الغش المعلوماتي: الركن المادي فها هو تغيير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية[2].

البند الأول: السلوك الجرمي للجريمة الإلكترونية

السلوك المجرم قانونا، هو كل سلوك خارجي واع وموجه يقوم به الإنسان بغرض إحداث تغيير في العالم الخارجي، فيظهر في العالم الخارجي مكونا من ماديا الجريمة التي ينص القانون على تجريمها ويقرر لها العقاب المناسب[3].

وقد يكون هذا السلوك إيجابي أو سلبي، فالسلوك الإجرامي الإيجابي سلوك إرادي محسوس يأتيه الفاعل باستعمال أي عضو من أعضاء جسمه في ارتكابه الجريمة، وبعبارة أخرى هو حركة عضوية إرادية يأتيها الإنسان لإحداث أثر مادي ملموس خرقا لنهي القاعدة الجنائية عن ،إتيانه، كقيام شخص بإزهاق روح إنسان حي بإطلاق النار عليه أو بخنقه أو بطعنه بسكين أو بأي أداة تحدث الوفاة «المادة 254 ق.ع»، أو في جريمة السرقة بنقل المال المسروق المملوك للغير خلسة من حيازة صاحبه أو بدون رضاه إلى حيازة السارق أو غيره بنية تملكه «المادة 350 ق.ع» أو تزوير في محرر رسمي بوضع توقيعات مزورة أو بإحداث تغيير فيها «المادة 214 ق.ع» ، أو بانتحال شخصية الغير أو الحلول محلها المادة 242 ق .ع»، أو اغتصاب فتاة عنوة بدون رضاها «المادة 336 ق . ع»، أو بحمل أوسمة أو نياشين بغير حق «المادة 244 ق . ع[4] .... وهذا يعني أن السلوك الإجرامي الإيجابي سلوك إرادي يتجه إلى تحقيق نتيجة مادية معينة، أي

[1] – بوضياف اسمهان، المرجع السابق، ص354.

[2] – المرجع نفسه، ص 354.

[3] – عبد الله أوهابية، المرجع السابق، ص 239.

[4] – المرجع نفسه، ص 241.

يتطلب فيه القانون أن يكون صادرا عن إرادة واعية وحرة باعتبارها القوة النفسية المدركة والمميزة لحقيقة –كنه – الفعل، ومسيطرة على الحركة العضوية[1].

وقد يكون سلبيا، وهو سلوك يختلف عن السلوك الإيجابي، إذ ليس فيه حركة عضوية، بل هو سلوك واع يتخذ فيه الإنسان موقفا سلبيا من أمر القانون أو واجب الذي يرتبه على المخاطب بالقاعدة القانونية المتضمنة أمرا بالقيام بعمل محدد، بالامتناع إراديا عن القيام به، فهو من ناحية المادية ظاهرة سلبية، ومن الناحية القانونية ظاهرة إيجابية، فالسلوك السلبي المجرم يقتضي بدوره وجود العلاقة النفسية بين المسلك السلبي المتخذ وإرادة صاحبه، كامتناع الأم عن ارضاع طفلها الرضيع، وامتناع القاضي عن الجلوس للنظر في القضايا المعروضة عليه أو الموظف العمومي ليقضي بين الناس فيما هو مختص فيه طبقا للمادة 316 ق ع ج، ترك طفل أو عاجز عن حماية نفسه في مكان خال طبقا للمادة 314 ق ع ج، وامتناع الشاهد عن الحضور أمام الجهة القضائية المختصة، أو امتناعه الإدلاء بالشهادة أمامها، أو امتناعه عن أداء اليمين طبقا للمادة 88 وما يليها من ق إ ج، وهذا يعني أن مثل هذا المسلك من أمر القانون للقيام بعمل أو سلوك ما، ليس موقفا مجردا من عنصر الإرادي بل هي جميعها تصرفات إرادية واعية قام بها الفاعل من أجل إتيان السلوك المكون للجريمة[2].

الركن المادي لجريمة الدخول الاحتيالي في الأنظمة المعلوماتية "دون التأثير عليها" الجريمة المتعلقة بالدخول الاحتيالي دون التأثير على نظام المعلوماتية معاقب عليها بالمادة 1-323 فقرة 1 ق.ع. فرنسي والمادة 394 مكرر فقرة 1 ق.ع. جزائري.

حسب هذه المادتين فإن الدخول يعتبر مكون للجريمة إذا تم بطريقة أو مناورة احتيالية (الغش) وبطريقة عمدية وبالتالي الدخول الخطأ أو بالصدفة إلى النظام غير معاقب عليه، من جهة أخرى يجب أن يكون مرتكب الجريمة على علم بأنه دخل إلى النظام المعلوماتي بطريقة[3]

[1] –عبد الله أوهابية، المرجع السابق، ص 241.

[2] – المرجع نفسه، ص 242.

[3] – دردور نسيم، الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذرة لنيل شهادة ماجستير، تخصص القانون الجنائي، كلية الحقوق، جامعة قسنطينة، 2012-2013، د ص.

غير عادية أي أنه على علم بأن الدخول إلى هذا النظام ممنوع، والجريمة لا تكون مؤسسة أمام القاضي الجزائي إلا بإثبات عملية الدخول إلى النظام[1]).

أما بالنسبة لجريمة الدخول الاحتيالي في الأنظمة المعلوماتية مع التأثير عليها، معاقب عليه في المادة 323–1 فقرة2 ق.ع فرنسي، والمادة 394 مكرر الفقرة 2 ق ع ج، وتجدر الإشارة أن التأثير السلبي على النظام المعلوماتي يعد ظرف مشدد للعقوبة، وفيما يخص الركن المادي المقرر بالنسبة للدخول بدون التأثير على النظام المعلوماتي إلا أنه يضاف إليها في هذه الحالة التأثير على النظام المعلوماتي بمعنى إفساد أو تخريب النظام المعلوماتي أو إنقاص من قدراته التقنية في المعالجة، أما جريمة البقاء الاحتيالي في الأنظمة المعلوماتية، هو مرحلة تلي الدخول الى النظام ونصت عليها كل من المادة 323–فقرة1 ق ع الفرنسي، والمادة 394 مكرر الفقرة 01 ق ع الجزائري، ومن جهة أخرى جريمة البقاء الاحتيالي في النظام المعلوماتي تعد من الجرائم المستمرة، فالجريمة تستمر كلما زادت مدة البقاء الغير المشروع داخل النظام وبالتالي استمرار الفعل الجرمي، وتكتمل باكتمال عملية البقاء الغير المشروع في النظام المعلوماتي[2]

البند الثاني: النتيجة الجرمية في الجريمة الإلكترونية

السلوك الاجرامي في الجرائم المعلوماتية قد يكون وقتيا أي يبدأ وينتهي بمجرد تمامه، مثل جريمة السرقة المعلوماتية أو الاعتداء على معطيات الحاسب الآلي بإتلافها، وقد يكون مستمرا مثل حيازة صور وافلام مخلة بالحياء وعرضها على شبكة الأنترنت، أو انشاء مواقع لتحريض القصر على الفسق والدعارة أو مواقع معادية بغرض الترويج للإرهاب

وتطرح مسألة النتيجة الإجرامية في جرائم المعلوماتية مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا باختراق جهاز حاسب آلي رئيسي وهو ما يعرف باسم " الخادم Server " في أحد البنوك في لفرنسا[3]، وهذا الجهاز

[1] – دردور نسيم، المرجع السابق، د ص.

[2] –المرجع نفسه، د ص.

[3] ––معتوق عبد اللطيف، المرجع السابق، ص24.

الخادم موجود في الصين فمعرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين وهذا ما يثير أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن[1].

البند الثالث: العلاقة السببية للجريمة الإلكترونية

لمساءلة شخص جنائيا عن نتيجة إجرامية معينة، يجب أن يكون قد تسبب بسلوكه في إحداثها، أي وجود رابطة بين السلوك والنتيجة، وهو ما يعرف بالعلاقة السببية، وهي عنصر ثالث من عناصر الركن المادي، وتعرف بأنها الرابطة أو العلاقة، بين السلوك الإجرامي والنتيجة، بحيث يكون السلوك هو سبب حصول تلك النتيجة، وبعبارة أخرى فإن النتيجة تعتبر ثمرة هذا السلوك المجرم، والذي يعتبر ضرورة لوقوع النتيجة، التي تعتبر بدورها أثرا له، فإذا انتفت هذه العلاقة بأن وقعت النتيجة بسبب سلوك آخر، انتفت العلاقة بينهما، وبالتالي عدم اكتمال عناصر الركن المادي، وعدم قيام الجريمة من الناحية القانونية، وهي علاقة يجب توافرها في جميع أنواع الجرائم عمدية أم غير عمدية[2].

ويتوقف اثبات علاقة سببية على حسب وجود فعل أو سلوك جرمي أو عدة سلوكيات جرمية متعاصرة ومتعاقبة، اذ يكون في الأولى الأمر سهلا ففي اثبات تحقيق النتيجة بفعل سلوك الجاني أو لا، لكن كيف عندما توجد أفعال ونتيجة واحدة، وللإجابة على هذا الاشكال أتى الفقه بنظريتين.

أ-نظرية تعادل الأسباب: تعمل هذه النظرية على أساس أن كافة الأفعال المتعاقبة مرتبطة بعلاقة سببية مع النتيجة، وبالتالي يسأل جميع من أتى تلك الأفعال الجرمية، مثال ذلك، شخص ضرب آخر ضربة غير قاتلة على رأسه[3]، ونقل إلى المستشفى وتعرضت سيارة

[1] --معتوق عبد اللطيف، المرجع السابق، ص24.

[2] - عبد الله أوهابية، المرجع السابق، ص 248.

[3] - جلال محمد الزغبي، أسامة أحمد مناعسة، جرائم تقنية نظم المعلومات الإلكترونية-دراسة مقارنة، ط01، دار الثقافة للنشر والتوزيع، 2010.، ص54.

الإسعاف الحادث يموت على أثره المصاب، فهل يسأل في هذه الحالة من ضرب ومن تسبب في الحادث عن جريمة قتل، ولأن انتقادات كثيرة وجهت لهذه النظرية، خصوصاً عدم العدالة، قيل بنظرية الأسباب المتفاوتة[1].

ب- نظرية الأسباب المتفاوتة: تعطي هذه النظرية لكل سبب قوة سببية مع النتيجة الجرمية التي حدثت ثم تختار أقوى العلاقات ومن ذلك:

-نظرية السبب الأخير تعتبر هذه النظرية أن العلاقة السببية تثبت بين النتيجة والسبب الأخير وهو في المثال السابق حادث التصادم، لكن في هذا توسيع لدائرة الإفلات من العقاب وغياب القاعدة العدالة، ونظرية السبب الأقوى توازن هذه النظرية بين جميع الأسباب والأفعال التي عاصرت وقوع النتيجة، ثم ترجح السبب الذي ترى أنه الأقوى لإحداث النتيجة. نظرية السبب المتحرك في هذه النظرية السبب المتحرك هو المسؤول عن إحداث الجريمة، وبالتالي تقوم معه العلاقة السببية، وذلك مع التمييز بين السبب المتحرك والسبب الساكن، مثال ذلك: شخص يصاب فيتوفى مع العلم أنه مريض بالقلب، هنا الإصابة التي تعرض لها هي السبب المتحرك، ومرض القلب هو السبب الساكن، ولكن في هذا تجاهل للسبب الساكن الذي قد يكون عاملا أساسيا في إحداث النتيجة. نظرية السبب الكافي وفق هذه النظرية تقوم العلاقة السببية بين النتيجة والفعل أو السلوك الجرمي الكافي وفق المجرى العادي للأمور لتحقيق النتيجة[2]

[1] - جلال محمد الزغبي، أسامة أحمد مناعسة، المرجع السابق، ص54

[2] - المرجع نفسه، ص55..

المطلب الثاني: الركن المعنوي والمفترض للجريمة الإلكترونية

سنحاول من خلال هذا العنوان تطرق إلى الركن المعنوي والمفترض للجريمة الإلكترونية.

الفرع الأول: الركن المعنوي للجريمة الإلكترونية

ان تحقق الركن المادي للجريمة لا يكفي وحدة لقيام المسؤولية الجنائية عنها وانما ينبغ يتوافر الركن المعنوي للجريمة الذي جوهره الإرادة الاجرامية ويتخذ الركن المعنوي إحدى صورتين القصد الجنائي، والخطأ غير العمدي، فيعرف القصد الجنائي على انه علم الجاني بالعناصر المكونة للجريمة واتجاه إرادته إلى احداث هذه العناصر أو الى قبولها، فالقصد الجنائي المتطلب لقيام الجرائم الالكترونية هو القصد الجنائي العام، الذي يفترض علم الجاني بعناصر الجريمة واتجاه إرادته نحو تحقيق هذه العناصر أو قبولها كما تطلب المشرع الى جانب القصد الجنائي العام قصداً خاصاً يتمثل في اتجاه الإرادة الى غاية معينة وهي نية التملك وغيرها من النوايا فالركن المعنوي يتعلق بالإرادة التي يصدر عنها الفعل فهو يتمثل الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني[1].

تشكل هذه العلاقة التي تربط العمل المادي بالفاعل ما يسمى بالركن المعنوي فلا تقوم الجريمة بدون توافر الركنين المادي والمعنوي علاوة على الركن الشرعي ويتمثل الركن المعنوي في نية داخلية يضمرها الجاني في نفسه وقد يتمثل أحيانا في الخطأ أو الإهمال وعدم الاحتياط، ومن ثم يتخذ الركن المعنوي للجريمة صورتين أساسيتين صورة الخطأ العمد أي القصد الجنائي القصد الجنائي، ويشكل الركن المعنوي في الجرائم العمدية وهي الجنايات وغالبية الجنح وبعض المخالفات[2].

[1] – خالد على نزار، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة دكتوراه، تخصص حقوق، كلية الحقوق جامعة المنصورة، مصر، 2020، 2021، ص 10.

[2] –أحسن بوسقيعة، المرجع السابق، ص141.

لم يعرف المشرع الجزائري القصد الجنائي على غرار غالبية التشريعات واكتفى بالنص في الجرائم على العمد، وأمام صمت التشريعات الجزائية اجتهد الفقه في تعريف القصد الجنائي:

أ- رأي الفقه انقسم الفقه فريقين:

1 المذهب التقليدي ويمثله كل من نورمان Normand وقارو Garraud وقارصون Garçon .

عرف "نورمان" القصد الجنائي بانه علم الجاني بأنه يقوم مختارا بارتكاب الفعل الموصوف جريمة في القانون وعلمه انه بذلك يخالف أوامره ونواهيه"، وعرفه "قارو" بأنه إرادة الخروج عن القانون بعمل أو امتناع وهو إرادة الأضرار بمصلحة يحميها القانون الذي يفترض العلم به الفاعل.

والقصد الجنائي هنا يتكون من عنصرين:

- ❖ اتجاه إرادة الجاني نحو ارتكاب جريمة
- ❖ العلم بتوافر أركان الجريمة كما يتطلبها القانون[1]

2- المذهب الواقعي: يرى فيري Ferri وهو من رواد المدرسة الوضعية أن النية ليس إرادة مجردة، وإنما هي إرادة محددة بسبب أو باعث[2].

جرائم المعلوماتية هي في أغلبها جرائم عمدية، حيث يستوجب المشرع فيها توفر القصد الجنائي بركنيه العلم والإرادة، إذ يجب أن تتجه ارادة المجرم إلى ارتكاب سلوك يحظره القانون، كالاعتداء على نظام المعالجة الآلية للمعطيات، بما يشمله من صور كفعل الإدخال لبيانات أو المحو أو التعديل، أو إلى نسخ البرامج بوجه غير شرعي من موقع على شبكة الانترنت أين يقوم القراصنة او الهاكرز بفك شيفرة الموقع أو تخريبه للحصول على البرمجيات إما للمنفعة المادية أو لإيقاع الضرر بالشركة المعتدى على منتجها[3].

[1] – أحسن بوسقيعة، المرجع السابق، ص 142.

[2] – المرجع نفسه، ص 144.

[3] –معتوق عبد اللطيف، المرجع السابق، ص 24.

ويختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة، أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي بما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله الى نظام الحاسب الآلي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غبير الشرعي[1].

وفي جريمة الاحتيال المعلوماتي التي هي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط في جريمة الاحتيال المعلوماتي هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع، أما في جريمة اتلاف المعلومات فان المشرع اشترط توفر القصد الجنائي العام فقط حيث يكفي علم الجاني بانه يقوم بأعمال من شانها أن تؤدي الى اتلاف المعلومات او محوها، وقد تباينت التشريعات المختلفة في اشتراط القصد الجنائي[2] .

الفرع الثاني: الركن المفترض للجريمة الإلكترونية

يعد الركنين المادي والمعنوي من الأركان الأساسية والعامة التي تشترك فيها جميع الجرائم، إلا أن هناك نوع من الجرائم ومن بينها الجرائم المعلوماتية لا تكتفي القيام بهذين الركنين، بل أن نموذجها القانوني يتطلب فضلا عن ذلك توافر عناصر خاصة – تميزها عن غيرها من الجرائم والمتمثلة في صفة في الجاني أو المجني عليه، أو في عناصر أخرى منها وسيلة ارتكاب الجريمة أو محلها، وترتبط تلك الصفات بهذا النوع من الجرائم وجودا أو عدما، وقد أطلقت عليها عدة مسميات منها الجرائم الخاصة أو الجرائم ذات الصفة، وبمعنى آخر الجرائم التي ينبغي لقيامها[3]

[1] – معتوق عبد اللطيف، المرج السابق، ص 24

[2] – المرجع نفسه، ص24.

[3] – عميمر عبد القادر، المرجع السابق، ص 92.

توافر الركن المفترض الذي يفترض القانون توافره وقت مباشرة الجاني نشاطه وبدونه لا يوصف هذا النشاط بأنه جريمة، ويستوجب القانون توافر الركن المفترض من أجل وجود الجريمة أو من أجل اعتبارها من نوع معين (جناية أو جنحة)، وفي الجريمة المعلوماتية يعد نظام المعالجة الآلية للمعطيات العامل المميز لهذه الجريمة عن غيرها من الجرائم، فبدونه لا يمكن القول أننا بصدد جريمة معلوماتية وقد يكون هذا النظام محلا للجريمة، أو وسيلة ارتكابها، وقد وفر قانون العقوبات الجزائري لهذه المنظومة حماية من كل أشكال الاعتداءات التي تطالها من خلال تجريم بعض الأفعال التي تشكل مساسا بها أو بأحد مكوناتها، وهي الأفعال التي يهدف الجاني من خلالها الدخول إلى هذه المنظومة أو جزء منها بغرض الاطلاع على محتوياتها، أو الاستفادة من خدماتها بوجه غير مشروع أو الوصول إلى مكوناتها من أجل إتلافها أو تعطيلها، كما أنه ادرج ضمن الجرائم المعلوماتية كل الجرائم المنصوص عليها في قانون العقوبات أو القوانين الخاصة التي ترتكب عن طريق المنظومة المعلوماتية[1].

وقد نصت المادة 394 مكرر من ق.ع.ج على تجريم فعل الدخول إلى المنظومة المعلوماتية أو جزء منها، أو محاولة ذلك، كما شددت العقوبة في حالة ما إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة كما رصد المشرع عقوبة تتراوح بين ثلاثة أشهر وثلاث سنوات وغرامة مالية تتراوح بين 500.000.00 دج و2.000.000 د. ج إذا ترتب عن الدخول تخريب نظام اشتغال المنظومة ولا تدخل ضمن نطاق هذه الجرائم الاعتداءات التي تستهدف الأجهزة والدعامات بصفة منفردة، لأن عنصر الترابط بين الأجهزة والدعائم والبرامج هو الركن الأساسي لإضفاء وصف المنظومة المعلوماتية، وكل الاعتداءات التي تطال أي جزء من هذه المنظومة يدخل ضمن الجرائم التقليدية مثل التحطيم والإتلاف والسرقة و حتى الأنظمة المتكاملة التي تخرج من الخدمة لا تطبق عليها أحكام الجريمة المعلوماتية ونفس الحكم تأخذه الاعتداءات على الأجهزة التي لم تدخل الخدمة بعد ولا تزال مودعة بالمخازن[2]

[1] – عميمر عبد القادر، المرجع السابق، ص 93.

[2] – المرجع نفسه، ص93.

خلاصة

الفصـــــل الأول

خلاصة الفصل الأول:

بانتهاء هذا الفصل نستخلص أن أن الجريمة الإلكترونية من الجرائم المستحدثة التي تختلف طبيعتها عن الجرائم التقليدية الذي دفع السياسة تشريعية لمسايرتها من خلال سن نصوص تجريميه ودراسة الفاعل الجرمي ألا وهو المجرم المعلوماتي، كما أنه لم يتفق الفقهاء لتعريف موحد لهذه الجريمة.

يمكن إدراج الجريمة الإلكترونية من الجرائم الخطيرة إذ أنها جريمة عابرة للقارات ومن جرائم الناعمة ويصعب اثباتها ويسهل طمس أدلتها، وقد تمس الأشخاص أو مؤسسات بواسطة النظام المعلوماتي أو عليه.

لقد حتم تطور التكنولوجي على المشرع وضع ترسانة قانونية تحت مسمى المساس بأنظمة المعالجة الآلية للمعطيات وهي المحددة في الفصل السابع مكرر من قانون العقوبات الجزائري تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات" والتي تحكمها المواد من 394 مكرر إلى 394 مكرر 7 من ق ع الجزائري.

الفصل الثاني

آليات التعاون الشرطي لمكافحة الجريمة الإلكترونية

الفصل الثاني: آليات التعاون الشرطي لمكافحة الجريمة الإلكترونية

لا يمكن سن قوانين واتفاقيات تجرم هذه الظاهرة فالمجال الشرطي أيضا يلعب دورا فعال لتصدي لهذه الجريمة، باعتبار أن الجريمة الإلكترونية جريمة عابرة للحدود.

في هذا الفصل سوف نكتشف كيف تتعاون أجهزة الشرطة على المستوى العربي والإقليمي والدولي لمواجهة التحديات المتزايدة للجريمة الإلكترونية، بالإضافة إلى دور المنظمات الدولية في تعزيز التعاون الشرطي وتبادل المعلومات، وسنتطرق أيضا لنماذج ناجحة للتعاون في مجال مكافحة الجريمة الإلكترونية، وعلى ما سبق ذكره قسمنا الفصل الى مبحثين، عنونا المبحث الأول التعاون الشرطي العربي والإقليمي لمكافحة الجريمة الإلكترونية، وقسمناه الى مطلبين، المطلب الأول خصصناه للتعاون الشرطي العربي والأوربي، أما المطلب الثاني معنون بآلية الاتحاد الإفريقي للتعاون الشرطي في مكافحة الجريمة الإلكترونية، أما المبحث الثاني معنون بدور منظمة الشرطة الجنائية الدولية لمكافحة الجريمة الإلكترونية، قسمناه إلى مطلبين، المطلب الأول مفهوم المنظمة الدولية للشرطة الجنائية، أما المطلب الثاني خصصناه المطلب الثاني: دور منظمة الشرطة الدولية لمكافحة الجريمة الإلكترونية.

المبحث الأول: التعاون الشرطي العربي والإقليمي

مع تزايد الجريمة المعلوماتية بشكل مستمر، استوجب ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، وهذا ما جعل بعض الدول استحدثت هذه الأجهزة على المستوى العربي والإقليمي وهذا ما سنعرضه من خلال هذا المبحث حيث قسمناه إلى مطلبين، المطلب الأول التعاون الشرطي العربي والأوربي لمكافحة الجريمة الإلكترونية، والمطلب الثاني آلية الاتحاد الإفريقي للتعاون الشرطي لمكافحة الجريمة الإلكترونية

المطلب الأول: التعاون الشرطي العربي والأوربي

قسمنا هذا المطلب الى فرعين، الفرع الأول التعاون الشرطي العربي لمكافحة الجريمة الإلكترونية والفرع الثاني التعاون الشرطي الأوربي.

الفرع الأول: التعاون الشرطي العربي لمكافحة الجريمة الإلكترونية

أولا: منظمة المكتب العربي لمكافحة التطرف والإرهاب.

أ-نشأة المكتب

صدر قرار رقم (691) من عام 2014 م القاضي بموافقة على إنشاء مكتب عربي للأمن الفكري وتقديم الشكر لحكومة المملكة العربية السعودية التي تكلفت باستضافته واتخاذ عاصمتها الرياض مقرا له ، صدر بعد ذلك قرار أصحاب السمو والمعالي وزراء الداخلية العرب رقم (728) لعام 2016 يقضي بتعديل تسمية المكتب العربي للأمن الفكري ليصبح (المكتب العربي لمكافحة التطرف والارهاب) وفي تاريخ 2017/10/16 تم توقيع اتفاقية المقربين حكومة المملكة العربية السعودية والمكتب العربي لمكافحة التطرف والإرهاب، ويعد المكتب رافدا للعمل الأمني العربي المشترك في مجال مكافحة التطرف و الإرهاب ومكسبا هاما لأجهزة مجلس وزراء الداخلية العرب وتأكيدا للدور البناء الذي يقوم به وزراء الداخلية في دول الأعضاء[1].

[1] – المكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات (الرياض)، تم الاطلاع عليه بتاريخ: 2024/05/30، على الساعة 17:47، في الموقع:https://www.aim-council.org/specialized-offices/riyadh/861

ومن أهم إنجازاته عقد الشركات ومذكرات تفاهم مع بعض المؤسسات والمراكز الحكومية والأهلية المتخصصة، والتي لها نشاطات في مواجهة التطرف والإرهاب وذلك من خلال تبادل الخبرات العلمية والعملية[1]

ب-دور المكتب العربي لتعاون الشرطي في مكافحة الجريمة الإلكترونية

في 15 أكتوبر 2022م نظم المكتب العربي لمكافحة التطرف والإرهاب باستضافة جامعة نايف اجتماع خبراء العرب لبحث الأمن السيبراني والجرائم الإلكترونية، حيث انطلقت أعمال اجتماع اللجنة المعنية بوضع تصور لتفعيل عمل مجلس وزراء الداخلية العرب في مجال الأمن السيبراني ومكافحة الجريمة الإلكترونية وذلك بمشاركة 13 دولة عربية، ومن أهم ما أكد عليه هذا الاجتماع وعلى لسان معالي الدكتور عبد المجيد بن عبد الله البنيان رئيس جامعة نايف العربية للعلوم الأمنية أهمية التعاون بين الأمانة العامة لمجلس وزراء الداخلية العرب والجامعة، مؤكدا أن الجامعة تهتم اهتماما بالغا بمجال الجرائم السيبرانية والأدلة الرقمية وبمجال الأمن السيبراني عمومًا، مشيرًا إلى أن الجامعة خلال إعداد خطتها الاستراتيجية الجديدة في عام 2018م، توجهت للجهات المختصة والمستفيدة من برنامج عمل الجامعة للاستعلام حول أهم المواضيع والتحديات والمخاطر التي يرون أنها تواجه الأجهزة الأمنية العربية، ولفت إلى أن جامعة نايف العربية للعلوم الأمنية وانطلاقًا من اهتمام الجامعة بهذه القضية مثار الاهتمام الدولي عملت على تأسيس مركز الجرائم السيبرانية والأدلة الرقمية واستقطبت له نخبة من الخبراء من حول العالم، ووفرت مجموعة من التقنيات المختلفة التي مكنت المركز من إجراء مجموعة من الدراسات والتقارير المختلفة[2].

وكما استعرض الاجتماع جهود الأمانة العامة لمجلس وزراء الداخلية العرب وجامعة نايف العربية للعلوم الأمنية في مجال الجريمة الإلكترونية، وأبرز مهام الوحدة المعنية بمواجهة جرائم

[1] – المكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات (الرياض)، تم الاطلاع عليه بتاريخ: 2024/05/30، على الساعة 17:50، في الموقع:https://www.aim-council.org/specialized-offices/riyadh/861

[2] –اجتماع نظمه المكتب العربي لمكافحة التطرف والإرهاب باستضافة جامعة نايف اجتماع خبراء عرب لبحث الأمن السيبراني والجرائم الإلكترونية، تم نشره 2022/10/05، تم اطلاع عليه بتاريخ: 30/05/2024، على الساعة 10:52، في الموقع: https://nauss.edu.sa/ar-sa/news/Pages/5-10-2022.aspx

تقنية المعلومات، يشار إلى أن مجلس وزراء الداخلية العرب شكل فريق خبراء معني بمواجهة الجرائم الإلكترونية خلال دورته الـ 35، نظرا لطبيعة الجريمة الإلكترونية وأبعادها المتعددة، واتخذ مجموعة من الإجراءات من بينها اعتماد الإستراتيجية العربية لمواجهة جرائم تقنية المعلومات في دورته السابعة والثلاثين بتاريخ 2020/30/01م[1].

ثانيا: تجربة الجزائر الرائدة في مكافحة الجريمة الإلكترونية

إن الشرطة الجزائرية اتخذت ما يلزم من إجراءات وقائية وردعية لمكافحة الجريمة الإلكترونية من خلال عصرنة الأجهزة واعتماد الحلول التقنية المبتكرة واستحداث مصالح مركزية وفرق متخصصة، تمكنت من فك لغز العديد من القضايا، إلى جانب العمل الاتصالي[2].

كما أشار المدير العام للأمن الوطني في كلمة تلاها نيابة عنه مدير الشرطة العام والتنظيم، مراقب الشرطة سي معاند محند السعيد خلال أشغال المؤتمر الـ 43 لقادة الشرطة والأمن العرب بتونس، بالمبادرة التي أطلقتها الأمانة العامة لمجلس وزراء الداخلية العرب بشأن إنشاء وحدة متخصصة في الأمن الإلكتروني، كما أكد أن هذا اللقاء يعتبر من أرقى الفضاءات المخصصة للبحث والتشاور بين أجهزة الشرطة العربية لدراسة أنجع السبل وأفضل الوسائل الكفيلة بمواجهة التحديات الأمنية، كما أكد المستوى الذي حققته الشرطة الجزائرية من خلال إستراتيجيتها الخاصة بمكافحة الجريمة العابرة للأوطان والجرائم الإلكترونية والإرهاب، حيث اعتمدت على تعزيز ودعم القدرات في مجال مكافحة الجريمة وتحديث أساليب العمل، كذلك توطيد علاقة الثقة مع المواطن، بالإضافة إلى تطوير التعاون الثنائي والمتعدد الأطراف على الصعيدين الإقليمي والدولي[3].

---

[1] – اجتماع نظمه المكتب العربي لمكافحة التطرف والإرهاب باستضافة جامعة نايف اجتماع خبراء عرب لبحث الأمن السيبراني والجرائم الإلكترونية، تم نشره 2022/10/05، تم اطلاع عليه بتاريخ: 30/05/2024، على الساعة 10:52 م، في الموقع: https://nauss.edu.sa/ar-sa/news/Pages/5-10-2022.aspx

[2] –اسعيداني سلامي، طارق طراد، «التجربة الجزائرية لمواجهة الجريمة الالكترونية في ظل البيئة التفاعلية الجديدة (عرض تشريعي قانوني)، مجلة الحقوق والعلوم السياسية، المجلد06، العدد02، كلية الحقوق والعلوم السياسية، جامعة خنشلة، 2019، ص250.

[3] –سمية م، تجربة الجزائر الرائدة في مكافحة "الجريمة الإلكترونية" و" الارهاب" على طاولة المؤتمر 43 لقادة الشرطة والأمن العرب، تم نشره 2019/12/11، تم الاطلاع عليه بتاريخ: 2024/05/30، على الساعة 10:52 م: https://alhirak-alikhbari.dz/article/3RaaSiCA7qWSCvS2H

إلى ذلك، ناقش المؤتمرون التصور المقترح للوحدة المعنية في نطاق الأمانة العامة لمجلس وزراء الداخلية العرب بتعزيز التعاون بين الدول العربية في مجال الأمن الالكتروني في صيغته المعدلة، تصور أولي لأهداف ومهام وآلية عمل لجنة دائمة للإحصاء الجنائي في نطاق الأمانة العامة، تقرير عن أعمال الاتحاد الرياضي العربي للشرطة لعام 2019، إلى جانب عرض التجارب الأمنية المتميزة لمختلف الدول المشاركة، كما تم عرض تجربة الشرطة الجزائرية، شهد مشاركة كل من مدير الشرطة العامة والتنظيم، مراقب الشرطة سي محاند محند السعيد، رفقة رئيس مكتب التعاون الدولي، عميد أول للشرطة بن لعلام احمد باي، في أشغاله التي ستدوم إلى غاية يوم غد، إلى جانب ممثلين من مختلف الدول العربية، وعن جامعة الدول العربية، المنظمة الدولية للشرطة الجنائية (الانتربول)، جامعة نايف العربية للعلوم الأمنية والاتحاد الرياضي العربي للشرطة[1].

الفرع الثاني: التعاون الشرطي الأوروبي لمكافحة الجريمة الإلكترونية

أولا: نشأة اليوروبول

اليوروبول اختصار لتسمية التي تطلق على المكتب الأوروبي للشرطة، وهو جهاز أمني مهمته تنسيق الجهد الأوروبي لمحاربة الجريمة المنظمة والعابرة للحدود ويتألف من وحدات أمنية تساهم بها بعض الدول الأعضاء في الاتحاد الأوروبي[2].

تأسست اليوروبول في عام 1999 بهدف محاربة "الإرهاب" والجريمة المنظمة ومواجهة التحديات التي تواجه الأمن الأوروبي، عموما كذلك في مبدأ حرية التنقل داخل الفضاء الأوروبي، كما يقع مقر اليوروبول في مدينة لاهاي الهولندية، ويتكون من تسعمئة عنصر[3]

[1] –سمية م، تجربة الجزائر الرائدة في مكافحة "الجريمة الإلكترونية" و" الارهاب" على طاولة المؤتمر 43 لقادة الشرطة والأمن العرب، تم نشره 2019/12/11، تم الاطلاع عليه بتاريخ: 2024/05/30، على الساعة 10:52 م، في الموقع : https://alhirak-alikhbari.dz/article/3RaaSiCA7qWSCvS2H

[2] –أحمد حبيب السماوي، «اليوروبول مهمته إنقاذ القانون»، مجلة شؤون قانونية، العدد 04، الدوحة، 2019، ص104.

[3] –مقال منشور على الموقع الكتروني موسوعة الجزيرة، «اليوروبول حارس أوروبا، شبكة الجزيرة الإعلامية، تم نشره 2016/02/01، تم الاطلاع عليه بتاريخ: 30–05–2024، على الساعة 10:52 م، في الموقع: https://www.aljazeera.net/news/2012/3/29/%D9%85%D8%B1%D9%83%D8%B2-%D8%A3%D9%88%D8%B1%D9%88%D8%A8%D9%8A-

يقع ضمن الهيكلة التنظيمية لوكالة اليوروبول عددا من المراكز البحثية والمعلومات التي تهتم بكافة المجالات المتعلقة بتنفيذ القانون ومن أهم المراكز:

أ-المركز الأوروبي لمكافحة الجرائم الإلكترونية (EC3).

أنشأ المركز عام 2013 لمكافحة الجرائم الإلكترونية ضمن دول الإتحاد الأوروبي من خلال تقديم المساعدات والدعم الفني لحماية المواطنين والشركات والحكومات الأوروبية من الجريمة المنفذة عر الإنترنت مثل الاختراقات وهجمات الفيروسات[1].

ب-وحدة مكافحة المحتوى الضار عبر الأنترنت

أنشأ عام 2015، تقوم الوحدة بمراقبة واكتشاف المحتوى الضار والتحقق منه على انترنت[2].

ثانيا: دور اليوروبول في مكافحة الجريمة الإلكترونية

يتميز التعاون في مجالي الشرطة وتسيير الحدود بشبكات مكثفة تعمل على تجميع المعلومات وتبادل أفضل الممارسات، كما هو الحال بالنسبة للأوروبول والأوروجيست والسيبول بالإضافة إلى الفرونتاكس الوكالة الأوروبية[3].

كما يهدف المركز الأوروبي لمكافحة الجريمة الإلكترونية للمساهمة في حماية المواطنين الأوروبيين والشركات من التهديدات المتزايدة التي يتعرض لها كل مستعمل للشبكة الأنترنت ، والمركز الجديد في مكتب الشرطة الأوروبية (يوروبول) في لاهاي بهولندا، وتسعى المفوضية الأوروبية لأن يصبح المركز نقطة محورية على المستوى الأوروبي في مجال مكافحة الجرائم الإلكترونية عبر التركيز على أنشطة غير المشروعة على الأنترنت، كما يتركز عمل المركز أيضا على حماية المعلومات الشخصية التي تضمها المواقع الاجتماعية ومكافحة عمليات القرصنة ويحتل ملف الاستغلال الجنسي للأطفال عبر الانترنت والهجمات الالكترونية التي يؤثر على البنية التحتية الحيوية ونظم المعلومات في الاتحاد الأوروبي صدارة اهتمامات المركز[4]

---

[1] -أحمد حبيب السماوي، «المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات . المانيا وهولندا»، تم نشره 2019/06/08، تم الاطلاع عليه بتاريخ: 30-05-2024، على الساعة 10:52 م، في الموقع: https://www.europarabct.com

[2] – المرجع نفسه، تم الاطلاع عليه الساعة21:37.

[3] -أمال حجيج، «نحو قوة أورو-متوسطية للشرطة والتسيير الحدودي، مجلة دفاتر السياسة والقانون، العدد 12، جامعة أم بواقي، الجزائر، 2015، ص253.

[4] -لبيب فهمي، «المركز الأوروبي لمكافحة الجريمة الإلكترونية»، تم الاطلاع عليه: 30-05-2024، على الساعة 10:52 مفي الموقع:

ثانيا: الأوروجيست

هو جهاز يتمتع بالشخصية القانونية، ويتكون من عضو وطني منتدب من كل دولة في الاتحاد الأوروبي، بشرط أن يكون متمتعا بصفة مدعي عام Procureur، قاضي أو ضابط شرطة له صلاحيات معادلة، علما أن كل عضو وطني يخضع لقانون دولته فيما يخص نظامه الأساسي[1]. تم إنشاؤه عام 2002، ومن اختصاصه عندما تمس الجريمة دولتين أو أكثر من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الاتحاد الأوروبي والأوروجيست وحدة للتعاون القضائي تكمن مهمته الأساسية في التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها صلاحيات الكاملة ما يؤهلها لفتح تحقيق ومباشرة متابعات جزائية[2].

المطلب الثاني: آلية الإتحاد الإفريقي للتعاون الشرطي لمكافحة الجريمة الإلكترونية

تعد الية الاتحاد الافريقي للتعاون الشرطي الأفريبول من بين أهم الآليات المؤسساتية الإقليمية في مجال مكافحة الإجرام الإلكتروني، وهذا ما سنشرحه من خلال هذا المطلب، حيث قسمناه إلى فرعين، الفرع الأول نشأة آلية الإتحاد الإفريقي للتعاون الشرطي، والفرع الثاني أجهزة آلية الإتحاد الإفريقي للتعاون الشرطي في مكافحة الإجرام الإلكتروني.

الفرع الأول: نشأة آلية الإتحاد الإفريقي للتعاون الشرطي

بالرجوع إلى النظام الأساسي لآلية الإتحاد الإفريقي في نص المادة الثانية منه، وصف هذه الآلية على أنها مؤسسة تقنية باعتبارها آلية للتعاون الشرطي بين الدول الأعضاء، بدأت فكرة إنشاء شرطة إفريقية خلال المؤتمر الإقليمي الإفريقي 22 الإنتربول والذي تم بين الفترة من 10 إلى 12 سبتمبر 2013 بوهران والتي شهدت حضور بالإجماع لقائدة الشرطة الأفارقة الواحدة والأربعون[3].

https://www.aljazeera.net/news/2012/3/29/%d9%85%d8%b1%d9%83%d8%b2-%d8%a3%d9%88

[1] –براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة دكتوراه تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، 2018، ص308

[2] –كعرار سفيان، «الآليات المؤسساتية الأوروبية لمكافحة الجريمة المنظمة عبر الوطن»، المجلة الاكاديمية للبحوث القانونية والسياسية، المجلد 04، العدد 01، جامعة الأغواط، 2020، ص 581.

[3] –ودرار أمين «الشرطة الجنائية الإفريقية الأفريبول»، حوليات، المجلد 34، العدد01، جامعة الجزائر، 2020، ص137.

وقد تم دعم هذه المبادرة على هامش الجمعية العامة ال 82 لمنظمة الإنتربول التي انعقدت من 21 إلى 23 أكتوبر 2013 في كولومبيا بدعوة من الجزائر، لعقد مؤتمر للمدراء والمفتشين العامين للشرطة حول الأفريبول يوم 10-11 فيفري 2014، تم اعتماد ورقة الجزائر المتعلقة بالأفريبول من قبل قادة ورؤساء الحكومات الأفارقة، أما في الاجتماع الثاني للجمعية العامة آلية الشرطة الجنائية، والذي انعقد بتاريخ 30 يناير 2017، أين اعتمد نظام الأساسي للآلية من قبل مؤتمر الإتحاد الإفريقي في دورته العادية رقم 28 المنعقدة في أديس أبابا بإثيوبيا، فقد تم الاتفاق على إنشاء ثلاث مجموعات عمل ، الأولى مختصة بمكافحة الجريمة المنظمة العابرة للحدود، الثانية مختصة بمكافحة الجريمة الإلكترونية والجريمة السيبرانية والثالثة في مكافحة الإرهاب والتطرف[1] .

ثانيا: أجهزة آلية الإتحاد الإفريقي للتعاون الشرطي في مكافحة الجريمة الإلكترونية

أ- **الجمعية العامة:**

تعتبر السلطة الفنية العليا في الأفريبول، وتتكون من قادة الشرطة للدول الأعضاء، وتضطلع بمسؤولية توفير التوجيه القيادي فيما تعلق بالتعاون الشرطي في قارة إفريقيا، ومن أهم المهام التي تناط بها المتصلة بالردع الإلكتروني تتمثل في:

- وضع تنفيذ مشروع الميزانية والهيكل المقترح الأفريبول، من أجل تعزيز دور هذه الآلية الإلكترونية وجر منهما على أجهزة السياسة للاتحاد الإفريقي وفقا للنظم واللوائح المالية للاتحاد

- وضع وتنفيذ والإشراف على السياسات المتعلقة بمجابهة الإجرام الإلكتروني داخل القارة الإفريقية وإعداد الخطوط التوجيهية وتحديد أولويات تعمل الأفريبول في هذا المجال.

- إعداد تقرير سنوي عن عملها وتقديمه إلى أجهزة صنع السياسة للاتحاد الإفريقي من خلال اللجنة الفنية المتخصصة للدفاع والسلامة الأمن[2].

[1] - ودرار أمين، المرجع السابق، ص ص 137، 138.

[2] - عبد العزيز لزعر، رشيد زياني، «آلية الاتحاد الإفريقي للتعاون الشرطي(الأفريبول)) ودورها في مكافحة الإلكترونية»، مجلة المتون، المجلد 14ن العدد03، جامعة سعيدة، 2021، ص255

ب-لجنة التوجيه لآلية الاتحاد الإفريقي للتعاون الشرطي

وتتكون لجنة التوجيه لآلية الاتحاد الإفريقي للتعاون الشرطي أفريبول من خمسة أعضاء، وهم:

مفوض السلم والأمن للاتحاد الإفريقي.

رؤساء المنظمات الإقليمية للتعاون الشرطي.

المدير التنفيذي لآلية الاتحاد الإفريقي للتعاون الشرطي.

ويترأس لجنة التوجيه رئيس الجمعية العامة، تحدد وظائف اللجنة ومعدلات اجتماعاتها وإجراءاتها بموجب قواعد الإجراءات[1].

ج- الأمانة

تتأسس أمانة لآلية الأفريبول على نحو تالي، حيث يتولى المدير المسؤولية التنفيذية وتقديم التقارير لمفوضية الأمن والسلم بالاتحاد الإفريقي، ويتم تعيين المدير بواسطة الجمعية العامة التي تتألف من رؤساء الشرطة للدول الأعضاء، وتشمل مهام الأمانة العامة ضمان الإدارة الفعالة للآلية وعقد الاجتماعات والتواصل مع السلطات المعنية بإنفاذ القانون[2].

الفرع الثاني: دور آلية الإتحاد الإفريقي للتعاون الشرطي في مكافحة الجريمة الإلكترونية

عملت الأفريبول لمكافحة الجريمة الإلكترونية بإنشاء ثلاث فرق تتكفل بمكافحة ثلاث جرائم ومنها الجريمة السيبرانية كذلك على مكافحتها إقليميا وذلك بتعزيز التعاون الشرطي وتبادل الخبرات كما دعمت الإنتربول الافريبول لمواجهة هذه الجريمة وهذا ما سنراه في هذا الفرع.

أولا: الجانب العملي للأفريبول لمكافحة الجريمة الإلكترونية

أ-إنشاء ثلاث فرق عمل تتكفل بمكافحة الجريمة العابرة للحدود والجريمة السيبرانية وكذا مكافحة الإرهاب والوقاية منه: حيث أن الجمعية العامة الثانية للأفريبول في ختام أشغالها بالجزائر العاصمة 19 أكتوبر 2008 قررت إنشاء ثلاث فرق عمل تتكفل بالجرائم الثلاثة

[1] -عبد العزيز لزعر، رشيد زياني، المرجع السابق، ص255.

[2] -المرجع نفسه، ص256.

والتطرف العنيف والوقاية منه، مع تسجيل بعض المقترحات العملية لكيفية التعامل مع هاته الظواهر، في كل الدول الإفريقية المعنية[1].

ب- تدعيم وتفعيل جهاز الاتصالات "فسيكوم"

أوصت الجمعية بتدعيم وتسريع وتفعيل جهاز الاتصالات "فسيكوم" لدى كافة أجهزة شرطة الدول الأعضاء بهدف تبادل المعلومات والوثائق بينهما، كما سجل الاجتماع ارتياح لما حققته الأفريبول في ظرف قصير جدا على غرار تنظيم 3 دورات تكوينية لخبراء شرطة الدول الأعضاء بالجزائر وتزويد عدد من أجهزة الشرطة إفريقيا.

ج- تفعيل الأفريبول من خلال تنظيم الاجتماعات وننقل الخبرات وتجهيزها بأحدث التقنيات

كما فند المفتش العام للشرطة الأنغولية" ألفريدو إدواردو مانويل مينكاس" والذي يشغل أيضا منصب رئيس منظمة التعاون الإقليمي لرؤساء أجهزة الشرط في إفريقيا الجنوبية، الدور الفعال لآلية الأفريبول في مجال ترقية التعاون والتنسيق الأمني لمكافحة الجريمة والحفاظ على أمن المواطنين وحماية الممتلكات، مشيدا بمجهود الجزائر في تفعيل آلية الإتحاد الإفريقي للتعاون الشرطي أفريبول، كما نوه بالتجربة المتميزة للشرطة الجزائرية[2].

كما كشفت شركة كاسبرسكي المتخصصة في أمن أجهزة الكمبيوتر أن الربع الأول من عام 2014 شهد وقوع ما يزيد على49 مليون هجوم إلكتروني في إفريقيا وجرى أكثر في الجزائر ومصر، جنوب إفريقيا وكينيا، وعلى ذلك فقد تم إبرام اتفاقية بين الدول الأعضاء في الإتحاد الإفريقي، وقد تم من خلال هذه الاتفاقية تحديد التوجهات العامة والإستراتيجية لمكافحة الجريمة الإلكترونية في إفريقيا[3].

من التوصيات التي دعا إليها المشاركون في الدورة العاشرة لمنتدى الأمن بإفريقيا التي اختتمت أشغالها في فبراير 2010 بمراكش المغربية إلى إحداث مرصدا إفريقي للأمن الإلكتروني تكمن مهمته في التنسيق بين الدول الأعضاء في الإتحاد الإفريقي في التصدي للجريمة الإلكترونية

[1] -أحلام بوكربوعة، «آلية الإتحاد الإفريقي للتعاون الشرطي "أفريبول "ودورها في مكافحة ظاهرة الإرهاب»، حوليات، المجلد 34، العدد 04، جامعة الجزائر، 2020، ص641.

[2] - أحلام بوكربوعة، المرجع السابق، ص641.

[3] - عبد العزيز لزعر، رشيد زياني، المرجع السابق، ص 255.

وتبادل المعلومات كما دعو إلى معالجة الثغرات التي تحول دون ذلك من خلال توحيد التشريعات والسياسات العمومية من أجل أمن إلكتروني إفريقي[1].

بما أن الجزائر وباعتبار المكانة التي تحتلها في القارة الإفريقية ليست بمنأى عن هذه التهديدات فقد عملت الجزائر على تعزيز البنية التحتية الرقمية، وتطوير التقنيات الحديثة لمكافحة الجرائم الإلكترونية. هذا يشمل تحديث أنظمة الاتصالات والشبكات الحاسوبية، وتعزيز الأمن السيبراني من خلال تطوير البرمجيات والحلول التقنية المتطورة بالإضافة إلى توفير التدريب والتوعية للموظفين والمجتمع بشأن مخاطر الجرائم الإلكترونية وكيفية التعامل معها[2].

ثانيا: التعاون الدولي بين الإنتربول والإتحاد الإفريقي للتعاون الشرطي لتعزيز مكافحة الجريمة الإلكترونية

يعمل الإنتربول والاتحاد الأفريقي يدا بيد بشأن المسائل ذات الاهتمام المشترك، ويتبادلان الموارد والخبرات، ويضعان ردودا مشتركة لتلبية احتياجات العمل الشرطي في أفريقيا. وأضفي طابع رسمي على هذا التعاون القائم بتوقيع مذكرة تفاهم بين الاتحاد الأفريقي والإنتربول في عام 2011.، وفي عام 2019، وقّع اتفاق تعاون مع الاتحاد الأفريقي لتحقيق التكامل بين الإنتربول وأفريبول وتفادي ازدواجية الجهود لدى البلدان الأعضاء المشتركة بين المنظمتين وتعزيز أوجه التآزر[3].

كما دعمت الإنتربول الافريبول ببرنامج ispa وبدأ تنفيذ هذا البرنامج سنة 2020 لفترة أولية امتدت حتى مارس 2023، وجرى تمديدها حتى ديسمبر 2026 ومن أهداف هذا البرنامج:

1. تعزيز إطار الحوكمة في أفريبول عن طريق تقديم المشورة الاستراتيجية والميدانية والقانونية، وتوفير الدعم في مجال حماية البيانات

2. تحسين قدرات أفريبول على تفكيك الشبكات الإجرامية الضالعة في الإرهاب، والجريمة المنظمة والناشئة والجريمة السيبرانية، والجريمة المالية.

---

[1] – عبد العزيز لزعر، رشيد زياني، المرجع السابق، ص 255.

[2] –المرجع نفسه، ص255.

[3] – مقال منشور على الموقع الكتروني، «الدعم المقدم إلى أفريبول»، تم نشره ماي 2023، تم الاطلاع عليه بتاريخ: 28-05-2024، على الساعة 17:54، في الموقع: https://www.interpol.int/ar/5/4/1

3. استحداث منظومة أفريبول للمعلومات وتعزيز التواصل عن طريق توفير الدعم التقني وتوسيع نطاق الوصول إلى منظومة الإنتربول العالمية للاتصالات الشرطية المأمونة 24/7-1+.

4. دعم وحدة أفريبول لتحليل بيانات الاستخبارات الجنائية من خلال توفير معدات تقنية وتقديم برامج تدريبية وتوجيهية مصممة حسب الاحتياجات.

5. بناء قدرات البلدان الأعضاء المشتركة بين أفريبول والإنتربول من خلال تقييم الاحتياجات والأولويات وتنظيم حلقات عمل.

وفي ماي 2023 دعمت الانتربول الافريبول على إقامة مركز بيانات في إطار تعزيز قدراتها العملياتية وتسيير التعاون الأمني الإقليمي وهذه البنية الأساسية؛ أقيمت في الجزائر في 17 ماي ستساعد على تبادل المعلومات عبر المنظومة الإفريقية للاتصالات الشرطية(afsecom)[1].

إلا أن ذلك يعتبر غير كاف فكان من اللازم تعزيز التعاون الاستراتيجي مع الآلية الدولية الشرطية نظرا للخبرات التي يتمتع بها أعضاءها وكذا اتساع نشاطها ليشمل كافة دول العالم خلافا للآلية الإفريقية التي يكمن نشاطها في الحيز الإفريقي فقط، وهو الأمر الذي يسهم في ضمان التشغيل البيني والتفاعل بين النظم المعلوماتية لكل من "الإنتربول" و"الأفريبول"[2].

المبحث الثاني: دور منظمة الشرطة الجنائية الدولية لمكافحة الجريمة الإلكترونية

إن الجريمة المعلوماتية بالغة الخطورة والانتشار، كما ذكرنا سابقا، بأنها عابرة للحدود الوطنية وبالتالي أصبحت وبالتالي أصبحت تهدد جميع دول العالم مجابهتها من خلال التعاون الشرطي لأنه لا يكفي سن قوانين فقط لتجريمها ، نظرا لحداثتها وارتباطها بالتكنولوجيا وهو الأمر الذي يفرض على جميع الدول العالم أن تعمل على مجابهتها لذلك ظهر ما يسمى بالمنطقة الدولية الشرطية الجنائية، والتي تعد أهم جهاز عالمي متخصص في مجال مكافحة الجريمة المعلوماتية والإرهاب الدولي، وهذا ما سيتم معالجته من خلال هذا المبحث، حيث قسمناه إلى

[1] – مقال منشور على الموقع الكتروني، «الدعم المقدم إلى أفريبول»، تم نشره ماي 2023، تم الاطلاع عليه بتاريخ: 28-05-2024، على الساعة 10:52 م، في الموقع: https://www.interpol.int/ar/5/4/1

[2] – عبد العزيز لزعر، رشيد زياني، المرجع السابق، ص 258.

مطلبين، المطلب الأول نشأة منظمة الشرطة الجنائية الدولية، والمطلب الثاني دور منظمة الشرطة الدولية لمكافحة الجريمة الإلكترونية.

المطلب الأول: مفهوم المنظمة الدولية للشرطة الجنائية

المنظمة الدولية للشرطة الجنائية الإنتربول من أبرز الأجهزة وأهمها للتعاون الشرطي الدولي فهي ترتبط بالعديد من الهيئات الإقليمية والدولية، كما أصبحت الدول الآن في حاجة ماسة للتعاون الشرطي الدولي، وهذا ما سوف نعالجه في هذا المطلب، حيث خصصنا الفرع الأول تعريفها وطبيعتها القانونية والفرع لثاني مبادئ واختصاصات وأهداف الأنتربول.

الفرع الأول: المنظمة الدولية للشرطة الجنائية وطبيعتها القانونية

أولا: تعريف المنظمة الدولية للشرطة

المنظمة الدولية للشرطة الجنائية، لها دور بارز في تعزيز التعاون الشرطي الدولي في مكافحة الجريمة الإلكترونية، كما أن تاريخه وأهدافه تشكل جزءا أساسيا في فهم كيفية تعاون الدول على مستوى عالمي وهذا ما سيتم شرحه أكثر في هذا الفرع.

يكاد يجمع المختصين على أن تأسيس هذه المنظمة يعود إلى عام 1923في مؤتمر فينا المتعقد ما بين 03 و07 سبتمبر 1923 (يوها نزشوبار الذي كان يرأس شرطة فينا[1]).

وتلبية لدعوة من الأمير ألبرت الأول يوناكو، ناقش محامون ومسؤولو شرطة من 24 بلدا مسألة التعاون لفك لغز الجرائم وأساليب كشف المجرمين وعمليات تسليمهم وهي منظمة حكومية دولية منها ل 196 بلدا عضوا[2].

ويقع مقر المنظمة حسب المادة الأولى من القانون الأساسي للمنظمة في العاصمة الفرنسية باريس، وينظم الوضع القانوني للمقر اتفاقية دولية أبرمت بين المنظمة والحكومة الفرنسية سنة 1972 وجددت في 03 نوفمبر 1982 ،ويتمتع مقر المنظمة بالحصانة الدولية، وتوفر له الحماية اللازمة من قبل الحكومة الفرنسية من أي اعتداء يطال المبنى أو العاملين فيه باعتبارهم موظفين دوليين يتمتعون بالحماية والحصانة الدبلوماسية وفقا للاتفاقية المبرمة بين الطرفين، والاتفاقيات

[1] –رحموني محمد، «منظمة الشرطة الجنائية الدولية (الإنتربول) آلية لمكافحة الجريمة المنظمة»، مجلة الآفاق العلمية، المجلد11، العدد04، المركز الجامعي تامنغست، 2011، ص62.

[2] – مقال منشور على الموقع الكتروني، «الدعم المقدم إلى أفريبول»، تم نشره ماي 2023، تم الاطلاع عليه بتاريخ: 28-05-2024، على الساعة 10:52 م، في الموقع: https://www.interpol.int/ar/5/4/1

الدولية الأخرى ذات الصلة بموضوع الحصانات، كما أن العضوية بالمنظمة مفتوحة لكل دولة بشرط قبول الجمعية العامة بأغلبية خاصة، وهذا ما قضت به المادة الرابعة 04 من القانون الأساسي للمنظمة وما يمكن الإشارة إليه، أنه بخصوص انقضاء العضوية، فإن القانون الأساسي للمنظمة لم يشر إلى ذلك بأي وجه من الأوجه، وهذا يدل على حرص المنظمة على زيادة عدد أعضاءها مما يساعدها في تحقيق الغرض الذي أنشأت من أجله[1].

ثانيا: الطبيعة القانونية للمنظمة الدولية لشرطة الجنائية

ذهب إلى تحديد الطبيعة القانونية للأنتربول اتجاهين الأول يرى أنه من أشخاص القانون الخاص، بينما الثاني يعتبر المنظمة من أشخاص القانون الدولي:

الاتجاه الأول: يرى هذا الاتجاه أن المنظمة من أشخاص القانون الخاص، أي غير حكومية، وذلك للاعتبار ات التالية:

أ. قرار المجلس الاقتصادي والاجتماعي التابع لهيئة الأمم المتحدة لسنة 1949، الذي اعتبر فيه المنظمة غير حكومية وذات طابع استشاري.

ب. اقتصار اختصاص المنظمة على الجانب الجنائي فقط دون التدخل في الأمور السياسية والعسكرية والدينية والعرقية، التي هي من اختصاص الحكومات.

ت. إن الاتفاق المنشئ للمنظمة تم بناء أًعلى موافقة سلطات الشرطة في كل دولة ليسوا، الحكومات، وهذا يتناقض مع قرار المجلس الاقتصادي والاجتماعي في هذا الشأن.

الاتجاه الثاني: يرى هذا الاتجاه أن المنظمة الدولية للشرطة الجنائية عبارة عن منظمة دولية حكومية، وبالتالي فهي شخص من أشخاص القانون الدولي العام، الذي يقوم على عدة عناصر يجب توافرها و: هي الكيان المميز الدائم (الإرادة الذاتية) الاستناد إلى اتفاقية دولية تنشئ المنظمة وتحدد نظامها القانوني، عدم انتقاص المنظمة من سيادة الدول المشتركة في عضويتها[2].

[1] – رحموني محمد، المرجع السابق، ص63.

[2] –حليمة خزار، «المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب»، مجلة الدراسات القانونية المقارنة، المجلد02، العدد01، جامعة شلف، 2016، ص ص 154،153.

أ. الكيان الدائم: إن إ طلاق اسم " منظمة" على الأنتربول يعبر عن انصراف إرادة منشئها إلى دمغها بطابع الدوام، شأنها في ذلك شأن أي منظمة دولية حكومية إضافة إلى الأجهزة التي تقوم عليها والتي تمارس نشاطاتها على طريقتها باستمرار.

ب. الإرادة الذاتية: تمتلك المنظمة الشخصية القانونية الدولية ، لكونها تتمتع بإرادة تميزها عن إرادات الدول الأعضاء ، والتي تظهر في مجال العلاقات الدولية الغامضة للقانون الدولي العام، كقيام الأنتربول بإبرام اتفاقية التعاون مع هيئة الأمم المتحدة سنة 1971، ويعرف هذا الاتفاق بالأنتربول كمنظمة دولية مقرها كما تبدو جليا الشخصية القانونية للأنتربول في مجال داخل الأراضي الفرنسية13 القانون الداخلي ، والذي يتجسد في الأجهزة الفرعية اللازمة لقيامها بمهامها، كما أن لها الحق في وضع القواعد المنظمة لمواردها ونفقاتها وميزانيتها.

ت. عدم انتقاص المنظمة من سيادة الدول المشتركة في عضويتها باعتبار ها في الواقع مجرد وسيلة من وسائل التعاون الاختيار ي بين مجموعة من الدول في مجالات يتفق عليها سلفا في الاتفاق المنشئ للأنتربول.

ث. الاستناد إلى اتفاقية دولية تنشئ المنظمة وتحدد نظامها القانوني، وتبين أهدافها واختصاصاتها، والأجهزة المختلفة المنوط لها تحقيق هذه الأهداف، والقواعد التي تحكم سير العمل عليها، وتطبيق هذه الحالة على الأنتربول قد يثير الشك في كون الأنتربول منظمة دولية حكومية، لكن الثابت أن المنظمة الدولية للشرطة الجنائية نشأت بمقتضى وثيقة أطلق عليها اسم "الدستور"، وأقرها مؤتمر ضم ممثلين لأجهزة الشرطة في دول المؤتمر وهؤلاء الممثلين إما أعموا فوضوا من قبل دولهم من أجل وضع هذا الدستور ، ومن ثم يعتبر معاهدة دولية بالمعنى السليم، وإما أنهم تصرفوا بصفتهم الشخصية ، وفي هذه الحالة لا تعتبر الدستور بمثابة الاتفاقية الدولية[1].

[1] –خراز حليمة، المرجع السابق، ص ص153، 154.

الفرع الثاني مبادئ واختصاصات وأهداف الأنتربول

تشمل المنظمة الدولية للشرطة الجنائية على عدة مبادئ تتميز بها عن باقي المنظمات كما للمنظمة الدولية اختصاصات وأهداف وسوف نعالجها من خلال هذا الفرع.

أولا: مبادئ الأنتربول

تعتمد المنظمة على مجموعة من المبادئ تحكمها منها ما يحدد علاقتها مع الدول الأعضاء ومنها ما يحدد طريقة ممارسة عملها ومن بين أهم المبادئ التي أجمع عليها الفقه الدولي:

-احترام مبدأ السيادة الوطنية:

هذا المبدأ يعتبر من أهم المبادئ التي تقوم عليها هذه المنظمة لأنه يلزم على احترام إرادة الدول الأعضاء ويكون ذلك ضمن احترام التشريعات والنظم الوطنية للدول[1].

-مبدأ المعاملة بالمثل الدول الأعضاء: يقوم هذا المبدأ على المساواة القانونية بين أشخاص القانون، وبما أن المنظمة الدولية للشرطة الجنائية كيانا دوليا تتعاون من خلاله أجهزة الشرطة في عدة دول ولا يتم التعاون إلا في إطار احترام هذا المبدأ، وكذا مبدأ مكافحة جرائم القانون العام فقط، حيث أشار دستور المنظمة الدولية للشرطة الجنائية إلى أنه يهدف إلى إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام وفي مكافحتها، كذلك أشار الميثاق أنه يحظر على المنظمة حظرا باتا أن تنشط وتتدخل في مسائل أو شؤون ذات طابع سياسي[2].

ثانيا: اختصاصات الأنتربول

تتولى الأنتربول الاختصاصات التالية:

يتألف من الأمانة العامة وهي التي تتولى تنسيق أنشطة الإنتربول اليومية لمكافحة مجموعة من الجرائم ويديرها الأمن العام، كما يعمل في الأمن العام ضباط شرطة والمدنيين، وهي تتخذ من ليون مقرا لها، ولها مجمع عالمي للابتكار في سنغافورة ولها العديد من المكاتب الفرعية في مناطق مختلفة من العالم، و المكتب المركزي الوطني للإنتربول يشكل نقطة أساسية للأمانة

[1] -حيدر علي حسن نبات السويعدي، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب السيبراني، مذكرة لنيل شهادة ماجستير، قانون العام، كلية القانون، جامعة كربلاء، العراق، 2023. ص 26.

[2] – المرجع نفسه، ص28..

العامة، والمكاتب المركزية الوطنية الأخرى، وتكون تابعة للوزارة الحكومية المسؤولة عن العمل الشرطي، أما الجمعية العامة هي هيئة إدارية العليا لدى الأنتربول والتي تجمع كافة البلدان مرة في السنة لاتخاذ القرارات[1].

ثالثا: أهداف المنظمة الدولية للشرطة الجنائية

تكمن أهداف هذه المنظمة في:

تسعى المنظمة لضمان حصول أجهزة الشرطة في العالم كافة على الأدوات والخدمات اللازمة لها لتأدية مهامها بفعالية، كما تساعد المنظمة أجهزة الشرطة وعناصرها في إدراك توجهات الإجرام على نحو أفضل، وتحليل المعلومات، وتنفيذ العمليات بغاية توقيف أكبر عدد من المجرمين[2].

تنسيق جهود بين الدول الأعضاء خاصة في مجال مسألة هروب المجرمين، كما وضعت الأمانة العامة للإنتربول في متناول الدول الأعضاء مجموعة من الأدوات الفنية والتقنيات التكنولوجية الحديثة لمكافحة الجريمة وملاحقتها، من أهم منظوماتها، منظومة الاتصالات أنتربول 24/7-1+، كما تمكن البريد المركزي الوطني-أنتربول الجزائر-من تحقيق الربط بين هذه المنظومة بتاريخ 21 أوت2003 [3].

إقامة وتنمية نظم قمع الوقاية من جرائم القانون العام من خلال مساهمتها في تشجيع البلدان على إنشاء أجهزة متحضرة في قمع الجرائم، بتقديمها لخدمات الدعم الشرطي وعقدها دورات لتدريب الأعوان، كما تدعم مبادرات تعديل وتلقيح القوانين الوطنية[4].

المعونة في مجال المساعدات التقنية وتبادل الخبرات، حيث ينبغي التعاون والمساعدة المتبادلة في المسائل المتعلقة بالجريمة عبر الحدود الوطنية الخطيرة حسب الاقتضاء أن يشمل

---

[1] - مقال منشور على الموقع الكتروني، «صحيفة الأيام البحرينية»، تم نشره ماي 2023، تم الاطلاع عليه بتاريخ: 28-05-2024، على الساعة 10:52 م، في الموقع:

=https://www.alayam.com/home/getnewsdesc?intNewsMainID=op2HnaarJ/g

[2] - محمد قسيمة، «الوسائل الفنية للمنظمة الدولية للشرطة الجنائية (الأنتربول) كآلية للتعاون الدولي الشرطي»، حوليات، مجلد 34، العدد02، جامعة الجزائر 01، 2020 ص128.

[3] -المرجع نفسه، ص128.

[4] - المرجع نفسه، ص129.

أيضا تدعيم نظم تبادل المعلومات بين الدول الأعضاء وتقديم المساعدات التقنية الثنائية والمتعددة، كذلك من أهدافها إنماء قدرات الكوادر المتخصصة بمكافحة الجرائم ورفع كفاءاتهم[1].

المطلب الثاني: دور منظمة الشرطة الدولية لمكافحة الجريمة الإلكترونية

تلعب الأنتربول دورا هاما في مكافحة الجريمة الإلكترونية فاهي تعمل على تعزيز التعاون الدولي وتساهم في مكافحة لجرائم العابرة للحدود، وهذا ما يميز الطابع الإجرامي للهجمات السيبرانية، وهذا ما سوف نعالجه فب في الفرع الأول وكذلك حققت هذه المنظمة إنجازات في مكافحة الجريمة الإلكترونية وهذا ما خصصناه في الفرع الثاني أما بالنسبة للفرع الثالث خصصناه لشرطة الويب الدولية وهي التي تعتبر من كيانات هذه المنظمة.

الفرع الأول: دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة الإلكترونية

أولا: أسس التعاون الشرطي الدولي لمكافحة الجريمة الإلكترونية

بالنظر إلى الطبيعة الخاصة للجرائم التي تنشأ وتقع في بيئة شبكة الإنترنت فإن التعاون الأمني الدولي في سبيل مكافحة هذه الأنماط الإجرامية، يجب أن يعتمد على آليات متطورة تواكب تطور هذه الجرائم، ويجب أن يتم هذا التعاون الدولي على أسس معينة تكفل في نهاية الأمر مكافحة هذه الجرائم بصورة بناءة، وعلى هذا فإن التعاون الأمني الدولي في مجال المكافحة والوقاية من جرائم الإنترنت يجب أن يقوم على الأسس التالية:

أ. التناول العلمي لبحث ظاهرة جرائم الإنترنت، وتوفير المعلومات الإحصائية والبيانات اللازمة، سواء مايتعلق بالجريمة ذاتها أو حيث إن هذه المعلومات تساعد على التعامل مع جرائم الإنترنت وفهم كل أبعاد هذه الجرائم، إنشاء مركز دولي للمعلومات والبيانات الخاصة بتلك الجرائم على مختلف صورها وأنماطها، والمتورطين معهم، والتحقيقات.

ب. التنسيق بين المؤسسات الأمنية بآلياتها المختلفة في الساحات الأمنية، الإقليمية والدولية، بما يحقق حصر معدلات الجريمة، ويحول دون استفحالها واستكمال أي نقص في المعلومات وذلك بالتعاون لتجميع عناصر تلك المعلومات، بها في النهابة كشف

[1] –حيدر علي حسن نبات السويعدي، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب السيبراني، مذكرة لنيل شهادة ماجستير، قانون العام، كلية القانون، جامعة كربلاء، العراق، 2023، ص 33.

أبعاد الجرائم وخطط لإعداد ارتكابها، وإتاحة الفرصة لإمكان دراسة الثغرات الأمنية الدولية والعمل على إيجاد أفضل أساليب التعديل منعا للجريمة وضبطا لجناتها.

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

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

ج. وضع استراتيجيات وقائية قادرة على خلق المناخ الملائم لأعمال المكافحة وتضييق الخناق على أنشطة تلك المنظمات الإجرامية، وحرمانها من البيئة الملائمة لممارسة أنشطتهم الإجرامية[1].

ثانيا: صور التعاون الشرطي الدولي لمكافحة الجرائم الإلكترونية:

أ–ربط شبكة الاتصال والمعلومات:

تحتاج الاتصالات الشرطية إلى وسائل للاتصال تحقق السرعة الملائمة لتتمكن أجهزة العدالة الجنائية من التواصل بين سلطات التحقيق لذا عمدت الدول والمنظمات الدولية تطوير الاتصال وتبادل المعلومات فيما بينها.

ب–لقيام ببعض العمليات الشرطية والأمنية المشتركة:

تعقب المجرم المعلوماتي وتعقب الأدلة الرقمية وضبطها، التفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثا عما قد تحويه من أدلة وبراهين على ارتكاب كلها أمور تستدعي القيام ببعض العمليات الشرطية[2]

ثالثا: إستراتيجية التعاون الشرطي الدولي لمكافحة الجريمة الإلكترونية

ففي عام 2004، أنشأت منظمة" الإنتربول "وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى(G8) بوضع استراتيجيات لمواجهة هذا

[1] –خراشي، عادل عبد العال إبراهيم، إشكالات التعاون الدولي في مكافحة الجريمة المعلوماتية، دط، دار الجامعة الجديدة، مصر، 2015، ص193.

[2] – المرجع نفسه، ص194.

النوع من الجرائم، من خلال إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة و7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف، كما استخدمت الإنتربول وسائل حديثة لمكافحة هذه الجريمة، كاستخدام قاعدة البيانات، وهي عبارة عن جملة من الملفات والقوائم تحتوي على معلومات مهملة كقاعدة بيانات الإسمية وقاعدة وثائق السفر، وقاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف، من خلال استخدام برنامج التحليل والمقارنة لتلك الصور، وتزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها، وتبحث الشرطة قواعد الأنتربول أكثر من 20 مليون مرة كل يوم أي ما يعادل 250 عملية بحث في الثانية[1].

وبهذا فإن شرطة الإنتربول تعد منظومة عالمية تختص بمكافحة الجرائم الدولية والعابرة للحدود الوطنية للدول، بما فيها الجرائم المعلوماتية، ما أكدته نتائج الدورة رقم (77) للجمعية العامة لمنظمة الإنتربول

حيث دعا الأمين العام للإنتربول السيد "بونالد نوبل" جميع الحكومات والدول لدعم وتطوير نظم تبادل المعلومات حول المشتبه بهم ومحاربة الإرهاب المتنامي في كل أنحاء العالم بكل صوره بما فيه الإرهاب وقد نجحت المنظمة الدولية للشرطة الجنائية- الإنتربول خلال الأعوام الأخيرة في جعل اسمها من أكثر الأسماء التي يخشاها.

كما نظم الأنتربول دورات تدريبية ومؤتمرات دولية لمكافحة الجرائم الإلكترونية أهمها:

أولا- الدورات التدريبية

ينظم الأنتربول دورات تدريبة سنوية، بهدف تبادل الخبرات ومن أهم هذه الدورات دورة سنغافورة من 17إلى 19 سبتمبر 2019، وهذه الدورة كانت إلكترونية بأكملها وموجهة للشرطة والأجهزة القضائية، أهم ما جاءت به هذه الدورة فهم الأدلة الرقمية وكيفية استخدامها في ملاحقات القضائية، شارك في دورة التدريب الإلكتروني حوالي 65 شخصا من 30 بلدا، وقدم فيها خبراء

[1] -طاهر ياكر، «مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية»، مجلة الصدى للدراسات القانونية والسياسية، المجلد 01، العدد01، جامعة خميس مليانة، الجزائر، 2022، ص16.

في المجالات ذات الصلة مجموعة من الدروس، كما شملت هذه الدورة أصول التحقيق في الشبكة الخفية ومقدمة إلى علوم الأدلة الجنائية الرقمية[1].

وكذلك دورة الأنتربول يطلق الأكاديمية الافتراضية لتسيير تدريب الشرطة خلال الكوفيد 19 ومن بين مواضيع هذه الدورة العملات المشفرة والجريمة السيبرية والشبكة الخفية[2].

كما نظمت الأنتربول مؤتمرات سنوية بهدف تبادل الخبرات ومن أهم هذه المؤتمرات:

مؤتمر سنغافورة من 28 إلى 30 سبتمبر 2016، اجتمع في هذا المؤتمر خبراء في الأمن السيبيري من أجهزة إنفاذ القانون والقطاع الخاص والأوساط الأكاديمية للعمل معا من أجل تذليل الصعوبات التي تعترض كشف مرتكبي الجرائم السيبرية، وتحت عنوان Solutions for Attribution (حلول لكشف الجناة)، يتبادل حوالى 200 مندوب من 56 بلدا أفضل الممارسات في هذا المجال ويبحثون لصالح أجهزة إنفاذ القانون في سبل تذليل العقبات التقنية والميدانية والاستراتيجية التي تعترضها عند التحقيق في الجرائم السيبرية والجرائم التي تسهّل الإنترنت ارتكابها، من جرائم مالية وأنشطة متصلة بالإرهاب واعتداءات جنسية على الأطفال، وكذا مؤتمر الانتربول واليوروبول لمكافحة الجريمة السريانية: من 09إلى 11كتوبر ركز هذا المؤتمر على التطورات الجديدة في التكنولوجيا التي يمكن أن يستغلها المجرمون كما شمل هذا المؤتمر فوائد وتحريات الذكاء الاصطناعي بالنسبة للشرطة والآثار المحتملة لتكنولوجيا الجيل الخامس G5 كذلك الوصول إلى الأدلة الإلكترونية عبر الحدود[3].

نظمت الانتربول أيضا مؤتمرات سنوية بهدف تبادل الخبرات ومن أهم هذه المؤتمرات مؤتمر الانتربول الثاني لمكافحة الإتجار بالبشر وتهريب المهاجرين من14 إلى 15 نوفمبر 17 2017 بمدينة ليون الفرنسية، أكد فيه المشاركون على ضرورة البدء بالعملية اللازمة لتحديد الدور

---

[1] -شعبان لامية، الجهود الدولية في مكافحة الاتجار بالبشر عبر الانترنت، أطروحة لنيل شهادة دكتوراه علوم، قمس الحقوق، جامعة العربي تبسي، تبسة، 2019-2020، ص344.

[2] -- مقال منشور على الموقع الكتروني، «كشف مرتكبي الجرائم السيبرية في صميم المناقشات في مؤتمر الإنتربول واليوروبول»، تم نشره 28 سبتمبر 2017، تم الاطلاع عليه بتاريخ: 30-05-2024، على الساعة 10:52 م، في الموقع: https://www.interpol.int/ar/1/1/2016/17

[3] – مقال منشور على الموقع الكتروني، «كشف مرتكبي الجرائم السيبرية في صميم المناقشات في مؤتمر الإنتربول واليوروبول»، تم نشره 28 سبتمبر 2017، تم الاطلاع عليه بتاريخ: 30-05-2024، على الساعة 10:52 م، في الموقع: https://www.interpol.int/ar/1/1/2016/17

الذي تلعبه شركة الانترنت في قضايا الاتجار بالبشر وتضمن المؤتمر البحث عن حلول مبتكرة لجمع المعلومات استخباراتية تشغيلية من الإنترنت فيما يتعلق بعمليات الإتجار بالبشر عن طريق الأنترنت[1].

الفرع الثاني: الإنجازات التي حققتها الأنتربول لمكافحة الجريمة الإلكتروني

لقد حققت الإنتربول إنجازات عديدة أهمها:

إن من بين الإنجازات التي حققها الإنتربول، في ظل مواجهة الجرائم المعلوماتية التي قامت بها المباحث الفيديرالية الأمريكية، بالاشتراك مع الإنتربول والمتعلقة بملاحقة الشخص الذي نشر دودة الحب غير الانترنت في فلبين، وكذلك العملية التي قامت بها شرطة الأنتربول بالاشتراك مع المباحث الفيدرالية، وكذا الشرطة الإنجليزية عام 1998 والتي أحرزت فيها إنجازات كبيرة، من خلال تفكيك منشور عليه أكثر من 75000 صورة سلبية لدعارة الأطفال[2].

وعلى غرار هذه المنظمة، أنشأ المجلس الأوربي عام 1991م في لكسمبورج، شرطة أوربية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول الأطراف، لملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالأنترنت[3].

كذلك عملياتCyber surge التي قادها الإنتربول في مناطق مختلفة، استهدفت أنشطة جبائية منظمة في الفضاء السيبيري، كما جمعت هذه العمليات محققين للعمل معا، استنادا إلى معلومات عن تهديدات جرى كشفها بالتعاون مع شركاء من القطاع الخاص، وبعد كشف عمليات قرصنة لتعدين العملات المشفّرة على الصعيد العالمي تستغل هشاشة موجِّهات MikroTic، نسق الإنتربول عملية Goldfish Alpha في جنوب شرق آسيا التي كشفت بداية عن أكثر من 20000 موجِّه مقرصن. وتعاون محققون وخبراء في مكافحة الجريمة السيبرية من أجهزة الشرطة والأفرقة الوطنية للتصدي للطوارئ الحاسوبية في المنطقة من أجل تحديد مكان الموجِّهات الملوثة[4].

---

[1] – شعبان لامية، المرجع السابق، ص342.

[2] –طاهر ياكر، المرجع السابق، ص16

[3] – طاهر ياكر، المرجع السابق، ص16

[4]– مقال منشور على الموقع الكتروني، «عمليات مكافحة الجريمة السيبرية»، تم الاطلاع عليه بتاريخ: 30-05-2024، على الساعة 10:52 م، في الموقع: https://www.interpol.int/ar/4/6/2

الفرع الثالث شرطة الويب الدولية

في الأصل هذه المنظمة تابعة لمنظمة الأنتربول وفي هذا ما سنشرحه أكثر في هذا لفرع.

أنشئت هذه المنظمة الأمنية في الولايات المتحدة الأمريكية عام 1986 لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة إلكترونيا والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة، ويضم فريق العمل بهذه المنظمة متخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من 61 دولة حول العالم، ونظرا لاتساع نشاط هذه المنظمة وما 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 وفي 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 وحقوق الإنسان من ناحية وإلا تستخدم الشبكة لأغراض إجرامية أو نشر مواد إباحية تسيء إلى المجتمع من ناحية أخرى[1].

[1] -- طاهر ياكر، المرجع السابق، ص17.

خلاصة

الفصـــــــل الثاني

خلاصة الفصل الثاني:

عند ختام هذا الفصل نستخلص أن: التعاون الشرطي في مكافحة الجريمة الإلكترونية يعتبر أساسيا في عصرنا الحالي، حيث تتجاوز الجرائم الإلكترونية الحدود الجغرافية وتتطلب استجابة سريعة ومتناسقة، يشمل هذا التعاون تبادل المعلومات والخبرات بين الجهات الشرطية في مختلف الدول، وإقامة شراكات مع القطاع الخاص والمؤسسات الدولية وتنسيق الجهود لتطوير استراتيجيات فعالة لمكافحة هذه الجرائم.

توجد أدوات ومنصات إلكترونية تسهل هذا التعاون وتساعد في تحديد الأنشطة الإجرامية وتتبع المتورطين بها.

تحديث القوانين وتطوير القدرات التقنية للشرطة أيضًا جزء أساسي من هذا العمل، حيث يتمثل التحدي في مواكبة التطورات التكنولوجية السريعة ومواجهة الأنشطة الإجرامية الجديدة والمتطورة في العالم الرقمي.

خـــاتمة

خاتمة:

من خلال طرح موضوع التعاون الشرطي لمكافحة الجريمة الإلكترونية، نقول ان الجريمة الإلكترونية تشكل تحديا متزايدا أمام أجهزة إنفاذ القانون في جميع أنحاء العالم، تتطور هذه الجرائم بسرعة مع تقدم التكنولوجيا، مما يجعل التعاون الشرطي العربي، والإقليمي، والدولي أمرا لا غنى عنه لمواجهتها بفعالية، وكما ذكرنا سابقا أهمية هذا التعاون في التصدي للجريمة الإلكترونية.

وأشرنا إلى الأدوات والتقنيات الحديثة التي تعزز من قدرات الشرطة في التتبع والملاحقة المجرمين الرقميين.

تتطلب مكافحة الجرائم الإلكترونية، استراتيجيات متعدد تشمل تبادل المعلومات، التدريب المستمر للكوادر الشرطية، واستخدام تقنيات متقدمة لتحليل البيانات وتعقب الأنشطة المشبوهة عبر الانترنت، كما يجب تعزيز التعاون بين الدول وتبادل الخبرات والمعرفة لمواجهة التحديات المشتركة.

أظهرت دراسة أن التعاون الشرطي الفعال يساهم في الكشف عن الجرائم الإلكترونية والحد من تأثيرها على الأفراد والمجتمعات، وتحقيق أقصى استفادة من هذا التعاون، يجب تبني سياسات واضحة واتفاقيات دولية تضمن تبادل المعلومات بشكل سريع وآمن، بالإضافة إلى تعزيز الثقة بين الأجهزة الشرطية المختلفة، كما تبقى مكافحة الجريمة الإلكترونية مسؤولية جماعية تتطلب التزاما وتنسيقا لضمان أمن وسلامة المجتمعات في العالم الرقمي.

ومن خلال هذا البحث توصلنا على النتائج التالية:

يساهم التعاون الشرطي في تبادل المعلومات والبيانات بين الدول لتحليل الأنماط الجديدة للجرائم الإلكترونية ومعالجتها.

يتيح التعاون الشرطي إمكانية إجراء التحقيقات المشتركة بين الدول لمكافحة الجرائم الإلكترونية التي تتجاوز الحدود الوطنية.

يساهم التعاون الدولي في تطوير قدرات الشرطة في التعامل مع التهديدات الإلكترونية من خلال تبادل الخبرات والتدريب.

يعزز التعاون العربي والإقليمي والدولي التنسيق بين وحدات الشرطة المختلفة لضمان استجابة فعالة وسريعة للتهديدات الإلكترونية.

خاتمة

يهدف التعاون الشرطي إلى تعزيز جهود مكافحة الجرائم الإلكترونية من خلال التعاون الدولي وتبادل المعلومات والخبرات.

وقبل اختتام دراستنا نقدم التوصيات التي يمكن العمل بها:

العمل على تأكيد أهمية التعاون الشرطي إقليميا ودوليا والشراكات الوثيقة بين الشرطات المحلية والمنظمات الدولية في مكافحة الجرائم الإلكترونية.

تعزيز التبادل الدولي للمعلومات والخبرات بين الجهات الشرطية في مختلف الدول لتحسين الاستجابة للجرائم الإلكترونية.

تأهيل الكوادر المحلية من أجل القدرة على التعاطي مع التطور المستمر للجرائم الإلكترونية.

تعزيز التعاون مع القطاع الخاص والمؤسسات الأكاديمية والمنظمات الدولية لتطوير حلول مبتكرة لمكافحة الجريمة الإلكترونية.

العمل على تشجيع وتوعية الجمهور بأهمية الأمن السيبراني وطرق الوقاية من الجرائم الإلكترونية، والإبلاغ عن الأنشطة الاحتيالية عبر الأنترنت.

العمل على تعزيز التدريب وبناء القدرات الفنية والتكنولوجية لدى الشرطة لمكافحة الجرائم الإلكترونية بفعالية.

قائمة

المصادر والمراجع

قائمة المصادر والمراجع:

أولا-المصادر

النصوص التشريعية:

الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم

قوانين:

قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5غشت سنة2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثانيا: مراجع

أ-الكتب متخصصة

1-جلال محمد الزغبي، أسامة أحمد مناعسة، جرائم تقنية نظم المعلومات الإلكترونية-دراسة مقارنة، ط01، دار الثقافة للنشر والتوزيع، 2010.

2-خراشي، عادل عبد العال إبراهيم، إشكالات التعاون الدولي في مكافحة الجريمة المعلوماتية، دط، دار الجامعة الجديدة، مصر، 2015.

3-عبد العال الدريبي، محمد صادق اسماعيل، الجرائم الإلكترونية -دراسة قانونية قضائية مقارنة، ط01، المركز القومي للإصدارات القانونية، 2012.

4-عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، ط01، النشر الجامعي الجديد، تلمسان، الجزائر، 2021.

5-محمد نصر محمد، الوسيط في الجريم المعلوماتية، ط 01، مركز الدراسات العربية للنشر والتوزيع، مصر، 2010.

6-نهلا عبد القادر المومني، الجرائم المعلوماتية، ط02، دار الثقافة للنشر والتوزيع، الأردن،2010.

ب- الكتب العامة:

1-أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، د ط، النشر الجامعي الجديد، تلمسان، الجزائر، 2022.

2-أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دط، النشر الجامعي الجديد، تلمسان، الجزائر، 2022.

3-عبد أوهابية، شرح قانون العقوبات الجزائري-القسم العام، دط، موفم للنشر، الجزائر، 2015.

ثالثا: مقالات علمية ومداخلات

1-أحلام بوكربوعة، «آلية الإتحاد الإفريقي للتعاون الشرطي "أفريبول "ودورها في مكافحة ظاهرة الإرهاب»، حوليات، المجلد 34، العدد 04، جامعة الجزائر، 2020.

2-اسعيداني سلامي، طارق طراد، «التجربة الجزائرية لمواجهة الجريمة الالكترونية في ظل البيئة التفاعلية الجديدة (عرض تشريعي قانوني)، مجلة الحقوق والعلوم السياسية، المجلد06، العدد02، كلية الحقوق والعلوم السياسية، جامعة خنشلة،2019.

3-أمال حجيج، «نحو قوة أورو-متوسطية للشرطة والتسيير الحدودي، مجلة دفاتر السياسة والقانون، العدد 12، جامعة أم بواقي، الجزائر، 2015.

4-إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة الآفاق للبحوث والدراسات، العدد04، المركز الجامعي إليزي، الجزائر، 2019.

5-بوضياف اسمهان، «الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر»، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف، مسيلة، الجزائر، 2018.

6-بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، مجلد 14، العدد04، جامعة قسنطينة02، الجزائر، 2021.

7-حليمة خزار، «المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب»، مجلة الدراسات القانونية المقارنة، المجلد02، العدد01، جامعة شلف، 2016.

8-حمزة بن فهم السليمي، الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي، مجلة الجامعة العربية، العدد59، جامعة العراق، العراق، 2023.

9-رحموني محمد، «خصائص الجريمة الإلكترونية ومجالات استخدامها»، مجلة الحقيقة، المجلد 16، العدد41، جامعة ادرار، الجزائر، 2018.

10- رحموني محمد، «منظمة الشرطة الجنائية الدولية (الإنتربول) آلية لمكافحة الجريمة المنظمة»، مجلة الآفاق العلمية، المجلد11، العدد04، المركز الجامعي تامنغست، 2011.

11-سي حميدي عبد المومن، قيرة سعاد، «الجريمة الإلكترونية وآليات التصدي لها في قانون الجزائري»، مجلة البيبان للدراسات القانونية والسياسية، المجلد 07، العدد01، كلية الحقوق والعلوم السياسية، جامعة برج بوعريريج، الجزائر، 2022.

12-صابر بحري، منى خرموش، «أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية»، مجلة دراسات في سيكولوجية الانحراف، المجلد06، العدد 01، جامعة سطيف، الجزائر، 2021.

13-طاهر ياكر، «مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية»، مجلة الصدى للدراسات القانونية والسياسية، المجلد 01، العدد01، جامعة خميس مليانة، الجزائر، 2022.

14-عبد العزيز لزعر، رشيد زياني، «آلية الاتحاد الإفريقي للتعاون الشرطي(الأفريبول)) ودورها في مكافحة الإلكترونية»، مجلة المتون، المجلد 14ن العدد03، جامعة سعيدة، 2021.

15-عفاف بعون، نسيمة أولاد سالم، «الجريمة الإلكترونية -قراءة سوسيوتاريخية في النشأة والآثار»، مجلة القبس للدراسات النفسية والاجتماعية، المجلد 05، العدد 20، جامعة المدية الجزائر، 2023.

16-عليوة سليم، «الجريمة المعلوماتية»، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 06، العدد01، كلية الحقوق والعلوم السياسية، مسيلة، الجزائر، 2021.

17-غريبي بشرى، «خصوصية المجرم المعلوماتي ودوافعه»، مجلة نوميروس الأكاديمية، المجلد 02، العدد 02، مركز الجامعي مغنية، تلمسان الجزائر، 2021.

18-كعرار سفيان، «الآليات المؤسساتية الأوروبية لمكافحة الجريمة المنظمة عبر الوطن»، المجلة الاكاديمية للبحوث القانونية والسياسية، المجلد 04، العدد 01، جامعة الأغواط، 2020.

19-لامية طالة، كهينة سلام «الجريمة الإلكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي»، مجلة الرواق للدراسات لاجتماعية والإنسانية، المجلد 06، العدد02، المركز الجامعي غليزان، 2020.

20-لطروش فيروز، بن عزوز حاتم، «الجريمة الإلكترونية في الجزائر: من جريمة فردية إلى جريمة منظمة»، مجلة الآفاق للعلوم، المجلد 01، العدد01، جامعة الجلفة، الجزائر، 2016.

21-محمد قسيمة، «الوسائل الفنية للمنظمة الدولية للشرطة الجنائية (الأنتربول) كآلية للتعاون الدولي الشرطي»، حوليات، مجلد 34، العدد02، جامعة الجزائر 01، 2020.

22-معاشي سميرة، «الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)»، مجلة المفكر، المجلد 13، العدد 17، كلية الحقوق والعلوم السياسية -بسكرة، الجزائر، 2018.

23-مقلاتي مونة، راضية مشري، «الجريمة الإلكترونية، دلالة المفهوم وفعالية المعالجة القانونية»، مجلة أبحاث قانونية وسياسية، المجلد 06، العدد 01، كلية الحقوق والعلوم السياسية، جامعة جيجل، الجزائر، 2021.

24-ودرار أمين «الشرطة الجنائية الإفريقية الأفريبول»، حوليات، المجلد 34، العدد01، جامعة الجزائر، 2020.

25-ياسمينة بونعارة، «الجريمة الإلكترونية»، مجلة المعيار، المجلد20، العدد39، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، الجزائر، 2015.

البحوث العلمية:

أ-رسائل الدكتوراه

1- براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة دكتوراه تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، 2018.

2-خالد على نزار، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة دكتوراه، تخصص حقوق، كلية الحقوق جامعة المنصورة، مصر، 2020، 2021.

3-ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة للنيل شهادة الدكتوراه في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة01، 2015-2016.

4-شعبان لامية، الجهود الدولية في مكافحة الاتجار بالبشر عبر الانترنت، أطروحة لنيل شهادة دكتوراه علوم، قمس الحقوق، جامعة العربي تبسي، تبسة، 2019-2020.

ب-رسائل الماجستير:

1-حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة ماجستير في العلوم القانونية، تخصص علم الاجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2011 -2012.

2-حيدر علي حسن نبات السويعدي، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب السيبراني، مذكرة لنيل شهادة ماجستير، قانون العام، كلية القانون، جامعة كربلاء، العراق، 2023.

3-دردور نسيم، الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذرة لنيل شهادة ماجستير، تخصص القانون الجنائي، كلية الحقوق، جامعة قسنطينة، 2012-2013.

4-سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، تلمسان،2010 ،2011.

مواقع إلكترونية:

https://alhirak-alikhbari.dz/article/3RaaSiCA7qWSCvS2H
https://nauss.edu.sa/ar-sa/news/Pages/5-10-2022.aspx
https://www.aim-council.org/specialized-offices/riyadh/861
https://www.alayam.com/home/getnewsdesc?intNewsMainID=op2HnaarJ/g
https://www.aljazeera.net/news
https://www.europarabct.com
https://www.interpol.int/ar/5/4/1

الملخص

ملخص مذكرة الماستر

التعاون الشرطي في مكافحة الجريمة الإلكترونية أمر بالغ الأهمية في عصرنا الحالي، حيث تتطور تقنيات الجريمة الإلكترونية بسرعة وتشكل تحديات كبيرة للأمن السيبراني. يتضمن التعاون الشرطي تبادل المعلومات والخبرات بين الجهات الإنفاذية المختلفة على الصعيدين الوطني والدولي، بما في ذلك المشاركة في التحقيقات الجنائية المشتركة وتبادل البيانات الرقمية لتتبع الجرائم وتقديم المساعدة في تقديم المتهمين للعدالة. تعتمد فاعلية هذا التعاون على الاتفاقيات الدولية والقوانين المحلية التي تسهل عملية التعاون وتوفر إطار قانونيا له.

الكلمات المفتاحية:

التعاون الشرطي؛ الجريمة المعلوماتية؛ الجريمة الإلكترونية؛ المعلومات؛ الخبرات؛ التبادل الرقمي؛ البيانات الرقمية؛ **الجرائم السيبرانية.**

Abstract of Master's Thesis

Cooperation in combating cybercrime is critically important in our current era, where cybercrime techniques evolve rapidly, posing significant challenges to cybersecurity. Police cooperation entails the exchange of information and expertise among various law enforcement agencies at both national and international levels. This includes participating in joint criminal investigations and exchanging digital data to track crimes and assist in bringing suspects to justice. The effectiveness of this cooperation relies on international agreements and local laws that facilitate collaboration and provide a legal framework for it.

Keywords:

Police cooperation; Cybercrime; Electronic crime; Information; Expertise; Digital exchange; Digital data; Cybercrimes.

الفهرس

الفهرس

الفهرس:

كلمة شكر	
إهداء	
قائمة المختصرات	
مقدمة	**1**
الفصل الأول: الأحكام الموضوعية للجريمة الإلكترونية	**4**
المبحث الأول: ماهية الجريمة الإلكترونية	**5**
المطلب الأول: تعريف الجريمة الإلكترونية وخصائصها	**6**
الفرع الأول: التعريف الفقهي والقانوني للجريمة الإلكترونية	**7**
الفرع الثاني: خصائص الجريمة المعلوماتية	**12**
المطلب الثاني: أنواع ودوافع الجريمة الإلكترونية	**19**
الفرع الأول: دوافع الجريمة الإلكترونية	**19**
الفرع الثاني: أنواع الجريمة الإلكترونية	**22**
المبحث الثاني: أركان الجريمة الإلكترونية	**26**
المطلب الأول: الركن الشرعي والمادي للجريمة الإلكترونية	**26**
الفرع الأول: الركن الشرعي للجريمة الإلكترونية	**26**
الفرع الثاني: الركن المادي للجريمة الإلكترونية	**28**
المطلب الثاني: الركن المعنوي والمفترض للجريمة الإلكترونية	**34**
الفرع الأول: الركن المعنوي للجريمة الإلكترونية	**34**
الفرع الثاني: الركن المفترض للجريمة الإلكترونية	**36**
خلاصة الفصل الأول	**38**
الفصل الثاني: آليات التعاون الشرطي لمكافحة الجريمة الإلكترونية	**39**
المبحث الأول: التعاون الشرطي العربي والإقليمي	**40**
المطلب الأول: التعاون الشرطي العربي والأوربي	**40**
الفرع الأول: التعاون الشرطي العربي لمكافحة الجريمة الإلكترونية	**40**

الفهرس

الفرع الثاني: التعاون الشرطي الأوروبي لمكافحة الجريمة الإلكترونية	**43**
المطلب الثاني: آلية الإتحاد الإفريقي للتعاون الشرطي لمكافحة الجريمة الإلكترونية	**45**
الفرع الأول: نشأة آلية الإتحاد الإفريقي للتعاون الشرطي	**45**
الفرع الثاني: دور آلية الإتحاد الإفريقي للتعاون الشرطي في مكافحة الجريمة الإلكترونية	**47**
المبحث الثاني: دور منظمة الشرطة الجنائية الدولية لمكافحة الجريمة الإلكترونية	**50**
المطلب الأول: مفهوم المنظمة الدولية للشرطة الجنائية	**51**
الفرع الأول: المنظمة الدولية للشرطة الجنائية وطبيعتها القانونية	**51**
الفرع الثاني مبادئ واختصاصات وأهداف الأنتربول	**54**
المطلب الثاني: دور منظمة الشرطة الدولية لمكافحة الجريمة الإلكترونية	**56**
الفرع الأول: دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة الإلكترونية	**56**
الفرع الثاني: الإنجازات التي حققتها الأنتربول لمكافحة الجريمة الإلكتروني	**60**
الفرع الثالث شرطة الويب الدولية	**61**
خلاصة الفصل الثاني	**62**
خاتمة	**63**
قائمة المصادر والمراجع:	**64**
ملخص مذكرة الماستر	