جامعة الدكتور الطاهر مولاي سعيدة

كلية الحقوق و العلوم السياسية

قسم الحقوق

خصوصية التحقيق في الجريمة المعلوماتية

مذكرة مقدمة لنيل شهادة الماستر في الحقوق

تخصص : القانون الجنائي وعلوم الجنائية

إعداد الطالب :

عبد العزيز أحمد

إشراف الأستاذ (ة) :

د . عياشي حفيظة

أعضاء لجنة المناقشة :

* د. هني عبد اللطيف .....رئيسا
* د . عياشي حفيظة .....مشرفا ومقررا
* د . حزاب نادية .....عضوا مناقشا

السنة الجامعية

2021 - 2022 م

1442 - 1443 هـ

جامعة الدكتور الطاهر مولاي سعيدة

كلية الحقوق و العلوم السياسية

قسم الحقوق

خصوصية التحقيق في الجريمة المعلوماتية

مذكرة مقدمة لنيل شهادة الماستر في الحقوق

تخصص : القانون الجنائي والعلوم الجنائية

إعداد الطالب :

عبد العزيز أحمد

إشراف الأستاذ (ة) :

د . عياشي حفيظة

أعضاء لجنة المناقشة

* د.هني عبد اللطيف .....رئيسا
* د . عياشي حفيظة .....مشرفا ومقررا
* د . حزاب نادية .....عضوا مناقشا

السنة الجامعية

2022 - 2021 م

1443 - 1442 هـ

شكر وتقدير

في البداية ، أحمد الله الذي اعطنا القوة والصبر

لإتمام هذا العمل العلمي المتواضع.

ثم أتوجه بجزيل الشكر والامتنان إلى الأستاذة عياشي

حفيظة لقبولها الإشراف على هذه المذكرة ،إذ لم

تبخل علينا بإرشاداتها وتوجهاتها القيمة.

كما أتقدم بجزيل الشكر إلى أعضاء اللجنة الموقرة

لقبولهم مناقشة هذه المذكرة .

ولا أنسى كل من قدم لي يد العون من قريب او من

بعيد في إنجاز هذا العمل

عبد العزيز أحمد

الإهداء

بعد بسم الله رحمان الرحيم وصلاة وسلام على أشرف المرسلين سيدنا محمد عليه صلاة وسلام لكم مني ☺ تحية الأسلام "سلام وعليم " ☺🖐🖐🖐☺

ولكم مني☺ تحياتي الأمازيغية " azoul fellawen" ☺🖐🖐🖐 ☺

أما بعد أهدي ثمرة جهدي :

* إلى ابي العزيز الغالي "عز الدين" أطال الله عمر وحفظه من كل سوء

* إلى مفاتيح الجنة أمي "نصيرة " الغالية شفها الله ورزقها لباس الصحة والعافية

* إلى من كان سندا لي دون ملل اخي وحبيبي "كريم" وزجته

* إلى أختي "سهام و جدجيقة " أنار الله طريقكم وجعلكم من أهل السعادة وسرور

* إلى كتاكيت ♥ كاميليا♥دهية ♥إسماعيل♥إسحاق ♥ أحبكم كثيرا ♥

* إلى عائلتي الثانية من أساتذة وطلاب وأعضاء نادي نخبة لكم من أحلى تحية 🖐☺

*وفي الاخير نسأل الله ان تبقى دوما هذه المحبة بيننا وأن تدوم في الدنيا والأخرة *

✍

عبد العزيز احمد

قائمة المختصرات :

* ق.ع .ج : هو اختصار قانون العقوبات الجزائري

* ق .أ.ج.ج : هو اختصار قانون الاجراءات الجزائية الجزائري

* **L'ONU**: **l'organisation des nations unies**.

* **OCDE** :**l'organisation de cooperation et de développement économiques**.

* **LOMPI**: **l'organisation mondiale de propriété intellectuelle**.

* **IC3**: **Internet Crime complaint center**.

* **IP** : **internet Protocol** .

* **incc** : **institut natoinal de criminalistique et criminologie**.

* **NCC** : **white collar crime**

* **FBI** : **Federal Bureau of Investigation**

* **IFCC** : **Internet Fraud Complaint Center**

مقدمة

لقد دخلت البشرية في بداية القرن الواحد وعشرين مرحلة جديدة من التطور الفكري والمعرفي في جميع مجالات الحياة ، وخصوصا في المجال التكنولوجي فبعد انتهاء عصر الثورة الصناعية ظهر بما يسمى عصر الثورة المعلوماتية ، ونقصد بالمعلوماتية هي اندماج الالة مع المعلومات والمعارف الانسانية ،مما ادى الى ظهور ما يسمى بالحاسب الالي الذي غير كل مفاهيم الحياة وأصبح الانسان يخزن كل معارفه ومعلوماته على دعائم جديدة مختلفة عن الدعائم التي كان يستعملها الانسان القديم،وخصوصا بعد ارتباط الحاسب الالي بما يسمى بشبكة الاتصال ، مما جعل معارف الانسان ومعلوماته تنتقل وتخزن وتعدل بشكل سريع ودقيق.

وبعد انتشار التكنولوجيي وبلوغ عصر الثورة المعلوماتية ذروته ساعد على تحقيق ما يسمى بالرقمنة ، والتي اخذت بها دول العالم في جميع مؤسستها الاقتصادية والإدارية والأمنية مما جعل هذه الدول تنتقل من العالم الحقيقي إلى العالم الافتراضي ، وهذا ما يسمى بمشروع الحكومة الالكترونية وبعد هذا الانتقال اضحت جميع مصالح هذه الدول في البيئة الافتراضية ، وذلك بسبب انتقال جميع الخدمات المالية وغير المالية في هذه البيئة.

ولعل كثرة الولوج الى العالم الافتراضي انتج بما يسمى بالمجتمع معلوماتي ومن الطبيعي ان تتنقل مع هذا المجتمع المعلوماتي جميع الظواهر السلبية الموجودة في العالم الحقيقي ، ومن هذه الظواهر هي الجريمة فكل جريمة كانت في العالم المادي انتقلت هي كذلك الى العالم المعنوي ، فلقد اضحى الكثير من الافراد يستخدمون الحاسب الالي لإغراض اجرامية تمس بمصلحة المجتمع المرتبطة بهذا التطور، فاليوم اصبح المجرم يرتكب سلوكه الاجرامي بطريقة اكثر احترافية من المجرم التقليدي وهذا ما يسمى بالمجرم المعلوماتي ، لان هذا الاخير يتميز بمستوى عالي من المهارات والذكاء وبعد ان كانت الجرائم التقليدية ترتكب بوسائل بسيطة مثل الضرب والجرح وتكسير الابواب وحمل السلاح ... ، أصبحت اليوم ترتكب الجرائم بشكل اكثر خطورة وبوسائل متطورة فمثلا يكمن اختلاس اموال طائلة بكبسة زر لا تكلف المجرم جهد بدني.

وعليه استوجب تدخل القانون محاولا تنظيم هذا التطور المعلوماتي وحماية مصالح المجتمع في هذه البيئة المعنوية ، وذلك عن طريق وضع تشريع يحمل في طياته قواعد موضوعية وإجرائية وتتمثل القواعد الموضوعية في تجريم كل الافعال التي قد تمارس في البيئة الافتراضية ، وتعود بالضرر الى العالم الحقيقي فمثلا المساس بالمنظومة المعلوماتية ومعالجة المعطيات الموجودة فيها تمس بمصالح افراد المجتمع وذلك بسبب ما تمثله هذه المعطيات من قيمة مالية او معلومات سرية او تصرفات في غاية الخطورة،لهذا جرم التشريع الجنائي هذه الافعال وسلط عقوبات على كل من تسول له نفسه في ارتكابها.

أما القواعد الاجرائية هي الاجراءات التي تتخذها الجهة القضائية للوصول إلى الحقيقة وكشفها وجمع الادلة التي تدين المشتبه فيهم ، حيث هذه الاجراءات تنظم التحقيق بجميع مراحله ابتدأ من مرحلة جمع الاستدلالات مرورا بمرحلة التحقيق الابتدائي وصولا إلى مرحلة المحاكمة ، وكل مرحلة من هذه المراحل تهدف الى ضبط الادلة التي تكشف المتهم وموجهته بها ،مما استوجب استحداث هذه الاجراءات مثل التفتيش في البيئة المعنوية والمعاينة و ضبط الادلة واستجواب المتهمين والسماع الشهود والتسرب الالكتروني وغيرها من الاجراءات.

والهدف من استحداث هذه الإجراءات هو مواكبة التطور التكنولوجي ومكافحة كل الجرائم التي ترتكب بواسطته ، ولا نجاح لهذه الإجراءات إلا عن طريق استخدام نفس التقنية التي يستخدمها المجرم الإلكتروني لمساعدة التحقيق ، وهذا ما يسمى بالخبرة الفنية التي تساعد المحقق في كشف الدليل القاطع لإدانة المتهم وكل دليل يتم ضبطه في البيئة الالكترونية يسمى بالدليل الالكتروني .

ويعتبر الدليل الالكتروني من بين الوسائل التي يعتمد عليها القاضي في تكوين قناعته في إصدار الاحكام والقرارات القضائية ، حيث بين المشرع سلطات القاضي في تقدير وقبول هذا الدليل لأن الدليل في البيئة الافتراضية يتمتع بخصوصيات تميزه عن الدليل في العالم الحقيقي ، فهو سريع الإخفاء وصعب الوصول إليه مما جعل جهات التحقيق تواجه صعوبة في إستخلاصه .

ولعل اكثر العوائق التي تواجه إجراءات التحقيق هي عدم توازن بين هذه الاجراءات والتطور السريع لتقنية المعلوماتية وكذلك عوائق التوازن بين مصلحة العدالة في محاربة الجريمة المعلوماتية وضمانات التي جاء بها القانون لحماية حقوق الانسان.

ومن خلال ما تم عرضه بصورة ملخصة لأهم المسائل المراد التطرق إليها ، تقودنا هاته الدراسة إلى طرح الاشكالية الرئيسية التي مفادها:

* ما هي الخصائص التي تتمتع بها إجراءات التحقيق والبحث والتحري في ظل التشريع الجزائري ؟ و ما هو موقف المشرع من وسائل الاثبات في الجريمة المعلوماتية ؟ وانطلاقا من هذه الإشكالية الرئيسية يمكن الخروج بالإشكاليات الفرعية التالية :

*ما مفهوم الجريمة المعلوماتية؟

* هل هناك أجهزة خصصها المشرع لمكافحة الجريمة المعلوماتية ؟

* هل يجب ان تتوفر بعض المهارات لدى المحقق لتحقيق في الجريمة المعلوماتية ؟

* هل الدليل الإلكتروني يختلف عن الدليل العادي في الجريمة المعلوماتية ؟

أسباب اختيار الموضوع :

لعل اسباب اختيار موضوع خصوصية التحقيق في الجريمة المعلوماتية تختلف فمنها أسباب ذاتية وأخرى موضوعية ، حيث الأسباب الذاتية تتمثل في الفضول وحب إكتشاف كل ما يتعلق بوسائل التكنولوجيا الحديثة ، و ما ينظمه القانون في هذا الجانب وكذلك حب التعمق في التخصص الجامعي ، أما الأسباب الموضوعية تتمثل في انتشار الجرائم المعلوماتية في المجتمع بشكل ملحوظ مما يجب تسليط الضوء عليها ، ودراسة أهم القواعد الإجرائية والموضوعية التي جاء بها المشرع لمكافحة هذا النوع من الجرائم.

أهمية الموضوع :

تتجلى أهمية دراسة هذا الموضوع من خلال معرفة الجرائم المرتكبة ضد الحاسوب وشبكة الانترنت وإلقاء العبء على الدولة بوضع التشريعات اللازمة لحماية المجتمع منها ، بالإضافة إلى أهمية معرفة مدى خطورة جرائم المعلوماتية التي تمس حياة الأفراد وتهدد الأمن القومي والسيادة الوطنية ، وكذلك تهديد إبداع العقل البشري ولذلك يجب الإلمام بما هية الجرائم الحاسوب وطبيعته وإظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها ودوافع مرتكبيها ، وهذا يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية.

أهداف دراسة الموضوع :

لعل من اهداف دراسة الموضوع هي تسليط الضوء على خصوصية التحقيق في مواجهة الجرائم المعلوماتية ،و إبراز أهم التحديات التي تواجه التحقيق في الجرائم المعلوماتية ، وكذلك كيفية التعامل مع الدليل الالكتروني للارتقاء بإجراءات التحقيق ، و تزويد الأشخاص المنوط لهم عملية التحقيق بالتقنيات الحديثة للكشف عن المجرم المعلوماتي ، و تنظيم التجارة الالكترونية الدولية وحمايتها من الأعمال الغير المشروعة وحماية مصالح المجتمع المعلوماتي بصفة عامة.

الدراسات السابقة :

تشمل الدراسات السابقة في موضوعنا هذا في الكتب ، و أطروحات الدكتورة و مذكرة ماستر كما يلي:

الكتب:

* كتاب بعنوان فن التحقيق الجنائي في الجرائم الإلكترونية " للدكتور خالد ممدوح إبراهيم الطبعة الأولى لسنة 2009 ، حيث تناول هذا الموضوع بشكل موسع وتطرق للجريمة ، الإلكترونية الواقعة على الأشخاص والأموال وعالج بعض صور الجريمة الالكترونية كالسب القذف عبر الانترنت و التصنت.

* يزيد بوحليط ،الجرائم الإلكترونية و الوقاية منها في القانون الجزائري،دار الجامعة الجديدة للنشر،الإسكندرية،مصر،2019 حيث تناولت هذه الدراسة كل جرائم المعلوماتية في التشريع الجزائري وكذلك اجراءات التحقيق فيها وكل وسائل الاثبات فما يخص الجريمة المعلوماتية.

أطورحات الدكتورة :

*ربيعي حسين ،آليات البحث و التحقيق في الجرائم المعلوماتية ، رسالة دكتوراه ، تخصص قانون العقوبات و العلوم الجنائية،قسم الحقوق،كلية الحقوق و العلوم السياسية ، جامعة باتنة الجزائر،سنة 2016-2015.

مذكرة ماستر:

*غربي جميلة ، آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر ، تخصص قانون جنائي قسم قانون عام ،كلية الحقوق و العلوم السياسية ، جامعة أكلي محمد أولحاج ، البويرة ؛ الجزائر ، سنة 2020-2021.

صعوبات الدراسة :

لقد تلقينا صعوبات في دراسة الموضوع وذلك بسبب ما يتميز به من مصطلحات تقنية خارج التخصص ، تستوجب فهمها مثل المعلوماتية ، والمكونات الحاسوب وشبكات الانترنت وكذلك وجهتنا صعوبة في تحديد الخطة ، المناسبة بسبب ان الموضوع يحتوي على محاور كثير ولا يمكن إدراجها كلها ضمن دراسات مذكرة ماستر المقيدة بعدد معين من الصفحات ، و نقص المراجع حيث كانت أغلب المراجع تركز دراستها على الجانب الموضوعي للجريمة المعلوماتية مع إهمال الجانب الاجرائي والذي هو محل درستنا اليوم.

منهج الدراسة :

اعتمدنا في دراستنا هذه على المنهج التحليلي و الوصفي ، كونه الأنسب لمثل هذه الدراسات من خلال تحليل مختلف المواد القانونية التي تتضمن إجراءات المتابعة في الجريمة المعلوماتية واختلافها عن النصوص الإجرائية التقليدية ، وكذا وصف وتحليل مختلف الاتفاقيات الدولية والعربية من أجل مكافحة هذا النوع من الإجرام المعلوماتي.

ومن أجل معالجة الإشكالية التي سبق طرحها وجب تقسيم هذه الدراسة وفقا لخطة المنهجية وهي كما يلي :

حيث الفصل الأول تناول الجريمة المعلوماتية وإجراءات التحقيق فيها ، والذي يضم مبحثين:الأول ماهية الجريمة المعلوماتية ؟ الذي يشمل في المطلب الأول مفهوم الجريمة المعلوماتية ، وفي المطلب الثاني تصنيف الجريمة المعلوماتية وسبل مكافحتها ، **أما** في المبحث الثاني تضمن إجراءات التحقيق في الجريمة المعلوماتية ، والذي يضم في المطلب الأول مراحل التحقيق في الجريمة المعلوماتية وصعوباته ،وفي المطلب الثاني الأجهزة المكلفة بالبحث وتحري عن الجريمة المعلوماتية .

أما في الفصل الثاني تناول الدليل الإلكتروني والقواعد الاجرائية لاستخلاصه ،والذي يضم مبحثين : الأول ماهية الدليل الإلكتروني ؟ ويشمل في المطلب الأول مفهوم الدليل الإلكتروني ، و في المطلب الثاني موقف المشرع الجزائري من الدليل الإلكتروني في مجال الإثبات الجنائي ، أما المبحث الثاني تضمن القواعد الإجرائية لاستخلاص الدليل الالكتروني ، ويضم مطلبين الأول القواعد الإجرائية التقليدية لاستخلاص الدليل الإلكتروني،و المطلب الثاني القواعد الإجرائية المستحدثة لاستخلاص الدليل الإلكتروني ، وفي الأخير الخاتمة ، وقائمة المراجع .

الفصل الأول :

الجريمة المعلوماتية وإجراءات التحقيق فيها

الجريمة المعلوماتية باعتبرها ظاهرة اجرامية تفشت في المجتمع وأضحت تهدد سلامته وأمنه ، إستوجب معرفتها وتبيان أهم المفاهيم التي توصل إليها الفقهاء ، وتحديد طرق ارتكاب هذه الجرائم وما تشكله من خطورة ، وكذلك تبيان أهم الاجراءات التحقيق فيها وسبل مكافحتها وخصائص التحقيق فيها ، وكذلك تبيان ما يتميز بيه أطراف هذه الجريمة كل من الجاني والشاهد والضحية و تبيان الأجهزة التي تسهر على مكافحة هذه الجريمة ، و أيضا تبيان موقف التشريعات الدولية والإقليمية والوطنية من هذه الجريمة وما هي القوانين الموضوعية والإجرائية التي جاء بها المشرع الجزائري ؟ لمحاربة هذه الجريمة والحد منها وعليه لقد قسما هذا الفصل إلى ما يلي :

***المبحث الاول : ماهية الجريمة المعلوماتية ؟**

***المبحث الثاني : إجراءات التحقيق في الجريمة المعلوماتية**

المبحث الاول : ماهية الجريمة المعلوماتية

لقد اختلف الفقه في وضع تعريف جامع ومانع للجريمة المعلوماتية وذلك بسبب ما تتميز بيه من طبيعة خاصة ومختلفة عن الجريمة التقليدية ، حيث الجريمة المعلوماتية تختلف في خصائصها و اركانها وأطرفها وهذا بسبب البيئة المختلفة التي تقع فيها ، و للجريمة المعلوماتية عدة انواع وأصناف حيث كل صنف فيها يختلف عن الأخر من حيث الأضرار ، وهذا ما أستوجب على المجتمع الدولي وحتى الوطني التحرك لمحاربتها بكل السبل والوسائل القانونية وعليه تم تقسم هذا المبحث إلى المطلب الأول مفهوم الجريمة المعلوماتية ، و المطلب الثاني تصنيف الجريمة المعلوماتية وسبل مكافحتها .

المطلب الاول : مفهوم الجريمة المعلوماتية

نظرا لتطور السريع للجريمة المعلوماتية اصبحت تتميز بعدة تعريفات فقهية وأصبح كل تعريف يصب في إتجاه خاص به ، حيث الوصول إلى تعريف دقيق فيه نوع من الصعوبة وذلك نظرا للخصائص التي تتميز بها ، فالجريمة المعلوماتية سريعة التطور وذات بيئة معنوية لأنها تقع في العالم الافتراضي وتتحقق أضرارها في العالم الحقيق ، وكذلك اطراف الخصومة كل طرف منهم يتميز بخصائص مختلفة عن أطراف الجريمة التقليدية .

الفرع الاول : تعريف الجريمة المعلوماتية

قبل الشروع في تعريف الجريمة المعلوماتية يتوجب علينا فهم أصل المعلومة والمعلوماتية والنظم المعلوماتية ،وأيضا يتوجب علينا معرفة أهم الضوابط والمعايير التي يجب الإعتماد عليها في تحديد المصطلح الأنسب لتعريف هذه الجريمة ، والمقصود بالمعلومات (information) هي مجموعة من الرموز والحقائق والمفاهيم التي تصلح ان تكون محلا للتبادل والاتصال [1]، وكان الانسان في القدم يحاول وضعها على بعض الدعائم مثل الحجر والخشب والأوراق...الخ ، وبعد تطور الانسان في شتى المجالات

[1] بن يحي اسماعيل،**التحقيق الجنائي في الجرائم الإلكترونية** ،رسالة دكتوراه،تخصص قانون الخاص،قسم حقوق كلية الحقوق و العلوم السياسية،جامعة أبي بكر الصديق بلقا يد،تلمسان،الجزائر،سنة 2020-2021،ص 25

وخصوصا في مجال الالة نجح في دمج هذه المعلومات مع الألة الحاسبة وهذا ما يسمى بالمعلوماتية (informatique)[1] ، حيث المعلوماتية تعرف بالعلم التفاعلي العقلاني بواسطة آلة أوتوماتكية مع المعلومات باعتبارها دعامة للمعارف الإنسانية في مختلفة الميادين ، و المقصود كذلك بنظم المعلوماتية (Systems informatiques)[2] هي كل آلة بمفردها او مع غيرها من الآلات المتصلة أو المرتبطة والتي يمكن أن تقوم سواء بمفردها او مع مجموعة عناصر اخرى تنفيذا لبرنامج معين بأداء معالجه الالية للبيانات المعلوماتية ، ومعنى هذه أنه كل معالجه للمعلومات والبيانات سواء تخزينها أو إدخالها أو إخراجها وتعديلها بواسطة الاله بشكل اوتوماتيكي.[3]

وبعد كل هذه التعريفات سنعرج إلى أهم المعايير والضوابط لتحديد التعريف الأنسب للجريمة المعلوماتية ، فهناك من يعرفها بالغش المعلوماتي وهناك من يعرفها بجرائم الانترنت...الخ وذلك بالإعتماد على بعض الضوابط والمعايير في تعريفها ، أولها معيار الدمج بين الجانب التقني والقانوني حيث المعلوماتية هي نتاج الحوسبة والاتصال، والمقصود بالحوسبة انها تقوم على وسائل تقنيه لإدارة وتنظيم ومعالجة المعطيات في اطار تنفيذ مهام محدده تتصل بعمل الحاسب والمنطق ، أما الاتصال فهو قائم على وسائل التقنية لنقل المعلومات ،ثم ربطها بالجانب القانوني هذا بالنسبة للضابط الأول ، اما الضابط الثاني يقوم على أساس البحث بشأن الحدود التي ينتهي عندها العبث أي عند انتهاء المسؤولية الاخلاقية التي تقوم عند إساءة استخدام الحاسب الآلي ، والحدود التي تبدأ عندها المسؤولية الجنائية أي تحديد الجرم لهذه الأفعال والضابط الثالث والأخير، هو أن يتم اختيار مصطلح شاملا ومحدود والمقصود بالشمولية

[1] Michal el char.la criminalité informatique devance la justice pénale. Edition juridique .sader. beyrook Liban 2004.pp.18-19.

[2] ربيعي حسين ، **آليات البحث و التحقيق في الجرائم المعلوماتية** ، رسالة دكتوراه تخصص قانون العقوبات و العلوم الجنائية ، قسم الحقوق ، كلية الحقوق و العلوم السياسية ، جامعة باتنة 1، الجزائر ، سنة 2015-2016 ، ص09-10.

[3] **نفس المرجع** ، ص 12.

هو أن يمس المصطلح كل جوانب موضوع الجريمة المعلوماتية ، المقصود بالمحدودية أي لا يخرج المصطلح عن نطاق جوانبه الموضوعية اثناء تعريفه.[1]

أما الآن وبعد تحديد الضوابط التي يعتمد عليها في تعريف الجريمة المعلوماتية سنتطرق إلى الاتجاهات الفقهية التي اختلفت في تعريف الجريمة المعلوماتية ، بين مضيق وموسع حيث الاتجاه الضيق يرى أنه يجب حصر مفهوم الجريمة المعلوماتية وربطها بعناصر عديدة كالحاسوب او مستخدمه او بموضوع الجريمة ، ومن أنصار هذا الاتجاه عدة فقهاء منهم الفقيه ماروي(merwe) عرفها بأنها الفعل الغير المشروع الذي يستخدم في ارتكابه الحاسب الآلي ويرى كذلك الفقيه روزبلات(rosbalt) انها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو وصول إلى معلومة مخزنه داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه ، ويرى كذلك ا لفقية الالماني تادمان(tademann) على انها كل أشكال السلوك الغير المشروع الذي يرتكب بإستخدام الحاسب الالي ، وهناك من عرفها أنها فعل غير مشروع تكون المعرفة بتقنية المعلوماتية لمرتكبها أو هي الجريمة التي تقع بواسطة الحاسب الالي أو عليه أو بواسطة شبكة[2] الانترنت ، والعديد من التعريفات تابعة إلى هذا الاتجاه وعليه يربط أنصار هذا الاتجاه ضرورة وجود الحاسوب الذي يكون أما أداة للجريمة او هدفا لها ووجود معارف واسعة ومسبقة بتكنولوجيا الكمبيوتر ، وهذا التعريف وجد انتقادا وذلك بسبب ربط الجريمة بالحاسوب أو بمستخدمه أو بموضوع الجريمة حيث يرى من أنتقد هذا الاتجاه أن ربط الجريمة بالحاسوب فيه نوع من الحصر على الاداة المستخدمة ، لأن هناك عديد من الاجهزة والتي هي في تطور مستمر غير الحاسوب مثل الهاتف واللوحات الذكية وأيضا هناك من إنتقد هذا الاتجاه على أنه لا يجب أن يكون هناك المعرفه الواسعة لارتكاب الجريمة المعلوماتية ، حيث يمكن لأي شخص أن يكون له معرفه بسيطة يرتكب هذا النوع من

[1] بغاديد نابية ، **آليات البحث والتحري عن الجريمة المعلوماتية** ، مذكرة ماستر ، تخصص قانون جنائي قسم الحقوق ، كلية الحقوق و العلوم السياسية،جامعة الدكتور مولاي الطاهر،سعيدة،الجزائر،سنة 2015-2016.ص8

[2] يزيد بوحليط، **الجرائم الإلكترونية و الوقاية منها في القانون الجزائري** ، دار الجامعة الجديدة للنشر، الإسكندرية ، مصر ، 2019 ، ص48

الجرائم كإرسال رسالة نصيه بالهاتف او عبر البريد الالكتروني او نسخ البيانات ...الخ ،كما أن حصر الجريمة في موضوعها والتي تقع على النظام المعلوماتي فيه تضييق لأنه تندرج في النوع واحد من الجرائم والمسماة بجرائم المعالجه الالية للمعطيات ، اذ يخرج عن نطاق هذا التعريف العديد من انواع الجرائم كجرائم الاحتيال المعلوماتي.[1]

وعليه ظهر الاتجاه الموسع والذي هو عكس الاتجاه السابق إذ لم يحصر الجريمة المعلوماتية في الحاسوب او مستخدمه او بموضوع الجريمة ، وإنما تم ربطها بالتقنية ذاتها المستخدمة في كافة الاجهزة المعلوماتية فهناك من يعرفها على أنها كل فعل إجرامي متعمد ، أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة للمجني عليه او كسبا يحققه الفاعل ، كما عرفتها المنظمه التعاون الاقتصادي والتنمية بأنها كل فعل او امتناع من شأنه الإعتداء على الاموال الماديه والمعنوية يكون ناتجا بطريقه مباشره او غير مباشره عن تدخل تقنية معلوماتية.[2]

ويرى الاستاذان(vivant وlestanc) بأن لجريمة المعلوماتية انها مجموعة من الافعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب ، وعرفت كذلك على انها سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الحاسوب ، أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد عرفها بأنها أي جريمة يمكن ارتكابها بواسطة نظام حاسوب أو شبكة حاسوبية ، أو تلك التي تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية[3].

[1] خالد ممدوح ابرهيم ، **الجرائم المعلوماتية** ،**دار الفكر الجامعي** ، الاسكندرية ، مصر ،طبعة الاولى ، ص 73

[2] حنان ريحان المبارك المضحكي ، **الجرائم المعلوماتية** ، دراسة مقارنة ، منشورات الحلبي الحقوقية ، بيروت لبنان ، الطبعة الاولى،2014،ص26

[3] نهلة عبد القادر مومني ، **الجرائم المعلوماتية** ، دار الثقافة للنشر و التوزيع ، عمان،الطبعة الثانية ، 2010 ،ص 48 -49

ونلاحظ أن التعريف الموسع حاول الإحاطة قدر الامكان بجميع الاشكالات الاجرامية للجريمة المعلوماتية ، سواء التي قد تقع بواسطة نظام المعلومات أو قد تشمل جميع جرائم الواقعه في البيئة الالكترونية ، فلم يركز هذا الاتجاه على فاعل الجريمة ومقدرته التقنية ولا على وسيلة إرتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية ، بل حاول عدم حصر الجريمة المعلوماتية في نطاق ضيق وذلك ما يتناسب مع مرونة مبدأ شرعيه الجرائم من أجل عدم افلات المجرم من العقاب.

الفرع الثاني : خصائص الجريمة المعلوماتية والصعوبات التي تتميز بها

تتمتع الجريمة بخصائص و صعوبات تميزها عن الجريمة التقليدية وهي كما يلي:

أولا :خصائص الجريمة المعلوماتية

الجريمة المعلوماتية باعتبارها من الجرائم المستحدثه فأنها تتمتع بمجموعة من السمات والخصائص حيث تسليط الضوء على هذه الخصائص يساعد في معرفه التعامل مع هذا النوع من الجرائم سنتطرق اليها كما يلي :

* خفاء الجريمة المعلوماتية وسرعة التطور في ارتكابها والمقصود بالخفاء انها تتسلل في خفاء دون أن يلاحظ المجني ، عليه ذلك وعلى أنه مراقب وهناك من يتجسس عليه او من يغير في البيانات والمعلومات الموجودة في الجهازه والمقصود بالسرعة انها تتم في بضعة ثواني من زمن.

* ترتكب في بيئة رقميه معلوماتية قوامها النظم المعلوماتية الحاسوبية وتجهيزات الحاسب الالي تتم بواسطة مكونات المادية للحاسوب هاردور (hardware) ومكونات البرمجيات سوفت وير[1](software)

* صعوبة الحصول على الدليل المادي في مثل هذه الجرائم وسهولة التخلص منها في نفس الوقت حيث على سبيل المثال متى ارتكبت الجريمة في مجال العمل معين مثل البنوك والمؤسسات بواسطة

[1] محمد حماد مرهج الهيتي ، **الجريمة المعلوماتية** ، دراسة مقارنة ، دار الكتب القانونية ، مصر ، 2014 ، ص 96

عاملين فيها ، فانه يسهل عليهم ارتكاب الجريمة وإخفاء الدليل بسهوله بحكم هم الاكثر تعامل مع الانظمة الموجودة فيها.[1]

* جريمة المعلوماتية تستلزم طرق خاصة مستحدثه للإثبات والوصول اليها وذلك بتدريب وتعليم المختصين على كل العلوم الحاسب الالي لأنها تحتاج الى شرطي إلكتروني ومحقق إلكتروني وقاضي إلكتروني وخبير كشف الدليل الذي يثبت ادانة المجرم.

* تتميز الجريمة المعلوماتية بعدم وجود حدود معلومة في ارتكابها فهي عالمية ممكن ان يكون الجاني من دوله والمجني عليه من دوله اخرى.

* تدني نسبة الإبلاغ عن الجريمة من طرف المجني عليه خاصة في حالة شركات ومؤسسات ، لتجنب الإساءة للسمعها و الرغبة في عدم زعزعة ثقة العملاء ففي إحدى الوقائع تعرض أحد البنوك وهو بنك (merchant bank city)[2] في بريطانيا لسرقة ثمانية مليون جنية إسترليني ، من إحدى أرصدته إلى رقم في سويسرا وتم ضبط الفاعل متلبسا يسحب المبلغ المسروق وبدلا من محاكمته ، قام البنك بدفع مليون جنية له بشرط إلتزام الفاعل بعدم الإعلام عن بجريمته و إعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن لحاسوب البنك الرئيسي[3].

* تكون غالبا الخسائر الناجمة عنها فادحة للمجني عليه فقد يخسر ماله او يفقد اعصابه بسبب ضغط الجاني عليه.

---

[1] نايري عائشة ، **الجريمة الالكترونية في التشريع الجزائري** ، مذكرة ماستر، تخصص قانون إداري ، قسم حقوق ،كلية الحقوق و العلوم السياسية ، جامعة أحمد داريه ، أدرار ، الجزائر ،سنة 2016-2017 ، ص 16.

[2] Ahmed Dahmani, La démocratie à l'épreuve de la société numérique, KARTHALA Editions, 1,Paris,France, 2007. P 58

[3] فريد منعم جبور، **حماية المستهلك عبر الانترنت ومكافحة الجرائم الالكترونية** ،منشورات الحلبي الحقوقية ،بيروت، لبنان، طبعة الاولى ،2010.ص 141

* الجريمة المعلوماتية من الجرائم التي لا يستعمل فيها العنف ولا أي مجهود مثل الجرائم التقليديه كالسرقة وكسر الاشياء والضرب ، بل هي تعتمد على قدرات ذهنيه للجاني دون اي ضجة او دليل مادي يكشف الجاني و دون الحاجه الى سفك دماء فالجريمة المعلوماتية عاده تتم بتعاون اكثر من شخص على ارتكابها وغالبا يكون لكل شخص دور معين يلعبه لتغطيه عمليه التلاعب وتحويل المكاسب.[1]

ثانيا: الصعوبات التي تتميز بها الجريمة المعلوماتية :

تتميز الجريمة المعلوماتية بمجموعة من الصعوبات و التي جعلتها تتميز عن الجرائم التقليدية و من أهم هذه الصعوبات كمايلي:

* صعوبة تحديد حجم الضرر الناتج عنها

* الضخامة البالغة للبيانات الرقمية المتعين فحصها أثناء التحريات.

*الداركنة (dark net) أو الشبكة السوداء بإستعمال الهوية المخفية

* إستعمال بروتوكولات التشفير المعقدة وذلك يصعب من مهمة قراءة البيانات

* دلائل الاثبات الرقمية في معظم القضايا تكون ضمن خوادم serveur خارج التراب الوطني.

* المعاملة المتصلة بالجريمة سبرانية معقدة و سريعة التطور

* أدلة الإدانة في الجرائم غير كافية و يرجع ذلك إلى عدة عوامل تتمثل في عدم وجود أي أثر كتابي إذ يتم نقل المعلومات بشخصيات إلكترونية قد تكون وهمية.[2]

[1] نعيم مغبغب ، **حماية برامج الكمبيوتر** ، منشورات الحلبي الحقوقية ، لبنان ،طبعة الثانية ، 2009، ص 141

[2] بشير حماني ،**خصوصية التحقيق في الجريمة الإلكترونية** ، مذكرة ماستر،تخصص قانون الجنائي و العلوم الجنائية ، قسم حقوق،كلية الحقوق و العلوم السياسية ، جامعة محمد بوضياف، المسيلة ،الجزائر،سنة 2018-2019،ص16.

الفرع الثالث : أركان الجريمة المعلوماتية

لا شك أن في الفقه الجنائي لا يوجد جريمة إلا ولها اركان محددة وسنتطرق في هذا الفرع الى اركان الجريمة المعلوماتية وفق ما يلي:

أولا : الركن الشرعي

معناه اعتراف المشرع بتجريم الفعل المرتكب وهو ما نصت عنه المادة الاولى من قانون العقوبات ، أي لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون وهذا ما نقصد به مبدأ الشرعية القوانين ، أما بالنسبة للجريمة المعلوماتية[1] فالمشرع الجزائري قد أحدث في قانون العقوبات في القسم السابع المكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

وكذلك القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و بعض النصوص الأخرى سنتطرق اليها لاحقا.[2]

ثانيا : الركن المادي

الركن المادي للجريمة الإلكترونية يقوم على صورتين أساسيتين :

* الصورة الأولى متمثلة في الاعتداء على نظام المعالجة الآلية وهذه الأخيرة تحتوي على نوعين من الاعتداء ، وهو الدخول والبقاء غير مشروع في نظام المعالجة الآلية للمعطيات وينطوي تحت هذا النوع ثلاث أفعال فعل الدخول والبقاء و عرقلة أو التعطيل ، أما النوع الثاني متمثل في الاعتداء العمدي

على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال وهي فعل الإدخال والمحو والتعديل.[1]

[1] أحسن بوسقيعة ،**الوجيز في القانون الجزائي العام**،دار الهومة للطباعة والنشر والتوزيع ،الجزائر، الطبعة11، 2012 ص 58

[2] **بشير حماني** المرجع السابق ، ص 11

* أما الصورة الثانية متمثلة في الاعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي.

وبهذا تم تحديد أهم الماديات الجريمة التي تبرز إلى العالم الخارجي في الجريمة المعلوماتية.

ثالثا : الركن المعنوي

يتكون الركن المعنوي للجريمة المعلوماتية من عنصرين العلم و إرادة :

* العلم:يتمثل في إدراك الفاعل للأمور وسلوك الاجرامي الذي يرتكبه .[2]

* أما الارادة : فهي اتجاه السلوك الإجرامي لتحقيق النتيجة طبقا للمبادئ العامة المعروفة في قانون العقوبات قد يكون القصد الجنائي عاما أو خاصا ، القصد الجنائي العام هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود ارتكاب الفعل ، أما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه الجريمة بل يذهب إلى التأكد من تحقيق النتيجة ، فمثلا في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه ، اما في الجريمة المعلوماتية ففي الأصل الفاعل يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ، ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام إذن فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء ، ولكن هذا لا يمنع أن بعض الجرائم المعلوماتية تتوافر فيها القصد الجنائي الخاص مثلا جرائم تشويه السمعة عبر الإنترنت وجرائم نشر الفيروسات عبر شبكة الاتصال وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.[3]

---

[1] غربي جميلة ،**آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري** ، مذكرة ماستر، تخصص قانون جنائي ، قسم قانون عام،كلية الحقوق و العلوم السياسية ، جامعة أكلي محمد أولحاج ، البويرة ، الجزائر،سنة 2020-2021 ، ص14.

[2] علي عبد القادر القهوجي ، **حماية جنائية لبرامج حاسب الالي** ، دار الجامعة الجديدة ، الاسكندرية ، مصر 2010 ص120-122

[3] بخي فاطمة الزهراء ، **إجراءات التحقيق في الجريمة الإلكترونية** ، مذكرة ماستر، تخصص القانون الجنائي ، قسم حقوق ،كلية الحقوق و العلوم السياسية،جامعة المسيلة،الجزائر سنة 2013-2014 ، ص36.

الفرع الرابع : أطراف الجريمة المعلوماتية

أن أطراف ومراكز القانونية لكل جريمة هم الجاني والمجني عليه و الشاهد ، وفي الجريمة المعلوماتية هناك مجموعة من الأنواع والخصائص يتمتعون بها هؤلاء الأطراف وهي كما يلي :

أولا : الجاني أو المجرم المعلوماتي

المجرم المعلوماتي هو ذلك المجرم الذي يرتكب جرائم في البيئة الالكترونية مثل جرائم القرصنة الالكترونية وتزوير او التهديد...الخ ، ويتمتع المجرم المعلوماتي بمجموعة من الخصائص تميزه عن المجرم التقليدي وكذلك ينقسم الى فئات كل فئة وهدفها من الاجرام وعليه سنتطرق اليها كمايلي[1] :

أ) الخصائص التي يتميز بها الجاني :

*المهارات(Competences) : حيث تعتبر المهارة من أبرز خصائص المجرم المعلوماتي ويكتسبها عن طريق ممارسته في مجال تكنولوجيا المعلومات.

* المعرفة (Connaissace) : والمقصود بالمعرفة هي دراسة الجاني كل المحيط الذي يستهدفه لإرتكاب الجريمة حيث يقوم بدراسة شاملة للمحيط قبل إرتكاب جريمته ، ثم يمهد كل الأفعال التي سيقوم بها ويتوقع كل المشاكل التي سيقع فيها أثناء ارتكابه لجريمته.

* الوسيلة أو الموارد (resources) أو (les moyenes)[2] : وهو الإمكانيات التي يتزود بها الفاعل لإرتكاب جريمتة سواء من الحواسيب أو الهواتف أو أجهزة أخرى تكنولوجية.

* السلطة (l'autorité) : ويقصد بها الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته كمعرفة شفرة الدخول إلى نظام معلوماتي معين ، وكذلك تمكنه من وضع ملفات لا يمكن للغير قرأتها أو كتابتها أو تعديله ...الخ.

[1] بخي فاطمة الزهرة ، المرجع السابق ، ص16-17

[2] Béatrice Géninet , L'indispensable du droit pénal, Studyrama, 2eme édition, 2004.P33

* الباعث (Motives) : هو الدافع الذي يجعل المجرم المعلوماتي يرتكب هذا النوع من الجرائم وينقسم هذا الدافع إلى دافع شخصي مثل ظروف المجرم والتي تدفعه للكسب المال مثلا ، أو الدوافع غير الشخصية وهي كجنون العظمة أو الانتقام أو إثبات الذات..الخ.[1]

ب) فئات المجرم المعلوماتي:

وتنقسم هذه الفئات كمايلي[2]:

* صغار مجرمي المعلوماتية هم فئة مهووسون بالمعلوماتية والحسابات الآلية وكثيرا ما لفتوا النظر في الآونة الأخيرة ، ويرتكب هؤلاء المجرمين الجرائم بنية المزاح مع الاخرين دون أن تكون نيتهم إحداث ضرر بالمجني عليه وأغلبهم من الفئات العمرية الصغيرة والمراهقون.

* محترفون في الجريمة الإلكترونية (les professionals) ويتمتع أصحابها بالخبرة والدراية أكبر من الفئة الأولى وينقسمون حسب خطورتهم إلى:

أ) متسللون الهواة (Hackers) : يهتمون بسرية جرائمهم وعدم ظهورهم إلى العلن يتمتعون بإبراز خطورتهم وهدفهم التسلل دون أن يشعر بهم أحد.

ب) المجرمون الخبيثون (crackers)هم أشخاص هدفهم كسب المال وإلحاق الضرر بالمجني عليه وهم من محترفي فيروسات الحاسب الآلي.

* فئة حلالي المشاكل (les selutionneurs) : هم أكثر شيوعا هدفهم كسب المال من أجل حل المشاكل الشخصية والأزمات المالية وغالبا يستهدفون مؤسسات المالية مثل البنوك.

* فئة المجرمين المهنيين هم مجرمون يتخذونها مهنة من أجل تحقيق أرباح غير مشروعة وغالبا ما يكونون في جماعة لهم تنظيم كبير وينطبق عليهم مصطلح الجريمة المنظمة .

---

[1] عبد الحكيم رشيد توبة، **جرائم تكنولوجيا المعلومات** ، دار المستقبل للنشر والتوزيع الاردن ، طبعة الاولى 2009 ، ص162

[2] بخي فاطمة الزهراء، مرجع سابق، ص18.

* أصحاب الدعوة المتطرفة أو المتطرفون :الهدف من ارتكابهم الجرائم هو معتقداتهم الدينية والسياسية وتوجهاتهم الفكرية ، بحيث يهاجمون كل من يخالفهم ومن الأمثلة على ذلك الجماعات الإرهابية المعروفة باسم (les brigades rouge) و قاموا بتدمير ما يزيد عن 60 مركز من حاسب للحسابات الآلية للفت الانتباه لأفكارهم ومعتقداتهم.[1]

* الجناة المقصرين (Les criminal negligent) :ويعتبر الإهمال واحد من أهم المشكلات التي تواجه مجال نظام المعلوماتي ، لأن الإهمال في هذا المجال قد ترتب عنه خطورة كبيرة فمثلا في نيوزيلندا قام اثنان من المبرمجي الحسابات الالية بتغيير احد البرامج التي تحدد خطة سير احدى الطائرات ولم يبلغوا قائد الطائرة بهذا التغيير، فكانت النتيجة اصطدام الطائرة بحدى الجبال كانت الحصيلة وفاة 60 راكبا كانوا على متنها وتمت محاكمة المبرمجي بتهمة القتل الخطاء.

ثانيا : المجني عليه في الجريمة المعلوماتية

النظم المعلوماتية باعتبارها من أهم مجالات الحياة اصبحت تتحكم في مختلف قطاعات الدولة سواء العامة او الخاصة وأصبح العمل بها أمر لا مفر منه ، ولكن أصبح المجرم المعلوماتي (cybercriminel) يستعمل طرق احتيالية لاختراق النظام المعلوماتي حيث يستهدف كل المكونات المادية و المنطقية للحاسوب ، و قد يكون المستهدف إما شخص طبيعي أو معنوي وليتحقق عليه معنى مصطلح المجني عليه إلكترونيا يجب أن يمس مكونات الحاسب و معلوماته ، و ما يميز الضحية الإلكتروني عن الضحية في الجرائم العادية أن أغلب الضحايا أو المجني عليهم لا يريدون التبليغ عن الجرائم[2] التي حدثت لهم و لا يعترفون أنهم وقعوا ضحية اعتداء إلكتروني ، و خصوصا المؤسسات المالية و البنوك فإنه يجدون أنفسهم في حوار مع الجاني[3] و يكون الجاني في موقف قوة حيث إن تم التبليغ عنه فإن المؤسسة

[1] بخي فاطمة الزهراء، مرجع سابق، ص19

[2] ربيعي حسين ، مرجع سابق ، ص 42-43.

[3] حسين الغافري ومحمد الألفي ، **جرائم الانترنت بين الشريعة الاسلامية والقانون** ، دار النهضة العربية ، القاهرة ، مصر، 2008 ص 41

ستخسر أضعاف المبالغ التي تحصل عليها الجاني ،و ذلك بسبب سماع المتعاملين أن أموالهم كانت محل اعتداء فيتم سحبها فورا و ذلك يجعل المؤسسات المالية و البنوك تتحمل خسائر كبيرة لأن المعتدي يمكن له التصرف في هذه المعلومات سواء عن طريق بيعها أو إتلافها أو مقايضتها ،و ذلك يكون في السوق السوداء للانترنت فمثلا المعلومات المستقاة من بطاقة الائتمان البنكية بدون رمز سري تساوي 25 دولار أمريكي ، أما في السوق السوداء مع رمزها السري تصل إلى 500 دولار و كذلك دون أن ننسى أن هناك بعض الفئات الاخرى مستهدفة مثل الأفراد و حياتهم الشخصية و المؤسسات الأمنية للدول مختلف القطاعات فحسب مجلة ressources informatique والتي اجرت تحقيقا احصائيا وجدت الاحصائيات التالية :

19% من أفعال الغش المعلوماتي تستهدف البنوك.

16% من أفعال الغش المعلوماتي تستهدف الإدارة.

10% من أفعال الغش المعلوماتي تستهدف الإنتاج الصناعي.

10% من أفعال الغش المعلوماتي تستهدف المعلومات.

و بعد ذلك تأتي شركات التأمين و الشركات الخاصة و في الواقع نجد الجريمة المعلوماتية في المقام الأول تستهدف المؤسسات المالية التي تتحكم في القيم الرأس مالية ، و على سبيل المثال فإن البنوك الأمريكية فقدت ما قيمته 90 مليون دولار سرقات في الجرائم التقليدية بينما خسرت قيمة 12 مليار دولار في الجرائم المعلوماتية ، وكذلك حسب موقع[1] (Francois sopin) فإن دولة إسرائيل أو الكيان الاسرائيلي تعتبر أول دولة من حيث الهجمات والاعتداءات الإلكترونية حيث تقدر عدد الهجمات بـ 1000 اعتداء في الدقيقة الواحدة ، ثم تليها الولايات المتحدة الأمريكية و كل الدول التي تتمتع بنظام الرأس مالي في مؤسساتها المالية ، وقد قدر مخبر (Norton) للأمن المعلوماتي الخسائر

[1] Francois sopin-rapport sur l'a actualite de cyber criminalite en 2012 date de consultation : 21/04/2022 a 3 :00 am.

الاقتصادية بالنسبة للعالم ، بـ 110 مليار دولار أمريكي نتيجة الاعتداءات المعلوماتية وكذلك معهد (Week research) سنة 2000 أعد تقريرا إحصائيا يفيد تسجيل خسائر مقدرة 1600 مليار دولار نتيجة الوقت الضائع عن تعطيل الأنظمة المعلوماتية بسبب هذه الاعتداءات ، أي ما قيمة 3.3 من قيمة وقت العمل وكذلك تقرير المكتب الأمريكي الفدرالي FBI و بالتعاون مع مركز lic3 الخاص بشكاوي كانت الخسائر 264 مليون دولار سنة 2008 ثم في سنة 2009 قدرت بـ 559.7 مليون دولار أي في ظرف سنة زادت الخسائر بالضعف ،و كذلك عدد الشكاوي كان في سنة 2008 يقدر بـ 275.224 ثم في سنة 2009 قدرت بـ 336.655 أي زيادة بـ 22% أما على المستوى الوطني ففي الجزائر حسب غرفة التحقيق على مستوى محكمة سيدي محمد بالجزائر العاصمة سنة 2012 كان هناك 21 اعتداء إلكتروني استهدف الإدارات العمومية بنسبة 60% ، بينما سجلت 7 اعتداءات ضد الأنظمة المعلوماتية للشركات الخاصة ، وبهذا يمكننا تصور حجم الخسائر التي تسببها الجريمة المعلوماتية وحجم الأضرار التي تعود عليها للمجتمع و الدولة على حد سواء.[1]

ثالثا : الشاهد في الجريمة المعلوماتية :

سماع الشهود هو أجراء من اجراءات التحقيق يهدف لجمع الأدلة المتعلقة بالجريمة بحيث يستدعي أشخاص ليس لهم علاقة بالجريمة ، إلى ان وجودهم ضروري للكشف عن الجرائم و القبض على مرتكبيها و تخلف الشاهد عن الحضور للإدلاء بشهادته يعرضه للمسائلة الجنائية ،و قبل تعريف الشاهد يجب علينا معرفة الشهادة أولا ثم معرفة ما يميز الشاهد التقليدي عن الشاهد الإلكتروني[2].

أ) **تعريف الشهادة** : تعددت التعاريف لدى الفقهاء فيما يخص الشهادة فهناك من يعرفها على أنها الأقوال التي يدلي بها الخصوم أمام سلطة التحقيق أو الحكم في شأن جريمة وقعت سواء تتعلق بثبوت الجريمة و ظروف ارتكابها أو إسنادها إلى المتهم أو براءته منها ، وهناك من يعرفها أنها إثبات واقعة معينة

[1] **ربيعي حسين**، مرجع سابق، ص44.

[2] بخي فاطمة الزهراء، مرجع سابق، ص61.

من خلال ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه عن هذه الواقعة بطريقة مباشرة و للشهادة ثلاثة أنواع :[1]

* **الشهادة المباشرة** : و هي أن يشهد الشاهد بما شاهده أو وقع تحت سمعه

* **الشهادة السماعية** : هي سماع شاهد فرعي لشاهد أصلي حيث يروي عنه ما شاهده أو سمعه و هي أقل شأنا من الشهادة الأصلية المباشرة.

* **الشهادة بالتسامع** : وهي شهادة تختلف عن الشهادة السماعية حيث تتعلق هذا الأخيرة بشهادة نقلت عن شخص معين قد شاهد الأمر بنفسه ، أما الشهادة بالتسامع هي نقل واقعة معينة لكنها ليست نقلا عن شخص معين بالذات و إنما يتداولها الناس فيما بينهم و يقولون سمعنا أو شاهدنا عن فلان كذا و كذا من هذه الواقعة.

ب) الشهادة الإلكترونية :

هناك من عرف الشاهد الالكتروني على انه الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي ، و الذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات ويمكن القول أن الشاهد الإلكتروني هو كل من :

* مشغلو الحاسب الآلي هو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به حيث تكون لديه الخبرة في مجال الحاسب الآلي.

* خبراء البرمجة هم الأشخاص المتخصصون في كتابة أوامر البرامج وينقسمون إلى فئتين الأولى هم مخططوا برامج التطبيقات والثانية هم مخططو برامج النظم.

[1] عبد الرحمان خلفي، **محاضرات في القانون الاجراءات الجزائية** ،دار الهدى ،عين مليلة ، جزائر ، طبعة الثانية ، 2010 ص 175

* مهندسو الصيانة واتصالاتهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب ومكوناته وشبكات الاتصال المتعلقة به.[1]

* مديرو النظمهم الذين توكل لهم أعمال الإدارة في النظم المعلوماتي.

* المحللون : هم الأشخاص الذين يحللون الخطوات ويقومون بتجميع البيانات الخاصة بنظام معين ، ودراسة هذه البيانات ثم تحليل النظام(تقسيمه) إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات ، كما ان يتتبعوا البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات ، واستنتاج الأماكن التي يمكن تحددها بواسطة الحاسوب.[2]

المطلب الثاني : تصنيف الجريمة المعلوماتية و سبل مكافحتها

مع ظهور الجريمة المعلوماتية و تطورها أصبح من الواجب دراستها قانونيا و تصنيفها وفق ما جاء به الفقهاء ، و كذلك نظرا لخطورتها على المجتمع و الدولة ككل استوجب مكافحتها في تشريع الدولي و الإقليمي و الوطني ، وبهذا قسمنا هذا المطلب الى فرعين الاول تصنيف الجريمة المعلوماتية والثاني سبل مكافحتها.

الفرع الأول : تصنيف الجريمة المعلوماتية

الجرائم الإلكترونية متعددة و متنوعة و نظرا لتطورها السريع لا يمكن حصرها بسهولة في تعريف واحد و ذلك للاختلاف عدة معايير من أجل تصنيفيها ، فهناك من يصنفها حسب الجرائم التي ترتكب على نظام الحاسوب و البعض الأخر يصنفها إلى الجرائم التي ترتكب بواسطته ، و آخرون يصنفونها إلى الاسلوب المتبع أو الباعث أو الدافع للارتكاب هذه الجرائم و غير ذلك من التصنيفات التي سنتطرق إليها كما يلي:

[1] خالد الممدوح ابراهيم ،**فن التحقيق الجنائي في الجريمة الالكترونية** ،دار الفكر الجامعي ،الاسكندرية ،مصر 2009 ص22

[2] بخي فاطمة الزهراء، مرجع سابق،ص44.

أولا : تصنيف الجريمة المعلوماتية تبعا لنوع المعطيات و محل الجريمة

ينقسم هذا التصنيف الى عدة جرائم وهي ما يلي :[1]

أ) الجرائم الماسة بقيمة معطيات الحاسوب :

و تضم قسمين الأول الجرائم الواقعة على المعطيات نفسها كجرائم الاتلاف و تشويه البيانات كاستخدام الفيروسات الخبيثة ، و القسم الثاني ما تمثله هذه المعطيات من قيمة مالية من أموال و أصول كجرائم الغش الحاسوب التي تستهدف الحصول على المال غير المشروع ، أو جرائم الاتجار بالمعطيات أو جرائم التلاعب بالمعطية المخزنة داخل نظام الحاسوب كتزوير المستندات و معالجتها آليا.

ب) الجرائم الماسة بالمعطيات الشخصية:

تضم البيانات المتعلقة بالحياة الخاصة للأفراد كالإطلاع على المراسلات و المحادثات و التجسس على حرمة الحياة الخاصة .

ج) الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب و ونظامه :

تضم الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب و ونظامه (جرائم قرصنة البرمجيات) والمقصود بذلك هو هناك بعض الشركات التي تنتج برامج الحاسوب كبرامج الكتابة أو برامج التخزين أو برامج تقديم الخدمات لمستخدميها ، إلا انه هناك اعتداءات تقع عليها كتقليدها أو نسخها أو إعادة بيعها دون رخصة و كل هذه الأفعال و التصرفات تشكل اعتداءات على الملكية الفكرية.[2]

ثانيا : تصنيف الجريمة المعلوماتية تبعا لدور الكمبيوتر في الجريمة

إن هذا التصنيف يبين أن الكمبيوتر يكون كوسيلة أو هدفا لارتكاب الجريمة و المقصود بأن يكون هدفا هو أن يستهدف الفعل الإجرامي المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر و شبكات الاتصال ، و المقصود بأن يكون وسيلة مثل جرائم الاحتيال ببطاقة الائتمان و التزوير وكذلك يكون جسرا لارتكاب جرائم أخرى كالمتاجرة بالمخدرات و غسيل الأموال مثلا ، وفي هذا الصدد ينتج عن دور

[1] يزيد بوحليط ، المرجع السابق ، ص 60

[2] نفس المرجع ، ص62.

الكمبيوتر في الجريمة مفهومين هما الأول يتعلق بجرائم التخزين و الثاني يتعلق بجرائم المحتوى ، و المقصود بجرائم التخزين هو تخزين المواد الإجرامية المستخدمة في إرتكاب الجريمة و الناشئة عنها ، أما جرائم المحتوى أو ما يعبر عنه بالمحتوى الغير المشروع مثل جرائم المقامرة(القمار) أو جرائم المحتوى الإباحية و الغسيل للأموال الإلكتروني[1]، فكلها تنصب على المحتوى الغير المشروع و بهذين المفهومين اللذان يتصلان بدور الكمبيوتر و شبكة الاتصال كبيئة لارتكاب الجريمة المعلوماتية أو في الوقت نفسه كوسيلة لارتكابها ،و مع تطور التدابير التشريعية في أوروبا و العالم قسم أغلب المشرعين هذه الجرائم إلى جرائم هدف و وسيلة و محتوى للكمبيوتر ، ومن أهمها اتفاقية بودبست لسنة 2001[2] وذلك في إطار خلق نوع من التعامل الدولي في مجال مكافحة الجريمة المعلوماتية ، و قد جاء في هذه الاتفاقية ما يلي :[3]

* الجرائم التي تستهدف العناصر السرية و سلامة المعطيات و النظم و تتمثل في الدخول الغير القانوني و تدمير هذه المعطيات.

* الجرائم المرتبطة بالكمبيوتر مثل التزوير المعلوماتي.

* الجرائم المرتبطة بالمحتوى و تضم الجرائم المتعلقة بالإباحية و الأفعال الغير الاخلاقية.

* الجرائم المرتبطة بحق المؤلف و الحقوق المجاورة مثل قرصنة البرمجيات.[4]

ثالثا : تصنيف الجريمة المعلوماتية تبعا لمساسها بالأشخاص و الأموال

يوجد هذا التصنيف في الدراسات و الأبحاث الأمريكية و أبرز تقسم في هذا الصدد هو ذلك التقسيم الذي جاء في مشروع القانون النموذجي لجرائم الكمبيوتر و الانترنت لسنة 1992 ، من قبل فريق أكاديمي أطلق عليه اسم(model state computer) و لقد قسم هؤلاء الباحثين هذا الصنف إلى جرائم واقعة على الأشخاص و على الأموال.

---

[1] يزيد بوحليط ، نفس المرجع، ص64.

[2] اتفاقية بودابست المؤرخة في 23نوفمبر.2000

[3] يوسف حسين يوسف ، **الجريمة الدولية للانترنت** ، المركز القومي الاصدرات القانونية ، القاهرة ، مصر ، الطبعة الاولى ،2011 ص 37

[4] عادل عزام ، سقف الحيط ،**جرائم الذم والقدح والتحقير المرتكبة في وسط الالكتروني** ، دار الثقافة للنشر والتوزيع ، عمان ؛ الاردن طبعة الاولى 2011 ص 123

أ) قسم الجرائم التي تستهدف الأشخاص :

ويضم نوعان الأول الجرائم الغير جنسية التي تستهدف الأشخاص كالقتل بالكمبيوتر و التسبب بالوفاة و جرائم الإهمال المرتبطة بالكمبيوتر و التحريض على الأنتحار أو التهديد أو الابتزاز أو المضايقة أو التحريض على القتل و غيرها ، من الجرائم التي تشكل خطر على حياة و سلامة الأفراد والثاني الجرائم الجنسية و تشمل الاستغلال الجنسي للقصر أو نشر صور الأشخاص في أوضاع خاصة و محتشمة أو نشر مواد إباحية عبر الأنترنت و الترويج للجرائم التي تخدش الحياء العام و الآداب العامة.

ب)قسم الجرائم التي تستهدف الأموال

وهي بالمفهوم المختصر الجرائم التي تستهدف الموارد المالية الإلكترونية أو المال الإلكتروني وذلك عن طريق التلاعب بالمعلومات و المعطيات و معالجتها بواسطة الكمبيوتر ، و من أهم هذه الجرائم هي جرائم الاحتيال و السرقة و جرائم التزوير وجرائم ضد الاخلاق وجرائم ضد الحكومة ، والمقصود بالأولى هي التلاعب بالمعطيات و النظم من أجل الحصول على الأموال الإلكترونية ،فمنها الاستيلاء على البطاقات المالية للغير أو قرصنة البرامج و سرقتها أو سرقة بعض الخدمات أو سرقة كلمة المرور للحسابات البنكية.. الخ ،و المقصود بالثانية هي تلك الجرام التي تشمل التزوير البريد الإلكتروني و الوثائق و السجلات المتعلقة بالهوية ، والمقصود بالثالثة جرائم المقامرة على الانترنت و ترويج للكحول و مواد الإدمان للقصر، والمقصود بالأخيرة كل تشويش على الأعمال الحكومية و تنفيذ القانون و تعطيل الإبلاغ عن الجرائم و الحصول على المعلومات السرية...الخ،من الجرائم التي تمس مؤسسات الدولة و إستقرارها.[1]

[1] يزيد بوحليط ، المرجع السابق ص 65

رابعا : تصنيف الجريمة المعلوماتية على أساس جرائم كمبيوتر و جرائم الانترنت

قبل ظهور شبكة الانترنت كان موجودا نمط محصور من الجرائم المعلوماتية لأنها كانت مرتبطة بالحاسوب فقط ، لكن مع التطور المذهل في هذا المجال تحقق ما يسمى بدمج بين الكمبيوتر و شبكة الإتصال أي بين الحوسبة و الإتصال مما جعل البعض يصف كل جريمة على حدى و هذا ما يعتمده هذا التصنيف، حيث يرى أنه هناك جرائم تتصل بالكمبيوتر و جرائم تتصل بالانترنت و من الجرائم التي تتصل بالانترنت هي التي تستهدف في استخدامها الأنترنت و ما يقع في بيئتها مثل جرائم الاعتداء على المواقع و تشويهها أو تعطيل الخدمات أو الترويج إلى المحتوى الضار، أما جرائم الكمبيوتر فهي الأنشطة التي تستهدف المعلومات و البرامج المخزنة داخل نظام الكمبيوتر وكذلك سرقة المعطيات ، و ما يعيب هذا التقسيم أنه مع التطور أصبح من الصعب الفصل بين نظام الحوسبة و نظام الإيصال هذا من جهة و من جهة أخرى أنه هناك من المفاهيم و التعريفات قد جمعت بين الحاسوب و كل ما يمس بمكوناته المادية و المعنوية و كل ما يتصل به.[1]

الفرع الثاني : سبل مكافحة الجريمة المعلوماتية

إن مكافحة الجريمة المعلوماتية أصبح أمرا ضروريا سواء على المستوى الدولي أو على المستوى الوطني وبالفعل لقد تحرك المجتمع الدولي و الوطني على حد سواء ، من أجل تشريع نصوص قانونية موضوعية و إجرائية لمكافحة هذه الظاهرة باعتبارها ماسة بأمن و مصلحة الدول و سوف نتطرق في هذا الفرع وباختصار شديد إلى أهم الجهود الدولية و الإقليمية و الوطنية من أجل مكافحة الجريمة المعلوماتية.

أولا : الجهود الدولية في مكافحة الجريمة المعلوماتية

أ) جهود منظمة الأمم المتحدة(L'ONU):

لقد حاولت هذه المنظمة بذل جهود لمكافحة الجريمة المعلوماتية و الأضرار الناجمة عنها وأولها كان مؤتمر الثامن حول منع الجريمة و معاملة المجرمين ،حيث أصدر قرارات متعلقة بجرائم الحاسوب و أشار القرار إلى

[1] **يزيد بوحليط** ، مرجع سابق ، ص68.

أن الإجراء الدولي لمواجهة الجرائم المعلوماتية يتطلب من دول الأعضاء اتخاذ عدة اجراءات و منها[1]:

* أن تكون القوانين دوما قابلة للتجديد و التحديث بما يتناسب مع كل جديد لهذه الجريمة.
* اتخاذ تدابير الأمن و الوقاية مع احترام خصوصية الأفراد و حقوق الإنسان.
* توعية المجتمع و القضاء و كل العاملين في هذه الأجهزة لخطورة هذه الجرائم و مكافحتها.
* التعاون مع المنظمات المهتمة بهذا الموضوع.
* حماية مصالح الدولة و حقوق الضحايا في الجرائم المعلوماتية.[2]

و بعد تزايد عدد الجرائم المعلوماتية عقدت هذه المنظمة اتفاقيات الخاصة بمكافحة استعمال التكنولوجيا لأغراض إجرامية سنة 2000 ، و أكدت على تعزيز و تنسيق التعاون الدولي لمكافحة هذه الجريمة ، وكذلك مؤتمر الثاني عشر لمنع الجريمة و العدالة الجنائية بالبرازيل بتاريخ 12 و 19 أبريل 2010 قامت بدراسة كل ما هو جديد في الجريمة المعلوماتية ، و ناقشت فيه دول الأعضاء كل التطورات الأخيرة في الجريمة المعلوماتية و الوسائل المستحدثة فيها و دعت إلى تأسيس فريق من الخبراء حكومي دولي مفتوح العضوية لدراسة شاملة و معمقة لمشكلة الجريمة السيبرانية و التصدي لها.

ب) **منظمة التعاون الاقتصادي و التنمية (OCDE)** :

تهدف هذه المنظمة إلى التطور الاقتصادي و تحقيق أعلى مستويات التنمية الاقتصادية و الاجتماعية وحماية كل الموارد الاقتصادية و لقد حاولت تجريم الجريمة المعلوماتية باعتبارها تمس باقتصاد الدول ، و قد اهتمت بالجرائم المرتكبة عبر الأنترنت سنة 1978 و أصدرت هذه المنظمة تقرير سنة 1983 بعنوان الجرائم المرتبطة بالحاسوب ، و لقد تضمن هذا التقرير تحليلا لسياسة الجنائية و تحديد قائمة من المقترحات الخاصة بدول الأعضاء و تنص فيها على الحد الأدنى للأفعال المسيئة للحاسوب و التي يجب

[1] صغير يوسف ، **الجريمة المرتكبة عبر الانترنت** ، مذكرة ماجيستر ، تخصص قانون دولي للأعمال ، قسم حقوق ،كلية الحقوق و العلوم السياسية،جامعة مولود المعمري ، تيزي وزو ، الجزائر ،2013 ، ص 93-94.

[2] اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية من طرف الجمعية العامة لمنظمة الامم المتحدة يوم 2000/11/15 صادقت عليها الجزائر بتحفظ موجب المرسوم الرئاسي رقم 04-165 المؤرخ 2004/6/8

على الدول أن تجرمها بنصوص و عقوبات خاصة ، و من بين هذه الأفعال الاستخدام أو الدخول إلى نظام و مصادر الحاسب على النحو غير مصرح به ، و تشمل الحاسوب و معلوماته المخزنة داخله وكذلك الإفشاء غير المصرح به للمعلومات المعالجة آليا وكذلك نسخ و إتلاف أو تخريب ما تحتويه من بيانات و برامج محمية قانونا.[1]

ج) منظمة العالمية للملكية الفكرية (l'ompi) :

هي منظمة عالمية دولية و ومن ضمن احدى الوكالات التابعة لمنظمة الامم المتحدة تعمل على حماية حقوق الملكية الفكرية ، ظهرت في سنة 1967 وتأسست سنة 1970، ومقرها في العاصمة الإدرية السويسرية بران[2] ، ولقد نصت على ضرورة تطوير تشريعاتها وخاصة تشريعات حق المؤلف وكذلك تسليط عقوبات على كل اعمال التزوير في العلامات التجارية والقرصنة المعتمدة والمرتكبة في اطار تجاري ، وبالطبع مع تطور التجارة الالكترونية وبرامجها اصبحت الأماكن الافتراضية أرضية خصبة لمثل هذه الجرائم وعليه حاولت هذه المنظمة سن قوانين من اجل حماية هذه البيئة وأهم المواد التي جاءت بها المادة الرابعة من معاهدة المنظمة العالمية للملكية الفكرية والمعتمدة في سنة 1996 على ما يلي:

" تتمتع برامج الحاسوب بالحماية باعتبارها منصات أدبية في وهذا في معنى المادة الثانية من اتفاقية بران ، وتطبق على برامج الحاسوب ايا كانت الطريقة التعبير عنها أو شكلها ، وتنص المادة الخامسة على أنه تتمتع مجموعات البيانات او المواد الاخرى بالحماية بصفتها هذه ايا كان شكلها اذ كانت تعتبر ابتكارات بسبب اختيار محتوياتها "

وبعد استقراء هذه المواد نفهم انه تم حماية برامج الحاسب الالي والنظم المعلوماتية وأصبحت من المصنفات الادبية المحمية عن طريق الملكية الفكرية .[3]

---

[1] صغير يوسف ، المرجع السابق، ص97-98.

[2] اتفاقية بران لحقوق المؤلف لسنة 1882 المعدلة والمتممة ، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 341/97 المؤرخ في 1997/09/13 (ج.ر) العدد 61 المؤرخة في 1997/09/14 .

[3] صغير يوسف، المرجع السابق، ص99.

ثانيا : جهود الهيئات والمنظمات الاقليمية في مكافحة الجريمة المعلوماتية :

تتمثل الجهود الاقليمية في مكافحة الجريمة المعلوماتية كما يلي

أ) الاتحاد الاوروبي :

توجهت جهود الاتحاد الاوروبي ومجلس الاوروبي إلى صدور إتفاقية بودابست لمكافحة الجريمة المعلوماتية وكان هدفها تحقيق وحدة التدابير التشريعية بين الدول الاوربية والتأكيد على اهمية التعاون الاقليمي والدولي في ميدان مكافحة الجريمة المعلوماتية ، وكذلك تحقيق التوازن بين حقوق الانسان و الاجراءات المتخذة لمواجهة هذه الجريمة حيث تقدم هذه الاتفاقية دليلا ارشاديا لتطوير القوانين والتشريعات ، وتقوم كذلك بتعريف وتحديد العقوبات التي يجب تسلطها على مرتكبي هذه الجرائم وانعقدت هذه الاتفاقية من طرف مجلس الاوروبي بالتعاون مع اليابان وجنوب افريقيا والولايات المتحدة الامريكية وعرضت لتوقيع في بودابست عاصمة المجر سنة 2001 ودخلت حيز التنفيذ عام 2004.[1]

ب) على مستوى العربي :

بعد انتشار صدى الجريمة المعلوماتية في الدول العربية حاولت هذه الدول ايجاد قوانين موضوعية وإجرائية لواجهة هذه الجريمة ، ومن اهم تلك الجهود القرار الصادر عن مجلس وزراء العدل العرب والذي اصدر القانون الجزائي الموحد وهد القانون يعتبر قانون نموذجي[2] عربي ، حيث نجد في الباب السابع الخاص بالجرائم ضد الاشخاص في مواده 461-464 والتي تنص على حماية حرمة الحياة الخاصة وأسرار الافراد من خطر المعالجة الالية للمعلومات ، وكيفية الاطلاع عليها والعقوبات المطبقة على مرتكبي هذه الجريمة ،وكذلك في مجال الملكية الفكرية تم إبرام الإتفاقية العربية لحماية حقوق المؤلف حيث أكدت

[1] **بغاديد نابية** ، المرجع السابق 43

[2] الاتفاقية العربية لمكافحة الجرائم تقنية المعلوماتية المحرر بالقاهرة بتاريخ 2010/12/21 صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14-258 المؤرخ في 2014/9/8.

هذه الاتفاقية على ضرورة توفير حماية قانونية للبرامج المعلوماتية وكل المؤلفات التي تقع في البيئة الكترونية باعتبارها ملكية فكرية .[1]

ثالثا : الجهود الوطنية في مكافحة الجريمة المعلوماتية

ان الجزائر مثلها مثل الدول العالم لم تسلم من الجريمة المعلوماتية وأضرارها من ما استوجب على المشرع الجزائري التدخل وسن قوانين موضوعية وإجرائية مستمدا ذلك من الاتفاقيات والمؤتمرات الدولية ، ومن اهم القوانين التي جاء بها المشرع الجزائري كما يلي[2] :

أ) قانون العقوبات :

ان اهم التعديلات التي قام بها المشرع الجزائري في قانون العقوبات لمواجهة الجريمة المعلوماتية هو التعديل قانون 15/04 المؤرخ في 10 نوفمبر 2004 في القسم السابع مكرر من الفصل الثالث من الباب الثاني من الكتاب الثالث من الجزء الثاني من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات ، في ثمانية مواد من المادة 394 مكرر الى 394 مكرر 7 ومن امثلة على هذه الأفعال المجرمة جريمة التواصل أو الدخول الغير مصرح به في المنظومة المعلوماتية ، و جريمة التزوير المعلوماتي وجريمة الاستيلاء على المعطيات ، وجريمة اتلاف وتدمير المعطيات ، وجريمة الاحتيال المعلوماتي ..الخ من الجرائم المنصوص عليها في هذا القانون.[3]

---

[1] صغير يوسف، مرجع سابق، ص100.

[2] بن نعوم خالد أمين، **إجراءات التحقيق في الجريمة المعلوماتية في التحقيق الجزائري** ، مذكرة ماستر ، تخصص فضائي ،قسم الحقوق،كلية الحقوق و العلوم السياسية ، جامعة عبد رالحميد بن باديس ،مستغانم ،الجزائر،سنة 2018-2019 ، ص37-38.

[3] انظر في المادة 394 مكرر ال ى المادة 394 مكرر 08 من القانون رقم 15/04 الصادر في 2004/11/10 يعدل ويتمم الامر رقم 66-156 المؤرخ في 08 يونيو 1966 والمتضمن قانون العقوبات (ج ر) العدد 71 المؤرخة في 2004/11/10.ص54.

ب) في قانون الاجراءات الجزائية :

نجد أن المشرع نص على العديد من الاجراءات مثل تمديد الاختصاص المحلي لوكيل الجمهورية في جرائم الإلكترونية في المادة 37 ،كذلك نص على التفتيش في المادة 45الفقرة 7 ،و توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51الفقرة 6 ، ونص على اعتراض المراسلات وتسجيل الأصوات و الصور من المادة 65مكرر 5 إلى 65مكرر 10 أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليه نفس إجراءات الجريمة التقليدية،و سنتطرق لهذه الإجراءات بالتفصيل.

ج) في قانون 04/09 للوقاية من جرائم المتعلقة بتكنولوجيا الاعلام والاتصال ومكافحتها:

ان قانون الوقاية من جرائم المتعلقة بتكنولوجيا الاعلام والاتصال ومكافحتها رقم 04/09 المؤرخ في 14 شعبان 1430 الموافق 2009/08/05 ، نص على بعض الاجراءات لمكافحة الجريمة المعلوماتية وكذلك قام بتعريف بعض المصطلحات التي لها علاقة بهذه الجريمة فمثلا في [1]المادة 2 إلى مادة 14 نجد ان هذا القانون أوضح مفهوم الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ، وكذلك مفهوم المنظومة المعلوماتية ومعطيات المعلوماتية ومقدمو الخدمات ،و كذلك بعض الاجراءات مثل مراقبة الاتصالات الالكترونية وقواعد التفتيش المنظومة المعلوماتية وحجز المعطيات المعلوماتية والتزامات مقدمي الخدمات ومساعدة السلطات ... الخ ، من الاجراءات التي سنتطرق لها في الفصل الثاني من هذه الدراسة.[2]

د) في بعض النصوص والتنظيمات الاخرى :

لم يكتفي المشرع بقانون العقوبات والإجراءات الجزائية بل حاول تمديد هذه الحماية الى جميع الميادين والقطاعات وذلك عن طريق النصوص القانونية المنظمة لهذه القطاعات وهي كمايلي:

[1] انظر إلى المادة 14 القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، (ج ر) العدد 47 المؤرخة في 2009/08/16.ص8

[2] فليح نور الدين،**الجريمة الإلكترونية و آلية مكافحتها في التشريع الجزائري** ، مذكرة ماستر، تخصص القانون الجنائي قسم الحقوق،كلية الحقوق و العلوم السياسية ، جامعة الدكتور مولاي الطاهر،سعيدة،الجزائر،سنة 2018-2019 ، ص97

* قانون 2000-03 المؤرخ في 2000/08/05 المتعلق بالبريد والموصلات السلكية ولا سلكية والذي ينظم التحويلات المالية عن طريق الالكترونيات[1] ولقد نص في مادة 87 كيفية العمل وتحويل المال المعلوماتي ، ولقد خصص المشرع في الفصل الثاني تحت عنوان الاحكام الجزائية من المادة 127 إلى 144 حماية لهذه المعلومات فمثلا في المادة 127 تنص على معاقبة كل من يخرب عمدا أو يتلف أو يحول أو ينتهك سرية هذه المرسلات والمعلومات وبهذا قد حاول المشرع حماية البريد والموصلات من كل تلاعب بالمال المعلوماتي.[2]

* في نصوص التي تنظم الملكية الفكرية مثل البرامج المعلوماتية التي تعتبر من العلامة التجارية أو المواقع التجارية أو براءة الاختراع والملكية الصناعية ...الخ

* قانون رقم 08-01 المؤرخ في 2008/01/23 والمتمم لقانون رقم 83 -01 المتعلق التأمينات الاجتماعية .[3]

[1] فليح نوردين ، المرجع السابق ص 98

[2] انظر مواد 127 إلى 144 من القانون 2000/03 الصادر في 2000/08/05 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية (ج ر) العدد 48 المؤرخة في 2000/08/06.ص 23 -24

[3] انظر الى المادة 93 مكرر القانون 01 -08 المؤرخ في 23/ 01 / 2008 والمتمم للقانون رقم 01-83 متعلق بالتأمينات ، (ج.ر) ، العدد 04 ، المؤرخة في 27 /01 /2008 . ص 05

المبحث الثاني : إجراءات التحقيق في الجريمة المعلوماتية

يعتبر التحقيق من أهم الإجراءات التي تتخذ بعد وقوع أي جريمة ، ولتحقيق في أي جريمة لابد أن يمر على مجموعة من المراحل ، ولكل مرحلة من هذه المراحل هناك من يشرف عليها ، وذلك من أجل تحقيق التوازن بين مصلحة العدالة في كشف الجريمة ، و ضمان أقصى حد من الحريات الأساسية لحقوق الانسان ، حيث كل من يشرف على هذه المراحل يجب أن يتمتع بمهارات وذكاء ودقة الملاحظة وخصوصا إذا كان التحقيق يواجه جريمة من جرائم المعلوماتية ، لأن هذه الاخيرة لا يكمن لمحقق التقليدي أن يحقق فيها بسبب ما تتميز به الجريمة المعلوماتية من جانب قانوني وجانب التقني وفني ، ولا يمكن للمحقق كشف هذه الجريمة بدون الاستعانة بأجهزة تساعده للوصول إلى الحقيقة ، حيث هذه الأجهزة التي تساعد المحقق نجدها على مستوى الدولي والإقليمي والوطني ،وعليه تم تقسم هذا المبحث إلى مطلبين : **الأول** المراحل التي يمر بها التحقيق و صعوباته ، **والثاني** يتمثل في الأجهزة التي تساعد التحقيق في هذه المراحل ، وعليه سنتطرق في المطلب الأول مراحل التحقيق في الجريمة المعلوماتية ، وفي المطلب الثاني الاجهزة المكلفة بالبحث وتحري في الجريمة المعلوماتية .

المطلب الاول : مراحل التحقيق في الجريمة المعلوماتية وصعوباته

يمر التحقيق بعدة مراحل عديدة حيث المرحلة الاولى تتمثل مرحلة جمع الاستدلالات ثم مرحلة التحقيق الابتدائي ثم مرحلة المحاكمة وسنتطرق إلى كل هذه المراحل والصعوبات التي تصادفها.

الفرع الاول : في مرحلة البحث و التحري

تعتبر مرحلة البحث و التحري أو مرحلة جمع الاستدلالات مرحلة تمهيدية لكشف الغموض عن الجريمة و جمع أقصى عدد ممكن من الادلة التي تساعد في كشف الجاني ، حيث بالنسبة للجريمة التقليدية فالتحقيق لا يواجه مشكلة لأن الجاني في أغلب الأحيان يترك أثارا تؤدي إلى [1]كشفه ، أما في الجريمة المعلوماتية فإن التحقيق يوجه بعض الصعوبات وذلك بسبب نقص الخبرة المحقق في مجال المعلوماتي من جهة ، ومن جهة أخرى الجاني يرتكب جرائم في العام الافتراضي و تتحقق النتيجة في العالم الحقيقي.

وعليه استوجب على الدول استحداث بعض اجراءات التحقيق و تطويرها بكل الوسائل ،التي يمكن أن تساعد التحقيق في هذا النوع من الجرائم حيث استوجب الدمج بين خبرة المحقق في العالم الحقيقي وأصحاب الخبرة الفنية للحاسب الآلي و شبكة الانترنت ، و تعتبر الضبطية القضائية هي من تتولى مهام البحث و التحري و جمع الاستدلالات ولهذا سنعرف الضبطية القضائية ثم تحديد الاجراءات التي تتبعها في هذه المرحلة

أولا: تعريف الضبطية القضائية

الضبطية القضائية هم فئات من الموظفين أوكلهم المشرع مهمة جمع الاستدلالات حول الجرائم و مرتكبيها تحت ادارة و اشراف النيابة العامة ، فهم ليسوا أعضاء في السلطة القضائية بل هم جهاز تابع للسلطة التنفيذية و يخضعون بحكم وظائفهم لسلطة رؤسائهم الاداريين تحت وصاية الوزارة التي يتبعون لها ، لكنهم في نفس الوقت يقومون بوظيفة الضبط القضائي و هم على إتصال دائم بالنيابة

[1] علي شملال، **المستحدث في قانون الاجراءات الجزائية الجزائري** ،الجزءالأول:الإستدلال والاتهام ، دار الهوما للطباعة و النشر و التوزيع، الجزائر، الطبعة الرابعة ،2019-2020

العامة وذلك لأن النيابة العامة هي التي تدير و تشرف على موظفي الضبطية القضائية في حدود ما يتعلق بالمهام القضائية فقط ، فالنيابة العامة باعتبارها جهة قضائية خول لها المشرع سلطة الاتهام و الدفاع عن المجتمع فلا يمكن تصور مباشرة مهامها بدون جهاز إداري يساعدها في كشف عن هذه الجرائم ، و تعقب مرتكبيها و ضبط الأدلة التي لها علاقة بالجريمة و إعطاء صورة عن ظروفها و ملابساتها و من خلال هذا الجهاز و المتمثل في الشرطة القضائية تتمكن النيابة العامة بالتصرف في نتائج الاستدلال التي وصل إليها هذا الجهاز ، و بذلك فإن المشرع الجزائري قد نظم الضبطية القضائية بموجب قانون الاجراءات الجزائية من المادة 12 إلى 28 ومنح صفة الضبطية القضائية في المادة 15 إلى كل من : [1]

* رؤساء المجالس الشعبية البلدية .

* ضبط الدرك الوطني .

* الموظفون التابعون للأسلاك الخاصة للمراقبين ومحافظي وضباط الشرطة للأمن الوطني .

* ضباط الصف الذين أمضوا في سلك الدرك الوطني ثلاثة سنوات ،على الأقل وتم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ، حافظ الاختام و وزير الدفاع الوطني ، بعد موافقة لجنة خاصة.

* الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ و أعوان الشرطة للأمن الوطني الذين أمضوا ثلاث سنوات على الأقل بهذه الصفة ، والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية وجماعات المحلية بعد موافقة لجنة الخاصة .

* ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك الصادر عن وزير الدفاع و وزير العدل .

[1] انظر إلى مادة 15 من القانون ، رقم 10/19 الصادر في 11 ديسمبر سنة 2019 ، المتضمن الاجراءات الجزائية ، (ج ر) ، العدد 78 ، المؤرخة في 18 ديسمبر 2019 ص 12.

ثانيا : مهام الضبطية القضائية

تتمثل مهام الضبطية القضائية في مرحلة جمع الاستدلالات في ما يلي :

أ) تلقي الشكاوي و البلاغات

بصورة عامة الشكاوي والبلاغات هي إخبار السلطة المختصة عن وقوع جريمة أو أنها على وشك الوقوع أو هناك إتفاقا جنائيا على إرتكابها ، ولابد من المبلغ و متلقي البلاغ أن يكون لديهم معرفة مقبولة بالجوانب الفنية للحاسب الآلي و شبكة الأنترنت حتى يتمكن المبلغ بتقديم معلومات تصف الحادث بشكل جيد ، وفي نفس الوقت يتمكن متلقي البلاغ فهم هذه المعلومات و تحليلها لمعرفة جميع ملابسات الجريمة وعليه يجب المرور ببعض الخطوات ، أولها تحديد المعلومات ثم وضع خطة عمل ثم تحديد الفريق الذي يصلح لهذه المهمة و سنتطرق إلى هذه الخطوات كما يلي:[1]

1- تحديد المعلومات:

تتباين المعلومات التي ينبغي أن يدونها المحقق عند تلقي البلاغ بتباين فئات الجرائم المعلوماتية و طبيعتها الفنية التي تتميز بها كل فئة من هذه الجرائم ، غير أنه هناك معلومات مشتركة بين هذه الفئات يمكن الحصول عليها من خلال طرح المحقق بعض الأسئلة كما يلي :

* تاريخ و وقت تلقي البلاغ

* المعلومات الخاصة بالمبلغ

* طبيعة و نوع الجريمة التي هي محل البلاغ

* الأسئلة المشهورة في التحقيق ماذا و أين ؟ و متى؟ و كيف؟ و من؟ ولماذا؟

[1] علي عدنان الفيل ، **اجراءات التحري و جمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية** ، المكتب الجامعي حديث ، الاسكندرية ، مصر،2012 ، ص 11.

* المعلومات ذات العلاقة بالأنظمة الحاسوبية مثل : طبيعة العتاد و نوعية البرمجيات و المسولين عن الأنظمة و طريقة الإيصال بينهم و غيرها.

و من خلال هذه المعلومات التي يقدمها المبلغ إلى المحقق أو ضابط الشرطة القضائية و التي تكون عن طريق إرسال رسائل الكترونية إلى الموقع المتخصص بتلقي البلاغات ، يساعد في التبليغ مثلا عن وجود صفحات أو مواقع غير مشروعة تمارس صور استغلال الجنسي للأطفال أو معلومات عن أشخاص يحترفون الإجرام المعلوماتي ...الخ ، كما تساعد هذه المعلومات المحقق على تحديد السلوك ما إن كان محل البلاغ يعد سلوكا إجراميا أم لا وأيضا يمكن للمحقق وضع تصور مبدئي عن خطة العمل المناسب للتحقيق و تحديد نوع الخبرة الفنية التي يحتاجها المحقق...الخ من التوقعات.[1]

2 – وضع المحقق خطة عمل:

قبل أن يضع المحقق خطة عمل يجب عليه ملاحظة بعض الأمور و الأخذ ببعض القواعد التي يستند عليها في وضع خطته ، أولها مراعاة حجم ونوع الجريمة التي يكون في صدد التحقيق فيها لأن الجرائم المعلوماتية تختلف درجة خطورتها فمنها الخطيرة و منها قليلة الخطورة ، وكذلك مراعاة الظروف المحيطة بالجريمة مثل مسرح الجريمة و الأجهزة المعلوماتية التي يتعامل معها ، و تحديد من هم المتهمون والأشخاص الذين يساهمون في كشف عن الجريمة ، و هل يحق للرأي العام الإطلاع على هذه الجريمة أم لا و يدرس المحقق كل الخطوات التي سيقوم بها و الأحتمالات التي يقع فيها سواء كانت صائبة أو مخطئة ، و يراعي أهمية البيانات و مدى حساسيتها التي قد تكون محل الجريمة و كذلك تحديد مستوى المهارات الفنية التي يتمتع بها الجاني و تحديد مستوى الاختراق الأمني الذي تسبب فيه الجاني و العديد من الخطوات و التي تعود إلى سلطه التقديرية.[2]

[1] **علي عدنان الفيل**، مرجع سابق ، ص13.

[2] نفس المرجع ، ص16.

3- تحديد فريق عمل :

يوجد في فريق العمل محققين جنائيين ذو خبرة طويلة في التحقيق و كذلك أخصائيون لهم خبرة و معرفة واسعة في مجال الحاسب الآلي و شبكة الإيصال ، و من النادر أن نجد هاتين المهارتين(خبرة التحقيق و خبرة الحاسب الآلي) في محقق واحد و لهذا استوجب تأسيس فريق عملي يشمل جميع الجوانب التي يحتاجها التحقيق في الجريمة المعلوماتية و هي كما يلي :

* الإستعانة بخبير البصمات و خبير تصوير لمعاينة مسرح الجريمة و الإطلاع على كل تفاصيلها.

* تحديد قائد فريق تكون له خبرة واسعة في التحقيق مع درايته بطبيعة الجرائم المعلوماتية وذلك من أجل أن يوزع المهام بدقة على كل أفراد الفريق ، و يقوم كذلك بالتنسيق مع جهات متخصصة لتساعده و اتخاذ كافة القرارات الحاسمة وتحمل المسؤولية الكاملة فيها

* محقق جنائي و قد يكون شخص أو أكثر حسب ظروف الجريمة و كذلك يكون له خبرة و معرفة بوسائل و أساليب التحقيق و في نفس الوقت يكون ملما بطبيعة الجرائم المعلوماتية ، و كيفية التعامل مع الأدلة الرقمية و كيف يتولى التفتيش عنها وكذلك أخذ إفادة الأشخاص ذوي العلاقة بمسرح الجريمة.

* خبير الحاسب الآلي و شبكة الإنترنت وقد يكون شخص أو أكثر له خبرة واسعة في المجال المعلوماتي مع إلمامه بإجراءات التحقيق و يكون مسؤولا عن رفع و تحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة و التي لا تأثر على سلامة الدليل و صلاحيته لإفادة الدعوة و عرضه على المحكمة.[1]

* خبير مدقق حسابات و هو مختص في المراجعة المحاسبية و على درجة من الخبرة في التفاعل مع الأنظمة البرمجية المستحدثة في المؤسسات المصرفية ، و يعمل مع خبير الحاسب الآلي و شبكات الاتصال على تحديد أسلوب الجريمة و ما إذ كان هناك تلاعب بالأنظمة المتضررة بالإضافة إلى تقدير حجم الخسائر المادية الناتجة عن الجريمة.

[1] علي عدنان الفيل ، المرجع السابق صح 17

* أعوان التحقيق و هم أشخاص قد يتطلب مسرح الجريمة تواجدهم إلا أن دورهم ليس وثيقا بالطبيعة الخاصة بالجريمة المعلوماتية ، وقلما يخلوا مسرح أي جريمة مهما كان نوعها من وجوده مثل أفراد حماية و تأمين مسرح الجريمة و كذلك أفراد القبض و أفراد التحريات وغيرها.[1]

ب) تحري و كشف الغموض:

تتميز الجرائم ذات صلة بالحاسب الآلي و شبكة الاتصال بحداثة أساليب ارتكابها و سرعة تنفيذها و سهولة إخفائها و دقة محو آثارها ، و عليه يجب على جهات التحقيق و حتى المحاكمة أن تكون على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي و شبكة الإتصال و طريقة تشغيله و أساليب ارتكاب الجرائم علية أو بواسطته ، و هذا ما يمكنها من كشف الغموض على هذه الجرائم و سرعة التصرف بشأنها من حيث كشفها و ضبط الأدوات التي استخدمت في ارتكابها و التحفظ على البيانات أو الأجهزة التي تكون محل الجريمة و قد واجهة أجهزة الشرطة و التحقيق عدة صعوبات في هذا النوع من الجرائم المستحدثة ، سواء في كشف الغموض عنها أو في الاجراءات المتبعة فيها مثل التفتيش و ضبط الأدلة ، مما استدعى إلى الحاجة في تدريب و تأهيل كوادر خاصة من الناحية الفنية لتسهيل هذه المهمة ففي بداية ظهور هذا النوع من الجرائم كان يقع المحققون في أخطاء جسيمة أدت إلى الإضرار بالأجهزة و الملفات و الأدلة الرقمية التي تفيد التحقيق ، فمثلا في الولايات المتحدة الأمريكية حدث أن طلبت إحدى دوائر الشرطة من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي لتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة ، وقد حدث نتيجة ذلك اتلاف ما كان قد سلم من ملفات و برامج و عليه فكشف الغموض في الجريمة المعلوماتية يستدعي خبرة في الحاسب الآلي و شبكة الإتصال دون أن ننسى دور المجني عليه في هذه الجرائم الذي يمكنه أن يقدم خدمة كبيرة لرجال الشرطة و ذلك عن طريق ما يقدمه من معلومات قد تفيد المحقق بشكل كبير.[2]

[1] **علي عدنان الفيل**، مرجع سابق ، ص17.

[2] هشام محمد فريد رستم ، **قانون العقوبات و مخاطر التقنية المعلوماتية** ، مكتبة الآلات الحديثة ،أسيوط ،1994 ، ص29 .

الفرع الثاني :في مرحلة التحقيق الإبتدائي

باعتبار مرحلة التحقيق الابتدائي مرحلة ثانية التي تلي مرحلة جمع الاستدلالات و هي مرحلة سابقة للمحاكمة ، و بهذا هي كذلك تتميز ببعض الخصائص و الاجراءات استوجب علينا في هذا الفرع تعريف التحقيق الابتدائي و أهميته ثم تبيان السلطة المختصة في إدارته ثم الضمانات التي يتمتع بها المتهم في هذه المرحلة وهي ما يلي:

أولا : تعريف التحقيق الابتدائي و أهميته

التحقيق الابتدائي باعتباره عملا قضائيا يخول لسلطات التحقيق القيام بإجراءات التحقيق كمرحلة تسبق المحاكمة و لقد تعددت التعريفات الفقهية بشأنه ، فهناك من يعتبر التحقيق الابتدائي بأنه مجموعة من الاجراءات التي تبشرها السلطة المختصة بالتحقيق في الدعوة العمومية عن جريمة ارتكبت لكشف الحقيقة و الغموض عنها ، وذلك بالبحث و التنقيب عن الأدلة و تجميعها و تقديرها لإثبات حدوث الجريمة و نسبها إلى المتهم ثم إحالتها للمحاكمة من اجل الفصل فيها سواء بالنفي أو الأدنة ،و هناك من يعرف التحقيق الابتدائي أنه مجموعة من الاجراءات تستهدف التنقيب عن الادلة بشأن جريمة ما ارتكبت ثم تجميع هذه الأدلة و تقديرها ما ان كانت كافية لإحالة المتهم الى المحاكمة أم لا.

وتتجلى أهمية التحقيق الابتدائي أنها تقوم بتهيئة الدعوة لقضاة الحكم و ذلك عن طريق سماع المتهم و التنقيب عن الادلة وفرزها و جمعها و استظهار قيمتها و استبعاد الأدلة الضعيفة و مواجهة المتهم و سماع الضحية و الشهود بكل دقة ، و الإشراف على كل الإجراءات التي تثري التحقيق و تساعد في كشف عن الجريمة مثل التفتيش و المعاينة و التسرب ...الخ التي سنتطرق اليها لاحقا.[1]

[1] بن يحي اسماعيل، مرجع السابق ، ص53..

ثانيا : السلطة المختصة بالتحقيق الابتدائي في الجريمة المعلوماتية

إختلفت التشريعات المقارنة حول الجهة المختصة بالتحقيق الابتدائي فهناك من التشريعات تجمع بين سلطة الاتهام و سلطة التحقيق ، وهناك من التشريعات التي تفصل بين سلطة التحقيق و سلطة الاتهام والمقصود بالجمع بين سلطة الإتهام والتحقيق أنه السلطة التي توجه الاتهام هي نفسها التي تحقق مع المتهم ، فمثلا في التشريع الاردني مهام التحقيق من إختصاص النيابة العامة وذلك في المادة 42 من قانون أصول المحاكمة الجزائية التي تنص بعبارة يتولى "المدعي العام التحقيق وهو نفسه من له سلطة الاتهام ، أما في التشريع الجزائري فقد عمل بمبدأ الفصل بين سلطة الإتهام وسلطة التحقيق وهذا ما نستخلصه في الفصل الاول من باب الثالث من الكتاب الاول تحت عنوان في جهات التحقيق من المادة 66 الى 71 ، وبصريح العبارة في المادة 68 فقرة 01 ""يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع الإجراءات التحقيق ، ونلاحظ كذلك أن المشرع لقد خانته الترجمة وذلك بقوله في الفصل الثاني من الباب الثاني تحت عنوان تحقيق الابتدائي في المواد 63 إلى 65 من ق. إ.ج.ج أنه سلطة التحقيق الابتدائي من اختصاص ضبطية القضائية غير[1] انه نجد في نظرتها باللغة الفرنسية كلمة تحقيق الاولي (des enquêtes préliminaire) و التحقيق الابتدائي (l instructio préparatoire) .

وعليه نستخلص ان مرحلة التحقيق الابتدائي في الجريمة المعلوماتية من اختصاص قاضي التحقيق وهذا عملا بمبدأ الفصل بين سلطة التحقيق و سلطة الاتهام . [2]

[1] **بن يحي إسماعيل** ، المرجع السابق ، ص56-57.

[2] القانون رقم 22/06 الصادر في 2006/12/20 يعدل ويتمم الامر رقم 66-155 المؤرخ 1966/6/8 والمتضمن قانون الاجراءات الجزائية ، (ج ر) العدد 84 المؤرخة في 2006/12/24.ص 7

ثالثا : ضمانات المتهم في التحقيق الابتدائي في الجريمة المعلوماتية

للمتهم في التحقيق الابتدائي بعض الضمانات محفوظة مهما كانت الجهة القضائية التي تحقق معه وهذه الضمانات نصت عليها جميع التشريعات الدولية الاقليمية وحتى الوطنية وهي كما يلي :

* **مبدأ قرينة البراءة** : لقد نصت عليها المادة الاولى من قانون الإجراءات الجزائية وهي تفسير الشك لصالح المتهم والحق في المحاكمة العادلة وسرعة المحاكمة ، و براءة المتهم حتى تثبت الجهة القضائية إدانته ومبدأ التعليل الاحكام والقرارات .[1]

* **مبدأ سرية التحقيق وحق الخصوم في الحضور** : والمقصود بالسرية التحقيق هنا هو عدم اطلاع الجمهور على محاضر التحقيق وليس للخصوم وذلك من اجل محافظة على سمعة المتهم امام العامة وكذلك محافظة على مجريات التحقيق وحماية الادلة من العبث وتلاعب بها ، اذن السرية في هذه الحالة تكون بالنسبة للجمهور وعلانية بالنسبة للخصوم حيث علانية التحقيق حق لكل الخصوم غير انه هناك استثناء في المادة 101 من قانون الاجراءات الجزائية وهو في حالة الاستعجال يمكن لجهة التحقيق ان لا تخطر الخصوم مثل استجواب شاهد في حالة الموت أو البحث عن دليل مستعجل ويجب على جهة التحقيق تعلل دواعي الاستعجال ويمكن لغرفة الاتهام إعادة نظر هذا الاستثناء.[2]

* **مبدأ التدوين** : مقصود به هو افراغ مجريات التحقيق وكل أقوال المتهم والضحية والشاهد في محاضر إستدلالية مكتوبة ، وذلك من أجل مساعدة جهة الحكم أو قاضي الموضوع في تكوين عقيدته للفصل في الدعوى وكذلك ضمان عدم تغيير الاقوال والتي قد تمس بموضوع الجريمة .

[1] انظر إلى المادة 47 من الدستور الجزائري لسنة 2020 الصادر بموجب مرسوم رئاسي رقم 442/20 في 30 ديسمبر 2020 المتعلق بإصدار تعديل دستوري جديد المصادق عليه بإستفتاء شعبي في 1 نوفمبر 2020 ،ج.ر العدد 82 المؤرخة في 30 ديسمبر 2020.ص 13

[2] **بن يحي اسماعيل** ، مرجع سابق ، ص58.

رابعا : خصائص المحقق في الجريمة المعلوماتية:

الجريمة الإلكترونية تختلف عن الجريمة التقليدية فلذلك لا يمكن أن يحقق فيها بدون أن يكون له صفات خاصة وهذه الصفات هي:

كأن يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة ، وأن يميل إلى تصميم البرامج أكثر من تشغيلها ويحب معرفة الجديد عن هذه البرامج ، وأن يستطيع تصميم وتحليل البرامج أو أنظمة التشغيل بسرعة ، وأن يؤمن بوجود أشخاص اخرين مثله لديهم القدرة على اختراق الأنظمة المعلوماتية ، وأنه يتعامل مع فئة من المجرمين لهم مستوى عالي من الذكاء وكل هذه الأمور لا تتوافر إلا لمن كان لديه إمكانات عقلية تزيد على متوسط العام المألوف.

الفرع الثالث : في مرحلة المحاكمة

مرحلة المحاكمة هي مرحلة النهائية من التحقيق وهي مرحلة التي يتم بناء قاضي الموضوع عقيدته والحكم بالبراءة او الادانة للمتهم وبذلك استوجب المشرع تنظمها وسنتطرق الى اهم عناصرها كما يلي :

اولا : في إختصاص المحكمة ينقسم اختصاص المحكمة الى اختصاص محلي ونوعي وهو كما يلي :

* **اختصاص المحلي** : طبقا نص المادة 37 من قانون الإجراءات يتحدد الاختصاص المحلي للجريمة في ثلاث ضوابط وهي مكان وقوع الجريمة أو المكان إقامة المتهم أو مكان القبض غير انه نظرا لبعض خصوصيات الجرائم والتي جاءت على سبيل الحصر من بينها الجريمة المعلوماتية ، فانه حسب المواد 37 و 40 من ق. أ.ج.ج يجوز تمديد الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق و جهات الحكم إلى خارج دائرة اختصاصهم ، وفي نطاق الجرائم المعلوماتية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان اخر ، فإن الاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة ، [1]وتعد الجريمة الإلكترونية

[1] بعرة سعيدة ، **الجريمة الإلكترونية في التشريع الجزائري** ، مذكرة ماستر، تخصص قانون جنائي، قسم حقوق،كلية الحقوق و العلوم السياسية، جامعة محمد خيضر،بسكرة ،ا لجزائر،2015- 2016، ص92..

إذا تمت عن طريق شبكة الانترنت جريمة مستمرة حيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت الجريمة .

فيه ومتى كانت الجريمة الإلكترونية أيا كان نوعها فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيات الإعلام والاتصال إذا ارتكبت خارج الإقليم الوطني ، أو إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي.

*** اختصاص النوعي :**

يتحدد الإختصاص النوعي للمحكمة للفصل في القضية معروضة عليها تبعا لنوع الجريمة التي ينظر فيها ، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة وبعض الجنح والمخالفات المرتبطة بها ، و والمحالة إليها بقرار نهائي من غرفة الاتهام هذا حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري ، حيث يوجد على مستوى كل مجلس محكمة جنايات ابتدائية و استئنافية كما يختص قسم الجنح والمخالفات الموجود على مستوى كل محكمة النظر في الجنح والمخالفات 328 من ق .إ.ج.ج .

غير أنه يمكن تمديد الاختصاص المحكمة إلى محاكم اخرى في بعض الجرائم المنصوص عليها في المادة 329 المتعلقة بالمتاجرة بالمخدرات ،والجريمة المنظمة عبر الحدود الوطنية ، وجرائم تبيض الأموال والإرهاب ، والجرائم المتعلقة بالتشريع الخاص بالصرف ، و جرائم الماسة بأنظمة المعالجة الالية للمعطيات بإجراءات خاصة إذا جعل الاختصاص ينعقد إلى دائرة اختصاص[1] أخرى وهذا ما نصت عليه المادة ، 329من قانون ،الإجراءات الجزائية أثر التعديل الذي جاء به القانون رقم 04/ 14المؤرخ في10نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 348/06 والمتعلق بالتنظيم القضائي حيث

[1] بعرة سعيدة ، مرجع سابق ،ص93.

نص على إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة ، قسنطينة ، وهران ، ورقلة.

ثانيا : في تشكيلة المحكمة

تختلف تشكيلة المحكمة الجزائية بحسب الجريمة اذا كانت جناية تختص فيها محكمة الجنايات و اذا كانت جنحة يختص بها قسم الجنح على مستوى المحكمة والغرفة الجزائية على مستوى المجلس القضائي وهي كما يلي : [1]

* على مستوى المحكمة يتشكل من قاضي فرد ويساعده كاتب ضبط وبحضور وكيل الجمهورية أو أحد مساعديه .

* أما الغرفة الجزائية على مستوى المجلس قضائي فالتشكيلة فيها ثلاثية ، أي تتشكل من رئيس غرفة ومستشارين إثنين بالإضافة إلى كاتب ضبط وبحضور النائب العام أو أحد مساعديه.
* أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبط والنيابة العامة أو من يمثلها. [2]

* على مستوى القطب الجزائي فتتشكل في اول درجة من قاضي ووكيل جمهورية وفي ثاني درجة ثلاثة قضاة و ونائب عام وكاتب ضبط على جميع الدرجات.

ثالثا : إجراءات المحاكمة

تستهل المحكمة جلستها بالإعلان أولا عن افتتاحها بالقول بإسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني ، والتأكد من حضورهم أو غيابهم ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها، وإذا

[1] بعرة سعيدة المرجع السابق ، ص 94

كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة ، وفي هذه الحالة وطبقا لأحكام المادة 339مكرر 6 المستحدثة بموجب الأمر 15-02المؤرخ في 23 جويلية 2015من قانون الإجراءات الجزائية تتخذ المحكمة إحدى الإجراءات التالية [1]:

* ترك المتهم حر.

*إخضاع المتهم لتدابير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 521 مكرر 1 من قانون الإجراءات الجزائية.

* وضع المتهم في الحبس المؤقت.

ولا يجوز الاستئناف في الاوامر التي تصدرها المحكمة وفقا لهذه المادة .

و إذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب إجراءات المثول الفوري ، فإنه يساق بواسطة القوة العمومية لحضور الجلسة ويخطره رئيس الجلسة بأن له الحق في اختيار محامي لدفاع عنه، فإن طلب ذلك أمهله القاضي مهلة لأتقل عن ثلاثة أيام لتحصيل دفاعه ، ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها بالتفصيل من طرف القاضي و بعدها يقوم القاضي بسماع الشهود ، وبعد الانتهاء من تحقيق تعطى الكلمة للطرف المدني فقط دون المطالبة بالعقوبات الجزائية ، لتقوم بعد ذلك النيابة العامة بالمرافعة وتقديم التماساتها في الشق الجزائي فقط وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم التماساتها ، ويكون بعدها لنيابة العامة والمدعى حق الرد على مرافقة محامي المتهم ، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه.

[1] **بغرة سعيدة** ، المرجع السابق ، ص95.

الفرع الرابع : صعوبات التحقيق في الجريمة المعلوماتية

وكما هو معروف أن التحقيق في الجرائم المعلوماتية وملاحقة مرتكبيها جنائيا يتسم بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق في بيئة رقمية ، قد تؤدي إلى وجود نتائج سلبية تنعكس على نفسية المحقق بفقده الثقة في نفسه ، وفي عملة بالإضافة أنها تصعد من قيمة مكافحة هذا النوع من الجرائم ومن أهم المعوقات التي قد تواجه القائمين على مكافحة الجرائم المعلوماتية والتحقيق فيها ، عوائق تتعلق بالجريمة وعوائق تتعلق بالجهات المتضررة وعوائق بجهات التحقيق وهو ما سنتناوله بالتفصيل:[1]

أولا : صعوبات تتعلق بالجرائم المعلوماتية :

* خفاء الجريمة وغياب الدليل المرئي وغير ممكن قراءته بشكل مفهوم.

* افتقاد أكثر للآثار مقارنتا بالجريمة التقليدية.

*إعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية كاستخدام كلمات السر.

*سهولة محو الدليل أو تدميره في زمن قصير جدا.

ثانيا : صعوبات تتعلق بالجهات المتضررة

*عدم إدراك خطورة الجرائم المعلوماتية من قبل المسؤولين بالمؤسسات تعد إحدى معوقات التحقيق.

* لأحجام عن الإبلاغ عن الأشخاص الميسورين أو صغار السن خوفا من المجتمع المحيط بهم وخشية الفضيحة يعد معوقا من معوقات التحقيق.

* عدم الإبلاغ عن الجرائم بصفة عامة يؤثر على التحقيق .[2]

[1] يوسف جفال ، **التحقيق في الجريمة الإلكترونية ،مذكرة ماستر**، تخصص قانون جنائي ، قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة محمد بوضياف،المسيلة ،الجزائر،سنة 2016-2017.ص 41

[2] نفس المرجع ، ص47

ثالثا : صعوبات تتعلق بجهات التحقيق

* قد تكون شخصية(معوقات تتعلق بالمحقق) مثل التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الإنترنت ، عدم الإهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.

* صعوبات تتعلق بالنواحي الفنية كنقص المهارة المطلوبة للتحقيق في هذا النوع من الجرائم و نقص المهارة في استخدام الكمبيوتر والانترنت وعدم توفر المعرفة بأساليب ارتكاب هذا النوع من الجرائم.

* قلة الخبرة في مجال التحقيق في الجرائم المعلوماتية.[1]

المطلب الثاني : الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية

مع تزايد الجريمة بشكل مستمرة استوجب ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجريمة بصفة عامة وفي الجريمة المعلوماتية بصفة خاصة وهذا ما جعل معظم الدول تقوم باستحداث هذه الاجهزة لمواجهة هذا النوع من الجرائم ولقد اختلفت تسمية هذه الاجهزة مثل شرطة الانترنت أو فرقة البحث وتحري المعلوماتية وتعمل هذه الاجهزة على مكافحة الجريمة المعلوماتية على المستوى الدولي والوطني

الفرع الاول : الاجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على مستوى الدولي والإقليمي.

سبق و أسلفنا الذكر بأن الجرائم المعلوماتية تتميز بأنها عابرة للحدود الوطنية يمكن أن يتعدى أثرها عدة دول لذلك كان لابد من وجود تعاون دولي و اقليمي من أجل مكافحة هذا النوع من الإجرام وسنذكر منه ما يلي:

[1] سعيداني نعيم ، **آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري** ، مذكرة لنيل شهادة ماجيستير ،تخصص علوم جنائية ، جامعة الحاج لخضر ، باتنة ، 2012-2013. ص 81

أولا: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على مستوى الدولي

تعد المنظمة الدولية للشرطة الجنائية الأنتربول[1] من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ، ومنها الجرائم المعلوماتية بصفة خاصة وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في دول الأطراف على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتية وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين:

* تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

* التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

وتعمل المنظمة الدولية للشرطة الجنائية في مجال الجرائم المعلوماتية بوضع قائمة اسمية لضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية ، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين ، ولقد انشأت هذه المنظمة وحدة متخصصة في مكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته.[2]

ثانيا : الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على مستوى الإقليمي

تعتبر الاجهزة الخاصة على مستوى الاقليمي من أهم وسائل مكافحة الجريمة المعلوماتية وهي كما يلي :

* **الشرطة الأوروبية أو الأوروبول** : وهو جهاز على مستوى الاتحاد الأوروبي تم إنشاؤه في لكسمبورغ عام 1992 ومقره في مدينة لاهاي بهولندا ، ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول

[1] المنظمة الدولية للشرطة الجنائية الأنتربول، مقرها في باريس وضع ميثاق هذه المنظمة في فترة 7-1956/06/13.

[2] **سعيداني نعيم** ، مرجع السابق ،ص 107-108

الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة ، وكذلك الإجرام المعلوماتي ،ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة لمختلف الدول الأعضاء ، وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتية وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه اسم (système de signalement en ligne de la criminality sur Internet)في سنة 2010 بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء.[1]

* **الأوروجيست (Eurojust)** : وهو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم ، تم إنشاؤه عام 2002 وينعقد اختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الإتحاد الأوروبي. ويعد الأروجيست وحدة للتعاون القضائي ، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيق و مباشرة متابعات جزائية.

* الافريبول **(Afripol)** : وهي أكبر منظمة شرطة في القارة الأفريقية المكونة من قوات الشرطة بـ 41 دولة انشئت بمبادرة من الدولة الجزائرية يوم 2015/12/13 مقرها الرئيسي الجزائر العاصمة ، وتم الإعلان رسميا عن بداية نشطها يوم 2017/07/06 بمناسبة اجتماع مسؤولي أجهزة الشرطة للدول الافريقية الاعضاء في الاتحاد الافريقي المنعقد بالجزائر ، وتكمن مهام الافريبول في مضاعفة رصيد التعاون الشرطي الاقليمي والدولي و تحديد السياسة العامة لشرطة الجنائية و توفير تكوين و إعادة تأهيل مختلف أجهزة الشرطة الافريقية ، التي تشهد تأخر وضعف على مستوى الاداء وكذلك تعزيز قيام سلم والأمن والاستقرار في القارة الأفريقية ، و إيجاد الحلول الفاعلة للجرائم التي توجهها بعض الدول الأفريقية مثل جرائم الارهاب و المخدرات و الجرائم المعلوماتية . [2]

[1] **بغاديد نابية**، المرجع السابق، ص47.

[2] براهمي جمال ، **التحقيق الجنائي في الجرام الالكترونية** ، اطروحة لنيل شهادة دكتورة ، تخصص قانون جنائي ، قسم الحقوق ، كلية الحقوق وعلوم السياسة جامعة مولود معمري ، تيزي وزو ، الجزائر 2018 ص 308

الفرع الثاني : الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على مستوى الدول الأجنبية

كانت الدول المتقدّمة سبّاقة بإحداث هذه الأجهزة إذ أنّ مكافحة الجرائم المعلوماتية مرتبط بمدى تقدّم الدول من الناحية التقنية وبمدى توفر الإمكانيات المادية اللازمة لإنشاء هذه الأجهزة ، ونذكر على سبيل المثال في هذا الصّدد الدول التالية [1]:

اولا : في الولايات المتحدة الأمريكيّة

قامت الولايات المتحدة الأمريكيّة بإنشاء عدّة أجهزة لمكافحة الجريمة المعلوماتية ومنها :

* **شرطة الواب web police** : وتعتبر نقطة مراقبة على الأنترنت إضافة إلى أنها تتلقى الشكاوي وتسعى إلى البحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة .

* **مركز تلقي شكاوي جرائم الأنترنت IC3** : والّذي تم إنشاؤه من طرف مكتب التحقيقات الفيدرالي FBI في سنة 2000 ثم في عام 2003 تم دمج مركز شكاوي الاحتيال عبر الأنترنت المعروف ب IFCC مع هذا المركز ويعمل مركز IC3 بصورة تشاركيّة ، مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاءNCC ويقوم هذا المركز بتلقي الشكاوي عبر موقعه على الأنترنت أين يقوم الشاكي بملىء استمارة إلكترونية ثم يقوم المختصون في هذا المركز بتحليل الشكاوي وربطها بالشكاوي الأخرى المستلمة من قبل.[2]

* **قسم جرائم الحاسوب والعدوان على حقوق الملكيّة الفكرية** : ويختص هذا القسم بالتعريف بهذه الجرائم و الكشف عنها وملاحقة مرتكبها.

[1] بغاديد نابية،مرجع سابق، ص48

[2] Myriam QUEMENER. YES CHARPENEL Cybercriminalité droit pénal applique économique septembre 2010 ،p. 209

* **نيابة جرائم الحاسوب والاتصالات CTC** : وتتألّف من مجموعة من قضاة النيابة العامة ممن تلقّوا تدريبات مكتفة على نظم المعالجة الآليّة للبيانات.

* **المركز الوطني لحماية البنية التحتية** : التابع للمباحث الفدرالية الأمريكيّة وقد حدّد هذا المركز البنيات التحتيّة التي تعتبر هدفا للهجمات و الاعتداءات عبر الأنترنت وعلى رأسها شبكات الاتصالات وإضافة إلى هذه الأجهزة يوجد أيضا في الولايات المتّحدة الأمريكيّة وحدة متخصّصة بمكافحة الإجرام المعلوماتي التابعة لقسم العدالة الأمريكي تتكوّن من خبراء في نظام الحوسبة.

ثانيا : في بريطانيا

قامت السلطات البريطانيّة بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصّصين في البحث و التحري عن الجرائم المعلوماتيّة ، وتضمّ هذه الوحدة نحو ثمانين عنصرا على درجة عاليّة من الكفاءة في المجال التقني وقد بدأت هذه الوحدة نشاطها عام 2001.

ثالثا :في فرنسا

قامت الحكومة الفرنسيّة بإنشاء عدّة أجهزة لمكافحة الجرائم المعلوماتية ونذكر من هذه الأجهزة ما يلي :

* **القسم الوطني لقمع جرائم المساس بالأموال و الأشخاص** : ويتكون هذا القسم من محققين بجرائم العالم الافتراضي وقد بدأ هذا القسم مهامه عام 1997[1].

* **المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات** : ويعد هذا المكتب سلاح الدولة الفرنسيّة في مكافحة الجرائم المعلوماتية ، وقد تم إنشاؤه في 15 /2001/05.

[1] بغاديد نابية ،المرجع السابق ، ص47

رابعا : في الصّين

قامت السلطات في هذا البلد بإنشاء وحدة متخصّصة على مستوى جهاز الشرطة تعرف باسم "القوّة المضادة للهاكر" وهي تختصّ برقابة المعلومات التي يسمح لمواطنيها الدّخول إليها عبر الانترنت.

خامسا :في مصر

قامت وزارة الداخلية في مصر بإنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم من خلال الشبكة المعلوماتية على النحو التالي:

* **إدارة مكافحة جرائم الحسابات وشبكات المعلومات** : أنشئت هذه الإدارة بموجب قرار وزاري وهي تابعة للإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة ، وتشرف عليها فنيا مصلحة الأمن العام التابعة لوزارة الداخلية ، وتضم ثلاث أقسام رئيسية وهي قسم العمليات و قسم التأمين وقسم البحوث والمساعدات الفنية ، وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم المعلوماتية فهي تتكون من ضباط متخصصين في مجال تكنولوجيا الحسابات والشبكات ، وتختص بمكافحة جرائم الإنترنيت على مختلف أنواعها.

* **قسم مكافحة جرائم الحاسبات وشبكات المعلومات** : وقد أنشئ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة ويتبع إدارة المعلومات والحاسب الآلي ، ويخضع من حيث الإشراف الفني لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات ، ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جرائم عليها، باستخدام الأساليب والتقنيات العلمية الحديثة. ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات.[1]

[1]. بغاديد نابية ، المرجع السابق ، ص49

الفرع الثالث: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الوطني

أما الوضع في بلادنا فإنه وبالنظر إلى الخصوصية التي تتميز بها الجريمة المعلوماتية كان الأمر محتما لتوفير كوادر وأجهزة متخصصة تعتني بعملية البحث والتحري عن الجريمة المعلوماتية ، وكان ذلك أما على مستوى جهاز الشرطة أو الدرك الوطني ، ولعل أبرز الهيئات المختصة في مجال مكافحة الجرائم الإلكترونية على المستوى الوطني تتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، و المعهد الوطني الادلة الجنائية وغيرها سنتطرق لها في هذا الفرع كما يلي :

اولا : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصالات

نص المشرع في المادة 13 من القانون 09 / 04 على ضرورة إنشاء هيئة ذات وظيفة تنسيقية تعمل على اتخاذ الإجراءات اللازمة للوقاية من هذه الجرائم ، وتتولى تنشيط و تنسيق عملية الوقاية من الجرائم الإلكترونية ، وكذلك مصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم

أ) التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تعرف حسب أحكام المواد من 01 إلى 04 من القانون 09/04 بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي و توضع لدى الوزير المكلف بالعدل ، ويقع مقرها بالجزائر العاصمة.[1]

ب) مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تنص المادة 14 من نفس القانون على انه ''تتولى الهيئة المذكورة في المادة 13 خصوصا المهام التالية :

تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، وكذلك مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة

[1] بشير حماني ، المرجع السابق ، ص 35-36

بتكنولوجيا الإعلام والاتصال ، بما في ذلك تجميع المعلومات وتبدلها مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.[1]

ج) اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال :

بينت الفقرة 02 من المادة 04 من الموسوم الرئاسي 15 /261 المهام الأساسية التي تكلف بها هذه الهيئة وهي على سبيل الحصر ، الهدف منها هو الوقاية من الجرائم الإلكترونية ومكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية ، وابرز مهام هذه الهيئة هي[2]:

* اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

* تنشيط وتنسيق عمليات الوقاية عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

* مساعدة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية .

* ضمان المراقبة الوقائية للاتصالات الإلكترونية قد تكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

* تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

* السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

---

[1] **بن نعوم خالد** ، المرجع السابق ، ص44-45.

[2] **بعرة سعيدة** ، المرجع السابق ، ص 100

* تـطـوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

* المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.

* المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

ثانيا :الهيئات القضائية الجزائية المتخصصة (الأقطاب القضائية)

أنشئت بموجب القانون 04 /14 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية تختص ببعض الجرائم الإستثنائية ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، طبقا للمواد 40.37.329 من ق.أ.ج.ج تتمتع بمباشرة مهامها في[1] دائرة الاختصاص الإقليمي الموسع طبقا للمرسوم التنفيذي رقم 06 / 348 المؤرخ في 2006/01/05 ، بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والإتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا. اذا كانت تستهدف مؤسسات الدولة والدفاع الوطني المادة 15 من القانون رقم 09-04.[2]

ثالثا : المديرية العامة للأمن الوطني.

تصدت هذه المديرية للجريمة المعلوماتية من مختلف الجوانب منها :

أ) الجانب القانوني والمتمثل في النصوص القانونية الأتية :

حيث نظمها القانون 22 /06 المؤرخ في 2006/12/10 و القانون 05 -03 من القانون المدني و كذلك القانون 04 /09 المؤرخ في 2009/08/05 الوقاية من جرائم التكنولوجيا والإعمال والاتصال وقانون العقوبات المواد من 394 مكرر إلى 397 مكرر 7 .

[1] احسن بوسقيعة ،**الاجراءات الجزائية في ضوء الممارسة القضائية** ، منشورات بارتي BERT ،الطبعة 16، 2021،ص 29

[2] انظر إلى المواد 329 .32.40 من القانون 14/04 الصادر في 2004/11/10 المعدل والمتمم لقانون الاجراءات الجزائية (ج ر) العدد 71 المؤرخة في 2004/11/10 ص 5- 6

ب)الجانب التنظيمي ويتمثل في التكوين المتواصل والتخصيص :

وهو تدعيم مخابر الشرطة العلمية و مصالح الولائية للشرطة القضائية و كذلك تدعيم هيكلة مصالح الشرطة القضائية للتصدي لهذه الجريمة

ج) الجانب التوعوي :

لم تغفل المديرية العامة للأمن الوطني عن الجانب الوقائي التوعوي يظهر ذلك من خلال برمجتها المديرية العامة لخطوات إستباقية للتصدي للجريمة المعلوماتية ، عن طريق تنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم المعلوماتية ، أما في إطار سياسة الشرطة الجوارية التي تنتجها قيادة المديرية ، قام الأمن الوطني بفتح موقع الكتروني خاص بالشرطة الجزائرية على الانترنت يستطيع من خلاله أي مواطن مهما كان مستواه العلمي أو الاجتماعي طرح انشغاله والتبليغ عن أي شيء يثير الشبهة.[1]

د) **الجانب الدولي:**

في إطار مكافحة الجريمة المعلوماتية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم لم ، تغفل المديرية العامة للأمن الوطني استغلال عضويتها الفعالة في هاته الأخيرة تتيح مجالات للتبادل مع (Interpol) المنظمة الدولية للشرطة الجنائية وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين ، وكذا مباشرة الإنابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا.

[1] **بعرة سعيدة** ، المرجع السابق ، ص103

و) الجانب التطبيقي و الميداني:

عالجت المديرية العامة للأمن الوطني على المستوى الوطني مجموعة من القضايا المتعلقة بالجريمة المعلوماتية من خلال الجدول التالي[1]:

السنوات	عدد القضايا المعالجة	عدد الأشخاص المتورطين
2007	31	31
2008	06	10
2009	29	21
2014	245	/
2015	409	347

[1] **بعرة سعيدة** ، المرجع السابق ، ص 103.

رابعا : المعهد الوطني للأدلة الجنائية وعلم الإجرام (Incc) :

وهو جهاز تابع للدرك الوطني أنشأ سنة 2004 بموجب المرسوم الرئاسي رقم 183/04 يتكون من 11 دائرة متخصصة في عدة مجالات تضمن الخبرة والتكوين والتعليم وتقديم المساعدات التقنية والبحوث والدراسات والتحاليل في علم الجريمة ، ويحتوي على عدة دوائر لكل دائرة مجال معين ومن بينها دائرة الاعلام الآلي والالكتروني التي تكلف بمعالجة تحليل وتقديم كل دليل الكتروني وتماثلي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة ، و يسهر أفراد الدائرة على تأمين اليقظة التكنولوجية من أجل تحيين المعارف التقنيات والطرق المستعملة في مختلف الخبرات العلمية ، ولإنجاز المهام المنوط بها تنقسم الدائرة الى ثلاثة مخابر وكل مخبر مزود بفصيلة مهمتها اقتناء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل وهي كما يلي :

* **مخبر الاعلام الالي** : يختص بتحليل ومعالجة حوامل المعطيات الرقمية (الهاتف القرص الصلب ، ذكرة الفلاش) كما يقوم بتحديد التزوير الرقمي للبطاقات البنكية .

* **مخبر الفيديو** : يختص بإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد كما يعمل على تحسين نوعية الصورة (فيديو، صورة، بمختلف التقنيات، ومقارنة الأوجه وشرعية الصور والفيديو) .

* **مخبر الصوت** :يختص بمعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية، ويعمل على تحسين نوعية اشارة الصوت بنزع التشويش وتعديل السرعة[1].

[1] **بعرة سعيدة** ، المرجع السابق ، ص105

خاتمة الفصل :

وفي الاخير بعد ما تناولنا في هذا الفصل مفهوم الجريمة المعلوماتية ، وتبيان خصائصها وأركانها و أطرفها وتصنيفها وسبل والجهود الدولية والإقليمية والوطنية لمكافحة هذه الجريمة ، تم كذلك التطرق إلى مراحل التحقيق و الأجهزة التي تساعده .

وعليه يمكن القول أن الجريمة المعلوماتية تختلف عن الجريمة التقليدية من حيث مكان وقوعها فالجريمة التقليدية تقع في بيئة حقيقة مادية ، والجريمة المعلوماتية تقع في بيئة افترضيه وهمية .

ونظرا لطبيعة الجريمة المعلوماتية وما تتميز به من خصائص ، يجب على المحقق أن يكون ملما بالجانب التقني للجريمة المعلوماتية ، مثل معرفة كل ما يتعلق بالحاسوب ومكوناته المادية والمعنوية .

و لقد بينا كذلك الشخص المسؤول عن التحقيق وصلاحياته في مجال الجريمة المعلوماتية ، كما تطرقنا إلى وجود عدة صعوبات التي تواجه التحقيق في هذا النوع من الجرائم ، و بينا كذلك أهم الاجهزة والمعاهد التي تساعد التحقيق والمحقق على حد سواء .

الفصل الثاني

الدليل الإلكتروني

و القواعد الإجرائية

لاستخلاصه

يهدف التحقيق إلى كشف الغموض عن الجريمة والوصول إلى مرتكبها ، ولا يمكن تصور الكشف عن مرتكب الجريمة دون الوصول إلى دليل قاطع لإدانة المتهم ، فالدليل هو الأثر الذي يتركه الجاني في كل جريمة لكن العوائق التي تواجه المحقق في الجريمة المعلوماتية ، هي أن الدليل في حد ذاته دليل معنوي غير مرائي عكس الدليل في الجريمة التقليدية ، الذي يخلف اثارا نرها في العالم الحقيقي وهذا ما جعل الدليل يحتاج جملة من الاجراءات التقليدية والمستحدثة للوصول إليه ، حيث تشمل الاجراءات التقليدية كل من المعاينة والتفتيش والخبرة الفنية ، وتشمل الاجراءات المستحدثة كل من اعتراض المرسلات وتجسس على الاتصالات التي يقوم بها المشتبه فيهم ، و كذلك الاعتماد على المعطيات التي يقدمها مقدمي الخدمات .

حيث أن كل هذه الاجراءات تمكننا الوصول إلى الدليل الموجود في البيئة الافتراضية ، وهذا ما يسمى بالدليل الرقمي او الدليل الالكتروني ، وكلما كان ضبط دليل الرقمي بشكل سليم ودقيق نضمن أن قاضي الموضوع ستكون له أحكام و قرارت قضائية سليمة ، حيث هذا الاخير له سلطة تقدير وقبول الادلة المعروضة أمامه ، والتي تساعده في تكوين عقيدته للوصول إلى إقتناعه في إدانة المتهم أو براءته .

وعليه تم تقسيم هذا الفصل الى مبحثين التاليين :

* **المبحث الاول : ماهية الدليل الالكتروني ؟**

* **المبحث الثاني : القواعد الاجرائية لاستخلاص الدليل الالكتروني**

المبحث الاول : ماهية الدليل الإلكتروني

لقد أثار الدليل الالكتروني الكثير من التساؤلات حول ما اذا كان يمثل الحقيقة أو لا يمثلها نظرا لقابلية التلاعب بيه وتزيفه وتعديله والعبث فيه ، وذلك بسبب الطبيعة الرقمية التي يتميز بيها وهذا ما جعل المشرع يتدخل وينظم مسالة الدليل الالكتروني ويحطه ببعض الضمانات التي يمكن أن توفر الحماية لهذا الدليل الذي يضمن لنا سلامة الأحكام التي يصدرها قاضي الموضوع ولعلى من بين هذه الضمانات هي مشروعية الدليل ومشروعية الحصول عليه وكذلك قيمته في الاثبات أمام القاضي و تنظيم الوسائل والطرق التي تساعد القاضي في تكوين عقيدته القضائية وبناء الاحكام عليها ، وعليه سنتطرق في المطلب الأول مفهوم الدليل الالكتروني وفي ، المطلب الثاني سلطة القاضي الجزائي في تقدير الدليل الالكتروني .

المطلب الأول : مفهوم الدليل الالكتروني

يعتبر الدليل الالكتروني الاداة الوحيدة التي تجعل المحقق يكشف الجاني ويقيم الحجية عليه ويوجه الاتهام إليه ولهذا سنتطرق في هذا المطلب الى تعريف الدليل الالكتروني وشرعيته وشرعية الحصول عليه .

الفرع الاول : تعريف الدليل الالكتروني

المقصود بالدليل الالكتروني هو الوسيلة المشروعة و المتحصل عليها بالطرق المشروعة من أجل تقديمها للقاضي من اجل تحقيق حالة اليقين لديه والحكم بموجبها[1]، وهناك من يعرفه بأنه الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجمعها وتحليلـــها

[1] نور الهدى محمودي ، **حجية الدليل الرقمي في إثبات الجريمة المعلوماتية** ، مجلة الباحث للدراسات الأكاديمية ، المجلد الرابع ، العدد 2 ، ص 908

باستخدام برامج معلوماتية ، وهي مكون رقمي لتقديم المعلومات في اشكال متنوعة مثل النصوص المكتوبة أو الاصوات أو الاشكال أو الرسوم وذلك من اجل اعتماده امام الجهات القضائية[1].

وعرفها البعض الاخر أنها معلومات يقبلها المنطق و العقل ويصدقها العلم ، ويتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال ، ويمكن استخدامها في أية مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة الفعل أو الشيء أو الشخص له علاقة بالجريمة[2].

والدليل الالكتروني وهو وسيلة من وسائل الاثبات العلمية الجنائية الحديثة التي يعتمد عليها القاضي في تكوين قناعته ، فهو أي معلومات سواء من صنع الانسان او تم استخلاصها من الحاسوب يتقبلها العقل والمنطق من اجل استقرائها والوصول الى الحقيقة .

الفرع الثاني : خصائص الدليل الالكتروني

يتمتع الدليل الالكتروني بمجموعة من الخصائص التي تميزه عن الدليل التقليدي وتتمثل في ما يلي :[3]

أولا :الدليل الإلكتروني دليل علمي

يتصف الدليل الالكتروني بأنه علمي لأنه مشكل من معطيات إلكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات ذات المبنى العلمي ، و ما يسري على الدليل العلمي يسري على الدليل الالكتروني ، و اذا كان الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة القانون

[1] سمير شبلاق ، **حجية الدليل الرقمي في الكشف عن الجريمة** ، مذكرة ماستر ، تخصص قانون جنائي عام ، قسم حقوق ، كلية لحقوق وعلوم السياسية ، جامعة دكتور مولاي الطاهر، سعيدة ،الجزائر 2019- 2020 ، ص 6

[2] قروج حنان ، **حجية الأدلة المعلوماتية في تكوين الاقتناع الشخصي للقاضي الجزائي** ،مذكرة ماستر ، تخصص علم الاجرام ، قسم الحقوق ، كلية الحقوق والعلوم السياسية ، جامعة دكتور مولاي الطاهر ، سعيدة ،الجزائر 2014-2015 ص 11

[3] براهمي جمال ، **التحقيق الجنائي في الجرام الالكترونية** ، اطروحة لنيل شهادة دكتورة ، تخصص قانون جنائي ، قسم الحقوق ، كلية الحقوق وعلوم السياسة جامعة مولود معمري ، تيزي وزو ، الجزائر 2018 ص 121.

مسعاه العدالة ، أما العلم فمسعاه الحقيقة إذ يستبعد تعارضه مع القواعد العلمية السلمية فان الدليل الالكتروني له الطبيعة ذاتها ، وبجب أن لا يخرج عما توصل إليه العلم الالكتروني الرقمي و إلا فقد معناه.

ثانيا : الدليل الإلكتروني دليل تقني

بمعنى انه مستوحى من البيئة التقنية التي يتواجد فيها والمتمثلة في مختلف الأجهزة تكنولوجية و من أجهزة الحاسب و الخوادم والمضيفات والهواتف والشبكات ، ولا يمكن تصور وجود الدليل الالكتروني خارج هذا الإطار.

ثالثا: صعوبة التخلص من الدليل الالكتروني

الدليل الالكتروني يختلف عن الدليل التقليدي حيث هذا الاخير يمكن التخلص منه فمثلا اذا كان مكتوب يمكن حرقه او يمكن تهديد الشاهد بعدم الاعتراف ...الخ .

أما الدليل الرقمي لا يمكن تخلص منه بسهولة وذلك بسبب القدرة على استرجاعه من الذاكرة الميتة للحاسوب أو شبكة الاتصال أو أحد دعائمه كما يمكن نسخه في عدة أجهزة [1].

رابعا : الدليل الالكتروني دليل متطور

يعني الدليل الالكتروني يأخذ عدة أشكال قد يكون في شكل بيانات مشفرة أو شكل صور أو شكل أرقام أو رموز أو نصوص رقمية ..الخ وكل ما تطورت البيئة الالكترونية يكون في تطور مستمر معها .[2]

خامسا : الدليل الالكتروني ذو طبيعة رقمية ثنائية

ومفاد هذا أن الدليل الالكتروني يتكون من تعداد غير محدود لأرقام ثنائية في هيئة الواحد والصفر (0-1) والتي تتميز بعدم التشابه فيما بينها رغم وحدة الرقم الثنائي الذي تتشكل منه ، فمثلا المعلومات و البيانات الموجودة داخل الحاسب الآلي سواء كانت في شكل نصوص أو حروف أو أرقام

[1] **قروج حنان** ، المرجع السابق ص 13

[2] EOGHN Casey –Digital evidence and foransic science ،computer and the internet ،computer crm 1st acadimic press USA UK 2000 p9

أو صور أو تسجيلات صوتية أو فيديو ليس لها الوجود المادي الذي نعرفه في شكل ورقي ، و إنما هي مجموعة من الأرقام التي ترجع إلى أصل وحد وهو الرقم الثنائي المذكور أعلاه فما من شيء في العالم الرقمي إلا ويتكون من معادلة ثنائية قوامها الرقمان(1) و(0) ، وهما في تكونهما الحقيقي عبارة عن نبضات وذبذبات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة مع العلم أن تكوين معطيات هذه المعادلة الثنائية تختلف في الحجم والموضوع وكمية أو حجم الرقمين (1-0) في ملف يمكن أن يختلف عن كميته في ملفات أخرى ، وما يمكن استخلاصه هو أن تمتع الدليل الالكتروني بالخصائص سالفة الذكر جعلته دليلا ذا طابع خاص يختلف عن باقي الأدلة المادية المألوفة ، وأصبح على حد تعبير بعض القانونيين المختصين انه الدليل الأحسن والأفضل لإثبات في الجرائم الالكترونية لكونه مستمدا من طبيعة الوسط الذي وقعت فيه.[1]

الفرع الثالث : مشروعية الدليل الالكتروني ومناقشته

المقصود بالمشروعية الدليل هو الأساس القانوني الذي يرتكز عليه سواء في وجوده أو في اجراءات الحصول عليه وبهذا ينقسم هذا الفرع إلى قسمين الأول مشروعية وجود الدليل الالكتروني والثاني مشروعية الحصول عليه.

اولا : مشروعية وجود الدليل الالكتروني

تقتضي مشروعية وجود الدليل الإلكتروني أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثبات الجنائي ويقصد كذلك بمشروعية الوجود أن يكون الدليل معترفا به ، بمعنى أن يكون القانون يجيز للقاضي الإستاد إليه والاستدلال به لتكوين عقيدته وقناعته للحكم بالإدانة أو البراءة ، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الإلكتروني تتمثل في طبيعة نظام الإثبات السائد في الدولة ، إذ يختلف النظام القانوني في موقفها من حيث الأدلة

[1] **براهمي جمال** ، المرجع السابق ، ص 124

التي يمكن قبولها في الإثبات وهناك اتجاهان رئيسيان الاتجاه الأول هو نظام الأدلة القانونية ، أما الاتجاه الثاني فهو نظام الإثبات الحر وسنشرح هذه الاتجاهات فما بعد .

وعليه نستخلص أن مشروعية وجود الدليل الالكتروني هي اعتراف المشرع بهذا الدليل ومنحه شرعية الاثبات أمام جهة القضائية .[1]

ثانيا : مشروعية الحصول على الدليل الالكتروني

من الضروري أن يتم رسم ضوابط و أطر معينة يجب أن تمارس في نطاقها عملية البحث عن الأدلة وتحصيلها والتحقيق فيها ، بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من ورائه ، وهو الوصول إلى الحقيقة الفعلية في الدعوى وهي الهدف الاسمى لقانون الإجراءات الجزائية .

ويعني مبدأ مشروعية الحصول على الدليل الإلكتروني بما يتضمنه من مفاهيم إلكترونية ضرورة اتفاق الإجراءات مع القواعد القانونية والأنظمة المتبعة في وحدات المجتمع المتحضر ، أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القواعد القانونية ، بل يجب أن تراعي المبادئ السامية لحقوق الانسان وقواعد النظام وحسن الآداب في المجتمع[2] ، و يشترط في الدليل الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة ، وذلك يقضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن ونحن هنا نبحث عن مشروعية الدليل الإلكتروني فإننا نقتصر على ما يثير جمع هذا الدليل من إشكالات قانونية بالنظر إلى طبيعته الخاصة ، ولذا يمكننا القول أن ما يثيره الدليل الالكتروني من حيث مشروعية الحصول عليه يتركز بشكل أساسي في اجراءات التفتيش للبحث عن هذا الدليل وذلك يتم بنقطتين رئيستين وهي الصفة القائمة بالتفتيش ومدى مشروعية التفتيش عن الدليل الالكتروني و ضبطه في الوسط الافتراضي .

---

[1] يوسف جفال ، **التحقيق في الجريمة الإلكترونية** ، مذكرة ماستر ، تخصص قانون جنائي ، قسم الحقوق ،كلية الحقوق و العلوم السياسية،جامعة محمد بوضياف،المسيلة ،الجزائر،سنة 2016-2017 ص 45

[2] هلال عبد الله محمد ، **حجية مخرجات الكمبيوتر في المواد الجنائية** ، الطبعة الثانية، دار النهضة العربية ، مصر، 2008 ، ص 104

ومن المقرر أن الإدانة في أي جريمة لا بد أن تكون مبنية على أدلة مشروعية في الحصول عليها وفق قواعد الأخلاق و النزاهة ، و احترام القانون من طرف الجهة المتخصصة بجمع الدليل الالكتروني بما يتضمنه من لأدلة مستخرجة من وسائل الكترونية[1] ، و لا يكون إلا إذا أجرى التفتيش عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء و إقامته أمامه بالطرق التي رسمها القانون ، فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالته الحقيقة وذلك لعدم مشروعيته ، وعلى هذا الأساس فإن إجراءات جمع الأدلة الإلكترونية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة ، وبالتالي بطلان الدليل المستمد منها ولا تصلح أن تكون أدلة تبنى عليها الإدانة في المواد الجنائية.

ثالثا : مناقشة الدليل الالكتروني

تعني قاعدة وجوب مناقشة الدليل في المواد الجنائية أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة و خضعت لحرية مناقشة أطراف الدعوى ، و يعد مبدأ المواجهة بين أطراف الدعوى من أهم المبادئ التي يجب أن يؤسس القاضي اقتناعه على ضوءها حيث يتطلب هدا المبدأ طرح الأدلة في الجلسة ، و أن تتاح الفرصة أمام طرفي الدعوي الجنائية لمناقشة الأدلة المطروحة ويرتبط هدا المبدأ بالمبدأ القانوني العام المتمثل في ضرورة احترام حقوق الدفاع الذي يعد أحد المظاهر الأساسية لدولة القانون ، وتعتبر قاعد وجوب مناقشة الألة من القواعد الاساسية ، حيث أن عناصر الإثبات يجب أن تكون محلا للمناقشة الحضورية بين الأطراف عن طريق ممثليهم القانونيين ، بينما يكون القاضي مصغيا لكل ما يمكن أن يطرح في الجلسة ، و تبنت التشريعات ذات الصياغة المختلطة نفس النهج فقد نص قانون الإجراءات الياباني على قاعدة وجوب مناقشة الأدلة ، حيث أن أطراف الدعوى المتمثلين في النيابة العامة أو الدفاع هم الذين يقومون بدحض العناصر الإثباتية المطروحة في الجلسة ، وتحت اشراف القاضي .

[1] **يوسف جفال** ، مرجع السابق ص 46

ويترتب على مبدأ وجوب مناقشة الدليل الجنائي نتجتان هامتان **الاولى** هي عدم جواز أن يحكم القاضي بناء على معلوماته الشخصية ، فلا يجوز للقاضي أن يحكم بناء على ما رآه بنفسه أو حققه في غير مجلس القضاء[1] و بدون حضور الخصوم ، أي لا يمكن أن يستمد معلومات أو أدلة خارج الوقائع المطروحة امامه .

أما النتيجة **الثانية** فهي عدم جواز أن يقضي القاضي بناء على رائي الغير فالقاضي الجنائي يجب ان يستوفي قناعته بنفسه من التحقيق في الدعوى ، ولا يعتمد على رأي الغير وهي نتيجة مهمة تترتب على قاعدة وجوب مناقشة الدليل وتأسيسا على ذلك لا يجوز للمحكمة أن تعتمد على أدلة ووقائع استقتها من أوراق قضية أخرى [2] ، لم تكن في مضمون الدعوى التي تفصل فيها و لم تطرح على بساط البحث في الجلسة ، وعليه لا يجوز للقاضي أن يحيل الحكم في وقائع الدعوى ومستنداتها إلى دعوى أخرى غير مطروحة و هذا المبدأ لا يعني حرمان القاضي نهائيا من الأخذ برأي الغير بل يجوز له الأخذ به و اعتباره من الأدلة المقدمة في الدعوى و بناء قناعته على هذا الرأي .

وفي الاخير يتبين لنا أن إجماع التشريعات الإجرائية في مختلف النظم القانونية على وجوب عرض الدليل المقدم في الدعوى للمناقشة وفي حالة عدم عرضه للمناقشة يتم نقض هذا الحكم وذلك بسبب مخالفة مبدأ وجوب مناقشة الأدلة .

المطلب الثاني : موقف المشرع الجزائري من الدليل الالكتروني في مجال الاثبات الجنائي

لكل دولة نظام قضائي جنائي خاص ولها تشريعات تنظم هذه الانظمة القضائية ويعتبر التشريع الجزائري من بين هذه التشريعات حيث تدخل التشريع الجزائري ، و أخذ موقف من وسائل الاثبات وكيفية التعامل مع الدليل وجعل للقاضي بعض القواعد التي تساعده في اثبات صحة الدليل الالكتروني

[1] علي محمود على محمود، **الأدلة المحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي** ، بحث مقدم إلى المؤتمر العلمي الاول حول الجوانب القانونية و الأمنية للعماليات الالكترونية ، دبي، الإمارت العربية المتحدة، 2003،ص 157

[2] **يوسف جفال** ، مرجع سابق ص 47

وتساعده في تكوين قناعته وعليه سنتطرق في هذا المطلب على تعريف أنظمة الاثبات و على موقف المشرع من الاثبات الجنائي.

الفرع الاول : أنظمة الاثبات الجنائي وموقف المشرع الجزائري منها

تختلف أنظمة الاثبات في كل دولة فنهاك من تأخذ بنظام الاثبات المقيد وهناك من تأخذ بنظام الاثبات الحر وسنشرح هذه الانظمة كما يلي :

أولا : نظام الإثبات المقيد

في نظام الاثبات المقيد يقوم المشرع بتحديد سلفا وبشكل حصري الأدلة التي يجوز للقاضي قبولها والاستعانة بها في الإثبات ، وكذلك تحديد القوة الاستدلالية لكل دليل بناء على قناعته بها ، في حين لا يكون للقاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها ، وإنما يقتصر دوره على فحص الدليل للتأكد من مدى مشروعيته وتوفره على الشروط التي حددها القانون ، وفي حالة انتفاء الشروط التي يتطلبها القانون في الدليل فإن القاضي لا يسع له الحكم بالإدانة حتى ولو تكونت لديه قناعة يقينية بارتكاب المتهم للجريمة المنسوبة إليه[1].

ومن هنا يتضح جليا بأن نظام الإثبات المقيد يقوم على مبدأين أساسيين ، **الأول** يتمثل في الدور الإيجابي للمشرع في عملية الإثبات لكونه الذي ينظم قبول الأدلة سواء عن طريق التعيين المسبق للأدلة المقبولة للحكم بالإدانة أو باستبعاد أدلة أخرى ، أو بإخضاع كل دليل لشروط معينة ولكونه الذي يحدد القيمة الإقناعية لكل دليل بأن يضفي الحجية الدامغة على بعض الأدلة والحجية النسبية على بعضها الآخر ، أما المبدأ **الثاني** فيتمثل في الدور السلبي للقاضي الجزائي في الإثبات إذ يلتزم التزاما صارما بما يرسمه له المشرع سلفا من أدلة إثبات على نحو يفقده سلطته في الحكم بما يتفق مع الواقع

[1] رمزي رياض عوض ، **مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها** ، د ارسة تحليلية تأصيلية مقارنة ، دار النهضة العربية، القاهرة، ،1997ص .85

فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام فيصبح القاضي كالآلة في إطاعته لنصوص القانونية .

و لذلك فقد إنتقد الفقه الجنائي هذا النظام بشدة خاصة فيما تعلق منه بتجريد القاضي من وظيفته الطبيعية المتمثلة في فحصه الدليل المعروض أمامه بكل حرية وتقدير قيمته لاقناعية وفقا لضميره المهني ، ومن ثم تكوين اقتناعه الشخصي ومنحها للمشرع ليحل بذلك محل القاضي بل أكثر من ذلك جعل اقتناع القاضي متوقفا على اقتناع المشرع ، بما يمليه عليه هذا الأخير من أدلة إدانة على سبيل الحصر ومن المسائل التي انتقدت في هذا النظام ، قيامه بتقنين اليقين بنصوص قانونية سلفا رغم أن اليقين مسالة يطرحها الواقع ترتبط بالظروف الخاصة والمتغيرة لكل قضية وتترك لتقدير قاضي الموضوع.

ونتيجة لهذه الانتقادات تراجع العمل بنظام الإثبات المقيد بشكل سريع في الآونة الأخيرة وتقلص نطاقه حتى في الدول التي تعتبر الأكثر اعتناقاً له ، فنجد بريطانيا مثلا وهي الدولة المؤسسة لهذا النظام قد بدأت تخفف منه ، وظهر فيها ما يعرف بقاعدة الإدانة دون أدنى شك ، والتي مفادها أن القاضي يستطيع أن يبني عقيدته من أي دليل و إن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قطعياً في دلالته.[1]

ثانيا : نظام الإثبات الحر

وهو نظام يسود فيه مبدأ حرية الإثبات إذ لا يحدد فيه المشرع طرقا معينة للإثبات ولا حجيتها أمام القضاء ، إنما يترك ذلك للقاضي الجزائي الذي يكون له دور ايجابي في البحث عن الأدلة المناسبة وتقدير قيمتها الثبوتية حسب اقتناعه بها ، فلا يلزمه القانون بالاستناد إلى أدلة معينة لتكوين قناعته فله أن يبني هذه القناعة على أي دليل يقدم في الدعوى و إن لم يكن منصوصا عليه مسبقا ،بل أن المشرع في مثل هذا النظام لا يختص بالنص بشكل محصور على أدلة الإثبات فكل الأدلة تتساوى قيمتها في نظر المشرع ، والقاضي هو الذي يختار من بين ما يطرح عليه من الأدلة ما يراه مفيدا للوصول إلى الحقيقة

[1] **رمزي رياض عوض** ، المرجع السابق ، ص 86

وهو في ذلك يتمتع بمطلق الحرية في قبول الدليل أو طرحه جانبا إذا لم يطمئن إليه، ودون أن يكون مطالبا بتسبيب اقتناعه .

ويجد هذا النظام مبرراته في كون الإثبات في المسائل الجزائية لا ينصب إلا على وقائع مادية أو نفسية خاصة بالجريمة ، ولا ينصب على تصرفات قانونية يتفق معها قيام المشرع سلفا بتحديد وسائل إثباتها ومدى الحجية التي تتمتع بها ، كما أن الإثبات ينصرف إلى وقائع إجرامية غالبا ما يعتمد الجناة بقدر المستطاع إلى إزالة ومحو آثارها ، الأمر الذي يحتم تحويل القضاء كافة الوسائل المتاحة والممكنة لكشف الجريمة وتقصي الحقيقة[1].

وعلى عكس نظام الإثبات المقيد فإن فلسفة هذا النظام ترتكز ايضا على مبدأين مختلفان **الأول** يتمثل في الدور السلبي للمشرع في عملية الإثبات ، ومن خلاله يمتنع المشرع عن تحديد الأدلة التي تصلح للإثبات مسبقا ، وهو ما يفتح المجال لأن تكون جميع الأدلة مقبولة وفقا لتقدير القاضي وليس المشرع ، كما يمتنع عن تحديد القيمة الاقناعية للدليل أو إظهار أي تسلسل بين هذه الأدلة في الحجية أو يرّجح أي دليل على الآخر ، أما المبدأ **الثاني** فهو الدور الإيجابي للقاضي الجزائي في الإثبات ويبدو ذلك من ناحتين ، فمن الناحية الأولى هي الحرية المطلقة التي يتمتع بها القاضي الجزائي في إثبات حقيقة الجريمة بكافة طرق الإثبات ، وسلطته الواسعة في اتخاذ جميع التدابير و الإجراءات التي يعتقد أنها مفيدة لإظهار هذه الحقيقة كسماع الشهود ، وندب الخبراء واستدعائهم ليقدموا إيضاحات عن التقارير المنجزة من طرفهم ،كما له أن يأمر باستكمال التحقيق إذا ما كانت عناصر الإثبات التي بين يديه غير كافية أو غير مقنعة.

[1] عفيفي كامل عفيفي ، **جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون** ، د ارسة مقارنة، منشو ارت الحلبي، دمشق، 2007 ص397

ثالثا : نظام الإثبات المختلط

وهو نظام وسط بين نظام الإثبات المقيد ونظاما لإثبات الحر، وفيه تم التصدي للانتقادات الموجهة لنظام الإثبات الحر حول خشية تعسف القاضي الجزائي و خروجه عن جادة الصواب ، كما تم تلاقي ما وجه من انتقادات لنظام الإثبات المقيد وذلك بأن حدد له وسائل الإثبات التي يلجأ إليها لتأسيس حكمه ، لما جعل دور القاضي سلبيا في عملية الإثبات ، وذلك من خلال إعطاء القاضي الجزائي الحرية في تقدير ووزن ما يعرض عليه من أدلة ثبوتية وفقا لاقتناعه الشخصي.

و من هنا يتبين بأن منطق هذا النظام يرتكز من جهة على تحديد قائمة أدلة الإثبات والقيمة الإثباتية لكل منها سلفا من قبل المشرع ، ومن جهة أخرى منح القاضي الجزائي سلطة تقديرية واسعة في موازنة وقبول الأدلة المطروحة أمامه ، وفقا لاقتناعه الذاتي.

و اعتبارا لما سبق نستنتج بأن مسألة مشروعية الدليل الالكتروني في الوجود تثور بالدرجة الأولى في الأنظمة القانونية التي تتبنى نظام الإثبات المقيد ، إذ لا يمكن في ظلّها الاعتراف للدليل الالكتروني بأية قيمة إثباتية ما لم ينص عليه القانون صراحة ضمن قائمة أدلة الإثبات المقبولة ، ومن ثم لا يجوز للقاضي الجزائي أن يستند إليه لتكوين قناعته مهما توافرت فيه شروط اليقين فيه ، أما بالنسبة للأنظمة القانونية التي تعتمد نظام الإثبات الحّر كما هو الحال في القانون الجزائري ،فمسألة مشروعية وجود الدليل الالكتروني لا تثار إطلاقا ، على اعتبار المشرع الذي لم يقيد القاضي بقائمة أدلة الإثبات فالأساس هو حرية الأدلة ، لذلك فمسألة قبول الدليل الالكتروني لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه لتقدير القاضي[1].

رابعا : موقف المشرع الجزائري من أنظمة الاثبات الجنائي

إن الإثبات الجنائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل بوجود الدليل على ذلك ، ويعتبر الدليل الوسيلة القانونية التي

[1] **براهمي جمال** ، المرجع السابق ، ص 143

يستعين بها القاضي للوصول إلى الحقيقة وكشف الجريمة ونسبتها إلى المتهم ، وقد ذهب الفقه الإجرائي إلى وضع نظامين إجرائيين في مجال الإثبات الجنائي يختلفان فيما بينهما من حيث الأسس التي يقوم عليها كل واحد منها وقد سبق الإشارة إليهما ، و تنتمي الجزائر إلى مجموعة الدول التي تتبنى نظام الإثبات الحر في مجال الإثبات الجنائي ، فهي تساير النظم اللاتينية كفرنسا وبلجيكا والأردن وسوريا ، وهو الأمر الذي كرستها لمادة 212 من قانون الإجراءات الجزائية التي جاء في نصها على أن يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص القانون غير ذلك ، و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ، ولا يجوز للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه وبهذا فان موقف المشرع بصفة عامة أخذ بنظام الاثبات الحر وبصفة استثنائية في بعض الجرام أخذ بنظام اثبات المقيد كجريمة الزنا المنصوص عليها في المادة 339 و 341 من ق.ع ، أما إقرار المشرع الجزائري للحرية في تقديم الأدلة وتركها للقانعة الشخصية لقاضي الموضوع هو عبارة عن تعزيز إثبات قرينة البراءة ، وتعزيز لممارسة حقوق الدفاع الفردية ، غير أن هذا الإطلاق بدون تحديد وتخصيص يعد قصورا تشريعيا واضحا فلا نجد ضمن قانون الإجراءات الجزائية ما يدل على أن الدليل الالكتروني ، هو دليل من نوع خاص شأنه شان الجرائم الإلكترونية ، فغياب أدنى نص قانوني في هذا الشأن يؤدي إلى ظهور إشكالات متعلقة بطبيعة

الأدلة المقدمة أمام الجهات القضائية بحيث يمكن لهذه الأخيرة وفي حال عدم إلمامها بتقنية المعلوماتية دحض هذا الدليل وعدم الاعتداد به ، ولو كان حائزا على القوة الثبوتية ، وتتوفر فيه كافه شروط الصحة وكذلك العكس صحيح[1].

الفرع الثاني : تعريف مبدأ الاقتناع الشخصي للقاضي

يعتبر مبدأ حرية الاقتناع الشخصي للقاضي الجزائي من أهم العناصر الاثبات في الدعوى الجنائية فالقاضي حر بأن يأخذ بالأدلة التي يرها مناسبة للكشف عن الحقيقة ، وله ان يتحرى بنفسه صدق

[1] يوسف جفال ، المرجع السابق ، ص 52

الادلة التي يرها مناسبة ، للكشف عن الحقيقة وله أن يتحرى بنفسه صدق الادلة كما أنه حر في تقديرها و له الحق في أن يستمد اقتناعه وعقيدته من أي مصدر يطمئن إليه ،كما أن الاقتناع في دلالاته القانونية يعني حاله إدراك يسلم معها العقل تسليما جازما بثبوت أو نفي واقعة أو عده وقائع استنادا لقواعد المنطق القائمه على الاستقراء والاستنتاج والمستمدة من أدله وبراهين قضائية حاسمة ، وحرية الاقتناع هي حرية خاصة بالقاضي من خلالها يعمل سلطته التقديريه ويبسطها على الادلة الجنائية وهذا ما يميز قاضي الجنائي عن دور القاضي المدني ، الذي يقتصر على موازنة بين الأدلة التي يقدمها الاطراف دون البحث عن حجج اخرى من تلقاء نفسه.[1]

وبما أن السائد في الفقه هو ان سلطه القاضي الجنائي يحكمها مبدأ الاقتناع القضائي أو الاقتناع الشخصي للقاضي حيث هذا المبدأ يؤدي بنا الى نتيجتين **الأولى** هي حرية القاضي في قبول الادلة **والثانية** هي حرية القاضي في تقدير الادلة ومنه عند الشروع في تقدير الادلة يتأكد القاضي من مشروعيه هذا الدليل اي طبقا لمبدأ الشرعيه الاجرائية وعليه عند تأكده من شرعية هذا الدليل.

و يخول القانون للقاضي حرية واسعة في البحث عن الادلة وتقديرها فإذا استراح ضمير القاضي ووجد هذه الأدلة كافيه ومنطقيه فيمكنه ان يستمد قناعته منها ويعول عليها في الحكم الذي ينتهي اليه، غير أن هذه الحرية احاطها المشرع بضوابط معينه ولم يتركها مطلقة خوفا من تعسف القاضي في استعمال قناعته خصوصا مع ظهور الدليل الرقمي أو الالكتروني للإثبات ، و اضطر القاضي معه لكشف انماط جديدة من جرائم المعلوماتية ، و في المقابل نقص الثقافة المعلوماتية لدى القاضي نهيك عن المشكلات التي تثيرها الطبيعة العلميه للدليل الالكتروني فهو دليل غير مرئي قابل للمحو والتعديل بما يثير صعوبة كبيره في استخلاصه ، وهذا ما يؤدي إلى إنقاص قيمته في إثبات الجرائم الالكترونية وفي هذا شأن كرس المشرع الجزائري هذا المبدأ بموجب المادتين 212 و 307 من قانون الاجراءات الجزائية حيث نصت الماده 307 أن القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي بها قد وصلوا إلى

[1] يزيد بوحليط ، المرجع السابق ، ص 412

تكوين اقتناعهم ولا يرسم لهم قواعد يتعين عليهم أن يخضعو لها ،[1] و استثناء لهذا المبدأ فان كل جريمة تتمتع بوصف خاص سواء كانت جنحة او مخالفة او جناية والجدير بالملاحظة هنا أن هذا المبدأ (اقتناع القاضي) هناك قاعدة التسبيب الأحكام القضائية عندما يتعلق الامر بالجنايات فإن القضاة غير مطالبين بتسبب أحكامهم ولا رقابة جهات الطعن عليهم أما اذا اخذ الجرم جنحة يختلف الامر لان محكمة الجنح هي محكمة دليل مما استوجب على القضاة تسبب احكامهم وخضوع لرقابة جهات الطعن عليهم وهذا استثناء للقاعدة العامه المنصوص عليها في الماده 307 قانون الاجراءات الجزائية .

وبعد تعريف بمبدأ الاقتناع الشخصي للقاضي إستوجب التلميح إلى وسائل تكوين هذا الاقتناع حيث الجهد الاستنباطي الذي يبذله القاضي من خلال نشاطه العقلي المكون لقناعته ، والذي ينصرف إلى إفراز الحقيقة من الدليل محل تقديره يرتكز فيه القاضي على قبول جميع الادلة المطروحة امامه في الجلسة ، ولا يحضر على القاضي أو يفرض عليه دليل محدد ولا يتقيد إلا بقيد مشروعيه الدليل و أنه قد تم طرحه للمناقشة بالجلسة و أن يقوم القاضي بوزن كل دليل على حدى عن باقي الادلة المطروحة أمامه وله أن يهدر أي دليل مهما كانت قيمته طالما انه لم يطمئن اليه ،كذلك سلطه القاضي في تنسيق الادلة المطروحة أمام ومساندة الادلة لبعضها البعض او ما يعرف بتساند الادلة .[2]

الفرع الثالث : ضوابط التي تحكم إقتناع القاضي الجنائي بالدليل الإلكتروني

القاضي الجنائي و إن تمتع بسلطة واسعة في تقديره للأدلة بما في ذلك الدليل الالكتروني فله أن يتحرى الحقيقة بكافه الأدلة دون الزامه بقيمة مسبقة بالدليل ما ، حتى ولو كان الدليل علميا كالدليل الالكتروني او تحديده لنوع معين من الأدلة لا يجوز الاثبات بغيرها غير هذه السلطة وخلافا لما ذهب اليه الفقه اعتبرها القضاء بأنها سلطة مطلقة وتحكمية غير أن المشرع وضع لها ضوابط وهي بمثابه صمام أمان

[1] ناير نبيل عمر ، **الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية** ، دار الجامعة الجديدة ، الاسكندرية مصر ، 2010 ، ص 179

[2] **يزيد بوحليط** ، مرجع السابق ، ص 413

ايذاء انحراف القاضي عند ممارسه لها وتنقسم هذه الضوابط الى قسمين ضوابط المتعلقة بمصدر الاقتناع وضوابط متعلقة ببلوغ الاقتناع ذاته .

أولا : الضوابط المتعلقة بمصدر الإقتناع

في هذا الشأن يحكم اقتناع القاضي بالأدلة الالكترونية ضابطان هما :

أ) شروط قبول الدليل الالكتروني :

باعتبار القاضي ليس حرا في تقدير اي دليل كان بل هو حر في فقط في تقدير الدليل الالكتروني المقبول في الدعوة بمعنى الحصول عليه بطريق مشروع اعمالا لمبدا الشرعية الإجرائية ، وبالتالي يستبعد في المقابل ذلك من المرافعات سائر الأدلة الإلكترونية غير غير المقبولة لأنها لا تدخل ضمن عناصر تقديره ،وعليه لا يجوز للقاضي الاستناد إلى دليل استمد من اجراءات باطلة لان ما بني على باطل فهو باطل.

ب) شرط وضعية الدليل الالكتروني :

من المعروف في القواعد الأساسية في الاجراءات الجنائية أنه لا يجوز للقاضي أن يبني حكمه على الأدلة لم تطرح للمناقشة الخصوم في الجلسة ، و المقتضى ذلك أن يكون الدليل أصل ثابت في أوراق الدعوة نتاجة للخصوم فرصة الاطلاع عليه ومناقشته ، ويقوم هذا الشرط على مبدأ الشفوية و المواجهة في المحاكمة الجنائية وهو مبدأ اساسي في الاجراءات الجزائية نص عليها المشرع الجزائري بموجب الماده 212 فقره 2 من قانون الاجراءات الجزائية ، التي تنص لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات التي حصلت المناقشه فيها حضوريا امامه [1]، اذ ينبغي على القاضي ان يطرح كل دليل مقدم في الدعوى للمناقشة امام الخصوم في الجلسة حتى يكونوا على علم مما قدم ضدهم من أدلة قصد تمكينهم من الدفاع ومواجهة هذه الاهتمامات و دحنها ، ويترتب على ذلك انه لا يجوز للقاضي الجنائي أن يبني اقتناعه على دليل قدمه أحد الاطراف الدعوى إلا اذا تم عرضه في الجلسات المحاكمة وخضع للمناقشة الاطراف.

[1] **يزيد بوحليط** ، المرجع السابق ،ص 415

ثانيا : الضوابط المتعلقة بالاقتناع ذاته

يتيح مبدأ الاثبات الجنائي حرية كبيره للقاضي في تقدير عناصر الاثبات بما في ذلك الأدلة الرقمية وعليه فان التقدير كفاية أو عدم كفاية الدليل الالكتروني في إثبات الجريمة الالكترونية ونسبتها إلى مرتكبها ،أمر متروك لمحكمه الموضوع المعروض عليها الدليل ولا تخضع في ذلك لرقابه محكمه النقض التي يقتصر دورها على مراقبه المنطق القضائي لمحكمة الموضوع عن طريق رقابتها على صحة التسبيب الحكم ، وعليه لبلوغ القاضي درجه الاقتناع التام للفصل في القضية لابد له من شروط تتمثل في ما يلي : [1]

أ) بلوغ الاقتناع القضائي درجه اليقين

تقتضي العدالة أن يصدر القاضي حكمه عن إقتناع يقيني بصحة ما ينتهي إليه من وقائع لا مجرد الظن والاحتمال ، لان الشك يفسر لصالح المتهم وهذا ما ينص على قرينة البراءة المنصوص عليها في الدستور الجزائري لسنة 2020 في الماده 41 ، كما انا شرط اليقين هو شرط عام تستوي فيه الأدلة الرقمية مع الأدلة التقليديه ويقوم اليقين القضائي على عنصرين **الاول** شخصي يتمثل في إرتياح ضمير القاضي حول ادانة المتهم و**الثاني** موضوعي يقوم على أدله من شأنها أن تؤدي لذلك وفقا لمقتضيات العقل والمنطق.

ب) توافق الاقتناع القضائي مع مقتضيات العقل والمنطق

ومعنى ذلك أن يكون إستخلاص محكمه الموضوع لوقائع الدعوى استخلاصا معقولا سائغا أن معيار المعقولية للاقتناع بما في ذلك الأدلة الرقمية هو أن تكون هذه الأدلة مؤديه إلى ما رتبه الحكم عليها من غير تعسف في الاستنتاج وتتعارض مع مقتضيات العقل والمنطق.

[1] **نعيم مغبغب** ، المرجع السابق ، ص 82

المبحث الثاني : القواعد لإجرائية لاستخلاص الدليل الالكتروني

إذا كانت ظاهرة الإجرام الالكتروني قد أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي ، بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم واحترام مبدأ الشرعية والتفسير الضيق للنصوص الجزائية ، فقد أثارت في الوقت نفسه مشكلات أكثر في نطاق القانون الاجرائي الجزائي ، وتزداد المشكلات الإجرائية في مجال الجرائم الالكترونية بتعلقها في العديد من الأحيان ببيانات المعالجة الآلية وكيانات منطقية غير مادية ، ومن ثم يصعب الكشف عنها وإثباتها نظرا للسرعة الفائقة والدقة غير المتناهية في تنفيذها ، ناهيك عن إمكانية محوها و تمويه آثارها وإخفاء الأدلة المتحصل منها بسهولة عقب تنفيذها باستعمال تقنيات تكنولوجيا عالية ،وعليه تم وضع قواعد اجرائية تستخدم نفس التقنية التي يستخدمها المجرم المعلوماتي للوصول إلى الدليل ، و سنتطرق إليها في هذا المبحث بالتفصيل ،حيث المطلب الأول يتمثل في القواعد الاجرائية التقليدية لاستخلاص الدليل الالكتروني ، والمطلب الثاني القواعد الاجرائية المستحدثة لاستخلاص الدليل الالكتروني .

المطلب الأول : القواعد الإجرائية التقليدية لاستخلاص الدليل الالكتروني

في بداية الامر لم يكن خيار للجهات القضائية في التصدي للجريمة المعلوماتية، إلا عن طريق توسيع من صلاحيات الاجراءات التي كانت موجودة ، وذلك من أجل محاربة الجريمة المعلوماتية بشكل مؤقت إلى غاية دراسة هذه الجريمة ومعرفة ما يتوجب استحداثه من النصوص لمكافحتها ، وحاول المشرع في بداية ظهور هذا النوع من الجرائم توسيع صلاحيات الاجراءات مثل المعاينة والتفتيش وضبط الادلة والتي سنتطرق لها في هذا المطلب كما يلي :

الفرع الاول : المعاينة والخبرة الفنية

تعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة ، ومن أهم إجراءات التحقيق على الإطلاق ، نظراً لما يمكن أن توفره من أدلة إثبات ، وتزداد أهميتها أكثر إذا تعلق الأمر بالجرائم الالكترونية وتعتبر الخبرة الفنية عمود الاساسي لتحقيق في الجريمة المعلوماتية وذلك بسبب تفسير الجانب الفني للمحقق بالنسبة لهذه الجرائم .

اولا : المعاينة

هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها كذلك جميع الأشياء الأخرى التي تفيد في كشف الحقيقة ، واتخاذ ما يلزم من إجراءات كضبط بعض الأشياء فالهدف من المعاينة هو لغرضين اثنين **الأول** جمع الأدلة الناتجة عن الجريمة (الآثار) ، و **الثاني** إتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة لكي تكون لديه فكرة واضحة لا لبس فيها وكشف الغموض عن كيفية وقوع الجريمة ، ولقد أشارت قوانين الإجراءات الجنائية إلى إجراء المعاينة باعتبارها إجراء من إجراءات التي تمتلكها السلطات التحقيق بمختلف فئاتها[1] وطوائفها ، وهذا ما ورد في نص المادة 79 من قانون الإجراءات الجزائية الجزائري " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها ، والمعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يرى المحقق أن لها صلة بالجريمة ، والأصل أن إجراء المعاينة متروك لتقدير المحقق لا يقوم بها إلا إذا كان هناك فائدة من ورائها ، كما أن هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة ، وهي حالة إخطارها بجناية متلبس بها ويرى البعض أن أهمية المعاينة تتضاءل في الجريمة الإلكترونية وذلك لندرة تخلف الآثار المادية عند ارتكاب الجريمة

[1] **بخي فاطمة الزهراء** ، المرجع السابق ، ص 83

الإلكترونية ، كما أن طول الفترة [1] بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار ، فعند تلقي بلاغ عن وقوع إحدى الجرائم الإلكترونية وهذا بعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته.

ومسرح الجريمة الإلكترونية يختلف عن مسرح الجريمة التقليدية كالقتل والسرقة فالجريمة الإلكترونية قد تكون جريمة مستمرة كما في حالة الجرائم ، (السرقة والاحتيال) وقد يكون مسرحها كالجرائم الأخرى كما في التزوير وإتلاف البرامج وتفجير المباني والمنشآت ، ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية تكون المعاينة هدفها المداهمة وضبط الأدلة على طبيعتها ، وفي الحالة الثانية وبعد وقوع الجريمة فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم وكذلك شهادة الشهود والقرائن ، وعند إجراء المعاينة بعد وقوع الجريمة في المجال الإلكتروني فيجب مراعاة الإجراءات التالية عند الانتقال إلى مسرح الجريمة :[2]

* ضرورة وجود معلومات مسبقة عن مكان الجريمة.

* مراعاة الأجهزة المطلوب معاينتها و معاينة شبكاتها مع وجود خريطة تبين الموقع المراد معاينته.

* تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة سواء من الضبط أو التأمين أو حفظ الأوراق.

* يجب على القائمين بالمعاينة ، تأمين الأجهزة التي يتم الاستعانة بها خلال إجراء المعاينة

* يجب إعداد فريق جاهز نفسيا و فنيا من أجل تنفيذ المعاينة بشكل متناسق مع بعضه البعض.

* مراعاة القوانين الاجرائية وذلك لي تجنب خرق مبدأ شرعية الاجرائية والذي يؤدي الى البطلان الدليل.

[1] خالد ممدوح ابراهم ، **فن التحقيق الجنائي في الجرائم الالكترونية** ، المرجع السابق ، ص 145

[2] **بخي فاطمة الزهراء** ، المرجع السابق ، ص 85

ثانيا : الخبرة الفنية

تعتبر الخبرة من الاجراءات التي تساعد التحقيق في الجانب الفني للجريمة ويعتمد عليها المحقق وهي كما يلي :

أ) تعريف الخبرة :

الخبرة القضائية هي استعانة الجهة القضائية بشخص مختص ينعت بالخبير حيث هذا الاخير يكون مختص في مجال معين ، يساعد القاضي في تفسير وقائع أو دليل أو تقنية علمية لا يمكن لشخص العادي تفسيرها.[1]

وهناك من يعرفها انها هي التفسير الفني للأدلة أو الدلائل عن طريق الاستعانة بمعلومات الخبير وكذلك ، يعرفها البعض بأنه كل شخص له دراية بمسالة من المسائل وقد يستدعي التحقيق فحص مسالة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه فيمكنه أن يستشير فيها خبيرا كما هو الحال في تقرير طب الشرعي ، في جرائم القتل أو تحليل المادة موضوعة في الاكل في جريمة تسمم أو فحص لخطوط الكتابة او تحليل حمض نووي ...الخ من خبرات .[2]

ب) الخبرة في الجريمة المعلوماتية :

من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة الإلكترونية ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات ، وكذلك إعداد البرمجيات وتشغيل الحاسب الآلي وعلومه ، وأن نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء ، وكذا يجب على المحقق الجنائي أن يحدد للخبير الإلكتروني دوره في المسالة الانتداب فيها على

[1] مروك نصر الدين ، **محاضرات في الإثبات الجنائي** ، دار هومة ، الجزائر ، جزء الأول ، 2003 ، ص 390

[2] فائدة فاطمة الزهرة ، **التحقيق الجنائي في الجرائم الإلكترونية** ، مذكرة ماستر ، تخصص القانون الجنائي والعلوم الجنائية ،قسم حقوق كلية الحقوق والعلوم السياسية ، جامعة محمد بوضياف ، مسيلة الجزائر 2020-2021 ص 37

وجه الدقة ، وبالنظر إلى أن الجريمة الإلكترونية لها الخصوصية التي تتعلق بها فإن الخبير الإلكتروني قد يكون من الجناة الذين سبق لهم ارتكاب مثل هذه الجرائم وتم تذويبهم داخل المؤسسات الإلكترونية للاستفادة من قدراتهم فضلا عن تأهيلهم كمواطنين صالحين.

ج) أساليب عمل الخبير في الجريمة الإلكترونية :

لعمل الخبيرة هناك اسلوبين وهما التالي : [1]

الأول : القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كجريمة التهديد أو النصب ،جرائم النسخ ..الخ ، ثم يقوم الخبير بعملية تحليل رقمي لها ، وذلك لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه ، وتحديد عناصر حركتها ، وكيف تم التوصل إلى معرفتها وأخيرا التوصل لمعرفة برتوكول الانترنت " IP" الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع.

الثاني : القيام بتجميع وتحصيل لمجموعة المواقع التي لا تشكل موضوعها جريمة في ذاتها ، ولكن الجرائم تقع من جراء تتبع موضوعات هته المواقع ، مثلما ما هو الحال في المواقع التي تساعد الغير على معرفة جرعات المخدرات والمؤثرات العقلية حسب وزن الإنسان ، بإيهامه أنه إذا تم تتبع التعليمات الواردة فيها لن يصل الشخص إلى حالة إدمان ، وكذلك الشأن بالنسبة لكيفية إعداد القنابل وتخزينها أو كيفية التعامل مع القنابل الزمنية ... الخ .

ويعم الخبير أيضا على مساعدة المحقق في تحصيل الدليل من البيئة الالكترونية دون إتلافه أو حذفه وذلك عن طريق ما يكتسبه هذا الخبير من مهارات ، مثل خبرته في تعامل مع نوع الجهاز ونقل الدليل من جهاز إلى جهاز وفك الرموز المشفرة برمجة نظام الحماية معرفة تصرفات وتحركات الجاني في البيئة الافتراضية ... الخ .

[1] **فائدة فاطمة زهرة** ، المرجع السابق ، ص 38

الفرع الثاني : التفتيش

يتطلب التحقيق أحيانا تفتيش شخص المتهم أو منزله أو غيره لضبط الأشياء المتعلقة بالجريمة ، والتفتيش كإجراء من اجراءات التحقيق الابتدائي هو في الأصل من اختصاص سلطة التحقيق المتمثلة ، في قاضي التحقيق والنيابة العامة ، إلا أنه يخول استثناء لرجال الضبطية القضائية في الحالات المحددة قانونا.

وقد جمع الفقه الجنائي أن التفتيش هو إجراء من إجراءات التحقيق ، يستهدف البحث عن الحقيقة في مستودع السر لذلك يعتبر من أهم الإجراءات لأنه غالبا ما يسفر عن أدلة مادية تؤدي إلى نسبها للمتهم ، و المستهدف في التفتيش بالنسبة للجريمة المعلوماتية هو الحاسوب بمكوناته المادية والمعنوية .[1]

فالأولى هي وحدات لكل منها وظيفة معينة متصلة ببعضها البعض في شكل نظام متكامل و الثانية هي الكيانات المنطقية مثل برامج ونظم المعلوماتية والبيانات فعندما يستهدف التفتيش الكيانات المادية لا يشكل عائق ، وإنما الإشكال يثور عندما ينصب على المكونات المعنوية لأنه هنا يتطلب الكشف عن الرقم السري للمرور إلى الملفات أو الشفرات أو ترميز البيانات.

اولا : تفتيش مكونات المادية للحاسوب

التفتيش بالنسبة للمكونات المادية لا يوجد اشكال حول إمكانية خضوعها للتفتيش ، غير أن ذلك يتوقف على طبيعة المكان فإذا كان المكان خاص لا يجوز تفتيشها إلا بنفس الضمانات المقررة قانونا في التفتيش التقليدي أما اذا كان المكان عام لا يجوز التفتيش إلا بنفس الضمانات والقيود المرتبطة بتفتيش الاشخاص .

[1] **نايري عائشة** ، المرجع السابق ، ص 48

ثانيا: تفتيش مكونات المعنوية للحاسوب

عرف الفقه اختلاف حول مدى خضوع المكونات المعنوية للحاسوب لإجراءات التفتيش و انقسم إلى اتجاهين ، اتجاه يرى عدم جواز تفتيش المكونات المعنوية للحاسوب ، وقد عملت الدول التي تبنت هذا الاتجاه إلى حماية هذه الكيانات المنطقية عبر قانون الملكية الفكرية ، واتجاه آخر يرى إمكانية تفتيش المكونات المعنوية للحاسوب لأن كل ما يشغل[1] حيزا ماديا في فراغ معين ، جاز تفتيش هذا الحيز و يمكن قياسه والتحكم فيه ، وبناءا عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ، ويمكن قياسه بمقياس معين هو" البايت" و" الكيلوبايت "و "الميغابايت"، وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسوب بعدد الحروف التي يمكن تخزينها فيها ، غير أن النصوص القانونية التي تنص على أحكام التفتيش تم سنها قبل أن يعرف القانون الأشياء غير المادية ، لذا فإن طبيعة البيانات و المعطيات المعالجة تتطلب قواعد خاصة تحكمها ، فالنصوص التقليدية الخاصة بالتفتيش لا يمكن إعمالها على النظم المعلوماتية ، لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائية.

الفرع الثالث : ضبط دليل الإلكتروني

يعتبر ضبط الأشياء المتعلقة بالجريمة هو الأثر المباشر للتفتيش ، ولذلك نجد أن التشريعات الإجرائية تجمع عادة بين أحكام الضبط والتفتيش في موضع واحد لكن ليس معنى ذلك ان الضبط هو التفتيش اذ قد يكون نتيجة معاينة وغيرها وهو ما سنتناوله كالأتي :

أولا : تعريف ضبط الأدلة الإلكترونية

هو وضع اليد على شيء يتصل بالجريمة ويفيد في كشف الحقيقة عنها وعن مرتكبيها وهو يرد إلا على الأشياء المادية ، وبالتالي الصعوبة في ضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر بالبصمات مثلا ، وإنما تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في اتلاف البرامج مثل

[1] زبيحة زيدان ، **الجريمة المعلوماتية في التشريع الجزائري والدولي** ، دار الهدى للطباعة والنشر، الجزائر، ،2011 ص 131

الفيروس وكذا المكونات المعنوية للحاسوب ، وفي هذا الإطار اختلفت التشريعات الإجرائية والاتجاهات الفقهية حول مسألة ضبط الأشياء المعنوية والكيانات المنطقية التي لا تصلح بطبيعتها محلا لوضع اليد ، وانقسم ذلك إلى اتجاهين وهما :

الاتجاه الاول : يرى أصحاب هذا الاتجاه أنه يمكن تصور اجراء ضبط على الكيانات المعنوية للحاسب الألي لانتقاء الكيان المادي عنها ، وبالتالي عدم صلاحيتها ومن بين التشريعات التي أخذت بهذا الاتجاه التشريع الألماني[1].

الاتجاه الثاني: يرى أصحاب هذا الاتجاه أن المعطيات المخزنة أليا تصلح أن تكون محلا للضبط المنصوص عليه في النصوص التقليدية.

غير أن المشرع الجزائري تدخل بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال حيث قررها أليات خاصة منها :

* حجز المعطيات المعلوماتية عندما تكتشف السلطة التي تباشر في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنه ليس من الضروري حجز كل منظومة ، يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز.

* حجز هذه المعطيات عن طريق منع الوصول إليها ، ويتم ذلك عادة عن طريق الترميز أو بتقييد الدخول إلى تلك المنظومة ، أو عن طريق أية وسيلة الكترونية.

*حجز المعطيات ذات المحتوى الإجرامي للمجرم وتقع تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به في قانون العقوبات وقانون الإجراءات الجزائية الجزائري ، حيث لا يجوز استعمال المعلومات

[1] ابتسام بغو ، **اجراءات المتابعة الجزائية في الجريمة المعلوماتية** ، مذكرة ماستر ، تخصص القانون الجنائي للأعمال ، قسم الحقوق ، كلية الحقوق والعلوم السياسية ، جامعة العربي بن مهدي ام بواقي ، الجزائر 2015-2016 ص 29

المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات والتحقيقات القضائية[1].

ثانيا : أنواع الأدلة الالكترونية

من بين الأشياء أو الأدلة التي تضبط وتحتفظ بها في الجرائم المتعلقة بالجريمة المعلوماتية والتي لها قيمة في اثبات تلك الجريمة وتنسبها الى المتهم :

* **الورق** :على الرغم من أن الكمبيوتر قلل من استخدام أو حجم الأوراق والملفات التقليدية ، حيث يتم حفظ المعلومات لأغراض المراجعة أو التأكد من الشكل العام ، للمستند او الرسالة وبالتالي فهي تعتبر من الأدلة التي ينبغي الاهتمام بها.

* **ضبط جهاز الكمبيوتر وملحقاته** : أي أن وجوده وضبطه امر مهم جد للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو أنها مرتبطة بالمكان أو الشخص الحائز على الجهاز ولأجهزة الكمبيوتر أشكال وأنواع مختلفة الامر الذي يتطلب على ضباط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه ومواصفاته بسرعة فائقة أما بنفسه أو بواسطة خبير.

* **البرمجيات** (**software**) : إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بالتثبيت وتنصيب هذا البرنامج امر في غاية الأهمية عند فحص الدليل[2].

* **وسائل التخزين المتحركة** :كالأقراص المدمجة "أقراص الليزر، والأقراص المرئية والأشرطة المغناطيسية وغيرها.

[1] **ابتسام بغو** ، المرجع سابق ص 30

[2] La preuve électronique, consulté le 19/09/2022, Site électronique: www.internetjuridique.net.

* **المودم** (**modem**): وهي الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الانترنت .

* **ضبط البريد الالكتروني** :عن طريق تحديد صندوق البريد الخاص بالمتهم محل التفتيش بعد معرفة إسم المستخدم و الرقم السري للدخول وفتح البريد الالكتروني أما عن طريق الوارد أو الصادر أو الحفظ أو المهملات أو ضبط الرسائل الالكترونية عن طريق تشغيل برامج البريد الالكتروني في جهاز المتهم ومراجعة قائمة الرسائل الجديدة ليلتقط الرسالة المطلوبة[1].

ثالثا : الصعوبات التي تواجه المحقق في ضبط الدليل الإلكتروني

ان عملية ضبط البيانات المعالجة اليا تواجه عدة صعوبات أهمها :

* ضخامة البيانات التي من الواجب فحصها.

* الضبط في مجال المعلوماتية قد يمثل أحيانا اعتداء على حقوق الغير أو على حرمة حياتهم الخاصة مما يستوجب اتخاذ ضمانات لازمة لحماية هذه الحقوق.

* قد توجد هذه البيانات والمعطيات في شبكات وأجهزة تابعة لدولة اجنبية مما يستدعي تعاونها مع جهات التحقيق الوطني.

المطلب الثاني : القواعد الاجرائية المستحدثة لإستخلاص الدليل الالكتروني

تعتبر القواعد الاجرائية المستحدثة من أهم الاجراءات التي جاء بها المشرع لمكافحة الجريمة المعلوماتية ، حيث تعتبر هذه الاجراءات وسيلة لكشف المشتبه بهم وذلك بسبب ما تتميز به من تجسس على الحياة الخاصة للمتهمين ورصد كل تحركاتهم ، وعليه سنتطرق إلى هذه الاجراءات وفق الفروع التالية :

[1] **خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية** ، المرجع السابق ، ص 274

الفرع الاول : اعتراض المرسلات و اتصالات السلكية و لا سلكية

لقد عرف المشرع الجزائري اعتراض المراسلات والاتصالات السلكية واللاسلكية في الماده 65 مكرر 5 من قانون الاجراءات الجزائية ، بأنها اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية ، وهذه المراسلات عبارة عن بيانات قابله للإنتاج والتوزيع والتخزين لاستقبال والعرض ،كما أنه نفس المادة جاءت على سبيل الحصر للجرائم التي يستوجب فيها اعتراض هذه المراسلات والاتصالات السلكية واللاسلكية ، حيث المقصود بالمراسلات هي جميع الرسائل أو الرموز أو تسجيلات أو أي شيء من هذا القبيل يكون في عالم الافتراضي او في البيئة الالكترونية ، والمقصود بالإتصال هو أي مكالمات وتسجيلات صوتية وصور وفيديوهات حيث المشرع أراد في هذه الجرائم ذات الخطورة أن يفعل هذا الاجراء وذلك من أجل ضبط ومراقبة جميع تصرفات الغير المشروعه ، التي تقع في هذه البيئة الالكترونية كما هو معروف فإن الدولة تعمل دائما على إقامه التوازن بين مصلحه العدالة في محاربة الجرائم وبين حماية حقوق وحريات الانسان وحرمته حياته الخاصة ، المنصوص عليها في دستور 2020 في الماده 47 بقولها لكل شخص حق في حماية حياته[1] الخاصة وشرفه ، ولكل شخص الحق في سرية مراسلته واتصالات الخاصة في أي شكل كانت ولا مساس بهذه المراسلات إلا بأمر معلل من السلطة القضائية ، وكذلك عرف القانون 04/09 المؤرخ في 5 أوت سنه 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، في الماده 2 الفقرة 2 أن الإتصالات الإلكترونية هي أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو اصوات او معلومات مختلفة بواسطة وسيلة إلكترونية ،كما نص نفس القانون في المادة 3 و 4 على كيفيه العمل بإجراء اعتراض المراسلات والاتصالات السلكية واللاسلكية و أهم الضمانات التي جاءت بها لحماية الاشخاص من المساس بحرمة مراسلاتهم و اتصالاتهم ، هي عن طريق تقييد الجهة القضائية بمجموعة من الخطوات قبل القيام بهذا الاجراء وهذا في نص المادة 04 من نفس القانون على الحالات التي تسمح باللجوء الى المراقبة

[1] **بن نعوم خالد أمين** ، المرجع سابق ، ص 96

الالكترونية ، وهي الوقاية من الافعال الموصوفة بجرائم الارهاب أو التخريب أو جرائم الماسة بأمن الدوله في حاله توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على النحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدوله أو الاقتصاد الوطني .

ومن أهم المرسلات التي يقوم بها المشتبه فيهم في البيئة الالكترونية غالبا ما تكون عن طريق البريد الالكتروني ، الان هذا الاخير محاط بحماية فنية ولا يكمن الوصول إليه إلا عن طريق إجراءات فنية خاصة ، مما جعل جهات التحقيق تولي له أهمية كبيرة حيث يمثل البريد الالكتروني مصدر غني للأدلة الاثبات في الجرائم المعلوماتية ، كون هذه التقنية أكثر استخدما في وسائل لاتصال[1] ، ومن هنا فعملية اعتراض ومراقبة البريد الالكتروني التي تجري بغرض ضبط الدليل الرقمي ، و المراسلات الالكترونية تنصب على ثلاثة عناصر أساسية وهي:

* الوارد:(IN) ويتم من خلاله مراقبة ومراجعة قائمة المراسلات الالكترونية التي وصلت المشتبه فيه.
* عن طرق الصادر : (OUT) وهو عكس الوارد يفيد في الكشف عن قائمة المراسلات التي أرسلت من طرف المشتبه فيه .

* أما العنصر الاخير فهو الحافظ سلة المهملات Trash الذي يسمح بالإطلاع على المراسلات المحفوظة داخل البريد الالكتروني الخاص بالمشتبه فيه والمحذوفة منه والتي تحفظ بشكل آلي في سلة المهملات .

وينبغي التنبيه في هذا الصدد إلى أن المراسلات التي تصلح لأن تكون محلا لإجراء الاعتراض أو المراقبة لابد أن تتسم بالسرية والخصوصية ، ولا يتحقق هذا الأمر إلا بتوفرها على عنصرين هامين يتعلق **الأول** بموضوع وفحوى المراسلة في حد ذاتها ، عندما ينصب على معلومات أو أفكار شخصية

[1] سارة قادري ، **أساليب التحري الخاصة في قانون الاجراءات الجزائية** ، مذكرة ماستر ، قسم الحقوق ، كلية الحقوق وعلوم السياسية ، جامعة قصدي مرباح ، ورقلة ، الجزائر ،2014، ص 32

وسرية فيما تخبر به أما العنصر **الثاني** ، فهو شخصي ويتعلق بإدارة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون المراسلة.

الفرع الثاني : التسرب

التسرب يعتبر من الاجراءات التي يتسلل فيها ضابط الشرطة القضائية وسط المجرمين ليجمع قدر الامكان من الادلة ونظر لخطورة هذا الاجراء وما يمسه من ضمانات دستورية احاطه المشرع بشروط وسنتطرق اليه كما يلي :

أولا : تعريف تسرب

حدد المشرع الجزائري نطاق هذا الإجراء بالجرائم المذكورة على سبيل الحصر في المادة65 مكرر 5 من قانون الإجراءات الجزائية والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

فالتسرب من الناحية الأمنية هو تلك العملية المحضر لها والمنظمة قصد التوغل داخل وسط لمعرفة الحقيقة معرفة جيدة ، من أجل الاستعلام عنه ومعرفة أدق التفاصيل فيه وخصوصياته و أسراره حسب تطلعات الجهات الأمنية [1]

أما من الناحية القانونية فالمشرع الجزائري حدد مقصود هذا الإجراء المادة 65مكرر 12 على أنه : "قيام ضباط أو أعوان الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك ويلاحظ من خلال ما سبق ذكره أن التسرب عملية معقدة ، تتطلب أن يدخل العون لمكلف بالعملية في اتصال بالأشخاص المشتبه فيهم و يربط معهم علاقات من أجل تحقيق الهدف النهائي من العملية " وتتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الإجرامية التي تسرب إليها , وعلى هذا فإن التسرب يرتكز على مبدأين :

[1] **فائدة فاطمة الزهرة** ، المرجع السابق ، ص 52

المبـــدأ العـــام : يســتند علــى تقــديم صــورة علــى الوســط المــراد التســرب فيــه , ويســتوجب ذلك معرفة عموميات عن هذا الوسط مع توثيق هذه المعطيات .

المبـــدأ الخـــاص : يســتند علــى تعميــق التحــري عــن هــذا الوســط ونشــاطاته ومميزاتــه ووسائله وطبيعة الأشخاص المنتمين إليه ، ليتم بعد ذلك دراسة الوظيفة العملياتية في هذا المجال بتوفير الوسائل البشرية و التقنية اللازمة .[1]

ثانيا : شروط التسرب

كون هذا الإجراء من أخطر الإجراءات انتهاكا لحرمة الحياة الخاصة للمشتبه فيهم ، فقد أحاطه المشرع الجزائري بجملة من الشروط وجب مراعاتها عندما تقتضي ضروريات التحري والتحقيق اللجوء إليها سنوجزها فيما يلي :

أ) الشروط الشكلية :

تتمثل الشروط الشكلية لهذا الإجراء في الإذن وما يجب أن يتضمنه حيث قوم وكيل الجمهورية أو قاضي التحقيق بمنح الإذن بالتسرب شرط أن يكون مكتوبا و إلا كان الإجراء باطلا وهذا ما جاء في المادة 65مكرر 15بنصها على أنه " **يجب أن يكون الإذن المسلم تطبيقا للمادة 65مكرر 11 مكتوبا ومسببا وذلك تحت طائلة البطلان** " كونا لأصل في العمل الإجرائي الكتابة ،كما أنه تتوقف صحة هذا الإجراء ذاته على مجموعة من الشروط كذكر هوية ضابط الشرطة القضائية المسئول عن عملية التسرب ، وتحديد مدة لا تتجاوز أربعة أشهر بحيث يمكن تمديدها على حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية ويمكن للقاضي الذي أذن بهذا الإجراء الأمر بوقفه قبل انقضاء المدة المحددة .

[1] **فائدة فاطمة الزهرة** ، المرجع السابق ص 53

ب)الشروط الموضوعية

تنحصر الشروط الموضوعية لعملية التسرب وفق الأحكام التي نظمها المشرع الجزائري في شرطين أساسين يتمثلان في :

* تحديد نوع الجريمة التي يجب أن لا تخرج عن الجرائم المذكورة على سبيل الحصر في المادة 65مكرر 5 في سبعة أنواع وهي " جرائم المخدرات ، الجريمة المنظمة العابرة للحدود الوطنية ، جرائم تبييض الأموال ، الجرائم الإرهابية ، جرائم الفساد ، الجرائم المتعلقة بالتشريع الخاص بالصرف ، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

* أن يكون الإذن بالتسرب مسببا ، لأنه من التسبيب تتضح العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن و كذا العناصر التي دفعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء ، و التي تكون ضمن موضوع طلبه الإذن لذلك كان لزاما عند إصدار الإذن بالتسرب سواء من طرف وكيل الجمهورية أو قاضي التحقيق إظهار جميع الأدلة بعد تقدير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية.

ثالثا : تسرب الإلكتروني

يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط شرطة قضائية أو عون الشرطة القضائية إلى العالم الافتراضي (شبكة الانترنت) ، وذلك بتسجيله على مواقع معينة كمواقع التواصل الاجتماعي أو اشتراكه في محادثات عبر غرف الدردشة أو حلقات الاتصال المباشر لرفع ومعاينة الجرائم ، أو ربط الاتصال مع المشتبه فيهم و الظهور بمظهر كما لو كان فاعلا مثلهم ، مستخدما في ذلك أسماء أو صفات مستعارة ووهمية سعيا منها للتعرف عليهم وتحديد أماكنهم[1].

[1] **سارة قادري** ، المرجع السابق ، ص 42

رابعا : جهات المشرفة على إجراء التسرب

أوكل المشرع مهمة منح الإذن بالتسرب إلى وكيل الجمهورية وقاضي التحقيق دون سواهما وهذا ما جاء صراحة في المادة 65مكرر 11من القانون 06 / 22 المعدل والمتمم ، لذلك فإن وكيل الجمهورية أوكل له قانون الإجراءات الجزائية بموجب المادة 12 كافة الصلاحيات لاتخاذ الإجراءات اللازمة للبحث والتحري عن الجرائم بصفة عامة قبل إحالتها على التحقيق ، وبهذه الصفة يحق له منح الإذن بنفس الشروط إلى ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب ، إذا تطلبت ضروريات التحقيق و التحري في الجرائم المحددة قانونا بنص المادة 65مكرر 5 السابق ذكرها ، وخول له كذلك سلطة اتخاذ هذا الإجراء في حالة التلبس في أي جريمة من الجرائم المحددة قانونا على سبيل الحصر.

أما قاضي التحقيق فأنه يمارس صلاحياته بعد إخطاره من قبل وكيل الجمهورية بموجب طلب افتتاحي ، وفقا لنص المادة 67 من نفس القانون لإجراء التحقيق لتصبح له الولاية الكاملة في اتخاذ ما يجب قانونا من الإجراءات ، التي تستوجبها ضروريات البحث والتحري عن الجريمة الالكترونية بغية الكشف عن الحقيقة [1].

الفرع الثالث : مقدمي الخدمات

لقد رأى المشرع انه في سبيل الوصول إلى الدليل الالكتروني والذي يتميز بصعوبة الحصول عليه من الضروري الاستعانة بمساعدة بالتقنيين الذين يقدمون خدمات الاتصال ، بأن يقدموا كل المعطيات المعلومات عن المشتبه فيه لمعرفة تحركات هذا الاخير ، ولقد عرفهم المشرع في الفصل الرابع من القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[1] **بشير حماني** ، المرجع السابق ، ص 70

أولا : تعريف مقدمي الخدمات

عرفت المادة الأولى من اتفاقية بودابست في الفقرة "ج" أن مزود أو مقدم الخدمة هم كل من يقوم بخدمات الإيصال أو معالجة البيانات أو خدمات تخزين البيانات ، وقد يكون جهة عامة أو خاصة وقد يقدم خدماته للجمهور أو لمجموعة من المستخدمين الذين يشكلون مجموعة مغلقة ، كما عرفته الاتفاقية العربية في المادة الثانية أنه " أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات ، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها .

وعرفه المشرع الجزائري بموجب المادة الثانية في فرتها السادسة من القانون 04 /09 بأنه" **كل كيان عام أو خاص يقدم لمستعملي خدماته ضمانة القدرة على الإتصال بواسطة منظومة معلوماتية أو نظام الاتصالات و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال** ".[1]

و أيضا مقتضيات المرسوم التنفيذي 2000/ 307 المتعلق بضبط شروط و كيفيات إقامة خدمات "الانترنت" و استغلالها بذكره لمقدمي الخدمات في المادة 04 فقرة 1منه أنهم أشخاص معنويين خاضعين للقانون الجزائري .

ثانيا : التزامات مقدمي الخدمات لمساعدة جهات التحقيق

ألزمت المادة 10من القانون 04/09 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش كما ألزمتهم أيضا بكتمان السر بخصوص العمليات التي ينجزونها بطلب من المحققين ، وما تحصل عن ذلك من معلومات وذلك تحت طائلة العقوبات التي يقررها القانون في حالة إفشاء أسرار التحقيق.

[1] **بشير حماني** ، المرجع السابق ، ص 73

و إلى جانب ذلك ألزمت المادة 11من القانون 04/09 مقدمي الخدمات بحفظ المعلومات التي من شأنها تمكين جهات التحقيق من التعرف على مستعملي الخدمة ، و ذلك لمدة سنة واحدة و ازالتها بعد ذلك لأن الحفظ إجراء وقتي ، إذن هم ملزمون بتسجيل وحفظ المعطيات التي ووضعها تحت تصرف المحققين بل أن أي عمل من شأنه عرقلة حسن سير التحقيق يؤدي إلى قيام مسؤولية جزائية لهؤلاء ، و يعرضهم للعقوبة المنصوص عليه في المادة 11 و هي الحبس من ستة أشهر إلى خمس سنوات وبغرامة من 50.000 دينار جزائري إلى 500.000 دينار جزائري .[1]

وما تجدر الإشارة إليه أن المشرع الجزائري حدد المعطيات المعلوماتية الواجب على مزودي الخدمات حفظها ، وهي معطيات المرور و حصرها في ، المعطيات التي تسمح بالتعرف على مستعملي الخدمة ، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال ، الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال ، المعطيات التي تسمح بالتعرف على المرسل إليه وكذا عناوين المواقع المطلع عليها.

[1] رابحي عزيزة ،**الأسرار المعلوماتية وحمايتها الجزائية** ، رسالة دكتوراه ،تخصص قانون خاص ، قسم الحقوق ،كلية الحقوق والعلوم السياسية،جامعة ابوبكر بلقا يد ، تلمسان ،الجزائر،2017-2018،ص 300

خاتمة الفصل الثاني :

وأخيرا يمكن القول أن الدليل الالكتروني يعتبر أهم وسيلة للوصول إلى الحقيقة ، وحتى نضمن سلامة الدليل منح المشرع بعض الصلاحيات للقاضي ، مثل مشروعية وجود الدليل ومشروعية الحصول عليه ، ولقد أحسن المشرع حين أخذ بنظام حرية الاثبات ، وذلك يكمن في أنه كل دليل قد يساعد جهات التحقيق للوصول إلى الحقيقة ، يمكن الاخذ به عكس نظام المقيد كما أن المشرع الجزائري منح سلطة تقديرية واسعة للقاضي في تقدير الدليل وقبوله ، وأحطها ببعض الضمانات من أجل عدم تعسف القاضي أثناء تكوين قناعته.

كما قسمنا اجراءات التحقيق الى إجراءات مادية تقتصر فقط على المعاينة التقنية و التفتيش المعلوماتي ، الذي يخضع تارة لأحكام قانون الإجراءات الجزائية (المكونات المادية) ، وتارة أخرى إلى قانون 09/04 (المكونات المعنوية) وتارة أخرى تكون شخصية تتمثل في الخبرة ، وشهادة شاهد إلكتروني وآخرها التسرب وهو من أساليب التحري الخاصة التي جاء بها تعديل قانون الإجراءات الجزائية ، الذي قررها هذا الأخير إلا على الجرائم الخطيرة.

الخاتمة

لقد أضحى العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية ، حيث أصبحت حياتنا اليومية تستدعي اللجوء إليها فقد مكنت طرق المعالجة الآلية المعطيات المجتمعات من تجاوز فكرة الحدود الإقليمية ، نظرا لكون التكنولوجيا هي عابرة للحدود.

وأمام هذا التطور فقد ارتبطت به ظهور ما يعرف بالإجرام المعلوماتي وذلك نتيجة استخدام السيئ للمعلوماتية أو الحاسوب ، الذي نتج عن هذا الاخير عدة أضرارا لا يمكن حصرها وذلك لأنها تهدد أمن المعطيات من جهة ، وتمس بحرية الافراد والمؤسسات من جهة أخرى.

ولقد قسمنا هذه الدراسة إلى فصلين حيث تناولنا في الفصل الأول مفهوم الجريمة المعلوماتية وقمنا بتبيان أهم التعريفات الفقهية والقانونية ، ثم تم تبيان أركان هذه الجريمة وخصائص التي تتميز بها ، و حددنا كل من الضحية والجاني والشاهد ثم شرحنا سبل مكافحتها على مستوى الدولي والإقليمي والوطني و تم شرح بعد ذلك مراحل التحقيق ومن يشرف على كل مرحلة من هذه المراحل .

وبعد ذلك تناولنا في الفصل الثاني مفهوم الدليل الالكتروني ومشروعية وجوده والحصول عليه ، وكذلك تطرقنا إلى أهم أنظمة الاثبات الموجودة في الفقه الجنائي ، ثم بينا مبدأ إقتناع القاضي والوسائل التي تساعده في تكوين قناعته ، وبعد ذلك تم تطرق إلى الاجراءات التقليدية وكيف وسع المشرع من صلاحياتها مثل التفتيش والمعاينة والخبرة الفنية ، ثم عرفنا القواعد الاجرائية المستحدثة لمكافحة الجريمة المعلوماتية مثل التسرب الالكتروني و إعتراض المرسلات والاتصالات السلكية ولا سلكية ومقدمي الخدمات و الضمانات التي جاء بها المشرع من أجل محافضة على حرمة الحياة الخاصة .

ومن خلال درستنا هذه تم توصل إلى النتائج التالية :

* من أهم مميزات هذا النوع من الجرائم أنها تنصب على محل من نوع خاص يختلف تماما على محل الجرائم التقليدية.

* عدم إجماع الفقهاء على تعريف موحد للجريمة الإلكترونية يعود أساسا إلى الاختلاف حول تحديد نطاق هذه الجريمة ، خصوصا أن البعض وسع كثيرا من نطاقها و أعتبر أن كل فعل غير مشروع يكون

للحاسب الآلي دورا في الجريمة الكترونية ، وقد تبنى هذا الاتجاه المشرع الجزائري حيث نص على ذلك في القانون رقم 04/09 و حدد نطاق الجريمة الإلكترونية بالجريمة التي تمس بالنظام المعلوماتي ، أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات ، وهو توسيع يتفق مع ماهية الجريمة الإلكترونية ، باعتبارها تستهدف بالدرجة الأولى الجانب البرمجي للنظم المعلوماتية .

* الجريمة المعلوماتية مع تعدد أنماطها واحتراف مرتكبيها ، سواء كانت جرائم واقعة على النظام المعلوماتي أو باستخدامه ، فإن لها جوانب سلبية خطيرة تهدد أمن وسلامة الفرد و المجتمع وتتسم بالغموض وصعوبة الاثبات مما يجعل جهات التحقيق امام مسؤولية كبيرة .

* جاء المشرع الجزائري بترسانة من القوانين المعدلة في منظومة القانونية الجزائية والمدنية من اجل مكافحة الجريمة المعلوماتية.

* المشرع الجزائري لم يقم بتحديد الجريمة المرتكبة باستخدام النظام المعلوماتي وترك المجال واسع ليدخل في نطاقها كل ما تفرزه التقنية الجديدة وتطوراها.

* قام المشرع الجزائري بإنشاء اجهزة تساعد جهات التحقيق في الميادين الفنية التي تجهلها هذه الجهات.

* حاول المشرع الجزائري مواكبة تطور الذي وصلت إليه الدول المتقدمة وكذلك محاول اثبات عضويته في جميع المنظمات والاتفاقيات التي تنصب حول موضوع مكافحة الجريمة المعلوماتية.

* الإجراءات الجديدة لاستخلاص الدليل في البيئة الإلكترونية قد تشكل خطرا كبيرا يهدد الحق في الخصوصية ، نظرا لما تتيحه لسلطات التحقيق من إمكانية الاطلاع على أسرار خاصة بأشخاص قد لا يكون لهم يد في الجريمة.

* مسألة قبول الدليل الإلكتروني من عدمه تخضع لمطلق تقدير القاضي الجزائي ، الذي يتمتع بدور إيجابي في مناقشة وموازنة القيمة القانونية للدليل الإلكتروني قبل أن يطمئن إليه .

* دوافع ارتكاب الجريمة الإلكترونية تختلف من شخص لآخر ، فقد تكون دوافع شخصية هدفها تحقيق مصالح شخصية ، أو قد تكون دوافع خارجية كالانتقام مثلا .

ومن خلال هذه النتائج نحاول اقتراح التوصيات الاتية :

* العمل على استحداث ضبطية قضائية متخصصة في مجال الجرائم المعلوماتية أسوة بالدول المتقدمة.

* الاهتمام بالتأهيل المناسب لكوادر الأجهزة القضائية بما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة المطلوبة منهم .

* لا يكفي الاعتماد على التشريعات القائمة لتجاوز الصعوبات الإجرائية التي تثيرها عملية البحث والتحقيق في الجرائم المعلوماتية ، بل لا بد من تدعيمها بنصوص خاصة حديثة تتضمن إجراءات تحقيق ملائمة مع طبيعة هذا الشكل من الإجرام ومسايرة للمتغيرات و التطورات الحاصلة في تقنيات و أساليب ارتكابه.

* ضرورة تكثيف التعاون و التنسيق الدولي بين الدول من أجل تطوير وتوحيد التشريعات الجزائية الموضوعية و الإجرائية التي تعنى بمكافحة الجرائم الإلكترونية.

* يتعين إدخال مادة " أخلاقيات استخدام الانترنت " ضمن المناهج الدراسية في التعليم ما قبل الجامعي.

* ضرورة نشر الوعي في أوساط المجتمع بالمخاطر الاجتماعية و النفسية وغيرها الناجمة عن الاستخدامات غير المشروعة و غير الآمنة للانترنت ، وبما يترتب عنها من انعكاسات سلبية على حياة الفرد و المجتمع.

* ضرورة تشديد الوصف الجنائي والعقوبات المقررة للأنماط الاجرامية للجريمة المعلوماتية ، بغية تحقيق الردع والقضاء على الاجرام المعلوماتي .

* من الافضل أن يسن المشرع قانون موحد لمكافحة الجرائم المعلوماتية ، يلم بكل النصوص الموضوعية والإجرائية والتنظيمية ، وهو ما يسهل عمل ضباط الشرطة القضائية ووكلاء الجمهورية وقضاة التحقيق والحكم ، ويساعد رجال القانون من الامام بكل ما يخص هذا النوع المستحدث من الجرائم .

قائمة

المصادر و المراجع

أولا : المـــــــــــــــصـــــــــــادر

❖ **الإتـــــــفـــــــــاقيـــــــات والمـــــــــنـــــظـــمـــــــات :**

- ✓ اتفاقية بودابست المؤرخة في 23نوفمبر سنة 2000 بعاصمة المجر .
- ✓ اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية من طرف الجمعية العامة لمنظمة الامم المتحدة يوم 2000/11/15 صادقت عليها الجزائر بتحفظ موجب المرسوم الرئاسي رقم 04-165 المؤرخ 2004/6/8.
- ✓ الاتفاقية العربية لمكافحة الجرائم تقنية المعلوماتية المحرر بالقاهرة بتاريخ 2010/12/21 صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14-258 المؤرخ في 2014/9/8.
- ✓ المنظمـة الدوليـة للشـرطة الجنائيـة الأنتربـول، مقرهـا في بـاريس وضـع ميثـاق هـذه المنظمـة في فـترة 1956/06/13.
- ✓ اتفاقية بران لحقوق المؤلف لسنة 1882 المعدلة و المتممة ، في العاصمة الإدارية السويسرية صادقت عليهـا الجزائـر بموجـب المرسـوم الرئاسـي رقـم 341/97 المـؤرخ في 1997/09/13 (ج.ر) رقـم 61 المؤرخة في 1997/09/14.

❖ **القـــوانـــيـــــن :**

- ✓ القـانون 09-04 المؤرخ فـي 2009/08/05 المتضـمن القواعـد الخاصـة للوقايـة مـن الجـرائم المتصـلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، (ج ر) العدد 47 المؤرخة في 2009/08/16.
- ✓ القانون 01 -08 المؤرخ في 23/ 01 / 2008 والمتمم للقانون رقـم 01-83 متعلق بالتأمينات، (ج.ر) ، العدد 04 ، المؤرخة في 27 /01 /2008 .
- ✓ دستور الجزائري لسنة 2020 الصادر بموجب مرسوم رئاسي رقـم 442/20 في 30 ديسمبر 2020 المتعلق بإصدار تعديل دستوري جديد المصادق عليه بإستفتاء شعبي في 1 نوفمبر 2020 ،ج.ر العدد 82 المؤرخة في 30 ديسمبر 2020.

- ✓ القـانون 2000/03 الصـادر في 2000/08/05 يحـدد القواعـد العامـة المتعلقـة بالبريـد والمواصـلات السلكية واللاسلكية (ج ر) العدد 48 المؤرخة في 2000/08/06.
- ✓ القـانون 14/04 الصـادر في 2004/11/10 المعدل والمتمم لقـانون الاجراءات الجزائية (ج ر) العدد 71 المؤرخة في 2004/11/10.
- ✓ القـانون رقـم 22/06 الصـادر في 2006/12/20 يعـدل ويـتمم الامـر رقـم 66-155 المـؤرخ 1966/6/8 والمتضمن قانون الاجراءات الجزائية ، (ج ر) العدد 84 المؤرخة في 2006/12/24.
- ✓ القانون رقم 15/04 الصادر في 2004/11/10 يعدل ويتمم الامر رقم 66-156 المؤرخ في 08 يونيو 1966 والمتضمن قانون العقوبات (ج ر) العدد 71 المؤرخة في 2004/11/10.
- ✓ القانون ، رقم 10/19 الصادر في 11 ديسمبر سنة 2019 ، المتضمن الاجراءات الجزائية ، (ج ر) ، العدد 78 ، المؤرخة في 18 ديسمبر 2019 .

ثـــانـيا : المـــــــــــراجـــــــــع

❖ **المـــــــــــؤلـــــــــفـــــــــات:**

الكـــــــتـــــــب العـــــامـــــــة :

- ✓ أحسن بوسقيعة ،**الاجراءات الجزائية في ضوء الممارسة القضائية** ، منشورات بارتي(BERTi)،الطبعة 16، 2021،
- ✓ أحسن بوسقيعة ،**الوجيز في القانون الجزائي العام،دار الهومة للطباعة والنشر والتوزيع** ،الجزائر، الطبعة11، 2012
- ✓ علي شملال،المستحدث في قانون الاجراءات الجزائية الجزائري،الجزء الأول:الإستدلال والاتهام،دار الهوما للطباعة و النشر و التوزيع،الجزائر،الطبعة الرابعة،2019-2020.
- ✓ عبد الرحمان خلفي، **محاضرات في القانون الاجراءات الجزائية** ،دار الهدى ،عين مليلة ، جزائر ، طبعة الثانية ،2010

الكتـــــــب المتخـــــصـــــــصـــــــــة :

- ✓ حسين الغافري ومحمد الألفي ، **جرائم الانترنات بين الشريعة الاسلامية والقانون** ،دار النهضة العربية؛ القاهرة ،مصر 2008.
- ✓ حنان ريحان المبارك المضحكي ،**الجرائم المعلوماتية دراسة مقارنة** ، منشورات الحلبي الحقوقية بيروت لبنان الطبعة الاولى،2014
- ✓ خالد الممدوح ابراهيم ،جرائم المعلوماتية ، **دار الفكر الجامعي الإسكندرية** ، مصر ،طبعة الاولى 2009
- ✓ خالد الممدوح ابراهيم ،**فن التحقيق الجنائي في الجريمة الالكترونية** ،دار الفكر الجامعي ،الاسكندرية ،مصر 2009.

- ✓ رمزي رياض عوض، **مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها** ، دارسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، ،1997
- ✓ عائشة بن قارة مصطفى ،**حجية الدليل الالكتروني في مجال الاثبات الجنائي**, دار الجامعة الجديدة؛ الاسكندرية ،2010.
- ✓ علي عدنان الفيل،اجراءات التحري و جمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية،المكتب الجامعي حديث ، الاسكندرية ، مصر،2012.
- ✓ عبد الحكيم رشيد توبة، **جرائم تكنولوجيا المعلومات ،دار المستقبل للنشر والتوزيع الاردن**، طبعة الاولى 2009.
- ✓ علي عبد القادر القهوجي، **حماية جنائية لبرامج حاسب الالي ،دار الجامعة الجديدة**، الاسكندرية، مصر 2010.
- ✓ عبد الصبور **عبد القوي علي مصري** ، **الجريمة الالكترونية** ، دار العلوم للنشر والتوزيع ،القاهرة؛ مصر،طبعة الاولى (ب .س .ط).
- ✓ عادل عزام سقف الحيط ،**جرائم الذم والقدح والتحقير المرتكبة في وسط الالكتروني** ، دار الثقافة للنشر والتوزيع ،عمان ،الاردن طبعة الاولى 2011.
- ✓ عفيفي كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دارسة مقارنة، منشو ارت الحلبي، دمشق، 2007
- ✓ علي محمود على محمود، **الأدلة المحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي** ، بحث مقدم إلى المؤتمر العلمي الاول حول الجوانب القانونية و الأمنية للعمالـيات الالكترونية، دبي، الإمـــارات العربية المتحدة، ، 2003.
- ✓ فريد منعم جبور، **حماية المستهلك عبر الانترنت ومكافحة الجرائم الالكترونية** ،منشورات الحلبي الحقوقية؛ بيروت، لبنان، طبعة الاولى ،2010.

- ✓ مر زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى للطباعة والنشر، الجزائر، ،2011ص 131 نصر الدين، محاضرات في الإثبات الجنائي، دار هومة، الجزائر، ط1، 2003.
- ✓ محمد حماد مرهج الهيتي ،**جريمة المعلوماتية** ،**دراسة مقارنة** ، دار الكتب القانونية ،مصر ،2014
- ✓ نهلة عبد القادر مومني،**الجرائم المعلوماتية**،**دار الثقافة للنشر و التوزيع**،عمان،الطبعة الثانية،2010.
- ✓ نائلة عادل محمد فريد قورة،**جرائم الحاسب الآلي الإقتصادي**،**منشورات حلبي الحقوقية**،لبنان،الطبعة الأولى،2005.
- ✓ نعيم مغبغب ،**حماية برامج الكمبيوتر، منشورات الحلبي الحقوقية**، لبنان ،طبعة الثانية ، 2009 .
- ✓ نور الهدى محمودي، **حجية الدليل الرقمي في إثبات الجريمة المعلوماتية**، مجلة الباحث للدراسات الأكاديمية، المجلد الرابع، العدد 2.
- ✓ ناير نبيل عمر ، **الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية** ،دار الجامعة الجديدة ،الاسكندرية مصر ،2010.
- ✓ هشام محمد فريد رستم،**قانون العقوبات و مخاطر التقنية المعلوماتية**، مكتبة الآلات الحديثة ، اسيوط ؛ 1994.
- ✓ هلال عبد الله محمد، **حجية مخرجات الكمبيوتر في المواد الجنائية**، الطبعة الثانية، دار النهضة العربية، مصر، 2008
- ✓ يزيد بوحليط،**الجرائم الإلكترونية و الوقاية منها في القانون الجزائري**،دار الجامعة الجديدة للنشر ،الإسكندرية ،مصر،2019.
- ✓ يوسف حسين يوسف ، **الجريمة الدولية للانترنت** ، **المركز القومي الاصدرات القانونية**، القاهرة ، مصر؛ الطبعة الاولى ، 2011 .
- ✓ يوسف ابو الحاج ، **اشهر الجرائم الكمبيوتر والانترنت** ، دار الكتاب العربي ، دمشق ،القاهرة ، الطبعة الاولى 2010.

❖ **أطـــــروحـــــات الـــــدكـــــتـــــــوراه :**

- ✓ بن يحي اسماعيل،**التحقيق الجنائي في الجرائم الإلكترونية** رسالة دكتوراه،تخصص قانون الخاص،قسم حقوق كلية الحقوق و العلوم السياسية،جامعة أبي بكر الصديق بلقا يد،تلمسان،الجزائر،سنة 2020-2021.
- ✓ براهمي جمال ، **التحقيق الجنائي في الجرام الالكترونية** ، اطروحة لنيل شهادة دكتورة ، تخصص قانون جنائي ، قسم الحقوق ، كلية الحقوق وعلوم السياسة جامعة مولود معمري ، تيزي وزو ، الجزائر 2018
- ✓ رابحي عزيزة،**الأسرار المعلوماتية و حمايتها الجزائية**،رسالة دكتوراه،تخصص قانون خاص ، قسم الحقوق،كلية الحقوق والعلوم السياسية،جامعة ابوبكر بلقا يد،تلمسان،الجزائر،2017-2018.
- ✓ ربيعي حسين،**آليات البحث و التحقيق في الجرائم المعلوماتية**،رسالة دكتوراه،تخصص قانون العقوبات والعلوم الجنائية،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة باتنة 1،الجزائر، سنة 2015-2016.

❖ **مـــــــذكـــــــرات مـــــاســـتـــــر:**

- ✓ إبتسام بغو ، **اجراءات المتابعة الجزائية في الجريمة المعلوماتية** ، مذكرة ماستر ، تخصص القانون الجنائي للأعمال ، قسم الحقوق ، كلية الحقوق والعلوم السياسية ، جامعة العربي بن مهدي ام بواقي ، الجزائر 2015-2016
- ✓ بغاد يد نابية،**آليات البحث و التحري عن الجريمة المعلوماتية**،مذكرة ماستر،تخصص قانون جنائي،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة الدكتور مولاي الطاهر،سعيدة،الجزائر،سنة 2015-2016.
- ✓ بخي فاطمة الزهراء،**اجراءات التحقيق في الجريمة الإلكترونية،مذكرة ماستر**،تخصص القانون الجنائي،قسم حقوق،كلية الحقوق و العلوم السياسية،جامعة المسيلة،الجزائر سنة 2013-2014.

- ✓ بشير حماني،**خصوصية التحقيق في الجريمة الإلكترونية**،مذكرة ماستر،تخصص قانون الجنائي و العلوم الجنائيـة، قسـم حقوق،كليـة الحقـوق و العلـوم السياسـية،جامعة محمـد بوضياف،المسيلة،الجزائر،سـنة 2019-2018.
- ✓ بـن نعـوم خالـد أمـين،**اجـراءات التحقيـق فـي الجريمـة المعلوماتيـة فـي التحقيـق الجزائـري**،مـذكرة ماستر،تخصـص قـانون فضائي،قسـم الحقوق،كليـة الحقـوق و العلـوم السياسـية،جامعة عبـد الحميـد بـن باديس ،مستغانم،الجزائر،سنة 2018-2019.
- ✓ سارة قادري ، **اساليب التحري الخاصة في قانون الاجراءات الجزائية** ، مذكرة ماستر ، قسم الحقوق ،كلية الحقوق وعلوم السياسية ، جامعة قصدي مرباح ، ورقلة ، الجزائر ،2014.
- ✓ غربي جميلة،**آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري**،مذكرة ماستر،تخصص قانون جنائي،قسم قانون عام،كلية الحقوق و العلوم السياسية،جامعة أكلي محمد أولحاج،البويرة،الجزائر،سنة 2021-2020.
- ✓ فليح نور الدين،**الجريمة الإلكترونية و آلية مكافحتها في التشريع الجزائري**،مذكرة ماستر،تخصص القـــانون الجنـــائي قســـم الحقوق،كليـــة الحقـــوق و العلـــوم السياســـية،جامعة الـــدكتور مـــولاي الطاهر،سعيدة،الجزائر،سنة 2018-2019.
- ✓ فائدة فاطمة الزهرة ، **التحقيق الجنائي في الجرائم الالكترونية مذكرة ماستر** ، تخصص القانون الجنائي والعلوم الجنائية ،قسم حقوق ،كلية الحقوق والعلوم السياسية ، جامعة محمد بوضياف ، مسيلة الجزائر 2021-2020.
- ✓ قروج حنان ، **حجية الأدلة المعلوماتية في تكوين الاقتناع الشخصي للقاضي الجزائي** ،مذكرة ماستر ، تخصص علم الاجرام ، قسم الحقوق ، كلية الحقوق والعلوم السياسية ، جامعة دكتور مولاي الطاهر ، سعيدة ،الجزائر 2014-2015.
- ✓ نـايري عائشـة،**الجريمـة الالكترونيـة فـي التشـريع الجزائـري**،مـذكرة ماسـتر،تخصـص قـانون إداري،قسـم حقوق،كلية الحقوق و العلوم السياسية،جامعة أحمد دارية،أدرار،الجزائر،سنة 2016-2017

✓ يوسف جفال، **التحقيق في الجريمة الإلكترونية** ،مذكرة ماستر ، تخصص قانون جنائي ، قسم الحقوق،كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف ،المسيلة ،الجزائر،سنة 2016-2017.

❖ **مـــــــذكـــــــرات المجـــــســـــتـــــار:**

✓ سعيداني نعيم ، **آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة لنيل شهادة ماجيستير ،تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2012-2013.

✓ صغير يوسف،**الجريمة المرتكبة عبر الإنترنت**،مذكرة ماجيستار،تخصص قانون دولي للأعمال،قسم حقوق،كلية الحقوق و العلوم السياسية،جامعة مولود العمري،تيزي وزو،الجزائر،2013.

❖ **المـــــــواقـــــع الالـــكتـــرونـــية :**

✓ francois sopin-rapport sur **l' actualite de cyber criminalite** en 2012 date de consultation : 21/04/2022 a 3 :00 am

✓ **La preuve électronique**, consulté le 19/09/2022, Site électronique: www.internetjuridique.net.

❖ **المـــــراجـــــع بـاللـغـة الاجـــنـــبـــيـة :**

✓ Ahmed Dahmani, **la démocratie à l'épreuve de la société numérique**, KARTHALA Editions, 1,Paris ,France, 2007.

✓ Béatrice Géninet, **L'indispensable du droit pénal**, Studyrama, 2eme édition, 2004.

✓ EOGHN Casey ،**Digital evidence and foransic science** ،computer and the computer crminal، 1st acadimic press USA UK 2000.

✓ Myriam QUEMENER. YES CHARPENEL **Cybercriminalité droit** pénal applique économique septembre 2010.

الفهرس

الفهرس : الصفحة:

(الإهداء)

(قائمة المختصرات)

(المقدمة) 02

(الفصل الأول : الجريمة المعلوماتية و إجراءات التحقيق فيها) 08

المبحث الأول : ماهية الجريمة المعلوماتية 10

➢ المطلب الأول : مفهوم الجريمة المعلوماتية.....10

* الفرع الأول : تعريف الجريمة المعلوماتية.....10

* الفرع الثاني : خصائص الجريمة المعلوماتية والصعوبات التي تتميز بها.....14

أولا : خصائص الجريمة المعلوماتي.....14

ثانيا : صعوبات التي تتميز بها الجريمة المعلوماتية.....16

* الفرع الثالث : اركان الجريمة المعلوماتية.....17

أولا : الركن الشرعي.....17

ثانيا : الركن المادي 17

ثالثا : الركن المعنوي.....18

* الفرع الرابع : أطراف الجريمة المعلوماتية.....19

أولا : الجاني أو المجرم المعلوماتي.....19

ثانيا : المجني عليه في الجريمة المعلوماتية.....21

ثالثا : الشاهد في الجريمة المعلوماتية.....23

➢ المطلب الثاني : تصنيف الجريمة المعلوماتية وسبل مكافحتها.....25

* الفرع الأول : تصنيف الجريمة المعلوماتية.....25

أولا : تصنيف الجريمة المعلوماتية تبعا لنوع المعطيات ومحل الجريمة 26

ثانيا : تصنيف الجريمة المعلوماتية تبعا لدور الكمبيوتر في الجريمة 26

ثالثا : تصنيف الجريمة المعلوماتية تبعا لمساسها بالأشخاص و الأموال.....27

رابعا : تصنيف الجريمة المعلوماتية على اساس جرائم الكمبيوتر وجرائم الانترنت 29

* الفرع الثاني : سبل مكافحة الجريمة المعلوماتي.....29

أولا : الجهود الدولية في مكافحة الجريمة المعلوماتية 29

ثانيا : الجهود الهيئات ومنظمات الإقليمية في مكافحة الجريمة المعلوماتية.....32

ثالثا : الجهود الوطنية في مكافحة الجريمة المعلوماتية.....33

المبحث الثاني : إجراءات التحقيق في الجريمة المعلوماتية 36

➢ المطلب الأول : مراحل التحقيق في الجريمة المعلوماتية وصعوباته.....37

* الفرع الأول : في مرحلة البحث والتحري.....37

أولا : تعريف الضبطية القضائية.....37

ثانيا : مهام الضبطية القضائية.....39

* الفرع الثاني : في مرحلة التحقيق الابتدائي.....43

أولا : تعريف التحقيق الابتدائي وأهميته.....43

ثانيا : السلطة المختصة بالتحقيق الابتدائي في الجريمة المعلوماتية.....44

ثالثا : ضمانات المتهم في التحقيق الابتدائي في الجريمة المعلوماتية.....45

رابعا : خصائص المحقق في الجريمة المعلوماتية 46

* الفرع الثالث : في مرحلة المحاكمة 46

أولا : في اختصاص المحكمة 46

ثانيا : في تشكيلة المحكمة 48

ثالثا : إجراءات المحاكمة.....48

* الفرع الرابع : صعوبات التحقيق في الجريمة المعلوماتية.....50

أولا : صعوبات تتعلق بالجرائم المعلوماتية 50

ثانيا : صعوبات تتعلق بالجهات المتضررة 50

ثالثا : صعوبات تتعلق بالجهات التحقيق.....51

➢ المطلب الثاني : الأجهزة المختصة بالبحث وتحري عن الجريمة المعلوماتية.....51

* الفرع الأول : الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية

على مستوى الدولي والإقليمي.....51

أولا : الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على مستوى الدولي 52

ثانيا : الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على مستوى الإقليمي.....52

* الفرع الثاني : الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على

مستوى الدول الأجنبية..... 54

أولا : في الولايات المتحدة الأمريكية.....54

ثانيا : في بريطانيا.....55

ثالثا : في فرنسا 55

رابعا : في الصين 56

خامسا : في مصر 56

* الفرع الثالث : الاجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على مستوى الوطني 57

أولا : الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصالات.....57

ثانيا : الهيئات القضائية الجزائية المختصة (الأقطاب القضائية) 59

ثالثا : المديرية العامة للأمن الوطني 59

رابعا : المعهد الوطني للأدلة الجنائية وعلم الإجرام 62

خاتمة الفصل 63

(الفصل الثاني : الدليل الإلكتروني و القواعد الإجرائية لإستخلاصه) ـــــــ 64

المبحث الأول: ماهية الدليل الإلكتروني ـــــــ 66

➢ المطلب الأول : مفهوم الدليل الإلكتروني 66

* الفرع الأول : تعريف الدليل الإلكتروني.....66

* الفرع الثاني : خصائص الدليل الإلكتروني.....67

أولا : الدليل الإلكتروني دليل علمي 67

ثانيا : الدليل الإلكتروني دليل تقني 68

ثالثا : صعوبة التخلص من الدليل الإلكترون.....68

رابعا : الدليل الإلكتروني دليل متطور.....68

خامسا : الدليل الإلكتروني ذو طبيعة رقمية ثنائية.....68

* الفرع الثالث: مشروعية الدليل الإلكتروني ومناقشته.....69

أولا : مشروعية وجود الدليل الإلكتروني 69

ثانيا : مشروعية الحصول على الدليل الإلكتروني.....70

ثالثا : مناقشة الدليل الإلكتروني.....71

➢ المطلب الثاني : موقف المشرع الجزائري من الدليل الإلكتروني في مجال الإثبات الجنائي.....72

* الفرع الأول : أنظمة الإثبات الجنائي وموقف المشرع الجزائري منها.....73

أولا : نظام الإثبات المقيد 73

ثانيا : نظام الإثبات الحر.....74

ثالثا : نظام الإثبات المختلط 74

رابعا : موقف المشرع الجزائري من أنظمة الإثبات الجنائي.....76

* الفرع الثاني : تعريف مبدأ الاقتناع الشخصي للقاضي.....77

* الفرع الثالث : ضوابط التي تحكم إقتناع القاضي الجنائي بالدليل الإلكتروني.....79

أولا : الضوابط المتعلقة بمصدر الاقتناع.....80

ثانيا : الضوابط المتعلقة بالاقتناع ذاته.....81

ـــــــ المبحث الثاني : القواعد الإجرائية لاستخلاص الدليل الإلكتروني ـــــــ 82

➢ المطلب الأول : القواعد الإجرائية التقليدية لاستخلاص الدليل الإلكتروني 82

* الفرع الأول : المعاينة والخبيرة الفنية 83

أولا : المعاينة 83

ثانيا : الخبرة الفنية 85

* الفرع الثاني : التفتيش 87

أولا : تفتيش المكونات المادية للحاسوب 87

ثانيا : تفتيش المكونات المعنوية للحاسوب 88

* الفرع الثالث : ضبط الدليل الإلكتروني 88

أولا :تعريف ضبط الأدلة الإلكترونية 88

ثانيا : أنواع الأدلة الإلكترونية 90

ثالثا : الصعوبات التي تواجه المحقق في ضبط الدليل الإلكتروني.....91

➢ المطلب الثاني : القواعد الإجرائية المستحدثة لاستخلاص الدليل الإلكتروني.....91

* الفرع الأول : اعتراض المرسلات و الإيصالات السلكية و لاسلكية.....92

* الفرع الثاني : التسرب 94

أولا : تعريف التسرب..... 94

ثانيا : شروط التسرب 95

ثالثا : التسرب الإلكتروني 96

رابعا : جهات المشرفة على إجراء التسرب 97

* الفرع الثالث : مقدمي الخدمات 97

أولا : تعريف مقدمي الخدمات..... 98.

ثانيا : التزامات مقدمي الخدمات لمساعدة جهات التحقيق..... 98

خاتمة الفصل الثاني. 100

(الخاتمة) ـــ 101

(قائمة المصادر والمراجع) ـــ 106

ملخص :

أضحت الجريمة الإلكترونية اليوم واقعاً مفزعاً يهدد الدول و الأفراد ، ويعود ذلك أساسا إلى الإمكانيات المتاحة للمجرم المعلوماتي ، الذي يستطيع تعطيل موقع إلكتروني ، يستهدف الأمن الوطني أو يقرصن حساب أحد الشخصيات المعروفة ،كما يمكنه اختراق البنوك و الاستيلاء على أرصدة عملائها أو بيع معطياتهم البنكية السرية على صفحات الشبكة العنكبوتية.

وهذا ما جعل المجتمع الدولي يتحرك من أجل مكافحة هذه الجريمة ، بمجموعة من النصوص القانونية الموضوعية والإجرائية ، حيث تتمثل النصوص الموضوعية في تجريم الافعال التي يقوم بها المجرم المعلوماتي ، اما النصوص الاجرائية تتمثل في الاجراءات التي تتبعها الجهة القضائية للإدانة المتهم أو براءته ،كما تقوم هذه النصوص على اقامة التوازن بين مصلحة العدالة في تتبع المجرم المعلوماتي و الحقوق وضمانات الدستورية لحفظ حرمة الحياة الخاصة للإنسان ،كما تقوم هده النصوص الاجرائية بتنظيم اجراءات التحقيق التي تساعد في كشف الغموض عن هذا النوع من الجرائم .

و لمنح التحقيق صبغة مستحدثة لمواكبة تطور الجريمة المعلوماتية ، استوجب الاستعانة بخبراء و تقنيين يستخدمون نفس التقنية التي يعتمد عليها المجرم المعلوماتي ، و ذلك من أجل مساعدة المحقق في بعض الإجراءات مثل اجراءات التفتيش و المعاينة و التسرب قصد الوصول بما يسمى الدليل الرقمي ، و الذي يساعد على تكوين عقيدة القاضي في اصدار احكامه وقراراته باعتماده على أنظمة الإثبات الموجودة في الفقه الجنائي.

حيث تختلف أنظمة الإثبات من نظام إثبات حر يجعل القاضي يكون عقيدته من أي دليل مطروح أمامه ، أما الاثبات المقيد فهو ذلك النظام الذي يحدد المشرع فيه مجموعة من الأدلة ولا يمكن للقاضي الخروج عنها .

Aujourd'hui, la cybercriminalité est devenue une terrible réalité qui menace les pays et les individus, principalement à cause de cela. Aux capacités dont dispose le cybercriminel , qui peut désactiver un site internet, viser la sécurité nationale ou pirater le compte d'une des personnalités connues, et il peut aussi pirater des banques et saisir les soldes de leurs clients ou revendre leurs données bancaires confidentielles sur les pages Web.

C'est ce qui a poussé la communauté internationale à agir pour lutter contre ce crime, avec un ensemble de textes juridiques de fond et de procédure. Les textes établissent un équilibre entre l'intérêt de la justice dans la traque des informations criminelles et les droits et garanties constitutionnels pour préserver le caractère sacré des vie privée de l'être humain..

Afin de donner à l'enquête un caractère actualisé pour suivre le développement de la criminalité informatique, elle a nécessité l'assistance d'experts et de techniciens qui utilisent la même technologie que celle sur laquelle s'appuie le criminel informatique, afin d'assister l'enquêteur dans certaines procédures telles que procédures d'inspection, d'inspection et de fuite afin d'accéder à la preuve dite numérique, qui aide à la formation de la croyance du juge dans l'émission de ses jugements et décisions en s'appuyant sur les systèmes de preuve trouvés dans la jurisprudence pénale.

Là où les systèmes de preuve diffèrent d'un système de preuve libre qui fait du juge son credo de toute preuve qui lui est présentée, et la preuve restreinte est le système dans lequel le législateur détermine un ensemble de preuves et le juge ne peut s'en écarter.