الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي

جامعة الشاذلي بن جديد-الطارف
كلية الحقوق و العلوم السياسية
قسم الحقوق

مذكرة بعنوان

التحقيق في الجرائم المعلوماتية

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص:
قانون الأعمال

اعداد الطلبة:
تونسي نور الصفاء
توام نريمان

اشراف الاستاذ(ة)
د/ سعدون بلقاسم

لجنة المناقشة

الاسم و اللقب	الرتبة	الهيئة المستخدمة	الصفة
د/ خوالدية فؤاد	استاذ التعليم العالي	جامعة الشاذلي بن جديد	رئيسا
د/ سعدون بلقاسم	استاذ مساعد –ب-	جامعة الشاذلي بن جديد	مشرفا و مقررا
د/ رحال سهام	استاذ محاضر-أ-	جامعة الشاذلي بن جديد	ممتحنا

السنة الجامعية:

2024-2023

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة):تونسي نور الصفاء

الحامل لبطاقة التعريف الوطنية رقم: 110001251004710005

الصادرة بتاريخ: 22-10-2023

عن دائرة: بن مهيدي -الطارف-

المسجل بقسم: الحقوق

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

التحقيق في الجرائم المعلوماتية

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

التاريخ: 2024/06/12

إمضاء المعني

إطلع على البصامات و إمضاء
السيد(ة): ...
بن مهيدي في ...
12 JUIN 2024

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): ...تواتي بشير.....

الحامل لبطاقة التعريف الوطنية رقم: 119951241006520008

الصادرة بتاريخ: ...2018.05.08.....

عن دائرة: .....القالة.....

المسجل بقسم: ...الحقوق...سنة ثانية ماستر (قانون الأعمال)

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

.....التحقيق في الجرائم المعلوماتية.....

.....

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

التاريخ: 2024/06/12

إمضاء المعني

عن رئيس المجلس الشعبي البلدي
و بتفويض منه
عادل سعدي

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي

جامعة الشاذلي بن جديد-الطارف
كلية الحقوق و العلوم السياسية
قسم الحقوق

مذكرة بعنوان

التحقيق في الجرائم المعلوماتية

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص:
قانون الأعمال

اعداد الطلبة:
تونسي نور الصفاء
توام نريمان

اشراف الاستاذ(ة)
د/ سعدون بلقاسم

لجنة المناقشة

الاسم و اللقب	الرتبة	الهيئة المستخدمة	الصفة
د/ خوالدية فؤاد	استاذ التعليم العالي	جامعة الشاذلي بن جديد	رئيسا
د/ سعدون بلقاسم	استاذ مساعد -ب-	جامعة الشاذلي بن جديد	مشرفا و مقررا
د/ رحال سهام	استاذ محاضر-أ-	جامعة الشاذلي بن جديد	ممتحنا

السنة الجامعية:

2024-2023

شكر وتقدير

نشكر المولى سبحانه وتعالى الذي أمدنا بالصبر والقوة لإنجاز هذه المذكرة

كما نتقدم بأسمى عبارات الشكر والامتنان إلى الدكتور

"سعدون بلقاسم"

لقبوله الإشراف على هذه المذكرة ولصبره معنا على تصويرها.

كما يشرفنا أن نتقدم أيضا بالشكر الجزيل

"للأساتذة أعضاء لجنة المناقشة"

لقبولهم مناقشة عملنا.

الإهداء

إلى من هي الحياة حياة إليك ينحني الحرف حبا وامتنان إلى الأميرة

التي قد ورثت في جوفها كيف أكون إنسانا قبل أن أصرخ صرختي الأولى

في هذا العالم إليك **أمي**.....

وعليكم السلام.

تونسي نور الصفاء

الإهداء

إلى صاحب السيرة العطرة والفكر المستنير، فلقد كان له الفضل الأول في بلوغي التعليم العالي

"والدي الحبيب"

أطال الله عمره.

إلى من وضعتني على طريق الحياة، وغمرتني بركتها وساندتني وخطت معي خطوتي

"أمي الغالية"

طيب الله أثرها.

إلى روح قلبي **اخوتي**، من كان لهم بالغ الأثر في كثير من العقبات والصعاب

إلى **جميع أساتذتي** الكرام.

إلى نفسي التي تعبت، وكدت، وحلمت، وسعت حتى توجت بأسمى معاني النجاح.

قائمة المختصرات:

- ج ر ج ج: الجريدة الرسمية للجمهورية الجزائرية.
- د س: دون سنة.
- ع: العدد.
- ط: الطبعة.
- ق إ ج: قانون الاجراءات الجزائية.
- ق ع: قانون العقوبات.
- ق م ج: قانون مدني جزائري.
- ص: الصفحة.

مقدمة

نظرا للتطور العلمي في مجال تكنولوجيا المعلومات و الاتصالات في العصر الحالي، فقد احدث ثورة علمية واسعة و شاملة لمختلف المجالات و كان لها الاثر الايجابي على تسهيل العديد من جوانب الحياة المعاصرة ويختصر على الناس الوقت والجهد في حياتهم اليومية، كما يصاحبها آثار سلبية تشكل خطرا على الفرد والمجتمع.

وتتنوع هذه الجرائم بشكل كبير كونها سرية ومرتبطة بأحدث التقنيات وشبكة الانترنيت، مما سهل ارتكابها و هذا جراء مرتكبو الجريمة المعلوماتية اشخاص و خبرة و احترافية في هذا المجال. و يمتازون بالمهارة التقنية و الذكاء المعتمد في ارتكابها و تشمل السرقة المالية، الاحتيال و الحاق الضرر بالبرمجيات و البيانات فالجريمة المعلوماتية خالية من اشكال العنف الامر الذي ميزها عن باقي الجرائم التقليدية المعتادة و جعلها صعبة الاثبات لتصبح تهديدا متزايد للأفراد و المؤسسات.

و قد اصطلح المشرع الجزائري على تسمية الجرائم الالكترونية بالجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و عرفها بموجب القانون 09-04 المؤرخ في 05 غشت 2009[1]، على أنها: "جرائم المساس بأنظمة المعالجة الالية للمعطيات الالية المحددة في قانون العقوبات و اية جريمة اخرى أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصال الالكتروني".

حيث جاء المشرع الجزائري في المادة 212 من الدستور[2] على أنه: "يبادر المجلس بأعمال التحسيس و الاعلام و الاتصال لترقية حقوق الانسان"، ولتأثير التوسع التكنولوجي نظم المشرع الجزائري الجريمة المعلوماتية، ووضع الاليات المختصة بالإجراءات المتطورة ذات طبيعة مشروعة للحصول على الدليل الرقمي

[1] -القانون رقم 09-04 ،المؤرخ في 14 شعبان عام 1430 الموافق ل 05 اوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، ج ر ج ج، ع47،2009.

[2] -المادة 212 ،من تعديل الدستور لسنة 2020، المؤرخ في 30 ديسمبر 2020، ج ر ج ج، ع82، 2020.

و بالإضافة الى عجز الادلة التقليدية و قصورها في مجاراة نسق تطور هذه الجرائم من حيث كم البيانات المدونة في جهاز الحاسوب الالي و كيفية اثبات الدليل الرقمي.

و لأجل ذلك توجب تحديث انظمة و جهات امنية و اجهزة مختصة بمعالجة القضايا الناتجة عن الجريمة المعلوماتية، و هو ما يدفع لتطوير اسلوب التحقيق بشكل عام الذي يعتمد على دور المحققين و الخبراء المكلفين بالبحث في الادلة و متابعتها، من خلال استخدام الوسائل و الاساليب المتطورة في مجال التحقيق و ضبط مرتكبيها بغرض ضمان فعالية و نجاعة الاجراءات المتخذة بهذا الشأن ليقع على عاتق الهيئات المختصة مهمة الاستعداد لمواجهة تلك التطورات و صعوبة دراستها و تفادي الاخطار التي تلحق الفرد و المجتمع.

أهمية الدراسة:

تتبع أهمية الدراسة لهذا الموضوع في التحقيق في الجرائم المعلوماتية وكيفية استخلاص الدليل الرقمي، ولا شك ان ظهور أنماط جديدة من الجرائم لم تكن مألوفة في السابق و نحن لا نزال في بداية عصر الانفجار المعلوماتي يعني توقع ظهور المزيد و المزيد من أنماط أخرى جديدة، مواكبة لعصرنا و هو عصر العولمة فيجب معها تحديث الانظمة و التعليمات و الجهات الامنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الانماط الجديدة و المتطورة، من خلال توسيع المعرفة في مجال التحري و الاجراءات القانونية الصحيحة الواجب اتباعها من قبل السلطات القضائية المختصة في الكشف عن الجرائم المعلوماتية، كما ان التحقيق بشكل عام يعتمد على ذكاء المحقق و فطنته و قوة ملاحظة و سرعة البديهية لديه و ان يحاول بكل الجهد الممكن أن يقوم بالتحقيق و البحث فيها و متابعتها و البحث في الادلة و التنقيب عنها وصولا الى الحقيقة.

أسباب اختيار الموضوع :

يكمن اختيار موضوع بحثنا و هي الرغبة الشخصية و العلمية في دراسة القضايا ذات الطابع الجنائي و المتمثل في التحقيق في الجرائم المعلوماتية. حيث أن ما لفت انتباهنا و اختيارنا لهذا الموضوع هو نوعية و طبيعة الموضوع في حد ذاته كونه ينصب في مجال تخصصنا، بالإضافة الى تزايد انتشار التكنولوجيا مع الاستخدام المتزايد لها في حياتنا اليومية و التطور السريع للجرائم الالكترونية، لهذا أصبح من الضروري توعية الجمهور و تدريب الجهات المختصة على كيفية التعامل مع هذه الجرائم و الوقاية منه.

أهداف الدراسة:

الهدف من هذه الدراسة هو تسليط الضوء على اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال و المعلوماتية، وابراز خصوصيتها بالنسبة للجرائم التقليدية وتسهيل هذه الاجراءات وملائمة السياسات، وصولا الى تحقيق فعال في الجرائم المعلوماتية كذلك تهدف الدراسة الى فحص وتحديد العوامل المؤثرة في الوصول الى تحقيق جنائي ناجح والتغلب على الصعوبات والمعضلات التي تعترض طريقه.

الدراسات السابقة:

نظرا لحداثة الموضوع من خلال عملية البحث، التي قمنا بها عبر المراجع المتعلقة بالتحقيق في الجريمة المعلوماتية و من الدراسات السابقة التي تناولها فقد وجدنا اطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث تخصص قانون خاص للطالبة أومدور رجاء خصوصية التحقيق في مواجهة الجرائم المعلوماتية 2020-2021، و كانت الاشكالية حول تكريس المشرع الجزائري احكام قانونية تتلاءم مع خصوصية التحقيق لضمان فاعليته في مواجهة الجرائم المعلوماتية و الجد من آثارها، و يرى الباحث من خلال دراسته مكانة التحقيق في مواجهة الجرائم المعلوماتية و التعرض لمبادئ التحقيق و دور اجهزته في مكافحة هذه الجريمة، كذلك يوضح آليات التحقيق و دور التعاون الدولي في ذلك من اهمية عمل اجهزة التحقيق بشكل

متكامل و متناسق لضبط الدليل و تأمينه من التلف أو الضياع و استعمال اساليب و ادوات معينة، للوصول لمرتكب الجرائم المعلوماتية و عدم افلاتهم من العقاب ناهيك عن منع تفاقم الاجرام النظم العابر للحدود.

حيث التقينا مع الباحث في الفصل الاول في المبحث الاول في التطرق الاطار المفاهيمي في الجرائم المعلوماتية و خصوصية التحقيق فيها، أما ما يتعلق بالمبحث الثاني فقد اختلفنا في تحديات التحقيق في الجرائم المعلوماتية.

اطروحة دكتوراه في الحقوق، التحقيق الجنائي في الجرائم الالكترونية للباحث خالد على نزال الشعار، كلية الحقوق جامعة المنصورة حيث تطرق و كانت الاشكالية حول مفهوم التحقيق الجنائي في الجرائم المعلوماتية و كذلك مفهوم المحقق الجنائي لبيان ان التحقيق الجنائي لا يعني اسئلة تلقى و اجابات تدون و لكنه دراسة و دراسة و خبرة و صراع لكشف البيانات و رصد حركة الجريمة و القبض على مرتكبيها و استعمال طرق و وسائل محددة كفلها القانون لإجراء التحقيق من قبل المحقق الجنائي و بالتالي اسلوب تفكير المحقق الجنائي يجب ان يتغير و يتطور لمواجهة فكر و اسلوب المجرم الالكتروني للبحث و النقيب للوصول للكشف عن الجريمة المعلوماتية.

كما صدفنا الباحث في الفصل الأول في المبحث الثاني من ناحية صعوبات التحقيق في الجرائم المعلوماتية و مهارة و ذكاء المجرم الالكتروني في اكتشافه ،و اختلفنا في الفصل الثاني من ناحية انه توسع في دور المحقق في التحقيق للجرائم المعلوماتية، بينما نحن تطرقنا لآليات التحقيق و دور الدليل الرقمي في آليات الجرائم المعلوماتية.

صعوبات الدراسة:

لا يسعنا الا القول بأنه تلقينا بعض الصعوبات في اختيار موضوع البحث في حد ذاته و هذا راجع في الاساس الى أن بعض عناصره مستحدثة نتكلم عن الدليل الرقمي في اثبات الجريمة المعلوماتية في القانون

الجزائري مثلا الذي هو موضوع مستحدث و ما يتسم به من صبغة علمية بحثه جديدة و غريبة في تصورنا عن رجال القانون لم نيل حظه من البحث و التحميص على مستوى الفقه الجزائي، كما أن معظم الدراسات و الابحاث القانونية التي تناولت الجريمة المعلوماتية و بالأخص موضوعنا " التحقيق في الجريمة المعلوماتية ترتكز على الجانب الموضوعي فقط،و هذا ما نتج عنه ندرة و قلة المراجع و المؤلفات التي تعرضت للجانب الاجرائي اضافة الى ذلك ان الجرائم الالكترونية أو المعلوماتية ترتبط بالحاسب الالي مما يدعو الى المعرفة بمكوناته و بنظام المعالجة الالية للمعلومات و الشبكات الإلكترونية كما أن الامر يحتاج الى دراية كافية باللغة و المصطلحات التقنية و الفنية و هذا ما يتطلب تعب و جهد كبير و هذا ما أثار اهتمامنا في هذا البحث.

الاشكالية المطروحة:

انطلاقا مما سبق فان اشكالية هذه الدراسة تتمحور حول:

ما هو النظام القانوني للتحقيق في الجرائم المعلوماتية في التشريع الجزائري؟

رجوعا لصعوبة كشف المعلومات و البيانات لضبط الادلة و اثبات الدليل الرقمي في الجرائم المعلوماتية الغالبة حدود الدولة الواحدة و سرعة انتشارها و تنفيذها، و بذلك ينتج عدم ملائمة القوانين و الانظمة احيانا لبعض القضايا المطروحة في هذا المجال الواسع و المتطور للحد منها.

المنهج المتبع:

نظرا لطبيعة الاشكالية المطروحة و تحقيق للأهداف المسطرة فقد رأينا أنه من الانسب لهذه الدراسة هو الاعتماد على المنهج الوصفي الذي يتناسب و دراستنا التي تقوم على وصف التحقيق في الجرائم المعلوماتية، و المنهج التحليلي من خلال تحليل النصوص القانونية المتعلقة بالتحقيق في الجرائم المعلوماتية.

تقسيم الدراسة:

تم تقسيم البحث الى فصلين:

يتضمن (**الفصل الاول**) التحقيق كإجراء من اجراءات المتابعة بالجرائم المعلوماتية اذ يحتوي على مبحثين، (**المبحث الاول**) مفهوم التحقيق في الجرائم المعلوماتية، أما (**المبحث الثاني**) فيتضمن الاجهزة المكلفة بالتحقيق في الجرائم المعلوماتية، و(**الفصل الثاني**) معنون بآليات التحقيق في الجرائم المعلوماتية، والذي بدوره يحتوي على مبحثين يتمثل (**المبحث الاول**) في اجراءات التحقيق في الجرائم المعلوماتية و(**المبحث الثاني**) يشمل الدليل الرقمي كوسيلة لإثبات الجريمة المعلوماتية.

الفصل الأول: التحقيق كإجراء من اجراءات المتابعة في الجرائم المعلوماتية

ان التحقيق في الجرائم المعلوماتية يعد اجراء من الاجراءات التابعة لها نظرا لاستحداث هذا النوع من الجرائم و تشكلها أخطار جسمية، التي تضر المجتمع باعتبار الجريمة المعلوماتية ظاهرة اجرامية مستحدثة في عصرنا الحديث و ارتباطها بالتكنولوجيا و وسائل التقنيات الحديثة من اجهزة الكمبيوتر و الانترنيت و المواقع الالكترونية فقد ترتب على ذلك احاطة هذه الظاهرة الكثير من الغموض الذي امد التحقيق اهمية كبيرة لإثبات وقوع الجرائم ،فيعد ضمان و حماية لحقوق الفرد في الخصوصية المعلوماتية اذ يتمثل في مرحلة جمع الإستدلالات، و ذلك بدورها مرحلة هامة في سبيل البحث و التحري في هذه الجريمة، اثر ان التحقيق المعلوماتي يواجه صعوبات قد ترجع لطبيعة الجريمة المعلوماتية أو الى الأجهزة المكلفة به[1].

و على ضوء ذلك سيتم تقسيم هذا الفصل تحت عنوان مفهوم التحقيق في الجرائم المعلوماتية أما المبحث الثاني فيتمثل في الأجهزة المكلفة به.

[1] -بوبعاية ابتسام، "التحقيق في الجريمة الالكترونية"، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، كلية الحقوق، جامعة محمد البشير الابراهيمي-برج بوعريريج، 2021-2022، ص 20.

المبحث الأول: مفهوم التحقيق في الجرائم المعلوماتية

التحقيق هو سلسلة من الاجراءات القانونية لكشف الجرائم المعلوماتية و يعتبر مرحلة ابتدائية في جمع الأدلة بهدف التنقيب عنها لكشف الحقيقة بما في ذلك من خصائص و صعوبات في هذا الأمر اذ يكون التحقيق في الجريمة المعلوماتية تحقيقا جنائيا معلوماتيا باعتبار مسرح و محيط هذه الأخيرة هو الفضاء الالكتروني و البيانات التقنية[1].

و من خلال هذا المبحث سنتطرق لمقصود التحقيق في الجريمة المعلوماتية من الناحية الفقهية و القانونية في المطلب الأول لذلك خصوصية التحقيق في الجرائم المعلوماتية و ذلك في المطلب الثاني.

المطلب الأول: المقصود بالتحقيق للجريمة المعلوماتية.

يعتبر التحقيق العلم الذي يضم مجموعة من الاجراءات النظرية و العلمية التي يقوم بها محقق هيئة و الادعاء العام بما يوصلهم لكشف الجريمة المعلوماتية و توفير الادلة الرقمية ضد مرتكبيها و تقديمهم للعدالة لمحاكمتهم[2]، و سنعرف في الفرع الاول الجريمة المعلوماتية فقهيا و في الفرع الثاني التعريف القانوني لها.

الفرع الأول: التعريف الفقهي للجريمة المعلوماتية.

لا يوجد تعريف متفق عليه بين فقهاء القانون نتيجة اختلاف المصطلح المستخدم حيث هناك من يعرفها بأنها الاستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات[3]. و يعود ذلك الاختلاف حول تحدي نطاق هذه الجريمة فالبعض من الفقهاء ينظر اليها بمفهوم ضيق و البعض الاخر ينظر اليها بمفهوم موسع[4].

[1] – أحمد فاروق زاهر، "التحقيق الجنائي في الجريمة الالكترونية"، البحث مقدم لاستفاء متطلبات الحصول على درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة، د س، ص 4.

[2] – المرجع نفسه، ص4.

[3] –جدي نسيمة، "جرائم المساس بأنظمة المعالجة الالية للمعطيات"، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2013-2014، ص8.

[4] –نايري عائشة، "الجريمة الالكترونية في التشريع الجزائري"، مذكرة لنيل الماستر في القانون الاداري، جامعة أحمد دراية–أدرار–،2016-2017، ص 6.

حيث يتمثل الاتجاه الضيق لتعريف الجريمة المعلوماتية ان انصاره فسرها على انها كل فعل مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم ارتكابه من ناحية لملاحقته و تحقيقه من ناحية اخرى، بنتيجة هذا ان يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة، و المختصين بملاحقتها من قضاة ضباط الشرطة و غيرهم، و هناك من يعرفها على أنها الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الاجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية[1] .

كما يرى الاستاذ TREDMANN أن الجريمة المعلوماتية تشمل اي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات[2].

و الاستاذ ROSENBLATT بأن الجريمة الالكترونية هي نشاط غير مشروع موجه لنسخ أو الوصول الى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه[3].

و من هذه التعاريف فان الأفعال غير المشروعة التي تستخدم فيها الحاسب لآلي كأداة لارتكابها تخرج من نطاق التجريم، و يرى الاستاذ باركاران الجريمة الالكترونية هي كل فعل اجرامي متعمد أيا كانت صلته بالمعلوماتية ينسأ عنه خسارة تحق بالمجني عليه أو كسب يحققه الفاعل[4]. أما بالنسبة للاتجاه الموسع للتعريف عكس الاتجاه السابق حيث يرى فقهاء آخرون ضرورة التوسيع من مفهوم هذه الجريمة و يبقى الهدف واحد و هو الكشف عن قضايا مستتر عليها، او نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب[5].

---

[1] -نايري عائشة، مرجع سابق،ص6.

[2] -حمزة بن عقون، "السلوك الاجرامي للمجرم المعلوماتي"، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الاجرام و العقاب ،جامعة باتنة، 2011-2012 ص14 .

[3] -حمزة بن عقون، المرجع نفسه ص15.

[4] -حسن الطوالة،" الجرائم الالكترونية"، ط1، جامعة العلوم التطبيقية، مملكة البحرين، 2008،ص48.

[5] -سميرة بيطام، الجريمة الالكترونية و تقنية الاجرام المستحدث، ص4/1، الموقع: https://www.alukah.net ،تاريخ الاطلاع :05-04-2024،الساعة:04:15.

كما عرفها الاستاتذة (lestanc) و (vivant) انها: مجموعة من الافعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب. كما أن الخبير الامريكي (parkee) تبني مفهوما واسعا للجريمة المعلوماتية على أنها كل فعل اجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل[1].

و حسب تعريف منظمة التعاون الاقتصادي و التنمية (OCDG) بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، كما تعرف ايضا: "تلك الجرائم المرتبكة ضد الاملاك باستعمال التقنية أو المعلوماتية" [2].

الفرع الثاني: التعريف القانوني للجريمة المعلوماتية.

أجذ المشروع الجزائري الجريمة المعلوماتية بتسميتها الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و عرفها بموجب احكام المادة 02 من القانون رقم 09-04 [3] على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و اي جريمة ترتكب أو يسها ارتكاب عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية".

و حسب المشروع الجزائري فانه قد تتحقق الجريمة الالكترونية بمجرد أن ترتكب الجريمة أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما ان التعريف تضمن تكرار كون ان مفهوم نظام الاتصالات الالكترونية يندرج ضمن مصطلح المنظومة المعلوماتية[4].

---

[1] -نهلا عبد القادر المومني، "الجرائم المعلوماتية"، دار الثقافة للنشر والتوزيع، عمان، 2008، ص49 .

[2] -بعرة سعيدة، "الجريمة الالكترونية في التشريع الجزائري"، (دراسة مقارنة)، مذكرة مكملة من مقتضيات نيل شهادة الماستر ،كلية الحقوق و العلوم السياسية، جامعة محمد خضير، بسكرة، 2015-2016، ص10.

[3] -القانون رقم 09- 04، مصدر سابق.

[4] -سوير سفيان، "جرائم المعلوماتية"، مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الاجرام، جامعة ابو بكر بلقايد، تلمسان، 2010-2011 ،ص ص: 14-16.

و نستنتج من هذا التعريف ان المشروع الجزائري اعتمد على معيار الجمع من عدة معايير لتعريف الجريمة المعلوماتية مثل معيار وسيلة الجريمة و معيار موضوع الجريمة و ايضا معيار الواجب التطبيق للجريمة المنصوص عليها في قانون العقوبات و كما حدد نطاق الجريمة الالكترونية و ذلك توضيحه بأنها ترتكب في نظام معلوماتي مما يعني سهولة ارتكابها و هذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري[1].

المطلب الثاني: خصوصية التحقيق في الجرائم المعلوماتية.

ان أهمية التحقيق في الجرائم المعلوماتية لها أهمية بالغة في الجريمة اذ ان خصوصيتها قد تنعكس على اجراءات التحقيق فمن ناحية تعتبر عنصر لا غنى عنه لمباشرة الاجراءات الجزائية، و من ناحية قد يستصعب الوصول اليها غير الملموسة و لطبيعة الدليل المستمد منها[2]. قسمنا هذا الفرع الى اثنان و ذلك للتعرف على خصائص الجريمة المعلوماتية اولا و خصائص التحقيق فيها ثانيا.

الفرع الأول: خصائص التحقيق في الجريمة المعلوماتية.

أولا: خصائص الجريمة المعلوماتية.

- **الجرائم المعلوماتية عابرة للحدود الوطنية (ذات طابع دولي):**

الجرائم المعلوماتية ذات طابع دولي لا تعرف الحدود و تنتشر بسرعة كبيرة و تنتقل البيانات و المعلومات و الأموال مما ينتج عنها صعوبات في اجراءات التحقيق لمرتكبي الجرائم المعلوماتية، و يتطلب تضافر الجهود الدولية في تنظيم أطر المواجهة و التعاون الدولي[3].

[1] –اسمهان بوضياف ، الجريمة الالكترونية و الاجراءات التشريعية لمواجهتها في الجزائر، مجلة الاستاذ الباحث للدراسات القانونية و السياسية،العدد11، سبتمبر، مسيلة، 2018 ،ص353.

[2] –د/عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية ، مجلة الباحث الأكاديمي في العلوم القانونية ،المركز الجامعي بأفلو / الاغواط، العدد السادس(6)، مارس، 2021 ،ص135.

[3] –رامي متولي القاضي ، مكافحة الجرائم المعلوماتية في التشريعات المقارنة و في ضوء الاتفاقيات و المواثيق الدولية، دار النهضة العربية ،ط1، مصر، 2011، ص53.

- **الجرائم المعلوماتية تتسم بالجاذبية:**

ان سوق المعلومات و البيانات و الانترنيت أصبح مصدر لتبيض الأموال فهي بذاتها ثروة كبيرة للمجرم المعلوماتي و لانتشار الاجرام المنظم حيث يتم توظيفها في تطوير تقنيات و أساليب تمكن الدخول الى الشبكات و سرقة معلوماتها أو اعتراض العمليات المالية و تحويل مسارها و غيرها[1].

- **الجرائم المعلوماتية مرنة لها سلبيات وخيمة:**

تتميز الجرائم المعلوماتية بغموض غير الجرائم التقليدية مما يصعب اكتشافها و ضبط مرتكبيها و محاكمتهم و قد يتم تدمير المعلومات التي من الممكن ان تستخدم كدليل اثبات في مدة لا تقل عن ثانية واحدة و تتسبب هذه الجرائم في اضرار جسمية و تشكل اضرار جسمية و من بينها تداخل الحاسب الالي في بيئة الاعمال التجارية و المعاملات في القطاع العام و الخاص و ايضا سوء استخدام الحاسب الالي في نشر الفيروسات الضارة و تقسيم المعلومات الارهابية و كذلك عدم الاستقرار السياسي فب العالم خاصة في الدول المتقدمة التي تعتمد كليا على التقنيات العالية[2].

كما يوجد خصائص يتميز بها المجرم الالكتروني في معظم الاعمال الاجرامية المنظم و المخطط القيام بها في عالم الشبكات الالكترونية فالمجرم الالكتروني يقوم بواجباته و يمارس حقوقه الاجتماعية و السياسية دون اي عائق في حياته اليومية اذ تعتبر هذه الخاصية امتداد سمة التخطيط و التنظيم حيث ان التكيف الاجتماعي ينشأ من مجموعة لها صفات مشتركة و تجمعهم روابط تساعدهم على ارتكاب الجريمة و قد تتعدى هذه الروابط النطاق المحلي حتى تنتشر على النطاق الدولي.[3]

---

[1] –اسراء جبريل رشاد مرعي، الجرائم الإلكترونية " الاهداف –الاسبال– طرق الجريمة و معالجتها" ،المركز الديمقراطي العربي للدراسات الاستراتيجية و الاقتصادية و السياسية، ألمانيا ،2016 بحث منشور على الموقع: https://democraticac.de/p35426 ، تاريخ الاطلاع :5-5-2024، الساعة 21:55.

[2] –محمد الامين البشري، "التحقيق في الجرائم المستحدثة"، ط1، مركز الدراسات و البحوث، الرياض، 2004 ،ص82 .

[3] –د/ خضري محمد،" مدخل للإجرام الالكتروني"، مطبوعة مقدمة لطلبة السنة الثانية ماستر، تخصص اعلام الي انترنيت ،كلية الحقوق و العلوم السياسية ،جامعة محمد البشير الابراهيمي ،برج بوعريريج ،2022-2023 ،ص 25 .

و يعرف المجرم الالكتروني بذكائه و مهارته في ارتكاب جرائمه فالجريمة المعلوماتية جريمة الاذكياء مقارنة بالجريمة التقليدية التي يكون فيها الميل للعنف ذلك ان تنفيذها يعتمد على المهارة في مجال تقنية الحاسوب و الانترنيت التي يكتسبها عن طريق الخبرة و يسعى المجرم الالكتروني دائما الى معرفة طرق جديدة و مبتكرة لا يعرفها أحد سواه من اجل اختراق الحواجز الامنية في البيئة الالكترونية و نيل مبتغاه.[1]

الاجرام الالكتروني ينشأ من تقنيات التدبير الناعمة اي ان يقوم المجرم الالكتروني بالتلاعب في بيانات و برامج الحاسوب لكي يمحو هذه البيانات او ان يعطل استخدام البرامج و ما عليه اللجوء الا لزرع الفيروسات في هذه البرامج لكي يعيق حركة النظام الالكتروني و يجعله غير قادر على القيام بوظائف الطبيعية قد يصل للاحترافية في الاجرام مما يشكل خطر كبيرا على المجتمع سواء كان فرد أو مجموعة منظمة. [2]

و ينشأ تطور في السلوك الاجرامي حيث يساهم وجود المجرم الالكتروني في جماعة اجرامية الى سرعة اكتساب المهارة التقنية التي تؤدي به الى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة لغاية الوصول لأعلى معدلات المهارة التقنية المتمثلة في اثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة. [3]

حيث يمكن تحديد أنواع من المجرمين منها المختصون في انشاء و تعديل البرمجيات و العتاد الحاسوبي ولهم المعرفة التقنية في مجال المعلوماتية و هم ما يسمى بالهاكرزّ أي صغار نوابع المعلوماتية و الاستماع باللعب و المزاح باستخدام هذه التقنية لاثبات قدراتهم و باكتشاف مواطن الضعف في الانظمة المعلوماتية دون الحاق ضرر بها و لديهم الرغبة في المغامرة و التحري و الاكتشاف و في الوقت الذي كثر فيه الحديث عن مخاطر هذه الفئة ظهرت مؤلفات و دراسات تخرج هذه الفئة من دائرة الاجرام الى دائرة العبث.[4]

---

[1] –سمية مزغيش، "جرائم المساس بالأنظمة المعلوماتية"، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي ،جامعة محمد خضير، بسكرة، 2013-2014 ،ص 20.

[2] –خضيري محمد، مرجع سابق، ص 25.

[3] –خضيري محمد، المرجع نفسه، ص 23.

[4] –خضيري محمد، المرجع نفسه، ص ص: 24-25.

وما يسمى بالكراكرز وهو المقتحم يكون من فئة المجرمين البالغين و اعمارهم تتراوح بين 25-45 من مميزاتهم انهم ذوي مكانة في المجتمع و من اهل الاختصاص في مجال التقنية الالكترونية ويتمتعون بمهارات فنية في مجال الانظمة تمكنهم من السيطرة الكاملة في مجال المعالجة المعلوماتي. [1]

و من هم من اشخاص لهم ميول و دوافع سياسية معينة تدفعهم لاختراق نظم الحاسب الالي غير المصرح بالدخول اليها و تحتوي على بيانات و معلومات غاية في السرية تتعلق بالدفاع و الامن الوطني.[2]

و ايضا طائفة الحاقدون لهم الرغبة في الانتقام من صاحب العمل الامر الذي يحرك نشاطهم او لتصرف معين قد لا يكونوا موظفين و ينتقم لمستخدمي للنظام بوصفهم موظفين او مشتركين بالنظام محل الجريمة و الى غرباء عن النظام تتوفر لديهم أسباب الانتقام من النشأ المستهدفة في نشاطهم و تتصف هذه الطائفة بالإلمام بالمعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه و يستخدمون تقنيات الفيروسات و البرامج و تعطيل النظام أو الموقع المستهدف ان كان من مواقع الانترنيت و تكون أعمارهم مختلفة و غياب عنصر التفاعل بين اعضاء هذه الطائفة و هم الاسهل من حيث اكتشاف انشطتهم لتوفر ظروف و عوامل على ذلك.[3]

الاحتراف من الناحية الاجرامية المعلوماتية يمكن المجرم من الوصول الى اهدافه باستخدام ما لديه من علم يطورونه باستمرار و هدفهم سحب الاموال من الارصدة و نيتهم احداث التخريب.[4]

يميل المجرم الالكتروني للتقليد و تأثيره بغيره و يبين ذلك من محاولة الفرد تقليد غيره بالمهارات الفنية مما يؤدي به الامر الى ارتكاب الجريمة و ذلك لعدم الاستواء في شخصية الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط و ينتهي به الامل الى التقليد و ارتكاب الجريمة.[5]

---

[1] -محمد علي العريان، "الجرائم المعلوماتية"، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص 64 .

[2] -نايري عائشة ، مرجع سابق، ص 23.

[3] -سمية مزغيش، مرجع سابق، ص ص: 23-24.

[4] -نايري عائشة، مرجع سابق، ص 26.

[5] -سمية مزغيش ، مرجع سابق، ص ص: 20-21.

يتصف المجرم الالكتروني بالخوف من كشف جريمته بصفة خاصة مما يكتشف أمره من ارتكاب مالي و فقد المركز الوظيفي في كثير من الاحيان كما ان طبيعة الانظمة المعلوماتية نفسها تساعد الجاني على الحفاظ على سرية أفعاله ذلك ان كثير ما يعرض المجرم الى اكتشاف امره و هو ان يطرأ تنفيذ جريمته عوامل غير متوقعة في حين أن أهم الاسباب التي تساعد على نجاح الجريمة المعلوماتية هي الحواسيب انما تؤدي عملها غالبا بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها اي من العمليات التي يقوم بها مرة اخرى.[1]

الرغبة في تحقيق الشراء السريع عن طريق اتاحة الاطلاع على معلومات معينة اساسية و ذات اهمية خاصة لمن يطلبها و تتعدد الاساليب اللازمة للوصول الى هذا الهدف المنشود و لذلك فان هذا السبب يعد من أكثر الاسباب التي تدفع الى انتشار الاجرام الالكتروني و تبرز الحاجة الى تحقيق الكسب السريع نتيجة وقوع البعص تحت ضغوط معينة.[2]

ثانيا: خصائص التحقيق في الجريمة المعلوماتية.

- التحقيق عموما هو علم يخضع لما يخضع له سائر انواع العلوم الاخرى فله قواعد ثابتة و راسخة اما قانونية او فنية فالأولى لها صفة الثبات الشرعي لا يملك التحقيق ازائها شيئا سوى الخضوع و الامثال، اما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته و فطنته و مهارته الكثير فبدونها لما كان للتحقيق هذه الميزة.[3]

- التحقيق هو الاجراء الذي يقوم به المحقق و التي تؤدي لاكتشاف الجريمة و معرفة مرتكبيها تمهيدا لتقديمهم الى المحاكمة و تتمثل هذا في مجموعة اجراءات كعملية التفتيش او برمجية كتحديد كيفية الدخول للمعطيات المخزنة في النظام المعلوماتي و هدفه التأكد من وقوع جريمة يعاقب عليها

---

[1] -نايري عائشة ، مرجع سابق ، ص ص: 18-19.

[2] -محمد علي العريان، مرجع سابق ، ص 66.

[3] -خالد ممدوح،" فن التحقيق الجنائي في الجرائم الالكترونية"، دار الفكر الجامعي، الاسكندرية، 2010، ص 56.

القانون و معرفة هذه الجريمة و نوعيتها و طرفيها (الجاني و المجني عليه) كذلك معرفة وقوعها و وسائل التي استعملت في ارتكابها و كل ما يتعلق بها وفق لمنهج تحقيق يختلف عن غيره بالنسبة للجرائم الاخرى.[1]

- وضع خطة عمل للتحقيق بتجميع الاستدلالات و تحديد فريق في لازم القيام بمعاينة مسرح الجريمة للتخطيط الفني للتخطيط و تسهيل المهمة لضمان مستوى جيد من الاداء.[2]
- وجوب التركيز على خطة العمل على مجموعة بنود أساسية التي يتم الارتكاز عليها أثناء تنفيذ الخطة التي تعتمد على تعيين الاشخاص الذين سيقدم التحقيق معهم و تحديد النقاط التي يجب استضامها معهم و تقدير مدى الخاصة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق و يجب مراعاة مدى أهمية الاجهزة و حساسية البيانات التي يتحمل سرقتها أو اتلافها و أيضا مستوى الاختراق الامني التي تسبب فيها الجاني و ثم وضع الاسلوب الامثل للتفتيش و ذلك من خلال وضع نوع الادلة التي يرد فريق التحقيق البحث عنها.[3]

- تشكيل فريق التحقيق من فنيين و أخصائيين ذوي خبرة في مجال الحاسوب و الانترنيت يمتازون بمهارات في التحقيق الجنائي بشكل عام و التحقيق الالكتروني بشكل خاص لهؤلاء المحققين ان يستعينوا بخبراء في مجال الحاسوب و الانترنيت ليتمكنوا من فك التعقيدات التي تفرضها ظروف و ملابسات كل جريمة [4]
- اشار المشروع الجزائري لإمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المختصين في مجال الحاسوب و النظم المعلوماتية و الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية و ذلك بغرض مساعدة جهات التحقيق في انجاز مهمتها و تزويدها بالمعلومات الضرورية لذلك.[5]

---

[1] -خالد ممدوح مرجع سابق، ص11.

[2] -بوبعاية ابتسام، مرجع سابق، ص22.

[3] -خالد ممدوح مرجع سابق، ص11.

[4] -بوبعاية ابتسام مرجع سابق، ص24.

[5] -المادة 50، الفقرة الاخيرة من القانون 09-04، مصدر سابق.

الفرع الثاني :صعوبات التحقيق في الجرائم المعلوماتية.

يواجه التحقيق في الجريمة المعلوماتية صعوبات لاكتشافها و اثباتها حق ان الوصول لنتيجة في بعض الحالات تكون قليلة اذا قورنت بما يتم اكتشافه من الجرائم التقليدية و يمكن رد الاسباب التي تقف وراء صعوبة في اكتشاف الجريمة الالكترونية و اثباتها الى عدة عوامل منها:[1]

أولا: ان الجريمة الالكترونية لا تترك آثار مادية، فهي جريمة تقع في بيئة الكترونية يتم فيها نقل المعلومات و تداولها بالنبضات الالكترونية و لا توجد مستندات ورقية، فهذه الجريمة عبارة عن ارقام تتغير في السجلات فالجريمة الالكترونية لا تترك شهودا يمكن استجوابهم و لا أدلة يمكن فحصها[2].

ثانيا: صعوبة الاحتفاظ بدليل الجريمة الالكترونية أذ يستطيع المجرم في أقل من ثانية أن يمحو أو يحرف أو يغير المعلومات الموجودة في الكمبيوتر[3].

ثالثا: لاكتشاف و التحقيق في الجريمة المعلوماتية يلزم خبرة فنية حيث تتطلب جريمة الكمبيوتر المام و معلومات واسعة سوداء لارتكابها أو التحقيق فيها، كما ان رجال الضبطية القضائية يجدون صعوبة للتعامل مع الدليل الالكتروني و قد يتسبب المحقق دون قصد في اتلاف الدليل الالكتروني أو تدميره، كما في حالة محو البيانات الموجودة على الاسطوانة الصلبة أو قد لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو الطابعة أو الماسح الضوئي، لذلك أصبح من الضروري في وقتنا اجراء دورات تدريبية لرجال الضبطية القضائية و رجال القضاء و الخبراء و الفنيين للتعاون فيما بينهم وصلا الى أحسن الطرق لمكافحة الجريمة الالكترونية [4].

---

[1] -ثنيان ناصر آل ثنيان، "اثبات الجريمة الالكترونية دراسة تأصيلية تطبيقية"، رسالة ماجستير، كلية الدراسات العليا قسم العدالة الجنائية ،جامعة نايف العربية للعلوم الامنية الرياض، 2012 ،ص24.

[2] -ليبيات خولة، عميرات أميرة، "الاثبات في الجريمة الالكترونية"، مذكرة مكملة لنيل شهادة الماستر الاكاديمي، جامعة محمد بوضياف، المسيلة، 2021-2022، ص13.

[3] -حسن فريحة، الجرائم الالكترونية و الانترنت، مجلة المعلوماتية، ع36، اكتوبر ،2011 ،ص3.

[4] -ليبيات خولة، عميرات أميرة ، مرجع سابق، ص14.

رابعا: للتعرف على مرتكبي الجريمة المعلوماتية يعتمد على اسلوب الخداع و الذكاء لاكتشافها و ذلك بإحجام البنوك و الشركات و مؤسسات الأعماء عن الابلاغ عما يرتكب من جرائم تجنبا للإساءة الى سمعتها و هز ثقة العملاء بها و اخفاء اسلوب ارتكاب الجريمة لعدم قيام الآخرين بتقليد هذا الأسلوب و هو ما يدفع المعني عليه الى الاحجام عن ابلاغ السلطات المختصة بها و هذا لان الجريمة المعلوماتية هي جريمة فردية أساسها مهارات عالية و إلمام بتكنولوجيا النظم المعلوماتية[1].

خامسا: صعوبة فحص و دراسة الكم الهائل للبيانات و المعلومات و التي قد تعيق عملية الاثبات في الجرائم المعلوماتية بهدف استخلاص دليل الجريمة حيث أن طباعة كل ما هو موجود في الدعامات الممقطة قد يتطلب مئات الالاف من الصفحات و في نفس الوقت قد لا تقدم هذه الاخيرة اية فائدة للتحقيق و لذلك على السلطات القائمة بالضبط و التحقيق ان لا تتمتع بالخبرة الفنية في مجال الحاسب الالي فقط و انما لا بد ان تمتلك هذه السلطات ايضا القدرة على فحص الكم الهائل من المعلومات و البيانات المخزنة على الانظمة المعالجة الالية.[2]

سادسا: استخدام المجرم المعلوماتي لشبكة الانترنيت بإخفاء هويته عن طريق استخدام بعض البرامج او التطبيقات التي تعمل على طمس الهوية مما يشكل صعوبة كبيرة امام المحققين أو القضاء لاستخلاص الادلة الجنائية الرقمية كذلك قد يلجأ الجناة الى اخفاء المعلومات او البيانات و هو ما يجعل عملية بناء الادلة الرقمية او استرجاعها امر في غاية الصعوبة امام الخبير.[3]

سابعا: قلة خبرة المحققين و الخبراء في الجرائم المعلوماتية و ذلك راجع كون الجريمة المعلوماتية دائمة التطور و بشكل سريع حيث ان مرتكبيها يتبعون كل جديد و يعملون على تطوير سبيل اخفاء أدلة جرائمهم و من هذا المنبر يتوجب على المحقق ان يكون على دراية ثانية بكل هذه التطورات المتعلقة

[1] -حسن فريحة، مرجع سابق ،ص3 .

[2] -بلينة حبيباتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الانسانية ،المجلد أ ،العدد 50 ،كلية الحقوق، جامعة الجزائر 1، ديسمبر، 2018 ،ص 89 .

[3] -منصور عبد السلام عبد الحميد حسان العجيل، "الضوابط القانونية لاثبات الجنائي بالأدلة الرقمية (دراسة مقارنة)"، المجلة القانونية (مجلة متخصصة في الدراسات و البحوث القانونية)، المجلد 9، ع 10،2021، ص 3400.

بجرائم الحاسوب و الانترنيت جراء عدم التدريب اللازم و المستمر ليواكب تطور هذه الجرائم من حيث الوحدات المتخصصة للمكافحة و التحقيق من ضمن مكتب التحقيقات الفيدرالية **و** من ناحية الاجهزة و المعدات و برمجيات متحدثة تساعد في اجراءات التحقيق و في فحص الاجهزة المضبوطة في الجريمة و المحافظة على الادلة.[1]

ثامنا: ضعف التعاون الدولي لمكافحة الجريمة المعلوماتية التي تخترق كل الحدود الاقليمية المعمول بها، كان من اللازم تفعيل سياسة التعاون الدولي و التنسيق بين الدول من اجل مكافحتها و اثباتها و جعل هذا التعاون صعبا من جهة الانظمة القانونية الكثيرة بين الدول و لا يوجد اتفاق موحد حول نماذج اساءة استخدام نظم المعلومات و شبكة الانترنيت الواجب تجريمها ومن جهة عدم وجود تنسيق في النظام الاجرامية أو معاهدات ثناية أو جماعية بين الدول باعتبار المعاهدات تبقى قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم برامج الحاسب و شبكة الانترنيت الذي قد يؤدي الى ارباك المشرع الوطني و ينعكس بشكل سلبي على التعاون الدولي في مجال جمع و تبادل الادلة الجنائية الرقمية.[2]

تاسعا: تثير مشكلة الاختصاص الجرائم المعلوماتية على المستوى الدولي عكس المستوى الوطني او المحلي الذي يتم الرجوع فيه الى المعايير المحددة قانونا لذلك بحيث تثار المسألة بالنسبة للاختصاص على المستوى الدولي من حيث اختلاف التشريعات و النظم القانونية و التي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالأنترنيت التي تتميز بكونها عابرة للحدود فقد يحدث ان ترتكب الجريمة في اقليم دولة معينة من قبل اجنبي فهنا تكون الجريمة خاضعة للاختصاص الدولة الثانية على اساس مبدأ الاختصاص الشخصي في جانبه و قد تكون هذه الجريمة من الج رائم التي تهدد امن دولة احرى فتدخل عندئذ في اختصاصها استناد الى مبدأ العينة.[3]

---

[1] -ليبيات خولة، عميرات أميرة، مرجع سابق ، ص 57.

[2] - ليبيات خولة، عميرات أميرة، المرجع نفسه، ص ص: 58-59.

[3] -بدري فيصل، "مكافحة الجرائم المعلوماتية في القانون الدولي و الداخلي"، اطروحة لنيل شهادة دكتوراه، قانون عام ،كلية الحقوق جامعة الجزائر 01 ،بن يوسف بن خدة ،2017-2018 ،ص113 .

المبحث الثاني: الاجهزة المكلفة بالتحقيق في الجرائم المعلوماتية.

ان أجهزة التحقيق المتخصصة بالتحقيق في الجرائم المعلوماتية تسعى إلى توكيل مهمة التحقيق الجنائي إلى فريق مختص من أصحاب الخبرة الفنية والكفاءة المهنية بغية الحصول على نتائج اكيدة ودقيقة وذات قيمة تفيد في مجريات سير الدعوى ، سنتطرق في هذا المبحث الى مطلبين الأول "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال "والثاني "الوحدات التابعة لسلك الامن و الدرك الوطني".

المطلب الاول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال.

حسب المادة 13 من القانون 09-04 المؤرخ في 5 اوت 2009 و المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحها تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها [1]،و نص المشرع الجزائري في المادة 14 من نفس القانون على ضرورة انشاء هيئة ذات وظيفة تنسيقية تعمل على اتخاذ التدابير والإجراءات اللازمة للوقاية من الجرائم الإلكترونية بالإضافة إلى تقديم المساعدة إلى الجهات القضائية المختصة في التحقيقات التي تجريها في هذا النوع من الجرائم.[2] و سنعرف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال في الفرع الاول و مهامها طبيعة عملها في الفرع الثاني.

الفرع الأول: التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال هي مؤسسة عمومية ذات طابع إداري بمعنى أن المشرع فيما يخص هذه الهيئة لم يتوجه إلى اعتبارها سلطة إدارية مستقلة على غرار الهيئة الوطنية للوقاية من الفساد ومكافحته وبالرغم من أن المشرح أخذ يعبر عن الأجهزة تارة بمصطلح "سلطة وتارة أخرى يصطلح هيئة وهذا يؤدي الى خلق فوضى في كيفية التعبير عن هذه المصطلحات،

[1] -المادة 13 من القانون 09-04، مصدر سابق.

[2] - المادة 14 من القانون 09-04، مصدر سابق.

وبعيدا عن هذا الخلط في المصطلحات وما يهم هو أن المشرع لم يضم الهيئة إلى فئة السلطات الإدارية المستقلة[1] وستعرف في هذا الفرع على أولا على الاعتراف بالشخصية المعتوية للهيئة وثانيا على نتائج الاعتراف بالشخصية المعنوية:

اولا : الاعتراف بالشخصية المعتوية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

تعتبر الشخصية المعنوية التي تتمتع بها السلطات الإدارية المستقلة ليست معيارا حاسما و دقيقا لقياس مدى الاستقلالية، إذ نجد أن المشرع اعترف للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بعبارة "... تتمتع بالشخصية المعنوية والاستقلال المادي"[2] وهذا على عكس الهيئات الأخرى.

حيث تعتبر الشخصية الاعتبارية داعمة لعملية تخصيص وتنظيم المهام والاختصاصات الإدارية بين مختلف أجهزة ومؤسسات الإدارة العامة في الدولة، ويتكون مفهومها من مجموعة من المفاهيم ويطرح عدة اجتهادات مختلفة حسب أبعاد تشريعات كل دولة، وقد أكد جماعة من الفقهاء على وجودها و ضرورتها و مهم من رفقها ولم يقبلها، ورغم وجود تعارضات قانونية في مفهومها إلا أنه يمكن القول إن الشخصية الاعتبارية هي مجموعة أشخاص أو أموال يعملان ويتعاونان معا لتحقيق المصالح والأهداف خلال فترة زمنية محددة مما يجعل هذه المجموعة من الأشخاص أو الصاديق جماعة جماعية مستقلة أن الأفراد والمصالح الفردية .[3]

---

[1] -سهيلة بوزبرة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام و الاتصال بين سرية المعطيات الشخصية الالكترونية و مكافحة الجرائم الالكترونية"، المجلة النقدية للقانون و العلوم السياسية كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، مجلد17، ع2، 2022، ص 563.

[2] -المادة 02 من المرسوم الرئاسي 20-183، مؤرخ في 21 ذو القعدة 1441 الموافق ل 13 يوليو 2020، المتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، ج ر ج ج،ع 40، الصادر في 18 جويلية 2020.

[3] -سهيلة بوزبرة، مرجع سابق، ص 564.

ثانيا: نتائج الاعتراف بالشخصية المعنوية للهيئة الوطنية للوقاية من الجرائم.

و للاعتراف بالشخصية الاعتبارية نتائج هامة اشارت اليها المادة 50 [1] من القانون المدني و هي :

- ذمة مالية.
- أهلية في الحدود التي يعينها عقد انشاء أو التي يقررها القانون .
- موطن و هو المكان الذي يوجد فيه مركز ادارتها.
- الشركات التي يكون مركزها الرئيسين في الخارج و لها نشاط في الجزائر يعتبر مركزها في نظر القانون الداخلي في الجزائر .
- نائب يعبر عن ادارتها.
- حق التقاضي .

من خلال تحليل المادة أعلاه نلاحظ ان المشرع يعترف للشخص الاعتباري تقريبا بنفس المميزات و الخصائص التي يعترف بها الشخص الطبيعي دون التغاضي عن اختلافهما من حيث الطبيعة فالخصائص التي تميز شخص الانسان لا يمكن الاعتراف بها للشخص المعنوي، و سنفصل أكثر في هذه النتائج من خلال ما يلي:

- **الأهلية:**

سواء كانت أهلية أداء أو أهلية وجوب و على اعتبارها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال شخص اعتباري فتكون لها أهلية الحدود و التصرفات التي يقررها القانون لذا يكون لها الحق في التعاقد، فتتمتع بحق ابرام العقود لممارسة نشاطها دون الحاجة الى اصدار اذن أو وثيقة رسمية لاثبات التعاقد[2].

- **الموطن:**

هو المكان الذي تستقر فيه، حيث نصت المادة 3 من المرسوم الرئاسي 15-261 و المرسوم 19-172 و المرسوم 21-439 يحدد مقر الهيئة بمدينة الجزائر و يمكن نقله الى اي مكان آخر في التراب الوطني بموجب مرسوم رئاسي، و تكمن أهمية الموطن في الاختصاص القضائي و تحديد المجال

[1] – المادة 50 من الامر 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، ج ر ج ج،ع 78، 1975.

[2] –بعلي محمد الصغير، القانون الاداري : التنظيم الاداري، النشاط الاداري، دار العلوم للنشر و التوزيع، عنابة، 2004، ص 41.

الجغرافي لممارسة حق التقاضي.[1]

- **حق التقاضي:**

للهيئة الحق في اللجوء الى القضاء بصفة مدعية أو مدعى عليها حيث نصت المادة 10 من المرسوم الرئاسي 21-439 أن المدير العام للمديرية العامة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال يتولى تمثيلها أمام القضاة[2].

- **الاستقلال المالي:**

تتسع الهيئة باعتبارها شخصية اعتبارية بمسؤولية مالية مستقلة عن الكيان الذي أنشأها، و الكيان قائم بحد ذاته مستقل عن ادارة الاشخاص الذين يتألفون منه ،كما أن مسؤولياتها المالية هي وعاء لحقوقها و الالتزامات الناشئة عن أنشطتهم و لهم التصرف المالي و حرية تحديد دخلهم المالي، و تنظيم الميزانية ضمن الحدود القانونية.

- **الاستقلال الاداري:**

للشخص الاعتباري أجهزة تتولى عملية ادارته و هذا ما تضمنته الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال حيث تتشكل من مجلس التوجيه و المديرية العامة يقومان بإدارتها دون تدخل أي أجهزة أخرى.[3]

---

[1] -المادة 3 من المرسوم الرئاسي 19-172،المؤرخ في 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الإتصال و مكافحتها و تنظيمها و كيفيات سيرها، ج ر ج ج، ع37، 2019.

[2] -المادة 10 من المرسوم الرئاسي 21-439، مصدر سابق.

[3] -لحرش عبد الرحيم و حضري حسان، "الاثار القانونية للشخصية الاعتبارية في القانون الجزائري"، مجلة التمكين الاجتماعي، مجلة فصلية دولية أكاديمية محكمة ، الجزائر، المجلد 1، ع4، ديسمبر، 2019، ص271.

الفرع الثاني: مهام و تشكيلة الهيئة و طبيعة عملها.

تنص الفقرة "02" من المادة الرابعة "04" من المرسوم الرئاسي 15-261 [1]على المهام الاساسية للهيئة و التي تهدف الى منع مكافحة الجرائم الالكترونية من خلال تعزيز أعمال البحث و التحقيق و تقديم المساعدة لمصالح الشرطة القضائية في شق مكافحة الجرائم المعلوماتية و من أبرزها مهام الهيئة، و متناول في هذا الفرع اولا مهام الهيئة و ثانيا تشكيلة الهيئة و طبيعة عملها.

أولا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الاعلام و الاتصال:

- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و كيفية التصدي لها .
- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال
- مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة.

بتكنولوجيات الاعلام و الاتصال بما في ذلك جمع المعلومات الدقيقة و الاستعانة بالخبرات القضائية.

- ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الارهابية و التخريبية و المساس بسيادة و امن الدولة تحت سلطة القاضي المختص باستثناء أي هيئات وطنية أخرى.
- تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من أجل استعمالها في الاجراءات القضائية .
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الاجنبية و تطوير تبادل المعلومات على المستوى الدولي في مجال اختصاصها.

[1] -المرسوم الرئاسي 15-261 ،مؤرخ في 24 ذي الحجة 1436الموافق ل8 اكتوبر 2015 ،يحدد تشكيلة و تنظيم كيفيات تفسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، ج ر ج ج ، ع53، الصادر في 8 اكتوبر ،2015.

ثانيا: تشكيلة الهيئة و طبيعة عملها:

1- التشكيلة الادارية للهيئة:[1]

تتشكل اللجنة من لجنة مديرة بالإضافة الى مديرية عامة حيث تتشكل اللجنة المديرة من الوزير المكلف بالعدل و هو رئيسها، بالإضافة الى آخرين و المتمثلين في الوزير المكلف بالداخلية و الوزير الكلف بالبريد و تكنولوجيا الاعلام و الاتصال و قائد الدرك الوطني و المدير العام للأمن الوطني اضافة الى ممثلين احدهما عن رئاسة الجمهورية و الاخر عن وزارة الدفاع و اخيرا قاضيان من المحكمة العليا.

2- التشكيلة التقنية للهيئة:[2]

تتشكل التشكيلة التقنية من مديريات تتميز من حيث افراد تشكيلها و مهامها بالصبغة التقنية ذلك لإنجازها للمهام التقنية المتعلقة بالوقاية و بمكافحة الجرائم الالكترونية و تتمثل هذه المديريات في:

- **مديرية المراقبة الوقائية و اليقظة الالكترونية:**

نجد هنا أن الامر الرئاسي 15- 261 لم يتطرق الى تشكيلة هذه المديرية لكن و بعد استقرار المادة 18 منه نجد أن تشكيلة هذه المديرية تتمثل في ضباط و أعوان للشرطة القضائية من المصالح العسكرية لاستعلام للأمن و الدرك الوطني و الامن الوطني المتخصصين في مجال مكافحة الجرائم المعلوماتية يتم تعيينهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل و الدفاع الوطني و الداخلية بالإضافة الى مستخدمي الدعم التقني و الاداري في نفس المجال و هذا لمساعدتهم .

و حسب المادة 11 من المرسوم تتجلى مهام هذه المديرية في:

1/ بناء اذن كتابي من السلطة القضائية و تحت اشراف هذه الاخيرة تتم المراقبة الوقائية على الاتصالات الإلكترونية و تتم المراقبة الوقائية على الاتصالات الالكترونية و يتم اجراءات التفتيش و الضبط ضمن نظام المعلومات في قضايا الارهاب و التخريب و الجرائم التي تمس الامن القومي و هذا تحت رقابة قاض مختص.

2/ ارسال المعلومات المتحصل عليها الى السلطات القضائية و مصالح الشرطة القضائية المتخصصة .

---

[1] -المادة 6 و 7 من المرسوم الرئاسي 15-261، مصدرسابق.

[2] -المادة 11 و 18 المرسوم الرئاسي 15-261، مصدر سابق.

3/ تنفيذ طلبات المساعدة القضائية الاجنبية في مجال تدخل الهيئة و حج المعطيات التي تأخذنا الى مكان المجرم الإلكتروني و التعرف عليه.

4/ جمع و مركزة جميع المعلومات المهمة و استغلالها في الكشف عن الجرائم الالكترونية.

5/ القيام بحملات توعية للتعريف بمخاطر تكنولوجيا الاعلام و الاتصال.

6/ تزوير السلطات القضائية و الجهات المختصة تلقائيا و بناء على طلبها بالمعطيات و المعلومات المتعلقة بالجرائم المعلوماتية بالإضافة الى تنفيذ توجيهات اللجنة المديرة.

نستنتج بعد التعرف على تشكيلة و مهام هذه المديرية يمكننا القول بأنها المركز التشغيلي و القلب النابض للوكالة لأنها مسؤولة عن الجوانب الفنية لإجراء ابحاث الجرائم المعلوماتية و الاعمال المتعلقة بالتحقيق فيها[1].

- **مديرية التنسيق التقني:**

نجد أن المرسوم الرئاسي 15-261 لم يتطرق الى تشكيلة هذه المديرية فيما يجدر بنا القول بأن تشكيل هذه الوكالة سيكون بناء على قرار مشترك بين وزراء العدل و الدفاع و الداخلية على شكل مديرية المراقبة الوقائية و اليقظة الالكترونية و لهذه المديرية مهام تقوم بها حسب المادة 12 من المرسوم المذكور أعلاه و هي:

- انجاز الخبرات القضائية في مجال اختصاص الهيئة.
- تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيا الاعلام و الاتصال و استغلالها.
- اعداد الاحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيا الاعلام و الاتصال.
- تيسير منظومة الاعلام للهيئة و ادارتها [2].

[1] -المادة 11 و 18 المرسوم الرئاسي 15-261، مصدر سابق.

[2] -المادة 12 من المرسوم الرئاسي 15-261، مصدر سابق.

المطلب الثاني: الوحدات التابعة لسلك الأمن و الدرك الوطني.

هناك مجموعة من الوحدات لدى المديرية العامة للأمن الوطني و الدرك الوطني و هذا لتنفيذ مهام في سبيل الحفاظ على الامن و النظام العام و هذا ما سنتعرف عليه في هذا المطلب فيما يخص هذه الوحدات. و سنتطرق في الفرع الاول للوحدات التابعة لسلك الامن الوطني و في الفرع الثاني للوحدات التابعة للدرك الوطني.

الفرع الاول: الوحدات التابعة لسلك الامن الوطني.

قامت المديرية العامة للأمن الوطني بإنشاء مخبر مركزي بمركز الشرطة حيث طوفان بالجزائر العاصمة و مخبرين جهويين بكل من قسنطينة و وهران يحتوي على فروع تقنية من بينها خلية الاعلام الالي و فرق متخصصة تكمن مهمتهم في التحقيق و الكشف عن الجرائم المعلوماتية بالإضافة الى انشائها ثلاثة مخابر على مستوى بشار ورقلة و تمنراست قيد الانجاز لأحمل تعميم هذا النشاط على كافة ربوع الوطن[1].

حيث يتولى كل مخبر سواء المركزي أو الجهوي لولاية قسنطينة أو وهران مهام البحث و التحقيق و تحليل الادلة الجنائية بمختلف أنواعها فنجد ان كل مخبر يضم دائرتين و هما الدائرة العلمية و التي تتولى أعمال البحث و التحقيق و تحليل الادلة التي لها علاقة بالمجال البيولوجي و الطب الشرعي و الكيمياء و المخدرات كذلك تلك المتعلقة بمجال التسميم و الحرائق و المتفجرات نجد كل منها على مستوى مخبر خاص أما الدائرة التقنية و تتولى مهام البحث و التحقيق و تحليل الادلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الاسلحة و القذائف بمختلف أنواعها بالإضافة الى جرائم التزوير و الجرائم الالكترونية حيث تباشر الاجراءات الخاصة بكل جرعة على مستوى دائرة مستقلة عن الاخرى[2].

كما ينظم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة و وهران مخبرا خاصا يتولى مهمة

---

[1] -سعيداني نعيم، "آليات البحث و التحري في الجرائم المعلوماتية في القانون الجزائري" ،مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ،تخصص علوم جنائية، كلية الحقوق و العلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2012-2013، ص 107.

[2] -ربيعي حسين، "آليات البحث و التحقيق في الجرائم المعلوماتية"، أطروحة مقدمة نيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات و العلوم الجنائية، كلية الحقوق و العلوم السياسية، قسم الحقوق ،جامعة باتنة 1، الجزائر، 2015-2016، ص178.

التحقيق في الجريمة المعلوماتية تحت اسم "دائرة الادلة الرقمية و الاثار التكنولوجية" و التي لم تكن عند استخدامها سنة 2004 و بسبب الانتشار المتزايد لتقنية المعلومات ادى الى ارتفاع ملحوظ في عدد قضايا الجرائم الالكترونية و قسمت الدائرة الى 03 أقسام و المتمثلة في:

1- قسم استغلال الادلة الرقمية الناتجة عن الحواسيب و الشبكات.

2- قسم استغلال الادلة الناتجة عن الهواتف النقالة.

3- قسم تحليل الاصوات (حيث ينشط هذ القسم على مستوى المخبر المركزي بالجزائر العاصمة) [1].

تضم الدائرة صفوفها 08 أعضاء محققين 04 منهم أعضاء من الشرطة بصفة رسمية، يتمتعون بصفة ضابط شرطة قضائية أما البقية فهم أعوان شبيهون، متحصل كل منهم على شهادة جامعية في تخصص الاعلام الالي اضافة الى المامهم بالجانب القانوني و فيما يزيد من فعاليتهم في مجال مباشرتهم لمختلف اجراءات البحث و التحري في الجرائم الالكترونية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الاطلاع على المستجدات القانونية و التقنية فيما يخص الاجرام المعلوماتي [2] .

حيث تختص الجهات القضائية المختصة بالجرائم الماسة بالأنظمة المعالجة الالية للمعطيات طبقا للمواد 37-329-40 من ق.ا.ج بالإضافة الى ان يمكن قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال المرتكبة في الخارج حتى و لو كان مرتكبيها أجنبيا اذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09-04 و تتوسع صلاحيات الضبطية القضائية فعند معاينة الجرائم الماسة بأنظمة المعالجة الالية يمكن تمديد الاختصاص المحلي الى كامل الاقليم الوطني المادة 16 من ق.ا.ج كما يمكن مشرع المحلات السكنية و غير السكنية في كل ساعة من ساعات الليل و النهار بإذن من وكيل الجمهورية حسب المادة 47 من ق.ا.ج و تكمن أساليب التحري الخاصة في اعتراض المراسلات الرقمية المادة 65 مكرر فقرة 06 فقرة ق.ا.ج المدرجة بموجب القانون 06-22 المؤرخ في 2006/12/20.

---

[1] -بوبعاية ابتسام، مرجع سابق ، ص 36.

[2] -ربيعي حسين، مرجع سابق ،ص 179 .

- تفتيش المنظومة الالكترونية المادة 05 من القانون رقم 09-04.
- حجز المعطيات الالكترونية المادة 06 رقم 09.
- نسخ المعطيات على دعامة تخزين الكترونية.
- فتح الاطلاع على المعطيات التي يشكل محتواها جريمة[1].

و حسب المادة 12 من قانون الاجراءات الجزائية و التي تقول ان الذي يقوم بمهمة الشرطة القضائية هم القضاة و الضباط و الاعوان و الموظفين و المبنيون في هذا الفصل و توقع الشرطة القضائية بدائرة اختصاص كل مجلس قضائي تحت اشراف النائب العام و يتولى وكيل الجمهورية ادارتها على مستوى المحكمة و ذلك تحت رقابة غرفه الاتهام .

و ضباط بالشرطة القضائية مهمة البحث و التحري عن الجرائم المقررة في قانون العقوبات و جمع الادلة عنها و البحث عن مرتكبيها مادام لم يبد انها تحقيق قضائي [2] .

أما المادة 14 [3] من قانون الاجراءات الجزائية فتطرقت الى تشكيلة الضبط القضائي و هي:

1. ضباط الشرطة القضائية.
2. أعوان الضبط القضائي.
3. الموظفون و الاعوان المتولا بهم قانونيا بعض مهام الضبط القضائي .

الفرع الثاني : الوحدات التابعة للدرك الوطني الجزائري.

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الامن و النظام العام و محاربة الجريمة بكافة أنواعها وحدات متنوعة و عديدة على مستوى القيادة العامة و على مستوى القيادات الجهوية وتتمثل في:

1- قيادة الدرك الوطني.

[1] -مولود ديدان، مرجع سابق ، ص 120 .

[2] -المادة 12 من الامر 66-155، المؤرخ في 08 جوان 1966، المتضمن قانون الاجراءات الجزائية،ج ر ج ج، المعدل و المتمم، ع 48، 1966.

[3] -المادة 14 من الامر 66-155،المصدر السابق.

2- الوحدات الاقليمية.

3- الوحدات المشكلة.

4- الوحدات المتخصصة وحدات الاسناد.

5- هياكل التكوين.

6- المعهد الوطني للأدلة الجنائية و علم الاجرام.

7- المصالح و المراكز العلمية و التقنية.

8- المصلحة المركزية للتحريات الجنائية.

9- المفرزة الخاصة للتدخل .

و نستخلص في هذا الفرع في دراسة وحدة من وحدات السابقة للذكر و هي المعهد الوطني للأدلة الجنائية و علم الاجرام للدرك الوطني [1].

يعتبر المعهد الوطني للأدلة الجنائية و علم الاجرام للدرك الوطني مكسب يدعم قدرات الدرك الوطني و مساعدتهم للكشف و مكافحة الجريمة بجميع أشكالها، حيث يتمركز هذا المعهد في بوشاري بالجزائر العاصمة و هو مؤسسة عمومية ذات طابع اداري تحت الوصاية المباشرة لويزة الدفاع الوطني انشئ بالمرسوم رقم 183-04 المؤرخ في 26 جوان 2004 و هو اكتر من مكسب مؤسساتي و يمثل قوة ردع في خدمة العدالة في مكافحة الجريمة و ضمان المحافظة على الحقوق الاساسية المواطن و هو المكلف بالمهام التالية:

- انجاز الخبرات و التحاليل بناء على طلبات القضاة المحققين و السلطات المؤهلة بغرض استخلاص الادلة التي تسمح لنا بالتعرف على مرتكب الجريمة .
- المساعدة التقنية للوحدات اثناء القيام بالتحريات المعقدة باستخدام المناهج العلمية المتعلقة بالوقاية و التقليل من كل أشكال الجرائم .
- تصميم و انجاز بنوك معطيات وفقا للقانون.

[1] -ربيعي حسين، مرجع سابق ،ص 183.

- المساهمة في تنظيم دورات الاتقان و التكوين ما بعد التدرج في تخصص العلوم الجنائية.
- المبادرة بالبحوث المتعلقة بالإجرام و اجرائها باللجوء الى التكنولوجيا الدقيقة.
- تصور و ضمان متابعة الابحاث الموكلة للغير.
- المشاركة في كل الملتقيات و المحاضرات و الندوات على الصعيدين الوطني و الدولي الضرورية لتحسين مستوى المعهد.

و لتأدية مهامه على أكمل وجه فان المعهد الوطني للأدلة الجنائية و علم الاجرام يتكون من العديد من الاقسام و المصالح المختصة لذكر منها:

- مصلحة البصمات، مصلحة الوثائق، مصلحة البيئة، قسم البلاستيك، قسم التحليل الدقيق و قسم السيارات [1].

سنتطرق في موضوع دراستنا الى دائرة الاعلام الالي و الالكترونيك، و هي أهم دائرة في موضوعنا حيث أنها مكلفة معالجة و تحليل و تقديم كل دليل رقمي للعدالة ،كما تعمل على مساعدة المحققين في أداء مهامهم كذلك تسهر أجهزة و مصالح الامن الوطني من قيادة و اطارات على تحسين معارفهم حتى توافي التطورات التكنولوجية الحاصلة لإنجاز المهام المنوطة بها في أكمل وجه و تنقسم دائرة الاعلام الالي الالكترونية الى ثلاثة مخابر، و هي:

أولا: مخبر الاعلام الآلي:

حيث يقوم هذا المخبر بتحليل و معالجة حوامل المعطيات الرقمية (هواتف، شرائح، أقراص) و العمل على حماية و تحديد للبطاقات الذكية سواء كانت بنكية أو متعلقة بالضمان الاجتماعي أو بطاقات مهنية أخرى بالإضافة الى أنه يحتوي على سبع قاعات، و هي:

- مكتب التوجيه.
- فصيلة الانظمة المشحونة.

[1] –موقع الدرك الوطني الجزائري http://www.mdn.dz ، تاريخ الاطلاع :25 ماي 2024، الساعة 08:00.

- فصيلة تحليل المعطيات.
- فصيلة الهواتف.
- فصيلة اقتناء المعطيات.
- قاعة التوزيع.
- قاعة التخزين [1].

تعمل هذه القاعات السالفة الذكر بقيادة أعوان أكفاء و تجهيزات عالية من محطات لإجراء الخبرات الاعلامية و أجهزة اقتناء الهواتف و الحواسيب و معطيات الترميم و الصيانة .

ثانيا: مخبر الفيديو :

حيث يقوم هذا المخبر بإعادة بناء مسرح الجريمة بشكل ثلاثي الابعاد (3D) و كذا تحسين مستويات الصور و الفيديوهات بمختلف التقنيات و مقارنة الصور و الفيديوهات و معرفة الحقيقة من المزيفة أو المعدلة، و يحتوي هذا المخبر على أربع قاعات و تتمثل في قاعتان للتحليل، قاعة توزيع و قاعة تخزين و تعمل هذه القاعات كغيرها بتجهيزات عالية و حديثة لقراءة الفيديوهات الرقمية و الممغنطة و على كافة الحوامل و أجهزة لحفظ الفيديوهات و الصور عالية الحماية.

ثالثا: مخبر الصوت:

حيث يتعهد هذا المخبر بتحسين نوعية الصوت و ذلك عن طريق نزع التشويش و تعديل السرعات و تحديد هوية المتكلم من خلال معرفة و مقارنة الاصوات كذا يعمل على تحديد شرعية هذه التسجيلات، و مدى اعتبارها دليلا صحيح من عدمه بالإضافة الى انه يحتوي على خمس قاعات ثلاثة منها للتحليل و قاعة توزيع و قاعة للتخزين.

[1] – عز الدين عز الدين، مداخلة بعنوان "الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها" مقدمة الملتقى الوطني حول الجرعة المعلوماتية بين الوقاية و المكافحة المنعقد، بجامعة بسكرة، يوم 16 نوفمبر 2015، ص 50.

حيث يعتبر المعهد الوطني للأدلة الجنائية و علم الاجرام أهم قلاع مكافحة الجريمة و تتبعها على مستوى الجزائر و هذا لاحتوائه على جميع الكفاءات و المعدات و الوسائل التكنولوجية المتطورة.

كما أن التقنية عامل يفرض نفسه اليوم اذ اصبحت وحدات الدرك الوطني مجهزة بوسائل و تقنيات حديثة تساعد على انجاز التحقيقات و التحريات في مجال التحقيق في الجرائم المعلوماتية حيث عالجت هذه المصلحة عدد من القضايا في السنوات الاخيرة .[1]

[1] –عز الدين عز الدين، مرجع سابق ، ص 59.

خلاصة الفصل الأول:

تطرقنا في هذا الفصل الى تعريف الجريمة المعلوماتية على أنها نشاط اجرامي يؤدي فيه نظام الكمبيوتر دور الإتمام في ارتكاب الجريمة، اي أنها تعتبر جرائم متصلة بتكنولوجيا الاعلام و الاتصال يتعلق بالمعالجة الآلية للبيانات أو ينقلها كما لها خصائص تميزها و تميز مرتكبيها عن المجرمين العاديين، و هي أنها جريمة عابرة للحدود لسرعة انتشارها و تنفيذها بين دول العالم و أقاليمه مع اكتساب و تميز المجرم الالكتروني بالذكاء و المهارة في المجال المعلوماتي و شبكة الانترنيت و الخبرة فيها بالتحكم في نقل المعطيات و البيانات و الأنظمة الآلية، مما ادى لصعوبة اثبات الجريمة الالكترونية على أنها خطيرة و صعبة الاكتشاف في تحديد مكان وقوعها أو مكان التعامل معها بسبب اتساع نطاقها المكاني و ضخامة البيانات حيث في المبحث الثاني ابرزنا الهيئات المختصة في مجال مكافحة الجرائم المعلوماتية منها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، اضافة الى الوحدات التابعة لسلك الامن و الدرك الوطني.

الفصل الثاني: آليات التحقيق في الجرائم المعلوماتية.

ان الجرائم المعلوماتية تدفع المشروع الجزائي الى اعادة النظر في الكثير من المسائل الجزائية، خاصة فيما يتعلق بمسألة الاثبات التي يتوجب تحديث الانظمة و التعليمات و الجهات الامنية المختصة بمعالجة القضايا الناتجة من ظهور هذه الانماط الجديدة، و ها ما يستتبع تطوير أسلوب التحقيق و التفتيش فيها.[1]

فالتحقيق بشكل عام يعتمد على ذكاء المحقق في المعاينة و جمع و ضبط الادلة في الجرائم المعلوماتية ،و علاوة عن ذلك يتميز مرتكبي هذه الجرائم عما عهدناه في مرتكبي الجرائم التقليدية بالذكاء و القدرة التقنية في اخفاء معالم الجريمة، و هو ما يؤدي الى صعوبة وصول الجهات المكلفة بالتحقيق الى دليل الذي يفيد في كشف الجريمة، كما قد يساهم الضحية نفسه في اعاقة سير اجراءات التحقيق.[2]

و بناء على هذا خصصنا هذا الفصل لمبحثين اولها الاجراءات التحقيقية لإثبات الجريمة المعلوماتية ،و المبحث الثاني الليل الرقمي لاثبات الجريمة المعلوماتية.

[1] – بوبعاية ابتسام، مرجع سابق ، ص40 .

[2] –د/ عز الدين عثماني، مرجع سابق ، ص50 .

المبحث الأول: الاجراءات التحقيقية في الجريمة المعلوماتية.

ان التطورات التكنولوجية في انظمة المعالجة الالية فضلا عن الطبيعة المحددة للأدلة الرقمية، ستؤدي حتما الى تغيرات في العديد من الافكار الشائعة حول اجراءات و طرق الحصول على الادلة الرقمية ،الامر سيتطلب حتما اعادة تقييم مدى صحة الادلة الرقمية، فتطور بعض الممارسات الاجرائية التقليدية و غيرها من القواعد الاجرائية في قانون الاجراءات الجنائية يتوافق مع طبيعة البيئة التقنية لان تطور الادلة ووسائلها أمر في غاية الاهمية لمكافحة هذا النوع الجديد من الجرائم.[1] سنتطرق في هذا المطلب الى الاجراءات التقليدية لاثبات الجريمة المعلوماتية ثم الى الاجراءات الحديثة في الجريمة المعلوماتية في **المطلب الثاني**.

المطلب الاول: الاجراءات التقليدية لاثبات الجريمة المعلوماتية.

تتشابه الجرائم الاخرى مع الجريمة المعلوماتية في الاجراءات التقليدية من ناحية المعاينة التفتيش و ضبط الادلة و جمعها و لا شك ان المشروع لا يجيز استخراج الادلة دون رقابة من خلال قواعد اجرائية معينة اهمها الفحص و الخبرة.[2] سنتطرق في هذا المطلب الى المعاينة و التفتيش في الجرائم المعلوماتية (الفرع الاول) و الى الضبط و الخبرة القضائية في الجرائم المعلوماتية (الفرع الثاني).

الفرع الاول: المعاينة و التفتيش في الجرائم المعلوماتية.

أولا: المعاينة.

عرف الفقه الجنائي بانها اجراء ينتقل بمقتضاه المحقق الى مسرح الجريمة يشاهد و يفحص بنفسه مكانا او شخص أو شيئا له علاقة بالجريمة لاثبات حالة و التحفظ على كل ما قد يفيد من الاثار في كشف الحقيقة.[3]

[1] -بوبعاية ابتسام، مرجع سابق، ص40.

[2] -معش زهية، غانم نسيمة، "الاثبات الجنائي في الجرائم المعلوماتية"، مذكرة تخرج لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2012-2013 ،ص5.

[3] -براهيمي جمال، "التحقيق الجنائي في الجرائم الالكترونية"، أطروحة لنيل شهادة الدكتوراه تخصص قانون، كلية الحقوق والعلوم السياسي، جامعة تيزي وزو، 2018، ص56.

و يشير لمصطلح المعاينة الالكترونية على أنها المشاهدة و رؤية اي شيء له علاقة بالجريمة لاثبات حالتها و الآثار المادية التي خلفها ارتكاب الجريمة المعلوماتية فالمعاينة هي من اهم مراحل التحقيق في الجرائم المعلوماتية بناءا على ما تستطيع توفيره من ادلة اثبات و تكمن اهمية المعاينة في معاينة البرمجيات أو الاقراص و كل ما يتعلق بجهاز الحاسب الالي بالرجوع لطبيعتها الخاصة في هذا المجال.[1]

حيث تقوم على ضبط كل ما يلزم و يفيد من الاشياء لكشف الحقيقة في الجريمة المعلوماتية و مرتكبيها بهدف المحافظة على الادلة التقنية من التلف أو محو أو التعديل.

و يبقى هدف المعاينة الكشف عن الحقيقة و لتحقيق ذلك لابد من مراعاة خطوات و ارشادات محددة منها:

1- تصوير الكمبيوتر و ما يتصل به من أجهزة و ملحقات و المحتويات و الاوضاع العامة بصورة دقيقة مع التركيز على الاجزاء الخلفية مع تسجيل وقت و تاريخ التقاط الصور.

2- مراعاة الطريقة التي تتم بها اعداد النظام و الاثار الالكترونية بما في ذلك السجلات الالكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال و نوع الجهاز الذي تم عن طريقه الولوج الى النظام او الموقع.

3- عدم اجراء اي نقل للمعلومات من مسرح الجريمة قبل اجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الكمبيوتر من اي مجالات لقوى مغناطسية يمكن ان تكون سببا في محو او اتلاف البيانات المسجلة.

4- التحفظ على المحتويات سلة المهملات من اوراق ممزقة او مستعملة الشرائط و الاقراص الممغنطة و غير السليمة لفحصها و رفع البصمات التي قد تكون له صلة بالجريمة المرتكبة[2].

5- يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجرونها بطلب من المحققين و كذا المعلومات المتصلة بها و ذلك تحت طائلة العقوبات المقررة لإفشاء اسرار التحري و التحقيق[3].

---

(1)- عيدة بلعابد ،مرجع سابق ، ص 140.

(2)-خالد ممدوح ابراهيم، مرجع سابق ، ص17.

(3)-المادة 10، الفقرة 2 من قانون رقم 09-04 ، مصدر سابق.

6- التحفظ على مستندات الادخال و المخرجات الورقية للحاسب ذات صلة بالجريمة لرفع و مضاهاة ما قد يوجد من بصمات.

7- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة.

8- فصل الكهرباء عن موقع المعاينة لمنع الجاني من القيام بأي عملية محو أو اتلاف على آثار الجريمة.

9- جعل المعاينة الالكترونية سرية و مقتصرة على فئة الباحثين و المحققين و الكفاءة العلمية و الخبرة الفنية.[1]

ثانيا: تعريف التفتيش.

نصت المادة 1/5 من القانون 09-04 المتضمن لقواعد خاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها [2]، يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في اطار قانون الاجراءات الجزائية و في الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش و لو عن بعد الى منظومة أو جزء منها و كذا المعطيات المخزنة فيها و منظومة تخزين المعلوماتية.

و يمكن تعريف التفتيش بأنه ذلك الاجراء الذي يدخل ضمن اجراءات التحقيق الابتدائي أو القضائي و لا يمكن أن يقوم به سوى النيابة و قاضي التحقيق.[3]

يعد التفتيش اجراء تحقيقي الغاية منه الحصول على ادلة جنائية تفيد في اثبات او نفي الجريمة المرتكبة و معرفة مرتكبيها لأعمال الاجراءات التحقيقية من جهة اخرى فان التفتيش بوجه عام يمس في أصله بالحياة الخاصة للأفراد و بالأخص الحياة المعلوماتية المتواجدة عبر مختلف مواقع التواصل الاجتماعي

[1] -خالد ممدوح ابراهيم، مرجع سابق ، ص17.

[2] -المادة 1/5 من القانون 09-04 ، مصدر سابق.

[3] -مصطفى عبد الباقي، التحقيق في الجريمة الالكترونية و اثباتها، كلية الحقوق و الادارة العامة، جامعة بيرزيت رام الله، فلسطين، المجلد 4، ع 4، 2018، ص 289.

من بريد الكتروني غير ان حماية المصلحة الخاصة و العامة كلها تبرز اللجوء الى التفتيش بما في ذلك التفتيش الالكتروني.[1]

و حسب المادة 03 القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها منه[2] على أنها: "مع مراعاة الاحكام القانونية التي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الاجراءات الجزائية و في هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و القيام لإجراءات التفتيش و الحجز داخل منظومة معلوماتية".

و منه التفتيش بشكل عام هو اجراء هدفه البحث في مستودع سر الانسان عن دليل متعلق بجريمة وقعت ينصب، اما على الاشخاص أو المساكن أو الممتلكات المادية وفق ضوابط قانونية اما التفتيش الالكتروني يتمثل في النظم المعالجة الالية للبيانات في العالم الافتراضي، فهو اجراء يسمح بجمع الادلة المخزنة أو المسجلة بشكل الكتروني للبحث و التنقيب عن الجريمة المعلوماتية و أدلتها الرقمية.[3]

كما يعني التفتيش المعلوماتي أنه الدخول الى الانظمة المعلوماتية للبحث عن التنقيب في البرامج المستخدمة و في ملفات البيانات المخزنة لإيجاد ما يفيد بارتكاب الجريمة و مرتكبيها، وفق ما يقتضيه التحقيق.[4]

1- الشروط الموضوعية للتفتيش:

و تتمثل هذه الشروط في الضوابط اللازمة لإجراء تفتيش صحيح و هي في الغالب تكون سابقة له و يمكن حصرها في ثلاث شروط اساسية هي: السبب، المحل و السلطة المختصة بالقيام بها.

[1] – عيدة بلعابد، مصدر سابق ، ص141.

[2] –القانون 09-04، مصدر سابق.

[3] –عيدة بلعابد، مرجع سابق ، ص 142.

[4] –عيدة بلعابد، المرجع نفسه .

أ- **سبب التفتيش:** و يقصد بالسبب هو الحصول على دليل هدفه تحقيق قائم من أجل الوصول الى حقيقة الحدث و يتمثل في وقوع جريمة ما جناية او جنحة او اتهام شخص أو أشخاص معنيين في كشف الحقيقة لدى المتهم أو مسكنه أو شخص غيره أو مسكنه.[1]

ب- **محل التفتيش:** محل التفتيش في الجريمة المعلوماتية هو الحاسب و الشبكة التي تتمثل في مكونات و المزود الالي و المصنف و الملحقات التقنية. [2]

ت- **السلطة المختصة بالتفتيش:** الاصل أن التشريع المصري يمنح للنيابة العامة سلطة الاختصاص بالتفتيش على خلاف التشريع الفرنسي و التشريع الجزائري اللذان أخذا بنظام الفصل بين سلطتي الاتهام و التحقيق.[3] أما الاستثناء يمنح لضباط الشرطة القضائية هذا الاختصاص في الحالات التالية:

- **بطلان اذن التفتيش:** ان مراقبة المحادثات الهاتفية سلكية و اللاسلكية و تسجيلها هو اجراء من اجراءات التفتيش الا انه نظرا لخطورة هذا الاجراء باعتباره يتعرض لمستودع سر الفرد و يزيل الحظر على بقاء يريته مقصورة على نفصه و من اراد ائتمائه عليه فيباح لغيره الاطلاع على مكنون سره فقد حرص الدستور و قانون اجراءات الجنائية على تأكيد ذلك و اشتراط لمراقبة المحادثات الهاتفية صدور أمر قضائي مسبب.[4]

2- **الشروط الشكلية:** الى جوانب الضوابط الموضوعية لتفتيش نظم الحاسب الالي هناك ضوابط اخرى و طابع شكلي يجب مراعاتها و الاخذ بها اثناء القيام بالتفتيش.

---

[1] -بلعيد منصورية، النظام الاجرائي للجريمة المعلوماتية في التشريع الجزائري، تخصص قانون قضائي، جامعة عبد الحميد بن باديس، مستغانم، 2019-2020 ،ص46.

[2] -بلعيد منصورية، المرجع نفسه، ص 47 .

[3] -عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري و المقارن، دار الجامعة الجديدة، كلية الحقوق، جامعة الاسكندرية ،2006 ،ص105 .

[4] -بن زرت آسيا، اثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر ،جامعة عبد الحميد بن باديس ،مستغانم، 2018-2019 ،ص 24.

و كما حددت المادة 44 من قانون الاجراءات الجزائية الجزائرية لا سيما بعد التعديل الذي حصل بموجب القانون 06-22 في سبتمبر 2006 الشروط الشكلية للتفتيش وهي: [1]

- وجود اذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.
- الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.
- أن يتضمن الاذن بيان و من الجريمة موضوع البحث عن الدليل بشأنها و عنوان الاماكن المقصودة بالتفتيش.
- حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.
- في حالة رفض الحضور يستدعي ضباط الشرطة القضائية شاهدين من غير الموظفين الخاضعين للسلطة.[2]

3- **الميقات:** قيد الميقات القانوني على أنه من الساعة الخامسة صباحا الى الساعة الثامنة مساءا و هناك حالات استثنائية كحالة الطوارئ و غيرها يجوز التفتيش في كل ساعة من ساعات الليل أو النهار.[3]

تفتيش المنظومة المعلوماتية عن بعد في الجرائم الالكترونية:

التفتيش في نطاق الجرائم المعلوماتية لا يخرج عن احدى الفرضيتين:

1- حالة جهاز متصل بجهاز المتهم داخل الدولة:

المشكلة في هذه القضية هي أنه عندما قامت جهة التحقيق بتفتيش الجهاز المتصل بجهاز المتهم و الموجود داخل الدولة، فقد تجاوزت الاختصاص المكاني لجهة التحقيق من جهة و انتهكت خصوصية الاخرين من جهة أخرى. و نظرا لوجود قصور في نصوص قانون ا.ج.ج لسنة 2006 تم مواجهة هذا

[1] -زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة ،الجزائر، 2011، ص ص: 20،21 .

2-مولود ديدان، قانون الاجراءات الجزائية، دار بلقيس الجزائر، ديسمبر 2014 ،ص121.

[3] -زبيخة زيدان، مرجع سابق ، ص 134.

القصور بأن سمح للسلطات القضائية المختصة تمديد التفتيش عن المعطيات المبحوث عنها بسرعة الى اي منظومة معلوماتية أو جزء منها تقع داخل الاقليم الوطني و هذا ما نص عليه الفقرة الثانية من المادة 05 من القانون رقم 09-04 و ما يدخل ضمن نطاق الاستعجال في تمديد الاختصاص خوفا من العبث بالأدلة الرقمية.[1]

1- حالة جهاز متصل بجهاز المتهم خارج الدولة:

في هذه الحالة تكون المشكلة اكبر اذا كانت المعدات المطلوب تفتيشها و توسيلها بالمحطة الطرفية للمدى عليه موجودة في الخارج، و في معظم الحالات ينوي مرتكبو الجرائم الإلكترونية تخزين بياناتهم الخاصة و التي ينظر اليها على انها دليل ادانة على الجرائم التي ارتكبوها و هم في الخارج. [2]

و بالنسبة للقانون الجزائري فقد تلافى مشكلة التفتيش عن بعد خارج الاقليم الوطني بموجب الفقرة الثالثة من المادة 05 من القانون 09-04 التي نصت على أنه اذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول اليها انطلاقا من المنظومة الاولى مخزنة في منظمومة تقع خارج الاقليم الوطني فان الحصول عليها يكون بمساعدة السلطات الاجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.[3]

الفرع الثاني: الضبط و الخبرة القضائية في الجرائم المعلوماتية

أولا: الضبط

ان الضبط في الجريمة المعلوماتية يختلف عن ضبط في الجرائم الاخرى، من حيث المحل لان الجريمة المعلوماتية على الاشياء ذات طبيعة معنوية ،و هي البيانات و المراسلات و الاتصالات المعلوماتية من جهة و لها طبيعة مادية كالورق و الكمبيوتر و ملحقاته و الاقراص الصلبة الخارجية و المرنة و أقراص

[1] -دلال مولاي ملياني،" اشكالية الاثبات في جرائم الانترنيت في التشريع الجزائري"، أطروحة دكتوراه، تخصص قانون خاص ،كلية الحقوق و العلوم السياسية، جامعة ابة بكر بلقايد، تلمسان ،الجزائر، 2017-2018 ،ص219.

[2] -معش زهية ،غانم نسيمة، مرجع سابق، ص 18.

[3] -المادة 5 من القانون رقم 09-04 ، مصدر سابق.

الليزر البطاقات الممغنطة.[1]

فإجراء الضبط يكون بعد عملية التفتيش المعلوماتي و ان كان ضبط الاشياء المادية المتعلقة بالجريمة المعلوماتية لا يطرح اي صعوبة أو اشكالية.

على خلاف المعلومات و البيانات المخزنة في ذاكرة الحاسوب" بنك المعلومات"[2]و يعرف الضبط على أنه وضع اليد على شيء يتصل بجريمة وقعت و يغيد في كشف الحقيقة عنها و عن مرتكبيها، أما الضبط الالكتروني يقصد بيه: وضع اليد على الدعائم المادية المخزنة فيها البيانات الالكترونية أو المعلومات التي تتصل بالجريمة المعلوماتية التي وقعت و تفيد في كشف الحقيقة عنها و عن مرتكبيها[3].

و ايضا هو نسخ البيانات المعلوماتية المتواجدة في الفضاء الالكتروني أو في الدعائم الممغنطة و وضعها في دعائم تخزين بغية كشف الحقيقة حول الجريمة المعلوماتية. وضع المشروع الجزائري في قانون 09-04 المتعلقة بتكنولوجيا الاعلام و الاتصال و مكافحتها طريقتين: أول تكون عن طريق نسخ المعطيات محل البحث و الثاني باستخدام التقنيات المناسبة [4].

ثانيا: الخبرة في الجرائم المعلوماتية.

للخبرة اهمية بالغة في مجال الجريمة المعلوماتية كونها تتعلق بشيكات الاتصال المرتبطة بالتخصصات العلمية و الفنية الدقيقة، فهي اجراء من اجراءات جمع الادلة لإحاطتها بمعلومات فنية تسمح باستنتاج و الوصول الى الدليل، فالخبرة تعد وسيلة من وسائل الاثبات هدفها جمع و كشف الادلة أو تحديد مدلولها من خلال الاستعانة بالمعلومات العلمية حيث يستند القاضي الى الخبرة لاتخاذ القرار المناسب.[5]

---

[1] – عيدة بلعابد ، مرجع سابق ، ص151.

[2] –زبيخة زيدان، مرجع سابق ، ص 148.

[3] – عيدة بلعابد، مرجع سابق ،ص 150.

[4] –لبيبات خولة، عميرات أميرة، مرجع سابق ،ص41 .

[5] –معش زهية، غانم نسيمة، مرجع سابق ، ص35 .

تفترض الخبرة وجود شيء مادي أو واقعة يستظهر منه الخبير رأيه نظرا لتقلقها بموضوع يتطلب الهاما بعلم معين لامكان استخلاص الدليل منه الذي يعتبر العنصر المميز في اثبات الدليل و الذي يتطلب معارف علمية خاصة لا تتوافر سواء لدى المحقق أو القاضي[1].

فالخبير هو الذي متخصص و صاحب خبرة في التقنية الالكترونية و شبكاتها و يكون قد رأى او سمع بحواسه معلومات هامة لازمة للدخول في نظام المعالجة الآلية الرقمية للبيانات اذا كانت مصلحة التحقيق تقتضي البحث عن الدليل الرقمي الالكتروني داخلة [2].

و بناءا على هذا صرح المشروع الجزائري لجهات التحقيق و للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم، حيث تنص المادة (143) من قانون الاجراءات الجزائية الجزائرية على: جهات التحقيق أو الحكم عندما تقرض لها مسألة ذات طابع فني أن يامر بندب خبير اما بناء على طلب النيابة العامة و اما من تلقاء نفسها أو الخصوم[3] في حين حدد المشروع اجراء بموجب نص المادة 125 من قانون الاجراءات المدنية و الادارية رقم: 08-09 المؤرخ في 2008/02/25 التي تنص على: "تهدف الخبرة الى توضيح واقعة مادية تقنية أو علمية محضة للقاضي".

- أنواع الخبرة في المجال المعلوماتي:

1- الخبرة الخاصة:

يعتمد هذا النوع من الخبرة على الاستعانة بأشخاص و كفاءة في مجال الحاسب الآلي و الانترنيت تعتبر خبرة فردية التي من أهم مظاهر الخبرة السائدة في هذا المجال، فهناك من الدول تقوم بمحاولة التعرف على قراصنة الذين تحولوا مع مرور ازمن الى رموز وطنية من جراء تحركاتهم عبر

[1] -أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتي، اطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث ل م د، تخصص قانون خاص، كلية الحقوق و العلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، 2020-2021، ص 162.

[2] -بوبعاية ابتسام ، مرجع سابق ،ص 45.

[3] -القانون رقم 66-155 مؤرخ في 08 يوليو 1966، المعدل و المتمم لقانون الاجراءات الجزائية، ج ر ج ج، ع 48، المعدل والمتمم للأمر 15-02، المؤرخ في 23 جويلية 2015، ع40، 2015.

الشبكة الالكترونية.[1]

2- الجهات التعليمية:

ان هدف المؤسسات التعليمية تطوير العلم و القضاء على المشكلات التي توجه الانسانية فهي بدورها يمكنها مواجهة الجريمة المعلوماتية حيث يتم تدعيمها ماديا و معنويا حتى تكون افضل سبيل للمواجهة و تمكينها من توفير خبراء على درجة علية من التفوق.[2]

3- جهات الضبط القضائي:

اسست الولايات المتحدة الامريكية منظمة الانتربول خصيصا لهذا المجال للخبرة و ايضا اعداد جهاز آخر و هو فرع جديد و ايضا اعداد جهاز آخر و هو فرع جديد في المباحث الفيدرالية الامريكية FBIهدفه مكافحة التصعيد الخطير في الجرائم المعلوماتية من خلال التصنيف و التحليل للدليل الرقمي و اهم دور يقوم به هذا المعمل هو التقاء العديد من منظمات الضبط القضائي من أجل التعاون فيما بينها.[3]

[1] -معمش زهية، غانم نسيمة، مرجع سابق ، ص 37.

2-خالد ممدوح ابراهيم ، مرجع سابق ،ص 299.

[3] -معمش زهية، غانم نسيمة، مرجع سابق ، ص38.

المطلب الثاني: الاجراءات الحديثة في الجريمة المعلوماتية.

نظرا لتطور طرق ارتكاب الجريمة المعلوماتية عن غيرها من الجرائم الاخرى فان المشرع الجزائري أكد على قواعد اجرائية حديثة لأجل مكافحة الجريمة المعلوماتية ، و بيان ذلك في القانون 06-22 المؤرخ في ديسمبر 2006 المعدل و المتمم للأمر رقم 66-155 المؤرخ في يوليو 1966 و المتضمن لقانون الاجراءات الجزائية[1]، سنتطرق في هذا المطلب الى التسرب الالكتروني (**الفرع الاول**) و التنصت والمراقبة الالكترونية في (**الفرع الثاني**).

الفرع الأول: التسرب الالكتروني.

والذي سندرس فيه تعريف التسرب الإلكتروني (**أولا**)، ثم تنفيذ عملية التسريب الإلكتروني (**ثانيا**).

أولا: تعريف التسرب الالكتروني:

عرف المشرع الجزائري التسرب من خلال نص المادة 65 مكرر 12 من قانون الاجراءات الجزائية بعد تعديله بقانون 22/06 و التي تنص على " يقصد بالتسرب قيام ضابط او عون شرطة قضائية، تحت مسؤولية ضباط الشرطة القضائية المكلفة بتنسيق العملية، بمراقبة الاشخاص المشتبه في ارتكابهم جناية او جنحة بإيهامهم أنه فاعل معهم أو شريك لهم، يسمح لضباط أو عون الشرطة القضائية أن يستعمل لهذا الغرض بهوية مستعارة ة ان يرتكب عند الضرورة الافعال المذكورة في المادة 69 مكرر 14 أدناه و لا يجوز تحت طائلة البطلان ان تشكل هذه الافعال تحريضا على ارتكاب الجرائم[2].

و يقصد بالتسرب اجراء يقوم به ضابط الشرطة القضائية أو أحد أعوانه تحت مسؤوليته بتنسيق العملية لمراقبة الاشخاص المشتبه فيهم بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.[3]

---

[1] -بوبعاية ابتسام، مرجع سابق ، ص 46.

[2] -المادة 65 مكرر 5 من قانون الاجراءات الجزائية، أمر رقم 66-156 ،مؤرخ في 8 جوان 1966، معدل و متمم وفقا للقانون 22/06، المؤرخ في 20 جويلية 2006 ،المتضمن قانون الاجراءات الجزائية، ج ر ج ج، ع 84، 2006.

[3] -المادة65 مكرر 12 من القانون 06-22 ،المتضمن قانون الاجراءات الجزائية المعدل و المتمم، ج ر ج ج.

جاء به المشروع الجزائري اذا اقتضت ضرورة التحري و التحقيق اللجوء له في الجرائم السبعة المحددة على سبيل الحصر و تتمثل في جائم المخمرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الجرائم الارهابية، جرائم تبيض الاموال، الجرائم المتعلقة بالتشريع الخاص بالصرف، اضافة الى جرائم القضاء.[1]

ثانيا: تنفيذ عملية التسرب الالكتروني.

اجاز المشروع الجزائري الاستعانة بمجموعة من الوسائل و القيام ببعض الافعال المنصوص عليها في المادة 65 مكرر 14 من القانون 06-22 دون ان يكون مسؤولا جزائيا و تتمثل في:

- اقتناء أو حيازة أو نقل أو تسليم أو اعطاء مواد أو أموال أو معلومات متحصل عليها من ارتكاب الجريمة أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي و كذا وسائل النقل أو التخزين أو الايواء أو الحفظ أو الاتصال.[2]

و منه التسريب الالكتروني يهدف لجمع البيانات و المعطيات الخاصة التي تشير الى كافة الاعمال الاجرامية و تمكين المصالح الامنية من معرفة الامكانيات المادية و البشرية المستعملة، و كذلك الاساليب و وسائل الاتصال و التنقل المستغلة من أجل ارتكاب أفعال مشبوهة.[3]

الفرع الثاني: التنصت و المراقبة الالكترونية

اجازت بعض التشريعات التنصت و المراقبة الالكترونية مثل التشريع الفرنسي و التشريع الهولندي لقاضي التحقيق ان يأمر بالتنصت على شبكات الاتصال الحاسب الآلي لهدف ضبط الجرائم الخطيرة و كذا امكانية التلكس و الفاكس و نقل البيانات.[4]

---

[1] -أومدور رجاء، مرجع سابق، ص177.

[2] -اومدور رجاء، المرجع نفسه ،ص ص: 179-178.

[3] - أعمر قادري، أطر التحقيق وفق أحكام نصوص الاجراءات الجزائية، ط2، دار هومة، 2015 ،ص 75.

[4] - معش زهية، غانم نسيمة مرجع سابق ،ص33.

أما القانون الجزائري المستحدثة في ديسمبر سنة 2006 نصوص قانونية تتعلق باعتراض المراسلات و تسجيل الاصوات و التقاط الصور و التي تضمن عدة أحكام منصوص عليها من المواد (65 مكرر 5 الى 65 مكرر 10) المتمثلة في امكانية قاضي التحقيق يأمر ضابط الشرطة القضائية بترخيص كتابي تحت اشرافه مباشرة للقيام باعتراض المراسلات التي تتم عن طريق الاتصال السلكية و اللاسلكية و وضع الترتيبات التقنية دون موافقة الشخص المعني من أجل القيام بالتقاط و تثبيت و تسجيل و بحث في سرية عن طريق وسائل الاتصال السلكية و اللاسلكية و وضع ترتيبات تقنية دون مراقبة المعنيين من اجل التقاط الصور و تثبي و بحث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية شخص أو عدة اشخاص في أماكن عامة أو خاصة.[1]

و هذا ما جاء به القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها في المادة 2 من الفقرة "و" في تعريفه للاتصال الالكترونية على أنها تراسل او ارسال او استقبال علامات او اشارات او كتابات أو صور او أصوات أو معلومات مختلفة بأي وسيلة كانت.[2]

و يقصد بالتنصت اجراء من اجراءات التحقيق تباشرها السلطة المختصة، للبحث عن ادلة اثبات الجريمة ضد شخص نسبت اليه ارتكابها أو لديه أدلة تتعلق بها و كانت هذه الجريمة على درجة من الخطورة لاتخاذ مثل هذا الاجراء الاستثنائي.[3]

و بالنسبة للمراقبة الالكترونية حدد المشرع الجزائري في القانون09-04 في المادة 03 منه كيفية مراقبة الاتصالات على النحو الاتي مع مراعاة الاحكام القانونين ،التي تتضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو مستلزمات و التحريات أو التحقيقات القضائية الجارية وفق للقواعد المنصوص عليها في قانون الاجراءات الجزائية، و في هذا القانون وضع ترتيبات تقنية لمراقبة

[1] -معش زهية، غانم نسيمة، مرجع سابق ،ص33.

[2] - بوبعاية ابتسام، مرجع سابق ،ص48.

[3] - معش زهية، غانم نسيمة، مرجع سابق ،ص33.

الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية.[1]

المراقبة الالكترونية هي من اهم الوسائل التقنية الحديثة للتحري عن مختلف الجرائم المتعلقة بالتكنولوجيا الحديثة، كما أنها مصدر للأدلة الرقمية ،و تتضمن نوعين من الرقابة، رقابة وقائية هدفها الوقاية من الجرائم المعلوماتية الخطيرة و مكافحتها، أما الثانية رقابة ضبطية قضائية تتضمن حالتين:

- الحالة الاولى: عندما يقتض الامر التحري و التحقيق في ذلك لاستصعاب القيام بذلك بالطرق العادية دون اللجوء الى المراقبة
- الحالة الثانية: و ذلك في ظل متطلبات التبادل و المساعدة القضائية بين الدول.[2]

المبحث الثاني: الدليل الرقمي لاثبات الجريمة المعلوماتية:

الى اثبات الجريمة المعلوماتية يعتمد بشكل كبير على جمع و تحليل الادلة الرقمية، لهذه الادلة تعد ضرورية لتحديد الجناة و اثبات وقوع الجريمة أمام المحاكم، حيث يختلف الدليل الرقمي عن الدليل الجنائي التقليدي هذه الاخيرة هي أدلة مادية ملموسة مرئية أو مسموعة يسهل على القضاء التعامل معها على عكس الدليل الجنائي الرقمي الذي لم تعيره القوانين اهتماما لأنه ظهر تدريجيا و حديثا بعض الشي تزامنا مع تزايد استخدام تقنية المعلومات الرقمية و تطورها و التي اصبحت تشكل مستودعا هاما للبيانات و المعلومات التي تساعد على الوصول الى الحقائق و كشف هذا النوع من الجرائم و تحقيق العدالة و الامن، لا يستطيع أن يتعامل معه الا أصحاب الاختصاص و أهل الخبرة[3]. سنتطرق في هذا المبحث في المطلب (**المطلب الاول**) الى الدليل الرقمي كوسيلة لاثبات الجريمة المعلوماتية و في (**المطلب الثاني**) الى حجية الدليل الرقمي لاثبات الجريمة المعلوماتية.

[1] -المادة 04 من القانون 09-04 ، مرجع سابق ، ص6.

[2] - لمادة 04 من القانون 09-04، المرجع نفسه.

[3] -د/ منصور عمر المعايطة، الادلة الجنائية و التحقيق الجنائي، دار الثقافة، ط 1، 2007، ص 16.

المطلب الأول: الدليل الرقمي كوسيلة لاثبات الجريمة المعلوماتية:

لقد تعددت الادلة الرقمية المستحدثة و ارتباطها بالحياة الرقمية لأفراد لكن قبل أن نذكر و نبين الادلة الرقمية يجدر بنا أن نعرف الدليل الرقمي ثم نبين أنواعه.[1] سنتطرق في هذا المطلب الى تعريف الدليل الرقمي و خصائصه (الفرع الاول) و الى تقسيمات الدليل الرقمي و مصادر الحصول عليه من الفرع الثاني.

الفرع الاول: تعريف الدليل الرقمي و خصائصه:

والذي سيتم دراسته كالتالي:

أولا: تعريف الدليل الرقمي:

تعريف الدليل لغة على أنه: المرشد و ما يتم به الارشاد و هو ما يستدل به، و الدليل هو الذال ايضا و الجمع: أدلة و دلالات[2] كذلك هو ما يستدل به و يقال أدلة فلان و فلان يذل فلان و الدليل المرشد أو الجمع أدلة و دلالات كما انه قد ورد ذكر الدليل في القرآن الكريم في قوله تعالى:" ثم جعلنا الشمس عليه دليلا"[3].

والدليل اصطلاحا: هو يتطلب معرفة أشياء أخرى أو هدفه ان يصل العقل الى اعتقاد ما او أمر مشكوك في صحته اي معرف الحقيقة [4].

أما الدليل في الاصطلاح القانوني فقد تعددت المحاولات في المجتمع الفقهي لوضع تعريف دقيق لها حيث عرفه البعض بأنه: الوسيلة التي يستخدمها القضاة لبلوغ الحقيقة المنشودة[5] او معنى الحقيقة في هذا السياق هو كل ما ينطق بالوقائع المقدمة الى القاضي بتطبيق حكم القانون، كما عرفها آخرون بأنها: الوقائع التي يستمد بالحكم الذي وصل اليه [6].

[1]- منصور عمر المعايطة، مرجع سابق ، ص 17.

[2]- منصور عمر المعايطة، المرجع نفسه ، ص17.

[3]- الآية 45، سورة الفرقان.

[4]- د/ بلهادي حميد، "حجية الدليل الرقمي في الاثبات الجنائي"، مجلة البحوث و الدراسات القانونية و السياسية، كلية و العلوم السياسية، جامعة البليدة2، المجلد 9 ،ع1، 2019، ص 15 .

[5]- د/ بلهادي حميد، المرجع نفسه، ص 16.

[6]- مأمون محمد سلامة، الاجراءات الجزائية في التشريع المصري ،دار النهضة العربية،ط2، القاهرة، مصر، 1992 ،ص191.

و يقصد بالدليل العلمي: النتائج التي تستمر عنها التجارب و الابحاث العلمية لتعزيز دليل مسبق تقدمه، سواء لاثبات أو نفي الواقعة التي يثور الشك حولها"[1].

- و فيما تقدم يمكننا القول بأن الدليل الجنائي بأنه: "مجموعة من الوقائع المادية و المعنوية اي تفيد في كشف اية جريمة و إظهار الحقيقة بصددها، و كل ما يقود الى صحة أو عدم صحة الواقعة أو الوقائع موضوع التحقيق، كذلك هو البرهان القائم على المنطق و العقل في اطار الشرعية الجزائية لاثبات صحة افتراض أو لرفع درجة اليقين الإقناعي في واقعة محل خلاف" [2]

- أما في المجال المعلوماتي هناك تعريفان مختلفة للمبادئ التوجيهية، سواء كانت واسعة أو ضيقة، و ذلك بسبب اختلاف الوضع العلمي الذي ينتمي اليه هذه المبادئ التوجيهية بين الباحثين في مجال القانون و التكنولوجيا الحديثة و من هنا سنحاول عرض أهم التعريفات فيما يلي:

يمكن أن تعرف الدليل بأنه هو البيانات التي يتم الحصول عليها من جهاز الكمبيوتر، و تكون على شكل مجالات أو نبضات مغناطسية و كهربائية يمكن جمعها و تحليلها باستخدام برامج و تطبيقات تكنولوجيا المعلومات [3] .

و هناك فريق آخر يعرف الدليل الرقمي بأنه: الادلة المقدمة من أو بالاستعانة بأنظمة برمجيات المعلومة الحاسوبية أو الاجهزة و المعدات و الادوات الحاسوبية أو الاجهزة و المعدات و الادوات الحاسوبية أو شبكات الاتصال، التي تقدم الى السلطات القضائية بعد الاجراءات القانونية و الفنية و التحليل العلمي [4] أو التفسير على شكل كلمات مكتوبة أو صور أو رسوم أو أشكال أو أصوات لاثبات ارتكاب الجريمة و اثبات البراءة أو الادانة[5].

---

[1]- بلهادي حميد، مرجع سابق ، ص 16.

[2]- بن فريدة محمد، "الدليل الجنائي الرقمي و حجيته أمام القضاء الجزائي (دراسة مقارنة)"، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر، ع 1، 2014، ص 277.

[3]- سالمي نضال، "الاطار التنظيمي للدليل الرقمي في الاثبات"، مجلة القانون والمجتمع ، كلية الحقوق و العلوم السياسية، جامعة وهران2،محمد بن احمد الجزائر، المجلد 10، ع1، 2022، ص 332.

[4]- بلهادي حميد، مرجع سابق ، ص 17.

[5]- عائشة بن قارة مصطفى، مرجع سابق، ص ص: 52-53.

و كما تبين فيما سبق فان الادلة الجنائية الرقمية هي بيانات رقمية مكونة من مجموعة من الارقام و الحروف و الرموز، تمثل معلومات و بيانات متنوعة بما في ذلك النصوص و الرسومات و الخرائط و الصور و الفيديوهات و غيرها من روابط المعلومات و تحتوي على البيانات المتعلقة بالافراد و الاشخاص الاعتباريين و الجماعات تكون مخزنة في أجهزة الكمبيوتر و ملحقاتها مثل الديسكات و الاقراص المرنة و غيرها من وسائل تطنولوجيا المعلومات مثل الطابعات و الفاكس أو من خلال شبكات نقل الاتصال و الانترنيت. كذلك استخدام التطبيقات و التقنيات الخاصة بالجمع و التحليل بهدف اثبات وقوع الجريمة و نسبتها الى مرتكبها[1].

ثانيا: خصائص الدليل الرقمي:

يتميز الدليل الرقمي بمجموعة من الخصائص التي تميزه عن غيره من طرق الاثبات و هي :

1- الدليل الرقمي دليل علمي:

الدليل الرقمي هو الحدث الذي يبني على وقوع جريمة او فعل غير قانوني، كما هو واقعه أساسها علمي من حيث ان اساس هذا العالم الرقمي هو اسا علمي حيث يصعب الحصول على الادلة الرقمية او الاطلاع على محتوياتها و لذلك و وفقا لقاعدة العدالة المقارنة فان استخدام الاساليب العلمية للعثور عبى الادلة يجب أن يكون متسعا مع مجموعة الحقائق و وفقا لقاعدة في القضاء المقارن مفادها "ان هدف القانون العدالة اما العلم فمسعاه الحقيقة" هذه الميزة مفيدة أيضا عندما نتطرق لمشكلة حفظ الادلة لان عملية الحفظ يجب أن تكون مبنية على اسس عملية كما ان تحرير محضر يتضمن دليلا علميا يختلف عن تحرير محضر يتناول جرعة عادية حيث يجب أن تكون هناك طريقة خاصة و علمية في تحريره لتتوافق مع ظاهرة الدليل العلمي تحديدا بحيث يجب أن لا يتخذ المحضر المظهر التقليدي[2] .

[1]-عائشة بن قارة مصطفى، مرجع سابق ، ص54 .

[2]- بلجراف سامية، "سلطة القاضي الجزائي في قبول و تقدير الدليل الرقمي"، مجلة الدراسات القانونية المقارنة، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، المجلد 7، ع1، 2021، ص 681.

2- الدليل الرقمي ذات طبيعة تقنية:

الادلة الرقمية ليست كالأدلة المادية التي يمكن استخلاصها بمجرد مشاهدتها أو النظر اليها بل انها في كثير الاحيان لا تكشف عن جريمة محددة بعد ما تشير و تثبت وجود مجرم معين، و تكمن هذه الخاصية في الجرائم الالكترونية فمثلها مثل الجرائم الالكترونية، يصعب على جهات التحقيق تحديد أصل المرسل و مكان مرتكب الجريمة لذلك يمكننا القول أنه لا يوجد دليل رقمي خارج البيئات التقنية أو مصادر البيانات الرقمية.[1]

3- الدليل الرقمي دليل يصعب التخلص منه:

و هذه من اهم الخصائص التي تميز الادلة الرقمية عن الادلة التقليدية فهناك العديد من برامج الكمبيوتر التي وظيفتها استعادة البيانات التي تم حذفها سواء كانت صورا او نصوص، أو رسومات أو غيرها، و هذا يعني أنه من الصعب على المجرمين اخفاء جرائمهم أو الاختباء من الامن و العدالة كذلك يتم تسجيل أنشطة المجرم المتمثلة في حذف الادلة الرقمية في ذاكرة الالة و استخراجها و تقديمها كدليل ضده [2].

4- الدليل الرقمي غير ملموس:

اي يتكون من بيانات و معلومات ذات هيئة الكترونية غير مرئية، و للتعرف عليها يتم استخدام أجهزة و معدات الحاسب الآلي (HARDUARE) و نظم برمجيات الكمبيوتر (SOFTWARE) [3].

[1]-يس حسن محمد عثمان، "الدليل الرقمي و أثره على الدعوى الجنائية"، مجلة العلوم القانونية والاجتماعية، كلية القانون والشريعة، قسم القانون، جامعة زيان عاشور بالجلفة، الجزائر، 2020 ،ص 320 .

[2]- سارة مساعدي، مشروعية الوسائط الرقمية في الاثبات الجنائي، المجلة الجزائرية للأمن الانساني، جامعة الجزائر 1،المجلد 5، ع1، 2022،ص 772.

[3]- عائشة بن قارة مصطفى، مرجع سابق ، ص61.

5- الدليل الرقمي قابل للنسخ:

هذه الخاصية تقلل أو تقضي على مخاطر اتلاف المعلومات الاصلية للدليل، بحيث تتطابق طريقة النسخ مع طريقة الانشاء مما يشكل ضمان فعال للحفاظ على الدليل من التلف، عن طريق نسخ طبق الاصل من الدليل الاصلي [1].

الفرع الثاني: تقسيمات الدليل الرقمي و مصادر الحصول عليه:

والذي تضمن مايلي:

أولا: تقويمات الدليل الرقمي

للدليل الرقمي أشكال مختلفة، حيث حددت وزارة العدل الامريكية سنة 2002 ان الدليل الرقمي يكن تقسيمه الى ثلاثة أقسام وهي: [2]

1- **السجلات المحفوظة في الحاسوب**: و هي الوثائق المحفوظة أو المخزنة مثل " البريد الالكتروني، رسائل غرف الدردشة، برامج المعالجة" [3].
2- **السجلات التي تم انشاؤها بواسطة الكمبيوتر**: و التي تتمثل في سجلات الهاتف و فواتير أجهزة السحب الآلي (ATM) و الكرت الالكتروني الذكي (LOG FILS) التي لا يستطيع الانسان أن يلمسها.
3- **السجلات المختلطة**: أي التي جزء منها تم حفظه بالإدخال و جزء آخر تم انشاؤه بواسطة الحاسب الالي، منها أوراق العمل المالية التي تم حفظها بالإدخال ثم معالجتها عن طريق برنامج EXEL لإجراء العمليات الحسابية[4] .

[1]- بهنوس آمال، "الدليل الرقمي في الإجراءات الجنائية"، المجلة الاكاديمية للبحث القانوني، جامعة وهران2، محمد بن أحمد، الجزائر، مجلد 16، ع2 ،2017 ،ص 178.

[2]- بن فردية محمد، مرجع سابق ، ص 249.

[3]- يس حسن محمد عثمان ، مرجع سابق ، ص 219.

[4]- يس حسن محمد عثمان ، المرجع نفسه ،ص 219.

و بالتالي هذه التقسيمات هي ببساطة تفسيرات للمصدر الذي تأتي منه الادلة الرقمية و كيفية استخلاص الاستدلالات فمن المعروف أن الجريمة الالكترونية هي جريمة تستمر في التطور مع تطور التكنولوجيا و أجهزة الكمبيوتر، و هنا لا بد من تطوير الادلة الرقمية لمواكبة التقدم، و الا فلن تتمكن من اثبات الجرائم فلا يقتصر استخدام الادلة الرقمية على الجرائم المعلوماتية فقط بل يمكن استخدام تلك الرموز و الارقام في القضايا المدنية كذلك لا سيما في نزاعات الحقود الالكترونية و ليس في الشق الجنائي فقط فالأدلة الرقمية تساعد كثيرا في تحقيق العدالة [1] .

ثانيا: الاشخاص المختصين بالبحث و التحري عن الجرائم المعلوماتية و مميزاتهم:

من المعروف أن سلطات التحقيق في الجزائر لديها صلاحية البحث و التحقيق في الجرائم و كتابة التقارير عنها و هي الشرطة القضائية و لها فروع و أشكال مختلفة، و يمكن للقضاة ذوي الاختصاص الأصلي اجراء التحقيقات و حتى القضاة قد يحكمون بطريقتهم الخاصة اذا رأوا ضروريا، و القضية الاساسية التي تواجه المحققين في جرائم انظمة المعلومات هي خلفية المحققين أنفسهم ، حيث قد يكون لدى خبير الكمبيوتر المعرفة التقنية اللازمة و لكنه ليس مدرب على تفهم دوافع الجريمة و جمع الادلة لتقديم المتهم للمحاكمة[2].

حيث يجب ان يكون المحققون على دراية بجميع جوانب التحقيقات و الجرائم، و هو أمر ضروري لحسن تنفيذ الاجراءات و التطبيق الامثل للأحكام القانونية و الذي بدوره يمكن أن يحقق العدالة في كثير من القضايا.

[1]- يس حسن محمد عثمان ، مرجع سابق ،ص 220.

[2]- يس حسن محمد عثمان ، المرجع نفسه ، ص 221.

نجد أن خبير الكمبيوتر يظن ان لديه أدلة قاطعة حول جريمة الكترونية، لكن من الناحية القانونية اتضح فيما بعد أن هذا الدليل لا يصلح لقضية ما، في حين أن المحقق يتمتع بخلفية قانونية و خبرة تحقيقية واسعة لكنه يفتقر الى الفهم الكافي لتقنيات الكمبيوتر التي يستخدمها مجرمو الانترنيت في مثل هذه الجرائم[1] .

1- الخصائص الفنية:

من مشاكل الحصول على الادلة الرقمية أن أفراد الشرطة القضائية يفتقرون للمؤهلات الكافية في المجال التقني، و بسبب جهلهم لأساليب الجرائم الالكترونية، حيث أفهم كثيرا ما يرتكبون الاخطاء مما قد يؤدي الى تدمير الادلة و حذفها مثل تدمير محتويات الاقراص و حاويات المعلومات التي يتم تخزين البيانات فيها لذا فان الكشف عن هذه الجرائم يتطلب أن تكون الجهات المعنية على دراية كاملة بأساسيات التعامل مع هذه الجرائم و كيفية التحقق فيها و عليه يجب على الضابط أو المحقق الالكتروني أن تتوفر فيه مجموعة من الشروط و هو ما سنناقشه فيما يلي: [1]

أ- الدراية الفنية:

ان المعركة من أجل العثور على الأدلة الرقمية لا تدور بين المحقق و الجهاز أو البيانات، بل بين عقل المحقق و عقل الجاني لذا يتعين على المحققين أن يفهموا طريقة عمل أجهزة الكمبيوتر و تكوينات الانترنيت و حفظ البيانات و تخزينها من فهم المحققين لهذه المبادئ، اذ من الضروري ان يتخيلوا كيف يمكن تنفيذ الجرائم في العالم الافتراضي، بما في ذلك اختراق الشبكات و اعتراض الحزم و اجتياز الشبكة،

[1]- سمير رفعي، "البحث و التحري عن الجريمة الالكترونية"، دار المثقف ،ط1،ا لجزائر، 2019 ،ص 70.

[1]- سمير رفعي، المرجع نفسه، ص71.

و التجسس عليها و اعادة توجيهها، كما انها تعطي للمحققين تصور جيدا عن مدى امكانية متابعة مصدر الاعتداء على الشبكة و المعوقات التي تحول دون ذلك هذا كله لن يتمكن منه المحقق اذا لم يكن خبير في هذا المجال [1].

ب- اتباع الاجراءات الصحيحة و المشروعة:

" ان صحة الاجراءات كما هي عامل أساسي عل المحققين معرفته فهو أكثر أهمية بالنسبة للجريمة المعلوماتية من أجل سرعة المحافظة على الادلة الالكترونية التي تدل على وقوع الجريمة من عدمه، و نسبتها لشخص الجاني و تخزينها في الاقراص المعدة لذلك وضع حذفها و الحرص على عدم تعريض سائط التخزين كالأقراص المرنة أو المدمجة لأية مؤثرات خارجية كالقوى حتى لا تتلف محتوياته [2] ".

1- التأهيل و التدريب.

ان طبيعة الجريمة المعلوماتية و ارتباطها بأجهزة الكمبيوتر تتطلب فهما واضحا لأنظمة الكمبيوتر و كيفية تشغيلها و أساليب اساءة استخدامها من قبل المستخدمين و لا يمكن اكتساب هذه المعرفة التقنية الا لتدريب المسؤولين عن أعمال التحقيق و التحريات المباشرة حيث دعا البعض في مجال الجرائم المعلوماتية الى النقاش حول ضرورة وجود خبراء و مكاتب نيابة متخصصة في هذا المجال[3].

و يجب أن يشمل التدريب كيفية تشغيل جهاز الكمبيوتر و ذلك يعد التعرف على أنواع و أنظمة أجهزة الكمبيوتر المختلفة، و اكتساب المهارات المعرفية المتعلقة بالبرمجة و معالجة البيانات الالكترونية و الجرائم التي تحدث على أجهزة الحاسوب، و كذلك أمن الكمبيوتر و طرق الاختراق و دراسة تطبيقية، أمثلة عن الجرائم التي حدثت من قبل و كيفية مواجهتها.[4]

---

[1]- سمير رفعي، مرجع سابق ، ص 71.

[2]- سمير رفعي، المرجع نفسه ، ص 72.

[3]- سمير رفعي، المرجع نفسه ، ص 72.

[4]- سمير رفعي، المرجع نفسه ، ص ص: 72- 73.

و في كثير بلدان العالم تعقد الدورات التدريبية المتخصصة لرجال الشرطة و أعضاء النيابة العامة، سواء داخل أو خارج الوطن أو في مراكز تابعة لوزارة الداخلية أو في المراكز المتخصصة التابعة لوزارة العدل، كما هو الحال في أمريكا و انجلترا و كندا، و هو ما يعمل به حاليا في الجزائر على مستوى مختلف الاجهزة المتخصصة في هذا النوع من القضايا و من أمثلها ما تقوم به المديرية العامة للأمن الوطني في هذا الباب حيث سطرت برنامجا لتكوين الملازمين الأوائل للشرطة يتطرق الى موضوع الجرائم الالكترونية منذ 2003. [1]

المطلب الثاني: حجية الدليل الرقمي لاثبات الجنائي .

ان مجرد الحصول على الادلة الالكترونية و تقديمها للقضاء لا يكفي للاعتماد عليها كدليل ادانة ، حيث ان الطبيعة الفنية للأدلة الرقمية تجعلها عرضة للتلاعب، علاوة على ذلك فان نسبة الخطأ في عملية الحصول على الادلة الصادقة تبدو عادية في مثل هذا النوع من الادلة لذلك تثور فكرة الشك في مصداقيتها كأدلة الاثبات الجنائي.[2] سنتطرق في هذا المطلب الى محل الدليل الرقمي و شروط الحصول عليه في الفرع الاول و الى موقف المشرع الجزائري بين الدليل الرقمي و تقديره أمام القضاء في الاثبات الجنائي في الفرع الثاني.

الفرع الاول: محل الدليل الرقمي و شروط الحصول عليه.

ان مسألة تقييم الدليل الجنائي في اثبات الوقائع الجرمية مسألة موضوعية محصنة للقاضي السلطة التقديرية المطلقة فيها.

أولا: تقييم الدليل الرقمي من حيث سلامته من التزوير

[1]- سمير رفعي، مرجع سابق ، ص ص: 72 و 73 .

[2]- نور الهدى محمودي، "حجية الدليل الرقمي للإثبات الجريمة الالكترونية"، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، ع11،جوان 2017، ص918.

يمكن التأكد من الدليل الرقمي من التلاعب بعده طرق نذكر منها:

- فكرة التحليل التخاطري الرقمي و التي من خلالها يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالأدلة الرقمية و من تم يتأكد من صدى حصول تلاعب في النسخة المستخرجة أم لا، و يستعان في ذلك باستخدام الحاسب الالي الذي يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في مضمون الدليل الرقمي، و هذا العلم يستعان به أيضا في كشف مدى التلاعب بمضمون هذا الدليل [1].
- استخدام عمليات حسابية خاصة تسمى الخوارزميات و يلحق الى هذه التقنية في حالة عدم الحصول على النسخة الاصلية للدليل الرقمي و في حالة التلاعب بالنسخة الاصلية بالإمكان التأكد من سلامة الدليل الرقمي من التحريف و التغيير باستعمال هذه العمليات الحسابية [2].
- استعمال الدليل المحايد و هو نوع من الادلة الرقمية للمخزون في البيئة الافتراضية لا علاقة له بمحل الجريمة في حين أنه يساعد في التأكد من مدى سلامة الدليل الالكتروني المقصود من حيث عدم حصول أي تعديل عليه في نظام الحاسب الآلي من جانب آخر تمثل الخبرة الفنية و التقنية دورا مهما في التأكد من سلامة الدليل الرقمي، فاذا كان للخبرة الفنية أهمية كبيرة في مجال الحصول على الدليل الرقمي، في المقابل لها ذات الدور في مصداقيته و تقييمه من حيث عدم حصول اي غلطة فيه، فنقص الثقافة المعلوماتية للقاضي الجزائي قد يحتم عليه كواجب قضائي ان يستعين في هذه المسائل بوسائل الخبرة كمنهج و هذا ليس من أجل استخلاص الدليل، فحسب و انما للبحث عن مصداقيته في مجال المعالجة الالية للمعلومات و تحقيق اليقينية لهذا الدليل [3].

[1]- ياسين بن عمر، "المعالجة القانونية الالكترونية في القانون الجزائري والتشريعات المقارنة"، مجلة العلوم القانونية و السياسية، جامعة باتنة، مجلد10، ع3، 2019، ص720.

[2]- خالد عياد الحلبي، "اجراءات التحري و التحقيق في الجرائم الحاسوب و الانترنيت"، دار الثقافة للنشر و التوزيع،ط1 ، عمان، ص 249.

[3]- خالد عياد الحلبي، المرجع نفسه، ص251.

ثانيا: تقييم الدليل الرقمي من حيث السلامة الفنية للاجراءات المتبعة في الحصول عليه

سبق الحديث على أن الدليل الالكتروني يتم استخلاصه باتباع مجموعة من الاجراءات الفنية و التي من الممكن أن يعتريها خطأ يشكك في مصداقية نتائجها الامر الذي يحتم اخضاعها الى اختبارات كوسيلة للتأكد من سلامة هذه الاجراءات من حيث انتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل اثبات و يتبع في ذلك مجموعة من الخطوات و هي:

- اخضاع الاداة المستخدمة لعدة تجارب للتأكد من الحصول على نتائج ، و يكون ذلك من خلال اتباع اختبارين أساسيين يتم التأكد من خلالها أن الادلة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الالكتروني حيث عدل الاختباران في :اختيار السلبيات الزائفة و مفاده أن تخضع الادلة المستخدمة في الحصول على الادلة لاختباريين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي و أنه لم يتم اغفال معطيات مهمة عنه، أما فيما يخص الاختبار الثاني و الذي يجري باختيار الايجابيات الزائفة مفاد اخضاع الادلة المستخدمة في الحصول على الدليل الرقمي، للاختيار يمكن من التأكد من أن هذه الوسيلة لا تعرض معطيات اضافية جديدة[1].
- الاعتماد على الادوات التي اثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل اذ بينت الدراسات العلمية و البحوث المنشورة في مجال تقنية المعلومات بالطرق السليمة التي يجب اتباعها في استخلاص الدليل الرقمي، و في المقابل بينت تلك الدراسات ايضا الادوات المشكوك في كفاءتها و هو ما يساهم في تحديد مصداقية المخرجات المستمدة من تلك الادوات [2].

[1]-بوبعاية ابتسام، مرجع سابق ،ص 61.

[2]- ياسين بن عمر، مرجع سابق ،ص 721.

- من خلال ما تقدم يمكن الوقوف على سلامة الدليل الالكتروني اذا توافرت في هذا الاخير الشروط العامة لما يمكن أن يمثل أساسا لتأكد الثقة في حين يمكن اهمال الشروط الخاصة كذلك و التي هي جد مهمة كذلك في استخلاص من الدليل الرقمي و التي تتمثل في:

1- يجب الحصول على الدليل بطريقة مشروعة " مبدأ مشروعية المخرجات الالكترونية":

يجب على القاضي الجنائي أن يستقي قناعته في الحكم من خلال أدلة مشروعة أما الأدلة التي جاءت وليدة اجراءات غير قانونية أو غير مشروعة أو باطلة فلا يجوز الاعتماد عليها و يجب طرحها نهائيا استنادا الى قاعدة مهمة و معروفة في القانون و هي " ما تبنى على باطل فهو باطل"، حيث أن المشروع بهدف الى اقتضاء و تأمين ضمانات المتهم و أولها حقه المقدس في الدفاع عن نفسه و اذا كان الدليل معيبا أو مشكوك فيه وجب استبعاده من بين الادلة و اذا لم تفعل المحكمة ذلك حكمها باطلا .[1]

فاقتناع القاضي القائم على الدليل الصحيح هو تطبيق للقواعد العامة التي توجب على المحاكم عدم الاعتراف الا بالإجراءات المشروعة و انه لا يكفي لسلامة الحكم أن يكون الدليل صادقا متى كان وليد اجراء غير مشروع لان الباطل يبطل الدليل و يعدمه و يبطل الحكم الذي بني عليه. [2]

فمسألة البحث على الدليل مقيدة باحترام حقوق الدفاع و قيم العدالة و اخلاقياتها و مقتضيات الحفاظ على كرامة الانسان و هو ما لا يمكن ان يتأتى الا اذا كان البحث عن الدليل قد تم باستخدام اجراءات مشروعة، فالطرق غير المشروعة للتحقيق يترتب عليها حتما عدم شروعية الدليل المستخلص و عدم قبوله في الاثبات [3].

1- ممدوح خليل البحر، "نطاق حرية القاضي الجنائي في تكوين قناعته الوجدانية"، مجلة الشريعة و القانون، مجلة علمية محكمة تصدر عن كلية الشريعة و القانون ،جامعة الامارات العربية المتحدة، ع 21 ، يونيو 2004 ،ص 353 .

2- ممدوح خليل البحر، المرجع نفسه، ص 354.

3- غانية خروفة، "سلطة القاضي الجنائي في تقدير الخبرة" ،رسالة ماجستير في قانون العقوبات و العلوم الجنائية، كلية الحقوق و العلوم السياسية ،جامعة منتوري ،قسنطينة، 2008 -2009، ص 101.

و على هذا الاساس فان اجراءات جمع الادلة الالكترونية المستخلصة من الوسائل الالكترونية اذا خالفت القواعد الاجرائية التي تنظم كيفية الحصول عليها لا تصلح ان تكون ادلة تبنى عليها الادانة في المواد الجزائية ،و من قبيل الادلة الرقمية غير المشروعة تلك المتحصل عليها من خلال اجراء مراقبة الاتصالات دون ان يكون محلا لاذن من السلطة القضائية المختصة او اتخاذ ترتيبات تقنية من اجل تفتيش منظومة معلوماتية تؤدي الى المساس بالحياة الخاصة للغير، او ممارسة اي اكراه معنوي او مادي على المشتبه فيه لفك شيفرة نظام من النظم المعلوماتية، أو بعد من الطرق غير المشروعة استخدام التدليس و الغش و الخداع في الحصول على الادلة الالكترونية [1] .

2- يجب أن تكون الادلة الرقمية غير قابلة للشك أي يقينية "مبدأ يقينية الدليل الرقمي":

يشترط أن تكون الادلة المستخلصة من الحاسب الالي و الانترنيت غير قابلة للشك حتى يتمكن القاضي بالحكم بالإدانة ذلك انه لا مجال للحض قرنية البراءة توقع عكسها الا عندما يصل اقتناع القاضي الى حد الجزم و اليقين و يمكن التوصل الى ذلك من خلال ما يعرض من الادلة الرقمية و المصغرات الفيلمية و غيرها من الاشكال الالكترونية المتوفرة . هكذا يستطيع القاضي من خلال ما هو معروض من الادلة عليه من مخرجات الكترونية و ما ينطبع في ذهنه من تصورات و احتمالات بالنسبة لها أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة الالكترونية الى شخص معين من عدمه كما يتحقق التميز للأدلة الرقمية أكثر بإخضاعها للتقييم التي بوسائل فنية و التأكد من سلامة صحة الاجراءات المتبعة في الحصول عليه من أجل تفادي العيوب التي تشويه [2].

[1]- سعيداني نعيم، مرجع سابق ، ص 217.

[2]- سعيداني نعيم، المرجع نفسه ، ص 218.

ان النتيجة التي بتطلبها اليقين القضائي في الدانة هي وجوب تفسير الشك لمصلحة المتهم حيث يستمد أصوله من قرينة البراءة ، و تعتبر قاعدة الشك المضرة لمصلحة المتهم هي من أهم الضمانات لاقتناع القاضي، فاذا لم تتوصل الجهة القضائية من خلال الادلة المجتمعة لديها الى اليقين باستناد التهمة الى المتهم الموجود أمامها فهنا يتعين عليها أن تحكم بالبراءة [1] .

3- امكانية مناقشة الادلة الرقمية المستخرجة من الحاسوب و الانترنيت:

و يقصد بهذا الضابط وجوب استخلاص القاضي لقناعته من الادلة القضائية أي تلك التي طرحت في الجلسة بحضور الخصوم و بصورة عالية، و هذا الضابط لمبدأ حرية القاضي في الاقتناع يحقق العدالة و يكشف الحقيقة و يضمن الدفاع من خلال فتح باب المناقشة العلنية أمام الخصوم فيما يقدم من أدلة و لا يكفي في الادلة أن تقدم اثناء الجلسة و أن يمكن الخصوم من مناقشتها بصورة علنية بل لا بد للاستناد اليها من أن يكون لها أصل في أوراق الدعوى[2].

كما أكدت المحكمة العليا في حكم لها بتاريخ 12-01-1982 " لا يمكن لقضاة الموضوع أن يؤسسوا قرارهم الا على الادلة المقدمة لهم أثناء المرافعات" [3] و هذا استنادا لنص اعادة 212 من قانون الاجراءات الجزائية الجزائري فقرة 02 و التي تقول: " و لا يسوغ للقاضي أن يبني قراره الاعلى الادلة المقدمة في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه" [4]

[1]- محمد مروان، نظام الاثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية ،الجزائر، 1999 ،ص 511 .

[2]- ممدوح خليل البحر، مرجع سابق ، ص ص: 181-182.

[3]- خالد عوني خطاب المختار، دور الوسائل العلمية الحديثة في الاثبات الجنائي، دار الكتب القانونية، مصر، 2017 ،ص 55.

[4]- المادة 212 من الأمر 66-155، المؤرخ في 08 جوان 1966، المتضمن قانون الاجراءات الجزائية، ج ر ج ج، المعدل و المتمم، ع48، 1966.

معنى ذلك أن العلنية توفر ضمانا للمتهم بأن تمكنه من الدفاع عن نفسه و عدم طرح الدليل للمناقشة اجراء موجب للبطلان كما يجوز للقاضي أن يستكمل اقتناعه الذاتي بالتحقيق الذي يتخذه في الجلسة بسماع الشهود و الخصوم بما يمكنه من استجلاء الحقيقة[1] فقاعدة وجوب مناقشة الدليل تعتبر ضمانة هامة و أكيدة للعدالة حتى لا يحكم القاضي الجزائي بمعلوماته الشخصية أو بناء على رأي الغير. [2]

الفرع الثاني: موقف المشرع الجزائري بين الدليل الرقمي و تقديره أمام القضاء في الاثبات الجنائي .

يتوجب على القاضي الجزائي سواء كان قاضي التحقيق أو غرفة الاتهام أو المحكمة الجزائية أن يقيم الدليل على المتهم و لا يجوز أن يحاكم المتهم و يدينه لمجرد وجود قرائن فقط بل لا بد أن تكون هذه الدلائل مكملة لبقية الادلة المادية الاخرى، كما يجب أن تتسم اجراءات جمع الادلة بالمشروعية كما ذكرتا سابقا في شروط اكتساب الدليل الرقمي و هذا احتراما للحرية الشخصية للمتهم فالمتهم برئ حتى تثبت ادانته [3] .

كما ان الاثبات الجنائي هو كل ما يؤدي الى كشف الجريمة و تطبيق الدليل على وقوعها و التأكد من ان المتهم هو مرتكب الجريمة بالفعل حيث يعتبر الدليل هو الوسيلة القانونية التي يستعين بها القاضي للوصول للحقيقة حيث تنتمي الجزائر الى مجموعة الدول التي تبني على نظام الاثبات الحرفي مجال الاثبات الجنائي فهي تساير النظم اللاتينية كفرنسا و بلجيكا و الاردن و سوريا و هو الامر الذي كرسته المادة 212 من قانون الاجراءات الجزائية السابقة الذكر و التي جاءت في نصها:

[1]- بوزيد اغليس،" تلازم مبدأ الاثبات الحر بالاقتناع الذاتي للقاضي الجزائي"، دراسة تحليلية مقارنة بين القانون الجزائري و القانون المصري والقوانين العربية، دار الهدى الجزائر، ط 2010، ص 120.

[2]- غانية خروفة، مرجع سابق ، ص 99.

[3]- ياسين بن عمر، مرجع سابق ، ص 721.

" يجوز اثبات الجرائم بأي طريقة من طرق حكمه تبعا لاقتناعه الخاص و لا يجوز للقاضي ان يبني قراره الا على الادلة المقدمة له في معرض المرافعات التي حصلت المناقشة فيها حضوريا أمامه" [1].

يمكن قرار المشرع الجزائري للحرية في تقديم الادلة المقنعة للقاضي الموضوع هو لتعزيز اثبات قرينة البراءة، و تعزيز ممارسة حقوق الدفاع الفردية غير أن هذا الاطلاق بدون تحديد و تخصيص يعد قصورا تشريعيا واضحا حيث لا نجد ضمن قانون الاجراءات الجزائية ما يدل على ان الدليل الرقمي هو دليل من نوع خاص شانه شأن الجرائم المعلوماتية فغياب النصوص القانونية في هذا الشأن يؤدي الى ظهور معضلات متعلقة بطبيعة الادلة المقدمة أمام السلطات القضائية بحيث يمكن [2] لهذه الاخيرة في حال عدم المامها بتقنية المعلومات دحض هذا الدليل و عدم الاعتماد عليه و لو كان حائزا على القوة التشريعية و توفر فيه كافة الشروط المصداقية و كذلك العكس.

أما فيما يخص سلطة القاضي الجزائي في تقدير الدليل الرقمي فان المادة العلمية للدليل الالكتروني جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، فهناك فريق من الفقهاء يرى أن الدليل العلمي و منه الدليل الرقمي له قوته الثبوتية الملزمة حتى للقاضي مستندين في رأيهم الى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها الى درجة اليقين و في المقابل هناك فريق آخر من الفقهاء يرى أن مبدأ حرية القاضي في الامتناع تكمن في ان يبسط القاضي كل سلطته على الادلة دون استثناء حق على الدليل الرقمي معتبرين أضفاء الدليل الرقمي صفة القوة الثبوتية التي لا يستطيع القاضي مناقشتها او تصديرها ، و يعد بمثابة الرجوع الى مذهب الاثبات القانوني المقيد و المشروع الجزائري كما سبق بيانه اجاز اثبات الجرائم بأية طريقة من طرق الاثبات ماعدا الجرائم التي يتطلب اثباتها دليلا معينا و منح

[1]- المادة 212 من الأمر 66-155، مصدر سابق.

[2]- بوبكر رشيدة ،جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائي المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2012، ص 507 .

القاضي الجزائي سلطة تقدير الدليل و الجرية في تكوين قناعته من اي دليل منعدمة فيه اي نسبة من الشك لإيصاله الى الحقيقة و تقدير الحكم المناسب .[1]

[1]- بوبكر رشيدة، مرجع سابق ،ص 508.

خلاصة الفصل الثاني:

تطرقنا في هذا الفصل الى آليات التحقيق في الجرائم التقليدية لإثبات الجريمة المعلوماتية و المتصلة في المعاينة والتفتيش، و التي هي تنقل المحقق الى مسرح الجريمة لفحصه لإيجاد شيء يتعلق بالجريمة قصد كشف الحقيقة بالإضافة الى التفتيش، و الذي يعد اجراء تحقيقي الغاية منه الحصول على ادلة جنائية تفيد في اثبات أو نفي الجريمة المرتكبة، حيث تكلمنا ايضا عن الضبط الذي يختلف بدوره في الجريمة المعلوماتية عن الجرائم الاخرى من حيث المحل، و يأتي دور الضبط به عملية التفتيش المعلوماتي و ضبط الادلة. حيث ان للخبرة أهمية بالغة و التي تساعد القاضي في اتخاذ القرار المناسب في المقابل تكلمنا عن الاجراءات الحديثة للكشف عن الجرائم المعلوماتية و المتمثلة في التسريب الالكتروني و هو اجراء يقوم به ضابط الشرطة القضائية أو أحد أعوانه لمراقبة الاشخاص المشتبه فيهم. بالإضافة الى التصنت عليهم عن طريق الاتصالات السلكية و اللاسلكية ،كما عرجنا كذلك على وسيلة هامة للكشف عن الجرائم المعلوماتية ايضا و هي الدليل الرقمي، الذي لديه صورة كبيرة لتحديد الجناة و اثبات وقوع الجريمة أمام المحاكم و سلطة القاضي الجزائي في تقديره.

خاتمة

تبين من خلال دراستنا لموضوع التحقيق في الجريمة المعلوماتية انها عملية معقدة تشمل مجموعة الاساليب و التقنيات للوصول للدليل الرقمي، لكون الجريمة المعلوماتية بطبيعتها من اصعب انواع الجرائم الاخرى نظرا لتطور التكنولوجيا و الانترنيت و الاحترافية في ذلك، الذي يمس حتى البيانات الشخصية الخاصة بالإغراء و المؤسسات و الشركات على حد سواء مما يشكل خطرا كبيرا على المجتمع.

كما يصعب تحليل الجريمة المعلوماتية و فهم كيفية ارتكابها، فهي تتطلب معرفة شاملة و عميقة في مجال الحاسوب و الانترنيت و الممارسات الامنية من طرف المحققين و الخبراء لتقديم المساعدة و تسهيل عملية اثباتها و اكتشاف مرتكبيها، نظرا لصعوبتها و غير الاكتفاء بالإجراءات التحقيقية التقليدية لمالها مميزات كبيرة في توسعها، و هذه الاخيرة تطلبت أحداث الادوات التقنية لاستعادة البيانات و ضبط الادلة لتقديم المساعدة و تسهيل عملية اكتشافها و تقديم الجناة الى العدالة.

و بناءا على ما تقدم، توصلنا الى مجموعة النتائج و منها:

- التحقيق في الجرائم المعلوماتية يعد اجراء من الاجراءات التابعة لها نظرا لاستحداث هذا النوع من الجرائم يهدف للتنقيب و البحث عن الادلة الرقمية لاثبات الجريمة المعلوماتية و اكتشاف مرتكبيها.
- توسع نطاق الجريمة المعلوماتية أدى لاختلاف الفقهاء على تعريف موحد لها.
- احترافية مرتكبي الجريمة المعلوماتية الواقعة على النظام المعلوماتي لها اضرار و خطر كبير يهدد امن و سلامة الفرد و المجتمع، فهي سريعة التنفيذ و صعب اثباتها، الذي ادى لاتباع اجراءات تحقيقية في سبيل الحصول على الدليل الرقمي و المتمثلة في عملية التفتيش و المعاينة و ضبط الادلة.

من خلال هذه النتائج توصلنا الى التوصيات الاتية:

- توعية فئات المجتمع بالجريمة المعلوماتية و مخاطرها بإقامة دورات خاصة بذلك و نشر الثقافة القانونية لتفاديها.
- كسب الخبرة و المهارات من التجارب الدولية لمكافحة الجريمة المعلوماتية و اكتشافها.

- التعاون الدولي بانضمام الجزائر للاتفاقيات الدولية لمحاربة هذه الجريمة.
- عدم الاعتماد فقط على القوانين المقررة و تطويرها و اصدار الجديدة منها في هذا المجال و تدريب المحققين بشكل تقني اكثر لاثبات الجريمة المعلوماتية.

قائمة المصادر و المراجع

قائمة المصادر و المراجع

أولا: قائمة المصادر

1- القرآن الكريم:

- الآية 45 من سورة الفرقان.

2- التشريع الأساسي:

- التعديل الدستوري لسنة 2020، الصادر بموجب المرسوم الرئاسي 20-442، المؤرخ في 15 جمادى الاول عام 1442 الموافق ل 30 ديسمبر 2020، ح ر ج ج، ع82، الصادر في 30 ديسمبر 2020.

3- القوانين العادية:

- القانون09-04 ،المؤرخ في 14 شعبان عام 1430 الموافق ل 5 اوت 2009 ،المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، ج ر ج ج، ع47،2009.

4- الأوامر:

- الأمر 66-155، المؤرخ في 8 جوان 1966، المتضمن قانون الاجراءات الجزائية ج ر ج ج، المعدل و المتمم، ع48، 1966.
- الأمر 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني ج ر ح ج ،ع 78، 1975.
- الامر 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن لقانون المدني ج ر ج ج،ع 78، 1975.
- الامر 66-155، المؤرخ في 08 جوان 1966، المتضمن قانون الاجراءات الجزائية،ج ر ج ج، المعدل و المتمم، ع 48، 1966.

- الامر 66-155، المؤرخ في 08 جوان 1966، المتضمن قانون الاجراءات الجزائية،ج ر ج ج، المعدل و المتمم، ع 48، 1966.

5- المراسيم الرئاسية:

- المرسوم الرئاسي 15-261 ،مؤرخ في 24 ذي الحجة 1436، الموافق ل 8 اكتوبر 2015 ،يحدد تشكيلة و تنظيم كيفيات تفسير الهيئة الوطنية للرقابة من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، الجريدة الرسمية، ج ر ج ج، ع 53، الصادر في 8 أكتوبر 2015.
- المرسوم الرئاسي رقم 21-439، مؤرخ في 2 ربيع الثاني 1443 ،الموافق ل 7 نوفمبر 2021، يتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، ج ر ج ج، ع 86، الصادر في 11 نوفمبر 2020.
- المرسوم الرئاسي 15-261، المؤرخ في 24 ذي الحجة 1436، الموافق ل 8 أكتوبر 2015،ج ر ج ج، ع 53، 2015.
- المرسوم الرئاسي 20-183 ،مؤرخ في 21 ذي القعدة 1441 الموافق ل 13 يوليو 2020، يتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، ج ر ج ج، 2020.
- المرسوم الرئاسي رقم 19-172 ،مؤرخ في3 شوال 1440 الموافق ل 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها و تنظيم و كيفيات سيرها، الجريدة الرسمية ج ر ج ج، ع 37، الصادر في 9 جوان 2019.

6- الكتب:

- الكتب الخاصة:

- حسن الطوالة ،الجرائم الالكترونية ، جامعة العلوم الطبيعية ،ط1، مملكة البحرين، 2008.
- خالد عوني خطاب المختار، دور الوسائل العلمية الحديثة في الاثبات الجنائي، دار الكتب القانونية، مصر،2007.

- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الاسكندرية 2010.
- خالد عياد الحلبي، اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنيت، دار الثقافة للنسر و التوزيع، ط1، عمان، 2011.
- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريع المقارنة و في ضوء الاتفاقيات و المواثيق الدولية، دار النهضة العربية، ط1، مصر ،2011.
- ربيعة زيدان، الجريمة المعلوماتية في التشريع الجزائرية و الدولي، دار الهدى، عين مليلة، الجزائر، 2011.
- سمير رفعي، البحث و التحري عن الجريمة الالكترونية، دار المثقف، ط1، الجزائر، 2019.
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الاثبات الجنائي في القانون الجزائري و المقارن، دار الجامعة الجديدة ،كلية الحقوق، جامعة الاسكندرية، 2006.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الازاريطة، 2004.
- منصور عمر المعايطة، الادلة الجنائية و التحقيق الجنائي، دار الثقافة، ط1، 2007.

نهال عبد القادر المؤمن ،الجرائم المعلوماتية، دار الثقافة للنشر و توزيع، عمان، 2008.

- الكتب العامة:

- بوزيد اغليس، تلازم مبدأ الحرب لاقتناع الذاتي للقاضي الجزائي، دراسة تحليلية مقارنة بين القانون الجزائري و القانون المصري و بعض القوانين العربية، دار الهدى، الجزائر، 2010.
- بوبكر رشيدة، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائي المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، مجلد 1، ط1، 2012.
- بعلي محمد الصغير، القانون الاداري، التنظيم الاداري، النشاط الاداري، دار العلوم للنشر و التوزيع، عنابة، 2004.

- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري و القانون المدني، دار الجامعة الجديدة ، الاسكندرية ، ط1، 2010.
- محمد الامين البشري، التحقيق في الجرائم المستحدثة، مركز الدراسات و البحوث، الرياض، ط1، 2004.
- مولود ديدان، قانون الاجراءات الجزائية، دار بلقيس، الجزائر ،د ط، ديسمبر، 2014.
- مأمون محمد سلامة، الاجراءات الجزائية في التشريع المصري، دار النهضة العربية، ط1، مصر، 1992.

- الرسائل العلمية:

أ- رسائل الدكتوراه:

- أحمد فاروق زاهر، التحقيق الجنائي في الجريمة الالكترونية، البحث مقدم لاستفاء متطلبات الحصول على درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة.
- براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، اطروحة لنيل شهادة الدكتوراه في العلوم القانونية، جامعة تيزي وزو، 2018.
- بدري فيصل، مكافحة الجرائم المعلوماتية في القانون الدولي و الداخلي، اطروحة لنيل شهادة دكتوراه، قانون عام، كلية الحقوق، جامعة الجزائر 01، يوسف بن خدة، 2017-2018.
- دلال مولاي، اشكالية الاثبات في جرائم الانترنيت في التشريع الجزائري، اطروحة دكتوراه، تخصص قانون خاص، كلية الحقوق و العلوم السياسية، جامعة ابو بكر بلقايد، تلمسان، الجزائر، 2017-2018.
- ربيعي حسين، آليات البحث و التحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم و الحقوق، تخصص قانون العقوبات و العلوم الجنائية، كلية الحقوق و العلوم السياسية، قسم الحقوق، جامعة باتنة1، 2015-2016.

ب- رسائل الماجستير:

- ثنيان ناصر آل ثنيان، اثبات الجريمة الالكترونية، دراسة تأصيلية تطبيقية، رسالة ماجستير كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الامنية، الرياض، 2012.
- حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الاجرام و العقاب، جامعة باتنة، 2011-2012.
- جدي نسيمة، جرائم المساس بأنظمة المعالجة الالية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي ،كلية الحقوق، جامعة وهران، الجزائر، 2013-2014.
- سعيداني نعيم، آليات البحث و التحقيق في الجرائم المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013.
- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علوم الاجرام جامعة ابو بكر بلقايد، تلمسان،2010-2011.
- غانية خروفة، سلطة القاضي الجنائي في تقدير الخبرة، رسالة ماجستير في قانون العقوبات و العلوم الجنائية، كلية الحقوق و العلوم السياسية، جامعة منتوري، قسنطينة، 2008-2009.

ت- رسائل الماستر:

- بوبعاية ابتسام، التحقيق في الجريمة الالكترونية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر اكاديمي في الحقوق، كلية الحقوق و العلوم السياسية، جامعة محمد البشير الابراهيمي ،برج بوعريريج، 2021-2022.
- بلعيد منصورية، النظام الاجرائي للجريمة المعلوماتية في التشريع الجزائري، كلية الحقوق و العلوم السياسية، تخصص قانون قضائية، جامعة عبد الحميد بن باديس، مستغانم، 2019-2020.
- بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، (دراسة مقارنة)، مذكرة مكملة من مقتضيات نيل شهادة الماستر، كلية الحقوق، جامعة محمد خضير، بسكرة ، 2015-2016 .

- بن زرد آسيا، اثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة عبد الحميد بن باديس، مستغانم، 2018-2019.
- ليبيات خولة، عميرات أميرة، "الاثبات في الجريمة الالكترونية"، مذكرة مكملة لنيل شهادة الماستر الاكاديمي، جامعة محمد بوضياف، المسيلة، 2021-2022.
- معش زهية، غانم نسيمة، الاثبات الجنائي في الجرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في الحقوق، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمان ميرة ،بجاية ،2012-2013.
- نايري عائشة، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل الماستر في القانون الاداري، جامعة أحمد دراية، أدرار، 2016-2017.
- نسيمة مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق ،تخصص قانون جنائي، جامعة محمد خضير، بسكرة، 2013-2014.

7- المقالات و المجالات:

- اسمهان بوضياف، الجريمة الالكترونية و الاجراءات التشريعية لمواجهتها في الجزائر، مجلة الاستناد للباحث للدراسات القانونية و السياسية، ع 11، سبتمبر، ميلة، 2018.
- بلينة حبيباتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الانسانية، المجلد أ، ع 50، كلية الحقوق، جامعة الجزائر 1، ديسمبر 2018.
- بلهادي حميد، حجية الدليل الرقمي في الاثبات الجنائي، مجلة البحوث و الدراسات القانونية و السياسية، كلية الحقوق و العلوم السياسية، جامعة البليدة2، المجلد9، ع 1، 2019.
- بلجراف سامية، سلطة القاضي الجزائي في قبول و تقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، المجلد7، ع 1، 2021.
- بن فردية محمد، الدليل الجنائي و حجيته أمام القضاء الجزائي (دراسة مقارنة)، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر.

- بهنوس آمال، الدليل الرقمي في الاجراءات الجنائية، المجلة الاكاديمية للبحث القانوني، المجلد16، العدد2، 2017.
- حسن فريحة، الجرائم الالكترونية و الانترنيت، مجلة المعلوماتية، العدد36، أكتوبر، 2011.
- سارة مساعدي، مشروعية الوسائط الرقمية في الاثبات الجنائي، المجلة الجزائرية للأمن الانساني، جامعة الجزائر1، المجلد5، ع 1 ، 2019.
- سالمي نضال، الاطار التنظيمي للدليل الرقمي في الاثبات، مجلة القانون و المجتمع، كلية الحقوق و العلوم السياسية، جامعة وهران2، محمد بن أحمد الجزائر، الجلد10، ع 1، 2022.
- سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام و الاتصال بين سرية المعطيات الشخصية الالكترونية و مكافحة الجرائم الالكترونية، المجلة النقدية للقانون و العلوم السياسية، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، جامعة الصديق بن يحي، جيجل، المجلد 17، ع2، الجزائر، 2022.
- عز الدين عثماني، اجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الاتصال و المعلوماتية، مجلة دائرة البحوث و الدراسات القانونية و السياسية، مخبر المؤسسات الدستورية و النظم السياسية، جامعة تبسة، ع 4، جانفي 2018.
- عبيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الاكاديمي في العلوم القانونية و السياسية، جامعة مولاي طاهر سكيكدة، ع 6 ، 2021.
- لحرش عبد الرحيم، حضري حسان، الاثار القانونية للشخصية الاعتبارية في القانون الجزائري، مجلة التمكين الاجتماعي، مجلة فصلية دولية اكاديمية محكمة، جامعة المنار تونس، جامعة الوادي، المجلد1، ع4، ديسمبر، 2019.
- منصور عبد السلام عبد الحميد حسان العجيل، الضوابط القانونية لاثبات الجنائي بالأدلة الرقمية (دراسة مقارنة)، المجلة القانونية (مجلة متخصصة في الدراسات و البحوث القانونية).

- ممدوح خليل البحر، نطاق حرية القاضي الجنائي في تكوين قناعته الوجدانية، مجلة الشريعة و القانون، مجلة علمية محكمة تصدر عن كلية الشريعة و القانون، جامعة الامارات العربية المتحدة، العدد21، يونيو، 2004.
- ياسين بن عمر، المعالجة القانونية الالكترونية في القانون الالكتروني في القانون الجزائري و تشريعات المقارنة، مجلة العلوم القانونية و السياسية، جامعة باتنة، المجلد 10، العدد3، 2019، ص 720.
- يس حسن محمد عثمان، الدليل الرقمي و أثره على الدعوى الجنائية، مجلة العلوم القانونية و الاجتماعية، كلية القانون و الشريعة، قسم القانون، جامعة زيان عاشور بالجلفة، الجزائر، المجلد5، ع 3، 2020.
- نور الهدى محمودي، حجية الدليل الرقمي لاثبات الجريمة الالكترونية، مجلة الباحث للدراسات الاكاديمية، جامعة باتنة1، ع 11، جوان، 2017.

8- مطبوعات:

- خضيري محمد، مدخل للإجرام الالكتروني، مطبوعة مقدمة لطلبة السنة الثانية ماستر، تخصص اعلام آليو انترنيت، كلية الحقوق و العلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، 2022-2023.
- محمد مروان، نظام الاثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999.

9- المداخلات:

- عز الدين عز الدين، مداخلة بعنوان "الاطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها"، مقدمة الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة المتعقد بجامعة بسكرة، يوم 16 نوفمبر 2015.

10- مواقع الانترنيت:

- اسراء جبريل رشاد مرعي، الجرائم الالكترونية "الاهداف-الاسباب-طرق الجريمة و معالجتها"، المركز الديمقراطي العربي للدراسات الاستراتيجية، الاقتصادية و السياسية، ألمانيا، 2016، بحث منشور على الموقع: https://democraicac.de/p35426 .
- سميرة بيطام، الجريمة الالكترونية و تقنية الاجرام المستحدث، ص 4/1 .
- موقع الدرك الوطني الجزائري .http://www.mdn.dz

الفهرس

شكر وتقدير

الاهداء

قائمة المختصرات

مقدمة.....**7– 12**

الفصل الاول: التحقيق كإجراء من اجراءات المتابعة بالجرائم المعلوماتية

المبحث الأول: مفهوم التحقيق في الجرائم المعلوماتية.....14

المطلب الأول: المقصود بالتحقيق في الجرائم المعلوماتية.....14

الفرع الأول: التعريف الفقهي للجريمة المعلوماتية.....14

الفرع الثاني: التعريف القنوني للجريمة المعلوماتية.....16

المطلب الثاني: خصوصية التحقيق في الجرائم المعلوماتية 17

الفرع الأول: خصائص التحقيق في الجرائم المعلوماتية 17

الفرع الثاني: صعوبات التحقيق في الجرائم المعلوماتية.....23

المبحث الثاني: الأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية.....26

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال.....26

الفرع الاول: التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال.....26

الفرع الثاني: مهام و تشكيلة الهيئة و طبيعة عملها.....30

المطلب الثاني: الوحدات التابعة لسلك الامن و الدرك الوطني.....33

الفرع الاول: الوحدات التابعة لسلك الامن.....33

الفرع الثاني: الوحدات التابعة للدرك الوطني الجزائري.....35

الفصل الثاني: آليات التحقيق في الجرائم المعلوماتية

المبحث الاول: اجراءات التحقيق في الجريمة المعلوماتية.....43

المطلب الاول: الاجراءات التقليدية لإثبات الجريمة المعلوماتية.....43

الفرع الاول: المعاينة و التفتيش في الجرائم المعلوماتية.....43

الفرع الثاني: الضبط و الخبرة القضائية في الجرائم المعلوماتية.....49

المطلب الثاني: الاجراءات الحديثة لإثبات الجريمة المعلوماتية.....53

الفرع الاول: التسريب الالكتروني.....53

الفرع الثاني: التنصت و المراقبة الالكترونية.....54

المبحث الثاني: الدليل الرقمي لإثبات الجريمة المعلوماتية.....56

المطلب الاول: الدليل الرقمي كوسيلة لإثبات في الجريمة المعلوماتية.....57

الفرع الاول: تعريف الدليل الرقمي و خصائصه.....57

الفرع الثاني: تقسيمات الدليل الرقمي و مصادر الحصول عليه.....61

المطلب الثاني: حجية الدليل الرقمي في الاثبات الجنائي.....65

الفرع الاول: محل و مراحل الدليل الرقمي.....65

الفرع الثاني: موقف المشرع الجزائري بين الدليل الرقمي و تقديره أمام القضاء في الاثبات الجنائي. 71

خاتمة.....**76**

قائمة المصادر والمراجع

الملخص

الملخص:

تعتبر الجريمة الالكترونية من الجرائم الخطيرة التي ظهرت في العصر الحديث و أصبحت تشكل مشكلة كبيرة للدول بصفة عامة و الافراد بصفة خاصة ، خاصة مع التطور التشريع الذي يشهده هذا العصر في مجال التكنولوجيا و المعلومات، حيث أن كل دول العالم تسعى جاهدة لإيجاد السبيل و الحلول اللازمة للحد من انتشار مثل هذه الجرائم و البحث في السبل الكفيلة للوقاية، رغم الصعوبات الكبيرة التي تعترض الجهات المختصة. الا انهما في كل مرة تصدر قوانين و اجراءات تحكم هذه الجرائم رغم التطور الرهيب لوسائل و كيفيات ارتكاب مثل هذه الجرائم العابرة للحدود الدولية.

و قد اسفرت هاته الدراسة على مجموعة من النتائج أهمها: التعريف الشامل للتحقيق في الجرائم المعلوماتية بعد ذلك تطرقنا الى الاجهزة المختصة في التحقيق في الجرائم المعلوماتية و الصعوبات التي تعترض طريق المحققين بداية التحقيق الأولى لمسرح الجريمة مرورا بالتفتيش و جمع الادلة و المعاينة و التي تعتبر المرحلة الأهم للوصول الى المجرم المعلوماتي، بالإضافة الى اننا تطرقنا الى طرق استخلاص الدليل الرقمي و حجية القاضي الجزائي في تقديره.

الكلمات المفتاحية: الجريمة الالكترونية، التحقيق، المجرم المعلوماتي، الدليل الرقمي.

Résumé:

La criminalité électronique est considérée comme l'un des délits graves apparus à l'ère moderne et est devenue un problème majeur pour les pays en général et les individus en particulier, en particulier avec le développement de la législation observée à cette époque dans le domaine de la technologie et de l'information, comme tous les pays du monde s'efforcent de trouver la voie et les solutions nécessaires pour limiter la propagation de ces crimes et explorer les moyens de les prévenir, malgré les grandes difficultés rencontrées par les autorités compétentes. Cependant, à chaque fois, il édicte des lois et des procédures régissant ces crimes, malgré le développement effroyable des moyens et des méthodes permettant de commettre de tels crimes au-delà des frontières internationales.

الملخص

Cette étude a abouti à un ensemble de résultats dont les plus importants sont : une définition globale de l'enquête sur les cybercriminalités. Après cela, nous avons abordé les agences spécialisées dans l'enquête sur les cybercriminalités et les difficultés qui se dressent sur le chemin des enquêteurs, dans un premier temps. Début de l'enquête sur la scène du crime, à travers l'inspection, la collecte des preuves et l'inspection, qui est considérée comme l'étape la plus importante est d'atteindre l'information criminelle, en plus de cela, nous avons discuté des méthodes d'extraction des preuves numériques et. L'autorité du juge pénal dans son appréciation.

Mots-clés : cybercriminalité, enquête, cybercriminel, preuve numérique.