دور التشريع الجزائري في مكافحة الجريمة الإلكترونية

The role of Algerian legislation in combating electronic crime

بوزيفي شريفة[1]

[1] جامعة الجيلالي بونعامة خميس مليانة، c.bouzifi@univ-dbkm.dz

مخبر نظام الحالة المدنية

تاريخ الإرسال: 10 / 04 /2026 تاريخ القبول: 18 / 10 /2026 تاريخ النشر: 17 / 11 /2026

ملخص:

تعتبر الجريمة الإلكترونية جريمة خطيرة بكل أنواعها نظرا لما تحققه من أذى بالأشخاص سواء جسديا او معنويا، كذلك بأمن الدولة و اقتصادها، ونظرا لتنوعها بين تزوير و سرقة المعلومات و اختراق للنظم الخ..

وعليه هي من أكثر الجرائم انتشارا و نظرا لخطورتها ونظرا انها ظاهرة إجرامية مستحدثة عملت مختلف التشريعات على التصدي لها من خلال وضع نصوص قانونية وهذا ما فعله المشرع الجزائري بسن قوانين من اجل مكافحة هاته الجرائم الا انه لا تعد كافية.

كلمات مفتاحية: الجريمة الإلكترونية، المجرم المعلوماتي، الجريمة المعلوماتية

Abstract:

Cybercrimes are considered serious crimes of all kinds due to the harm they cause to people, whether physical or moral, as well as to the security and economy of the state, and due to their diversity between counterfeiting, stealing information, hacking systems, and others. Therefore, it is one of the most widespread crimes, and due to its

seriousness, it is a new criminal phenomenon. Various legislations have worked to confront them by developing legal texts, and this is what the Algerian legislator did, as he enacted laws in order to combat these crimes, but they are not considered sufficient.

Keywords: *Cybercrime; Information criminal; Information crime.*

1- المؤلف المرسل: بوزيفي شريفة، **الإيميل:** c.bouzifi@univ-dbkm.dz

مقدمة :

تعتبر الجريمة الالكترونية جريمة مستحدثة و بالتالي تختلف عن الجريمة التقليدية من حيث تعريفها و أنواعها و شخص مرتكبها و سماته ، فالجريمة الالكترونية ظهرت بوجود التحول الرقمي و الحواسيب و وسائل الاتصال

و بالتالي عند اختراع الانترنت لم يكن في الحسبان انه سوف يتم استعمالها في الجانب السلبي و مع مرور الوقت اصبح الأشخاص يستغلون هاته الوسائل و استعمال تقنيات عدة للقيام بجرائمهم الاكترونية و عليه ظهر هذا النوع الجديد من الجرائم.

ومنه حاول المشرع الجزائري التصدي لها من خلال وضع منظومة قانونية لمجابهة هذا النوع من الجرائم نظرا لما يلحقه من اضرار على الأشخاص و المؤسسات.

وتكمن أهمية هاته الدراسة في ابراز اهم العناصر التي توضح لها الجريمة الالكترونية و المجرم المعلوماتي و كذا كيف حاول المشرع مكافحة هذا النوع من الجرائم.

ومنه تثور الإشكالية التالية: الى أي مدى حقق المشرع الجزائري الحد من الجريمة الالكترونية و التصدي لها؟

وللإجابة على هاته الإشكالية سوف نتبع المنهج الوصفي التحليلي وعليه قسمنا الخطة الى مبحثين المبحث الأول المعنون الاطار المفاهيمي للجريمة الإلكترونية و المبحث الثاني المعنون الاطار القانوني لمكافحة الجريمة الالكترونية في التشريع الجزائري

1. المبحث الأول: الإطار المفاهيمي للجريمة الالكترونية

مع التطور التكنولوجي وانتشار استخدام الانترنت أصبحت هناك جرائم الى جانب الجرائم التقليدية و هي الجرائم الالكترونية والتي تعد احد التحديات التي تواجه الدولة وبالتالي نظرا لخطورتها أصبحت تشكل خطرا على الافراد و المؤسسات ، و هاته الهجمات الالكترونية المتطورة تستدعي ضرورة استخدام تقنيات لمجابهتها و الحد من آثارها السلبية[1].

و عليه سنتناول في هذا المبحث مطلبين المطلب الأول المعنون بمفهوم الجريمة الالكترونية و المطلب الثاني المعنون بالمجرم المعلوماتي

1.1 المطلب الأول: مفهوم الجريمة الالكترونية

لقد أدى التطور التكنولوجي و انتشار وسائل الانترنت ظهور اشكال جديدة من الجرائم ، مما انعكس هذا التطور الى ظهور سلوكيات تهدد بالأفراد جسديا و معنويا و كذا تهدد امن و استقرار الدولة، بحيث تم اصطلاحها بالجرائم المعلوماتية او الجرائم السيبرانية او الجرائم الالكترونية او جرائم الانترنت، رغم ما احدثه التطور التكنولوجي و انتشار وسائل الاتصال من نتائج إيجابية في تسهيل المعاملات الالكترونية في الدولة و كذا المعاملات الالكترونية بين الافراد وما حققه من رقي الا انه كان له اثر سلبي على مصالح الأشخاص و

الدولة وهذا ما دفع بالمشرع في بعض الدول الى تجريمها و تقرير عقوبات عنها ، وكل هذا بسبب التطور التكنولوجي و انتشار الانترنت [2]، و عليه سنتناول في هذا المطلب ثلاث فروع ، الفرع الأول المعنون بتعريف الجريمة الالكترونية ، الفرع الثاني المعنون بخصائص الجريمة الالكترونية، الفرع الثالث المعنون بأنواع الجريمة الالكترونية.

1.1.1 الفرع الأول: تعريف الجريمة الالكترونية

نظرا لانتشار الجريمة الالكترونية بصفة سريعة و على نطاق واسع فالمجتمع الجزائري اصبح متضرر كغيره من المجتمعات المتضررة وعليه لابد من وضع سياسة جنائية لمكافحة و تصدي لهذا النوع من الجرائم من خلال تقنيات متقدمة والتي من خلالها تحقق حماية قانونية جزائية .

ونظرا لحداثة هاته الجرائم و التشريعات المنظمة لها الا انه لازالت تعرف قصور فأصبح من الضرور توفير الأسس القانونية و الأطر الإجرائية الواضحة للحد من هاته الجرائم[3].

و يشير مصطلح الجريمة المعلوماتية او الجريمة الالكترونية الى أي جريمة من الجرائم المرتكبة عن طريق الحاسوب، أي يكون هو الوسيلة المرتكبة لتحقيق هذا النوع من الجرائم الالكترونية ، ويمكن تعريف الجريمة الالكترونية على انها

يشير مصطلح الجريمة الالكترونية الى أي جريمة تتضمن الحاسوب ، او الشبكات الحاسوبية قد يستخدم الحاسوب في ارتكاب الجريمة وقد يكون هو الهدف ويمكن تعريف الجريمة الالكترونية على انها أي مخالفة ترتكب ضد افراد او جماعات بدافع جرمي ونية الإساءة لسمعة الضحية او لجسدها سواءا

كان ذلك بطريقة مباشرة او غير مباشرة ، وان يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الانترنت (غرف الدردشة او البريد الإلكتروني او المجموعات.. الخ)

وقد عرفت الجريمة الالكترونية بأنها:" الجريمة تتم باستخدام جهاز الكمبيوتر من خلال الاتصال بالأنترنت ويكون هدفها اختراق الشبكات او تخريبها او التعريف او التزوير او السرقة او الاختلاس او قرصنة و سرقة حقوق الملكية الفكرية[4].

حددت المادة 02 من القانون 09-04 تعريف الجريمة الإلكترونية بقولها:

يقصد في مفهوم هذا القانون بما يأتي:

- الجرائم المتصلة بتكنولوجيا الاعلام والاتصال: وهي الجرائم مرتكبة عن طريق نظام اتصالات الالكترونية او المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات.
- منظومة معلوماتية: وهي مجموعة من الأنظمة المنفصلة او المتصلة ببعضها تقوم بتنفيذ برنامج معين من خلال معالجة آلية للمعطيات .
- معطيات معلوماتية: عبارة عن معلومات و معطيات تعرض في شكل جاهز للمعالجة داخل منظومة معلوماتية بما فيها برامج التي تجعل المنظومة تؤدي وظيفتها.
- بالإضافة الى مقدمو الخدمات و المعطيات المتعلقة بحركة السير و الاتصالات الالكترونية[5].

2.1.1 الفرع الثاني: خصائص الجريمة الالكترونية

1.2.1.1 أولا: ترتكب بواسطة شبكة الانترنت

أي ان الجريمة الالكترونية يتم ارتكابها بواسطة الانترنت ، حيث ان الانترنت تربط بين كل الأهداف التي تسعى الجريمة الالكترونية تحقيقها كالاشخاص و الشركات و المؤسسات الخ.

2.2.1.1 ثانيا: الجريمة الإلكترونية جريمة مستحدثة

اصبح التقدم العلمي و التكنولوجي سبب في ضعف الدولة على تطبيق قوانينها مما اصبح يهدد امنها، فهي جريمة مستحدثة أي ظهرت وتطورت مع تطور التكنولوجي و كذلك اصبح السبيل الى ارتكابها ميسر خاصة مع انفتاح الشعوب على العالم الخارجي و اصبح من سهل نقل المعلومة صوت وصورة و انتقلت الحياة من عالم الواقعي الى عالم افتراضي و الجريمة من جرائم تقليدية الى الكترونية وهذا من خلال الاتصال بالانترنت و ارتكاب مختلف الجرائم كالاحتيال و القرصنة و النظم البنكية ..الخ[6].

3.2.1.1 ثالثا: صعوبة اكتشاف الجريمة الالكترونية

عدم القدرة على اكتشاف ارتكاب هاته الجريمة من قبل الضحية لأنه تتم مثلا عن طريق ارسال فيروسات او سرقة البيانات و المعلومات و السرقة و حتى وبجود الضحية الا ان لا يستطيع كشفها .

وبالتالي تحتاج طرق فنية عالية للكشف عنها لانه لا تترك اثر بعد ارتكابها [7].

4.2.1.1 رابعا: جريمة عابرة للحدود

بعد ان كان الهدف من الربط بين الشبكات الالكترونية للاستعمال الإيجابي ونقل المعلومات و الاتصالات أصبحت تستعمل كوسيلة لارتكاب الجرائم الالكترونية ، فهاته الجرائم لا تعرف الحدود أي لا ترتكب على المستوى الوطني فقط وانما يمكن ان يخرج نطاقها المكاني الى خارج حدود الدولة وذلك من خلال الربط الالكتروني بين الحواسيب.

فقد ترتكب جريمة بواسطة الحاسب الآلي عن طريق الشبكات الدولية و تتحقق نتيجتها الاجرامية في دولة أخرى من العالم مرورا بمزود خدمة او قنوات اتصال في إقليم دولة ثالثة، و يترتب على البعد الوطني للجريمة المعلوماتية عدة إشكاليات مشابهة لتلك المرتبطة بالجرائم ذات الطابع غير الوطنية أهمها ، اصدار إجراءات التحقيق و ضبط المتهمين و ملاحقتهم بمبدأ السيادة الوطنية للدولة و خاصة في الجرائم التي تتطلب اتخاذ اجراء من إجراءات التحقيق في إقليم دولة اجنبية ، وكذلك إشكالية الاختصاص القضائي و إشكالية تحديد القانون واجب التطبيق ، كما انه من جهة أخرى تشكل الإجراءات الرسمية المعقدة والتي تستغرق وقتا وليس بالقصير في حالات المساعدة القانونية او القضائية بين الدول ، والتي تتعارض مع طبيعة الجرائم المعلوماتية التي تتطلب سرعة في التحقيقات[8].

5.2.1.1 خامسا: سهولة ارتكاب الجريمة بعيدا عن الرقابة الأمنية

حيث ترتكب خفية حتى ولو كانت بوجود الجاني حيث انه لا يكتشفها الا بعد مرور مدة طويلة وذلك عند ارسال الفيروسات او سرقة البيانات او التجسس الخ، أي ان الضحية لا يلاحظها و يعلم بارتكابها وكشفها الا بعد مرور فترة وجيزة وذلك بسبب تمتع الجاني بمهارات و قدرات فنية تمكنه من ارتكاب هاته الجرائم

6.2.1.1 سادسا: التنفيذ عن بعد

أي ان هذا النوع من الجرائم لا يشترط وجود الجاني في مكان الجريمة وانما يمكنه من القيام بها عن بعد أي في دولة أخرى سواء ارتكبت بالحاسب الالي او عن طريق الهاتف المحمول مما يصعب اكتشافها و التحقيق فيها[9].

7.2.1.1 سابعا: جرائم هادئة:

هي جرائم ترتكب بهدوء فهي تعتمد على التفكير و الدراسة الذهنية ولا تعتمد على الجهد العضلي فهي عكس الجريمة التقليدية التي تحتاج الى القوة في ارتكابها كالقتل الخ.
وذلك ان هاته الجرائم تعتمد على البيانات و المعلومات المخزنة في ذاكرة الحواسيب[10].

8.2.1.1 ثامنا: إخفاء الجريمة

ان هاته الجرائم يسهل اخفائها الا انها تظهر و تلاحظ آثارها، وما يسهل ارتكابها خاصة اذا ارتكبت من قبل الأشخاص العاملين في تلك المؤسسة نظرا للثقة الممنوحة لهم.
و يصعب التحقيق فيها من طرف المحقق العادي خاصة بالنسبة للجرائم القائمة على البريد الالكتروني حيث يصعب تحديد المرسل و بالتالي تحتاج طرق وتقنيات لاثباتها فهي تحتاج رجل الشرطة الالكترونية.

9.2.1.1 تاسعا: الجاذبية:

تعتبر اكثر جذبا لاستثمار الأموال و سرقة المعلومات و بيعها[11].

3.1.1 الفرع الثالث: أنواع الجرائم الالكترونية

1.3.1.1 أولا: القرصنة الالكترونية

يهدد هذا النوع من الجرائم سمعة المؤسسة كما يمكن ان يكون من اجل الاستفادة المالية و تتم هاته القرصنة بقيام الجاني بسرقة المعلومات او ارقام السرية او مستندات الضحية مما يسبب اضرار للمؤسسات و الأشخاص

اما من خلال تعطيل الحسابات وفقدان بيانات الخ[12].

2.3.1.1 ثانيا: جرائم شبكة المعلومات

يتطلب للقيام بهذا النوع من الجرائم ان يكون هناك اتصالا بالانترنت و كذلك وجود حاسب آلي ، وبالتالي يقوم هذا الفعل على وثيقة موجودة بالشبكة مثل انتهاك الادبي و العلمي .

وعليه عند استخدامه الحاسب الآلي و اتصاله بالانترنت من اجل التوصل الى قواعد البيانات من اجل الاطلاع عليها اوتغييرها[13].

3.3.1.1 ثالثا: جرائم الابتزاز الالكتروني

بما انه الجريمة الالكترونية تعتبر جريمة مرتكبة عبر وسائل الاتصال و الحواسيب و الهاتف فان جريمة الابتزاز هي جريمة تهديد الضحية معنويا و ماديا .

و يكون هذا الابتزاز عبر وسائل الأنظمة المعلوماتية مما ينعكس على نفسية الضحية سلبا نظرا لعجزه في المواجهة.

كما يمكن ان يتم الابتزار الالكتروني عن طريق قرصنة الحسابات و تهديد الضحية .

4.3.1.1 رابعا: الاحتيال الالكتروني

شهد هذا النوع من الجرائم ازدياد ملحوظ في السنوات الأخيرة ، ويكون الهدف منه هو الوصول الى البيانات الشخصية من اجل استعمالها في أمور غير قانونية، ويتم الاحتيال الالكتروني بواسطة الايميلات او مواقع الانترنت، بحيث يتم وهم الضحية و خداعه سواء كان شخص او مؤسسة وذلك من اجل الحصول على البيانات المهمة مثل تفاصيل الحسابات البنكية[14].

5.3.1.1 خامسا: جرائم الفيروسات و البرمجيات الخبيثة

ترتكب هاته الجرائم عن طريق ارسال برمجيات خبيثة و فيروسات عبر الروابط الانترنت او تنزيل ملفات تحتوي على فيروسات و كذا عند تحويلها من ملف الى ملف، و بالتالي يتم ارسال هاته الفيروسات عبر روابط اما عبر الايميل او رسائل نصية او روابط في الصفحات، وعند ولوج الضحية الى الرابط يتعطل الجهاز اما كليا بوصول الفيروس الى البيانات المخزنة او جزئيا، وعن وصول الفيروسات تتعطل الأجهزة و يمكن حتى فقد كل البيانات .

كذلك هناك مجموعة أخرى من الجرائم وهي الجرائم التي يقوم بها الجاني من تجميع معلومات شخصية للضحية عن طريق وسائل الاتصال ومواقع التواصل الاجتماعي و المجموعات و غرف الدردشة وهذا من اجل تعريض الضحية الى مضايقات و كذا مطاردات الكترونية ، كذلك جرائم التشهير لتشويه السمعة و جرائم السب و الشتم[15].

6.3.1.1 سادسا: الإرهاب الالكتروني

الهدف من هاته الجريمة هو ضرب استقرار الدول و نشر الفوضى و يتم ذلك من خلال التعدي على الشبكات الحكومية او العسكرية، و بالتالي يتم هذا عبر الانترنت عن طريق الهجوم باستخدام الفيروسات من اجل ضرب استقرار الدول من خلال تعطيل الخدمات ذات أهمية بالغة مثل الخدمات الضحية ، وبما انه هي جريمة الكترونية و مرتكبة عن بعد فيصعب تحديد مرتكبها[16].

2.1 المطلب الثاني: المجرم المعلوماتي

أي جريمة من الجرائم الالكترونية تستعدي وجود طرفين مثل الجرائم العادية التي نجد بها المجني و المجني عليه ، كذلك الجرائم المعلوماتية تتطلب وجود

طرفين وهما الفاعل الذي يرتكب الجريمة المعلوماتية او الالكترونية و المجني عليه أي الضحية الذي كان محل هاته الجريمة الالكترونية ووقعت عليه افعال المجني عليه سواء جريمة كانت بواسطة الحاسب الآلي او الهاتف او شبكات الانترنت.

وعليه الجريمة الالكترونية تناولتها التشريعات مثل الجرائم العادية و بالتالي لابد من وجود طرفين فيها ، فقط الاختلاف بينهما يكمن في الشخصية مرتكبة الفعل باعتباره جاني معلوماتي غير مسلح بوسائل مادية كالسلاح الخ وانما مسلح بوسائل ذهنية تقنية معلوماتية مكنته من ارتكاب مثل هاته الجرائم و يحقق من خلالها أهدافه سواء تعطيل الحسابات او سرقة الأموال الى غير ذلك[17].

وعليه سنتناول في هذا المطلب فرعين الفرع الأول المعنون بتعريف المجرم المعلوماتي و الفرع الثاني المعنون بسمات المجرم المعلوماتي

1.2.1 الفرع الأول: تعريف المجرم المعلوماتي

يعتبر الجاني في الجريمة الالكترونية الذي يسمى في الاصطلاح الالكتروني " الهاكر" اما في الاصطلاح القانوني" المجرم المعلوماتي"

بحيث يعد الشخص الذي يقوم بقرصنة الحسابات و اختراق الحاسب الآلي من اجل الاطلاع على البيانات و المعلومات وهو يختلف على مصطلح " كراكر" الذي يسمون به الأشخاص الذين لديهم القدرة على الاختراق.

كما يوجد تسمية أخرى وهم " المحطمون" الذين يقومون بالهجوم على الأنظمة المعلوماتية بواسطة أدوات برمجية ينشؤونها[18].

فالمجرم المعلوماتي يرتكب الجريمة عن بعد فهو لا يحتاج ارتكاب الجريمة في مكان المجني عليه وانما فقط باستعمال شبكات الانترنت او الحواسيب او الهاتف و بذلك يحقق الهدف الذي يسعى اليه.

2.2.1 الفرع الثاني: سمات المجرم المعلوماتي

1.2.2.1 أولا: الذكاء

الذكاء هو قدرة الشخص على الاستيعاب و التفكير و الفهم

فالمجرم المعلوماتي لا يحتاج قدرات بدنية للقيام بفعله الاجرامي و انما الى قدرات عقلية ذهنية بحيث يكون على دراية بالامور التقنية ، و بالتالي عند ارتكابه الجريمة الالكترونية لا يتطلب عنف بدني بل فقط قدرة و مكنة عقلية تمكنه من ارتكاب الفعل .

فمثلا اتلاف بيانات المعلوماتية لا تتطلب جهد بدني او عنف و انما مجرد الوصول الى الشبكة و الى الحاسب ليقوم بهاته العملية وبالتالي يحدث عن طريق نشر فيروسات معلوماتية لتحقق هذا الغرض.

وبالتالي حتى يقوم المجرم المعلوماتي بجريمته هنا يتطلب منه ان يقوم بعدة محاولات و كذا استعمال تقنيات عدة و برامج و كذا يحتاج وقت طويل لتحقيق النتيجة كما يقوم بتغيير الشبكات او البرامج حتى يصل الى البرنامج و التقنية التي تحقق هدفه.

كذلك يقوم بعمليات التي تمنع اكتشاف فعلته و تتبعه و تقصي اثره، هذا كله يحتاج دراية و فطنة و ذكاء من المجرم المعلوماتي[19].

2.2.2.1 ثانيا: اجتماعي

ان المجرم المعلوماتي يعيش في بيئة اجتماعية عكس المجرم التقليدي، و بالتالي تجد المجرم المعلوماتي يحب ان يرى نفسه محل ثقة المجتمع لكي يسهل عليه ارتكاب جرائمه و بالتالي لا يحب ان يكون سيء سمعة و محل شبهة فهذا يصعب عليه ارتكاب جرائمه المعلوماتية، عكس المجرم التقليدي فهو بارتكاب جرائمه يصبح محل شبهة و سيء السمعة و يفقد ثقة المجتمع به.

و بالتالي فالمجرم المعلوماتي شخص اجتماعي ولكما زادت اجتماعيته زادت خطورة ارتكابه لجرائمه[20].

3.2.2.1 ثالثا: غير عنيف

ان المجرم المعلوماتي لا يميل الى العنف في ارتكاب جرائمه وانما الى استعمال الحيلة و العقل ، و بالتالي لا يسعمل جهد بدني يستدعي القوة و العنف.

لان المجرم المعلوماتي لا يرتكب سلوك اجرامي مباشر اما شخص مادي وانما يرتكبه بواسطة وسائل الاتصال و المعلومات و البيانات التي تتطلب جهد ذهني وليس عضلي[21].

4.2.2.1 رابعا: يتمتع بالخبرة و المهارة

ان المجرم المعلوماتي لو لم يكن بالمهارة الكافية و الخبرة الكافية لما استطاع ارتكاب الجريمة الالكترونية فهو عكس المجرم العادي الذي يتمتع بالقوة العضلية لارتكاب الجريمة التقليدية.

بينما المجرم المعلوماتي يتمتع بالخبرة و التقنيات العالية لاستلاء على البيانات و اختراقها و القرصنة فهو على دراية فنية بالحاسب الآلي و انترنت و كيفية استخدامها[22].

5.2.2.1 خامسا: مثابر و صبور

ان المجرم المعلوماتي يحتاج ان يكون يتمتع بالصبر لانه هنا عمليات تحتاج وقتا طويلا لتحقيق النتيجة المرجوة .

كذلك لا بد ان يكون مثابر و ذلك بتكرار المحاولات مرات عدة حتى يحقق مبتغاه فالمجرم المعلوماتي عند خفق المحاولة الأولى لا ييأس و انما يكررها مرارا و تكرارا حتى يحقق ما يريد[23].

6.2.2.1 سادسا: التعاون و التواطؤ

يعتبر المجرم المعلوماتي شخص اجتماعي بطبعه كما يبق الإشارة اليه و عليه يبني علاقات تساعده على استكمال و إتمام نشاطه الاجرامي وذلك من خلال شخص يكون متخصص في الحاسب و شخص من الخارج يغطي العملية الاجرامية .

وعليه فالمجرم المعلوماتي يمكن ان يرتكب جريمته بسبب تعرضه لطرد من المؤسسة فيريد الانتقام ، او من اجل النصب و الاحتيال او بدافع اظهار مهاراته[24].

7.2.2.1 سابعا: من حيث العود الى الجريمة

ان المجرم المعلوماتي يتسم بعودته الى ارتكاب الجريمة الالكترونية اما بهدف سد الثغرة التي أدت الى اكتشاف جرمه و الإمساك به ومحاكمته وعند عودته يتم الإمساك به كذلك .

و اما بسبب ميوله لارتكاب هذا النوع من الجرائم و توسيع من خبراته في هذا المجال وكذا من اجل شعوره بالقدرة على الاختراق الالكتروني[25].

2 المبحث الثاني: الاطار القانوني لمكافحة الجريمة الالكترونية في التشريع الجزائري

ان التطور التكنولوجي و التحول الرقمي نظرا لما له من إيجابيات الا انه لم يسلم من السلبيات منها الجريمة الالكترونية ، وهذا ما دفع بالمشرع الجزائري الى وضع اليات لمجابهة هاته الظاهرة[26].

وعليه سنتناول في هذا المبحث مطلبين ، المطلب الأول المعنون بنطاق تجريم الجريمة الالكترونية و المطلب الثاني المعنون بالآليات القانونية للحد من الجريمة الالكترونية في التشريع الجزائري.

1.2 المطلب الأول: نطاق تجريم الجريمة الالكترونية

ان اركان الجريمة الالكترونية هي الأساس الذي تقوم عليه الجريمة فهي لا تختلف عن الجريمة العادية من حيث الأركان العامة حيث يشترط وجود الركن الشرعي وهو الأساس القانوني لتجريم الجريمة الالكترونية ، و الركن المادي بالإضافة الى الركن المعنوي الذي يقوم على علم و دراية الشخص الجاني و كذا الإرادة في ارتكاب السلوك الاجرامي.

اما الأركان الخاصة فهي ما يتم اضافته الى الأركان العامة و التي يكون النص عليها قانونا، وبالتالي يشترط في الجرائم الالكترونية وجود ركن خاص وهو نظام المعالجة الآلية للمعطيات حتى يتم البحث في وجود ام عدم وجود اركان الجريمة [27] ، و عليه سنتناول في هذا المطلب الأركان الجريمة الالكترونية و التي سنتفصل فيها على النحو التالي: الفرع الأول المعنون بالركن الشرعي و الفرع الثاني المعنون بالركن المادي و الفرع الثالث المعنون بالركن المعنوي.

1.1.2 الفرع الأول: الركن الشرعي

ان المشرع الجزائري ينص في المادة أولى من قانون العقوبات:" انه لا جريمة ولا عقوبة الا بنص" و انطلاقا من هذا جرم القانون رقم 15/04 بعض من أنواع الجريمة الالكترونية و حدد العقوبات المقررة و الموقعة على مرتكبيها في القسم السابع مكرر تحت عنوان:" المساس بأنظمة المعالجة للمعطيات" من الفصل الثالث المعنون" الجنايات و الجنح ضد الأموال" من الباب الثاني المتعلق" بالجنايات و الجنح ضد الافراد و ذلك في المواد من 394 مكرر الى 394 مكرر 08 من قانون العقوبات المعدل و المتمم.

كذلك جاء القانون 04/09 الذي تضمن قواعد للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال ومكافحتها وهذا كجانب احترازي من وقوع الجرائم الاكترونية.

ومنه عند نص المشرع على هاته الجرائم في قوانين هذا ما يمنع القاضي من استعمال القياس عند تطبيق العقوبة أي لا يمكن له النص على عقوبة منصوصة على فعل معين و تطبيقها على فعل اخر فقط بسبب ان هناك تشابه و بتالي يمنع القياس[28].

2.1.2 الفرع الثاني: الركن المادي

يعتبر الركن المادي هو قيام الشخص باتيان الفعل الجرامي أي يكون فيه السلوك الاجرامي و النتيجة الاجرامية و العلاقة السببية و بالتالي المجرم المعلوماتي عند قيامه بالجريمة الالكترونية يكون قام بسلوك الاجرامي من اجل تحقيق النتيجة الاجرامية و تكون هناك علاقة سببية فيما بينهما.

و بالتالي فالركن المادي في الجريمة الالكترونية كما سبق وان قلنا هو إتيان السلوك الاجرامي وبالتالي الاعمال التحضيرية كشراء المعدات و الأدوات هنا

لا يعاقب عليها القانون ولكن ان تم استعمالها في الجريمة الاكترونية هنا يتم المعاقبة.

ومنه لتوافر السلوك الاجرامي لابد من توافر وسائل كمبيوتر و ووسائل معلوماتية و عند قيام الجاني بجريمته يكون على علم بانه يقوم بسلوك اجرامي و سوف يحقق نتيجة اجرامية[29].

3.1.2 الفرع الثالث: الركن المعنوي

يعتبر الركن المعنوي هو توفر القصد في ارتكاب هاته الجريمة أي تكون هناك نية و إرادة آثمة و بالتالي يكون على دراية بانه فعله يعتبر فعل معاقب عليه قانونا.

فالمجرم المعلوماتي يكون على دراية بان فعله سلوك اجرامي و كان عليه بمجرد الولوج الى الحسابات التراجع لان هذا يعتبر تخطي الحدود و اطلاع على اسرار الافراد و بالتالي فالقصد الجنائي متوفر.

ولا يمكن القول انه لا يتوفر القصد الجنائي لانه كل الأشخاص المجرمين المعلوماتيين يتمتعون بخبرة [30].

2.2 المطلب الثاني: الآليات القانونية للحد من الجريمة الالكترونية في التشريع الجزائري

ان المشرع الجزائري حاول الالمام بالجريمة المعلوماتية من خلال النص على قوانين منظمة لها و نص على العقوبات المقررة على مرتكبيها[31] وعليه سنتناول في هذا المطلب فرعين الفرع الأول المعنون قانون العقوبات و الفرع الثاني المعنون ب القانون 04/09 و الفرع الثالث المعنون ب قانون الملكية الأدبية

والفنية و نصوص التوقيع الالكتروني و القانون المتعلق بالمواصلات السلكية ولاسلكية

1.2.2 الفرع الأول: قانون العقوبات

نص المشرع الجزائري و جرم الأفعال الماسة بأنظمة الحاسب الآلي وهذا بموجب قانون العقوبات 15/04 حيث تضمن هذا القسم 8 اقسام تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات"[32].

وعند قراءة و تحليل نصوص المواد من قانون العقوبات نجده يتضح انه المشرع قسمها الى أربعة فئات و تتمثل فيمايلي:

الطائفة الأولى : و تتضمن جرائم الولوج الى المعطيات المعالجة آليا عن طريق الغش و التزوير وكذا جريمة الحذف و التغيير و التخريب في هذه المعطيات.

الطائفة الثانية: تخص الجرائم الالكترونية بواسطة النظام المعلوماتي ، والتي من أهمها استعمال او افشاء او نشر معلومات منصوص عليها في قانون العقوبات ، و كذا البحث او التجميع في معطيات مخزنة في نظام معلوماتي.

الطائفة الثالثة: الجرائم الالكترونية المتعلقة بأمن الدولة و مؤسساتها كجرائم التجسس و الإرهاب و المساس بالأمن الوطني للدولة.

الطائفة الرابعة: الجرائم الالكترونية للشخص المعنوي والتي تعادل عقوبتها خمس مرات عقوبة الشخص الطبيعي المادة 394 مكرر 4 من قانون العقوبات[33].

ثم سنة 2006 عدل المشرع قانون العقوبات و ادرج تعديلات في القصم الخاص بالجرائم الماسة بمعالجة المعطيات الآلية و شدد العقوبات المقررة لها[34].

2.2.2 الفرع الثاني : القانون 04/09

جمع هذا القانون بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية و القواعد الوقائية التي تتيح الرصد المبكر لاعتداءات المحتمل وقوعها وكذا التدخل من اجل التصدي لها و تحديد مصدرها، بحيث نص على ست فصول تناول في الفصل الأول الاحكام العامة ، اما الفصل الثاني مسمى بمراقبة الاتصالات الإلكترونية حدد الحالات التي تسمح باللجوء الى المراقبة الالكترونية و الفصل الثالث حدد القواعد الإجرائية تفتيش المنظومات المعلوماتية و حجز المعطيات المعلوماتية و الفصل الرابع التزامات مقدمي الخدمات من خلال مساعدة السلطات و حفظ المعطيات المتعلقة بحركة السيرو الالتزامات الخاصة بمقدمي خدمة " الانترنت" و الفصل الخامس الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحته و الفصل السادس التعاون و المساعدة القضائية الدولية [35].

لقد اشارت المادة الأولى من هذا القانون ، الى انه يهدف الى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها

وكما سبق الإشارة اليه ان المادة 2 منه أوردت انه يقصد في مفهوم هذا القانون بما يأتي:

1.2.2.2 أولا : الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال

وتشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، او أي جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام لاتصالات الالكترونية.

2.2.2.2 ثانيا: منظومة معلوماتية

أي نظام منفصل او مجموعة من الأنظمة المتصلة ببعضها البعض، او المرتبطة يقوم واحد منها او اكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

3.2.2.2 ثالثا: معطيات معلوماتية

أي عملية عرض للوقائع و المعلومات او المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

4.2.2.2 رابعا: مقدمو الخدمات

أي كيان عام او خاص يقدم لمستعملي خدماته ، القدرة على الاتصال بواسطة منظومة معلوماتية او نظام للاتصالات، واي كيان اخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة او لمستعملها

5.2.2.2 خامسا: المعطيات المتعلقة بحركة السير

أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة الاتصالات ، توضح مصادر الاتصال و الجهة المرسل اليها و الطريق الذي يسلكه و تاريخ وحجم ومدة الاتصال و نوع الخدمة.

6.2.2.2 سادسا: الاتصالات الالكترونية

أي تراسل او ارسال او استقبال علامات او إشارات ، او صور او أصوات او معلومات مختلفة بواسطة أي وسيلة الكترونية[36].

3.2.2 الفرع الثالث: قانون الملكية الأدبية و الفنية ونصوص التوقيع الالكتروني و قانون المتعلق بالمواصلات السلكية و اللاسلكية

1.3.2.2 أولا: قانون الملكية الأدبية و الفنية

نظم المشرع من خلال الامر 05/03 المؤرخ في 2003/07/23 المتعلق بحقوق المؤلف و الحقوق المجاورة حماية المؤلفات و المصنفات الرقمية .

وعليه وضع برامج معلوماتية لحماية هاته المؤلفات كما شدد العقوبات في حالة المساس بهاته المؤلفات و المصنفات الرقمية وبهذا يضمن حقوق المؤلف

2.3.2.2 ثانيا: نصوص التوقيع الالكتروني

جاء القانون 03/15 المتعلق بعصرنة العدالة و تناول في القسم الأول من الفصل الثاني المنظومة المعلوماتية المركزية لوزارة العدل و القسم الثاني تناول التصديق الالكتروني.

اما الفصل الثالث تناول فيه ارسال الوثائق و الإجراءات القضائية بالطريق الالكترونية و الفصل الرابع استعمال المحادثات المرئية عن بعد اثناء الإجراءات القضائية و الفصل الخامس الاحكام الجزائية .

اما القانون 04/15 حدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترون

3.3.2.2 ثالثا: القانون المتعلق بالمواصلات السلكية و اللاسلكية

نص القانون رقم 03/2000 المتغلق بالبريد و المواصلات السلكية و اللاسلكية على احكام جزائية تعاقب أي مخالف للنظام القانوني، و بالتالي أي شخص من عمال و المرخص لهم تقديم خدمة المواصلات السلكية و اللاسلكية في اطار وظيفتهم ، ويقومون بانتهاك هاته المهمة بانتهاك الخصوصية و سرية المراسلات او غيرهم ممن يقومون بمثل هاته الأفعال يتم عقابهم طبقا لنص المادة 137 من قانون العقوبات يعاقب بالحبس و الغرامة[37].

الخاتمة

و في الأخير يمكن القول ان الجريمة الالكترونية مثلها مثل الجريمة التقليدية تقوم على ثلاث اركان الركن الشرعي الذي يقضي ان لا جريمة ولا عقوبة الا بنص وعلى الركن المادي و الذي يتوفر فيه السلوك الاجرامي و النتيجة الاجرامية و العلاقة السببية وكذا الركن المعنوي و هو التوجه الى الإرادة الآثمة لارتكاب الحريمة ومنه تدارك المشرع الجزائري خطورة هاته الجرائم بحث قام بالنص على نصوص قانونية في قانون العقوبات و كذا نصوص أخرى منها قانون المتعلق بمكافحة الجرائم التكنولوجيات الاعلام و الاتصال.

و عليه توصلنا الى النتائج التالية:

1- الجريمة الالكترونية تمس الأشخاص و المؤسسات
2- المجرم المعلوماتي عكس المجرم التقليدي فهو يرتكب جرائم معلوماتية تقوم على وسائل الاتصال و الحواسيب عكس المجرم التقليدي الذي يقوم بجرائم تقوم على الجهد العضلي و العنف
3- كذلك المجرم المعلوماتي يتسم بالذكاء و المهارة في الأمور التقنية و بالتالي لا يتطلب جهد عضلي وانما جهد عقلي

4- حاول المشرع النص و الحث على هاته الجرائم في نصوص و النص على العقوبات المقررة لها.

ومنه توصلنا الى هاته التوصيات:

1- تكوين المتخصصين في مجال مكافحة الجريمة الالكترونية
2- توحيد النصوص القانونية المتعلقة بالجريمة الالكترونية في قانون خاص
3- استحداث مقياس خاص بالجريمة الإلكترونية في الكليات الحقوق و العلوم السياسية لنشر الوعي
4- توعية الافراد بمخاطر الجريمة الالكترونية و عدم الخضوع للابتزاز

التهميش و الإحالات:

[1]- أنظر صباح عادل عارف الرواشدة: دور أنظمة الذكاء الاصطناعي في مكافحة الجريمة الالكترونية : دراسة ميدانية
في الأردن، المجلة الأردنية في إدارة الأعمال، المجلد 21، العدد 1 سنة 2025، الأردن ، ص122.

[2]- انظر حمالي سمير: التحديات القانونية لمواجهة الجريمة السيبرانية، اعمال الملتقى الوطني الافتراضي، الجرائم الالكترونية في المجتمع الجزائري(تشخيص الواقع وتحديات الامن السيبراني) ، جامعة يحي فارس المدية، المنعقد يوم 15 مارس 2022، ص21، 22.

[3]- انظر ياكر الطاهر: الجرائم الالكترونية احكام موضعية وإجرائية دراسة مقارنة، دار بلقيس، الجزائر، 2024، ص16.

[4]- انظر حسين شفيق: الاعلام الجديد و الجرائم الالكترونية(تسريبات، التجسس ، الإرهاب الإلكتروني) ، دار الفكر و فن، 2015، ص 16

[5]- انظر المادة 02 من القانون 04/09 المرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال،جريدة رسمية عدد 47، ص 5.

[6]- انظر ياكر الطاهر، مرجع سابق، ص 29، 30.

[7]- انظر رحموني محمد : خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41 ، ص 441.
[8]- بن مالك اسمهان: خصائص الجريمة المعلوماتية و أسباب ارتكابها، ص 116.
[9]- انظر ياكر الطاهر: مرجع سابق، ص 30.
[10]- انظر رحموني محمد: مرجع سابق، ص 442.
[11]- انظر ياكر الطاهر: مرجع سابق، ص 31.
[12]- انظر حمد محمد الدوسري: أنواع الجرائم الالكترونية و تحديات مكافحتها، مجلة المنار للدراسات و البحوث القانونية و السياسية، المجلد 9، العدد 1 ، جامعة يحي فارس المدية، جوان 2025، ص 97.
[13]- انظر إبراهيم رمضان إبراهيم عطايا: الجريمة الالكترونية و سبل مواجهتها في الشريعة الإسلامية و الأنظمة الدولية(دراسة تحليلية)، ، ص 371، 372.
[14]- انظر حمد محمد الدوسري: أنواع الجرائم الالكترونية و تحديات مكافحتها، مرجع سابق، ص 98.
[15]-انظر ياكر الطاهر: مرجع سابق، ص 26، 27.
[16]- انظر حمد محمد الدوسري: أنواع الجرائم الالكترونية و تحديات مكافحتها، مرجع سابق،ص 97.
[17]- انظر درقاوي عبد القادر، فليج غزلان: المجرم معلوماتي، مجلة الدراسات القانونية و السياسية، المجلد 11، العدد 2 ، جوان 2025، ص 61.
[18]- انظر غريبي بشرى: خصوصية المجرم المعلوماتي و دوفعه، مجلة نوميدروس الاكاديمية، المجلد 2، العدد 2، سنة 2021، ص 103.
[19]- انظر درقاوي عبد القادر، فليج غزلان: المجرم معلوماتي، مرجع سابق، ص 63، 64.
[20]- انظر ربيعي حسين: المجرم المعلوماتي -شخصيته و اصنافه- مجلة العلوم الإنسانية، العدد 40، محمد خيضر بسكرة، ص 289.
[21]- انظر ياكر الطاهر : مرجع سابق، ص 35.
[22]- انظر غريبي بشرى: خصوصية المجرم المعلوماتي و دوفعه، مرجع سابق، ص 105.
[23]- انظر ربيعي حسين: المجرم المعلوماتي -شخصيته و اصنافه، مرجع سابق، ص 290.
[24]- انظر درقاوي عبد القادر، فليج غزلان: المجرم معلوماتي، مرجع سابق، ص 65.
[25]- انظر غريبي بشرى: خصوصية المجرم المعلوماتي و دوافعه، مرجع سابق، ص 106.
[26]- انظر قنيول ياسمنية : الاطار التشريعي و المؤسساتي لمكافحة الجريمة الالكترونية، مجلة السياسة العالمية ، المجلد 8 ، العدد2 ، ص 255.

[27]- انظر مهداوي حنان : التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، مجلة الفكر القانوني و السياسي ، المجلد 6، العدد2، 2022، ص 1064.
[28]- انظر حمزة خضري، عشاش حمزة: خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية و السياسية، المجلد 06، العدد02 ، جوان 2020، ص 173.

[29]- رمال امين: دور القطب الجزائي في مكافحة الجريمة السيبرانية، اعمال الملتقى الوطني الافتراضي ، الجرائم الالكترونية في المجتمع الجزائري(تشخيص الواقع و تحديات الامن السيبراني) ، جامعة يحي فارس المدية، المنعقد يوم 15 مارس 2022، ص 86، 87.
[30]- انظر مهداوي حنان : التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، مرجع سابق، ص 1067.
[31]- انظر فاروق خلف: الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات ، العدد2، 2015، ص 15.
[32]- انظر راضية عيمور: الجريمة الالكترونية و آليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية و السياسية، المجلد 6، العدد 01، 2022، ص 96.
[33]-ياكر الطاهر: مرجع سابق، ص 45.
[34]- انظر راضية عيمور: الجريمة الالكترونية و آليات مكافحتها في التشريع الجزائري، مرجع سابق، ص 96.
[35]- انظر فاروق خلف: الآليات القانونية لمكافحة الجريمة المعلوماتية، مرجع سابق، ص 18، 19.
[36]- المادة 02 من القانون 04/09 المرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال، مرجع سابق، ص 5.
[37]- انظر فاروق خلف: الآليات القانونية لمكافحة الجريمة المعلوماتية، مرجع سابق، ص 18.

قائمة المراجع

القوانين:

1- القانون 04/09 المرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال،جريدة رسمية عدد 47.

المؤلفات:

1- ياكر الطاهر، (2024) الجرائم الالكترونية احكام موضعية وإجرائية دراسة مقارنة، الجزائر، دار بلقيس.
2- انظر حسين شفيق، (2015)، الاعلام الجديد و الجرائم الالكترونية(تسريبات، التجسس ، الإرهاب الإلكتروني) ، دار الفكر و فن.

المقالات:

1-صباح عادل عارف الرواشدة، 2025، دور أنظمة الذكاء الاصطناعي في مكافحة الجريمة الالكترونية : دراسة ميدانية في الأردن، المجلة الأردنية في إدارة الأعمال، المجلد 21، العدد 1 ،.ص 122.
2-حمد محمد الدوسري،جوان 2025، أنواع الجرائم الالكترونية و تحديات مكافحتها، مجلة المنار للدراسات و البحوث القانونية و السياسية، المجلد 9، العدد 1، ص 91، 98.
3-درقاوي عبد القادر، فليج غزلان، جوان 2025، المجرم معلوماتي، مجلة الدراسات القانونية و السياسية، المجلد 11، العدد 2 ، ص65،61،63،61.
4-غريبي بشرى، 2021،خصوصية المجرم المعلوماتي و دوفعه، مجلة نوميدروس الاكاديمية، المجلد 2، العدد 2، ص 103، 106،105.
5-ربيعي حسين: المجرم المعلوماتي -شخصيته و اصنافه- مجلة العلوم الإنسانية، العدد 40، 289، 290.
6-مهداوي حنان ،2022، التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، مجلة الفكر القانوني و السياسي ، المجلد 6، العدد2، ص 1064، 1067.
7-حمزة خضري،جوان 2020، عشاش حمزة: خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية و السياسية، المجلد 06، العدد02 ،ص 173.

8-فاروق خلف،2015، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات ، العدد2، ص 15، 18، 19.
9-راضية عيمور،2022، الجريمة الالكترونية و آليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية و السياسية، المجلد 6، العدد 01، ص 96.

المداخلات

1- رمال امين، المنعقد يوم 15 مارس 2022، دور القطب الجزائي في مكافحة الجريمة السيبرانية، اعمال الملتقى الوطني الافتراضي ، الجرائم الالكترونية في المجتمع الجزائري(تشخيص الواقع و تحديات الامن السيبراني) ، جامعة يحي فارس المدية.
2- حمالي سمير، يوم 15 مارس2022، التحديات القانونية لمواجهة الجريمة السيبرانية، اعمال الملتقى الوطني الافتراضي، الجرائم الالكترونية في المجتمع الجزائري(تشخيص الواقع وتحديات الامن السيبراني) ، جامعة يحي فارس المدية.