الجمهورية الجزائرية الديمقراطية الشعبية
RépubliqueAlgérienneDémocratique et populair

Ministère de l'Enseignement Supérieur et
de la Recherche Scientifique.
Université de Ghardaïa

Faculté de Droit et des Sciences Politiques
Département de Droit

وزارة التعليم العالي و البحث العلمي
جامعة غرداية
كلية الحقوق والعلوم السياسية
قسم الحقوق

شهادة تصحيح

يشهد الأستاذ خنان أنور بصفته(ها) رئيسا للجنة مناقشة مذكرة الماستر ل:

الطالب(ة): بن حمودة علي رقم التسجيل: 9068196

الطالب(ة): حسيني جيلالي رقم التسجيل: 9080250

تخصص :ماستر قانون جنائي وعلوم جنائية دفعة 2025 لنظام(ل م د).

أن المذكرة المعنونة بـ:

الآليات القانونية لمكافحة الجرائم الإلكترونية

تم تصحيحها من طرف الطالب / الطالبين وهي صالحة للإيداع.

غرداية في: 2025/06/22

إمضاء الأستاذ رئيس اللجنة المكلف بمتابعة التصحيح :

د/ .....

الدكتور
خنان أنور

رئيس القسم:

جامعة غرداية
قسم الحقوق

رئيس قسم الحقوق
أبو القاسم عيسى

ملاحظة: تترك هذه الشهادة لدى القسم.

جـــامعـة غـــــرداية

كلية الحقوق و العلوم السياسية

قسم الحقوق

العنـــوان:

الآليات القانونية لمكافحة الجرائم الالكترونية

مذكّرة مقدمة لاستكمال متطلّبات نيل شهادة ماستر أكاديمي حقوق

تخصص قانون جنائي و علوم جنائية

إعداد الطالبين:

- بن حمودة علي
- حسيني الجيلالي

إشراف الأستاذ:

د. لشقر مبروك

لجنة المناقشة :

لقب و إسم الأستاذ	الرتبة	الجامعة	الصفة
خنان أنور	أستاذ محاضر "أ"	جامعة غرداية	رئيسا
لشقر مبروك	أستاذ محاضر "أ"	جامعة غرداية	مشرفا مقررا
مجدوب آمنة	أستاذ محاضر "أ"	جامعة غرداية	عضوا مناقشا

نوقشت بتاريخ : 2025/06/16

السنة الجامعية

1446-1447هـ/2024-2025م

جـــامعـة غـــــرداية

كلية الحقوق و العلوم السياسية

قسم الحقوق

العنـــوان:

الآليات القانونية لمكافحة الجرائم الالكترونية

مذكّرة مقدمة لاستكمال متطلّبات نيل شهادة ماستر أكاديمي حقوق

تخصص قانون جنائي و علوم جنائية

إعداد الطالبين:

- بن حمودة علي
- حسيني الجيلالي

إشراف الأستاذ:

د. لشقر مبروك

لجنة المناقشة :

لقب و إسم الأستاذ	الرتبة	الجامعة	الصفة
خنان أنور	أستاذ محاضر "أ"	جامعة غرداية	رئيسا
لشقر مبروك	أستاذ محاضر "أ"	جامعة غرداية	مشرفا مقررا
مجدوب آمنة	أستاذ محاضر "أ"	جامعة غرداية	عضوا مناقشا

نوقشت بتاريخ : 2025/06/16

السنة الجامعية

1446-1447هـ/2024-2025م


بسم الله الرحمن الرحيم

شكر و تقدير

الحمد لله الذي بنعمته تتم الصالحات

فاللهم لك الحمد كما ينبغي لجلال وجهك و لعظيم سلطانك نحمدك و نشكرك على توفيقنا لإتمام هذه المذكرة

نتقدم بالشكر الجزيل الى أستاذنا الفاضل و المشرف علينا في هذا العمل

المتواضع الدكتور لشقر مبروك و الذي لم يبخل علينا بوقته وجهده

كما نوجه تحية شكر و عرفان الى أساتذتنا الأفاضل أعضاء لجنة المناقشة بصفة خاصة

و تحية شكر و امتنان الى جميع الأساتذة من طور الابتدائي و المتوسط و الثانوي

الى الجامعي و الى كل من ساعدنا في إنجاز هذا العمل .

الإهداء

أهدي ثمرة جهدي إلى :

أبي و أمي حفظهما الله و أطال في عمرهما و إلى إخوتي

و أخواتي و أصدقاء دربي و زملائي

و إلى زوجتي قرة عيني و سندي و إلى ابنيا و ابنتي حفظهم الله

و إلى كل من ساهم و ساعدني في إنجاز هذا العمل .

بن حمودة علي

الاهداء

اهدي هذا العمل

إلى من كلله الله بالهيبة والوقار، الى من رباني صغيرا وصاحبني كبيراً
إلى الوالدين الكريمين أطال الله في عمرهما، دمتما لي نبضا يرافقني
حتى المشيب
إلى عائلتي الكريمة و اخوتي حفظهم الله بالذكر إلى كافة اصدقائي
والاحباب
وكل من ساعدنا من قريب او بعيد وانار دربنا

حسيني الجيلالي

قائمة المختصرات:

ج : الجزء

د ذ د ن : دون ذكر دار النشر

د ذ س ن : دون ذكر سنة النشر

ص : الصفحة

ص– ص: من الصفحة الى الصفحة

ط : الطبعة

د ذ ط : دون ذكر الطبعة

ج ر: جريدة رسمية

مقدمة

مقدمة

شهدت الجرائم تطور على مر العصور، وذلك راجع إلى تطور الإنسان منذ القدم فالجرائم مرتبطة بوجوده فلا يمكن تصور وقوع جريمة بغير الانسان، وقد عرفت الجريمة تنامي متزايد في عصرنا هذا والتي تطورت بصورة رهيبة من خلال التطورات المتلاحقة والمتغيرات الكبيرة التي أفرزتها الظروف السياسية والثقافية والاقتصادية العالمية التي نقلت هذه الجرائم من التقليد الى الحداثة بالاعتماد على التقنيات الحديثة، حيث أصبح الحاسوب والبرمجيات ركيزة للأنشطة في كل مناحي حياة الانسان.

هذه المتغيرات أثبتت أن الجريمة نبت من غرس لمعطيات المجتمعات و إفراز لذاتية الانسان فيها، فالتطورات هذه أنتجت أدوات وخدمات جديدة يسرت على الإنسان الوقت والجهد والمال، وهذا ما أدى إلى ظهور نمط جديد من الجرائم لإساءة استخدام هذه الخدمات، وهذا ما يسمى بالجرائم المعلوماتية أو الإلكترونية والتي تختلف في وسائلها وشكلها ومضمونها عن الجرائم التقليدية، بحيث يستمد هذا النوع من الإجرام من الإمكانات التكنولوجية الحديثة للحاسوب والبرامج وتطور شبكات الانترنت.

وبما أن العالم اليوم يتسم بأشكال جديدة من الجرائم لم تكن مألوفة، كان لزاما على المشرع الجزائري وكل الأنظمة في العالم تكييف نصوصها القانونية مع هذه التطورات بالنظر الى الطبيعة الخاصة بالجرائم المعلوماتية، بحيث عجزت الأجهزة الأمنية الوطنية والدولية المتطورة عن ملاحقتها والحد منها، الأمر الذي تطلب اتخاذ اجراءات وقائية وردعية تتماشى مع هذه الأنواع من الاجرام.

وأمام هذه التطورات أصبحت هذه الجرائم محط دراسة واهتمام لكل الباحثين لإدراكهم مدى خطورة إستفحالها داخل المجتمعات، الأمر الذي دفع بالمشرع الجزائري الى وضع آليات جديدة تتلاءم وطبيعتها، كما هو الحال لباقي التشريعات الغربية والعربية، وتطوير الوسائل التقليدية بما يكفل مكافحة هذا النوع من الجرائم.

تأتي أهمية هذا البحث كون هذه الجرائم موضوع حديث النشأة بدأ الاهتمام به، وإظهار الآليات التي إعتمدها المشرع الجزائري بوجه خاص وباقي التشريعات العربية والغربية بوجه عام.

وكذا تبيان طبيعة هذه الجرائم التي لها مميزات وخصائص تميزها عن الجرائم التقليدية، كون هذا البحث من المواضيع المعاصرة والتي وجب البحث والتعمق فيها، بحيث يكتسب البحث أهمية كونه يلم بالآليات المتخذة على الصعيد الوطني وعلى الصعيد الدولي.

ويرجع سبب اختيارنا لهذا الموضوع الى أسباب ذاتية و أخرى موضوعية.

فمن الأسباب الذاتية هو إستفحال وانتشار الجرائم المعلوماتية وخطورتها على المجتمعات، ونظرا لحداثة الموضوع والذي لم يحظى بالعناية الكافية من الدراسات ،و سبب آخر يعود لوظيفتي في مجلس القضاء فمعظم الجرائم المرتكبة الا و يتخللها أو ترتكز على الوسائل الإلكترونية.

أما الأسباب الموضوعية فنظرا للأضرار التي تلحقها هذه الجرائم ما يستوجب إقامة أجهزة وفرض آليات لمكافحتها، وكذا توضيح شامل للجرائم الالكترونية وإبرازها للباحثين أو للذين يعملون على تطبيق النص الاجرامي.

أما أهداف الدراسة فتتلخص في ما يلي:

– التعرف على الآليات القانونية لمكافحة جرائم المساس بأنظمة الكمبيوتر والاتصال ومواقع خللها.

– الانفتاح على الآليات القانونية لمكافحة هذه الجريمة على المستوى الدولي.

– إعادة ترتيب الآليات وفق ما أصدره المشرع من مراسيم و قوانين.

– التعرف على أبرز الجهود الدولية في مكافحة الجرائم المعلوماتية من خلال الآليات المستحدثة.

وقد قام الكثير من الباحثين بدراسات سابقة وتم أخذ دراستين :

-أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق براهيمي جمال "التحقيقي الجنائي في الجرائم الإلكترونية" ، جامعة ميلود معمري، كلية الحقوق والعلوم السياسية، تيزي وزو، 2018/06/27 .

- مذكرة ماستر "آليات مكافحة الجريمة الالكترونية" جامعة صالحي أحمد، النعامة كلية الحقوق، شرويلي فاطمة، ديدي فضيلة، سنة 2023/2022، تطرقتا إلى التحديات القانونية لمكافحة الجرائم الإلكترونية.

وأثناء العمل على تحضير هذا البحث المتواضع لمسنا صعوبة في جمع المعلومات المتعلقة بهذا الموضوع و يتعلق الأمر بالمصادر والمراجع المتخصصة في هذا المجال ، و سبب آخر يتمثل في ضيق الوقت .

وعليه بناء على ما سبق ذكره نطرح إشكالية الدراسة الرئيسية:

ماهي الآليات القانونية لمكافحة الجرائم الإلكترونية وطنيا و دوليا؟

اعتمدنا في بحثنا المتواضع على المنهج الوصفي والتحليلي، الذي قمنا من خلالهما بوصف أحكام الجريمة الإلكترونية وخصائصها في الفصل الأول بالإعتماد على المنهج الوصفي، أما الفصل الثاني إستندنا على كلى المنهجين في وصف وتحليل الآليات القانونية الدولية والجزائرية وفهمها على حد سواء.

ولدراسة موضوعنا هذا بطريقة تسهل على القارئ أو الباحث قسمنا بحثنا إلى فصلين، لكل فصل مبحثين وهي كالتالي:

سنتناول في الفصل الأول أحكام الجرائم الإلكترونية والذي يحتوي على مبحثين، الأول تحت عنوان مفهوم الجرائم الإلكترونية، أما الثاني بعنوان أركان الجريمة الإلكترونية و أنواعها.

أما الفصل الثاني بعنوان الآليات القانونية لمكافحة الجرائم الإلكترونية، المبحث الأول بعنوان الآليات الدولية في مكافحة الجرائم الإلكترونية أما المبحث الثاني تم تطرق فيه الى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري.

وخلصنا في هذه الدراسة بخاتمة أجبنا فيها عن الإشكالية وتناولنا أهم النتائج التي توصلنا اليها.

الفصل الأول:

أحكام الجرائم الإلكترونية

الفصل الأول: أحكام الجرائم الالكترونية

تمهيد :

لقد شهد العالم في الآونة الأخيرة تطور ملحوظ في المجال التقني، مما نتج عنه إستعمال الحاسوب الآلي وشبكة الأنترنت في جميع الميادين، لكن مع إستخدام هذه الوسائل بطرق غير مشروعة انحدر عنه إرتكاب جرائم لها علاقة بهذا المجال، وهو ما يعرف بالجريمة الإلكترونية نتيجة للتطور التكنولوجي مثلها مثل الإدارة الإلكترونية والتجارة الإلكترونية، فكما أن التطور الإلكتروني عاد بالنفع على حياة المجتمعات في العصر الحالي، حيث أصبحت الرقمية تدخل في عمل جميع القطاعات لتقديم خدماتها بصورة أفضل وبأسرع وقت وبأقل تكلفة، وتوج التطور المتلاحق في تقنية المعلومات بظهور الأنترنيت، فإنه كان مرفوق أيضا بظواهر سلبية نتيجة الإستعمال السيء لهذه التكنولوجيات، من قبل الأشخاص وخاصة في الأفعال الإجرامية وغير المشروعة، ونظرا لحداثة هذه الجريمة، فقد إختلف الفقهاء في وضع تعريف موحد لها، كما إتسمت بمجموعة من الخصائص، والدوافع لارتكاب هذه الجريمة ولفهم هذا النوع الجديد من الجرائم قسمنا الفصل الأول إلى مبحثين تناولنا في المبحث الأول: مفهوم الجرائم الإلكترونية و في المبحث الثاني أركان الجريمة الإلكترونية وأنواعها .

المبحث الأول: مفهوم الجرائم الالكترونية

في البداية علينا التعرف على الجريمة الإلكترونية وكيف عرفها الفقهاء وعلى التعريف الذي وضعه المشرع الجزائري، ثم نتطرق الى خصائص الجريمة ومميزاتها فالجريمة الإلكترونية جريمة تتشارك مع الجريمة التقليدية في خصائص وتنفرد بخصائص أخرى تميزها عن غيرها.

المطلب الأول: تعريف الجرائم الالكترونية

لا يوجد إجماع على تعريف ثابت وشرعي للجريمة الإلكترونية لما يثيره المصطلح من تعقيدات مفاهيمية،[1] لذا سنحاول أن نتعرض لبعض التعاريف من حيث الجانب اللغوي ثم من الجانب الفقهي، وأخيرا ما جاء به التشريع الجزائري.

الفرع الأول: التعريف اللغوي والفقهي للجريمة الإلكترونية

قبل أن نشرع بالتعريف الفقهي لكلمة جريمة إلكترونية سنبدأ بالتعريف اللغوي أولا، لأن مدلولات اللغة غالبا ما تؤثر في المصطلحات و المعاني التي يصطلح عليها الناس.

أولا: التعريف اللغوي للجريمة الإلكترونية:

تتكون الجريمة الإلكترونية من كلمتين:

جريمة: أصلها من جرم بمعنى كسب وقطع والجرم بمعنى الحر، وقيل إنها كلمة فارسية معربة والجرم مصدر الجارم الذي يجرم نفسه وقومه شرا، كما تعني التعدي والذنب فالجريمة والجارم بمعنى الكاسب، وأجرم فلان أي إكتسب الإثم كما تعني ما يأخذه الوالي من المذنب و رجل جريم وامرأة جريمة أي ذات جرم أي ذات جسم وجرم الصوت جهارته والجريمة تعني الجناية والذنب.[2]

والجريمة اصطلاحا: هي مجموع السلوكيات والأفعال الخارجة عن نطاق القانون.

---

[1] عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، شبكة الانترنت وشبكة الهواتف التقليدية والآليات والمطبوعات، دار الثقافة للنشر والتوزيع، 2019، ص 37.

2 سامية عزيز، مازيا عيساوي، الجريمة من منظور سيسيولوجي الأسباب و الأثار، مجلة دراسات في سيكولوجية الانحراف، المجلد 6، العدد 1، 2021، ص 128.

إلكترونية: يوصف جزء من الحاسوب وعمله، وعرفتها الأستاذة بوزيدي مختارية: "مجموع المخالفات التي ترتكب ضد الأفراد والمجموعات من طرف أفراد أو مجموعات أخرى بدافع الجريمة وبقصد إيذاء سمعة الضحية أو القيام بأذى مادي أو عقلي للضحية بطريقة مباشرة أو غير مباشرة باستخدام شبكات الاتصالات مثل الأنترنت".[1]

كما عرفتها الدكتورة غنية باطلي:" أن إستعمال مصطلح الجريمة الإلكترونية من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية والغش المعلوماتي أو جرائم الإعتداء على معطيات الحاسب الآلي وجرائم الأنترنت وبالتالي كان فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة"[2] علما أنه لم يركز الفقهاء على التعريف اللغوي للجريمة الإلكترونية لتقارب المفاهيم التقنية في هذا المجال، والمشتقة من الغش الإلكتروني والإجرام المعلوماتي حيث يرتكب الجرم بواسطة الحاسوب الآلي.

ثانيا: التعريف الفقهي للجريمة الالكترونية

إختلف الفقهاء ورجال القانون في تعريف الجريمة الإلكترونية، حيث أن كل إتجاه أسس تعريفه بناءا على الزاوية التي يرى فيها الجريمة (وسيلة ارتكابها وهناك من يوسع في رؤيته للجريمة وهناك من يركز على جزء من الجريمة) وسنتطرق الى بعض التعاريف الفقيهة وفقا لما يلي:

1. التعريف الفقهي الضيق للجريمة الإلكترونية:

كل إتجاه فقهي إعتمد وجهة نظر ضيقة في تعريفه للجريمة الإلكترونية، فمنهم من إعتمد على أداة الجريمة ومنهم من إعتمد على توافر المعرفة بتقنيات جهاز الحاسب الآلي ومنهم من اعتمد في تعريفه بناءا على موضوع الجريمة.

---

[1] بوزيدي مختارية، ماهية الجريمة الإلكترونية، ورقة بحثية مقدمة ضمن ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع، الجزائر، يوم 29 مارس 2017، ص 234.

[2] غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، ط 2015، ص 23.

أ- على أساس معيار أذاة الجريمة:

تم تعريف الجريمة الإلكترونية وفقا لهذا المعيار على أساس أداة الجريمة، فالجريمة تكون جريمة إلكترونية طالما أن الحاسوب أو إحدى الوسائل التقنية من وسائل ارتكابها (الهواتف الذكية ...).

عرفها الأستاذ MASS بأنها: "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق ربح.

أما الفقيه الألماني TIEDMANN فعرفها كما يلي: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بواسطة جهاز الحاسوب"

" كما عرفها الفقيه MAWRE "الجريمة الإلكترونية هي الفعل غير المشروع الذي يتورط الحاسب الألي في إرتكابه[1]"

ب-على أساس معيار توفر المعرفة بتقنية المعلومات:

أصحاب هذا الإتجاه لا يعتمدون على الحاسوب الآلي، ولكن على الشخص الذي يستخدمه فبدون إمتلاكه المعرفة بالتقنية لا يمكنه أن يستعمل الحاسوب ولا أن يرتكب جريمة أصلا، فالأستاذ DAVID THOMSON عرفها بأنها "أي جريمة يكون متطلب لإقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب"، هنا المعيار الشخصي المتعلق بالجاني هو المعيار المعتمد ،إذ تتم متابعة وملاحقة مقترف الفعل غير المشروع في حالة واحدة وهي علمه بتكنولوجيا الحاسوب الألية.

[1] غنية باطلي، المرجع السابق، ص 15.

ج-على أساس معيار موضوع الجريمة

يرى آخرون أن تعريف الجريمة الإلكترونية إنما يرجع إلى موضوعها وغير متعلق بالوسيلة المستعملة أو الفاعل، حيث يرى هؤلاء أن الجريمة الإلكترونية هي التي يكون موضوعها المال المعلوماتي المعنوي دون النظر فيما إذا كان الحاسب هو الأداة المستعملة في ارتكابها.[1]

2. التعريف الموسع للجريمة الإلكترونية:

من المتعارف عليه أن الوسيلة التي ترتكب بها الجريمة التقليدية لا تدخل في تعريفها ولا حتى تمكن الجاني من التقنية، وتفاديا للانتقادات التي وجهت للمفهوم الضيق ظهر المفهوم الواسع كما يلي:

عرفها PARKER بما يلي: " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه".

"كل استخدام في صورة فعل أو إمتناع من شأنه الإعتداء على أي مصلحة مشروعة سواء كانت مادية أو يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ومعاقب عليه قانونا أيا كان غرض الجاني "[2]

أما الفقيهان MIEL و CREDO فعرفاها بأنها: "تشمل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج المصرح به لحاسوب المجنى عليه أو بياناته "

المنظمة الأوروبية للتعاون والتنمية الاقتصادية عرفتها على أنها: " كل عمل أو إمتناع يأتيه الإنسان إضرارا بمكونات الحاسب الآلي المادية والمعنوية وشبكات الإتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد تحت مظلة قانون العقوبات لحمايتها"[3]

---

[1] غنية باطلي، المرجع نفسه، ص 17.

[2] دمان ذبيح عماد، بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر، مجلة الحقوق والعلوم السياسية، العدد 13، جانفي 2020، ص 140.

[3] غنية باطلي، مرجع سابق، ص 19.

عملت الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا هاما، أو هي فعل إجرامي يستخدم الحاسب الآلي في إرتكاب كأداة رئيسية[1]

وعرفها مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقدة في فيينا 2000 بـ: "يقصد بالجريمة الإلكترونية أي جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك التي تشمل من الناحية المدنية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[2]

واشتمل تعريف الجريمة الإلكترونية الذي جاء به الدكتور عبد الفتاح بيومي حجازي "جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات، وتطال إعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات"

3. التعريف الفقهي المختلط أو الجامع:

إن إعطاء تعريف موسع للجريمة الإلكترونية أدخل في نطاقها كل التصرفات غير المشروعة التي لها علاقة بالحاسب، سواء وسيلة أو موضوع أو مناسبة إرتكاب هذا ما أدى إلى ظهور اتجاه ثالث وهو الاتجاه الجامع ويعتمد هذا الإتجاه في تعريف الجريمة الإلكترونية على معيار المصلحة المحمية.

وقد اعتمده M ALTERMAN وH BLOCH " كل سلوك غير مشروع أو يتعارض مع قواعد السلوك أو غير مرخص والذي يخص المعالجة الآلية للمعطيات أو لنقل المعطيات "وهو تعريف منظمة التعاون والتنمية الاقتصادية للغش المعلوماتي والذي أوردته بلجيكا في تقريرها

[1] ذياب سليمة بوترعة بلال، الجريمة الالكترونية الأسس والمفاهيم، مجلة تطوير العلوم، المجلد 13، العدد 01، جامعة زيان عاشور الجلفة، الجزائر ،2020 ، ص 10 .

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي نموذجي الإسكندرية، دار الفكر العربي، القاهرة، ص 33.

بأن الجرائم المعلوماتية: "هي كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[1] .

الفرع الثاني: تعريف الجريمة الإلكترونية في التشريع الجزائري

وضع المشرع الجزائري مفهوما للجريمة المتصلة بتكنولوجيات الإعلام والاتصال ضمن القانون 09-04 المؤرخ في: 14 شعبان عام 1430 الموافق لـ 05 أوت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذا القانون المنشئ للقطب الجزائي الوطني المختص الأمر رقم 21-11 المؤرخ في: 16 محرم عام 1443 الموافق لـ 25 أوت سنة 2021 يتمم الأمر رقم 66-155 المؤرخ في: 18 صفر عام 1386 الموافق لـ 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية جريدة رسمية رقم: 65 .

بداية فإن ملاحظة هامة ملفتة للانتباه تتعلق بالتسمية التي اعتمدها المشرع الجزائري بخصوص هذا النوع من الجرائم، حيث وعلى خلاف ما درج عليه الفقه من تسميات وكذا ما اعتمدته بعض التشريعات المقارنة من قبيل "الجرائم السيبرانية"، و"الجرائم الإلكترونية" والجرائم المعلوماتية وجرائم الأنترنت وغيرها، فإن المشرع الجزائري قد اعتمد تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في محاولة منه لمد نطاق التجريم إلى أقصى الحدود الممكنة، ومن أجل لفت الانتباه إلى السلوك الإجرامي يتجاوز المساس أو التلاعب بالمعطيات الآلية إلى استعمال الوسائل التكنولوجية لارتكاب حتى الجريمة بصورها التقليدية.

هذا وتحقيقا لمبدأ الشرعية وضمانا لمد مجال تطبيق الأحكام الجزائية الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال إلى كل السلوكيات المشتبه في اعتبارها جرائم من هذا النوع، تدخل المشرع الجزائري بوضع تعريف تشريعي للجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال القانون 09-04 كما تضمن أيضا القانون 21-11 إضافة هامة بهذا الخصوص.

[1] خالد داودي، الجريمة المعلوماتية، دار الاعصار العلمي للنشر والتوزيع، الجزائر، ط 1، 2008، ص 25.

حيث عرفها المشرع ضمن القانون 09-04 في الفقرة أ من المادة 2 على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية" .

ومن خلال هذا النص يبدو أن المشرع الجزائري قد أحسن بوضع هذا التعريف الذي جمع فيه بخصوص هذا النوع من الجرائم بين تلك السلوكيات الماسة بأنظمة المعالجة الآلية للمعطيات، والتي وردت ضمن قانون العقوبات كجرائم معلوماتية وبين جملة الأفعال التي ترتكب بواسطة أو ضد أنظمة المعلومات.

حيث تتمثل الأولى في جملة الأفعال الماسة بنظام المعالجة الألية للمعطيات، بينما تتمثل الثانية في تلك الجرائم التقليدية التي ترتكب أو يسهل إرتكابها بإستخدام منظومة معلوماتية والتي تختلف بين تلك التي نص عليها المشرع ضمن قانون العقوبات وتلك التي تناولتها نصوص خاصة.

وبالرجوع إلى القانون 21-11 نجد أن المشرع قد حافظ على التعريف ذاته الخاص بجرائم الإعلام والاتصال ضمن المادة 211 مكرر 23 غير أنه جاء بالجديد من ناحيتين هما:

- تحديد أصناف الجرائم التي تمثل اختصاصا نوعيا حصريا للقطب الجزائي الوطني كما سنبينه لاحقا، وكذا استعماله لمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ويقصد بها كل الجرائم ذات الارتباط بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال في محاولة لمد التجريم إلى كل ما يتم أو يرتبط بالنظم المعلوماتية[1].

- اعتماد مفهوم الجريمة المتصل بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والتي عرفها بأنها: "... الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها

[1] بن عمير امينة، بوحلايس الهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ورقة بحثية مقدمة ضمن فعاليات الملتقى الدولي القانون الجنائي للأعمال نحو توجه جديد للتجريم، المنعقد يوم 21 اكتوبر 2021، عبر التحاضر المرئي عن بعد zoom، المجلد 7، العدد 1، لسنة 2022، ص 71 .

المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة أو خبرة متخصصة أو اللجوء إلى تعاون قضائي دولي "[1]

المطلب الثاني: خصائص الجرائم الالكترونية

تتميز الجرائم الالكترونية عن غيرها من الجرائم بخصائص كثيرة ولا يوجد مفهوم موحد لها في كامل الدول بالإضافة إلى عدم وجود كفاية في التعاون الدولي بشأنها واحتمال وجود أوصاف عديدة لمحل الجريمة،[2] ونذكر فيما يلي أهم خصائص الجريمة الإلكترونية وأكثرها شيوعا.

الفرع الأول: خصائص متعلقة بالجريمة

تم تقسيمها الى سبعة عناصر و هي كالآتي :

أولا- تتطلب وجود جهاز إلكتروني والتحكم بتقنية إستخدامه :

تتميز الجرائم الالكترونية بأنها تعتمد في إرتكابها على جهاز إلكتروني متطور هو أداة ووسيلة الجريمة، فالجهاز الإلكتروني هو أساس الجريمة الإلكترونية وأساس تسميتها والا ما وجدت الجريمة الإلكترونية من الأساس، إضافة إلى ضرورة وجود شبكة أنترنت وتحكم الجاني في التكنولوجيا وامتلاكه دراية في مجال المعلوماتية والاتصالات، فلا نتصور إرتكاب الجريمة الإلكترونية دون وجود تقنية المعلومات ولا شبكة الأنترنت، وتزيد خطورة المجرم كلما زادت قدرته على التحكم في الجوانب الثلاثة، وتتم الاعتداءات في هذه الجرائم على المعنويات (البرامج والبيانات والمعطيات) وليس على المكونات المادية فلا أثر مادي للجريمة بالكسر أو التحطيم أو السرقة، فهنا الجريمة تقليدية فالمشكل عندما يتم التعدي على المكونات المعنوية للحاسوب أي البيانات المخزنة فيه، وهنا يظهر تحكم الجاني في تشغيل الجهاز واستخدامه حتى يتمكن من الاعتداء على مكوناته المعنوية عند إختراق نظامه بسرقة المعلومات أو تعديلها أو مسحها أو تقليدها أو التلاعب بها واساءة استخدامها.[3]

---

1 المرجع نفسه .

[2] خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2019،ص 82 و 87 .

[3] خالد ممدوح ابراهيم، المرجع السابق، ص 86 .

ثانيا – جريمة مستحدثة:

الجريمة الإلكترونية جريمة مستحدثة فهي نمط إجرامي حديث لم يكن مألوفا من قبل، فالأساليب المستخدمة لارتكاب الجريمة أساليب حديثة، وهي وليدة التحولات التي شهدتها الحياة المعاصرة من تطور في مجال المعلومات والاتصالات وارتباطها بالمعلوماتية، وعالم الحواسيب والأجهزة الالكترونية وهي نتاج التطور التكنولوجي الحديث الذي مس أيضا أساليب ومجال الإجرام، حيث أصبح يستعمل العلوم والتقنية كوسيلة للتنفيذ من دول مختلفة (شبكات دولية تشارك في التخطيط والتنظيم والتنفيذ) في الخفاء بكل إحترافية كما أن الجرائم المستحدثة مازالت لم تتناول ولم تعالج بنصوص قانونية صريحة، رغم توافر كامل أركان الجريمة (من مجرم وضحية وفعل إجرامي)، أي هناك صعوبة في التحديد الدقيق لها.

حيث أن الجريمة تسبق القانون كما يقول علماء الإجرام، وهي من أهم سلبيات ومساوئ التقدم التكنولوجي الذي ساهم في ارتكاب الجرائم وأظهر جرائم جديدة ،كتبييض الأموال والاتجار بالبشر[1] فشبكة الأنترنت هي حلقة الوصل بين كافة أهداف الجريمة (بنوك ومؤسسات).

ثالثا– ارتكاب الجريمة الإلكترونية أثناء تشغيل نظام المعالجة الآلية للمعلومات

إن الجريمة الإلكترونية ترتكب بعد تشغيل نظام معالجة البيانات، ورغم وجود جرائم يمكن ارتكابها عند الادخال والاخراج الا أن مرحلة معالجة البيانات هي أخطر مرحلة وأسهلها لارتكاب هذه الجريمة، فكل جهاز في وضعية الإيقاف أو مغلق هو في وضع آمن سواء جهاز كمبيوتر أو جهاز إلكتروني ذكي، نستعرض المراحل التي ترتكب فيها الجريمة الإلكترونية كما يلي:

أ– مرحلة الإدخال: يسهل إدخال بيانات ومعلومات غير صحيحة وتكون كذلك بعدم إدخال المعلومات المطلوبة والوثائق الأساسية وهي أكثر مرحلة ترتكب فيها الجرائم المعلوماتية.

[1] خالد ممدوح ابراهيم، المرجع نفسه.

ب- مرحلة تشغيل نظام المعالجة الآلية للبيانات: هنا يكون ارتكاب الجريمة الإلكترونية بإدخال تعديلات على برامج الحاسوب بالتلاعب فيقوم المجرم بإدخال معلومات غير مصرح بها، فيكون الاعتداء بتشغيل برامج تعطل جزئيا أو كليا عمل البرامج الأصلية ويكون المجرم محترفا وملما بالتقنية اللازمة ليحقق هدفه.

ج- مرحلة المعالجة الآلية للبيانات والمعطيات: تكون هنا البيانات في حالة نشاط إن صح القول وهي المرحلة المقصودة، حيث يكون الاعتداء على البيانات المخزنة في النظام من أجل معالجتها إلكترونيا ويمكن للمستخدمٌ إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو إسترجاعها أو طباعتها، وهذه العملية وثيقة الصلة بارتكاب الجرائم المعلوماتية [1].

د- مرحلة الاخراج: هذه هي المرحلة الأخيرة حيث يرتكب العمل الإجرامي على النتائج التي يخرجها النظام المعلوماتي للحاسوب وتكون عملية إدخال البيانات صحيحة ومعالجتها صحيحة لكن التلاعب يكون في النتائج، أي أن النتائج لا تتوافق مع البيانات الموجودة في النظام.

رابعا_ عالمية وعابرة للحدود:

إن الجريمة الالكترونية كما يدعوها بعض الباحثين بأنها خمر معتق في قوارير جديدة خاصة[2]، حيث تقع في العالم الافتراضي انطلاقا من حاسوب أو جهاز ذكي (هاتف محمول أو لوح إلكتروني)، من مكان تواجد الجاني في دولة ما على محل جريمة في دولة ثانية أو دول متعددة، متجاوزا بذلك الحدود الجغرافية التي لم يصبح لها وجود بظهور الشبكة العنكبوتية العالمية (الأنترنت) التي جعلت العالم قرية صغيرة ولم تعد الحدود حاجزا في نقل وتبادل كميات هائلة من المعلومات بين الحواسيب والأنظمة المعلوماتية المنتشرة في مختلف أقطار العالم المتباعدة، لأنها تقع في عالم افتراضي واتصالها بعالم الأنترنت وتقنية المعلومات فيسهل الاتصال بين حواسيب لا حصر لها في عدة دول والجرائم الالكترونية ترتكب عن بعد، فيرتكبها

[1] يوسف عبد النبي شكري، المعلوماتية وازمة الشرعية، د ذ د ن، الكوفة، د ذ ط، 2008، ص 115.

[2] عادل عزام سقف الحيط ، مرجع سابق ، ص 188 .

شخص جالس أمام شاشة الكمبيوتر ببلد ولا يكون في مسرح الجريمة، كما قد تتضرر عدة دول وفي آن واحد بهذه الجريمة حيث يتواجد الأشخاص والأموال المستهدفة. كما قد يكون الجاني والضحية في نفس البلد أو المجنى عيه في بلد، كما أن الجريمة الإلكترونية الواحدة قد تمس ضحايا في بلدان مختلفة في وقت واحد خاصة في ظل ازالة الحدود الاقتصادية بفضل إنتشار التجارة الإلكترونية التي أزالت الحواجز الجمركية، وسمحت بسهولة انتقال رؤوس الأموال وعالمية الجريمة الإلكترونية خلق إشكالات فيما يخص القانون الواجب التطبيق، كون التخطيط يكون في بلد والتنفيذ في بلد والضحية في بلد آخر من جهة، ومن جهة آخرى مشكل تسليم المجرمين المعلوماتيين[1] هذا ما يؤدي إلى ضرورة وجود تعاون دولي في تبادل المعلومات وتسليم المجرمين عن طريق إبرام إتفاقيات وفي تسليم الأدلة والجناة وحتى التعاون في التحقيق...

خامسا – قلة الإبلاغ عن الجريمة الإلكترونية:

من صعوبات الكشف عن الجريمة الإلكترونية قلة التبليغ عنها، وهذا ما دل على قلة القضايا الإلكترونية، حيث أن إكتشافها لا يكون الا بعد مدة من إرتكابها ويكون صدفة خاصة أن الضحايا مؤسسات عامة أو خاصة أو متعددة الجنسيات لا يلجؤون إلى التبليغ حتى لا تتأثر سمعتم، وحتى لا تتأثر ثقة زبائنهم بهم خاصة إذا كنت بنوكا أو مؤسسات مالية، أو خوفا من التداعيات النفسية والاجتماعية إذا كان الضحايا أشخاصا طبيعيين لاسيّما في حالة الابتزاز والتهديد بنشر معلومات أو صور خاصة.[2]

سادسا_ صعوبة اكتشاف الجريمة الإلكترونية وإثباتها:

من أهم خصائص الجريمة الإلكترونية أنها صعبة الاكتشاف وصعبة الإثبات، تعود أسباب صعوبة اكتشاف الجريمة الإلكترونية وإثبات وقوعها لعدة عوامل فهناك أسباب تتعلق

[1] طارق عفيفي صادق احمد، الجرائم الالكترونية جرائم الهاتف المحمول، د ذ د ن، مصر، ط 1، 2015، ص 35.

[2] خالد ممدوح ابراهيم، مرجع سابق، ص 86.

بوسيلة الجريمة ذاتها وهناك ما هو راجع إلى المجرم المعلوماتي كما أن هناك أسبابا تتعلق بالضحية.

سابعا- صعبة الاكتشاف لخصوصية الوسيلة :

لأنها هادئة وناعمة فيصعب اكتشاف حدوثها لأنها تقنية بحتة، وهي معقدة ليست في متناول الجميع من حيث الاستعمال والتشغيل، فمعظم الجرائم الإلكترونية يكتشف صدفة بعد وقت طويل من اقترافها، فالجريمة تتم في أقل من بضع ثواني وبمجرد لمسة على لوح المفاتيح، وتحدث وتنتهي بلا صخب ولا ضجة من طرف مجرم بعيد عن مسرح الجريمة قد يتواجد في بلد آخر أو في قارة أخرى.

أنها مخفية لا يلاحظ إرتكابها الا بمعاينة آثارها بعد مدة من إرتكابها والتخمين بوقوعها فالسرقة الإلكترونية تتم عن طريق نقل البيانات من حاسوب الى آخر مثلا لا تلاحظ الا بعد مدة عكس السطو المسلح الذي يكون بإشتباك مع رجال الأمن وهناك عنف وتحطيم، وحتى في حالة اكتشاف الجريمة قد يصعب إثباتها من قبل رجال الضبطية القضائية والمحققين لأسباب عديدة:

-عدم وجود الاعتراف القانوني من طرف المجرم كما في الجريمة التقليدية وعدم وجود الشهود للاستدلال بأقوالهم.

-سرعة تنفيذ الجريمة الإلكترونية التي تكون في ثواني رغم أن التخطيط لها والتحضير قد يكون في مدة زمنية معتبرة وبمجرد لمسة زر في أقل من ثواني[1].

-عدم وجود دليل مادي لأن الجريمة الإلكترونية لا تترك أثرا ماديا خارجيا ملموسا في مسرح الجريمة، يمكن فحصه فهو ليس مسروقات مادية كالمجوهرات أو أوراق نقدية وليس جثة تعاين أو بصمات يتم التحقق من صاحبها، ولكن أرقام محفوظة ومخزنة في سجلات يمكن محو

[1] عبد الصديق الشيخ، الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد1، لسنة 2020، ص 196.

آثارها بفضل أجهزة الاتصال بكل سهولة، كما يمكن التلاعب بها بالتغيير أو الإزالة حتى عند ضبط الدليل من طرف رجال الضبطية القضائية ورجال التحقيق قد يصعب عليهم التعامل معه، فهو يحتاج إلى مهارة وخبرة فنية من طرف أفراد مؤهلين وخبراء في هذا المجال متمكنين من تقنيات الكمبيوتر والأنظمة المعلوماتية، وهناك دول لا زالت لحد الآن تتعامل مع الجريمة الإلكترونية بنفس الاساليب وإجراءات البحث والتحري والتحقيق التي تتبعها في الجرائم التقليدية وعدم تكوين وخبرة رجال الضبطية القضائية في متابعة الجرائم الإلكترونية وعدم إمتلاكهم الوسائل التقنية المتطورة والمعرفة العلمية اللازمة، مما يصعب عليهم عملهم عند إكتشاف الجريمة في الحصول على الدليل الإلكتروني.

-رجال الضبطية القضائية والمحققون يجدون صعوبة في التعامل مع الدليل الإلكتروني فقد لا يستطيعون تقدير أهميته، كما يمكن أن يتجاهلوه أو قد يتسببون في إتلافه أو تدميره بمجرد لمس لوح المفاتيح أو لا يقومون بمصادرة الدليل أو أداة الجريمة مثل جهاز الذاكرة أو الكمبيوتر أو لواحقه مثل جهاز الماسح الضوئي.

-غالبا ما يرفض القاضي الدليل الإلكتروني لعدم اقتناعه بأدلة الإثبات التي حصل عليها المحققون[1] ويدمر الدليل كذلك بمجرد استعماله.

وحسب رجال القانون لا يتم إكتشاف الجريمة غالبا الا لغباء الجاني وسوء تخطيطه.

الفرع الثاني: خصائص متعمقة بالجاني

تم تقسيمه هو الآخر الى عنصرين :

-أولا: سمات الجناة الخاصة:

بما أن الجريمة المعلوماتية جريمة خاصة فإن المجرم المعلوماتي له صفات خاصة حصرها الاستاذ باركر[2] في كلمة SKRAM وهي:

- المهارة وتعني SKITHS

[1] المرجع نفسه .

[2] خالد داودي، مرجع سابق، ص 32 .

-المعرفة وتعني KNOWLEDG

-الوسيلة وتعني RESOURS

- السلطة وتعني AUTHORITY

-الباعث وتعني MOTIVES

-المجرم المعلوماتي ذكي محترف بحيث يمتلك مهارات تقنية تؤهله لتوظيف إمكانياته في الاختراق والاعتداء ويرتكب جريمته بمقابل مالي لصالح غير.

-مجرم متخصص و متعود على الإجرام فهو مجرم له مهارة عن طريق الدراسة والتخصص أو عن طريق الخبرة التي إكتسبها بسبب مجال عمله في مجال تكنولوجيات المعلومات فهو متخصص في التنفيذ لقدرته الفائقة ومهارته التقنية في مجال المعلوماتية، يستغلها في كسر كلمات المرور وحل الشيفرات ليقوم بإختراق الشبكات والبرامج للحصول على البيانات الغالية الثمن، كما أن هذا المجرم المعلوماتي يستغل دائما قدراته في معاودة الاعتداء والاختراق على الحواسيب والمعلومات المخزنة قصد إثبات تفوقه.

-مجرم إجتماعي وهادئ فلا يلجأ إلى العنف في إرتكاب جريمته معتمدا على الجهد الذهني والفكري بدل الجهد العضلي، وهو إنسان مثقف وعادي يتمتع بحقوقه السياسية والاجتماعية يعيش بين أفراد المجتمع ويعمل سواء في مجال المعلوماتية أو في مجال آخر، وهو إجتماعي لا تظهر عليه علامات الإجرام فهو يمارس حياته الطبيعية الهادئة ويدخل في تجمعات تظم مجرمين مثله لتبادل المعلومات والمهارات وكل ما هو جديد[1] .

ثانيا :طوائف المجرمين الإلكترونيين:

التطور التكنولوجي والمعلوماتي أدى إلى تطور الإجرام الإلكتروني وبالتالي ظهور أصناف من المجرمين المعلوماتيين ويختلف الباعث والدافع لارتكابهم الجرم فهناك من يجد المتعة وهناك من يسعى إلى الانتقام، وآخر إلى الاضرار بشخص أو مؤسسة بمقابل مالي أو بدون

[1] غنية باطلي، مرجع سابق، ص 35 .

مقابل،.... هذا ما أدى إلى تصنيف وتجميع المجرمين الإلكترونيين في مجموعات تجمعهم ميزات مشتركة:

1- القراصنة: وهم هواة ومحترفين هدفهم التسلية والمزاح وليس إحداث الضرر ولا الربح المادي وينقسمون إلى نوعين بينهما تعاون هما:

أ – الهاكرز: هو مصطلح أطلقه طلبة أمريكيون على المتميزين والمتمتعون بقدرة عالية من التقنية، أغلبهم صغار سن ولهم شغف بالحاسوب وهم هواة وهم مقتحمي النظم وهم شباب أو طلبة موهوبون لا يبغون مالا ولا ضررا إنما إثبات قدراتهم ومهارتهم على اكتشاف أو إظهار الأنظمة المخترقة بدافع اللهو والفضول والمزاح.

ب – الكراكرز: قراصنة محترفين هم بالغون تتجاوز اعمارهم 25 سنة فأكثر أو مهنيون ذوي إختصاص هدفهم التخريب وإلحاق الضرر بالضحية، يعيشون من عائدات جرائمهم ويعاودون فعلهم[1].

2-الحاقدون المخربون: ليس لهم فئة عمرية محددة فهدفهم ليس المكاسب ولكن الانتقام من أصحاب العمل والهيئات التي كانوا يعملون لديها، فهم موظفون سابقون تم الاستغناء عنهم، هدفهم إحداث الضرر وليس الحصول على مكاسب مالية، يستغلون معرفتهم بأنظمة الحواسيب لدى هذه المؤسسات لنشر بيانات أو إستعمال البيانات المخزنة في نظامها المعلوماتي أو مسحها.

3-المتجسسون: بدل الطرق التقليدية يستخدم المجرم من جهة إستخباراتية ويستعمل المعلوماتية في جريمته للحصول على معلومات سرية عن دولة وإفشائها لدولة أخرى وتكون عسكرية صناعية أو اقتصادية ويكون غالبا أحد مستخدمي الجهاز المستهدف [2].

[1] المرجع نفسه .

[2] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد، تلمسان، 2018، ص 108.

4-مخترقوا الأنظمة: هم جهاز بحد ذاته يتبادلون المعلومات ويعقدون المؤتمرات لتجديد معلوماتهم حول مواطن الضعف في الأنظمة المعلوماتية، نشاطهم ليس تخريبيا ولكن تستعملهم الأجهزة المختصة والشركات المنتجة لبرامج معالجة البيانات أحيانا لفحصها واختبارها قصد إيجاد برامج أو وسائل حماية من الاعتداء، هدفهم المتعة وليس التخريب.

5- المتطرفون والإرهابيون: ينتمون فيها إلى طائفة معينة ذات أفكار وتوجه خاص بها تستعمل الأنترنت لبث أفكارها وترويجها، والتطرف يكون دينيا أو عرقيا أو جهويا هدفه تغيير المجتمع وفقا لما يعتقد وليس لتحقيق مكاسب شخصية أو معنوية، أما الارهابيون فعادة يرسلون رسائل تهديد ويقومون بتدمير البيانات المخزنة في الأنظمة الحكومية[1] لتسجيل وجهة نظرهم ويستعملون أساليب إقناع وتأثير أحيانا يقع ضحيتها المختصون الذين يدرسونها لمواجهتها.

6- طائفة الربح المادي: وهؤلاء يعملون في مجال الجريمة المنظمة هدفهم الحصول على الأموال بوجه غير مشروع، أو حتى الأفراد الذين يعملون لصالحهم فيرتكبون الجريمة بهدف حل مشاكلهم المادية كلما كانوا بحاجة إلى ذلك.

7-طائفة صغار السن: أو كما يسميهم البعض صغار نوابغ المعلوماتية و في اصطلاح ثاني القانون يطلق عليهم الأحداث[2].

المبحث الثاني: أركان الجريمة الالكترونية وأنواعها:

نتعرض في المطلب الأول الى أركان الجريمة الالكترونية ثم ندرس أنواعها في المطلب الثاني.

[1] المرجع نفسه.

[2] طارق عفيفي، مرجع سابق، ص 63.

المطلب الأول: أركان الجريمة الإلكترونية

لا تختلف الجريمة الإلكترونية رغم ارتكابها على الفضاء الافتراضي عن الجريمة العادية في اشتراط توفر أركان لقيامها. فلها ركن معنوي وركن مادي وركن تشريعي وكل نوع منيا يختص بميزة عن جريمة أخرى، حيث كل جريمة تكاد تنفرد وتختلف عن الأخرى. كما أن هذه الأركان تتسم بالافتراض اي ترتكب في العالم الافتراضي ونوجزها فيما يلي:

الفرع الأول: الركن الشرعي.

أي أن هناك نص قانوني يجرم بهذا الفعل ويدينه ويكون بعد صدور هذا النص فلا يمكن ملاحقة الفاعل بعد الغاء النص، ولا يمكن التوسع في تفسيره بل يجب الالتزام به من طرف القاضي عملا بمبدأ عدم رجعية القوانين الا بنص صريح .في حالة تطبيق الأصلح للمتهم، هناك من دمج الجريمة الالكترونية في القوانين العادية بتكييف النصوص القديمة مع هذه الجرائم الحديثة وهناك من وضع نصوص جديدة خاصة بها [1].

الفرع الثاني: الركن المادي

هي الأفعال والسلوكيات الصادرة عن الانسان العاقل، ومعرفة بداية النشاط والشروع فيه وتحقيق نتيجة، فالأعمال التحضيرية في الجريمة التقليدية لا يعاقب عليها القانون عكس الجريمة الإلكترونية حيث يختلف الأمر، فشراء برامج الاختراق ومعدات فك الشفرات وكلمات المرور، أو حيازة صور دعارة الأطفال هي جريمة بحد ذاتيا دون الدخول في نشاط فارتكاب الجريمة يكون بإتيان تصرف (الايجابي) أو الامتناع عن فعل (السلبي) تسبب في احداث نتيجة هي الحاق ضرر بحق دستوري أو قانوني. وفي الجريمة الالكترونية أيضا لابد من وجود فعل مادي ولابد من وجود البيئة الرقمية والانترنت ومعرفة انه شرع في ارتكاب الفعل وسيرتب نتيجة إذ لابد من توفر:

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، د ذ ط، 2006، ص 25.

01- سلوك مادي

فلا عقاب على الأفكار والخيال والخواطر التي تجول بنفس الفرد، مالم يكن هناك سلوك مادي ايجابي بالقيام بالفعل أو الامتناع عنه، وهو الذي يحدد عدم المشروعية الفعل، وفي الجريمة المعلوماتية لابد من وجود البيئة الرقمية التي هي مسرح الجريمة وأداتها ولابد من وجود شبكة الأنترنت.

02- مباشرة النشاط التقني

السلوك المادي وحده لا يكفي لوجود الجريمة الالكترونية فلا بد من مباشرة نشاط تقني بالدخول غير المشروع الى نظام معالجة أو قواعد المعطيات، فبمجرد وجود دخول الى النظام يعد سلوكا اجراميا حتى ولو لم يتم المساس بالأنظمة والمعطيات، فالنشاط الذي قام به باستخدام جهاز الكمبيوتر والدخول الى شبكة الأنترنت شكل نشاطا او جزءا منه.[1] ورصد هذا الدخول يعد جريمة والنشاط الاجرامي يكون بالاطلاع على المراسلات السرية وعلى البريد الالكتروني، أو الادلاء ببيانات كاذبة.

الفرع الثالث: الركن المعنوي:

هو الركن الثالث للجريمة ويتمثل في الحالة النفسية للجاني والمسلك الذهني وتوافر الإرادة الإجرامية حين ارتكابه الفعل وتوجيهها الى القيام بعمل غير مشروع كانتحال شخصية الغير كما يكون على علم بنتيجة افعاله.

ويتميز الركن المعنوي للجريمة الالكترونية بالتنوع والتغير حسب الجريمة الالكترونية المرتكبة كونها جريمة افتراضية.

فالدخول غير المشروع أولا الى النظام يجب ان يكون على علم بكافة عناصر الجريمة من أن الفعل الذي قام به يشكل جريمة واعتداء على نظام المعالجة الالية وعلى المعلومات والبيانات الموجودة عليه، كما أن دخوله كان بسبب الاختراق الغير مسموح به وان هناك غش

[1] المرجع نفسه .

في الدخول، فيه على علم بأن الدخول غير مسموح لان نظام المعالجة محمي لكن اعتدى عليه، وأحيانا يكون مسموحا لشخص بالدخول الى النظام المعلوماتي ويتجاوزه فيه مقيد بحدود فلا يمكنه الدخول الى انظمة اخرى. لكن هنا الجريمة التي ارتكبها هي جريمة ولوج الى الأنظمة التي ليس مسموحا له بدخولها.

- حالة توافر القصد الجنائي أي يرتكب الفعل قصد احداث الضرر.
- حالة تجاوز الضرر الذي حدث ما كان متوقعا.
- يفترض القصد اذا قام الفاعل او امتنع عن الفعل فادى ذلك النتيجة كانت ضرر جسيم كانت بسبب نشاط الجاني وبالتالي يتحمل النتيجة حتى ولو كان لم يقصدها أو يتحملها[1]. كما ان البقاء ايضا جريمة فحتى لو كان دخوله خطا وبدون قصد فان استمراره في البقاء متعمدا غير مشروع، ويظهر ذلك من خلال تفحص النظام والعلميات التي قام بها اثناء تواجده فيها.
- الاعتداء على سير نظام المعالجة هنا يكون الاعتداء عمديا لان المجرم يقوم بأفعال أما تعرقل سير النظام ببث فيروسات أو تعطله تماما، أو باللهو بمحتوى المعطيات وتعد جريمة إلكترونية الحالة التي يستعمل فيها الموظف الحاسوب لحسابه الشخصي وبحسن نية وأثناء ذلك يلحق ضرار بنظام الحاسوب أو عند ادخال قرص مرن خاص به فتنقل فيروسات.

المطلب الثاني: أنواع الجريمة الإلكترونية

إن أنواع الجرائم الإلكترونية كثيرة حيث لم يوضع لها معايير محددة من أجل تصنيفها وهذا راجع إلى التطور المستمر للشبكة والخدمات التي تقدمها.

الفرع الأول: الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي:

تم تقسيم هذا الفرع الى ثلاث عناصر و هي :

[1] نبيلة هبة هروال، مرجع سابق، ص27 .

أولا: الجرائم الواقعة على الأشخاص:

فرغم الإيجابيات والقواعد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد إلا أنها جعلته أكثر عرضة للانتهاك، ومنها:

1-جريمة التهديد: يقصد به زرع الخوف في النفس، بالضغط على إرادة الإنسان وتخويفه من أضرار ما ستلحقه أو ستلحق أشخاص له صلة بها، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس أو مال الغير.

2-إنتحال شخصية: وهو استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته، ولقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية. وتتم بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيته، للاستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة كالاسم، العنوان الشخصي، رقم بطاقة الائتمان للتمكن من الوصول لماله أو سمعته ..... عن طريق الغش.

3-إنتحال شخصية أحد المواقع: ويتم ذلك عن طريق اختراق أحد المواقع للسيطرة عليه، ليقوم بتركيب برنامج خاص به هناك، باسم الموقع المشهور[1].

4-جرائم السب والقذف: المساس بشرف الغير وسمعتهم، واعتبارهم ويكون القذف والسب كتابيا أو عن طريق مطبوعات أو رسوم، عبر البريد الإلكتروني أو الصوتي، صفحات الويب، بعبارات تمس الشرف. فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية، وقد يكون شخصا طبيعيا أو معنويا، لتصل المعلومات المراد نشرها إلى عدد كبير من مستخدمي شبكة الأنترنت..

5-المواقع الإباحية والدعارة: وجود مواقع على شبكة الانترنيت تحرض على ممارسة الجنس للكبار والقصر، وذلك بنشر صور جنسية للتحريض على ممارسة المحرمات، والجرائم المخلة

[1] محمد عبد الله بن علي المنشاوي، جرائم الإنترنيت في المجتمع السعودي، ماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 55.

بالحياء عن طريق صور، أفلام، رسائل ..... بالإضافة إلى انتشار الصور ومقاطع الفيديو المخلة بالآداب على مواقع الإنترنيت من قبل الغزو الفكري لكي يتداولها الشباب وإفساد أفكارهم وإضعاف إيمانهم. وتوفير الشبكة تسهيلا للدعارة، عبر آلاف المواقع الإباحية، وتسويق الدعارة وتستثمر لها مبالغ ضخمة مع استخدام أحدث التقنيات.

6-التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مظللة أو مغلوطة عن ضحيته، والذي قد يكون فردا أو مؤسسة تجارية أو سياسية.

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كلفها القانون وفي مقدمته الدستور الجزائري حيث تنص المادة 40 منه: "تضمن الدولة عدم انتهاك حرمة الإنسان.[1]

وعليه فإن استخدام الشبكة المعلوماتية في الاعتداء على حرية الفرد وحياته الخاصة وحرمته، والحريات العامة للأفراد، مخالف للقانون ومعاقب عليه.

ثانيا: الجرائم الواقعة على الأموال:

أصبحت معاملات الشراء، البيع والإيجار تتم عبر الشبكة المعلوماتية، وما أنجز عليه من وسائل الدفع والوفاء، فابتكرت معه طرق ووسائل للسطو على هذا التداول المالي بطريق غير مشروع، كالتحويل الإلكتروني، السرقة، القرصنة وغيرها.

1_السرقة الواقعة على البنوك: يتم سرقة المال بالطرق المعلوماتية، عن طريق اختلاس البيانات والمعلومات الشخصية للمجني عليهم، والاستخدام لشخصية الضحية ليقوم بعملية السرقة المتخفية، ما يؤدي بالبنك إلى تحويل البنكي للأموال الإلكتروني أو المادي إلى الجاني. حيث يستخدم الجاني الحاسب الآلي لدخول شبكة الأنترنت والوصول إلى المصاريف والبنوك،

[1] بنظر المادة 1/40 من دستور 1996، ج. ر رقم 76 المؤرخة في 8 ديسمبر 1996، المعدل والمتمم بالقانون رقم 16-01 المؤرخ في 6 مارس 2016، ج. ر رقم 14، المؤرخة في 07 مارس 2016.

وتحويل الأموال الخاصة بالعملات إلى حسابات أخرى.[1] مثال: كالاستيلاء على ماكينات الصرف الآلي والبنوك، يتم فيها نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية.

2_ تجارة المخدرات عبر الأنترنت: تتعلق بالترويج للمخدرات وبيعها، والتحريض على استخدامها، وصناعتها بمختلف أنواعها.

3 _غسيل الأموال: تمارس عبر الأنترنت، حيث استفاد الجناة ما وصلت إليه عصر التقنية المعلوماتية لتوسيع نشاطهم غير المشروع في غسيل أموالهم، بتوفير السرعة وتفادي الحدود الجغرافية، والقوانين المعيقة لغسيل الأموال، وكذا لتشفير عملياتهم وسهولة نقل الأموال واستثمارها لإعطائها الصيغة الشرعية.[2]

4_ قرصنة البرمجيات: هي عملية نسخ وتقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها لناس بسعر أقل، وجريمة نسخ المؤلفات العلمية والأدبية بالطرق الإلكترونية المستحدثة، حيث أن المعلومة الأدبية والفكرية ذات قيمة أدبية ومادية بالإضافة إلى براءات الاختراع التي تحول لمالكها حق معنوي وآخر مالي، نص عليها المشرع في الدستور في المادة44: "حقوق المؤلف يحميها القانون.[3] "بالإضافة إلى قوانين متعلقة بحقوق المؤلف والحقوق المجاورة، وبراءات الاختراع[4]

ثالثا: الجرائم الواقعة على أمن الدولة:

[1] عباس أبو شامة، التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، ونشاطها في الدول العربية، الندوة العلمية للظواهر الإجرامية المستحدثة وسبل مواجهتها، السعودية، أيام 29-30 جوان 1999، ص 20.

[2] صالحة العمري، جريمة غسيل الأموال وطرق مكافحتها، مجلة الاجتهاد القضائي، العدد الخامس، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة د. ذ. س. ن، ص 179.

[3] انظر المادة 2/44 من الدستور ، مرجع سابق.

[4] ينظر الأمر 03-05 المؤرخ في 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، وكذلك الأمر 03 – 07 المؤرخ في 19 جويلية 2003 المتعلق ببراءة الاختراع، ج ر رقم 44 المؤرخة في 23 جويلية 2003.

تقع هذه الجرائم باستعمال النظام المعلوماتي سواء لإفشاء الأسرار التي تخص مصالح الدولة ونظام الدفاع الوطني أو الإرهاب، التجسس...

نصت عليها المادة 394 مكرر 2: "تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد".[1]

1_الإرهاب: تستخدم المجموعات الإرهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن.

2 _التجسس: يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسسات الوطنية أو الدولية، وتستهدف خاصة، التجسس العسكري، السياسي الاقتصادي، وذلك باستخدام التقنية المعلوماتية، وتمارس من قبل دولة على دولة، أو من شركة على شركة.... وذلك بالاطلاع على المعلومات الخاصة المؤمنة في جهاز آلي وغير مسموح الاطلاع عليه، كأن تكون من قبل أسرار الدولة.

الفرع الثاني: الجرائم المعلوماتية الواقعة على النظام المعلوماتي:

وهي الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف سواء المكونات المادية لنظام المعلومات أو برامج النظام المعلوماتي، أو المعلومات المدرجة بالنظام المعلوماتي على النحو التالي:

[1] ينظر المادة 394 مكرر 2 من الأمر 66- 156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل المتمم.

أولا: الاعتداء على برامج النظام المعلوماتي:

ويتوجب هنا معرفة ودراية ذات درجة عالية في مجال البرمجة، وتقع هذه الجرائم إما على البرامج التطبيقية أو برامج التشغيل.

1_البرامج التطبيقية: وهنا يقوم الجاني بتحديد البرامج ثم التلاعب فيها للاستفادة منه ماديا، وذلك بتعديل البرنامج: ويكون الهدف من تعديل البرامج اختلاس النقود، حتى ولو كان باستقطاع مبالغ قليلة لكن لفترات زمنية طويلة لتحقيق الفائدة، بدون إثارة الشبهات، أما التلاعب: فيأخذ عدة أشكال، فقد يكون عن طريق زرع برنامج فرعي في البرنامج الأصلي مثلا يسمح له الدخول غير المشروع في العناصر الضرورية للنظام المعلوماتي حيث يصعب اكتشاف هذا البرنامج لدقته وصغر حجمه.[1]

2 _برامج التشغيل: وهي البرامج المسؤولة عن عمل نظام معلوماتي من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام.

وتقوم الجريمة هنا عن طريق تزويد البرامج بمجموعة تعليمات إضافية ليسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي.[2]

شكلين هما وتأخذ المصيدة وهو إعداد برنامج به ممرات وفراغات في البرنامج وتفرعات إضافية، وهنا يمكن للمبرمج استخدام البرنامج في أي وقت، ويصبح المهيمن على النظام وعلى صاحب العمل. أما تصميم البرنامج هو القيام ببرنامج خصيصا يصعب اكتشافه لارتكاب الجريمة ومراقبة تنفيذها.

ثانيا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

ويقصد به الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات، الكابلات والاعتداء عليها يكون بالسرقة لهذه المعدات، أو عن طريق الإتلاف العمدي كإحراقها ضرب

[1] نبيلة هبة هروال، مرجع سابق، ص 30،

[2] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، الطبعة الثانية، 2006، ص87 .

الآلات بشيء ثقيل، العبث بمفاتيح التشغيل خربشة الأسطوانات لكي لا تصبح صالحة للاستعمال[1]

ثالثا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

إن المعلومات المعالجة آليا هي أساس عمل النظام المعلوماتي، لأنها ذات قيمة مادية واقتصادية، لذلك تعد هدفا للجرائم الإلكترونية من خلال التلاعب فيها أو إتلافها.

1_التلاعب: يكون في المعلومات الموجودة على النظام المعلوماتي بطريقة مباشرة أو غير مباشرة، فيتم التلاعب المباشر عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، كضم مستخدمين غير موجودين بالعمل بهدف الحصول على مرتباتهم أو الإبقاء على مستخدمين تركوا العمل للحصول على مبالغ شهرية، أو عن طريق تحويل مبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك، وتسجيلها وإعادة ترحيلها وإرسالها لحساب آخر في بنك آخر، بهدف اختلاس الأموال.[2]

أما التلاعب الغير مباشر، فيتم عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين، أو التلاعب عن بعد بمعرفة أرقام وشفرات

الحسابات،[3] قصد التلاعب في الشرائط الممغنطة، أو باستخدام الجاني كلمة السر أو مفتاح الشفرة، وإمكانية تسلل الجاني إلى المعلومات المخزنة والحصول على المنفعة المالية من مسافات بعيدة.

2_إتلاف المعلومات: في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج والبيانات المخزنة والمتبادلتين الحواسب وشبكاته، وتدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي، ويكون الإتلاف العمدي

---

[1] زكي زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجامعة المصرية للقانون الجنائي، القاهرة أيام 25 – 28 أكتوبر 1993، ص471 .

[2] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط 2، دار النهضة العربية، القاهرة، 1994، ص 7.

[3] المرجع نفسه .

للبرامج والبيانات كمحوها أو تدميرها الكترونيا، أو تشويهها على نحو يجعلها غير صالحة للاستعمال.

خلاصة الفصل الأول:

من خلال دراستنا لمفهوم الجريمة الإلكترونية يتضح أنه لم يتفق الفقهاء على تعريف جامع وموحد للجريمة الإلكترونية، والجرائم الإلكترونية تعد من أخطر الجرائم والشخص الذي يرتكبها هو مجرم غير تقليدي له مميزاته الخاصة، وهي من الجرائم العابرة للحدود ويصعب إكتشافها وإذا ما اكتشفت يصعب إثباتها وما يزيد من خطورة هذه الجرائم أن للضحية دور مهم فيها والجرائم الإلكترونية تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية، وبشكل عام فإن إستخدام وسائل الإثبات الإلكترونية في إثبات الجرائم الإلكترونية يعتمد على التكنلوجيا والتقنيات المتاحة والقانون الذي يحكم الدولة .

الفصل الثاني

الآليات القانونية لمكافحة الجرائم الإلكترونية

تمهيد :

إن موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية أصبح هاجسا يؤرق رجال القانون بصفة خاصة لذلك بات من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في التقنيات الرقمية ورجال القانون والمؤسسات الرسمية في الدولة وعلى المستوى الدولي أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم كما تبرز أهمية هاته الدراسة من الناحية النظرية في معرفة مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية وردع مرتكبيها و مدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة ، و تعد الجرائم الالكترونية ذات طابع عالمي فهي جرائم عابرة للحدود كما أنها تترك أثرا ماديا في مسرح الجريمة، وهناك العديد من الأليات والإجراءات المعمول بها لقمع الجريمة المعلوماتية على المستوى الوطني والدولي لما تشكله من خطر على أمن الدولة والأفراد والمصالح الخاصة و تعد مكافحة الجريمة الإلكترونية أو أي نشاط ضار من أولويات التخطيط لأي سياسة سواء كانت تجريميه أو عقابية، تسعى لتحقيق هدف هام وفعال هو فرض الأمن والطمأنينة بين الناس من خلال حفظ مصالحهم ، و سنتناول في هذا الفصل الآليات الدولية لمكافحة الجريمة الإلكترونية في المبحث الأول ، و آليات مكافحة الجرائم الإلكترونية في المبحث الثاني .

المبحث الأول: الآليات الدولية لمكافحة الجريمة الإلكترونية

أضحت الجرائم الإلكترونية كإحدى الجرائم المعلوماتية في العصر الراهن التي رافقت عمر التقدم التكنولوجي، خاصة بعد ظهور شبكة المعلومات الدولية بسبب تقدم العلمي من خلاله ساعد على انتشار وتنوع السلوك الإجرامي الذي أصبح يهدد الأفراد في مختلف المجالات، فأصبح اهتمام بعض الدول والمنظمات الدولية للبحث عن الثغرات المكافحة الجريمة الإلكترونية. ومن هنا ستحاول عرض في هذا المبحث الجهود الدولية والعربية لمكافحة الجريمة.

المطلب الأول: الجهود الغربية لمكافحة الجريمة الإلكترونية

توجد العديد من الهيئات والمنظمات تلعب دورها ما في إبرام اتفاقيات في محاولة اقامة تعاون دولي لتحقيق أهداف مجتمع دولي ويردع من مقرها الجرائم سنتطرق في هذا المطلب إلى التعاون الدولي وجهود المبذولة لمكافحة الجريمة المعلوماتية من خلال فروع.

الفرع الأول: التعاون الدولي

ان التعاون الدولي في المسائل الجنائية وفقا للالتزامات الدولية والقوانين الوطنية هو حجز الزاوية في الجهود التي تبذلها الدول لمنع الجريمة، لا سيما في أشكالها عبر الوطن مثل جرائم المعلومات، ومحاكمة ومعاقبة مرتكبيها، ويشجع دول العالم على مواصلة وتعزيز هذه الأنشطة على جميع المستويات.[1]

1.التعاون القضائي:

تتطلب إجراءات التحقيق في الجرائم الإلكترونية وملاحقتها تتبع النشاط الإجرامي والأمر الذي يلزم نقص أثار الجريمة من مصدرها إلى نهاية تنفيذها وتحديد مواقع الضرر الذي تسببت فيه

[1] مناصرة يوسف، جرائم المساس بأنظمة المعالجة الألية للمعطيات، د ذ ط، دار الخلدونية، الجزائر، 2018، ص 263.

الجريمة. هناك نوع من التعاون بين السلطات القضائية في هذه الدول من أجل توسيع نطاق الاختصاص، وستعرض أهم صورتين في مجال التعاون القضائي.

1.1. التعاون الأمني

من الواضح أن الحدود الجغرافية ومشكلة الاقتصاص الإقليمي نفق حاجر أمام الإجراءات الجنائية لمعالجة مرتكبي الجرائم، وخاصة في جرائم الأنترنت والتي تتميز بأنها جريمة عابرة للحدود والحاجة الماسة إلى توحيد الجهود فيما يتعلق بتبادل البيانات والمعلومات المتعلقة بالجريمة التي تتيح الكشف عن هوية المجرمين، حيث يستحيل على الدولة وحدها القضاء على هذه الجريمة.

فأجهزة الشرطة لا يمكنها تعقب مرتكبي الجرائم وملاحقتها إلا من نطاق حدودها أي أنه إذا كان المجرم خارج حدود الدولة فإنه يبقى في مأمن من المتابعة ونجد في هذا الإطار أن هناك ثلاثة أوجه لإقامة هذا التعاون:

أولا انشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي جرائم الأنترنت ونشرها القصد فيها هو تنمية التعاون بين سلطات الدول القضائية في مجال مكافحة الجريمة وملاحقة المجرمين بإضافة الى تقديم المعونة وتبادل الخبرات عند الاقتضاء [1] .

2.1. التعاون في إطار المنظمة الدولية للشرطة الجنائية الأنثربول:

وتهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف بطرق فعالة في مكافحة الجريمة من خلال جمع البيانات والمعلومات المتعلقة بالجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أراضي الدولة. المنظمة إليها و تبادل فيما بينها بالإضافة أن التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في دول الأطراف.

3.1.القيام بعمليات أمنية مشتركة : عندما يتم تعقب الجريمة المعلوماتية، يتم تتبع الأدلة الرقمية ومصادرتها ويتم إجراء عمليات التفتيش عبر الحدود بواسطة أجهزة الإعلام الآلي

[1] فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق ،فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2010، ص 375 و376.

والأنظمة المعلوماتية وشبكات الاتصالات بحثا عن الأدلة والبراهين وكل هذه الإجراءات تتطلب تعاونا دوليا.

2. المساعدات القضائية بوجه عام

المقصود بالمساعدة القضائية الدولية هو كل إجراء قضائي تتخذه دولة ما من شأنه تسهيل عملية المتابعة والمحاكمة الجزائية في بلد ما فيما يتعلق بجريمة ما. وبناء على هذا التعريف تظهر الحاجة الملحة للمساعدة القضائية الدولية في عملية مكافحة الجرائم بوجه عام والجريمة الإلكترونية بوجه خاص. وتتخذ المساعدة القضائية صور نذكر منها:

أولا: تبادل المعلومات، يتم ذلك عن طريق تبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية أثناء قيامها بعملية التحقيق في الجريمة التي يتم فيها رفع دعوى ضد أحد رعاياها أو مواطني دولة أخرى ، والتي يشمل تبادل السوابق القضائية لأتباع مثل هذه الجرائم ونجد عدة تطبيقات لهذه الصورة و ورد في الفقرات 3 و4 من المادة الثامنة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

ثانيا: نقل الإجراءات تعني أن قيام دولة ما بناء على اتفاقية أو معاهدة تتخذ إجراءات جنائية أثناء قيامها بعملية ارتكاب جريمة في أراضي دولة أخرى ولصالح هذا البلد عند استفاء شروط معينة من أهمها التجريم المزدوج ويعنى أن الفعل المنسوب إلى شخص يشكل جريمة في البلد الطالبة، والدولة المطلوبة إليها نقل الإجراءات. وبالإضافة إلى شرعية الإجراءات المطلوب اتخاذها، بمعنى أن الإجراءات الواجب اتخاذها مقررة في قانون الدولة المطلوب منها من نفس الجريمة، كما أن أحد الشروط التي يجب استفاؤها هو أن الإجراءات المطلوب اتخاذها مهمة جدا بحيث تلعب دوراً مهما في الوصول إلى الحقيقة [1].

ثالثا: الإنابة القضائية الدولية، يقصد بالإنابة القضائية الدولية طلب اتخاذ إجراء قضائي من اجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك للفصل في مسألة معروضة على السلطة القضائية في الدول الطالبة ويتعذر عليها القيام

[1] المرجع نفسه ، ص 377 .

فالإنابة القضائية تعبر عن قيام دولة ما لمباشرة إجراء فضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمة لدولة أخرى نيابة عنها، بناء على طلب تلك الدولة المناب عنها، ووفقا لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن وهدفها هو نقل الإجراءات الجنائية لمواجهة التطور الحاصل في الظواهر الإجرامية وتذليل العقبات التي تعترض سير الإجراءات الجنائية المتعلقة بالقضايا التي تتجاوز الحدود الوطنية.

رابعا: تعليم المجرمين: حيث يعتبر من صور المساعدة القضائية الدولية المتبادلة في تسليم المجرمين، والمقصود بالتسليم هو تخلي الدولة عن أي شخص موجود على أراضيها إلى دولة أخرى تتم ملاحقته أو الحكم عليه فيها، وبناء على طلب الدولة وينطبق على هذا المفهوم كل من عبارات تسليم المجرمين، الاسترداد أو نقل الأشخاص.

وتستخدم معظم التشريعات الثانية والمتعددة الأطراف والاتفاقيات القضائية عبارة التسليم والاسترداد لأن كل واحدة تهدف إلى نفس المعنى، أما فيما يتعلق ينقل الأشخاص فهو يستخدم في مجال المحكوم عليهم لتنفيذ الأحكام الصادرة بحقهم.

فإن التسليم أو الإسترداد نجد أساسه القانوني في التشريعات الداخلية و الإتفاقيات الثنائية والمتعددة الأطراف التي تنظم القواعد المتعاقدة بشأن تبادل المجرمين سواء كانوا في طور الملاحقة أو المحكومين. بحيث تطبق الاتفاقية التي تعلو على القانون من حيث التطبيق [1].

الفرع الثاني: الاختصاص القضائي الدولي.

قسمنا هذا الفرع الى بندين و هما :

البند الأول: الإختصاص القضائي الدولي

تثار مشكلة الاختصاص القضائي الدولي فيما يتعلق بالجرائم المرتكبة في نطاق إقليم دولة واحدة، حيث يمكن للدولة المعلوماتية إلى حد أكبر مما هي عليه على مستوى إقليم دولة

[1] المرجع نفسه ، ص 379 .

و الحد من المشكلة على المستوى الوطني أو المحلي، من خلال النصوص القانونية التي يمكن الموافقة عليها في هذه الدولة أو تلك، لأن الجريمة محصورة في النطاق الإقليمي للدولة ومعالجتها مرتبطة بكل دولة على حدى، على عكس مشكلة الاختصاص على المستوى الدولي لأن الجريمة في الأخير لا ترتبط بالحدود الإقليمية لدولة ما بل بالعكس هي جريمة عابرة للحدود بإضافة إلى اختلاف التشريعات والأنظمة القانونية من دولة إلى دولة أخرى في مواجهة هذه الجرائم، وقد يحدث أن الجريمة ارتكبت في إقليم دولة معينة من قبل أجنبي، وفي هذه الحالة تخضع الجريمة للإختصاص الجنائي للدولة الأولى على أساس مبدأ الإقليمية، وتخضع أيضا لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي وقد تكون هذه الجريمة احدى الجرائم التي تهدد أمن وسلامة دولة أخرى، ثم تتدخل في اختصاصها بناء على مبدأ العينة [1].

البند الثاني: الاختصاص القضائي الداخلي

يطلق على هذا النوع من الاختصاص القضائي بالاختصاص الإقليمي أو الداخلي. نظراً لأن القضاء الوطني هو المختص بالفصل في القضايا الجزائية، ويستند إلى تحديد الإطار الجغرافي، أو دائرة الاختصاص المكاني في منطقة معينة من أراضي الدولة، ويستند هذا التقسيم إلى ثلاث معابر هي: مكان وقوع الجريمة، أو مكان الإقامة المتهم، أو مكان القبض على المتهم.

وبهذا الخصوص تحت المادة 37 ق. إ. ج. ج بقولها يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص ولو حصل هذا القبض لسبب آخر.

[1] مناصرة يوسف ، مرجع سابق ،ص 271 .

وكما نصت المادة 329 ق إ ج ج: "تختص محليا بالنظر في الجنحة محكمة محل الجريمة، أو محل إقامة أحد المتهمين أو شركائهم، أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبا آخر.[1]

ومن خلال النصين السابقين يتضح أن الاختصاص القضائي يتطلب توافر حالة من الحالات الثلاثة التالية:

1/ أن تكون الجريمة قد أركبت في محلها، أو أن أحد عناصرها مادي، أو تم تحقيق شكل من أشكال الاستمرارية للجريمة المستمرة، أو أي فعل اعتيادي أو متسلسل فيما يتعلق بالجريمة المركبة فعل من أعمال الشروع في التنفيذ في منطقة الاختصاص المكاني لعضو النيابة العامة أو قاضي التحقيق.

2/ أن تكون إقامة المتهم أو المشتبه به، أو إقامة أحد المشتبه بهم في دائرة اختصاص عضو النيابة العامة أو قاضي التحقيق، ويتحدد مكان الإقامة بوقت اتيان الجريمة.

3/ أن يكون قد ألقى القبض على أحد المتهمين أو المشبه بهم في نطاق تلك الدائرة.

وقد مدد المشرع الجزائري الاختصاص القضائي بالنسبة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات، وغيرها من الجرائم[2] "ما نصت المادة (37) والمادة (80) والمادة (329) ق ا ج ج .

حيث نصت المادة 37 فقرة 2 على أنه: "يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

[1] انظر المادة 37 ق 1 والمادة 329 من الأمر رقم 04-14 المحل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية عند 71، المؤرخ في 10 نوفمبر 2004 .

[2] فايز محمد راجح غلاب، مرجع سابق، الصفحة 377 .

كما نصت المادة 80 على: "يجوز لقاضي التحقيق أن ينتقل صحبة كاتبه بعد إخطار وكيل الجمهورية بمحكمته إلى دوائر اختصاص المحاكم المجاورة للدوائر التي يباشر فيها وظيفته للقيام بجميع إجراءات التحقيق إذا ما إستلزمت ضرورات التحقيق أن يقوم بذلك وعلى أن يخطر مقدما وكيل الجمهورية بالمحكمة التي سينتقل إلى دائرتها وينوه في محضره إلى الأسباب التي دعت إلى انتقاله"

وكذلك تحت المادة 329 فقرة 5 على: "يجوز تحديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف".[1]

وعليه فإن المشرع الجزائري قد حسم مشكلة تنازع الاختصاص بين السلطات القضائية المتواجدة في إقليم الدولة، وهو اختصاص يتم تحديده بـ:

1-نطاق ضرورة التحقيق حيث أجازت المادة 80 ق إ ج ج لقاضي التحقيق أن يقوم بكل إجراءات التحقيق في نطاق إختصاص المحاكم المجاورة لنطاق اختصاصه وفق شروط:

- أن تكون هناك ضرورة للانتقال خارج نطاق اختصاصه المكاني.
- أن يخطر وكيل الجمهورية الذي يعمل في نفس دائرة اختصاصه .
- اخطار وكيل الجمهورية في نطاق الاختصاص لدعائم التمديد اليه
- تحديد الأسباب التي جعلته يمتد لدائرة اختصاصه المكانية في محضر المعاينة.

2- كما يتم تمديد الاختصاص وفقا للقضايا الأخرى التي تشمل جرائم معينة تشكل تهديد أكبر لأمن المجتمع، بما في ذلك الجرائم التي تؤثر على أنظمة معالجة البيانات الآلية. حتى يتمكن وكيل الجمهورية من توسيع نطاق اختصاصه المحلى إلى اختصاص المحاكم الأخرى، ويمكن

[1] انظر المادة 37 فـ2 و80 والمادة 329 فـ5 من القانون 04-14 المتضمن قانون الاجراءات الجزائية، مرجع سابق .

لقاضى التحقيق إجراء أي تفتيش أو حجز على امتداد الأراضي الوطنية، ويمكن أيضا توسيع اختصاص المحكمة ليشمل اختصاص المحاكم الأخرى.[1]

الفرع الثالث: جهود الأمم المتحدة والأوربية لمكافحة الجريمة الإلكترونية

قسمناه هو الآخر الى بندين و هما :

البند الأول : جهود الأمم المتحدة لمكافحة الجريمة الإلكترونية:

تبذل الأمم المتحدة جهوداً كبيرة في مجال مواجهة الجرائم المعلوماتية، وتؤكد على ضرورة تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون للحد من انتشارها وتفاقم آثارها،[2] أصدرت منظمة الأمم المتحدة في مؤتمرها الثامن لمنع الجريمة ومعاملة المجرمين قراراً بشأن الجرائم المتصلة بالحاسوب وتبين من هذا القرار أن إجراء الدولة لمكافحة الجرائم المعلوماتية يتطلب من الدول الأعضاء اتخاذ إجراءات وتتلخص في:

- تحديث القوانين والأغراض الجنائية الخاصة بها، بما في ذلك الإجراءات المتخذة لضمان إجراء التعديلات ويتم تطبيق القوانين الجنائية (التحقيق ، قبول الأدلة) بالشكل المناسب إذا دعت الضرورة.
- مصادرة العائدات من الأنشطة غير مشروعة.
- اتخاذ الإجراءات الأمنية والوقائية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.
- حماية مصالح الدولة وحقوق ضحايا جرائم المعلوماتية وكذلك التعاون مع المنظمات المهتمة بموضوع جرائم الأنترنت وتدريس الآداب المتبعة في استخدام الحاسوب ضمن المناهج المدرسية.

[1] فايز محمد راجح غلاب، مرجع سابق، الصفحة 377و 378 .

[2] فاروق خلف ،الآليات القانونية لمكافحة الجريمة المعلوماتية ، مجلة الحقوق و الحريات، كلية الحقوق، جامعة جمة الخضر، الوادي، العدد 2، 2015، ص 11 .

فتزايد الجرائم المرتكبة عبر الانترنت والمشكلات التي تثيرها أدى إلى قيام الأمم المتحدة بإبرام اتفاقية خاصة بمكافحة إساءة استخدام التكنولوجيا للأغراض الإجرامية في عام 2000، حيث أكدت على ضرورة تعزيز التكنولوجيا و التنسيق والتعاون بين الدول، وكذلك :

عقد منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية في البرازيل أيام 12، 19 أفريل 2010 وبناء على ذلك ناقشت في دول الأعضاء بعض التطورات الحديثة في استخدام العلوم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة جرائم الحاسوب.[1]

البند الثاني: الجهود الأوروبية لمكافحة الجريمة الإلكترونية

تشكل الجرائم المعلوماتية مصدر قلق كبير للدول الكبيرة وتمثل تحديا جديدا للمجتمع الدولي، خاصة في ظل التطور السريع والمتعاقب والذي يصاحبه تطور سريع في هذه الجرائم فتعددت الجهود المبذولة لمواجهة هذه الجرائم سواء كانت من طرف منظمة التعاون الاقتصادي والتنمية أو من طرف المجلس الأوروبي.

أولا : منظمة التعاون الاقتصادي والتنمية

اهتمت منظمة التعاون الاقتصادي والتنمية بالمشكلات التي أثارها ظهور نظم المعلومات في الحياة الاقتصادية عام 1977م، وقد بدأ هذا الاهتمام في البداية يميل إلى حماية الخصوصية من التهديد المعلوماتي لها، وهذا الاهتمام أنتج قواعد ارشادية وتوصيات للدول الأعضاء في تشريعاتها الوطنية. حيث نصت على عقوبة جنائية في حالة مخالفة هذه الإرشادات والتوصيات فهذه التوصيات والتعليمات تتعلق بحماية الأدلة ذات طابع شخصي (البينات الشخصية)، وتتمثل هذه القواعد والإرشادات في:

- تحديد الهدف الذي يتم جمع البينات من أجليه.
- يجب مراعاة القواعد الشكلية للمحافظة على البيانات.

[1] بن علية بن جدو، تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، جامعة بومرداس، المجلد07، العدد02، تاريخ 2022/03/01، ص 309 و 308.

- الإنفتاح وهذا يتطلب أن يكون على ما يتعلق بالحياة الشخصية، من حيث السياسة العامة للتطوير والتخطيط والتنفيذ ويكون متاحا معرفتها للجميع.

المشاركة العربية تتطلب أن يكون للناس حق في الوصول إلى بياناتهم ومعرفتها والحق في الرد عليها.

فهذه القواعد لا تعد الزامية بل هي إرشادات وتوصيات فقط، وتغطى على الأشخاص العادين وتطبق أيضا على القطاع العام والخاص وتتعلق المعالجة آليا [1].

وبداية من عام 1983م بدأت المنظمة باهتمام بجرائم المعلوماتية من خلال اجتماعات مؤتمرات للبحث عن هذه الظاهرة الإجرامية وفي 1985م تم تشكيل لجنة لدراسة الجريمة المعلوماتية من خلال إجراء مسح لهذه الجريمة لكل دول أعضاء المنظمة، وفي 1986م تم صدور تقرير بخصوص جرائم الحاسب الآلي وأوصت اللجنة في تقريرها بعد تحليل النظم القانونية بالدول الأعضاء بضرورة مراجعة المشكلات الناجمة عن الجرائم الإلكترونية في قوانينها الداخلية وبعد ذلك اتجهت المنظمة إلى الاهتمام بحماية أنظمة وشبكات المعلوماتية وذلك بإصدار التوصيات الخاصة بالتدابير والإجراءات المفروضة على الأعضاء لحماية أنظمة المعلومات.

ثانيا: جهود المجلس الأوروبي في مكافحة الجريمة الإلكترونية (المعاهدة الأوروبية):

حيث وقعت اللجنة الخاصة بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية للمعاهدة وهدفها مساعدة الدول في مكافحة الجرائم الإلكترونية وبعد إتمام المصادقة عليها من قبل رئاسة المجلس وتوقيعها من قبل البلدان ، يستلزم منها القوانين الضرورية بالحد الأدنى للتعامل مع جرائم التقنية العالمية بما في ذلك الدخول غير المصرح به والتلاعب بالبيانات والاحتيال والتزوير التي لها علاقة بالكمبيوتر.

وتضمنت المعاهدة والتي تم تعديلها 27 مرة قبل الموافقة عليها، حيث تتكفل الحكومات بحق المراقبة وتلزم الدول بمساعدة بعضها في جمع الأدلة وفرض القانون .

[1] بن مكي نجاة، السياسة الجنائية لمكافحة الجرائم المعلوماتية، دار الخلدونية، الجزائر، 2017، ص 117، 119.

فصلاحيات الدولة الجديدة ستكون على حساب حماية المواطنين من إساءة الحكومة من استخدام السلطات التي أعطتها لهم تلك الاتفاقية التي قد يسوء استخدامها[1].

الفرع الرابع: أهم الاتفاقيات والمنظمات المواجهة للجرائم المعلوماتية

تم تقسيمه الى أربعة بنود و هي :

البند الأول: إتفاقية بودابست: هي من أبرز الاتفاقيات الدولية التي أبرمت لمكافحة الجريمة الإلكترونية ووقعت في العاصمة بودابست والمعروفة بالاتفاقية الدولية لمكافحة الإجرام عبر الأنترنت حيث تتكون الاتفاقية من ديباجة وثماني وأربعون مادة موزعة على أربعة فصول:

الأول: يعالج استخدام المصطلحات، أما الثاني يعالج الإجراءات الواجب اتخاذها على المستوى الوطني، والفصل الثالث يتضمن التعاون الدولي، والفصل الرابع يحدد الأحكام الختامية.[2]

فالهدف من الاتفاقية هو السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية، وتم التأكيد على التعاون الإقليمي والدولي في مواجهة جرائم الكمبيوتر وايجاد دليل للتدابير التشريعية الوطنية، وتهدف أيضا لتحقيق التوازن بين حماية حقوق الإنسان الأساسية (المعترف بها بموجب اتفاقية مجلس أوربا لحماية حقوق الإنسان 1950م والاتفاقية العالمية الأخرى في ميدان حقوق الإنسان) وتحديد الحقوق المتصلة بالرأي وحرية الوصول للمعلومات وحرية البحث والتنقل للمعلومات والأفكار.[3]

البند الثاني: اتفاقية برن لحماية المصنفات الأدبية والفنية

في القرن التاسع عشر بدأ الحديث عن الإطار التشريعي لقوانين الملكية الفكرية بصفة عامة، وعندما اشتدت الحركة الدولية التي تطالب بحماية حقوق الملكية الفكرية فتم عقد معاهدة برن

[1] جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، ط 1، دار البداية ناشرون الموزعون، عمان، 2010، ص 228، 229.

[2] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، الجامعة الجديدة، الإسكندرية، 2015، ص98

[3] عبد الله عبد الكريم عبد الله، الجرائم المعلوماتية والأنترنت، ط 1، منشورات الحلبي الحقوقية، لبنان، 2007، ص 127، 126.

بسويسرا في 9 سبتمبر 1886 والمكملة بباريس في 4 ماي 1896 والمعدلة ببرلين في 13 نوفمبر 1908، والمكملة بيرن في 20 مارس 1914 والمعدلة بروما في 2 جوان 1971 والمكملة في 28 سبتمبر 1979، حيث أقرت الاتفاقية لحماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية والعلمية أيا كانت طريقة التعبير عنها.

وبموجب مرسوم رئاسي رقم 97-341 المؤرخ في 13 سبتمبر 1997 انضمت الجزائر بتحفظ إلى اتفاقية الحماية للمصنفات الأدبية والفنية فإنها تعتبر البحر الأساسي في مجال الحماية الدولية لحق المؤلف.

ويستلزم من أعضاء الاتفاقية توفير الحد الأدنى لحماية حقوق المؤلف لفترة زمنية ويستنتج أن هذه الاتفاقية هي أول اتفاقية عالمية وضعت مبادئ عامة لحقوق الملكية الفكرية وكذا اهتمامها بالقواعد الموضوعية وتعتمدها كل الاتفاقيات اللاحقة كمرجع، ولكن من الجانب الآخر لم تتطرق الى حماية برامج الحاسب الآلي بصورة مباشرة ولكن هذا لا يعنى عدم الحاجة إلى اتفاقيات أخرى تعتنى أكثر ببرامج الحاسوب وتخضعها للتنظيم وهذا ما حاول الجهد الدولي بلوغه.[1]

البند الثالث: جهود منظمة الانتربول Interpol

انشأت منظمة الإنتربول نظاما خاصا للتعاون، ويعتبر نظام وطني والمرجعية المركزية ويوجد في كل دولة من الدول الأعضاء في منظمة الإنتربول مكتب مركزي وطني يمثل نقطة الاتصال مع الإدارات الأجنبية التي تجرى تحقيقات خارج حدودها.

وتضم شبكة من المحققين العاملين في الوحدات الوطنية المعنية بالجرائم إجراء الاتصالات الميدانية بين الدول الأعضاء والاستماع فيه قدر الامكان، ومن مهام هذا النظام تطوير الاستراتيجيات والمعلومات المتعلقة بأحداث الأساليب الإجرامية في مجال جرائم تقنية المعلومات.

[1] بن مكى نجاة، مرجع سابق، ص 96.

كما قامت المنظمة بوضع برنامج خاص لمكافحة الإجرام المعلوماتي بالتركيز على التدريب والعمليات ويعمل على مواكبة التهديدات ويهدف هذا البرنامج إلى:

- تقديم دورات تدريبية لوضع معايير معينة والتزام بها.
- تنسيق ودعم العمليات الدولية .
- مساعدة الدول الأعضاء على التحقيق في الهجمات أو الجرائم الالكترونية من خلال تقديم خدمات في مجال التحقيق وقواعد البيانات .
- تحديد التهديدات وتبادل معلومات الاستخبار في هذا المجال مع الدول الأعضاء.
- إنشاء بوابة آمنة على شبكة الأنترنت لنشر المعلومات والوثائق العملياتية.[1]

البند الرابع : جهود الإتحاد الإفريقي ومجموعة الدول الثمانية G8

من أهم الاتفاقيات والمنظمات المواجهة للجرائم المعلوماتية نجد :

أولا: جهود الإتحاد الإفريقي:

قام الاتحاد الافريقي بطلب انعقاد مؤتمر استثنائي لوزارة الاتحاد الأفريقي المسؤولة عن تكنولوجيا المعلومات والاتصالات، الذي انعقد في جنوب افريقيا في فترة 02 إلى 05 نوفمبر 2009 من مفوضية الاتحاد الإفريقي بالاشتراك مع لجنة الأمم المتحدة الاقتصادية لإفريقيا الإعداد لاتفاقية حول التشريع القضائي القائمة على حاجيات القارة والالتزام بالمتطلبات القانونية والتنظيمية للمعاملات الإلكترونية والأمن الإلكتروني وحماية البيانات الشخصية وأوصت بضرورة توفير الحماية القانونية لأنظمة المعلوماتية التي تعتبر قيمة بالنسبة للمجتمع مما يجعل من التشريعات ضد الجريمة الإلكترونية في جوان 2014، حيث اجتمع مجموعة من القادة الاتحاد الإفريقي مكون من 54 حكومة ووافقوا على اتفاقية الاتحاد الأفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية.

ثانيا : جهود مجموعة الدول الثماني G8

[1] مراد مشوس، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، جامعة غرداية، العدد02، 2019/12/20.

تبنت وزارة العدل والداخلية لبلدان الثمانية في اجتماعاتهم المختلفة سياسات لمكافحة العديد من الجرائم الإلكترونية على أساس المبادئ التالية:

وهي عدم توفير الملاذ الأمن للمعتدى على تقنية المعلومات والتنسيق بين جميع الدول المعنية في ملاحقة و مقاضات مرتكبي الجرائم الإلكترونية وتدريب العاملين في مجال تنفيذ القانون وتجهيزهم بالمعدات اللازمة للتعامل مع جرائم التكنولوجيا العالمية. وعليه دعت الدول الثمانية لمواصلة العمل للوصول إلى حلول دولية ناجحة ومن خلال عقد اتفاقية دولية، ومن توصيات "68" بالنسبة للجرائم الإلكترونية موجودة في إطار الباب من المعاهدة وتتلخص في:

وجب على الدول أن تجرم الانتهاكات على حقوق غير على الشبكة العنكبوتية التي يستوجب فرض عقوبات جزائية التي تعالج المشاكل المتعلقة بالتحقيقات القضائية لمنع الجريمة وإقامة تعاون دولي يتعلق بمكافحة هذه الانتهاكات واتخاد خطوات لمنع الجريمة ذات التقنية العالية.[1]

وجدير بالذكر فقد تطرقت سابقا إلى جهود منظمة التعاون الاقتصادي والتنمية فهي أيضا اهتمت بمجال الجرائم المعلوماتية وحاولت التصدي لها من خلال قواعد و ارشادات.

المطلب الثاني : الجهود العربية المبذولة لمواجهة الجريمة الإلكترونية

انتشرت الجريمة الإلكترونية في المنطقة العربية كما انتشرت في بقية العالم وفي ظل غياب أطر قانونية واضحة وشاملة تضمنت مكافحة الجرائم المتعلقة بحماية المعاملات الإلكترونية فبادرت العديد من الدول العربية إلى تبني تشريعات لمكافحة الجرائم المعلوماتية

ومن هذا المنطلق فقد تطرقنا إلى:

[1] فاروق خلف، مرجع سابق، ص 13، 14.

الفرع الأول: مكافحة الجريمة الإلكترونية على مستوى الدول العربية

ان أبرز ما يمكن قوله من الجهود العربية المبذولة للحماية من جرائم المعلوماتية وهو اعتماد قانون الجزائر العربي الموحد كقانون نموذجي بموجب القرار رقم 229 لسنة 1996، حيث صدر فيه النموذج العربي أو القانون الاسترشادي في موضوع مكافحة جرائم المعلومات نتيجة العمل المشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد أن اتضح أن كلاهما قدم مشروعا بهذا الشأن وبالفعل تم اجتماعهما المشترك في 2003/05/21 فتم النظر في المسودتين اللتين تم إعدادهما في إطار الغرفتين، وتم إعداد مشروع قانون مشترك ثم عرضه على المجلسين في الجلسة العادية لكل منهما حيث تمت الموافقة عليه، بعد الموافقة على هذا المشروع لا يوجد أي عذر لأي مشروع عربي للتقاعس عن الشروع في إصدار تشريعات وطنية تتضمن مواجهة الجرائم المعلوماتية التي تجد تطبيقها في جميع أنحاء العالم وفي أي دولة بغض النظر عن تصنيفها من حيث الاستخدام للحاسوب والأنترنت ومهما كانت. درجة تقييمها.[1]

وبالرجوع إلى المذكرة الإيضاحية لهذا القانون ومراجعة الفصل السابع الخاص بالجرائم ضد الأشخاص تجد أن هذا القانون قد تضمن فعلا الاعتداء على حقوق الأشخاص الناتجة عن معالجة المعلومات وذلك من المادة 461 وأشارت المواد من 461 إلى 463 على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات والاطلاع عليها ، أما المادة 464 نصت على عقاب كل من يقوم بفعل الدخول عن طريق الغش إلى أنظمة المعلوماتية وعرقلتها وتغيير المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية، وسرقة المعلومات.

وتحدث عن جرائم المعلومات بجميع أشكالها وتتراوح بين جرائم الاحتيال الحاسب الآلي من خلال اختراقها وسرقة المعلومات المخزنة عليها أو إتلافها، إلى الجرائم الأكثر خطورة مثل

[1] بن مكي نجاة، مرجع سابق، ص 130، 131.

التزوير المعلوماتي، سرقة الأموال عن طريق الوسائط الإلكترونية وكذلك الجرائم كالإتجار بالبشر وغيرها من أصناف الاجرام المستحدثة. "

الفرع الثاني: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

تعرف الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية بأنها اتفاقية إقليمية دولية مبرمة بين الدول العربية في نطاق جامعة الدول العربية بصورة خطية في أكثر من وثيقة وقد وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعها الذي عقد في مقر الأمانة العامة الجامعة الدول العربية بتاريخ 2010/01/21 القاهرة وتسمية الاتفاقية الإتفاقية العربية لمكافحة جرائم تقنية المعلومات وتتكون الاتفاقية من ديباجة وثلاثة وأربعين مادة موزعة على خمسة فصول.[1]

وتصدق الاتفاقية إلى تعزيز وتقوية التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات حفاظا على أمن ومصالح الدول العربية، وتعتبر هذه الاتفاقية مهمة من حيث وجودها، والأهم أن هذه الاتفاقية تنعقد لحماية أمن الدول العربية من الجرائم التقنية بسبب انتشار هذه الجرائم ووجود تعاون بين الدول العربية يساهم في الحد من انتشارها، ووجود نوع من هذه الاتفاقيات بين الدول لتسليم المجرمين أو عمل ما بين التشريعات الوطنية والاتفاقات العربية حتى لا يكون هناك تعارض في تطبيق العقوبة بين التشريع والاتفاقية.

وتجدر الإشارة أن الاتفاقية كان لها الأصل في وضع الجرائم في الفصل الثاني منه مثل في حالة الاعتداء على سلامة البيانات، وجريمة التزوير، جريمة الاحتيال، الشروع والاشتراك في ارتكاب الجرائم....

وأما على المستوى الإجرائي تضمنت الاتفاقية مجموعة من القواعد الإجرائية في بيئة الجرائم المعلوماتية، واعتبرت هذه الاتفاقية أن كل دولة تبنت في قوانينها الداخلية والإجراءات

[1] أحمد حيمين، صور جرائم تقنية المعلومات وفق للإتفاقية العربية، مجلة العلوم القانونية والسياسة، المركز الجامعي بتمنراست، المجلد 10، العدد 01، الجزائر، 2014، ص 778و 779.

الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث الذي يحتوي على أحكام إجرائية[1].

الفرع الثالث: نظام الملكية الفكرية العربية بوجه عام

اهتمت الدول العربية بقضايا الملكية الفكرية، حتى تجد أن بعضها ساهم في الجهد الدولي لحماية الملكية الفكرية منذ القرن التاسع عشر، كما هو الحال في الجمهورية التونسية على سبيل المثال، وأن عددا من الدول العربية من بين الدول الرئيسية في عضويتها في عدد من اتفاقيات الملكية الفكرية الدولية.

إن استجابة الدول العربية لحماية الملكية الفكرية عالية في ظل موجات التشريعات التي تظهر فيها في الخمسينات مشاهدات موجة واسعة من التشريعات في غالبية الدول العربية في مجال حماية براءات الاختراع والعلامات التجارية والرسوم والنماذج الصناعية فقد شهدت في الثمانينيات والتسعينيات موجه واسعة من الإجراءات التشريعية في مجال حماية حق المؤلف[2].

وشهدت أوائل التسعينات اعتماد عدة قوانين وتعديلات للقوانين القائمة فيما يتعلق بحماية برامج الكمبيوتر و قواعد البيانات ضمن قوانين حقوق النشر .

والجدير بالملاحظة فإن الاتفاقية تلزم الدول الأعضاء بإتباع سياسات عامة فيتعين اتفاق مع الاتجاه العام ولكن قد تختلف في تفاصيل مع دولة أخرى. وموقف الدول العربية من الاتفاقيات الدولية في حفل الملكية الفكرية فإن غالبية الدول العربية هي أعضاء في اتفاقيات منها اتفاقية انشاء المنظمة العالمية للملكية الفكرية، واتفاقية بيرن للملكية الأدبية واتفاقية باريس للملكية الصناعية وتتضمن قوانين حماية الملكية الفكرية العربية نصوصا تحمي برامج الحاسوب وقواعد البيانات وفقا لحق المؤلف بوجه عام طيلة حياة المؤلف ولمدة خمسين عاما بعد وفاته[3].

---

[1] أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص11و 12.

[2] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت، من الأولى، مركز الدراسات العربية، ط 1، مصر، 2016، ص 172.

[3] مروة زين العابدين صالح، المرجع نفسه، ص 173و 179.

المبحث الثاني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري

إن موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية أصبح هاجسا يؤرق رجال القانون بصفة خاصة لذلك بات من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في التقنيات الرقمية ورجال القانون والمؤسسات الرسمية في الدولة وعلى المستوى الدولي أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم كما تبرز أهمية هاته الدراسة من الناحية النظرية في معرفة مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية وردع مرتكبيها ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة، وسنتطرق إلى دارسة مكافحة الجريمة الإلكترونية بموجب القوانين العامة والخاصة.

المطلب الأول: آليات مكافحة الجرائم الإلكترونية بموجب القوانين العامة

في هذا المطلب سنتطرق إلى القوانين العامة التي تكافح الجرائم الإلكترونية والتصدي لها.

الفرع الأول: مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري والقانون المدني:

تم تقسيم هذا الفرع الى عنصرين :

أ. مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري: لقد كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية الحقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم إنتهاك حرمة الإنسان وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجزائية وقوانين خاصة أخرى [1] والتي تحظر كل مساس بهذه

[1] فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي 14 حول الجرائم الالكترونية ،طرابلس، 2017، ص 127 .

الحقوق، ومن أهم المبادئ الدستورية العامة:

المادة: 38 الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

المادة: 44 حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن وحقوق المؤلف يحميها القانون لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي،[1] الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون.

تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة، إذ لا يجوز إنتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، كما أن القانون يحمي سرية المراسلات و الإتصالات الخاصة بكل أشكالها و يضمنها.

ب . مكافحة الجريمة الإلكترونية بموجب القانون المدني الجزائري: ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه إعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وفق هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124 من التقنين المدني الجزائري "كل عمل أيا كان يرتكبه المرء يسبب ضرر للغير يلزم من كان سببا في حدوثه بالتعويض" وقد جاء هذا النص عاما وشاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة، وقد أورد هذا النص مبدأ مهم هو حق من وقع إعتداء على حياته الشخصية في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض "فالفعل الضار هو أساس المسؤولية"، وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الأنترنت، وهو عنصر متحول وصعب التحديد في الجرائم التي تمس

[1] المرجع نفسه، ص 128 .

الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات في تحديد هوية المعتدي، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الاثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ يشكل إعتداء قابل للإثبات وإن وقع على الشبكة.[1]

الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب قانون العقوبات الجزائري وقانون الإجراءات الجزائية الجزائري .

قسم هذا الفرع هو الآخر الى عنصرين و هما كالآتي :

أ . مكافحة الجريمة الإلكترونية بموجب قانون العقوبات الجزائري: لقد تطرق المشرع الجزائري إلى تجريم الافعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04 -15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 22-15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 7.[2]

قام المشرع الجزائري بموجب القانون رقم 04-15[3] بإستحداث جملة من النصوص التي تجرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات، وحدد كل فعل منها ما يقابله من الجزاء، إذ قام المشرع الجزائري بسن جملة من القواعد القانونية الموضعية والتي حدد

[1] حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الإعتداء على حق الحياة الخاصة، أعمال الملتقى الوطني، جامعة مولود معمري، تيزي وزو، الجزائر، 2017، ص 121و 122.

[2] فضيلة عاقلي، مرجع سابق، ص 127.

[3] قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156 يتضمن قانون العقوبات، جريدة الرسمية، عدد 71، الصادرة بتاريخ 10 نوفمبر 2004، معدل ومتمم.

من خلالها كل الأفعال الماسة بنظام المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة،[1] وإلى جانب ذلك قام المشرع بسن قواعد جزائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجرائم الالكترونية وذلك من خلال تعديل قانون الاجراءات الجزائية بموجب قانون رقم 06-22.[2]

إذ نصت المادة 394 مكرر: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك "، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة وإذا ترتب عن الافعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج"، وذلك مهما كانت قاعدة المعلوماتية أو طبيعتها لذلك يمكن أن تندرج ضمن هذه الاعتداءات تلك التي تمس ببعض صور الحياة الخاصة، ونصت المادة 394 مكرر2 على أنه: "يعاقب ...كل من يقوم عمدا وعن طريق الغش بما يأتي.

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

[1] قانون رقم 06-22 مؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66_155 يتضمن قانون الإجراءات الجزائية، جريدة رسمية، عدد 84، صادرة بتاريخ 24 ديسمبر2006.

2 براهيمي جمال، التحقيقي الجنائي في الجرائم الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، جامعة ميلود معمري، كلية الحقوق والعلوم السياسية، تيزي وزو، 2018، ص 124و 125.

ونصت المادة 394 مكرر6 أنه بالإضافة إلى العقوبات الأصلية أي الحبس والغرامة وبالاحتفاظ بحقوق غير الحسن النية يحكم بالعقوبات التكميلية التالية: "يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".[1]

ب – مكافحة الجريمة الإلكترونية بموجب قانون الإجراءات الجزائية الجزائرية:

بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والشهادة والخبرة.[2]

نجد أن المشرع نص على تمديد الإختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 قانون الإجراءات الجزائية، ونص على التنفيش في المادة 45 الفقرة 7،[3] من نفس القانون المعدل حيث إعتبر أن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية الموضوعية، فالتفتيش وإن كان إجراء من إجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على إعتراض المراسلات وتسجيل الاصوات والتقاط الصور من المادة 65 مكرر 5.[4]

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تفادي وقوع الجريمة الإلكترونية أو على الأقل

[1] حسين نوارة، مرجع سابق، ص 119و 118.

[2] فضيلة عاقلي، مرجع سابق، ص 130.

[3] مولود ديدان، قانون الإجراءات الجزائية، الأمر 11-02، دار بلقيس، الجزائر، ص 33.

[4] فضيلة عاقلي، المرجع نفسه، ص 130.

الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما إستدركه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية تسجيلها والتسرب. يقصد بإعتراض المراسلات إعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض، التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة و جمع الأدلة عنها [1].

ولقد أشار المشرع الجزائري إلى الظروف وكيفية اللجوء لهذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية على النحو: "إذا إقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في ... الجرائم الماسة بأنظمة المعالجة الالية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن:

-بإعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

- وضع الترتيبات التقنية، دون موافقة المعنيين من أجل إلتقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة اشخاص في أماكن خاصة أو عمومية أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص "بموجب هذه المادة فإن المشرع الجزائري يسمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الإلكترونية، اللجوء إلى إجراء اعتراض المراسلات السلكية وتسجيل المحادثات والأصوات و إلتقاط الصور، والاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة، ومع هذا فإن المشرع الجزائري لم يطلق حق اللجوء

[1] براهيمي جمال، مرجع سابق، ص 437و 139و 140 .

إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد.[1]

المطلب الثاني: آليات مكافحة الجرائم الإلكترونية بموجب القوانين الخاصة

في هذا المطلب سنحاول دراسة القوانين والهياكل الخاصة لمكافحة الجريمة الإلكترونية بفرعين الأول بموجب القوانين الخاصة والثاني بموجب الهياكل الخاصة.

الفرع الأول: مكافحة الجريمة الإلكترونية بموجب القوانين الخاصة:

تم تقسيمه الى أربعة عناصر و هي :

أ-القانون الخاص بحماية حقوق المؤلف والحقوق المجاورة: يرى معظم الفقهاء أن "الموقع الالكتروني مصنف متعدد الأغراض" يتم إستخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسوق أو الدعاية عن غيرها على شبكة الانترنت، أو كإسم تجاري أو شعار لجذب الجمهور، كما يمكن أن يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو لوحاتهم الزيتية أو ألعاب الفيديو... وغيره، وفي كل الحالات يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو إسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة عن إبرام العقد مع إحدى الشركات التي تقدم الخدمات على الشبكة وبمجرد تسجيل إسم الموقع يحظى بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه أي يتحدد القانون الواجب التطبيق حسب الطبيعة

[1] المرجع نفسه .

القانونية للمواقع تعقد تسجيل كمصنف أدبي أو فني "لا يجوز أن يعتدي على أي جانب من جوانب الحياة الخاصة للأفراد"[1]

ب- قانون البريد والاتصالات اللاسلكية: بإستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات، لاحظنا أن هناك تسارع في مواكبة التطور الذي شهدته التشريعات العالمية مسايرة للتطور التكنولوجي، لذلك بات من السهولة بإمكان إجراء التحويلات المالية عن الطريق الإلكتروني، ذلك ما نصت عليه المادة 87 منه، كما نصت المادة 02/84 منه على إستعمال حوالات دفع عادية أو الكترونية أو برقية، كما نص في المادة 105 منه على إحترام المراسلات، بينما أتت المادة 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحاول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر.[2]

ج- القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته: لقد جاء في القانون 09-04 مجموعة من التدابير الوقائية التي يتم إتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر، وهي كالتالي:

مراقبة الاتصالات الإلكترونية: لقد نصت المادة 4 من القانون 09-04 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي:

*الوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد أمن الدولة.

[1] حسين نوارة، مرجع سابق، ص 121و 122.

[2] فضيلة عاقلي، مرجع سابق، ص 118.

*عندما تتوفر معلومات عن إحتمال وقوع إعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.

*لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

*في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

2-إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية:

وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد، 10، 11، 12 بالشكل التالي:

*الالتزام بالتعاون مع مصالح الأمن المكلفة بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات والتحقيق.

*الالتزام بحفظ المعطيات المتعلقة بحركة السير وكل المعلومات التي من شأنها أن تساهم في الكشف عن الجرائم ومرتكبيها، وهذين الالتزامين موجهين لكل مقدمي خدمات الاتصالات الالكترونية (services de fournisseurs) دون إستثناء.

*الالتزام بالتدخل الفوري لسحب المحتويات التي تسمح لهم للاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الوصول إليها غير ممكن.

*الالتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم بوجودها [1].

[1] براهيمي جمال، مرجع سابق، ص 151و 154 .

-إضافة إلى التدابير الوقائية السالفة الذكر تبنى المشرع القانون رقم 09-04 إجراءات جديدة يدعم بها تلك المنصوص عليها في قانون الاجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجية الإعلام الآلي والاتصال تتلخص فيما يلي:

* السماح للسلطات الجزائرية المختصة اللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام والاتصال غير الوطنية ومرتكبيها، وذلك عن طريق تبادل المعلومات أو إتخاذ تدابير إحترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة[1]

*السماح للجهات القضائية المختصة وضباط الشرطة بالدخول لغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها واستنساخها، مع إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى التي يمكن الدخول إليها بواسطة المنظومة الأصلية، بشرط إخطار السلطات المختصة مسبقا.

*إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل.

*توسيع دائرة إختصاص الهيئات القضائية الجزائية لتشمل النظر في الجرائم المتصلة بتكنولوجية الإعلام والاتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية والدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة.

د- قانون التأمينات: لقد تطرق هذا القانون إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة

[1] المرجع نفسه .

في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له إجتماعيا أو في المفتاح الإلكتروني لهيكل العالج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية حسب المادة 93 مكرر2.[1]

الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب الهياكل الخاصة:

تم تقسيمه الى ثلاث عناصر هي :

أ-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال: نصت على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها "تنشا هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم "أما مهامها فقد أوردتها المادة 14 من نفس القانون [2] .

•مهام الهيئة:

للهيئة دوران أساسيان هما:

1-الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على

[1] فضيلة عاقلي، مرجع سابق، ص 132.

[2] براهيمي جمال، مرجع سابق، ص 155 .

الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء أو ببطاقات إئتمانهم، إختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية... إلخ

2-مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بحسب نص المادة 14 من القانون 04/09 فهناك نوعان من المكافحة تقوم بهما هذه الهيئة:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 13 و14 من القانون 04/09 تتعلق بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هذه الهيئة تتمثل [1] في:

-تنشيط وتنسيق عمليات الوقاية من الجرائم المعلوماتية ومكافحتها أي تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشتركين في إرتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات بما في ذلك جمع المعلومات وإنجاز الخبرات القضائية.

-تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجده.

- التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة (المادة 4 فقرة 2 من القانون 04/09 في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به).

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 232و 233 .

–من أجل القيام بمهامها فلها تركيز تحليل، إستقراء كل المعلومات المتعلقة بأفعال أو جرائم متصلة بتكنولوجيات الإعلام والاتصال، والاتصال بكل من مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة)، وكذلك كل الادارات والمصالح العامة للدولة المعنية للقيام بمهامها.

– تقديم المساعدة لمصالح الأمن والدرك الوطنين، ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة) فيما يخص الجرائم التي تدخل في إختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح.

3– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل العمليات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم: في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات (الهيئات) المماثلة لها على مستوى الدول، بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم.[1]

ب– المعهد الوطني للأدلة الجنائية على الاجرام: يتكون من إحدى عشرة دائرة مختصة في مجالات مختلفة جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية ودائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات.[2]

ج– الهيئات القضائية الجزائية المتخصصة: إن السلطة القضائية ستتعامل تأكيدا في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ولاسيما بعد اللجوء الواسع والمتزايد

[1] المرجع نفسه .

[2] فضيلة عاقلي، مرجع سابق، ص 133.

إلى الشبكات الرقمية في حياة المواطنين، بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي.

خلاصة الفصل الثاني:

في الفصل الثاني حاولنا دراسة الآليات القانونية لمكافحة الجريمة الإلكترونية والتي تعد من الجرائم الحديثة والخطيرة في نفس الوقت والتي أصبحت تسجل لها أرقام كبيرة في مختلف دول العالم ومن بينها الجزائر، فتطرقنا الى الآليات الدولية لمكافحة الجريمة الإلكترونية المتمثلة في الجهود الغربية والجهود العربية لمكافحة الجريمة الإلكترونية وهذا ما جعل أهل الإختصاص في إيجاد حلول عصرية لمكافحتها والحد من إنتشارها من خلال التعاون الدولي لكل من المنظمات الدولية والجمعية العربية، وكان للجزائر دور فعال من خلال وضع قوانين ردعية عامة وخاصة للحد ومواجهة الإجرام الإلكتروني.

خاتمة

خاتمة:

من خلال دراستنا لموضوع الآليات القانونية لمكافحة الجرائم الإلكترونية تبين أن هذه الجرائم أخطر من الجرائم التقليدية لخصائصها الحساسة، فالمشرع الجزائري ذكرها تحت مصطلح جرائم متصلة بتقنيات الإعلام والاتصال في إشارة الى توسيع نطاق تجريم كل فعل يمس بأنظمة المعالجة الآلية للمعطيات أو أي جريمة يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية، بينما لم يتم الاتفاق على تعريف موحد لهذه الجرائم، فتعتبر هذه الجرائم مستحدثة عالميا وأنها عابرة للحدود وأهم ما يميزها أنها صعبة الكشف والإثبات ولهذه الجرائم عدة أنواع أهمها تلك الواقعة على الافراد كالتهديد وانتحال الشخصية أو تلك الواقعة على الأموال كسرقة أرصدة البنوك وغسيل الاموال، أو الاجرام الماس بأمن الدول كالتجسس والإرهاب الإلكتروني، وهناك جرائم واقعة على برامج النظام المعلوماتي أو على المكونات المادية لهذه البرامج والكثير من الأفعال التي جرمها المشرع وأغلب الدول في العالم.

ولمحاربة هذه الجرائم عرف العالم تحركا متسارعا بعقد عدة مؤتمرات ولقاءات والدفع بإبرام إتفاقيات تعاون أمني وقضائي من شأنها محاربتها بما يخدم مصالح الدول، ومنها إتفاقية بودبست وبرني وأهمها هيئة الشرطة الدولية.

أما المشرع الجزائري فقد إعتمد على آلية الوقاية والعقوبة لردع هذه الجرائم من خلال القوانين والتعديلات الأخيرة التي أكدت على حفظ الحقوق والحريات وهو ما أكده الدستور الجزائري ونصت عليه مجموعة القوانين العامة كالقانون المدني وقانون الاجراءات الجزائية الذي جرم هذه الافعال وأكده قانون العقوبات من خلال العقوبات المسلطة على الجناة، فقد إعتمد على إجراءات وقائية كإعتراض المراسلات، في الوقت الذي تم إنشاء هيئات خاصة ومخابر خاصة، منها الهيئة الوطنية لمكافحة جرائم الإعلام والاتصال وإصدار قانون الوقاية من الجرائم

المتصلة بتكنولوجيا والاتصال وقانون الاتصال، فالمشرع الجزائري إعتمد على آليات المكافحة والعقاب من خلال حزمة القوانين والنصوص الصادرة من خلال القوانين العامة والخاصة، كما كان للتعاون الدولي والانخراط في الاتفاقيات الدولية والمجالس المختصة بالتنسيق دوليا لمكافحة هذه الجرائم.

وإزاء التطور العلمي الهائل فإن المزايا التي جلبتها المعلوماتية قد جلبت إلى جانبها أيضا مخاطر عدة ناجمة عن إساءة إستخدام شبكة الأنترنت وتطويعها لصالح المجرم المعلوماتي لممارسة نشاطاته الإجرامية، حيث سهلت ظهور طائفة جديدة من الجرائم المستحدثة، بالإضافة إلى إمكانية إرتكاب الجرائم التقليدية، والتي تعجز النصوص العقابية في مواجهة أغلب صورها المستحدثة، فالقوانين الجنائية التقليدية والموضوعية والإجرائية باتت قاصرة عن مواجهة الجرائم المرتكبة عبر الأنترنت، فلابد أن تكملها إستراتيجيات مختلفة على المستوى الفني والتقني والقضائي، وذلك بمراقبة الأمن في مجال تقنية المعلومات أو في مجال التدريب، أو حتى في مجال التعاون والتنسيق الدولي لمواجهة هذا النوع المعقد من الاجرام.

إن الجرائم الإلكترونية أصبحت تشكل نمطا خطيرا من الإجرام تتطلب مواجهته مهارات فنية فائقة بالإضافة الى إطار قانوني من حيث التجريم والعقاب والردع، بالإضافة إلى الجانب التوعوي الذي يمكن أن تساهم الجهات الأمنية المختصة والجامعات والمساجد والأسر لتوضيح الصورة عن مدى خطورة هذه الجريمة لدى مختلف الفئات، خاصة المتمدرسة منها لأننا في بلدنا على مشارف مرحلة ستلعب فيها الوسائل الإلكترونية الأداة الرئيسية في المنهج التعليمي والتكويني في مختلف المؤسسات على المستوى الوطني، هاته الوسائل التي ستكون المحرك الرئيسي في الإدارات الجزائرية التي تسعى لأن تكون في مصف الإدارات الإلكترونية المتطورة.

لقد خلصت هذه الدراسة إلى جملة من النتائج والمقترحات المتمثلة في:

النتائج:

1- عدم وجود تعريف جامع مانع للجريمة الإلكترونية.

2-من خلال دراسة خصائص الجريمة الإلكترونية تبين أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية.

3- لم يضع المشرع الجزائري نصا قانونيا خاصا بالجرائم الإلكترونية رغم ما تسببه هذه الجرائم من أضرار على المجتمع والدولة معا، خاصة وأن الجزائر تتجه نحو رقمنة الإدارة الجزائرية بما يتماشى مع العصرنة الحاصلة في العالم.

4-آليات المكافحة الحالية غير كافية لمجابهة الجريمة الإلكترونية، فلا يمكن لأي دولة مهما بلغ تطورها الإلكتروني أن تتصدى لهذه الجريمة العالمية بمفردها، فالمجرم الإلكتروني قد يكون في دولة ما وينفذ جريمته الإلكترونية في دولة ثانية، وبالإمكان أن تتحقق نتيجتها في دولة ثالثة، أو حتى في عدة دول، مما يصعب عملية متابعته، خاصة في حالة عدم وجود إتفاقية بين الدولة التي يتواجد على أرضها كل هذا راجع الى ضعف التعاون الدولي.

5- نقص التنسيق بين الجهات المعنية وغياب التنسيق الدولي للتعامل مع جرائم المساس بأنظمة المعالجة الآلية للمعطيات إذا كان مصدرها دولة أجنبية .

6-الإدمان على الأنترنت والمخدرات الرقمية هما حقيقة موجودة رغم إنكارها من قبل الكثيرين، فإنشغال الشباب بالألعاب الإلكترونية بالساعات، وسقوط بعضهم في مصيدة مصممي الألعاب الإلكترونية الخطيرة خير دليل على ذلك.

7-تعد مراكز معالجة الإدمان على الأنترنت آلية إستباقية مهمة للحد من الاستعمال المفرط للإنترنت والذي قد يوقع صاحبه في مخاطر الجرائم الإلكترونية سواء كضحية أو كمرتكب للجريمة الإلكترونية.

8-تأخر التشريعات الوطنية .

الحلول والمقترحات:

1-ضرورة إعطاء تعريف موحد للجريمة الإلكترونية يشمل كل السلوكيات المجرمة.

2- ضرورة توحيد القواعد المتعلقة بالإجراءات المتبعة في مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات في مدونة واحدة تبعا لخصوصيات هذه الجرائم وخصوصية مرتكبيها، أو إدماجها في قانون الإجراءات الجزائية، وبالتالي وجوب تعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلاءم مع أنواع الجرائم الإلكترونية وإصدار قانون خاص بالجرائم الإلكترونية وطرق مكافحتها.

3- إنشاء وحدات متخصصة أو محاكم متخصصة بالجرائم الإلكترونية في كل المجالس القضائية لمجابهة هذه الظاهرة.

4- ضرورة تخصيص شرطة جنائية خاصة بجرائم الأنترنيت في كل ولاية ويستحسن إنشاء شرطة مختصة بهذه الجرائم، تكون مهمتها الوحيدة متابعة هذا النوع من الجرائم مع تكوين لجان خبراء لهذا الشأن.

5- تعزيز التعاون والمساعدة الوطنية والدولية في مجال مكافحة جرائم الأنترنت.

6- تكوين هيئة وطنية لمراقبة ومتابعة جرائم الأنترنيت و تطوير برامج توعوية و تدريبية في مجال مكافحة الجرائم الإلكترونية.

7-يتعين على الدولة حجب المواقع المخالفة للقوانين والأخلاق.

8-تشجيع البحث العلمي في المجال الجنائي، وبالأخص ما يتعلق بالجريمة الإلكترونية والعمل بنتائجه في السياسة الجنائية.

9-وجوب تعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلاءم مع أنواع الجرائم الإلكترونية أو إصدار قانون خاص بالجرائم الإلكترونية وطرق مكافحتها و تحديث التشريعات بشكل دوري .

10-لابد من تفعيل آليات التعاون الدولي التي تتسم بسرعة التنفيذ حتى لا يترك للمجرم الإلكتروني ملاذا آمن يلتجئ إليه، وتوسيع الاتفاقيات الدولية الثنائية والجماعية لمكافحة الجرائم الإلكترونية.

قائمة المصادر

والمراجع

قائمة المراجع

النصوص القانونية:

-المادة 01/40 من دستور 1996، ج ر رقم 76 المؤرخة في 8 ديسمبر 1996، المعدل والمتمم بالقانون رقم 16-01 المؤرخ في 6 مارس 2016، ج ر رقم 14 المؤرخة في 07 مارس 2016.

-المادة 394 مكرر من الأمر 155/66 من قانون العقوبات المؤرخ في جوان 1966، المعدل والمتهم بالقانون 15/04 المؤرخ في 10 نوفمبر 2004، ج ر71 بتاريخ 10 نوفمبر 2004.

-القانون 04-14 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، جريدة رسمية عدد 71.

-القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156 يتضمن قانون العقوبات، جريدة الرسمية، عدد 71، الصادرة بتاريخ 10 نوفمبر 2004، معدل ومتمم.

-القانون رقم 06-22 مؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66_155 يتضمن قانون الإجراءات الجزائية، جريدة رسمية، عدد 84، صادرة بتاريخ 24 ديسمبر 2006.

-القانون رقم 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر، عدد، 47 مؤرخة في 16 أوت 2009.

-الأمر 03-05 المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف أو الحقوق المجاورة، وكذلك الأمر 03-07 المؤرخ في 19 جويلية 2003، المتعلق ببراءات الاختراع، ج ر رقم 44 المؤرخة في 23 جويلية 2003.

-الأمر رقم 21-11 المؤرخ في: 16 محرم عام 1443 الموافق لـ 25 أوت سنة 2021 يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، جريدة رسمية رقم: 65.

الكتب:

-أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، ط 2، 2006.

-أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، الجامعة الجديدة، الإسكندرية، 2015.

-بن مكي نجاة، السياسة الجنائية لمكافحة الجرائم المعلوماتية، دار الخلدونية، الجزائر، 2017.

-جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، ط 1، دار البداية ناشرون الموزعون، عمان، 2010.

خالد داودي، الجريمة المعلوماتية، دار الاعصار العلمي للنشر والتوزيع، الجزائر، ط1، 2008.

-خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2019 .

-فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، كلية الحقوق، جامعة جمة الخضر، الوادي، العدد 2، 2015.

-طارق عفيفي صادق أحمد، الجرائم الالكترونية جرائم الهاتف المحمول، د ذ د ن، مصر، ط 1، 2015.

-عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية – شبكة الانترنت وشبكة الهواتف التقليدية والآليات والمطبوعات- دار الثقافة للنشر والتوزيع، 2019.

-عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007.

-عبد الله عبد الكريم عبد الله، الجرائم المعلوماتية والأنترنت، ط1، منشورات الحلبي الحقوقية، لبنان، 2007.

-غنية باطلي، الجريمة الإلكترونية -دراسة مقارنة- الدار الجزائرية للنشر والتوزيع، الجزائر، سنة 2015.

-محمد عبد الله بن علي المنشاوي، جرائم الإنترنيت في المجتمع السعودي، ماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2003 .

-محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط 2، دار النهضة العربية، القاهرة، 1994.

-مناصرة يوسف، جرائم المساس بأنظمة المعالجة الألية للمعطيات، د ذ ط، دار الخلدونية، الجزائر، 2018.

-مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت، مركز الدراسات العربية، ط 1، مصر، 2016.

-مولود ديدان، قانون الإجراءات الجزائية، الأمر 11-02، دار بلقيس، الجزائر.

-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات دار الفكر الجامعي الإسكندرية، د ذ ط، 2006.

-يوسف عبد النبي شكري، المعلوماتية وأزمة الشرعية، د ذ د ن، الكوفة، د ذ ط، 2008.

البحوث الجامعية:

رسائل الدكتوراه:

-براهيمي جمال، التحقيقي الجنائي في الجرائم الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، جامعة ميلود معمري، كلية الحقوق والعلوم السياسية، تيزي وزو، 2018/06/27.

-رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعموم السياسية، جامعة ابوبكر بلقايد، تلمسان، 2018.

-فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق ،فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2010.

رسائل ماجستير:

-أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018.

المقالات:

- أحمد حيمين، صور جرائم تقنية المعلومات وفق للإتفاقية العربية، مجلة العلوم القانونية والسياسة، المركز الجامعي بتمنراست، المجلد 10، العدد 01، الجزائر، 2014.

-بن علية بن جدو، تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، جامعة بومرداس، المجلد07، العدد02، تاريخ 2022/03/01.

- دمان ذبيح عماد- بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر، مجلة الحقوق والعلوم السياسية، العدد 13، جانفي 2020.

– ذياب سليمة بوترعة بلال، الجريمة الالكترونية الأسس والمفاهيم، مجلة تطوير العلوم، جامعة زيان عاشور الجلفة، المجلد 13، العدد 01، الجزائر،2020.

– سامية عزيز، مازيا عيساوي، الجريمة من منظور سيكولوجي الأسباب والأثار، مجلة دراسات في سيكولوجية الانحراف، المجلد 6، العدد 1، السنة 2021.

– صالحة العمري، جريمة غسيل الأموال وطرق مكافحتها، مجلة الاجتهاد القضائي، العدد الخامس، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة د.ذ.س.ن.

– عبد الصديق الشيخ، الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ملجة معالم للدراسات القانونية والسياسية، المجلد 4، العدد1، 2020.

– مراد مشوس، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، جامعة غرداية، العدد 02، 2019/12/20.

ملتقيات ومداخلات:

– بوزيدي مختارية، ماهية الجريمة الإلكترونية، ورقة بحثية مقدمة ضمن ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع، الجزائر، يوم 29مارس2017.

–بن عمير أمينة، بوحلايس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ورقة بحثية مقدمة ضمن فعاليات الملتقى الدولي القانون الجنائي للأعمال نمو توجو جديد للتجريم، المنعقد يوم 21 أكتوبر 2021، عبر التحاضر المرئي عن بعد zoom، المجمد 7 العدد1 لسنة 2022.

– زكي زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجامعة المصرية للقانون الجنائي، القاهرة أيام 25 و28 أكتوبر.

-عباس أبو شامة، التعريف بالظواهر الإجرامية المستحدثة حجمها، أبعادها، ونشاطها في الدول العربية، الندوة العلمية للظواهر الإجرامية المستحدثة وسبل مواجهتها، السعودية، أيام 29-30 جوان 1999.

-فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي 14 حول الجرائم الالكترونية، طرابلس، 2017.

حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الإعتداء على حق الحياة الخاصة، أعمال الملتقى الوطني، جامعة مولود معمري، تيزي وزو، الجزائر، 2017.

فهرس المحتويات

شكر و تقدير	
الإهداء	
قائمة المختصرات	
مقدمة	أ
الفصل الأول : أحكام الجرائم الالكترونية	
المبحث الأول : مفهوم الجرائم الالكترونية	7
المطلب الاول : تعريف الجرائم الالكترونية	8
الفرع الأول : التعريف اللغوي و الفقهي للجريمة الإلكترونية	8
الفرع الثاني : تعريف الجريمة الإلكترونية في التشريع الجزائري	13
المطلب الثاني : خصائص الجرائم الالكترونية	15
الفرع الأول : خصائص متعلقة بالجريمة	15
الفرع الثاني: خصائص متعمقة بالجاني	21
المبحث الثاني : أركان الجريمة الالكترونية وأنواعها	24
المطلب الأول : أركان الجريمة الالكترونية	24
الفرع الأول: الركن الشرعي	24
الفرع الثاني: الركن المادي	24
الفرع الثالث: الركن المعنوي	25
المطلب الثاني :أنواع الجريمة الإلكترونية	27
الفرع الأول: الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي	27
الفرع الثاني: الجرائم المعلوماتية الواقعة على النظام المعلوماتي	31
خلاصة الفصل الأول :	34
الفصل الثاني :الآليات القانونية لمكافحة الجرائم الإلكترونية	
المبحث الأول: الآليات الدولية لمكافحة الجريمة الإلكترونية	36
المطلب الأول: الجهود الغربية لمكافحة الجريمة الإلكترونية	36

الفرع الأول: التعاون الدولي	36
الفرع الثاني : الإختصاص القضائي الدولي	39
الفرع الثالث: جهود الأمم المتحدة والأوربية لمكافحة الجريمة الإلكترونية	42
الفرع الرابع: أهم الإتفاقيات والمنظمات المواجهة للجرائم المعلوماتية	46
المطلب الثاني : الجهود العربية المبذولة لمواجهة الجريمة الإلكترونية	49
الفرع الأول: مكافحة الجريمة الإلكترونية على مستوى الدول العربية	49
الفرع الثاني: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.	50
الفرع الثالث : نظام الملكية الفكرية العربية بوجه عام	51
المبحث الثاني : آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري	52
المطلب الأول: آليات مكافحة الجرائم الإلكترونية بموجب القوانين العامة	53
الفرع الأول : مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري والقانون المدني	53
الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب قانون العقوبات الجزائري وقانون الإجراءات الجزائية الجزائري .	55
المطلب الثاني : آليات مكافحة الجرائم الإلكترونية بموجب القوانين الخاصة	59
الفرع الأول: مكافحة الجريمة الإلكترونية بموجب القوانين الخاصة	59
الفرع الثاني: مكافحة الجريمة الالكترونية بموجب الهياكل الخاصة	63
ملخص الفصل الثاني	66
خاتمة	67
قائمة المراجع	73

ملخص

الملخص:

عرفت البشرية مرحلة من التطور التكنولوجي خاصة المعلوماتي، والذي كثر معه استعمال الوسائل الإلكترونية، التي تعتبر أشد خطورة لأنها تشكل تهديدا كبيرا على أمن الدولة والمجتمعات والأفراد معا، الأمر الذي جعلها من مواضيع البحث العلمي القانوني، تثير عدة إشكاليات تستوجب الوقوف عندها، وما دراستنا هذه إلا نموذج عن الدراسات السابقة، حيث تضمنت هذه المذكرة مفهوما للجريمة الإلكترونية، وخصائصها وأنواعها، وتضمنت أيضا مجموعة من الآليات القانونية التي لها دور كبير في مكافحة هذه الجرائم الإلكترونية، من بينها آليات قانونية وإجرائية وآليات قانونية مؤسساتية لمكافحة الجريمة الإلكترونية، بالإضافة إلى آليات مساعدة على مكافحة الجريمة الإلكترونية، كالجمعيات ومراكز معالجة الإدمان على الإنترنت.

كلمات مفتاحية: جريمة إلكترونية، أدلة إلكترونية، آليات مكافحة.

Abstract :

Humanity has witnessed a period of technological development, particularly in the information technology sector, which has led to the widespread use of electronic media. These media are considered more dangerous because they pose a significant threat to the security of the state, societies, and individuals alike. This has made them a subject of legal scientific research, raising several issues that require further consideration, This study is merely a model of previous studies, as it includes a concept of cybercrime, its characteristics, and types. It also includes a set of legal mechanisms that play a significant role in combating these cybercrimes. These include legal, procedural, and institutional mechanisms for combating cybercrime, in addition to mechanisms that assist in combating cybercrime, such as associations and internet addiction treatment centers.

Keywords: cybercrime, electronic evidence, combat mechanisms.