جامعة الجزائر 1

بن يوسف بن خدة

كلية الحقوق

آليات مكافحة الجريمة الإلكترونية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر

فرع القانون العام

تخصص القانون الجنائي

لجنة المناقشة

د. جمال الدين دوادي..... رئيسا

د. كريمة عنان..... مشرفا ومقررا

د. فوزي لواتي..... مناقشا

من إعداد الطالبة:

ليدية سايح

تحت إشراف الأستاذة:

د. كريمة عنان

السنة الجامعية:2024/2023

الشكر

الحمدلله الذي أنار لي درب العلم والمعرفة وأعانني على أداء هذا الواجب ووفقني في إنجاز هذا العمل المتواضع، فاللهم لك الحمد على توفيقك وجميل إحسانك.

أتوجه بالشكر الجزيل إلى الأستاذة المشرفة كريمة عنان على تقديم العون العلمي لي ورحابة صدرها وطول صبرها علي، حيث أفادتني كثيرا بنصائحها فوجهتني حين الخطأ وشجعتني حين الصواب، وأشكرها على إسهاماتها المفيدة وبصمتها الواضحة في هذا العمل، وإنها كانت نعم المشرفة والموجهة علما وأدبا وخلقا، وأدعو لها بالتوفيق والسداد.

وكل الشكر والتقدير إلى السادة الأفاضل أعضاء لجنة المناقشة على كرمهم وجود همتهم في مناقشة هذه الرسالة، فشكر الله سعيهم وجزاهم كل خير. وإلى كل الأساتذة الكرام ومن تعاقبوا على تعليمي.

وإلى من ساعدني من قريب أو من بعيد في هذا المشوار وكان سببا في بعث العزيمة في نفسي للاجتهاد أكثر وتقديم الأفضل.

الإهداء

بكل حب أهدي هذا الجهد الذي هو ثمرة مشوار دراسي طويل إلى:

إلى روح أخي وحبيبي بهاء الذي كان تاجا أضعه على رأسي أغلى الناس وأقربهم إلى قلبي، الذي لم يتوانى لحظة عن إسعادي، مهما غبت عني إلا أن حنانك وابتسامتك لم تفارقني، أخي الغالي أسأل الله أن يرحمك ويسكنك الفردوس الأعلى.

فاللهم اغفر لأخي بهاء

اللهم اغفر له وارحمه وعافه واعف عنه، وأكرم نزله، ووسع مدخله، واغسله بالماء والثلج والبرد، ونقه من الخطايا كما ينقى الثوب الأبيض من الدنس، وأبدله دارا خيرا من داره، وأهلا خيرا من أهله، وزوجا خيرا من زوجه، وأدخله الجنة، وأعذه من عذاب القبر، ومن عذاب النار

اللهم اغفر له وارحمه، اللهم اجعل قبره مد بصره واجعله روضة من رياض الجنة ونعيمها

اللهم اغفر له وارحمه وتقبله برحمتك الواسعة وأسكنه فسيح جناتك واجعل مثواه الفردوس الأعلى يارب

اللهم اغفر له وارحمه وتجاوز عن سيئاته واسكنه الفردوس الأعلى من الجنة مع النبيين والصديقين والشهداء والصالحين وحسن أولئك رفيقا

اللهم اغفر له وارحمه برحمتك التي وسعت كل شيء ونقه من الذنوب والخطايا وأبدل سيئاته حسنات يارب العالمين

مقدمة

مقدمة

تعد الجريمة من إفرازات الحياة الاجتماعية، ومظهرا من مظاهرها ونتيجة من نتائج السلوك الإنساني في علاقاته المستمرة والمتطورة عبر التاريخ، فتطور الجريمة انعكاس لتطور الحياة الإنسانية وهذا ما يجعلها تحظى بالدراسة والبحث والاهتمام لكونها من جهة ظاهرة اجتماعية يعد ارتكابها مخلا بالنظام الاجتماعي، وهذا يقتضي بتحليلها ومعرفة أبعادها المختلفة، وصولا إلى مواجهتها بكل الوسائل التي تؤدي إلى الحد من ارتكابها.

ومن جهة أخرى ظاهرة قانونية تعتمد على سياسة التجريم والعقاب، لكونها تمس بالمصالح المحمية والأفعال التي يمكن أن تهددها، فيتم تجريمها وتحديد العقوبة المناسبة لها، ويتم التعامل مع الجريمة بعد وقوعها وفقا لهذه السياسة مع توضيح أركان الجريمة بصورة تساعد على إثباتها ومن ثمة معاقبة مرتكبها.

ونتيجة للتطور العلمي الذي شهده العصر الحديث تطورت الجريمة وانتقلت من صفتها التقليدية وأبعادها المحدودة إلى آفاق جديدة تعتمد على التقنية والتكنولوجيا الحديثة تعتمد في تنفيذ الجرم على أساليب مبتكرة وطرائق لم تكن معروفة في السابق حيث ظهر نمط جديد من الإجرام أطلق عليه بالجريمة الإلكترونية.

ومما يزيد انتشار الجرائم الإلكترونية تطور الوسائل التكنولوجية الحديثة التي انتشرت بشكل واسع جدا، وقد لفت هذا أنظار الدول والهيئات العالمية إلى إدراك خطورة تلك الجرائم نظرا لسهولة ارتكابها وتأثيرها المباشر في جميع المجالات ومساسها المباشر بحماية وحرية الأفراد، فضلا عن تهديدها بكافة مستويات الأمن، الأمر الذي جعل مسألة مكافحتها من أولويات المجتمع الدولي والحكومات.

والجزائر على غرار دول العالم استشعرت مدى خطورة الجرائم الإلكترونية، وعقدت العزم على التصدي لها ومعاقبة المتسببين في حدوثها، وذلك من خلال وضع قوانين صارمة للحد منها وملاحقة مرتكبيها وردعهم.

عملية اختياري لهذا الموضوع دون غيره من المواضيع تولدت نتيجة جملة من الدوافع **والأسباب الذاتية والموضوعية**، يمكن حصرها فيما يلي:

السبب الرئيسي في اختيار الموضوع هو وقوع حادثة واقعية عبر مواقع التواصل الاجتماعي كانت ضحيتها فتاة قاصر لم تبلغ من العمر 16 سنة كاملة، تعرضت للابتزاز من طرف شاب قام بالتشهير بها ونشر صورها عبر صفحات مواقع التواصل الاجتماعي، ما دفعها على الإقدام بمحاولة انتحار.

الأمر الذي عزز رغبتي في دراسة موضوع الجريمة الإلكترونية من خلال التعريف بمفهومها، حيث يمكن لأي فرد من أفراد المجتمع التعرض لهذا النمط المستحدث من الجرائم، خصوصا في ظل الاستخدام الواسع لمواقع التواصل الاجتماعي، وانتشار الثقافة الرقمية لدى جميع شرائح المجتمع وخصوصا فئة الشباب، وبالتالي فأي استغلال سيئ لهذه التكنولوجيا يمكن تصنيفه ضمن نطاق الجريمة الإلكترونية وتعريض المتسبب للعقاب والمحاكمة.

أما **الأسباب الموضوعية** فتجلت في التعرف على النصوص والآليات العقابية على المستويين الوطني والدولي باعتبارها العامل الأهم للتصدي للجريمة الإلكترونية والحد من انتشارها.

كانت جملة **الأهداف** التي دعت إلى إجراء هذه الدراسة ما يلي:

التعرف على الجريمة الإلكترونية من المنظورين الوطني والدولي من خلال مختلف القوانين الرادعة التي سنها المشرع الجزائري والآليات التي تبنتها الدولة

الجزائرية للتصدي لهذا البعد الجديد من الإجرام، والسبيل الذي يؤدي إلى الوقاية منه من الجانب التشريعي والمؤسساتي، وكذا الاتفاقيات والمعاهدات الدولية التي وضعت لمكافحة الجريمة الإلكترونية على الصعيد العالمي.

تتجلى **أهمية** هذه الدراسة في كون ظاهرة الجريمة الإلكترونية تعد من أبرز الجرائم المستحدثة، وهي في كثير من الأحيان تعتبر المحرك الأساسي الذي يتم من خلاله ارتكاب معظم الجرائم التقليدية، ولموضوع البحث أهمية من الناحية النظرية والعلمية باعتباره يمس كافة مصالح المجتمع، وأيضا المساس بالحياة الخاصة للأفراد، لذا توجبت دراسة هذا الموضوع من أجل التمعن الدقيق في هذا المفهوم الجديد المتمثل في الجريمة الإلكترونية وإبراز آليات وإستراتيجيات المكافحة التي وضعت لحماية وأمن الأفراد، وأيضا لردع المجرمين وتعقبهم جنائيا.

البحوث السابقة تعتبر مصدر إلهام لا غنى عنها بالنسبة للباحث، لأن كل بحث ما هو إلا امتداد للبحوث التي سبقته.

ومن خلال اطلاعي ومراجعتي فقد اعتمدت على بعض الدراسات السابقة التي تصب في إطار آليات مكافحة الجريمة الإلكترونية، وسيتم تناولها حسب حداثتها كالتالي:

- دراسة بعنوان **الجريمة الإلكترونية واقع وتحدي** من إعداد الطالبتين: رزيق ليلة ورمضاني حميدة، لسنة 2018/2017، والتي جاءت لدراسة مدى فعالية النصوص القانونية في مكافحة الجريمة الإلكترونية.
- دراسة تمحورت حول **الجريمة الإلكترونية وإجراءات مواجهتها**، للطالبين شاهين خضر ورضوان سعادة، لسنة 2021/2020، والتي جاءت للتعريف بالجريمة الإلكترونية وإجراءات مواجهتها.

- دراسة للطالبين لمعرق منير وعمارة خليل، لسنة 2021/2020، تحت عنوان **مكافحة الجريمة الإلكترونية** والتي جاءت للبحث في السبل القانونية والآليات المتبعة للحد من الجريمة الإلكترونية سواء على الصعيد الدولي أو المحلي.
- دراسة بعنوان **آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري** للطالبتين بيكة باكة وموساوي لمياء، لسنة 2023/2022، وذلك للتعرف عن الآليات القانونية والمؤسساتية لمكافحة الجريمة الإلكترونية في التشريع الجزائري.

وكانت هذه الدراسات مجتمعة بمثابة مرشد ودليل علمي حيث أفادتني في تكوين الفكرة الأساسية عن موضوع البحث وتحديد معالم الدراسة بدقة، عبر ضبط الأبعاد والعناصر الرئيسية لها وكذا توسيع المعلومات حول الموضوع، كما ساعدتني في وضع خطة البحث والاستناد عليها بالإضافة إلى إعانتي في الوصول للمادة العلمية من خلال التوجه مباشرة إلى المراجع والمؤلفات الخاصة بالجريمة الإلكترونية.

من خلال ما سبق تمحورت **إشكالية** الدراسة في:

فيما تتمثل الآليات الدولية والوطنية لمكافحة الجريمة الإلكترونية؟

وقد تفرعت عدة **تساؤلات** عن هذه الإشكالية ومن بينها:

- ما هي الجريمة الإلكترونية؟
- ما هي الآليات الدولية لمكافحة الجريمة الإلكترونية؟
- ما هي الآليات الوطنية لمكافحة الجريمة الإلكترونية؟

للقيام ببحث موضوعي ومنظم أو تتبع ظاهرة معينة لابد من تبني **منهج** علمي يتوافق مع الإشكالية المطروحة، وذلك للوصول إلى نتائج دقيقة، والمنهج المتبع في هذه الدراسة هو المنهج الوصفي التحليلي الذي اعتمدت عليه للتطرق للمعلومات

والتعاريف والمصطلحات التي تناولتها هذه الدراسة، وكذا تحليل النصوص القانونية على مستوى التشريع الجزائري.

الصعوبة الجوهرية هي اختلاف المصطلحات بين الإلكترونية والمعلوماتية والسيبرانية، رغم أن المصطلح الأصح والمتفق عليه هو هذا الأخير إلا أنني ارتأيت اختيار المصطلح الأكثر تداولا في المراجع حتى يتسنى لي استخراج الفقرات بدون المساس بمصطلحاتها عند الاقتباس والنقل.

لمعالجة مسألة الجريمة الإلكترونية وآليات مكافحتها وللإجابة على الإشكالية المطروحة اتبعت **الخطة** التالية:

الفصل الأول حول خصوصية الجريمة الإلكترونية وآليات مكافحتها دوليا وقد ضم مبحثين؛ المبحث الأول تضمن تعريفات الجريمة الإلكترونية وأركانها بالإضافة إلى أنواعها وخصائصها. أما المبحث الثاني فجاء بعنوان الآليات الدولية لمكافحة الجريمة الإلكترونية وتضمن أبرز الجهود الإقليمية والدولية المبذولة في سبيل مكافحة الجريمة الإلكترونية.

والفصل الثاني تمحور حول مكافحة الجريمة الإلكترونية على المستوى الوطني وقسم إلى مبحثين؛ الأول تطرق إلى المكافحة الموضوعية للجريمة الإلكترونية من خلال القوانين التي سنها المشرع الجزائري بموجب القوانين العامة والخاصة، أما المبحث الثاني فتناول المكافحة الإجرائية للجريمة الإلكترونية من خلال تبيان إجراءات التحقيق والإثبات في الجريمة الإلكترونية محليا، وكذا الجهاز المؤسساتي العملياتي القائم على محاربة الجريمة الإلكترونية في الجزائر.

وقد توجت الدراسة بخاتمة تتضمن إجابة عن الإشكالية المطروحة كحوصلة عن موضوع آليات مكافحة الجريمة الإلكترونية، وتم التطرق فيها إلى أهم النتائج المتوصل إليها، بالإضافة إلى إبداء بعض التوصيات.

الفصل الأول

خصوصية الجريمة الإلكترونية وآليات مكافحتها دوليا

الفصل الأول: خصوصية الجريمة الإلكترونية وآليات مكافحتها دوليا

لقد كان للتطور التكنولوجي أثر على الأفراد والدول على حد سواء، فمع بروز الثورة المعلوماتية وتوسع استخدام شبكة الإنترنت اتسع مجال المعاملات بين الأشخاص ليشمل العديد من الميادين، وبدأت تظهر جرائم من نوع خاص أخذت العديد من الصور والأشكال، يطلق عليها اسم الجرائم الإلكترونية وهي خطيرة لما لها من خصائص تميزها عن تلك التقليدية.

ونظرا للصبغة العالمية للجريمة الإلكترونية، فإن مكافحتها تستدعي تضافر جهود الدول المهددة بها، قصد اعتماد اتفاقيات دولية توحد الحلول والإجراءات لمجابهتها وحتى لا يكون المجرم المعلوماتي في مأمن من التتبع والعقاب أينما وجد في العالم.

ومما تقدم سيتم التعرف على الجريمة الإلكترونية وأهم الآليات الدولية لمكافحتها من خلال المبحثين التاليين:

- **المبحث الأول: خصوصية الجريمة الإلكترونية**
- **المبحث الثاني: الآليات الدولية لمكافحة الجريمة الإلكترونية**

المبحث الأول: خصوصية الجريمة الإلكترونية

أدى التقدم التكنولوجي المذهل للمعلومات إلى ظهور ما يعرف بالجريمة الإلكترونية، ويرجع ذلك إلى استخدام التكنولوجيا والإنترنت في كامل جوانب الحياة اليومية للأفراد، ونتيجة لارتباط الجريمة الإلكترونية بالتطور العلمي ظهرت هناك اتجاهات فقهية قامت بتحديد مفهوم هذه الجريمة وخصائصها التي تتميز بها نظرا لحداثتها وأنواعها التي تتميز بموجبها عن الجريمة التقليدية.

وسوف يتم التطرق في هذا المبحث إلى مطلبين؛ يعالج المطلب الأول مفهوم الجريمة الإلكترونية، بينما يخصص المطلب الثاني إلى خصائص وأنواع الجريمة الإلكترونية.

المطلب الأول: مفهوم الجريمة الإلكترونية

سيتناول هذا المطلب الجريمة الإلكترونية ومختلف التعريفات التي أسندت إليها، بالإضافة إلى أركانها الأربعة؛ الركن الشرعي والمادي والمعنوي والمفترض، وهذا من خلال الفرعين المواليين:

الفرع الأول: تعريف الجريمة الإلكترونية

وسيتم التطرق في هذا الفرع إلى مختلف تعاريف الجريمة الإلكترونية والمجرم الإلكتروني.

أولا: تعريف الجريمة الإلكترونية لغة:

1. تعريف الجريمة لغة:

الجريمة والجُرُم معناها في اللغة الذنب، ومن اشتقاقاتها جرم وأَجْرم واجترام، وتجرَّم عليه معناها ادعى عليه ذنباً لم يفعله، وكلمة لا جرم تعني القسم، والجرم هو الذنب أو الجناية.[1]

2. **تعريف الإلكترونية لغة:**

يقصد بها المعالجة الآلية للمعلومات وهي ترجمة للمصطلح الفرنسي (Informatiqe) وهي اختصار للكلمتين الفرنسيتين (Information) معلومات (Automatique) ذاتيا، وصاحب هذا المصطلح هو "فليب داريفوس" الذي أراد أن يعني به العلم الذي يربط علم الحاسوب (Computer Science) والمعلومات (Information) والاتصالات (Telecommunication).[2]

أما المفهوم الاجتماعي للجريمة فهو يقوم على أساس اعتبارها خطيئة اجتماعية، إذ تمثل خروجا على القيم الاجتماعية العليا للمجتمع كما تستوجب استنفار المجتمع لمعاقبة فاعله وبما يكفل أمن المجتمع واستقراره. ويعرف علماء الاجتماع الجريمة بأنها: "كل الأفعال المتنافية للقيم السائدة في المجتمع والذي يتبع إتيانه ردود فعل من السلطة المختصة لحماية القيم عن طريق وسائل الردع والعقاب التي توقع على مرتكبي تلك الأفعال".[3]

---

[1] ابن منظور، لسان العرب، ط1، القاهرة، دار المعارف، د س ن، ص263.

[2] زين العابدين الكردي، جرائم الإرهاب المعلوماتية، ط1، لبنان، منشورات الحلبي الحقوقية، 2018، ص46.

[3] جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية: دراسة مقارنة، دط، د ب ن، دار الثقافة للتوزيع والنشر، 2010، ص37.

ثانيا: تعريف الجريمة الإلكترونية اصطلاحا

يعرفها البعض بأنها: "كل عمل يرتكب من شخص كامل الأهلية باستخدام الحاسب الآلي أو شبكة الانترنت يلحق الضرر والأذى بالغير، وأن يقع على الحاسب الآلي نفسه ويكون هذا الفعل معاقبا عليه بالقانون".[1]

وتعرف الجريمة الإلكترونية اصطلاحا بأنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة على الحاسب أو التي تحول عن طريقه. كما أنها كل فعل إجرامي أيا كان صلته بالمعلومات وسينشأ عنه خسارة تلحق بالمجني وكسب يحققه الفاعل".[2]

ويقصد بها أيضا: "عمل أو امتناع يسبب أضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض لها عقابا".[3]

ثالثا: التعريف الفقهي للجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها ولم يتفق الفقهاء على إعطاء تعريف موحد للجريمة الإلكترونية، لارتباط هذا النوع من الجرائم بنظم المعالجة الآلية للمعطيات، لذلك جاءت تعاريفهم بين موسع وضيق.

---

[1] ميرفت محمد حبابية، مكافحة الجريمة الإلكترونية، ط1، الأردن، دار اليازوري العلمية، 2020، ص36.

[2] شاهين خضر ورضوان سعادة، الجريمة الإلكترونية وإجراءات مواجهتها، مذكرة مقدمة لنيل شهادة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2021/2020، ص11. نقلا عن: سليمة سعيدي وبلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، ط1، الإسكندرية، دار الفكر الجامعي، 2017، ص55.

[3] حميدة رمضاني وليلة رزيق، الجريمة الإلكترونية واقع وتحدي، مذكرة مقدمة لنيل شهادة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018/2017، ص6. نقلا عن: احسن رابحي، (الجريمة الإلكترونية: النقطة المظلمة بالنسبة للتكنولوجيا المعوماتية)، المجلة الجزائرية للعلوم القانونية الاقتصادية السياسية، العدد01، جامعة الجزائر1، كلية الحقوق، الجزائر، 2011، ص227.

1. الاتجاه الموسع:

يذهب أنصار هذا الاتجاه إلى التوسع في تعريف الجريمة المعلوماتية واعتبارها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، ويهدف إلى الاعتداء على الأموال والأشياء المعنوية فيعرفونها بأنها: "كل سلوك إجرامي يتم بمساعدة الكومبيوتر"، أو هي: "كل جريمة تتم في محيط أجهزة الكومبيوتر".[1]

وقد توسع الخبير الأمريكي "Poker" في تعريف الجريمة الإلكترونية واعتبرها: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل".[2]

وعليه فإن أنصار هذا الاتجاه، يعتمدون على وسيلة الارتكاب (الكومبيوتر) في تحديد تعريف الجريمة الإلكترونية، فكل سلوك إجرامي يعتمد على الكومبيوتر فهو جريمة الإلكترونية، أي بمجرد إدخال الحاسب الآلي في النشاط الإجرامي نكون أمام جريمة الإلكترونية.

2. الاتجاه الضيق:

اختلف أنصار هذا الاتجاه في تعريف الجريمة الإلكترونية حسب المعيار المعتمد في ارتكابها، فهناك من اعتمد على معيار وسيلة الارتكاب (الكومبيوتر)، وعرفها بأنها: "الجرائم التي تلعب فيها بيانات الكومبيوتر والبرامج المعلوماتية دورا مهما، أو هي كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية"،[3] ويذهب البعض الآخر إلى التضييق بدرجة كبيرة في مفهوم الجريمة الإلكترونية، فيشترط لارتكابها أن يكون

---

[1] أمير فرح يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر، ط1، مصر، مكتبة الوفاء القانونية، 2011، ص10.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، مصر، دار الثقافة للنشر والتوزيع، 2008، ص49.

[3] حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، ط1، بيروت، منشورات الحلبي الحقوقية، 2014، ص25.

الجاني يتوفر على معرفة كبيرة بتقنيات الحاسوب، فيعرفونها بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى".[1]

ويلاحظ على هذه التعاريف أنها ضيقت من مفهوم الجريمة الإلكترونية، حيث أنها جاءت كلها قاصرة على ظاهرة الإجرام الإلكتروني مع الاختلاف في المعيار المعتمد في ارتكاب الجريمة، وسواء كان موضوع الجريمة، أو وسيلة ارتكابها أو معيار النتيجة إلا أنهم اتفقوا على أن هذه الجريمة بالرغم من الطابع التقني لها، إلا أنها قد ترتكب من شخص لا يملك قدر كبير من المعرفة، لأن الأهم هو الفعل غير المشروع في البيئة الرقمية.

ويعرفها **الفقه الجزائري** بأنها: "الجريمة التي تتم باستخدام جهاز الكومبيوتر من خلال الاتصال، أو أنها تستخدم الأجهزة التقنية الحديثة، مثل الحاسب الآلي والهاتف النقال، أو أحد ملحقاتهما أو برامجهما في تنفيذ أغراض مشبوهة أو أمور غير أخلاقية لا يرتضيها المجتمع"[2].

رابعا: موقف المشرع الجزائري

لم يتطرق المشرع الجزائري إلى تعريف الجريمة الإلكترونية في قانون العقوبات، واكتفى بالعقاب على بعض الأفعال التي تشكل جرائم الانترنت في المواد من 394 مكرر إلى 394 مكرر7 تحت عنوان: "الجرائم الماسة بنظام المعالجة الآلية للمعطيات".[3]

---

[1] نائلة عادل محمد فريد، جرائم الحاسب الاقتصادي، ط1، القاهرة، دار النهضة العربية، 2013، ص21.

[2] زليخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، ط1، الجزائر، دار الهدى، 2011، ص42.

[3] القانون 04-15، المؤرخ في 2004/11/10، المعدل والمتمم لأمر 66-155، المؤرخ في 1966/06/08، المتضمن قانون العقوبات، الجريدة الرسمية، الجزائر، 2004، العدد47.

غير أن المشرع الجزائري تبنى مفهوما موسعا للجريمة الإلكترونية في القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، حيث أطلق عليها في هذا القانون مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، والتي تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات (أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام الاتصالات الإلكترونية)، واعتبر أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات مادية (محلا للجريمة)، ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحقيقه لتوفر أركان الجريمة وعليه فإن مفهوم الجريمة المعلوماتية في التشريع الجزائري لم يعد مقتصرا فقط على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء، بل تشمل أيضا الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها[2].

ولم يتطرق المشرع الجزائري أيضا إلى مفهوم الجريمة المعلوماتية في القانون 18-05 المتعلق بالتجارة الإلكترونية[3]، رغم أنه تطرق إلى بعض الجرائم الإلكترونية والعقوبات المقررة لها في الفصل الثاني من الباب الثالث، تحت عنوان "الجرائم والعقوبات".

وبما أن لكل جريمة مجرم ينفذها، فإن **المجرم الإلكتروني** أخطر من نظيره التقليدي، حيث يطلق مصطلح المجرم الإلكتروني على ذلك الفاعل الرئيس في عملية الجريمة الإلكترونية، كونه يتمتع بذكاء ودراية معلوماتية ناتجة عن تعلم وخبرة ميدانية

[1] القانون 09-04، المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، الجزائر، 2009، العدد47.

[2] صليحة بوجادي، (الإطار المفاهيمي للجريمة المعلوماتية)، مجلة الدراسات القانونية المقارنة، مخبر القانون الخاص، العدد1، المجلد7، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2021، ص2530.

[3] القانون 18-05، المؤرخ في 2018/05/10، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، الجزائر، 2018، العدد28.

في عالم الإلكترون.. إذ أن الجريمة الإلكترونية لا تقع على أرض الواقع ولا بالوسائل المادية والأدوات المستعملة في الجريمة التقليدية ولا تثبتها قرائن مادية، إنما تقع في فضاء رقمي بواسطة التقنيات الحديثة المرتبطة بالشبكة العالمية مما يصح أن تسمى بالجريمة العابرة للحدود، يتميز الفاعلين فيها بصفات وسمات لم تكن موجودة عند المجرمين التقليديين، ويتوفر المجرم الإلكتروني على مهارة عالية في مجال المعلوماتية والبرمجة حيث يمكنه اختراق الشبكات بمهارات فائقة في كسر الشفرات وكلمات المرور للحصول على أدق المعلومات، ويشغل أجهزة عن بعد بكل سرية من خلال ارتباطه بشبكة الإنترنت مستغلا تجربته وذكاؤه في تطوير الأنظمة الأمنية المعلوماتية وتعديلها[1].

ويتميز المجرم الإلكتروني بعدة سمات وهي:

- **إنسان متخصص:** المجرم الإلكتروني شخص متخصص ماهر في مجال الحاسوب وتقنياته؛
- **الشخصية الاجتماعية:** يعتبر المجرم الإلكتروني إنسانا اجتماعيا قادرا على التكيف مع المجتمع ويتوافق معه كونه شديد الذكاء؛
- **الاحترافية والذكاء:** يتميز المجرم الإلكتروني بالذكاء وعدم الميول لاستعمال العنف والقوة؛
- **السلطة تجاه النظام الإلكتروني:** وهي مجموعة من المزايا التي تضمن للمجرم الإلكتروني ارتكاب جريمته، تتمثل في الشيفرة الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات التي تتيح قرصنة الملفات والعبث بها.[2]

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ط1، مصر، دار الكتب القديمة، 2007، ص83.

[2] نهلا عبد القادر المومني، المرجع السابق، ص80.

الفرع الثاني: أركان الجريمة الإلكترونية

تتمثل أركان الجريمة الإلكترونية كغيرها من الجرائم في الركن الشرعي والركن المادي والركن المعنوي:

أولا: الركن الشرعي

ويقصد به اعتراف المشرع والنص القانوني على تجريم الفعل المرتكب، حيث أنه لا جريمة ولا عقوبة إلا بنص، وتأكيدا على ذلك فإن المشرع الجزائري قد أحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات".[1]

ثانيا: الركن المادي

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة كالتبليغ عن الجريمة قبل تحقق نتيجتها، إلا أنه لا مناص من معاقبة الفاعل.

وقد يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب كجريمة الغش المعلوماتي، حيث يتجسد الركن المادي فيها في تغيير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية.

ثالثا: الركن المعنوي

يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين هما العلم والإرادة:

- **العلم:** وهو إدراك الفاعل للجرم أو الفعل المجرم.

[1] المادة 394 مكرر من القانون رقم 04-15 المؤرخ في 2004/11/10.

- **الإرادة:** توجه السلوك الإجرامي أي الرغبة لتحقيق الجريمة.

رابعا: الركن المفترض

ويتمثل هذا الركن في وجود جهاز إلكتروني في الغالب وهو جهاز الكمبيوتر كركن مفترض يشكل الوسيلة المستخدمة لارتكاب السلوك في الركن المادي للجرائم الإلكترونية بوجود تلك البيئة الرقمية المتصلة بالإنترنت.[1]

المطلب الثاني: خصائص وأنواع الجريمة الإلكترونية

سيتم التفصيل ضمن هذا المطلب في خصائص وأنواع الجريمة الإلكترونية، وذلك في فرعين على النحو التالي:

الفرع الأول: خصائص الجريمة الإلكترونية

إن ارتباط الجريمة الإلكترونية بجهاز الحاسب الآلي وشبكة الإنترنت أضفى عليها مجموعة من الخصائص التي تميزها عن الجرائم التقليدية، ولعل من أهمها ما يلي:

أولا: الخصوصية المتعلقة بالجريمة في حد ذاتها:

- **جرائم تقنية:** جرائم الحاسوب ترتكب بواسطة الحاسب الآلي وكذلك عبر شبكة الإنترنت فهي حلقة الوصل الرئيسية بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات وغيرها من الأهداف التي تكون غالبا الضحية لتلك الجرائم؛
- **جريمة عابرة للدول:** حيث أنها جريمة عابرة للحدود، فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان

[1] صهيب ياسر محمد شاهين وبشرى محمد محسن أبو ترابي، (الجريمة الإلكترونية وبعدها القانوني)، مجلة نومبروس الأكاديمية، العدد1، المجلد2، جامعة عباس لغرور، خنشلة، الجزائر، 2021، ص155.

دون أن تخضع لحرس الحدود، وهو ما خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى شكليات تتعلق بإجراءات الملاحقة القضائية وغيرها من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام؛

- **صعوبة الكشف عنها:** تتميز الجريمة الإلكترونية بصعوبة التحري والتحقيق نظرا لارتكابها في الخفاء، وعدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من أفعال إجرامية، فالتحري عنها ينطوي على العديد من المشكلات والتحديات الإدارية والقانونية، والتي تتصل ابتداء من عملية ملاحقة الجناة فإذا تحققت إمكانية الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجريمة؛
- **جرائم معقدة:** تتسم بالخطورة البالغة من عدة جوانب، فمن ناحية أولى نجد الخسائر الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية خاصة جرائم الأموال، ومن ناحية ثانية نجدها ترتكب من فئات متعددة تجعل من التنبؤ بها أمرا صعبا ومن ناحية ثالثة تنطوي على سلوكيات غير مألوفة؛
- **عدم الإبلاغ عنها:** قلة الإبلاغ عن وقوع الجريمة الإلكترونية، وذلك راجع لسببين أولهما الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الإنترنت تم الكشف عنها بالصدفة أو بعد فترة طويلة من ارتكابها والسبب الثاني هو عدم اكتشاف الضحية للجريمة مما يعني أن الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها.

ثانيا: الخصوصية المتعلقة بالمجرم الإلكتروني:

الصورة التقليدية للمجرم تكاد تختفي في الجرائم الإلكترونية بل وعلى العكس من ذلك فالمجرم الإلكتروني عادة ما ينتمي إلى مستوى اجتماعي مرتفع عن غيره من المجرمين، كما أنه لا ينظر إليه كمجرم بالمعنى المتعارف عليه لهذه الكلمة وذلك لكون الأسباب والعوامل التي تقف وراء ارتكاب الجريمة المعلوماتية تختلف بالمقارنة بالجريمة التقليدية.[1]

الفرع الثاني: أنواع الجرائم الإلكترونية

تعددت وتنوعت الجرائم الإلكترونية، حيث قسمها الفقه إلى طائفتين رئيستين وهما:

أولا: الجرائم الواقعة بواسطة النظام المعلوماتي

تتنوع الجرائم الواقعة بواسطة النظام المعلوماتي إلى جرائم اقتصادية، أو قرصنة المعلومات، أو ذات طابع سياسي أو متعلقة بالأمن القومي، أو قد تقع هذه الجرائم على أشخاص طبيعية أو الاعتبارية، وتتمثل هذه الجرائم في:

1. **الجرائم الإلكترونية الواقعة على الأشخاص:** كجريمة التهديد والمضايقة عبر البريد الإلكتروني أو عن طريق وسائل التواصل الاجتماعي مثل الفايسبوك ومن أهم جرائم الأشخاص جرائم التشهير والابتزاز التي تتخذ أشكال مختلفة انطلاقا من الصور إلى التسجيلات المرئية والمسموعة التي تتم عبر الإنترنت.

[1] محمد عبد الرحمان عنانزة، القصد الجرمي في الجرائم الإلكترونية، دط، عمان، دار الأيام للنشر، 2017، ص51.

2. **الجرائم الإلكترونية المتعلقة بالأموال:** كالسطو والسرقة والتحويل الإلكتروني غير المشروع للأموال وجريمة غسيل الأموال إلكترونيا وقرصنة الحسابات البنكية بطريقة غير مشروعة.
3. **الجرائم الواقعة على أمن الدولة:** وهي من أخطر الجرائم الإلكترونية وأهمها الإرهاب الإلكتروني والتجسس الإلكتروني الذي يهدد الأسرار العسكرية والاقتصادية للدول مما يسهل خلق الفوضى والمساس بأمنها الداخلي.

ثانيا: الجرائم الواقعة على النظام المعلوماتي

يمس هذا النوع من الجرائم إما المكونات المادية للنظام المعلوماتي كالكابلات أو المكونات المعنوية (البرامج)، حيث يستلزم معرفة فنية عالية في مجال البرمجة وتقع هذه الجرائم إما على برامج التطبيق أو برامج التشغيل.[1]

يتبين من خلال هذا الفرع أن صور وأنواع الجرائم الإلكترونية لا تخرج من كونها إما جرائم ضد الأشخاص أو ضد الأموال أو ضد أمن الدولة، وهي ذات الصور التي تعرفها الجرائم التقليدية، حيث أن الاختلاف يكمن في الوسيلة المستعملة وهو الحاسوب ولواحقه، وهو ما يجعل بعض الفقهاء يعتبرون أن خصوصية هذه الجريمة تكمن في ركنها المفترض وهو استعمال المعلوماتية أو العالم السيبراني.

[1] سالمي علي عياد حامد، الجريمة الإلكترونية، ط1، الإسكندرية، دار الفكر الجامعي، 2007، ص39.

المبحث الثاني: الآليات الدولية لمكافحة الجريمة الإلكترونية

إن بروز الإجرام الإلكتروني كشكل جديد من أشكال الجرائم المختلفة والمنتشرة حول العالم، وبالنظر إلى تزايد خطورته وتهديداته للأمن والاستقرار العالميين لخصوصية طبيعته لكونه يعتمد بالدرجة الأولى على التطور التكنولوجي المتسارع، دفع معظم الدول إلى بذل الجهود والتكاتف فيما بينها من أحل حماية الأنظمة المعلوماتية، حيث بادرت باتخاذ جملة من التدابير والإجراءات وعقد الاتفاقيات المناسبة في سبيل ذلك، وهذا سعيا منها لسد الفجوة القانونية في هذا المجال.

وسيتم التطرق للجهود الدولية والإقليمية المبذولة في هذا المجال وفق مطلبين؛ يعالج المطلب الأول الجهود الإقليمية لمكافحة الجريمة الإلكترونية، بينما يخصص المطلب الثاني إلى الجهود الدولية لمكافحة الجريمة الإلكترونية.

المطلب الأول: الجهود الإقليمية لمكافحة الجريمة الإلكترونية

تشكل الجهود التي سعت إليها الدول ومختلف المنظمات العالمية من خلال التنسيق بين مختلف الوسائط التقنية والأكاديمية، وتكثيف آليات الاتصال والتعاون من خلال وضع استراتيجيات مختلفة لمواجهة التهديدات الإلكترونية في نطاق ومسؤولية كل طرف، وعليه سيتم التعرض إلى الجهود الإقليمية لمكافحة الجريمة الإلكترونية وذلك وفق فرعين.

الفرع الأول: الجهود العربية

سيتم من خلال هذا الفرع عرض الاتفاقية العربية لمكافحة جرائم تقنية المعلومات باعتبارها من أهم الاتفاقيات العربية التي انعقدت في هذا المجال.

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهم المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 21 ديسمبر 2010 وتحتوي على (43) مادة وجاء في مضمون المادة الأولى منها *"تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها"* ونجد في الفصل الثاني تفصيلا للأفعال التي تعد مجرمة، وفي الفصل الثالث تتعرض لنطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع تعرضت للتعاون القانوني والقضائي وفي الفصل الخامس تعرضت إلى أحكام ختامية.[1]

الفرع الثاني: الجهود الأوروبية والإفريقية

مع تطور المعلومات وظهور الجريمة الإلكترونية سارعت الدول الأوروبية والإفريقية لإيجاد استراتيجيات لمواجهة هذا التهديد الجديد.

أولا: الجهود الأوروبية

1. اتفاقية بودابست:

تعد اتفاقية بودابست الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر وباستخدام شبكة الإنترنت، وهي تمثل ركيزة أساسية منذ دخولها حيز النفاذ في الأول من جويلية لعام 2004 أعلى مستوى الدول أعضاء مجلس الاتحاد الأوروبي وكما سبق الإشارة فلقد وقعت عليها العديد من الدول من غير أعضاء مجلس أوروبا مثل كندا واليابان وجنوب إفريقيا، كما صادقت عليها

[1] يوسف محمود حسنين، الجريمة المعلوماتية وسبل مكافحتها محليا ودوليا، ط1، الإسكندرية، دار الفكر الجامعي، 2013، ص139.

الولايات المتحدة الأمريكية، كما تعتبر هذه الاتفاقية بمثابة دعوة موجهة إلى دول العالم للتفاعل مع الإنترنت جاءت نتيجة محاولات عديدة منذ ثمانينيات القرن العشرين حتى ظهرت بشكلها النهائي في 23 نوفمبر 2001 في بودابست، ووقعت عليها ثلاثون دولة أوروبية بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوروبي للمشاركة في إعداد هذه الاتفاقية، وفي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية، وقد تضمنت هذه الاتفاقية الأقسام التالية:

- **القسم الأول:** تحديد المصطلحات؛
- **القسم الثاني:** الخطوات الواجب اتخاذها في إطار التشريع الوطني؛
- **القسم الثالث:** التعاون الدولي؛
- **القسم الرابع:** الشروط النهائية حول الانضمام إلى الاتفاقية.[1]

2. اتفاقية المجلس الأوروبي

اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ عام 1976، وفي عام 1996 أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة الإلكترونية، عملت اللجنة بين سنتي 1997 و2000 على الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر أفريل 2001، وتم التصديق على الاتفاقية من قبل 30 دولة بحلول العام 2010، واتفاقية جرائم الإنترنت هي المعاهدة الدولية الأولى التي تسعى لمعالجة الجرائم الإلكترونية عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى.

[1] محمود أحمد عبابنة ومحمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دط، عمان، دار الثقافة للنشر والتوزيع، 2009، ص119.

ومن أهم أهداف الاتفاقية:

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية؛
- توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونيا؛
- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخل في محتواها؛
- تتضمن الاتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.[1]

ثانيا: الجهود الإفريقية

تعتبر إفريقيا هي الأخرى من القارات التي تأثرت بتفشي مثل هذه الظاهرة الإجرامية، حيث سعى الاتحاد الإفريقي لإيجاد حلول وآليات للحد من هذه الظاهرة، وهو ما سيتم التفصيل فيه.

الاتحاد الإفريقي:

طلب المؤتمر الاستثنائي لوزارة الاتحاد الإفريقي المسؤولين عن تكنولوجيا المعلومات والاتصالات المنعقد في جنوب إفريقيا من 02 إلى 05 نوفمبر 2009 من مفوضية الاتحاد الإفريقي القيام بالاشتراك مع لجنة الأمم المتحدة الاقتصادية لإفريقيا بإعداد اتفاقية حول التشريع القضائي على أساس احتياجات القارة والالتزام بالمتطلبات القانونية والتنظيمية للمعاملات الإلكترونية والأمن الإلكتروني وحماية البيانات الشخصية، كما أوصت بضرورة توفير الحماية القانونية لأنظمة المعلوماتية التي تعتبر قيمة بالنسبة للمجتمع مما يجعل من الضروري سن التشريعات ضد الجريمة

[1] علي حسن الطوالبة، الجرائم الإلكترونية، ط1، البحرين، دار الحقوق التطبيقية، 2008، ص100.

الإلكترونية، وفي يونيو 2014 اجتمع مجموعة من قادة الاتحاد الإفريقي المكون من 54 حكومة إفريقية في القمة الـ 23 للاتحاد الإفريقي، ووافقوا على اتفاقية الاتحاد الإفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية.[1]

المطلب الثاني: الجهود الدولية لمكافحة الجريمة الإلكترونية

سنتعرف في هذا المطلب على الجهود والمساهمات التي يتم بموجبها التصدي للجريمة الإلكترونية على الصعيد الدولي.

الفرع الأول: التعاون القضائي في مجال مكافحة الجريمة الإلكترونية

إن إجراءات التحقيق والملاحقة القضائية في جرائم الإنترنت تقتضي تتبع النشاط الإجرامي، الأمر الذي يستوجب تقصي آثار الجريمة من مصدرها إلى غاية تنفيذها وتحديد مواقع الأضرار التي مستها، وهذه الأفعال قد تقع في مختلف البلدان ولهذا يتطلب ملاحقة مرتكبي هذه الجرائم وذلك بالتعاون القضائي الدولي وتمديد صلاحيتها إلى كل البلدان ليكون التعاون دولي وفعال للقضاء على هذه الظاهرة الإجرامية ويمكن وفق ذلك استعراض شكلين من أشكال التعاون القضائي وهما:

أولا: التعاون الأمني

بما أن الجريمة الإلكترونية هي جريمة دولية فمن المفروض أن لا تكون الحدود الجغرافية معضلة تقف في وجه الإجراءات الجنائية للتصدي لهذه الجرائم وملاحقة مجرمي المعلومات المنتشرين في كل مكان، فمثلا يمكننا أن نجد مجرم يحمل جنسية دولة معينة ويقوم بأفعاله ونشاطاته في نطاق وبأجهزة دولة أخرى في حين تقع آثار وأضرار هذه الجريمة على دولة أخرى، ولذا كانت الحاجة ملحة وضرورية جدا لتوحيد

[1] سامي علي عياد حامد، المرجع السابق، ص44.

الجهود وتضافر كل الدول بقوانينها ومراسيمها الجنائية أن تتوحد لمتابعة مجرمي المعلومات للكشف عن هوياتهم وشركائهم والمؤسسات التي تساعدهم في ذلك، لأن جهود الدولة الواحدة وبأنظمتها الأمنية لا تكفي للقضاء على الجريمة الإلكترونية، لكونها تطارد مجرمين في نطاقها الجغرافي فقط وفي حالة فرار المجرم إلى دولة أخرى تتوقف ملاحقته وهو يستمر في أفعاله غير المشروعة وكبد الدولة التي يتواجد بها أضرار مماثلة للتي قام بها في دولته الأم.[1]

وهناك عدة **أشكال** للتعاون الأمني لمكافحة الجريمة الإلكترونية وهي:

1. إنشاء مكاتب وهيئات متخصصة لجمع المعلومات حول مرتكبي الجرائم الإلكترونية ونشرها:

الغرض منها هو تنمية تعاون السلطات القضائية الدولية في مجال مكافحة الجريمة، من خلال جمع البيانات والمعلومات الخاصة بالمجرم وتعميمها بين الدول وكذا تبادل الخبرات وتقديم العون لكل الأطراف إن استلزم الأمر ذلك.

2. التعاون في إطار المنظمة العالمية للشرطة الجنائية "الأنتربول":

الهدف من إنشائها هو تأكيد وتشجيع التعاون الدولي بين أجهزة الشرطة بشكل فعال وسلس في مكافحة الجريمة الإلكترونية والمنتمون إليها سواء أشخاص أو مؤسسات، وذلك بجمع المعلومات والبيانات عن هؤلاء المجرمين من خلال المكاتب المركزية الوطنية للشرطة الدولية المتواجدة في كل دولة منضوية تحتها وتبادلها فيما بينها، وقد ساهمت هذه المنظمة الدولية في حل الكثير من القضايا المتعلقة بالجريمة الإلكترونية خاصة فيما يتعلق بتبييض الأموال والتجارة الإلكترونية والقبض على عدة مجرمين مبحوث عنهم وتسليمهم للدولة لمقاضاتهم وتسليط العقوبات عليهم.

[1] محمود أحمد عبابنة ومحمد معمر الرازقي، المرجع السابق، ص132.

3. القيام بعمليات أمنية مشتركة لمتابعة مجرمي المعلومات:

ويتم ذلك بتتبع الأدلة والبيانات الرقمية وضبطها والقيام بعمليات التفتيش العابر للحدود لمكونات الأجهزة الإلكترونية منها أجهزة الإعلام الآلي وشبكات الاتصال للبحث عن الأدلة والبراهين، وهذا لا يتأتى إلا بالتعاون الدولي والاشتراك في عمليات نوعية مكثفة ودورية وفي مناسبات خاصة، وما من شأنه أن يصقل المهارات وتبادل الأفكار والخبرات بين المشاركين من أجل مكافحة للجريمة الإلكترونية والتصدي لها[1].

ثانيا: المساعدات الدولية القضائية لمكافحة الجريمة الإلكترونية

يمكن استنتاج المبادئ العامة التي تحكم الالتزام بالمساعدة الفضائية المتبادلة في الفقرة 1 من المادة 25 من اتفاقية بودابست بالمجر للإجرام الإلكتروني والالتزام بالمساعدة، يجب أن يتوفر لأقصى حد ممكن وتكون شاملة وممتدة وخالية من الصعوبات والمعوقات.

وتتخذ المساعدة القضائية عدة **أشكال** نذكر منها:

1. تبادل المعلومات حول الجريمة الإلكترونية:

ويتم ذلك بتبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها السلطة القضائية بصدد النظر في جريمة ما وتبادل السوابق القضائية للمتابعين ولملفاتهم القضائية للجرائم المتابع فيها في دولته الأصل، ونجد لهده الصورة تطبيقات عديدة منها ما ورد في الفقرتين 6 و7 من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في القضايا الجنائية وكذلك الفقرات 3 و4 من المادة الثامنة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة.

[1] محمد عبد الله قاسم، الحماية الجنائية للمعلومات الإلكترونية، ط1، مصر، دار الكتب القانونية، 2010، ص128.

2. نقل الإجراءات الجنائية لجرائم المعلومات:

يقصد به قيام دولة معينة بموجب اتفاقية معينة باتخاذ جملة من الإجراءات الجنائية بصدد جريمة ارتكبت في حدود دولة أخرى ولمصلحة تلك الدولة بناء على توفر جملة من الشروط من أهمها التجريم المزدوج الذي يعني أن يكون الفعل مجرم في كل من الدولة الطالبة والدولة المطلوب لها نقل الإجراءات بالإضافة إلى مشروعية الإجراءات المطلوب اتخاذها، أي أن توافق قانون الدولة المطلوب منها وأن تكون جدية وذات أهمية بالقدر الذي يسهم في الوصول إلى الحقيقة في الكشف عن ملابسات الجريمة، وقد أقرت العديد من المواثيق والمعاهدات على هذا الشكل نذكر مثلا معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في مادتها 21 والمادة 23 من اتفاقية بودابست للإجرام الإلكتروني.

3. الإنابة القضائية الدولية:

وتعني اتخاذ إجراء قانوني من إجراءات الدعوى الجنائية لأثره المباشر من أجل الفصل في مسألة معروضة على السلطة القضائية التي تعذر على الدولة التي تقدمت بطلب الإنابة القيام به بنفسها والهدف منها هو تسهيل الإجراءات الجنائية بين الدول لضمان إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، وعادة ما يتم طلب الإنابة عبر قنوات ديبلوماسية تفاديا لتعقيدات الإجراءات وبطئها للتعجيل بتطبيق الإجراءات وغالبا ما تكون الطلبات موجهة إلى وزارة العدل.

وبالرغم من أن التعاون القضائي في مجال مكافحة الجريمة الإلكترونية يشكل أحد أهم الآليات والسياسات لمكافحتها إلا أن الملاحظ أن أغلبية الاتفاقيات والمعاهدات كانت سطحية في تطرقها للجريمة الإلكترونية، ولأن الوضع الدولي العام

يوحي بعمق الأضرار والآثار السلبية للجريمة الإلكترونية الناجمة عن التطور السريع في هذا المجال فإن هذا الوضع ينذر بخطر كبير على المجموعة الدولية وعلى أمنها الإلكتروني لهذا باتت الحاجة ملحة وضرورية إلى عقد اجتماعات عاجلة وعقد اتفاقيات تواكب هذا التطور الهائل في المجال الإلكتروني والمعلوماتي، ويجب أن تتصف هذه الاتفاقيات بالصرامة، الفعالية، والالتزام بتطبيق فحواها بشكل صادق وحقيقي.[1]

الفرع الثاني: تطبيق سياسة تسليم المجرمين كآلية دولية لمكافحة الجريمة الإلكترونية

إن عملية تسليم المجرمين تعتبر شكلا من أشكال مكافحة الجريمة الإلكترونية على الصعيد العالمي والذي اتخذته أغلب الدول للحفاظ على أمنها الإلكتروني وجاءت كنتيجة حتمية للتطور السريع في مجال الاتصالات والمعلوماتية، وأصبح المجرم الإلكتروني أكثر ذكاء وسرعة في تنفيذ جريمته في عدة دول وفي وقت قصير، كأن يخطط لعملية إجرامية إلكترونية في دولة ما ويطبقها في أخرى لضرب استقرارها وإلحاق الضرر بها.

أولا: أشكال تسليم المجرمين الإلكترونيين

وفقا للممارسات الدولية في مجال مكافحة الجريمة الإلكترونية فقد وضعت ثلاث أنظمة لتسليم المجرمين الإلكترونين وهي:

[1] رامي متولي القاضي، الجريمة الإلكترونية في القانون الجنائي الدولي: تحديات وأبعاد، ط2، مصر، دار النهضة العربية، 2012، ص97.

1. التسليم القضائي:

والذي يميزه هو أن الجهة القضائية هي التي تتحمل مسؤولية إصدار قرار تسليم المجرمين إلى الدول التي طلبت ذلك وكذا الحفاظ على حقوق الأفراد في دفاعهم عن أنفسهم، ومن سلبيات هذا النوع البطء في إجراءات التسليم وهذا ما ينعكس سلبا على ما تستدعيه سرعة ملاحقة المجرمين لسهولة اندثار أدلة الإثبات عليها.

2. التسليم الإداري:

والجهة المختصة في تسليم المجرمين هي السلطة التنفيذية والتي تملك الصلاحية المطلقة لقرار التسليم من عدمه ويتميز بالسرعة وتجنب الإجراءات التي تعيق من إنهاء عملية التسليم وما يعاب عليها أنها مهدرة لحقوق الأفراد الدفاعية، وكذا خضوع قرار التسليم إلى اعتبارات سياسية، مع جهل الجهة المنفذة للتسليم بالخلفية القانونية.

3. التسليم المختلط:

وهو النوع الأكثر انتشارا، وهو مزيج بين مميزات النظامين السابقين حيث يسهل الإجراءات ويقوم على تسريعها ويضمن حق الدفاع للمتهمين.[1]

ثالثا: قانون الأونيسترال النموذجي:

جاء هذا القانون بعد اقتناع الدول المتضررة من الجرائم الإلكترونية وإيمانا منها بأن الحماية الدولية للأشخاص والمؤسسات العالمية لا تتأتى إلا بتضافر جهودها والعمل بطريقة شاملة وديناميكية لمكافحة ظاهرة الإجرام الالكتروني، وقد صيغ هذا القانون من قانون متعلق بالتجارة الإلكترونية والآخر بشأن التوقيعات الإلكترونية.

[1] محمد الشناوي، إستراتيجية مكافحة جرائم النصب المستحدثة: الإنترنت بطاقات الائتمان الدعاية التجارة الكاذبة، ط1، القاهرة، دار البيان للطبع والنشر، 2006، ص92.

1. القانون المتعلق بالتجارة الإلكترونية:

تنطبق نصوصه على أي نوع من المعلومات التي تكون على شكل رسالة بيانات مستخدمة في سياق نشاط تجاري، يتم تسليمها وتخزينها بوسائل إلكترونية، ويتم تبادلها ونقلها إلكترونيا من حاسب آلي إلى أخر باستعمال معيار متعارف ومتفق عليه.

2. القانون المتعلق بالتوقيعات الإلكترونية:

وجاء هذا القانون لتعويض التوقيعات التقليدية بالتوقيعات الإلكترونية لكسر قيود المسافات والأقاليم الدولية لأنه يتسم بالسرعة والسرية، وهو عبارة عن رمز سري أو شفرة سرية التي يتم الحصول عليها بعد عدة إجراءات واعتمد هذا القانون بتاريخ 05 جويلية 2001.[1]

[1] سامي علي عياد حامد، المرجع السابق، ص51.

خلاصة الفصل الأول

ومما سبق يمكن استخلاص أن الجريمة الإلكترونية أضحت اليوم من أكثر الجرائم انتشارا بالنظر للتطور الكبير الحاصل في تكنولوجيا المعلومات، ما يجعل أمر مكافحتها في غاية الأهمية، إلا أن التحديد الدقيق لمفهوم الجريمة الإلكترونية صعب نوعا ما عملية مجابهتها وكذا إيجاد الآليات والاستراتيجيات التقنية والقانونية للتعامل معها، ذلك أن مفهومها تواجد في ظل رؤى معرفية متباينة ومختلفة تبعا لاتجاهات معينة.

كما أثبت الواقع العملي عدم قدرة أي دولة على مكافحة الجريمة الإلكترونية لوحدها، ونظرا لصبغتها العالمية ولكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي والجنائي، وفي هذا الإطار لعبت اتفاقية بودابست دورا فعالا في مكافحة الجريمة الإلكترونية، كما ساهمت اتفاقية الاتحاد الإفريقي في وضع القاعدة الأولى للتصدي لهذه الجريمة إفريقيا، وقد حاولت الدول العربية من جهتها إيجاد حلول مشتركة لمقاومة الجريمة الإلكترونية.

الفصل الثاني

مكافحة الجريمة الإلكترونية على المستوى الوطني

الفصل الثاني: مكافحة الجريمة الإلكترونية على المستوى الوطني

سيتم التطرق في هذا الفصل إلى مجهودات الدولة الجزائرية للتصدي لهذا البعد الإجرامي الجديد والمتمثل في الجريمة الإلكترونية من خلال مرتكزين أساسيين وهما الجانب التشريعي الذي عرف بدوره تعديلات كثيرة على القوانين ذات العلاقة بالمجال الإلكتروني بالإضافة إلى سن حزمة جديدة من القوانين التي تتماشى والتطور الذي تشهده الجريمة الإلكترونية. والجانب الثاني المتمثل في الهياكل المؤسساتية من خلال استحداث وإنشاء مراكز ومصالح مختصة في محاربة الجريمة الإلكترونية والمواجهة الفعالة لها.

وقسم هذا الفصل إلى مبحثين على النحو التالي:

- **المبحث الأول: المكافحة الموضوعية للجريمة الإلكترونية**
- **المبحث الثاني: المكافحة الإجرائية للجريمة الإلكترونية في التشريع الجزائري**

المبحث الأول: المكافحة الموضوعية للجريمة الإلكترونية

أغفل المشرع الجزائري إلى وقت قريب تنظيم مجال الجريمة الإلكترونية قانونا، إلا أنه سارع إلى تدارك ذلك الفراغ القانوني من خلال سن قواعد قانونية لمواجهة هذه الجريمة، وذلك ما تجلى في القانون 04-15 ثم تلاه بالقانون 09-04 وغيره من القوانين التي سيتم تناولها في هذا المطلب وفق مطلبين يعالج المطلب الأول مكافحة الجريمة الإلكترونية بموجب القوانين العامة، بينما يخصص المطلب الثاني إلى مكافحة الجريمة الإلكترونية بموجب القوانين الخاصة.

المطلب الأول: مكافحة الجريمة الإلكترونية بموجب القوانين العامة

سيتم ضمن هذا المطلب تناول الآليات القانونية والتشريعية التي أوردها التشريع الجزائري في إطار مكافحة الجريمة الإلكترونية، وهذا ضمن فرعين.

الفرع الأول: مكافحة الجريمة الإلكترونية بموجب الدستور والقانون المدني

تدخل المشرع بآليات قانونية لمواجهة الجريمة الإلكترونية حيث عمد إلى الحماية بموجب الدستور والقانون المدني وقانون العقوبات على النحو التالي:

لقد كفل دستور الجزائر لسنة 2020 حماية حقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية العامة:

- **المادة 35:** *"الحريات الأساسية وحقوق الإنسان والمواطن مضمونة".*
- **المادة 47:**

- *"لكل شخص الحق في حماية حياته الخاصة وشرفه".*
- *"لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت".*
- *"لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية".*
- *"حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي". "يعاقب القانون على كل انتهاك لهذه الحقوق".*

- **المادة 6/54:** *"الحق في نشر الأخبار والأفكار والصور والآراء في إطار القانون، واحترام ثوابت الأمة وقيمها الدينية والأخلاقية والثقافية".*

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124 من التقنين المدني الجزائري *"كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض".*[1]

الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب قانون العقوبات

يعتبر قانون العقوبات وسيلة ردعية للكف عن ارتكاب الجرائم بصفة عامة، وبما أن الجرائم الإلكترونية تلحق أضرار بالغير فقد أقر المشرع عقوبات ردعية لتلك الجرائم وهي كالتالي:

[1] إسمهان بوضياف، (الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد03، المجلد03، جامعة محمد بوضياف، المسيلة، الجزائر، 2018، ص362.

أولا: المساس بأنظمة المعالجة الآلية للمعطيات

وهي من أبرز الجرائم التي عالجتها المحاكم الجزائرية، وهذا بموجب القانون رقم 04-15 المتعلق بقانون العقوبات[1] وذلك من خلال المواد 394 مكرر إلى 394 مكرر 7، فمن خلال استقراء هذه المواد حاول المشرع الجزائري حصر هذه الجرائم والعقوبات المقرر لها فيما يلي:

1. جريمة دخول معالجة آلية للمعطيات عن طريق الغش:

نصت عليها المادة 394 مكرر من قانون العقوبات[2]، حيث تعاقب بالحبس والغرامة عند الدخول أو البقاء بالغش في المنظومة المعلومة وفرق المشرع في هذه الحالة بين ما إذا كانت الجريمة بسيطة ومضاعفة العقوبة إذا ترتب عنها حذف أو تغيير المنظومة وبين ما إذا ترتب على ذلك تخريب نظام اشتغال المنظومة.

2. جريمة إزالة أو تعديل معطيات في نظام المعالجة الآلية بطرق تدليسية:

نصت عليها المادة 394 مكرر من قانون العقوبات[3]، حيث اعتبر المشرع الجزائري أن إزالة أو تعديل المعطيات التي يتضمنها النظام بطريق الغش عملان إجراميان ويقصد بإزالة المعطيات سواء جزئيا أو كليا إما محوها أو إتلافها أو تخريبها من أجل منع النظام من القيام بمهامه أو تعطيل النظام المعلوماتي، أما تعديل المعطيات ويقصد به إما إدخال معلومات وهمية أو تزويرها في النظام المعلوماتي.

---

[1] القانون 04-15، المؤرخ في 2004/11/10، المعدل والمتمم لأمر رقم 66-156، المتضمن قانون العقوبات، الجريدة الرسمية، الجزائر، 2004، العدد 71.

[2] المادة 394 مكرر من القانون رقم 04-15، المصدر نفسه.

[3] المادة 394 مكرر 1 من القانون رقم 04-15، المصدر نفسه.

3. جرائم نشر حيازة أو الاتجار بالمعطيات المخزنة أو المعالجة:

نصت عليها المادة 394 مكرر2 من قانون العقوبات[1]، حيث تعد هذه الجريمة من أكثر الجرائم وقوعا في العالم الافتراضي، ولقد اعتبر المشرع الجزائري عملية اصطناع برنامج مخصص لارتكاب فعل الغش المعلوماتي أو إعداد برنامج ناقص من الناحية الفنية وخاصة المبرمج من أجل خلق فجوات وثغرات فيه لممارسة فعل الغش أو تجميع أو التقاط البيانات بغرض استغلالها أو نشرها خاصة عن طريق الإنترنت أو الاتجار فيها من الجرائم المعاقب عليها، بحكم أن جريمة الإنشاء والنشر تتسم بخطورة على الحياة الخاصة.

4. جرائم المعالجة الآلية الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام:

طبقا للمادة 394 مكرر 3 من قانون العقوبات[2] حيث اعتبر المشرع الجرائم الإلكترونية التي تستهدف الدفاع الوطني أو أي مؤسسة رسمية بمثابة ظرف تشديد ويستخلص من نص المادة 394 مكرر 3 من قانون العقوبات أن العقوبة المشددة على جميع الجرائم المنصوص عليها في المادة 394 مكرر والمادة 394 مكرر 1 ومكرر 2 من قانون العقوبات وحرص المشرع الجزائري على ضمان حماية مطلقة لهيئات الدفاع الوطني ولمؤسسات الدولة الجزائرية وتوسع في هذه الحماية وذلك بإدراج جميع الجرائم المنصوص عليها في المادة 394 مكرر من قانون العقوبات كلها.[3]

---

[1] المادة 394 مكرر2 من القانون رقم 04-15، المصدر السابق.

[2] المادة 394 مكرر3 من القانون رقم 04-15، المصدر نفسه.

[3] فاروق خلف، (الآليات القانونية لمكافحة الجريمة المعلوماتية)، مجلة الحقوق والحريات، العدد02، المجلد03، جامعة محمد خيضر، بسكرة، الجزائر، 2015، ص16.

5. الجرائم المعلوماتية للشخص المعنوي:

نصت عليها المادة 394 مكرر 4 من قانون العقوبات[1] حيث أقر المشرع الجزائري المسؤولية الجزائية للأشخاص المعنوية وشدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية، حيث أن الغرامة المطبقة على الشخص المعنوي تتراوح بين واحد إلى خمس أضعاف الغرامة المقررة على الشخص الطبيعي.

6. جريمة تكوين جمعية أشرار معلوماتيين لغرض التحضير للجرائم الماسة بأنظمة المعالجة الآلية:

وذلك طبقا للمادة 394 مكرر 5 من قانون العقوبات[2] حيث يتضح من خلال نص المادة أن العقوبات تطال من يشارك أي مجموعة أو في اتفاق الغرض منه التحضير أو الإعداد لارتكاب الجرائم الإلكترونية مع توفر القصد الجنائي، كما يستخلص أن مجرد المشاركة أو الاتفاق المجسد بفعل مادي يوحي بالتحضير للجريمة، خاصة أن ذلك يمكن أن يتم عبر الشبكات المعلوماتية.

7. العقوبات التكميلية:

وذلك وفقا للمادة 394 مكرر 6 من قانون العقوبات[3] حيث نص المشرع في هذه المادة على العقوبات التكميلية للجرائم السالفة الذكر وتتمثل في مصادرة الأجهزة المستعملة والبرامج والوسائل المستعملة مع إلحاق ذلك بغلق المواقع وأماكن الاستغلال شريطة أن تكون بعلم صاحبها.

---

[1] المادة 394 مكرر4 من القانون رقم 04-15، المصدر السابق.

[2] المادة 394 مكرر5 من القانون رقم 04-15، المصدر نفسه.

[3] المادة 394 مكرر6 من القانون رقم 04-15، المصدر نفسه.

8. العقاب على الشروع في الجريمة المعلوماتية:

وطبقا لنص المادة 394 مكرر 7 من قانون العقوبات[1] أن فعل الشروع أو البدء في ارتكاب الجريمة يعاقب عليه بنفس العقوبة المقررة للجنحة ذاتها، ونظرا لكون جرائم الاعتداء على نظام المعالجة الآلية ذات وصف جنحوي أقر المشرع العقاب لها بمثل الجريمة نفسها.

9. استعمال تكنولوجيا الإعلام لارتكاب أفعال الإرهابية:

نصت المادة 87 مكرر 11[2] أن استعمال تكنولوجيا الإعلام والاتصال بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو تلقي التدريب عليها، تعتبر جناية يعاقب عليها بالسجن من 05 إلى 10 سنوات وبغرامة من 100.000 إلى 500.000 دج.

كما تضمنت المادة 394 مكرر 8[3] صور الأفعال التي يعاقب عليها القانون مقدم خدمات الإنترنت عند رفضه لإعذارات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أو صدور أوامر وأحكام قضائية.[4]

---

[1] المادة 394 مكرر 7 من القانون رقم 04-15، المصدر السابق.

[2] المادة 87 مكرر 11 من القانون 02-16، المتضمن تعديل قانون العقوبات.

[3] المادة 394 مكرر 8 من القانون رقم 04-15، المصدر السابق.

[4] مراد مشوش، (الجريمة المعلوماتية في ظل قانون العقوبات وقانون الحماية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال)، مجلة القانون، العدد01، المجلد09، الجزائر، ص118،119.

ثانيا: حماية حرمة الحياة الخاصة

من خلال التعديل الذي جاء في القانون رقم: 06-23 المتعلق بقانون العقوبات[1] فإن المادة 303 مكرر من قانون العقوبات[2] تعاقب بالحبس والغرامة كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت سواء بالتقاط أو تسجيل أو نقل صور أو مكالمات خاصة أو سرية دون إذن رضا صاحبها. أما المادة 303 مكرر 1 من قانون العقوبات[3]، تعاقب بالعقوبة ذاتها على من يحتفظ أو يضع في متناول الجمهور الصور أو الوثائق بأية وسيلة كانت.

ثالثا: حماية حرمة رموز الدولة

من خلال التعديل الذي جاء في القانون رقم 11-14 المؤرخ في 02 أوت 2011 المتعلق بقانون العقوبات[4]، حيث نصت المادة 144 مكرر منه[5]، على عقوبة الغرامة المالية فقط كل من أساء لرئيس الجمهورية بأية وسيلة كانت أو بوسيلة إلكترونية وفي حالة العود تضاعف الغرامة.

المطلب الثاني: مكافحة الجريمة الإلكترونية بموجب القوانين الخاصة

سنتطرق في هذا المطلب الآليات القانونية والتشريعية التي أوردها التشريع الجزائري في إطار مكافحة الجريمة الإلكترونية، وهذا ضمن فرعين.

---

[1] القانون 06-23، المؤرخ في 2006/12/20، المتضمن قانون العقوبات، الجريدة الرسمية، الجزائر، 2006، العدد48.

[2] المادة 303 مكرر من القانون 06-23، المصدر نفسه.

[3] المادة 303 مكرر1 من القانون 06-23، المصدر نفسه.

[4] القانون 11-14 المؤرخ في 2011/08/02، المتضمن قانون العقوبات، الجريدة الرسمية، الجزائر، 2011، العدد44.

[5] المادة 144 مكرر من القانون 11-14، المصدر نفسه.

الفرع الأول: مكافحة الجريمة الإلكترونية بموجب الآليات القانونية الخاصة

وتشمل هذه القوانين الخاصة الحماية في قانون التأمينات الاجتماعية، وكذلك الحماية من خلال نصوص الملكية الفكرية، وأيضا الحماية في نصوص التوقيع الإلكتروني بالإضافة إلى الحماية المتعلقة بالمواصلات السلكية واللاسلكية.

أولا: الحماية في قانون التأمينات الاجتماعية:

بمقتضى أحكام قانون التأمينات الاجتماعية رقم 08-01[1] المؤرخ في 23 جانفي 2008 شدد العقوبة فيما يتعلق بالمساس غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا، وعاقب المشرع الجزائري كل من يسلم أو يستلم بهدف الاستعمال غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا المفتاح الإلكتروني لهيكل العلاج أو المفتاح لمهني الصحة طبقا للمادة 93 مكرر 2[2] من نفس القانون، كما يشمل العقاب التعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية أو نسخ البرمجيات المتعلقة باستعمال البطاقة الإلكترونية، أو المحاولة لارتكاب الفعل طبقا لنص المادة 93 مكرر 3 منه[3]، كما أقر المشرع أيضا عقوبة للشخص المعنوي تتمثل في الغرامة ضعف المقررة للشخص الطبيعي طبقا لنص المادة 93 مكرر 5[4] من ذات القانون، ومصادرة الأجهزة والوسائل المستعملة وكذا غلق المحلات وأماكن الاستغلال التي تكون محل الجنح.

---

[1] القانون 08-01 المؤرخ في 2008/01/23، المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، الجزائر، 2008، العدد04.

[2] المادة 93 مكرر2 من القانون 08-01، المصدر نفسه.

[3] المادة 93 مكرر3 من القانون 08-01، المصدر نفسه.

[4] المادة 93 مكرر5 من القانون 08-01، المصدر نفسه.

ثانيا: الحماية من خلال قانون الملكية الأدبية والفنية:

حاول المشرع الجزائري مواجهة الجريمة الإلكترونية من خلال قانون الملكية الأدبية والفنية المتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم 03-05[1] المؤرخ في 23 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، حيث وسع قائمة المؤلفات المحمية، وذلك بإدماج برامج المعلوماتية، ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج المعلوماتية، كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المصنفات الرقمية التي تشملها الحماية.

ثالثا: الحماية في نصوص التوقيع الإلكتروني:

أصدر المشرع الجزائري قانون رقم 15-03[2] المتعلق بعصرنة العدالة، حيث تطرق في الفصل الثاني إلى المنظومة المعلوماتية المركزية لوزارة العدل والإشهاد على صحة الوثائق الإلكترونية وضمان حمايتها، أما الفصل الثالث تعرض إلى إرسال الوثائق والإجراءات القضائية بالطريق الإلكترونية، والفصل الخامس فتعرض إلى الأحكام الجزائية لحماية التوقيع والتصديق الإلكترونيين، حيث أن المادة 17[3] منه تعاقب على كل من يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر. أما المادة 18[4] تعاقب كل شخص حائز على شهادة إلكترونية يستعملها بعد انتهاء صلاحيتها أو إلغائها.

---

[1] الأمر 03-05، المؤرخ في 2003/07/19، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، الجزائر، 2003، العدد44.

[2] القانون 15-03، المؤرخ في 2015/02/01، المتعلق بعصرنة العدالة، الجريدة الرسمية، الجزائر، 2015، العدد02.

[3] المادة 17 من القانون 15-03، المصدر نفسه.

[4] المادة 18 من القانون 15-03، المصدر نفسه.

رابعا: الحماية المتعلقة بالمواصلات السلكية واللاسلكية:

تضمن الفصل الثاني من الباب الرابع من القانون رقم 2000-03[1] المتعلق بالبريد والمواصلات السلكية واللاسلكية الأحكام الجزائية المترتبة على مخالفة النظام القانوني، فالأشخاص المرخص لهم تقديم خدمة المواصلات السلكية واللاسلكية والعمال متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات السلكية واللاسلكية أو المساعدة على ذلك يعاقبون طبقا لنص المادة 137 من قانون العقوبات أو غيرهم ممن يرتكب هذه الأفعال يعاقب بالحبس والغرامة.

خامسا: الحماية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها رقم 09-04[2]:

وتكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، وقد جرم الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا.

وقد حدد القانون الحالات التي يسمح فيها اللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات عن احتمال اعتداء منظومة معلوماتية. وقد تعرض الفصل الأول من القانون إلى أهدافه وتحديد مفهوم التقنية، أما الفصل الثاني فقد تعرض إلى أحكام

---

[1] القانون 2000-03، المؤرخ في 2000/08/05، المتعلق بالقواعد العامة المتعلقة بالبريد السلكية واللاسلكية، الجريدة الرسمية، الجزائر، 2000، العدد06.

[2] القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المصدر السابق.

خاصة بمراقبة الاتصالات الإلكترونية، والفصل الثالث تعرض إلى القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والفصل الرابع تعرض إلى تحديد الالتزامات التي تقع على المتعاملين في الاتصالات الإلكترونية، ثم الفصل الخامس الذي نص على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحتها والفصل السادس فقد نص على التعاون والمساعدة القضائية الدولية بخصوص مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خاصة منها بالمساعدة وتبادل المعلومات.[1]

الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب النصوص التشريعية المستحدثة

بداية بالقانون رقم 15-04[2] المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، أنشأ في هذا المجال ما يسمى بمزود خدمة للمصادقة الإلكترونية، والذي يفي بعدد من الالتزامات القانونية لخلق بيئة إلكترونية آمنة للمعاملات عبر الإنترنت ولحماية المستهلك الإلكتروني من مخاطر السلع والخدمات التي يحصل عليها، ومنعه من الوقوع ضحية للعقود الإلكترونية، وعلى هذا الأساس جاء القانون رقم 18-05[3] المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الذي يتعامل مع التجارة الإلكترونية العامة، وخاصة حماية المستهلك الإلكتروني والذي يتم تنفيذه من خلال سلسلة من الالتزامات، يفرض المورد بعض العقوبات على سلوك المستهلك الإلكتروني ويشرف على العملية الإلكترونية بين أطراف العقد الإلكتروني.

[1] مراد مشوش، المرجع السابق، ص124.

[2] القانون 15-04، المؤرخ في 2015/02/01، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، الجزائر، 2015، العدد06.

[3] القانون 18-05، المتعلق بالتجارة الإلكترونية، المصدر السابق.

كما عزز المشرع الجزائري الوضع القانوني لوكالات مراقبة الاتصالات البريدية والإلكترونية وفقا للقانون رقم 18-04، كما جاء القانون 18-07[1] المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، نتيجة الاعتداء على البيانات الشخصية جراء التطور التكنولوجي وتأثيراتها على حياة الأفراد وجعلها عرضة لهجمات خارجية في الفضاء السيبراني، ويأتي المرسوم التنفيذي رقم 20-233 المؤرخ في 22 نوفمبر 2020 الذي يتعلق بنشاط الإعلام الإلكتروني وبحق الرد وحق التصحيح الإلكتروني، امتدادا للمادتين 66 و113 من القانون العضوي 12-05 المتعلق بالإعلام، إذ يهدف خاصة إلى ترقية الصحافة الإلكترونية المكتوبة ووضعها في مسار يتوافق وأهداف القانون.

[1] القانون 18-07، المؤرخ في 2018/06/10، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، الجزائر، 2018، العدد34.

المبحث الثاني: المكافحة الإجرائية للجريمة الإلكترونية في التشريع الجزائري

للتحقيق والإثبات في الجرائم الإلكترونية يجب الإلمام والمعرفة الجيدة بمجال التكنولوجيا والحاسب الآلي، وكيفية الاستفادة من هذه المعرفة واستخدامها بكفاءة في التحقيق والتحري واستخلاص الأدلة، ثم معرفة ما يمكن استخدامه كدليل في المحكمة، بالإضافة إلى ذلك لابد من توفر مجموعة من المتخصصين والمحققين لديهم معرفة وخبرة طويلة في مجال هذا النوع الجديد من الجرائم، وكيفية التعامل مع الدليل الإلكتروني، كما سنتعرف أيضا على مختلف الهياكل والهيئات التي أنشأتها الدولة الجزائرية للتصدي للجريمة الإلكترونية وذلك وفق مطلبين؛ يعالج المطلب الأول إجراءات التحقيق والإثبات في الجريمة الإلكترونية في التشريع الجزائري، بينما يخصص المطلب الثاني إلى الجهاز المؤسساتي العملياتي لمكافحة الجريمة الإلكترونية في الجزائر.

المطلب الأول: إجراءات التحقيق والإثبات في الجريمة الإلكترونية في التشريع الجزائري

التحقيق والإثبات أمران مرتبطان مع بعضهما، فالمشرع الجزائري لم يتبنى أفعال الاعتداء على الأنظمة المعلوماتية إلا من خلال تعديل قانون العقوبات 15-04 المؤرخ في 2004/11/10 فالإثبات في هذه الجرائم الخطيرة أمر صعب لذا اعتبر الدليل الرقمي وسيلة فعالة ومهمة للإثبات.

الفرع الأول: إجراءات التحقيق في الجريمة الإلكترونية في التشريع الجزائري

أولا: إجراءات التحري المألوفة والتقليدية

اعتمدت الجزائر في البداية على النصوص الجزائية القائمة بمختلف فروعها الموضوعية والإجرائية، وذلك من أجل معاقبة الجناة والتي تتمثل في: المعاينة التفتيش ضبط الأدلة والخبرة التقنية.

1. المعاينة في الجرائم الإلكترونية:

وهي رؤية لعين المكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة ومعاينة مسرح الجرائم المعلوماتية، ويجب التفرقة بين حالتي معاينة الجرائم الواقعة على مكونات الحاسوب كشاشة العرض الأقراص...الخ ومعاينة الجرائم الواقعة على المكونات غير المادية كفحص مسار الإنترنت، معاينة أنظمة الاتصال بشبكة الانترنت...الخ.

2. التفتيش في البيئة الإلكترونية:

يكون التفتيش بالنسبة للشخص المتهم أو مكان إقامته أو ضبط أشياء متعلقة بالجريمة في منزله، وهو من اختصاص النيابة العامة كأصل عام والضبطية كاستثناء،ويشمل التفتيش المكونات المادية للحاسب الآلي التي قد تكون في مسكن المتهم أو مكان عمله، ومن خلال المواد 44 إلى 47 من قانون الإجراءات الجزائية بين المشرع إجراءات التفتيش مثل الحصول على إذن مكتوب، وأن يكون التفتيش نهارا من الساعة الخامسة صباحا إلى الثامنة مساء، كما يشمل التفتيش في المجال الإلكتروني العناصر غير المادية للحاسب الآلي، حيث تنص المادة 47 الفقرة 04 من قانون الإجراءات الجزائية *"إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية*

للمعطيات يمكن لقاضي التحقيق أن يقوم بأي عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك".

3. ضبط الأدلة في الجرائم الإلكترونية:

يقصد بضبط الأدلة إجراءات جمعها، وهو الخلاصة النهائية لآلية التفتيش الذي يقصد به وضع اليد على الجريمة المتعلقة به كالأقراص الصلبة، الأشرطة، برامج، طباعة، بطاقات الائتمان...الخ.[1]

وقد تبنى المشرع الجزائري في القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05 إجراءات خاصة بضبط البيانات المعلوماتية تحت عنوان حجز المعطيات المعلوماتية، وخص لها المواد التالية (06، 07، 08).[2]

4. الخبرة التقنية في مجال الجرائم الإلكترونية:

نظرا لطبيعة هذه الجرائم يتم فيها الاستعانة بخبير، وهو شخص يتمتع بمؤهلات عملية وقدرة في التحكم في مجال الإعلام الآلي وهو ما نصت عليه المادة 05 الفقرة الأخيرة من قانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيا الإعلام والاتصال.

---

[1] عبد القادر فلاح، (التحقيق الجنائي في الجرائم الإلكترونية)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد02، المجلد04، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، 2019، ص1697.

[2] القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المصدر السابق.

وتخضع الخبرة لمجموعة من الضوابط لتكون لها نتائج أمام القضاء وهي:

- اختيار الخبير من جدول الخبراء مع أداء اليمين القانونية، والتزامه بأداء مهامه بنفسه؛
- اعتماد الخبير على وسائل علمية متطورة لإنجاز الخبرة.[1]

ثانيا: الإجراءات المستحدثة في الجرائم الماسة بأنظمة المعالجة الآلية للبيانات

نظرا لخطورة الجريمة الإلكترونية وصعوبة اكتشاف المجرم الإلكتروني وإيجاد الآلية المناسبة للتحقيق التقليدي، قام المشرع الجزائري باستحداث آليات تحقيق خاصة بموجب قانون الإجراءات الجزائية الجديد والقانون 09-04 سالف الذكر وهي: التسرب الإلكتروني، المراقبة الإلكترونية، اعتراض المراسلات، الحفظ والإفشاء، الحجز، الاستجواب، وسماع الشهود.

1. التسرب الإلكتروني أو الاختراق:

نظم المشرع الجزائري هذا الإجراء من خلال المواد من 65 مكرر 11 إلى غاية المادة 65 مكرر 18 من قانون الإجراءات الجزائية حيث تناول مفهومه وشروطه،[2] وتتمثل عملية التسرب في نطاق الجريمة الإلكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي باختراق مواقع معينة، أو الاشتراك في محادثات غرف الدردشة والظهور بمظهر كما لو كان فاعل مثلهم مستخدما أسماء أو صفات وهمية لإيقاع الجاني.

[1] عبد القادر فلاح، المرجع السابق، ص1698.

[2] المواد من 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية.

2. المراقبة الإلكترونية:

من خلال استقراء نصوص قانون 09-04 السالف ذكره نجد بأن المشرع الجزائري لم يعرّف صراحة المراقبة الإلكترونية وتركها للفقه الذي عرفها بأنها: "عبارة عن عمل أمني أساسي له نظام معلومات إلكتروني يقوم فيه المراقب بالمراقبة بواسطة الأجهزة الإلكترونية وعبر شبكة الإنترنت لتحديد غرض محدد وإفراغ النتيجة في ملف الكتروني. كما نص المشرع الجزائري على اشتراط اللجوء إلى تقنية المراقبة الإلكترونية، وهي أن تنفذ تحت سلطة القضاء وبإذن منه وهذا ما نصت عليه المادة 04 من قانون 09-04.[1]

3. اعتراض المراسلات:

لقد استحدث المشرع الجزائري فصلا كاملا تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" في قانون الإجراءات الجزائية رقم 06-02 وأكدها القانون 09-04، حيث أتاح لضابط الشرطة القضائية القيام ببعض الأعمال الخاصة بالبحث والتحري عن الجرائم الإلكترونية، كما أجاز لوكيل الجمهورية أن يأمر ضابط الشرطة القضائية باعتراض المراسلات التي تجري عن طريق الوسائل السلكية واللاسلكية ووضع الترتيبات التقنية لالتقاط الصور وتسجيل المكالمات السرية دون موافقة المعني، ويكون تنفيذ هذه العمليات تحت إشراف ورقابة وكيل الجمهورية، وفي مرحلة التحقيق تحت إشراف قاضي التحقيق.

[1] القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المصدر السابق.

4. الحفظ والإفشاء العاجلان للمعطيات الإلكترونية:

يعتبر كل من الحفظ والإفشاء إجرائيين جديدين وقد تضمنت المادة 10 من القانون 09-04 الخاص بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال عدد من الالتزامات على مزودي خدمة الانترنت بتقديم المساعدة في التحقيق مثل حفظ البيانات والمعلومات، وإفشاء أي معلومة مهمة لمساعدة رجال الضبطية القضائية، وفي حال عدم التزامهم تترتب عليهم المسؤولية الجزائية.[1]

5. الحجز:

ويقصد بالحجز وضع اليد على شيء مرتبط بجريمة تمت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، ويمكن حجز المكونات المادية للحاسب الآلي وملحقاته الأساسية والثانوية، كما يمكن عدم حجز كل المنظومة، حيث يتم نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز.[2]

ويتم الحجز حسب القانون 09-04 في حالتين نصت عليهما المادتين 06 و07 وهما حجز المعطيات المعلوماتية والحجز عن طريق منع الوصول إلى المعطيات. حيث أجاز المشرع في الحالة الأولى للسلطة التي تباشر التفتيش في منظومة معلوماتية حجز المعطيات المخزنة التي تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، وذلك من خلال نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية

[1] القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المصدر السابق.

[2] عبد القادر فلاح، المرجع السابق، ص1699.

تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.[1]

6. الاستجواب:

ويعرف بأنه: "مساءلة المتهم ومناقشته عن وقائع القضية المنسوبة إليه ارتكابها ومجابهته بالأدلة وسماع ما لديه من دفوع للتهمة المنسوبة إليه". والهدف من الاستجواب هو كشف الحقيقة واستظهارها بالطرق القانونية واستجواب المتهم في الجرائم المعلوماتية تحكمه ذات القواعد العامة لاستجواب متهم في أي جريمة تقليدية، إلا أنه لابد أن تكون السلطة المختصة التي تتولى الاستجواب مؤهلة للتحقيق في الجرائم المعلوماتية حتى يمكن الاستيعاب والتعامل مع مفردات الجريمة المعلوماتية، وقد أحاط المشرع الاستجواب بعدة ضمانات لابد من الالتزام بها لضمان حقوق المتهم.[2]

7. سماع الشهود:

سماع الشهود كسائر إجراءات التحقيق في الطريقة التقليدية، فالقاضي له أن يسمع الشهود أو يستغني عنهم، فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه، والأمر متروك للسلطة التقديرية للقاضي والشاهد في الجرائم المعلوماتية يطلق عليه اسم الشاهد المعلوماتي تميزا له عن الشاهد التقليدي، والمقصود بالشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسوب، والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعاجلة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة

---

[1] القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المصدر السابق.

[2] عبد الأمير العكيلي وسليم حربة، أصول المحاكمات، ط2، القاهرة، دار الكتب للطباعة والنشر، 2008، ص44.

الجريمة، وتضم طائفة الشهود: مشغلو الحاسوب، خبراء البرمجة، محللو البيانات مهندسو الصيانة، ومديرو النظم.[1]

الفرع الثاني: إجراءات الإثبات في الجريمة الإلكترونية في التشريع الجزائري

أولا: القيمة القانونية للدليل الإلكتروني

تظهر قيمة الدليل الإلكتروني من خلال إبراز مميزاته التي تميزه عن غيره من الأدلة:

1. تعريف الدليل الإلكتروني:

تعددت تعاريف الدليل الإلكتروني بين من اعتمد في تعريفه على الجانب التقني ومن اعتمد على الجانب القانوني. فعرف الدليل الإلكتروني بأنه: "كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما".[2]

ويقصد به أيضا "جميع البيانات الرقمية التي يمكن أن تثبت بأن هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني أو علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، خرائط الصوت أو الصورة".[3]

وبالرجوع للمشرع الجزائري نجد أنه لم يعرف الدليل الإلكتروني سواء في القانون 09-04 أو حتى في المرسوم 15-261 المتعلق بتنظيم الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال.

---

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص192.

[2] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، ط1، مصر، دار الجامعة الجديدة، 2010، ص53.

[3] عبد القادر فلاح، المرجع السابق، ص1700.

2. مميزات الدليل الإلكتروني:

يتصف الدليل الإلكتروني بعدة خصائص تميزه عن الدليل العادي وهي:

- الدليل الإلكتروني دليل علمي يتشكل من معطيات إلكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات؛
- إمكانية نسخ الدليل الإلكتروني، بحيث يمكن نسخ نسخة مطابقة للأصل وهذه الميزة لا تتوفر في الأدلة التقليدية؛
- الدليل الإلكتروني متنوع ومتطور ويمكن أن يكون وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة أو معدة بنظام التسجيل السمعي، أو أن تكون مخزنة في نظام البريد الإلكتروني؛
- صعوبة التخلص من الدليل الإلكتروني وهي أهم الخصائص التي يتسم بها، حيث يمكن استرجاعه بعد محوه وإصلاحه، وذلك باستخدام أدوات وبرمجيات ذات طبيعة رقمية متطورة.[1]

3. خصائص الدليل الإلكتروني:

تتميز بيئة الدليل الإلكتروني بالرقمنة نتيجة المجال الافتراضي الذي ينشأ فيه ومن ثمة فإن مسرح الجريمة هو إلكتروني بطبيعته وهذا ما يجعل من الدليل الإلكتروني يتميز بالخصائص التالية:

- **دليل ذو طابع علمي:** الدليل الإلكتروني هو عبارة عن معلومة ذات قيمة في الإثبات الجنائي وتكون محملة أو مخزونة أو منقولة في صورة رقمية، وهذه المعلومة هي التي يمكن أن تقود إلى اكتشاف الجريمة مبناها طبيعة البيئة التي

[1] فتحي أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، ط1، مصر، دار الفكر والقانون للنشر والتوزيع، 2010، ص67.

أخرجت لنا هذه المعلومة، وبالتالي لا يمكن الحصول عليها أو الإطلاع على فحواها إلا باستخدام الأساليب العلمية المتخصصة؛

- **دليل ذو طابع تقني:** بفضل الطبيعة التقنية للدليل الإلكتروني فإنه اكتسب مميزات من حيث قابليته للنسخ أي يمكن استخراج نسخ من الأدلة الإلكترونية مطابقة للأصل ولها نفس القيمة العلمية وهذه الخاصية لا تتوفر في الدليل المادي العادي مما يشكل ضمانة شديدة الفعالية ويمكن الحفاظ عليها ضد التلف أو التغيير أو الحذف؛
- **دليل سهل الإخفاء:** إن التخلص من الدليل الإلكتروني قد يقابله مسألة أخرى ذات علاقة بمسألة التطور المستمر في تكنولوجيا المعلومات، وهي أن الدليل الإلكتروني نتيجة لمرونته فإنه يسهل فقدانه بسبب بإتلافه أو إضاعته أو إلغاءه؛
- **دليل ديناميكي:** كما يتميز الدليل الإلكتروني أنه دليل ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات اتصال متعدية الزمان والمكان.[1]

4. أشكال الدليل الإلكتروني:

يتمتع الدليل الإلكتروني بأشكال مختلفة وهي:

- **الصور الرقمية:** هي عبارة عن تجسيد للحقائق حول الجريمة وفي العادة تقدم الصورة في شكل ورقي أو مرئي على شاشة الكمبيوتر.
- **التسجيلات الصوتية:** يمكن تعريفها على أنها عبارة عن ترجمة للتغييرات المؤقتة لموجات الصوت الخاصة بالكلام أو الموسيقى إلى نوع آخر من الموجات أو التغيرات الدائمة، ويكون التسجيل عادة بواسطة آلة تترجم موجات

[1] عمر يونس، الدليل الرقمي، ط1، مصر، مطبعة جامعة القاهرة، 2008، ص46.

الصوت إلى اهتزازات خاصة، وتكون التسجيلات هي التي يتم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الالكتروني والبيانات المسجلة بأجهزة الحاسب الآلي. وتتخذ أدوات التسجيل الصوتي أنواع عديدة منها أجهزة الاتصال السلكي الخارجي أو اللاسلكي والميكروفونات الصغيرة التي لا يتعدى حجمها عود ثقاب، وميكروفونات الليزر وكذلك الميكروفونات المسمارية.

- **النصوص المكتوبة:** وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الإلكتروني والبيانات المسجلة بأجهزة الحاسب الآلي.[1]

ثانيا: دور الدليل الإلكتروني في مجال الإثبات في الجزائر

يعتبر الدليل الإلكتروني أهم دليل في إثبات وضبط جرائم الكمبيوتر والإنترنت، لما له من دور مهم وحجية في الكشف عنها.

1. حجية الدليل الإلكتروني:

يقصد بحجية الدليل الإلكتروني قوته الاستدلالية في إبراز الحقيقة وصدق نسب الفعل الإجرامي إلى شخص معين أو كذبه، وتتوقف القيمة القانونية التي يتمتع بها الدليل الإلكتروني على مسألتين مهمتين هما: مشروعية هذا الدليل والمصداقية التي يتمتع بها.[2]

[1] صالح عبد الزهرة الحسون، أحكام التفتيش وآثاره في القانون العراقي، ط1، بغداد، منشورات جامعة بغداد، 2009، ص125.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص55.

أ- مشروعية الدليل الإلكتروني:

يتسع ويضيق قبول الدليل الإلكتروني تبعا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة، وفي هذا الصدد نجد المشرع الجزائري وكغيره من المشرعين أفرد نصوص تحفز القاضي على قبول أو عدم قبول أي دليل بما في ذلك الدليل التقني. كما أن حرية الإثبات في المسائل الجزائية من المبادئ المستقرة في نظرية الإثبات وبذلك أقر المشرع الجزائري مبدأ حرية الإثبات الجزائي في المادة 212 من قانون الإجراءات الجزائية، حيث نصت على أنه:"*يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكما تبعا لاقتناعه الشخصي*".

ومن بين مبررات الأخذ بمبدأ حرية الإثبات ظهور الأدلة العلمية الحديثة التي كشف عنها العلم الحديث في إتيان الجريمة ونسبها إلى المهتم كبصمة الصوت والبصمة الوراثية.[1]

ويتجلى الدور الإيجابي للقاضي الجزائري في الجرائم الإلكترونية في عنصرين هامين هما:

- توفر الدليل من خلال البحث عن الدليل باستعمال السلطات المخولة له قانونا، حيث يستطيع أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إليه من خلال الإفصاح عن كلمات المرور والشفرات الخاصة بتشغيل البرنامج؛

[1] صالح عبد الزهرة الحسون، المرجع السابق، ص138.

- سلطة الأمر بتفتيش نظم الحاسوب بجميع مكوناته بحثا عن الدليل الإلكتروني.[1]

ب- مصداقية الدليل الإلكتروني:

زاد ظهور الدليل الإلكتروني من دور الإثبات العلمي الذي كان دور الخبراء فعال في ذلك وهذا بالنظر إلى الجرائم الإلكترونية، وللخبرة التقنية أهمية في استخلاص الدليل الإلكتروني التي لها دور في البحث عن مصداقيته في مجال المعالجة الآلية للمعلومات.[2]

2. سلطة القاضي الجزائي في تقدير الدليل الإلكتروني:

إن الغاية الأساسية من الإثبات الجنائي هو معرفة الحقيقة الواقعية المرتبطة بما حدث بالعالم الخارجي من وقائع إجرامية ومدى ثبوتها، وباعتبار أن للقاضي الجزائي له سلطة تقديرية في تقدير الأدلة الجنائية بغية الوصول إلى الحقيقة الواقعية، ومن جانب آخر أيضا فإن مبدأ الاقتناع القضائي من أبرز المبادئ الأساسية التي يقوم عليها الإثبات الجنائي ويعني هذا الأخير: "أن يتوفر أمام القاضي الجزائي مجموعة من الأدلة المطروحة أمامه تكفي لتسبيب اعتقاده بثبوت الوقائع أو نفيها كما أوردها في حكمه ونسبها إلى المتهم".

وتعتبر عملية تقدير الأدلة هي جوهر مرحلة الحكم، حيث لا يمكن الوصول إلى الحكم النهائي إذا لم يمارس القاضي سلطته التقديرية على جميع الأدلة سواء كانت

[1] عائشة بن قارة مصطفى، المرجع السابق، ص59.

[2] صالح عبد الزهرة الحسون، المرجع السابق، ص139.

أدلة مادية أو معنوية، والدليل الإلكتروني شأنه شأن الأدلة الأخرى يخضع لنفس القواعد المقررة لباقي الأدلة.[1]

ولقد أشار المشرع الجزائري إلى هذه المسألة بنصه على مبدأ الاقتناع الجزائي في المادة 307 من قانون الإجراءات الجزائية التي تنص على: *"إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص في ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المستندة إلى المتهم وأوجه الدفاع".* وفي إطار إعمال مبدأ الإقناع القضائي يترتب عن ذلك حرية القاضي في قبول وتقدير الدليل الإلكتروني[2].

3. حرية القاضي الجزائي في قبول وتقدير الدليل الإلكتروني:

يعد قبول الدليل الإلكتروني بصفة خاصة الخطوة الإجرائية الأولى التي يمارسها القاضي الجزائي، حيث أن مسألة تقييم الدليل في إثبات الواقعة الإجرائية مسألة موضوعية محضة تخضع لسلطة القاضي التقديرية، ونجد سلطة القاضي في قبول وتقدير الأدلة سندها في إعمال مبدأ الاقتناع القضائي الذي يعتبر النتيجة الضرورية له، ونتيجة لذلك فإن القاضي يمكنه أن يتصرف في وسائل الإثبات ويقم بتوجيه أبحاثه طبقا للضرورة التي يراها، وعلى هذا فمبدأ الاقتناع القضائي الجزائي سلطة ليست فقد في الوسيلة وإنما في قوتها الثبوتية، ويظهر تبرير هذا المذهب فيما يلي:

---

[1] يسرى لعريبي، (التحقيق والإثبات في الجريمة المعلوماتية)، مجلة الفكر السياسي والقانوني، العدد01، المجلد07، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2022، ص181.

[2] المادة 307 من قانون الإجراءات الجزائية، المصدر السابق.

- ما دام أن الهدف الأساسي من أحكام القانون الجزائي في الدعوى هو كشف حقيقة الدعوى، ولبلوغ هذا الهدف السامي يجب إعطاء القاضي حرية واسعة لاختيار وتقدير وسائل الإثبات؛
- ذاتية القانون الجنائي في إعطاء دور إيجابي سواء للقاضي أو لأطراف الدعوى في تقديم الأدلة للمحكمة والتي يرونها مفيدة في دعم ادعاءاتهم على عكس الوضع في الدعاوي المدنية يكون دور القاضي سلبي لحد كبير.

4. اقتناع القاضي الجزائي درجة اليقين:

يستوجب على القاضي الجنائي تحري الحقيقة ويمكن الوصول إلى اليقين عن طريق نوعين من المعرفة العقلية التي يقوم بها العقل عن طريق التحليل والاستنتاج في الأدلة الإلكترونية المتحصلة وغيرها من الأشكال الإلكترونية التي تتوافر عن طريق الوصول المباشر، أم كانت مجرد عرض لهذه المخرجات المعالجة.

ويترتب على ذلك أن كافة مخرجات الوسائل الإلكترونية من مخرجات ورقية أو إلكترونية أو أقراص مغناطيسية أو مصغرات فيلمية تخضع لتقدير القاضي الجزائي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك ومستعملا في ذلك المعرفة الحسية التي يدركها بالحواس من خلال معاينته لهذه المخرجات وفحصها وعن طريق المعرفة العقلية وما يقوم به من استقراء واستنتاج ليصل إلى الحقيقة.

5. أن تتم مناقشة الدليل الإلكتروني في جلسة علنية:

وذلك حتى يتم تكوين قناعة القاضي بناء على أدلة طرحت أمامه في الجلسة، ويترتب عن ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تمنح للخصوم حق الإطلاع على هذه الأدلة وهذا ما جاء في نص المادة 212 فقرة 2 من قانون الإجراءات الجزائية على: *"ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له*

في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه، وهذا يعني أنه على القاضي الجزائي الاجتهاد في الحكم في الجرائم المعلوماتية وعدم الاعتماد على رأي الغير إلا إذا كان هذا الغير من الخبراء وذلك على سبيل الاستدلال".[1]

المطلب الثاني: الجهاز المؤسساتي العملياتي لمكافحة الجريمة الإلكترونية في الجزائر

وتتمثل في المراكز والوحدات والمصالح التي استحدثتها الدولة الجزائرية في إطار إستراتيجيتها لمكافحة الجريمة الإلكترونية والتصدي لها، وذلك وفق الفرعين التاليين:

الفرع الأول: الهياكل الخاصة بالأمن الوطني والدرك الوطني

الهياكل المتخصصة في مجال مكافحة الجريمة الإلكترونية هي وحدات تسند إليها مهام الوقاية ومكافحة الجرائم الإلكترونية.

أولا: هياكل الدرك الوطني

1. مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:

أنشأ هذا المركز سنة 2008، ويعتبر الجهاز الوحيد المختص بهذا المجال في الجزائر، ويهدف أساسا إلى تأمين منظومة المعلومات لخدمة الأمن العمومي واعتبر بمثابة مركز توثيق ويتواجد مقره ببئر مراد رايس، هذا المركز يعمل على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أفراد أو جماعات، وكل هذا من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها، واستطاعت قيادة الدرك الوطني من خلال

[1] يسرى لعريبي، المرجع السابق، ص182،183.

التكوين المستمر والمتميز لأفرادها والملتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال قانون، وهذا من أجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها، وفي ذات السياق استطاع المركز معالجة العديد من الجرائم الإلكترونية والرقمية وأيضا تلك المتعلقة بوسائل التواصل الاجتماعي وكذلك الجرائم المتعلقة باختراق مواقع رسمية لمؤسسات عامة وخاصة استهدف مجرموها أنظمة المعالجة الآلية للمعطيات.[1]

2. المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاؤه بموجب المرسوم الرئاسي رقم 04-183 المؤرخ بتاريخ 26 جوان 2004، وهو يشكل أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، ولعل الخدمة الأساسية التي يقدمها هذا المعهد هي خدمة العدالة ودعم وحدات التحري في إطار الشرطة القضائية، ولهذا فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام مكلف بالمهام الآتية:

- القيام بالخبرات العلمية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح؛
- مساعدة المحققين للسير الحسن للمعاينات خاصة عن طريق الوضع تحت تصرف الأفراد المؤهلين أثناء الحاجة؛
- المبادرة وإجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة؛

[1] سمير بارة، (الأمن السيبراني في الجزائر: السياسات والمؤسسات)، المجلة الجزائرية للأمن الإنساني، العدد04، المجلد01، جامعة باتنة1، باتنة، الجزائر، 2017، ص271.

- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.

ثانيا: هياكل الأمن الوطني

1. المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

استجابت مصالح الأمن الجزائرية لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية من خلال إنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية.

وقد كانت المصلحة عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني DGSN، والتي أنشأت سنة 2011، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بجرائم تكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني،وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.[1]

2. نيابة مديرية الشرطة العلمية والتقنية التابعة للمديرية العامة للأمن الوطني:

أسندت المديرية العامة للأمن الوطني مهمة مكافحة الجريمة الإلكترونية لنيابة مديرية الشرطة العلمية والتقنية، وتضع هذه الأخيرة لخدمة هذا الهدف مصالح علمية مختصة بذلك، تتولى أعمال البحث والتحري بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذه الوحدات هي: المخبر المركزي للشرطة العلمية والكائن مقره

[1] إلهام غازي، (الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري)، مجلة الجيش، العدد630، 2016، ص44.

بالجزائر العاصمة، المخبر الجهوي للشرطة العلمية –قسنطينة– والمخبر الجهوي للشرطة العلمية –وهران–.

ويتولى كل مخبر سواء المركزي أو الجهوي لولاية وهران أو قسنطينة مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها، ولأجل ذلك يضم كل مخبر دائرتين هما:

- **الدائرة العلمية:** وتتولى أعمال البحث والتحقيق وتحليل الأدلة المتصلة بالمجال البيولوجي والطب الشرعي والكيمياء والمخدرات وكذلك تلك المتعلقة بمجال التسميم والحريق والمتفجرات كل منها على مستوى مخبر خاص.
- **الدائرة التقنية:** وتتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة والقذائف بمختلف أنواعها، إضافة إلى الجرائم المعلوماتية، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى.[1]

الفرع الثاني: المراكز والهيئات الوطنية

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

أنشئت هذه الهيئة بموجب المرسوم الرئاسي رقم 15-261[2] وهي سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة يترأسها وزير العدل وتضم

[1] سمير بارة، المرجع السابق، ص273.

[2] المرسوم الرئاسي رقم 15-261، المؤرخ في 2015/10/08، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وتضم الهيئة كذلك قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.

وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.[1]

ثانيا: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تم إنشاء هذا القطب بموجب الأمر رقم 21-11 المؤرخ في 25 أوت 2021، المعدل والمتمم لقانون الإجراءات الجزائية والقاضي باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ويتواجد على مستوى مقر محكمة مجلس قضاء الجزائر.

وقد تم تحديد مفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وفقا لهذا القانون على أنها: "أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات

[1] إلهام غازي، المرجع السابق، ص45.

الإعلام والاتصال". وقد أوكلت لهذا القطب الجزائي الوطني مهمتين أساسيتين تتمثلان في:

- المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها؛
- الحكم في الجرائم المنصوص عليها في الباب السادس من الأمر رقم 21-11، إذا كانت تشكل جنحا.[1]

وقد شهدت إحصائيات الجرائم الإلكترونية ارتفاعا قياسيا، حيث ارتفعت من 12 ألف جريمة سجلت في سنة 2022 إلى 14 ألف جريمة خلال سنة 2023، حيث سجلت مصالح الأمن الوطني المختصة في الجرائم الإلكترونية وفرقها العملياتية التابعة لمصالح الشرطة القضائية، خلال الفترة الممتدة من 1 جانفي إلى غاية 31 أكتوبر 2023؛ 3325 قضية راح ضحيتها 2315 شخصا وتورط فيها 4138 جاني.

كما سجلت مصالح الدرك الوطني وفرقها العملياتية المختصة في الإجرام الإلكتروني 4500 قضية، وبالمقابل عالجت مصالح الأمن العسكري ما يقارب 4000 قضية مصنفة في خانة السرية.

وحسب تفاصيل مصالح الأمن المشتركة فإن الرابط الوحيد بين هذه الجرائم هو سوء استخدام التكنولوجيا، حيث شملت الجرائم المالية والاقتصادية، الابتزاز، السب والشتم والقذف، والتهديد والتشهير الإلكتروني، اختراق مواقع مؤسسات وشركات

[1] الأمر رقم 21-11، المؤرخ في 2021/08/25، المعدل والمتمم لقانون الإجراءات الجزائية والقاضي باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الجريدة الرسمية، الجزائر، 2021، العدد65.

عمومية وخاصة، المساس بالحريات الشخصية والحياة الخاصة عبر شبكات التواصل الاجتماعي، كما أن 65 بالمئة من الجرائم المرتكبة تمت عن طريق الفايسبوك.[1]

الفرع الثالث: الصعوبات التي تعترض مكافحة الجريمة الإلكترونية

رغم الجهود التي تبذلها الدول والهيئات الوطنية في مكافحة الجرائم الإلكترونية، إلا أن هناك بعض الصعوبات التي تعوق عملية القضاء على هذه الجرائم والحد منها ومن أبرزها:

- عدم وجود نموذج موحد متفق عليه فيما يتعلق بالنشاط الإجرامي، بسبب الأنظمة القانونية في دول العالم التي لم تتفق على صورة محددة للجريمة الإلكترونية؛
- عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال الإجرام الإلكتروني، وحتى في حال وجودها فإن هذه المعاهدات تبقى قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب الآلي والإنترنت؛
- عدم وجود تنسيق وانسجام الرؤى فيما يتعلق بالإجراءات الجنائية الخاصة بالجريمة الالكترونية كأشكال التحقيق والحصول على الأدلة والبراهين؛
- قصور التشريع الخاص بالجريمة الإلكترونية وعدم مسايرته للتطور السريع لتكنولوجيا الاتصال والمعلومات؛

[1] نوارة باشوش، "14 ألف جريمة سيبرانية في 2023 والتسوق الإلكتروني في الصدارة"، *الشروق أونلاين*، تاريخ النشر 2023/02/18، تاريخ زيارة الموقع 2024/06/06 على الساعة 19:35، متاح على الموقع: www.echoroukonline.com

- جهل الجناة وحتى الضحايا بالقانون، بمعنى أن الجاني لا يدرك أن الفعل الذي ارتكبه يندرج ضمن الجريمة الإلكترونية، والضحية لا يعتقد أنه يوجد قانون يجرم تلك الأفعال فيعدلون عن التبليغ عنها.[1]

[1] جيلالي ماينو، (الجريمة السيبرانية في صورها المستحدثة)، مجلة القانون والتنمية، العدد01، المجلد04، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار، الجزائر، 2022، ص63.

خلاصة الفصل الثاني

في ختام هذا الفصل يمكن القول أنه مع تنامي ظاهرة الجريمة الإلكترونية التي لم يسلم منها الأفراد والدول، وتأثيرها على كافة جوانب الحياة سياسيا واقتصاديا واجتماعيا، سارعت الدولة الجزائرية على غرار باقي الدول إلى مراجعة سياستها الأمنية والقانونية عبر انتهاج إستراتيجية مزدوجة من أجل الوقوف في وجه هذه الظاهرة.

فمن الجانب القانوني نجد أن المشرع الجزائري قام باتباع خطوتين أساسيتين أولهما تعديل النصوص والقوانين السارية ذات العلاقة، وثانيا قام باستحداث وتبني آليات وتشريعات جديدة من أجل مواكبة التطورات التي فرضها المجال الرقمي سعيا إلى مكافحة هذا الشكل الجديد من الجرائم والتصدي له بمختلف الأساليب.

أما من الجانب المؤسساتي فتظهر جهود الدولة الجزائرية في مجال مكافحة الجريمة الإلكترونية من خلال إنشاء مراكز خاصة بالأمن والدرك الوطنيين على حد سواء وكذا مختلف الهيئات الوطنية التي تقوم بأدوار جد مهمة في المتابعة والتحقيق والحكم في هذه الجرائم.

خاتمة

خاتمة

تعد الجريمة الإلكترونية كما ذكر آنفا من أخطر جرائم العصر الحديث نظرا لسهولة انتشارها وسرعة تنفيذها وتميز مرتكبيها بالخطورة والمهارة الفائقة، فضلا عن سهولة طمس معالم الجريمة وصعوبة إثبات دليلها الذي يتسم بالصبغة الرقمية، أضف إلى ذلك عدم الاتفاق على تعريف شامل وجامع وموحد لها بسبب اختلاف الرؤى والزوايا التي ينظر إليها، ما أدى بطبيعة الحال إلى صعوبة الاتفاق على وضع قانون موحد لمعاقبتها الأمر الذي وضعها تحت المجهر ومنحها خصوصية أكثر من الجرائم التقليدية الأخرى.

وقد بذلت في سبيلها جهود ومساعي دولية وإقليمية حثيثة لما لها من تأثير خطير على المصالح الاقتصادية والسياسية والاجتماعية لأي دولة، وأصبح العالم في أمس الحاجة إلى تعاون دولي مكثف بصددها، الأمر الذي توج بعقد اتفاقيات مهمة شكلت القاعدة الأولى التي مهدت الطريق نحو نصوص قانونية مميزة بعيدة عن دائرة التجريم التقليدي وهو ما يبرره خصوصية الجريمة الإلكترونية عن الجريمة التقليدية.

والمشرع الجزائري من جهته قد خطى خطوات بارزة في مجال مكافحة الجريمة الإلكترونية من خلال استحداث العديد من الآليات العقابية في صورة قانون العقوبات، وإنشاء هيئات ومؤسسات أمنية تمثل القاعدة والأرضية الصلبة التي يستند عليها مجال مكافحة الجريمة الإلكترونية في الجزائر.

وتطور الجريمة الإلكترونية يواكب التطور التكنولوجي والعلمي الحاصل في هذا العصر وعليه فمحاربتها تستدعي اليقظة الدائمة وتحيين القوانين لتتناسب مع التغيرات الحاصلة في مجال الجريمة الإلكترونية، إلا أنه بالرغم من كل هذه القواعد والقوانين المفروضة على هذا النوع من الجرائم لازالت تعاني من بعض القصور ذلك النقص

الذي فرضه التجديد الدائم للجريمة الإلكترونية وابتكار أنماط وصور مستحدثة لها. وبالمقابل عجز النظام القانوني على التطور بنفس الوتيرة التي تشهدها الجريمة الإلكترونية والإبقاء على نفس القوانين التي لا تغطي كافة جوانبها بصورتها المحدثة ما من شأنه إحداث ثغرات قانونية قد يستغلها المجرمون للإفلات من العقاب.

النتائج:

- نظرا لحداثة الجريمة الإلكترونية لا يوجد لحد الآن إجماع فقهي وتعريف قانوني موحد لها؛
- المجرم الإلكتروني يختلف عن المجرم التقليدي فهو يتمتع بعلم وكفاءة ويتميز بقدرات عقلية وذهنية تمكنه من الإفلات من العقاب؛
- الجريمة الإلكترونية ذات طابع دولي عابرة للحدود الوطنية، فهي جريمة عالمية الوجود؛
- قصور القوانين التقليدية أمام هذه الجريمة المستحدثة؛
- رغم اجتهاد المشرع الجزائري إلا أنه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة؛
- وجود عدة مساهمات دولية وإقليمية للحد من الجريمة الإلكترونية، من أبرزها اتفاقية بودابست والمجلس الأوروبي بالإضافة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وجهود الاتحاد الإفريقي.

التوصيات:

- ✓ ضرورة توحيد الجهود الوطنية والدولية من أجل إيجاد تعريف موحد للجريمة الإلكترونية وبالتالي توحيد النصوص القانونية لمكافحتها؛
- ✓ على الجزائر التفكير في التوجه إلى التعاون التشريعي والقضائي من خلال الانضمام إلى اتفاقيات دولية من أجل محاربة الجريمة الإلكترونية والعمل على

الاستفادة من خبرة وتجربة الدول الرائدة في هذا المجال، بهدف تحسين آليات مكافحة الجريمة الإلكترونية بشتى أنواعها؛

- ✓ وجوب وضع آليات ردعية وتعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلاءم مع التطور الحاصل في مجال الجريمة الإلكترونية؛
- ✓ تشجيع الجامعات والمراكز البحثية على تنظيم الندوات والمؤتمرات التي تعالج الجريمة الإلكترونية والتعريف بالقوانين التي سنت لأجلها، بالإضافة إلى كيفية مكافحتها والحد من آثارها؛
- ✓ ضرورة خلق ثقافة اجتماعية جديدة تندد بالجرائم الإلكترونية، مع نشر الوعي الرقمي بين مستخدمي شبكة الإنترنت، وحثهم على الاستخدام الأمثل لهذه التقنيات.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

قائمة المصادر

القوانين والمراسيم

1. المرسوم الرئاسي رقم 15-261، المؤرخ في 2015/10/08، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
2. الأمر رقم 21-11، المؤرخ في 2021/08/25، المعدل والمتمم لقانون الإجراءات الجزائية والقاضي باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الجريدة الرسمية، الجزائر، 2021، العدد65.
3. الأمر 03-05، المؤرخ في 2003/07/19، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، الجزائر، 2003، العدد44.
4. القانون 02-16، المتضمن تعديل قانون العقوبات.
5. القانون 18-07، المؤرخ في 2018/06/10، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، الجزائر، 2018، العدد34.
6. القانون 15-04، المؤرخ في 2015/02/01، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، الجزائر، 2015، العدد6.
7. القانون 2000-03، المؤرخ في 2000/08/05، المتعلق بالقواعد العامة المتعلقة بالبريد السلكية واللاسلكية، الجريدة الرسمية، الجزائر، 2000، العدد.
8. القانون 15-03، المؤرخ في 2015/02/01، المتعلق بعصرنة العدالة، الجريدة الرسمية، الجزائر، 2015، العدد02.
9. القانون 08-01 المؤرخ في 2008/01/23، المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، الجزائر، 2008، العدد04.

10. القانون 11-14 المؤرخ في 2011/08/02، المتضمن قانون العقوبات، الجريدة الرسمية، الجزائر، 2011، العدد44.
11. القانون 06-23، المؤرخ في 2006/12/20، المتضمن قانون العقوبات، الجريدة الرسمية، الجزائر، 2006، العدد48.
12. القانون 18-05، المؤرخ في 2018/05/10، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، الجزائر، 2018، العدد28.
13. القانون 09-04، المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، الجزائر، 2009، العدد47.
14. القانون 04-15، المؤرخ في 2004/11/10، المعدل والمتمم لأمر 66-155، المؤرخ في 1966/06/08، المتضمن قانون العقوبات، الجريدة الرسمية، الجزائر، 2004، العدد47.

قائمة المراجع:

أولا: الكتب

15. أمير فرح يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر، ط1، مصر، مكتبة الوفاء القانونية، 2011.
16. جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية: دراسة مقارنة، دط، د ب ن، دار الثقافة للتوزيع والنشر، 2010.
17. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، ط1، بيروت، منشورات الحلبي الحقوقية، 2014.
18. رامي متولي القاضي، الجريمة الإلكترونية في القانون الجنائي الدولي: تحديات وأبعاد، ط2، مصر، دار النهضة العربية، 2012.
19. زيدان زليخة، الجريمة المعلوماتية في التشريع الجزائري والدولي، ط1، الجزائر، دار الهدى، 2011.

20. زين العابدين الكردي، جرائم الإرهاب المعلوماتية، ط1، لبنان، منشورات الحلبي الحقوقية، 2018.
21. سالمي علي عياد حامد، الجريمة الإلكترونية، ط1، الإسكندرية، دار الفكر الجامعي، 2007.
22. سعيدي سليمة وحجازي بلال، جرائم المعلومات والشبكات في العصر الرقمي، ط1، الإسكندرية، دار الفكر الجامعي، 2017.
23. الشناوي محمد، إستراتيجية مكافحة جرائم النصب المستحدثة: الإنترنت بطاقات الائتمان الدعاية التجارة الكاذبة، ط1، القاهرة، دار البيان للطبع والنشر، 2006.
24. صالح عبد الزهرة الحسون، أحكام التفتيش وآثاره في القانون العراقي، ط1، بغداد، منشورات جامعة بغداد، 2009.
25. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ط1، مصر، دار الكتب القديمة، 2007.
26. العكيلي عبد الأمير وحربة سليم، أصول المحاكمات، ط2، القاهرة، دار الكتب للطباعة والنشر، 2008.
27. علي حسن الطوالبة، الجرائم الإلكترونية، ط1، البحرين، دار الحقوق التطبيقية، 2008.
28. فتحي أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، ط1، مصر، دار الفكر والقانون للنشر والتوزيع، 2010.
29. بن قارة مصطفى عائشة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، ط1، مصر، دار الجامعة الجديدة، 2010.
30. محمد عبد الرحمان عنانزة، القصد الجرمي في الجرائم الإلكترونية، دط، عمان، دار الأيام للنشر، 2017.
31. محمد عبد الله قاسم، الحماية الجنائية للمعلومات الإلكترونية، ط1، مصر، دار الكتب القانونية، 2010.

32. محمود أحمد عبابنة ومحمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دط، عمان، دار الثقافة للنشر والتوزيع، 2009.
33. ميرفت محمد حبابية، مكافحة الجريمة الإلكترونية، ط1، الأردن، دار اليازوري العلمية، 2020.
34. نائلة عادل محمد فريد، جرائم الحاسب الاقتصادي، ط1، القاهرة، دار النهضة العربية، 2013.
35. نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، مصر، دار الثقافة للنشر والتوزيع، 2008.
36. يوسف محمود حسنين، الجريمة المعلوماتية وسبل مكافحتها محليا ودوليا، ط1، الإسكندرية، دار الفكر الجامعي، 2013.
37. يونس عمر، الدليل الرقمي، ط1، مصر، مطبعة جامعة القاهرة، 2008.

ثانيا: القواميس والمعاجم

38. ابن منظور، لسان العرب، ط1، القاهرة، دار المعارف، د س ن.

ثالثا: الرسائل الجامعية

39. خضر شاهين وسعادة رضوان، الجريمة الإلكترونية وإجراءات مواجهتها، مذكرة مقدمة لنيل شهادة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2021/2020.
40. رمضاني حميدة ورزيق ليلة، الجريمة الإلكترونية واقع وتحدي، مذكرة مقدمة لنيل شهادة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018/2017.

رابعا: المقالات

41. بارة سمير، (الأمن السيبراني في الجزائر: السياسات والمؤسسات)، المجلة الجزائرية للأمن الإنساني، العدد04، المجلد01، جامعة باتنة1، باتنة، الجزائر، 2017.

42. بوجادي صليحة، (الإطار المفاهيمي للجريمة المعلوماتية)، مجلة الدراسات القانونية المقارنة، مخبر القانون الخاص، العدد1، المجلد7، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2021.

43. خلف فاروق، (الآليات القانونية لمكافحة الجريمة المعلوماتية)، مجلة الحقوق والحريات، العدد02، المجلد03، جامعة محمد خيضر، بسكرة، الجزائر، 2015.

44. رابحي حسن، (الجريمة الإلكترونية: النقطة المظلمة بالنسبة للتكنولوجيا المعوماتية)، المجلة الجزائرية للعلوم القانونية الاقتصادية السياسية، العدد01، جامعة الجزائر1، كلية الحقوق، الجزائر، 2011.

45. صهيب ياسر محمد شاهين وبشرى محمد محسن أبو ترابي، (الجريمة الإلكترونية وبعدها القانوني)، مجلة نومبروس الأكاديمية، العدد1، المجلد2، جامعة عباس لغرور، خنشلة، الجزائر، 2021.

46. بوضياف إسمهان، (الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد03، المجلد03، جامعة محمد بوضياف، المسيلة، الجزائر، 2018.

47. غازي إلهام، (الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري)، مجلة الجيش، العدد630، 2016، ص44.

48. فلاح عبد القادر، (التحقيق الجنائي في الجرائم الإلكترونية)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد02، المجلد04، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، 2019.

49. لعريبي يسرى، (التحقيق والإثبات في الجريمة المعلوماتية)، مجلة الفكر السياسي والقانوني، العدد01، المجلد07، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2022.
50. ماينو جيلالي، (الجريمة السيبرانية في صورها المستحدثة)، مجلة القانون والتنمية، العدد01، المجلد04، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار، الجزائر، 2022.
51. مشوش مراد، (الجريمة المعلوماتية في ظل قانون العقوبات وقانون الحماية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال)، مجلة القانون، العدد01، المجلد09، الجزائر.

خامسا: المواقع الإلكترونية

52. باشوش نوارة، "14 ألف جريمة سيبرانية في 2023 والتسوق الإلكتروني في الصدارة"، *الشروق أونلاين*، تاريخ النشر 2023/02/18، تاريخ زيارة الموقع 2024/06/06 على الساعة 19:35، متاح على الموقع: www.echoroukonline.com

فهرس المحتويات

ملخص

إن الجريمة الإلكترونية من أخطر الجرائم المستحدثة لما تتميز به من خصائص تتحدى القوانين وتستوجب جمع وسائل قانونية وقضائية رادعة لمكافحتها، باعتبارها تشكل تهديدا مباشرا للأمن الدولي والمجتمعي كما تمس بالحريات الشخصية للأفراد خاصة مع استمرار تطورها بشكل لافت وما يصاحب ذلك التطور من آثار خطيرة تمس مختلف الكيانات. ونظرا لذلك عملت مختلف الدول على استحداث حزمة من التشريعات والآليات القانونية والمؤسساتية لكشف الجناة وملاحقتهم وتقديمهم للعدالة، والجزائر كباقي الدول رصدت جملة من التدابير والآليات التشريعية للوقوف في وجه هذا النمط الجديد من الإجرام إلا أن الصعوبة تكمن في عدم وجود مفهوم واضح للجريمة الإلكترونية وإطار شرعي وقانوني موحد يمكن من خلاله الحد منها والعمل على التخفيف من حدتها، الأمر الذي يستلزم تكاتف الجهود المحلية والدولية ومضاعفة اليقظة وتحيين القوانين للقضاء على الجريمة الإلكترونية.

الكلمات المفتاحية: الجريمة الإلكترونية، المجرم الإلكتروني، الآليات الدولية، المشرع الجزائري، مكافحة الجريمة الإلكترونية.

Résumé:

Les criminalités électroniques est parmi les crimes les plus dangereux de nos jours en raison de leurs caractéristiques qui défient les lois et nécessitent la mise en place de moyens juridiques dissuasifs pour les combattre. Ils constituent une menace directe pour la sécurité internationale et sociale, tout en portant atteinte aux libertés individuelles, notamment avec leur évolution continue et les effets graves qui l'accompagnent, touchant diverses entités.

Par conséquent, différents pays ont travaillé à l'adoption d'un ensemble de législations, de mécanismes juridiques et institutionnels pour détecter les criminels, les poursuivre et les traduire en justice. L'Algérie, comme d'autres pays, a identifié un ensemble de mesures et de mécanismes législatifs pour faire face à ce nouveau modèle de criminalité. Cependant, la difficulté réside dans l'absence d'un concept clair de criminalité électronique et d'un cadre juridique unifié permettant de le limiter et

d'atténuer sa gravité, ce qui nécessite une coopération des efforts locaux et internationaux, une vigilance accrue et la mise à jour des lois pour lutter contre la criminalités électronique

Mots clés: la criminalités électronique, le criminel électronique, mécanismes internationaux, législateur Algérien, lutte contre la criminalités électronique.