وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص :إعلام آلـــــي و الأنترنت

الموسومة بـــ

التحقيق في الجريمة الإلكترونية

إعداد الطلبة:

- جبراني نورة
- لعماري سهام

إشراف الدكتور:

* دريسي عبد الله

- لجنـــة المناقشـــــــــة:

ذوادي عبد الله	أستاذ مساعد أ	رئيسا
دريسي عبد الله	أستاذ مساعد ب	مشرفا ومقررا
بلعقون محمد الصالح	أستاذ مساعد ب	مناقشا

السنة الجامعية 2024/2023

بسم الله الرحمن الرحيم

الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi - BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

إذن بالإيـــداع

أنا الممضي أسفله الأستاذ : د. بسكري عبد اللطيف .....

الرتبة : ..... أستاذ مساعد "ب" .....

المشرف على مذكرة الماستر الموسومة بـ : ..... التحقيق في الجريمة الإلكترونية .....

.....

من إعـــداد :

الطالب الأول : ..... جبيرة نورة .....

الطالب الثاني : ..... لغماري سهام .....

أوافق على إيداع الطالب (الطالبين) لمذكرة التخرج لدى الإدارة من أجل برمجتها للمناقشة.

إمضاء الأستاذ المشرف

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): جبراني نورة الصفة: طالب، أستاذ، باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم 177229265 والصادرة بتاريخ 2017/06/12

المسجل(ة) بكلية / معهد العلوم الإسلامية قسم العقوة

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: التحفيز في الجريمة الإلكترونية

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2021/06/12

توقيع المعني (ة)

شوهد لأجل تصديق الإمضاء
السيد: جبراني نورة
بت و او ر: 177229265
الصادرة بتاريخ: 2017/06/12

2021 جوان 21

عن رئيس المجلس الشعبي البلدي
وبتفويض منه
رئيس المصلحة التقنية للحالة المدنية
لقطي محمد

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): لعماري سوهام الصفة: طالب، أستاذ، باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم 405403419 والصادرة بتاريخ 2023/04/02

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: التحقيق في الجريمة الالكترونية

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2024/05/26

توقيع المعني (ة)

شوهد لأجل تصديق الإمضاء

السيد: لعماري سوهام

بت و اورس: 405403419

الصادرة بتاريخ: 2023/04/12

2024 ماي 29

رئيس المجلس الشعبي البلدي

وبتفويض من

رئيس مصلحة التنظيم والشؤون العامة

نقطي محمد

شكروعرفان

نحمد الله عزوجل أولا و نشكره

حيث وفقنا في إنجاز هذا العمل المتواضع الذي بذلنا فيه قصار جهدنا إعترافا بالفضل و الجميل نتوجه بخالص الشكر وعميق التقدير والامتنان

إلى الأستاذ المحترم **دريسي عبد الله** بقبوله الإشراف على هذا العمل في جميع مراحل إنجازه جزاه الله كل خير كما نتوجه بخالص الشكر والتقدير إلى الأساتذة أعضاء اللجنة بقبولهم مناقشة هذه المذكرة.

إهداء

لوالدتي رمز العطاء ونموذج الصبر والحب غير المشروط

إلى روح والدي سر عزيمتي وإلهامي وإيماني .

إلى زوجي رفيق دربي وشريك حياتي

إلى قرة عيني أولادي

هبة الرحمان، آلاء الرحمان، أنس عبد الرحمان

إلى النجوم المضيئة إخوتي وأخواتي وزوجة أخي

لهم جميعا أهدي هذا الجهد المتواضع

جبراني نورة

إهداء

أهدي ثمرة جهدي إلى روح فقيدايا الطاهرة أسأل الله تعالى أن يرحمها وينير قبرهما ويسكنهما فسيح الجنان *جدي و جدتي*

إلى أمي الثانية أطال الله في عمرها ورزقها الصحة خالتي الغالية

إلى التي أخرجتني من النور وملأت حياتي حبا وحنانا إلى التي أفاضت عليا بفضلها وكرمها إلى التي أعانتني بالدعوات و الصلوات أمي الحبيبة أدامها الله لي ورزقها الصحة وطول العمر

إلى من عمل بكد في سبيلي وعلمني معنى الكفاح وأوصلني إلى ما أنا عليه أبي الكريم أدامه الله لي

إلى سندي في هذه الحياة أخواتي الغاليات حرسهن الله لي و حفظهن من كل أذى

إلى أخي الوحيد وزوجته حفظهما الله و رعاهما

لعماري سهام

قائمة المختصرات :

أولا : باللغة العربية:

ج رج ج : الجريدة الرسمية للجمهورية الجزائرية

ص : الصفحة

ص ص : من الصفحة إلى الصفحة

ط : الطبعة

د ط : دون طبعة

د س ن : دون سنة النشر

ثانيا: باللغة الفرنسية

p:

page

مقدمة

مقدمة

عرف عالمنا المعاصر نقلة نوعية جد متسارعة،في مجال التطور العلمي والتكنولوجي في جميع المجالات خاصة ما تعلق منها بالشبكات الرقمية وسرعة تنقل المعلومات، أو ما يعرف بتكنولوجيات الإعلام والاتصال، حيث عرفت هذه الأخيرة قفزة وطفرة علمية وتكنولوجية جد متقدمة، حيث بات يعرف عصرنا اليوم بعصر المعلومات، بحيث تلاشت الحدود الجغرافية بين الدول والشعوب والأفراد وأصبح العالم مجرد قرية صغيرة، أين اجتاحت هذه التقنيات حياة الأفراد وأصبحت من الضروريات يستحيل الاستغناء عنها، حيث سمحت هذه الأخيرة بربط شبكات اتصال بين الأفراد والدول وجعلتهم في اتصال دائم ومستمر، خاصة بعد ظهور الحواسيب المحمولة والهواتف الذكية الأقمار الصناعية وشبكات الانترنت وقوة سرعة تدفقها التي بلغت الجيل الخامس والتي تبلغ سرعتها 01 جيغابايت في الثانية، لتشكل شبكة هائلة لنقل المعلومات حيث يمكن للمستخدم الولوج إليها في أي وقت وفي أي مكان باستعمال تقنيات جد حديثة في المعالجة الآلية للمعطيات والبيانات أو نقلها، ما انعكس سلبا وإيجابا على كثير من جوانب الحياة المعاصرة وما توفره من جهد ووقت وتكلفة، ما جعل حياة الإنسان أكثر بساطة وأكثر سهولة، الشيء الذي أدى إلى تضاعف الطلب على هذا النوع من التكنولوجيا وتوسع ميادين استعمالها بالرغم من الإيجابيات والمزايا التي سبق ذكرها بفضل تقنيات وسائل تكنولوجيا المعلومات والاتصال إلا أنها لا تخلو من الجوانب السلبية، حيث تمثل في بعض الحالات تهديدا خطيرا يمس الأمن والاستقرار، ما أدى إلى بروز نوع جديد من الجرائم المستحدثة لم تكن معروفة من قبل، ما اصطلح على تسميتها " بالجرائم الإلكترونية" أو "الجرائم المعلوماتية، ذات طبيعة خاصة، وهي لا تقل في خطورتها وحجم الأضرار التي قد تلحقها بالمجتمع عن خطورة أهم وأشد الجرائم التقليدية، غير أن التحقيق فيها بغية إثباتها كان أمر بالغ الصعوبة على القائمين بهذه المهمة، وذلك لعدم قدرة الوسائل والأساليب العامة على مواجهة هاته الجرائم المستحدثة، وضعفها في الكثير من الأحيان في الوصول إلى مرتكبيها، وتحديد المسؤولية الجنائية في هذا الإطار، وخاصة وأن مرتكبي هاته الجرائم تميزوا بالإحترافية

واستغلالهم للوسائل العلمية والتقنية الحديثة وتثير مسالة الإثبات في الجرائم الإلكترونية عوائق ومشاكل عديدة في مجال التحقيق وجمع الأدلة الجنائية، نظرا لمميزات وخصوصيات هذه الجريمة ما يشكل عقبة كبيرة أمام كشفها كما تكمن صعوبة إثبات في هذا النوع من الجرائم، في تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر الانترنت في سهولة محو الدليل الإلكتروني، كما لا يترك مرتكبيها أثار مادية بسبب دقتها وسرعة القيام بها وإمكانية محو أثارها وإخفاء الأدلة عقب وقوع الجريمة مباشرة كما أن ارتكاب هذه الجرائم يتعدى الاختصاص الإقليمي للدول يثير مشكلة الاختصاص المكاني والقانون الواجب التطبيق,كل ما سبق ذكره من خصوصيات للجرائم الإلكترونية وعوائق التحقيق فيها، دفع المختصون في مجال القانون والإعلام الآلي وتكنولوجيات الإعلام والاتصال، يكثفون جهودهم العلمية بالعمل على تطوير المنظومة القانونية وتطوير أساليب الحماية للنظم والبرامج الإلكترونية، وسد الثغرات التي تعتري النصوص الجزائية للتشريعات التقليدية القائمة، لمواجهة هذه الجريمة باستنباط الدليل الذي يتوافق مع الطبيعة التقنية التي يتميز بها هذا النوع من الجرائم.

تتبع أهمية الدراسة إلى أهمية الموضوع، باعتبار أن مرحلة التحقيق تعتبر من أهم مراحل الدعوى الجنائية، حيث تسمح هذه المرحلة بالحصول على دليل إثبات قوي ومتماسك لا يمكن دحضه من أجل ضمان حماية حقوق الضحايا ومحاكمة الجاني محاكمة عادلة وتوقيع الجزاء المناسب مبنية على مبدأ الشرعية، كما تبرز أهمية الموضوع في التطور السريع والمستمر الذي تتميز به الجريمة الإلكترونية الأمر الذي ألزم المشرع وسلطات التحقيق العمل على تطوير وسائل وأساليب التحقيق، فهي جريمة بلا حدود تمس الأشخاص المعنوية والطبيعية على حد سواء كما أن الخاصية اللامادية للدليل الإلكتروني خلقت صعوبات غير مسبوقة أمام سلطات التحقيق بالتالي كان من المنطقي أن تنصب دراستنا على الجوانب الإجرائية المتعلقة بجمع الدليل الإلكتروني ونتيجة ذلك سوف نركز في بحثنا هذا على السلطات المختصة بالتحقيق في الجريمة الإلكترونية وكذلك على الجانب الإجرائي وما تقوم به هذه السلطات من إجراءات لجمع الدليل الإلكتروني وكذلك الهيئات المناط بها مهمة التحقيق الجنائي، بالتالي

بات من الضروري إعطاء هذا الموضوع الأهمية القصوى واتخاذ التدابير والإجراءات الضرورية لحماية الأشخاص الطبيعية والمعنوية والمجتمع من هذه الجريمة.

ترجع أسباب اختيارنا لموضوعنا: "التحقيق في الجريمة الإلكترونية" يرجع في حقيقة الأمر إلى العديد من الأسباب بعضها أسباب شخصية والأخرى موضوعية **فالأسباب الشخصية** تكمن في التعرف أكثر على هذا النوع من الجرائم نظرا لحداثتها وتقنية الوسائل المستعملة والتزايد الهائل لعدد القضايا المطروحة في أروقة العدالة وانتشارها بمعدلات قياسية لا متناهية تزامنا مع التطور التكنولوجي المستمر الذي يعرفه هذا المجال بظهور الهواتف الذكية والاهتمام بمجال المعلوماتية وإجراءات المتابعة في جريمة المعالجة الآلية للمعطيات التي تختلف كل الاختلاف عن إجراءات التحقيق التقليدية بالإضافة إلى أنه موضوع جديد ومتجدد، والرغبة الشديدة في الغوص في مجال إجراءاتها الفني والتقني.

أما الأسباب الموضوعية فتكمن فيما يطرحه موضوع الحماية الإجرائية للجريمة المعلوماتية منً إشكاليات قانونية التي لا بد من الوقوف عندها نظرا لحداثتها ومن جانب تجريم الأفعال والاعتداءات الماسة ب أنظمة المعالجة الآلية للمعطيات والقواعد الإجرائية الحديثة التي جاء بها المشرع بتعديل قانون الإجراءات الجزائية الجزائري وكذا قانون /09 04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته وغيرها من القوانين التنظيمية.

تهدف هذه الدراسة: تسليط الضوء على هذا النوع من الجرائم المستحدثة التي تزداد انتشارا، مع الانتشار المتسارع لتكنولوجيات الإعلام والاتصال بشكل رهيب وتطور شبكة الانترنت وازدياد سرعة تدفقها وكثرة استعمال وسائل التواصل الاجتماعي على غرار الفايسبوك والأنستغرام....الخ وبالتالي التركيز من خلال بحثنا هذا على التعرف على الجرائم الإلكترونية وخاصة إجراءات التحقيق وكيفية مواجهتها مواكبتها.

وما يواجه هذا الموضوع من صعوبات اعترضننا أثناء إعداد هذا العمل المتواضع حيث تتمثل في حداثة هذا الموضوع ونقص المراجع والمؤلفات المتخصصة في هذا المجال ولو أن هناك

مجموعة من المراجع والمقالات التي تطرقت إلى الموضوع لكن بشكل جزئي دون تناول كل جوانبه وإنما تمت معالجته بشكل سطحي بالإضافة إلى ارتباط هذا النوع من الجرائم بالحاسب الآلي والذكاء الاصطناعي وما يتطلبه من إحاطة بمكونات هذا ألخير وما بتطلبه من تقنيات تتعلق بهذا النوع من الجرائم وكل ما يحتاجه من جهد فني وقانوني، بالتالي صعوبة الإلمام بالموضوع والحصول على المعلومات الكافية.

ومن هذا نطرح الإشكالية التالية:

_ ما مدى خصوصية التحقيق في الجريمة الإلكترونية في التشريع الجزائري؟

ومنه يمكننا الخروج بإشكاليات فرعية:

- ما مفهوم الجريمة الإلكترونية؟
- هل هناك أجهزة خصصها المشرع لمكافحة الجريمة الإلكترونية ؟
- هل يجب أن تتوفر بعض المهارات لدى المحقق للتحقيق في الجريمة الإلكترونية ؟

ومنه للإجابة عن هذه الإشكالية اعتمدنا على المنهج الوصفي التحليلي، وصفي لأن دارستنا سترتكز على وصف المفاهيم العامة الخاصة بالجريمة المعلوماتية وآليات التحقيق في الجرائم الالكترونية في ظل التشريع الجزائري لاستخلاص الدليل والعقبات التي تعتريها، وتحليلي لأننا سنستعرض أهم العقبات القانونية التي تطرحها المواجهة الإجرائية للجريمة الالكترونية، ثم مناقشتها وتحليلها بشكل مفصل والغوص في جزئياتها.

ومن الدراسات السابقة التي تناولت موضوع التحقيق في الجريمة الإلكترونية، ومن خلال عملية البحث التي قمنا بها عبر المراجع المتعلقة بالموضوع، ونظرا لحداثته، فقد وجدنا رسالة ماجستير للطالب سعيداني نعيم تحت عنوان: " آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري" جامعة باتنة 2013 وكذلك أطروحة دكتوراه للطالب براهيمي جمال المعنونة ب: التحقيق الجنائي في الجرائم الإلكترونية جامعة تيزي وزو 2018،وكذلك رسالة

دكتوراه للطالبة حبيباتتي بثينة تحت عنوان" الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" جامعة الجزائر سنة 2020.

الفصل الأول:

ماهية التحقيق الجنائي في الجريمة الإلكترونية

الفصل الأول ماهية التحقيق الجنائي في الجريمة الإلكترونية

شهد عصر المعلوماتية تطورا ملحوظا فيما يخص وسائل التحقيق الجنائي، وكان ذلك تزامنا مع حركة الجريمة وتطور أساليب ارتكابها، فبعد أم كانت وسائل التحقيق تتميز بالعنف والتعذيب بغية الوصول إلى الدليل أصبحت في مرحلة لاحقة تتميز بالطابع العلمي وذلك بالاستعانة بالأساليب العلمية واستخدام الانترنت، ويرجع ذلك الى حدوث طفرة علمية في مجال تكنولوجيا المعلومات والاتصالات واستخدام الوسائط الالكترونية في شتى مجالات الحياة، فكلما اكتشف العلم شيئا حديثا وجد هذا الاكتشاف طريقه في مجال الإثبات الجنائي، هذا التطور العلمي أدى الى ظهور أنماط جديدة من الجرائم لم تعهد من قبل فالمجرم والجريمة في تجدد مستمر مع العصر الأمر الذي أيستوجب معه تعديل الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الجرائم واستحداث وتطوير أساليب التحقيق فيها.

ولتحقيق بصفة عامة يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهية لديه، وأن يحاول بكل جهده أن يقوم بالتحقيق في الجريمة ومتابعتها وبالبحث فيها وفي أدلة الإثبات من أجل إظهار الحقيقة، لذلك سوف نتطرق في هذا الفصل إلى ماهية التحقيق الجنائي في الجريمة الإلكترونية حيث يتضمن المبحث الأول الإطار المفاهيمي للتحقيق الجنائي في الجريمة الإلكترونية والمبحث الثاني يتمثل في الأجهزة المكلفة بالبحث والتحري في الجرائم الإلكترونية.

المبحث الأول:الإطار المفاهيمي للتحقيق الجنائي في الجريمة الإلكترونية:

أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم، حيث ظهرت عدة أراء فقهية في محاولة فهم مقصود الجريمة الإلكترونية.

وعليه سنحاول من خلال هدا المبحث أن نتطرق إلى مفهوم الجريمة الالكترونية والتحقيق فيها حيث يتضمن المطلب الأول ماهية الجريمة الالكترونية فنتطرق في الفرع الأول إلى تعريف الجريمة الإلكترونية والفرع الثاني خصائصها، أما المطلب الثاني يتضمن ماهية التحقيق الجنائي بفرعيه الأول يتمثل في تعريف التحقيق الجنائي والمحقق ويتضمن الثاني خصائص التحقيق والمحقق في الجريمة الإلكترونية.

المطلب الأول: ماهية الجريمة الإلكترونية

ظهرت تعاريف كثيرة التي تعرف الجريمة الالكترونية مابين مضيق لمفهومها وموسع كما تعددت المصطلحات المستخدمة للدلالة عليها فالبعض استخدم مصطلح جرائم استخدام الحاسب أو جرائم المعالجة الآلية للبيانات والبعض الأخر أطلق عليها أسم الإجرام ألمعلوماتي وفيما يأتي تفصيل لمفهوم الجريمة الإلكترونية وخصائصها.

الفرع الأول: تعريف الجريمة الإلكترونية

إن غياب تعريف قانوني دقيق لهذا المصطلح وترك الأمر إلى الفقهاء لإعطاء مفاهيم وتصورات مختلفة جعل الأمر أكثر تعقيدا، ويعتبر هذا الاختلاف مصدر التداخل أو الخلط لهذه المصطلحات سواء على مستوى مجال انعكاسه، أو المصطلح المختار.

وهذا الخلط الاصطلاحي يشكل عائقا أمام رجال القانون لبحث وفهم هذه الجريمة وقد يكون السبب في عدم وجود تعريف محدد وموحد، طبعا في ظل غياب نص قانوني يعرف الجريمة الإلكترونية _أنها جريمة مستحدثة نسبيا، وأن وضع تعريف قد يضيق من نطاقها وقد يطرح إشكالية التماثل أو الاختلاف بين الجريمة الإلكترونية والجريمة المعلوماتية، فهل الجريمة

الإلكترونية تحوي الجريمة المعلوماتية أو العكس؟ وللإجابة على هذا التساؤل يستدعي الأمر تحليل بعض المفاهيم.

والغالب أن التشريعات الخاصة يردع هذا النوع من السلوكيات عادة ما لا تضع تعريف، بالتالي يطبق عليها تعريف الجريمة بشكل عام، وهنا يبرز دور الفقهاء حيث أن كل منهم يعرفها بحسب وجهة نظره منطلقا من الزاوية التي ينظر من خلالها للجريمة الإلكترونية فهناك من يضيق من نطاقها فيقصرها إما على المال ألمعلوماتي المعنوي (البرامج والمعلومات)، أي الجريمة التي يكون الحاسوب الإلكتروني بمكوناته المادية والمعنوية موضوعا لها، أو أن الحاسوب الإلكتروني وسيلة أساسية لارتكابها، وقد ينظر إلى الفاعل حيث تكون له خبرة في مجال الإلكترونيات، ويعتمد على هذه المعايير كل على حدى وهناك من يعرفها تبعا لمنظور موسع يقتضي أن الجريمة الإلكترونية هي كل السلوكات غير مشروعة التي ترتكب باستخدام الحاسب الآلي[1].

أولا:تعريف الجريمة لغة:

الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه وجريمة الرجل على قومه وإليهم: أذنب وحتى جناية [2]

ثانيا: تعريف الجريمة اصطلاحا: معظم الفقهاء المؤلفين في هذا الباب يردون تعريف الجريمة في الفقه إلى ما قرره الماوردي في الأحكام السلطانية بقوله: "الجرائم محظورات شرعية زجر الله عنها بحد أو تعزير يعني إذا كانت ممن يتعمد ارتكابها "، أما الإمام ابو زهرة فبعدما ذكر تعريف الماوردي وأيده ساق من بين نصوصه تعريفا أخر للجريمة فقال: "هي المعصية التي يكون فيها عقاب يقرره القانون[3].

[1] غنية باطلي، الجريمة الإلكترونية(دراسة مقارنة) دار الجزائرية ، الجزائر د_ط ، ص 13

[2] علي بن هادية بلحسن البليش والجيلالي بن الحاج يحي، القاموس الجديد للطلاب، الشركة الوطنية، الشركة التونسية، الجزائر، تونس، ط1، 1979 ص 251

[3] ضياء مصطفى عثمان، السرقة الإلكترونية، دار النفائس، عمان، ط1، 2011، 1979 ص 32

ثالثا: تعريف الجريمة الإلكترونية فقها:

مما يلاحظ في هذا الشأن هو عدم وجود اتفاق سواء على المستوى التشريعي أو الفقهي على استعمال مصطلح معين للدلالة على هذا الظاهرة الجرمية الناشئة في بيئة الكمبيوتر والإنترنت، وهو إختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات، فهناك من يطلق عليها مصطلح جرائم الغش المعلوماتي، أو الجرائم المعلوماتية، أو الجرائم الإلكترونية، أو جرائم الحاسب الألي، أو جرائم تقنية المعلومات، أو الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو جرائم التكنولوجيا الحديثة، أو جرائم الكومبيوتر والإنترنت، ويرجع السبب في ذلك إلى عدة عوامل منها التطور المستمر واللا متناهي لتكنولوجيا المعلومات والاتصالات، مما نتج عنه جرائم مستحدثة اختلفت التشريعات حول وضع مفاهيم موحدة لها، وقد يكون السبب أيضا ترك المجال أمام المشرع لاحتواء التقنيات المتلاحقة في هذا الميدان، ولعدم حصر قاعدة التجريم في نطاق أفعال معينة تتبدل في المستقبل، ويثير هذا الإشكال العديد من التحديات أهمها صعوبة مواجهتها وتعذر الحلول المناسبة لمكافحتها سواء على المستوى الداخلي أو الدولي، ورغم هذه الصعوبات حاول الفقهاء جاهدين وضع مفهوم لهذه الجرائم المستحدثة أين برز اتجاهين هما:

1 – الاتجاه الضيق لمفهوم الجريمة الإلكترونية:

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وربطها بعناصر عديدة كالحاسوب، أو مستخدمه، أو بموضوعالجريمة، حيث عرفها الفقيه ماروي على أنهاَ:"الفعل الغير المشروع الذي يستخدم في ارتكابه الحاسب الآلي، وهناك من عرفها على أنها:"فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه، أو هي "الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الانترنت "، كما عرفت أيضا بأنها:"الجرائم التي تقع على جهاز الكمبيوتر

أو داخل نظامه فقط"، أو هي "مجموعة من المخالفات الجزائية التي تقع ضد شبكات الإعلام الآلي[1].

وفي تعريف أخر هي "الأفعال غير القانونية المرتكبة بواسطة العمليات الالكترونية والتي تمس، بالنظام المعلوماتي أو بالمعطيات التي يحتويها ومهما كان الهدف من ذلك ,من جانب آخر عرفها الفقيه روزبلايت: كل نشاط غير مشروع موجه لنسخ أو تغيير أو الوصول إلى المعلومة المخزنة داخل الكمبيوتر أو ذلك التي يتم تحويله عن طريقه، كما عرفها الفقيه الألماني تادمان على انها: "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب، من جهة أخرى عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا,

وعليه يربط أنصار هذا الاتجاه تعريفهم لهذه الجرائم بضرورة وجود الحاسوب الذي قد يكون أداة للجريمة أو هدفا لها، ناهيك عن وجود معارف مسبقة بتكنولوجيا الكمبيوتر ليس فقط من المجرم المعلوماتي، وإنما أيضا من القائمين على ملاحقة هذا النوع من الجرائم، وهذا يضيق على نحو كبير من الجريمة الإلكترونية التي هي في إتساع يوما بعد يوم تبعا لتطور تكنولوجيا المعلوماتية ,

من جهة أخرى، هناك جرائم الكترونية لا تتطلب هذا القدر كله من المعرفة على اعتبار أن المعلوماتية صارت متاحة للجميع مثل:إرسال رسالة نصية بالهاتف أو بالبريد الإلكتروني، أو نسخ بيانات من حاسوب ,,,,,إلخ، كما أن حصر الجرائم الإلكترونية هي المسماة"بجرائم المعالجة الألية للمعطيات"، إذ يخرج من هذا النطاق جانب كبير من الأفعال غير المشروعة التي يستخدم الحاسب كأداة لارتكابها مثل:جرائم الاحتيال المعلوماتي، وبالتالي يتسم تعريف هذا الاتجاه للجرائم الالكترونية بالنقصان مما أدى إلى ظهور اتجاه ثان مخالف له نتناوله فيما يأتي:

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات – د_ط ، دار الجامعة الجديدة الإسكندرية سنة 2019 ، ص 31

1 – الاتجاه الموسع لمفهوم الجريمة الإلكترونية

على عكس الاتجاه السابق، يذهب فريق من الفقهاء إلى التوسع في مفهوم الجرائم الإلكترونية أو المعلوماتية وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية، فيعرفونها على أنها " كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل، كما عرفتها منظمة التعاون الاقتصادي والتنمية بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، كما تعرف أيضا على أنها:تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية المعلوماتية[1].

هذه التعريفات واسعة تتيح الإحاطة الشاملة قدر الإمكان بظاهرة التقنية، كما أنها تعبر عن الطالع التقني أو المميزالذي تنطوي تحته أبرز صورها، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية، ويعرفها آخرون على أنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الألية للبيانات أو بنقلها، إذ يعتمد هذا التعريف على معيارين أولهما وصف السلوك، وثانيهما إتصال السلوك بالمعالجة الألية للبيانات أو نقلها، كما يجمع الفقه الفرنسي بصفة عامة على القول بأن الغش المعلوماتي التي تعادل جرائم الحاسب الألي تشمل العديد من الأفعال المتنوعة، حيث عرف كل من الفقيه ميشال والفقيه ريدو الجريمة المعلوماتية بأنها:"سوء استخدام الحاسب ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، وكذا الإستخدام غير المشروع لبطاقات الائتمان وإنتهاك ماكينات الحاسب الألي بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب وسرقة الحاسب الألي في حد ذاته أو أي مكون من مكوناته، كما عرفت المادة (01) من القانون العربي النموذجي الموحد بشأن مكافحة سوء إستخدام تكنولوجيا المعلومات والإتصال لسنة 2003 الجرائم الإلكترونية

[1] يزيد بوحليط، المرجع السابق، ص 31-32-33

على أنها:"كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني"، وعرفت المادة نفسها الوسيط الإلكتروني على أنه: "شبكة الحاسب الألي أو الأنترنيت أو أي شبكة إلكترونية أخرى"، أو هي:"مجموعة المخالفات التي تقع على شبكات الإتصال عموما وعلى شبكة الانترنت خصوصا.

وبذلك تمثل هذه التعاريف المفهوم الموسع للجرائم الإلكترونية، والتي تتم بالحاسوب سواء كان هدفا لها أو وسيلة لارتكابها، أو عن طريق شبكة الانترنت أو بأي وسيلة إلكترونية أخرى تظهر مستقبلا كوسائل الاتصال الحديثة مثل الهاتف النقال وجهاز الفاكس وغيرها.

مما لا شك فيه أن هذا الاتجاه ينطوي على توسع كبير لمفهوم الجرائم الإلكترونية، فهي كل جريمة تتم بمساعدة الحاسوب أو في محيطه، أو عن طريق شبكة الأنترنت أو أجهزة الإتصال الحديثة. وبناء على التعريفات السابقة تتخذ الجريمة الإلكترونية صور عديدة، تتمثل في استخدام الحاسوب كوسيلة لارتكاب الجرائم أو الاعتداء على الحاسوب نفسه ونظامه أو استخدام أي وسيلة إلكترونية أخرى توفرها التقنيات الحديثة، بمعنى آخر فإن الجرائم الإلكترونية تزاوج بين تقنية الحوسبة وتقنية الإتصالات الحديثة، فإذا عدنا للحقيقة الأولى المتصلة بوالدة وتطور تقنية المعلومات نجد أن تقنية المعلومات تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما، فرع الحوسبة وفرع الاتصال أما الحوسبة فتقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها[1].

هذه الدلالة يحددها الأستاذ زياينغ إكزيوو(الرسائل والأخبار والبيانات والمعرفة والوثائق الأدب والفكر والرموز والعلامات والإرشادات الخفية والأنباء المفيدة والسرية وغير ذلك).

وباستقرائنا لمختلف التعريفات نجد أن تعريف منظمة التعاون الاقتصادي والتنمية السابق الذكر يتسم بالوضوح والشمول وذلك للأسباب التالية:

[1] يزيد بوحليط، المرجع السابق، ص 34

– تحديد لماهية السلوك الإجرامي للجريمة، إذ شمل كل من الفعل الإيجابي والسلوك السلبي المتمثل في الإمتناع.

– إعتماد تعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة الجرائم التقنية، وذلك لربطه بين الجريمة وأي تدخل للتقنية المعلوماتية بصفة مباشرة أو غير مباشرة كما تتسم هذه التقنية بالتطور المستمر[1].

– يعبر عن الطابع التقني المميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية.

– يتيح إمكانية التعامل مع التطورات المستقبلية في مجال تقنية المعلوماتية ونظم الإتصالات ونستخلص مما سبق أن اختلاف الفقه في وضع تعريف للجريمة المعلوماتية أو الإلكترونية مرده، الاختلاف في المعيار المعتمد عليه والزاوية التي ينظر إليها كل اتجاه إلى هاته الجريمة المستحدثة، إلا أنه يمكن إعطاء تعريف ملخص تبعا لهذه الاتجاهات فهي:" سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر" فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ومعاقب عليه قانونا، لأن إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك، ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة، البرامج بأنواعها المعلومات المستخرجة، والمتبادلة بين الأنظمة المعلوماتية....إلخ)، وأما الكمبيوتر فهو "النظام التقني بمفهومه الشامل الذي يزاوج بين تقنيات الحوسبة والاتصال"بما في ذلك شبكات المعلومات.

وعلى هذا الأساس فإن محاولة إعطاء تعريف لهذا النوع من الجرائم المستحدثة الذي يتم في بيئة افتراضية يجب أن يراعى فيه عدة اعتبارات منها:

[1] يزيد بوحليط، المرجع السابق ، ص35

1- يجب أن يتلاءم هذا التعريف مع فكرة عالمية المعلومات والاتصالات وأن يكون واضحا عالميا.

2- يجب مراعاة التطورات المتلاحقة في عالم الحوسبة والاتصال ويسمح باستيعاب كل ما يستجد من صور للجرائم الالكترونية.

3- يجب توضيح خصوصية الجرائم الالكترونية لما تحتويه على أشكال مختلفة للسلوك الإجرامي بحيث يظهر جليا دور الحاسوب في ارتكاب هذه الجرائم[1].

رابعا: تعريف الجريمة الإلكترونية قانونا:

من المعلوم أن المشرع الجزائري وإلى وقت قريب أغفل تنظيم مجال الجريمة الالكترونية قانونا، إلا أنه مافتئ أن تدارك ذلك الفراغ القانوني من خلال سن قواعد قانونية لمواجهة هذه الجريمة، وذلك ما تجلى في القانون 04_15 المتضمن تعديل قانون العقوبات، الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الألية للمعطيات، ثم تلاه بالقانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

1- تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 04-15:

بالرجوع إلى قواعد القانون 04-15 من المادة 394 مكرر 2 نجد أنه حدد مفهوم المساس بأنظمة المعالجة الألية للمعطيات،حيث حددها في المادة 394 مكرر بالأتي[2]:

- الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.

[1] القانون رقم 04-15 المؤرخ في 10 نوفمبر، يعدل ويتمم الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج_ر، العدد 71 لسنة 2004.

[2] رحموني محمد،خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة ، جامعة أحمد دراية-أدرار العدد 41، ص 438-439

– حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكرر 1 فقد أشارت إلى ما يلي:

– إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

وبالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من الآتي:

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

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[1]..

1- تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 09-04:

– حددت المادة (02) منه الجريمة الإلكترونية بقولها: " يقصد في مفهوم هذا القانون"[1] بما يأتي:

– **الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:** جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

[1] القانون 09-04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، العدد 47 لسنة 2009.

– **منظومة معلوماتية:** أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

معطيات معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها[1].

الفرع الثاني:خصائص الجريمة الإلكترونية

تتميز الجرائم الواقعة على الحاسوب والإنترنت أي بواسطتها عن الجرائم التقليدية بعدة خصائص منها:

أولا:جرائم عابرة للقارات، بحيث يمكنها أن ترتكب في دولة وأثرها يكون في دولة أخرى، لذا هي جرائم لا تعترف بالحدود الجغرافية للدول، وهذا الأمر يتطلب ضرورة التعاون الدولي لمواجهة هذا النوع المستحدث من الجرائم أسوة بالجرائم العابرة للحدود الأحرى، كالمخدرات وتجارة الرقيق وغيرها، وتجدر الإشارة إلى أن هذه الجرائم الأخيرة يمكن ارتكابها عبر الحاسوب أو الإنترنت[2].

ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهذا ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إلا أن الفاعل لا يتواجد في مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي لحصول الجريمة الإلكترونية في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر الفاعل وبين المعلومات محل الإعتداء فقد يوجد

[1] _رحموني محمد– المرجع السابق، ص440

[2] – علي حسن الطوالبة– جامعة العلوم التطبيقية مملكة البحرين، الجرائم الالكترونية، ص 59

الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الكمبيوتر الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث[1].

ثانيا:صعوبة الإثبات والإكتشاف:

ويعود هذا الأمر إلى عدم وجود أثر مادي ملموس بعد ارتكابها، وتعتمد في العادة على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.

كما أنها صعبة الإكتشاف لأنها تنفذ بواسطة وسائل دقيقة ومتطورة فهي تتميز بكونها مستترة ومتخفية في غالب الأحيان ولا تترك أي ذليل كتابي أو مادي واضح لتنفيذها بوسائط إلكترونية تؤثر على الضحية اما في مال أو شخصه إما بالسرقة أو التعديل أو الإتلاف أو التحطيم والسبب في عدم ترك أثر أو دليل خارجي وقدرته على محوه في أقل من ثانية.[1]

ثالثا:جرائم ناعمة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة، وغيرها، فالجرائم الإلكترونية لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، علة أساس أن الجاني في الجرائم الإلكترونية هو إنسان متوافق مع المجتمع، ولكنه يقترف هذا النوع من الجرائم بدافع اللهو او لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما.[2]

رابعا:تحقق مكاسب مادية كبيرة بسهولة:

تميزها عن جرائم الأموال العادية، حيث يمكن تحويل مبالغ مالية ضخمة من بنك إلى بنك آخر، أو غسل الأموال من دولة إلى دولة أخرى، ولسهولة الاختفاء فيها شكلت عامل إغراء للكثيرين لارتكاب جرائم واقعة على الأموال من خلال الحاسوب والأنترنت.[3]

[1] نائلة محمد قورة، جرائم الحاسب الآلي الإقتصادية، ط 1، منشورات الحلبي الحقوقية بيروت 2005، الجرائم، ص 32.

المطلب الثاني: ماهية التحقيق الجنائي في الجرائم الإلكترونية

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، والتحقيق في الجرائم الالكترونية يختلف عن التحقيق في الجرائم العادية من حيث الإجراءات وذلك لحداثة هذه الجريمة ومهارة مرتكبيها في الإجرام ومحو الأدلة.

الفرع الأول: تعريف التحقيق الجنائي في الجريمة الالكترونية:

تعريف التحقيق في الجريمة الإلكترونية لا يختلف عنه في الجرائم الأخرى وسنتناول تعريفه اصطلاحا وحتى يكتمل التعريف بالتحقيق يجدر بنا التطرق إلى تعريف المحقق الذي يقوم بكافة إجراءات التحقيق.

أولا – تعريف التحقيق إصطلاحا: عرف التحقيق بمعناه العام أنه: "اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها"[1].

وعرف التحقيق على أنه: مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة، كذلك هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا، بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة[2].

[1]– عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، رسالة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية، 2007، ص. 22.

[2]– عمر بن إبراهيم بن حماد العمر، مرجع سابق، ص23.

وكما عرف التحقيق أيضا بأنه " مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهدف التنقيب عن الأدلة وتقديرهاوالكشف عن الحقيقة في شأن جريمة ارتكبت لتقرير لزوم محاكمة المدعي عليه أو عدم لزومها[1].

كما يمكن تعريف التحقيق الجنائي في الجرائم الالكترونية بأنه عمل قانوني يقوم به مأمور الضبط القضائي المختص والمتخصص لضبط الجرائم الإلكترونية من فاعل ودليل الكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل.[2]، وهناك من قسم التحقيق إلى:

- **التحقيق الجنائي العملي:**

و يقصد به جميع إجراءات التحقيق التي يباشرها المحقق الجنائي عند وقوع جريمة أو حادث، توصلا إلى معرفة الحقيقة وقواعد أساسها التجارب العلمية التي وصل إليها المحققون في تحقيق القضايا الهامة.

- **التحقيق الجنائي الفني:** ويرتكز على الأبحاث العلمية والتجارب الفنية التي يمكن تطبيقها لاكتشاف حقيقة الحوادث الجنائية والاهتداء إلى مرتكبيها[3].

ثانيا – تعريف المحقق:

ذهب جانب من الفقه إلى تعريف المحقق بأنه: " كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، وتحقيقها ويسهم بدوره في كشف غموضها وصولا

[1]– حسن الجوخندار، التحقيق الإبتدائي في قانون أصول المحاكمات الجزائية، ط 01، دار الثقافة، عمان، 2008، ص.11

[2]– مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط01، مطابع الشرطة المرور، القاهرة، 2008، ص 166

[3] عبد الفتاح مراد، المرجع السابق، ص 11.

إلى معرفة حقيقة الحادث وكشف مرتكبه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة" [1].

أما المشرع الجزائري فقد وضع تعريف لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية حيث جاء في نصها ما يلي:" يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي[2].

كما يمكن تعريف التحقيق الجنائي في الجرائم الالكترونية بأنه عمل قانوني يقوم به مأمور الضبط القضائي المختص والمتخصص لضبط الجرائم الإلكترونية من فاعل ودليل الكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل[3].

– يشكل التحقيق الجنائي المعلوماتي أو التحقيق الجنائي في البيئة المعلوماتية تحديا كبيرا للدول بالنظر إلى طبيعة هذا التحقيق وطبيعة هذه معظم الدول تستحدث أجهزة متخصصة تتولى مهمة التحري والكشف عن هذه الجرائم الإلكترونية، وعلى المستوى الوطني أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بـ: شاطوناف الجزائر العاصمة إذ يحتوى على مخبر خلية الإعلام بالإضافة إلى مخبرين جهويين بكل من وهران وقسنطينة كما توجد على مستوى مركز الأمن الولائي فرق متخصصة في التحقيق في الجريمة الإلكترونية بالتنسيق مع المخابر، كما يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي قسم الإعلام والإلكترونيك يختص بالتحقيق في هذا النوع من الإجرام.[4]

---

[1]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط01، دار الفكر الجامعي، مصر، 2009، ص 87

[2]– الأمر رقم 66–155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم، العدد رقم 48 الصادر يوم 10 جوان 1966

[3]– مصطفى محمد موسى، مرجع سابق، ص. 166

[4]– عيدة بلعابد خصوصية التحقيق في الجريمة المعلوماتية، **مجلة الباحث الأكاديمي في العلوم القانونية والسياسية**، جامعة مولاي الطاهر سكيكدة، العدد: 06، 2011، ص. 137.

وعلى ذلك يتضح أن إجراءات التحقيق تمر بثلاث مراحل كلها تهدف إلى ضبط الجاني وتقديمه للادعاء بأدلة اتهامه ثم إلى المحكمة لإعداد الحكم في القضية وهذه المراحل هي:

1- مرحلة جمع الاستدلالات بواسطة مأموري الضبطية القضائية المختصين بالبحث في الجرائم ومرتكبيها.

2- مرحلة التحقيق الابتدائي لمعرفة النيابة العامة او قاضي التحقيق لتحريك الدعوى أو حفظ التحقيق لعدم كفاية الأدلة.

3- مرحلة التحقيق النهائي في محكمة الموضوع وفيها مرافعات من اتهام ودفاع عن المتهم.

الفرع الثاني: خصائص التحقيق في الجريمة الالكتروني

تعد مرحلة التحقيق الابتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات مرحلة هامة في سبيل البحث والتحري عن الجرائم وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة الالكترونية لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبق متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلي الطبيعة التقنية لهذه الجرائم.

ففي كثير من الجرائم الإلكترونية لم يترك الجاني ورائه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإعجاب والإحباط معا[1].

و يتميز التحقيق في الجريمة الإلكترونية بمجموعة من الصفات أو السمات تميزه عن التحقيق الجنائي في الجرائم التقليدية وترجع هذه الذاتية للأسباب التالية:

[1]- محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الأنترنت ، ط01، منشورات الحلبي الحقوقية، 2011، ص. 230.

1- إن مرتكبي الجريمة الالكترونية لديهم قدرة الكترونية قادرة على سرعة إتلاف وتشويه وإضاعة الدليل الالكتروني الرقمي في وقت قصير.

2- أن هذه النوعية من الجرائم الإلكترونية الرقمية لا تترك أثرا ماديا في كثير منها في مسرح الجريمة الالكترونية

3- أن التحقيق في الجريمة الالكترونية ذات البنية الرقمية يحتاج لإمكانيات مادية قواعد وإجراءات تختلف عن التحقيق في الجرائم التقليدية سواء من حيث طبيعة السلوك الإجرامي الالكتروني أو من حيث الدليل الالكتروني أو وسائل آليات كشف الجريمة والوصول إلى الدليل الإلكتروني.

أولا - المختصون في التحقيق الابتدائي في الجريمة الإلكترونية

يجب أن يتشكل فريق التحقيق من فنيين وأخصائيين ذوي خبرة طويلة في مجال الحاسوب والانترنت يمتازون بمهارات تقنية في الحاسوب والتحقيق الجنائي بشكل عام والتحقيق الجنائي الالكتروني بشكل خاص، أو أن يستعين هؤلاء المحققون بخبراء في مجال الحاسوب والانترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة.[1]

إن التحقيق في هذه الجرائم قد يتطلب الاستعانة ببعض خبراء الجرائم التقليدية مثل خبير البصمات وخبير التصوير الذي يعتبرون من الخبراء الأساسين في معظم أنواع الجرائم، بالإضافة إلى غيرهم من الخبراء الذين قد يفرضهم ارتباط جريمة الحاسوب والانترنت محل التحقيق بجريمة أخرى من الجرائم التقليدية كجريمة القتل وغيرها، ومجالات الخبرة هذه وإن كانت مهمة في مساعدة المحقق على معاينة مسرح الجريمة وجمع الأدلة بشكل سليم إلا أنها لا تختص بالتعامل مع جرائم الحاسوب والانترنت دون غيرها من الجرائم بل هي تخصصات عامة يكاد لا يستغني التحقيق عنها في أية جريمة[2].

---

[1]- عبد الله حسين محمود، إجراءات جمع الأدلة في مجال الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003، ص612

[2]- محمد البشرى، التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والأنترنت، الإمارات، 2000، ص 73.

ونظرا لان التحقيق في جرائم الحاسوب والانترنيت يتطلب مهارات فنية قد لا تتوافر لدى كثيرين من المحققين فان تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم قد يكون أمر ضروريا وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في جرائم الإلكترونية لما تتطلبه من مهارات وخبرات متنوعة ومتعددة.

وعلى هذه الأساس يتكون فريق التحقيق في الجرائم الالكترونية من الخبراء التالين وهم:

1- المحقق الرئيس من ذوي الخبرة الطويلة في جرائم الحاسوب والأنترنت وكذلك في مجال التحقيق الجنائي.

2- خبراء الحاسوب والشبكات الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم.

3- خبراء ضبط وتحرير الأدلة الإلكترونية الجنائية العارفين بأمور تفتيش الحاسوب وأخذ إفادة العاملين على الأجهزة التي وقعت الجريمة عليها.

4- خبراء العمليات المحاسبية الذين يتعاملون مع الأنظمة البرمجية وتبادل النقد الإلكتروني المستخدمة في المؤسسات المصرفية.

5- خبراء التصوير وخبراء البصمات وخبراء الرسم التخطيطي.

6- الخبير الإستشاري.

و في هذا الإطار نجد أن المشرع الجزائري قد أشار إلى إمكانية إستعانة الجهات المكلفة بالتحقيق بالخبراء المختصين في مجال الحاسوب والنظم المعلوماتية ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات

المعلوماتية وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك[1].

ثانيا- العناصر الأساسية للتحقيق في مجال المعلوماتية

ونقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي[2].

1/ الإجراءات التي يجب مراعاتها قبل البدء في التحقيق:

- تحيد نوع نظام المعالجة الأولية للمعطيات فهل هو كومبيوتر معزول ام متصل بشبكة معلومات.

-وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.

- إذا وقعت الجريمة على شبكة فانه يجب حصر طرفيات الاتصال بها او منها لمعرفة الطريقة التي تمت بها عملية الاحتراق من عدمه.

- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.

-مراعاة أن الجاني فد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار الجريمة.

---

[1]- المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في: 5 أوت 2009، ج، ر، ج، ج، عدد:47، الصادرة بتاريخ:2009/08/16

[2]- مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها، مجلة كلية الحقوق والإدارة العامة، جامعة بيزيت، رام الله فلسطين، المجلد: 45، العدد: 4، 2018، ص. 286.

– فصل خطوط الهاتف حتى لا يسئ الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم فد يسيئون استخدامها لطمس البيانات.

–التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك انه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتقليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.

– إبعاد الموظفين عن أجهزة الحاسوب الآلي بعد الحصول منهم على كلمة السر وكذا الثغرات في حالة وجودها.

– تصوير الأجهزة المستهدفة من أمام والخلف لإثبات بأنها كانت تعمل.

2/الإجراءات التي يجب مراعاتها أثناء التحقيق:

– عمل نسخة احتياطية من الأقراص الصلبة قبل استخدامها والتأكد فنيا من دقة النسخ.

– نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

– العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

– حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.

– العمل على فحص وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلومات.

– أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص وتحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة المعلومات والملفات الممسوحة، وكذلك معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب[1].

و يجب أن تتوافر بعض الأمور للمحقق ليقوم بعمله على أحسن وجه:

– معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب الانترنت والي تتعلق بالجريمة المرتكبة.

– وصول البلاغات عن الجرائم الواقعة على الحاسوب والانترنت من الفنيين الذين يعملون على هذه الأجهزة.

– تشكيل فرق تحقيق فني وإعطاء كل واحد منهم مهمة معينة من خلال عملية التفتيش على مسرح الجريمة.

– إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الالكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك ومنع حذفها.

– البحث عن الأدوات المستخدمة في ارتكاب الجريمة وطرق الدخول على البرامج المخزنة وكيفية الحـصول على الأرقام السرية والشفرات الفنية التي تمكنهم من الدخول إلى الحاسوب.

– وضع خطة عمل مع جميع أعضاء فريق التحقيق والتشاور معهم لمعرفة جميع الجوانب الفنية للجريمة التي يجري التحقيق بشأنها.

المبحث الثاني: الأجهزة المكلفة بالبحث والتحري في الجرائم الإلكترونية

[1]– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة لنيل شهادة الماجستير، علوم جنائية، كلية الحقوق والعلوم السياسية الحاج لخضر، جامعة باتنة، الجزائر، 2012– 2013، ص، ص. 112، 114.

لا شك أن التطور التكنولوجي والتقنيات الحديثة قد أثرت بشكل كبير على جميع مجالات الاقتصادية والاجتماعية والقانونية، حيث هيمنت الانترنت ووسائل الاتصال الحديثة على حياة الفرد، إلى درجة أصبح لا يستطيع الاستغناء عنها لكنها في المقابل أدت إلى استفحال نوع جديد من الجرائم هي الجرائم الإلكترونية، التي أصبحت تشكل تهديدا حقيقيا على أمن الدولة وأمن الفرد على السواء، لذلك كان لزاما على الدول أن تتخذ خطوات جدية لمواجهة هذه الجرائم وتحقيق الأمن المعلوماتي، سواء فيما بينها في إطار اتفاقيات أو داخلها بواسطة تشريعات وطنية وهيئات، أما في الجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إضافة إلى وحدات قضائية تابعة لسلك الأمن والدرك الوطني.

لذلك سوف نتطرق في المبحث الثاني إلى الأجهزة المكلفة بالبحث والتحري في الجرائم الإلكترونية حيث يتضمن المطلب الأول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والمطلب الثاني الوحدات التابعة لسلك الأمن الوطني والدرك الوطني.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

اهتمت الجزائر كغيرها من الدول بجانب الجرائم الالكترونية بشكل عام، حيث أخضعت قانوني العقوبات وقانون الإجراءات الجزائية للعديد من التعديلات، كما أصدرت بشكل خاص سنة 2009 القانون رقم 09-04 مؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]. وقد أنشأ هيئة خاصة للوقاية من هذه الجرائم ومكافحتها وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب المادة 13 منه: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، والتي تتمتع بتنظيم متميز باعتبارها تنتمي إلى فئة السلطات

[1] القانون رقم: 09-04 مؤرخ في:2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج، ر، ج، ج، عدد: 47 مؤرخة في:2009/08/16 .

الإدارية المستقلة وبمهام خاصة، وأحال بخصوص تشكيلتها، تنظيمها وكيفيات سيرها إلى التنظيم وقد صدر تباعا لذلك المرسوم الرئاسي رقم: 15-261[1].

لكن الأمر تغير سنة 2019، حيث تراجع المشرع من تكييف هذه الهيئة وحولها إلى مِؤسسة عمومية ذات طابع إداري تحت وصاية وزارة الدفاع الوطني بموجب المرسوم الرئاسي رقم: 19-172 مؤرخ في: 2019/06/06[2].

الفرع الأول: مفهوم وتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

للإحاطة بمفهوم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، لا بد علينا أن نتطرق لتعريفها لننتقل بعدها للبحث في تشكيلتها.

أولا- تعريف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تعتبر "الهيئة " كما يصطلح عليها في صلب نصوص المرسوم الرئاسي حسب أحكام المواد من 01 إلى 04 منه بأنها: "سلطة إدارية مستقلة، تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل، يقع مقرها بالجزائر العاصمة، تتولى الهيئة المهام المنصوص عليها في المادة 14 من القانون 09-04 وذلك تحت رقابة السلطة القضائية طبقا لأحكام قانون الإجراءات الجزائية[3].

ثانيا- تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

في ظل المرسوم الرئاسي رقم 15-261 كانت الهيئة تضم مجموعة من الهياكل تتمثل في:

---

[1] المرسوم الرئاسي رقم: 15-251 مؤرخ في: 2015/10/08 يحدد كيفية تشكيل وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج، ر، ج، ج، عدد: 35 الصادرة في:2015/10/08.

[2] المرسوم الرئاسي رقم: 19-172 مؤرخ في:2019/06/06 يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتنظيمها وسيرها، ج، ر، ج، ج، عدد: 37 الصادرة في:2019/06/09.

[3] المادة 14 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المصدر السابق.

لجنة مديرةَ، مديرية عامة، مديرية للمراقبة الوقائية واليقضة الإلكترونية، مديرية للتنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية[1].

-**اللجنة المديرة**:تتشكل من الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء، ويعين ممثل رئاسة الجمهورية ووزارة الدفاع الوطني بموجب مرسوم رئاسي يرأسها الوزير المكلف بالعدل[2].

-**المديرية العامة:** نص المرسوم الرئاسي على رئاسة المديرية العامة من قبل مدير عام يعين بموجب مرسوم رئاسي، من دون ضبط وتجديد تشكيلتها.

أما باقي الهياكل، فلم يحدد المرسوم الرئاسي رقم 15-261 تشكيلتها ولا تنظيمها محيلا الأمر لصدور قرار مشترك بين الوزراء المكلفين بالعدل والدفاع الوطني والداخلية.

أما بعد صدور المرسوم الرئاسي رقم 19-172 فقد أصبحت الهيئة مكونة من جهازين هما: مجلس التوجيه ومديرية عامة لنص المادة 04 من هذا المرسوم.

-**مجلس التوجيه:** حددت المادة 5 من المرسوم الرئاسي رقم 19-172 تشكيلة مجلس التوجيه من ممثلي الوزارات الآتية: وزارة الدفاع الوطني، الوزارة المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالمواصلات السلكية واللاسلكية، برئاسة وزير الدفاع الوطني أو ممثله.

المديرية العامة: اكتفى المرسوم الرئاسي بوضعها تحت إدارة مدير عام وتضم مديرية تقنية، مديرية للإدارة والوسائل، مجموعة من المصالح، من دون تحديد تشكيلتها بدقة.

الملاحظ أن المرسوم الرئاسي الجديد قد لجأ إلى التقليص من الهياكل الرئيسية المكونة للهيئة على خلاف سابقه، وعوضها بهياكل جديدة فرعية تعمل تحت سلطة المديرية العامة وتتمثل في: مديرية تقنية، مديرية للإدارة والوسائل، مصالح، من دون تحديد تشكيلتها، التي ترجع من دون شك للمدير العام بتفويض من وزير الدفاع بالنظر للمهام التي تقوم بها.

[1] طبقا للمادة 06 من المرسوم 15-261، المصدر السابق

[2] طبقا للمادة 07 من المرسوم 15-261، المصدر السابق.

النتيجة التي نخلص إليها أن المرسوم الرئاسي الجديد اتجه إلى تركيز هياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال إحلال نظام تدرج لصالح المديرية العامة بعد أن كان لصالح اللجنة المديرة في ظل المرسوم السابق.

الفرع الثاني: مهام وسير عمل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تقوم الهيئة بعدة مهام تدخل ضمن نطاق عملها، ويمكن إيجازها فيما يلي:

أولا- مهامها.

بتاريخ 05 أوت 2009 صدر القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ونص في المادة 13 منه "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، تحدد تشكيلة الهيئة وتنظيمها و كيفيات سيرها عن طريق التنظيم"، وفي ذات القانون نصت المادة 14 منه على: "الهيئة المذكورة في المادة 13 منه أعلاه خصوصا المهام الآتية:

أ-تنشيط وتنسيق عمليات الوقاية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

ب-مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

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

إلا أن المرسوم الرئاسي 15-261 الخاص بإنشاء الهيئة لم يرى النور حتى تاريخ 08 أكتوبر سنة 2015 أي بعد أكثر من 06 سنوات من تاريخ الإشارة إلى هذا الكيان القانوني ذو الأهمية البالغة فهو بذلك تماطل في تطبيق نص المادة 13 من القانون رقم 09-04 المشار أعلاه.

ونصت المادة 04 من المرسوم 15-261 على أنه: تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05

غشت سنة 2009، تحت رقابة السلطة القضائية، طبقا لأحكام التشريع الساري المفعول لا سيما منها قانون الإجراءات الجزائية والقانون رقم 09-04 المذكور أعلاه.

تكلف الهيئة في ظل احترام الأحكام التشريعية المبينة أعلاه على الخصوص بما يأتي:

– اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– تنشيط وتنسيق عمليات الوقاية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئة وطنية أخرى.

– تجميع وتسجيل المعطيات الرقمية وتحديد مصدرها 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.

– تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

– المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

صحيح أن مضمون المادة 04 من المرسوم الرئاسي 15-261 يتطابق وأحكام المادة 14 من القانون 09-04 من حيث المهام الموكلة للهيئة[1].

ثانيا- سير عمل الهيئة:

أضاف المرسوم الرئاسي 15-261 تنظيم المواد من 21 إلى 30 كيفيات سير الهيئة وأهم ما جاء في هذه المواد:

-إضافة صلاحية مهمة للهيئة حيث تكلف حصريا بمراقبة الاتصالات الإلكترونية وتسجيل وتجميع مستواها في الحين، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية،

-إمكانية طلب أي وثيقة أو معلومة ضرورية لإنجاز مهامها من أي جهاز أو مؤسسة أو مصلحة.

-إمكانية طلب المساعدة من الوزارات المعنية للأعوان العموميين المختصين في مجال تكنولوجيات الإعلام والاتصال.

- وجوب المحافظة على السر المهني.

- استعمال الوسائل والتجهيزات الالكترونية أو استيراد أو اقتناء أو حيازة لا يكون إلا من طرف الهيئة في حدود اختصاصها، أو عند الاقتضاء سلطة ضبط الاتصالات السلكية واللاسلكية، والمؤسسة العمومية المكلفة بشبكات الاتصالات.

- تفتيش أي مكان أو هيكل أو جهاز بلغ إلى علم الجهات المختصة بأنه يجوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات[2]

المطلب الثاني: الوحدات التابعة لسلك الأمن الوطني والدرك الوطني

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم الإلكترونية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين من مخبرين

[1] ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيات المعلوماتية بين النصوص التشريعية والخصوصية التقنية، د ط ، دار النشر الجزائر، ص ص 79-80-81.

[2] المواد من 21 إلى 30 من المرسوم 15-261 المؤرخ في 24 ذي الحجة 1436هـ/لموافق ل8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام[1].

الفرع الأول: الوحدات التابعة لسلك الأمن الوطني

توجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية

وهي كالتالي:

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية بقسنطينة.
- المخبر الجهوي للشرطة العلمية بوهران.

في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوي ولايات الوسط، الشرق، الغرب والجنوب، لتقوم فيما بعد بتعميم الخلايا على جميع مصالح أمن ولايات الوطن[2].

الفرع الثاني:الوحدات التابعة لسلك الدرك الوطني

أهم الوحدات التابعة للدرك الوطني والمكلفة بالبحث والتحقيق في الجرائم المعلوماتية على المستوى المركزي نجد المعهد الوطني للأدلة الجنائية وعلم الإجرام والكائن مقره في بوشاوي، وهو مؤسسة وطنية ذات طابع إداري تم إنشاؤه بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 جوان 2004، الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى أنواع الجرائم بما فيها الجريمة المعلوماتية[3]، حيث يوجد بهذا

---

[1] محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري و الإتفاقيات الدولية، **مجلة إيليزا للبحوث والدراسات**، المركز الجامعي إيليزي، الجزائر، العدد الثاني، ديسمبر2017، ص. 34.

[2]مجذوب نوال، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية_الجزء 01، المركز الديمقراطي العربي –برلين –ألمانيا د س ن ، ص 24.

[3] عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث العلمي، د، ط، الكتب والوثائق المصرية، مصر_ 2006، ص 46.

المركز قسم الإعلام الآلي والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية. كما توجد أجهزة أخرى على مستوى الدرك الوطني نذكر منها:

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.
- مديرية الأمن العمومي والاستغلال.
- المصلحة المركزية للتحريات الجنائية.

إضافة إلى كل فصائل الأبحاث التابعة للدرك الوطني والمكلفة بالتحقيق في الجرائم المعلوماتية[1].

[1] علي حسن الطوالبة– جامعة العلوم التطبيقية مملكة البحرين، الجرائم الالكترونية، ص 60.

الفصل الثاني:

آليات التحقيق في الجرائم الالكترونية

الفصل الثاني: آليات التحقيق في الجرائم الالكترونية

إذا كانت ظاهرة الإجرام الالكتروني قد أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوص التقليدية على هذا النوع من الجرائم واحترام مبدأ الشرعية والتفسير الضيق للنصوص الجزائية فقد أثارت في الوقت نفسه مشكلات أكثر في نطاق القانون الجزائي الإجرائي، 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 وتمويه أثارها وإخفاء الأدلة المتحصل منها بسهولة عقب تنفيذها باستعمال تقنيات تكنولوجيا عالية ولقد امتد تأثير التقنية المعلوماتية إلى الجانب الإجرائي من القانون الجزائي بشكل أوسع مع مرور الوقت لان نصوص هذا القانون صيغت ووضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية ترتكب في عالم محسوس وملموس يؤدي فيه السلوك المادي الدور الأكبر والاهم على خلاف الجريمة الالكترونية التي ترتكب في مسرح الكتروني افتراضي وغير مادي يختلف كليا عن المسرح التقليدي.

وعلى إثر ذلك تم تقسيم هذا الفصل إلى مبحثين في المبحث الأول نتطرق فيه للإجراءات التحقيق في الحصول على الدليل الالكتروني والمبحث الثاني القيمة القانونية للدليل الالكتروني.

المبحث الأول: إجراءات التحقيق في الحصول على الدليل الالكتروني

لم يكن لدى الدول خيار آخر للتصدي لظاهرة الإجرام الالكتروني في بداية ظهورها إلا الاعتماد على النصوص الجزائية القائمة بمختلف فروعها الموضوعية والإجرائية وذلك تفاديا لإفلات الجناة من العقاب من جهة وعدم وجود قواعد قانونية أخرى تتلائم وطبيعة هذه الجرائم المستحدثة من جهة أخرى.

ولكن بعد التطور السريع الحاصل في مجال المعلوماتية وما صاحبه من انعكاسات على الجرائم في الوسائل المستعملة لارتكابها والمحل الذي تقع عليه ونوع الجناة الذين يرتكبونها جعل هذه القوانين غير مواكبة لها، وعليه فإن هذا النوع من الجرائم تستوجب تحديث القوانين والتعليمات وكذلك خلق جهات أمنية متخصصة للتحقيق فيها.

ومن خلال هذا البحث سنتناول القواعد الإجرائية التقليدية في الحصول على الدليل الالكتروني في المطلب الأول من خلال التفتيش وضبط الأدلة والمعاينة والخبرة والقواعد الإجرائية الحديثة في الحصول على الدليل الالكتروني في المطلب الثاني من خلال التطرق إلى التسرب الالكتروني و إعتراض المراسلات والمراقبة الالكترونية.

المطلب الأول: القواعد الإجرائية التقليدية في الحصول على الدليل الالكتروني:

إن القوانين التقليدية التي كانت تنظم إجراء التحقيق كالتفتيش والمعاينة لا يمكن تطبيقها على الجريمة الالكترونية كونها جريمة ذات طبيعة خاصة لأنها تتعلق بالبيانات والمعلومات غير الملموسة مما يصعب تحديد هوية وأمكنة المجرمين وملاحقتهم وهذا ما يرهق المحققين الذين يصعب عليهم جمع الأدلة من خلال البنية الالكترونية ذات الطبيعة المعقدة والغامضة.

وفي هذا المطلب سنتطرف إلى أهم القواعد الإجرائية التقليدية والتي تتمثل في التفتيش وضبط الأدلة والمعاينة والخبرة.

الفرع الأول:التفتيش وضبط الأدلة في الجرائم المعلوماتية.

يعتبر التفتيش وضبط الأدلة أهم إجراءين قد يتخذهما المحقق في الجرائم الالكترونية، لذلك سنتناول كليهما كما يلي:

أولا–التفتيش:

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق يهدف إلى البحث عن الأدلة لإثبات وقوع جريمة ما في مكان معين، حيث أنه ونظرا لخطورته تشترط أغلب التشريعات الحصول على رخصة للتفتيش من الجهة القضائية المختصة وهذا ما سنتطرق إليه.

أ/ تعريف التفتيش:

لا يوجد تعريف قانوني للتفتيش لذا سيتم اللجوء إلى التعريف الفقهي والتي تصب كلها في فلك واحد هو اعتبار أن التفتيش " إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا للإجراءات القانونية المقررة ".[1]

ويعرف تفتيش نظام الحاسوب و الأنترنت أيضا بأنه: " البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبها إليه ".[2]

ثانيا/كيفية التفتيش الإلكتروني:

تتكون نظم الحاسوب من مكونات مادية وأخرى معنوية كما أنه تربطه بغيره من الحواسيب شبكات إتصال بعدية.

[1]– هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلومات (دراسة مقارنة)، ط1، دار النهضة العربية، مصر، 1997، ص. 47.

[2]–علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديثة، ط1 ، 2004.

تفتيش المكونات المادية للحاسب الآلي:

إن الولوج إلى مكونات المادية للحاسوب الآلي من أجل البحث عن أدلة مادية التي تكشف عن حقيقة الجريمة الإلكترونية ومرتكبيها تخضع لإجراءات التفتيش المألوفة لأن حكم التفتيش في هذه الكيانات المادية يتوقف أساسا على طبيعة المكان الموجود فيه فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له علمه بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن وملحقاتها، مع الأخذ بإعتبار إذا كانت مكونات الكمبيوتر المراد تفتيشه منعزلة عن أجهزة الكمبيوتر أم أنها تتصل بأجهزة كمبيوتر آخر في مكان آخر.[1]

التفتيش في المكونات المعنوية (المنطقية) للحاسوب ومدى صلاحيتها:

تعرف على أنها مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة المعالجة البيانات بحيث ثار جدل تشريعي وفقهي حول شأن مدى جواز تفتيش المكونات المعنوية أو المنطقية للحاسب تمهيدا لضبط الأدلة الإلكترونية.[2]

التفتيش في شبكات الحاسوب(التفتيش عن بعد):

إن الشبكة المعلوماتية يقصد بها اتصال جهازين أو أكثر من أجهزة الحاسب الآلي اتصالا سلكيا أو لاسلكيا وتكون هذه الأجهزة مرتبطة ببعضها البعض في موقع واحد فيطلق عليها بالشبكة المحلية أو إذا كانت موزعة على عدة أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف فيطلق عليها بالشبكة الانترنت، [3] وهنا يكون الموقع الفعلي للبيانات داخل اختصاص

---

[1]– براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة دكتوراه في القانون، كلية الحقوق، جامعة تيزي وزو ,2018، ص16.

[2]–احمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، أطروحة لنيل الدكتوراه في القانون، كلية حقوق جامعة عين الشمس، د س ن، ص 374.

[3]–براهيمي جمال، المرجع السابق، ص 21.

قضائي آخر وفي بلد آخر مما تثار مشكلة الاختصاص القضائي، واثر تفتيش الأنظمة المتصلة بالنظام المأذون تفتيش إذا وجدت في دوائر اختصاص مختلفة مما تتصور هنا حالتين مختلفين هما:

الحالة الأولى:اتصال حاسب المتهم بحاسب آلي آخر أو منظومة معلوماتية متواجدة في موقع آخر داخل إقليم الدولة نفسها.

إن هذه الفرضية تتحقق عندما يقوم المتهم بتحويل عبر الانترنت معلومات أو بيانات متعلقة بجريمة الكترونية من حاسوبه إلى حاسوب آخر أوإلي منظومة معلوماتية ملك للغير وتخزينه فيها وفي هذه الحالة تقع على سلطات التحقيق تجاوز الاختصاص المكاني والاعتداء على حرمة خصوصية غيره لهذا السبب عمدت لبعض التشريعات الإجرائية إلي تنظيم هذه المشكلة لنص صريح حول إمكانية امتداد التفتيش ليشمل أجهزة الحاسوب أو أية منظومة معلوماتية مرتبطة بحاسوب المتهم الجاري تفتيشه من اجل إثبات الجريمة دون التقيد بالحصول على إذن مسبق من السلطات القضائية المختصة بخصوص هذا الامتداد.[1]

الحالة الثانية: اتصال حاسب المتهم بحاسب آخر أو منظومة معلوماتية متواجدة في إقليم دولة أجنبية، من بين المشاكل التي تواجهها سلطات التحقيق في جمع الأدلة الالكترونية عند قيام مرتكبي الجريمة بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمي في تلك شبكة الاتصال البعدية يهدف عرقلة التحقيق وسير العدالة ونتيجة لذلك فان امتداد التفتيش على الأنظمة حتى ولو كانت متواجدة خارج الإقليم القانون الفرنسي يجيز هذا الفعل من خلال المادة 1/57 من القانون الإجراءات الجزائية لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المعلوماتية المتصلة المتواجدة خارج الإقليم الوطني.[2]

---

[1]– طرشي نورة، مكافحة الجريمة المعلوماتية، رسالة لنيل شهادة الماجستير في قانون، فرع قانون الجنائي، كلية الحقوق جامعة الجزائر1، 2011، ص. 110.

[2]– عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة ' رسالة لنيل شهادة الماجستير في الحقوق، كلية الحقوق جامعة إسكندرية، 2009، ص59.

ثالثا- شروط التفتيش الإلكتروني

يعتبر التفتيش من الإجراءات التي تمس بالحرية الشخصية للأفراد وبحرمة حياتهم الخاصة ونجد معظم التشريعات تقيده بشروط وتنقسم هذه الشروط إلى:

1- الشروط الموضوعية للتفتيش: ويقصد بها تلك الضوابط التي لابد من توفرها ليكون تفتيش صحيح ونلخص هذه الشروط في السبب والسلطة المختصة بالتفتيش ومحل لتفتيش

أ- سبب التفتيش: إن السبب الأساسي للتفتيش هو الحصول على دليل مادي يفيد جهات التحقيق من أجل الحصول على الحقيقة وهو ما ينطبق على الجريمة الإلكترونية إلا بتوفر العناصر التالية:

- وقوع جريمة معلوماتية تحمل وصف الجناية أو جنحة.

- لابد من توافر أدلة قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم بالجريمة الإلكترونية أو غيرها.

ب- محل التفتيش: وهي تخص نظم الحاسوب بكل مكوناته المادية والمعنوية بالإضافة إلى شبكات الاتصال الخاصة به والأشخاص الذين يستعملون الحاسوب محل التفتيش.

ج- السلطة المختصة بالتفتيش: لكي يكون التفتيش في الجرائم الإلكترونية صحيح لابد أن يتم من طرف سلطات التحقيق الأصلية وهذا مع مراعاة الإختصاص المحلي للجريمة و كإستثناء يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية وفق الشروط المنصوص عليها في القانون.[1]

د- تحرير محضر التفتيش: يشترط أن يحرر محضر التفتيش الذي يدون فيه كل الخطوات والإجراءات المتخذة أثناء عملية التفتيش، بحيث محضر التفتيش لا يتقيد بشكل وشروط خاصة بل يكتفي بالكتابة باللغة الرسمية تاريخ تحريره، توقيع محررة والشروط الأساسي الذي يجب

[1]-براهيمي جمال، المرجع السابق، ص 39

التقيد به هو الاستعانة بكاتب يتم اصطحابه لتحرير المحضر وتدوين مجريات التفتيش وهذا حسب نص المادة 02/68 من قانون الإجراءات الجزائية الجزائري.[1]

***الشروط الشكلية للتفتيش الالكتروني:** يجب احترامها من اجل ضمان صحة إجراءات التفتيش وهي ثلاثة شروط:

ا-وقت إجراء التفتيش: لابد من تحديد الميعاد الزمني أو الفترة الزمنية التي يتم فيها التفتيش ذلك صونا لحرية الأفراد وحرمة مسكنهم والمشرع الجزائري حدد وقت التفتيش بين الخامسة صباحا والثامنة ليلا حسب المادة 07 من قانون الإجراءات الجزائية.[2]

وهنا نشير إلي أن المشرع الجزائري قد اشتمل على هذا الاستثناء في الجرائم الالكترونية حيث أجازت المادة 47 فقرة 2 إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني وبأي ساعة من ساعات النهار أو الليل فيما يخص جرائم الاعتداء على نظم المعالجة الآلية للمعطيات بشرط إذن مسبق من وكيل الجمهورية المختص ويعتبر هذا خروجا عن القاعدة المنصوص عليها في المادة 47 ق اج التي تحدد مواقيت عملية التفتيش من الساعة الخامسة صباحا إلي الثامنة ليلا.

ب- إجراء التفتيش يكون بحضور المتهم أو من ينوب عنه:

لا يكون التفتيش إلا بحضور المتهم أو من يقوم مقامه أو من ينوب عنه كونه شرط ضروري بفرضه القانون لصحة إجراء التفتيش أو شاهدين من غير المعنيين بالتحقيق.[3] بينما المشرع الجزائري يقضي لإجراء التفتيش بحضور المشتبه به أو من يمثله ولم يشترط حضور الشهود إلا في حالة تعذر حضور هؤلاء حسب المادة 01/45 من قانون الإجراءات الجزائية.

[1]-بن يحي اسماعيل، التحقيق الجنائي في الجرائم الالكترونية، اطروحة لنيل شهادة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد تلمسان، 2021، ص207.

[2]-بن يحي اسماعيل، المرجع السابق، ص209.

[3] -براهيمي جمال، المرجع نفسه ص 43

ويلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون 06-22 من المادة 45 منه [1]، حيث إستغنى المشرع عن ضمانة حضور الأشخاص المحددين في الفقرة الأولى من هذه المادة في جرائم معينة منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني خاصة وأن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه حتى عن بعد، كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي بدأت تأخذ بإجراء التفتيش عن بعد.[2] أو ما يطلق عليها في الفقه الفرنسي مصطلح التفتيش على المباشر perquisition "[3]en ligne"

ثانيا: ضبط دليل الإلكتروني

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

1-تعريف ضبط الأدلة الالكترونية:

[1] -القانون رقم 06-22 يعدل ويتمم الأمر رقم 66-155 المتعلق بقانون الإجراءات الجزائية الجزائري، الجريدة الرسمية رقم 84 المؤرخة في 2006/12/24.

[2]- يقصد بالتفتيش عن بعد قيام مأمور الضبط القضائي بالتفتيش وهو جالس في مكتبه باستخدام برامج خاصة تحمل في طابقها قاعدة التفتيش عن الجريمة وبثير هذا الإجراء العديد من المشكلات القانونية أبرزها التعدي على الخصوصية – التعدي على سيادة دولة أخرى ذلك لأنه يعد من قبيل التجسس وانتهاك حواسيب وخوادم لهذه الدولة خاصة إذا كانت من الدول التي لا تعترف بمشروعية هذه البرمجيات.

[3] - yann padova un aperçu de lutte contre la cybercriminalité science criminelle et droit penale n 4 dalloz 2002 p 770.

وهو وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو من إجراءات التحقيق[1].

وإذا كان الضبط هو الأثر المباشر للتفتيش فليس الصعوبة في ضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر كالبصمات مثلا وإنما تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل 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.

ولقد حسمت الاتفاقية الأوروبية لجرائم المعلوماتية لعام 2001 هذه المسالة بإقرارها صراحة صلاحية المكونات المنطقية والوسائل الالكترونية لان تكون محلا للضبط وذلك من خلال الفقرة 3 من المادة 19 التي نصت على ".... يجب على كل طرف تبنى الإجراءات التشريعية التي يراها ضرورية من أجل تخويل هيئاتها المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين 01 و02....".

تبنى المشرع الجزائري من خلال القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05 إجراءات مستحدثة خاصة بضبط وتحريز المعطيات والبيانات المعلوماتية وغيرها من الأدلة الرقمية بما يتناسب وطبيعتها اللامادية تحت عنوان " حجز المعطيات المعلوماتية من خلال المادة 06 و07 و08 من القانون السالف الذكر.

الفرع الثاني: المعاينة

[1]-عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية (دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، ط1، دار النهضة العربية، مصر، 2009، ص 669.

حتى تتمكن سلطات التحقيق من استخلاص الدليل الإلكتروني عن طريق الآثار التي أحدثها المجرم بمسرح الجريمة على هذه الأخيرة التنقل وبسرعة من أجل معاينة مسرح الجريمة وجمع الاستدلالات والآثار وهذا ما سنتطرق إليه من خلال هذا الفرع.

أولا: تعريف المعاينة:

هي أول إجراء من إجراءات البحث والتحري فهو الإجراء الأكثر أهمية لأنه يسمح بالمعاينة المادية للوقائع المشكلة للجريمة، والإنطلاق بشكل سريع ومباشر في عملية البحث وضبط الأدلة التي تساعد على معرفة وقت وكيفية إرتكاب الجريمة وهوية فاعلها وعادة ما تستند هذه المهمة لأفراد الشرطة العلمية والتقنية نظرا لضرورة التدخل بسرعة وبطريقة مدروسة تتلائم وطبيعة الجريمة محل المعاينة من خلال القيام بسلسلة من العمليات التي تستلزم خبرة ميدانية ووسائل من نوع خاص.[1]

وتتم المعاينة في الجرائم الالكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الالكترونية المرتكبة واذا كانت الجريمة واقعة على المكونات المادية للأجهزة الالكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص الممغنطة فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعد أدلة مادية تدل على وقوع الجريمة وانتسابها لشخص معين ثم ضبطها ووضعها في أحراز مختومة تقدم للنيابة العامة.

أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الالكترونية أو بواسطتها كتلك الواقعة على برامج الحاسب وبياناته بواسطة الانترنت فيكون الانتقال للمعاينة هنا افتراضيا أو الكترونيا، ويمكن للمحقق إجراء المعاينة الافتراضية أو الالكترونية بالولوج والانتقال إلى

[1] –charle diaz- la police techenique et scientifique 2 eme édition -édition presse universitaire défonce france 2006-p54

مسرح الجريمة عبر الانترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه أو من خلال مقهى الانترنت أو إحدى مقرات مزود خدمات الانترنت.[1]

ثانيا: إجراءات المعاينة بمسرح الجريمة الإلكترونية:

تتبع سلطات التحقيق لمعاينة مسرح الجريمة الإلكترونية الخطوات الآتية:

-1 إبعاد الأشخاص الغير مرخص لهم بالتواجد في مسرح الجريمة والمساس بأي من الأجهزة الإلكترونية.

-2 التريث في نقل أي مادة معلوماتية إلى حين التأكد من عدم وجود أي عامل قد يؤدي إلى إتلافها كالمجالات المغناطسية مثلا.

-3 القيام بتصوير شاشة الحاسوب.[2]

الفرع الثالث: الخبرة

وبما أن الجريمة الالكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة وإخطاره مسبقا حتى يستعد من الناحية التقنية والعملية ويعد خطة مناسبة للمعاينة وأكيد قبل كل شئ يجب مراعاة ما جاء في القوانين الجنائية حول المعاينة ذلك تحقيقا لمبدأ الشرعية، وهذا ما سنتطرق إليه من خلال هذا الفرع.

اولا: تعريف الخبرة

[1]-براهيمي جمال، المرجع السابق، ص. 58.

[2] نبيلة هبة هروال، الجوانب الإجرائية للجريمة المعلوماتية دار الفكر الجامعي، الإسكندرية 2007 ، ص ص 219-220

فالخبرة هي " إجراء يهدف الاستعانة بالقدرات الفنية أو العلمية لشخص الخبير والتي لا تتوفر لدى رجال القضاء والمحققين لاستخلاص دليل يفيد في معرفة الحقيقة بشأن جريمة وقعت أو نسبتها إلى المتهم أو تسمح بتحديد ملامح شخصيته الإجرامية".[1]

إن الواقع العملي وحاجة سلطات التحقيق إلى الخبراء الفنيين خاصة في مجال مكافحة الجريمة الالكترونية ونظرا لخصوصيتها وطبيعتها الغير المادية والبيئة الافتراضية التي بداخلها ارتكاب الجريمة يفرض على التحقيق الاستعانة وندب خبراء في مجال المعلوماتية والتقنيات الحديثة للوصول إلى الحقيقة.[2]

ثانيا: إجراءات الخبرة في مجال الجريمة الالكترونية:

إن ابرز الخطوات والمراحل التي تمر بها إجراءات الخبرة تتمثل فيما يلي:

– مرحلة ما قبل التشغيل والفحص يتم من خلالها إحصاء وجود المكونات التي ثم ضبطها.

– مرحلة التشغيل والفحص يتم من خلالها نسخ البيانات الموجودة وإظهار التي تم إخفائها واسترجاع ما تم محوه.

– مرحلة تحديد الارتباط بين الدليل المادي والدليل الالكتروني.

–مرحلة تدوين النتائج التي تم التوصل إليها الخبير لإعداد تقرير الخبرة بخصوص المهام التي اسندت اليه عند تسخيره وتكليفه بالمهمة[3].

[1]– أحمد شوقي الشلقاني، مبادىء الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999، ص. 259.

[2]–بن يحي اسماعيل، مرجع سابق، ص 216

[3]– بن يحي اسماعيل، المرجع السابق، ص16

المطلب الثاني: القواعد الإجرائية الحديثة في الحصول على الدليل الإلكتروني

إن الجرائم الإلكترونية التحقيق فيها يختلف عن الجرائم الأخرى فجمع الأدلة وفك ألغاز الجريمة والوصول إلى مخطط العملية يوجب على المحقق الإلمام الواسع بأجهزة الإعلام الآلي، وطبيعة عملها ومعرفة بيئتها الحقيقية وكذا شبكة الأنترنت وكيفية التفتيش فيها وضبط الأدلة التي تبقى غير ملموسة ويسهل محوها أو إتلافها، لهذا لابد من التطرق لأساليب البحث والتحري للوصول إلى كشف حقيقة الجرائم الإلكترونية، وعليه سوف نتطرق في هذا المطلب إلى التسرب الإلكتروني في الفرع الأول و اعتراض المراسلات والمراقبة الإلكترونية في الفرع الثاني.

الفرع الأول: التسرب الإلكتروني

يعتبر التسرب من بين أهم إجراءات التحقيق الجديدة والمستحدثة من خلال هذا الفرع سنتناول تعريف التسرب وشروطه وكيفية الإستعانة به في مجال الجرائم الإلكترونية.

أولا –تعريف التسرب الإلكتروني:

تناول المشرع الجزائري موضوع التسرب من خلال المواد 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية.

حيث عرفه في المادة 65 مكرر 12 على أنه " يقصد بالتسرب قيام الضباط 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 لهم أو خاف ويسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على إرتكاب جرائم" وهذه الجرائم هي:

– إفشاء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من إرتكاب الجرائم أو مستعملة في ارتكابها.

– إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الإيواء أو الحفظ أو الإرسال.[1]

ويلاحظ أن المشرع شدد على حماية الضابط أو العون المتسرب ونص على معاقبة كل من يكشف هويتهم خلال مراحل التحقيق بالحبس من سنتين إلى خمس سنوات وبغرامة من 50.000 د ج إلى 200.00 د ج.

حيث أن المشرع الجزائري أعفى أو ضابط الشرطة القضائية المتسرب من المسؤولية الجزائية على كل الأفعال الغير المشروعة التي يقوم بها طوال العملية بالتالي المشاركة في تشكيل الخلية الإجرامية.[2]

وكما أحاط المتسرب بعدة ضمانات لحمايته وحماية أسرته أثناء القيام بعملية التسرب حيث نصت المادة 65 مكرر 16 من قانون الإجراءات الجزائية: "....لا يجوز إظهار الهوية الحقيقية لضابط أو عون الشرطة القضائية المتسرب بل تتم تحت هوية مستعارة طيلة مراحل القيام بهذا الإجراء...."."[3]

ثانيا:شروط مباشرة عملية التسرب: بإعتبار أن عملية التسرب إجراء أو أسلوب من أساليب التحري الخاصة التي تمس بالحريات الخاصة للأفراد وخصوصيتهم، فقام المشرع الجزائري بتقييدها بجملة من الشروط نظرا للخطورة التي يشكلها هذا الإجراء على حرمة الحياة الخاصة وهي كالآتي:

1– **الشروط والضوابط الاجرائية:**فتتمثل في الإذن القضائي وكل ما يجب أن يتضمنه من شروط وأحكام فلا يمكن لضباط وأعوان الشرطة القضائية القيام بعملية التسرب من دون إذن مسبق من

[1]– زبيحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي دار الهدى عين مليلة الجزائر، سنة الطبع 2011 ص170

[2]– القانون 06 – 22 المؤرخ في 20 / 12/ 2006 المتضمن ق إ ج ج المرجع نفسه.

[3]–أنظر المادة 65 مكرر 14 من ق إ ج ج المرجع نفسه.

طرف الجهات القضائية المختصة، فيقوم بإصدار هذا الإذن السيد وكيل الجمهورية ذلك قبل إفتتاح التحقيق أو قاضي التحقيق بعد إفتتاح التحقيق على أن تتم العملية تحت الرقابة المباشرة للسلطة الصادرة للإذن لتفادي وقوع أي تجاوزات حفاظا على الحريات الفردية للأشخاص.

– كما يجب أن يكون الإذن مكتوبا وإلا كان إجراء التسرب باطلا حسب ما نصت عليه المادة 65مكرر 15 من قانون الإجراءات الجزائية "... يجب أن يكون الإذن مكتوبا تحت طائلة البطلان.[1]

– ويشترط أيضا أن يتضمن الإذن جملة من البيانات تقوم عليها صحة الإجراء كتحديد نوع الجريمة محل التسرب، اسم ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته كذلك تحديد المدة المطلوبة لهذه العملية والتي لا يجب أن تتجاوز الأربعة 04 أشهر قابلة للتجديد حسب متطلبات ومقتضيات التحقيق، حيث يجوز في أي وقت للسلطة مصدرة الإذن حسب الحالة أن توقف هذا الإذن حتى قبل انقضاء الآجال المحددة.[2]

2– **الشروط والضوابط الموضوعية:** حدد المشرع الجزائري ضوابط وشروط الموضوعية يمكن إختصارها في عنصرين هامين:

أ– **التسبيب:** تضمنته المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري يتمثل في الدوافع والمبررات والحجج التي تم التأسيس عليها طلب سلطات التحقيق للجهات القضائية لمنحها الإذن للقيام بعملية التسرب فعلى ضابط الشرطة القضائية أن يحدد الأسباب ضمن طلب الإذن.[3]

---

[1] –تنص المادة 65 مكرر 11 من ق إ ج ج على أنه: " يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة مباشرة عملية التسرب..."

[2]– المادة 65 مكرر 15 من ق إ ج ج المرجع نفسه .

[3]–علاوة هوام، التسرب كآلية للكشف عن الجرائم في القانون الجزائري، **مجلة الفقه والقانون**، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012، ص 03.

ب – تحديد نوع الجريمة محل عملية التسرب: حيث لا يجب أن تخرج عن الجرائم التي حددتها المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري على سبيل الحصر فيظهر لنا من خلال هذه المادة أن الجرائم التي خصها المشرع بإجراء عملية التسرب هي جرائم خطيرة جدا نظرا لسرعة إنتشارها و إمتداد تداعياتها خارج الحدود الوطنية فهي تقوم على التخطيط وتسخير كل الوسائل لمحو أثار الجريمة وطمس معالمها.[1]

الفرع الثاني: اعتراض المراسلات والمراقبة الإلكترونية

إن الإقدام الهائل للأفراد والمؤسسات على وسائل الاتصال الحديثة والاستخدام المفرط للشبكات المعلوماتية في الآونة الأخيرة، جعل المشرع في العديد من الدول يدرك الصعوبات الكثيرة التي تثيرها محاولة مد نطاق إجراءات الاعتراض والمراقبة وفق النصوص التقليدية لتشمل المراسلات والاتصالات عبر الشبكات المعلوماتية لذلك عمدت العديد من هذه الدول إلى مراجعة قوانينها الإجرائية لوضع نصوص صريحة تنظم هذه العملية.[2]

أولا– تعريف إعتراض المراسلات و المراقبة الإلكترونية:

عرف المشرع الجزائري عملية اعتراض المراسلات من خلال المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري كالآتي: " اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية أو اللاسلكية وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض....".

فيظهر من خلال هذا التعريف أن المشرع الجزائري حدد المراسلات التي يمكن أن تكون محلا بإعتراض وهي المراسلات التي تتم بواسطة الاتصال السلكية واللاسلكية من دون أن يحدد

[1]– زورو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، **مجلة دفاتر السياسة والقانون**، العدد11، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2014، ص 121.

[2]– براهيمي جمال، المرجع السابق، ص87.

طبيعة هذه المراسلات أي الوسائل المكتوبة بغض النظر عن شكلها أو الدعامة التي تنصب عليها أو الوسيلة المستعملة في إرسالها.

كما أن القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها عرف الإتصالات الإلكترونية في المادة الثانية الفقرة "و" بأنها " أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة بواسطة أي وسيلة إلكترونية ".

وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فإن عملية الإعتراض والمراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون علم أو موافقة المعنيين وذلك لغرض التصنت والتقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن عامة أو خاصة ومن ثم إستعمالها كدليل لمواجهة المتهم.[1]

ثانياً: المراقبة الإلكترونية:

ولقد تم تعريفها بأنها:" مراقبة شبكات الإتصالات الإلكترونية أو العمل الذي يقوم به المراقب بإستخدام التقنية الإلكترونية لجمع بيانات ومعلومات عن المشتبه فيه أو شيئا حسب طبيعته مرتبط بالزمن أي التاريخ والوقت لتحقيق غرض أمني أو لأي عرض آخر.[2]

ومن خلال الاطلاع على المادة 04 من قانون 09-04 يظهر لنا أن المشرع الجزائري أعطى تسريحا إلى سلطات التحقيق لاستعمال عملية مراقبة الاتصالات الإلكترونية كإجراء وقائي إستباقي حيث أن مجرد احتمال وقوع أو اكتشاف جريمة متصلة بتكنولوجيا الإعلام والاتصال ويحتمل أن تشكل خطرا على أمن الدولة كالأفعال الموصوفة بجرائم الإرهاب والتخريب وجرائم الاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو

[1]-زبيحة زيدان، المرجع السابق، ص157.

[2]- نبيلة هبة هروال، المرجع السابق ، ص 198.

مؤسسات الدولة، ولكن هناك مجموعة من القيود والضوابط الواجب مراعاتها أثناء تنظيم عملية اعتراض ومراقبة المراسلات نذكر منها::

- **الحصول على إذن السلطات القضائية المختصة:**

قيد المشرع هذه العملية بشرط الحصول على الإذن المسبق من الجهات القضائية، ويكون هذا الإذن مكتوبا ومسببا ويمنح هذا الإذن عادة من طرف السيد وكيل الجمهورية أثناء مرحلة التحقيق وإستثناء يمنح من طرف النائب العام بمجلس قضاء الجزائر إذا تعلق الأمر بالوقاية من أفعال إرهابية أو التخريب أو الجرائم الماسة بأمن الدولة أو قاضي التحقيق في مرحلة التحقيق القضائي.[1]

فالسلطة القضائية هي المختصة بإصدار هذا الإذن ويعتبر هذا ضمانة لازمة لمشروعية هذه العملية، وحتى يكون هذا الإذن صحيحا يجب أن يتضمن مجموعة من العناصر الأساسية تتمثل في:

-نوع الجريمة التي تبرر هذا الإجراء.

-التعريف بالعملية.

-تسبيب اللجوء إلى إجراء اعتراض أو مراقبة المراسلات الالكترونية.

-تحديد الجرائم محل الاعتراض.

- سرية الإجراء وكتمان السر المهني.

المبحث الثاني: القيمة القانونية للدليل الإلكتروني

[1]- الفقرتين6و7 من المادة 04 من القانون 09-04، مصدر سابق.

إن محور القانوني ينصب على كيفية إيصال الحق لصاحبه وحتى يكون لهذا الحق قيمة من المنطلق القانوني فلابد لصاحبه أن يثبته فالحق المجرد من أي وسيلة إثبات هو دون أي قيمة ومن هنا تبرز أهمية وسائل إثبات الحق[1].

ولقد كان موضوع إقامة الدليل منذ الأزل محل انشغال الكثيرين، حتى أمست هناك أنظمة مختلفة تنظم موضوع الإثبات وعليه فإن إثبات الحق يكون من خلال وسائل قانونية معينة كالكتابة، الشهادة،....ومن غيرها من الأدلة المتعارف عليها في ظل الثورة العلمية، وأثارها على جميع مجالات الحياة فإن هذا الأثر طال أيضا أدلة الإثبات لتفرض هذه الثورة أدلة حديثة لم تكن في الحساب وهي الأدلة الإلكترونية[2].

وبناءا على ما تقدم فإن البحث في الأدلة الإلكترونية يتطلب بلا شك تسلط الضوء على ماهية الدليل الإلكتروني وخصائصه (المطلب الأول) تعريف الدليل الإلكتروني وخصائصه (الفرع الأول)

وبعد ذلك نحاول التطرق إلى تقسيمات الدليل الالكتروني (الفرع الثاني)

المطلب الأول:ماهية الدليل الإلكتروني

من المعلوم أن الدليل الرقمي من المواضيع التي حضيت باهتمام فقهاء القانون الجنائي والمشرعين، وهذا في مجال الإثبات الجنائي على اختلاف نظمه، وهذا الاهتمام جاء نتيجة لكون الدليل الرقمي عامل مهم في إثبات الجريمة من عدمه، وهذا في حد ذاته يتطلب منا التعرف إلى مفهوم الدليل الرقمي من خلال تعريفه.

الفرع الأول: تعريف الدليل الإلكتروني وخصائصه

[1] عائشة بن قارة مصطفى، ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي–دراسة مقارنة–مذكرة لنيل شهادة الماجستير، كلية الحقوق–جامعة الإسكندرية_2009 ص 11.

[2] أحمد حمو، علاء عواد، ولاء عبد الله، بحث في الأدلة الإلكترونية من الناحية القانونية، دراسة تحليلية مقارنة – جامعة بيروت، د ط 2015 ص 22.

نتعرض في هذا المطلب إلى بيان مختلف التعاريف والدلالات المتعلقة بالدليل الرقمي، كما نتطرق أيضا على خصائصه التي تميزه عن غيره.

أولا:التعريف اللغوي للدليل الرقمي:

الدليل في اللغة هو المرشد وما يستدل به وجمعه أدلة، كما يقصد به كذلك تأكيد الحق بالبينة، والبينة هي الدليل أو الحجة أو البرهان[1].

وقد جاء في القرءان الكريم معنى الدليل بقوله تعالى:ألم تر إلى ربك كيف مد الظل ولو شاء لجعله ساكنا ثم جعلنا الشمس عليه دليلا}[2].

ثانيا:التعريف الاصطلاحي للدليل الرقمي القانوني

في ظل عدم تعريف الدليل الجنائي الرقمي من قبل المشرعين الجزائري والفرنسي، سنقدم بعض التعريفات التي أتى بها فقهاء القانون الجنائي وقد عرف البعض بأنه: الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل موجات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليله اباستخدام برامج وتطبيقات تكنولوجية خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء.[3]

كما يعرف بأنه:الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة أو هو تلك المعلومات التي يقبلها المنطق والعقل ويعتمدها العلم ويتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب ألآلي وملحقاتها وشبكات الاتصال

[1]جميل صليبا– المعجم الفلسفي المصطلحات القانونية، الجزء الأول، ، دار الكتاب اللبناني، بيروت، ط1، 1982–، ص 564.

[2]الآية 45 من سورة الفرقان.

[3]ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006، ص 88.

ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة ما أو المجني عليه[1].

الدليل الرقمي هو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل الرموز والنصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم يعبر عن فكر وقول يطلق عليه الكتابة الرقمية بالمعنى الواسع، التي لا تشمل الكتابة التقليدية على الورق فحسب، وإنما تشمل أيضا الكتابة التي تتم عن طريق وسائل الاتصال الحديثة (شبكة المعلومات الدولية وما في حكمها)مهما كانت الدعامة المستخدمة في تثبيتها.[2]

وهناك من يعرف الدليل الرقمي على أنه جميع المعلومات والبيانات الرقمية التي تقوم بإثبات أن هناك جريمة قد ارتكبت، أو وجود علاقة بين الجريمة أو الجاني أو بن الجريمة والمتضرر منها، والبيانات الرقمية هي عبارة عن مجموعة من معلومات أو بيانات ذات قيمة في التحقيق، والتي جرى إرسالها أو تخزينها عبر جهاز إلكتروني[3].

وعليه يمكننا القول بأن الدليل الرقمي هو:"الدليل المستخلص من أجهزة الحاسب الآلي وملحقاته أو من شبكة الانترنت أو أي جهاز آخر له خاصية معالجة أو تخزين المعلومة، وهو عبارة عن نبضات مغناطيسية أو كهرومغناطيسية يمكن جمعها وتحليلها باستخدام برامج وتطبيقات خاصة، لتشكل لنا بيانات مختلفة يمكن اعتمادها في مرحلة التحقيق أو المحاكمة[4].

---

[1] عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية، جامعة د مولاي الطاهر_سعيدة-، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو/الأغواط، العدد السادس(06) مارس 2021، ص 152-153.

[2] رحموني محمد و بن الطيبي مبارك، شروط قبول الدليل الإلكتروني كدليل إثبات في الجريمة المعلوماتية، جامعة أدرار، مجلة القانون والعلوم السياسية، المجلد05 لعدد 02 سنة 2019، ص 23.

[3] The technical working group for electrinic crime scence investingation.electronic crime investigation ,the national instituteof justice,the united states of america,2001 ?page6.

[4] Eoghan Casey ,Digital Evidence and compter Crime,Third edition,Published by Elsevier Inc,London,2011,page 07.

ثالثا: خصائص للدليل الرقمي: على غرار خصائص ومميزات الجريمة الإلكترونية أيضا يتميز الدليل الرقمي بعدة خصائص ينفرد بها عن الدليل التقليدي نذكر منها[1]:

1-الدليل الرقمي دليل علمي غير ملموس: إن الدليل الإلكتروني يتصف بأنه علمي ومكوناته عبارة عن بيانات ومعلومات ومعطيات إلكترونية غير ملموسة لا تدرك بالحواس العادية يتم إدراكها بالاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية واستخدام نظم برامجية حاسوبية[2]، وعليه فإن ما يسري على الدليل العلمي يسري على الدليل الإلكتروني فإذا كان الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة الكاملة وهذا طبقا للقاعدة التي تنص على أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة بمعنى أن الدليل الإلكتروني يتماشى مع العلم الإلكتروني وإذا خرج عن ما توصل إليه فقد معناه.

2-الدليل الرقمي دليل تقني:

طبيعة الدليل الإلكتروني الرقمية تجعل من ادراكها يتطلب معالجتها تقنيا وذلك بالاستعانة بالوسائل والأجهزة وأدوات الحواسيب الآلية، وباستخدام أنظمة معالجة حاسوبية، ليتم من خلالها تحويل بياناته الأساسية إلى معلومات يمكن استخدامها كدليل إثبات[3].

3-الدليل الرقمي متنوع ومتطور:

مع توسع قاعدة الدليل الرقمي، يمكن لهذا الأخير أن يشمل أنواعا متعددة من المعلومات والبيانات الرقمية والتي بدورها تصلح أن تكون دليلا جنائيا بإدانة المتهم أو براءته، وأما ميزة التطور التي يختص بها الدليل الرقمي، فهي نتيجة تزايد استخدام تقنية المعلومات الرقمية، بعد أن أصبح كل من الحاسب الآلي وشبكات الانترنت يشكلان موطنا هاما للبيانات والمعلومات

[1]عائشة بن قارة مصطفى، المرجع السابق ص 34.

[2] براهيمي جمال، المرجع السابق ، ص 124.

[3]خالد ضو، حجية الدليل الإلكتروني وشروط قبوله في الإثبات الجنائي، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية-المركز الجامعي بأفلو/الأغواط، العدد الثامن مارس 2022 ، ص 205.

الرقمية، ومن وجهة أخرى نجد أن تطورها اليومي جاء لتلبية احتياجات المستخدمين الشيء الذي أدى إلى ظهور أنواع جديدة من هذه الأدلة[1].

4-الدليل الرقمي له سعة تخزين عالية:

يمتاز الدليل الرقمي بالسعة التخزينية العالية وآلة الفيديو الرقمية يمكنها تخزين مئات الصور وقرص صغير يمكنه تخزين مكتبة صغيرة، كما بإمكان الدليل الرقمي رصد معلومات عن الجاني ويحللها في ذات الوقت، حيث يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

5-صعوبة التخلص من للدليل الرقمي:

هذه الميزة من أهم مزايا الدليل الإلكتروني على الإطلاق، بل يمكن القول بأنها الميزة التي يتمتع بها الدليل الإلكتروني دون غيره من الأدلة التقليدية وهو بذلك يشبه الدليل العلمي المتعلق بالحمض النووي إذ أن كليهما يصعب التخلص منهما.

فالأدلة الإلكترونية يمكن إظهارها بعد إخفاؤها، وإصلاحها بعد إتلافها، واسترجاعها بعد حذفها، حيث يوجد العديد من برامج الحاسوب التي يمكن من خلالها استعادة البيانات التي يتم حذفها، ومما يزيد من صعوبة التخلص مننها أنه يمكن استخراج نسخ مطابقة للأصل ولها ذات القيمة والحجية في الإثبات، كما أن نشاط الجاني لمحو الدليل يشكل كدليل أيضا، فنسخة من هذا الفعل أي فعل الجاني لمحو الدليل يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقا كدليل إدانة ضده[2].

---

[1]سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر-باتنة_كلية الحقوق والعلوم السياسية، 2013، ص 124.

[2]عائشة بن قارة مصطفى، المرجع السابق، ص 42.

الفرع الثاني: تقسيمات للدليل الرقمي:

إن الدليل الإلكتروني لا يوجد على صورة واحدة وإنما له خاصية التنوع نظرا لما تتمتع به طبيعته من ضرورة توفقه مع الواقعة الإجرامية، لهذا فإن هناك محاولات فقهية وتشريعية لتقسيم الدليل الإلكتروني، سنحاول إبرازها كما يلي:

1-المحاولات الفقهية لتقسيم الدليل الإلكتروني:

تم تقسيم الدليل الإلكتروني إلى أربعة أقسام تتمثل فيما يلي:

القسم الأول:الأدلة الرقمية الخاصة بأجهزة الحاسب الآلي وشبكاتها.

القسم الثاني:الأدلة الرقمية الخاصة بالانترنت.

القسم الثالث:الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

القسم الرابع:الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات.

2-المحاولات التشريعية لتقسيم الدليل الإلكتروني:

وفقا لوزارة العدل الأمريكية (2002) فإن الدليل التقني يمكن تقسيمه إلى ثلاث مجموعات وهي كالتالي:

أ-السجلات المحفوظة في الحاسوب،وهي الوثائق المكتوبة والمحفوظة مثل البريد الإلكتروني وملفات برامج معالجة الكلمات ووسائل غرف المحادثة علة الانترنت,

.ب-السجلات التي تم إنشاؤها بواسطة الحاسوب، وتعتبر مخرجات برامج الحاسوب

.ج-السجلات التي جزء منها تم حفظه الإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب

وبطبيعة الحال فإن أي محاولة لتقسيم الدليل التقني من طرف الفقهاء، أو الهيئات الرسمية يمكن أن يكون محل جدل فقهي، وذلك بسبب التطور المستمر الذي يطرأ على البيئة التقنية التي يعيش فيها هذا الدليل.

على العموم يمكن تقسيم الأدلة الإلكترونية إلى أدلة ذات طابع مادي، وأدلة ذات طابع معنوي.

ويقصد بالأدلة ذات الطابع المادي كل دليل يأخذ شكل المخرجات الورقية التي تسجل عليها المعلومات الموجودة على الحاسوب، ويستخدم في ذلك الطابعات وذلك إنتاج نسخ مطبوعة من البيانات.

وعلى الرغم من اتخاذ الدليل الإلكتروني شكل مادي سواء تمثل في طباعته أو نسخه على أسطوانات ليصبح في شكل مادي ملموس، لا يفقده ذلك كونه دليلا إلكترونيا نشأ وتكون في بيئة تقنية معلومات[1].

أما الأدلة ذات الطابع المعنوي فيقصد بها تلك الأدلة التي تتخذ مظهرين مظهر حقيقي وآخر معلوماتي أو معنوي، وتتكون المظهر الحقيقي من الطبيعة الأصلية للدليل الإلكتروني والمتمثلة في الأرقام الثنائية صفر وواحد والتي يفهمها الحاسوب.

أما المظهر المعلوماتي فيتمثل في النتيجة التي يظهر بها الدليل الإلكتروني في شكل معلومة مفهومة ومن طبيعة يمكن للعقل البشري أن يتقبلها ويترجم موضوعها، كما لو ظهر الدليل في شكل رسالة مكتوبة . والتي يمكن قراءتها بواسطة شاشة الحاسوب أو وحدة العرض المرئي والتي يتم عن طريقها استعراض أي بيانات أو معلومات تكتب على لوحة المفاتيح بواسطة المستخدم أو تكون مخزنة في ذاكرة الحاسوب أو شبكة الانترنت.

كما قد يتمثل الدليل الإلكتروني في شكل أوعية لا ورقية أو غير مطبوعة كالأشرطة والأقراص الممغنطة أو الضوئية وغيرها من الأشكال غير المادية والتي يتواجد الدليل الإلكتروني عليها ويتخذ منها أنواع وأشكال مختلفة ومتعددة.

[1] حبيباتني بثينة، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أطروحة الدكتوراه في القانون العام –تخصص قانون جنائي وعلم الإجرام، جامعة الجزائر_كلية الحقوق والعلوم السياسية، 2020، ص ص 385-386.

وعليه فإن تنوع الدليل الإلكتروني هو نتيجة لطبيعة نشأته في البيئة التقنية، لذلك بات من الضروري اعتراف المشرع الإجرائي الجنائي بالدليل الإلكتروني، نظرا لأهميته وضرورته في إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1]..

المطلب الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي

يعد قبول الدليل الخطوة الإجرائية الأولية التي يمارسها القاضي تجاه الدليل الجنائي بصفة عامة والدليل الإلكتروني بصفة خاصة وذلك قبل البدء في تقديره التأكد من مدى صلاحيته وملاءمته لتحقيق ما قدم من أجله، وقبول القاضي الجنائي الدليل الإلكتروني في الإثبات الجنائي لابد أن يستند على أساس، وهذا ما سنعرضه في مطلبنا هذا من خلال دراسة تقدير الدليل الإلكتروني أمام القضاء الجنائي، لننتقل إلى وموقف المشرع الجزائري من الدليل الإلكتروني في الإثبات الجنائي.

الفرع الأول: تقدير الدليل الإلكتروني أمام القضاء الجنائي

القاضي الجنائي يتمتع بسلطة واسعة في تقدير أدلة الإثبات ووضع المشرع على الأدلة الرقمية شروط لا يجوز للقاضي الانحراف عليها عند ممارسته لها، ولقبول الدليل الإلكتروني كحجية للإثبات تبنى عليه الحقيقة في الدعوى الجزائية لابد من توفر بعض الشروط وهذا ما سنتطرق إليه من خلال هذا الفرع.

أولا – شروط اكتساب الدليل الإلكتروني حجية في الإثبات

الدليل الإلكتروني شأنه شأن باقي الأدلة الأخرى يخضع لنفس القواعد المقررة لباقي الأدلة سواء كانت هذه القواعد تتعلق بسلطته في قبول الدليل الإلكتروني أو تتعلق بسلطته في تقدير هذا النوع من الدليل ذلك أن القاضي لا يقدر إلا الدليل المقبول ولا يكون مقبولا إلا بعد التيقن

[1] حبيباتني بثينة، المرجع نفسه، ص 387.

من مراعاة الدليل لقاعدة المشروعية والتي لا يمكن من دونها أن يرتب الدليل الإلكتروني أي آثار قانونية.

وبالنظر إلى الطبيعة الخاصة التي يتميز بها الدليل الإلكتروني وما قد يصاحب الحصول عليه من خطوات معقدة فإن قبوله في الإثبات قد يثير العديد من المشكلات، حيث أن مستودع هذه الأدلة هو الوسائل الإلكترونية ولذا التلاعب فيها وتغيير الحقيقة أمر وارد وهذا ما نتساءل كيف نضمن مصداقية الدليل الإلكتروني وأنها بالفعل تعبر عن الحقيقة التي تهدف إليها الدعوى الجنائية.

وعلى ذلك ستكون الإجابة على هذا الإشكال من خلال تعرضنا بالدراسة إلى شروط اكتساب الدليل الإلكتروني حجية في الإثبات الجنائي وتتمثل في:

1- شرط مشروعية الدليل الإلكتروني:

إن القاضي الجنائي يتمتع بسلطة تقدير الدليل الإلكتروني ويشترط لقبوله أن يتحصل عليه بطرق مشروعة وفقا للنزاهة والأمانة وأن يستمد قناعته من هذا الأخير لأن محل الحرية والسلطة التقديرية التي يتمتع بها القاضي الجنائي هو الأدلة المقبولة.[1] وأن الدليل الإلكتروني عندما يكون مشروعا ضامنا للحرية الفردية وإذا استخدمت وسائل غير مشروعة في الحصول عليه أبطلت الإجراءات ويكون غير صالح كدليل إدانة في المواد الجنائية.[2]

2- شرط مناقشة الدليل الإلكتروني:

يجب على القاضي أن يبني حكمه على أدلة طرحت أمامه لمناقشة الدليل في الجلسة وهذا الأمر من أهم القواعد الإجرائية حتى تمنح للخصوم فرصة الاطلاع عليه ومناقشته، بحيث

[1]- عائشة بن قارة مصطفى، المرجع السابق، ص. 268.

[2]- علي محمود علي حمودة، الأدلة المحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، **بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية**، ط1، الإمارات العربية المتحدة، 2003، ص 23.

يترتب على أن يكون الدليل أصل ثابت في أوراق الدعوى أو على شكل بيانات معروضة على الحاسب الآلي أو معلومات مخزنة على الأقراص أو أشرطة ممغنطة، أو في شكل مطبوعات فجميعها تكون محلا للمناقشة إذا أخذت كدليل إثبات أمام المحكمة.[1]

ومناقشة الدليل تمنح الفرصة للخصوم للاطلاع على الدليل الإلكتروني والرد عليه وحتى يتمكن الخصوم في مواجهة هذه الأدلة، وهنا يتجسد مبدأ الوجاهية وإحاطة المتهم علما بالتهمة المنسوبة إليه وسماح له بالاستعانة بمحامي ومنحه الوقت الكافي لتحضير دفاعه وفي أثناء عملية المناقشة يسمح لكل طرف من الخصوم تقديم بعض المستندات وكذلك سؤال الشهود والخبراء.[2]

فالقاضي الجنائي لا يمكن أن يبني قناعته على رأي الغير إلا إذا كان من طرف خبراء وفنيين استشارهم من قبل وفقا للقانون وضميره كان مرتاح لرأيهم بما يوافق مع الأدلة المقدمة إليه في أوراق الدعوى المعروضة عليه.[3]

3- شرط يقينية الدليل الإلكتروني:

يستلزم للقاضي على أن يصدر حكم عن اقتناع يقيني من خلال الأدلة المتوفرة لديه فيعرف اليقين على أنه وجود حقيقة يستخلصها القاضي الجنائي بواسطة المعرفة الحسية بعيدا عن الغموض أو احتمال، ويكون ذلك من خلال فحص ومعاينة القاضي لهذه الوسائل أو الأدلة بالمعرفة الذهنية واستقراء النتائج ليبرهن على جودة الحقيقة.[4]ولكي يستطيع القاضي بلوغ درجة اليقين والحزم في إقتناعه بالأدلة ونسبها إلى المتهم يعتمد على نوعين من المعرفة:

---

[1]- سليمان أحمد فضيل، المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية الأنترنت، دار النهضة العربية، القاهرة، 2008، ص. 375.

[2]- عائشة بن قارة مصطفى، المرجع السابق، ص،ص 271، 272.

[3]- علي محمود على حمودة، المرجع السابق، ص37.

[4]- المرجع نفسه، ص 120.

فالمعرفة الأولى: هي المعرفة الحسية التي تستنبط من الحواس بعد المعاينة والفحص لهذه المخرجات.

- **أما المعرفة الثانية:** هي المعرفة العقلية التي تدرك عن طريق التحليل والاستنتاج والاستقراء التي يجريها على المخرجات الإلكترونية، ويربطها مع الملابسات الموجودة بها.[1]

ويتميز الدليل الإلكتروني بالطبيعة التقنية إلا أن هناك قواعد محددة تم وضعها من طرف المختصين التي تتحكم في يقينيتها ومن أهمها استعمال الوسائل الفنية ومن طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته من العبث وصحة الإجراءات المتبعة للحصول عليه وأهم الوسائل التقنية تتمثل في:

أ/ تقييم الدليل الإلكتروني من حيث سلامته من العبث:

للتأكد أن الدليل الإلكتروني لم يعبث في سلامته يجب أن نتبع طرق التالية: بحيث يلعب علم الكمبيوتر دور مهم في تقدير مختلف المعلومات الفنية التي تعمل على فهم مضمون الدليل الإلكتروني ويستعمل هذا النوع من العلوم في الكشف عن التلاعب بالدليل عن طريق فكرة التحليل التناظري الإلكتروني التي تكشف لنا عن مصداقية الدليل وهي تقنية يتم مقارنة الدليل الإلكتروني المقدم للقضاء بالأصل المدرج بالأدلة الرقمية.[2]

وتستخدم عمليات حسابية خاصة بالخوارزميات في حالة عدم الحصول على النسخة الأصلية للدليل أو في حالة ما كان هناك شك أن عبث في دليل وهذه التقنية تسمح لنا من التأكد من مصداقية الدليل الإلكتروني.

ب/ تقييم الدليل الإلكتروني من حيث القيمة الفنية:

[1]– إيمان محمدة علي الجابري، يقين القاضي الجنائي، منشأة المعارف، الإسكندرية، 2005، ص131.

[2] – جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، القاهرة، 2014، ص27.

نسبة الخطأ الفني في الحصول على الدليل الإلكتروني ضئيلة جدا باعتباره تطبيقا من الدليل العلمي وهذا لا يعني أنها منعدمة بل يظل الوقوع في الخطأ ممكنا أثناء استعماله ويكون ذلك إما بسبب الخطأ في استخدام الأداة المناسبة لاستخلاص الدليل كخلل في الشفرة المستخدمة، أو بسبب معلومات خاطئة ومن أجل تجنب مثل هذه الأخطاء يمكن إتباع بعض الاختبارات والتطبيقات للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الإلكتروني من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات نلخصها كالآتي[1]:

إخضاع الأداة المستخدمة في الحصول على الدليل لعدة تجارب بغية التأكد من دقتها في إعطاء النتائج المرجوة[2].

الاستعانة بأدوات ذات قيمة عالية أثبتت التجارب العلمية نجاعتها في تقديم نتائج أفضل.

ثانيا – أساس قبول الدليل الإلكتروني على ضوء أنظمة الإثبات

تختلف طريقة الاعتراف بالدليل الإلكتروني وقبوله كدليل إثبات من دولة إلى أخرى بحسب طبيعة نظام الإثبات السائد فيها وتنقسم هذه الأنظمة إلى ثلاثة أولها النظام اللاتيني – نظام أنجلوسكسوني – نظام مختلط التي سوف نتطرق إليها كالآتي:

أ- النظام اللاتيني:

يطلق عليه بنظام الإثبات الحر، يسود هذا النظام مبدأ حرية الإثبات لا يحدد فيه المشرع طرق معينة أو محددة للإثبات ولا حجيتها أمام القضاء بل يترك الحرية للقاضي في تأسيس حكمه وفقا لاقتناعه الشخص أمام أدلة موجودة ودون أن يفرض عليه دليل معين وأن القاضي الجنائي هو الذي يختار من بين الأدلة ما يراه مناسبا ومفيد للوصول إلى الحقيقة.[3]

[1] – براهيمي جمال، المرجع السابق ص 141.

[2]–براهيمي جمال، المرجع السابق ص 156

[3]– عائشة بن قارة مصطفى، المرجع السابق، ص، ص 192، 193.

هذا النظام يرتكز على مبدأين أساسين ومختلفين هما: الأول يتمثل في الدور الإيجابي للقاضي في الإثبات وقبول وتقدير الدليل الإلكتروني.[2]

بينما الدور الثاني السلبي للمشرع يتمثل في عملية الإثبات التي من خلالها يمتنع المشرع عن تحديد الأدلة التي تصلح للإثبات مسبقا مما يجعل جميع الأدلة مقبولة وفقا لتقدير القاضي وليس المشرع الذي يقتصر دوره على تحديد الشروط اللازمة لصحة الدليل وطريقة تقديمه ضمانا للحرية الفردية وكفالة حسن سير العدالة.[1] ومن بين التشريعات التي انتهجت هذا النظام نجد كل من فرنسا – الجزائر – مصر.

ب- نظام الأنجلوسكسوني:

ويعرف بنظام الإثبات المقيد وفي هذا النظام يقوم المشرع بتحديد وحصر الأدلة التي يستعين بها ويقبلها القاضي في عملية الإثبات فلا يجوز للقاضي أن يقوم ببناء حكم على خلافها ولا خروج عليها ولا يمكنه تقدير الأدلة أو البحث عنها بل يقتصر دوره على فحص الدليل للتأكد من مدى مشروعيته وتوفره على الشروط التي حددها القانون، يلتزم القاضي الجنائي أن يؤسس حكمه على أساس هذا الدليل وإن لم يكن مقتنعا به.[2]

يعتمد هذا النظام على مبدأين أساسين بحيث يمثل الدور الإيجابي للمشرع في عملية الإثبات باعتباره هو الذي ينظم قبول الأدلة سواء عن طريق التعيين المسبق للأدلة المقبولة للحكم بالإدانة أو باستبعاد أدلة أخرى كونه هو الذي يحدد القيمة الإقناعية لكل دليل.[3]

الدور الثاني هو سلبيا للقاضي الجنائي في الإثبات بحيث يلزم بما يرسمه له المشرع وهذا ما يفقده سلطته في الحكم بما يتناسب مع الواقع ويصبح القاضي كالآلة في طاعته لنصوص

[1] – أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015، ص 195.

[2] – شيماء عبد الغاني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص387.

[3] – براهيمي جمال، المرجع السابق، ص، ص 138، 139.

القانون دون إبراز قناعته الشخصية.[1] ومن بين التشريعات التي أخذت بهذا النظام نجد إنجلترا وأمريكا الجنوبية وجنوب إفريقيا.

ج- نظام الإثبات المختلط

هو نظام وسط بين نظام الإثبات المقيد ونظام الإثبات الحر [2]. وهذا النظام دمج بين النظامين عن طريق تحديد قائمة أدلة الإثبات والقيمة الثبوتية من طرف المشرع من جهة ومن جهة أخرى منح للقاضي الجنائي السلطة التقديرية في موازنة وقبول الأدلة المطروحة أمامه، كما أن هذا النظام يقوم على تحديد أدلة الإثبات سلفا، كما نجده يحدد قيمتها وحجيتها مع إعطاء القاضي حرية في تقدير القضية المعروضة أمامه أي القاضي له دور إيجابي في ظل هذا النظام.

واعتبر الفقهاء هذا المذهب أفضل من نظام الإثبات المقيد والحر لأنه يجمع محاسنهما ويستبعد مساوئهما فهو يوازي بين تحقيق العدالة وما يتطلبه من مرونة وحرية في الإثبات وما يتطلبه استقرار التعامل من تقييد الإثبات في بعض الأحيان.

الفرع الثاني: موقف المشرع الجزائري من الدليل الإلكتروني في الإثبات 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 يستعين بها القاضي للوصول إلى الحقيقة وكشف الجريمة ونسبتها إلى المتهم، ومن خلال المادة 212 من قانون الإجراءات الجزائية حيث تنص على أنه " يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ولا يجوز للقاضي أن يبني قراره إلا على

[1] – سامي جلال فقي، الأدلة المتحصلة من الحاسب وحجتها في الإثبات، دار كتب القانونية، القاهرة، 2011، ص 93.

[2]– عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، منشورات الحلبي، دمشق، 2007، ص 373.

الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه ".[1] وهي مستوحاة من المادة 535 من القانون الفرنسي.[2]

والمادة 307 من قانون الإجراءات الجزائية ".....القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما....".[3]

ومن خلال المادتين السابقتين أخذ المشرع الجزائري بصفة عامة بنظام الإثبات الحر وبصفة استثنائية بنظام الإثبات المقيد في بعض الجرائم كجريمة الزنا المنصوص عليها في المادة 339 و341 من ق ع.

وأما إقرار المشرع الجزائري للحرية في تقديم الأدلة وتركها للقناعة 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 الإلكتروني هو دليل من نوع خاص شأنه شان الجرائم الالكترونية، 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 كافة شروط الصحة وكذلك العكس صحيح.

---

[1]– المادة 212 من القانون 06 – 22 المؤرخ في 20 / 12/ 2006 المتضمن قانون الإجراءات الجزائية ، المرجع نفسه.

[2] -articil 535 du C.p.p dispose que"la loi ne demande pas compte aux juges des moyens par lesquels ile se sont convaincus elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d' une preuve elle leur prescrit de s'interroger aux même dans le silence et le recueillement et de chercher dans la sincérité de leur conscience quelle impression ont fait sur leur raison les preuves rapportées contre l'accuse et les moyens de sa défense la loi ne leurfait que cette seule question qui renferme toute la mesure de AVEZ - VOUS UNE INTIME CONVICTION?

[3]– المادة 307 من القانون 06 – 22 المؤرخ في 20 / 12/ 2006 المتضمن قانون الإجراءات الجزائية ، المرجع نفسه.

أما بالنسبة لسلطة القاضي الجزائري في تقدير الدليل الالكتروني فان المادة العلمية للدليل الالكتروني جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، إن هناك من يرى أن الدليل العلمي ومنه الدليل الالكتروني له قوته الثبوتية الملزمة حتى للقاضي مستندين في رأيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين، وهناك من يرى بان مبدأ حرية القاضي في الامتناع يجب أن يبسط سلطته على كل الأدلة دون استثناء حتى على الدليل الرقمي، معتبرين أن إعطاء الدليل الرقمي قوة ثبوتية لا يستطيع القاضى مناقشتها يعد بمثابة الرجوع إلى مذهب الإثبات القانوني المقيد، والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الجرائم التي يتطلب إثباتها دليلا معينا ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين قناعته من أي دليل يطمئن عليه.[1]

[1] – بوبكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص508.

خاتمة

الخاتمة:

من خلال انجاز هذه المذكرة نستخلص بان موضوع التحقيق في مجال الجرائم الإلكترونية هو موضوع مركب ومتشعب، هذا النمط الجديد من الجرائم هو وليد ثورة تقنية للمعلومات والاتصالات التي يعرفها عالمنا المعاصر اليوم، وإن سوء استخدام على نحو غير مشروع أدى إلى تهديد أمن المعطيات من جهة وحرية الأفراد وممتلكاتهم والمؤسسات من جهة أخرى، فالحماية الفنية مهما بلغت درجتها من التعقيد والصعوبة فهي لا تستطيع المقاومة أمام التطور التقني الذي تشهده تقنيات الاختراق وكذا عجز النصوص التقليدية في توفير الحماية خاصة من الناحية الإجرائية، ومن خلال كل ما سبق توصلنا إلى مجموعة من النتائج والتوصيات نوجزها فيما يلي:

من خلال هذه الدراسة تم استخلاص النتائج الآتية:

01- إن الجريمة الإلكترونية تعد من المواضيع المستحدثة التي فرضت نفسها في الآونة الأخيرة بقوة على المستوى الوطني أو الدولي وأجبرت الدول على دق ناقوس الخطر والتدخل من أجل مواجهتها.

02- إن الجريمة الالكترونية من الجرائم العابرة للقارات وهذا ما أثر سلبا على التحكم فيها وذلك أن الدول تستطيع إصدار التشريعات التي تحكم هذا النوع داخل حدودها إلا أنها لا تستطيع ذلك خارج حدودها.

03- صعوبة الحصول على الأدلة في مثل هاته الجرائم مما يزيد من خطورتها وإن هاته الأدلة سهلة التخلص منها عكس الجرائم التقليدية التي يكون فيها الدليل مرئيا ويسهل الحصول عليه.

04- إن الكثير من الأشخاص والمؤسسات التي تتعرض إلى الهجمات الالكترونية لا تقوم بالتبليغ وهذا ما يؤدي إلى تفاقم هاته الجرائم واكتساب المجرمين ثقة كبيرة والتمادي في ممارسة نشاطهم الإجرامي.

05- إن المشرع الجزائري لم يقم بتحديد الجريمة المرتكبة باستخدام النظام المعلوماتي وترك المجال واسع ليدخل في نطاقها كل تفرزه التقنية الجديدة وتطوراتها.

06- سلطات التحقيق تفتقر إلى مهارات التحقيق وتقنيات البحث والتحري لعدم استفادة العنصر البشري من تكوين ذو مستوى وجودة عالية لمواجهة خصائص ومميزات الجرائم الالكترونية والدليل الالكتروني باعتباره دليل غير مادي لا يمكن إدراكه بالحواس ويسهل التلاعب به وتغييره وتدميره كما قد يكون هذا الدليل مشفر يتطلب الاعتماد على برامج معقدة ورموز سرية تعقد من مهمة سلطات التحقيق من الوصول إليه.

07- الأخذ بالدليل الالكتروني يخضع لتقدير القاضي الجنائي، بحيث يملك الحق في مناقشة الظروف والملابسات المحيطة بالدليل وله الحق أن يرفضه إن لم يقتنع بظروف وملابسات القضية عكس القيمة العلمية القاطعة التي يتميز بها الدليل الالكتروني فلا يمكن للقاضي الفصل فيها لأنها مسألة فنية تعود لأهل الاختصاص.

08- التحقيق الجنائي في مجال الجرائم الالكترونية يواجه صعوبات متعلقة بشخص المجرم وصعوبة تحديد هويته الإلكترونية والتعرف على عنوانه الالكتروني بحيث يمكنه التلاعب به وإخفائه بحيث يتمكن بعض المجرمين من اختراق أجهزة أشخاص آخرين لينفذ أعماله الإجرامية انطلاقا من تلك الأجهزة ما يساعد على تضليل أجهزة التحقيق.

09- عجز أجهزة التحقيق في مواجهة الجريمة الالكترونية بالاعتماد على الإجراءات التقليدية المادية للتحقيق وافتقارها إلى التكنولوجيات الحديثة والوسائل التقنية المتطورة لمواكبة التطور السريع والهائل الذي تعرفه الجرائم الالكترونية.

10- للتركيز على العمل التوعوي والتحسيسي داخل المجتمع بإشراك المجتمع المدني والعمل على الاستخدام الأمثل للتطبيقات الحديثة وإدراك المواطن للمخاطر الناجمة عن الاستخدام الغير المشروع للأنترنت وما يترتب عنه من انعكاسات سلبية على المستوى النفسي، الاقتصادي والاجتماعي...إلخ وذلك مثلا من خلال برمجة حملات تحسيسية للتوعية من مخاطر الجرائم

الالكترونية خاصة على مستوى المؤسسات التعليمية والجامعات بتسطير برنامج من طرف وزارة التربية الوطنية ووزارة التعليم العالي والبحث العلمي.

وبناءا على هذه النتائج نقترح التوصيات التالية:

01- أن يتم إضافة نصوص قانونية تهتم بكيفية إجراء الضبط والتفتيش وأخذ الدليل الالكتروني من الأجهزة الالكترونية دون أن يمس ذلك بحرية الأفراد وعدم المساس بالحرية الشخصية لأنها مصانة مع عدم العبث بالأجهزة وما تحتويه من مخزونات .

02- يجب النص على الدليل الالكتروني كدليل إثبات في القوانين ذات الصلة بأدلة الإثبات.

03- ضرورة انضمام الجزائر في الاتفاقيات الدولية والعربية للتعاون على مكافحة الجريمة الالكترونية.

04- ضرورة إنشاء وحدات أمن وأجهزة قضائية متخصصة في مكافحة الجرائم الالكترونية ليكون لديهم الإلمام الكافي بالجوانب التقنية والفنية لمتابعة وكشف وضبط تلك الجرائم ومرتكبيها.

05- ضرورة وضع برامج تأهيل لعناصر الضبطية القضائية ورجال الأمن المكلفين بعمليات البحث والتحري حول كيفية التعامل مع الأدلة وضبطها والاستعانة بذوي التخصصات الدقيقة من التقنيين والفنيين في أنظمة الحاسوب والانترنت وشبكات الاتصال الأخرى.

06- ضرورة عقد دورات تدريبية لرجال القضاء والمحققين في مجال تقنية المعلومات حتى يتسنى لهم مواجهة الجرائم الالكترونية.

07- ضرورة الاهتمام بالبحوث والدراسات القانونية والاجتماعية التي تهتم بالجريمة الالكترونية والأخذ بالتوصيات التي توصل إليها الباحثين في هذا المجال.

08- إبرام إتفاقيات تعاون داخلية بين القضاء ومهندسو الإعلام الآلي من أجل إثراء المعرفة الفكرية في ميدان المعلوماتية.

09- حث المواطنين عن التبليغ عن الجريمة الإلكترونية.

10- الإسراع في الانضمام إلى مختلف الاتفاقيات الدولية الخاصة بمكافحة الجريمة الإلكترونية وكل ما من شأنه تكثيف الجهود على المستوى الدولي والإقليمي كإنشاء الدول الإفريقية أو العربية لأجهزة وهيئات ومنظمات تهتم بالتنسيق الأمني في مجال مكافحة الجريمة الإلكترونية والعمل على تطوير كفاءاتها وخبراتها في هذا المجال.

11- تفعيل التعاون بين سلطات التحقيق ومزودي خدمة الانترنت بشكل يسمح تحصيل المعلومات اللازمة في الوقت المناسب لغرض التحقيق وبالتالي استخلاص الدليل الإلكتروني في أسرع وقت ممكن.

قائمة المراجـــع

قائمة المصادر:

القرآن:

01- الآية 45 من سورة الفرقان.

النصوص القانونية:

01-القانون رقم 04-15 المؤرخ في 10 نوفمبر، يعدل ويتمم الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71 لسنة 2004.

02- القانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 155/66 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، ج ر,عدد 84.

03- القانون 09-04 المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، العدد 47 الصادرة بتاريخ 16 أوت 2009.

الأوامر:

01- الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 جوان 1966 في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، المنشور في الجريدة الرسمية، العدد رقم 48 الصادر يوم 10جوان 1966.

مراسيم رئاسية:

01- المرسوم الرئاسي رقم 15-251 مؤرخ في:2015/10/08 يحدد كيفية تشكيل وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج، ر، عدد 35 مؤرخة في:2015/10/08.

02- المرسوم الرئاسي رقم 19-172 مؤرخ في:2019/06/06 يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتنظيمها وسيرها، ج، ر، عدد 37 مؤرخة في:2019/06/09

03- المرسوم 15-261 المؤرخ في 24 ذي الحجة 1436هـ/لموافق ل8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال,

الكتب:

اولا: باللغة العربية:

01- أحمد شوقي الشلقاني، مبادىء الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999.

02- أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، د ط ، دار النهضة العربية، القاهرة، 2015.

03- إيمان محمدة علي الجابري، يقين القاضي الجنائي، منشأة المعارف، د ط ،الإسكندرية،2005 .

04- بوبكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012 .

05- جميل صليبا- المعجم الفلسفي المصطلحات القانونية، الجزء الأول، ط1، دار الكتاب اللبناني، بيروت، 1982.

06- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، د ط ، دار النهضة العربية، القاهرة، 2014.

07- حسن الجوخندار، التحقيق الإبتدائي في قانون أصول المحاكمات الجزائية، ط 01، دار الثقافة، عمان، 2008 .

08- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط01، دار الفكر الجامعي، مصر، 2009.

09- زبيحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي ، د ط ، دار الهدى عين مليلة، الجزائر، 2011.

10- سامي جلال فقي، الأدلة المتحصلة من الحاسب وحجتها في الإثبات، دار كتب القانونية، القاهرة، 2011.

11- سليمان أحمد فضيل، المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية الأنترنت، دار النهضة العربية، القاهرة، 2008 .

12- شيماء عبد الغاني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية،د ط ، دار الجامعة الجديدة، الإسكندرية، 2007

13- ضياء مصطفى عثمان، السرقة الإلكترونية، ط1 ، دار النفائس، عمان، 2011.

14- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلومات دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، ط1 ، دار النهضة العربية، مصر، 2009 .

15- عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث العلمي، د، ط، الكتب والوثائق المصرية، مصر ،2006.

16- عبد الله محمود، إجراءات جمع الأدلة في مجال الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية،د ط ، دبي، 2003.

17-عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، ط2، منشورات الحلبي القانونية ، دمشق,2007.

18- علي بن هادية بلحسن، البليش والجيلالي بن الحاج يحي، القاموس الجديد للطلاب، ط1،الشركة الوطنية، الشركة التونسية، الجزائر، تونس، 1979 ,

19- علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب و الأنترنت ،ط 1 ، عالم كتب الحديثة ، 2004.

20- غنية باطلي، الجريمة الإلكترونية(دراسة مقارنة)،د ط ، دار الجزائرية ، الجزائر , 2016 .

21- مجذوب نوال، الجريمة المعلوماتية وأثرها على التنمية الاقتصاديةالجزء 01، المركز الديمقراطي العربي ، د س ن –برلين –ألمانيا، ط1 ، سنة النشر جويلية 2020.

22- محمد البشرى، التحقيق في جرائم الحاسب الآلي، د ط ، مؤتمر القانون والأنترنت، الإمارات،2000.

23- محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الأنترنت (الأحكام الموضوعية والأحكام الإجرائية)، ط1، منشورات الحلبي الحقوقية، 2011.

24- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة المرور، القاهرة، 2008 .

25- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، د ط ، دار الكتب القانونية، مصر، 2006.

26- ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيات المعلوماتية بين النصوص التشريعية والخصوصية التقنية،ط 1، دار النشر،الجزائر2018.

27- نائلة محمد قورة، جرائم الحاسب الآلي الإقتصادية، ط1، منشورات الحلبي الحقوقية ، بيروت، 2005.

28- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2007.

29- هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلومات (دراسة مقارنة)، ط1، دار النهضة العربية، مصر، 1997 .

30- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، د ط ، دار الجامعة الجديدة الإسكندرية ،2019 .

الأطروحات:

رسائل دكتوراه:

01- أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، أطروحة لنيل الدكتوراه في القانون، كلية حقوق جامعة عين الشمس، القاهرة، د س ن .

02- براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة دكتوراه في القانون، كلية الحقوق، جامعة تيزي وزو، 2018.

03- بن يحي اسماعيل، التحقيق الجنائي في الجرائم الالكترونية، اطروحة لنيل شهادة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، د ط ، جامعة ابو بكر بلقايد تلمسان ،2021 .

04 – حبيباتني بثينة، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أطروحة دكتوراه ل.م.د في القانون العام –تخصص قانون جنائي وعلم الإجرام، جامعة الجزائر، كلية الحقوق والعلوم السياسية، 2020.

رسائل الماجستير:

01- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير علوم جنائية، كلية الحقوق والعلوم السياسية الحاج لخضر، جامعة باتنة، الجزائر، 2013/2012.

02- طرشي نورة، مكافحة الجريمة المعلوماتية، رسالة لنيل شهادة الماجستير في قانون، فرع قانون الجنائي، كلية الحقوق جامعة الجزائر 1، 2011.

03- عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، رسالة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية، 2007.

04-عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات الجنائي دراسة مقارنة، رسالة لنيل شهادة الماجستير في حقوق، كلية الحقوق جامعة الاسكندرية، 2009.

المقالات:

01- خالد ضو، حجية الدليل الإلكتروني وشروط قبوله في الإثبات الجنائي، **مجلة الباحث الأكاديمي في العلوم القانونية والسياسية**-المركز الجامعي بآفلو/الأغواط، العدد الثامن مارس 2022.

02- رحموني محمد و بن الطيبي مبارك، شروط قبول الدليل الإلكتروني كدليل إثبات في الجريمة المعلوماتية، جامعة أدرار، **مجلة القانون والعلوم السياسية**، المجلد05 ، العدد 02 2019.

03- رحموني محمد، خصائص الجريمة الالكترونية ومجالات استخدامها، **مجلة الحقيقة**، جامعة أحمد دراية، أدرارالعدد41،2018 .

04- زورو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، **مجلة دفاتر السياسة والقانون**، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد11، 2014.

05- سعيدة بوزنون، مكافحة الجريمة المعلوماتية في ظل التشريع الجزائري، **مجلة العلوم الإنسانية**، ، كلية الحقوق جامعة الإخوة منتوري-قسنطينة-،العدد 52، ديسمبر2019.

06- علاوة هوام، التسرب كآلية للكشف عن الجرائم في القانون الجزائري، **مجلة الفقه والقانون**، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012 .

07- عيدة بلعابد خصوصية التحقيق في الجريمة المعلوماتية، **مجلة الباحث الأكاديمي في العلوم القانونية والسياسية**، جامعة مولاي الطاهر سكيكدة، العدد 06، 2011.

08- مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها، **مجلة كلية الحقوق والإدارة العامة، جامعة بيزيت**، رام الله فلسطين، المجلد: 45، العدد: 4، 2018.

09- زناتي محمد السعيد، الجريمة المعلوماتية في ظل التشريع الجزائري والإتفاقيات الدولية، **مجلة إيليزا للبحوث والدراسات**، العدد الثاني،المركز الجامعي إيليزي، الجزائر، ديسمبر 2017.

بحوث متخصصة :

01- أحمد حمو، علاء عواد، ولاء عبد الله، بحث في الأدلة الإلكترونية من الناحية القانونية والتقنية، أوراق بحثية في القانون ومكافحة الفساد، دراسة تحليلية مقارنة ، د ط جامعة بيروت، 2015.

02- علي محمود علي حمودة، الأدلة المحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية نظمته أكاديمية شرطة دبي، ط1 ، الإمارات المتحدة 2003.

ثانيا: المراجع باللغة الفرنسية:

01-charle diaz- la police techenique et scientifique 2 eme édition -édition presse universitaire défonce france 2006.

02- yann padova un aperçu de lutte contre la cybercriminalité science criminelle et droit penale n 4 dalloz 2002.

ثالثا: المراجع باللغة الإنجليزية:

01_Eoghan Casey ,Digital Evidence and compter Crime,Third edition,Published by Elsevier Inc,London,2011.

02-The technical working group for electrinic crime scence investingation.electronic crime investigation ,the national instituteof justice,the united states of america,2001.

فهرس المحتويات

فهرس المحتويات:

العنوان	الصفحة
بسملة	
شكر وعرفان	
إهداء	
قائمة المختصرات	
مقدمة	01
الفصل الأول ماهية التحقيق الجنائي في الجريمة الإلكترونية	07
المبحث الأول:الإطار المفاهيمي للتحقيق الجنائي في الجريمة الإلكترونية:	08
المطلب الأول: ماهية الجريمة الإلكترونية	08
الفرع الأول: تعريف الجريمة الإلكترونية	08
الفرع الثاني:خصائص الجريمة الإلكترونية	17
المطلب الثاني: ماهية التحقيق الجنائي في الجرائم الإلكترونية	19
الفرع الأول: تعريف التحقيق الجنائي في الجريمة الالكترونية:	19
الفرع الثاني: خصائص التحقيق في الجريمة الالكتروني	22
المبحث الثاني: الأجهزة المكلفة بالبحث والتحري في الجرائم الإلكترونية	28
المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال	28
الفرع الأول: مفهوم وتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال	29
الفرع الثاني: مهام وسير عمل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال	31
المطلب الثاني: الوحدات التابعة لسلك الأمن الوطني والدرك الوطني	34
الفرع الأول: الوحدات التابعة لسلك الأمن الوطني	34
الفرع الثاني:الوحدات التابعة لسلك الدرك الوطني	34
الفصل الثاني: آليات التحقيق في الجرائم الالكترونية	37
المبحث الأول: إجراءات التحقيق في الحصول على الدليل الالكتروني	38

فهرس المحتويات:.....

المطلب الأول: القواعد الإجرائية التقليدية في الحصول على الدليل الالكتروني	38
الفرع الأول:التفتيش وضبط الأدلة في الجرائم المعلوماتية.	39
الفرع الثاني: المعاينة	46
الفرع الثالث: الخبرة	47
المطلب الثاني: القواعد الإجرائية الحديثة في الحصول على الدليل الإلكتروني	49
الفرع الأول: التسرب الإلكتروني	49
الفرع الثاني: اعتراض المراسلات والمراقبة الإلكترونية	52
المبحث الثاني: القيمة القانونية للدليل الإلكتروني	55
المطلب الأول:ماهية الدليل الإلكتروني	55
الفرع الأول: تعريف الدليل الإلكتروني وخصائصه	56
الفرع الثاني: تقسيمات للدليل الرقمي:	60
المطلب الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي	62
الفرع الأول: تقدير الدليل الإلكتروني أمام القضاء الجنائي	62
الفرع الثاني: موقف المشرع الجزائري من الدليل الإلكتروني في الإثبات الجنائي	69
خاتمة	73
قائمة المراجع	78

الملخص:

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة التي تتطلب لارتكابها وسائل ذات تقنية عالية، وعليه فإجراءات التحقيق فيها تتمتع بنوع من الخصوصية نظرا لطبيعة الجريمة الإلكترونية،هذاما دفع بالمشرع الجزائري إلى تدعيم ترسانته القانونية بقانون خاص زود من خلاله المحقق بالمزيد من القواعد الإجرائية و الوقائية التي بدورها تسهل التحريات في مكافحة هذا النوع من الإجرام, فقد سن القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الذي جاء لينسق بين القواعد الإجرائية الخاصة(كتفتيش المنظومات وحجز المعطيات المعلوماتية) والهدف من ذلك هو إمكانية الكشف المبكر عن هذا النوع المستحدث من الجرائم الذي يهدد العالم بأسره.

الكلمات المفتاحية:الجريمة الإلكترونية، التحقيق الجنائي، إجراءات التحري، التشريع الجزائري.

Summary

Cybercrime is considered one of the new crimes that require high-tech means to commit, and therefore the investigation procedures enjoy a kind of privacy due to the nature of cybercrime. This is what prompted the Algerian legislator to strengthen his legal arsenal with a special law through which the investigator was provided with more procedural and preventive rules, which in turn To facilitate investigations in combating this type of crime, Law No. 09-04 of August 5, 2009 was enacted, which includes the special rules for preventing and combating crimes related to information and communication technology, which came to coordinate the special procedural rules (such as inspecting systems and seizing information data) and the goal of This is the possibility of early detection of this new type of crime that threatens the entire world.

key words:

Cybercrime, criminal investigation, investigation procedures, Algerian .legislation