جامعة قاصدي مرباح ورقلة
كلية الحقوق و العلوم السياسية
قسم الحقوق

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي

الميدان: الحقوق و العلوم السياسية

الشعبة: الحقوق

التخصص: قانون جنائي

إعداد الطالبة: يومايلة ابتسام

بعنوان

مناهج التحقيق الجنائي في ظل تفشي الجريمة الرقمية

نوقشت و أجيزت بتاريخ :.....

أمام اللجنة المكونة من السادة:

الاسم واللقب	الرتبة	المؤسسة	الصفة
أ.د/ شنين صالح	أستاذ التعليم العالي	جامعة ورقلة	رئيسا
د/ طيبي الطيب	أستاذ محاضر ب	جامعة ورقلة	مشرفا مقررا
د/بن عمر ياسين	أستاذ مساعد أ	جامعة ورقلة	مناقشا

السنة الجامعية 2021/2020

بسم الله الرحمن الرحيم

الإهداء

اهدي هذا الجهد المتواضع إلى مثلي الأعلى في الحياة أبي الغالي أطال الله في عمره

إلى منبع الحب و الحنان إلى أمي الغالية أطال الله في عمرها

إلى رفيق دربي و شريك حياتي زوجي الغالي.... إلي نور عيناي أياد و جاد

إلى إخوتي و أخواتي الأعزاء و كل عائلتي

إلى كل أصدقائي و زملائي

إلى كل من يتصفح أوراق المذكرة و يستفيد من المعلومات الموجودة فيها.

ابتسام.

كلمة شكر

من باب قوله تعالى " لئن شكرتم لأزيدنكم " سورة إبراهيم الآية 07.

الحمد و الشكر لله الذي وفقنا و أنار لنا درب العلم و المعرفة في انجاز هذا العمل

اسمي عبارات الشكر و الامتنان إلى الذي شجعني و وقف وراء هذا العمل بكل مجهوداته و نصائحه القيمة التي أنارت طريقنا و قومت مسارنا و كانت عونا لنا في إتمام هذا البحث

إلى رمز العلم و العمل و الالتزام أستاذي المشرف الدكتور طيبي الطيب

كما أتوجه بجزيل الشكر إلى من مد لي يد العون من قريب أو من بعيد في انجاز هذا العمل.

إلى كل الأساتذة الكرام في جامعة ورقلة و مسؤولين و إطارات الذي بدلوا جهودا كبيرة في فتح الأبواب لاستكمال مسيرتي العلمية

جزيل الشكر و العرفان إلى اللجنة الموقرة التي أعطتنا من وقتها الثمين و قبلت مناقشة هذا البحث المتواضع

كن عالما....فان لم تستطع فكن متعلما فان لم تستطع فأحب العلماء فان لم تستطع فلا تبغضهم

ابتسام.

قائمة المختصرات

ق.ا.ج : قانون الإجراءات الجزائية.

ج ر : الجريدة الرسمية.

ط : الطبعة .

ص: الصفحة .

الخ : الى آخره.

مقدمة

مقدمة:

ان التطور الهائل الذي شهدته كل من مجال تقنية المعلومات و مجال الاتصالات والاندماج المذهل الذي حدث بينهم فيما بعد كان المحور الأساسي الذي قامت عليه تقنية المعلومات إذ أصبحت جميع القطاعات المختلفة تعتمد في آداء عملها بشكل أساسي على استعمال الأنظمة المعلوماتية لما تتميز به من عنصرين السرعة و الدقة في تجميع المعلومات و تخزينها و معالجتها و من ثم نقلها و تبادلها بين الافراد و الشركات والمؤسسات المختلفة داخل الدولة الواحدة او بين عدة دول.

فبات يلق على هذا العصر عصر المعلومات فمنذ وقت ليس ببعيد كان كم من المعلومات المتولدة من التفاعلات البشرية محدودة الى حد كبير و لم يشكل حجمها أي مشكل امام تجميعها و تخزينها و إعادة استرجاعها الا انه و مع تقدم البشرية و تزايد معارف الانسان و علومها بدأ كم المعلومات في التزايد و التكاثر، و صارت الطرق التقليدية لتجميع و تنظيم هذه المعلومات عاجزة عن تلبية احتياجات المستفيدين منها بكفاءة و فعالية و اصبح من اللزوم اللجوء الى أليات علمية و تقنية متطورة لمواجهة هذه الظاهرة، كما ظهرت الحاسبات الالكترونية و مستحدثات تقنية كأقراص الفيديو الرقمية و أقراص الليزر و وسائل الاتصال ، ذلك من اجل تسهيل التحكم في المعلومات و معالجتها و استرجاعها .

و في مرحلة لاحقة من مسار عصر تقنية المعلومات ثم التوصل الى فكرة الربط بين أجهزة الاعلام الآلي و وسائل الاتصال، الامر الذي اثر على ظهور شبكات المعلومات ولعل اهمها على الاطلاق هي شبكة الانترنيت ثم استتبع اتساع و نماء كل من تكنولوجية الاتصال و الحاسبات من جهة و البرمجة من جهة أخرى و الاندماج التي حصل بينهما الى الوصول الى استحداث تقنية المعالجة الالية للمعطيات و تضاعفت أهمية هذه التقنية والاعتماد عليها في نقل و تبادل المعلومات و الصوت و الصورة عبر انحاء العالم لما تتميز من شمول و سعة محتواها و ما توفره من مال و جهد و وقت، و أصبحت بذلك نظم المعالجة الالية للمعطيات بسبب التقنيات التي تقوم عليها و المتمثلة في الحواسيب والشبكات المعلوماتية اكثر انتشارا في كل القطاعات وز المجالات كالصناعة و التجارة و غيرها .

و لكن على الرغم من المزايا الهائلة التي تحققت كل يوم بفضل هذه التقنية على جميع الأصعدة و في شتى ميادين الحياة المعاصرة الا ان هذه الثروة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية جراء الاستخدام السيء و غير المشروع مما الحق الضرر بمصالح الفرد و الجماعة على حد سواء ، و على ضوء ذلك فان هذه الظاهرة الاجرامية التقنية اثارت العديد من المشكلات في نطاق قانون الإجراءات الجزائية التي وضعت نصوصه لتحكم الإجراءات المتعلقة بالجرائم التقليدية . لا نوجد صعوبات كبيرة في اثباتها و التحقيق فيها.

و الجزائر باعتبارها واحدة من الدول التي مسها او تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان إيجابيا او سلبيا فهي أيضا معنية بالمكافحة فكان لابد من إيجاد اطار قانوني مناسب لملءw الفراغ الاجرائي ، بذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية و الجرائم المعلوماتية عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل و إجراءات خاصة تتماشى و طبيعة الجرائم المستحدثة و منها الجريمة المعلوماتية و منها إجراءات تطبق فقط على الجريمة المعلوماتية التي تم النص عليها في القانون 09-04.

هذه الجرائم الذكية تنشا و تحدث في بيئة خاصة و يقترفها اشخاص متميزون مما يسبب خسائر كبيرة على جميع المستويات الاقتصادية و الاجتماعية و الثقافية و الأمنية فهي قد تستهدف فضح الاسرار الشخصية و القذف او التشهير بالشركات أو الأشخاص يقصد الاضرار بالسمعة الشخصية او المالية او بداعي الانتقام كما قد تكون سرقة او فسيل أموال أو تحويلها من حساب لآخر و قد تستدف تدمير المعلومات او الاحتيال وتزوير البطاقات الشخصية التي زاد خطر انتشارها نظرا لصعوبة التوصل الى مرتكبيها.

غير انه لا ينبغي ان يزعجنا هذا التطور المتسارع في وسائل ارتكاب الجرائم طالما ان العلوم الحديثة وفرت أيضا التقنيات المناسبة لمواجهة التطور الاجرامي ، كما يجب على القضاء و أجهزة الشرطة ان تنهض بإمكاناتها العلمية و الفنية و الإرتقاء بالكادر البشري بالقدر الذي يؤهلها لمواجهة مستجدات الجريمة و كيفية التعامل معها شكلا و موضوعا خاصة في مراحل التحقيقات الأولية و جمع الاستدلالات و استخدام التقنيات العالية و الذكاء الصناعي و المعلومات الرقمية في التخطيط و التنفيذ ، و بصفة عامة استخدام طرق

و أساليب حديثة من اجل الكشف و اثبات هذا النوع من الجرائم و هو ما عمل عليه المشرع الجزائري حين ادرج نصوص و قواعد قانونية توسع من الاختصاص القضائي لوكلاء الجمهورية و قضاة التحقيق و تعزيز صلاحيات الضبطية القضائية و وضع اليات حديثة للبحث و التحري للوصول للدليل الرقمي.

و على ضوء ما تقدم نجد ان الإشكالية التي يجب معالجتها من خلال هذه الدراسة هي :

فيما تتمثل مناهج التحقيق المتبعة في الجريمة الرقمية .

و على ضوء الإشكالية الرئيسية يمكن طرح جملة من التساؤلات الفرعية المتمثلة في:

ماهي المبادي الأساسية للتحقيق الجنائي في الجرائم الرقمية؟

ماهي الأجهزة المكلفة بالتحقيق في الجرائم الرقمية؟

ماهي الاليات الاجرائية المتبعة في الكشف عن الجرائم الرقمية ؟

لأجل هذه الأسئلة و غيرهاو نتيجة لخطورة و انتشار ظاهرة الجريمة الرقميةارتأينا تناول هذا الموضوع في ظل القوانين المستحدثة من طرف المشرع القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

و تتجلى أهمية هذا البحث أساسا في كون الجرائم المعلوماتية جرائم جديدة و بالتالي لا يمكن تطبيق الاجراءات التي تطبق على الجرائم التقليدية ، و بالتالي خصوصية تعامل جهات التحقيق مع هذا النوع من الجرائم كون التحقيق فيها يتن في وقت معاصر لوقوع الجريمة أو اثر ذلك مباشرة مما يتيح فرصة التنقيب و جمع ادلتها ذات الطابع الخاص في الوقت الملائم و أي تأخير قد يؤدي الى ضياع الدليل و افساده.

إن اختيار موضوع مناهج التحقيق الجنائي في الجرائم الرقمية يرجع في حقيقة الامر الى أسباب شخصية و أسباب موضوعية .

فالأسباب الشخصية تكمن في اهتمامي بمجال الجريمة المعلوماتية و ما يلقاها من جرائم و كذا اجراءات التحقيق الخاصة فيها بالإضافة الى انه موضوع جديد و رغبتي

الشديدة في الغوص في هذه الإجراءات و الوقوف على حقيقة التعامل مع الجريمة المعلوماتية من الناحية الإجرائية.

و الأسباب الموضوعية تكمن فيما طرحه موضوع مناهج التحقيق الجنائي في الجرائم الرقمية من إشكاليات قانونية و التي لابد من الوقوف نظرا لحداثة الموضوع من الجانب الموضوعي لتجريم الأفعال و الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات و القواعد الإجرائية الحديثة التي جاء بها قانون الإجراءات الجزائية و كذا قانون 09-04المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

و قد واجهنا خلال عملنا هذا بعض الصعوبات تمثلت في نقص المراجع المتخصصة في التحقيق الرقمي و في الإجراءت المستحدثة و مناهج التحقيق في الجرائم الرقمية بالرغم من الكم الهائل من المراجع التي تناوبت الجرائم الرقمية بصفة عامة ، اضافة الى صعوبة البحص في هذا الموضوع لاتصاله بالجانب العلمي التقني الذي يتعلق بالمعطيات الآبية.

و للإجابة عل الإشكالية المطروحة أعلاه و الأسئلة الفرعية اتبعنا المنح التحليلي الوصفي كونه الأنسب لمثل هذه الدراسات من هلال تحليل مختلف المفاهيم القانونية المتعلقة بالموضوع و شرح عدة مواد قانونية من قانون الإجراءات الجزائية و القانون 09-04 و المرسوم الرئاسي 15-261 و قد اعتمدنا لدراسة موضوعنا الخطة التالية :

الفصل الأول نعالج فيه الاطار المفاهيمي للتحقيق الجنائي في الجرائم الرقمية (مبحث اول) و من هو المحقق في الجرائم الرقمية (مبحث ثاني).

و الفصل الثاني تطرقنا فيه الى اليات وأساليب التحقيق الجنائي في الجرائم الرقمية من خلال مبحثين عرضنا في (المبحث الأول) الى الإجراءات العامة للتحقيق الجنائي في الجرائم الرقمية و في (المبحث الثاني) الإجراءات الخاصة بالتحقيق الجنائي في الجرائم الرقمية .

الفصل الأول:

ماهية للتحقيق الجنائي في الجرائم الرقمية

الفصل الأول: ماهية للتحقيق الجنائي في الجرائم الرقمية

يشهد العالم الحديث تحديات كبيرة و متزايدة نتيجة التطورات السريعة في شتى الميادين و على وجه الخصوص الميدان العلمي و التكنولوجي خلال الربع الأخير من القرن الماضي حيث اصبح الحاسب الألي ركيزة أساسية في عصرنا الذي تطور دوره بحيث تعدى اجراء العمليات الحسابية المعقدة ليجعل العالم قرية صغيرة لا يعترف فيها بالحدود الجغرافية و ذلك من خلال استغلال شبكات الانترنت غير ان هذه التقنية لم تسلم من الاستغلال غير الشرعي لها مما أدى الى ظهور نوع جديد من الاجرام يسمى الاجرام المعلوماتي او الرقمي و التي أدت بالاشخاص الى ارتكاب جرائمهم بطرق و وسائل جديدة دون ترك اثر لهم و دون معاناة الامر الذي حتم تطوير الأنظمة و التعليمات و الجهات الأمنية المختصة بمعالجة هذه القضايا و اتباع طرق و وسائل تحقيق متطورة تتميز بالطابع العلمي لاستكشافها .

و من جهة أخرى فان التحقيق عموما يعتمد على فطنة المحقق و قوة ملاحظته و ذكائه و سرعت البديهة لديه و ان يسعى بكامل جهده في البحث عن الجريمة و متابعتها و التنقيب على الأدلة وصولا لإظهار الحقيقة، و لذلك سوف نتطرق في هذا الفصل الى الاطار المفاهيمي للتحقيق في الجرائم الرقمية في (المبحث الأول) و نتعرض الى أجهزة التحقيق الجنائي في الجرائم الرقمية في (المبحث الثاني)

المبحث الأول :الاطار المفاهيمي للتحقيق الجنائي في الجرائم الرقمية

يعد التحقيق اجراء من اهم الإجراءات التي تتخذ بهد وقوع الجريمة لما له من أهمية في التثبت من حقيقة وقوعها و إقامة الاسناذ المادي على مرتكبها بادلة الاثبات على اختلاف أنواعها فهو الضبط القضائي على الجاني على ادانته او براءته ، و الثابت

ان إجراءات التحقيق تمر بثلاث مراحل تهديف جميعها الى ضبط الجاني و تقديمه امام جهات التحقيق بادلة اتهام و بعدها الى جهات الحكم و هذه المراحل تتمثل في[1] :

1-مرجلة جمع الاستدلالات : بواسطة الضبطية القضائية المختصة بالبحث في الجرائم و مرتكبيها .

2-مرحلة التحقيق الابتدائي : الذي يثوم به قاضي التحقيق او النيابة العامة لتحريك الدعوى الجنائية او حفظ التحقيقات لعدم كفاية الدليل.

3-مرحلة التحقيق النهائي : بجلسة المحاكمة .

و لذلك سنحاول تقسيم هذا المبحث الى مطلبين نتناول في (المطلب الأول) المبادئ الأساسية للتحقيق الجنائي في الجرائم الرقمية و (المطلب الثاني) أساليب التحقيق الجنائي في الجرائم الرقمية .

المطلب الأول : الضوابط الأساسية للتحقيق الجنائي في الجرائم الرقمية

يتطلب التعرف على الضوابط الأساسية للتحقيق غي الجرائم الرقمية الى تبيان مفهوم التحقيق الجنائي في هذه الجرائم (الفرع الأول) و كذا عناصره (الفرع الثاني) و ضمانات المتهم في مرحلة التحقيق الجنائي (الفرع الثالث) و ذلك على النحو التالي :

الفرع الأول: مفهوم التحقيق الجنائي في الجرائم الرقمية

و يتجلى هذا المفهوم من هلال تعريف التحقيق الجنائي في الجرائم الرقمية و التطرق الى دراسة خصائص هذا التحقيق .

أولا: تعريف التحقيق الجنائي في الجرائم الرقمية

يهدف التحقيق الى جمع الأدلة و التنقيب عنها

[1] انظر عبد الله بن حسين ال حجرافالقحطاني ، تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية ، رسالة مقدمة لنيل شهادة الماجستير ، قسم العلوم الشرطية جامعة نايف للعلوم الأمنية الرياض 2014 ، ص 20 .

1 – تعريف التحقيق لغة : التحقيق مأخوذ من حقق يحقق تحقيقا حقق الظن بالله صدقه الامر احكمه– مع فلان – في قضيته أخذ رايه فيها[1]

2 – تعريف التحقيق اصطلاحا : عرف التحقيق بمعناه العام انه اتخاذ جميه الإجراءات و الوسائل المشروعة التي توصل الى كشف الحقيقة و ظهورها[2].

و قد عرف التحقيق في اصطلاح الفقه الإسلامي بانه اثبات المسالة بدليلها.

و في اصطلاح شراح القانون تعددت التعريفات الفقهية للتحقيق الابتدائي الا انه على الرغم من تعددها فهي لا تخرج عن تعريفه بانه مجموعة من الإجراءات القضائية تمارسها سلطات التحقيق بالشكل المحدد قانونا[3] ، بغية التنقيب عن الأدلة في شان جريمة [4]ارتكبت و تجميعها ثم تقديرها لتحديد مدى كفايتها في إحالة المتهم الى المحاكمة او الامر بالا وجه للمتابعة .

و هناك من عرفه بانه مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط و الأوضاع المحددة قانونا بهدف التنقيب عن الأدلة و تقديرها و الكشف عن الحقيقة في شان جريمة ارتكبت لتقرير لزوم محاكمة المدعي عليه او عدم لزومها.

و قد عرف أيضا بانه التحري و التدقيق في البحث تلمسا لمعرفة الجاني في جناية ارتكبت او شرع في ارتكابها و كذلك في ظهور ارتكابها ، و من أولى متطلبات الأساسية استعمال الوسائل المطروحة للتحقيق.

3 – تعريف التحقيق في الجرائم الرقمية :

---

[1]علي بن هادية ، لحسن البليش ، الجيلالي بن الحاج يحي ، القاموس الجديد للطلاب ، الشركة الوطنية ، الشركة التونسية ، الجزائر ، تونس ، ط1 ، 1979 ، ص 286 .

[2] عمر بن إبراهيم بن حماد العمر ، إجراءات الشهادة في مرحلتي الاستدلال و التحقيق الابتدائي في ضوء نظام الإجراءات السعودي ، مذكرة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، 2007 ص 22 .

يختلف التحقيق في الجريمة الرقمية عن التحقيق في الجريمة العادية من حيث الإجراءات و ذلك لحداثة هذه الجريمة و مهارة مرتكبيها في الاجرام و محو الأدلة.

يبدا التحقيق في الجريمة المعلوماتية من خلال تلقي المحقق البلاغ عن وقوع الجريمة مرورا بالاجراءات التي يتخذها المحقق في كشف غموضها و ضبط الفاعل و اسناد الاتهام قبله و تقديمه للمحاكمة أما العوهد الفنية فهي تلم التي تحكم المحقق منذ تلقيه البلاغ حتى ضبط المتهم و تقديمه للمحاكمة بعد اسناد الاتهام اليه .

فالتحقيق الجنائي في الجريمة الرقمية اذن هو ذلك العمل القانوني الذي يقوم به المحقق لكشف الجريمة الالكترونية أو الرقمية و نسبتها الى الفاعل .

ثانيا : خصائص التحقيق الجنائي في الجريمة الرقمية

– الجرائم التي ترتكب بواسطة الحاسوب ترتكب في الخفاء و ينصب الاعتداء فيها على معطيات الحاسوب المخزنة و المعلومات المنقولة عبر نظم و شبكات المعلومات و عليه فالتعامل مع مسرح الجريمة الالكترونية و التحفظ على الأدلة و مناقشة الشهود و غيرها تعتبر من اساسيات التحقيق[1]

– سرعة انجاز التحقيق للمحتفظة على الأدلة الجريمة و اثارها دون ان تمس او تمحى و بمنع من ضياعها كون ان المجرم الالكتروني يتميز بالذكاء فبديه القدرة على اتلاف و تشويه و إضاعة الدليل الالكتروني الرقمي بشكل سريع في وقت قصير جدا بسبب ان الأدلة التي تخلفها الجريمة الالكترونية فير ملموسة .

– الجريمة الالكترونية ترتكب في بيئة بيانية مما يسمح باخفاء معالم الجريمة و ذلك لغياب الدليل المرئي الممكن بالقراءة فهمه.

الفرع الثاني : عناصر التحقيق الجنائي في الجرائم الرقمية

[1] خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنيث، دار الثقافة ، الأردن ، ط 1 ، 2011 ، ص 183 ، 147 .

اثناء القيان بالتحقيق في الجرائم الرقمية فالمحقق يقع عليه استظهار الركن المادي و المعنوي للجريمة و تحديد مكان و زمان حدوثها لخصوصية محل هذه الجريمة .

أولا : تبيان الركن المادي للجرائم الرقمية

ان السلوك المادي في جرائم الانترنيت يتطلب وجود بيئة رقمية و اتصال بالانترنيت و يتطلب أيضا بداية هذا النشاط و الشروع فيه و نتيجته ، لكن ليس كل جريمة تستلزم وجود اعمال تحضيرية[1] ، و في واقع الحال يصعب الفصل بين العمل التحضيري و البدء غي النشاط الاجرامي في نطاق الجريمة الالكترونية ، حتى و لو كان القانون لا يعاقب على الاعمال التحضيرية الا ان الامر يختلف في مجال تكنولوجيا المعلومات ،فشراء برامج اختراق و برامج فيروسات و معدات لفك الشفرات و كلمات مرور تمثل جريمة في حد ذاتها.

ثالثا : تحديد محل الجرائم الرقمية

انه بالنظر الى الأهمية التي ينبغي ان يوصف بها الدور الذي يؤديه نظام الحاسي الاليلاتمام النشاط الاجرامي في الجرائم المعلوماتية فان ذلك يؤدي الى اختلاف محل الجريمة بحسب الزاوية التي ينظر اليها و الدور الذي يلعبه هذا الحاسب ذاته ، و هنا نفرق بين ثلاث حالات :

1 – وقوع الجريمة على المكونات المادية للنظام المعلوماتي

ان الاعتداء على المكونات المادية للنظام المعلوماتي يتحقق ان كان الحاسوب والأجهزة الملحقة به من معدات و كابلات و شيكات الربط و الات الطباعة محلا للاعتداء ، و تقوم الجريمة في هذه الحالة بإتيان أي فعل مادي من شانه اخراج الحاسوب من حيازة مالكه و إدخاله غي حيازة شخص اخر او اتلاف الجهاز و تدميره و غير ذلك من الأفعال المجرمة.

[1] خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي ، الإسكندرية ، ط 1 ، 2009، ص 52 .

2 – وقوع الجريمة باستعمال أنظمة الحاسب الالي:

في هذه الحالة لا يكون الحاسب محلا او موضوعا للجريمة و انما الجانب الحاسب في ارتكاب الجرائم ، فما هو اذن الا وسيلة لارتكابها ن و محل هذه الجرائم يختلف بحسب الشيء الذي ينصب عليه سلوك الفاعل و الذي يشكل محلا للحق او المصلحة المحمية .

3 – وقوع الجريمة على المكونات المعنوية للنظام المعلوماتي :

و تتحقق هذه الحالة عندما تكون مكونات الحاسب غير المادية المتمثلة في المعلومات بكل صورها من البينات و البرامج المخزنة في ذاكرة الحاسب محلا للاعتداء كان يتم سرقتها او اتلافها او تزويرها و العبث بها و غير ذلك من الافعال غير المشروعة ، و ترتيبا عليه فيبقى في النهاية ان تكون المعلومة بمفهومها الواسع[1] هي وحدها محلا للجريمة الالكترونية.

الفرع الثالث : ضمانات المتهم في مرحلة التحقيق الجنائي في الجرائم الرقمية

ان الهدف من التحقيق الجنائي هو تحقيق العدالة لجميع اطراف المجتمع و كذلك بالنسبة للمحق فانه يستهدف تحقيق الحماية الكاملة له في حال اتخاذ الإجراءات الصحيحة و توافر كافة الضمانات يءدي الى شعور الجميع بالاطمئنان و تتمثل اهم هذه الضمانات في :

أولا : سرية التحقيق بالنسبة للجمهور

تعتبر من اهم الضمانات التي اكدتها معظم الدول كونها تهدف الى عدم التشهير بالمشتبه فيه من قيل المجتمع قبل ادانته و الحكم عليه الامر الذي يؤثر سلبا على نفسيه لاسيما بعد الحكم ببراءته ، إضافة الى إيجابية ذلك بالنسبة للمدامع بمنع انتشار الشائعات فيه ، و قد يرد على هذه القاعدة العامة استثناءات تتمثل في انه يمكن للمحقق

[1] و تشمل المعلومة بمفهومها الواسع البيانات و المكونات المنطقية كالبرامج و التطبيقية و برامج التشغيل.

في حالة الضرورة و الاستعجال ان يباشر إجراءات التحقيق في غيبة الخصوم[1] لذلك وجب السماح للمحامي بالاطلاع على أوراق التحقيق عند طلبها لان من حق المتهم الاستعانة بمحامي للدفاع عن نفسه.

ثانيا : علانية التحقيق بالنسبة للخصوم

على خلاف مبدا السرية المقرر بالنسبة للجمهور فان المشرع اقر علانية التحقيق بالنسبة لأطراف الدعوى العمومية و ذلك من اجل احاطة المتهم بضمانته و كيفية سير التحقيق في جميع مراحله .

ثالثا :حق المتهم في محاكمة عادلة و سريعة

و ذلك بإنجاز و اتخاذ كل إجراءات التحقيق بصورة سريعة خاصة فيما يتعلق بمدة الحيس و هي محددة في المواد 309 مكرر و مايليها.

رابعا : حق المتهم في الاستعانة بمحام

حق الدفاع من المبادئ الأساسية و قد كفله القانون للمتهم حتى و لو لم تكن له القدرة المالية و ذلك لتوكيل محام للدفاع عنه ، فحضور المحامي مع موكله اثناء التحقيق ضمانة له لسلامة الإجراءات و لعدم استعمال الوسائل غير الجائزة قانونا.

المطلب الثاني : وسائل التحقيق الجنائي في الجرائم الرقمية

التحقيق الجنائي عموما هو علم يخضع لما يخضع له باقي العلوم الأخرى فله قواعد ثابتة و راسخة يدونها ما كان ليتمتع التحقيق بتلك الصفة ، و هذه القواعد اما ان تكون قانونية و اما فنية ، فالأولى لها صفة الثبات التشريعي لا يملك المشرع ازاءها الا شيئا سوى الخضوع و الامتثال ، اما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته و فطنته و مهارته[2] ، ففكر المحقق الجنائي في الجريمة الالكترونية يجب ان

---

[1] المادة 101 من ق ا ج الصادر بموجب الامر رقم 66-153 المؤرخ في 08-06-166—966 المعدل و المتمم بالقانون رقم 04-14 المؤرخ في 10-11-2004 منشور بالجريدة الرسمية في 10-06-1966 ع 48.

[2] خالد ممدوح إبراهيم ن المرجع السابق ، ص 56.

يكون متطورا لمواجهة المجرم الالكتروني ، و في ذلك فهو يحتاج لوسائل مادية و إجرائية لذلك فنحاول من خلال هذا المطلب التطرق الى أسلوب التحقيق الجنائي في الجرائم الرقمية (فرع أول) و الى الوسائل المادية للتحقيق (فرع ثاني) ثم الوسائل الإجرائية (فرع ثالث).

الفرع الأول :أسلوب التحقيق الجنائي في الجرائم الالكترونية

التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق و تؤدي الى اكتشاف الجريمة و معرفة مرتكبيها تمهيدا لتقديمهم للمحاكمة و قد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمضاهاة البصمات أو برمجية كتحديد كيفية الدخول الى المعطيات المخزنة في النظام المعلوماتي .

و الهدف من التحقيق الابتدائي هو التأكد أولا من وقوع جريمة يعاقب عليها القانون و من ثمة معرفة نوع هذه الجريمةو من هو الجاني و من هو المجني عليه و كذا معرفة وقوعها و ما هي الوسائل التي استعملت في ارتكابها ، و يكون ذلك في لجريمة المعلوماتية وفقا لمنهج تحقيقي يختلف عن غيره بالنسبة للجرائم الأخرى و يتمثل هذا المنهج في تحديد خطة عمل و تكوين فريق متكامل .

أولا : وضع خطة عمل التحقيق

يبدا المحقق عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه ، و تحديد الفريق الفني اللازم للقيام بمساعدته في اعمال التحقيق و ذلك على النحو التالي :

1 – وضع الخطة المناسبة و التي لا تبدا الا لعد معاينة مسرح الجريمة و التعرف على أنظمة الحماية و تحديد مصدر الخطر و وضع التصورات الكفيلة للتصدي للجريمة،

و يتم التخطيط للتعامل مع حوادث الحاسب الالي و شبكات الانترنيت على ثلاث مستويات مختلفة يبنى كل مستوى منها على الآخر[1].

أ –تخطيط استراتيجي :

و هو تخطيط بعيد المدى يهتم بحماية البنية التحتية لشبكات الحاسوب الوطنية ، من خلال تحديد مصادر الهطر المحتملة التي قد تمثل تهديدا لها و يهتم بوضع تصورات على درجة من المرونة تكون كفيلة بالتصدي لهذا النوع من الجرائم قبل وقوعها و ضبطها و الحد من آثارها في حال وقوعها ، و يتم هذا التخطيط على مستوى واضعي السياسات الأمنية . حيث يهدف بشكل عام الى منع هذا النوع من الجرائم من الوقوع داخل إقليم الدولة ، و الحد من قابلية الحواسب و الشبكات الوطنية من التعرض للهجوم و من ثم السيطرة على الحوادث و ضبطها و الحد من اثارها.

و من اهم ما يميز هذا النوع من التخطيط انه يضه الخطوط الاسترشادية التي تسترشد بها الجهات المختلفة ذات العلاقة في وضع خطط التعامل مع هذا النوع من الجرائم كما يحدد الآليات اللازمة لتنفيذ الخطة.

ب– تخطيط تكتيكي :

ينبثق من الخطة الاستراتيجية و يتم على مستوى الجهات الرسمية و غير الرسمية التي لها علاقة بتقنية المعلومات و يدعم اهداف و غايات الخطة الاستراتيجية للتعامل مع جرائم الحاسوب و الانترنيت ، و يمتاز بان له طابع تفصيلي أكثر من التخطيط الاستراتيجي ، و الخطط التكتيكية الخاصة بالتعامل مع جرائم الانترنيت يجب ان تتضمن إجراءات مسبقة التحديد على درجة عالية من التفصيل و الوضوح للتحقيق في هذه الجرائم.

ج – خطة العمل :

[1]حسين بن سعيد الغافري ، التحقيق ، جمع الأدلة في الجرائم المتعلقة بشبكات الانترنيت ، موقع المنشاوي للدراسات و البحوث على الموقع WWW.minshawi.com اطلع عليه بتاريخ 11-02-2018 ص 6 .

و يقصد به التخطيط الذي يقوم به المحقق لتحديد الأسلوب الأمثل في التعامل مع حادث بعينه ، و ذلك في الاطار العام للإجراءات الواردة في الخطة التكتيكية و بما يتناسب مع خصوصية ظروف و ملابسات الحادث .

2 – مرتكزات خطة العمل :

نجد من اهم الأمور التي يجب على المحقق اخدها بعين الاعتبار كمرتكزات تساعده في تحديد خطة العمل المناسبة للتحقيق في أي جريمة من الجرائم الرقمية و الانترنيت .

أ – حجم و نوع الحادث الذي يكون المحقق بصدد التحقيق فيه و يرتبك يه تحديد حجم و نوع فريق التحقيق ، فجرائم الانترنيت منها الصغير و منها الكبير و لكل جريمة مهما كان حجمها ، طبيعتها الفنية الخاصة التي تفرض على أعضاء فريق التحقيق امتلاك معارات فنية خاصة تعتبر ضرورية للتعامل مع هذا النوع من الجرائم ، و هو امر يجب مراعاته عند اختيار أعضاء الفريق.

ب – بعض الظروف المحيطة بالحادث تمثل عوامل مهمة يجب مراعاتها عند وضع خطة العمل لما يترتب عليها من قرارات على درجة كبيرة من الأهمية تتعلق بالتحقيق ، و من هذه العوامل :

–مدى أهمية الأجهزة الحاسوبية و الشبكات المتضررة لعمل المنظمة أو المؤسسة

–مدى حساسية البيانات التي قد تكون محل الجريمة الحاسوبية .

–المتهمون المحتملون.

–اطلاه الراي العتم على الجريمة أم لا .

مستوى الاختراق الأمني الذي تسبب فيه الجاني.

–مستوى المهارة الفنية التي يتمتع بها الجاني.

ج- كبيعة مسرح الجريمة تفرض الأسلوب الأمثل للتفتيش بحثا عن الأدلة التي تكون موجودة فيه و الذي يعتبر من اهم خطوات عملية التحقيق و عدم نجاح المحقق في تحديد هذا الأسلوب و قد يؤي الى عدم الحصول على اية نتائج أو الحصول على كم كبير من النتائج التي لا فائدة منها ، فقائد فريق التحقيق مسؤول عن تحديد حجم المهمة و نوع الأدلة التي يتم البحث عنها بحسب نوع الجريمة ، و كذلك تحديد انسب الطرق لتنفيذ عملية التفتيش و ما يتبع ذلك من توزيع للأدوار و الواجبات على فريق التحقيق.

د-تعيين الأشخاص الذين سيتم استجوابهم ، و تحديد النقاط التي يجب استيضاحهم من اجلها و كذلك تقدير مدى الحاجة الى الاستعانة ببعض الأشخاص من ذوي الاختصاصات الفنية التي يتطلبها التحقيق و لا تتوافر ضمن افراد التحقيق.

ثانيا : تشكيل فرق تحقيق

ان التحقيق الابتدائي في الجرائم المعلوماتية يكون في الغالب اكثر من ان يتولاه شخص واحد بمفرده حتى و لو كانت المضبوطات هب مجرد حاسب شخصي واحد و لذلك فانه يفضل ان يتعاون عدة محققين في انجاز مهمة التحقيق و العثور على الأدلة و يجب ان يتشكل فريق التحقيق من فنيين اخصائيين ذوي هبرة في مجال الحاسوب الانترنيت .

كما ان التحقيق في هذه الجرائم قد يتطلب الاستعانة ببعض خبراء مسرح الجريمة التقليدية ، مثل خبير البصمات و خبير التصوير الذين يعتبرون من الخبراء الأساسيين في معظم انواه الجرائم .

و على هذا الأساسي يمكن تقسيم فريق التحقيق في هذا النوع من الجرائم الى فئتين :

الفئة الأولى:

و تتمثل في الأشخاص الذين يتصل عملهم مباشرة بجرائم الحاسب الآلي و الانترنيت و لا يمكن التحقيق في أي جريمة تنتمي الى هذه النوعية من الجرائم الا بهم و

و جودهم ضروري في مسرح الجريمة ، و يمكن تحديد أعضاء هذه الفئة على النحو التالي[1] :

1 – قائد الفريق او المحقق الرئيسي : يشترط فيه أي يكون له خبرة طويلة في مجال التحقيق الجنائي و لديه معرفة بالطبيعة الخاصة بجرائم الحاسب الآلي و الانترنيت يتولى السيطرة الكاملة على مسرح الجريمة و توزيع المهام على الفريق و الاشراف على قيامهم بأعمالهم ، و التنسيق مع الجهات و اتخاذ كافة القرارات المتصلة بالتحقيق.

2 – محقق جنائي : شخص او اكثر بحسب ظروف الجريمة لديه خبرة و معرفة بوسائل و أساليب التحقيق و اجراءاته ، مع المامه بطبيعة جرائم الحاسوب و الانترنيت و كيفية التعامل مع الأدلة الرقمية فيتولى التفتيش عن الأدلة و اخذ افادة الأشخاص ذوب العلاقة في مسرح الجريمة .

3 – خبير حاسب آلي و شبكات : شخص او اكثر بحسب الظروف يجمع بين المعرفة بعلوم الحاسوب و الشبكات و بين الالمام باجراءات التحقيق الجنائي و اساليبه و كيفية التعامل مع مسرح الجريمة و يكون مسؤول عن رفع و تحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة التي لا تؤثر على سلامة الدليل و صلاحيته لاقامة الدعوى و العرض على المحكمة.

4 – خبير تدقيق حسابات : متخصص في المراجعة المحاسبية و على درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة في المؤسسات المصرفية و الآليات المختلفة التي يتم بواسطتها تبادل النقد الالكتروني ، و يعمل مع خبير الحاسب الآلي و الشبكات على تحديد أسلوب الجريمة و ما إذا كان هناك تلاعب في الأنظمة المتضررة بالإضافة الى تقدير الخسائر المادية الناتجة عن الجريمة .

5 – خبير تصوير : يتولى تصوير مسرح الجريمة كما هو متبع في جميع الجرائم فيعمل على تصوير كل المواقع داخل مسرح الجريمة و خارجه و تصوير ادلة الجريمة بالتصوير الفوتوغرافي و الفيديو.

[1] حسين بن سعيد الغافري، المرجع السابق، ص 7.

6 –خبير بصمات : لرفه البصمات من مسرح الجريمة كإجراء عام في معظم الجرائم مع التركيز على المكونات المادية للحواسب و الشبكات المتضررة أو المشتبه بوجود صلة لها بالجريمة، خاصة لوحة المفاتيح و الفارة ، و ذلك بعد اتهاذ الاحتياطات الفنية اللازمة من طرف هبير الحاسوب .

7 – هبير رسم تخطيطي : يقوم بعمل رسم تخطيطي (كروكي) لمسرح الجريمة بطريقة فنية دقيقة مستخدما مقياس مناسب للرسم ، بما يوضح تقسيماته و أماكن تواجد الأدلة و الأشخاص فيه.

الفئة الثانية :

و هي تمثل الأشخاص الذين قد يتطلب ظروف مسرح الجريمة تواجدهم ، الا ان دورهم ليس وثيق الصلة بالطبيعة الخاصة بجرائم الحاسب الآلي ، و قلما يخلو مسرح أي جريمة مهما كان نوعها من وجودهم ن مثل افراد حماية و تامين المسرح و افراد القبض و افراد التحريات و غيرهم و تحديد الأعضاء نوعا متروك لتقدير المحقق على ضوء المعلومات المتوافرة لديه عن الجريمة ن و حسب ما تفرضه طبيعة مسرح الجريمة و حجمها و ظروفها.

الفرع الثاني : الوسائل المادية للتحقيق الجنائي في الجرائم الرقمية

يحتاج المحقق في تنفيذ التحقيق الى وسائل فنية تستعمل في بيئة نظم المعلومات ، و التي يمكن باستخدامها تنفيذ إجراءات التحقيق لاثبات وقوع الجريمة و تحديد شخصية مرتكبها[1] ، و غالبا مع تكون جرائم التي ترتكب عبر شبكة الانترنيت اصعب في الاثبات و تستدعي تدخل الجهات الأمنية اكثر من جرائم النظم الأخرى ، و من اهم هذه الوسائل :

أولا : عناوين الانترنيت

[1]السوفي نور الهدي ، التحقيق في الجريمة المعلوماتية ، مذكرة لنيل شهادة الماستير اكاديمي في الحقوق ، تخصص قانون جنائي ، جامعة قاصدي مرباح ورقلة ، 2017.

و البريد الالكتروني و برامج المحادثةMCA . IP

عنوان الانترنيت هو المسؤول عن تراسل حزم البيانات هبر الانترنيت و توجيهها الى اهدافها و يوجد هذا العنونان بكل جهاز مرتبط بشبكة انترنيت و يتكون من اربعة أجزاء الجزء الواحد له ثلاث خانات ، يشير الجزء الأول من اليسار الى المنطقة الجغرافية و يشير الجزء الثاني لمزود الخدمة و الثالث لمجموعة الحواسب و المرتبطة و الرابع يحدد الكمبيوتر الذي تم الاتصال منه ، و في حالة وجود أي مشكلة فان اول ما يقوم به المحقق هو البحث عن رقم الجهاز و تحديد موقعه لمعرفة الجاني ، و توجد اكثر من طريقة لمعرفة هذا العنوان الخاص بجهاز الحاسوب ، منها في حالة العمل على نظام التشغيل بكتابة ويندواز في امر التشغيل ليظهر مربع حوار يبين فيه هذا العنوان.

ثانيا : البروكسي

البروكسي وسبلة لوصل موقع الويب و الشبكات المحلية للانترنت ، فهو برنامج يعالج حركة النقل الى الأنظمة المضيفة نيابة عن البرامج المستظافة المشتغلة على الشبكة المحلية مما يعني إمكانية المستخدم الوصول الى الانترنت عبر الجدار الناري لكن لا يمكن للدخلاء رؤية الداخل[1]، و يعمل البروكسي كوسيط بين الشبكة و مستخدمها حيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لادارة الشركة و ضمان الامن و توفير خدمات الذاكرة الجاهزة ، حيث يتلقى مزود البروكسي عبر الانترنيت طلبا من المستخدم بحيث يبحث عن الصفحة المطلوبة ضمن الذاكرة المخفية المحلية فيتحقق البروكسي من وجودها[2]، و لذا لم تكن موجودة فانه يعمل كمزود زبون و يرسل الطلب الى العالمية حيث يستخدم احد عناوين (ا ب) كما يمكن للذاكرة الخفية الاحتفاظ بالعمليات التي تمت عليها مما يجعل دورها قويا في الاثبات.

ثالثا : برامج التتبع

---

[1]بلال بن جامع ، المشكلات الأخلاقية و القانونية المثارة حول شبكة الانترنيت، ماجستير في علم المكتبات تخصص اعلام علمي و تقني جامعة منتوري قسنطينة ، 2006 ، ص 163

[2]خالد عياد الحلبي ، المرجع السابق ، ص 206.

هذه البرامج يمكنها ان تقوم بالتعرف على محاولات الاختراق و من قام بها و مصمم العمل في الأجهزة المكتبية و ساكن في خلفية المكتب ، و عند رصده لأي محاولة قرصنة يساره بإغلاق منافذ الدخول أمام المخترق ثم يبدا في عملية المطاردة لاقتفاء اثر المخترق و هذا البرنامج يتكون من شاشة رئيسة تقدم للمستخدم بيانا شاملا لعمليات الاختراق ت و تفصل اسم الحدث و تاريخ الحدوث عنوانه (ا ب) الذي تم من هلاله ن و الشركة المزودة لخدمة الانترنيت المستضيفة للمخترق[1] ، و فور حدوث أي محاولة للاختراق تظهر امام المستخدم شاشة صغيرة مصحوبة بتحذير صوتي يظهر على الشاشة عنوانه (ا ب) الخاص به.

رابعا : نظام كشف الاختراق

يرمز له ب (ا د س) و هذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الانترنيت مع تحليلها بحثا عن اية إشارة قد تهدد امن الحاسوب ، و يتم من خلال تحليل رزم البيانات اثناء انتقائها عبر الشبكة و مراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الاحداث فور وقوعها في الشبكة ، و في حال اكتشاف النظام وجود احدى هذه التواقيع يقوم بانذار مدير النظام بشكل فوري و بطرق عدة .

خامسا : أدوات الضبط

ان جهات التحقيق و جمع الاستدلالات تحتاج الى ضبط ماديات الجريمة و اثبات وقوعها و المحافظة على الأدلة حتى يتم نسبتها الى الجاني لتقديمها للنيابة العامة لكسب اعترافه و لذا يوجد أدوات تقوم بضبط ماديات الجريمة كغالبية برامج الحماية و أدوات المراجعة و أدوات المراقبة المستخدمين و التقارير التي تنتجها نظم امن البيانات كما يمكن استخدم اغلب الأدوات المستخدمة في الجريمة كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين[2].

---

[1] نفس المرجع ص 207 ن 208 .

[2] خالد عياد الحلبي نفس المرجع ص210

سادسا : أدوات فحص و مراقبة الشبكات

يمكن ان يستخدم المحقق عدة أدوات منها :

1 – أداة (ا غ ب) وظيفتها تحديد مكان الحاسوب الفيزيائي على الشبكة و هو يحتفظ بجميع ارقام كروت الشبكة و به عدة مداخل مستعملة معه .

2 – برنامج (فيزوال روث) هو برنامج يلتقط اية عملية فحص عملت ضد الشبكة فيقوم بإعطاء أجوبة معينة تبين العمليات التي حدث فيها المسح و المناطق التي تم فيها الهجوم و بعد معرفة عنوان (ا ب) يوضح مسار الهجوم بين مصادره ن و الجهة التي استهدفها الهجوم[1].

3 – أداة التتبع (ثراسور) ترسم مسارا بين جهازين تظهر فيها كل التفاصيل عن مسار الرزم و العناوين التي زارها الجاني ن و توجه من خلالها الوقت و القفازات ن و هي تمح برؤية المسار الذي اتخذه (ا ب) من مضيف لآخر .

4 – أداة تفحص حالة الانترنيت (ناث سثات) هي أداة فحص حالة الاتصال الحالي للبروتوكول و لها عدة مهمات من أهمها عرض جميع الاتصالات الحالية و منافذ التصنت و غرض المنافذ و العناوين بصور رقمية و عرض كامل جدول التوجيه.

الفرع الثالث : الوسائل الإجرائية للتحقيق الجنائي في الجرائم الرقمية

و تتمثل في الإجراءات المستخدمة من حق المحقق و التي من خلالها يتم تنفيذ طرق و أساليب التحقيق لاثبات وقوع الجريمة و تحديد شخصية مرتكبها ، و تتمثل في :

أولا : اقتفاء الأثر

اخطر ما يخشاه المجرم الالكتروني هو تقصي اثره اثناء ارتكابه الجريمة ، لهذا فأهمية اقتفاء الأثر في الجريمة الالكترونية اكثر أهمية من أهمية الشهادة في الجرائم

[1] خالد عياد الحلبي ، مرجع سابق، ص 211

التقليدية ، و يمكن تقصي الأثر بطرق عدة سواء كان ذبك عن طريق بريد الكتروني تم استقباله او عن طريق تتبع الأثر للجهاز الذي تم استخدامه للقيام بعملية الاختراق.

ثانيا : الاطلاع على عمليات النظام المعلوماتي و أسلوب حمايته

على المحقق الاطلاع على النظام المعلوماتي و مكوناته من شبكات و تطبيقات و خدمات تقدم للعملاء، كما يجب عليه معرفة نوعية برامج الحماية و أسلوب عملها من التقارير التي تنتجها نظم امن البيانات و تقارير الجدران النارية .

ثالثا : الاستعانة بالذكاء الاصطناعي

و يتم ذلك من هلال حصر الحقائق و الاحتمالات و الأسباب و الفرضيات ، بعدها تتم معرفة النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسوب وفق برامج تعد لذلك ، و التي تعطي كافة الاحتمالات ، ثم اكثر الاحتمالات وصولا ثم الاحتمال الأقوى مع إعطاء الاسباب[1] .

رابعا :التوقيف خلال فترة التحقيق

تعد وسيلة مهمة من وسائل التحقيق و هو ما يعرف بالحبس الاحتياطي و هو سلب حرية المتهم مدة من الزمن تحددها مقتضيات التحقيق و مصلحته وفق ضوابط حددها القانون و قد ينتهي بالإفراج أو الإدانة اذ تحقق هذه الوسيلة عدد من الأغراض كبقاء المتهم في متناول سلطة التحقيق للمحافظة على ادلة الجريمة عن محاولة المتهم اخفاءها أو طمسها ، و منع التواطؤ بالحيلولة بين اتصال المتهم بباقي شركائه في ارتكاب الجريمة ، و يغل يده عن تجهيز شهود نفي مزيفين أو من تهديد شهود الاثبات.

خامسا : اظهار الحقيقة

قد تلجأ الجهة المتضررة الى التبليغ عن جرائم نظم المعلومات أو ان الجهات الأمنية تتحرك عند تلقيها معلومات تشير الى وقوع جريمة أو ضبط أفراد متلبسين او توفر معلومات من خلال النشر على شبكة الانترنيت تشير الى انتشار فيروسات أو وقوع

[1]خالد عياد الحلبي ، المرجع السابق ، ص 213 ، 214.

عمليات اختراق ، او قرصنة فيقوم المحقق يالاجراءات التي تتبع تلقي البلاغ من التأكد من صحة البلاغ، و التحفظ على مكان الجريمة و كل من له صلة بها و حصر الشهود و منع مغادرتهم و حصر الأدلة و رفه الآثار ، و يلزم على المحقق اظهار مجموعة من الحقائق في مرحلة جمع الاستدلالات و اثباتها في محضر نظرا لأهميتها في تحديد الجريمة و رسم خطوات البحث في المجهول على النحو التالي :

1 – التثبت من توافر اركان الجريمة

ان تحقق وقوع الجريمة المعلوماتية يكون يتوافر ركنيها المادي و المعنوي الأول الذي يتمثل في النشاط الاجرامي و النتيجة التي تحقق و علاقة السببية بينهما ، أما الركن المعنوي فيقصد به الإرادة التي اقترن بها الفعل المرتكب و يأخذ صورة القصد الجنائي في الجريمة المتعمدة و صورة الخطأ غير المقصود في الجريمة غير العمدية ن و بالتالي فعلى المحقق استظهار الأركان ثم الجزم بوقوع الجريمة من عدمه .

2– تحديد مكان الجريمة و وصفه

ان التوصل الى الجاني له أهمية كبيرة في نجاح عملية البحث عن مكان الجريمة الذي توجد فيه الاثار و الأدلة الجنائية و لذلك يقوم الجناة بمحاولة نقل هدف الجريمة الى مكان آخر بهدف طمس معالمها و تضليل التحقيق.

3 – تحديد وقت وقوع الجريمة

و يتم ذلك بتحديد تاريخ و ساعة وقوعها و بتم استخلاص ذلك من تصريحات المجني عليه او المبلغ او الشهود و قد يتم عن طريق الخبراء أو المختصين و هو من اهم العناصر التي تساعد في تحديد مسؤولية المتهم في ارتكاب الجريمة و معرفة مكان وقوعها و الأشخاص الذين كان معه ، كما ان الوقت في بعض الجرائم يعتبر ظرفا مشددا.[1]

[1]سليمان مهجع العنزي ، وسائل التحقيق في جرائم نظم المعلومات ، رسالة ماجيستير في العلوم الشرطية ، كلية الدراسات العالية ، اكادمية نايف العربية للعلوم الأمنية ، الرياض ، 2003 ص 108 .

4 – تحديد أسلوب ارتكاب الجريمة

و يقصد بها الطريقة التي سلكها المشرع في ارتكاب جريمته ، و للأسلوب أهمية كبيرة في تحديد خطة البحث عن الجاني فلكل مجرم أسلوبه الاجرامي الذي لا يغبره الا ناذرا فمن الأسلوب يستطيع المحقق حصر قطاع محدد من المجرمين.

5 – تحديد أداة ارتكاب الجريمة

يقع على الباحث عبئ التفتيش و ضبط الأداة التي ارتكبت بها الجريمة فهو امر جوهري لتحديد شخص الجاني و من هذه الأدوات برامج التنصت على الشبكات ن أقراص بدا التشغيل و غيرها.

6 – إيضاح الظروف المحيطة

و ذلك بتبيان الظروف المحيطة بالجريمة و معرفتها ، فيكون بعضها سابق على وقوع الجريمة مثل سوء سمعة المتهم و سلوكه و الشكاوى و المشكلات السابقة التي حدثت بالمؤسسة و البعض الآخر قد يكون معاصرا للجريمة و هناك ظروف قد تكون لاحقة للجريمة .

7 – تحديد دوافع الجريمة

يسعى المحقق الى كشف أسباب وقوع الجريمة بمعرفة الوقائع المادية التي حدثت فأثرت في نفسية الجاني أدت به الى ارتكابها و هو امر نفسي داخلي مرتبط أساسا بمجموعة من الغرائز الإنسانية و توجه السلوك لاشباعها ، و في جرائم المعلومات من الصعب جدا معرفة سبب الحادث لان دوافع الجناة غير واضحة او قد تحدث الجريمة خطأ ، و بمكن للمحقق تحديد سبب الجريمة من خلال عدة عوامل كنوع الجريمة و المعاينة و الاستعانة باهل الخبرة.

سادسا : اتباع القواعد الفنية لكشف الجريمة

يجب على المحقق اثناء القيام بتحقيقاته و في سبيل الكشف عن الجريمة القيام بالإجراءت اللازمة المتمثلة في المعاينة و التفتيش[1] و انتداب الخبراء و سماع الشهود و استجواب أطراف الجريمة و جميع التحريات اللازمة .

المبحث الثاني : المحقق في الجرائم الرقمية

أمام التكور التقني و التكنولوجي الذي صاحب الجريمة المعلوماتية قان المختصين بالتحقيق في هذا النوع من الاجرام المستحدث يختلفون عن أولئك المختصين بضبط الجرائم التقليدية من حيث الخصائص و طريقة التكوين ذلك لان التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية و انما يعتمد على البناء العلمي و التكنولوجي و هم يتولون مهمة البحث عن الجرائم المعلوماتية و كشف النقاب عنها ، و لذلك سنتطرق في هذا المبحث الى مهمة المحقق في الجريمة الرقمية و هذا في مطلبين يتضمن (المطلب الأول) القائم بالتحقيق في الجرائم الرقمية و في (المطلب الثاني) صلاحياته.

المطلب الأول : القائم بالتحقيق في الجرائم الرقمية

يقوم المحقق الجنائي بأهم و اخطر المهام على الاطلاق و هي تحقيق العدل لذا فانه يتعين ان يكون ذا صفات معينة و عزيمة جبارة و ان يكون شديد اليقظة و الانتباه و الحزم ، ذا قدرة على استخلاص المعلومات ن و في سبيل آدائه لمهامه يجب ان يبذل العناية الواجبة فيما يعرض عليه من تحقيقات و شكاوى و التزام النزاهة و الحياد فيما يتخذه من إجراءات ، و الحرص على انزال حكم القانون صحيحا و في سبيل ذلك اسند له المشرع مساعدين يعملون الى جانيه لذلك نحاول معرفة المحقق (الفرع الأول) و مساعدو المحقق (الفرع الثاني).

عن هذا الاطار نص قانون الإجراءات الجزائري عن صلاحيات ضباط الشرطة القضائية مهام البحث و التحري المادة 12 و قاضي التحقيق المادة 38.[1]

الفرع الأول : مفهوم المحقق في الجرائم الرقمية

تعتبر مهنة المحقق من افضل و امتع المهن و سنتطرق بالتفصيل الى تعريف المحقق و خصائصه الفنية و تأهيله.

أولا : تعريف المحقق في الجرائم الرقمية

المحقق الجنائي هو الشخص القائم بأعمال و إجراءات التحقيق الجنائي ن و لا يختلف تعريف المحقق الجنائي في الجرائم التقليدية عنه في الجرائم المعلوماتية بل الفرق يكمن في نوعية الجريمة و ليس في المحقق.

و قد ذهب بعض الفقه الى تعريف المحقق بانه " هو كل من عهد اليه القانون لتحري الحقيقة في البلاغات و القضايا و الجرائم المطلوب التحقيق فيها ، و يسهم دوره في كشف غموضها وصولا الى معرفة حقيقة الحادث ن و كشف مرتكبيه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة .

كما عرفه البعض الآخر بانه هو يقوم بمباشرة التحقيق بمعناه القانوني.

و من خلال التعريفات السابقة يتضح بان الاختلاف راجع الى الاختلاف في زاوية النظر الى عمل المحقق او تحديده.

و عليه يمكن تعريف المحقق بانه " هو شخص لديه خبرة و معرفة بوسائل و أساليب التحقيق و اجراءاته مع المامه بطبيعة جرائم الحاسبة الالكترونية و الانترنيت و كيفية التعامل مع الأدلة الرقمية ، فيتولى التفتيش عن الأدلة و اخذ افادة الأشخاص ذوب العلاقة في مسرح الجريمة.[1]

[1]علي عدنان الفيل ، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية ن دراسة مقارنة ، المكتب الجامعي الحديث ، الإسكندرية ، بدون طبعة ، 2012 ، ص 17 .

ثانيا : خصائص المحقق في الجرائم الرقمية :

تتمثل في الخصائص الفنية للمحقق الالكتروني ، و تاهيل و تدريب المحقق الالكتروني.

1 – الخصائص الفنية للمحقق الالكتروني :

أضاف ظهور الجرائم المعلوماتية النابعة من التطور التكنولوجي أعباء جديدة على أجهزة التحقيق لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يالفها رجال الضبطية القضائية و لم يتعودوا عليها ما يستلزم ضرورة توفير الإمكانيات و المهارات المطلوبة غي هذا المجال ، لذلك كان من اللازم عند مباشرة المحقق للتحقيق في الجريمة المعلوماتية معرفة العديد من الجوانب الفنية ليقوم بعمله على احسن وجه و تتمثل اهمها فيما يلي :

أ – معرفة الجوانب الفنية و التقنية للأجهزة الحاسوبية و الانترنيت لان افتقار ضابط الشرطة القضائية الى التأهيل الكافي في الميدان التقني قد يؤدي الى اتلاف و تدمير الدليل.

ب – اتباع الإجراءات الصحيحة و المشروعة من أجل سرعة المحافظة على الأدلة الالكترونية التي تثبت وقوع الجريمة و تخزينها في الأقراص المعدة لذلك ، و منع حذفها و الحرص على عدم تعرض وسائط التخزين كالأقراص المرنة لأي مؤثرات خارجية ، كالقوة الكهرومغناطيسية حتى لا تتلف محتوياتها .

ج – معرفة آلية عمل تشكيلات الحاسوب و الانترنيت ، و تبرز أهمية فهم المحقق لهذه المبادئ كونها ضرورية لتصور كيفية ارتكاب الفعل الاجرامي في العالم الافتراضي من اختراق للشبكات و اعتراض حرم البيانات اثناء انتقالها عبر الشبكة و التجسس عليها و تحويلها عن مسارها ، كما انها تعطي للمحقق تصورا جيدا عن مدى امكانية متابعة مصدر الاعتداء على الشبكة و المعوقات التي تحول دون ذلك[1] .

[1] ين سعيد حسن الغافري ، المرجع السابق ، ص 06.

د – معرفة المحقق بالأنظمة المختلفة لكي يشارك في متابعة فحص و تفتيش مسرح الجريمة.

و – معرفة معطيات الحاسوب لمعرفة صيغ الملفات و ما تحتويه ن و معرفته لاهم التطبيقات التي يمكنه من خلالها قراءة و مشاهدة محتوى هذه الملفات .

هـ – معرفة و ادراك أساليب ارتكاب الجريمة الالكترونية و تقنيات الامن المعلوماتي و التي تساعد المحقق في معرفة الجناة و مواقع ارتكاب الجريمة.

2 – تأهيل و تدريب في الجرائم الرقمية :

في مكافحة الجرائم المعلوماتية بصفة عامة لابد من وضع سياسة جنائية رشيدة تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة ، و لهذا فانه من الضروري اعداد المحققين في الجرائم المعلوماتية باعتبارهم يواجهون أنشطة إجرامية معقدة و تنفذ بطرق دقيقة و ذكية و يتأتى ذلك من خلال الإسراع في ان يطور رجال البحث الجنائي وسائلهم البحثية و قدراتهم العلمية ، و ليس بالضرورة ان يكون المحقق في الجريمة المعلوماتية هبيرا في الحاسوب و النظم المعلوماتية ، و لكن لابد من الالمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي و حسن استغلالهم في كشف الجرائم و جمع الأدلة كما انه من الضروري ان يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة و التدابير اللازمة لتامين الأدلة و معلوماتها الممغنطة بصورة علمية و سليمة.[1]

و اذا كانت الشركات الخاصة تستعين بمحققين هم خبراء في الحواسيب ن فالجهات الحكومية أولى باعداد كوادرها للضبط و التحقيق غي الجرائم المعلوماتي، و يرى الفقه الجنائي انه حال التدريب على التحقيق في الجريمة المعلوماتية بتعين مراعاة عناصر أساسية تتمثل في شخص المتدرب و منهج الدورة التدريبية و صفة و أسلوب التدريب.

[1]محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي ، بحث مقدم الى مؤتمر القانون و الكمبيوتر و الانترنات بكلية الشريعة و القانون ن جامعة الامارات العربية المتحدة الفترة من 01 الى 03 ماي 2000.

و لقد نصت الفقرة 10 من المادة 04 من المرسوم الرئاسي 15-261 المؤرخ في 08-10-2015 الذي يحدد تشكيلة و تنظيم و كيفيات سيلا الهيئة الوطنية للوقاية من الجرائم المتصلة بتقنيات الاعلام و الاتصال و مكافحتها على "المساهمة في تكوين المحققين في مجال التحريات التقنية المتصلة بتكنولوجيات الاعلام و الاتصال" و بالتالي فقد أكدت على ضرورة تكوين محققين متخصصين في المجال التقني بتكنولوجيات الاعلام و الاتصال.

الفرع الثاني : مساعدو المحقق في الجرائم الرقمية

ان المحقق في الجرائم الرقمية و حتى يتمكن من متابعة تحقيقاته بسهولة حتم الامر امداده بعدد من الاعوان يختلفون بحسب طبيعة الجريمة و من اهم هؤلاء المساعدين ظ

أولا : رجال الضبطية القضائية

ان مباشرة التحقيق في القضايا الجنائية يعتبر امرا في غاية الأهمية ، فنجد مختلف الأطراف تعمل لجانبه و تقوم بوظائف مكملة لبعضها البعض ، فيباشر رجال الضبط القضائي تحرياتهم ثم يقدمون ما توصلوا اليه حول الوقائع الجنائية الى المحقق و هي ضرورية كونها ترشده الى الاتجاه الصحيح المؤدي الى كشف الحقيقة ن و عليه فانهم من الركائز القوية لنجاح همل المحقق ، فيكون مطمئنا الى ما يقومون به من استدلالات و تعتبر هذه المرحلة تمهيدية للتحقيق.

_ جهازي الامن الوطني و الدرك الوطني :

لقد سعت المديرية العامة للامن الوطني و كذا جهاز الدرك الوطني في انشاء فرق خاصة لمكافحة الجرائم المعلوماتية و كذا تكوين عناصر متخصصة في هذا المجال، بالإضافة الى توافر هاذين الجهازين من مخبريين علميين للشرطة العلمية و التقنية يتوفرون على احدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الاجرام.

1 – الوحدات التابعة لسلك الامن الوطني :

وضعت مديرية الامن الوطني في اطار تحديد سياسة امنية فعالة كافة الإمكانيات البشرية و التقنية المتاحة لديهم لاجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الالكترونية و التي تعتبر نتاج القصور الحاصل على المستوى الدولي و الوطني في مجال تكنولوجيات الاعلام و الاتصال ، و توجد على مستوى جهاز الامن الوطني ثلاث وحدات مكلفة بالبحث و التحقيق في الجرائم المعلوماتية هي :

أ – المخبر المركزي للشرطة العلمية بالجزائر العاصمة .

ب – المخبر الجهوي للشرطة العلمية بقسنطينة

ج – المخبر الجهوي للشرطة العلمية بوهران .

ثانيا : الوحدات التابعة للقيادة العامة للدرك الوطني

يضع الدرك الوطني تنفيذ مهامه في مجال الحفاظ على الامن الوطني و النظام العام و محاربة الجريمة بكافة أنواعها ، وحدات عديدة و متنوعة على مستوى القيادة العامة ، أو على مستوى القيادة الجهوية و المحلية نذكر منها :

أ – المصالح و المراكز العلمية و التقنية.

ب – هياكل التكوين.

ج – المصلحة المركزية للتحريات الجنائية .

د – المعهد الوطني لعلم الاجرام بيوشاوي بالجزائر العاصمة و يختص بالتحقيق في الجرائم الالكترونية قسم الاعلام و الالكترونيك حيث يقوم بتحليل الدعامات الالكترونية و انجاز المقاربات الهاتفية و تحسين التسجيلات الصوتية و الفيديو و الصورة لتسهيل استغلالها.

ثانيا : مقدمو الخدمات : عرفهم القانون بانهم :" 1 – أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/او نظام

للاتصالات 2 –و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة او لمستعمليها "[1].

كما تنص المادة 10 من نفس القانون على انه " في اطار تطبيق احكام عذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة .

و يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين و كذا المعلومات المتصلة بها و ذلك تحت طائلة العقوبات المقررة لإفشاء اسرار التحري و التحقيق".

و من ثمة فان مقدمو الخدمات بما لديهم من تقنيات متماشية مع تطور التكنولوجيات الحديثة للاعلام و الاتصال دور مهم في مكافحة الجرائم المعلوماتية ، و ذلك بتقديم المساعدة التقنية للسلطات المكلفة بالبحث و التحري عن هذه الجرائم المرتكبة بواسطة او ضد هذه التكنولوجيات الحديثة ، كما اوجب عليهم المشرع حفظ المعطيات المعلوماتية الامر الذي يسمح للمتحري بتتبع الجريمة و حركة المجرمين ، و خصهم أيضا بالتزامات خاصة تتمثل في التدخل الفوري من اجل سحب المحتويات التي يتاح لهم الاطلاع عليها بمجرد علمهم بطريقة مباشرة او غير مباشرة بمخالفتها للقانون ، او كانت مخلة بالآداب العامة أو النظام العام ، أو جعل الدخول اليها غير ممكن او محظور ، و كذا وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول الى الموزعات التي تحوي معلومات مخالفة للنظام العام و الآداب العامة و اخبار المشتركين لديهم بوجودها .

و بالتالي فان التزامات مقدمي الهدمة تتمثل في ثلاث نقاط أساسية هي مساعدة السلطات و حفظ المعطيات المتعلقة بحركة السير و أخيرا التزامات خاصة بمقدمي خدمة الانترنيت[1].

---

[1] المادة 02 من القانون 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها .

و على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين و كذا المعلومات المتصلة بها و ذلك تحت طائلة العقوبات المقررة لافشاء اسرار التحري و التحقيق ، إضافة الى حفظ محتوى هذه الاتصالات لمدة سنة كاملة.

ثالثا : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال

لقد نص القانون 09-04 في مادته 13 على انشاء هيئة وطنية للوقاية من الاجرام المتصل بتكنولوجيات الاعلام و الاتصال و مكافحته تتولى تنشيط و تنسيق عمليات الوقاية من الجرائم الالكترونية و مساعدة مصالح الشرطة القضائية في التحريات التي تجريها بشان هذه الجرائم ، كما تتكفل اللجنة أيضا بتبادل المعلومات مع نظيرتها في الخارج باعتبار ان هذا القانون اكد على مبدا التعاون الدولي.

و تعتبر الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي ، توضع لدى الوزير المكلف بالعدل و بحدد مقرها بمدينة الجزائر العاصمة[2].

تضم الهيئة قضاة و ضبط و أعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية و الدرك و الامن الوطنيين وفقا لقانون الاجراءات الجزائية ، تكلف بتجميع و تسجيل و حفظ المعلومات الرقمية و تحديد مصدرها و مسارها من اجل استعمالها في الإجراءات القضائية و ضمان المراقبة و الوقاية للاتصالات الالكترونية وذلك قصد الكشف على الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى تحت سلطة القاضي المختص.

كما تتولى الهيئة عدة مهام في مجال مكافحة الجريمة الالكترونية إذ تعمل على مساعدة السلطات القضائية و مصالح الشرطة في التحريات التي تجريها بصدد الجرائم ذات الصلة بتكنولوجيات الاعلام و الاتصال و خاصة التي تمس بأنظمة المعالجة الآلية

---

[1]انظر المواد 11 و 12 من القانون 09-04 .

[2]انظر المادة 02 من المرسوم الرئاسي 15-261 المؤرخ في 08-10-2015 يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها ، ج ر عدد 53 ، بتاريخ 08-10-2015 ، ص 16

للمعطيات ، و تزويدهم بكل المعلومات و الخبرات اللازمة و وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها و تسليمها الى الشرطة القضائية[1].

رابعا : الخبراء

و هو ذوي المعرفة و التخصص في الجوانب العلمية و تخص بالذكر الفئة المختصة في معالجة و تحليل ادلة الجرائم المعلوماتية ، بحيث لا يمكن الكشف عن غموض الجريمة و الوصول الى الحقيقة إذا لم يكن هناك تعاون فعلي معهم ، و استطلاع رأي اهل الخبرة.

خامسا : القضاة و المحامون

ان القضاة بحكم عملهم يمكنهم توجيه المحقق في الأمور الشرعية التي يكون لها تأثير في صحة و بطلان الإجراءات القانونية المتخذة لذلك فان المحقق يجب ان يسعى الى خلق جو التفاهم و التعاون بينه و بين هذه الفئة لخدمة الصالح العام و كذلك الامر بالنسبة للمحامين الذين يدافعون عن المتهمين ، و عليه يجب على المحقق ان يستوعب الدور الأساسي الذي يؤديه المحامي ن و مدى أهمية التعاون معه لما ينتج عنه من حماية لحقوق و حريات الافراد و تحقيق العدالة بين افراد المجتمع.

المطلب الثاني : صلاحيات المحقق في الجرائم الرقمية

يمر التحقيق في التشريع الجزائري بمرحلتين ، مرحلة التحقيق الابتدائي و هي مرحلة البحث و التحري و جمع الاستدلالات من اختصاص ضباط الشرطة القضائية ، و مرحلة التحقيق القضائي و هي من اختصاص قاضي التحقيق و قد حدد قانون الإجراءات الجزائية صلاحيات كمل منهما و سنحاول من خلال هذا المطلب حصر صلاحيات الضبطية القضائية (الفرع الأول) و اختصاصات قاضي التحقيق (الفرع الثاني) .

الفرع الأول: صلاحيات الضبطية القضائية

[1]انظر المادة 04 من المرسوم الرئاسي 15-261 .

نصت المادة 12 من ق ا ج على ان اختصاص الضبطية القضائية هو جمع الأدلة و البحث و التحري عن مرتكبي الجرائم و ذلك في حدود الدائرة التي يباشرون فيها وظائفهم المعتاد و لذلك يتعين ان يكون مطان وقوع الجريمة او محل إقامة المتهم او محل القبض عليه.

أولا : امتداد الاختصاص الاقليمي للضبطية القضائية

أجاز القانون تمديد الاختصاص لضباط الشرطة القضائية في حالة الاستعجال اة بناء على طلب السلطة القضائية و هو ما نصت عليه المادة 16 فقرة 02 من ق ا ج (دائرة المجلس) ، و كذا تمديد الاختصاص المحلي الى كامل التراب الوطني في الجرائم الخطيرة و هو ما نصت عليه المادة 16 فقرة 7 من ق ا قيما يتعلق ببحث و معاينة جرائم المخدرات و الجريمة المنظمة العابرة للحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبيض الأموال و الإرهاب و الجرائم الخاصة بالتشريع الخاص بالصرف ، فعلى ضباط الشرطة القضائية في هذه الجرائم بعد تلقي الشكاوى و البلاغات بخصوص هذه الجرائم أن يبادروا دون تمهل في اخطار وكيل الجمهورية و ان يوافوه باصول المحاضر و ما يتبعها من مستندات و وثائق و هي المحاضر التي حدد القانون مهلة ارسالها الى النيابة بخمسة أيام الموالية لتاريخ معاينة المخالفة على الأكثر اذا تمت المعاينة من دو الرتب في الشرطة البلدية و ذلك عن طريق ضباط الشركة القضائية و هو ما أكدته المادة 26 من ق ا ج.

ثانيا :تعزيز صلاحيات الضبطية القضائية و نلخصها في ما يلي :

1 – منح صلاحيات التحري لضباط الشرطة القضائية

منح المشرع صلاحيات البحث و التحري لأعوان الضبطية القضائية و اشترط ان تكون تحت رقابة ضابط الشرطة القضائية ما أكدته المادة 63 من ق ا ج " يقوم ضباط الشرطة القضائية و تحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الابتدائية بمجرد علمهم بوقوع الجريمة اما بناء على تعليمات وكيل الجمهورية و اما من تلقاء انفسهم".

2 – تمديد مدة التوقيف للنظر طبقا للمادة 51 من ق ا ج و مدد فترة التوقيف للنظر في الجرائم المعلوماتية و ذلك بتمديده مرة واحدة ، و هذا لصعوبة التحقيق غي هذه الجرائم و تعقيدها نظرا لاستخدام مرتكبيها لأساليب حديثة و متطورة.

الفرع الثاني : صلاحيات قاضي التحقيق

تتحدد صلاحيات قاضي التحقيق باختصاصه المحلي من خلال مكان وقوع الجريمة او مكان القبض على المشتبه فيه أو مكان اقامته و باختصاصه النوعي من هلال نوع الجريمة.

أولا : الاختصاص المحلي

نصت المادة 40 من ق ا ج على الاختصاص الموسع لقاضي التحقيق اذا تعلق الامر بالجرائم الخطيرة المذكورة في الفقرة الثانية "يجوز تمديد الاختصاص المحلي لقاضي التحقيق الى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف" و هو ما نصت عليه كذلك المواد 329 و 37 من نفس القانون بحيث يصبح لقاضي التحقيق التابع لهذه المحكمة اختصاص إقليمي يتجاوز حدود اختصاصه العادي ن و يمكنه التنقل او انتداب أي ضابط شرطة قضائية للقيام بمهام تتعلق بالتحقيق في الجرائم الخطيرة السابقة الذكر[1].

و في سنة 2006 صدر المرسوم التنفيذي 06-348 المؤرخ في 05-10-2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق ، و قد تنشأ هذا المرسوم ما يعرف بالجهات القضائية ذات الاختصاص الموسع أو الأقطاب الجزائية و نص على امتداد الاختصاص المحلي لمحاكم سيدي محمد بالجزائر ، قسنطينة ، ورقلة ، وهران و وكلاء الجمهورية و قضاة التحقيق بها الى محاكم

[1]قريشي حمزة ، الوسائل الحديثة للبحث و التحري في ضوء القانون الجزائري، منشورات السائحي ، الجزائر، ط 1 ، 2017 ، ص 27 .

مجالس قضائية أخرى ، و قد عدل هذا المرسوم بموجب المرسوم التنفيذي رقم 16-267 المؤرخ في 17-10-2016 بتعديل هذا الاختصاص الموسع لمحكمتي ورقلة و وهران.

ثانيا: الاختصاص النوعي

يختص قاضي التحقيق في كل الجرائم التي قدم له بشأنها طلبا افتتاحيا بإجراء تحقيق ، و القاعدة العامة ان التحقيق وجوبي في الجنايات و جوازي في الجنح و المخالفات يخضع لتقدير النيابة العامة ، و قد أضاف ق ا ج في تعديله لسنة 2006 القانون رقم 06-22 سلطات أخرى لقاضي التحقيق ، بحيث اذا اقضت ضرورة التحقيق يمكن اللجوء الى أساليب التحري الجديدة في الجرائم الخطيرة و هي التسرب و المراقبة الالكترونية و اعتراض المراسلات و تسجيل الأصوات و التقاط الصور.

يتصل قاضي التحقيق بالدعوى الخاصة بالجريمة الالكترونية اما عن طريق طلب افتتاحي من السيد وكيل الجمهورية او بشكوى مصحوبة بادعاء مدني من طرف المتضرر ما بينته المادة 38 من ق ا ج في فقرتها الثالثة

الفصل الثاني

الأليات الإجرائية للتحقيق الجنائي في الجرائم الرقمية

الفصل الثاني: آليات التحقيق الجنائي في الجرائم الرقمية

لم تكتف التشريعات الحديثة بحماية معطيات الحاسب الآلي بصفة عامة من خلال تجريم صور الاعتداء عليها أي الحماية الموضوعية ، و انما نظرا لخطورة الاجرام الالكتروني في حد ذاته لكون محل الجريمة مجموعة معطيات هي عبارة في الحقيقة عن ذبذبات الكترونية يصعب على الجاني القيام بعمل اجرامي عليها دون ترك آثار و دون ان يستغرق هذا العمل وقتا طويلا و هو ما يجعلها صعبة الاكتشاف و الاثبات ، الامر الذي أدى الى ظهور مشكلات إجرائية وضعت المحقق ذاته في حيرة امام هذه الجرائم كونها حديثة و لا يمكن تطبيق النصوص التقليدية عليها.

لذلك وضعت مجموعة من الإجراءات في مرحلة التحقيق منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية و الجرائم الخاصة بالمعطيات و منها لا يطبق الا على الجريمة المعلوماتية ، و لذلك سنحاول التطرق لإجراءات التحقيق العامة في الجرائم الرقمية (المبحث الأول) ثم إجراءات التحقيق الخاصة (المبحث الثاني).

المبحث الأول : الإجراءات العامة للتحقيق الجنائي في الجرائم الرقمية

عملت الدولة الحديث على اتباع السياسة الجنائية المناسبة بوضع استراتيجيات أيديولوجية لمواجهة المسائل التي لها علاقة بالوقاية من الجريمة و قمعها[1] ، و الجريمة الرقمية من بين هذه الجرائم التي يتطلب التحقيق فيها من حيث ثبوت التهمة و نسبتها الى المتهم من عدمه و استخلاص الدليل الى إجراءات يخرج تنفيذها عن نطاق مكتب التحقيق او ما تستخلصه محاضر الضبطية القضائية بل يستلزم الامر في بعض الجرائم الانتقال لاجراء معاينات مادية و عمليات تفتيش و ضبط و هي نفس الإجراءات المتبعة في الجرائم التقليدية ، و سنحاول في هذا المبحث التطرق الى الإجراءات العامة المادية – المعاينة و التفتيش و الضبط– (المطلب الأول) و الإجراءات العامة الشخصية –الخبرة و الشهادة– (المطلب الثاني).

(1) Marie , cristine / droit penal general, ed ellicses, parie, France 2002 , p 15

المطلب الأول : الإجراءات المادية الخاصة بالتحقيق في الجرائم الرقمية.

و يمكن حصر هذه الإجراءات في المعاينة التقنية من جهة (الفرع الأول) و التفتيش في بيئة الكترونية (الفرع الثاني) و ضبط الدليل الرقمي (الفرع الثالث).

الفرع الأول : المعاينة

عند العلم بوقوع الجريمة فان اول خطوة يقوم بها مأمور الضبط القضائي هو الانتقال الى مسرح الجريمة لإجراءات المعاينات اللازمة ، لان هذا الخير هو حجر الزاوية في التحقيق الجنائي و مكن الآثار و الأدلة الجنائية ، و لذلك تعتبر المعاينة من اهم إجراءات التحقيق لاهميتها القصوى في اثبات الواقعة الاجرامية فهي تعبر على الوقائع و الحقيقة تعبيرا صادقا فتمكن المحقق من تصور كيفية وقوع الجريمة و ظروف و ملابسات ارتكابها و سنحاول إعطاء تعريف للمعاينة.

أولا : تعريف المعاينة في الجرائم الرقمية

نتطرق الى تعرفها لغة و اصطلاحا .

1 – تعريف المعاينة لغة : المعاينة هي المشاهدة بالعين ، عاين غيره رآه بعينه و جاء في الامثال و العيان لا يحتاج الى بيان و بضرب لإظهار مزايا الشاهد للتصديق بالشيء دون برهان.

2 – تعريف المعاينة اصطلاحا : هي اجراء بمقتضاه ينتقل المحقق الى مكان وقوع الجريمة ليشاهد بنفسه و يجمع الآثار المتعلقة بالجريمة ، و كيفية وقوعها كذلك جميع الأشياء الاخرة التي تفيد في كشف الحقيقة و اتخاذ ما يلزم من إجراءات كضبط بعض الاشياء[1].

[1] محمد حماد مرهج الهيتي ، جرائم الحاسوب ، دار المناهج ، عمان ، ط 1 ،2006، ص 255.

و المعاينة هي " الكشف الحسي المباشر و المادي لاثبات حالة الشيئ أو المكان او الشخص و كل ما يفيد في كشف الحقيقة "[1].

فالهدف من المعاينة هو لغرضين اثنين الأول جمع الأدلة الناتجة عن الجريمة (الاثار) و الثاني اتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة لكي تكون لديه فكرة واضحة لا لبس فيها و لا غموض عن كيفية وقوع الجريمة.[2]

و بهذا المعنى تستلزم المعاينة الانتقال الى محل الواقعة أو أي محل توجد به الأشياء أو اثار يرى المحقق أن لها صلة بالجريمة ، كما ان المعاينة في الجرائم التقليدية تكون ذات أهمية في تصور كيفية وقوع الجريمة و ظروف ملابساتها و توفير ادلة مادية ، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة الالكترونية و ضبط الأشياء التي تفيد في اثباتها و نسبتها الى مرتكبيها ، لان الجريمة التقليدية غالبا لها مسرح تجرى عليه الاحداث التي تخلف أثار مادية على خلاف الجريمة الالكترونية يتضاءل دورها في الإفصاح عن الحقيقة المؤدية للأدلة المطلوبة ، لان الجريمة الالكترونية قلما تخلف أثار مادية ، و ان كثير من الأشخاص يردون الى مسرح الجريمة خلال فترة من زمان وقوع الجريمة ، و حتى اكتشافها أو التحقيق فيها و هي طويلة نسبيا الامر الذي يجعل الجاني يغير او يتلف او يعبث بالاثار المادية للجريمة ان وجدت و هذا ما يورد الشك في دلالة الأدلة المستقاة من المعاينة.

و بقصد بإجراء المعاينة في الجرائم المعلوماتية معاينة الآثار التي يخلفها مستخدم الشبكة المعلوماتية أو الانترنيت و تشمل الرسائل المرسلة منه او التي استقبلها و كافة الاتصالات التي تمت من خلال الكمبيوتر و الشبكة العالمية.

ثانيا : محل المعاينة في الجريمة الرقمية

يعتبر مكان ارتكاب الجريمة الوعاء الأساسي الذي يحتوي على اهطر الأدلة الجنائية التي يخلفها الجاني وراءه اثناء ارتكابه للجريمة ، و اذا كانت المعاينة غي الجرائم

---

[1] حسن الجوخدار ، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية ، دار الثقافة للنشر و التوزيع ، الأردن ، ط 1 ،2008 ، ص90.

[2] محمد حماد مرهج الهيتي ، المرجع السابق ، ص 256.

التقليدية تتم على مسرح الجريمة المادي فان المعاينة في الجريمة المعلوماتية تتم على مستويين :

1 – المسرح التقليدي :

و هو المسرح الذي يقع عادة خارج بيئة الحاسوب و يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة و هو قريب من مسرح الجريمة التقليدية ، و من امثلة هذه الجرائم تلم الواقعة على اشرطة الحاسب و الكابلات الخاصة به و مفاتيح التشغيل و الأقراص و غيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس ن و في هذه الحالة تتميز المعاينة بالسهولة كونها منصبة على عناصر ملموسة.

2 – المسرح السبيراني او الافتراضي :

و المسرح الافتراضي يقع عادة داخل البيئة الالكترونية ، و يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله ، و في مقدمتها الجرائم الواقعة على برامج الحاسب الآلي او بياناته او التي تتم بواسطتها ، و كذلك الجرائم التي تتم بطريق الانترنيت و منها جرائم التزوير المعلوماتي و التخريب[1].

و تتميز المعاينة في العالم الافتراضي بصعوبات تتمثل في :

أ – ندرة الاثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلومات .

ب – الاعداد الهائلة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية و حتى يمكن للمحقق القيام بالمعاينة في العالم الافتراضي لابد عليه ان ينتقل الى العالم الافتراضي للمعاينة من مكتبه او اللجوء الى مقهى الانترنيت او الى الخبراء و غيرها من الأماكن التي تساعده في اظهار الحقيقة .

و للمعاينة في الجرائم المعلوماتية اشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة على ان هناك طرق عامة تتوافق مع طبيعة الاتصال بالأنترنيت او الوسيلة المستخدمة مثلا : وسيلة تصوير شاشة الحاسوب ز التي تكون بواسطة آلة تصوير تقليدية

[1] عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 164 .

عن طريق استخدام برمجة حاسوب متخصصة في اخذ صورة لما يظهر على الشاشة و هذا ما يصطلح عليه تجميد مخرجات الشاشة و غيرها[1].

ثالثا : إجراءات معاينة مسرح الجريمة الرقمية

ان إجراءات المعاينة في الجرائم الرقمية تختلف عنها في الجرائم التقليدية بالنظر لخصوصية الجريمة ، و لذلك لابد على المحقق اتباع بعض القواعد و الارشادات الفنية عند معاينة مسرح الجريمة المعلوماتية، و تتمثل هذه الإجراءات في :

1 – عند العثور على حاسبات آلية او أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها ، ادوين الحالة التي هي عليها اذا كانت منطفئة او في حالة تشغيل موصولة بالكهرباء أو بجهاز لاحق آخر ، كما ينبغي ترقيم لواحقها بشكل متسلسل.

2 – يجب تحرير الأوراق المطبوعة على الحاسب الآلي و التي عثر عليها في مسرح الجريمة و وضعها في أكياس حسب حالتها ن و يمكن إعادة الطباعة اذا كان الجهاز في حالة تشغيل و تحرير الأوراق التي تمت طباعتها بالإضافة الى تفقد الجهاز و تسجيل ما اذا كانت هناك برامج تم استخدامها لحظة دخول مسرح الجريمة[2].

3 – عند العثور على دعائم التخزين (أسطوانات ، أقراص ، حوامل مغناطيسية) يجب ترقيمها و تسجيل الحالة التي هي عليها و المكان الذي وجدت فيه (داخل الحاسب الآلي أو خارجه).

4 – عند الانتهاء من الترقيم يجب تصوير الأجهزة و ملحقاتها في الحالة التي هي عليها.

5 – يجب تحرير جميع العينات التي عثر عليها من أجهزة و دعائم داخل أكياس خاصة (بلاستيكية أو ورقية) كما ينبغي حمايتها من الكسر و تاثير العوامل الجوية و

---

[1] نبيلة هبة هروال ، الجوانب الإجرائية لجوانب الانترنيت في مرحلة جمع الاستدلالات ، دار الفكر الجامعي ، الإسكندرية ، 2013 ، ص 212.

[2] محمد امين احمد الشوابكة ، جرائم الحاسوب و الانترنيت، ط 1 ،دار الثقافة للنشر و التوزيع ، عمان ، 2004 ، ص 122.

ابعادها عن أي مجال مغناطيسي لتفادي فقدان المعلومات و ارسالها الى المخبر لاجراء الخبرة.

و تقتضي القاعدة العامة ان تكون هناك استعانة بالخبراء في المسائل العلمية و التقنية التي تحتاج الى اجراء خبرة ، و يحتاج خبراء الأدلة الجنائية الرقمية لتأدية أعمالهم التقنية و اكتشاف المعلومات التي يحتويها كل دليل ، و من خذه الاجهزة و الأنظمة و البرمجيات مايلي :

أجهزة بقدرة عالية على التحليل و تخزين المعطيات.

نسخ من مختلف أنظمة التشغيل المستعملة لدى الافراد و المؤسسات.

نسخ من برامج حذف و كسر كلمات المرور لمختلف الحاسبات ، برامج نسخ الأقراص المدمجة و المحمولة ، برامج الضغط و فك الضغط ، برامج التشفير و فك التشفير ، برامج حماية الأنظمة و الشبكات من الاختراق ، برامج كشف الأجهزة المخفية من الأقراص الصلبة ، برامج استعادة الملفات المحذوفة ، و برامج البحث عن الانترنيت.

قصر المعاينة على الباحثين و المحققين الذين لديهم كفاءة علمية و خبرة فنية في مجال الحسابات و الشبكات و استرجاع المعلومات ، و لن يكونوا قد تلقوا تدريبا جيدا على التعامل مع نوعية الآثار و الأدلة التي يحويها مسرح الجريمة المعلوماتية[1].

و يجب تحرير محضر المعاينة عن طريق كاتب و يجب عند اجرائها اخطار الخصوم بمكان المعاينة و زمانها و يتم توثيق مسرح الجريمة و وصفه بكامل محتوياته بشكل جيد مع توثيق كل دليل على حدى بما فيها الأدلة الرقمية بحيث يتم توضيح مكان الضبط و الهيئة التي كان عليها و من قام برفعه و تحريزه.

و قد أجاز المشرع الجزائري المعاينة في الجرائم المعلوماتية المتلبس فيها بنص المادة 3/47 من قانون الإجراءات الجزائية و التي تنص على انه عندما يتعلق الامر بالجرائم الخاصة بأنظمة المعالجة الآلية للمعطيات فتنه يجوز اجراء المعاينة في كل محل سكني

[1] حسين بن سعيد الغافري ، المرجع السابق ص 10.

أوغير سكني و في كل ساعة من ساعات النهار و الليل و ذلك بناء على اذن مسبق من وكبل الجمهورية المختص [1].

الفرع الثاني : التفتيش في الجرائم الرقمية

يعتبر التفتيش اجراء من إجراءات البحث و التحري و يهدف الى البحث عن ادلة مادية لجناية او جنحة تحقق وقوعها بمكان يتمتع بالحرمة أو تفتيش شخص ، و ان لاجراء التفتيش أهمية بالغة و خطورة معتبرة على الحياة الخاصة ، و لهذا نص عليه المشرع الجزائري بمقتضى قواعد دستورية[2] ، حيث تضمن الدولة عدم انتهاك حرمة منزل فلا تفتيش الا بمقتضى القانون و في اطار احترامه فلا تفتيش الا بأمر مكتوب صادر عن السلطة القضائية المختصة ، هذا و بالإضافة الى نصوص قانون الإجراءات الجزائية و القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها.

غير أنه في الجريمة المعلوماتية يثور التساؤل حول إمكانية تطبيق القواعد العامة للتفتيش على صورة تفتيش نظم الحاسوب و الانترنيت.

لكن من المعروف ان نظم المعالجة الآلية تتكون من مكونات مادية و أخرى غير مادية ترتبط بغيرها عبر شبكات اتصال بعدية[3] .

أولا : تعريف التفتيش

يهدف التفتيش الى جمع الأدلة من مكان وقوع الجريمة

1 – تعريف التفتيش لغة : من مصدر فتش أي بحث و سأل ، فتش الرجل عن الشيء أي تصفحه .

---

[1] صالح شنين ، الحماية الجنائية الحماية الجنائية للتجارة الالكترونية ، أطروحة لنيل شهادة الدكنوراه في القانون الخاص ، جامعة أبو بكر بلقايد تلمسان ، كلية الحقوق ، الجزائر ، 2013 .

[2] المادة 40 من الدستور الجزائري لسنة 1996

[3] عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 378.

2 – تعريف التفتيش قانونا : هو البحث المادي في مكان ما بهدف البحث عن الأشياء المتعلقة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها[1].

3 – تعريف التفتيش فقها : تعددت التعريفات الفقهية في هذا الشأن ، فعرفه الفقه الفرنسي بأنه بحث بوليسي أو قضائي عن عناصر الدليل عن جريمة ما و يمكن وفقا لقواعد قانونية خاصة ان ينفذ في المسكن الخاص باي شخص ، أو في أي مكان آخر حيث يمكن ان توجد أشياء يكون اكتشافها مفيدا في اظهار الحقيقة[2].

و عرف جانب من الفقه التفتيش بانه اجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يتم بالبحث في مستودع السر عن ادلة الجريمة التي وقعت و كل ما يفيد في كشف الحقيقة و يتمثل مستودع السر في شخص المتاهم أو في المكان الذي يعمل به و يقيم فيه.

و يمكن تعريف التفتيش بانه ذلك الاجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي او القضائي الغرض منه البحث عن ادلة الاثبات المرتكبة ، و كل ما يفيد للوصل الى الحقيقة في متابعة شخص يشتبه في انه مرتكب الجريمة[3].

ثانيا : القواعد العامة في تفتيش نظم الحاسوب و الانترنيت

ان الغرض من التفتيش هو البحث عن الأدلة المتعلقة بالجريمة التي تساعد في كشفها و التفتيش في الجريمة الالكترونية ينقسم الى تفتيش ماديات الجريمة الملموسة ، و التفتيش في نظم الحاسوب غير الملموسة و التي تخضع لقواعد عامة هي :

1 – القواعد الشكلية لتفتيش نظم الحاسوب و الانترنيت

---

[1]محمد حزيط ، قاضي التحقيق في النظام القضائي الجزائري ، دار هومة للطباعة و النشر 2009 ، ص 91.

[2]بكري يوسف بكري ، التفتيش عن المعلومات في وسائل التقنية الحديثة ، دار الفكر الجامعي ، الإسكندرية ط 1 ، 2011 ، ص 58 .

[3]بلعليات إبراهيم ، اركان الجريمة و طرق اثباتها في قانون العقوبات الجزائري ، دار الخلدونية ، الجزائر ط 1 ، 2006 ص 214

الأصل ان التفتيش لا تقوم به الا سلطة التحقيق ، فيخضع التفتيش في هذه الحالة للخصائص العامة لكافة إجراءات التحقيق المتمثلة في وجوب التدوين بمعرفة كاتب و السرية عن الجمهور و حضور الخصوم و وكلائهم كلما امكن ذلك.

و هناك شروط للتفتيش تختص بها الجريمة المعلوماتية دون غيرها من بينها توافر الخبرة الفنية لدى القائم بالتفتيش من خلال تلقي المحقق تدريبات فنية خاصة تعرفه كيفية التعامل مع التقنية الحديثة ن و كيفية ضبط الأدلة و الحفاظ عليها في هذا المجال ، كذلك يجب ان يتم التفتيش بصورة صحيحة من الناحيتين الموضوعية و الشكلية[1].

كذلك من القواعد الشكلية التي تحكم التفتيش عدم التجاوز في التفتيش و ذلك بمنع التفتيش عندما لا توجد تحريات جدية تنبئ عن وجود دلائل قوية عن معلومات تفيد في كشف الحقيقة مع وجوب ان يكون التفتيش في حدود الاذن المكتوب المؤرخ و الموقع من الجهة التي أصدرته و الا كان التفتيش باطلا.

و يجب ان يكون اذن التفتيش محدد المدة التي تحتسب من يوم الاذن الى الجهة المأدون لها اجراء التفتيش[2]

و أخيرا بما ان التفتيش عن الملفات الموجودة في جهاز الكمبيوتر من الأمور المعقدة لانها تحوي عمليات الكترونية غامضة يمكن تخزينها حتى على راس ابرة و تحريكها حول العالم في أي وقت ، و يجب عل المحقق اتباع الخطوات التالية :

تجميع فريق عمل يتكون من رجل الضبط القضائي المكلف بالمهمة ، وكيل الجمهورية ، خبير فني قبل القيام بالتفتيش قدر الإمكان .

التعرف قدر الإمكان على نظم الكمبيوتر قبل اجراء التفتيش.

وضع خطة لتنفيذ التفتيش.

---

[1] بكري يوسف بكري ، المرجع السابق ، ص 105 ، 106.

[2] خالد ممدوح إبراهيم ، المرجع السابق ، ص 223.

العناية بمسودة اذن التفتيش –اشتمالها على وصف محل التفتيش– و شرح استراتيجية التفتيش الممكنة.[1]

و بالرجوع الى القانون 09-04 نلاحظ بان المشرع الجزائري بم يوضح بدقة هذه الإجراءات الشكلية و انما اخضعها للقواعد العامة المنصوص عليها في المادة 44 و ما يليها من ق ا ج و من بينها :

أ – الحصول على اذن مكتوب صادر عن السلطات القضائية المختصة : و يكون الاذن صادر عن وكيل الجمهورية او قاضي التحقيق المختص حسب الحالة و ضرورة استظهاره قبل الدخول الى المسكن و القيام بعملية التفتيش .

غير ان القانون 09 –04 نص بضفة عامة على ضرورة اعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش الى منظومة حاسوبية أخرى ، و نص على ان تفتيش رجال الضبطية القضائية لنظم الحواسيب يكون بناء على قواعد ق ا ج التي تفرض عليهم عند الانتقال لتفتيش مساكن الأشخاص المشتبه في ارتكابهم أفعال جنائية ان يكون مصحوبين باذن مكتوب من وكيل الجمهورية او قاضي التحقيق مع وجوب استظهاره قبل الدخول الى المنزل و الشروع في التفتيش طبقا للمادة 05 من القانون 09-04.

ب – تسبيب الاذن : نصت المادة 04 من القانون 09-04 على ان تحدد السلطة القضائية المختصة في الاذن بالتفتيش سبب إصداره و تظهر أهمية ذلك في تقييد سلطة الجهة القضائية المختصة التي وجب عليها اثبات مبررات اللجوء الى اجراء التفتيش لما فيه من مساس بحريات الأشخاص و كذا تمكين الجهة القضائية من بسط رقابتها على المبررات التي استندت اليها السلطة المختصة في اصدار الامر[2].

ج –ذكر بيان وصف الجرم : يجب ان يتضمن الاذن بالتفتيش وصف الجرم الذي يجري التفتيش بشأنه من اجل البحث عن دليل فيه و كذا عنوان المسكن الذي سيتم فيه عملية التفتيش تحت طائلة البطلان.

---

[1] خالد ممدوح إبراهيم ، المرجع السابق ، ص 225 ، 226.

[2] ثابت دنيازاد ، مراقبة الاتصالات الالكترونية و الحق في حرمة الحياة الخاصة في القانون الجزائري ، مجلة العلوم الاجتماعية و الانسانية . جامعة تبسة ، العدد 6 ، 2012.

د – حضور المتهم عملية التفتيش : تنص المادة 1/45 من ق ا ج على وجوب حضور صاحب المسكن عملية التفتيش أو تعيين من يمثله أو حضور شاهدين يتم تسخيرهما من طرف ضابط الشرطة القضائية ، و نظرا للطابع الخاص بالجريمة المعلوماتية أجاز المشرع التفتيش دون حضور صاحب الحق على المسكن أو من ينوبه و دون تسخير شاهدين في حال ما اذا كان هاربا و ذلك بفرض الإسراع في استخلاصه ن اما اذا كان المشتبه فيه محجوز للنظر أو محبوس في مكان آخر و بتعذر نقله لأسباب امنية أو لمقتضيات النظام العام أو وجود خطر اختفاء الأدلة هلال مدة نقله لمكان اجراء التفتيش فانه في هذه الحالات يجوز اجراء التفتيش من دونه و لكن بحضور شاهدين خاضعين لسلطة ضابط الشرطة القضائية[1] ، و هذا من اجل الحصول على الدليل المستهدف من عملية التفتيش في الوقت المناسب.

هـ – المدة القانونية للتفتيش :و هو ان يتم التفتيش في الوقت المحدد قانونا من الساعة الهامسة صباحا الى الساعة الثامنة مساء ن غير انه و نظرا لطبيعة الجرائم المعلوماتية و سرعة اتلاف و تعديل المعطيات خاصة اذا علم الجاني بوجود تفتيش مما يؤدي الى محو الأدلة فقد أجاز المشرع في المادة 47 فقرة 03 من ق ا ج التفتيش و المعاينة و الحجز في كل محل سكني او غير سكني في أي ساعة من ساعات النهار او الليل بناء على اذن مسبق من وكيل الجمهورية و هنا فان المشرع غلب المصلحة العامة على المصلحة الشخصية للافراد نظرا لذاتية الجريمة المعلوماتية المتمثلة في إمكانية اختفائها بسرعة و من جهة أخرى افتراض كون الدليل الرقمي هو الدليل الوحيد في الدعوى الجزائية و من ثم ارتكاز كل العملية الاثباتية على وجوده[2].

2 – القواعد الموضوعية لتفتيش نظم الحاسوب و الانترنيت :

يجب مراعاة القواعد التالية عند قيام المحقق بعملية التفتيش :

---

[1]احسن بوسقيعة ، التحقيق القضائي ، دار هومة للطباعة و النشر، الجزائر ، ط 10 ، 2013 .

[2]جولحي عبد الستار، جرائم الحاسوب – دراسة مقارنة بين الشريعة الإسلامية و القانون الجزائوي– مذكرة تخرج تدخل ضمن متطلبات الحصول على شهاد الماستر في العلوم الإسلامية ، جامعة الشهيد حمه لخضر ، كلية العلوم الاجتماعية و الإنسانية ، قسم العلوم الإنسانية ، الجزائر ، 2015 ، ص 64.

أ – وجود سبب للتفتيش : الاذن بالتفتيش لا يصح إصداره الا لضبط ماديات الجريمة الواقعة بالفعل و اتهام شخص او عدة اشخاص بارتكابها و لذلك يجب توافر مجموعة من الشروط تتمثل في :

–ان يكون التفتيش بصدد جريمة معلوماتية واقعة بالفعل سواء كانت جنحة او جناية فمن غير الممكن القيام بالتفتيش دون وقوع جريمة ، غير ان المشرع خرج عن هذا المبدأ و جعل من التفتيش مهمة وقائية الهدف منها هو الحيلولة دون وقوع الجريمة المعلوماتية من خلال القيام بعمليات المراقبة المسبقة للاتصالات طبقا للمادة 03 من القانون 09–04[1]

في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الاقتصاد الوطني فهذا التفتيش وقائي قد تسفر عنه ادلة يمكن ان تكون اثبات لتخطيط مسبق يراد به ارتكاب جرائم ذات خطورة على الامن الداخلي للدولة ، و هناك من يعتبر هذا الأسلوب الوقائي اعتداء فعليا على الحياة الخاصة للأشخاص لان القانون لم يحدد صفات من يقع عليهم هذا التفتيش.

–لابد من اتهام شخص او اشخاص معينين بارتكاب هذه الجريمة الالكترونية او المشاركة في ارتكابها.

لابد من توافر دلالات و امارات قوية على وجود أجهزة ، ادلة معلوماتية تفيد في كشف الحقيقة لدى المتهم.

ب – محل التفتيش : التفتيش في الجريمة التقليدية ينصب على شخص المتهم او فير المتهم و كذلك على مسكن المتهم و ما في حكمه و ملحقاته غير ان المحل في الجريمة المعلوماتية هو جهاز الحاسوب و شبكة الانترنيت الذين يكونان محلا للاعتداء و ليس وسيلة لارتكاب الجريمة فحسب ، فيقع التفتيش على الأشياء المادية و برامج الحاسب الآلي و بياناته أي كل ما يحتويه مشروع السر و كب ماله علاقة بالجريمة من أجهزة الحاسوب و الآلات و النظم و البرامج و الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش ، و نظرا لامكانية قيام الجاني بالتخلص من البيانات التي يستهدفها التفتيش عبر

[1]زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، الجزائر ، بدون طبعة ، 2011.

ارسالها من خلال نظام معلوماتي من مكان الى آخر ة ارتباط شبكة الحواسيب ببعضها البعض فقد أجاز المشرع في المادة 05 من القانون 09-04 تمديد التفتيش بسرعة الى منظومة معلوماتية أخرى او جزء منها بعد اعلام السلطة القضائية المختصة مسبقا بذلك ، و بالتالي فالتفتيش قد يقع على الأشخاص او المساكن التي تحتوي على تلك الأجهزة او الشبكات المعلوماتية[1]. و يتم تحرير محضر يثبت فيه ما تم من إجراءات.

ثالثا: تفتيش المنظومة المعلوماتية

و تضم المنظومة المعلوماتية المكونات المادية للحاسب الآلي و المكونات المعنوية و الشبكات المتصلة بالحاسوب عن بعد.

1 – تفتيش المكونات المادية للحاسب الآلي :

تخضع المكونات المادية لنظام المعالجة الآلية للمعطيات لإجراءات التفتيش المنصوص عليها في المادة 44 من ق ا ج الجزائري أي انه يجب مراعاة مكان وجود ذلك الحاسوب اثناء مباشرة ذلك الاجراء قيما اذا كان مكانا عاما أو خاصا ذلك ان لصفة المكان أهمية خاصة في مجال التفتيش ، فاذا كان موجودا في مكان خاص كمسكن المتهم فلا يجوز تفتيشه الا في الحالات التي يجوز فيها تفتيش مسكنه و بنفس الضمانات المقررة قانونا كما سبق بيانه.

و يرد التفتيش على المكونات المادية للحاسب الآلي و ملحقاته بما في ذلك البيانات المخزنة في اوعية او رسائل مادية كالأشرطة الممغنطة و الأقراص الصلبة و الضوئية.

2 – تفتيش المكونات المعنوية للحاسب الآلي : يقصد بها أنظمة الكمبيوتر و البيانات المخزنة فيه التي جرى التلاعب فيها او تغييرها ن و غيرها من الوسائط التي تساعد على تخزين المعلومات[2].

كذلك و ان الامر يتعلق بمدى صلاحية نظم الحاسوب للتفتيش و بالاجهزة المختصة بالتفتيش نظام الحاسوب و الانترنيت.

---

[1] خالد ممدوح إبراهيم ، المرجع السابق ، ص 222 .

[2] خالد عياد الحلبي ، المرجع السابق ، ص159.

اما مدى صلاحية معطيات الحاسوب للتفتيش فهو امر تفرضه طبيعة الجريمة المرتكبة و الراي المستقر عليه ان معطيات الحاسوب تصلح للتفتيش عن الأدلة الجرمية و ضبطها لان الغاية من التفتيش هو الحصول على دليل خاص بالجريمة و كشف الغموض الذي أحاط بها[1].

و يتضح موقف المشرع الجزائري من خلال النص في المادة 05 من القانون 09-04 على إجازة تفتيش المنظومات المعلوماتية و قد نصت على " يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في اطار قانون الإجراءات الجزائية....الدخول بغرض التفتيش و لو عن بعد الى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المحزنة فيها و كذا منظومة تخزين معلوماتية.

3 – تفتيش الشبكات المعلوماتية المتصلة بالحاسوب (التفتيش عن بعد)

تعرف الشبكة المعلوماتية بانها مجموعة مكونة من اثنين فاكثر من أجهزة الحاسوب و المتصلة ببعضها اتصالا سلكيا او لا سلكيا و قد تكون الأجهزة موجودة في نفس الموقع و تسمى بالشبكة المحلية او قد تكون موزعة في أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف و تسمى بالشبكة بعيدة المدى[2]

و مسالة التفتيش في هذه الحالة على درجة من الخطورة تتعلق بالتفتيش عن بعد و ذبك نتيجة للطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أداة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي بتفتيش و هو ما يزيد المسالة تعقيدا باعتبار ان الشبكة المعلوماتية ممتدة في انحاء العالم.

رابعا : بطلان التفتيش في الجرائم الرقمية

---

[1] عبد الفتاح بيومي ، المرجع السابق ، ص 159.

[2] يتم الاتصال و نقل المعلومات بواسطة الشبكية باشكال ثلاث هي :

اتصال احادي الجانب و يام بين جهاز الحاسوب المستفيد مع جهاز مركزي

اتصال ثنائي غير متكامل المعلومات و يتم بين جهازين يرسيل الأول المعلومات و الثاني يستقبلها و بعد انتهاء الأول يقوم الثاني بارسال المعلومات و يستقبلها الأول و هكذا

و اتصال ثنائي كامل المعلومات و يتم بين جهازي الارسال و الاستقبال في نفس الوقت.

راعى المشرع في شان قواعد التفتيش الموازنة بين حماية حريات الاشخاص و عدم المساس بحقهم في الخصوصية و عدم افشاء الاسرار[1]، و حصانة مساكنهم و بين المصلحة العامة في الكشف عن الحقيقة و لذلك على جهة التحقيق مراعاة القواعد الموضوعية و الشكلية للقيام بالتفتيش حتى لا يترتب على ذلك البطلان .

وقد اختلف الفقه الجنائي في جعل قواعد البطلان من النظام العام من عدمه غير ان الراجح هو جعلها قواعد جوهرية يترتب على مخالفتها البطلان و هذا البطلان لا يتعلق بالنظام العام.

الفرع الثالث : الضبط في الجرائم الرقمية

ان النتيجة الطبيعية التي ينتهي اليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها اثناءه ، فالضبط اذن هو غاية التفتيش القريبة و الأثر المباشر الذي يسفر عليه الاجراء.

و الأساس القانوني للضبط هو العلاقة التي تربط بينه و بين الأشياء المتعلقة بالجريمة التي يشملها التحقيق و التي تفيد في كشف الحقيقة ما طان منها ضد المشتبه فيه أو ما كان في مصلحته.

أولا : تعريف الضبط في الجرائم الرقمية

الضبط هو وضع اليد على شيء متصل بجريمة معلوماتية وقعت بفيد في كشف الحقيقة عنها و عن مرتكبها.

و لقد تعودت جهات التحقيق في الجرائم التقليدية ان يقع الضبط على الأشياء المادية فقط بوصفها ادلة مادية للجريمة التي يجري التفتيش بشأنها ، لكن في مجال الجرائم المعلوماتية الطبيعة العلمية المعقدة للدليل الرقمي الذي يوجب التفتيش عنه و ضبطه لإثبات هذا النوع من الجرائم ليس كالدليل التقليدي ، فالبيئة الافتراضية لا تنتج سكينا او سلاحا ناريا بل تنتج نبضات رقمية تشكل قيمة و جوهر الدليل الرقمي .

[1] بكري يوسف بكري ، ص 60.

ثانيا : حجز المعطيات المعلوماتية

ان الأشياء المضبوطة في الجرائم المعلوماتية تكون ذات طبيعة معنوية فقد يرد ضبط الأشياء على عناصر معلوماتية منفصلة ممثل الأسطوانات الممغنطة ، و هنا لا يثور أي اشكال عند القيام بالضبط لكن الصعوبة تكون عندما يلزم ضبط النظام كله أو الشبكة كلها لانها تحتوي على عناصر لا يمكن فصلها ، اما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الاتية : وحدات الادخال (لوحة المفاتيح ، الفأرة ، نظام القلم الضوئي) ، و ضبط وحدة الإخراج (الشاشة ، الطابعة ، الرسم ، المصغرات الفيلمية) و كل ما يتم ضبطه من بيانات الكترونية يتعين تحريرها و تأمينها فنيا[1].

و لقد نصت المادة 06 من القانون رقم 09-04 على انه "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية مغطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها و انه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز و الوضع في احراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية..." و بالتالي فقد كان اتجاهه هو امكانية حجز المنظومة المعلوماتية برمتها بشروط، كما حرص المشرع على جعل المعلومات محل البحث في مأمن باستخدام التقنيات اللازمة لمنع الوصول اليها ، و ذلك في حالة استحالة حجزها لأسباب تقنية كما لو كانت المعطيات مخزنة بأنظمة التشغيل التي لا يمكن نسخها و هو ما نصت عليه المادة 07 من القانون 09-04 و ذلك لمنه تهريبها و تدميرها.

و في النهاية نستخلص ان هناك نوعين من إجراءات الضبط:

-اجرءات مبدئية تحفظية : الهدف منها هو الحفاظ على البيانات المخزنة التي تكون لها أهميتها في التحقيق ببقائها في امكنتها في النظام المعلوماتي للكمبيوتر او في دعامة التخزين و منع الوصول اليها أو الغائها أو التصرف فيها ، و ذلك للكشف عن مرتكب الجريمة و سهولة اثباتها .

---

[1]بوعناد فاطمة زهرة ، مكافحة الجريمة الالكترونية في التسريع الجزائري ، مجلة الندوة للدراسات القانونية ، سيدي بلعباس ، 2013 ،العدد 01 .

-إجراءات لاحقة بالضبط : و هي إجراءات لاحقة للتفتيش و الدخول و يقصد بها جميع البيانات سواء بأحد دعامة تخزين المعلومات أو اخذ نسخة من البيانات المخزنة بها أو بالنظام المعلوماتي للكمبيوتر في ورق أو أقراص

ثالثا : ضوابط الحجز في الجرائم الرقمية

خص المشرع حجز الأدلة وفقا لنص المادة 84 من ق ا ج بضوابط تتمثل فيما يلي:

الاطلاع على المستندات المراد حجزها و هذا مخول فقط لقاضي التحقيق او ضابط الشرطة القضائية الذي انابه عته قبل حجزها و وضعها في احراز مختومة و يحرر محضرا بضبطها .

الاحترام التام لمقتضيات و ضرورات التحقيق و على الاخص ضمان احترام سر المهنة و حقوق الدفاع.

كما نصت الماد 84 السالفة الذكر ان الاحراز و الوثائق المحجوزة لا يتم فتحها الا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا ، و بالتالي فالمشرع حافظ على مبدأين اساسين هما السرية و حقوق الدفاع و هو اكنه المادة 09 من القانون 09-04 .

المطلب الثاني : إجراءات التحقيق الجنائي الشخصية في الجرائم المعلوماتية

اذا كانت الإجراءات المادية تتعلق بالشيء محل التحقيق فان الاجراءات الشخصية هي إجراءات تتعلق بالشخص قي حد ذاته و تتمثل قي الخبرة و الشاهد الالكتروني.

الفرع الاول : الخبرة في الجرائم الرقمية

لقد ترتب عن التطور التقني في نظم المعالجة الآلية الى تغير كبير في المفاهيم السائدة حول الدليل و قاد مثل هذا القول الى تعاظم دور الاثبات العلمي و اعلان انضمام التقنية الى عالم الخبرة القضائية ، ذلك ان اشتقاق الأدلة الرقمية المطلوبة في اثبات الجرائم المعلوماتية و كشف انماطها أمر يطلع به الخبراء المتخصصون في هذا المجال.

و لا يمكن التصور ان يرفض القاضي اللجوء الى نذب خبير في قضايا تقنية المعلومات ، اذ هي قضايا فنية تتطلب خبرة خاصة ، و يكون حكمة مجانبا للمنطق العلمي و معيبا اذا لم يستند الى الخبرة التقنية في هذا المجال[1] تحقيقا لمبدأ عام هو مبدأ التخصص.

و تعتبر الخبرة من اهم الإجراءات التي تتخذ للتثبيت عن الأدلة التي تساعد في الكشف عن الجريمة الالكترونية ، كون الجريمة الالكترونية ترتكب بوسائل مستحدثة و معقدة بصعب التعامل معها.[2]

أولا : تعريف الخبرة في الجرائم الرقمية

لمعرفة الخبرة في الجريمة الالكترونية يجب التطرق أولا لتعريف الخبرة لغة و اصطلاحا.

1 – تعريف الخبرة لغة : الخبير لغة هو اسم من أسماء الله تعالى و هو العالم بما كان و ما سيكون.

2 – تعريف الخبرة اصطلاحا : الخبير في اطلاح المحاكمة هو من يعين للتدقيق في مختلف الأمور المتعلقة بشتى القضايا ، و يكون لرأيه فيها الراي الفاصل.

و الخبرة هي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات ، فهي في الحقيقة ليست دليلا مستقلا عن الدليل المادي و انما هي تقييم فني لهذا الدليل و العنصر المميز للخبرة عن غيرها من إجراءات الاثبات كالمعاينة و الشهادة و التفتيش.[3]

و الخبرة في مجال المعلوماتية تكون بتحري الحقيقة عن طريق جمع المعلومات من الأدلة الرقمية و تحصيلها من خوادم الموقع و من الجهاز المعتدى عليه بعد التوصل الى تحديده ثم يقوم الخبير بعملية تحليل رقمي لها بمعرفة كيفية اعدادها البرمجي و نسبتها الى

---

[1] عادل عزام سقف الحيط ، جرائم الدم و القدح و التحقير المرتكبة غبر الوسائط الالكترونية ، دراسة قانونية مقارنة ، دار الثقافة للنشر و التوزيع ، ط 1 ،2011 .

[2] ضريفي نادية ، سلطات القاضي الجنائي في تقدير الدليل الالكتروني المستمد من التفتيش الجنائي ، مجلة الأستاذ الباحث للدراسات القانونية و السياسية المجلد 04 ، العدد 02 ، ص 124.

[3] غبد الفتاح بيومي الحجازي ، المرجع السابق ، ص 321 .

مسارها الذي اعدت فيه و تحديد عناصر حركتها ثم التوصل الى معرفة بروتوكول الانترنيت للحاسوب الذي صدرت منه الرسائل و النبضات الالكترونية.[1]

ثانيا : أساليب عمل الخبير و دوره في حفظ الدليل في الجريمة الالكترونية

الخبير هو كل شخص له دراية بمسألة من المسائل ، و قد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشهر المحقق بتوافرها في نفسه فيمكنه ان يستشير فيها خبيرا.

و من المعلوم ان هناك حاجة دائمة الى خبراء و فنيين عند وقوع الجريمة الالكترونية و يمتد عملهم ليشمل المراجعة و التدقيق على العمليات الآلية للبيانات ، و كذلك اعداد البرمجيات و تشغيل الحاسب الآلي و علومه ، و ان نجاح اعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة و تخصص هؤلاء الخبراء ، و كذا يجب على المحقق الجنائي أن يحدد الخبير الالكتروني دوره في المسالة الانتداب فيها على وجه الدقة .

و هناك اسلوبان لعمل الخبير هما :

1 – القيام بتجميع و تحصيل المجموعة المواقع التي تشكل جريمة في ذاتها كجريمة التهديد أو النصب و جرائم النسخ ...الخ ، ثم يقوم الخبير بعملية تحليل رقمي لها ، و ذلك لمعرفة كيفية اعدادها البرمجي و نسبتها الى مسارها الذي اعدت فيه و تحديد عناصر حركتها ، و كيف تم التوصل الى معرفتها و أخيرا التوصل لمعرفة برتوكول الانترنيت (ا ب) الذي ينسب الى جهاز الحاسوب الذي صدرت عنه هذه المواقع[2].

2 – القيام بتجميع و تحصيل لمجموعة المواقع الذي لا تشكل موضوعها جريمة في ذاته ، و لكن الجرائم تقع من جراء تتبع موضوعات هاته المواقع ، مثلما ما هو الحال في المواقع التي تساعد الغير على معرفة جرعات المخدرات و المؤثرات العقلية حسب وزن الانسان بإيهامه انه اذا تم تتبع التعليمات الواردة فيها لن يصل الى الشخص الى حالة ادمان

---

[1] سعيداني نعيم ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، تخصص علوم جنائية ، جامعة الحاج لخضر ، باتنة ، 2012–2013 ، ص 171 .

[2] خالد ممدوح إبراهيم ، المرجع السابق ، ص 301.

، كذلك الشأن بالنسبة لكيفية اعداد القنابل و تخزينها أو كيفية التعامل مع القنابل الزمنية.. الخ.[1]

و التحفظ على الأدلة الالكترونية تحتاج الى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الكمبيوتر.

المبحث الثاني: الآليات الإجرائية الخاصة للتحقيق الجنائي في الجرائم الرقمية

نتيجة التطور الحاصل في مجال التكنولوجيات الرقمية أصبح المجرمين أكثر ذكاء باستعمالهم لوسائل تقنية حديثة في مختلف الجرائم, التي سهلت تنقلاتهم الإجرامية والتي امتدت الى خارج الحدود الوطنية لتشمل دول أخرى وتهدد أمنها واستقرارها وعليه أصبح من الصعب تتبع تحركات هاته الشبكات الإجرامية مما استدعى المشرع الى التدخل لمكافحة هذا النوع من الجرائم عن طريق تعديل القانون رقم 06-22 المؤرخ في 2006/07/20 المتضمن قانون الاجراءات الجزائية حيث أدخل أساليب البحث والتحري الخاصة التي تقوم بها جهات متخصصة بغية التحري في جرائم خطيرة مقررة في قانون العقوبات كما استحدث المشرع القانون رقم 04/09 المؤرخ في 2008/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

وعليه سوف نتطرق الى هذه الأساليب من خلال ثلاث مطالب بحيث يتضمن المطلب الأول اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والمطلب الثاني مراقبة الاتصالات الالكترونية والمطلب الثالث نتناول فيه التسرب .

المطلب الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

سعيا من المشرع لمكافحة الجرائم الخطيرة ومراقبة نشاطات الشبكات الاجرامية الذين يستعملون تقنيات حديثة تتسم بالسرعة والفعالية قام بإدخال الوسائل التقنية في مجال البحث والتحري في التحقيقات الجنائية الخاصة بهذه الجرائم ولقد نظم المشرع الجزائري كل من اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المواد من 65 مكرر 5 إلى غاية

[1] خالد ممدوح إبراهيم ، ص 301.

65 مكرر 10ق ا ج بحيث يجوز لضباط الشرطة القضائية واعوانهم القيام بهذه الاعمال إذا اقتضت ضرورة التحري في الجرائم المتلبس بها وفي بعض الجرائم الأخرى عن طريق إذن من وكيل الجمهورية أو قاضي التحقيق.

وعليه سنتناول هذا المطلب من خلال ثلاث فروع، الفرع الاول نتطرق فيه الى تعريف اعتراض المراسلات، والفرع الثاني نتطرق فيه الى تعريف تسجيل الأصوات والتقاط الصور، والفرع الثالث ندرس فيه اجراءات وشروط اعتراض المراسلات وتسجيل الاصوات والتقاط الصور.

الفرع الاول: تعريف اعتراض المراسلات

لم ينص قانون الإجراءات الجزائية على تعريف خاص لعملية اعتراض المراسلات بل اكتفى بتنظيمها في المواد المذكورة اعلاه فقد عرفها الباب الثالث من القانون الفدرالي الامريكي لسنة 1968 انها الاكتساب السمعي عن طريق السمع لمحتويات أية أسلاك أو أية اتصالات شفوية عن طريق استخدام جهاز الكتروني أو ميكانيكي او جهاز اخر وبصفة عامة فإن أي جهاز يمكن استعماله لتسجيل اتصالات يقع ضمن ما يقصده القانون[1] .

وعرفها اجتماع لجنة الخبراء للبرلمان الاوربي بيستراسبورغ بتاريخ 2006/10/06 المتعلق بأساليب التحري التقنية وعلاقتها بالأفعال الارهابية بانها عملية مراقبة سرية للمراسلات السلكية واللاسلكية وذلك في اطار البحث والتحري عن الجريمة وجمع الادلة او المعلومات حول الاشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجرائم .

ويقال أيضا يتمثل في اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ويقصد به التصنت التلفوني[2] .

وعرفها القضاء بالتصنت على المكالمات وهو تقنية يتم من خلالها الإعتراض عن طريق ربط خط هاتفي لشخص ما مع اللجوء الى تسجيل المكالمات في أشرطة مغناطيسية .

---

[1] حمزة قريشي ، المرجع السابق ، ص 36.

[2] احسن بوسقيعة المرجع السابق ص 113.

ويراد بهاأيضا تلقي أية مراسلة مهما كان نوعها مكتوبة أو مقروءة أو مسموعة وبغض النظر عن وسيلة ارسالها وتلقيها سواء كانت سلكية أو لاسلكية من غي الشخص الموجه اليه أو الذي أرسلها [1].

ويمكن القول أنها اجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع الى الحديث ومن ناحية اخرى حفظه على الاشرطة عن طريق أجهزة مخصصة لهذا الغرض .

وهنا يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة فبينما يكون الأول دون رضا المعني فيكون الثاني بطلب أو برضا صاحب الشأن ويخض لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

وقد حدد المشرع الجزائري في نص المادة 65 مكرر 05 الفقرة02 ق إ ج نوع المراسلات محل الإعتراض وهي المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية .

وبما ان المشرع لم يتطرق الى مفهوم اعتراض المراسلات فهل كان يقصد بها التنصت الهاتفي فقط واستبعد بذلك الخطابات الخطية التي تتم عن طريق البريد حرصا منه على ضمان حرية المراسلات بين الافراد المكفولة دستوريا ام ان الامر يمتد الى هذه المراسلات المتبادلة بالحاسب الالي لكل من المتهم والغير ممن يتبادلون معه المراسلات هناك من يرى ان المشرع قصد أساس التنصت الهاتفي إذ كثيرا ما تتطلب إجراءات التحري والتحقيق اللجوء الى مراقبة المحادثات الهاتفية غير انه وعلى اعتبار ان وسائل الاتصال الحديثة ساهمت بشكل كبير في تسهيل ارتكاب جرائم منظمة سواء عن طريق المكالمات الهاتفية أو المراسلات الإلكترونية المتبادلة عبر الشبكات المعلوماتية فقد أجازت اتفاقية بودابست للجرائم الالكترونية الاعتراض الشرعي لكل أشكال النقل الإلكتروني للبيانات سواء

---

[1] تاصيلية تحليلية و مقارنة للتنصت على المحادثات التلفونية و التي تجرى عبر الانترنات و الاحاديث الشخصية نظريا و علميا دار المطبوعات الجامعية ،الإسكندرية ، ط 1 ، 2019 ، ص 150 .ياسر الأمير فاروق ، مراقبة الاحاديث الخاصة في الإجراءات الجنائية ، دراسة

تم عبر التلفون أو الفاكس أو البريد الإلكتروني ...إلخ وتشمل الإتصالات محل الاعتراض محتوى غير مشروع أو دليل على الأفعال الإجرامية الخطيرة التي يعرفها القانون الداخلي لكل دولة طرف في الإتفاقية مما يستوجب ضرورة اعتراض المراسلات الالكترونية المتبادلة عبر الحاسب الآلي أيضا لدرء خطر الجريمة وملاحقة الجناة وهذا ما قصده المشرع الجزائري صراحة من خلال اعتراض المراسلات السلكية واللاسلكية وما اتجه إليه من خلال القانون 04/09 حيث أجاوضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية والقيام بالتفتيش والحجز داخل المنظومة المعلوماتية .

وما اتجه إليه أيضا من خلال القانون 03/2000 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية حيث أجاز اعتراض المراسلات المتبادلة عن طريق التلغراف والفاكس والبريد الالكتروني (الايميل) الرسائل القصيرة و sms.

عن طريق الهاتف المحمول والاتصالات المرئية.....الخ وإذا كان الحال كذلك وكل إشارة أو كتابة أو صورة مطلوب التقاطها أو مكالمة هاتفية يجوز أن تكون محل للإعتراض .

وعليه يمكن أن نقول وجب أن يتضمن أسلوب اعتراض المراسلات خصائص معينة هي التي تساعد في تحديد مضمونها وطبيعة العمل به وتتمثل في :

- أن يتم خلسة دون علم ورضا صاحب الشأن .
- يمس بالحق الشخصي في سرية الحديث .
- يستهدف الحصول على دليل غير مادي لأن الأحاديث والأقاويل غي مادية.
- يستخدم فيه أجهزة قادرة على التقاط الأحاديث خاصة مع تطور التكنولوجيا أصبح هناك أجهزة مختلفة الأحجام والأشكال.

الفرع الثاني:تسجيل الأصوات والتقاط الصور

لم يقدم المشرع تعريف صريحا لتسجيل الأصوات والتقاط الصور وبالرجوع الى المادة

65 مكرر05 ق إ ج نستشف أن المقصود من تسجيل الأصوات هو وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة او عمومية[1] .

ويقصد به كذلك حفظ الحديث على جهاز معد لذلك بهدف الاستماع إليه مرة أخرى.

والتسجيل الصوتي الذي يهمنا في هذه الدراسة هو الذي يجريه رجال الضبطية القضائية مكن أجل التحري والتحقيق عن الجرائم الخطيرة السابقة الذكر .

ويمكن القول أنه تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان خاص أو عام .

أما التقاط الصور فنفس الامر كذلك لم يعرف المشرع الجزائري هذه العملية صراحة وقد أشار اليها بالالتقاط وهناك من عرفها من أنها تلك العملية التقنية التي تتم دون موافقة المعنييين من اجل التقاط صور لشخص او عدة أشخاص وغن تواجدوا في مكان خاص.

ويمكننا ان نعرف تسجيل الأصوات والتقاط الصور بانها تسجيل المحادثات الشفوية بين الأفراد بصفة سرية او خاصة في مكان عام اوخاص وكذلك التقاط صور لشخص او عدة أشخاص يتواجدون في مكان خاص .

وتجدر الإشارة أن المشرع عندما جمع بين اعتراض المراسلات وتسجيل الاصوات والتقاط الصور وجعلها في عنوان واحد لاعتبار أنهم يؤدون نفس الغرض متى توافرت الضمانات المنصوص عليها في المواد من 65 مكرر5 إلى غاية 65 مكرر10 ق إ ج.

الفرع الثالث: إجراءات وشروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

حق الانسان في الخصوصية وأن يعيش حياة هادئة من المبادئ القدسية التي كرسها الدستور في المادة 39 منه الا أن المشرع الجزائري ولضرورة التحقيق في بعض الجرائم الحساسة سمح بالقيام بمثل هذه العمليات بحيث تكون مصلحة التحقيق وكشف المجرمين أولى بالرعاية من الحفاظ على أسرار الحياة الخاصة وذلك من خلال المواد من 65 مكرر5

[1] احسن بوسقيعة K المرجع السابق ص 113.

الى غاية 65 مكرر 10 ق إ ج. حيث أتاح للضبطية القضائية حق استعمال الأساليب والوسائل التقنية في إطار البحث والتحري في الجرائم المستحدثة ولكن وفقا للشروط والإجراءات التالية:

01/ طبيعة الجريمة:

بالرجوع الى نص المادة 65 مكرر 5 ق إ ج تكون اجراءات التحري الخاصة في حالة التلبس أو التحقيق الابتدائي في جرائم المخدرات – الجريمة المنظمة العابرة للحدود الوطنية – الجرائم الماسة بأنظمة المعالجة الالية – جرائم تبييض الأموال– الجرائم الارهابية جرائم الصرف والفساد واذا اكتشفت اثناء التحريات الخاصة جرائم أخرى غير مذكورة في الاذن فهذا لا يكون سببا لبطلان الإجراءات العارضة وفقا لأحكام المادة 65 مكرر 2/6 ق.إ.ج.

02/ الإذن من وكيل الجمهورية أو قاضي التحقيق: وهو شرط أساسي لمباشرة عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور ، ويشترط لصحته ما يلي:

– أن يكون مكتوبا وهذا كمبدأ عام من الأعمال المخولة للضبطية القضائية حسب نص المادة 18 ق.إ.ج[1].

– أن يتضمن جميع المعلومات المكونة للجريمة والتي تسمح لوكيل الجمهورية أو لقاضي التحقيق بالتعرف على الإتصالات المطلوب إلتقاطها والأماكن المقصودة من ذلك .

تحديد المدة الزمنية للعملية بأربعة أشهر قابلة للتجديد حسب مقتضيات التحري.

03/ الرقابة القضائية: يجب خضوع هذه العمليات المسموح بها قانونا الى رقابة واشراف وكيل الجمهورية المختص. كما انه في حالة فتح تحقيق قضائي فإن هذه العمليات تكون بإذن من قاضي التحقيق وتحت رقابته.

[1] المادة 18 فقرة 01 من قانون الإجراءات الجزائية " يتعين على ضباط الشرطة القضائية أن يحرروا محاضر باعمالهم و ان يبادروا بغير تمهل الى اخطار وكيل الجمهورية بالجنايات او الجنح التي تصل الى علمهم".

04/ وضع التقنية: بعد الحصول على الإذن يسمح لضباط الشرطة القضائية بوضع الترتيبات التقنية في الأماكن الخاصة والعمومية وغيرها دون موافقة وعلم الأشخاص المعنيين وهذا للمحافظة على سرية العملية ، كما أجاز المشرع أن تكون هذه الترتيبات خارج الميقات القانوني ، أي خارج المواعيد المحددة في نص المادة 47 ق. إ.ج

05/ الإطار المكاني للأساليب التقنية في التحري عن الجرائم: بالرجوع إلى المادة 65 مكرر 5 ق.إ.ج نجدها نصت على الاماكن التي يتم فيها استعمال الوسائل التقنية وهي الاماكن العمومية – الأماكن الخاصة – المحلات السكنية [1].

06/ المحافظة على السر المهني يلزم على الضبطية القضائية أثناء اداء مهامهم او وظيفتهم بكتمان السر المهني الذي اطلعوا عليه سواء كان عن طريق تسجيل الاصوات او التقاط فقرة الصور خاصة إذا تعلق الأمر بأماكن يشغلها أشخاص ملزمون بكتمان السر المهني مثل مكاتب المحامين او الموثقين او إذا تعلق الأمر بأشخاص يحملون أسرار مهنية مثل القضاة, الأطباء.....

فحتمية عدم استثناء هذه الأماكن من إجراء الاعتراض يستوجب اتخاذ التدابير اللازمة لضمان احترام السر المهني الذي يخصها .

07/ تسخير الأعوان المؤهلين والمكلفين بالمواصلات السلكية والاسلكية: أجاز المشرع لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له باستعمال الوسائل الخاصة في البحث والتحري ولقاضي التحقيق أو ضباط الشرطة القضائية الذي ينوبه أن يكلف عون مؤهل وصاحب خبرة وكفاءة في مجال المواصلات السلكية واللاسلكية بالتكفل بالجوانب التقنية لعمليات اعتراض المراسلات وتسجيل الأصوات وهذا ما جاء في نص المادة 65 مكرر 8 ق إ ج.[2]

---

[1] الأماكن العامة : و هي التي يتم الدخول اليها و الخروج منها بحرسة تامة كالأسواق ⊣ الأماكن الخاصة هي الأماكن او المحلات المعدة لنشاطات معينة كالفنادق و العيادات ، المحلات السكنية عرفتها المادة 355 من قانون العقوبات أنظر اكثر لوجاني نور الدين ، نفس المرجع ، ص 9.

[2] انظر المادة 65 مكرر 8 من قانون الإجراءات الجزائية.

08/ تحرير محضر عن العملية: كمبدأ عام يجب على ضباط الشرطة القضائية تدوين وتحرير تقارير عن كل عملية تطبيقا لنص المادة 65 مكرر09 ق إ ج التي جاء فيها أنه يجب تحرير محضر يذكر فيه جميع التفاصيل العملية من بدايتها الى نهايتها وكذلك يذكر فيه تاريخ وساعة بداية العملية وتاريخ الانتهاء منها.[1]

أما بخصوص نتائج التحريات التي تتعلق بمضمون المراسلات المسجلة والصور الملتقطة فعلى المأذون له بهذه العمليه أو المناب أن ينسخ أو يصف المحتوى الضروري والمهم لاظهار الحقيقة في محضر ليودع بالملف أما إذا كانت المكالمات باللغة الأجنبية فإنه يتم الاستعانة بمترجم لترجمة محتوى المكالمات ونسخها.

09/ ضبط التسجيلات ووضعها في أحراز: بما أن التسجيلات أو الأشرطة المصورة تعتبر أدلة اثبات مادية أصلية تقتضي الشرعية الإجرائية حفظها بطريقة خاصة وذلك بوضعها في أحراز مختمة بنا يضمن عدم التلاعب بها أو العبث في الحديث المسجل سواء بالحذف أو الاضافة وضمها الى المحضر وهذا ما نستنتجه من خلال إسقراء نصوص المواد 18 و45 ق.إ.ج وتجدر الاشارة هنا الى ان المشرع الجزائري لم يشر الى عرض هذه التسجيلات والصور على المشتبه فيهم في مرحلة جمع التسجيلات ويرجع ذلك الى الطابع السري الذي تتميز به هذه الجرائم الخطيرة على عكس مانجده في المادة 42 من نفس القانون حيث اوجب عرض الاشياء المضبوطة على المشتبه فيهم لتميزها بطابع العلنية.

المطلب الثاني: مراقبة الاتصالات الالكترونية

أكد المشرع الدستوري الجزائري على حماية القانونية للحياة الخاصة للأفراد حيث لا يجوز انتهاك حرمة المواطن وحرمة شرفه وسرية مراسلاته واتصالاته الخاصة بأي شكل من الأشكال ولكن نظرا للظروف الامنية التي يعيشها المجتمع الدولي وخاصة مع تطور التكنولوجي الذي سهل عمل الشبكات الاجرامية وحفاظا منه على الا من العام والنظام العام تدخل المشرع عن طريق القانون 04/09 السالف الذكر وسمح بصفة استثنائية للسلطات القضائية وفي اطار قرار معلل بمراقبة الاتصالات الالكترونية.

[1] عبد الله أوهايبية ، شرح قانون الإجراءات الجزائية الجزائري ، دار هومة للطباعة و النشر الجزائر ، ط 2 ، 2011 ، ص 280.

وعليه سوف نتطرق من خلال هذا المطلب الى مفهوم مراقبة الاتصالات الالكترونية الفرع الاول ونتطرق الى حالات اللجوء الى المراقبة الالكترونية الفرع الثاني ونعرج الى الضمانات المقررة لتنفيذ مراقبة الاتصالات الالكترونية الفرع الثالث .

الفرع الاول: مفهوم المراقبة الالكترونية

لم يتطرق المشرع الجزائري الى تعريف مراقبة الاتصالات الالكترونية بل اكتفى فقط بتحديد مفهوم الاتصالات الالكترونية

أولا: تعريف المراقبة

1- لغة: المراقبة تعني الملاحظة فراقب الشيء حرصه أو رصده والرقيب هو الحارس أو الحافظ والمراقب آلة لرصد الفلك

2- اصطلاحا: المرقبة هي وضع الشخص أو وسائل نقل او اماكن او مواد بصورة سرية تحت رقابة سرية او دورية بهدف الحصول على المعلومات خاصة بالنشاط او كشف شخصية الافراد وهي تفيد في منع اتمام الجريمة وجمع الادلة عنها والتأكد من صحة المعلومات ثم الحصول عليها بالفعل[1]

ثانيا: تعريف الاتصالات الالكترونية :عرفها المشرع الجزائري بموجب الفقرة (و) من المادة 02من القانون 04/09 السالف الذكر على انها اي تراسل او ارسال او استقبال علامات او اشارات او كتابات او صور او اصوات او معلومات مختلفة بواسطة اي وسيلة الكترونية وتعرف الاتصالات الالكترونية في الفقه المقارن بأنها الاتصالات التي تتم عن طريق جهاز الحاسب الالي والتي تتخذ شكل البريد الالكتروني email او شكل محادثة فورية message instanyt والتي تتم عن طريق شبكة الانترنت

[1]جبار فطيمة ، مراقبة الاتصالات الالكترونية بين الحظر و الاباحة في التشريع الجزائري ، مجلة الدراسات القانونية المقارنة ، جامعة مولود معمري بتيزي وزو ن العدد 3 ، ديسمبر 2016 ، ص 14.

وعليه يمكن تعريف مراقبة الاتصالات الالكترونية انها عملية تتمثل في ترصد الرسائل الالكترونية واجراء فحوصات تقنية وذلك بغية الوصول الى مصدرها ومعرفة صاحبها[1]

الفرع الثاني : حالات اللجوء الى المراقبة الالكترونية

بعد استقراء المادة 04 من قانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها نجدها تتضمن حالات تطبيق الاجراء الجديد في مراقبة الاتصالات الالكترونية وقد جاءت على سبيل الحصر وهي كالاتي:

أولا الوقاية من الافعال الموصوفة بجرائم الارهاب او التخريب او الجرائم الماسة بأمن الدولة :

المراقبة الوقائية كأصل عام لا تطبق على المتابعة القضائية لجريمة مرتكبة وانما تختص بكشف اي خطر او تهديد لأمن الدولة بحيث تهدف الى البحث عن اي معلومة سياسية او اقتصادية او عمومية او عسكرية من شأنها ان تمس باستقرار الدولة والشخص الذي يخضع لهذا الاجراء التقني لا يعتبر متهم او مشتبه فيه طبقا لأحكام قانون العقوبات ولكن نشاطه يمكن ان يشكل خطرا على الامن الوطني لان هذه الجرائم لم ترتكب ولكن المشرع سمح في اطار الوقاية منها بإجراء عملية مراقبة الاتصالات الالكترونية لأشخاص او مجموعات يحتمل توريطهم مستقبلا في القيام بأعمال ارهابية او تخريبية او جرائم تمس بأمن الدولة ولا يشترط توافر ادلة قوية ضدهم بل يكفي فقط مجرد الشك في امكانية ارتكابهم تلك الافعال ويتخذ هذا الاجراء خدمة للصالح العام للدولة والمواطن معا من جرائم محتملة الوقوع

ثانيا: في حالة توافر معلومات على احتمال وقوع اعتداء على منظومة حاسوبية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الاقتصاد الوطني : ان اكتشاف الجريمة قبل وقوعها وخاصة في الجرائم الالكترونية يعتبر احتمال ضئيل لأن هذه الجرائم يصعب اكتشافها وعادة ما يكون ذلك صدفة او عن طريق تحريات في

[1]قادري سارة ، أساليب التحري الخاصة في قانون الإجراءات الجزائية ،كذكرة مكملة لنيل شهادة الماستر اكاديمي في القانون ، تخصص قانون عام للاعمال ن جامعة قاصدي مرباح ورقلة ن 2014 ، ص 56 .

جرائم اخرى وعليه يعتبر وفي اطار الوقاية من الجرائم الرقمية ان مجرد توافر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية تمس بالمصالح السابقة الذكر يجعل من اجراء المراقبة الالكترونية فعلا شرعيا.

ثالثا: لمقتضيات التحريات والتحقيقات القضائية : في حالة صعوبة الوصول الى نتيجة تفيد التحقيقات والابحاث الجارية دون اللجوء الى مراقبة الاتصالات الالكترونية ويعتبر اجراء قضائي لانه يتم في مرحلة البحث والتقصي عن الدليل ويمكن ان يطبق على كافة جرائم القانون العام بشرط ان تكون هناك صعوبة في الحصول على نتيجة تهم التحقيق دون اللجوء الى المراقبة الالكترونية

ربعا: في اطار تنفيذ طلبات المساعدة القضائية الدولية : تتعلق بالجرائم التي ترتكب خارج الاقليم الوطني بحيث من شأن مراقبة الاتصالات في التراب الوطني ان تفيد الدولة المعنية بنتائج تتعلق بمعاينة الجرائم الماسة بتكنولوجيات الاعلام والاتصال وتقديم المعلومات الضرورية عن مكان تواجد مرتكبي هذه الجرائم ويكون ذلك في اطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل هذا ما أشارت اليه المادة 4/11 من المرسوم الرئاسي 261/15

الفرع الثالث : الضمانات المقررة لتنفيذ مراقبة الاتصالات الالكترونية

ويتم تنفيذ عملية المراقبة الاتصالات الالكترونية عن طريق لاتخاذ بعض الاجراءات وتتمثل في أولا: سرية الاجراءات وتتم هده العملية بسرية تامة اي دون علم ورضا المشبه فيهم وكذلك يخضع الموظفون الذين يدعون الى الاطلاع على معلومات سرية الى اداء اليمين امام المجلس القضائي قبل تنصيبهم وهم ملزمون بكتمان السر المهني[1]

ثانيا : التسخير حيث يجوز لوكيل الجمهورية او قاضي التحقيق او لضباط الشرطة القضائية ان يسخر عون مؤهل لدى هيئة مكلفة بالاتصالات سواء كانت عامة او خاصة بهذا الاجراء كما يمكنه طلب المساعدة من قبل الهيئة الوطنية للوقاية من

[1]انظر المواد 27-28 من المرسوم الرئاسي 15-261.

الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته لأن من مهام هذه الهيئة تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذالت الصلة بتكنولوجيات الاعلام والاتصال

ثالثا: تحرير محضر بالعمليات التقنية التي تم القيام بها يجب على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص تحرير محضر عن كل العمليات ووضع التدابير التقنية لمراقبة الاتصالات الالكترونية وما اسفرت عنه من نتائج كما يجب ان يذكر فيه تاريخ وساعة بداية هذه العمليات والانتهاء منها وجميع الشروط الشكلية العامة في جميع المحاضر

رابعا : حماية المعطيات المتحصل عليها : نصت المادة 09 من القانون 09-04 السالف الذكر انه لا يجوز استعمال المعطيات المتحصل عليها من عملية المراقبة الا في الحدود الضرورية للتحقيقات القضائية وهو مايستدعي تجريم كل استعمال لها خارج هذا الاطار[1]

خامسا: الاذن: اشار المشرع الجزائري في نص المادة 4 من قانون 4/9 انه في حالة ما اذا تعلق الامر بالوقاية من الافعال الموصوفة بجرائم الارهاب او التخريب او الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين الى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته اذن لمدة 6 اشهر قابلة للتجديد وذلك بموجب تقرير يوضح ويبين فيه طبيعة الترتيبات التقنية المستعملة والاغراض الموجهة لها.

اما في غير هذه الجرائم الثلاث فإنه يتم الاخذ بالقواعد العامة المنصوص عليها قانون الاجراءات الجزائية وهي صدور الاذن من وكيل الجمهورية او قاضي التحقيق كل حسب اختصاصه بهدف اعتراض المراسلات مع تحديد العناصر المهمة في الاذن ويسلم مكتوبا لمدة 4 اشهر قابلة للتجديد عند الضرورة

[1] انظر المادة 09 من القانون 09-04.

سادسا: عدم المساس بالحرية الشخصية للفرد: بحيث ضابط الشرطة القضائية ملزم بالإجراءات التي وضعها القانون لحماية حقوق الافراد وحرياتهم الشخصية كما هو ملزم بالتقيد بالإذن المقدم له من قبل السلطة القضائية المختصة واي خروج على مضمون الاذن يترتب عليه مساس بالحرية الشخصية الذي يعرض ضابط الشرطة القضائية الى العقوبة

وتجدر الاشارة في الاخير ان المشرع الجزائري قد وضع اجراء مراقبة الاتصالات الالكترونية تحت سلطة القضاء وذلك ضمانة لعدم المساس بحريات الافراد والحياة الخاصة بهم باعتبار ان القاضي يهدف الى الموازنة بين ضرورات التحقيق والزامية حماية الافراد المشتبه فيهم لأن مجرد الاشتباه لا يجعل من الفرد مجرما وهذا مايطلق عليه بضمانات المحاكمة العادلة

المطلب الثالث: التسرب

لقد ادرك المشرع ان المواجهة الفعالة للجرائم الالكترونية لا تكون فقط بإرساء قواعد قانونية ذات طبيعة ردعية بل لابد من مصاحبة هذه الاخيرة قواعد قانونية اجرائية وقائية من شأنها ان تتفادى وقوع هذا النوع من الجرائم وقد استدرك هذا الموقف عن طريق تقنين عملية التسرب في القانون 22/6 في الفصل الخامس من الباب الثاني للكتاب الاول من قانون الاجراءات الجزائية حيث استحدثت هذه العملية في البحث والتحري عن جرائم معينة ومنها الجريمة الالكترونية

وعليه سوف نتطرق في هذا المطلب الى تعريف التسرب الفرع الاول، وتنظيم عملية التسرب الفرع الثاني، ثم الاثار المترتبة عن عملية التسرب وبطلان اجراءاته الفرع الثالث.

الفرع الاول: تعريف التسرب

يعتبر التسرب تقنية جديدة من تقنيات التحري الخاصة يقوم بها ضابط او عون الشرطة القضائية وهي من أخطر العمليات وأصعبها وسوف نتطرق الى تعريف التسرب من خلال النقاط التالية:

اولا/ التعريف اللغوي للتسرب

تسرب: تسربا سرب من الماء دخل في البلاد: دخلها خفية كقولك ترب الجواسيس وتعني كلمة التسرب بالفرنسية infiltration

ثانيا: التعريف القانوني للتسرب

عرفه المشرع في المادة 65 مكرر 12 ق.إ.ج على انه قيام ضابط او عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الاشخاص المشتبه في ارتكابهم جناية او جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف .

واطلق عليه الاختراق ايضا في القانون رقم: 06/01 المتعلق بالوقاية من الفساد ومكافحته في نص المادة 56 منه .

و في القانون الأمريكي يطبق على التسرب العملية تحت التغطية و يقصد بذلك كل تحقيق يتم عند القيام بأعمال او نشاطات يستدعي اسم مستعار أو شخصية خيالية من طرف عون من مكتب التحقيقات الفدرالي[1].

وعرفه المشرع الفرنسي في نص المادة : 81/ 706 الفقرة الثانية من قانون الاجراءات الجزائية الفرنسي على انه : يقوم بالتسرب ضابط او عون شرطة القضائية يخول خصيصا بموجب شروط محددة قانونا ويتصرف تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الاشخاص المشتبه في ارتكابهم جناية او جنحة ويضهر امامهم كأنه فاعل أو شريك أو خاف من خلال هذا نلاح ضان المشرع الجزائري اخذ نفس التعريف الوارد في التشريع الفرنسي

ثالثا: التعريف العملي للتسرب

Maria luiza, nouvelles methodes de lutte contre a criminalite normalisation de l’exception , [1]etude compare,2017, p 135.

يكمن تعريف التسرب انه تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضباط او عون شرطة قضائية بالتوغل داخل جماعة اجرامية وذلك تحت مسؤولية ضابط الشرطة القضائية اخر مكلف بتنسيق عملية التسرب بهدف مراقبة اشخاص مشتبه فيهم وكشف انشطتهم الاجرامية وذلك بإخفاء الهوية الحقيقة وتقديم المتسرب لنفسه على انه فاعل او شريك او خاف وعليه يعتبر التسرب من اخطر طرق التحري وجمع المعلومات ويقوم بها الضابط او الاعوان اصحاب الخبرة الكفاءة ويستخدم فيها اساليب التنكر والاحتيال لكسب ثقة المشتبه فيه فيهم وايهامهم بأنه فاعل معهم او شريك وتقديم المساعدة لهم بقصد تحديد طبيعة ومدى النشاط الاجرامي في الجرائم المذكورة حصريا في المادة 65 مكرر 56 ق.ا.ج وهي جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية – الجرائم الماسة بأنظمة المعالجة الالية للمعطيات– جرائم تبييض الاموال والارهاب الجرائم المتعلقة بالتشريع الخاص بالصرف جرائم الفساد بإذن من وكيل الجمهورية أو قاضي التحقيق بعد اخطار وكيل الجمهورية وتحت رقابته فالمشرع وضع قواعد وضوابط تكفل نجاح وسلامة هذه العملية من خلال تقنين نصوص قانون الاجراءات الجزائية

الفرع الثاني: تنظيم عملية التسرب

نظم المشرع عملية التسرب في المواد من 65 مكرر 11 الى غاية 65 مكرر 18 ق اج ، ووضع شروط شكلية وموضوعية تضمن نجاح عملية التسرب وهذا ما سنتطرق اليه بالتفصيل في هذا الفرع كما سنشير ايضا الى خصوصية التسرب في الجريمة الالكترونية

اولا: الشروط الشكلية للتسرب بالنظر الى ماتتطلبه عملية التسرب من دقة وحذر بسبب خطورتها على حياة المتسرب وجب توافر شروط شكلية تضمن صحة ومشروعية هذا الاجراء وهي كالتالي :

1- تحرير تقرير من طرف ضابط الشرطة القضائية : بالرجوع الى المادة 65 مكرر 13 ق.ا.ج والتي تنص على يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك

التي قد تعرض للخطر امن الضابط او العون المتسرب وكذا الاشخاص المسخرين طبقا للمادة 65 مكرر 14 ادناه وعليه قبل مباشرة عملية التسرب وجب على ضابط الشرطة القضائية كتابة تقرير الى وكيل الجمهورية وهذا كمبدأ عام على اعمال الشرطة القضائية ويجب ان يتضمن التقرير العناصر التالية:[1]

أ – طبيعة الجريمة: طبقا لنص المادة 65 مكرر 5 ق.ا.ج يمكن لوكيل الجمهورية او قاضي التحقيق بعد اخطار وكيل الجمهورية ان يأذن تحت رقابته مباشرة عملية التسرب اذا اقتضت ضرورات التحقيق في الجريمة المتلبس يبها او التحقيق الابتدائي في جرائم المخدرات او الجريمة المنظمة العابرة للحدود الوطنية او الجرائم الماسة بأنظمة المعالجة الالية للمعطيات او الجرائم المتعلقة بالتشريع الخاص بالصرف او جرائم الفساد.

السبب وراء اجراء عملية التسرب: يجب على ضابط الشرطة القضائية ان يذكر سبب ودواعي اللجوء الى عملية التسرب وغالبا ما يكون السبب مرتبط بضرورة التعمق في البحث والتحري في هدا النوع من الجرائم

ج – تحديد عناصر الجريمة بمعنى ذكر كل المعلومات المتعلقة بالجريمة والعناصر المكونة لها فيتضمن التقرير هوية المشتبه فيهم من اسمائهم والقابهم ... والوسائل المستعملة في الجريمة من مركبات او اماكن مرتادة اي ذكر كل المعلومات المتعلقة بالجماعة المقصودة من عملية التسرب

د – ذكر هوية ضابط الشرطة القضائية: وهو الضابط الذي تتم عملية التسرب تحت مسؤوليته ويشرف على تنفيذها ويجب عليه ان يذكر في تقريره جميع البيانات المتعلقة بهويته من الاسم واللقب والرتبة والمصلحة

2- طلب الاذن بمباشرة التسرب: الاذن هو محرر رسمي صادر عن هيئة مختصة ممثلة في وكيل الجمهورية او قاضي التحقيق مسلم الى ضابط الشرطة القضائية وهو اجراء شكلي اشترطه المشرع طبقا لنص المادة 65 مكرر 15 ونشير ان وكيل الجمهورية هو المسؤول الاول عن تقدم رخصة الاذن بصفته الممثل الاول

بوطبة روميصاء ، صلاحيات الضبطية القضائية في ضوء القانون رقم 06-22 مذكرة لاستقبال متطلبات شهادة الماستر ، قانون جنائي ، جامعة قاصدي مرباح ورقلة ، 2015 ، ص 29.[1]

للنيابة العامة او قاضي التحقيق بعد اخطار النيابة العامة وتكون بين قاضي التحقيق والضبطية القضائية في اطار التحقيق ضمن انابة قضائية من طرف قاضي التحقيق الى ضابط الشرطة القضائية

3- وجوب توافر جملة من الشروط في الاذن وهي :

* الكتابة: يجب ان يكون الاذن مكتوبا والا يقع تحت طائلة البطلان

* التسبيب: اي ذكر مبررات اللجوء الى هذا الاجراء ويترتب على تخلفه ايضا البطلان

* ذكر الجريمة التي تبرر اللجوء الى هذا الاجراء يمنح الاذن للتعمق في البحث والتحري في الجرائم المنصوص عليها في المادة 65 مكرر 5 السالفة الذكر

* ذكر هوية ضباط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته : من اسم ولقب والرتبة و المصلحة التابعة لها ... الخ

* المدة الزمنية للتسرب : تقدر مدة التسرب بأربعة اشهر طبقا للمادة 65 مكرر 5 ق ا ج ويجب تحديد بداية ونهاية العملية ويجوز للقاضي المختص تمديد المدة بحسب مقتضيات التحري او التحقيق كما ي جوز له ان يأمر بوقفها في اي وقت قبل انضاء المدة المحددة قانونا وتودع الرخصة في ملف الاجراءات بعد الانتهاء من عملية التسرب

وفي حالة ما اذا تقرر وقف العملية او عند انقضاء المهلة المحددة في رخصة التسرب ولم يتم تمديدها يجوز للعون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر 14 ق ا ج من اقتفاء او حيازة او نقل او تسليم او اعطاء اموال او منتجات او وثائق او معلومات متحصل عليها... الخ واعطائه الوقت الكافي لتوقيف عمليات المراقبة في ظروف تضمن سلامته وامنه دون ان يكون مسؤولا جزائيا على ان لا يتجاوز ذلك مدة اربعة اشهر وفي حالة انقضاء هذه المدة دون ان يتمكن العون المتسرب من توقيف نشاطه في ظروف ملائمة تضمن سلامته يمكن للقاضي ان يأمر بتمديدها اربعة اشهر على الاكثر[1].

[1] فوزي عمارة ، اعتراض المراسلات و تسجيل الأصوات والتقاط الصور و التسرب كاجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية ، كلية الحقوق و العلوم السياسية ، جامعة منتوري قسنطينة ، العدد 33 جزان 2010.

ثانيا: الشروط الموضوعية للتسرب

ولابد لإتمام عملية التسرب توافر بعض الشروط الموضوعية وتتمثل في :

1-السلطة المختصة بمباشرة عملية التسرب : بالرجوع الى نص المادة 65 مكرر 12 ق ا ج يتضح ان المختص بإجراء عملية التسرب هو ضابط الشرطة القضائية المكلف بتنسيق العملية ومسؤولا عنها ويقوم بالتحضير والتنظيم المحكم لها ويتولى تنفيذ هذه العملية ضابط اخر او عون شرطة قضائية ويعرف بالعون المتسرب فالضابط يكون بمثابة همزة وصل بين المتسرب الذي كلفه الضابط بالعملية وقاضي التحقيق غير ان هذا الاجراء لا تكون له في مرحلة التحقيق اية قيمة قانونية اذا لم يكن تحت رقابة قاضي التحقيق .

وعليه نستطيع القول ان عملية التسرب تقوم بوجود العون المتسرب الذي يقوم بتنفيذ العملية والضابط المنسق الذي يسهر على تنسيق بين المتسرب والجهة الاذنة بالتسرب

2-دوافع عملية اجراء عملية التسرب ينصب على جناية اوجنحة متعلقة بالجرائم المنصوص عليها في المادة 65 مكرر 5 قاج فإنه يجب ان يكون هو الاجراء الوحيد او الانسب الذي يمكن بواسطته اظهار الحقيقة بعد لان اثبتت الاجراءات الاخرى عدم نجاعتها ، فالمشرع الجزائري اجاز لوكيل الجمهورية او قاضي التحقيق ان يأذن للقيام بعملية التسرب شريطة ان تقتضي ضرورات التحقيق والتحري ذلك لان التسرب اجيز لعملية معينة ولغرض خاص وبصفة استثنائية فتخلف هذه الاسباب يمنع القاضي من الاذن به والا عد تعسفا فالتسرب الذي لا يلتمس من وراءه فائدة لإظهار الحقيقة يعتبر تسربا تحكيما.

3-السرية لعملية التسرب : تعتبر السرية شرط اساسي لنجاح عملية التسرب وذلك حماية للشخص المتسرب والمصلحة العامة ومنه الوصول الى كشف الحقيقة ولم يكتفي المشرع بعدم علانية التحقيق وانما فرض عقوبات جزائية على كل من يكشف هوية ضابط او عون شرطة قضائية

1/ ان يقوم ضابط الشرطة القضائية المنتدب وباعتباره المسؤول عن عملية التسرب بتحرير تقرير حول العملية ثم يحيلها الى قاضي التحقيق على اساس انه المنسق بين هذا الاخير والعون المسرب

وبالرجوع الى النصوص القانونية التي تنظم عملية التسرب نلاحظ ان المشرع لم يشر الى مصير الاشياء عليها نتيجة عملية التسرب ولا الى موقف القانون من الجرائم التي تم اكتشافها عرضا اثناء عملية التسرب وكذلك لم يشر الى امكانية الطعن بالنقض في الاذن بالتسرب عن طريق الاستئناف

2/ بعد الانتهاء من عملية التسرب يتم سماع ضابط الشرطة القضائية التي جرت عملية التسرب تحت مسؤوليته وبالتنسيق معه دون سواء كشاهد عن العملية وهذا من باب الحماية غير المباشرة للعون المتسرب

3/ توفير الحماية للعون المتسرب من اي خطر قد يتعرض له او يمتد الى افراد عائلته بعد العملية وذلك من خلال فرض عقوبات نص عليها في المادة 65 مكرر16 ق اج التي تعاقب كل شخص يكشف الهوية الحقيقة للعون المتسرب

4/ انعدام المسؤولية الجزائية للعون المتسرب عن بعض الافعال المجرمة سواء من اقتفاء او حيازة او نقل او غيره من الافعال التي نصت عليها المادة 65 مكرر 14 ق ا ج وعليه عند اقتراف العون المتسرب هذه المخالفات اثناء عملية التسرب تعفيه من المسؤولية الجزائية لأنها افعال مبررة قانونا

غير ان المشرع لم يوضح القيمة الثبوتية لتصريحات المتسرب عن طريق المسؤول عن العملية بحث هل يمكن اعتبارها استدلالات او شهادات مكتوبة فقط الامر الذي يستدعي معه تطبيق القواعد العامة للإثبات واعتبارها استدلالات لا ترقى الى دليل مالم ترفق بدلائل او عناصر ثبوتية اخرى

الفرع الثالث: بطلان اجراءات التسرب

كمبدأ عام يكون البطلان اما لسبب مخالفة الاحكام الجوهرية المتعلقة بصفة عامة بحقوق الدفاع وحق الخصوم واما بطلان قانوني يتولى المشرع

تحديد حالاته وهذا مانلتمسه من خلال المواد 65 مكرر 12 و 65 مكرر 15 ق ا ج التي تبين حالات بطلان اجراءات التسرب وتتمثل في :

يتعرض العمل الاجرائي لضباط الشرطة القضائية في اطار عملية التسرب الى بطلان عند مخالفة الشروط الشكلية الو الموضوعية المتعلقة بالإذن لمباشرة عملية التسرب باستثناء حالة عدم ذكر الجريمة وهوية ضابط الشرطة القضائية المسؤول عن عملية التسرب و المدة التي تستغرقها وهو ما يعني ان عدم مراعاة الشكليات المنصوص عليها في الفقرة الثانية والثالثة من المادة 56 مكرر 15 السالفة الذكر لا يترتب عليه بطلان الاذن بالتسرب[1]

– اذا كان العون المتسرب محرضا على ارتكاب مخالفة غبر الذي سمحت له قانونا.[2]

[1]غوزي عمارة ، المرجع السابق ، ص 248.

[2]السوفي نور الهدي ، المرجع السابق ص 55.

خاتمة

خاتمة

لقد تم التوصل من خلال هذه الدراسة أن التحقيق في الجرائم الرقمية يختلف عن التحقيق في الجرائم التقليدية و أن هذا الإختلاف راجع أساسا لعدم إمكانية تطبيق أحكام الجرائم التقليدية على الجرائم المرتكبة في العالم الإفتراضي بأصلها ،و كون التحقيق فيها يأخذ طابعا خاصا مستمد أساسا من خصوصية هذه الجرائم.

انطلاقا من هذه الخصوصية فقد أدركت كل دول العالم و المنظمات الدولية و الإقليمية مدى خطورة هذا النوع من الجرائم و مدى التحديات التي تفرضها عليها ،الأمر الذي يستدعي ضرورة الإسراع في وضع إطار قانوني لها لتحقيق فعالية أكبر في مكافحتها، و قد تم إبرام عدة مؤتمرات و معاهدات دولية و إقليمية مثل اتفاقية بودابست سنة 2001 التي وضعت الأسس السليمة لمكافحة الجريمة المعلوماتية.

و لقد حاول المشرع الجزائري هو الآخر مواكبة هذه التطورات بتعديل قانون العقوبات بموجب القانون 15/04 ،و بعدها إصدار القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام و الإتصال ، و كذا إدراج تعديلات على قانون الإجراءات الجزائية تتلاءم و خصوصية التحقيق في هذه الجرائم من أجل الوصول إلى الأدلة اللازمة للكشف عنها من أجل ضمان محاكمة عادلة.

و لقد خلصنا إلى أن موضوع الدراسة يطرح العديد من الإشكالات و جعلتنا نخلص إلى مجموعة من النتائج على النحو الآتي:

1 . مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظام المعالجة الآلية للمعطيات التي تستهدف البيئة الإلكترونية ،و بذلك فإن محل الجريمة المعلوماتية هو افتراضي فقط مقارنة بالجريمة التقليدية.

2 . مرتكب الجريمة الإلكترونية يتميز عن المجرم العادي بمجموعة من الصفات ،منها أنه اجتماعي و ذكي يتمتع بالخبرة في مجال التقنية الحديثة ،بالإضافة إلى أنه غير عنيف ،فهذا النوع من الإجرام لا يتطلب القوة و العنف،كما أن دوافع ارتكاب

الجريمة الإلكترونية تختلف من شخص لآخر ،فقد تكون دوافع شخصية هدفها تحقيق مصلحة خاصة ،و قد تكون خارجية بهدف الإنتقام مثلا.

3 . الجريمة الإلكترونية كغيرها من الجرائم التقليدية تتميز بالخطورة لكونها تمس الإنسان و المؤسسات و تتعدى حتى لأن تكون خطرا على أمن الدولة و استقرارها و كذلك هي من الجرائم العابرة للحدود لارتباطها بشبكة الأنترنيت ،كما تتميز الجريمة الإلكترونية بكونها تعتمد على التقنيات الحديثة ،و صعوبة اكتشافها و إثباتها لذا فالمحقق يواجه عدة معوقاتللكشف عن الجريمة الرقمية و القبض على مرتكبيها و نسبتها إليهم ،أهمها معوقات تشريعية تكمن في عدم حصر لكل صور الجريمة في القوانين الجنائية.

4 . اعتماد المحقق على عناوين الأنترنيت كبروتكول الأنترنيت (IP) الموجود بكل جهاز مرتبط بالأنترنيت الذي يساعد على تحديد مكان الحاسب الآلي كوسيلة للتحري في مثل هذا النوع من الجرائم.

5 . المعاينة في الجريمة الإلكترونية أقل أهمية منها في الجرائم العادية، لقلة الآثار المادية بينما الخبرة تعتبر من أهم إجراءات التحقيق في الجرائم الإلكترونية و هذا ما تستدعيه طبيعة هذه الجريمة كونها تعتمد بالدرجة الأولى على وسائل مستحدثة.

6 . إجراءات استخلاص الدليل الرقمي من الممكن أن تؤدي إلى المساس بخصوصية الحياة الخاصة للأشخاص، لذلك فاستعمال هذه التقنيات يكون بحسب ضرورة الحالة.

و بناءعلى هذه النتائج يمكن اقتراح مجموعة من التوصيات على النحو التالي:

1. إنشاء دورات تكوينية للمحققين في مجال نظم المعلوماتية و الحواسيب ،فدور القاضي مهم في توجيه مسار القضايا،فتقدير خطورة المجرم المعلوماتي مرتبط أساسا بدور القاضي المحقق الذي ينبغي أن يكون ملمابالجوانب الفنية التقنية الحديثة.

2. عدم حصر صور الجريمة الإلكترونية في المواد القانونية و فتح المجال للمحقق في أن ينظر في جميع الجرائم المتعلقة بالجرائم الإلكترونية التي توجه إليه ،لأنه

و تطبيقا لمبدأ الشرعية يبقى دور المحقق مرتبط فقط بالتحقيق في الجرائم المذكورة على سبيل الحصر في التشريعات الوطنية ،و كما ذكر سابقا فالجرائم في تطور مستمر ،مما يجعل القوانين التقليدية غير كافية.

3. ينبغي على المشرع وضع إجراءات حديثة تعتمد على ذات الوسائل المستخدمة في الجريمة للكشف عنها و تتبع فاعليتها و ذلك باعتبار أن المجرم الإلكتروني يعتمد بالدرجة الأولى على وسائل تقنية حديثة و لأن الإجراءات التقليدية غير كفيلة بمكافحة هذه الجرائم .

4. ضرورة التزام الدول بوضع نظام مراقبة عبر شبكة الأنترنيت يسمح بتتبع الملفات المدخلة و المستخرجة ،و تعقب الإختراقات غير المشروعة للأنظمة و تخريبها و ملاحقة مرتكبيها.

5 . على دارس القانون البحث في موضع إجراءات التحقيق فيما يخص هذا النوع من الجرائمنظرا لأهميتها و حداثتها،و انتشارها الواسع على الصعيدين الوطني و الدولي.

قائمة المصادر و المراجع

Les références

قائمة المصادر و المراجع

قائمة المصادر :

أولا :الدستور الجزائري لسنة 1996 الصادر بموجب مرسوم رئاسي رقم 96-438 مؤرخ في 07-12-1996 ج ر ن العدد 76 الصادرة بتاريخ 08-12-1996.

ثانيا القوانين و الأوامر :

-1 امر رقم 66-155 مؤرخ في 08-06-1966 المتضمن قانون الإجراءات الجزائية الجزائري ج ر عدد 48 ، الصادرة بتاريخ 10-06-1966.

- 2 أمر رقم 66-156 المؤرخ في 08-06-1966 المتضمن قانون العقوبات منشور في ج ر عدد 49 بتاريخ 11-06-1966.

- 3 القانون رقم 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الاعلام و الاتصال و مكافحتها منشور ج ر عدد 47 الصادرة بتاريخ 06-08-2009.

- 4 القانون رقم 06-22 مؤرخ في 20-12-2006 معدل و متمم لقانون الإجراءات الجزائية ج ر 84 الصادرة بتاريخ 27-12-2006.

ثالثا : التنظيمات

1 - مرسوم رئاسي رقم 15-261 مؤرخ في 08-10-2015 يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ج ر عدد 53 الصادرة في 08-10-2015.

2 - مرسوم تنفيذي رقم 06-348 مؤرخ في 05-10-2006 المتعلق بالتقسيم القضائي منشور في ج ر عدد 63 بتاريخ 08-10-2006.

قائمة المراجع :

أولا : الكتب (بالعربية)

1 – علي بن هادية ، لحسن البليش ، الجيلالي بن الحاج يحي ، القاموس الجديد للطلاب ، الشركة الوطنية ، الشركة التونسية ، الجزائر ، تونس ، ط1 ، 1979.

2 –خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنيث، دار الثقافة ، الأردن ، ط 1 ، 2011 .

3 – خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي ، الإسكندرية ، ط 1 ، 2009،

4 – علي عدنان الفيل ، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية ن دراسة مقارنة ، المكتب الجامعي الحديث ، الإسكندرية ، بدون طبعة ، 2012 .

5 – قريشي حمزة ، الوسائل الحديثة للبحث و التحري في ضوء القانون الجزائري، منشوراتالسائحي ، الجزائر، ط 1 ، 2017 .

6 – [1]محمد حماد مرهج الهيتي ، جرائم الحاسوب ، دار المناهج ، عمان ، ط 1 ،2006.

7 – حسن الجوخدار ، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية ، دار الثقافة للنشر و التوزيع ، الأردن ، ط 1 ،2008 8 – [1]نبيلة هبة هروال ، الجوانب الإجرائية لجوانب الانترنيت في مرحلة جمع الاستدلالات ، دار الفكر الجامعي ، الإسكندرية ، 2013 .

9 – [1]محمد امين احمد الشوابكة ، جرائم الحاسوب و الانترنيت، ط 1 ،دار الثقافة للنشر و التوزيع ، عمان ، 2004 ، ص 122.

[1]10 – صالح شنين ، الحماية الجنائية الحماية الجنائية للتجارة الالكترونية ، أطروحة لنيل شهادة الدكنوراه في القانون الخاص ، جامعة أبو بكر بلقايد

[1]11– محمد حزيط ، قاضي التحقيق في النظام القضائي الجزائري ، دار هومة للطباعة و النشر 2009 ، ص 91.

12[1] – بكري يوسف بكري ، التفتيش عن المعلومات في وسائل التقنية الحديثة ، دار الفكر الجامعي ، الإسكندرية ط 1 ، 2011 ، ص 58 .

13–ثابت دنيازاد ، مراقبة الاتصالات الالكترونية و الحق في حرمة الحياة الخاصة في القانون الجزائري ، مجلة العلوم الاجتماعية و الانسانية . جامعة تبسة ، العدد 6 ، 2012.

احسن بوسقيعة ، التحقيق القضائي ، دار هومة للطباعة و النشر، الجزائر ، ط 10 ، 2013 .

14[1] – زبيحةزيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، الجزائر ، بدون طبعة ، 2011

15 – بوعناد فاطمة زهرة ، مكافحة الجريمة الالكترونية في التسريع الجزائري ، مجلة الندوة للدراسات القانونية ، سيدي بلعباس ، 2013 ،العدد 02.

16 – عادل عزام سقف الحيط ، جرائم الدم و القدح و التحقير المرتكبة غبر الوسائط الالكترونية ، دراسة قانونية مقارنة ، دار الثقافةللنشر و التوزيع ، ط 1 ،2011 .

17 – سعيداني نعيم ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، تخصص علوم جنائية ، جامعة الحاج لخضر ، باتنة ، 2012–2013.

18 – عبد الله أوهايبية ، شرح قانون الإجراءات الجزائية الجزائري ، دار هومة للطباعة و النشر الجزائر ، ط 2 ، 2011 .

19 – فوزي عمارة ، اعتراض المراسلات و تسجيل الأصوات والتقاط الصور و التسرب كاجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية ، كلية الحقوق و العلوم السياسية ، جامعة منتوري قسنطينة ، العدد 33 سنة 2010.

الكتب (بالفرنسية)

- Marie ,cristine / droit penalgeneral, edellicses, parie, France 2002 .

- Maria luiza, nouvelles methodes de lutte contre a criminalite normalisation de l'exception ,etude compare,2017.

الرسائل العلمية :

1 – عمر بن إبراهيم بن حماد العمر ، إجراءات الشهادة في مرحلتي الاستدلال و التحقيق الابتدائي في ضوء نظام الإجراءات السعودي ، مذكرة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، 2007 ص 22.قادري سارة ، أساليب التحري الخاصة في قانون الإجراءات الجزائية ،كذكرة مكملة لنيل شهادة الماستر اكاديمي في القانون ، تخصص قانون عام للاعمال ن جامعة قاصدي مرباح ورقلة ، 2014 .

2 – عبد الله بن حسين ال حجرافالقحطاني ، تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية ، رسالة مقدمة لنيل شهادة الماجستير ، قسم العلوم الشرطية جامعة نايف للعلوم الأمنية الرياض.

3 – بلال بن جامع ، المشكلات الأخلاقية و القانونية المثارة حول شبكة الانترنيت، ماجستير في علم المكتبات تخصص اعلام علمي و تقني جامعة منتوري قسنطينة .

4 – سليمان مهجع العنزي ، وسائل التحقيق في جرائم نظم المعلومات ، رسالة ماجيستير في العلوم الشرطية ، كلية الدراسات العالية ، اكادمية نايف العربية للعلوم الأمنية ، الرياض ، 2003 ص 108 .

7 – السوفي نور الهدي ، التحقيق في الجريمة المعلوماتية ، مذكرة لنيل شهادة الماستير اكاديمي في الحقوق ، تخصص قانون جنائي ، جامعة قاصدي مرباح ورقلة ، 2017.

8 – بوطبة روميصاء ، صلاحيات الضبطية القضائية في ضوء القانون رقم 06-22 مذكرة لاستقبال متطلبات شهادة الماستر ، قانون جنائي ، جامعة قاصدي مرباح ورقلة ، 2015 .

مواقع الأنترنت:

- حسين بن سعيد الغافري ، التحقيق ، جمع الأدلة في الجرائم المتعلقة بشبكات الانترنيت ، موقع المنشاوي للدراسات و البحوث على الموقع WWW.minshawi.com اطلع عليه بتاريخ 11-02-2018.

الفهرس

الفهرس

الإهداء

الشكر

قائمة المختصرات

مقدمة..... 1

الفصل الأول: ماهية للتحقيق الجنائي في الجرائم الرقمية 7

المبحث الأول :الاطار المفاهيمي للتحقيق الجنائي في الجرائم الرقمية 7

المطلب الأول: الضوابط الأساسية للتحقيق الجنائي في الجرائم الرقمية 8

الفرع الأول: مفهوم التحقيق الجنائي في الجرائم الرقمية 8

الفرع الثاني: عناصر التحقيق الجنائي في الجرائم الرقمية 10

الفرع الثالث : ضمانات المتهم في مرحلة التحقيق الجنائي في الجرائم الرقمية..... 12

المطلب الثاني: وسائل التحقيق الجنائي في الجرائم الرقمية..... 13

الفرع الأول: أسلوب التحقيق الجنائي في الجرائم الالكترونية..... 14

الفرع الثاني : الوسائل المادية للتحقيق الجنائي في الجرائم الرقمية 19

الفرع الثالث: الوسائل الإجرائية للتحقيق الجنائي في الجرائم الرقمية..... 22

المبحث الثاني: المحقق في الجرائم الرقمية 26

المطلب الأول: القائم بالتحقيق في الجرائم الرقمية..... 26

الفرع الأول: مفهوم المحقق في الجرائم الرقمية..... 27

الفرع الثاني: مساعدو المحقق في الجرائم الرقمية 30

المطلب الثاني : صلاحيات المحقق في الجرائم الرقمية 34

الفرع الأول: صلاحيات الضبطية القضائية 34
الفرع الثاني: صلاحيات قاضي التحقيق 36
الفصل الثاني: آليات التحقيق الجنائي في الجرائم الرقمية 42
المبحث الأول : الإجراءات العامة للتحقيق الجنائي في الجرائم الرقمية 42
المطلب الأول : الإجراءات المادية الخاصة بالتحقيق في الجرائم الرقمية..... 43
الفرع الأول : المعاينة 43
الفرع الثاني : التفتيش في الجرائم الرقمية 48
الفرع الثالث : الضبط في الجرائم الرقمية 56
المطلب الثاني : إجراءات التحقيق الجنائي الشخصية في الجرائم المعلوماتية..... 58
الفرع الاول : الخبرة في الجرائم الرقمية 58
المبحث الثاني: الآليات الإجرائية الخاصة للتحقيق الجنائي في الجرائم الرقمية 61
المطلب الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور 61
الفرع الاول: تعريف اعتراض المراسلات..... 62
الفرع الثاني:تسجيل الأصوات والتقاط الصور 64
الفرع الثالث: إجراءات وشروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور. 65
المطلب الثاني: مراقبة الاتصالات الالكترونية 68
الفرع الاول: مفهوم المراقبة الالكترونية 69
الفرع الثاني : حالات اللجوء الى المراقبة الالكترونية 70
الفرع الثالث : الضمانات المقررة لتنفيذ مراقبة الاتصالات الالكترونية 71
المطلب الثالث: التسرب 73

الفرع الاول: تعريف التسرب 73
الفرع الثاني: تنظيم عملية التسرب..... 75
الفرع الثالث: بطلان اجراءات التسرب 79
خاتمة..... 85
قائمة المصادر و المراجع..... 88

ملخص:

لقد واجهت عملية التحقيق في الجريمة المعلوماتية صعوبات كثيرة في كشف غموض هذه الجرائم التي يتطلب لارتكابها وسائل ذات تقنية عالية ، إضافة الى ذكاء و خبرة المجرم في مجال الانترنت و الحاسب الآلي، الامر الذي يخلف أثار غير مادية فيكون من الصعب كشف الجريمة و القبض على الجاني ، هذا الوضع دفه الى ضرورة تطوير عمليه التحقيق و استعمال أساليب ذي تقنية عالية لاستخلاص الدليل الرقمي ن حيث أصبحت وسائل التحقيق المادية و الإجرائية تتميز بالطابع العلمي و ذلك بالاستهانة بالأساليب العلمية و استخدام الانترنت لكشف هذا النوع من الجرائم ، و أيضا الرفع من قدرات الجهات المختصة القائمة بالبحث و التحري ، لان التحقيق بصفة عامة يعتمد على ذكاء المحقق و فطنته و ان يحاول بكل جهده إظهار الحقيقة.

إضافة الى الطابع الخاص للجريمة المعلوماتية أنتج نوع خاص من الأدلة من نفس طبيعتها بحيث يصعب اكتشافها و ضبطها عن طريق الآليات العامة للتحقيق المتمثلة في المعاينة و التفتيش و الحجز و الخبرة مما دفع بالمشرع الجزائري الى ضرورة تطوير القوانين و إدخال تعديلات على مستوى قانون الجزائية ، إضافة الى استحداث قوانين جديدة تتلائم و خصوصية هذه الجريمة التي تقوم في عالم افتراضي ، فاستحدث بذلك أليات خاصة تتمثل في اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و التسرب و المراقبة الالكترونية.

الكلمات المفتاحية:

الجريمة، التحقيق الجنائي، ، أساليب خاصة، الدليل.

Résumé

L'instruction en matière de cybercriminalité s'est confrontée à de multiples difficultés en raison de l'opacité de ses crimes, les quels pour être commis exigent une haute technicité en plus de l'intelligence et l'expérience de l'auteur dans le domaine de l'internet et de l'ordinateur, crimes qui causent des dommages immatériels et leur découverte reste difficile ainsi que la neutralisation du criminel.

Cette situation met en exergue la nécessité du développement de l'instruction et l'utilisation de procédés de haute technicité afin d'arriver à la preuve numérique, parce que les moyens et outils matériels et procédures de l'instruction se distinguent par leur caractère scientifique.

A fortiori, l'utilisation de procédés scientifiques et de l'internet pour découvrir ce genre de crimes reste impérative, ainsi que la formation et le perfectionnement des instances compétentes en matière de recherche et d'enquête.

Il faut souligner que l'instruction en général exige l'éveil et l'intelligence de l'instructeur qui fera tout pour arriver à la vérité.

En outre, le caractère particulier et spécifique de ces crimes dans le domaine de l'internet a donné lieu à des preuves particulières et de même nature, et les découvrir et les déterminer restent difficiles par l'utilisation des procédés usuels tels la perquisition, l'inspection, la saisie et l'expertise….

Cet état de fait a amené le législateur algérien à voir la nécessité de l'actualisation des textes législatifs et des lois et leur modification et surtout le Code de Procédure Pénale et la mise en place de nouveaux textes pouvant régir ce genre de criminalité d'un monde virtuel avec la création de procédés spéciaux consistant dans l'interception des correspondances, l'enregistrement des voix, de sons, de scènes, de photos et images et la surveillance électronique et contrôle.

Mots clés : crime, procédures criminelle, procédés spéciaux, preuve.

Summary :

Information crime investigation process has witnessed a set of hurdles to unveil the vagueness of such crimes that entail methods of high tichniques to the criminal's smartness and experience in feild of internet and computing, the fact that could have non-material concequences making it much harder to reveal the crime and to arrest the unsuh, this situation has enforced the necessity for developing the investigation process and using highly technical methods of investigation are of scientific nature using scientific methods and internet to reveal such crimes, along with increasing the qbilities of specialized donors of researdch and investigation, because generally investigation's intelligence and wit and deploying all eforts to reveal the crime .

In addition to the specificity of information crime , a new kinds of evidences is emanated, the fact harden the crime's detection and control merely vby public mechanisms wich led the algerian legislator for the necessity to enforce the laws fiting in with this crime's specificity

happening in the virtual word, thus creating specific mecanisms for correspondences interception, voter registation and pictures taking along with electronic leakage and control.

KEYWORDS

Crime, criminal investigation, special procedures ,proof.