الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف - المسيلة

كلية الحقـــوق و العلـــــوم السياسية
قسم: الحقوق
رقم: .....

ميدان: الحقـــوق و العلـــــوم السياسية
فرع: الحقوق
تخصص: قانون جنائي

مذكرة مقدمة لنيل شهادة الماستر أكاديمـــي

إعداد الطالب(ة): والي بدرة

تحت عنوان

المواجهة الاجرائية لجرائم المعلوماتية

لجنة المناقشة:

أ.دحية ع اللطيف	جامعة: محمد بو ضياف	رئيســا
أ. قرقور حدة	جامعة: محمد بو ضياف	مشرفا و مقررا
أ. قسمية محمد	جامعة: محمد بو ضياف	مناقشا

السنة الجامعية: 2019/2018

﴿ وَلْتَكُنْ
مِنْكُمْ أُمَّةٌ يَدْعُونَ إِلَى الْخَيْرِ وَيَأْمُرُونَ بِالْمَعْرُو
فِ وَيَنْهَوْنَ عَنِ الْمُنْكَرِ وَأُولَئِكَ هُمُ
الْمُفْلِحُونَ ﴾

آل عمران 104

شكر و عرفان

أتوجه بجزيل الشكر و الإمتنان إلى الأستاذة

قرقور حدة ، على إشرافها على هذه المذكرة

إذ لم تبخل عليا بإرشاداتها و توجيهاتها

القيمة لإثراءهذا العمل رغم كثرة مشاغلها .

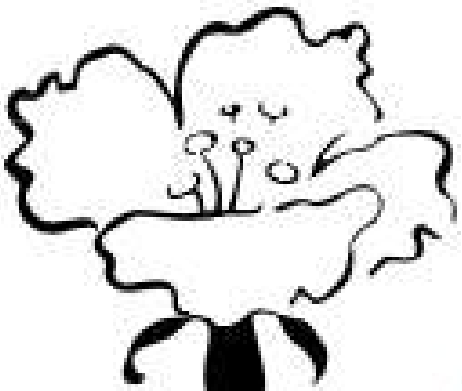
كما أشكر اللجنة المحترمة على مناقشة

هذه المذكرة .

ولا أنسى أن أشكر كل من قدم لي يد العون

من قريب أو بعيد

والي بدرة



إهداء

إلى من لا يمكن للكلمات أن توفي حقهما،

الوالدين الكريمين

إلى من لا أستطيع الاستغناء عنهم،

زوجي و أولادي

وإلى إخوتي.

و جميع الأصدقاء و الزملاء

أهدي ثمرة جهدي.

بدرة.

قائمة المختصرات

ج. ر .ج.ج : الجريدة الرسمية للجمهورية الجزائرية .

م : مجلد

ق. ع .ج : قانون العقوبات الجزائري .

ق. إ .ج .ج : قانون الإجراءات الجزائية الجزائري .

ع : عدد

ط : طبعة .

س : سنة .

د.ذ.د.ن : دون ذكر دار النشر .

د.ذ. س. ن : دون ذكر سنة النشر .

د.ذ.ب.ن : دون ذكر بلد النشر .

المقدمة:

إن التطور الهائل الذي شهده العالم لاسيما بعد ثورة تكنولوجيا المعلومات في مجال الحواسيب الآلية و شبكة الانترنت و الاندماج المذهل بينهما, انعكس بصورة إيجابية على مستخدميها في مختلف مجالات الحياة المعاصرة, نظرا لما توفره من الوقت و الجهد و التكلفة ,و لا سيما عنصري السرعة و الدقة في تجميع المعلومات و تخزينها و معالجتها و نقلها و تبادلها بين الأفراد و الشركات و المؤسسات المختلفة داخل الدولة أو بين عدة دول, الأمر الذي زاد من الإقبال على الأنظمة المعلوماتية و الاعتماد عليها بشكل أساسي في كل القطاعات العامة و الخاصة للحد الذي يصعب معه تصور قيام هذه القطاعات نشاطها دون الاستعانة بهذه التقنية الحديثة.

و لقد أدت ثورة تكنولوجية المعلومات مزايا عديدة لا يمكن حصرها في مختلف جوانب الحياة المعاصرة ,و لا سيما في مجال التحقيق الجنائي أين ساهمت الوسائل العلمية الحديثة في الكشف عن مرتكبي الجرائم من خلال الآثار المادية التي يخلفونها على مسرح الجريمة كآثار البصمات و بقايا الشعر و بقع الدم و مختلف إفرازات الجسم ,من خلال تقنية البصمة الوراثية (ADN), و كما تم استخدام التكنولوجيا في مجال أكثر حساسية و هو تنفيذ العقوبات السالبة للحرية الأقل من 3 سنوات خارج أسوار المؤسسات العقابية باستخدام تقنية السوار الإلكتروني أو ما يعرف بالحبس المنزلي أو الوضع تحت نظام المراقبة الإلكترونية.

و رغم المزايا الهائلة التي أحدثتها ثورة تقنية المعلومات ,إلا أنه صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء الاستخدام السيئ لهذه التقنية و استغلالها على نحو غير مشروع, الأمر الذي أدى لظهور أشكال جديدة من الجرائم تعرف باسم الجرائم المعلوماتية ,و التي تقع في بيئة إلكترونية و تنصب على المعلومات و البيانات بكافة أشكالها, و هناك من يطلق عليها اسم جرائم الكمبيوتر و الانترنت جرائم التقنية العالية, الجرائم الرقمية, السيبركريم, الجرائم الالكترونية , الجرائم الناعمة, و غيرها من المصطلحات التي أطلقت على الجرائم المعلوماتية ,التي أحدثت انقلابا خطير في النظرية التقليدية للجريمة و أساليب التحري و التحقيق الخاص بها.

و لقد أصبحت منظومة معالجة المعلومات و برامج الحاسوب الآلي وشبكات الاتصال هدف أساسيا لعمليات التخريب و التعطيل و المحو مهددة بذلك الأفراد و المؤسسات الحكومية و الخاصة

المقدمة :

التي تعمد في أعمالها بشكل أساسي على هذه المنظومة, كما أن التهديد قد يصل إلى تهديد أمن الدول و القارات باعتبارها من الجرائم العابرة للحدود الوطنية, أين يقوم المجرم المعلوماتية باستخدام التقنية الحديثة لارتكاب جرائمه في العالم الافتراضي بجهد أقل و دون الحاجة للتنقل لمسرح الجريمة و ترك آثار مادية, لا سيما شبكة الانترنت و هي عبارة عن شبكة عالمية غير مقيدة بحدود جغرافية أو سياسية و لا تخضع لسلطة حكومية أو خاصة , و التي تجعل أغلب مستخدميها من دول العالم في حالة اتصال دائم و إمكانية تبادل المعلومات و البيانات و الاتصالات الصوتية و المصورة في خلال ثوان معدودة.

و تكمن الخطورة في هذا النمط المستحدث نسبيا من الإجرام المعلوماتي محل الدراسة في كونه من أخطر و أعقد الجرائم و يأتي في مقدمة الأشكال الجديدة للجريمة المنظمة العابرة للحدود, في طبيعتها المتميزة و المعقدة من حيث أساليب ارتكابها في البيئة الرقمية دون أن تخلف آثار مادية تنصب على إشارات و ذبذبات كهرومغناطيسية تنساب عبر نظم المعالجة الآلية و شبكات الاتصال, و أن آثارها غير محصورة في النطاق الإقليمي للدولة فهي جرائم تقنية عابرة للحدود الوطنية, فضلا على اتسام مرتكبوها بالذكاء و المهارة و الخبرات الفنية و التقنية العالية لأنظمة المعالجة الآلية للمعطيات ,مستغلا بذلك فكرة التزاوج بين الذكاء البشري و الذكاء الصناعي و التقني .

و نظرا لخصوصية الجريمة المعلوماتية و اختلافها عن الجرائم التقليدية في طبيعتها و نطاقها و أنواعها و خصائصها ووسائل ارتكابها و خصوصية مرتكبيها, أين أصبح المجرم المعلوماتي يفكر مليا قبل الإقدام على نشاطه الإجرامي في الأسلوب الذي يخلصه من قبضة العدالة و الإفلات بذلك من العقاب و تحمل المسؤولية الجزائية ,خاصة أمام الفراغ أو القصور التشريعي مستغلا التقنية العالية لتكنولوجيا المعلومات لسرعة ارتكابها و محو آثارها, الأمر الذي استدعى لضرورة التصدي لهذه الظاهرة الإجرامية المستحدثة, بوضع نصوص خاصة بها و استخدام أساليب و إجراءات خاصة التحري و التحقيق فيها باستخدام وسائل تقنية كفيلة بتتبع آثار الجريمة في البيئة الالكترونية ,مع ضرورة خضوعها لضوابط و شروط موضوعية و شكلية تحت طائلة بطلانها, كونها تنطوي على مساس بالحريات و حرمة الحياة الخاصة للأفراد المكفولة دستوريا .

كما أن تكريس إطار قانوني أكثر ملائمة و انسجام مع خصوصية هذه الجريمة و خطورتها لا يقتصر على الشق الموضوعي فقط ,و الذي طرح إشكالية مدى إخضاعها لنصوص تقليدية و ما يشكله من مساس بمبدأ الشرعية و التفسير الضيق للنصوص الجزائية و حضر القياس, بل يمتد للشق الإجرائي الذي يثير عدة إشكالات من الناحية العملية أثناء مرحلة البحث و التحري و التحقيق في هذه الجرائم الواقعة في البيئة الالكتروني ة و إمكانية محو آثارها و تشفير البيانات و تخزينها إلكترونيا ,الأمر الذي يزيد من صعوبة إثباتها و نسبتها لمرتكبها و وضع سلطات البحث و التحقيق في مأزق حقيقي لم يألفوا على مواجهته بالوسائل و الأساليب التقليدية للتحري, و ما يزيد من صعوبة إثباتها امتداد آثار الجريمة المعلوماتية خارج الإقليم الوطني و الاصطدام بمبدأ سيادة الدول

و مع إدراك الصعوبات و الإشكالات التي تطرحها المواجهة الإجرائية للجرائم المعلوماتية و التنبه لآثارها السلبية و المخاطر الناتجة عنها ,فقد حظيت باهتمام الحكومات و الهيئات الدولية و الخبراء و الفنيون لتركيز جهودهم و تضافرها ,من أجل تطوير أساليب الحماية للنظم و البرامج المعلوماتية و تقليص فرص الاعتداء عليها باستحداث نصوص قانونية و موضوعية و إجرائية تعتمد على استخدام التقنية لمواجهتها, و كذا تفعيل آليات التعاون الدولي القانوني و القضائي لاسيما في مجال تسليم المجرمين و الإنابات القضائية, و ننوه أن نطاق الدراسة ينصب على السياسة الجزائية التي انتهجها المشرع الجزائري في إطار مكافحة الجريمة لاسيما في مجال إجراءات و أساليب التحري الخاصة و الأجهزة المكلفة بمواجهتها ,و حالات الخروج عن الاختصاص المحلي و كيفية حل مشاكل تنازع الاختصاص باعتبارها من الجرائم العابرة للحدود الوطنية.

أهمية الدراسة:

بالإضافة لما سبق ذكره ,تكمن أهمية دراسة موضوع المواجهة الإجرائية للجرائم المعلوماتية باعتبارها من جرائم الرقمنة المستحدثة نسبيا ,و التي تعرف تطور متسمر بسبب تزايد استخدام تقنية المعلومات التي تعد العصب المحرك لكل نواحي الحياة, الأمر الذي يستدعي التطرق لماهيتها و آليات مواجهتها, كما أنه يعد من المواضيع المهمة التي تظهر مدى كفاءة الدول في التعامل مع الإجرام المعلوماتي الذي بات محط اهتمام الهيئات و الأجهزة الدولية و الإقليمية و الوطنية كونها من الجرائم العابرة للحدود الوطنية.

صعوبات الدراسة:

واجهتنا بعض الصعوبات ,كنقص المراجع المتخصصة في الجانب الإجرائي للجرائم المعلوماتية لاسيما في التشريع الجزائري , في حين أن أغلب المراجع و الدراسات و الأبحاث القانونية عنيت بالجانب الموضوعي للجريمة ,وهذا بالإضافة لندرة الأحكام القضائية في هذا المجال,و كذلك الاهتمام بالجانب التقني في مجال المنظومة المعلوماتية بالموازاة مع الجانب القانوني لفهم هذه الظاهرة الإجرامية .

أسباب اختيار موضوع الدراسة :

إن من أسباب اختياري لموضوع الدراسة هو محاولة إلقاء الضوء على الجانب الإجرائي كونه يتسم بصبغة علمية بحتة تتعلق بنظم المعالجة الآلية للمعطيات ,و تقوم على مصطلحات تستعصي فهم رجال القانون ,و التي تتطلب حد أدنى من المعلومات الخاصة بنظام الحواسيب و شبكات الاتصال و كيفية تخزين المعلومات و أرشفتها و معالجتها و نقلها, هذا بالإضافة إلى أن الصعوبات و الإشكالات القانونية و العملية و التقنية التي تطرحها تشكل تحديا للجهات التحري و التحقيق و الحكم.

و لعل من أهم الأسباب التي دفعتني للخوض في هذا الموضوع هو عملي في مجال المحاماة لمعرفة سبل الدفاع عن المتهم أو الضحية, خاصة أمام تنامي هذا النوع من الجرائم الذي يفرض نفسه بقوة في المستقبل القريب, و إن كانت لا تصل للعدالة بسبب قلة وعي الضحايا بمخاطرها و إعراضهم عن الإبلاغ عنها و صعوبة التحقيق فيها و إثباتها بالوسائل التقليدية, و كذا محاولة إثراء المكتبة الجامعية القانونية ولو بالقليل .

الإشكالية: إن الإشكالية التي يطرحها موضوع الدراسة هي:

مدى فعالية المواجهة الإجرائية للنمط المتجدد و المتطور للجرائم المعلوماتية في التشريع الجزائري ؟

و تندرج تحت الإشكالية الرئيسية جملة من التساؤلات الفرعية التالية وهي:

المقدمة :

ما المقصود بالجرائم المعلوماتية وهل هي نفسها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؟ أم أنها تمثل إحدى صورها فقط.؟

أين تكمن خصوصية الجريمة المعلوماتية و التي تؤثر فيما بعد على خصوصية التحقيق فيها ؟

ما مدى قابلية تطبيق القواعد الإجرائية التقليدية للتحقيق في الجرائم المعلوماتية الواقعة في البيئة الالكترونية ؟

ما هي أساليب التحري الخاصة التي رصدها المشرع الجزائري لمكافحة الجريمة المعلوماتية؟

هل التشريعات الوطنية كفيلة بمواجهة الإجرام المعلوماتي أم أن تعزيز التعاون الدولي أصبح ضرورة حتمية كونها من الجرائم العابرة للحدود ؟

ما هي القيمة القانونية للدليل الرقمي و كيفية استخلاصه؟

المنهج المتبع:

تم الاعتماد على المنهج الوصفي و التحليلي, المنهج الوصفي لأن دراستنا تنصب على الإطار المفاهيمي للجريمة المعلوماتية و الإجراءات المتبعة للبحث و التحري و استخلاص الدليل الرقمي و العقبات التي تعتريها, و استخدمت المنهج التحليلي لتحليل النصوص التشريعية لاسيما الإجرائية منها و المتعلقة بالجريمة المعلوماتية مناقشتها .

و للإجابة على هذه الإشكالية الرئيسة و التساؤلات المتفرعة عنها اتبعنا التقسيم الثنائي للخطة كما ما يلي: **الـــــــفصل الأول : الآلـــيات القانونية لمواجهة الجريمة المعلوماتية**

المبحث الأول : الـــجريمة المعلوماتية و آلـيات مـــواجهتها

المبحث الثاني : خصوصية التحقيق في الجريمة المعلوماتية

الـــــفصل الثاني : الآليات الإجرائية للتحقيق في الجريمة المعلوماتية

المبحث الأول : الـقواعد الإجرائية لاستخلاص الـــدليل الرقمي

المبحث الثاني : القيمة الثبوتية للدليل الرقمي أمام القاضي الجزائي

الفصل الأول:

الآليات القانونية لمواجهة الجريمة المعلوماتية

لقد أدى الدمج بين وسائل الحوسبة و الاتصال إلى ظهور مفهوم جديد يعرف بتقنية المعلومات , و الذي يتيح التبادل الواسع لمختلف أنماط المعلومات و البيانات في بيئة رقمية , إلا أن الاستخدام السيئ للتقنية تكنولوجي ا المعلومات أفرزت ما يعرف بالجرائم المعلوماتية ,و التي أصبحت تشكل هاجسا و تحديا كبيرا للجهات التشريعية و القضائية و حتى الأمنية من أجل مواجهتها.

وقد أخذت الجريمة المعلوماتية حيزا كبيرا من الدراسات و اهتمام الفنيين و رجال القانون باعتبارها ظاهرة إجرامية حديثة نوعا ما و يكتنفها الكثير من الغموض , لذا ينبغي التطرق لبعض المسائل الجوهرية و الهامة ,و ذلك للإلمام بماهية الجرائم المعلوماتية و آليات مواجهتها .

و هذا ما سنتناوله في المبحث الأول تحت عنوان الجريمة المعلوماتية و آليات مواجهتها, أين سنلقي الضوء على مفهوم الجريمة المعلوماتية خاصة أمام غياب تعريف فقهي و قانوني موحد لها ,و خصائصها التي تميزها عن الجرائم التقليدية , كونها صعبة الاكتشاف و الإثبات , عابرة للحدود و خصوصية المجرم المعلوماتي , ثم تناولنا التقسيمات الفقهية للجريمة المعلوماتية ,منها الجرائم الواقعة على النظام المعلوماتي و جرائم واقعة بواسطة النظام المعلوماتي .

أما في المبحث الثاني سنتطرق لآليات مواجهة الجريمة المعلوماتية , و سنتناول فيه لآليات التعاون الدولي و الإقليمي لمواجهة الجريمة المعلوماتية , و الآليات التشريعية في القوانين العامة و الخاصة , ثم الآليات المؤسساتية على مستوى الأجهزة و الخاصة بمواجهة الإجرام المعلوماتي .

المبحث الأول:

الجريمة المعلوماتية و آليات مواجهتها

تعد الجريمة المعلوماتية من جرائم العصر الرقمي التي تمس المعلومات بكافة أشكالها و التي تمخضت عن الاستغلال السيئ لتكنولوجيا المعلومات , أين تسببت في انقلاب خطير في مفهوم النظرية التقليدية للجريمة و التي ترتكب من قبل المجرم المعلوماتي, الأمر الذي استدعى ضرورة استحداث أساليب خاصة للتحري و التحقيق فيها , وكذا آليات مسبقة للوقاية منها سواء على مستوى الوطني أو الدولي باعتبارها من الجرائم العابرة للحدود و التي لا تعترف بالحدود الجغرافية, أين تتيح شبكة الانترنت لأي مستخدم على مستوى أغلب دول العالم تحميل و نشر البيانات و المعلومات في غضون ثوان معدودة و بمجرد ضغطة زر على لوح المفاتيح .

وسنحاول إلقاء الضوء في هذا المبحث على ماهية الجرائم المعلوماتية باعتبارها ظاهرة إجرامية حديثة نوعا ما, وما تطرحه من إشكالات عملية سواء من الناحية القانونية أو الفنية ,و هذا ما سنتناوله في المطلب الأول من خلال التطرق لتعريفها و خصائصها و أنواعها , أما المطلب الثاني سنتطرق فيه للأجهزة المكلفة بمواجهة الجريمة المعلوماتية سواء على المستوى الوطني أو الإقليمي أو الدولي.

المطلب الأول: ماهية الجريمة المعلوماتية

لقد انفردت الجريمة المعلوماتية بطبيعة خاصة و التي استمدتها من الوسيلة التي تستخدم في ارتكابها من حواسيب و هواتف ذكية و شبكة لانترنت و حتى الأقمار الصناعية في بعض الأحيان, و أصبحت تدق ناقوس الخطر بسبب سرعة انتشارها و حجم المخاطر و الخسائر التي تخلفها , الأمر الذي جعل التشريعات الوطنية تقع في موقع المتفرج و العاجر عن الإلمام بهذه الظاهرة الإجرامية, خلافا للجرائم التقليدية التي نالت جانبا من الاهتمام بتحديد مفاهيمها و تعريفها و طرق مواجهتها.

لذالك فإن الجريمة المعلوماتية ما زالت قيد البحث و الدراسة من قبل المتخصصين في مجال القانون و تشغل اهتمامهم في محاولة منهم لفهم طبيعتها و الإلمام بماهيتها , و الأمر لا يكتمل دون إيجاد عن تعريف لها و معرفة خصائصها و أنواعها .

الـــــــــــفرع الأول: مفهوم الجريمة المعلوماتية

في البداية يجب أن ننوه بأن مسألة تعريف الجريمة المعلوماتية من المسائل الشائكة و أن الفقه لم يتمكن من إيجاد تعريف جامع لها, و يرجع ذلك للأسباب التالية :

1- غياب تعريف قانوني للجريمة المعلوماتية في اغلب التشريعات لذلك يبقى أمر تعريفها يرجع للفقه[1]

2- عدم وجود مصطلح قانوني موحد للدلالة على هذه الظاهرة الإجرامية الناشئة في البيئة الرقمية, و التي تغيرت تسميتها بتطور تقنية المعلومات من جرائم الكمبيوتر جرائم الانترنت, جرائم التقنية العالمية , الجريمة المعلوماتية , الجريمة الرقمية , الجرائم السبرانية أو السيبركريم , و الجرائم الإلكترونية[2].

3- بالإضافة لصعوبة حصر نطاق الجريمة المعلوماتية في إطار تجريمي محدد بسبب سرعة وتيرة تطور تقنية المعلومات , فإن الإشكالية الأساسية التي تزيد من صعوبة إيجاد تعريف جامع للجريمة المعلوماتية ,و تجعلها تقاوم التعريف هو تباين الدور الذي تلعبه تقنية المعلومات في ارتكابها, فقد يكون النظام المعلوماتي محلا أو موضوعا لها, كالدخول الغير المشروع للمواقع و العبث بالبيانات الرقمية و إتلافها, و قد يكون وسيلة لارتكاب الجرائم كجرائم السب القذف و غسيل الأموال و تجارة المخدرات و الإرهاب الالكتروني , و يترتب عنه بالتبعية اختلاف في تعريفات الجريمة المعلوماتية [3].

لذا تباينت التعريفات الفقهية للجريمة المعلوماتية و أغلبها يتسم بالقصور كونها تعتمد على معيار واحد فقط , إما المعيار التقني فقط [4], أو المعيار القانوني أو معيار المجرم المعلوماتي , أو معيار المعلوماتية باعتبارها محلا للجريمة أو وسيلة لارتكابها , و تكون بذلك أعطت مفهوما ضيقا

[1] -احمد عبد اللاه المراغي, الجريمة الالكترونية و دور القاضي الجنائي في الحد منها , المركز القومي للإصدارات القانونية ' القاهرة ,ط 1 , 2017 , ص 20.

[2] - سعيدي سليمة و حجازي بلال , جرائم المعلومات و الشبكات في العصر الرقمي , دار الفكر الجامعي , الإسكندرية , ط 1 , 2017 , ص.

[3] سعيدي سليمة و بلال حجازي، المرجع نفسه , ص56.

[4] المعيار التقني لمصطلح المعلوماتية يشمل شقين هما الحوسبة و الاتصال , أي أنها تقوم على وسائل تقنية كالحواسيب الآلية و الهواتف الذكية أو أي جهاز يعمل بنفس المواصفات , و تستخدم شبكة الانترنت لنقل المعلومات و البيانات و معالجتها , راجع في ذلك ريحان مباركي مضحكي , المرجع السابق , ص 19 .

للجريمة المعلوماتية و حصرت من نطاقها , و هناك من أعطى لها مفهوما موسعا باعتماده على أكثر من معيار , كونها في تطور مستمر و بشكل سريع جدا يصعب تداركه , ونذكر من بين هذه التعريفات ما يلي :

عرفها الخبير الأمريكي Parken بأنها : "كل فعل إجرامي متعمد أيا كانت صلته بالمعلومات و ينشأ خسارة تلحق بالمجني عليه , و كسب يحققه الفاعل".[1]

عرفها الفقيه Rosblat بأنها :" كل نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه"[2].

كما عرفها جانب من الفقه بالاستناد على وسيلة ارتكاب الجريمة المعلوماتية بأنها :

" كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب عن طريق الحاسب الآلي" [3] ,و بأنها :" كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات و يهدف للاعتداء على الأموال المادية أو المعنوية".[4]

وجاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة المنعقدة في فينيا سنة 2000 , "يقصد بالجريمة المعلوماتية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية , أو داخل نظام حاسوبي , وهي تشمل جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".[5]

كما عرفتها منظمة التعاون الاقتصادي و التنمية التابعة للأم المتحدة بأنها : " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية و يكون ناتج بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الالكترونية" [6].

و عرفتها الدكتورة هبة قشقوش بأنها :" كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات " , أو هي, "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبط بتقنية المعلومات"[1] .

1 سعيدي سليمة ,المرجع السابق , ص 57.
2 خالد عياد الحلبي , إجراءات البحث و التحري في جرائم الحاسوب و الانترنت , دار الثقافة للنشر ة التوزيع , الأردن , ط 1 , 2011 , ص21 .
3حنان ريحان المضحكي , الجرائم المعلوماتية , منشورات الحلبي الحقوقية , لبنان , ط 1 , 2014 م , ص 21 .
4 فتوح الشاذلي و عفيفي كمال , جرائم الكمبيوتر , منشورات الحلبي الحقوقية , لبنان , ب.ذ.ط , 2003 , ص 18 .
5خالد عياد الحلبي , المرجع السابق , ص 30 .
6أحمد اللاه المراغي , المرجع السابق , ص 27 .

و ما يلاحظ على التعريفات السابقة أنها مشوبة بالقصور لاعتمادها على أحد المعايير فقط و تضيق من مفهومها , و هناك من ذهب لاعتماد المفهوم الموسع لها باعتبارها في تطور مستمر و لا يمكن حصرها و إعطائها مفهوم مرن يستجيب لفكرة تطورها .

وعليه فإن التطور التكنولوج ي لتقنية المعلومات قد ألقى مسؤولية كبيرة على عاتق المشرع الجنائي لإيجاد تعريف لها , و أما عن المشروع الجزائري فقد تبنى تعريفا لجرائم المعلومات بموجب المادة :02 من الفصل الأول من القانون: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها بأنها : "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات , أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية"[1] .

أما مصطلح المساس بنظم المعالجة الآلية الذي آثر المشرع استخدامه في قانون العقوبات , فهو ينصرف للجرائم التي ترتكب على النظام المعلوماتي في حد ذاته [2] , أي أنه يخرج من نطاقه كل الجرائم التي يكون نظام المعالجة الآلية وسيلة لارتكابها رغم أنها الأكثر انتشارا [3].

و يلاحظ بأن التعريف الذي أخذ به المشرع الجزائري بخصوص جرائم الإعلام و الاتصال كمرادف لمصطلح الجرائم المعلوماتية في القانون : 09/04 بأنه مصطلح يتسم بالمرونة بما يسمح باستيعاب و مواكبة جميع صور الجريمة المعلوماتية سواء التي تقع على نظام المعالجة الآلية للمعطيات , أو جميع الجرائم المرتكبة باستعمال تكنولوجيا الإعلام و الاتصال .

الفرع الثاني : خصائص الجريمة المعلوماتية

تتسم الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية و ذلك لارتباطها بتكنولوجيا المعلومات ,الأمر الذي أضفى عليها جملة من الخصائص و السمات التي

7. خالد عياد الحلبي , المرجع السابق , ص 28 ,و هدى قشقوش , جرائم الحاسب الالكتروني في التشريع المقارن , دار النهضة العربية القاهرة , 1992 , ص 17 .

[1] القانون : 04/09 , المؤرخ في 14 شعبان 1430, الموافق ل : 5 غشت 2003 , و المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ,ج ر , العدد : 47 , الصادر بتاريخ : 16 أوت 2009 .

[2] ويقصد بنظام المعالجة الآلية في المجال التقني بأنه مجموعة العمليات المترابطة و المتسلسلة بدءا من تجميع المعطيات و إدخالها لنظام المعالجة الآلية و معالجتها وفق برامج و إخراجها بصورة معلومات . وهو تعبير فني و تقني يصعب إدراكه .

[3] رشيدة بوبكر , جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن , منشورات الحلبي الحقوقية , ط 1 , 2012 , ص : 28.

أثرت بدورها على المجرم المعلوماتي الذي يتميز بصفات تميزه عن المجرم التقليدي ,و سنلقي الضوء على أهمها:

أولا :الجريمة المعلوماتية عابرة للحدود الوطنية

إن أهم ما يميز الجريمة المعلوماتية هو تخطيها للحدود الوطنية, وذلك بسبب تقنية المعلومات من حواسيب و شبكة الانترنت التي اختصرت العالم في قرية صغيرة أين يقوم المجرم المعلوماتي بارتكاب جرائمه عن بعد و دون ضرورة لتواجده بمسرح الجريمة [1] .

ولقد أثارت هذه الخاصية لجرائم المعلوماتية عدة إشكالات قانونية بخصوص تحديد الدولة صاحبة الاختصاص القضائي و القانون الواجب التطبيق, الأمر الذي دفع بالدول لضرورة التعاون الدولي لمواجهة الجرائم المعلوماتية لاسيما في مجال تبادل المعلومات و تسليم المجرمين, رغم بعض الصعوبات التي تعيق هذا التعاون كانعدام النموذج القانوني الموحد للجرائم المعلوماتية وفقا لاتفاقية دولية موحدة, و كذا اختلاف النظم الإجرائية لكل دولة في مجال أساليب التحري و التحقيق الخاص.

ثانيا: الجريمة المعلوماتية صعبة الاكتشاف:

بما أن الجريمة المعلوماتية تقع في بيئة الكترونية ولا تترك أثار مادية ,فهي صعبة الاكتشاف لأنها تتم عادة في الخفاء,أين يقوم المجرم المعلوماتي بإخفاء هويته و محو أثار نشاطه الإجرامي بعد تلاعبه بالبيانات بنقلها أو حذفها أو محوها,لذلك فإن أمر اكتشافها غالبا يتم بمحض الصدفة فقط أو بعد مدة طويلة من الزمن ,لاسيما لدى الدول التي تفتقر مؤسساتها الأمنية للمهارات الفنية و التقنية للكشف عن هذه الجرائم المعلوماتية ,خاصة تلك التي ترتكب خارج الحدود الوطنية,وما يزيد من صعوبة اكتشافها هو إعرا ض الضحايا خاصة المؤسسات المالية عن الإبلاغ لدى الجهات المعنية عن تعرض أنظمتها المعلوماتية للانتهاك تجنبا لهز ثقة المتعاملين معها و الإضرار بسمعتها.[2]

(1) نبيلة هبة هروال, الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات , دار الفكر الجامعي , الإسكندرية , مصر , 2007,ص 39.
[2] هلال عبد الله احمد,التزام الشاهد بالإعلام في الجرائم المعلوماتية, القاهرة, ط 1, 1997, ص 23.

ثالثا: صعوبة إثبات الجريمة المعلوماتية: إن مسألة إثبات الجريمة المعلوماتية هي من المسائل الأكثر تعقيدا ,على خلاف إثبات الجرائم التقليدية لأنها تتم في بيئة افتراضية تتم في الخفاء وبمجرد التلاعب بالنبضات و الذبذبات الالكترونية للبيانات ,من قبل مجرم معلوماتي يمتلك المهارة الفنية اللازمة لطمس آثار جريمته في ظرف ثوان معدودة.

هذا بالإضافة إلى أنها لا تترك أثرا بعد ارتكابها و صعوبة الاحتفاظ الفني بآثارها إن وجدت,و يصعب على المحقق العادي التعرف على مرتكبيها,كما أن الضحية قد يسهل أو يساهم بطريقة غير مباشرة في ارتكابها بسبب عدم توفير نظام حماية لحاسوبه أو تشفير ملفاته مما يسهل اختراقها

كل هذه العوامل تصعب الأمر على رجال الضبطية القضائية في مجال البحث و التحري و جهات التحقيق في الجرائم المعلوماتية, وتستدعي ضرورة الإلمام بتقنيات تكنولوجي ا الإعلام و الاتصال و مواكبة التطور السريع لهذه التقنية من أجل استخلاص الدليل الالكترون ي و التحقق من سلامته[1].

رابعا : خـــصوصية الـــــــــــمجرم الـــــــمعلوماتي

يتميز المجرم المعلوماتي عن المجرم العادي باتسامه بمستوى معرفي في مجال تقنية المعلومات و قدرته على استعمال جهاز الحاسوب وشبكة الانترنت ,و المهارة الفنية خاصة في مجال الجرائم الاقتصادية كالتحويل الالكتروني الغير مشروع للأموال و سرقة المعلومات المشفرة[2] .

لذلك فإن المجرم المعلوماتي هو مجرم متخصص و يتمتع باحترافية عالية في مجال تقنية المعلومات, و له القدرة على تخطي جميع الحواجز المخصصة لحماية أنظمة الحواسيب و كسر كلمات المرور أو الشفرات التي تعدها شركات البرمجة, وقدرته على طمس هويته و محو أثار جريمته.

وكل هذه المهارات قد يكتسبها المجرم المعلوماتي إما بالممارسة أو بالدراسة المخصصة في مجال تقنية المعلومات, وذلك بدافع تحقيق مصلحة خاصة به أو لحساب شخص معنوي كالشركات العامة أو الخاصة و التي تعمل في مجال المعلوماتية[3] , ويصنف مجرمو المعلوماتية إلى:

[1] سعيدي سليمة و حجاز بلال, المرجع السابق, ص 34
[2] نهلة عبد القادر المومني, مرجع سابق,ص 57
[3] حنان ريحان مبارك المضحكي,المرجع السابق, ص57

أ/الهاكرز أو القراصنة : ومنهم الهواة و الفضوليين بغرض التسلية فقط و منهم المحترفون و يطلق عليهم اسم الهاكرز أو المخترقين لهم قدرات عالية على الإتلاف و التخريب و الاختراق باستخدام فيروسات أو قنابل منطقية[1].

ب/الجواسيس: يهدفون لجمع المعلومات لمصلحة بلدانهم أو لمصلحة بعض الشركات المنافسة.

ج/المخادعون: يتمتعون بقدرات تقنية عالية في مجال المعلوماتية تمكنهم من اختراق الكود السري لتغيير المعلومات و تقليد البرامج أو التحويل في الحسابات [2].

و عليه فالباعث وراء ارتكاب الجرائم المعلوماتية يختلف بحسب اختلاف أنماط المجرم المعلوماتي, فقد يكون بغرض التسلية فقط بدون الإضرار بالغير, أو بإثبات قدرته على اختراق الحواجز الأمنية و كلمات المرور المشفرة,كما قد يكون بغرض تحقيق ربح مادي بطريقة غير مشروعة أو للحصول على معلومات و بيانات لمصلحة شركات منافسة, أو بغرض الانتقام و الإضرار بشخص أو مؤسسة ما كان يعمل بها أو لمحو ديونه السابقة[3] .

الفرع الثالث: أنواع الجريمة المعلوماتية

ننوه في البداية أنه لا يمكن حصر أنواع الجرائم المعلوماتية لاختلاف أصنافها من مجتمع لأخر حسب درجة استخدامه للحاسب الآلي و شبكات الانترنت في مختلف مجالات الحياة ,كما أنها في تزايد مستمر و لا يمكن حصرها لذا اختلف فقهاء القانون الجنائي في تصنيفها باختلاف الزاوية التي ينظر منها, وسنتطرق للتقسيم الفقهي الأكثر شيوعا و تداولا و الذي يأخذ بمعيار محل الجريمة المعلوماتية ,فقد يكون نظام المعلومات محلا أو موضوعا للجريمة .

أولا : الجرائم الواقعة بواسطة النظام المعلوماتي

يعد الحاسب الآلي و برامجه و شبكة الانترنت وسيلة لارتكاب هذا النوع من الجرائم أين يلجأ المجرم المعلوماتي لها لتسهيل تحقق النتيجة الإجرامية و طمس هويته و محو أثارها ,و هي تنقسم إلى:

---

[1] سعيدي سليمة و حجازي بلال , المرجع السابق , ص 30 . خالد عياد الحلبي , المرجع السابق , ص 34 .

[2] حنان ريحان مبارك مضحكي , المرجع السابق , ص 42 .

[3] سعيداني نعيم, آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري, مذكرة ماجستير ,تخصص علوم جنائي, قسم الحقوق, كلية الحقوق و العلوم السياسية, جامعة باتنة, 2003 ص60 .

أ/ جرائم واقعة على الأشخاص : وهي الجرائم المعلوماتية التي يكون الغرض منها الاعتداء على الأشخاص, و نذكر منها على سبيل المثال لا الحصر, كجرائم السب و الشتم و القذف,و جرائم الاعتداء على الحياة الخاصة للأفراد, السرقة و نشر المعلومات, التحريض على الانتحار [1] .

ب/ جرائم واقعة على الأموال : بعدما أصبحت الكثير من المعاملات المالية تتم إلكترونيا عبر شبكات الانترنت, أدى ذلك إلى ظهور العديد من الجرائم المعلوماتية التي ينصب فيها الاعتداء على المال, نذكر منها مثلا: التحويل الالكترون ي الغير مشروع للأموال, قرصنة أرقام البطاقات الممغنطة, جرائم غسيل الأموال و القمار عبر الانترنت, و غيرها من الجرائم التي ساهمت الشبكة العنكبوتية في انتشارها و تطورها حتى بين الدول[2].

ج/ جرائم واقعة على أمن الدولة:

لم تعد مخاطر الجرائم المعلوماتية تهددا الأفراد و الشركات و أموالها و حسب ,و إنما امتدت لتمس بأمن الدول خاصة تلك التي تستهدف المؤسسات العسكرية أو الحكومية التي لم تعد بمنأى عن الجناة المعلوماتيين و المنظمات الإرهابية و المخابرات الأجنبية ,و التي تشكل خطرا و تهديدا على أمن الدولة الداخلي و الخارجي [3], وهي تعد من أخطر الجرائم المعلوماتية خاصة الإرهاب المعلوماتي أين أتاحت الانترنت للكثير من المنظمات الإرهابية الترويج لأفكارها, و جرائم التجسس الإلكتروني على الدول بالإطلاع على الأسرار الاقتصادية و العسكرية, و جرائم تخريب المعطيات الخاصة بمؤسسات الدولة, و إهانة رموز الدولة, و المساس بالنظام العام...الخ.

ثانيا:الجرائم الواقعة على النظام المعلوماتي

وهي الجرائم التي ينصب الاعتداء فيها على النظام المعلوماتي, ونميز هنا بين الجرائم التي تستهدف المكونات المادية للنظام من الحواسيب و الأجهزة الملحقة بها كالأسطوانات و الطابعات, و كل اعتداء عليها يندرج ضمن الجرائم التقليدية تحت وصف السرقة أو خيانة الأمانة أو الإتلاف العمدي أو الحرق ,و بين الجرائم الواقعة على المكونات المعنوية للنظام المعلوماتي أو ما يعرف بنظام المعالجة الآلية للمعطيات بالمعنى الفني الدقيق [4], أين ينصرف الاعتداء على

[1] عبد الفتاح بيومي حجازي ,مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت , دار الفكر و الحياة , الإسكندرية , 2006 , ص 325 .
[2] خالد عياد الحلبي , المرجع السابق , ص 60 .
[3] عبد الفتاح بيومي حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت, المرجع السابق, ص 325 .
[4] حنان ريحان مبارك مضحكي , المرجع السابق , ص 44 .

المعطيات و المعلومات و البيانات والبرامج الالكترونية المخزنة في ذاكرة الحاسب إما بالإتلاف أو المحو أو الاستبدال أو حتى بالتعرض لحق انسياب هذه المعلومات[1].

المطلب الثاني

آليات مواجهة الجريمة المعلوماتية

لقد دق الإجرام المعلوماتي ناقوس الخطر لأغلب دول العالم, بسبب ثورة تقنية تكنولوجي ا المعلومات التي تعرف تطور سريع و ملحوظ بتطور تقنية المعلومات ,أين توسعت دائرة ضحاياه و شملت حتى الدول و كبرى الشركات, و تفاقمت الأضرار الناجمة عنه , الأمر الذي دفع بالدول لتكثيف جهودها ولا سيما الجزائر في سبيل مواجهة الجريمة المعلوماتية من خلال عدة آليات و ووسائل قصد رصدها المبكر و جمع الأدلة عنها, و سنتناول في هذا المطلب لآليات التعاون الدولي و الإقليمي لمواجهة الجريمة المعلوماتية في الفرع الأول , و الآليات التشريعية لمواجهتها سواء في القوانين العامة أو الخاصة مواجهتها في الفرع الثاني . ثم الآليات المؤسساتية في الفرع الثالث .

الفرع الأول : التعاون الدولي و الإقليمي لمواجهة الإجرام المعلوماتي

إن تنامي ظاهرة الإجرام المعلوماتي العابر للحدود الوطنية زاد في الحاجة لتضافر الجهود الدولية لمكافحته , و ملاحقة مرتكبيه , رغم بعض العوائق التي تجعل التعاون صعبا.

أولا: التعاون في إطار المنظمات الدولية

هناك العديد من الهيئات و المنظمات التي أدت دور ملحوظ في إبرام الاتفاقيات و ترسيخ التعاون الدولي لمواجهة الإجرام المعلوماتي[2], و نذكر منها :

1-**مؤتمر الأمم المتحدة السابع** : المنعقد بميلانو"ايطاليا" سنة 1985 الذي أكد على ضرورة مواجهة التشريعات الحديثة للجرائم المنظمة العابرة للحدود الوطنية و تقديم المساعدة التقنية للبلدان النامية .

[1] خالد ممدوح إبراهيم, فن التحقيق الجنائي في الجرائم الالكترونية , دار الفكر الجامعي , الإسكندرية , ط 1 , 2009 , ص 92 .
[2] نبيلة هبة هروال , المرجع السابق , ص 147 .

2-**الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية** "**بودابست** "بتاريخ : 22 نوفمبر 2001, و تناولت كل ما تتعلق بالجريمة المعلوماتية , وحددت صور الإجرام المعلوماتي و حثت على ضرورة التعاون الدولي لمكافحة الجريمة و القبض على المجرمين[1].

3-**الجهود العربية في إطار مكافحة الجريمة المعلوماتية** : أين تم إعداد قانون عربي نموذجي سنة 1996 من قبل المنظمة العربية لمكافحة الجرائم المعلوماتية, وحددت صورها سواء التي تتم عبر أو باستخدام شبكة الانترنت, و هدفها تعزيز التعاون العربي في مجال مكافحة جرائم تقنية المعلومات العابرة للحدود و كيفية التحقيق فيها و متابعة مرتكبيها, و لو ارتكبت في أكثر من دولة نصت على أساليب التعاون القانوني و القضائي و الاختصاص و تسليم المجرمين .[2]

و قد انضمت الجزائر لهذه الاتفاقية العربية في 21ديسمبر 2010 ,بعدما انضمت في إطار التعاون الدولي للعديد من الاتفاقيات الدولية الهادفة لمكافحة الجريمة المعلوماتية.

و قد نص المشرع على إمكانية التعاون الدولي في مجال المساعدة و تبادل المعلومات للكشف عن الجرائم المنصوص عنها في ظل القانون : 04/09 السالف الذكر .

ثانيا: التعاون الدولي الأمني : بالإضافة للأجهزة الأمنية الحكومية على مستوى كل دولة, فإن مكافحة الإجرام المعلوماتي يستدعي تعاون أجهزة الشرطة بين الدول و تنسيق العمل فيما بينها لضبط المجرمين , و تبلور هذا التعاون الدولي في إنشاء المنظمة الدولية للشرطة الجنائية – الأنتربول –التي تقيم علاقات مع الدول الأعضاء في المنظمة لتبادل المعلومات بين سلطات التحقيق بخصوص الجرائم المعلوماتية المتشعبة و ذات الطابع العالمي[3] .

كما أنشأ المجلس الأوروبي في عام 1991 المنظمة الدولية للشرطة الأوروبية – الأوروبول – تختص بملاحقة الجرائم العابرة للحدود و التي يمكن إن تمتد آثارها لعدة دول[4]

هذا بالإضافة إلى المكتب العربي للشرطة الجنائية لتأمين التعاون بين أجهزة الشرطة للدول الأعضاء في مكافحة الجريمة المعلوماتية ,و تقديم الدعم و التعاون , و تطوير أجهزة الشرطة.

---

[1] احمد عبد الله المراغي, المرجع السابق, ص 124-125

[2] سعيدي سليمة و حجازي بلال , المرجع السابق , ص 147 .

[3] نبيلة هبة هروال , المرجع السابق , ص 159 .و نبيلة هبة هروال , المرجع السابق , ص 149 .

[4] احمد عبد اللاه المرغي, المرجع السابق, ص 129

ثالثا: الـــــــتعاون الدولي الـــــــــقضائي لمواجهة الجريمة المعلوماتية

تعرف المساعدة القضائية دوليا بأنها: "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم" [1], و تتخذ هذه المساعدة القضائية في المجال الجنائي عدة صور منها:

1-**تبادل المعلومات** : و تكون بتبادل البيانات و الوثائق و المواد الاستدلالية التي تطلبها سلطة قضائية أجنبية بصدد النظر في جريمة ما , وتتبادل السوابق القضائية مابين الدول الأعضاء .

هذا بالإضافة إلى إمكانية نقل الإجراءات من دولة لأخرى, كما نصت عليه المادة: 16 من النموذج الاسترشادي لاتفاقية التعاون القضائي و القانوني الصادر عن مجلس التعاون الخليجي 2003 [2]

2-**الإنابة القضائية الدولية** : وتعني اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية المعروضة على الجهات القضائية للدولة التي تقدمت بطلب الإنابة و تعرض عليها القيام بهذا الإجراء الجنائي, و يتم هذا الطلب من وزارة العدل عادة عبر القنوات الدبلوماسية لتفادي بطئ الإجراءات[3] .

3-**تسليم المجرمين** تعد من أهم آليات مكافحة الجرائم المعلوماتية , و حماية المجتمعات من المخلين بأمنها و استقرارها حتى لا يبقون بمنأى عن العقاب ,خاصة عندما يرتكبون جريمة في دولة و النتيجة في دولة أخرى و يفر لبلد ثالث للهروب من العدالة ,فهو من جهة يضمن تحقيق مصلحة الدولة الأولى و يضمن معاقبة الفرد الذي أخل بتشريعاتها ,و يحقق من جهة أخرى للدولة الثانية المطلوب منها التسليم تطهير إقليمها من المجرمين ,و سواء كان التسليم إداري أو قضائي فهو يتطلب شروط خاصة تتعلق بالجريمة و إجراءات خاصة به.

الفرع الثاني: الآليات التشريعية لمواجهة الإجرام المعلوماتي

في إطار مكافحة الجريمة المعلوماتية سن المشرع الجزائري بسن تشريعات قانونية سواء في قانون العقوبات و قانون الإجراءات الجزائية أو في القوانين الخاصة.

---

[1] بدري فيصل, مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي , أطروحة دكتوراه , جامعة الجزائر يوسف بن خدة , كلية الحقوق , 2018/2017 , ص 68

[2] أحمد عبد الله المراغي , المرجع السابق , ص 129 .

[3] أحمد عبد الله المراغي , المرجع نفسه , ص134 .

أولا/ الأمن المعلوماتي في قانوني العقوبات وقانون الإجراءات الجزائية: قام المشرع الجزائري في سبيل سد الفراغ القانوني لمواجهة الإجرام المعلوماتي بتعديل قانون العقوبات بموجب القانون 15/04 2014 المتمم للأمر 156/66 المتضمن لقانون العقوبات [1] , تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات في القسم السابع مكرر في المواد 394 مكرر إلى 394 مكرر 7 منه .

كما أدخل تعديلا أخر لقانون العقوبات بموجب القانون 23/06 مؤرخ في 20 ديسمبر 2006 بخصوص القسم السابع السالف الذكر و شدد في العقوبة المقررة في الأفعال الماسة بنظام المعالجة الآلية للمعطيات بسبب تزايد خطورتها على امن الدولة و الاقتصاد الوطني [2].

و قام المشرع الجزائري بحصر الجرائم الماسة بنظام المعالجة الآلية المعطيات و ما هي إلا صورة من صور الجرائم المعلوماتية و تتمثل في:

- الدخول أو البقاء الغير المشروع في كل أو جزء من المنظومة للمعالجة أو محاولة ذلك ,
- الغش المعلوماتي في معطيات النظام بالحذف أو التعديل .
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار بمعطيات مخزنة أو معالجة أو مرسلة في منظومة معلوماتية .
- تكوين جمعية أشرار لإعداد الجرائم المنصوص عنها في هذا القسم .
- الجرائم المعلوماتية التي يرتكبها الشخص المعنوي.

كما قام المشرع الجزائري باستحداث مجموعة من الإجراءات الجزائية لمواجهة الجريمة المعلوماتية تتماشى و الطبيعة الخاصة بها, رغم أنها تخضع في العموم لنفس إجراءات متابعة الجرائم التقليدية لا سيما في إجراءات التحقيق و المحاكمة[3] وهي باختصار:

- تمديد الاختصاص الإقليمي لضباط الشرطة القضائية لمعاينة جرائم المعلوماتية.

[1] الأمر : 15/04 , المؤرخ في 10 نوفمبر 2014' جر , عدد : 71 , المتمم للأمر : 156/66 المؤرخ في : 18 صفر 1386 , الموافق ل: 8 يونيو 1966 , المتضمن لقانون العقوبات ,ج ر, عدد : 49 .

[2] القانون : 23/06 , المؤرخ في : 20 ديسمبر 2006 ' ج ر , عدد : 84 ,المعدل و المتمم للأمر :156/66 ' المؤرخ في : 18 صفر 1386 , الموافق ل: 8 يونيو 1966 , المتضمن لقانون العقوبات ,ج ر, عدد : 49 .

[3] أمال قارة, الحماية الجزائية للمعلومات في التشريع الجزائري , دار هومة للطباعة و النشر , الجزائر , ط 1 , 2006, ص 130

-تمديد الاختصاص المحلي لوكيل الجمهورية حسب المادة: 37 من قانون الإجراءات الجزائية.
-النص على قواعد استثنائية لتفتيش المنظومة المعلوماتية في المادة 7/45 من نفس القانون.
-النص على التوقيف للنظر في جرائم المعلوماتية في المادة 6/51 من نفس القانون .
-النص على أساليب التحري الخاصة بأنظمة المعالجة و تتعلق باعتراض المراسلات و تسجيل الأصوات و التقاط الصور و كذا التسرب ,و هو ما سنتناوله في المطالب اللاحقة[1]

ثانيا: الأمن المعلوماتي في القوانين الخاصة

1-**قانون البريد و الاتصالات السلكية و اللاسلكية رقم 2000/03** [2] ,أين تضمن الفصل الثاني من الباب الرابع الجزاءات المترتبة على مخالفة أحكامه و جرم الأفعال التالية:

-تخريب البريد و انتهاك سرية الاتصالات من كل موظف البريد و المواصلات و كل شخص مرخص له تقديم خدمة اتصالات سلكية و لاسلكية.
-استغلال شبكة اتصالات دون ترخيص أو تحويل خطوط الاتصالات السلكية و اللاسلكية.
-إفشاء أو نشر بدون ترخيص من المرسل أو المرسل إليه مضمون المراسلات[3].

2-**قانون التأمينات: رقم 08/01** [4] المعدل و المتمم للقانون: 73/01 المتعلق بالتأمينات, أين نص المشرع على الجزاءات المقررة عند الاستعمال الغير مشروع للبطاقة الالكتروني ة للمؤمن له اجتماعيا أو للمفتاح الالكتروني لمهن الصحة ,أو كل من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية و الإدارية المدرجة في البطاقة الالكترونية أو المفتاح الالكتروني[5] .

3-**القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها رقم 04/09** [6]: أين تدارك المشرع الجزائري القصور أو الفراغ التشريعي الوارد في القانون رقم

[1] مولود ديدان, المرجع السابق, ص 18.
[2] القانون : 2000/03 , المؤرخ في : 05 أوت 2000 , و يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية , ج ر , عدد : 48 , صادر بتاريخ : 06 أوت 2000 .
[3] المواد 105 و 127 من القانون 2000/03 المتعلق بقانون البريد و المواصلات السلكية و اللاسلكية , المرجع نفسه .
[4] القانو : 08/01 , المؤرخ في : 23 جانفي 2008 , المعدل و المتمم للقانون رقم : 11/83 المتعلق بالتأمينات الاجتماعية , ج ر , العدد رقم : 04 , الصادر بتاريخ : 27 جانفي 2008 .
[5] المادة 93 مكرر 2و3 من القانون 08/01 المتعلق بالتأمينات الاجتماعية , المرجع نفسه .
[6] القانون : 04/09 المؤرخ في : 14 شعبان 1430, الموافق ل : 5 غشت 2009 , و المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاتصال و الإعلام و مكافحتها , ج ر , العدد : 47 , بتاريخ : 16 أوت 2009 .

15/04 المعدل للأمر رقم: 156/66 المتضمن قانون العقوبات ,الذي نص على نوع من الجرائم المعلوماتية بمفهومها الضيق, و هي تتعلق بالاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات و حصر صورها في المواد: 394 مكرر إلى 394 مكرر 7 , وحاول سد الفراغ القانوني والتوسيع من مفهوم الجريمة المعلوماتية .

و بذلك أصبحت الجريمة المعلوماتية و التي أطلق عليها المشرع الجزائري مصطلح الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و تشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات, و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.[1]

و يجمع هذا القانون بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية و بين القواعد الوقائية التي تسمح بالترصد المبكر للاعتداءات المحتملة و تحديد مكان مرتكبي الجرائم المعلوماتية.

4-**القانون المتعلق بحقوق المؤلف رقم 03/05** [2]:

الذي نص على تجريم كل انتهاك لحقوق المؤلف و الحقوق المجاورة عن طريق التقليد بأي وسيلة كانت بما فيها منظومة المعالجة المعلوماتية [3] .

5-**القانون المتعلق بعصرنة العدالة رقم 03/15** [4]: حيث تطرق في الفصل الثاني إلى المنظومة المعلوماتية المركزية لوزارة العدل ,و الإشهاد على صحة الوثائق الالكترونية و ضمان حمايتها؛ أما الفصل الثالث فتعرض إلى إرسال الوثائق و الإجراءات القضائية عبر الوسائل الالكترونية,أما الفصل الخامس فتعرض إلى الأحكام الجزائية لحماية التوقيع و التصديق الإلكتروني.

الفرع الثالث: الآليات المؤسساتية لمواجهة الإجرام المعلوماتي

إن طبيعة الجرائم المعلوماتية أوجبت استحداث أجهزة متخصصة بمكافحة هذا النوع من الجرائم و الكشف مرتكبيها و الوقاية منها ,و هناك أجهزة على المستوى الدولي و يطلق عليها اسم

[1] المادة 2 من القانون 04/09, المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاتصال و الإعلام , المرجع السابق .
[2] القانون : 03/05 , المؤرخ في : 2003/07/19 , المتعلق بحقوق المؤلف و الحقوق المجاورة , ج ر , عدد : 44 , الصادر بتاريخ : 2003/07/23 .
[3] المادة : 52 من القانون : 03/05 , المتعلق بحقوق المؤلف و الحقوق المجاورة , المرجع السابق .
[4] القانون : 03/15 , المؤرخ في : أول فبراير 2015 , و المتضمن عصرنة العدالة , جر , العدد : 06 .

شرطة الانترنت كالمنظمة الدولية للشرطة الجنائية –الأنتربول – , و أجهزة على المستوى الإقليمي كالشرطة الأوروبية –الأوروبول – , أما على المستوى الوطني فهناك عدة أجهزة تقوم بعملية البحث والتحري ,لأن أغلب التشريعات المقارنة توجهت لإسناد هذه المهمة لأجهزة متخصصة و هي:

أولا/ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال :

و التي أنشئت بموجب القانون رقم : 09/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها, ومن مهامها:

– تفعيل التعاون القضائي والأمني الدولي, و إدارة و تنسيق عمليات الوقاية و المساعدة التقنية للجهات القضائية .

–و يمكن تكليفها قضائيا للقيام بخبرة قضائية عند الاعتداء على منظومة معلوماتية تهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاقتصادية للوطن.

– مراقبة الاتصالات الالكترونية كإجراء وقائي منذ جرائم الإرهاب و الجرائم الماسة بأمن الدولة بإذن من النائب العام لدى مجلس قضاء الجزائر.

– الوقاية من كل اعتداء على منظومة معلوماتية على نحو يهدد بمؤسسات الدولة و الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني بإذن من السلطة المختصة .[1]

ثانيا: المعهد الوطني للأدلة الجنائية و علم الإجرام:

و يوجد مقره ببوشاوي بالعاصمة, يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة و تقوم بإنجاز الخبرة, التكوين و التعليم و تقديم المساعدات التقنية, الدراسات و التحاليل في علم الجريمة و إنجاز الخبرة, البحوث,أما دائرة الإعلام الآلي و الالكتروني فهي مكلفة بمعالجة و تحليل و تقديم الأدلة الرقمية المساعدة للقضاء, كما تقدم كل المساعدات التقنية للمحققين في الجرائم المعلوماتية المعقدة, و تتكون كل دائرة من ثلاث مخابر و هي:

أ–**مخبر الإعلام الآلي و الالكتروني** : لمعالجة المعطيات الرقمية للحواسيب و الهواتف و ذاكرة الفلاش و تحديد التزوير الرقمي للبطاقة البنكية.

[1] سعيداني نعيم , المرجع السابق ,ص 34 .

ب-مخبر الفيديو : يقوم بتحليل و مقارنة شرعية الفيديو و الصورة و إعادة بناء مسرح الجريمة بتقنية ثلاثية الأبعاد, و تحسين نوعيتها.

ج-مخبر الصوت : يعمل على تحسين نوعية إشارة الصوت و نزع التشويش و تحديد شرعية التسجيلات الصوتية و معرفة المتكلم[1].

ومن مهام المعهد الوطني للأدلة الجنائية و علم الإجراء القيام بمساعدة و حدات الدرك الوطني للبحث عن مرتكبي الجرائم المعلوماتية والتعرف على عناوينهم الالكترونية و أرقام المرسلين محل التحريات.

ثالثا/ المديرية العامة للأمن الوطني :

في سنة 2007 استحدثت المديرية العامة للأمن الوطني لدى مخابر الشرطة العلمية المتواجدة بالجزائر العاصمة و قسنطينة ووهران ,أقساما متخصصة في تتبع الأدلة الرقمية لمساعدة القضاء في الكشف عن الجرائم المعلوماتية.

أما في سنة 2010 قامت المديرية العامة للأمن الوطني باستخدام خلايا مختصة بمكافحة الجريمة المعلوماتية على مستوى جميع مصالح امن ولايات الوطن

كما أن المديرية العامة للأمن الوطني تعد عضوة في المنظمة الدولية للشرطة الجنائية(INTERPOL) لإتاحة مجال التعاون و تبادل المعلومات ,و تسهيل إجراءات تسليم المجرمين, و تنفيذ الإنابات الدولية و القضائية و نشر أوامر القبض للمبحوث عنهم دوليا[2].

[1] هواري عياش, المرجع السابق, ص3

[2] عبد الرحمن حملاوي, مداخلة ب عنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية, جامعة بسكرة, كلية الحقوق, 2016

المبحث الثاني

خصوصية التحقيق في الجريمة المعلوماتية

تعد الجريمة المعلوماتية آفة العصر و الأخطبوط الذي أنجبته الحضارة التقنية لثورة المعلومات و التكنولوجيا, و الذي تمتد أذرعه لجميع أنحاء دول العالم, و لم تفلت من قبضته لا الدول الضعيفة ولا المتطورة ,و أصبحنا نعيش في عصر الاستعمار الالكتروني أين أصبحت كل الدول و المؤسسات و الأفراد مستهدفون من هذا النوع من الإجرام المعلوماتي الذي عجزت حتى الدول الغربية عن تطويقه, رغم أنها تقوم باستمرار لاكتشاف أدوات رقابة جديدة أكثر فعالية و فرض قوانين أكثر صرامة.

و نظرا لخصوصية الإجرام المعلوماتي انجر عنه خصوصية في التحقيق المعلوماتي , لاسيما أمام عدم كفاية أساليب التحري و التحقيق الكلاسيكية , و تظهر هذه الخصوصية من خلال إبراز خصائص التحقيق و المحقق المعلوماتي , و الصعوبات التي تعترض التحقيق في المطلب الأول , أما في المطلب الثاني سنتناول فيه لقواعد الاختصاص القضائي لمواجهة الإجرام المعلوماتي , من خلال التطرق لمبادئ الاختصاص التي تحكمه و حالات تمديده والصعوبات التي تحول دون التعاون الدولي لمواجهة الجريمة المعلوماتية العابرة للحدود .

المطلب الأول

خصائص التحقيق في الجريمة المعلوماتية

تعد مرحلة التحقيق الابتدائي من مسائل المهمة في سبيل البحث و التحري عن الجرائم المعلوماتية و حجر الزاوية في التحقيق الجنائي, وهو علم يقوم على ضوابط فنية و قانونية معا,و سنتناول في هذا المطلب لسمات و خصائص التحقيق في الجريمة المعلوماتية في الفرع الأول , ثم نبرز خصائص المحقق المعلوماتي في الفرع الثاني , أما في الفرع الثالث سنتطرق للصعوبات التي تواجه التحقيق الجنائي المعلوماتي .

الفرع الأول: سمات التحقيق المعلوماتي:

لقد أدى الاستخدام السيئ و الغير مشروع لتقنيات تكنولوجيا الإعلام و الاتصال, إلى ظهور علم جديد في البحث الجنائي هو علم التحقيق المعلوماتي (الرقمي) .

أولا: تعريف التحقيق المعلوماتي : التحقيق بصفة عامة هو مجموع إجراءات التحقيق الجزائي التي يباشرها المحقق الجزائي عند وقوع الجريمة للوصول للحقيقة بالشكل المحدد قانونا[1].

أما التحقيق المعلوماتي فهو مجموعة الإجراءات و الوسائل المشروعة قانونا و التي يقوم بها المحقق للكشف عن الجريمة المعلوماتية و إسنادها لمرتكبها بضبط الأدلة الرقمية و تقديمها لسلطات التحقيق القضائي[2].

و عليه يمكن القول أن التحقيق المعلوماتي هو عملية جمع أكبر قدر من المعلومات و الأدلة من أجهزة و حواسيب المشتبه بهم ,من قبل ضباط الشرطة القضائية بكيفية تخزين المعلومات في القرص الصلب و مختلف أنظمة الملفات و استرجاع المخفي منها و حتى المحذوفة كليا من النظام و كذا فك التشفير ,ولو بعد قيام المجرم المعلوماتي بالتلاعب بالدليل أو إخفاء آثاره و طمس هويته,بالاستعانة ببرامج متخصصة لاستعادتها.

ثانيا : سمات التحقيق المعلوماتي

بالإضافة لخصائص التحقيق المتعارف عليها من سرية التحقيق بالنسبة للعامة و العلنية بالنسبة للخصوم, و كذا تدوين إجراءات التحقيق في محاضر حتى تكون لها حجية, و ضمان حياد و استقلالية المحقق و السرعة في التحقيق [3] , إلا إن التحقيق المعلوماتي يتسم بجملة من المواصفات التي تميز عن التحقيق العادي و يرجع ذلك للأسباب التالية:

- الجرائم المعلوماتية في الغالب لا تترك أثرا ماديا في مسرح الجريمة.
- قدرة المجرم المعلوماتي على إتلاف الدليل المعلوماتي (الرقمي) في وقت قياسي ,و خاصة المحترف الذي يمكنه جعل حاسوبه يحذف جميع الملفات و المعلومات و البيانات تلقائيا

[1] عمر بن إبراهيم بم حماد العمري, إجراءات الشهادة في مرحلتي الاستذلال و التحقيق الابتدائي في ضوء نظام الإجراء السعودي, رسالة ماجيستير جامعة نيف العربية, 2007, ص22

[2] د/ مصطفى محمد موسى, التحقيق الجنائي في الجرائم الالكترونيةِ,.مطابع الشرطة , القاهرة , ط 1 , 2009, ص 165 .

[3] د/ احمد ممدوح إبراهيم, فن التحقيق الجنائي في الجريمة المعلوماتية, المرجع السابق , ص 56 .

عند بدء التشغيل في حال عدم إدخال كلمة المرور, لذلك فالمحقق إذا قام بإدخال كلمة مرور خاطئة قد يتسبب في إتلاف الدليل الرقمي.

-يتسم التحقيق المعلوماتي باعتماده على وسائل تقنية و البرامج الكفيلة بكشف الجرائم المعلوماتية من خلال تفتيش المنظومة المعلوماتية

- كما إن فاعلية التحقيق المعلوماتي مرهونة بالمعرفة القانونية و الفنية معا للمحقق المعلوماتي, وضرورة احترامه لضوابط إجراءات التفتيش و الضبط و سلامته إجراءات الحصول على الدليل الرقمي[1] , و كذا الحفاظ على خصوصية المشتبه فيه و سري المعلومات الأخرى التي تم الاطلاع عليها بمناسبة إجراءات التحري.

-ضرورة تشكيل فريق للتحقيق لإنجاز مهمته البحث و التحري و العثور على الأدلة في النظام المعلوماتي (مسرح الجريمة الالكتروني ة), و يتشكل الفريق من مختصين في التحقيق الجنائي المعلوماتي و خبراء فنين في الإعلام الآلي وشبكة الانترنت.

- السرعة في الحصول على الدليل المعلوماتي و عمل نسخة احتياطية من الاسطوانات و الأقراص الصلبة للحاسب , و تحليل المعلومات الموجودة بالنظام المعلوماتي و استعادة الملفات المخفية أو المحذوفة أو المشفرة, خوفا من إتلافها من قبل المجرم المعلوماتي من خلال شبكة الانترنت ولو من جهاز حاسب آلي آخر أو هاتفه الذكي

ثالثا: أدوات البحث الجنائي المعلوماتي:

هناك عدة أدوات و برامج مخصصة لأنظمة الويندوز يستخدمونها رجال الضبطية القضائية و المحققون الجنائيين بالتعاون مع شركة مايكروسوفت لتسهيل المعلومات و الأدلة من أجهزة المشتبه بهم ,و تحديد المواقع التي تم تصفحها و الوصول لكلمات المرور, ثم تخزينها في ذاكرة USB دون أي تعديل على النظام أو دون الحاجة لنقل الجهاز للمختبر لتحليله .

وهذه الأدوات و البرامج ليست مخصصة للعامة بل توزع على أجهزة الشرطة و توجد على جهاز المحقق أو مثبت على ذاكرة USB ,وتقوم بتحليل المعلومات إعداد تقرير مفصل عن الجهاز و تخزين الدليل الرقمي.

[1] د/ مصطفى محمد موسى, التحري في مجتمع المعلومات و المجتمع الافتراضي , ب.د.ن , 2011 , ص 167 .

الفرع الثاني: خصائص المحقق المعلوماتي:

المحقق الجنائي المعلوماتي هو الشخص الذي يقوم بإجراءات التحري و التحقيق في البلاغات و الشكاوى عن الجرائم المعلوماتية, و الكشف عن مرتكبيها و تجميع الأدلة الجنائية الرقمية.[1], بصورة مباشرة أو بتكليف من قاضي التحقيق [2].

وعليه من خلال هذا التعريف يظهر لنا صنفين من المحققين في الجرائم المعلوماتية, النوع الأول يتمثل في المتخصصين في مجال التحقيق الجنائي, و النوع الثاني يتمثل في الخبراء الفنين المتخصصين في مجال الحاسب الآلي و شبكاته [3] ,و الخبرة لوحدها غير كافية بل يجب أن تكون بالموازاة مع عمل المحقق الجنائي, فقد يعتقد الخبير الفني أنه تحصل على الدليل الحاسم في الجريمة المعلوماتية لكن من الناحية القانونية غير مقبول.

و يكون بذلك ظهور الجرائم المعلوماتية بسبب تطور تقنية المعلومات قد أضاف أعباء ثقيلة على عاتق رجال الضبطية القضائية في أن يكون لهم القدر الكافي من الثقافة الفنية و التقنية في أنظمة الحواسيب, والتي لم يتعودوا عليها ولم يألفوها ,في سبيل التحقيق في عالم افتراضي .

أولا: الميزات الفنية للمحقق الجنائي:

يتميز المحقق المعلوماتي بجملة من الخصائص التي تميزه عن المحقق العادي في الجرائم التقليدية', نظرا لخصوصية الجريمة المعلوماتية, و ذلك من خلال الضوابط التي يعمل وفقها, وهي:

- إلمام المحقق المعلوماتي بالجوانب الفنية و التقنية لأجهزة الحاسوب و الانترنت.
- تشكيل فرقة تحقيق فنية, لضمان جدية و فاعلية التحقيق المعلوماتي مع إسناد لكل واحد المهمة حسب تخصصه خلال عملية التفتيش في مسرح الجريمة
- الحصول على الدليل المعلوماتي بطرق قانونية مشروعة و تخزينها في أقراص معدة لذلك ومنع حذفها , و الحرص على عدم تعريضها لأية مؤثرات خارجية كالقوى الكهرومغناطيسية حتى لا يتلف محتواها .

[1] مصطفى محمد موسى, المرجع السابق, ص253 .
[2] مصطفى محمد موسى, المرجع السابق, ص254 . و محمود حماد مرهج الهيتي , أصول البحث و التحقيق الجنائي , دار الكتابة القانونية , القاهرة , 2014 , ص 23 .

- وضع خطة عمل من قبل أعضاء فريق التحقيق و التشاور فيما بينهم في سبيل الحصول على الدليل المعلوماتي و تفادي إتلافه و الحفاظ على سلامته لتقديمه أما الفضاء.[1]
- إعداد المحقق المعلوماتي لمحاضرة التحقيق يكون بناءا على التقارير التي يعدها الخبراء الفنيون في أنظمة الحواسيب, والذي يكون على دراية و فهم رموز هذه التقارير و تصب عن كيفية ارتكاب الجرائم في الفضاء المعلوماتي و تجنب إتلاف الدليل الالكتروني[2].

ثانيا: تأهيل و تدريب المحقق المعلوماتي:

لقد تنبهت العديد من الدول و توجهت نحو التخصص المهني و التدريب الفني للمحقق المعلوماتي سواء كان ضابط شرطة قضائية أو قاضي تحقيق ,و إعدادهم بالشكل الذي يسمح لهم بمواجهة نوع جديد من الإجرام المعقد بالتعاون مع الخبير الفني في نظام المعلوماتي و يكون عملهما متكامل و متناسق.

وليس بالضرورة أن يكون المحقق المعلوماتي خبير في الحاسوب و مختلف النظم المعلوماتية و شبكات الانترنت ,بقدر ما يكون ملم ببعض المسائل الأولية و كيفية تأمين الدليل المعلوماتي و صحة استخلاصه من الناحية الفنية و القانونية [3].

ضرورة التكوين المستمر سواء عن طريق دورات داخل أو خارج الوطن, أو حتى التكوين عن بعد من قبل مختصين في الأنظمة المعلوماتية حتى يكون مستعدا لمواجهة مختلف مظاهر الإجرام المعلوماتي الذي يعرف تزايد ملحوظ و ملفت للنظر .

الفرع الثالث: صعوبات التحقيق المعلوماتي

يتعرض التحقيق و البحث و التحري في الجرائم المعلوماتية للعديد من العراقيل و الصعوبات التي تعيق الوصول للحقيقة و إثباتها و نسبتها لمرتكبها ,مما يسجل عجز جهات التحقيق عن مواجهة الإجرام المعلوماتي و التصدي لها, إما بسبب الطبيعة الخاصة للإجرام لمعلوماتي و الجهات المتضررة, أو معوقات خاصة بجهات التحقيق, و أخرى تشريعية وهو ما سنتناوله باختصار كما يلي:

[1] خالد عياد الحلبي, إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت, المرجع السابق , ص 183 .
[2] مصطفى محمد موسى , المرجع السابق , ص 269 .
[3] مصطفى محمد موسى , المرجع نفسه .ص 256 .

أولا: الصعوبات الخاصة بالجهات المتضررة: هناك عدة أسباب تساهم في إعاقة سلطات التحقيق في عمليات البحث و التحري عن الإجرام المعلوماتي, وتتمثل فيما يلي :

- غياب الدليل المادي في مسرح الجريمة و اختفاء أثار الجريمة و محوها بفضل مهارة المجرم المعلوماتي الذي هو في حالة تطوير لمعلوماته باستمرار [1] مستغلا تقنية تكنولوجيا المعلومات
- استخدام المجرم المعلوماتي لمختلف وسائل الحماية التقنية و تشفير مواقعهم لمنع الوصول إلى محتواها أو استنساخها: الأمر الذي يصعب الوصل للدليل المعلوماتي .
- ضخامة المعلومات و البيانات المتعين فحصها والتي يمكن إن تتعدى نطاق أو إقليم الدولة
- لجوء الجناة المعلوماتيين لمقاهي الانترنت لتفادي مسألة تعقبهم.
- أما بالنسبة للصعوبات المتعلقة بالجهات المتضررة , فتمثل في النقاط التالية:
- عدم إدراك مسؤولي المؤسسات لخطورة الجرائم المعلوماتية التي تهدد كيانها, كونها تستخدم النظام المعلوماتي لتقديم خدماتها لعملائها بشكل أسرع.[2]
- إحجام المتضررين من الجريمة المعلوماتية من أفراد و مؤسسات عن الإبلاغ عنها, إما لعدم علمهم بها أصلا, أو خوفا من الفضيحة, أو الظهور بمظهر مشين أمام الآخرين ,و يعطي انطباعا بقلة خبرة هذه المؤسسات و عدم اتخاذها إجراءات الحماية الأمنية لأنظمتها المعلوماتية, و تقرر تفضيل سمعة المؤسسة و مصداقيتها على الإبلاغ عنها [3].

ثانيا /صعوبات تتعلق بجهات التحقيق : هناك عدة عراقيل و صعوبات تواجه جهات التحقيق بمناسبة عملية البحث و التحري عن الجرائم المعلوماتية[4], نذكر منها ما يلي:

– قلة خبرة المحقق المعلوماتي بمتابعة و مواكبة تطورات المنظومة المعلوماتية , على خلاف المجرم المعلوماتي الذي يعمل باستمرار على مواكبة التطور التقني للمعلومات لاختفاء هويته و آثار جرائمه.

– قلة تدريبات أجهزة الأمن حول مستجدات الإجرام المعلوماتي ,تؤثر في قدرتها على مواجهة مختلف أشكال الإجرام المعلوماتي[1] , لاسيما و أنها تتطلب تكاليف باهضة .

[1] خالد ممدوح إبراهيم ,المرجع السابق , ص 65 .خالد ممدوح الحلبي , المرجع السابق , ص 222 .
[2] طارق عبد الله الشدي, آلية البناء لنظم المعلومات, دار الوطن للطباعة و النشر, الرياض 1423هـ, , ص 210
[3] خالد عياد الحلبي , المرجع السابق , ص 225 .
[4] خالد ممدوح الحلبي , المرجع السابق , ص 224 .

– عدم توفر الأجهزة و البرامج الحديثة للكشف عن الجرائم المعلوماتية و تتبع مرتكبيها.

– ضرورة اللجوء لوحدات تحقيق متخصصة للتحقيق في الجرائم المعلوماتية تضم محققين قضائيين و خبراء فنيين مختصين في مجال تقنية المعلومات, وعلى دراية بكل مستجداتها.[2]

ثالثا: الـــصعوبات الـــــتشريعية:

لقد أدى التطور العلمي في المجال المعلوماتي لظهور أنواع جديدة من الإجرام المعلوماتي و تطور أشكالها, و يقابله جمود النصوص التشريعية عن مواجهتها و حصر أنواعها و أركان كل نوع منها و وضع العقوبة المناسبة لها, الأمر الذي أثار عدة إشكالات قانونية , فمن جهة القاضي الجنائي مقيد عند نظره في الدعوى بمبدأ شرعية الجرائم و العقوبات(الشرعية الموضوعية) ,أي أنه لا يستطيع تجريم أفعال لم ينص عليها المشرع صراحة حتى ولو كانت هذه الأفعال ضارة أو خطيرة و على مستوى عال من الخطورة الإجرامية [3] , و كذا حصر القياس في النصوص الجزائية الموضوعية ,فهل يمكن قياس أنماط من الجرائم المرتكبة في المنظومة المعلوماتية على أنماط جرائم تقليدية؟ أم ينبغي رصد نصوص تشريعية خاصة بها نظرا لخصوصيتها؟

و ذهب جانب من الفقه إلى القول بعدم حصر الجرائم المعلوماتية خاصة و أنها تعرف تطور مذهل و مستمر بتطور تقنية المعلومات, و أدى ذلك لظهور فكرة تطويع النصوص التقليدية و تعديلها بشكل يلائم الطبيعة الخاصة للجرائم المعلوماتية.

و هو المنهج الذي اتبعه المشرع أين اكتفى بتجريم و حصر صور الجرائم الماسة بنظام المعالجة الآلية للمعطيات في قانون العقوبات, ثم تدارك هذا النقص ووسع من نطاقها في القانون: 04/09 لتشمل أي جريمة أخرى ترتكب بواسطة منظومة معلوماتية بالرغم أنها الأكثر انتشارا ,إلا أن المشرع لم يخصها بنصوص خاصة و يحدد الجزاء المناسب لها, الأمر الذي خلق عدة إشكالات قانونية و وضع القاضي الجزائي المقيدة بمبدأ الشرعي في موقف محرج منها.

[1] خالد عياد الحبلي, المرجع نفسه, ص 225 .خالد ممدوح الحلبي , المرجع السابق , ص 222 .
[2] حنان ريحان مبارك, المرجع السابق, ص 361 .
[3] خالد عياد الحلبي , المرجع السابق , ص 220 .

المطلب الثاني

قواعد الاختصاص القضائي في الجرائم المعلوماتية

الاختصاص القضائي هو السلطة السياسية للدولة التي تمكنها من تطبيق قوانينها الوطنية داخل إقليمها, و تعد الجرائم المعلوماتية من أكثر الجرائم التي تطرح مسألة الاختصاص القضائي, لأنها لا تعترف بالحدود نظرا لطبيعتها التقنية و ارتباطها بشبكات الاتصال العالمية , أين يمكن أن يصبح إقليم أكثر من دولة مسرحا لجريمة واحدة[1] ,الأمر الذي ينجم عنه تنازع في الاختصاص .

و عليه سنتناول في هذا المطلب للمعايير المعتمدة في تحديد القضاء المختص بالتبعية في الفرع الأول ,ثم نتطرق لتمديد الاختصاص الإقليمي للأقطاب الجزائية المتخصصة و جهات البحث و التحري في الفرع الثاني, أما في الفرع الثالث فننوه عن صعوبات التعاون الدولي في مكافحة الجرائم المعلوماتية العابرة للحدود.

الفرع الأول: مبادئ تحديد الاختصاص القضائي لمواجهة الجريمة المعلوماتية

قد يحصل أن ترتكب الجريمة المعلوماتية في إقليم دولة معنية من طرف أجنبي فتخضع الجريمة لاختصاص قضاء الدولة التي ارتكبت في إقليمها استنادا لمبدأ الإقليمية, و كذا اختصاص الدولة التي ينتمي إليها الجاني انطلاقا من مبدأ الشخصي, أما إذا ألحقت هذه الجريمة تهديدا بأمن و سلامة دولة أخرى فتدخل في اختصاص هذه الأخيرة استنادا لمبدأ العينية, الأمر الذي ينشأ عنه تنازع إيجابي في الاختصاص بين الدول.

أولا مبدأ الاختصاص الإقليمي:

تأخذ أغلب التشريعات الوضعية بهذا المبدأ الذي يعني خضوع الجرائم التي تقع على إقليم دولة معنية لقانونها الجنائي, و لا يمتد سريان قانونها الجنائي خارج الإقليم ,لاصطدامه بمبدأ سيادة الدول إلا في الأحوال الاستثنائية التي تقتضيها حماية المصالح الجوهرية للدولة أو متطلبات التعاون الدولي في مكافحة الإجرام.[2]

[1] عادل سقف الحيط, جرائم الذم و القدح و التحقير المرتكبة عبر الوسائط الإلكترونية, دار الثقافة للنشر و التوزيع, الطبعة الاولى, 2011 عمان, ص 349.
[2] عدنان الخطيب, موجز القانون الجزائي, الكاتب الأول, المبادئ العامة في قانون العقوبات, مطبعة الجامعة, دمشق,ص 1963, ص 79

و الأصل أن عناصر الركن المادي للجريمة من سلوك و نتيجة يكتمل في نطاق إقليم دولة واحدة كأن يقوم شخص بإرسال رسالة إلكترونية أو برنامج فيروس من جهاز يقع بدولة ما إلى أجهزة أخرى لعدة دول أخرى[1].

وأخذ المشرع الجزائري بهذا المبدأ في المادة: 3 من قانون العقوبات التي تنص على أنه: " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية".

كما تنص المادة: 586 ف.إ.ج على أنه : (تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانه المكونة لها قد تم في الجزائر).

إلا أن هذا المبدأ يجد صعوبة كبيرة في تطبيقه بالنسبة للجرائم المعلوماتية ,و هذا بالنظر لطبيعتها و خصائصها التي تميزها عن الجرائم التقليدية, لا سيما بخصوص تحديد مكان وقوعها بدقة, لأنه شرط أولى لعقد الاختصاص للقاضي الوطني ,وذهب الفقه لتغليب هذا المبدأ لضمان سرعة ملاحقة الجريمة و التحقيق فيها عن قرب .

ثانيا: مبدأ الاختصاص الشخصي:

و يعني تطبيق القانون الجزئي على مرتكب الجريمة الذي يحمل جنسية الدولة و لو ارتكب الجريمة خارج إقليمها, و قد أخذ به المشرع الجزائري في المادتين: 582 و 583 من قانون الإجراءات الجزائية[2], بخصوص الجنايات و الجنح المرتكبة من طرف جزائريين خارج إقليم الوطني فإن قانون العقوبات الجزائري يطبق عليها ,لكن بتوفر شروط محددة حصرا نذكر منها أن يكون الفعل المعاقب عليه في كلا البلدين, عودة المتهم إلى الجزائر و لم يصدر ضده حكم نهائي في الخارج ,فلا يجوز محاكمته مرتين على واقعة واحدة .[3]

غير أن الاختصاص لا ينعقد للمحاكم الوطنية بشكل تلقائي بخصوص الجرائم التي تقع في الخارج إلا بعد إعلام النيابة العامة بها و بتوفر الشروط القانونية, و يعتمد بصفة أساسية في الكشف عن هوية الجاني و من ثم التعرف على جنسيته, و هو أمر صعب نوعا ما لا سيما

[1] عبد الفتاح بيومي حجازي, المرجع السابق, ص 49
[2] سعيدي نعيم, المرجع السابق, ص 98.
[3] أحسن بو سقيعة ,الوجيز في القانون الجزائي العام, دار هوما, الجزائر, الطبعة الخامسة, 2007, ص 81

بخصوص الجرائم المعلوماتية أين يستعمل الجاني التشفير و الأسماء المستعارة و صعوبة اكتشافها فضلا عن كونها تحتاج لإجراءات طويلة و شاقة و معقدة و مكلفة.

ثالثا: مبدأ الاختصاص العيني : و يعني تطبيق القانون الجزائي الوطني على الجرائم التي ترتكب بالخارج بصرف النظر عن جنسية مرتكبها لمساسها بسيادة الدولة و مصالحها الأساسية [1], وهو ما أخذ به المشرع الجزائري من خلال المادة 588 من قانون الإجراءات الجزائية و نص المادة 15 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا ت الإعلام و الاتصال و مكافحتها, أين وسعت من اختصاص القضاء الجزائي الجزائري ليشمل الجرائم المرتكبة من أجنبي في الخارج و التي تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني, وذلك لسهولة ارتكابها باستخدام تكنولوجيا ت الإعلام و الاتصال و خطورتها[2], إلا أنه و نظرا لخصوصية الجريمة المعلوماتية لصعوبة اكتشافها ,و هوية الجاني المجهولة و تنوع الأنظمة القانونية في العالم و اختلافها يترتب عليه البطء و التعقيد و طول مدة الإجراءات.

رابعا: مبدأ الاختصاص العالمي : أين يطبق القانون الجزائي على كل جريمة يقبض على مرتكبها في إقليم الدولة أيا كان مكان ارتكابها و جنسية الفاعل أو الجاني [3], و يعطي هذا المبدأ للقانون الجزائي مجالا موسعا ليشمل العالم كله, فلا يتقيد بمكان ارتكاب الجريمة أو أحد سلوكياتها ولا بجنسية مرتكبيها ولا بطبيعة الجريمة و مساسها بالسيادة و المصالح الوطنية, و إنما يتطلب فقط القبض على الجاني في إقليم الدولة ليعطي للقانون الجزائي الوطني الاختصاص.

و هذا المبدأ يتلاءم كثيرا و طبيعة الجريمة المعلوماتية ,رغم ما يطرحه من تنازع حاد بين التشريعات الجزائية للدول, كونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة و تمتد عناصرها المادية و سلوكياتها الإجرامية بين أكثر من دولة و في فترات زمنية قصيرة جدا, و يبقى هذا المبدأ –أي العالمية– عاجزا عن معالجة جميع القضايا مالم يكن هناك تعاون دولي جاد و سريع, و كذا إعداد تشريعات وطنية لتجريم الظاهرة حتى يمكن معاقبة كل شخص يتم القبض عليه على إقليم الدولة دون مراعاة لجنسية أو مكان وقوع الفعل الإجرامي.

[1] أحسن بو سقيعة ,الوجيز في القانون الجزائي العام,المرجع السابق , ص 82 .
[2] احمد موسود مريم, آليات مكافحة جرائم تكنولوجيا لإعلام و الاتصال في ضوء القانون :04/09 , رسالة ماجستير , قاصدي مرباح ' جامعة ورقلة , 2013/2012 , ص 54 .
[3] علي عبد الله سليمان ,شرح العقوبات الجزائري , ديوان المطبوعات الجامعية , ص 115 .

و نرى بأن أغلب التشريعات الوطنية و منها المشرع الجزائري لم ينص على هذا المبدأ بالرغم من أهميته خصوصا في مجال مكافحة الجريمة المعلوماتية, رغم أن الاتفاقيات الدولية تعول عليه كثيرا في هذا المجال خاصة اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية و كذا القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة معلوماتية 2003 في المادة: 26 منه .

و عليه توصلنا إلى السريان المكاني للقانون الجنائي الوطني يتحدد وفقا لأحد المبادئ الأربعة: الإقليمية,العينية,الشخصية, العالمية, وأغلب التشريعات تأخذ بمبدأ الإقليمية كأصل عام ثم تكمله بالمبادئ الأخرى ,كونه المعيار الأكثر فعالية في ملاحقة الجريمة المعلوماتية و لسهولة إجراءات عمليات البحث و التحري و التحقيق فيها ,هذا بالإضافة لضرورة تفعيل المعايير الأخرى التي كانت تعد احتياطية كمعيار العينية و العالمية , وكذا تفعيل التعاون الدولي القانوني في مجال الاتفاقيات و القضائي في مجال تسليم المجرمين و تبادل المعلومات لتجاوز تحديات الإجرام المعلوماتي و تسهيل مهمة التحقيق فيه.

الفرع الثاني: تمديد الاختصاص الإقليمي لمواجهة الجريمة المعلوماتية

توجه المشرع الجزائري في إطار إصلاح العدالة و تطويرها إلى فكرة تطويق بعض الجرائم الخطيرة , كالجريمة المنظمة العابرة للحدود الوطنية و الجريمة المعلوماتية عن طريق القانون : 14/04 المؤرخ في : 2004/11/10 المتضمن تعديل الأمر : 155/66 المتعلق بقانون الإجراءات الجزائية , حيث عدل المواد : 37 ,40 ,329 منه بغرض توسيع الاختصاص المحلي لوكيل الجمهورية و قاضي التحقيق و المحكمة إلي دائرة اختصاص محاكم أخرى تحدد عن طريق التنظيم ,و هذا بمناسبة متابعة جرائم معينة بالتحديد .

وبصدور المرسوم التنفيذي رقم : 348/06 [1]المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق , تم بموجبه تحديد أربع محاكم على المستوى الوطني و توسيع اختصاصها المحلي ليشمل اختصاص محاكم أخرى موزعة على محاكم الوطن ويطلق عليها اسم الأقطاب الجزائية هي محكمة سيدي أمحمد, محكمة قسنطينة, محكمة وهران, محكمة ورقلة.

[1] المرسوم التنفيذي رقم :348/06 , المؤرخ في : 12رمضان 1427 ه الموافق ل: 2006/10/15 , المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق , ج ر , عدد : 63 .

و بمناسبة الحديث عن الأقطاب الجزائية المتخصصة فإنه ينبغي التطرق للاختصاص الإقليمي لوكيل الجمهورية و قاضي التحقيق و المحكمة و كذلك الضبطية القضائية .

كما يمتد الاختصاص المحلي للمحاكم الجزائرية إلى خارج حدود الإقليم طبقا لنص المادة 15: من القانون : 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجي ا الاتصال و الإعلام و مكافحتها , بخصوص الجرائم التي ترتكب من طرف أجنبي في الخارج و تستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني , وهذا الأمر يقتضي تعاون دولي في إطار المساعدة القضائية و في إطار الاتفاقيات الدولية و مبدأ المعاملة بالمثل [1].

أولا : الاختصاص الإقليمي الموسع لضباط الشرطة القضائية

في الأصل يتحدد الاختصاص الإقليمي للشرطة القضائية تحت سلطة وكيل الدولة في مرحلة جمع الاستدلالات بمكان ارتكاب الجريمة أو مكان إقامة المتهم أو مكان إلقاء القبض على المتهم .

غير أنه بناءا على المواد : 16 و 16 مكرر , 40مكرر1 , 40 مكرر2 ' و 40مكرر3 من قانون الإجراءات الجزائية فإنه يتوسع الاختصاص الإقليمي لضباط الشرطة القضائية وفقا لأحكام المرسوم التنفيذي رقم 06-348, و يمتد ليشمل كامل التراب الوطني ,إذا ما تعلق الأمر بالتحريات في جرائم محددة على سبيل الحصر في المادة 16 فقرة 7 وهي جرائم المخدرات و الجرائم المنظمة العابرة للحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف, أين يمتد اختصاصهم ليشمل كامل التراب الوطني.

في سنة 2014 و بموجب المرسوم الرئاسي رقم 14-183 [2]تم إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام و الأمن, أين تم تحديد مهامها بدقة وفق المواد 4و5و6و8 من المرسوم أعلاه, و تقوم بجمع الأدلة المادية و المعنوية بخصوص الجرائم التابعة لاختصاصها حسب المواد 5و6 من المرسوم, بما في ذلك الجرائم المتصلة بتكنولوجيا الإعلام و

[1] المادة : 15 من القانون :04/09 , المرجع السابق .
[2] المرسوم الرئاسي :183/14 , المؤرخ في : 2014/06/11 , المتضمن إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلية بدائرة الاستعلام و الأمن , ج ر , عدد : 32 , الصادر بتاريخ : 12 جوان 2014 .

الاتصال, كما تقوم بتنفيذ الإنابات و طلبات الجهات القضائية طبقا للقانون و تعالج ملفات التعاون القضائي المتبادل.

وهذا بالإضافة لضباط الشرطة لقضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ,يمارسون مهامهم على مستوى كامل التراب الوطني.

ثانيا: الأقطاب الجزائية المتخصصة

قام المشرع بتوسيع الاختصاص الإقليمي لبعض المحاكم في بعض الجرائم , في إطار إصلاح العدالة و تطويرها تماشيا مع التطورات التي عرفتها الجريمة و سرعة انتشارها و لاسيما بعد مصادقة الجزائر على جملة من الاتفاقيات الدولية ,ترتب عنها تعديل قانون العقوبات و قانون الإجراءات الجزائية و النصوص الخاصة المتعلقة بالفساد و تكنولوجيا الاتصال و الإعلام .

و في إطار الحديث عن الاختصاص الموسع للأقطاب الجزائية فانه ينبغي الطرق بالموازاة للاختصاص المحلي لوكيل الجمهورية و قاضي التحقيق و المحكمة الوارد ذكرها في المواد 37,40,329 من قانون الإجراءات الجزائية ,أين تم توسيع الاختصاص الإقليمي بخصوص الجرائم الستة المذكورة أعلاه [1],كما يلي:

1 – **تمديد اختصاص وكيل الجمهورية** : نصت المادة 37 الفقرة 2 من قانون الإجراءات الجزائية على انه:"يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات و الجرائم المنظمة العابرة للحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية و جرائم تبييض الأموال و الإرهاب و الصرف".

2 – تمديد اختصاص قاضي التحقيق: حيث أجازت المادة 40 فقرة 2 من قانون الإجراءات الجزائية تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الستة السالفة الذكر.

[1] محمد بكر أرشوش , الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري , جامعة محمد بن أحمد , وهران , ط 1 , دار صبحي للطباعة و النشر , الجزائر , 2014 , ص 28 .

3 – الاختصاص الموسع للأقطاب الجزائية : أين تناولت المادة 329 فقرة 5 من قانون الإجراءات الجزائية مسألة تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الستة السالفة الذكر بما فيها الجرائم المعلوماتية.[1]

و نشير إلى أن هذه النصوص عدلت بموجب القانون رقم: 04-14 المؤرخ في 10 نوفمبر 2004 المذكور أعلاه بإنشاء الأقطاب الجزائية المتخصصة, و التي تقوم على فكرة المحاكم الجزائية ذات الاختصاص الموسع, و أن المواد 37 و 40 و 329 أشارت إلى أن تمديد الاختصاص لكل من وكيل الجمهورية و قاضي التحقيق و المحكمة المختصة للجرائم الستة تعود للتنظيم بموجب المرسوم التنفيذي رقم 06-348 .

و عليه فإن توسيع الاختصاص الإقليمي للأقطاب الجزائية يترتب عنه بالتبعية توسيع اختصاص وكيل الجمهورية و قاضي التحقيق و قاضي الحكم العاملين بدائرتها و كذلك الأمر بالنسبة للضبطية القضائية كنتيجة حتمية للارتباط الوظيفي بينهم.

الفرع الثالث: الصعوبات التي تواجه تحديد الجهة القضائية المختصة على المستوى الدولي

رغم المناداة بضرورة التعاون الدولي في مجال مكافحة الجريمة المعلوماتية و الذي بات مطلب تسعى له أغلب الدول لا سيما بعد قصور المجهودات الفردين لكل دولة للتصدي لهذا النمط المستحدث من الجرائم العابرة للحدود و هو ما تناولناه سابقا, إلا أنه ثمة صعوبات و تجعل هذا التعاون ليس بالأمر الهين, و يرجع ذلك للأسباب التالية:

أولا: عدم وجود نموذج موحد للنشاط الإجرامي

لم تتفق الأنظمة القانونية في مختلف بلدان العالم على صورة موحدة و نموذج موحد بالاتفاق المشترك بين الدول حول الجريمة المعلوماتية, خاصة و أن ما يكون مجرم منها في بعض الأنظمة قد لا يكون كذلك في دولة أخرى [2]

[1] سعيداني نعيم , المرجع السابق , ص 92 .
[2] عبد الفتاح بيومي حجازي , المرجع السابق , ص 188 .

فعدم الاتفاق على صور الإجرام المعلوماتي جعل من البيئة الالكتروني ة فضاءا لقراصنة الحاسب الآلي لارتكاب جرائمهم العابرة للحدود.

ثانيا: اختلاف النظم القانونية الإجرائية

بسبب هذا الاختلاف قد تكون هنالك طرق للتحري و التحقيق و المحاكمة التي تثبت فعاليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى, أو لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الالكتروني, بالإضافة إلى أنه قد لا تسمح دولة ما باستخدام دليل إثبات تم جمعه بطرق ترى الدولة الأخرى أنها غير مشروعة أو أن فيها اعتداء على الحريات الخاصة.

ثالثا: الـــتجريم الـــــــــــــمزدوج

يعتبر التجريم المزدوج من أهم شروط تسليم المجرمين ,و قد يكون هذا الشرط عقبة أمام التعاون الدولي في مجال تسليم المجرمين بخصوص الجريمة المعلوماتية, لا سيما و أن معظم الدول مازالت نصوصها العقابية خالية من هذا النمط الإجرامي .

و في الحقيقة فان المصلحة المشتركة للدول تقتضي البحث عن الوسائل التي تساعد في التغلب عن هذه الصعوبات و إيجاد تعاون دولي حقيق يتفق مع طبيعة هذا النوع المستحدث من الجرائم للتحقق من خلو الفوارق بين الأنظمة القانونية العقابية الداخلية [1] .

[1] سعيداني نعيم , المرجع السابق , ص 95 .

خلاصة الفصل الأول :

ومن خلال ما سبق ذكره في هذا الفصل فإن الجريمة المعلوماتية هي من الجرائم المستحدثة التي تستهدف الاعتداء على نظام المعالجة الآلية للمعطيات أو تتخذها وسيلة لارتكابها في عالم افتراضي ,و تناولنا لأهم التعريفات التي تطرق لها الفقه الجنائي , و اقترحنا تعريف شامل يضم أكثر من معيار ,ثم تطرقنا لخصائص الجريمة المعلوماتية و التي تميزها عن الجرائم التقليدية , و أهمها أنها من الجرائم العابرة للحدود الوطنية, و ترتكب من قبل مجرم يتصف بالذكاء و المهارة , كما أنها تتسم بصعوبة إثباتها , و هي في تطور مستمر بتطور تقنية المعلومات ,و قسمها فقهاء القانون لجرائم واقعة على النظام المعلوماتي و جرائم ترتكب بواسطة النظام المعلوماتي .

كما تطرقنا لخصوصية التحقيق المعلوماتي من خلال التعرف على سمات المحقق و التحقيق المعلوماتي, و الصعوبات التي تعترضه .

ثم قمنا بتسليط الضوء على الجهود المحلية و الدولية المبذولة في إطار مكافحة الجريمة المعلوماتية مبرزين أهم الإشكالات و الصعوبات التي تطرحها ,لاسيما مشكلة الاختصاص للإجرام المعلوماتي العابر للحدود , و تعرفنا على المبادئ التي تحدد القانون الواجب التطبيق و تحدد الجهة القضائية المختصة في حالة التنازع الايجابي .

فمن غير المعقول إخضاعها لقوالب و معايير الاختصاص التي تحكم الجرائم التقليدية بخصوص مسألة تنازع الاختصاص , و ينبغي تبني حلول أكثر فعالية و مرونة , مما دفع بالحكومات لتبني التعاون الدولي القانوني في إطار الاتفاقيات الدولية و التعاون القضائي في إطار تسليم المجرمين و تبادل المعلومات و الإنابات القضائية , كمحاولة لتذليل الصعوبات التي تواجهها في سبيل مواجهة الإجرام المعلوماتي , لا سيما لاختلاف النظم القانونية و الإجرائية ,و التجريم المزدوج و عدم وجود نموذج موحد للإجرام المعلوماتي التي عرقلت مكافحتها .

الـــفصل الـــــثاني

الآليات الإجرائية للتحقيق في الجريمة المعلوماتية

لا تقتصر الصعوبات التي تثيرها الجريمة المعلوماتية في القانون الجنائي على الشق الموضوعي بل امتدت لتشمل نطاق القانون الجنائي الإجرائي, والتي وضعت في الأساس لمواجهة جرائم تقليدية بخصوص أساليب البحث و التحري و التحقيق فيها, و جمع الأدلة التي تخضع لتقدير القاضي وفقا لمبدأ الحرية في الاقتناع الشخصي بالدليل, في حين أن مسألة إثبات الجريمة المعلوماتية و التحقيق فيها عبر بيئة الكترونية افتراضية يطرح عدة إشكالات عملية ,نظرا لسرعة و دقة ارتكابها و سهولة محو آثارها, الأمر الذي يضع جهات التحري و التحقيق في مأزق عند مواجهة الإجرام المعلوماتي الغير مألوف بالنسبة لهم ,و خاصة إذا امتدت آثاره لخارج الحدود الإقليمية للدولة مصطدمة بالولاية القضائية و سيادة الدول.

كما أن الجريمة المعلوماتية وفي إطار مواجهتها ,فإنه ينبغي تضافر جهود الفنين و الخبراء في مجال تقنية المعلومات بوضع حواجز و أنظمة أمنية للحواسيب و شبكة الانترنت و البرامج المعلوماتية حتى لا تكون فريسة للاعتداءات, و بالموازاة فإنه ينبغي توجه التشريعات الجنائية لاستحداث إجراءات خاصة كفيلة بمواجهة الإجرام المعلوماتي المتجدد و المتطور يتوافق مع طبيعته الخاصة لوقوعه في بيئة افتراضية ولكون الأساليب التقليدية قاصرة عن مواجهتها.

وسنتناول في الفصل الثاني الآليات الإجرائية لمواجهة الجريمة المعلوماتية ,من خلال التطرق في المبحث الأول للقواعد الإجرائية لاستخلاص الدليل الرقمي , و نتناول فيه إجراءات التحقيق و التحري التقليدية من معاينة و تفتيش و ضبط معلوماتي في المطلب الأول , و إجراءات التحري و التحقيق المستحدثة و هي المراقبة الالكترونية عن طريق اعتراض المراسلات و التقاط الصور وتسجيل المكالمات, و التسرب و حفظ المعطيات خلال حركة السير في المطلب الثاني.

أما المبحث الثاني فنتناول فيه القيمة القانونية للدليل الرقمي في الإثبات الجنائي ,و هو مقسم بدورة لمطلبين, الأول يتضمن القيمة القانونية للدليل الرقمي من خلال التعرف على ماهيته

و مشروعيته و صعوبات استخلاصه ,أما المطلب الثاني يتضمن دور القاضي في تقييم الدليل الرقمي , و نتناول فيه حجية الدليل الرقمي و تقييمه من حيث سلامته الفنية و الإجرائية , و دور الخبرة الفنية في تقييم الدليل الرقمي .

المبحث الأول

القواعد الإجرائية لاستخلاص الدليل الرقمي

الجرائم المعلوماتية كغيرها من الجرائم الأخرى التقليدية تخضع لنفس إجراءات سير الدعوى الجنائية وآليات البحث و التحري و التحقيق, إلا أن أمر مواجهتها معقد نوعا ما نظرا للطبيعة الخاصة لهذا النوع من الجرائم ,الذي يعرف تطورا مستمرا متزامنا مع تطور تقنية المعلوماتية,الأمر الذي استدعى ضرورة تدخل المشرع لاستحداث آليات و أساليب خاصة تتناسب و طبيعة الجريمة المعلوماتية و فك رموزها و ترجمة نبضاتها و ذبذباتها الالكتروني ة لكلمات أو صور أو بيانات أو معلومات مادية تشكل لنا دليل إثباتها .

و بالإضافة لإجراءات التحقيق كسماع المتهم و الشهود و الاستجواب و المواجهة والتي لا تطرح أي إشكال أو صعوبات بشأنها, فإننا سنركز على إجراءات التحري و التحقيق التقليدية من معاينة الفضاء الرقمي و تفتيش المنظومة المعلوماتية و ضبط الأدلة الرقمية في المطلب الأول,

أما في المطلب الثاني سنتناول لإجراءات التحري و التحقيق المستحدثة و المتمثلة في : التسرب, اعتراض المراسلات و التقاط الصور و تسجيل المكالمات و حفظ المعطيات المتعلقة بحركة السير للكشف عن الجريمة المعلوماتية.

المطلب الأول

إجراءات التحري و التحقيق التقليدية في الجرائم المعلوماتية

إن الطبيعة الخاصة للدليل الرقمي أدت لتغيير كبير في المفاهيم السائدة حول إجراءات الحصول عليه, الأمر الذي يستدعي معه إعادة تقسيم الإجراءات الواردة في قانون الإجراءات الجزائية للبحث و التحري كالمعاينة و التفتيش و الضبط, و كيفية ملائمتها و تطويرها لكي تتناسب مع الطبيعة الخاصة للإجرام المعلوماتي, و سنتناول المعاينة في البيئة الرقمية في الفرع الأول , ثم التفتيش المعلوماتي في الفرع الثاني , و ضبط الأدلة الرقمية في الفرع الثالث .

الفرع الأول: المعاينة المعلوماتية

أولا / تعريف المعاينة : المعاينة هي ملاحظة و فحص حسي لمكان أو لشخص له علاقة بالجريمة لإثبات حالته و الكشف و التحفظ على ما قد يفيد من الأشياء في كشف الحقيقة.[1]

وهي إجراء ينتقل بمقتضاه المحقق إلى مكان وقوع الجريمة ليجمع الآثار المتعلقة بالجريمة و كيفية وقوعها[2]

ثانيا / أهمية المعاينة : مع التسليم بأهمية المعاينة في كشف غموض الكثير من الجرائم التقليدية ,أين يتم الحصول على آثار مادية من مسرح الجريمة ,و التحفظ عليها تمهيدا لفحص مدى صحتها كدليل للإثبات, إلا أن الأمر يختلف في مجال الجرائم المعلوماتية, و يرجع للأسباب التالية:

1. عدم ترتب آثار مادية على الجرائم المعلوماتية .
2. تردد عدد كبير من الأشخاص على مسرح الجريمة المعلوماتية ما بين فترة اقترافها و الكشف عنها, الأمر الذي يزيد من فرصة العبث بأثر الجريمة ,و من ثم التشكيك في صحته كدليل.
3. إمكانية التلاعب في البيانات عن بعد أو محوها من قبل الجاني[3].

[1] نبيلة هبة هروال, المرجع السابق, ص 213.
[2] خالد ممدوح إبراهيم, المرجع السابق, ص 149.
[33] نبيلة هبة هروال, المرجع السابق, ص 217.

ثالثا/ كيفية المعاينة المعلوماتية: تتم المعاينة في الجريمة المعلوماتية بالانتقال لمحل الواقعة الإجرامية في عالمها الافتراضي أو الالكتروني, من قبل ضابط الشرطة القضائية أو المحقق بصفة عامة من خلال الكمبيوتر أو جهاز الحاسوب الخاص به ,أو باللجوء لمقهى الانترنت أو إلى مقر عمل مزود بخدمة الانترنت ,أو من مقر مكتب الخبير الفني[1].

و العبرة بالانتقا ل للمعاينة في العالم الافتراضي أن يكون على وجه السرعة الكافية لمنع زوال آثار الجريمة, ومع مراعاة المحقق الجنائي للخطوات و الإجراءات التالية[2]:

1 تصوير شاشة الحاسوب Impréssion de capture décran ,إما بآلة تصوير أو برنامج"frozen" لتجميد مخرجات الشاشة ,أو حفظ الموقع باستخدام خاصية"save as" .
2 توفير معلومات مسبقة عن مكان الجريمة و نوع و عدد الأجهزة المتوقع مداهمتها و شبكاتها لإمكانية التعامل معها فنيا من حيث الضبط و التأمين و حفظ المعلومات[3].
3 الاستعانة بالأجهزة و البرامج الضرورية في الفحص و التشغيل.
4 تأمين التيار الكهربائي حتى لا يتم التلاعب أو التخريب عن طريق فصل التيار أو تعديل الطاقة الكهربائية من قبل المجرم المعلوماتي بغرض محو آثار الجريمة.
5 إعداد فريق محققين من المتخصصين في مجال الشرطة القضائية و الفنين في النظام المعلوماتي
6 عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل التأكد من خلو المحيط الخارجي للحاسب الآلي من أية محاولات مغناطيسية كفيلة بمحو الدليل أو البيانات المسجلة
7 التحفظ على محتويات سلة المهملات و القيام بفحص الأقراص الممغنطة و رفع البصمات إن وجدت , تحديد تاريخ ووقت الانتقال لإجراء المعاينة أو الآثار[4].
8 تحرير الأدلة الالكترونية المتحصلة من مسرح الجريمة المعلوماتية سواء كانت صفحات المواقع web pages أو البريد الكتروني email ,أو فيديو رقمي digital video, أو صوت

[1] خالد ممدوح إبراهيم, المرجع السابق, ص 156.
[2] نبيلة هبة هروال, المرجع السابق, ص 217 .
[3] نبيلة هبة هروال, المرجع نفسه ,ص 218 .
[4] خالد ممدوح إبراهيم , المرجع السابق , ص 176 .

رقمي digital audio, أو غرف المحادثات و الدردشة, أو صورة مرئية digital still images.[1]

الفرع الثاني: التفتيش المعلوماتي

أولا / تعريف التفتيش المعلوماتي : التفتيش هو إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق و كل ما يفيد في كشف الحقيقة, ويقصد به البحث في مستودع سر المتهم عن أشياء تفيد في كشف الحقيقة و نسبتها إليه.[2]

أما عن التفتيش في النظم المعلوماتية فلا يختلف عن مدلوله في فقه الإجراءات الجزائية السالف الذكر و يقصد به أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للمعطيات بما تشمله من مدخلا ت و تخزين و مخرجات للبيانات, و البحث من خلالها على الأفعال الغير مشروعة و نسبها لمرتكبيها. [3]

و يعد التفتيش عن أدلة الجريمة المعلوماتية من الأمور الصعبة , لقدرة الجاني في التخلص من البيانات محل التفتيش أو تزويدها برقم سري للمرور إليها, أو يستخدم أي تقنية أو برنامج للتشفير لا يعرفه إلا المتهم الأمر الذي يعيق مسألة رقابة و تفتيش البيانات المخزنة أو المنقولة. [4]

ثانيا / محل التفتيش المعلوماتي : التفتيش المعلوماتي قد يقع على المكونات المادية للنظام و تتكون من الحواسيب و الأجهزة الملحقة بها من كابلات و طابعات, أو يقع على المكونات المعنوية أو المنطقية للنظام المعلوماتي التي تشمل البرامج و التطبيقات و الشبكات المتصلة بالحاسب الآلي كجرائم الدخول الغير مشروع لنظم الغير.

فالجرائم التي ترتكب عل الكيانات المادية يسهل اكتشاف أمرها و ضبطها, في حين أن الجرائم المرتكبة على الكيانات المعنوية فإنه يصعب اكتشافها إذا ظلت على شكل نبضات أو ذبذبات الكترونية مالم يتم تحويلها لمستندات و معطيات أو بيانات. [5]

---

[1] علي حسن الطوالبة, التفتيش الجنائي على نظم الحاسوب و الانترنت, عالم الكتب الحديث, اربد الأردن, الطبعة الأولى , 2004, ص 11.
[2] عبد الاعله احمد الهلالي, تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي, (د.ط) , دار النهضة العربية, القاهرة, 1977, ص 73.
[3] خالد عياد الحلبي, المرجع السابق, ص 152.
[4] خالد ممدوح إبراهيم, المرجع السابق, ص 200.

لكن السؤال المطروح هو حول إمكانية إجبار المجرم المعلوماتي على تقديم السلطات المختصة بالتحقيق بمفاتيح المرور لتسهيل الولوج لنظامه المعلوماتي ؟ أم له التمسك بحق الصمت و عدم إجباره على الإدلاء بأقواله ضد نفسه ؟

و قد تضاربت آراء الفقهاء بين مؤيد و معارض و لكل مبرراته, إلا أن القاعدة أنه لا ينبغي إجبار المتهم على الإدلاء بأي تصريح, في حين يجوز إجبار غير المتهم على تقديم المعلومة التي تسهل الدخول للمنظومة المعلوماتية كمقدمي الخدمة مثلا, بتقديم كلمات المرور و تحديد مكان الوصول للاتصالات, وهو ما نصت عليه المواد: 10و11 من القانون04/09.[1]

ثالثا / شـــــروط التفتيش المعلوماتي:

لقد حرصت معظم التشريعات الإجرائية على إحاطة عملية التفتيش بجملة من الشروط ,و التي تعد كضمانات قانونية في سبيل الكشف عن الإجرام المعلوماتي و مرتكبيه, لما فيه من اعتداء على حقوق الأفراد و حرياتهم و حرمة مساكنهم و حياتهم الخاصة, منها الشكلية والموضوعية وهي:

1- **الضمانات الموضوعية للتفتيش المعلوماتي** : و تتمثل في الشروط الواجب توفرها في التفتيش حتى يكون صحيحا و تتمثل في سبب التفتيش و محله و السلطة المختصة به

أ/ **سبب التفتيش** : فلا يجوز لسلطات التحقيق إجراء التفتيش إلا لضبط جريمة واقعة بالفعل يتم بموجبها توجيه الاتهام للشخص المراد تفتيشه بناءا على أدلة أو قرائن قوية تفيد تورطه في الجريمة المعلوماتية, وإلا كان التفتيش باطلا لانتفاء السبب الذي يبرره .

وعليه يمكن القول بأن الإذن بالتفتيش لا يصح إصداره إلى لضبط جناية أو جنحة وقعت بالفعل[2] و ترجحت نسبتها لمتهم معني, و هناك من الدلائل ما يكفي للتصدي لحرمة مسكنة أو حرمته الشخصية حتى يكون التفتيش مشروعا.[3]

ب/ **مـــــحل التفتيش** : فيشترط لصحة و مشروعية التفتيش المعلوماتي إن ينصب على محل معلوماتي سواء تعلق بالمكونات المادية أو المعنوية للنظام المعلوماتي, و إذا تعلق الأمر بحاسب محمول أو هاتف نقال فإنه يجب مراعاة مكان تواجده[1].

[1] المواد : 10 -11 من القانون : 04/09 , المرجع السابق .
[2] نبيلة هبة هروال, المرجع السابق, ص 232.
[3] خالد ممدوح إبراهيم, المرجع السابق,ص 209 .

ويشترط أن يكون المحل الذي يقع عليه التفتيش معينا تعيينا نافيا للجهالة و مما يجوز تفتيشه, فلا يجوز تفتيش كل الحواسيب المتواجدة في شركة ما أو الحواسيب المحمولة أو الهواتف النقالة الخاصة بكل أفراد العائلة. و يستثنى تفتيش أعضاء السلك الدبلوماسي و أعضاء المجالس النيابية و مكاتب المحامين و سيارتهم و مساكنهم لتمتعهم بالحصانة و إلا كان التفتيش باطلا[2].

ج/ **السلطة المتخصصة بالتفتيش** : حتى يكون التفتيش المعلوماتي صحيحا و منتجا لآثاره, يجب أن يصدر إذن من سلطة التحقيق المختصة بتفتيش مسكن المتهم و الولوج لجهاز حاسوبه الآلي و البحث عن أدلة ارتكاب الجريمة المعلوماتية التي تتطلب جرأة و مهارة فنية معينة في المحقق حتى يتمكن من المحافظة على الأدلة من الإتلاف أو الشطب أو التعديل. [3] ويمكنه الاستعانة بخبراء فنيين بإذن من السلطات المختصة[4].

2/ الضمانات الشكلية للتفتيش المعلوماتي:

بالإضافة للضوابط الموضوعية لتفتيش النظم المعلوماتية فإنه يجب مراعاة ضوابط أخرى ذات طابع شكلي عند القيام بهذا الإجراء و ذلك صونا للحريات الفردية و هي:

أ/**احترام الميعاد الزمني للتفتيش** : لقد حضرت بعض التشريعات التفتيش ليلا و اعتبرته ضمانة للأفراد في مواجهة سلطة الدولة ,و اختلفت التشريعات في وقت تنفيذه ليلا و الاستثناءات التي يجوز فيها ذلك, بالرغم أن اغلب الجرائم المعلوماتية تتم ليلا لسهولة الدخول للمواقع المراد اختراقها بسبب قلة المستخدمين في هذا الوقت في المؤسسات و البنوك العامة و الخاصة.[5]

و بالرجوع لنص المادة: 47 من قانون الإجراءات الجزائية نجد أن المشرع قد وضع قيودا زمنية للتفتيش مابين الخامسة صباحا إلى الثامنة ليلا, و استثناءا أجاز الخروج عن هذا الميعاد إذا تعلق الأمر بالجرائم الواردة في نص المادة 47 /3 من قانون الإجراءات الجزائية , بما فيها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ,أين يجوز إجراء التفتيش و المعاينة في كل محل سكني أو

[1] خالد ممدوح إبراهيم, المرجع السابق , ص 194 .
[2] رشيدة بوبكر , المرجع السابق , ص 399 .
[3] خالد عياد الحلبي, المرجع السابق, ص 155
[4] علي حسن الطوالبة , المرجع السابق , ص 89 .
[5] خالد ممدوح إبراهيم , المرجع السابق , ص 220 . و علي حسن محمد طوالبة, المرجع نفسه,ص60.

غير سكني في كل ساعة من ساعات النهار أو الليل بناءا على إذن مسبق من وكيل الجمهورية المختص.

ويكون المشرع بذلك قد تفطن للطبيعة الخاصة للجرائم المعلوماتية و خصوصيتها في إمكانية محو الدليل الرقمي و تدميره, وأن ارتكابها يكون في أي وقت و أي تأخير في التفتيش قد يسبب عرقلة سير التحقيق و ضياع الدليل[1]

ب/ **إجراءات التفتيش بحضور المتهم أو من ينوب عنه**:

حرصت معظم التشريعات الإجرائية على عدم جواز إجراء التفتيش إلى بحضور المتهم أو من يمثله أو شاهدين من غير المعنييـن بالتحقيق, وهو ما نص عليه المشرع الجزائري في المادة 1/45 من قانون الإجراءات الجزائية , إلا انه استثنى بموجب الفقرة الأخيرة من نفس المادة حضور الأشخاص المحددين في الفقرة الأولى–وهم المتهم أو ممثله وفي حالة امتناعه أو هروبه حضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائي–في عدة جرائم من بينها جرائم المساس بنظم المعالجة الآلية للمعطيات نظرا لطبيعتها التقنية الخاصة التي تستدعي السرعة في استخلاص الدليل الرقمي قبل فقدانه[2]

ج/ **الإذن بالتفتيش** : لم ينص المشرع الجزائري في المادة : 5 من القانون : 04/09 السالف الذكر صراحة على وجوب استصدار الإذن بتفتيش النظم المعلوماتية من طرف ضباط الشرطة القضائية , كما هو الحال بالنسبة للمراقبة الالكترونية للاتصالات , لكن المادة : 05 تنص على أنه: " يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية .... " ,أي أن تفتيش النظم المعلوماتية يكون بناءا على القواعد العامة الواردة في قانون الإجراءات الجزائية , و التي تقتضي أن يأخذ ضباط الشرطة القضائية إذن مكتوب من أجل القيام بتفتيش المساكن [3].

كما نصت المادة : 05 السالفة الذكر على إمكانية الدخول بغرض التفتيش إلى المنظومة المعلوماتية و لو عن بعد ,إذا ما كانت المعطيات المراد تفتيشها مخزنة في منظومة معلوماتية أخرى

[1] رشيد بوبكر, المرجع السابق,ص 416.
[2] رشيد ابو بكر, المرجع نفسه, ص 415, علي حسن محمد الطوالبة, المرجع السابق ص 48 .
[3] خالد ممدوح إبراهيم .المرجع السابق , ص 220 .

و لا يمكن الدخول إليها إلا من المنظومة الأولى, فإنه يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة .

د / إعداد محضر التفتيش المعلوماتي:

لا يختلف محضر التفتيش في الجرائم المعلوماتية عن غيره في الجرائم التقليدية, إذ يجب تحرير محضر من قبل محقق معلوماتي مختص مستعينا بأهل الخبرة ليساعده في تحرير هذا المحضر ليغطي كل الجوانب الفنية للتفتيش, و أن يكون موقعا و يتضمن كافة الإجراءات المتبعة.[1]

الفرع الثالث : ضبط الأدلة الرقمية

أولا / تعريف الضبط : أو حجز المعطيات : إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة المتحصل عليها أثناء تفتيش المنظومة المعلوماتية, و الضبط يعني: وضع اليد على أي شيء يتصل بالجريمة المعلوماتية للكشف عن مرتكبيها.[2]

أما الضبط المعلوماتي فهو ينطبق على المكونات المادية و المعنوية للنظام المعلوماتي ,كما أنه تعتريه عدة صعوبة بسبب ضخامة البيانات الواجب فحصها من المحقق المعلوماتي و قدرة المجرم المعلوماتي على إخفاء أو محو آثار جريمته ,و في المقابل عجز السلطات التحقيق عن كسر كلمات السر أو شفرات المرور.

ثانيا /إجراءات الضبط المعلوماتي: و تتمثل إجراءات الضبط فيما يلي :

- الحصول على إذن من السلطات المختصة تجيز تفتيش المنظومة المعلوماتية, و أن يتضمن الإذن لتحديد النظام محل كل التفتيش بدقة و عنوان المتهم و اسمه, و الجهاز الذي يقوم بالدخول لنظام الحاسوب و ضبط ما يحتويه من معطيات و بيانات
- قدرة المحقق المعلوماتي على التعامل مع الدليل بطريقة فنية و المحافظة عليها دون إتلافها أو محوها و كذا إتباع القواعد الفنية لتحرير الدليل الرقمي المضبوط.

[1] خالد ممدوح إبراهيم, المرجع السابق, ص 224.
[2] خالد عياد الحلي ,المرجع السابق, ص 168.

- أخذ نسخة احتياطية عن الجهاز وعن وسائط تخزين المعلومات , لضمان عدم المساس بالدليل الأصلي الذي يترك للخبراء لفحصه .
- تخزين الدليل في أماكن غير معرضة لمجالات كهرومغناطيسية أو الكهرباء الساكنة أو الغبار و درجة الحرارة تتراوح بين : 4 و 32 درجة مئوية ,و قد تصل مدة تخزين الأقراص و الأشرطة لثلاث سنوات[1].

وتجدر الإشارة أن المشرع الجزائري قد نص في المادة: 06 من القانون : 09/ 04 السالف الذكر على أنه : "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها ,و أنه ليس من الضروري حجز كل منظومة, يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في قانونا لإجراءات الجزائية ".[2]

المطلب الثاني

إجراءات التحري و التحقيق المستحدثة لجرائم المعلوماتية

لقد أحدثت الجريمة المعلوماتية نظرا لطبيعتها الخاصة كونها جريمة تقنية و غير مادية أمام القائمين بعمليات البحث و التحري و التحقيق عدة عقبات جعلتهم في وضع محرج بسبب عدم كفاية إجراءات التحري و التحقيق التقليدية كالتفتيش و الضبط لاستخلاص الدليل الإلكتروني, الأمر الذي استدعى لضرورة استحداث الدول لإجراءات خاصة للتحري فيها تتماشى و الطبيعة الخاصة للإجرام المعلوماتي, و هو ما فعله المشرع الجزائري باستحداث إجرائي التسرب و اعتراض المراسلات السلكية و اللاسلكية و الواردة في قانون الإجراءات الجزائية, و كذا استحداث إجرائي ن آخرين هما: المراقبة الالكترونية و حفظ المعطيات الواردة في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال , هذا بالإضافة لإجراء التفتيش عن بعد الذي سبق التطرق له .

[1] نبيلة هبة هروال, المرجع السابق, ص 273.
[2] رشيدة بوبكر, المرجع السابق, ص 419

الفرع الأول: التسرب المعلوماتي : لقد استحدث المشرع الجزائري لهذا الإجراء كوسيلة للبحث و التحري في بعض الجرائم المحددة على سبيل الحصر في نص المادة: 65 مكرر(ق.إ.ج) ,و من بينها الجرائم الماسة بنظام المعالجة الآلية للمعطيات و يطلق عليه مصطلح الاختراق في القانون: 01/06 المتعلق بالوقاية من الفساد و مكافحته في نص المادة: 65 منه [1] .

أولا: تعريف التسرب : عرفته المادة: 65 مكرر 12 من قانون الإجراءات الجزائية بأنه:" قيام ضابط أو عون شرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك"[2]

و أحاط المشرع الجزائري العنصر المتسرب بعدة ضمانات لحمايته و حماية أسرته, و أعفاه من المسؤولية الجزائية عن الأفعال غير المشروعة أو الجرائم التي يرتكبها في سبيل التسرب في الخلية الإجرامية. كما أنه لا يتصور اللجوء لعملية التسرب إلى في بعض الجرائم البالغة الخطورة التي حددها المشرع الجزائري على سبيل الحصر و من بينها الجرائم المعلوماتية.

أين يتم ولوج ضابط أو عون شرطة قضائية للعالم الافتراضي و مشاركته في محادثات غرف الدردشة أو حلقات النقاش في كيفية الاختراق و بث الفيروسات مستخدما هوية مستعارة [3], و يمنع بأي حال من الأحوال الكشف عن هويته تحت طائلة العقوبات.[4]

ثانيا : ضوابط التسرب المعلوماتي : باعتبار التسرب ممارسة غير مألوفة لضابط أو عون الشرطة القضائية ,بل تعد من أخطر الإجراءات انتهاكا للحياة الخاصة للمتهم, لذلك أحاطه المشرع بجملة من الضمانات الشكلية و الموضوعية, نوجزها كما يلي:

1-**الشروط أو الضوابط الشكلية** و تتمثل في:

أ/ **صدوره بإذن قضائي :** من قبل وكيل الجمهورية أو قاضي التحقيق, و هذا حسب نص المادة: 65 مكرر 11 من قانون الإجراءات الجزائية ,و ذلك لحماية الحقوق الأساسية المكرسة دستوريا

[1] القانون 01/06 , المؤرخ في 2006/02/20 , المتعلق بالوقاية من الفساد و مكافحته , ج ر , عدد : 14 ,الصادر بتاريخ : 2006/03/08 .
[2] المادة : 35 من القانون رقم 01/06 المؤرخ في: 2006/2/20 المتعلق بالوقاية من الفساد و مكافحته, ج ر,عدد 14. الصادرة بتاريخ: 2006/03/08
[3] رشيدة بوبكر, المرجع السابق,ص 434.
[4] المادة 65 مكرر 16 من (ق.إ.ج), المرجع السابق.

ب / **أن يكون مكتوبا:** وهو ما نصت عليه المادة: 65 مكرر 15 من قانون الإجراءات الجزائية التي اشترطت أن يكون الإذن المسلم مكتوبا تحت طائلة البطلان, و أن يتضمن جملة من البيانات كذكر نوع الجريمة محل عمليات التسرب ,واسم ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته و تحديد مدة عملية التسرب التي لا تتجاوز أربعة أشهر مع إمكانية تجديدها حسب متطلبات التحقيق و التحري, و ضرورة إبقاء الإذن بالتسرب خارج ملف الإجراءات لغاية انتهاء المهلة حفاظا على السرية المطلوبة[1].

2/ **الشروط و الضوابط الموضوعية للتسرب:** و تتمثل في ضابطين أو شرطيين هما:

أ/ **السبب** : و تطرقت له المادة 65 مكرر 15 قانون الإجراءات الجزائية , و تعني الدوافع و المبررات التي أقنعت الجهات القضائية المتخصصة بمنح الإذن بالتسرب .

ب / **نوع الجريمة :** فإن عملية التسرب كإجراء خاص للبحث و التحري و التحقيق لا ينصرف إلا في الجرائم الستة المحددة على سبيل الحصر و هي جرائم المخدرات,و الجريمة المنظمة العابرة للحدود الوطنية, الجرائم الماسة بنظم المعالجة الآلية للمعطيات, جرائم تبييض الأموال, جرائم الإرهاب, الجرائم المتعلقة بالتشريع الخاص بالصرف , و في جرائم الفساد يطلق عليه مصطلح الاختراق .

و يرجع ذلك كونها من الجرائم الخطيرة جدا لسرعة انتشارها و امتدادها حتى خارج الحدود الإقليمية للوطن, كما أنها تتم أو ترتكب من مجرمين خطيرين يتسمون بالذكاء, وقدرتهم على إخفاء آثار جرائمهم, الأمر الذي يبرر اللجوء لهذا الإجراء للكشف عن هذه الجرائم و مرتكبيها.[2]

الفرع الثاني : اعتراض المراسلات و تسجيل الأصوات و التقاط الصور:

استحدث المشرع الجزائري لهذا الإجراء في الفصل الرابع من قانون الإجراءات الجزائية رقم: 22-06 المعدل و المتمم تحت عنوان "اعتراض المراسلات و تسجيل الأصوات و التقاط

[1] رشيدة بوبكر, المرجع السابق, ص 436.

[22] سعيدي نعيم, المرجع السابق, ص87, و: زورو هدى, التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري, مجلة دفاتر السياسة و القانون العدد 21, كلية الحقوق و العلوم السياسية, جامعة محمد خيضر بسكرة, 2014, ص 121.

الصور", و حدد ضمانات استخدامها نظرا لقدرة هذا الإجراء على تعقب الدليل الالكتروني و الكشف عن الجرائم ضمانات استخدامها, نظرا لقدرة هذا الإجراء على تعقب الدليل الالكترونـي و الكشف عن الجرائم .

وتجد الإشارات إلى أن المشرع استحدث نفس الإجراء في القانون : 04/09 السالف الذكر تحت مسمى المراقبة الالكترونية للاتصالات كأحد إجراءات التحري و التحقيق, و أعطى تصريحا للجهات القضائية باستعمال هذا الإجراء التقني في إطار الوقاية من الجرائم التي تشكل خطرا على أمن الدولة والجرائم الإرهابية أو التخريبية , وكذا جرائم الاعتدا ء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة[1]

أولا: مفهوم اعتراض المراسلات السلكية ولا سلكية:

عرفت لجنة الخبراء للبرلمان الأوروبي ستراسبورغ بتاريخ: 2006/10/06 اعتراض المراسلات في إطار دراسة أساليب التحري التقنية, بأنه "عملية مراقبة سرية للمراسلات السلكية و ذلك عن إطار البحث و التحري عن الجريمة و جمع الأدلة حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجرائم.[2]

واقتبس المشرع الجزائري نفس التعريف في نص المادة: 65 مكررة من قانون الإجراءات الجزائية ,و عرف عملية مراقبة المراسلات بأنها:" اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية, وهذه المراسلات عبارة عن بيانات قابلة للتوزيع, و التخزين, الاستقبال [3].

ولكن المشرع لم يحدد طبيعة هذه المراسلات في القانون هل هي كتابة, رمو ز ,صور , غير انه في نص المادة 2 فقرة و من القانون: 04/09 عرف الاتصالات الالكترونية أنها: " أي تراسل أو إرسال أو استقبال مكالمات أو إشارا ت أو كتابات أو صور أو أصوات أو معلوماتي مختلفة بواسطة انه وسيلة الكترونية".

أما عن تسجيل الأصوات و التقاط الصور فقد عرفها المشرع ضمنيا في المادة:

[1] المادة : 4 من القانون. 09-04, المرجع السابق .
[2] بوبكر رشيدة, المرجع السابق.ص
[3] مهدي شمس الدين . النظام القانوني للتسرب في القانون الجزائري , مذكرة لنيل شهادة ماجستير , جامعة محمد خيضر , بسكرة , كلية الحقوق , 2014 , ص 27 .

65 مكرر 5 من قانون الإجراءات الجزائية بأنها: "وضع و استعمال الوسائل و الترتيبات التقنية دون موافقة المعنيين من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية, من طرف شخص أو عدة أشخاص يتواجدون في أماكن عامة أو خاصة."[1]

و هناك جانب من الفقه اتجه لانتقاد هذا الإجراء لأنه يعد مساس بحرمة الحياة الخاصة و الحريات الفردية, المنصوص عنها في المادة 39 من الدستور الجزائري والتي تنص على انه:"لا يجوز انتهاك حرمة حياة المواطن الخاصة و حرمة شرفه يحميها القانون, سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة " ,وكذا نصت المادة: 303 من قانون العقوبات التي تعاقب على إفشاء السر المهني عند القيام بهذا الإجراء من الجهات المعنية , في حين توجه جانب آخر من الفقه لضرورة الاستعانة بهذا الإجراء للكشف عن بعض الجرائم الخطيرة و المستعصية كالجرائم المعلوماتية وفق ضوابط و شروط معينة. [2]

ثانيا: الضمانات المقررة لاعتراض المراسلات السلكية و اللاسلكية:

كقاعدة أصلية فإنه لا يجوز اعتراض المراسلات و تسجيل المكالمات و التقاط الصور دون علم الشخص ورضاه, إلا أنه استثناء يسمح المشرع الجزائري بها في سبيل تحقيق مصلحة عليا ألا و هي الكشف عن الجرائم و حماية مصلحة المجتمع ,و اعتبرها الأولى بالحماية من الحفاظ على أسرار الحياة الخاصة ,أين أتاح للضبطية القضائية استعمال هذه الوسائل التقنية في إطار البحث و التحري عن الجرائم المستحدثة و[3] لكنه في المقابل أحاطها بعدة ضمانات نذكرها اختصار:

1- **استخدام الأساليب التقنية في الجرائم الخاصة** فقط و المحددة حصرا في المادة 65 مكرر5 من قانون الإجراءات الجزائية , دون الجرائم الأخرى باستخدام وسائل تقنية دون علم المشتبه بهم .

[1] مهدي شمس الدين, النظام القانوني للتسرب في القانون لجزائري, المرجع السابق ر, ص: 27.
[2] قادري سارة , أساليب التحري الخاصة في قانون الإجراءات الجزائية – مذكرة ماجستير, جامعة قاصدي مرباح ورقلة, كلية الحقوق و العلوم السياسية, تمم الحقوق, ص 27.
[3] علي حسن محمد طوالبة , المرجع السابق ,ص 229 .

2-**ضرورة الحصول على الإذن من السلطات المختصة** (وكيل جمهورية أو قاضي التحقيق)

قبل عملية اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور, وأن يكون هذا الإذن مكتوب مسبب و يتضمن نوع الجريمة و ينطبق على أحد الصور الواردة بنص المادة: 65 مكرر 5 من قانون الإجراءات الجزائية , و طبيعة المراسلة أو الاتصال, و مدته التي لا تتجاوز 4 أشهر وهي قابلة للتجديد و هذا طبقا لنص المادة : 65 مكررة فقرة 2 التي تنص على أنه : " يسلم الإذن مكتوبا بمدة أقصاها أربعة أشهر قابلة للتجديد..."، و كذا تحديد الإطار المكاني لأساليب التقنية و تتمثل إما في الأماكن العمومية أو الخاصة, أو حتى المحلات السكنية[1].

3-**الحفاظ على السر المهني** : فعلى القائم بهذا الإجراء من ضباط الشرطة القضائية مراعاة احترام السر المهني و عدم المساس به, إذا كان في الأماكن الخاصة كمكاتب المحامين و الموثقين وهذا حسب نص المادة: 65 مكرر 6 من قانون الإجراءات الجزائية .

4-**تحرير محضر** : عن كل عملية اعتراض المراسلات أو تسجيل المكالمات أو التقاط الصور من قبل ضابط الشرطة القضائية, و يذكر جميع الترتيبات و نتائج التحريات.[2]

و تجدر الإشارة إلى أن المشرع لم يشر صراحة لكيفية وضع الأدلة المستخلصة من اعتراض أو مراقبة الاتصالات في أحراز مختومة باعتبارها من أدلة الإثبات الرقمية المضبوطة, لضمان عدم إتلافها أو العبث بها وضمها لملف الإجراءات مع المحاضر الأخرى للتحري و التحقيق و إخضاعها للمادة: 84 من قانون الإجراءات الجزائية التي تنص على: "..... ويجب على الفور إحصاء الأشياء و الوثائق المضبوطة ووضعها في أحراز مختومة ....".

4 **الاستعانة بذوي الخبرة الفنية** و التقنية في مجال تكنولوجيا الإعلام و الاتصال, لإنجاح أيه عملية مراقبة إلكترونية حسب نص المادة : 05 من القانون :04/09 السالف الذكر .

[1] رشيدة بوبكر, المرجع السابق, ص 443 .
[2] نور الهدى السوفي , المرجع السابق, ص 45.

الفرع الثالث: حفظ المعطيات المتعلقة بحركة السير

نظرا لصعوبة استخلاص الدليل الإلكتروني بالوسائل و الأساليب السالفة الذكر للتحري و التحقيق , و نظرا لسهولة إزالته من المنظومة المعلوماتية من قبل المجرم المعلوماتي, فإن السبيل الوحيد للحصول عليه هو اللجوء إلى أرشفة المراسلات الالكترونية لاستغلالها عند الحاجة, وذلك عن طريق إلزام مزودي الخدمات بحفظ المعطيات.

و هو ما توجهت له الجمعية العامة للأمم المتحدة في قرارها تحت رقم : 63/55 المؤرخ في 22 يناير 2001 المتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات, أين ألزم في المادة: 1 فقرة "و" منه الدول بالسماح لحفظ المعطيات الإلكترونية للاستعانة بها في التحقيقات, كما تناوله المشرع الجزائري في نص المادة: 11 من القانون: (04/09) تحت عنوان : "حفظ المعطيات المتعلقة بحركة السير" كالتزام يقع على عاتق مقدمي الخدمات و تقديمها للسلطات المكلفة بالبحث و التحري.

أولا: المقصود بمزودي الخدمات : عرف المشرع الجزائري مزود أو مقدم الخدمة بموجب الفقرة (د) من المادة: 2 من القانون رقم (04/09) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها بأنه : " 1- أي كيان عام أو خاص يقدم لمستعملي خدماته : القدرة على الاتصال بواسطة منظومة معلوماتية و / أو نظام للاتصالات . 2- و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها"

ونذكر على سبيل المثال للتوضيح, المراسلة عبر البريد الالكترون ي و التي يتم استقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه والتي لم يطلع عليها ف إنها تبقى في حالة تخزين إلكتروني و حفظ نسخة منها كإجراء مؤقت لحين استقبالها من المرسل إليه من قبل مزود الخدمة الاتصالات والذي يقوم بحذفها بمجرد استقبالها أو تخزينها أو الاحتفاظ بنسخة منها.[1]

[1] رشيدة بوبكر, المرجع السابق, ص477.

وهنا تظهر أهمية قيام مزود خدمات الخدمة يحفظ المعطيات و أرشفة المعطيات بتخزينها بالشكل الذي يضمن سلامتها و سريتها و ضمان أمن المعطيات من التغيير أو الحذف.

ثانيا : مفهوم حفظ المعطيات المتعلقة بحركة السير

عرفت المادة 2 في الفقرة هـ من القانون 04/09 السالف الذكر المعطيات المتعلقة بحركة السير بأنه: "أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات توضح مصدر اتصال و الوجهة المرسلة إليها و الطريق الذي يسلكه ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة" .

و يتضح من خلال استقراء المادة 2 المذكورة أعلاه أن المقصود بحفظ المعطيات هو قيام مزودي الخدمات بحفظ و أرشفة معطيات المرور أو حركة السير التي توضح مصدر الاتصال و الطريق الذي يسلكه و مدة الاتصال و نوع الخدمة, لتحديد هوية جهاز الاتصال رقم الهاتف أو عنوان بروتوكول الانترنت و التعرف على هوية الشخص الذي أرسل الفيروسات .

ثالثا: التزامات مزودي أو مقدمي الخدمات

لقد ألزم المشرع الجزائري في القانون (04/09) مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية بجمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها و حفظها ووضعها تحت تصرف سلطات البحث و التحقيق.

كما ألزمه بكتمان سرية العمليات التي يجريها مزود الخدمات بطلب من المحققين و كذا المعلومات المتصلة بها و ذلك تحت طائلة العقوبات المقررة لإنشاء أسرار التحري و التحقيق [1],وحدد المشرع المعطيات التي يقوم مقدم الخدمات بحفظها مع مراعاة طبيعية و نوعية الخدمات و هي:

– المعطيات التي تسمح بالتعرف على مستعملي الخدمة .

–المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال .

[1] المواد : 8 و 10 من القانون 04/09, المرجع السابق

-الخصائص التقنية و كذا تاريخ و وقت و مدة كل اتصال .

-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها .

- المعطيات التي تسمح بالتعرف على المرسل إليه, و كذا عناوين المواقع المطلع عليها .

-بالنسبة لنشاطات الهاتف, يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة 1 و تلك التي تسمح بالتعرف على مصدر الاتصال و تحديد مكانه[1]

و بما أن حفظ المعطيات هو إجراء وقتي فإن مقدمي الخدمات ملزمون بحفظ المعطيات و تخزينها لمدة سنة من تاريخ تسجيلها و هذا حسب مقتضيات المادة 11 من نفس القانون بقولها:" ... تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة من تاريخ التسجيل"

هذا بالإضافة إلى التزامين خاصين بمقدمي خدمة الانترنت حسب نص المادة 12 من نفس القانون و هما:

1- التدخل الفوري بحسب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن

2-وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي على معلوماتي مخالفة للنظام العام أو الآداب العامة و إخبار المشتركين لديهم بوجودها[2].

و في حالة عدم قيام مقدم أو مزود الخدمات بحفظ المعطيات التقنية المفروضة عليه تخزينها و المتعلقة بهوية المتصلين و ساعة الاتصال فإنه تقوم مسؤوليته الجزائية و تتم طباعته لأنه بذلك يعرقل السير العادي للعدالة و التحقيق دون الإخلال بالعقوبات الإدارية[3] .

[1] المادة : 11 من القانون 04/09, المرجع السابق .
[2] المادة :12: من القانون : 04/09 , المرجع نفسه .
[3] المادة 11 / أخيرة , من لقانون : 04/09 , المرجع نفسه .

المبحث الثاني

القيمة الثبوتية للدليل الرقمي أمام القاضي الجزائي

إن عملية استخلاص الدليل الرقمي من المسائل الشائكة التي تثير مشاكل قانونية و فنية في مجال التحقيق و الإثبات الجنائي للجريمة المعلوماتية , خوفا من عدم تعبيره عن الحقيقة بسبب تعرضه للتزييف ,الأمر الذي يثير مسألة مشروعية الدليل الرقمي ومدى حجيته و دور القاضي الجنائي في تقييمه لا سيما بسبب الصعوبات التي تصاحبه خلال عملية استخلاصه ,هذا بالإضافة إلى التطور الملحوظ في استعمال التقنية الذي يمكن من أن يساهم تزييف الدليل الرقمي على غير حقيقته .

و عليه سنتناول في هذا المبحث للقيمة القانونية للدليل الرقمي في الإثبات الجزائي في المطلب الأول , أين سنتعرض لماهية الدليل الرقمي و مشروعيته و صعوبات استخلاصه , أما في المطلب الثاني سنتطرق لدور القاضي في تقييم الدليل من خلال معالجة مدى حجيته في الإثبات الجزائي , و كيفية تقييمه من حيث سلامته الفنية و الإجرائية ,و التطرق لدور الخبرة الفنية في عملية الإثبات .

المطلب الأول

القيمة القانونية للدليل الرقمي في الإثبات الجنائي

أدى التطور في استخدام تكنولوجيا الاتصال و الإعلام إلى تطور وسائل ارتكاب الجرائم المعلوماتية بمختلف أشكالها, الأمر الذي أدى بالتبعية إلى ضرورة الاعتراف بوسائل الإثبات بصورتها الجديدة لا سيما الرقمية منها .

وسنتطرق في هذا المطلب إلى ماهية الدليل الجنائي الرقمي من خلال التعرف على مفهومه و خصائصه و مصادر استخلاصه في الفرع الأول , أما الفرع الثاني نتناول مشروعيته , و في الفرع الثالث : صعوبات استخلاص الدليل الرقمي .

الفرع الأول: ماهية الدليل الجنائي الرقمي

لمعرفة ماهية الدليل الرقمي علينا أن نوضح تعريفه و خصائصه و كيفية استخلاصه .

أولا / تعريف الدليل الرقمي:

هو الدليل المأخوذ من الأجهزة و الحواسيب و شبكة الانترنت فيكون في شكل نبضات أو ذبذبات مغناطيسية أو كهربائية يمكن تجميعها و تحليلها باستخدام برامج و تطبيقات و يتم تقديمها بشكل مادي للقضاء [1], و ما يلاحظ من هذا التعريف أنه يقتصر على الأدلة الرقمية المستمدة من الحواسيب فقط في حين انه يمكن استخلاصه من شبكة الانترنت و الأجهزة الملحقة بالحاسوب .

و هناك من عرفه بأنه مكون رقمي لتقديم معلومات على شكل نصوص مكتوبة أو صور أو أصوات أو رسوم من أجل الربط بين المجرم و الجريمة [2],أو هو الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الالكترونيةة من معطيات الحاسوب و شبكات الانترنت و الأجهزة الالكتروني ة الملحقة و المتصلة به و شبكات الاتصال من خلال إجراءات قانونية لتقديمها للقضاء كدليل الكتروني جنائي يصلح لإثبات الجريمة[3],و يمكن استخدامه في جميع مراحل التحقيق و المحاكمة .

ثانيا/ خصائص الدليل الرقمي : يختلف الدليل الرقمي عن باقي الأدلة الجنائية الأخرى لأنه نشأ في بيئة افتراضية (إلكترونية) ,الأمر الذي انعكس على طبيعته و هو يتميز بالخصائص التالية:

1-**دليل علمي** :يتطلب استخلاص الدليل الجنائي الرقمي طرق غير تقليدية, أي أنه لا يمكن الحصول عليه إلا باستخدام أساليب علمية و فنية و هذا راجع للبيئة التي تكون فيها هذا الدليل .

2-**دليل ذو طبيعة تقنية** : التقنية تعني المعدات و الأجهزة و المعدات الفنية التي يمكن توظيفها في تأدية مهمة ما [4], و يقصد بها الأجهزة الخاصة التي تتيح استخلاص الدليل الرقمي من مجالات

---

[1] محمد الأمين البشري, التحقيق في الجرائم المستحدثة, ط1, منشورات جامعة نايف العربية للعلوم الأمنية, الرياض 2014, ص 234.

[2] ممدوح عبد الحميد عبد المطلب, البحث و التحقيق الجنائي الرقمي في جرائم الحاسب الآلي و الانترنت, دار الكتب القانونية, المجلة الكبيرة , مصر 2006 ص 88.

[3] خالد عياد الحلبي, المرجع السابق . ص 230.

[4] فيصل مساعد العنزي, اثر الإثبات بوسائل التقنية الحديثة على حقوق الإنسان, رسالة ماجستير, قسم العدالة الجنائية, جامعة نايف العربية للعلوم الأمنية, الرياض 2007 ص 10 .

مغناطيسية أو كهربائية, الأمر الذي يميزه عن باقي الأدلة الأخرى, أين يمكن استخراج نسخ من الدليل الجنائي الرقمي مطابقة للأصل و لها نفس القيمة العليمة ,و من ثم يتم الحفاظ على الدليل الأصلي من التلف و الفقدان و التغيير[1].

إن استعمال التقنية يمكننا من معرفة هل تم العبث بالدليل الالكترون ي و تعديله أم لا ؟ كما يمكننا من استرجاع الدليل بواسطة برامج و تطبيقات خاصة , لأنه يبقى محفوظ في حاويات التخزين

3-**اتساع نطاق الدليل الرقمي** : أي انه يشمل جميع البيانات و المعلومات الرقمية التي يتم تداولها رقميا بمختلف أشكالها, سواء كانت متعلقة بالحاسب الآلي أو شبكة الانترنت أو شبكة الاتصال السلكية و اللاسلكية و قد تتمثل في المواقع الالكتروني ة, البريد الالكترونـي, النصوص و الصور و الفيديوهات الرقمية, الملفات المخزنة في الأنظمة المعلوماتية[2].

4-**صعوبة التخلص من الدليل** :أي أنه كل ما تم إدخال أي بيانات في الأنظمة المعلوماتية فإنه يصعب التخلص منها ,ولو كان ذلك باستخدام أعتى أنواع برامج الإلغاء و الحذف ,فعندما يتم حذف ملف ما فإن محتوى الملف يمكن استرداده لأن المساحة التي كان يشغلها الملف تظل متاحة مال يتم شغلها من قبل ملف آخر.

و عليه فإنه يمكن استرداد الملفات التي قام المجرم المعلوماتي بحذفها بواسطة برامج مخصصة لذلك, و تحديد تاريخ إنشاء الملف و آخر تعديل له و آخر مرة تم فتحه, و يمكن التعرف على الأدلة الرقمية المزورة أو التي جرى عليها التحريف و إمكانية استرجاعها من الحواسيب حتى بعد حذفها.

5- أنه يتكون من حقول مغناطيسية و نبضات كهربائية غير ملموسة لا يدركها الرجل العادي .

6-أنه ليس أقل مادية من الأدلة المادية الأخرى بعد نقله على دعامة مادية .

[1] عبد الناصر محمد محمود, فرغلي و محمد عبيد سيف سعيد مسماري, الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية جامعة نايف العربية للعلوم الأمنية, السعودية 2007, ص 15 .
[2] سعيداني نعيم المرجع السابق ص 124.

7-يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل و لها ذات القيمة العلمية و الحجية الثبوتية ,و هو ما لا يمكن تصوره في الأدلة العلمية الأخرى .

8-يستخدم الدليل الرقمي في رصد المعلومات عن الجاني و تحليلها و تسجيل تحركاته[1] .

ثالثا : مصادر استخلاص الدليل الرقمي

تظهر مشكلة استخلاص الدليل الرقمي من خلال صعوبة الحصول عليه لتعلقها بكم البيانات الخاصة بالجريمة المعلوماتية ,و من حيث ضخامتها و سهولة تدميرها بضغطة زر واحدة على لوح المفاتيح

وهناك عدة مصادر للحصول على الدليل الرقمي من البيئة الرقمية انطلاقا من أجهزة الحاسوب الخاصة بالمشتبه به أو الضحية وكذا من خلال أجهزة مقدم الخدمة, لأن الحصول على الدليل الرقمي تطلب فحص نظم الاتصالات بالإنترنت و فحص مركبات الحاسب و كل جهاز يمكنه الولوج إلى الانترنت بالهواتف النقالة ,و هي تختلف بحسب تواجد هذا الدليل و ذلك من اجل تعقب المجرم و تقديمه للمحاكمة[2] و هي تنقسم إلى :

1- **فحص نظام الاتصال بالشبكة** : و يتمثل في نظام فحص مسار الانترنت و فحص بروتوكولات الانترنت (ip) بواسطة برامج لمعرفة نوع الجهاز الذي وقعت فيه الحركة المعلوماتية و إمكانية معرفة مكان و هوية الجاني خاصة إذا كان يستخدم حاسوبه الشخصي

2- فحص مركبات الحاسوب : إن أهم مصادر الدليل الرقمي هو الحاسوب الخاص بالجاني أو حتى المجني عليه عن طريق البحث في الحواسيب و ملحقاتها, والتي تقوم بحفظ كل المعلومات و النشاطات في ذاكرتها, وذلك بفحص القرص الصلب الذي يحوي بدوره على مجموع البيانات الرقمية [3] و استرداد الملفات المحذوفة, كما يمكن الوصول لصور أو صفحات الواب ورسائل في البريد

[1] خالد عياد الحلبي المرجع السابق ص 231.
[2] سعيداني نعيم المرجع السابق ص 130.
[3] عمر محمد بن يوسف المرجع السابق , ص 10.

الالكتروني من خلال فحصه للقرص الصلب, هذا بالإضافة لفحص برمجيات الحاسوب و التي تشكل المكون المعنوي للحاسوب

كما يمكن فحص حاسوب الضحية الذي قد يكون شخص طبيعي أو معنوي ذلك بتتبع الآثار التي تركها المجرم المعلوماتي في مسرح الجريمة الرقمية [1]

3-**مزود أو مقدم الخدمة** : أين يمكن الاستعانة بمقدم الخدمات لاكتشاف أدلة رقمية مثل Google/Yahoo محركات بحث تقوم بحفظ كل بيانات مشتركيها عبر الانترنت, و التعرف على الملفات المحملة و المواقع التي ارتادها المجرم المعلوماتي ,وقد تناولناه فيما سبق فلا داعي للتكرار

الفرع الثاني: مشروعية الدليل الرقمي

أولا / مفهوم شرعية استخلاص الدليل الرقمي : إن مبدأ شرعية الجرائم و العقوبات و كذا مبدأ الشرعية الإجرائية هما الدعامة الأساسية التي يقوم عليها بنيان القانون الجنائي, الأمر الذي ينعكس بدوره على قواعد الإثبات الجنائي و ضرورة خضوعها لمبدأ الشرعية ,و التي تستدعي عدم قبول أي دليل رقمي تم الحصول عليه بطريقة غير مشروعة[2].

ويقصد بمشروعية الدليل هو أن يكون هذا الدليل معترف به أي أن القانون أجاز استخدامه و قبله ضمن أدلة الإثبات الجنائي التي يستند عليها القاضي في تكوين قناعته, وكذلك مشروعية الحصول عليه التي تقتضي أن يكون إجراءات جمع الأدلة و استخلاصها وفقا للإجراءات التي رسمها القانون و إلا كانت باطلة و يترتب عنه بطلان الدليل المستنبط من إجراء غير مشروع [3]

كما أن استخدام الوسائل العلمية الحديثة في الإثبات لاسيما الأدلة الرقمية يجب أن يكون بتحفظ و في إطار المشروعية و النزاهة في استخلاصه, فكل مراقبة للاتصالات أو تفتيش في

[1] عمر محمد بن يوسف , المرجع السابق , ص 10 .
[2] خالد عياد الحلبي, المرجع السابق, ص 235.
[3] د- عبد الفتاح بيومي حجازي, الدليل رقمي في جرائم الكمبيوتو و الانترنت بهجت للطباعة و النشر, القاهرة 2009, ص 64.

المنظومة المعلوماتية دون إذن مسبق و دون وضع ترتيبات تقنية يؤدي إلى المساس بحرمة الحياة الخاصة للفرد, أو كل إكراه مادي أو معنوي من قبل ضباط الشرطة القضائية في سبيل الحصول على الدليل للضغط على المشتبه فيه لفك شفرة النظام المعلوماتي يعد من الطرق الغير مشروعة و التدليسية.

و عليه فإن الشرعية في تحصيل و استخلاص الدليل الرقمي هي الجوهر بين ضمان و حماية حقوق الأفراد و حرياتهم و الحفاظ على حرمة حياتهم الخاصة و سرية مراسلاتهم من جهة , و بين حق الدولة في توقيع العقاب على المجرمين للحفاظ على أمن و استقرار المجتمع من جهة ثانية.

و من نتائج الحصول على دليل رقمي خارج القواعد الإجرائية التي تنظم كيفية و ضوابط الحصول عليه هو بطلان الدليل المستمد منها [1].

ثانيا/ موقف القضاء من الدليل الرقمي غير المشروع:

لقد أثيرت مسألة قيمة الدليل الرقمي غير المشروع في الإثبات الجنائي في إطار البحث حول مشروعية الدليل التقني, الأمر الذي يحيلنا للتمييز بني أدلة الإدانة و أدلة البراءة لمعرفة قيمته و موقف القضاء منه , كما يلي:

1- بالنسبة لدليل الإدانة:

وفقا لقاعدة أن الأصل في الإنسان البراءة فإن المتهم يعامل على أساس أنه برئ في جميع مراحل الدعوى لحين صدور حكم نهائي بالإدانة, و يجب أن يؤسس حكم الإدانة على دليل ثم الحصول عليه بطريقة مشروعة, و عليه لا يمكن للقاضي أن يستند في حكم الإدانة على دليل ناتج عن عملية التسرب أو تفتيش بدون إذن مسبق, أو كان متحصلا نتيجة إكراه للمتهم المعلوماتي من أجل فك شفرة الدخول للنظام المعلوماتي أو ملفاته[2].

[1] د/ احمد فتحي سرور, نظرية البطلان في قانون الإجراءات الجزائية, رسالة دكتوراه كلية الحقوق. جامعة القاهرة, 1959, ص 382 .
[2] جميل عبد الباقي الصغير أدلة الإثبات الجنائي و التكنولوجيا الحديثة, دار النهضة العربية القاهرة, 2002, ص 111

و عليه فإن الإجراء الباطل لعملية البحث و التحري يترتب عنها بطلان الإجراءات اللاحقة له ,و بطلان الدليل المستمد منها ولا يمكن التمسك به لإدانة المتهم .

2-بالنسبة لدليل البراءة:

اختلف الفقهاء حول مدى مشروعية الدليل الرقمي لإثبات براءة المتهم إلى ثلاث اتجاهات كما يلي[1]:

أ- **الاتجاه الأول** يرى أن المشروعية لازمة سواء في دليل الإدانة أو البراءة و أن المشروعية شرط أساسي حتى في إثبات براءة المتهم.

ب- **الاتجاه الثاني** يرى أن المشروعية ضرورية في أدلة الإدانة فقط دون أدلة البراءة لأن الأصل في الإنسان البراءة ولا حاجة لإثباتها .

ج- **الاتجاه الثالث** فيرى أن أدلة البراءة الغير مشروعة يمكن الأخذ بها و قبولها في حالات فقط بشرط أن لا تصل لحد الجريمة و تتضمن مخالفة قاعدة إجرائية بسيطة .

و الراجح من بين هذه الاتجاهات هو الثاني الذي يقصر المشروعية على دليل الإدانة فقط دون البراءة, لأن عدم قبول دليل البراءة بحجة انه غير مشروع يؤدي لنتيجة خطيرة و هي إمكانية إدانة برئ[2] ,و نرى بأنه الرأي الراجح على أساس أن قرنية البراءة مفترضة لا تحتاج لإثبات .

الفرع الثالث: صعوبات استخلاص التدليل الرقمي

أصبحت الجرائم المعلوماتية تشكل تحديا كبيرا للأجهزة المختصة بالبحث و التحري و التحقيق نظرا للصعوبات التي تعرقل عملها في سبيل الحصول على الدليل التقني و هذه التحديات كانت موضوع عدة مؤتمرات دولية و نذكر من بينها ما يلي:

[1] رشيدة بكري, المرجع السابق, ص 293.
[2] سعيدي نعيم, المرجع السابق, ص 213.

1 انتشار استخدام مقاهي الانترنت من المجرم لارتكاب أفعاله ,مما يؤدي لصعوبة التوصل إليه و صعوبة تعقب الدليل خاصة بعد تنقله عبر أكثر من مقهى انترنت.

2 استخدام المجرم لتكنولوجيا (A.D.S.L) أو ما يعرف باسم "الانترنت فائق السرعة" في تنفيذ مخططاته الإجرامية, عن طريق اشتراكه مع عدة أشخاص في جهاز واحد عن طريق موزع خطوط الأمر الذي يصعب معه اكتشافه.

3 ظهور الإنترنت اللاسلكية, الذي سهل الأمر للمجرمين المعلوماتيين التنقل لعدة أمكنة في اليوم الواحد دون قيام هذه الخدمة بتسجيل دخولهم للانترنت و من هنا تظهر أهمية إلزام مقاهي الانترنت بتسجيل معطيات مستخدمي الشبكة العالمية للمعلومات (الانترنت)

4 أما التحدي الرابع فهو يتعلق بعملية البر وكسي (Proxy) التي تسمح بالتخفي أثناء التجوال عبر الشبكة التي تؤمنها بعض المواقع, وهو ما يلجأ له قراصنة و مصممو الفيروسات.[1]

هذا بالإضافة لعدة تحديات أخرى , و هي :

أولا/ الصعوبات المتعلقة بالطبيعة التكوينية للدليل الرقمي

ويقصد بها المشاكل التي تتعلق بطبيعة الدليل التقني النابع من تكنولوجيا المعلومات, سواء بسبب طبيعته الغير مرئية أو الديناميكية أو خاصية تبخره و التي تضعف من عملية استخلاصه و سنذكرها على التوالي:

1- الطبيعة الغير مرئية للدليل الرقمي:

فهو عبارة عن نبضات مغناطيسية أو كهربائية تقع في البيئة الرقمية و التي لا يدركها الرجل العادي بحواسه, يتم تخزينها في العالم الافتراضي في شكل ملفات و التي تختلط عادة مع ملفات عادية لمستخدمي الانترنت الأبرياء, الأمر الذي يهدد معه خصوصية هؤلاء[1]

[1] رشيدة بوبكر, المرجع السابق, ص 454 .

فغالبا ما يقوم المجرمون بإخفاء ملفاتهم تحت عناوين مضللة و تشفير المعلومات المخزنة الكترونيا أو المنقولة عبر الانترنت, مما يعيق عمل سلطات البحث و التحقيق في تتبعها.

1 **الطبيعة الديناميكية للدليل الرقمي:**

الدليل الرقمي ذو طبيعة ديناميكية فائقة السرعة إذ يتنقل عبر الشبكات الاتصال بسرعة فائقة و إمكانية تخزين المعلومات حتى في الخارج, الأمر الذي يعيق مهمة تتبعه في إطار عمليات البحث و التحري و ما ينجر عنه من مساس بسيادة الدولة الأخرى عند القيام بتفتيش منظومة معلوماتية متصلة بنظام آخر خارج الدولة, مالم تتم في إطار التعاون الدولي.

و هو ما ذهب له المشرع الجزائري في القانون: 04/09 ,أين نص على ضرورة التعاون و المساعدة القضائية الدولية لمواجهة الإجرام المعلوماتي.

3- مشكلة تبخر الدليل الرقمي الذي يمكن تعديله أو محوه في ثواني:

وقوع الجرائم المعلوماتية في عالم افتراضي أو بيئة الكترونية الأمر الذي انعكس على عدم مرئية الدليل المترتب عنها ,و يجعل من مسألة حذفه أو تعديله أمر في غاية السهولة من قبل المجرم المعلوماتي و خلال مدة وجيزة ,وهنا تظهر عدم كفاية إجراءات التفتيش و الضبط أم خاصية تلاشي أو تبخر الأدلة, مما استدعى ضرورة اللجوء أو الاستعانة ببرامج لاستعادة الملفات المحذوفة و كذا إلزام مزودي الخدمات بحفظ على المعلومات المخزنة لديهم و عناوين الأشخاص المشتركين و التي تساعد في التعرف على هويتهم .

ثانيا :صعوبات متعلقة بجهات التحقيق

إن من أهم معوقات التحقيق تلك المتعلقة بشخص المحقق و قلة معرفته التقنية في استخدام الحاسوب و شبكة الانترنت و بمصطلحاتهما, و عدم مواكبته لمستجدات الإجرام المعلوماتي, و عدم

[1] ممدوح عبد الحميد عبد المطلب, استخدام بروتوكول(tcplip) في بحث و تحقيق الجرائم على الكمبيوتر., المرجع السابق , ص 19 .

التنسيق بين عمل جهات التحري و التحقيق و الخبراء و المختصين في الأنظمة المعلوماتية [1], الأمر الذي يستدعي لإنشاء خلايا على مستوى مراكز الشرطة ووحدات الدرك الوطني تكون متخصصة في مجال مكافحة الإجرام المعلوماتي ,من خلال تكوين خبراء مختصين من رجال الضبطية القضائية في جمع الأدلة الجنائية الرقمية سواء في داخل أو خارج الوطن و الاستفادة من تجارب الدول الرائدة في مجال مكافحة الإجرام المعلوماتي[2].

إلا أن ضعف الميزانيات المالية المقررة للتكوين ,و كذا التطور السريع للمنظومات المعلوماتية و برامجها جعلت من مسألة التكوين لوحدها غير كافية.

ثالثا: الصعوبات المتعلقة بالجريمة و أطرافها

هناك عدة أمور تعيق عمل جهات التحقيق نظرا للطبيعة الخاصة للإجرام المعلوماتي ,والتي تزيد من صعوبة اكتشافها ويرجع ذلك لكون الجريمة المعلوماتية هي جريمة متسترة تتم في بيئة رقمية ولا تخلف آثار مادية, و إن وجد الدليل فيكون محمي بنظام أمن أو مشفر يصعب الوصول إليه أو استنساخه, بالإضافة لسهولة محوه في زمن وجيز, ناهيك عن الضخامة البالغة لحجم المعلومات و البيانات المتعين فحصها.[3]

ولعل أكبر سبب وراء ذلك هو الهوية المجهولة للجاني أو أنه يكون بهوية مستعارة, رغم توفر إمكانية التعرف على عنوان و رقم الحاسوب الذي استخدم في ارتكاب جرائم الاعتداء على نظم المعالجة الآلية[4], وهو ما يعرف بتقنية(IP).

كما أن مسألة تحديد مصداقية الهوية عبر الانترنت (IP) خاصة في الدول العربية تتقلص بسبب أن خط هوية الانترنت قد يشترك فيه أكثر من شخص [5] , ولا يطرح أي إشكال إذا تعلق الأمر

[1] خالد عياد الحلبي, المرجع السابق, ص 224.
[2] سعيداني نعيم, المرجع السابق, ص 188.
[3] حسين الغافري., المرجع السابق . ص 20 .
[4] عمر أبو بكر بن يونس, الجرائم الناشئة عن استخدام الانترنت,المرجع السابق , ص 835.
[5] نبيلة هبة هروال, المرجع السابق, ص 98.

بحاسوب موضوع في منزل أو في شركة أو مكتب , لكن الأمر يزداد صعوبة إذا كان الحاسوب في مكان شبه عام معد لتقديم خدمة للجمهور, كما هو الحال بالنسبة لمقاهي الانترنت مثلا. [1]

هذا بالإضافة لقدرة بعض المجرمين المحترفين باستخدام برامج ضارة و خبيثة تقوم بإدخال معلومات كاذبة عن حقيقة عنوان (IP) ,و إرسالها لمزود خدمة شبكة الانترنت على أساس أن هذه المعلومات جاءت من نظام معلوماتي معين في حين أنها كانت من كمبيوتر آخر.

أما بالنسبة للصعوبات المتعلقة بالجهات المتضررة من جرائم الحاسوب و الانترنت فهي تتعلق بعدم إدراكهم لخطورة هذه الجرائم, و عدم تزويد أنظمتهم المعلوماتية ببرامج و جدار حماية كفيل بحماية معلوماتها و بياناتها من خطر القرصنة.

وكذا الإحجام عن التبليغ عن هذه الجرائم لدى السلطات المختصة ,رغبة منها في إخفاء ظهورها بمظهر مشين يدل على إهمالها و قلة خبرتها أو عدم وعيها الأمني ,و عدم أخذها للاحتياطات الأمنية لحماية معلوماتها, مما يضعف ثقة المتعاملين معها [2], كما أن الكثير من الشكاوى في الجرائم المعلوماتية تكون مقيدة ضد مجهول .

رابعا: الصعوبات التشريعية :يعد القصور التشريعي سواء في شقه الموضوعي المتعلق بالتجريم و العقاب أو في شقة الإجرائي المتعلق باستخلاص الأدلة الجنائية الرقمية من أكبر و أهم المعوقات و الصعوبات التي تعترض الفنيين و المحققين المختصين في مكافحة الجريمة المعلوماتية.

فعدم وجود نصوص تجريمية لبعض أنواع الجرائم التي تعرف تطور مستمر والتي لا يمكن حصرها و خاصة أنها تجعل من الفعل مباح و يعرقل بذلك عمل جهات التحقيق.

هذا بالإضافة إلى مشكلة الاختصاص المكاني و القانوني الواجب التطبيق في حال ارتكاب الجريمة في دولة و أثارها في دولة أخرى, و في ظل غياب أي اتفاقيات و معاهدات دولية بين الدولتين تقر بالتعاون الدولي و القضائي, فلا يمكن بذلك لجهات التحقيق القيام بأي إجراء من

[1] رشيدة ابأو بكر, المرجع السابق, ص 476.
[2] عبد الرحمن بحر, ص 39,و خالد عياد الحلبي,المرجع السابق, ص 224.

إجراءات البحث و التحري في سبيل الحصول على الدليل الالكتروني ة و معرفة هوية مرتكبي الجرائم[1].

كما توجهت الدول لتحديث منظومتها القانونية في الجانب الإجرائي و استحداث آليات قانونية أو ما يعرف بأساليب التحري الخاصة التي تسهل من عملية الحصول على الأدلة الرقمية, و هو ما قام به المشرع الجزائري باستحداثه لإجرائي التسرب و اعتراض المراسلات و التقاط الصور و تسجيل المكالمات في قانون الإجراءات الجزائية و كذا إجراء المراقبة الالكترونية و حفظ المعطيات و التفتيش عن بعد و هذا في القانون 04/09.

و عليه يمكن القول بأنه رغم الجهود المبذولة في إطار التشريع المعلوماتي في شقيه الموضوعي و الإجرائي إلا أن التحدي في استخلاص الأدلة الرقمية مازال قائما مما يستدعي ضرورة التحديث الدوري للتشريعات الداخلية بشكل يتوافق نسبيا مع مجاراة تطور الجريمة المعلوماتية, و كذا تطوير مهارات المحققين المتخصصين و تكوينهم الدوري لتمكينهم من تذليل الصعوبات السالفة الذكر, و قدرتهم على ملاحقة مرتكبي الجرائم المعلوماتية و استخلاص الأدلة الرقمية التي تثبت إدانتهم.

المطلب الثاني

دور القاضي في تقييم الدليل الرقمي

تعد مرحلة الحكم هي المرحلة الحاسمة في الدعوى الجنائية, أين يتم مناقشة الأدلة الإلكترونية المتوفرة من قبل قاضي الحكم للفصل في الجرائم المعلوماتية المطروحة أمامه و تخضع لسلطته التقديرية, أين يخضع الدليل الالكتروني كباقي الأدلة الجناية الأخرى للقواعد المقررة للإثبات الجنائي, سواء ما تعلق منها بقواعد الإثبات الحر أو المقيد أو المختلط, أو ما يتعلق بسلطة القاضي الجنائي في قبول الدليل الرقمي بعد التأكد من مشروعيته حتى يرتب آثاره القانونية.

[1] خالد عياد الحلبي, المرجع نفسه, ص 221. و سليمان العنزي,المرجع سابق ص 113.

و سنتناول في هذا المطلب لحجية ويقينية الدليل الرقمي في الإثبات الجزائي في الفرع الأول , ثم تقييم هذا الدليل من حيث سلامته الفنية و الإجرائية في الفرع الثاني, و دور الخبرة الفنية في تقييم الدليل الرقمي في الفرع الثالث.

الفرع الأول: حجية الدليل الرقمي في الإثبات الجزائي

إن مجرد الحصول على الدليل الإلكتروني الرقمي و تقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة, ذلك إن الطبيعة التقنية الخاصة بهذا الدليل تمكن من العبث بمضمونه على نحو يحرف الحقيقة ,ووحده الخبير الفني من يكتشف ذلك[1] .

و من ثم تثور فكرة الشك في مصداقيته كدليل للإثبات و إمكانية استبعاده لتعارضه مع قرنية البراءة, و الشك في الدليل الالكترونـي لا يتعلق بمضمونة كدليل و إنما بعوامل مستقلة عنه [2] ولكنها تؤثر في حجيته, أي ينبغي التأكد من سلامة الدليل من العيوب ومن صحة الإجراءات المتبعة في سبيل الحصول عليه , ثم مناقشته في الجلسة .

و تختلف النظم القانونية في موقفها من الدليل الرقمي حسب نظام الإثبات الجنائي المتبع لدى كل دولة.

أولا: حجية الدليل الرقمي في أنظمة الإثبات: و نميز بين نظام الإثبات المقيد و الحر.

أ-حجية الدليل الرقمي في نظام الإثبات المقيد : أو ما يعرف بنظام الأدلة القانونية, و المشرع هو من يضبط وسائل الإثبات و القاضي ملزم بتطبيق ما جاء به القانون وما فرضه من أدلة فلا يجوز له الحكم بالإدانة عند عدم توفر الدليل ولو كان لديه اقتناع شخصي بأن المتهم هو من ارتكب الجريمة.[3]

[1] د/ هلال احمد, تفتيش نظم الحاسب الآلي, ص205 .
[2] خالد عياد, المرجع السابق, ص 247 .
[3] محمد مروان, نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري, الجزء الأول, ديوان المطبوعات الجامعية الجزائر, 1999, ص 34 .

إلا أن مسألة تقديم نسخة من البيانات و المعطيات المخزنة في الحاسب تطرح أمام القضاء عدة إشكالات حول مدى مطابقة الدليل الرقمي الأصلي و تشكل في عدم تحريفه[1] .

و توجه التشريع الأمريكي في هذا الصدد إلى اعتبار أن الدليل الرقمي المستخرج من الطابعة يعد دليل أصلي في المادة: 3/101 من قانون الإثبات الأمريكي معتبرا بذلك أن النسخة طبق الأصل للبيانات المخزنة بالحاسوب تعد كالنسخ الأصلية[2]

ب-حجية الدليل الرقمي في نظام الإثبات الحر : و يعني هذا النظام هو حرية القاضي في اقتناع الشخص بالدليل الذي يراه مناسبا و حرا في تقييمه, [3] فالأدلة في نظام الإثبات الحر لا تكون محددة مسبقا وترك للأطراف حرية تقديم دليل الإثبات لقاضي الموضوع, و يقتصر دور المشرع في تحديد شروط صحة الدليل أو الضوابط استخلاصه في إطار حماية الحريات و الحقوق الخاصة, و القاضي له سلطة تقديرية واسعة في الاستناد على الدليل الذي يراه مناسبا .

و بما أن إطار دراستنا هو التشريع الجزائري, فإنه ينبغي الإشارة إلى أن المشرع أقر بمبدأ حرية الإثبات الجنائي وهذا بموجب نص المادة 212 من قانون الإجراءات الجزئية و التي نصت على: " يجوز إثبات الجرائم بأي طريق من طريق الإثبات ما عدا في الأحوال التي ينص عليها هذا القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص.

ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه" .

و عليه فالدليل الرقمي شأنه شأن الأدلة الأخرى هو مقبول مبدئيا في الإثبات الجنائي للجرائم المعلوماتية, و تبقى حرية الأطراف في تقديم أدلة الإثبات مقيدة فقط بضوابط المشروعية أثناء استخلاصه, هذا بالإضافة إلى أن قرينة البراءة تلقى على عاتق النيابة العامة أو سلطة توجيه الاتهام

[1] بن فريدة محمد, " الدليل الجنائي الرقمي و حجيته أمام القضاء الجزائري" مقال في المجلة الأكاديمية للبحث القانوني الصادر عن كلية الحقوق و العلوم السياسية, قسم الحقوق, جامعة جامعة عبد الرحمن ميرة بجاية, الجزائر, جانفي 2014, ص 387 .
[2] سامي جلال فقي حسين, المرجع السابق ,ص 91 .
[3] محمد مردانا, المرجع السابق ص39 .

عبئ الإثبات في ظل نظام حرية الإثبات لتسهيل مهمتها, و تبقى مسألة تقدير هذا الدليل بالقبول أو والرفض من قبل القاضي الجنائي[1] وفقا لسلطته التقديرية .

و يلعب القاضي الجنائي في مجال 'ثبات الجرائم المعلوماتية دورا إيجابيات في الحصول على الدليل الرقمي أين لا يكتفي بالأدلة المقدمة له من أطراف الدعوى ,و إنما يبادر من تلقاء نفسه لاتخاذ جميع إجراءات التحقيق التي تساهم في إظهار الحقيقة [2] ,كأن يوجه أمرا لمزود خدمة الانترنت بتقديم معلومات و بيانات تخص مستخدم الشبكة كمواقع الانترنت التي زارها و الصفحات التي اطلع عليها و الملفات التي حملها أو شاركها و الرسائل الالكترونية التي استلمها و أرسلها, عن طريق ندب الخبراء نظرا لما لها من دور كبير و فعال في مساعدة القضاء لكشف الحقيقة ,لاسيما في مجال الجرائم المعلوماتية نظرا لتعدد صور الاعتداء على نظم المعالجة الآلية .

الفرع الثاني :تقييم الدليل الرقمي من حيث سلامته الفنية و الإجرائية

رغم تمتع الدليل الرقمي بالقيمة الثبوتية العلمية قد تصل لحد اليقين شأنه في ذلك شأن الأدلة العلمية الحديثة, لكن ذلك لا ينفي الشك في سلامته من العبث به بالتحريف أو التغيير, أو في صحة الإجراءات المتبعة للحصول عليه , بالإضافة لضرورة مناقشته في الجلسة [3].

أولا: مناقشة الأدلة الرقمية في الجلسة

بالإضافة إلى ضرورة استناد القاضي على أدلة مقبولة و مشروعة في تكوين قناعته التي بني علها حكم الإدانة أو البراءة, إلا أنه ينبغي أن يستمد قناعته من الأدلة التي طرحت بالجلسة و تمت مناقشتها من الخصوم[4] ,حتى يتمكن الأطراف من الاطلاع عليها و مناقشتها و إبداء رأيهم بشأنها في إطار مبدأ شفوية المحاكمة الجنائية , فلا يكتفي القاضي الجنائي بالأدلة المدونة في محاضر التحقيق , و إنما يتوجب عليه سماع الشهود و اعتراف المتهم بنفسه و ما يدلي به الخبراء و طرحها

[1] رشيدة بوبكر, المرجع السابق, ص 484 .
[2] عائشة بن قارة مصطفى., حجية الدليل الرقمي في مجال الإثبات الجنائي , رسالة ماجستير , كلية الحقوق , جامعة الاسكندرية , 2009 ,ص 121 .
[3] طارق محمد الجملي, المرجع السابق , ص 26 .
[4] اشرف عبد القادر قديل, المرجع السابق, ص 236 .

للمناقشة الشفوية ,الأمر الذي يتيح للأطراف بيان موقفها من الدليل و يتيح للقاضي تكوين قناعته من حصيلة المناقشات الواقعة أمامه قي الجلسة و تحرر في محضر الجلسة ,و إذا استدعىالأمر الاستعانة بخبرة تساعده في بناء قناعته .

ثانيا : تقييم الدليل الرقمي من حيث سلامته من العبث

إن التقنية الحديثة تمكن من العبث بالدليل الرقمي بسهولة بحيث يظهر بمظهر و كأنه نسخة أصلية في تعبيرها عن الحقيقة, و يمكن التأكد من سلامته من العبث بعدة طرق نذكر أهمها:

أ – **تقنية التحليل التناظري الرقمي** : و يتم من خلال هذه التقنية مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية للتأكد من مدى العبث بالنسخة المستخرجة من جهاز الحاسوب[1].

ب – استخدام عملية الخوارزميات : هي عبارة عن عمليات حسابية للتأكد من سلامة الدليل الرقمي من التبديل أو العبث به[2]

ج - استخدام الدليل المحايد : وهو نوع من الأدلة الرقمية المخزنة في البيئة الافتراضية ولا علاقة له بموضوع الجريمة, ولكنه يساهم في التحقق من مدى سلامة الدليل التقني من عدم تعرضه لتعديل أو تغيير.

ثالثا / تقييم الدليل الرقمي من حيث السلامة الفنية لإجراءات استخلاصه :تتبع جملة من الإجراءات الفنية للحصول على الدليل الرقمي, إلا أنه قد يعتريها خطأ قد يشكك في سلامة نتائجها وإن كانت ضئيلة جدا ,و للتأكد من سلامة الإجراءات المتعبة في الحصول على الدليل من الناحية الفنية ينبغي ما يلي:

أ–إخضاع الأداة المستخدمة في الحصول على الدليل لعدة تجارب للتأكد من دقتها في إعطاء النتائج المرجوة : و يكون ذلك باستخدام اختيارين رئيسيين للتأكد من إن الأداة المستخدمة عرضت

[1] د/ ممدوح عبد الحميد عبد الحميد عبد المطلب, زبيدة محمد قاسم, عبد الله عبد العزيز, مرجع سابق, 22 .
[2] خالد عياد الحلبي, المرجع السابق, ص248 .

كل المعطيات المتعلقة بالدليل الرقمي و انه لم يتم إضافة أي بيان جديد ,الأمر الذي يضفي عليها مصداقيته و حجية أكبر في الإثبات الجنائي[1].

ب-الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم أفضل النتائج:

أثبت الدراسات العلمية في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل الرقمي ,وكذلك الأدوات المشكوك في كفاءتها لاستبعادها, الأمر الذي يساهم في تعزيز مصداقية المخرجات المستمدة من تلك الأدوات.[2]

و عليه يمكن القول أن عملية التشكيك في سلامة الدليل الرقمي من ناحية العبث به أو سلامة الإجراءات الفنية للحصول عليه, تبقى مسألة فنية بحتة تخضع لأهل الخبرة و الاختصاص و بذلك تلعب الخبرة الفنية دورا مهما في تكوين عقيدة القاضي حول مصداقية و صحة الدليل الرقمي.

و يبقى للقاضي الجزائري الحرية في اختيار الدليل الذي يراه مناسبا لتكوين اقتناعه الشخصي به شأنه في ذلك الوقت شأن كل الأدلة الأخرى يمكنه الاستعانة بأهل الخبرة في المسائل الفنية[3]

الفرع الثالث:دور الخبرة الفنية في تقييم الدليل الرقمي

أولا - مفهوم الخبرة الفنية : لقد أصبحت الخبرة التقنية ضرورة حتمية في عالم الخبرة القضائية و ذلك بالاستعانة بخبراء و مختصين كمطلب ملح لفحص الأدلة الرقمية و تحليلها و لإثبات الجرائم المعلوماتية ,و ذلك لعجز جهات التحري التحقيق و الحكم للقيام بها لتعلقا بمسائل فنية [4]خاصة بعد محو الدليل الرقمي.

و إذا كان للخبرة الفنية أو التقنية أهمية كبرى في استخلاص الدليل الرقمي ,فإن دورها في بحث مصداقيته في مجال المعالجة الآلية للمعطيات أهم ,و ذلك لدحض الشك في سلامته الفنية و الإجرائية.

[1] رشيدة بكري, المرجع السابق, ص 501 .
[2] طارق احمد الجبلي.المرجع السابق, ص 28 .
[3] ين بلاغة عقيلة .المرجع السابق, ص 59 .
[4] رشيدة بوبكر المرجع السابق, ص 424 .

و تقوم المحكمة بتعيين خبراء فنين في النظام المعلوماتي إما من تلقاء نفسها أو بطلب من أحد الخصوم, وهو ضرورة حتمية لاستخلاص الدليل الرقمي و إثبات جرائم الاعتداء على نظم المعالجة الآلية, خاصة عند عجز جهات البحث و التحري و كذا التحقيق عن جمع أدلة الجريمة ,أو بسبب تدمير الدليل الرقمي أو محوه جهلا أو إهمالا من قبل الضبطية أو المجرم .

و نص المشرع الجزائري في المادة: 5 فقرة أخيرة من القانون: 04/09 على أنه:"يمكن للسلطات المكلفة تفتيش المنظومات المعلوماتية تسخير أي شخص له دراية بعمل المنظومة المعلوماتية محل البحث, أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها قصد مساعدتها و تزويدها بكل المعلومات الضرورية لانجاز مهمتها " .

و يكون بذلك قد وسع المشرع من دائرة الخبراء الفنيين لتشمل المختصين في الإعلام الآلي و تكنولوجيا الإعلام و الاتصال و مزودي خدمات العبور للانترنت و مزودي خدمات الإيواء, و كل من له دراية في هذا المجال.

و نذكر في هذا الصدد دور بعض الأجهزة في تقديم الخبرات القضائية , و التي تم التطرق لها في الفصل الأول .

ثانيا: إجراءات الخبرة التقنية : يتم اختيار الخبير من الجدول الذي تعده المجالس القضائية, و الذي قام بأداء اليمين القانونية قبل أداء مهامه.[1]

يقوم الخبير الفني أو تقني بأداء مهامه الموكلة له تحت رقابة القاضي الذي أمر بإجراء الخبرة, و عليه إبداع تقرير في خلال المدة المحددة في أمر و حكم الندب, و يودعها لدى أمانة ضبط الجهة التي أمرت بالخبرة في الآجال.

[1] المادة 145 من (ق.إ.ج), المرجع السابق.

ثالثا: الوسائل التقنية المساعدة للخبير المعلوماتي:

و يعتمد الخبير الفني على عدة برامج و وسائل فنية تساعده في استخلاص الدليل الرقمي و الكشف عن المجرم المعلوماتي و نذكر منها ما يلي[1]

1 -بروتكول الانترنت (ip), و يسمى بعنوان الانترنت, و يشتمل على مجموعة من البيانات الموجودة على كل حاسوب مرتبط بشبكة الانترنت, كفيلة بتحديد رقم الجهاز المستخدم في ارتكاب الجريمة و تحديد موقعه و منه الوصول للجاني

2 -نظام البروكسي (proxy): يعمل هذا النظام كوسيط بين شبكة الانترنت و مستخدميها, أين يوفر له م خدمة الذاكرة الجاهزة يخزن فيها كل عمليات التنزيل و التحميلات بغية توفير مساحة بنظامهم المعلوماتي, و هي تساعد الخبير المعلوماتي في تقفي آثار الجريمة.

3 -أنظمة كشف الاختراق: (ids) : والتي تقدم للخبير أو المستخدم بيانات شاملة عن عمليات الاختراق التي تعرض لها الجهاز و كل بيانات الشبكة و أرقام هاتف المخترق .

4 برامج استرجاع العمليات المعلوماتية: (auditing tools)

تستعمل لمراقبة كل العمليات التي تجري على الملفات و أنظمة التشغيل و تسجيلها في ملف يسمى (logs), ويقوم باسترجاع الملفات في حالة حذفها أو محوها ,وتأتي هذه البرامج إما مضمنة في أنظمة التشغيل ,أو كبرامج مستقلة ليتم إعدادها و تفعيلها مسبقا للعمل بها قبل وقوع الجريمة, والتي تساعد الخبير في استنباط الدليل الالكتروني [2].

رابعا: مدى حجية تقرير الخبير التقني : بعد إعداد الخبير لتقرير الخبرة يتضمن ما قام به من أعمال و ما توصل له من نتائج يودعه لدى المحكمة التي طلبت منه إجراء الخبرة, و يعد هذا التقرير مجرد استدلالات لإنارة القاضي فهي مجرد رأي استشاري من الخبير و لا يقيد القاضي و له إن يأخذ بها أو يطرحها أو إن يفاضل بين تقارير الخبراء و يأخذ منها ما يرتاح إليه و يطرح ما دون ذلك, و له الأمر بإجراء خبرة إضافية إذا كان هذا التقرير يعتريه النقص أو الغموض[3].

[1] إبراهيمي جمال: المرجع السابق, ص80/79/78
[2] د/ خالد ممدوح ابراهيم, المرجع السابق, ص 303 إلى 306
[3] رشيدة بوبكر, المرجع السابق, ص 429.

و نفس الأمر ينطبق على الخبرة الفنية في مجال المعالجة الآلية للمعطيات لكن من الناحية العملية فإن القاضي يسلم بما خلص إليه الخبير في تقريره , و يبني حكمه على أساسه لأنه يتعلق بمسألة فنية يجهلها القاضي و أي تفنيد لها يستدعي تعيين خبير أخر للقيام بتسجيل معطيات وحدات المكونات المضبوطة للحاسب الآلي كالنوع و الطراز و الرقم التسلسلي و التأكد من صلاحية وحدات نظام التشغيل و مدى مطابقة محتويات إحراز المضبوطات لما هو مدون عليها, و مدى سلامة الدليل الرقمي من العبث به و تزوير حقيقته[1].

وإظهار الملفات المخبئة و النصوص المخفية داخل الصور,عمل نسخة من وسائط التخزين المضبوطة على رأسها القرص الصلب(HARD DISK) ,لإجراء عملية الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برامجية, استرجاع الملفات التي تم محوها من الأصل و ذلك باستخدام أحد برامج استعادة المعلومات المحذوفة أو المعطلة أو التالفة مثل: (recover 4 all professional easy recover)[2] .

إعداد قائمة يجرد فيها الخبير كل الأدلة التقنية و المعلومات المستخلصة و تخزينها على أسطوانة أو ديسك خاص به لتحويل الدليل التقني لهيئة مادية [3], كما يقوم الخبير بتحديد مدى ترابط بين الدليل المادي و الدليل الرقمي بفحصهما و الربط بينهما للتأكد من يقينية الدليل الرقمي حتى يتم قبوله لدى جهات التحقيق و الحكم [4], مستخدما العديد من الأساليب العلمية و البرامج التي تمكنه إما من استخلاص الدليل الرقمي أو التأكد من سلامته من العبق و سلامة الإجراءات الفنية لاستخلاصه, و ليس للمحكمة رفض تلك الأساليب و كل رفض يجب إن يكون مسببا بشكل منطقي و إلى تعرض حكمها للنقض.

[1] رشيدة بوبكر, المرجع السابق, ص 430.
[2] ممدوح عبد الحميد عبد المطلب, زبيدة محمد جاسم و عبد الله عبد العزيز, نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر, المرجع السابق, ص 22 .
[3] عبد الناصر محمد محمود فرغلي, عبيد سيف سعيد المسماري , ورقة بحثية مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي و الاثبات الجنائي بالأدلة الرقمية ,الرياض , المنعقد في الفترة : 2-4 /11/ 1148 ه الموافق ل :2-2007/11/4 , ص 35 .
[4] رشيدة بوبكر, المرجع السابق, ص 432.

خلاصة الفصل الثاني:

يجب الاعتراف بأن تكريس المشرع الجزائري لأساليب التحري الخاصة بالجريمة المعلوماتية كالمراقبة الالكترونية للاتصالات السلكية و اللاسلكية و التفتيش المعلوماتي عن بعد و حفظ المعطيات المتعلقة بحركة السير يعد خطوة جريئة تحسب له ,رغم أنه يعد من أخطر إجراءات التحري و التحقيق في العالم الافتراضي ,لأنها تنطوي على مساس بالحقوق و الحريات التي كرسها الدستور لا سيما حرمة الحياة الخاصة .

و باعتبار أن الجزائر من الدول العربية الرائدة في مكافحة الجريمة المعلوماتية ,ورغم الجهود المبذولة من قبل المشرع ,إلا أنها تبقى عاجزة عن مواجهة صعوبات و تحديات الإجرام المعلوماتي العابر للحدود , وعليه يجب الاستفادة من تجارب الدول الرائدة في هذا المجال و الاهتمام بتفعيل التعاون الدولي بالانضمام لاتفاقيات دولية خاصة اتفاقية بودابست ,و اتفاقيات إقليمية عربية و إفريقية لإعطاء مفهوم موحد للجريمة المعلوماتية و توحيد إجراءات التحقيق و المساعدة القضائية .

و نلاحظ أنه و بقدر اتساع مساحة الأدلة الرقمية بقدر ما تتضاءل مهمة القاضي الجنائي في التقدير خاصة أمام عدم كفاءته و ثقافته المعلوماتية الأمر الذي يؤثر على قناعته ,و بذلك يكون لرأي الخبير القول الفصل و دور كبير في تقييم مصداقية الدليل كونه معرض للعبث و التلف بسهولة في العالم الافتراضي بعد التحقق من سلامته الفنية و الإجرائية.

كما ننوه إلى ضرورة التأهيل التقني و الفني للقضاة لتمكينهم من التعامل مع الدليل الرقمي الذي يكون محل مناقشة علمية و قانونية في الجلسة و تساعده في تكوين قناعته في الاستناد على هذا الدليل أو طرحه و يبني عليها حكمه إما بالإدانة أو البراءة.

الـــخاتمة :

بعد أن فرغنا من دراسة موضوع المواجهة الإجرائية للجرائم المعلوماتية, و الذي يعد من المواضيع المهمة و المعقدة التي أفرزتها تقنية تكنولوجي ا المعلومات و على رأسها شبكة الانترنت ,التي أدت لتصاعد وتير ة ارتكاب الجرائم المعلوماتية ,و التي طرحت عدة إشكالات و صعوبات قانونية و عملية أدت لإحداث انقلاب و تحول كبير في النظرية التقليدية للجريمة, خاصة أمام قصور المنظومة التشريعية في شقيها الموضوعي و الإجرائي عن مواجهة الإجرام المعلوماتي, الأمر الذي أدى لإفلات مجرمي المعلوماتية من المتابعة الجزائية و توقيع العقاب.

و حاولنا من خلال دراستنا لهذا الموضوع الدمج بين الطابع القانوني و الطابع الفني و التقني بالاعتماد على مزيج من المفاهيم و المصطلحات القانونية و المعلوماتية و التي تساهم فهم هذه الظاهرة الإجرامية المستحدثة نسبيا, و من ثم معرفة آليات التصدي لها و إجراءات البحث و التحقيق المستحدثة الكفيلة بمواجهتها كالمراقبة الالكترونية ,و التي تعتمد على التقنية في الكشف عنها و ملاحقة مرتكبيها في البيئة الإلكترونية من قبل متخصصين في مجال التحقيق المعلوماتي , هذا بالإضافة لضرورة تعزيز التعاون الدولي في مجال الاتفاقيات الدولية و المساعدات القضائية, و الاستفادة بذلك من خبرات الدول الرائدة في هذا المجال .

و بعد الإحاطة بمختلف جوانب دراسة المواجهة الإجرائية للجريمة المعلوماتية و على ضوء الإشكالية الرئيسية و الأسئلة المتفرعة عنها , توصلنا للإجابة عنها بجملة من النتائج كما يلي:

1 -الجرائم المعلوماتية هي : "كل سلوك غير مشروع موجه للمساس بنظم المعالجة الآلية للمعطيات بالاعتداء على سرية مكوناتها الغير المادية أو في وفرتها أو إتاحتها أو في سلامتها أو في تكاملها , أو التي تتم باستخدام المنظومة المعلوماتية " .

2 -إن محل الجريمة المعلوماتية هو نظم المعالجة الآلية للمعطيات بمكوناتها المعنوية التي تستهدف المعلومات بكافة أشكالها في البيئة الرقمية (من صور و أصوات , رموز أو برامج

و سواء كانت معلومات مدخلة أو معالجة , مخزنة أو في طور النقل و التبادل) , كما قد يكون محلها أو موضوعها الجرائم التي ترتكب باستخدام النظم المعلوماتية و هي الأكثر انتشارا و شيوعا .

3 -تكمن خطورة المجرم المعلوماتي في دمجه للذكاء البشري بالذكاء التقني لتكنولوجي ا المعلومات و سعيه الدائم لتطوير أساليبه الإجرامية بشكل يخلصه من قبضة العدالة بإخفاء هويته و محو أثار الجريمة في غضون ثوان و لو عن بعد, و ما يعزز ثقته بنفسه أكثر هو قصور التشريعات الجزائية عن مواجهة هذا النمط المتجدد من الإجرام المعلوماتي, كما يساهم الضحايا في ارتكابها بسبب عدم تأمين نظمهم المعلوماتية بأساليب الحماية كالجدار الناري و برامج مكافحة الفيروسات , بالإضافة لعزوفهم عن الإبلاغ عنها .

4 إن القصور الذي اعترى النصوص الجزائية في مواجهة مختلف صور الإجرام المعلوماتي ترتب عنه إفلات الجناة من العقاب في أغلب الحالات , خاصة أمام صعوبة اكتشافها و إثباتها و التزام القاضي الجزائي بالتفسير الضيق للنصوص التقليدية و احترام مبدأ الشرعية .

5 عالج المشرع الجزائري للجرائم المعلوماتية بمفهومها الضيق في القسم السابع من قانون العقوبات تحت اسم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات , ثم وسع من نطاقها لتشمل كل جريمة ترتكب عبر المنظومة المعلوماتية في القانون الخاص بالوقاية من جرائم تكنولوجيا الاتصال و الإعلام ,و رغم ذلك فإن المعالجة التشريعية تتسم بالجمود و القصور في استيعاب كافة أنماط و صور الإجرام المعلوماتي .

6 -إن استحداث أساليب للتحري و التحقيق الخاصة بالجرائم المعلوماتية و التي تعتمد على استخدام التقنية كالمراقبة الإلكترونية باعتراض المراسلات السلكية و اللاسلكية , و التفتيش المعلوماتي و حفظ المعطيات خلال حركة السير من قبل مزودي الخدمات , لاسيما بعد عجز الأساليب التقليدية عن استخلاص الدليل الرقمي ينطوي على المساس بالحريات الفردية و الاعتداء على الحياة الخاصة للأفراد , لذلك قيدها المشرع بجملة من الضوابط و الشروط الشكلية و الموضوعية تحت طائلة البطلان .

7 -الدليل الرقمي هو عبارة عن معلومات و بيانات مخزنة في نظم المعالجة الآلية و ملحقاتها أو المتنقلة عبرها , و تكون في شكل نبضات كهربائية أو ذبذبات مغناطيسية يمكن تجميعها و تحليلها و معالجتها باستخدام برامج و تطبيقات لتظهر في شكل دعامة مادية ورقية أو إلكترونية كالأقراص المضغوطة أو بأي شكل يمكن عرضه على جهاز الحاسوب , ويستخدم في إثبات وقوع الجريمة و الاعتماد عليه في تقرير الإدانة أو البراءة , وذلك بعد التأكد من مشروعيته و مناقشته في الجلسة .

8_أمام صعوبة اكتشاف الجريمة المعلوماتية و عدم إمكان إجبار المجرم المعلوماتي على كسر شفرة المعطيات و تمسكه بحق الصمت ,و كذا تطويره المستمر لأساليب التخفي في الفضاء الإلكتروني باستغلال التقنية المعلوماتية ,قام المشرع بوضع التزامات على عاتق مزودي الانترنت بحفظ المعطيات و تخزينها تلقائيا لمدة سنة من تاريخ التسجيل , و التي تسهل في عملية الكشف عن الجرائم المعلوماتية و التحقيق فيها و إسنادها لمرتكبيها .

9 _منح القاضي الجزائي سلطة تقديرية واسعة و دور إيجابي في قبول الدليل الرقمي و تقدير قيمته الثبوتية ,و عدم الاكتفاء بما قدمه الخصوم من أدلة, بل يقوم بأي إجراء يراه مناسبا لإظهار الحقيقة لاسيما الاستعانة بالخبرة الفنية .

10-المواجهة الإجرائية للجريمة المعلوماتية لا تتم باستحداث تشريعات موضوعية و إجرائية فقط , بل لا بد من تفعيل استراتيجيات محكمة على المستوى الفني و التقني و التوجه نحو التخصص والتأهيل البشري لجهات التحري و التحقيق و الحكم ,و ضرورة دعم و تعزيز التعاون الدولي القضائي و الاتفاقي للتصدي لهذا النمط المتجدد و المعقد من الإجرام المعلوماتي العابر للحدود, خاصة أمام عجز المجهودات الفردية للدول وقصور الآلة التشريعية على احتوائها و مكافحتها .

الهـــــخاتمة :

و على ضوء النتائج التي تم التوصل إليها في دراستنا , خلصنا لبعض الاقتراحات التي تساهم في حل بعض الإشكالات و الصعوبات التي عرقلت مكافحة الجريمة المعلوماتية لاسيما من الناحية الإجرائية , و نوجزها كما يلي :

_ ضرورة اعتماد مصطلح موحد للجريمة المعلوماتية و الاتفاق عليه دوليا , باعتباره المصطلح الأكثر شيوعا في وصف الظاهرة الإجرامية لتعلقها بنظام المعلومات من حواسيب و شبكة الانترنت .

_ إبرام اتفاقيات و معاهدات دولية و إقليمية ثنائية و متعددة الأطراف في مجال التعاون الدولي لتقريب منظوماتها التشريعية , و الاتفاق على قواعد الاختصاص في الجرائم المعلوماتية العابرة للحدود الوطنية و تسليم المجرمين و تبادل المعلومات و الخبرات الفنية في هذا المجال .

_ انضمام الجزائر لاتفاقية بودابست الأوروبية باعتبارها مرجع أساسي و مهم و مفتوحة للتوقيع و التصديق من كل الدول و لا سيما الدول العربية , لاشتمالها على تدابير و إجراءات جزائية و آليات للتعاون الدولي و القضائي , لضمان التصدي لهذا الإجرام المستحدث و الاستفادة من خبرة الدول الرائدة في هذا المجال و تعديل قوانينها الداخلية بشكل يتوافق مع أحكام الاتفاقية .

_ إفراد قواعد إجرائية خاصة بالجريمة المعلوماتية تتلاءم و خصوصيتها , و تنظيمها في قانون الإجراءات الجزائية , و أن لا تكون متفرقة بين هذا الأخير و القوانين الخاصة .

_ إفراد مقرر مستقل و خاص بالجرائم المعلوماتية في كليات القانون و مدارس الشرطة و القضاء في إطار التكوين القاعدي المتخصص .

_ ضرورة التحيين المستمر و المراجعة الدورية للمنظومة التشريعية في شقيها الموضوعي و الإجرائي لإزالة أي غموض أو ثغرات تسهل إفلات الجناة من قبضة العدالة .

_ عدم اكتفاء المشرع باستحداث أساليب خاصة للتحري في المجال التشريعي لمواجهة التحديات و الصعوبات التي تفرزها الجريمة المعلوماتية , بل الاهتمام بالتزود بآخر الأساليب التقنية المتطورة و الخاصة بترصد و تعقب مجرمي المعلوماتية , والاهتمام بتكوين و تأهيل

الجانب البشري للجهات الأمنية و القضائية , و تفعيل الدور الإيجابي لمقدمي الخدمات وبالأخص مسيري مقاهي الانترنت و إلزامهم بحفظ المعطيات المخزنة لديهم و هوية المستخدمين و المواقع التي تم زيارتها.

_ إنشاء وحدات خاصة بالتحري و التحقيق في البيئة الرقمية سواء على المستوى الوطني أو العربي أو القاري تقوم برصد و تحليل الجرائم المعلوماتية العابرة للحدود .

– الاهتمام الدوري بالتدريب و التكوين المعمق و العالي المستوى لرجال الضبطية القضائية و المحققين المعلوماتيين .

–التوجه نحو تخصص قضاة النيابة و التحقيق و قضاة الحكم لاسيما على مستوى الأقطاب الجزائية , و لما لا تعميمها على مستوى قضاة المجالس القضائية .

–العمل على وضع مواقع إلكترونية مخصصة للتبليغ عن الجرائم المعلوماتية و إرسالها للجهات المختصة , وهو ما يعرف باسم البلاغ الرقمي .

–وضع سجل أمني يتضمن قائمة مجرمي المعلوماتية يسمح بوضعهم تحت المراقبة الأمنية لرصد نشاطاتهم المشبوهة عبر شبكة الانترنت كإجراء وقائي قبل وقوع الجرائم .

_ الاهتمام بالجانب التوعوي و التحسيسي بمخاطر الإجرام المعلوماتي على الأمن العام و أمن الشركات و الأفراد, و ضرورة مساهمتهم في حماية بياناتهم الشخصية باستخدام برامج الحماية و نظام تشفير الملفات, للتقليل من فرص اختراقها و قرصنتها ,و ذلك في إطار الوقاية من هذه الجرائم , و خاصة بعد توجه الجزائر نحو الحكومة الالكترونية , و ذلك من خلال تنظيم أيام دراسية و تحسيسية من قبل الجهات الأمنية و الجامعات و عبر و سائل الاتصال السمعية و البصرية .

كانت هذه جملة من المقترحات التي نتمنى تجسيدها على أرض الواقع في إطار مكافحة الجريمة المعلوماتية , و أرجو أن أكون قد وفقت لحد ما في معالجة هذا الموضوع .

أولا : المصادر

1 -الـــــــقرآن

2 -الـــقوانين و الأوامـــــــر :

1-قانون الإجراءات الجزائية الجزائري الصادر بموجب الأمر رقم : 156/66 المؤرخ في / 18 صفر 1386 , الموافق ل : 8 يونيو 1966 ,المنشور في ج ر العدد رقم : 48 , الصادر يوم : 10 جوان 1966 , و المعدل بالقانون رقم : 22/06 , ج ر , العدد : 84, المؤرخ في : 24ديسمبر 2006 م .

2-قانون العقوبات الجزائري , الصادر بموجب الأمر رقم : 156/66 المؤرخ في : 18 صفر 1386 , الموافق ل : 8 يونيو 1966 , المنشور في ج ر العدد : 49 , و الصادر بتاريخ : 11 جوان 1966 , و آخر تعديل له لغاية 2006 بموجب القانون رقم : 06/23 , المنشور في ج ر , العدد : 71,المؤرخ في : 26 ديسمبر 2006 م .

3-القانون رقم : 2000/03 المؤرخ في : 05 أوت 2000 , و يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية , ج ر عدد : 48 , صادر بتاريخ : 06 أوت 2000 .

3 -القانون رقم : 03/05 المؤرخ في : 2003/07/19 , المتعلق بحقوق المؤلف و الحقوق المجاورة , ج ر , عدد : 44 ' الصادر بتاريخ : 2003/07/23 م .

4 -القانون رقم : 01/08 , المؤرخ في : 23 جانفي 1008 , المعدل و المتمم للقانون رقم / 11/83 المتعلق بالتأمينات الاجتماعية , المنشور في ج ر , العدد رقم : 04 , الصادر بتاريخ : 27 جانفي 2008 م .

5 -القانون : 01/06 المؤرخ في : 2006/02/20 , المتضمن الوقاية من الفساد و مكافحته , ج ر , عدد : 14 , الصادر بتاريخ : 2006/03/08 .

6 -القانون رقم : 04/09 المؤرخ في : 14 شعبان 1430, الموافق ل: 5 غشت 2009 , و المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا ت الاتصال و الإعلام و مكافحتها , ج ر عدد :47 ,صادر بتاريخ :16 أوت 2009 .

7 -الأمر : 02/15 المؤرخ في : 13 جويلية 2015 , و المتضمن تعديل أحكام ق إ ج , المنشور في ج ر , العدد رقم : 40 , الصادر بتاريخ : 23 جويلية 2015 م .

8 _ القانون : 03/15 , المؤرخ في أول فبراير 2015 , و المتضمن عصرنة العدالة ,ج ر , العدد : 6 .

3_ المراسيم :

1 المرسوم الرئاسي رقم : 261/15 المؤرخ في : 08 أكتوبر 2015 , و المتضمن تحديد و تشكيل و تنظيم و كيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الاتصال و الإعلام و مكافحتها , المنشور في ج ر العدد : 53 , الصادر بتاريخ : 8 أكتوبر 2015 م .

2-المرسوم التنفيذي رقم : 348/06 المؤرخ في : 2006/10/05 , المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق .

ثانيا : الـــــــــــــــمراجع

1 -الـــمراجع العـــامة :

1-أحسن بوسقيعة ,الوجيز في القانون الجنائي العام , ط 8 ,دار هومة للطباعة و النشر ,الجزائر ,2009 .

2-نبيل صقر , الوسيط في شرح الأموال , دار الهدى , عين مليلة ,الجزائر , بدون ذكر الطبعة , 2012 .

3_ محمد مروان , نظام الاثبات في المواد الجنائية في القانون الوضعي الجزائري , الجزء الأول , ديوان المطبوعات الجامعية الجزائر , 1999 .

2 -المراجع المتخصصة :

1-أحمد عبد اللاه المراغي , الجريمة الإلكترونية و دور القاضي الجنائي في الحد منها , المركز القومي للإصدارات القانونية , القاهرة , الطبعة الأولى ,2017 .

2-آمال قارة ,الحماية الجزائية للمعلوماتية في التشريع الجزائري , ط 1 ,دار هومة للطباعة و النشر و التوزيع ,الجزائر , 2006 .

3-بلال أمين زين الدين , جرائم نظم المعالجة الآلية للمعطيات الآلية للبيانات في التشريع المقارن و الشريعة الإسلامية , دار الفكر الجامعي , الإسكندرية , ط 1, 2008 م .

4-حنان ريحان مبارك المضحكي , الجرائم المعلوماتية , منشورات الحلبي الحقوقية .لبنان , ط 1 , 2014 م .

5-خالد عياد الحلبي , إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت , دار الثقافة للنشر و التوزيع , الأردن , ط 1 , 2011 م .

6-خالد ممدوح إبراهيم ـ فن التحقيق الجنائي في الجرائم الإلكترونية , دار الفكر الجامعي , الإسكندرية , ط 1 , 2009 م .
7- رشيدة بوبكر , جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن , منشورات الحلبي الحقوقية , ط 1, 2012 م .
8-سعدي سليمة ,و حجازي بلال , جرائم المعلومات و الشبكات في العصر الرقمي ' دار الفكر الجامعي ' الإسكندرية , ط 1 , 2017 م .
9_ عبد الإله أحمد الهلالي , تفتيش نظم الحاسب و ضمانات المتهم المعلوماتي , د .ط , دار النهضة العربية , القاهرة , 1977 .
10-علي حسن محمد طوالبة , التفتيش الجنائي , علم الكتب الحديث , إربد -الأرن , 2004 م .
11-عبد الفتاح بيومي حجازي , مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت , دار الفكر الجامعي , الإسكندرية , ط 1 , 2006 م .
12-علي عدنان الفيل , إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية – دراسة مقارنة , دار الكتاب الجامعي الحديث , الإسكندرية , مصر 2012 م .
13-فتوح الشاذلي , و عفيفي كمال , جرائم الكمبيوتر , منشورات الحلبي الحقوقية ' لبنان , ب. ذ. ط , 2003 م .
14- مصطفى محمد موسى , التحقيق الجنائي في الجرائم الالكترونية , مطابع الشرطة ,القاهرة , ط 1 , 2009 م .
15- مصطفي محمد موسى , التحري في مجتمع المعلومات و المجتمع الافتراضي , ب .د . ن , 2011 م .
16-منير محمد الجنبيهي , و ممدوح محمد الجنبيهي , جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها , دار الفكر الجامعي الإسكندرية , 2004 .
17-ممدوح عبد الحميد عبد المطلب , البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت , دار الكتب القانونية , مصر , 2007 م .
18-نبيلة هبة هروال , الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات , دار الفكر الجامعي , الإسكندرية , مصر , 2007 م .
19-هدى قشوش , جرائم الحاسب الإلكتروني في التشريع المقارن , دار النهضة العربية القاهرة , 1992 م .
20-هلال عبد الله , تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي – دراسة مقارنة , دار النهضة العربية , القاهرة , 2006 م .

ثالثا : الرسائل العلمية

1 -أحمد موسود مريم ,آليات مكافحة جرائم تكنلوجيا الإعلام و الاتصال في ضوء القانون : 04/09 ,رسالة ماجستير ,قاصدي مرباح ,جامعة ورقلة ,2013/2012 .

2 -بدري فيصل , مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي ,أطروحة دكتوراه ,جامعة الجزائر يوسف بن خدة ,كلية الحقوق ,2017/**2018 .**

3 -براهيمي جمال ,التحقيق الجنائي في الجرائم الإلكترونية , أطروحة دكتوراه ،جامعة مولود معمري تيزي وزو ,2018 .

4 -سعيداني نعيم , أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري , مذكرة ماجستير , كلية الحقوق جامعة باتنة , 2003 .

5 -فيصل مساعد العنزي ,أثر الإثبات بوسائل التقنية الحديثة على حقوق الإنسان , رسالة ماجستير , قسم العدالة الجنائية , جامعة نايف العربية للعلوم الأمنية , الرياض , 2007 .

6 -قادري سارة , أساليب التحري الخاصة في (ق أ ج), مذكرة ماجستير , دامعة قاصدي مرباح ورقلة , كلية الحقوق و العلوم السياسية , 2014/2013 .

رابعا : المقالات العلمية و التقارير

1-بن فريد محمد , الدليل الجنائي الرقمي و حجيته أمام القضاء الجزائري , "مقال في المجلة الأكاديمية للبحث القانوني " الصادر عن كلية الحقوق ة العلوم السياسية , جامعة عبد الرحمن ميرة , بجاية , 2014 .

2 _عبد الرحمان حملاوي , دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية , بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة , 16 و 17 نوفمبر 2015 , كلية الحقوق ' جامعة بسكرة , الجزائر .

3 _ ممدوح عبد الحميد عبد المطلب , " إستخدام البروتكول (T C P Li L i p) في بحث و تحقيق الجرائم على جرائم الكمبيوتر " ورقة بحثية مقدمة للمؤتمر العلمي الأول المنعقد في دبي يومي : 26 _ 28 نيسان 2003 , دبي .

4_ طارق محمد الجملي , الدليل الرقمي في مجال الإثبات الجنائي , ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية و القانون " , المنعقد في الفترة من : 28 _29 /10 / 2009 , أكادمية الدراسات العليا , طرابلس

الملخص:

تعد الجرائم المعلوماتية من الأنماط الإجرامية الحديثة التي أفرزتها تقنية تكنولوجيا الإعلام و الاتصال , و هي تختلف تماما عن الجرائم التقليدية في طبيعتها و خصائصها و أساليب ارتكابها ووقوعها في بيئة الكترونية و خصوصية مرتكبيها , مما جعل منها ظاهرة غريبة عن قواعد القانون الجزائي التقليدي بشقيه الموضوعي و الإجرائي , و عليه فكل محاولة لإخضاع هذا النمط من الإجرام المعلوماتي لأساليب التحري و التحقيق و قواعد الإثبات التقليدية تبوء بالفشل لقصورها عن مواجهة الصعوبات و التحديات التي تطرحها الجريمة المعلوماتية .

و لكن نموها بشكل ملفت للانتباه و تطورها المستمر بتطور تقنية المعلومات و لا سيما استخدام شبكة الانترنت , أدى بالدول لترشيد نصوصها الإجرائية التقليدية و استحداث نصوص أخرى تتلاءم و خصوصية الإجرام المعلوماتي .

فما مدى فعالية المواجهة الإجرائية للنمط المتجدد و المتطور للجرائم المعلوماتية في التشريع الجزائري ؟ و هو ما حاولنا الإجابة عنه من خلال هذه المذكرة .

Summary:

The cybercrime is a modern criminal pattern produced by the technique of ICT (information and communication technology) . It is completely different from traditional crimes in terms of nature, characteristics, methods of committing it and in the fact of its occurrence in an electronic environment and the particularity of its perpetrators as well. This makes it a phenomenon that is strange to the rules of traditional penal code. Therefore, any attempt to subdue this particular type of crime to the traditional methods of investigation and rules of evidence fails because of the difficulties and challenges posed by the cybercrime.however, cybercrime growth is clearly remarkable, going through the development of information technology and in particular the use of the Internet, it has made states rationalise their traditional procedural texts and develop special texts adapted to the cybercrime.

How effective is the procedural response to the renewed and evolving pattern of cyber crime in Algerian legislation? It is the problematic that we have tried to answer through this thesis.