جامعة غرداية
كلية الحقوق والعلوم السياسية
قسم: الحقـوق

عنوان المذكرة

التحقيق الجنائي في الجرائم الرقمية

مذكرة ضمن متطلبات نيل شهادة ماستر أكاديمي حقوق
تخصص قانون جنائي

إعداد الطالبتين:
- عزيزة بدودة
- سعاد علالي

إشراف الدكتور:
بن فردية محمد

أمام اللجنة المكونة من السادة:

- بن حمودة مختار	أستاذ مساعد "أ" جامعة غرداية	رئيسـا
- بن فردية محمد	أستاذ محاضر "أ" جامعة غرداية	مشرفا و مقررا
- طيبي الطيب	أستاذ مساعد "أ" جامعة غرداية	عضوا مناقشا

الموسم الجامعي1438- 1439هـ/ 2017- 2018 م

جامعة غرداية
كلية الحقوق والعلوم السياسية
قسم: الحقـوق

عنوان المذكرة

التحقيق الجنائي في الجرائم الرقمية

مذكرة ضمن متطلبات نيل شهادة ماستر أكاديمي حقوق
تخصص قانون جنائي

إعداد الطالبتين:
عزيزة بدودة
سعاد علالي

إشراف الدكتور:
بن فردية محمد

أمام اللجنة المكونة من السادة:

- بن حمودة مختار	أستاذ مساعد "أ" جامعة غرداية	رئيسـا
- بن فردية محمد	أستاذ محاضر "أ" جامعة غرداية	مشرفا و مقررا
- طيبي الطيب	أستاذ مساعد "أ" جامعة غرداية	عضوا مناقشا

الموسم الجامعي1438- 1439هـ/ 2017- 2018 م

قال تعالى

بسم الله الرحمن الرحيم

﴿ يَا أَيُّهَا الَّذِينَ آمَنُوا إِن جَاءَكُمْ فَاسِقٌ بِنَبَإٍ فَتَبَيَّنُوا أَن تُصِيبُوا قَوْمًا بِجَهَالَةٍ فَتُصْبِحُوا عَلَى مَا فَعَلْتُمْ نَادِمِينَ ﴾

صدق الله العظيم

الحجرات الآية 06

قال رسول الله صلى الله عليه وسلم

" لو يعطى الناس بدعواهم لادعى أناس دماء رجال و أموالهم ولكن البينة على من إدعى واليمين على من أنكر "

صدق رسول الله

شكر وعرفان

من باب قوله تعالى " لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ" سورة إبراهيم الآية 07

الحمد و الشكر لله الذي وفقنا وأنار لنا درب العلم و المعرفة في إنجاز هذا العمل

ومن باب قول المصطفى عليه السلام " **من لم يشكر الناس لم يشكر الله**"

أسمى عبارات الشكر والإمتنان إلى الذي شجعنا و وقف وراء هذا العمل بكل مجهوداته ونصائحه القيمة التي أنارت طريقنا وقومت مسارنا وكانت عونا لنا في إتمام هذا البحث

إلى رمز العلم والعمل و الإلتزام أستاذنا المشرف الدكتور محمد بن فردية

كما نتوجه بجزيل الشكر والعرفان إلى كل من مد لنا يد العون من قريب أو من بعيد في إنجاز هذا العمل، وفي تذليل ما واجهناه من صعوبات طوال فترة الإنجاز

فإننا لنجد أنفسنا أسرى فضل ولا يسعنا إلا أن نفرده بالشكر الخاص

إلى كل أساتذتنا الكرام في جامعة غرداية و مسؤولين وإطارات الذين قدموا لنا الكثير باذلين بذلك جهودا كبيرة في فتح أبواب ذهبية لاستكمال مشوار مسيرتنا العلمية

يسرني أيضا أن أتقدم بجزيل الشكر و العرفان إلى اللجنة الموقرة التي أعطتنا من وقتها الثمين وقبلت مناقشة هذا البحث المتواضع

وقبل أن نمضي نقدم أسمى آيات الشكر و الإمتنان والتقدير والمحبة إلى الذين حملوا أقدس رسالة في الحياة

إلى الذين مهدوا لنا طريق العلم و المعرفة

إلى جميع أساتذتنا الأفاضل

كن عالما... فإن لم تستطع فكن متعلما، فإن لم تستطع

فأحب العلماء، فإن لم تستطع فلا تبغضهم.

الإهداء

أهدي هذا الجهد إلى مثلي الأعلى في الحياة والدي الغالي أطال الله في عمره.

إلى من علمتني العطف والصدق إلى أمي العزيزة أطال الله في عمرها.

إلى سندي في الحياة إخواني و خاصة الدكتورة علالي كوثر.

إلى كل أصدقائي و زملائي.

إلى كل أساتذتي الكرام.

إلى كل الأهل والأقارب من قريب وبعيد.

إلى كل طلبة الحقوق،

إلى كل من يتصفح أوراق المذكرة ويستفيد من المعلومات الموجودة فيها.

علالي سعاد

الإهداء

إلى من تنحني هامتي لها خجلا فلا الكلمات توفيها حقها، ولا الأرقام تحصي فضائلها

إلى رمز الحب وبلسم الشفاء التي تعبت في تربيتي وأنارت دربي و أعانتني بالدعوات

إلى القلب الناصع مصدر قوتي ومثالي في الصبر نبع الحنان أمي الغالية أطال الله في عمرها

إلى روح أبي الطاهرة راجية من الله أن يتغمده برحمته الواسعة ويسكنه فسيح جنانه

إلى من أشد بهم أزري وسندي في هذه الحياة منبع المحبة و الحنان إخوتي وأخواتي

إلى زوجات الإخوة والحفيد الغالي أحمد عبد الوهاب وكل العائلة الكريمة

لى من جمعتني بهم الأقدار من الأحبة و الأصدقاء رفقاء الدرب

إلى من لاقتني بهم أروع الصدف زملاء الدفعة

إلى كل من كان لي سندا في هذه الحياة

إلى جميع أساتذتي الكرام وعلى رأسهم الأستاذ بن حمودة مختار،

بن سديرة فوزي، طيبي الطيب، فخار حمو، نهائلي رابح، فروحات السعيد، ولاد العربي. غ

إلى كل طلبة الحقوق

أهدي ثمرة جهدي

بروة عزيزة

قائمة المختصرات:

ق.إ.ج.ج	قانون الإجراءات الجزائية الجزائري
ق.ع.ج	قانون العقوبات الجزائري
ج.ر	الجريدة الرسمية
ط	طبعة
د.ن	دون طبعة
ص	صفحة
آلخ	إلى آخره

الكلمات المفتاحية:

الجريمة الرقمية، التحقيق، أساليب البحث و التحري، المحقق، التسرب، اعتراض المراسلات، المعاينة الإلكترونية.

ملخص البحث

لقد واجهت عملية التحقيق في الجريمة المعلوماتية صعوبات كثيرة في كشف غموض هذه الجرائم التي يتطلب لارتكابها وسائل ذات تقنية عالية، إضافة إلى ذكاء وخبرة المجرم في مجال الأنترنت و الحاسب الآلي، الأمر الذي قد يخلف آثار غير مادية فيصعب بذلك كشف الجريمة و القبض على الجاني، هذا الوضع دفع إلى ضرورة تطوير عملية التحقيق واستعمال أساليب ذي تقنية عالية لاستخلاص الدليل الرقمي، حيث أصبحت وسائل التحقيق المادية و الإجرائية تتميز بالطابع العلمي وذلك بالإستعانة بالأساليب العلمية واستخدام الانترنت لكشف هذا النوع من الجرائم، و أيضا الرفع من قدرات الجهات المختصة القائمة بالبحث و التحري، لأن التحقيق بصفة عامة يعتمد على ذكاء المحقق وفطنته وأن يحاول بكل جهده إظهار الحقيقة.

إضافة إلى أن الطابع الخاص للجريمة المعلوماتية أنتج نوع خاص من الأدلة من نفس طبيعتها بحيث يصعب إكتشافها و ضبطها عن طريق الآليات العامة للتحقيق المتمثلة في المعاينة والتفتيش والحجز والخبرة مما دفع بالمشرع الجزائري إلى ضرورة تطوير القوانين و إدخال تعديلات على مستوى قانون الإجراءات الجزائية، إضافة إلى استحداث قوانين جديدة تتلاءم وخصوصية هذه الجريمة التي تقوم في عالم افتراضي، فاستحدث بذلك آليات خاصة تتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، و أيضا التسرب و المراقبة الإلكترونية.

Summary:

Information crime investigation process has witnessed a set of hurdles to unveil the vagueness of such crimes that entail methods of high techniques, additionally to the criminal's smartness and experience in field of internet and computing, the fact that could have non-material consequences making it much harder to reveal the crime and to arrest the unsub, This situation has enforced the necessity for developing the investigation process and using highly technical methods to tease out the digital evidence. Physical and measuring methods of investigation are of scientific nature, using scientific methods and internet to reveal such crimes, along with increasing the abilities of specialized donors of research and investigation, because generally investigation depends on the investigator's intelligence and wit and deploying all efforts to reveal the crime.

In addition to the specificity of information crime, a new kind of evidences is emanated, the fact that harden the crime's detection and control merely by public mechanisms of investigation, being constatation, inspection, detention and expertise which led the Algerian legislator for the necessity to enforce the laws and bring about amendments on penal measures law, along with creating new laws fitting in with this crime's specificity happening in the virtual world, thus creating specific mechanisms for correspondences interception, voter registration and pictures taking along with electronic leakage and control.

مقـــدمـــة

مقدمـــة

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة سميت بالثورة المعلوماتية وفي ذلك إشارة للدور البارز الذي أصبحت تلعبه المعلومة في الوقت الراهن ومما لاشك فيه أن الثورة المعلوماتية ونتيجة للتقنيات العالية التي تقوم عليها والمتمثلة في استخدام الحواسيب والشبكات المعلوماتية التي تربط بينها قد تركت آثارا إيجابية وشكلت قفزة حضارية نوعية في حياة الأفراد والدول ذلك أن مختلف القطاعات في الوقت الراهن تعتمد في عملها وبشكل أساسي على استخدام الأنظمة المعلوماتية نظرا لسرعتها ودقتها في تجميع المعلومات وتخزينها ومعالجتها، كما أصبحت هذه الأنظمة مستودعا لأسرار الأشخاص المتعلقة بحياتهم الشخصية أو العملية التي تأخذ قدرا من الأهمية والسرية.

غير أن هذا الجانب الإيجابي لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية العالية والتي تتمثل في الإستعمال السيء للأنظمة المعلوماتية واستغلالها على نحو غير مشروع بشكل يضر مصالح الأفراد والجماعات ومن ثمة ظهور أنماط مستحدثة من الجرائم منها الجرائم الرقمية، ونتيجة لحداثة هذه الأخيرة فقد كانت هناك اتجاهات مختلفة في تعريفها بذلك لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها فالبعض يطلق عليها جريمة الغش المعلوماتي والبعض الآخر يسميها بجريمة الإختلاس المعلوماتي أو الإحتيال المعلوماتي وهناك من يسميها بالجريمة المعلوماتية وجانب آخر يرى أن هذه الجريمة ناشئة أساسا من التقدم التكنولوجي ففضل أن يطلق عليها اصطلاح "جرائم التكنولوجيا الحديثة" وذلك بالنظر إلى ارتباطها الوثيق بالتكنولوجيا ولحداثتها النسبية وارتباطها بأجهزة حديثة ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل.

وقد تباين الفقه في تعريف الجريمة المعلوماتية فلم يرد لها تعريفا موحدا، ويمكن القول بأنها ذلك الفعل غير المشروع الذي يرتكب بواسطة الحاسب الآلي، أو هو كل فعل إجرامي يستخدم في اقترافه الحاسوب باعتباره الأداة الرئيسية في ذلك.

كما عرفها المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته سنة 2000 بقوله «أنها جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية»، فإيجاد مفهوم دقيق للجريمة المعلوماتية مر بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ففي المرحلة الأولى من شيوع استخدام الحاسوب في الستينات ظهرت أول المعالجات لجرائم الكمبيوتر آنذاك واقتصرت على مقالات صحفية ناقشت التلاعب بالبيانات المخزنة وتدمير أنظمة الحاسوب والتجسس المعلوماتي والإستخدام غير المشروع للبيانات المخزنة في نظم الحاسب الآلي، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد حالة عابرة، أم ظاهرة إجرامية مستجدة؟، بل ثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني، أم مجرد سلوكات غير أخلاقية في البيئة المعلوماتية؟ وبقى التعامل معها أقرب إلى النطاق الأخلاقي منه إلى النطاق القانوني، ومع تزايد استخدام الحواسيب واعتماد المجتمع على الأنظمة المعلوماتية في إنجاز أعماله مع منتصف السبعينات، ظهر عدد من الدراسات القانونية، التي اهتمت بجرائم المعلوماتية، وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكات مستهجنة أخلاقيا، وفي الثمانينات ظهر مفهوم جديد لجرائم المعلوماتية، ارتبط بعمليات اقتحام نظم المعلومات عن بعد، و أنشطة نشر الفيروسات التي تقوم بتدمير الملفات أو البرامج عبر شبكات الكمبيوتر، وشاع اصطلاح (الهاكرز) وغيرها من عناصر الجريمة المعلوماتية بالمفهوم الحديث، كما شهدت فترة التسعينيات تناميا هائلا للجريمة التقنية وما أحدثته شبكة الأنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات وظهور أنماط جديدة كأنشطة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد و أنشطة الرسائل والمواد الكتابية المنشورة على الأنترنت أو المرسلة عبر البريد الإلكتروني.

هذه الجرائم الذكية تنشأ و تحدث في بيئة خاصة ويقترفها أشخاص متميزون (أذكياء ويملكون أدوات المعرفة التقنية) مما يسبب خسائر كبيرة على جميع المستويات الإقتصادية

والإجتماعية و الثقافية والأمنية فهي قد تستهدف فضح الأسرار الشخصية أو القذف أو التشهير بشركات أو أشخاص بقصد الإضرار بالسمعة الشخصية أو المالية أو بداعي الإنتقام كما قد تكون سرقة أو غسيل أموال و تحويلها من حساب لآخر وقد تستهدف تدمير المعلومات أو الإحتيال أو تزوير البطاقات الشخصية أو بطاقات الإئتمان التي زاد خطر انتشارها نظرا لصعوبة التوصل إلى مرتكبيها أو باستخدام البريد الإلكتروني.

وإخفاء آثار الجريمة لا يشكل معضلة قانونية حقيقية من حيث التجريم والعقاب أو من حيث تصنيف الأنماط وتحديد العناصر والأركان كما يعتقد البعض فحسب بل تكمن المعضلة الحقيقية التي تفرزها ظاهرة الجرائم الرقمية في صعوبة عمليات الرصد والمتابعة وتعقيدات الإكتشاف والضبط ومخاطر جمع الأدلة والتحقيق مع فئة المجرمين الأذكياء بجانب ضعف التشريعات الشكلية.

غير أنه لا يجب أن يزعجنا هذا التطور المتسارع في وسائل ارتكاب الجرائم طالما أن العلوم الحديثة وفرت أيضا التقنيات المناسبة لمواجهة التطور الإجرامي، كما يجب على القضاء وأجهزة الشرطة أن تنهض بإمكاناتها العلمية والفنية والإرتقاء بالكادر البشري بالقدر الذي يؤهلها لمواجهة مستجدات الجريمة وكيفية التعامل معها شكلا وموضوعا خاصة في مراحل التحقيقات الأولية وجمع الاستدلالات، واستخدام التقنيات العالية والذكاء الإصطناعي والمعلومات الرقمية في التخطيط والتنفيذ.

ولعل بروز ظاهرة الجرائم الرقمية تشكل في حد ذاتها تحديا حقيقيا للسياسات الجنائية السائدة وأجهزتها التشريعية والتنفيذية والقضائية في كشف هذا النمط من الجرائم والوصول إلى دليل جنائي رقمي عن طريق تطوير القواعد القانونية الخاصة بالبحث والتحري واستخدام طرق وأساليب حديثة من أجل إثبات هذا النوع من الجرائم وهو ما عمل عليه المشرع الجزائري حين أدرج قواعد و نصوص قانونية توسع من الإختصاص القضائي لوكلاء الجمهورية وقضاة التحقيق، وتعزيز صلاحيات الضبطية القضائية بوضع آليات جديدة خاصة بالبحث والتحري تدعم الآليات العامة من أجل الوصول إلى الدليل الرقمي.

وعلى ضوء ما تقدم نجد أن **الإشكالية** التي يجب معالجتها من خلال هذه الدراسة هي:

فيما يتجسد الإطار القانوني المتبع للتحقيق في الجريمة الرقمية؟

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

فيما تتجسد المباديء الأساسية للتحقيق الجنائي في الجرائم الرقمية؟

ماهي الجهات المكلفة بالتحقيق في الجرائم الرقمية؟

ماهي الآليات المتبعة للكشف عن الجرائم الرقمية؟

من أجل هذه الأسئلة وغيرها ونتيجة استفحال ظاهرة الجرائم الرقمية في المجتمع الجزائري ارتأينا تناول هذا الموضوع في ضل القوانين التي استحدثها المشرع الجزائري من أجل مكافحة الجرائم الرقمية منها القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها والمستقاة مواده من إتفاقية بودابست 2001 للجرائم الإلكترونية والتعديلات التي جاء بها قانون الإجراءات الجزائية.

وتتجلى **أهمية هذا الموضوع** في أن التحقيق الجنائي وجمع الإستدلالات يعد من الأنشطة الأمنية التي تأتي في مقدمة محاولات مواجهة الجرائم الرقمية فهو مرحلة تمهيدية الغاية منها تحضير الدعوى الجزائية للفصل فيها عند طرحها أمام القضاء لأن هذه الجرائم على درجة كبيرة من التعقيد والغموض والتشعب لا يمكن الفصل فيها مباشرة أمام القضاء لما يتميز به من خصائص العلنية والشفوية والحضورية الأمر الذي يستلزم أن يمهد له تحقيق سابق فعال وسريع ومدون، يتم فيه بحث معمق وشامل و دقيق للوقائع والأدلة ومن خلال ذلك يمكن للمحقق توجيه القضية إما بالإحالة على المحكمة إذا ما ثبتت أدلة الإدانة أو عدم الإحالة في حال كانت الأدلة ضعيفة، ففي هذه المرحلة تكون وسائل البحث عن الحقيقة أكثر فاعلية ومرونة منها أمام القضاء.

– كما تتضح الأهمية أيضا في كيفية تعامل جهات التحقيق مع هذه الجريمة لاستخلاص الدليل الرقمي، فالتحقيق في الجرائم الرقمية يتم في وقت معاصر لوقوع الجريمة أو إثر ذلك مباشرة مما يتيح فرصة التنقيب وجمع أدلتها ذات الطابع الخاص في الوقت الملائم وأي تأخير

قد يؤدي إلى العبث بها وإفسادها مما يفقدها قيمتها في الإثبات، كما أن هناك من الإجراءات العامة أو الخاصة ما تفرض طبيعته ضرورة مباشرته في أقرب وقت من وقوع الجريمة على اعتبار أن هذا النوع من الجرائم يقوم في بيئة افتراضية.

– وتظهر كذلك في حداثة الموضوع واعتماد الجهات المكلفة بالتحقيق إلى جانب الإجراءات العامة إجراءات تحقيق مستحدثة تتناسب وطبيعة الجريمة المعلوماتية وأيضا استخدام وسائل تقنية لاستخلاص الدليل الرقمي، كما منح المشرع للجهات المكلفة بالتحقيق صلاحيات واسعة من خلال تعديل قانون الإجراءات الجزائية وكذا القانون 04/09 السالف الذكر والمرسوم الرئاسي 261/15

فهذه الأهمية هي من كانت **الدافع أو السبب في اختيارنا لهذا الموضوع** فراحت بين أسباب ذاتية وأخرى موضوعية؛ **فالأسباب الذاتية** ترجع إلى الرغبة في الخروج عن دراسة الجرائم الكلاسيكية وتناول مثل هذه المواضيع الشيقة التي لم يتم التطرق إليها بصفة دقيقة، أما **الأسباب الموضوعية** فتمثلت في حداثة الموضوع وطرح العديد من الإشكالات حول كيفية ممارسة إجراءات التحقيق في الجرائم الرقمية التي تقوم في عالم افتراضي.

والهدف المتوخى من هذه الدراسة هو إثبات حقيقة وقوع الجريمة في العالم الإفتراضي ومعرفة الكيفية التي نفذت بها والظروف التي واكبت ارتكابها ذلك أن الغاية الأساسية من التحقيق هو الكشف عن الحقيقة و التنقيب عن الأدلة وجمعها في إطار التقييم القانوني لها.

– أيضا كشف دور التحقيق في معرفة الأسباب والدوافع المؤدية لارتكاب الجريمة لما لها من أهمية في التوصل إلى معرفة الجاني الحقيقي والقبض عليه وتسليمه للعدالة ويعد ذلك ثمرة نجاح المحقق الذي يبقى عليه أن يدعم إدانته للمتهم بالأدلة القوية سواء كانت مادية ملموسة أو مخزنة في العالم الإفتراضي، وقد يواجه المحقق قضايا تكون فيها شخصية الجاني غامضة ومجهولة مما يستلزم بذل المزيد من الجهد لمعرفة الفاعل، خصوصا وأن الجريمة المعلوماتية تقوم على الدليل الرقمي من أجل إثبات التهمة على المجرم المعلوماتي وهذا ما يسعى إليه التحقيق في هذه الجريمة.

– كذلك توضيح الطابع الخاص الذي تكتسيه الآليات العامة للتحقيق و مدى نجاعة الآليات الخاصة في كشف غموض الجرائم الرقمية و الحصول على دليل رقمي و توضيح مدى اختلاف التحقيق في هذه الجرائم عن الجرائم التقليدية.

وقد تناولت العديد من **الدراسات السابقة** الجريمة الرقمية بصفة عامة وهي عديدة و متعددة منها مذكرة صغير يوسف في الجريمة المرتكبة عبر الأنترنت، جواحي عبد الستار صاحب مذكرة جرائم الحاسوب...، أو أنها تخصصت في دراسة الآليات الخاصة كإجراءات تحقيق قضائي كمذكرة أحمد مسعود مريم أو أطروحة بن فردية محمد التي تناولت الإثبات الجنائي لهذه الجرائم، غير أن هذه الدراسة جاءت متخصصة في التحقيق الجنائي والدور الذي يلعبه المحقق في كشف الجرائم الرقمية، كما أننا حاولنا التوسع أكثر في هذا البحث عن مذكرة كانت قد تناولت ذات الموضوع بشكل مختصر جدا وهي مذكرة لـ: السوفي نور الهدى، وسعينا لاستدراك جميع النقائص التي وردت فيها إذ لم تتطرق إلى العديد من النقاط كتوسيع إختصاص الضبطية القضائية وقاضي التحقيق، ودور مقدمو الخدمات، والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، وهو ما جاءت به مذكرتنا إضافة إلى إضفاء نفسنا على النقاط المشتركة بين المذكرتين.

وقد **واجهنا خلال عملنا هذا بعض الصعوبات** تمثلت في نقص المراجع المتخصصة في التحقيق الرقمي وفي الآليات المستحدثة في مكافحة الجرائم الرقمية بالرغم من توافر كم لا بأس به من المراجع التي تناولت الجريمة الرقمية بصفة عامة أو التي أخذت الموضوع في شكل جزئي منها، إضافة إلى عدم وجود قانون خاص ينظم الجرائم المعلوماتية ويحدد الإجراءات المتبعة بشأنها كما لمسنا صعوبة البحث في هذا الموضوع لاتصاله بجانب تقني فني يتعلق بالنظام المعلوماتي بشقيه المادي والمعنوي.

وبغرض الإجابة على الإشكالية المطروحة أعلاه والأسئلة المتفرعة عنها، ومن أجل الوصول إلى تحقيق مادة علمية ثرية تطلب منا إعداد هذا البحث **الإعتماد على المنهج التحليلي** من خلال تحليل بعض المفاهيم القانونية المتعلقة بالموضوع وكذلك شرح المواد ذات

الصلة به منها بعض المواد في قانون الإجراءات الجزائية وكذا القانون 04/09، والمرسوم الرئاسي رقم:261/15، وقد اعتمدنا في ذلك **الخطة** التالية:

الفصل الأول نعالج فيه التحقيق الجنائي في الجريمة الرقمية والقائمين به من خلال مبحثين نتطرق في **(المبحث الأول)** إلى الإطار المفاهيمي للتحقيق الجنائي في الجرائم الرقمية، و في **(المبحث الثاني)** إلى معرفة المحقق في الجريمة الرقمية.

أما **الفصل الثاني** فندرس فيه الآليات التي يتم بها التحقيق الجنائي في الجرائم الرقمية وذلك من خلال مبحثين نتطرق في **(المبحث الأول)** إلى الآليات الإجرائية العامة للتحقيق في الجرائم الرقمية، ثم نعرج في **(المبحث الثاني)** إلى الآليات الإجرائية الخاصة للتحقيق في الجرائم الرقمية.

الفصل الأول

ماهية التحقيق الجنائي في الجرائم الرقمية

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

والتحقيق بصفة عامة يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهية لديه، وأن يحاول بكل جهده أن يقوم بالتحقيق في الجريمة ومتابعتها وبالبحث فيها وفي أدلة الإثبات من أجل إظهار الحقيقة، لذلك سوف نتطرق في هذا الفصل إلى الإطار المفاهيمي للتحقيق الجنائي في الجرائم الرقمية في **(المبحث الأول)** ونتعرض للمحقق الجنائي في الجرائم الرقمية في **(المبحث الثاني)**.

المبحث الأول: الإطار المفاهيمي للتحقيق الجنائي في الجرائم الرقمية

يعد التحقيق الجنائي في الجرائم الرقمية أحد الأنشطة القانونية المتعلقة بإجراءات ضبط الجرائم والبحث عن مرتكبيها وجمع الإستدلالات التي يتطلبها التحقيق والدعوى الجنائية ككل فهو الضبط القضائي للجاني والدليل على إدانته أو براءته ويتجلى دور المحقق في هذه المرحلة في تلقي البلاغ وجمع الإستدلالات ضد مرتكب الجريمة من أجل تقديمها إلى جهات التحقيق من هذا يتضح أن إجراءات التحقيق تمر بثلاث مراحل تهدف جميعها إلى ضبط الجاني وتقديمه أمام جهات التحقيق بأدلة إتهام وبعدها إلى جهات الحكم وهذه المراحل تتمثل في[1]:

1/ مرحلة جمع الإستدلالات[2] بواسطة الضبطية القضائية المختصة بالبحث في الجرائم ومرتكبيها.

2/ مرحلة التحقيق الإبتدائي[3] الذي يقوم به قاضي التحقيق أو النيابة العامة لتحريك الدعوى الجنائية أو حفظ التحقيقات لعدم كفاية الأدلة.

3/ مرحلة التحقيق النهائي[4] وهي مرحلة المحاكمة.

---

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

[2] خلال هذه المرحلة يكون لرجال الشرطة دور جد مهم في اتخاذ الإجراءات اللازمة للكشف عن الجريمة ومرتكبيها وذلك بقبول البلاغات والشكاوى والتثبت من وقوع الجريمة والبحث عن مرتكبيها وإجراء المعاينات والإستدلال على الشهود وسماع أقوالهم وإجراء التحريات وجمع المعلومات والأدلة وتحديد شخصية الجناة وضبطهم وجمع العناصر التي تصلح لأن تكون أساسا في بدء التحقيق الإبتدائي ويتم إثبات جميع هذه الإجراءات في محضر يسمى بمحضر جمع الاستدلال

[3] وهي المرحلة التي يقوم بها أعضاء هيئة التحقيق والإدعاء العام أو من تثبت لهم صفة المحقق من ضباط الشرطة، وتأتي هذه المرحلة بعد مرحلة جمع الإستدلالات فلأجهزة التحقيق الجنائي الحق في التصرف في محضر جمع الإستدلالات سواء بإقامة الدعوى الجنائية وعرضها على القضاء أو بردها لعدم صلاحيتها للعرض.

[4] وهو التحقيق الذي يجرى في جلسة المحاكمة فللقاضي الحق في اتخاذ ما يراه مناسبا وفقا لأصول المحاكمات لتكوين قناعته الشخصية قبل إصدار الحكم ومن ذلك سؤال المتهم ومناقشته عن التهمة المنسوبة إليه ومواجهته بما توفر ضده من أدلة وسماع دفاعه

وحتى يتم الإلمام بمفهوم التحقيق الجنائي في الجرائم الرقمية ارتأينا تقسيم هذا المبحث إلى مطلبين نتناول في (المطلب الأول) المبادئ الأساسية للتحقيق الجنائي في الجرائم الرقمية وفي (المطلب الثاني) وسائل التحقيق الجنائي في الجرائم الرقمية.

المطلب الأول: المبادئ الأساسية للتحقيق الجنائي في الجرائم الرقمية

إن التعرف على المبادئ الأساسية للتحقيق الجنائي في الجرائم المعلوماتية يتطلب التعرض إلى مفهوم التحقيق الجنائي في الجرائم الرقمية (الفرع الأول) وكذا العناصر الأساسية للتحقيق (الفرع الثاني) وضمانات المتهم في مرحلة التحقيق الجنائي (الفرع الثالث) وذلك على النحو التالي:

الفرع الأول: مفهوم التحقيق الجنائي في الجرائم الرقمية: ويتجلى هذا المفهوم من خلال التطرق إلى تعريف التحقيق الجنائي في الجرائم الرقمية و خصائص التحقيق الجنائي فيها.

أولا: تعريف التحقيق الجنائي في الجرائم الرقمية:

قبل التطرق إلى معرفة التحقيق الجنائي في الجرائم الرقمية ارتأينا التعرض أولا إلى معرفة التحقيق الجنائي بصفة عامة لغة واصطلاحا.

1/ التحقيق لغة: "مأخوذ من حققت الأمر، إذا تيقنته أو جعلته ثابتا لازما، وحقيقة الشيء منتهاه وأصله المشتمل عليه"، ويقال "حق الأمر حقا: صح وثبت وصدق ويقال أحقه على الحق: غلبه وأثبته عليه"، وقد ورد للحق أيضا معانٍ أخرى منها: " المال والمِلك بكسر الميم وبمعنى الموجود الثابت، وبمعنى الصدق والموت والجزم، ويقال تحقق الرجل الأمر أي تيقنه ، ويقال تحقق عند الخبر أي صح، والحق اليقين بعد الشك"[1].

[1] غسان مدحت الخيري، أصول التحقيق الإبتدائي كحق من حقوق الإنسان، دار الراية للنشر والتوزيع، الأردن، ط1، 2013، ص 19.

وعرفه بن المنظور "بأنه التصديق أو التأكيد أو التثبت، نقول حقق فلان ظنه بمعنى صدقه وحقق الأمر أي أكده وثبته"[1].

والمعنى القريب لما يستخدم حاليا هو التيقن من حقيقة الأمر وثبوته بعد الشك.

2/ التحقيق إصطلاحا:

في اصطلاح الفقه الإسلامي عرف التحقيق بأنه: "إثبات المسألة بدليلها"[2].

وفي اصطلاح شراح القانون تعددت التعريفات الفقهية للتحقيق الإبتدائي إلا أنه على الرغم من تعددها فهي لا تخرج عن تعريفه بأنه مجموعة من الإجراءات القضائية تمارسها سلطات التحقيق بالشكل المحدد قانونا[3]، بغية التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها في إحالة المتهم إلى المحاكمة، أو الأمر بألا وجه للمتابعة.

وعرف أيضا بأنه مجموعة من الإجراءات التي تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم على المحكمة[4].

من هذا التعريف يتضح أن للتحقيق الجنائي بصفة عامة معنيان، معنى عام أو واسع ومعنى خاص أو ضيق.

فالتحقيق الجنائي بالمعنى الواسع هو مجموعة الإجراءات التي تتخذها سلطة التحقيق وذلك بالتحري عن الجريمة وجمع الأدلة أي إتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها.

---

[1] السوفي نور الهدى، التحقيق في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر أكاديمي في الحقوق، تخصص قانوني جنائي، جامعة قاصدي مرباح، ورقلة، 2017، ص7.

[2] غسان مدحت الخيري، مرجع سابق، ص 19

[3] حسن الجوخدار، التحقيق الإبتدائي في قانون أصول المحاكمات الجزائية، دار الثقافة للنشر و التوزيع، الأردن، ط1، 2008، ص 11.

[4] محمد حمدان عاشور، أساليب التحقيق والبحث الجنائي، أكاديمية فلسطين للعلوم الأمنية، قسم المنهاج، فلسطين، 2010، ص6

أما التحقيق الجنائي بالمعنى الضيق هو تلك الإجراءات التي تختص بها سلطة التحقيق وحدها والتي تتميز عن أعمال جمع الإستدلالات فالتحقيق بالمعنى الضيق يمثل المرحلة الوسطى بين مرحلة جمع الإستدلال وبين التحقيق النهائي في الدعوى الجزائية.

هناك من رجال الشرطة من عرفه "بأنه العلم الذي يرشد المحقق إلى كيفية السير في التحقيق من بدايته إلى نهايته ويعلمه كيف يكتشف الجرام الغامضة بتتبع أثر الجاني إذا فر من وجه القضاء كي يتمكن من القبض عليه و ينال ما يستحق من جزاء"[1].

3/ التحقيق في الجرائم الرقمية:

يمكن تعريف التحقيق الجنائي في الجريمة الالكترونية على أنه ذلك العمل القانوني الذي يقوم به ضابط الشرطة القضائية المختص والمتخصص لضبط الجرائم الإلكترونية الرقمية من فاعل ودليل إلكتروني رقمي إلى سلطات التحقيق القضائي المختصة في هذا النوع من الجرائم[2].

فالتحقيق الجنائي إذا هو ذلك العمل القانوني الذي يقوم به ضابط الشرطة القضائية لكشف الجريمة ونسبتها إلى الفاعل وتقديم أدلة الإثبات إلى سلطات التحقيق من أجل تحريك الدعوى الجنائية.

ثانيا: خصائص التحقيق الجنائي في الجرائم الرقمية:

يتميز التحقيق الجنائي في الجرائم الإلكترونية عن ذلك التحقيق الجنائي في الجرائم التقليدية بصعوبة وتعقيد بالغين مردها جملة من الأسباب نذكر منها:

1/ الجرائم التي تقع على الحاسب الآلي وشبكات المعلومات مستترة أو خفية في أكثر صورها فلا يلاحظها المجني عليه أو يدرى حتى بوقوعها و الإمعان في حجب و إخفاء السلوك المكون

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ط1، 2009، ص 166.

[2] نفس المرجع والصفحة.

لها وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئي بالنبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها[1].

2/ أن المجرم الإلكتروني يتميز بالذكاء فلديه القدرة على إتلاف وتشويه وإضاعة الدليل الإلكتروني الرقمي بشكل سريع في وقت قصير جدا.

3/ الكثير من الجرائم الإلكترونية لا تترك أثرا ماديا في مسرح الجريمة الالكترونية.

كما أن التحقيق في الجريمة الالكترونية يحتاج إلى إمكانيات مادية وقواعد إجراءات تختلف عن التحقيق في الجرائم التقليدية سواء تعلق الأمر بطبيعة السلوك الإجرامي الإلكتروني أو بطبيعة الدليل الالكتروني أو وسائل وآليات كشف الجريمة والوصول إلى الدليل الإلكتروني الأمر الذي يميز بعض الإجراءات الشكلية المتبعة في التفتيش والضبط وتكوين فرق العمل وأساليب تأمين الأدلة الإلكترونية الرقمية والمادية عن إجراءات التفتيش في الجرائم العادية[2].

الفرع الثاني: العناصر الأساسية للتحقيق الجنائي في الجرائم الرقمية

يجب على المحقق أن يستظهر الركن المادي والركن المعنوي للجريمة محل التحقيق، وتحديد وقت ومكان ارتكاب الجريمة المعلوماتية.

أولا: إظهار الركن المادي للجرائم الرقمية

إن السلوك المادي في جرائم الأنترنت يتطلب وجود بيئة رقمية واتصال بالأنترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل الكمبيوتر ببرامج اختراق أو أن يقوم بإعداد هذه البرامج بنفسه وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف hosting server كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.

[1] هشام محمد فريد رستم، الجرائم المعلوماتية: أصول التحقيق الجنائي الفني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة و القانون جامعة الإمارات العربية المتحدة، مجلد 2، الفترة من01 إلى03 ماي 2000، ص 420.

[2] مصطفى محمد موسى ، المرجع السابق ، ص 167.

لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية[1] وفي واقع الحال يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الالكترونية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق وبرامج فيروسات ومعدات لفك الشفرات وكلمات مرور مثل هذه الأشياء تمثل جريمة في حد ذاتها.

وقد نص المشرع الجزائري في محتوى المادة 394 مكرر7 على أن الشروع في ارتكاب الجريمة المعلوماتية يعاقب عليه بنفس العقوبة المقررة للجنحة ذاتها[2].

ثانيا: إظهار الركن المعنوي للجرائم الرقمية

الركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني أي توافر العلم والإرادة في ارتكاب الجريمة.

ثالثا: تحديد وقت ومكان ارتكاب الجريمة الرقمية

تثير مسألة النتيجة الإجرامية في جرائم الأنترنت مشاكل عدة منها صعوبة تحديد مكان وزمان تحقق النتيجة الإجرامية في حال ما إذا كانت الجريمة عابرة للحدود كما يثور أيضا الإشكال حول القانون الواجب التطبيق مثال ذلك قيام أحد المجرمين في أمريكا باختراق جهاز خادم server أحد البنوك في الإمارات وهذا الخادم موجود في الصين، فكيف يمكن تحديد وقت حدوث الجريمة هل هو توقيت بلد المجرم أو البلد الموجود فيه البنك المسروق أو توقيت الجهاز في الصين[3].

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الاسكندرية، ط1 ، 2009، ص 52.

[2] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، بدون طبعة، 2011 ، ص 107.

[3] خالد ممدوح إبراهيم، نفس المرجع، ص 53.

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

يهدف التحقيق الجنائي إلى تحقيق العدالة بين جميع أطراف الدعوى وكلما توافرت للتحقيق الجنائي كافة الضمانات أدى ذلك إلى شعور الجميع بالإطمئنان وعدم وقوع أي منهم تحت وطأة الظلم ومن أهم الضمانات نذكر:

أولا: علانية التحقيق بالنسبة للخصوم

إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة ولهذا قيل أن العلانية في مرحلة المحاكمة لا يقتصر فيها الأمر على وضع الطمأنينة في قلب المتهم بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلا للشك أو الخضوع تحت التأثير كما أن فيها اطمئنانا للجمهور على أن الإجراءات تسير في طريق طبيعية.

والعلانية في التحقيق الإبتدائي تختلف عنها في مرحلة المحاكمة ففي الأولى تكون العلانية نسبية قاصرة على الخصوم فقط في الدعوى الجنائية أما في التحقيق النهائي تكون مطلقة أي يجوز لأي فرد من أفراد الجمهور الدخول إلى قاعة الجلسة وحضور المحاكمة.

غير أن هناك جانب من الفقه يرى ضرورة تطبيق قاعدة العلانية على إجراءات التحقيق الإبتدائي مثلما هو الشأن في التحقيق النهائي فيتعين إجراؤه في حضور الجمهور بدون تميز لأنه من شأن ذلك إيجاد رقيب غير متحيز يحكم في تصرفات المحقق فيدفعه إلى الإلتزام بالحياد و النزاهة في البحث عن الحقيقة[1].

ثانيا: سرية التحقيق بالنسبة للجمهور

من الضمانات المتعلقة بالمتهم في مرحلة التحقيق والتي تحرص عليها أغلب القوانين الجزائية المتعلقة بهذا الشأن جعل التحقيق الإبتدائي ذا طبيعة سرية بالنسبة للجمهور ويجب على القائمين بالتحقيق عدم إفشاء أسرار التحقيق تجنبا لأي إساءة أو تشهير للمتهم قبل أن تثبت إدانته ذلك أن الإتهام الموجه له لا يعدو سوى وقائع مادية أو قانونية نسبت له على

[1] غسان مدحت الخيري. المرجع السابق، ص95.

خلاف الأصل الذي يتمتع به كل فرد وهو البراءة، كما أن هذه السرية تحد من انتشار الشائعات بين أفراد المجتمع والتنبؤ بأحداث القضية والمبالغة في الوقائع المنسوبة إلى المتهم.

والبحث عن الأدلة يقتضي أن يتم في سرية حتى لا يتمكن من لم يتناوله التحقيق من الوقوف على ما سيتخذ من إجراءات فيعمد إلى إفساد الأدلة أو طمسها ومن ثمة يعمل على تضليل العدالة فلا تتمكن محكمة الموضوع من الوقوف على الحقيقة و إفلات الجاني من العقاب[1].

وكل شخص يساهم في هذه الإجراءات من خبراء و أمناء ضبط و مترجمين... ملزمين بكتمان السر المهني بالشروط المبينة في قانون العقوبات تطبيقا لنص المادة 11 ق.إ.ج[2].

ثالثا: حق المتهم في محاكمة عادلة وسريعة

التحقيق الجنائي يهدف إلى تحقيق العدالة وليس سيفا مسلطا على المتهم لذلك أقر المشرع بضرورة السرعة في إنجاز التحقيق بما لا يخل من الدقة والموضوعية لتجنب الإضرار بالمتهم الموضوع رهن الحبس الاحتياطي.

كما أن سرعة إتلاف الدليل في الجرائم الرقمية تستدعي السرعة في التحقيق في ظل الحاجة للتدخل السريع من أجل ضبط متعلقات الجريمة.

رابعا: حق المتهم في الإستعانة بمحام

لقد كفل القانون للمتهم حق الدفاع حتى لو لم يكن لديه القدرة المادية لتوكيل محام للدفاع عنه، وحق الإستعانة بمدافع يعتبر من أهم ضمانات التحقيق فحضور المحامي مع موكله أثناء التحقيق فيه ضمان لسلامة الإجراءات ولعدم استعمال الوسائل الممنوعة أو غير الجائزة مع المتهم، فضلا عن أنه يهدئ من روع المتهم ويساعده على الإتزان والهدوء في إجاباته.

[1] حسن الجوخدار، المرجع السابق ، ص 38.

[2] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر، الجزائر، ط2، 2009، ص22.

المطلب الثاني: وسائل التحقيق الجنائي في الجرائم الرقمية

عند قيام المحقق بالتحقيق في جريمة ما عليه أن يلتزم في ذلك بقوانين وتشريعات وقواعد فنية في سبيل الكشف عن الحقيقة والوصول إلى الجاني فالمحقق يتبع الإجراءات المحددة والمحكومة باللوائح المنظمة والقواعد الفنية للتحقيق، كما يتبع أساليب متغيرة كل أسلوب منها يعالج حالة معينة في ظروف معينة، فالمحقق يدرس الحالة ويقرر الأسلوب المناسب من خلال دراسته لقضية التحقيق، بالتالي فهو يحتاج لعدة وسائل مادية وطرق والأساليب لضبط الجريمة وجمع الأدلة بهدف إثبات وقوعها ونسبتها إلى الجاني، وهذه الوسائل قد تكون مادية أو إجرائية وينبغي في ذلك إتباع منهجا محددا، لذلك سيتم من خلال هذا المطلب التطرق إلى منهج التحقيق الجنائي في الجريمة الرقمية (الفرع الأول) و إلى الوسائل المادية للتحقيق (الفرع الثاني) ثم الوسائل الإجرائية(الفرع الثالث).

الفرع الأول: منهج التحقيق الجنائي في الجرائم الرقمية

التحقيق الجنائي له قواعد قانونية و أخرى فنية، تتمثل الأولى في تلقى المحقق البلاغ عن وقوع الجريمة متبعا في ذلك الإجراءات اللازمة للكشف عن غموضها وضبط الفاعل وتقديمه للمحاكمة أما القواعد الفنية للتحقيق الجنائي فتتمثل في تلك التي تحكم المحقق منذ تلقيه البلاغ حتى ضبط المتهم، وحتى يتمكن من التوصل إلى هذه النتيجة عليه أن يتبع منهجا أو أسلوبا محددا في التحقيق يتمثل في تحديد خطة عمل وتكوين فريق متكامل.

أولا: تحديد خطة عمل التحقيق

بعد استكمال جمع المعلومات اللازمة عن الواقعة الإجرامية يبدأ المحقق معتمدا على تلك المعطيات المتوفرة لديه بتحديد خطة عمل مناسبة وفريق عمل للتحقيق في الحادثة ولابد أن تكون هذه الخطة قد اكتملت في ذهن المحقق بمجرد انتهائه من معاينة موقع الحادث واتضحت لديه الصورة الأولية عن الحادث[1].

[1] حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ط1، 2000 ، ص 231.

1/ تحديد خطة العمل المناسبة:

يتم التخطيط للتعامل مع حوادث الحاسب الآلي وشبكة الأنترنت على ثلاث مستويات مختلفة يبنى كل مستوى منها على الآخر[1].

أ/ تخطيط استراتيجي:

وهو تخطيط بعيد المدى يهتم بحماية البنية التحتية لشبكات الحاسوب الوطنية، من خلال تحديد مصادر الخطر المحتملة التي قد تمثل تهديدا لها وتحديدها، ويهتم بوضع تصورات على درجة من المرونة تكون كفيلة بالتصدي لهذا النوع من الجرائم قبل وقوعها وضبطها والحد من آثارها في حال وقوعها، ويتم هذا التخطيط على مستوى واضعي السياسات الأمنية، حيث يهدف بشكل عام إلى منع هذا النوع من الجرائم من الوقوع داخل إقليم الدولة، والحد من قابلية الحواسيب والشبكات الوطنية من التعرض للهجوم، ومن ثم السيطرة على الحوادث إن وقعت وضبطها والحد من آثارها.

ومن أهم ما يميز هذا النوع من التخطيط أنه يضع الخطوط الإسترشادية 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 الإستراتيجية ويتم على مستوى الجهات الرسمية وغير الرسمية التي لها علاقة بتقنية المعلومات ويدعم غايات وأهداف الخطة الإستراتيجية للتعامل مع جرائم الحاسوب والأنترنت، ويمتاز بأن له طابع تفصيلي أكثر من التخطيط الإستراتيجي، والخطط التكتيكية الخاصة بالتعامل مع جرائم الأنترنت يجب أن تتضمن إجراءات مسبقة التحديد على درجة عالية من التفصيل والوضوح للتحقيق في هذه الجرائم.

[1] حسين بن سعيد الغافري، التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنات، موقع المنشاوي للدراسات و البحوث على الموقع WWW.minshawi.com أطلع عليه بتاريخ: 2018/02/11، ص 6.

ج/ خطة العمل:

ويقصد به التخطيط الذي يقوم به المحقق لتحديد الأسلوب الأمثل في التعامل مع حادث بعينه، وذلك في الإطار العام للإجراءات الواردة في الخطة التكتيكية وبما يتناسب مع خصوصية ظروف وملابسات الحادث.

2/ **مرتكزات خطة العمل:**

تعد من أهم الأمور التي يجب على المحقق أخذها بعين الإعتبار كمرتكزات تساعده في تحديد خطة العمل المناسبة للتحقيق في أي جريمة من الجرائم الرقمية والانترنت[1].

أ/ حجم ونوع الحادث التي يكون المحقق بصدد التحقيق فيه يرتبط به تحديد حجم ونوع فريق التحقيق، فجرائم الانترنت منها الصغير ومنها الكبير ولكل جريمة مهما كان حجمها، طبيعتها الفنية الخاصة التي تفرض على أعضاء فريق التحقيق امتلاك مهارات فنية خاصة تعتبر ضرورية للتعامل مع هذا النوع من الجرائم، وهو أمر 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، ومن هذه العوامل:

- مدى أهمية الأجهزة الحاسوبية والشبكات المتضررة لعمل المنظمة أو المؤسسة.
- مدى حساسية البيانات التي قد تكون محل الجريمة الحاسوبية.
- المتهمون المحتملون.
- اطلاع الرأي العام على الجريمة أم لا.
- مستوى الإختراق الأمني الذي تسبب فيه الجاني.
- مستوى المهارة الفنية التي يتمتع بها الجاني.

ج/ طبيعة مسرح الجريمة تفرض الأسلوب الأمثل للتفتيش بحثا عن الأدلة التي تكون موجودة فيه والذي يعتبر من أهم خطوات عملية التحقيق وعدم نجاح المحقق في تحديد هذا الأسلوب قد

[1] حسين بن سعيد الغافري، المرجع السابق، ص6.

يؤدي إما إلى عدم الحصول على أية نتائج أو الحصول على كم كبير من النتائج التي لا فائدة منها، فقائد فريق التحقيق مسؤول عن تحديد حجم المهمة ونوع الأدلة التي يتم البحث عنها بحسب نوع الجريمة، وكذلك تحديد أنسب الطرق لتنفيذ عملية التفتيش وما يتبع ذلك من توزيع للأدوار والواجبات على فريق التحقيق.

د/ تعيين الأشخاص الذين سيتم استجوابهم، وتحديد النقاط التي يجب استيضاحهم بشأنها، وكذلك تقدير مدى الحاجة الى الإستعانة ببعض الأشخاص من ذوي الإختصاصات الفنية التي يتطلبها التحقيق ولا تتوافر ضمن أفراد التحقيق.

ثانيا: تكوين فريق التحقيق

إن التحقيق في قضايا نظم المعلومات عادة ما يكون أكبر من أن يتولاه شخص واحد بمفرده، حتى و إن كانت المضبوطات مجرد حاسب شخصي واحد، فمن الأفضل أن يتعاون عدة أشخاص في إنجاز مهمة التحقيق و العثور على الأدلة[1]؛ فهناك محققون جنائيون ذوو خبرة طويلة، وهناك أخصائيون في الحاسب الآلي والشبكات ذو معرفة واسعة، ولكنه من النادر أن يوجد شخص واحد يمتلك مهارات عالية في الاثنين معا، لاسيما وأن عالم الحاسوب والشبكات عالم متعدد ومتشعب وعلى درجة كبيرة من التعقيد وسرعة التطور، ولذلك كان من الضروري أن يستعين المحقق بخبراء في هذا المجال بحسب ما تفرضه ظروف كل قضية وملابساتها.

كما أن التحقيق في هذه الجرائم قد يتطلب الإستعانة ببعض خبراء مسرح الجريمة التقليدية، مثل خبير البصمات وخبير التصوير الذين يعتبرون من الخبراء الأساسيين في معظم أنواع الجرائم.

وعلى هذا الأساس يمكن تقسيم فريق التحقيق في هذا النوع من الجرائم إلى فئتين هما:

[1] حسن طاهر داود، المرجع السابق، ص 223.

الفئة الأولى:

وتمثل الأشخاص الذين يتصل عملهم مباشرة بجرائم الحاسب الآلي والأنترنت ولا يمكن التحقيق في أي جريمة تنتمي إلى هذه النوعية من الجرائم إلا بهم، ووجودهم ضروري في مسرح الجريمة ويمكن تحديد أعضاء هذه الفئة على النحو التالي:[1]

1- **قائد الفريق أو المحقق الرئيسي:** يشترط فيه أن يكون له خبرة طويلة في مجال التحقيق الجنائي، ولديه معرفة بالطبيعة الخاصة بجرائم الحاسب الآلي والأنترنت يتولى السيطرة الكاملة على مسرح الجريمة، وتوزيع المهام على الفريق والإشراف على قيامهم بأعمالهم، والتنسيق مع الجهات ذات العلاقة، واتخاذ كافة القرارات المتصلة بالتحقيق.

2- **محقق جنائي:** شخص أو أكثر بحسب ظروف الجريمة، لديه خبرة ومعرفة بوسائل وأساليب التحقيق وإجراءاته، مع إلمامه بطبيعة جرام الحاسوب والأنترنت وكيفية التعامل مع الأدلة الرقمية فيتولى التفتيش عن الأدلة وأخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة.

3- **خبير حاسب آلي وشبكات:** شخص أو أكثر بحسب الظروف يجمع بين المعرفة بعلوم الحاسوب والشبكات وبين الإلمام بإجراءات التحقيق الجنائي وأساليبه وكيفية التعامل مع مسرح الجريمة ويكون مسؤول عن رفع وتحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة التي لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوى والعرض على المحكمة.

4- **خبير تدقيق حسابات** متخصص في المراجعة المحاسبية وعلى درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة في المؤسسات المصرفية والآليات المختلفة التي يتم بواسطتها تبادل النقد الإلكتروني، ويعمل مع خبير الحاسب الآلي والشبكات على تحديد أسلوب الجريمة وما إذا كان هناك تلاعب في الأنظمة المتضررة بالإضافة إلى تقدير الخسائر المادية الناتجة عن الجريمة.

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

5- **خبير تصوير** يتولى تصوير مسرح الجريمة كما هو متبع في جميع الجرائم فيعمل على تصوير كل المواقع داخل مسرح الجريمة وخارجه وتصوير أدلة الجريمة بالتصوير الفوتوغرافي والفيديو[1].

6- **خبير بصمات:** لرفع البصمات من مسرح الجريمة كإجراء عام في معظم الجرائم مع التركيز على المكونات المادية للحواسيب والشبكات المتضررة أو المشتبه بوجود صلة لها بالجريمة، خاصة لوحة المفاتيح والفأرة، وذلك بعد اتخاذ الاحتياطات الفنية اللازمة من قبل خبير الحاسوب.

7- **خبير رسم تخطيطي:** يقوم بعمل رسم تخطيطي (كروكي) لمسرح الجريمة بطريقة فنية دقيقة مستخدما مقياسا مناسبا للرسم، بما يوضح تقسيماته وأماكن تواجد الأدلة والأشخاص فيه.

الفئة الثانية:

وهي تمثل الأشخاص الذين قد يتطلب ظروف مسرح الجريمة تواجدهم، إلا أن دورهم ليس وثيق الصلة بالطبيعة الخاصة لجرائم الحاسب الآلي، وقلما يخلوا مسرح أي جريمة مهما كان نوعها من وجودهم، مثل أفراد حماية وتأمين المسرح وأفراد القبض وأفراد التحريات وغيرهم، وتحديد الأعضاء نوعا وكما متروك لتقدير المحقق على ضوء المعلومات المتوفرة لديه عن الجريمة، وحسب ما تفرضه طبيعة مسرح الجريمة وحجمها وظروفها.

الفرع الثاني: الوسائل المادية للتحقيق الجنائي في الجرائم الرقمية

ويقصد بالوسائل المادية تلك الأدوات الفنية التي غالبا ما تستخدم في بيئة نظم المعلومات والتي يمكن باستخدامها يتم تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتحدد شخصية مرتكبها[2]، وفي الغالب ما تكون الجرائم التي تقع بواسطة شبكة الأنترنت تكون أصعب في الإثبات وتستدعي تدخل الجهات الأمنية أكثر من جرائم النظم الأخرى التي تعلن عنها المؤسسات والتي يكون فيها المجرم غير خاضع للنظام الداخلي

[1] المهندس حسن طاهر داود، المرجع السابق، ص 224.

[2] السوفي نور الهدى، المرجع السابق، ص 15.

للمؤسسة ولا يعمل لديها ومن هنا جاء التركيز على الجرائم التي ترتكب عن طريق شبكة الانترنت وبالرغم من أن الشبكات الأخرى لها نفس الخصائص ومن أهم هذه الوسائل نذكر:

أولا: عناوين (IP[1] و MAC[2] والبريد الإلكتروني وبرامج المحادثة)

عنوان الأنترنت (IP) هو المسؤول عن تراسل حزم البيانات عبر الأنترنت وتوجيهها إلى هدفها، ويشبه إلى حد كبير العنوان على مغلف رسائل البريد التقليدي بعد وضعها بصندوق البريد، وهو يتيح للموجهات والشبكات المعنية بنقل الرسالة، يوجد عنوان (IP) بكل جهاز مرتبط بالأنترنت ويتكون من أربعة أجزاء والجزء الواحد يتكون من ثلاث خانات، فيكون المجموع إثناعشر خانة كحد أقصى حيث يشير الجزء الأول من اليسار إلى المنظمة الجغرافية، والجزء الثاني لمزود الخدمة والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الحاسب الآلي الذي تم الإتصال منه، وفي حالة وجود أي مشكلة أو أي أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، ويمكن لمزود خدمة الأنترنت أن يراقب المشترك، كما يمكن للشركة التي تقدم خدمة الإتصال الهاتفي أن تراقبه أيضا إذا توفرت لديها أجهزة وبرامج خاصة لذلك، توجد أكثر من طريقة لمعرفة عنوان (IP) الخاص بجهاز الحاسب الآلي في حال الوصول المباشر، منها في حالة العمل على نظام تشغيل windows بكتابة winipcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP) مع ملاحظة أنه قد يتغير كلما تم الإتصال بالأنترنت مرة أخرى وفي حالة إستخدام أحد برامج المحادثة كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى لو لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعداد البريد الإلكتروني معلومات صحيحة، كما يمكن الإستعانة بعنوان MAC الذي يحدد أرقام

[1] هو مختصر لـ: internet protocol adresse

[2] هو مختصر لـ: media access control

كروت الشبكة MAC للتعرف على عنوان (IP) بشكل صحيح والذي بدوره يحدد شخصية المتصل.

ثانيا: البروكسي Proxy

يعمل البروكسي كوسيط بين الشبكة ومستخدمها، بحيث تضمن الشركات الكبرى المقدمة لخدمة الإتصال بالشبكات قدرتها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة cache memory، يتلقى مزود البروكسي عبر الأنترنت طلبا من المستخدم بحيث يبحث عن الصفحة المطلوبة ضمن ذاكرة كاش cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فإذا كانت كذلك بالفعل أعادها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يجد مزود البروكسي الصفحة المطلوبة ضمن ذاكرة cache فإنه يعمل كمزود زبون ويرسل الطلب إلى الشبكة العالمية بحيث يستخدم أحد عناوين (IP)[1]، وأهم مزايا مزود البروكسي أن cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دورها قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.

ثالثا: برامج التتبع

تقوم هذه البرامج بالتعرف على محاولات الإختراق التي تمت ومن قام بها وإشعار الجهة المتضررة بعملية الإختراق، ومن الأمثلة على تلك البرامج، برنامج hack tracer v 1,2 وهو مصمم للعمل في الأجهزة المكتبية web وساكنا في خلفية سطح المكتب وعندما يرصد أي محاولة للقرصنة أو إختراق جهاز الحاسب الآلي يسارع بإغلاق منافذ الدخول أمام المخترق ثم

[1] بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، جامعة الجزائر، كلية الحقوق، الجزائر، 2015، ص 170.

يبدأ في عملية مطاردة تستهدف إقتفاء أثر مرتكب عملية الإختراق حتى يصل إلى الجهاز الذي حدثت العملية من خلاله[1].

ويتكون البرنامج من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الإختراق التي تحدث ضد جهازه، وتحمل إسم الحدث event وتاريخ حدوثه، وعنوان (IP) الذي تمت من خلاله، وإسم الشركة المزودة لخدمة الأنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الأنترنت ومعلومات أخرى[2]، وفور حدوث أي محاولة للإختراق تظهر أمام المستخدم شاشة أخرى صغيرة مصحوبة بتحذير صوتي ويظهر على الشاشة عنوان (IP) الخاص به ويمكن للمستخدم الإختيار مابين أربعة أوامر موجودة في هذه الشاشة الفرعية منه report it والأمر الثاني هو trace it، وبمجرد الضغط على هذا الأمر تظهر شاشة أخرى وعليها إسم الدولة التي تمت منها محاولة الإختراق وعلى المستخدم أن يضغط على أمر next حتى يقوم البرنامج باستكمال عملية إقتفاء الأثر، وبعدها تظهر شاشة ثالثة عليها خريطة العالم وخط طويل ممتد من المدنية التي تمت منها محاولة الإختراق إلى المدينة التي يقيم فيها المستخدم ويوجد أسفل الخريطة مجموعة من الأوامر هي:

- الأمر الأول map وبالضغط عليها تظهر خريطة عليها خط سير محاولة الإختراق.
- والأمر الثاني هو trace وبالضغط عليه يظهر إسم الشركة المستضيفة وعنوان (IP) ورقم المنفذ port أو البوابة الخاصة بها.
- وهناك أمر network وبالضغط عليه تظهر البيانات الكاملة للشبكة التي تتبعها الشركة المستضيفة للمخترق بما فيها أرقام التليفونات والفاكسات الخاصة بها وآخر تحديث قامت به في جهاز الخدمة الخاص بها.

[1] سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العالية، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2003 ، ص100.

[2] نفس المرجع ، ص 101.

– وهناك أمر registrant ويقدم معلومات الشركة المستضيفة، ثم أمر اقتفاء الأثر وتحديث المعلومات ويظهر على شكل دائرة عليها خطان متقاطعان، ويمكن الحصول على هذا البرنامج من موقع www.zdnet.com كما يمكن تحديد جهة مرسل الرسائل عن طريق البريد الإلكتروني باستخدام برامج تتبع مصدر الرسائل.

رابعا: نظام كشف الإختراق IDS[1]

وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجرى حدوثها على أجهزة الإعلام الآلي أو الشبكة مع تحليلها بحثا عن أي إشارة قد تدل على وجود مشكلة تهدد أمن الحاسوب أو الشبكة، ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحساب الآلي أو الشبكة ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للإعتداءات على الأنظمة الحاسوبية[2].

خامسا: أدوات الضبط

تعد هذه الأدوات من الوسائل المادية التي تساعد في ضبط الجريمة، وإثبات وقوعها والمحافظة على الأدلة، ونسبتها إلى الجاني، لتقديمها إلى هيئة التحقيق من هذه الأدوات برامج الحماية، أدوات المراجعة auditing، أدوات مراقبة المستخدمين للشبكة، أدوات التنصت على الشبكة، التقارير التي تنتجها نظم أمن البيانات، مراجعة قاعدة البيانات، برامج النسخ الإحتياطي والتسجيل.

سادسا: الأدوات المساعدة بالتحقيق

يجب على المحقق إختيار ما يناسبه من الأدوات التي تساعده في التحقيق لأنه يحتمل أن الجاني قد قام بتشفير البرامج أو غير كلمات المرور أو أخفى تلك المعلومات أو غير فيها أو قام بإتلاف أدوات الحفظ الخارجية أو دمر المعلومات بأدوات الجريمة مثل الفيروسات

[1] هو مختصر لـ: intrusion détection system

[2] سوفي نور الهدى، المرجع السابق، ص17.

وغيرها ولذا يحتاج إلى أدوات مساعدة كأدوات استرجاع المعلومات من الأقراص التالفة، وبرامج كسر كلمة المرور، وبرامج الضغط وفك الضغط، برامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسب وبرامج نسخ البيانات، كما يتطلب استخدام برامج منع الكتابة على القرص الصلب بعد ارتكاب الجريمة وذلك من أجل حماية مسرح الجريمة، كما يمكن عن طريق برامج استرجاع الملفات استعادة الملفات التي قام الجاني بحذفها نهائيا من الحاسب الآلي.

سابعا: أدوات فحص ومراقبة الشبكات.

يمكن أن يستخدم المحقق عدد من الأدوات في فحص البروتوكول TCP/IP وذلك لمعرفة المشاكل المتعلقة بالشبكات والعمليات التي تعرضت لها ومن بين تلك الأدوات نذكر.

– أداة ARP التي تحدد مكان الحاسب الفيزيائي على الشبكة ومعرفة رقم كرت الشبكة عند تعيين عنوان (IP).

– برنامج Visual route 5,3 a: يلتقط هذا البرنامج أي عملية فحص عملت ضد الشبكة ويقوم هذا البرنامج برسم خط يوضح مسار الهجوم بين مصدره والجهة التي استهدفها.

– أداة tracer : يرسم مسار بين جهازين بإظهار كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتحديد الوقت ويمكن معرفة مكان الخلل والمشاكل التي تعرض لها الشبكة والإختراقات التي حصلت بها.

– أداة netstat تعمل على فحص حالة الإتصال الحالي للبروتوكول TCP/IP كعرض جميع الإتصالات الحالية ومنافذ التنصت والعناوين بصورة رقمية[1].

الفرع الثالث: الوسائل الإجرائية للتحقيق الجنائي في الجرائم الرقمية

ويقصد بهذه الوسائل تلك الإجراءات التي من خلالها يتم تنفيذ طرق و أساليب التحقيق التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها.

[1] سليمان مهجع العنزي، المرجع السابق، ص 104.

أولا: اقتفاء الأثر

في جرائم نظم المعلومات يتم التركيز على إقتفاء الأثر أكثر من التركيز على الشهود في الجريمة التقليدية، فاقتفاء الأثر هو فحص جهاز الحاسوب الخاص بالضحية أو المجرم بحثا عن دليل للإدانة سواء كان بريدا الكترونيا أو سجل لغرف المحادثة أو غيرها من الأدلة، فتقصي الأثر هو أكثر ما يخشاه المجرم المعلوماتي، فكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل نصائح أولها هي" قم بمسح آثارك COVER YOUR TRACKS "فلو لم يقم المخترق بمسح آثاره فإنه سيتم القبض عليه حتى ولو قام بالإختراق بشكل سليم.

ثانيا: الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته

يجب على المحقق أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء والإطلاع على عمليات النظام المعلوماتي، كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة موارد النظام، والمستفيدين، والملفات، والإجراءات وغيرها ويجب على المحقق معرفة نوعية برامج الحماية وأسلوب عملها والإستفادة من التقارير التي تنتجها.

ثالثا: الاستعانة بالذكاء الصناعي

أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية وتحليل القرائن واستنتاج الحقائق، كما يمكن الإستعانة بالذكاء الإصطناعي من خلال حصر الحقائق والإحتمالات والأسباب والفرضيات، ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي وفق برامج صممت خصيصا لهذا الغرض، تعتمد على نظرية الإحتمالات وذلك بإعطاء كافة الإحتمالات ثم أكثر الإحتمالات وصولا إلى الإحتمال الأقوى مع إعطاء الأسباب[1].

[1] محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، دار الحامد للنشر والتوزيع، الأردن، ط1، 2014، ص 126.

رابعا: التوقيف خلال فترة التحقيق

تعد وسيلة مهمة من وسائل التحقيق وهو ما يعرف بالحبس الإحتياطي وهو سلب حرية المتهم مدة من الزمن تحددها مقتضيات التحقيق ومصلحته وفق ضوابط حددها القانون وقد ينتهي بالإفراج أو الإدانة، إذ تحقق هذه الوسيلة عدد من الأغراض كبقاء المتهم في متناول سلطة التحقيق للمحافظة على أدلة الجريمة عن محاولة المتهم إخفائها أو طمسها، ومنع التواطؤ بالحيلولة بين إتصال المتهم بباقي شركائه في ارتكاب الجريمة، و بغل يده عن تجهيز شهود نفي مزيفين أو من تهديد شهود الإثبات[1].

خامسا: إظهار الحقائق

قد تلجأ الجهة المتضررة إلى التبليغ عن جرائم نظم المعلومات أو أن الجهات الأمنية تتحرك عند تلقيها معلومات تشير إلى وقوع جريمة أو ضبط أفراد متلبسين، أو توفر معلومات من خلال النشر على شبكة الأنترنت تشير إلى انتشار فيروسات أو وقوع عمليات اختراق، أو قرصنة، فيقوم المحقق بالإجراءات التي تتبع تلقي البلاغ من التأكد من صحة البلاغ، والتحفظ على مكان الجريمة وتأمينه، وتحديد أطراف الجريمة وكل من له صلة بها، وحصر الشهود ومنع مغادرتهم، وحصر الأدلة ورفع الآثار، ويلزم على المحقق إظهار مجموعة من الحقائق في مرحلة جمع الإستدلالات وإثباتها في محضره نظرا لأهميتها في تحديد الجريمة ورسم خطوات البحث في المجهول على النحو التالي:

1- التثبت من توافر أركان الجريمة

إن تحقق وقوع الجريمة المعلوماتية يكون بتوافر ركنين أساسيين وهما الركن المادي[2] ويقصد به الواقعة أو الضرر المادي للجريمة ويتمثل في نشاط الفاعل والنتيجة التي يحققها وعلاقة السبب بينهما، أما الركن المعنوي فيقصد به الإرادة التي اقترن بها الفعل المرتكب ويأخذ

[1] سليمان مهجع العنزي، المرجع السابق، ص 106.

[2] أنظر أكثر براهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، جامعة مولود معمري، تيزي وزو, العدد02، 2016 ، ص 131.

صورة القصد الجنائي في الجريمة المتعمدة[1] وصورة الخطأ غير المقصود بذلك على محقق جمع الاستدلالات أن يظهر أولا وجود هذه الأركان ثم الجزم بوجود أو عدم وجود الجريمة.

2- تحديد مكان الجريمة ووصفه

إن التوصل إلى الجاني له أهمية كبيرة في نجاح عملية البحث عن مكان الجريمة الذي توجد فيه الآثار والأدلة الجنائية المتصلة بها، ونتيجة لذلك يعمد كثير من الجناة إدراكا منهم لهذه الحقائق إلى نقل هدف الجريمة من مكان إتمام الجريمة وإلقائه في مكان آخر لتضليل المحقق وتعقيد عملية البحث.

3- تحديد وقت وقوع الجريمة

يتضمن تحديد وقت الجريمة تحديد تاريخ وساعة وقوعها ويتم ذلك من خلال أقوال المجني عليه أو المبلغ أو الشهود وقد يتم عن طريق الخبراء والمتخصصين وهو عنصر هام لتحديد مسؤولية المتهم في ارتكاب الجريمة عند مناقشته عن خط سيره والأماكن والأشخاص الذين كان بصحبتهم في الفترة المعاصرة لارتكاب الجريمة واكتشاف مدى صدق البلاغ وصحة شهادة الشهود كما أن الوقت في بعض الجرائم يعد ظرفا مشددا.

4- تحديد أسلوب ارتكاب الجريمة

الأسلوب هو الكيفية المتغيرة في طريقة الوصول إلى الهدف والتي سلكها الجاني في ارتكاب جريمته، وللأسلوب أهمية كبيرة في تحديد خطة البحث عن الجاني فلكل مجرم أسلوبه الإجرامي الذي لا يغيره إلا نادرا فمن الأسلوب يستطيع المحقق حصر قطاعا محددا من المجرمين يركز البحث عن الجاني بينهم ويكون التسجيل الجنائي مفيدا في تحديد أسلوب ارتكاب الجريمة ومعرفة مجرمين اعتادوا ارتكاب الجرائم المشابهة للجريمة المرتكبة.

[1] أنظر أكثر بن فردية محمد، المرجع السابق، ص 90.

5- تحديد أداة ارتكاب الجريمة

يقع على الباحث عبء التفتيش وضبط الأداة التي ارتكبت بها الجريمة فهو أمر جوهري لتحديد شخص الجاني ومن هذه الأدوات برامج التنصت على الشبكات، أقراص بدء التشغيل وغيرها.

6- إيضاح الظروف المحيطة بالجريمة

يجب على المحقق إيضاح الظروف التي تحيط بالجريمة، ومعرفتها فيكون بعضها سابقا على وقوع الجريمة مثل سوء سمعة المتهم وسلوكه والشكاوى والمشكلات السابقة التي حدثت بالمؤسسة، والبعض الآخر قد يكون معاصرا لارتكاب الجريمة مثل مكان وجود المتهم حال الجريمة وساعة ارتكاب الجريمة وكذلك هناك ظروف تكون لاحقة على ارتكاب الجريمة مثل تصرفات وسلوك من تحوم حولهم الشكوك على ارتكاب الجريمة[1].

7- تحديد دوافع الجريمة

تعد دوافع الجريمة من الأمور المهمة التي يسعى المحقق لكشفها وتتمثل في السبب والوقائع المادية التي حدثت فأثرت في نفسية الجاني مما أدى إلى بروز الدافع على ارتكابه للجريمة وهو أمر نفسي داخلي مرتبط أساسا بمجموعة من الغرائز الإنسانية وتوجه السلوك لإشباعها وتحديد الدافع في بعض الجرائم يشكل دليلا على ارتكاب الجريمة، كما أن تحديد السبب يكفل حصر دائرة البحث في عدد من الأشخاص كما يحصر للمحقق طرق الكشف عن الجريمة وعدم وضوح السبب ودوافع الجريمة يعد دليل نفي قد يشير إلى براءة من تحوم حوله الشبهات واستبعاده من قائمة الإتهام.

وفي جرائم نظم المعلومات غالبا ما يصبح من الصعب جدا معرفة سبب الحادث وذلك لأن دوافع الجناة غير واضحة، أو قد تحدث الجريمة بالخطأ، أو أن الجاني لا يحدد هدفا للجريمة وهذا راجع لأسلوب ارتكاب الجريمة حيث كمجرم نظم المعلومات الذي يبحث في المنافذ المفتوحة فقط في أي جهاز حاسب آلي.

[1] سليمان مهجع العنزي، المرجع السابق، ص 109.

وهناك عدة عوامل تساعد المحقق في تحديد سبب الجريمة نذكر منها.

– نوع الجريمة: غالبا ما يحدد سبب ارتكابها فجريمة سرقة الأقراص يكون سببها الحصول على المعلومات، وجريمة تدمير المعلومات سببها الانتقام.

– المعاينة تشكل عاملا هاما لكشف سبب الجريمة فمعاينة مسرح الجريمة يسفر عن اكتشاف الجريمة، فمثلا وجود بعض البرامج المزروعة كالفيروسات تشير في حد ذاتها إلى أن الدوافع من وراء هذه الجريمة هو الإنتقام أو العدوانية.

– أهل الخبرة: أحد أعوان الباحث الذين يرشدونه كثيرا عن الأسباب المحتملة لوقوع الحادث ومثال ذلك تقصي آثار الجاني وأساليبه والأدوات التي استخدمها قد يحدد سبب الجريمة[1].

سادسا: إتباع القواعد الفنية لكشف الجريمة

يقوم المحقق في سبيل الكشف عن الجريمة بالإجراءات اللازمة المتمثلة في المعاينة والتفتيش وانتداب الخبراء وسماع الشهود واستجواب أطراف الجريمة وجمع التحريات ويجب على المحقق أمام الأدلة الضخمة التي أمامه أن يقوم بـ:

– مراعاة الإحتمالات الشائعة في الجرائم: كاحتمال عدم وجود جريمة أصلا أو احتمال كذب البلاغ أو تصويره على غير حقيقته أو أن الجريمة وقعت فجأة ونتيجة لظروف عارضة.

– تقدير احتمالات وقوع الجريمة: ويقصد بها الخطوات التي يتصور المحقق أن الجريمة قد سارت فيها منذ مرحلة نشوء أسبابها والتفكير فيها والتحضير لها ثم تنفيذها معتمدا في تلك على الأدلة والوقائع التي جمعها كما يترتب عليه استبعاد عدد من الوقائع.

– فحص الإحتمالات: بعد حصر المحقق الإحتمالات التي يمكن أن تقع على أساسها الجريمة، وذلك في ضوء مدلولات الأدلة والحقائق التي استنتجها منها وما استبعده من احتمالات وما استخلص من تصورات لكيفية ارتكاب الجريمة يقوم بعدها بفحص كل احتمال

[1] محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، المرجع السابق، ص 124.

من هذه الإحتمالات متبعا في ذلك القواعد الفنية رسم خطة البحث والبدء بالاحتمال الأقوى، وعدم التشبث باحتمال واحد، وعدم التعجل للوصول إلى نتيجة إيجابية من فحص الاحتمال[1].

المبحث الثاني: المحقق في الجرائم الرقمية

يلعب المحقق دور أساسي و مهم في عملية البحث و التحري عن الجرائم الالكترونية التي تمتاز بالصعوبة و الدقة، فهو بذلك يختلف عن المحقق في الجرائم العادية لما يمتاز به من صفات، فلابد أن يكون ملما بجملة من المعارف و المعلومات عن أجهزة الحاسوب والتقنيات التي تقوم عليها و ذلك حتى يتمكن من متابعة و مواكبة مجريات التحريات و منه كشف الحقيقة، وعليه سوف نتعرف في هذا المبحث على دور المحقق في الجريمة الرقمية من خلال مطلبين، يتضمن(المطلب الأول) القائم بالتحقيق في الجرائم الرقمية و (المطلب الثاني) صلاحيات المحقق في الجرائم الرقمية.

المطلب الأول: القائم بالتحقيق في الجرائم الرقمية

إن الغاية التي يصبو إليها المحقق هي الكشف عن الجريمة و ملابساتها، غير أن تحقيق هذا الهدف يستدعي تكاثف الجهود فخصه المشرع بمساعدين يعملون إلى جانبه، وعليه سنتطرق في هذا المطلب إلى معرفة القائم بالتحقيق في الجريمة الرقمية من خلال التعريف بالمحقق في (الفرع الأول) و مساعدو المحقق في (الفرع الثاني).

الفرع الأول: مفهوم المحقق في الجرائم الرقمية

ونتطرق فيه بالتفصيل إلى تعريف المحقق الرقمي و خصائصه الفنية و كذلك إلى تأهيل وتدريب المحقق.

أولا: تعريف المحقق في الجرائم الرقمية

لقد أورد الفقهاء العديد من التعاريف للمحقق الجنائي و نذكر منها ما يلي:

[1] سليمان مهجع العنزي، المرجع السابق، ص 111.

أنه ذلك الشخص المخول له قانونا الإشراف على عملية التحقيق في الجريمة المعلوماتية واتخاذ كافة الإجراءات النظامية فيما يصل إلى علمه من الجرائم، بهدف الكشف عن غموضها واستظهار الأدلة منها و التوصل إلى فاعليها و تقديمهم للعدالة لمحاكمتهم[1].

و يقال أيضا "هو المكلف بالبحث عن الحقيقة في الجرائم الالكترونية و الكشف عن مرتكبيها وتجميع أدلة الإدانة أو البراءة ضدهم لإحالتهم على القضاء"[2].

ويقال أيضا أنه "الشخص الذي عهد إليه القانون باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل علمه من جرائم بهدف الكشف عن غموضها و ضبط فاعلها وتقديمه للمحاكمة"[3].

وعليه يمكن تعريف المحقق "هو شخص لديه خبرة و معرفة بوسائل و أساليب التحقيق وإجراءاته مع إلمامه بطبيعة الجرائم الحاسبة الالكترونية و الانترنت و كيفية التعامل مع الأدلة الرقمية فيتولى التفتيش عن الأدلة و أخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة"[4].

ثانيا: خصائص المحقق الجنائي الرقمي

إن من أهم الضمانات لنجاح التحقيق أن يتولاه شخص يتميز بالعديد من الصفات من بينها الحيادية و النزاهة، الصبر، الذكاء، الفطنة، حفظ أسرار التحقيق و سرعة التصرف في إجراءات التحقيق و سرعة إحضار الشهود و مناقشتهم وغيرها من الصفات العامة التي وجب توافرها في كل محقق، إلا أن المحقق في الجرائم الالكترونية يختلف عن غيره في الجرائم التقليدية من حيث بعض الخصائص و طريقة التكوين التي يعتمد فيها على البناء الفكري والتكنولوجي الذي يساعد في البحث و التحري في مثل هذه الجرائم وعليه سوف نتطرق إلى الخصائص الفنية للمحقق في الجريمة الالكترونية و كذلك إلى تأهيل و تدريب المحقق.

---

[1] عبد الله بن حسين أل حجراف القحطاني، المرجع السابق، ص21.

[2] مصطفى محمد موسى، المرجع السابق، ص 253.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص 87.

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

1- الخصائص الفنية للمحقق في الجرائم الرقمية

عند مباشرة التحقيق في الجرائم الالكترونية وجب توافر خصائص فنية معينة لدى المحقق وهذا كي يتمكن من إجراء عمله على أكمل وجه ونذكر منها:

- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنت والتي تتعلق بالجريمة المرتكبة، لأن افتقار ضباط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يؤدي إلى تدمير وضياع الدليل، على اعتبار أن جهله بأساليب ارتكاب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شانها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص المضغوطة و الأوعية المعلوماتية التي تخزن بها البيانات، وبالتالي فان الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية تامة بأساسيات التعامل مع هذه الجرائم[1].

- معرفة آلية عمل تشكيلات الحاسوب والانترنت، و ذلك من أجل القدرة على تصور مكان مسرح العمليات و كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي ومنه التمكن من معرفة مكان الاعتداء على الشبكة.

- أن تكون لديه معرفة بلغات البرمجة و أنظمة التشغيل الجديدة[2]، بحيث يلم بجميع الأنظمة التشغيلية لأجهزة الحاسوب وما تتسم به من خصائص و مميزات كل نظام على حدى، لأنه ملزم بالتعامل معها لكي يتمكن من كشف حقيقة الجريمة.

- الدراية التامة بالأساليب المستعملة في ارتكاب الجريمة المعلوماتية وتقنيات الأمن المعلوماتي لأنها تمكنه من فهم واستيعاب التقارير الجنائية التي يعدها خبير الحاسوب بحيث تعد من الوثائق المهمة في محضر التحقيق.

- إتباع الإجراءات الصحيحة و المشروعة من أجل المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة، و تخزينها في الأقراص المعدة لذلك، ومنع حذفها و الحرص على عدم

[1] السوفي نور الهدى، المرجع السابق، ص 22.

[2] مصطفى محمد موسى، المرجع السابق، ص 265.

تعريض وسائط التخزين كالأقراص المرنة و المدمجة لأيه مؤثرات خارجية كالقوة الكهربائية والمغناطيسية حتى لا تتلف محتوياتها.

- معرفة الجرائم المتعلقة بالأنترنت والخصائص التي تميزها، بحيث الوعي الجيد بهذه الخصائص يعتبر بمثابة حجر الأساس في مواجهة هذه الجرائم و الكشف عنها، وكما وجب على المحقق الإطلاع على بعض الجوانب النظرية أيضا، خاصة التشريعات والقوانين المختصة بهذه الجرائم و كذلك الاتفاقيات و المعاهدات الدولية التي تنظمها، كلها تساعد المحقق في الكشف عن الحقائق[1].

- مهارات العرض والتوثيق بحيث وجب على المحقق الالكتروني أن يكتب تقاريره بشكل واضح ومباشر ويسهل فهمه، أي يجيد استخدام الألفاظ و المصطلحات و الكلمات و مختصراتها والمقصود منها تحديدا[2] حول كل الحقائق التي توصل إليها من بداية التحقيق إلى نهايته، دون إحداث أي تغيير أو تأويل و يقدمها للجهة القضائية المختصة للفصل في الموضوع، و مثال ذلك في حالة المواقع المدمرة وجب على المحقق توثيق وتسجيل بيانات كل من زار هذه المواقع من الاسم والساعة وسبب الزيارة وغيره من المعلومات من أجل المحافظة على مسرح الجريمة.

2- تأهيل و تدريب المحقق الرقمي

بما أن الجريمة الإلكترونية تعتبر من الجرائم المعقدة و ذات تقنيات دقيقة و ذكية، فإنه لابد من الإرتقاء بالمحققين من خلال تطوير قدراتهم العلمية و كذلك وسائل البحث، فليس بالضرورة أن يكون المحقق في الجريمة الإلكترونية خبيرا في الحاسوب بل يكفي أن يكون ملما بالمسائل الأولية لكي يتمكن من التفاهم مع الخبراء في هذا المجال و كذلك من أجل تأمين الأدلة بصورة علمية سليمة.

وعليه فإنه من باب أولى للجهات الحكومية إعداد كوادرها للضبط في الجرائم الالكترونية وإطلاعهم على التقنيات العلمية الحديثة في هذا المجال و ذلك عن طريق منهجية يعتمد فيها

[1] حسن بن سعيد الغافري، المرجع السابق، ص 3 و4.

[2] مصطفى محمد موسى، المرجع السابق، ص 270.

على تدريب متخصص و منتظم تتمثل عناصره الأساسية في الشخص المتدرب و منهج الدورة التدريبية وصفة و أسلوب التدريب[1].

وهناك من يرى أن توكل مهمة التحقيق في الجرائم الالكترونية إلي بيوت الخبرة المتخصصة في هذا المجال و لكن هذا الأمر يشكل خطورة من حيث تخلي أجهزة العدالة الجنائية الحكومية عن دورها، حيث تضع حقوق المجتمع تحت رحمة أفراد أو شركات همها الوحيد تحقيق الربح المادي على حساب العدالة، و كذلك الإخلال بمبدأ سرية التحقيق خاصة لو تعلق الأمر بجرائم تمس أمن الدولة[2].

وكما يمكن للجهات المختصة في التحقيق استقطاب الكفاءات المهنية المتخصصة في هذا المجال للاستعانة بهم في التحقيق في الجرائم الالكترونية، بحيث يمكن طلب المساعدة من الموظفين في قطاع المواصلات السلكية واللاسلكية و ذلك عن طريق تسخير عون مؤهل في هيئة عمومية أو خاصة للتكفل ببعض الجوانب التقنية لعملية اعتراض المراسلات التي تتم بواسطة الاتصالات السلكية واللاسلكية وكذلك في حالة التقاط صور وجب وضع ترتيبات تقنية خاصة[3].

وتجدر الإشارة هنا إلى أن المادة 04 الفقرة 10 من المرسوم الرئاسي 15-261 المؤرخ في: 2015/10/08 يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، قد حثت على ضرورة تكوين محققين متخصصين في المجال التقني بتكنولوجيات الإعلام و الاتصال بقولها «المساهمة في تكوين المحققين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام و الاتصال».

[1] هشام محمد فريد رستم، المرجع السابق، ص 495.

[2] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون و الكومبيوتر و الانترنت، المجلد الثالث، كلية الشريعة و القانون جامعة الإمارات العربية المتحدة، الفترة من01 إلى03 ماي 2000، ص 1072 و1073.

[3] السوفي نور الهدى، المرجع السابق، ص 24.

الفرع الثاني: مساعدو المحقق في الجرائم الرقمية

يحتاج المحقق الجنائي إلى عدد من الأعوان يختلفون بحسب طبيعة الجريمة و من أهم الأعوان نذكر ما يلي:

أولا- رجال الضبطية القضائية: إن مباشرة المحقق للتحقيق في القضايا الجنائية يعتبر أمر في غاية الأهمية، فنجد مختلف الأطراف تعمل لجانبه وتقوم بوظائف مكملة لبعضها البعض، فيباشر رجال الضبط القضائي تحرياتهم ثم يقدمون استدلالاتهم و كل ما توصلوا إليه حول الوقائع الجنائية والتي تعتبر ضرورية لأنها تساعد المحقق وترشده إلى الاتجاه الصحيح المؤدي إلى كشف الحقيقة، وعليه فإنهم من الركائز القوية لنجاح عمل المحقق فيكون مطمئنا لما يقومون به في مرحلة الاستدلالات و هي مرحلة تمهيدية للتحقيق.

ثانيا- مقدمو الخدمات[1]: تنص المادة 10 من القانون 04/09 المؤرخ في: 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها على ما يلي: «في إطار تطبيق أحكام هذا 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.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق»

[1] عرفهم القانون 04/09 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، ج ر عدد 47، الصادرة بتاريخ 2009/08/16 في المادة2 الفقرة-د- أنهم "1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام للاتصالات 2- و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".- المنظومة المعلوماتية هي: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

وعليه يلعب مقدمو الخدمات بما لديهم من تقنيات متماشية مع تطور التكنولوجيات الحديثة للإعلام و الاتصال دور مهم في مكافحة الجرائم المعلوماتية، وذلك بتقديم المساعدة التقنية للسلطات المكلفة بالبحث و التحري عن هذه الجرائم المرتكبة بواسطة أو ضد هذه التكنولوجيات الحديثة، كما أوجب عليهم المشرع حفظ المعطيات المعلوماتية الأمر الذي يسمح للمتحري بتتبع الجريمة و حركة المجرمين، وخصهم أيضا بالتزامات خاصة تتمثل في التدخل الفوري من أجل سحب المحتويات التي يتاح لهم الإطلاع عليها بمجرد علمهم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون أو كانت مخلة للآداب العامة و النظام العام أو جعل الدخول إليها غير ممكن أو محظور، وكذا وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام و الآداب العامة و إخبار المشتركين لديهم بوجودها.

ومنه يتضح أن التزامات مقدمي الخدمات تتمثل في ثلاث نقاط أساسية و هي مساعدة السلطات و حفظ المعطيات المتعلقة بحركة السير و أخيرا التزامات خاصة بمقدمي خدمة الانترنت[1].

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، إضافة إلى حفظ محتوى هذه الاتصالات لمدة سنة كاملة.

ثالثا- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

أنشأت بموجب القانون 04/09 السالف الذكر بحيث تنص المادة 13 على ما يلي «تنشأ هيأة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها»،

[1] أنظر المواد 11 و 12 من القانون 04/09.

وهي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الإستقلال المالي توضع لدى الوزير المكلف بالعدل و يحدد مقرها بمدينة الجزائر العاصمة[1].

وتتولى الهيئة عدة مهام في مجال مكافحة الجريمة الالكترونية وما يهمنا في هذه الدراسة هو دورها في عملية البحث و التحري عن الجرائم المعلوماتية، إذ تعمل على مساعدة السلطات القضائية و مصالح الشرطة في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال وخاصة التي تمس بأنظمة المعالجة الآلية للمعطيات وتزويدهم بكل المعلومات والخبرات اللازمة، و وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وتجميع و تسجيل محتواها و تسليمها إلى الشرطة القضائية[2].

كما أن للهيئة دور مهم في إطار التحريات أو التحقيقات القضائية الدولية حيث يمكن لها في حالة الاستعجال و مع مراعاة الإتفاقيات الدولية و مبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية لمكافحة هذه الجريمة طبقا لنص المادة 16 من القانون 09-04.

رابعا_ الخبراء: هم أصحاب الخبرة الفنية المتميزة في الجوانب العلمية، وأهمهم الفئة التي تختص في معالجة و تحليل أدلة الجرائم المعلوماتية، بحيث لا يمكن الكشف عن غموض الجريمة و الوصول إلى الحقيقة إذا لم يكن هناك تعاون فعلي معهم و استطلاع رأي أهل الخبرة، وعليه و جب على المحقق خلق جو من التفاهم بينه و بين الخبراء ليستمر نجاح مجريات التحقيق.

خامسا- القضاة و المحامون: إن القضاة بحكم عملهم يمكنهم توجيه المحقق في الأمور الشرعية التي يكون لها تأثير في صحة و بطلان الإجراءات القانونية المتخذة لذلك فإن المحقق وجب عليه أن يسعى إلى خلق جو التفاهم و التعاون بينه وبين هذه الفئة لخدمة الصالح العام و كذلك الأمر بالنسبة للمحامين الذين يدافعون عن المتهمين، وعليه يجب على المحقق أن

[1] أنظر المادة 02 من المرسوم الرئاسي 15-261 المؤرخ في 2015/10/08 يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، ج ر عدد53، بتاريخ 2015/10/08،ص 16

[2] أنظر المادة 04 من المرسوم الرئاسي 15-261.

يستوعب الدور الأساسي الذي يؤديه المحامي و مدى أهمية التعاون معه لما ينتج عنه من حماية لحقوق وحريات الأفراد و تحقيق العدالة و النزاهة بين أفراد المجتمع[1].

المطلب الثاني: صلاحيات المحقق في الجرائم الرقمية

المعمول به في التشريع الجزائري هو أن التحقيق يمر بمرحلتين، مرحلة التحقيق الأولي و هي مرحلة جمع الإستدلالات يباشرها أعضاء الضبطية القضائية والمرحلة الثانية هي مرحلة التحقيق القضائي وهي من اختصاص قاضي التحقيق، وقد حدد المشرع صلاحيات كل منهما، وهذا ما سوف نعالجه من خلال (الفرع الأول) يتضمن صلاحيات قاضي التحقيق و (الفرع الثاني) نتطرق فيه إلى صلاحيات الضبطية القضائية.

الفرع الأول: صلاحيات قاضي التحقيق

ويقصد بها الحدود التي بينها المشرع الجزائري لقاضي التحقيق ليباشر فيها ولاية التحقيق في الدعوى المعروضة عليه، و يتحدد اختصاصه النوعي من خلال نوع الجريمة والمحلي من خلال مكان وقوع الجريمة أو محل القبض على المشتبه فيه أو مكان إقامته، ولقد أورد المشرع بعض التعديلات فيما يخص الجرائم الخطيرة، وهذا ما سوف نعالجه من خلال النقاط التالية:

أولا: الإختصاص المحلي

بالرجوع إلى نص المادة 40 ق.إ.ج نجد أن المشرع قد وسع من الإختصاص المحلي لقاضي التحقيق التابع للمحكمة ذات الاختصاص الواسع إذا تعلق الأمر بالجرائم الخطير والمذكورة في الفقرة الثانية على النحو التالي «يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة إختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف»، وهو ما نصت عليه كذلك المواد 329 و37 من نفس القانون، بحيث يصبح لقاضي التحقيق التابع لهذه المحكمة اختصاص إقليمي

[1] عبد الله بن حسين ال حجراف القحطاني، المرجع السابق، ص 25.

يتجاوز اختصاصه العادي و يمكنه التنقل أو انتداب أي ضابط شرطة قضائية للقيام بمهام تتعلق بالتحقيق في الجرائم الخطيرة السابقة الذكر[1].

وبموجب المرسوم التنفيذي رقم:348/06 المؤرخ في:2006/10/05 المعدل والمتمم بالمرسوم رقم: 267/16 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق، تم تمديد الإختصاص المحلي لقضاة التحقيق إلى دوائر اختصاص محاكم أخرى كما حددته المواد من 2 إلى 5 منه إذا تعلق الأمر بالجرائم الخطيرة السابقة الذكر[2].

وعليه فإن امتداد اختصاص قاضي التحقيق، يجعل المحكمة التابع لها قاضي التحقيق المعني بهذا التمديد مختصة بالنظر في الجريمة محل المتابعة، وعلى هذا الأخير إخطار وكيل الجمهورية بمحكمته قبل الإنتقال إلى الدوائر الأخرى.

ويتصل قاضي التحقيق بالدعوى الخاصة بالجريمة الالكترونية إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي لطلب افتتاحي لإجراء التحقيق، و إما عن طريق شكوى من المتضرر، وهذا ما أوضحته المادة 38 ق.إ.ج في فقرتها الثالثة والتي جاء فيها «يختص بالتحقيق في الحادث بناء على طلب من و كيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و73»[3].

ثانيا: الإختصاص النوعي

القاعدة العامة أن قاضي التحقيق مختص بالتحقيق في الجرائم الموصوفة جناية إلزاميا، أما الجنح و المخالفات فهو اختياري يخضع لتقدير النيابة، أي يحقق في كل الجرائم التي قدمت النيابة العامة بشأنها طلبا إفتتاحيا، و هناك أيضا سلطات خاصة لقاضي التحقيق أجازها له المشرع بموجب القانون رقم: 22/06 المؤرخ في: 2006/12/20 المعدل و المتمم لقانون

[1] حمزة قريشي" الوسائل الحديثة للبحث و التحري في ضوء القانون الجزائري"، منشورات السائحي، الجزائر، ط1، 2017، ص 27.

[2] زيبحة زيدان، المرجع السابق، ص 115.

[3] أحسن بوسقيعة، "التحقيق القضائي"، دار هومة للطباعة و النشر، الجزائر، ط10، 2013، ص29.

الإجراءات الجزائية إذا اقتضت ضرورات التحقيق ذلك في جرائم معينة يمكن اللجوء إلى أساليب تحري خاصة، و تتمثل في الآليات و الوسائل الجديدة في التحري عن الجرائم الخطيرة وهي: التسرب والمراقبة الالكترونية واعتراض المراسلات وتسجيل الأصوات والتقاط الصور وسوف نتطرق لهم بالتفصيل في الفصل الثاني.

الفرع الثاني: صلاحيات الضبطية القضائية

من خلال نص المادة 12 ق.إ.ج[1] يتضح أن البحث والتحري عن الجرائم بالنسبة للضبطية القضائية ينحصر في جمع الأدلة والبحث و التحري عن مرتكبي الجرائم في دائرة اختصاصهم، و لكن يجوز امتداده إلى كافة التراب الوطني إذا تعلق الأمر بالبحث و التحري عن الجرائم الخطيرة و نخص بالذكر الجريمة الالكترونية محل الدراسة، وعليه سوف نتطرق في هذا الفرع إلى تمديد الاختصاص الإقليمي للضبطية القضائية و تعزيز صلاحياتهم على ضوء القانون 22/06 المؤرخ في: 2006/12/20 المعدل و المتمم لقانون الإجراءات الجزائية.

أولا: تمديد الإختصاص الإقليمي للضبطية القضائية

تنص المادة 7/16 ق.إ.ج على «غير أنه فيما يتعلق ببحث و معاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني»، بحيث أجاز المشرع تمديد الإختصاص الإقليمي للضبطية القضائية عبر كامل التراب الوطني إذا تعلق الأمر بهذه الجرائم، وعلى ضباط الشرطة القضائية بعد تلقي الشكاوى و البلاغات بخصوص هذه الجرائم، أن يبادروا دون تمهل بإخطار وكيل الجمهورية وأن يوافوه بأصول المحاضر وما يتبعها من مستندات ووثائق وهي المحاضر التي حدد القانون مهلة إرسالها إلى النيابة بخمسة أيام الموالية لتاريخ معاينة

[1] المادة 12/ 3" و يناط بالضبط القضائي مهمة البحث و التحري عن الجرائم المقررة في قانون العقوبات و جمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها بتحقيق قضائي"

المخالفة على الأكثر إذا تمت المعاينة من طرف ذو الرتب في الشرطة البلدية و ذلك عن طريق ضباط الشرطة القضائية[1] و هذا ما أكدته المادة 26 ق.إ.ج [2].

ويعتبر صحيحا كل ما يصدر عن الضبطية القضائية أثناء البحث والتحري أو جمع الاستدلالات للكشف عن الجرائم و مرتكبيها ووضع المشتبه فيهم تحت النظر خاصة في الجرائم المتلبس بها، و تمارس هذه المهام تحت إدارة وكيل الجمهورية و إشراف النائب العام ورقابة غرفة الاتهام المختصة ماعدا ضباط الشرطة التابعين للأمن العسكري فيؤول الاختصاص بشأنهم إلى غرفة الإتهام بالجزائر العاصمة وفقا للمادة 2/207 ق.إ.ج والتي تنص على «غير أن غرفة الإتهام بالعاصمة تعتبر صاحبة الاختصاص فيما يتعلق بضباط الشرطة القضائية للأمن العسكري، و تحال القضية على غرفة الاتهام من طرف النائب العام بعد استطلاع رأي وكيل الجمهورية العسكري الموجود بالمحكمة العسكرية المختصة إقليميا»[3].

ثانيا: تعزيز صلاحيات الضبطية القضائية

و نستطيع تلخيصها في النقاط التالية:

1- منح صلاحيات التحري لأعوان الضبطية القضائية: منح المشرع صلاحيات القيام بالتحريات الإبتدائية لأعوان الضبطية القضائية ولكن اشترط أن تكون تحت رقابة ضابط شرطة قضائية وهذا ما أكدته المادة 63 ق.إ.ج « يقوم ضباط الشرطة القضائية وتحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الإبتدائية بمجرد علمهم بوقوع الجريمة إما بناء على تعليمات وكيل الجمهورية وإما من تلقاء أنفسهم».

2- تمديد مدة التوقيف للنظر: لقد أصبح التحقيق في الجرائم المذكورة في المادة 16 السالفة الذكر يعتبر صعب و معقد وذلك لاستخدام مرتكبيها أساليب جد حديثة و متطورة تمكنهم من

[1] زيبحة زيدان، المرجع السابق، ص 119.

[2] المادة 26 "يرسل ذو الرتب في الشرطة البلدية محاضرهم إلى وكلاء الجمهورية عن طريق ضباط الشرطة القضائية الأقرب . و يجب أن يرسل هذه المحاضر خلال خمسة أيام الموالية لتاريخ معاينة المخالفة على الأكثر".

[3] علي شملال، الجديد في شرح قانون الإجراءات الجزائية، الكتاب الأول، الإستدلال و الإتهام، دار هومه للطباعة والنشر، الجزائر،ط3 ، 2017، ص 30.

الإفلات من العقاب، من أجل ذلك تدخل المشرع بنص المادة 51 ق.إ.ج و مدد فترة التوقيف للنظر في الجرائم المعلوماتية بقوله في الفقرة الخامسة « يمكن تمديد آجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص:

مرة واحدة (1) عندما يتعلق الأمر بجرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات »

الفصل الثاني

آليات التحقيق الجنائي في الجرائم الرقمية

يرى الباحث أن جرائم الحاسب الآلي التي تستهدف الإعتداء على المعطيات بدلالتها التقنية الواسعة قد أمست من أخطر الجرائم التي تقترف في مجتمعات العصر، ومرد ذلك أن هذه الجرائم لا تخلف آثارا ظاهرة خارجية فهي تنصب على البيانات والمعلومات المختزنة في نظم المعلومات والبرامج الأمر الذي ينفي وجود أي أثر مادي يمكن الإستعانة به في إثباتها، ومما يزيد من هذه الصعوبة هو ارتكابها في الخفاء حيث يتم نقل المعلومات بواسطة النبضات الإلكترونية التي تتم عن بعد فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، لهذا السبب تزايدت خطط مكافحة هذه الجرائم وانصبت الجهود على دراستها المتعمقة وخلق آليات قانونية للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية إدراكا منها لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية وآليات الكشف والضبط والتحري عنها فكان لزاما على العديد من الدول وضع قوانين وتشريعات خاصة أو تعديل قوانينها العامة من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم، إذ تهدف إجراءات التحقيق فيها إلى جمع وفحص الأدلة الإلكترونية القائمة على وقوع الجريمة ونسبتها إلى فاعلها، والمشرع الجزائري كغيره من التشريعات الأخرى ودعما منه للإجراءات العامة المتمثلة في التفتيش والمعاينة والضبط قام باستحداث آليات تحري خاصة تمثلت في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والمراقبة الإلكترونية والتسرب في سبيل البحث والتحري عن الجرائم المستحدثة والتي تشمل من بينها الجريمة المعلوماتية، وقد ورد ذلك في نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية.

من خلال هذا سوف نتطرق في هذه الدراسة إلى الآليات التي تقوم بها جهات التحقيق في مكافحة الجرائم المعلوماتية فنتعرض أولا إلى الآليات الإجرائية العامة للتحقيق الجنائي في الجرائم الرقمية في **(المبحث الأول)** ثم نعرج إلى الآليات الإجرائية الخاصة للتحقيق الجنائي في الجرائم الرقمية في **(المبحث الثاني)**.

المبحث الأول: الآليات الإجرائية العامة للتحقيق الجنائي في الجرائم الرقمية

إن الهدف من إجراءات التحقيق هو التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه ففي الجرائم التقليدية لا ينحصر التحقيق في مكتب قاضي التحقيق أو ما تنقله محاضر الضبطية القضائية بل تستلزم بعض الجرائم الإنتقال لإجراء معاينات مادية أو القيام بعمليات التفتيش أو الحجز التي يراها مفيدة لإظهار الحقيقة وهي ذاتها الإجراءات التي يلجأ إليها المحقق في الجريمة الرقمية غير أن أدلتها تكون من البيئة الرقمية التي تعد مسرح الجريمة.

من هنا سوف نتطرق في هذا المبحث إلى معرفة طبيعة هذه الإجراءات في عالم الجريمة الرقمية وذلك من خلال المطالب التالية؛ نتطرق في (المطلب الأول) إلى المعاينة وفي (المطلب الثاني) إلى التفتيش والضبط وفي (المطلب الثالث) إلى الخبرة.

المطلب الأول: المعاينة في الجرائم الرقمية

تعتبر المعاينة من أهم إجراءات التحقيق لما لها من أهمية قصوى في إثبات الواقعة الإجرامية فهي تعبر عن الوقائع والحقيقة تعبيرا صادقا لا تكذب ولا تحابي ولا تخدع فتعطي المحقق صورة صحيحة واقعية للحادثة الإجرامية خصوصا في الجرائم التقليدية إذ تمكن المحقق من تصور كيفية وقوع الجريمة وظروف وملابسات ارتكابها وتوفير الأدلة المادية التي يمكن تجميعها عن طريق المعاينة لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها[1] **ويرجع سبب ذلك إلى:**

– أن هناك تقريبا مسرحا للجريمة التقليدية حيث يتمكن المحقق من التنقيب عن الواقعة عن طريق معاينة الآثار المادية التي خلفها ارتكاب الجريمة بينما لا توجد عادة مسرح للجريمة

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر و الأنترنت، دار الكتب القانونية، مصر، بدون طبعة، 2004، ص 60.

المعلوماتية باعتبار مكان الإغارة هو العالم الإفتراضي أو الفضاء الإلكتروني[1] فالإنتقال للمعاينة في الجريمة المعلوماتية لا يكون إلى العالم المادي بل إلى العالم الإفتراضي.

– أن الجريمة المعلوماتية قلما تخلف آثارا مادية ظاهرة خارجية فهي تنصب على البيانات والمعلومات المخزنة في نظم المعلومات والبرامج مما ينفي وجود أثر مادي[2].

– أن الجاني باستطاعته التردد على مسرح الجريمة من وقت ارتكابها حتى اكتشافها لأنه قد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها الأمر الذي يعطيه الفرصة أن يعبث بالآثار المادية إن وجدت فيورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة[3].

غير أنه قد تكون الجريمة المعلوماتية جريمة مستمرة فيكون بذلك مسرحها كالجرائم الأخرى ففي هذه الحالة يكون الهدف من المعاينة هو المداهمة و ضبط الأدلة الطبيعية فتقع المعاينة على مجموعة من البرمجيات أو الأقراص وكل ما يتعلق بجهاز الحاسب الآلي.

وحتى يتجلى هذا اللبس في دور المعاينة في الكشف عن الجرائم الرقمية ارتأينا التطرق إلى تعريف المعاينة في (الفرع الأول) وإلى محل المعاينة في (الفرع الثاني) وأخيرا إلى إجراءات معاينة مسرح الجريمة الرقمية في (الفرع الثالث).

الفرع الأول: تعريف المعاينة في الجرائم الرقمية

المعاينة في اللغة تعني النظر للشئ ومشاهدته، وفي الإصطلاح الجنائي هي رؤية محل ارتكاب الوقائع الجنائية وإثبات حالتها بالشكل الذي تركها به الجاني عقب ارتكاب الجريمة.

كما تنصرف إلى فحص جسم المجني عليه والمتهم وإثبات ما يوجد بهما من آثار[4].

[1] معمش زهية وغانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في الحقوق، جامعة عبد الرحمان مريم بجاية، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، الجزائر، 2013، ص 8.

[2] محمد فريد رستم، المرجع السابق، ص 484.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص 153.

[4] نفس المرجع، ص 147.

أو هي مشاهدة مسرح الجريمة وإثبات الحالة فيها أي مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة للمساعدة على اكتشاف الحقيقة[1].

وهناك من عرفها أنها "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة"[2].

من خلال ما سبق يمكن الإجماع على أن المعاينة هي "الكشف الحسي المباشر والمادي لإثبات حالة الشيء أو المكان أو الشخص وكل ما يفيد في كشف الحقيقة"[3] باستعمال الحواس ويجوز اللجوء إلى المعاينة في كافة الجرائم ولا تتطلب في الغالب الإنتقال إلى الميدان فمن الجائز أن تتم في مكتب قاضي التحقيق[4].

ويلاحظ أن المعاينة قد تكون إجراء تحقيق أو إستدلال ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد فإذا جرت المعاينة في مكان عام كانت إجراء إستدلال وإذا اقتضت دخول مسكن أو مكان له حرمة خاصة كانت إجراء تحقيق[5].

ومعاينة مسرح الجريمة المعلوماتية يقصد به معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الأنترنت وتشمل الرسائل المرسلة منه أو التي استقبلها وكافة الإتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية[6].

[1] غسان مدحت الخيري، المرجع السابق، ص 40.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص 149.

[3] حسن الجوخدار، المرجع السابق، ص 90.

[4] أحسن بوسقيعة، المرجع السابق، ص 82.

[5] صالح شنين، الحماية الجنائية للتجارة الإلكترونية، رسالة لنيل شهادة الدكتراه في القانون الخاص، جامعة أبو بكر بلقايد تلمسان ، كلية الحقوق، الجزائر، 2013، ص 103.

[6] خالد ممدوح إبراهيم، نفس المرجع ، ص 165.

الفرع الثاني: محل المعاينة في الجرائم الرقمية

تنصب المعاينة على الأشياء المجودة بالمكان من مكونات ثابتة أو محتويات منقولة أو آثار ومخلفات لها صلة بكشف الحقيقة بمسرح الجريمة والمحقق يجد نفسه في الجريمة المعلوماتية أمام مسرحين.

أولا: مسرح تقليدي: ويقع خارج البيئة الإلكترونية لأنه يتكون من مكونات مادية للمكان الذي ارتكبت فيه الجريمة ويشبه في ذلك مسرح الجريمة التقليدي والذي يترك فيه الجاني عدة آثار كالبصمات، أو معدات أو وسائط تخزين وغيرها.

ثانيا: مسرح سيبراني أو إفتراضي: ويقع داخل البيئة الإلكترونية لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب والشبكة وفي ذاكرة الأقراص الصلبة الموجودة بداخله[1] فالجاني يترك أيضا بصمات في المسرح الإلكتروني كما في المسرح التقليدي فالموقع الذي يزوره يفتح سجلا خاصا عن معلومات المتصفح كاسمه والمكان الذي يتصل منه وعنوان بريده الإلكتروني...، ويعتقد بعض الجناة أن استخدام أسماء مستعارة أو الإستعانة ببرامج إخفاء الهوية قد يمكنه من إخفاء معلوماته بشكل كامل غير أن الجهة الوسيطة ISP تحتفظ بسجل عن كافة تحركاته و الأعمال التي يقوم بها[2].

والتعامل مع الأدلة في هذا المسرح يتم على يد خبير متخصص في التعامل مع الأدلة الرقمية.

وعلى سلطة التحقيق الإنتقال إلى العالم الإفتراضي بالسرعة الكافية من أجل منع زوال آثار الجريمة ويتم هذا الإنتقال لمعاينة الجريمة إما من قبل قاضي التحقيق أو ضابط الشرطة القضائية كالتالي:[3]

[1] السوفي نور الهدى، المرجع السابق، ص 31.

[2] سليمان مهجع العنزي، المرجع السابق، ص 124.

[3] معمش زهية وغانم نسيمة ، المرجع السابق، ص 9.

- من مكتبه بالمحكمة من خلال جهاز الحاسوب الخاص به.
- اللجوء إلى مقهى الأنترنت.
- اللجوء إلى مكان عمل مزود بخدمة الأنترنت.

ويتولى القاضي معاينة جميع الرسائل المرسلة أو المستقبلة عن طريق الشبكة وكل الإتصالات التي قام بها وكل الآثار الرقمية المستمدة من أجهزة الكمبيوتر، فقد تكون ثرية فيما تحتويه من معلومات مثل صفحات المواقع المختلفة والبريد الإلكتروني وغيرها.

الفرع الثالث: إجراءات معاينة مسرح الجريمة الرقمية

نظرا لتميز مسرح الجريمة المعلوماتية كما قدمنا عن مسرح الجريمة التقليدية وحتى يكون للمعاينة فائدة في الكشف عن الحقيقة وعن مرتكبها في الجرائم المتعلقة بشبكة الأنترنت يتعين على المحقق مراعاة عدة إجراءات أبرزها:[1]

- يجب على المحقق الجنائي قبل الإنتقال لإجراء معاينة لمسرح الجريمة المعلوماتية إتباع الخطوات التالية:

• وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها.

• تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة سواء من حيث الضبط أو التأمين أو حفظ الأوراق والمستندات المتداولة.

• إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

• أن تتم كل هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.

• تأمين عدم انقطاع التيار الكهربائي لأن معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي.

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، دار النهظة العربية، مصر، ط1، 2009، ص 586.

• إعداد خطة الهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على أن تكون الخطة موضحة الرسومات وتتم مراجعتها مع أعضاء الفريق قبل بدء التحرك[1].

• الإحتفاظ بسرية الغارة حتى نهاية التفتيش إذ أن المعلومات التي يتم البحث عنها يمكن إتلافها بسهولة من قبل المتهمين أو المتورطين في الجريمة.

– وبعد وصول فريق التحقيق إلى مسرح الجريمة أو مكان الغارة يتم تأمين والسيطرة على المكان والبدء في التفتيش[2].

ويرى الفقه الجنائي أن هناك عدة ضوابط لبد من أخذها بعين الإعتبار أثناء معاينة مسرح الجريمة من بين هذه الضوابط نذكر:[3]

• السيطرة على المناطق المحيطة بمسرح الجريمة وذلك عن طريق إغلاق الطرق والمداخل.

• وضع حراسة كافية على مكان الجريمة ومراقبة التحركات داخل مسرح الجريمة ورصد جميع الإتصالات الهاتفية الواردة والصادرة من مسرح الجريمة وتكون الحراسة على كل جهاز حتى لا يتمكن أحد من المتهمين من إتلاف المعلومات[4].

• تحديد أجهزة الحاسب الآلي الموجودة بمكان المعاينة وتحديد مواقعها بشكل سريع في حال وجود شبكة إتصالات يجب البحث عن خادم الملف File Server من أجل تعطيل الإتصالات لمنع تخريب الأدلة الموجودة أو محوها.

• تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة وسائر ملحقاته والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب ويراعى تسجيل وقت وتاريخ ومكان إلتقاط كل صورة.

---

[1] محمد الأمين البشري. الجرائم المعلوماتية: أصول التحقيق الجنائي الفني. بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، جامعة الإمارات العربية المتحدة، المرجع السابق، ص 1055.

[2] علي عدنان الفيل ، إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة) ، دار الكتب والوثائق القومية، مصر، بدون طبعة، 2012، ص35. أنظر أيضا هشام محمد فريد رستم، المرجع السابق، ص487.

[3] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، مصر، بدون طبعة ، 2008، ص222

[4] بن فردية محمد، المرجع السابق، ص126.

• العناية البالغة بملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها ومعرفة السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الإتصال ونوع الجهاز المتصل وذلك بالدخول إلى النظام أو الموقع أو الدخول معه في حوار وبروتوكولات الإتصال عبر الأنترنت (IP).

• ينبغي أيضا ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام الأمر الذي قد يمكن من تحليل البيانات ومقارنتها والوصول عبرها إلى دليل الجريمة.

• عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات القوى المغناطيسية (أو الممرات المغناطيسية) التي قد تتسبب في محو البيانات، ويتم ذلك عن طريق خبراء الحاسب الآلي.

• التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وشرائط و أقراص ممغنطة وغير سليمة أو محطمة ورفع البصمات التي تكون عليها.

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

والجدير بالذكر أنه يجب تحرير محضر بالمعاينة عن طريق كاتب ويجب عند إجرائها إخطار الخصوم بمكان المعاينة و زمانها و يتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد مع توثيق كل دليل على حدى بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها ومن قام برفعه وتحريزه وكيف ومتى تم ذلك، بل إن البعض يرى أن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي تربط بها الأجهزة محل

[1] حسين بن سعيد الغافري، المرجع السابق، ص 10. أنظر أيضا علي عدنان الفيل ، المرجع السابق، ص 34.

التحقيق ولعل أبرز الأماكن التي تحوي الأدلة الجنائية في جرائم الأنترنت الورق، جهاز الحاسب الآلي وملحقاته، البرمجيات، وسائط التخزين المتحركة، المراشد، المودم[1].

كما تجدر الإشارة إلى أن المشرع الجزائري أجاز المعاينة في الجرائم المعلوماتية المتلبس فيها بنص المادة 3/47 ق.إ.ج والتي تنص على أنه عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإنه يجوز إجراء المعاينة في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص[2].

يستهدف التحري الأولي الحصول على أكبر قدر ممكن من المعلومات عن السلوك المكون للجريمة المعلوماتية و أسلوب وظروف ارتكابها في غضون وقت قصير نسبيا وجمع هذه المعلومات يمكن أن يتم بصفة مبدئية عن طريق مقابلات إستطلاعية تجرى مع ممثلي الجهة المجني عليها.

المطلب الثاني: التفتيش والضبط في الجرائم الرقمية

تهدف وسائل الإثبات الجنائي جميعا إلى الحصول على دليل لكشف الحقيقة، لكن التفتيش يتميز عن بعضها بأن ما يهدف إليه هو الوصول إلى ضبط دليل مادي للجريمة المعلوماتية فشهادة الشهود والإستجواب والإعتراف قد توصل إلى أدلة تبين الحقيقة ولكنها أدلة قولية لذلك ارتأينا من خلال ذلك تقسيم هذا المطلب إلى فرعين يتضمن (الفرع الأول) التفتيش و(الفرع الثاني) الضبط.

الفرع الأول: التفتيش في الجرائم الرقمية

هنا ينبغي التفرقة بين تفتيش الحاسب الآلي نفسه ككيان منطقي يمكن أن يقود إلى الدليل الجنائي في الجريمة التي وقعت، وبين تفتيش الشخص القائم على نظام الحاسب الآلي أو

[1] صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، الجزائر، 2013، ص 86.

[2] صالح شنين، المرجع السابق، ص 233

المكان الذي يوجد فيه الحاسب الآلي، فهذا الأخير لا يعد تفتيشا لنظام الحاسب الآلي وإنما هو تفتيش للأشخاص والأماكن يخضع للقواعد العامة لتفتيش الأماكن والأشخاص.

وفي الجريمة المعلوماتية ولأجل الحصول على الدليل الجنائي فيها يستلزم إتخاذ إجراءات التفتيش للنظام المعلوماتي[1] نفسه وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى في ظل شيوع الشبكات الداخلية على مستوى الشركات والمؤسسات والشبكات المحلية والدولية، ويعتبر هذا الإمتداد محل تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش[2]، وهذا ما سيتم التعرف عليه من خلال هذه الدراسة.

أولا: تعريف التفتيش في الجرائم الرقمية

يقصد بالتفتيش **لغة** البحث والإستقصاء.

أما **إصطلاحا** فلم تتضمن مختلف التشريعات تعريفا للتفتيش مما يترك المجال مفتوحا لكل من القضاء والفقه الذي تعددت تعريفاته للتفتيش فقد عرفه البعض بأنه إجراء من إجراءات التحقيق وكل ما يفيد في كشف الحقيقة وهو ينطوي على مساس بحق المتهم في سرية حياته الخاصة[3] يقوم به موظف مختص طبقا للإجراءات المقررة قانونا، في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم.

---

[1] أوضحت المذكرة التفسيرية لإتفاقية بودابست أن المقصود بالنظام المعلوماتي: هو جهاز يتكون من مكونات مادية و مكونات منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية وهو يشمل وسائل لإدخال و إخراج و تخزين البيانات، وهذا الجهاز قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق الشبكة، وكلمة آلية تعني دون تدخل بشري ومعالجة البيانات تعني مجموعة من العمليات التي تطبق على البيانات من خلال برنامج معلوماتي. أنظر أكثر أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضل القانون 09/ 04 مذكرة لنيل شهادة الماجستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2013، ص86.

[2] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الأنترنت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، لبنان، ط1، 2007، ص 46.

[3] بكرى يوسف بكرى، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، ط1 ، 2011 ، ص 57.

وهناك من عرفه بأنه "إجراء تحقيق يختص به المحقق ويستهدف التنقيب في مستودع السر عن الأدلة المادية لجريمة وقعت فعلا، ويتم رغم إرادة صاحب الشأن"[1].

وهناك من عرفه بأنه ذلك البحث المادي في مكان ما بهدف البحث عن الأشياء المتعلقة بالجريمة الجاري جمع الإستدلالات أو حصول التحقيق بشأنها[2].

والمشرع الجزائري لم يرد تعريفا خاصا ودقيقا للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق وإحاطته بضوابط صارمة نظرا لأهميته في كشف الأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم وهو ما ورد في نص المادة 40 من الدستور التي جاء فيها «فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة».

أما تفتيش الأنظمة المعلوماتية، فقد عرفه بعض الفقهاء بأنه البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة و نسبتها إليه أو هو البحث الدقيق والإطلاع على محل خصه القانون بحماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكنا أو جهاز حاسوب أو أنظمة أو الأنترنت[3].

كل هذه التعريفات لا تخرج في مجملها عن كون التفتيش هو إجراء من إجراءات التحقيق غايته ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة في شأنها[4]، فالتفتيش ليس غاية في حد ذاته وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تساهم في ظهور الحقيقة.

[1] حسن الجوخدار، المرجع السابق، ص 104.

[2] محمد حزيط، المرجع السابق، ص 91 .

[3] رضى هميسي، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة العلوم القانونية و السياسية، جامعة الوادي، العدد5، جوان 2012، ص 160.

[4] زيبحة زيدان، المرجع السابق، ص 130.

وقد نصت المادة 1/19 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية بودابست[1] التي أعدها المجلس الأوربي وتم التوقيع عليها في بودابست في: 2001/11/23 على وجوب تبني كل دولة طرف تشريعات تخول السلطة المختصة إختصاص التفتيش أو الدخول المشابه أو ما يعبر عنه بالولوج[2].

والتفتيش يعد من أهم الإجراءات المخولة لضباط الشرطة القضائية بحسب نص المادة 1/5 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وكذلك قانون الإجراءات الجزائية.

ثانيا: شروط التفتيش في الجرائم الرقمية

إن التفتيش سواء في العالم المادي أو الرقمي هو اعتداء على حرية الأشخاص والإطلاع على أسرارهم ولضمان صحة التفتيش أجازه المشرع بوصفه إجراء تحقيق بعد أن أحاطه بضمانات كي لا يساء استعماله، فيغدو عملا تعسفيا باطلا مع كل ما تولد عنه من آثار وتهدف هذه الضمانات إلى مباشرة التفتيش في حدود الغاية منه ولضمان صحته.

وإذا كان التفتيش المتعارف عليه نوعان تفتيش المساكن وتفتيش الأشخاص كما ورد النص عليه في قانون الإجراءات الجزائية في المادة 44 و 64 منه فإن التفتيش المنصب على المنظومة المعلوماتية بالرغم من أنه يتفق معه في المباديء العامة والإجراءات إلا انه يختلف عنه كلية من حيث الشروط الشكلية والشروط الموضوعية التي تحكمه وكذا موضوع التفتيش[3].

---

[1] معاهدة بودابست لمكافحة الجرائم المعلوماتية و الموقعة في العاصمة المجرية بودابست في 23 نوفمبر 2001 المتعلقة بالإجرام الفضائي، حيث تتكون هذه الإتفاقية من 48 مادة موزعة على أربعة أبواب خصص الباب الأول في استخدام المصطلحات، الباب الثاني: الإجراءات الواجب اتخاذها على المستوى القومي، الباب الثالث: التعاون الدولي، والباب الرابع: الشروط الختامية. للمزيد راجع بن فردية محمد، المرجع السابق ص 27.

[2] الولوج هو مصطلح خاص بنظم التكنولوجيا والإتصال يحقق الوصول إلى البيانات المخزنة ويقتضيه بطبيعة الحال إجراء التفتيش والحصول على الأدلة فهناك إذا فرق بين المصطلحين فالدخول إجراء للتفتيش، و التفتيش وسيلة لجمع الأدلة وإن كان من الناحية العملية كل منهما يترتب على الآخر. أنظر أكثر وليد طه، التنظيم التشريعي للجرائم الإلكترونية في إتفاقية بودابست، بحث على الموقع: Htt://leagueofarabstates.net أطلع عليه بتاريخ:2018/03/31، ص 29)

[3] زيبحة زيدان، المرجع السابق، ص 131.

غير أن التفتيش في البيئة الرقمية يثير لدينا التساؤل حول إمكانية تطبيق القواعد العامة للتفتيش على صورة تفتيش نظم الحاسوب والأنترنت ذلك أن هذا الإجراء يهدف إلى جمع الأدلة المادية في حين أن النظم المعلوماتية عبارة عن كيان معنوي حيث تنتفي صفة المادة من ذلك لأنها تشمل على بيانات وبرامج الحاسوب[1].

فالتفتيش في العالم الإفتراضي أو النظم الحاسوبية ذو طبيعة خاصة ينصب على بيانات ومعلومات موجودة داخل جهاز الحاسوب أو أحد ملحقاته وما تشمله من مكونات.

1/ الشروط الشكلية للتفتيش:

يعد تفتيش المنظومة المعلوماتية من أخطر الإجراءات مساسا بالحق في حرمة الحياة الخاصة لهذا يجب إحاطته بضمانات تكفل حماية هذا الحق عن طريق مباشرته وفقا لأشكال معينة، وبالرجوع إلى القانون 09-04 نلاحظ أن المشرع الجزائري لم يوضح بدقة هذه الإجراءات الشكلية وإنما أخضعها للقواعد العامة الواردة في نص المادة 44 وما يليها من قانون الإجراءات الجزائية مع مراعاة ما تضمنه القانون 09-04.

ومن هذه القواعد الشكلية نذكر:[2]

- **الحصول على إذن مكتوب صادر عن السلطات القضائية المختصة؛** من أهم الضمانات التي وضعها المشرع هو الحصول على إذن مكتوب مسبق من قبل وكيل الجمهورية أو قاضي التحقيق المختص حسب الحالات، ووجوب الإستظهار بهذا الإذن قبل الدخول إلى المسكن أو الشروع في عملية التفتيش.

[1] جواحي عبد الستار، جرائم الحاسوب – دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري– مذكرة تخرج تدخل ضمن متطلبات الحصول على شهادة الماستر في العلوم الإسلامية، جامعة الشهيد حمه لخضر الوادي، كلية العلوم الإجتماعية والإنسانية، قسم العلوم الإنسانية، الجزائر، 2015 ، ص 63.

[2] طيبي الطيب، البحث والتحقيق في جريمة تبييض الأموال في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في الحقوق، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2012، ص 92.

غير أنه في القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة في القانون 04/09 لا نجد المشرع يتحدث عن هذا الشرط إطلاقا كل ما في الأمر أنه تحدث عن إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة حاسوبية أخرى.

لكنه نص على أنه عند قيام ضباط الشرطة القضائية بتفتيش نظم الحواسيب يكون بناءا على قواعد قانون الإجراءات الجزائية التي تفرض عليهم عند الإنتقال لتفتيش المساكن والأشخاص المشتبه فيهم قيامهم بأفعال جنائية أن يكونوا مصحوبين بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب الإستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش[1] طبقا للمادة 5/5 من القانون04/09، كما أن الدستور نص على وجوب أن يتم التفتيش بأمر مكتوب صادر عن السلطات القضائية المختصة[2]، إضافة إلى أنه وبالرجوع إلى الأعمال التحضيرية لمناقشة مشروع القانون04/09 ذكر وزير العدل صراحة أن يكون التفتيش بإذن مسبق من القضاء[3].

إلا أن هذا الشرط يحمل بعض المخاطر كأن يكون البحث عن الأدلة يستدعي التفتيش في نظام معلوماتي آخر غير الذي صدر الإذن بشأنه والمخاطر تتمثل في إمكانية قيام الجاني بتدمير أو محو البيانات أو نقلها أو تعديلها خلال الفترة التي يراد الحصول على إذن مكتوب بشأنها فمواجهة لهذا الخطر يرى البعض أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي آخر في أي مكان غير مكان البحث، ويرى البعض أنه في حالة إمتداد الإختصاص فيمكن أن يصدر الأمر بالإمتداد شفويا من قاضي التحقيق، تحقيقا للسرعة المطلوبة، ثم يصدر فيما بعد الإذن المكتوب شريطة أن يتم الدخول إليها بواسطة المنظومة المعلوماتية الأولى الصادر بشأنها الإذن بالتفتيش[4].

[1] جواحي عبد الستار، المرجع السابق، ص 70.

[2] المادة 40 من دستور 1996.

[3] ثابت دنيازاد، مراقبة الاتصالات الالكترونية و الحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية و الإنسانية، جامعة تبسة، العدد 6، 2012، ص 215.

[4] علي عدنان الفيل، المرجع السابق، ص 40.

- **تسبيب الإذن:** وهو بيان الأسانيد الواقعية والقانونية التي أدت إلى إصداره وهي إحدى الحالات التي نصت عليها المادة 4 من القانون 04/09 فعلى السلطة القضائية المختصة ذكر سبب إصدار الإذن بالتفتيش حتى ولو لم ينص القانون صراحة على ذلك وهو الأصل المعمول به في كل الأوامر الصادرة عن السلطة القضائية، وتظهر أهمية التسبيب في تقييد سلطة الجهة القضائية المختصة التي يجب عليها أن تثبت مبررات اللجوء إلى هذا الإجراء لما فيه مساس بحريات الأفراد وكذا تمكين محكمة الموضوع من بسط رقابتها على المبررات التي استندت إليها السلطة المختصة في إصدار الأمر[1].

- **يجب أن يتضمن الإذن بيان وصف الجرم** الذي يجري التفتيش بشأنه من أجل البحث عن دليل فيه وكذا عنوان المسكن الذي سيتم فيه عملية التفتيش تحت طائلة البطلان.

- **حضور المتهم عملية التفتيش:** تنص المادة 1/45 ق.إ.ج على وجوب حضور صاحب المسكن عملية التفتيش أو تعيين من يمثله أو حضور شاهدين يتم تسخيرهما من طرف ضابط الشرطة القضائية، غير أنه ونظرا للطابع الخاص للجريمة المعلوماتية أجاز المشرع إجراء التفتيش دون حضور صاحب الحق على المسكن أو من ينوبه ودون تسخير شاهدين في حال ما إذا كان هاربا، وهو ما يعد إقرار منه بذاتية هذا النوع من الجرائم وما يتطلبه التحقيق بشأنها من بسط نوع من السرية أثناء جمع الدليل الرقمي بالإضافة إلى الإسراع في استخلاصه قبل فقدانه[2].

أما إذا كان المشتبه فيه محجوز للنظر أو محبوس في مكان آخر وتعذر نقله لأسباب أمنية أو لمقتضيات النظام العام، أو وجود خطر إختفاء الأدلة خلال مدة نقله لمكان إجراء التفتيش فإنه في هذه الحالات يجوز إجراء التفتيش من دونه ولكن بحضور شاهدين من غير

[1] ثابت دنيازاد، المرجع السابق ، ص 219 و 220.

[2] جواحي عبد الستار، المرجع السابق، ص 68.

الخاضعين لسلطة ضابط الشرطة القضائية[1]، وهذا من أجل الحصول على الدليل المستهدف من عملية التفتيش في الوقت المناسب.

– **الميقات القانوني للتفتيش:** وهو أن تتم عملية التفتيش في الأوقات المحددة قانونا من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا.

ونظرا لطبيعة المعطيات المعلوماتية وسرعة إتلافها أو تعديلها خاصة إذا علم الجاني بوجود تفتيش فيقوم بإتلاف الدليل في ظرف ثوان مما يؤدي إلى إفساد الأدلة وعرقلة عمل التحقيق، أجاز المشرع طبقا لنص المادة 3/47 ق.إ.ج[2] التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في أي ساعة من ساعات النهار أو ليلا وذلك بناءا على إذن مسبق من وكيل الجمهورية وفي هذه الحالة قد غلب المصلحة العامة على حريات الأفراد، ومرد ذلك إلى اعتبارين:

– ذاتية الجريمة المعلوماتية المتمثلة في إمكانية اختفائها بسرعة فائقة.

– إفتراض كون الدليل الرقمي هو الدليل الوحيد في الدعوى الجزائية ومن ثم ارتكاز كل العملية الإثباتية على وجوده[3].

2/ الشروط الموضوعية للتفتيش:

يقصد بهذه الشروط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له وتنحصر هذه الشروط في السبب ومحل التفتيش.

أ/ سبب التفتيش

حتى يعتبر التفتيش في الجريمة المعلوماتية مشروعا لابد من توافر شروط تتمثل في:[4]

[1] أحسن بوسقيعة، المرجع السابق، ص 85.

[2] أنظر المادة 47 من ق إ ج.

[3] جواحي عبد الستار، المرجع السابق، ص 64.

[4] عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية، دار هومة للطباعة والنشر والتوزيع، الجزائر، بدون طبعة، 2009 ، ص 56.

– وقوع جريمة من جرائم الكمبيوتر بالفعل وأن تشكل جناية أو جنحة من نصوص التجريم والعقاب وتستبعد المخالفات نظرا لقلة أهميتها باعتبارها لا تصل إلى درجة المساس بحريات الأشخاص أو إنتهاك لحرمات منازلهم[1] وباعتبار التفتيش أحد إجراءات التحقيق يبادر به عند ارتكاب فعل مجرم من أجل جمع الأدلة والقرائن فمن غير الممكن القيام به دون وقوع جريمة، غير أن المشرع الجزائري خرج على هذا المبدأ واستبق الأحداث وجعل من التفتيش مهمة وقائية الهدف منها هو الحيلولة دون وقوع الجريمة المعلوماتية من خلال القيام بعمليات المراقبة المسبقة للإتصالات الإلكترونية طبقا لنص المادة 3 من القانون 09– 04[2].

في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني فهذا التفتيش وقائي[3] قد تسفر عنه أدلة يمكن أن تكون إثبات لتخطيط مسبق يراد به ارتكاب جرائم ذات خطورة على الأمن الداخلي للدولة، وهناك من يعتبر أن هذا الأسلوب الوقائي إعتداء فعلي على الحياة الخاصة للأشخاص لأن القانون لم يحدد صفات من يقع عليهم هذا التفتيش أهم مجرمون سابقون، أو من لهم علاقة بمجرمين ارتكبوا هذه الأفعال.....آلخ[4].

– توجيه الإتهام لشخص أو لمجموعة من الأشخاص ممن يظهر أنهم قد ساهموا في الجريمة، فلا يمكن مباشرة التفتيش لمجرد وقوع جريمة من جرائم الكمبيوتر بل لابد من نسبتها لشخص أو أشخاص معينين بالدلائل الكافية بصفته فاعلا أو شريكا أو حائزا لأشياء تتعلق

[1] معمش زهية وغانم نسيمة، المرجع السابق، ص 20.

[2] زيبحة زيدان، المرجع السابق، ص 138.

[3] التفتيش الوقائي أو الإفتراضي يختلف عن مراقبة الإتصالات الإلكترونية من حيث التقنية، فالمراقبة تعني اعتراض المراسلات (SMS ، E-MAIL غرف الدردشة) وكشف محتواها بدون الدخول إلى النظام المعلوماتي للجهاز الذي يتم مراقبته، أما التفتيش عن بعد فهو يتم عن طريق برنامج تجسس (حصان طروادة) يسمح بالولوج للنظام المعلوماتي. أنظر أكثر أحمد مسعود مريم، المرجع السابق ، ص 92.

[4] نفس المرجع، ص 89.

بالجريمة، فلا يقتصر الأمر على مجرد تجميع قرائن بل لابد أن تتوفر لديه دلائل قوية تدعو إلى الإعتقاد بمساهمته في ارتكاب الجريمة المعلوماتية[1].

ويمكن الإستدلال على ذلك بنص المشرع الجزائري بقوله «لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية ويحوزون أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش»[2].

فالهدف من التفتيش هو الحصول على دليل مادي للوصول إلى الحقيقة، إضافة للهدف الوقائي في مواجهة ارتكاب الجريمة الإلكترونية دون الحاجة لتوجيه الإتهام لأي شخص كان.

ب/ محل التفتيش:

التفتيش في الجريمة التقليدية ينصب على شخص المتهم أو غير المتهم وكذلك على مسكن المتهم وما في حكمه وملحقاته، لكن في الجريمة المعلوماتية يعد جهاز الحاسوب وشبكة الأنترنت محلا للإعتداء وليس وسيلة لارتكاب الجريمة فحسب، فيقع التفتيش على الأشياء المادية وبرامج الحاسب الآلي وبياناته أي كل ما يحتويه مشروع السر وكل ماله علاقة بالجريمة من أجهزة الحاسوب والآلات والنظم والبرامج والأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش، وعلى اعتبار أن الجاني بإمكانه التخلص من البيانات التي يستهدفها التفتيش عبر إرسالها من خلال نظام معلوماتي من مكان إلى آخر وارتباط شبكة الحواسيب ببعضها البعض فقد أجاز المشرع من خلال نص المادة 5 من القانون 09-04.

تمديد التفتيش بسرعة إلى منظومة معلوماتية أخرى أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك فهذا الإمتداد يتم بشكل سريع تماشيا مع طابع السرعة الفائقة الذي يجري عليه نقل المعلومة وهذا الولوج إلى منظومة المعلومات يتم بمجرد الشك أو الإعتقاد بتواجد المعلومات محل البحث داخلها.

[1] رضى هميسي، المرجع السابق، ص 165.

[2] المادة 46 ق.إ.ج.

فالتفتيش إذا قد يقع على الأشخاص و المساكن التي تحتوي على تلك الأجهزة أو الشبكات المعلوماتية[1].

يتم تحرير محضر لكي يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة ولم يتطلب القانون شكل خاص للمحضر وبالتالي لا يشترط لصحته سوء ما تستوجبه القواعد العامة في المحاضر عموما[2].

ثالثا: مدى قابلية المنظومة المعلوماتية للتفتيش: وتظم المنظومة المعلوماتية المكونات المادية للحاسبة الإلكترونية، والمكونات المنطقية والشبكات المتصلة بالحاسوب عن بعد.

1/ مدى قابلية المكونات المادية للحاسبة الإلكترونية للتفتيش

إن اللجوء إلى تفتيش المكونات المادية للحاسبة الإلكترونية بحثا عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش ولا توجد فيه أي مشكلة في التنفيذ لإمكانية ذلك وسهولته مع الأخذ بعين الإعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها وتأتي سهولة هذا التفتيش لأنه يرد على المكونات المادية للحاسب الآلي (hardware) و ملحقاته بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة و الأقراص الصلبة و الضوئية ولا خلاف حول خضوعها للتفتيش طبقا لقواعد قانون الإجراءات الجزائية[3]، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هي من الأماكن العامة أو الخاصة أو ما إذا كانت منعزلة عن غيرها من الحسابات الأخرى أم متصلة بحاسب آلي آخر أو بنهاية طرفية في مكان آخر... كمسكن غير المتهم مثلا[4].

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 222. أنظر أيضا: عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، المرجع السابق، ص 637.

[2] بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2016، ص 79 .

[3] جواحي عبد الستار، المرجع السابق، ص 64 .

[4] علي عدنان الفيل ، المرجع السابق، ص 41.

فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها الكشف عن الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، فإذا وجد شخص يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة سواء أكانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أو كانت من الأماكن العامة بالتخصيص كالمقاهي، المطاعم، والسيارات العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[1]، أما إذا كانت موجودة بمسكن المتهم أو أحد ملحقاته فتحكمها القواعد ذاتها التي يخضع لها تفتيش المسكن.

2/ مدى قابلية المكونات المنطقية للحاسبة الإلكترونية للتفتيش

لقد ثار جدل كبير في الفقه حول إمكانية خضوع المكونات المنطقية للحاسبة الإلكترونية (software) للتفتيش[2].

– **الرأي الأول** يرى جواز ضبط البيانات الإلكترونية بمختلف أشكالها ذلك أن الإذن بضبط (أي شيء) يشمل بيانات الحاسبة المحسوسة وغير المحسوسة مستندين في ذلك إلى أن المادة هي كل ما يشغل حيزا ماديا في فراغ معين وأن هذا الحيز يمكن قياسه والتحكم فيه وبناءا على ذلك فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ويمكن قياسه بمقياس معين هو البايت والكيلوبايت والميغابايت ...آلخ[3] وأنها أيضا تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها تعد وفقا لذلك ذات كيان مادي و تتشابه مع التيار الكهربائي الذي اعتبره الفقه و القضاء في فرنسا و مصر من قبيل الأشياء المادية، لأن الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فهذا المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها.

[1] بن فردية محمد، المرجع السابق، ص 130.

[2] صغير يوسف، المرجع السابق، ص 78.

[3] حسين بن سعيد الغافري، المرجع السابق، ص 12.

– **الرأي الثاني** على نقيض الرأي الأول يرى عدم انطباق المفهوم المادي على بيانات الحاسبة غير الملموسة، فيقتصر بذلك التفتيش على الأدلة المادية بمعنى عدم إمكانية إنسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما يتطلبه كشف الحقيقة في الجرائم الحاسوبية من بحث وتنقيب عن الأدلة في برامج الحاسوب وبياناته، ومن بين الأدلة التي استندت عليها للبرهنة على ذلك أن هناك من التشريعات من حدد هدف التفتيش هو البحث عن الأشياء وضبطها وهذا الشيء يقتصر بمفهومه على المال ذي الحيز المادي المحسوس ولا يمتد في نطاق شموله إلى الكيانات المنطقية، وقد عملت هذه الدول التي أخذت بهذا الاتجاه إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية[1].

– **الرأي الثالث** ذهب إلى أن الضبط يقع على البيانات الحاسبة الإلكترونية إذا اتخذت شكلا ماديا، فالبيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس ومع ذلك فيمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة لهذا فقد أجاز الفقه والتشريعات التي صدرت في هذا المجال إمكانية أن يكون محل لتفتيش البيانات المعالجة إلكترونيا والمخزنة بالحاسبة الإلكترونية، ثم ضبطها والتحفظ عليها أو ضبط الوسائط الإلكترونية التي سجلت عليها هذه البيانات، والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام فالتفتيش أو البحث في الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدلة المطلوبة[2].

ويتضح موقف المشرع الجزائري من خلال القانون 04/09 حينما أجاز صراحة تفتيش المنظومات الحاسوبية، وذلك بموجب المادة 05 منه التي نصت على أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية...

[1] جواحي عبد الستار، المرجع السابق، ص 65.

[2] علي عدنان الفيل، المرجع السابق، ص 39.

الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات الرقمية المخزنة فيها وكذا منظومة تخزين معلوماتية.

فمن الآثار التي يتركها متصفح الأنترنت صفحات الويب التي إطلع عليها و تحديد وقت دخوله إلى الشبكة ومدة بقائه فيها و الأشخاص الذين تم التواصل معهم والملفات التي تبادلها وكذا معرفة محتوى صندوق بريده الإلكتروني، فالمعطيات السلوكية التي يدونها مستعمل الشبكة تبقى آثارا عليها وكل إساءة استعمال لهذه البيانات يمكن كشفه من قبل الجهات المؤهلة بالبحث عن سلوك المستخدمين ويتم هذا الأمر بدون علم أو رضا ذلك المستخدم[1].

3/ تفتيش الشبكات المتصلة بالحاسوب عن بعد

تزامنا مع التطور التكنولوجي لثورة الإتصالات لم يعد نطاق الإتصالات محدود في إقليم دولة واحدة، وإنما امتد ليشمل كل أرجاء العالم على إثر ظهور شبكة الأنترنت والتي هي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لامركزية، ويدخل في تركيب هذه الشبكة ملايين الحواسيب عبر العالم وخضوع شبكات المعالجة الآلية للتفتيش على درجة كبيرة من الخطورة تتعلق بالتفتيش عن بعد وذلك نتيجة للطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية[2] في أماكن مجهولة بعيدا تماما عن الموقع المادي للتفتيش فقد يكون الموقع الفعلي للشبكات داخل اختصاص قضائي آخر وحتى في بلد آخر، وهو ما يزيد المسألة تعقيدا باعتبار أن الشبكة الحاسوبية ممتدة في أرجاء العالم تقريبا، وبالتالي فإن الحاسوب أو النهاية الطرفية التي يمكن أن ترتكب عليها أو بواسطتها جرائم الكمبيوتر تخضع للقانون الإجرائي الخاص بتلك المنطقة.

[1] رضى هميسي، المرجع السابق، ص 163.

[2] جواحي عبد الستار، المرجع السابق، ص 66.

فبهذا الصدد يثار التساؤل حول أثر تفتيش الأنظمة الحاسوبية المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة، وهنا يمكن التمييز بين احتمالين على النحو التالي:[1]

– **الإحتمال الأول:** إتصال حاسب المتهم أو المشتبه فيه بحاسب آخر موجود في مكان آخر داخل الدولة، وهنا يثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب هو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم؟

في هذه الحالة أجاز المشرع الجزائري تفتيش النظم الرقمية المتصلة بالحاسوب الذي يجري تفتيشه من خلال القانون 09/ 04[2] الذي ورد فيه أن حالة تفتيش منظومة حاسوبية أو جزء منها وكذا المعطيات الحاسوبية عنها مخزنة في منظومة حاسوبية أخرى وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها دون استصدار إذن قضائي وإنما يكفي إعلام السلطة القضائية المختصة مسبقا بذلك[3] طبقا للمادة 2/5 من القانون 04/09 ولعل انتظار صدور الإذن قد يأخذ وقت ما قد يؤدي إلى تلاشي الدليل واندثاره في وقت قياسي كأن يقوم المشتبه فيه بمحوه و إتلافه إذ يكفي الضغط على مكان معين لإنهاء وجود المعلومة وضياع الدليل[4].

ويتم هذا التفتيش شريطة:

• أن تكون النهاية الطرفية المتصلة بالحاسب الآلي موجودة داخل الدولة المعنية.

• أن تتضمن النهاية الطرفية المتصلة بالحاسب الآلي بيانات مخزنة تستهدف إظهار الحقيقة.

[1] جواحي عبد الستار، المرجع السابق، ص 67.

[2] المادة 4 من القانون 04/09.

[3] المادة 2/5 من القانون 04/09.

[4] رضى هميسي، المرجع السابق، ص 168.

وقد سمحت الإتفاقية الأوربية لجرائم الأنترنت بودابست 2001 في القسم الرابع فحوى نص المادة 19 في فقرتها الثانية[1] للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به عن طريق شبكة الإتصالات إذا كان في هذا الأخير معلومات يتم الدخول إليها من خلال الجهاز محل التفتيش.

- **الإحتمال الثاني:** إتصال حاسب المشتبه فيه أو المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة، وهنا يحتمل أن يقوم المتهم بتخزين البيانات في أنظمة حاسوبية خارج الدولة عن طريق شبكات الإتصال البعيدة بهدف عرقلة سلطات التحقيق في جمع الأدلة والتحقيقات وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة المختصة التي صدر من جهتها الإذن ودخوله في المجال الجغرافي للدولة الأخرى وهو ما يسمى بالولوج أو التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها[2].

يرى جانب من الفقه أن التفتيش الإلكتروني العابر للحدود لابد أن يتم في إطار إتفاقيات خاصة ثنائية أو دولية تجيز هذا الإمتداد تعد بين الدول المعنية، وبالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في غياب تلك الإتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم المرتكبة عبر الأنترنت، كما أجازت المادة 32 من الإتفاقية الأوروبية بودابست إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين:

الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور.

والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش[3].

---

[1] «يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل التأكد مما إذا كانت سلطاته تقوم بالتفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي معين أو جزء منه على أرضه، و أن هذه البيانات يمكن الوصول إليها بشكل قانوني سواء من خلال النظام الأول أو من خلال كونها مهيأة من أجله، وأن هذه السلطات المذكورة ستكون قادرة على التوسع العاجل لنطاق التفتيش أو الولوج بطريق مشابه لنظام آخر»

[2] صغير يوسف، المرجع السابق، ص 78.

[3] بن فردية محمد، المرجع السابق، ص 141.

وتصديا لهذا الإحتمال أجاز المشرع الجزائري تفتيش الأنظمة المتصلة بالرغم من تواجدها خارج الإقليم الوطني في نص المادة 3/5 من القانون 04/09 بقوله «إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى مخزنة في منظومة حاسوبية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل».

رابعا: بطلان التفتيش في الجرائم الرقمية

لقد راعى المشرع في شأن قواعد التفتيش الموازنة بين حماية حريات الأشخاص وعدم المساس بحقهم في الخصوصية وعدم إفشاء الأسرار[1] وحصانة مساكنهم وبين المصلحة العامة في الكشف عن الحقيقة والوصول إلى الهدف المرجو من ثم لابد على جهة التحقيق مراعاة القواعد الموضوعية والشكلية للقيام بالتفتيش حتى لا يترتب على ذلك البطلان.

وقد اختلف الفقه الجنائي في شأن ترتيب البطلان على مخالفة القواعد الخاصة بالتفتيش فهناك من يرى أنها تتعلق بالنظام العام وللمحاكم أن تقضي به من تلقاء نفسها وهناك من يرى أن البطلان يتعلق بمصلحة الخصوم.

ولكن في الحقيقة أن قواعد التفتيش تعد قواعد جوهرية ترتب البطلان على مخالفتها لكن هذا البطلان لا يتعلق بالنظام العام[2] لأن هذه القواعد تتعلق بمصلحة الخصوم ودليل ذلك أن المحكمة لا تقضي به من تلقاء نفسها ويجب أن يتمسك به ذوي الشأن وهو الشخص الذي وقع التفتيش الباطل مساسا بحريته الشخصية أو بحرمة مسكنه ومتى كان التفتيش باطلا فإن البطلان يتناول جميع الآثار القانونية المترتبة عليه مباشرة فلا تعتد المحكمة بما أسفر عنه التفتيش من ضبط للأشياء تتعلق بالجريمة ولا أثر له على بقية الأدلة التي لم تكن مترتبة عليه[3].

[1] بكرى يوسف بكرى، المرجع السابق، ص 60.

[2] حسن الجوخدار، المرجع السابق، ص 182.

[3] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية،المرجع السابق، ص 639.

الفرع الثاني: الضبط في الجرائم الرقمية

يترتب على التفتيش نشوء حق في ضبط الأشياء التي تفيد في كشف الحقيقة عن الجريمة والعثور على أدلة في الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها، هذه الأشياء محل الضبط في نطاق التفتيش في الوسائل التقنية الحديثة قد تكون أشياء مادية كالأجهزة كما يمكن أن تكون أشياء معنوية كالمراسلات والإتصالات الإلكترونية والمعلومات المعالجة إلكترونيا وكافة المكونات المعنوية للوسائل التقنية الحديثة[1].

أولا: تعريف الضبط في الجرائم الرقمية

الضبط هو وضع اليد على شيء متصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبيها والضبط هو الغاية من التفتيش ونتيجته المباشرة المستهدفة، ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تنطبق بشأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط[2].

ويترتب على هذا الإرتباط بين التفتيش والضبط أن هذا الأخير لا يجوز أن يقع على شيء إلا بوصفه دليلا من أدله الجريمة التي يجرى التفتيش بشأنها ولذلك فإنه يباشر من أجل الحقيقة المطلقة، أي مادام أن التفتيش يستهدف ذات الحقيقة فيتعين أن يباشر ضبط ما يتعلق بها من أدلة سواء كانت للإدانة أم للبراءة لأن ما يضبط في الحالتين يحقق العدالة الجنائية ويفيد معنى الإرتباط بالتفتيش.

وقد يرد الضبط في الجريمة الرقمية على مكونات مادية للكمبيوتر كالورق وجهاز الكمبيوتر وملحقاته، الأقراص الصلبة الخارجية والمرنة، أقراص الليزر... ويجب على القائم بالتفتيش والحجز أن يحافظ على هذه الأجهزة بالحالة التي كانت عليها، كما قد يرد الضبط

[1] بكرى يوسف بكرى، المرجع السابق، ص 127.

[2] مصطفى محمد موسى، المرجع السابق، ص 208.

على أشياء ذات طبيعة معنوية كالمراسلات والبيانات والإتصالات الالكترونية[1] التي تم نقلها من حاسب لآخر عن طريق شبكات الإتصال.

ثانيا: حجز المعطيات المعلوماتية

إذا وقعت الجريمة على المكونات المادية للحاسب كالبيانات أو المعطيات المثبتة على دعامة أو حوامل كالأقراص أو أشرطة ممغنطة فإن حجز هذه الأشياء لم يثير أي إشكال بين الفقهاء في تقرير صلاحية هذه الأدلة بموجب قواعد التفتيش التقليدية لأن الضبط في الأصل لا يرد إلا على أشياء مادية.

غير أن الإشكال يثور في توقيع الحجز على منظومة معلوماتية، ذلك أن المعلومات هي في الأصل شيء معنوي وهو ما يطلق عليها حديثا بمصطلح الأموال المعنوية أو بنك المعلومات[2]، أو إذا استخدمت في الجريمة الواقعة على برامج الحاسب وسائل فنية مثل الفيروسات فتثور الصعوبة في ضبط الأشياء[3].

– **الرأي الأول:** يرى أنها لا تصلح لأن تكون محلا للضبط لانتفاء الكيان المادي ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس عن طريق التصوير الفوتوغرافي، أو نقلها على دعامة أو غيرها من الوسائل المادية.

– **الرأي الثاني:** يرى أن هذه البيانات المعالجة إلكترونيا هي ذبذبات إلكترونية أو موجات كهرومغناطيسية تقبل التسجيل والحفظ والتخزين على وسائط مادية و بالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها بالتالي وجودها المادي لا يمكن إنكاره، وفي ذلك نص قانون الإثبات الكندي في المادة 7/29 منه على «إن التفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 274.

[2] زيبحة زيدان، المرجع السابق، ص 148.

[3] صبايحية خديجة، جرائم السرقة و الإحتيال عبر الأنترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم الإسلامية، جامعة الجزائر، كلية العلوم الإسلامية، 2013، ص 110.

مالية يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة، يستوي في ذلك أن تكون السجلات مكتوبة أم في شكل الكتروني»[1].

بالتالي إذا كان الأمر قد انتهى بنا إلى ضرورة أن يشمل التفتيش المكونات المعنوية للوسائل التقنية الحديثة فإنه من الضروري أن يترتب على ذلك إباحة ضبطها.

– **رأي المشرع الجزائري:** لقد ذهب المشرع الجزائري من خلال نص المادة 6 من القانون 09-04 إلى القول بإمكانية حجز المنظومة المعلوماتية برمتها إذا كان ضروريا لمصلحة التحقيق أو القيام بحجز المعطيات المعنية بالذات وذلك بعد نسخها على دعامة مادية أو أي وعاء للبيانات كطبعها على الورق أو ضبطها على الشاشة وذلك لتسهيل قراءتها والتعامل معها، إذ أشارت المادة 6 السالفة الذكر إلى عبارة «دعامة تخزين إلكترونية تكون قابلة للحجز» فحجز الأدلة يجري وفقا لمقتضيات قانون الإجراءات الجزائية فدعائم التخزين التي يتم نسخ المعلومات محل البحث عليها يجب أن تكون ذات قابلية للحجز والوضع في أحراز[2]، وإضافة إلى الحجز فإن قانون العقوبات نص على تدابير أخرى منها مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع محل الجريمة تطبيقا لما جاء في نص المادة 394 مكرر6 ق.ع.

كما حرص المشرع على جعل المعلومات محل البحث في مأمن باستخدام التقنيات اللازمة لمنع الوصول إليها وذلك في حالة استحالة حجزها لأسباب تقنية كما لو كانت المعطيات مخزنة بأنظمة التشغيل التي لا يمكن نسخها وهو ما نصت عليه المادة 07 من القانون 09-04 وذلك لمنع تهريبها أو تدمير تلك الأدلة المؤدية لها.

والهدف من هذا الإجراء الإحترازي هو الحفاظ على الأدلة في محيطها الإلكتروني، ومنع أي محاولة لطمسها أو إخفاء معالمها، وهو الأمر الذي سيكون له الأثر الإيجابي في نجاح إجراءات التفتيش والحجز.

[1] علي عدنان الفيل ، المرجع السابق، ص58.

[2] رضى هميسي، المرجع السابق، ص 175.

من هذا يتضح أن إجراءات الضبط نوعين؛ وهو الأمر الوارد في نص المادة 3/19 من إتفاقية بودابست وهما:[1]

– إجراءات مبدئية تحفظية: الهدف منها هو الحفاظ على البيانات المخزنة التي تكون لها أهميتها في التحقيق ببقائها في أمكنتها في النظام المعلوماتي للكمبيوتر أو في دعامة التخزين ومنع الوصول إليها أو إلغائها أو التصرف فيها وذلك للكشف عن مرتكب الجريمة وسهولة إثباتها عليه.

– إجراءات لاحقة بالضبط: وهي إجراءات لاحقة للتفتيش والدخول ويقصد بها جمع البيانات سواء بأخذ دعامة تخزين المعلومات أو أخذ نسخة من البيانات المخزنة بها أو بالنظام المعلوماتي للكمبيوتر في ورق أو أقراص.

ثالثا: ضوابط الحجز في الجرائم الرقمية:

لقد خص المشرع الجزائري حجز الأدلة وفقا لنص المادة 84 ق.إ.ج بضوابط تتمثل فيما يلي:[2]

– الاطلاع على المستندات المراد حجزها مخول فقط لقاضي التحقيق أو ضابط الشرطة القضائية الذي أنابه عنه قبل حجزها ووضعها في أحراز مختومة ويحرر محضرا بضبطها.

– الإحترام التام لمقتضيات وضرورات التحقيق وعلى الأخص ضمان إحترام سر المهنة وحقوق الدفاع.

وعلى الفور يتم فرز الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة وأكدت المادة 84 ق.إ.ج السالفة الذكر بأن الأحراز والوثائق المحجوزة لا يتم فتحها إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا وفضلا عن ذلك يستدعى كل من ضبطت لديه هذه الأشياء وذلك لحضور هذا الإجراء، و ورود كلمة (الأشياء) في نص المادة 84 ق.إ.ج تنصرف إلى المعطيات المعلوماتية المبحوث عنها.

[1] وليد طه ، المرجع السابق، ص 30.

[2] زيبحة زيدان، المرجع السابق، ص 151 . أنظر أيضا بكرى يوسف بكرى، المرجع السابق، ص 130.

فالمشرع هنا يكون قد حافظ على مبدأين هامين وهما: السرية وحقوق الدفاع كما نصت المادة 85 ق.إ.ج بمعاقبة كل من أفشى أو أذاع مستندا متحصلا من تفتيش لأي شخص ليست له علاقة في الإطلاع عليها وهو ما أكدته أيضا المادة 09 من قانون 09-04.

وبعد القيام بعملية التفتيش و الحجز وجب على السلطة التي قامت بذلك المحافظة على سلامة المعطيات في المنظومة المعلوماتية محل التفتيش باتخاذ الوسائل الفنية المطلوبة حفاظا على سلامة المعطيات المعلوماتية التي تم حجزها.

المطلب الثالث: الخبرة في الجرائم الرقمية

يقوم المحقق الجنائي في سبيل الكشف عن غموض الجريمة وفاعلها باتخاذ إجراءات عدة ووسائل متنوعة لتحقيق هدفه غير أن هذا الأمر يتطلب جهد كبير ليس باستطاعة المحقق أن يقوم به بمفرده كما أنه قد يخرج عن مجال تخصصه مما يستدعي الإستفادة بأهل الخبرة، ومنذ ظهور الجرائم الإلكترونية أصبح الخبراء الإلكترونيون في العصر الحالي أهم أعوان المحقق والباحث الجنائي وتعد أعمالهم من أهم الأدلة الجنائية الإلكترونية لأنها تساعد المحقق في فك غموض العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق.

فيقوم الخبير بالتنقيب عن الحقيقة بناءا على الأشياء المضبوطة ويقدم الدليل المستنبط للقاضي الذي يمكن أن يبني عليه حكمه.

وحتى يتضح دور الخبرة في تقديم دليل جنائي في الجرام الرقمية لابد من التطرق لتعريف الخبرة (الفرع الأول) أهميتها (الفرع الثاني) وشروط صحتها (الفرع الثالث) عمل الخبير وأساليبه (الفرع الرابع).

الفرع الأول: تعريف الخبرة في الجرائم الرقمية

الخبرة هي عبارة عن استشارة فنية يستعين بها قاضي التحقيق لتقدير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوافر لدى قاضي التحقيق بحكم تكوينه[1].

[1] أحسن بوسقيعة، المرجع السابق، ص 107.

أو هي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالإستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو الدليل المادي، وإنما هي تقييم لهذا الدليل، والشيء المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة والتفتيش هو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها التدليلية في الإثبات[1].

ويطلق لفظ الخبير على كل شخص مختص فنيا في مجال من المجالات الفنية أو العلمية يستطيع بما لديه من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية والتي تحتاج إلى خبرة فنية خاصة، كالخبير الإلكتروني الذي تعمق في دراسة عمل من الأعمال الإلكترونية وتخصص في أدائه فترة زمنية أكسبته الخبرة[2] فلا يشترط في الخبير كفاءة علمية عالية فحسب في مجال التخصص بل يجب أن يضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه وعلى وجه الخصوص الجرائم ذات الصلة بالحاسبة الإلكترونية.

الفرع الثاني: أهمية الخبرة في الجرائم الرقمية

إذا كانت الإستعانة بخبير فني في المسائل الفنية البحته أمر واجب على جهة التحقيق والقاضي فهي أوجب في مجال الجرائم المعلوماتية حيث تتعلق بمسائل فنية جد معقدة والتطور في أساليب ارتكابها سريع ومتلاحق فلا يكشف هذا الغموض إلا متخصص، فإجرام الذكاء والفن لا يكشفه إلا ذكاء وفن مماثلين، وأمام عجز المحقق الجنائي في كشف غموض الجرائم الرقمية نظرا لنقص الكفاءة والتخصص في الجوانب التقنية والتكنولوجية تظهر أهمية الخبرة في هذا النوع من الجرائم من أجل ذلك ترك المشرع للمحقق الجنائي في الجرائم بصفة عامة والإلكترونية بصفة خاصة الحرية الكاملة في الإستعانة بالخبير لإيضاح مسألة يستعصى توازنه

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، المرجع السابق، ص 593.

[2] مصطفى محمد موسى، المرجع السابق، ص 221. أنظر أيضا علي عدنان الفيل، المرجع السابق، ص 28.

الفكري أن يفهمها حتى لا يتسبب في تدمير الدليل أو محوه عن جهل في التعامل معه وأهم المسائل التي يستعان بالخبير الإلكتروني فيها[1].

– كيفية عزل النظام المعلوماتي دون تلف الأدلة أو تدميرها أو تعديلها أو إلحاق الضرر بالأجهزة.

– كيفية نقل أدلة الإثبات الإلكترونية الرقمية إلى وحدات تخزين خارجية بغير أن يلحقها تلف.

– كيفية إخراج الأدلة الإلكترونية الرقمية في وسيلة ورقية تتيح للقاضي قراءتها وفهمها

– توضيح عمل الأنترنت وطرح رأيه حول النقاط الغامضة في الجريمة.

– إجراء الإختبارات التكنولوجية والعلمية عليه لاختباره والتحقق من مصدره.

– إستخدام وسائل فنية تساعد الخبير في الوصول إلى المجرم المعلوماتي ومعرفة كيفية وقوع الجريمة[2].

من هذا نستنتج أن الخبرة في الجرائم الرقمية أصبحت حتمية فهي وسيلة تساعد في إثبات الجريمة وتهدف إلى كشف بعض الدلائل أو تحديد مدلولها بالمعلومات العلمية وقد تكون إلزامية الإستعانة بالخبير في جميع مراحل الدعوى، الأمر الذي دفع بالكثير من التشريعات لا تكتفي بالنصوص التقليدية وعمدت إلى إدراج نصوص قانونية خاصة تنظم الخبرة، وفي ذلك لم يتخلف المشرع الجزائري عن هذه التشريعات حين أشار لها في القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بقوله "يمكن للسلطات المكلفة بتفتيش المنظومة الحاسوبية تسخير كل شخص له دراية بعمل المنظومة الحاسوبية محل البحث أو التدابير المتخذة لحماية المعطيات الحاسوبية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[3]، وهو الأمر المؤكد بنص المادة

[1] مصطفى محمد موسى، المرجع السابق ، ص 224.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص 303.

[3] جواحي عبد الستار، المرجع السابق ، ص 72.

19 من المرسوم الرئاسي رقم 15-261 بقولها "يمكن أن تستعين الهيئة بأي خبير أو أي شخص يمكن أن يعينها في أعمالها".

الفرع الثالث: شروط الخبرة في الجرائم الرقمية

نظرا للدور البالغ الأهمية الذي تلعبه الخبرة في عملية الإثبات في المجال الجنائي، فقد حرصت معظم التشريعات على تنظيم الخبرة ووضع شروط وضوابط لها، هذه الشروط والضوابط منها ما تعلق بالخبير ومنها ما يتعلق بتقرير الخبرة.

عن الشروط المتعلقة بالخبير نذكر

- إختياره من قائمة الخبراء المحددة أسماؤهم ضمن الجدول المعد مسبقا وقد نصت المادة 144 ق.إ.ج على ذلك بقولها «يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة».

إن الإستعانة بالخبراء وفق المنهج التقليدي في الإجراءات الجنائية يرتبط في الحقيقة بمنطق تقليدي يجب أن يتسع صدر المشرع الإجرائي بصددها بما يسمح بتجاوزها في إطار جرائم الأنترنت، ذلك أنه فضلا عن قاعدة أنه ليس في القانون ما يمنع محكمة الموضوع من ندب خبراء من غير المقيدين بجدول المحكمة فإن هذا التوجه القضائي يجب أن يتم تطويره لكي يمكن الإستعانة بخبراء في العالم الإفتراضي دون حاجة لإبداء أسباب في منطق الإستعانة بالخبراء من خارج الجدول، على أن يشمل التطوير إمكانية أن يكون الإستعانة بالخبراء ممتدا إلى أبعد من النطاق الإقليمي والمادي ممثلا في الحدود المادية بين الدول، وبحيث يمكن أن يكون هؤلاء الخبراء في خارج الإقليم، وهو أمر تسمح به مقومات العالم الإفتراضي هنا كونه يعد بيئة إتصالية رقمية كاملة[1].

- حلف اليمين القانونية، إذ يجب لصحة عمل الخبراء أداء اليمين القانونية وذلك لحمله على الصدق والأمانة في عمله وبث الطمأنينة في آرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة بقية أطراف الدعوى، ولا يغني عن هذا الإجراء أي ضمانة أخرى من

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 291.

الضمانات، وقد أوجب المشرع الجزائري ذلك في نص المادة 145 ق.إ.ج بقوله « يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس».

– يجب أن يكون الخبير صاحب مقدرة وإمكانيات علمية وفنية في المسألة موضوع الخبرة ويستطيع القيام بدوره على أكمل وجه في أن يبين المكان المحتمل لأدلة الإثبات وشكلها وهيئتها والآثار المترتبة على التحقيق في الجريمة المعلوماتية وكيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها[1].

بالتالي يتعين في خبراء الحاسب الآلي المنتدبين للتحقيق أن تتوافر لديهم القدرة الفنية والإمكانات العلمية في المسألة موضوع الخبرة فلا يكتفي بذلك حصول الخبير على شهادة علمية، بل يجب مراعاة الخبرة العملية لأنها هي التي تحقق الكفاءة الفنية وبالتالي لا وجود لخبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرمجياتها وشبكاتها أو لديه قدرة على التعامل مع كل أنواع الجريمة المرتكبة عبر الانترنت[2].

من بين هذه الأمور الفنية والعلمية:

– الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية، والأجهزة الطرفية الملحقة به، وكلمات المرور أو السر وكود التشفير.

– طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

– قدرة الخبير على إتقان المهمة دون أن يترتب على ذلك أعطاب أو تدمير الأدلة المحصلة من الوسائل الإلكترونية، بذلك يجب أن تكون الخبرة في هذا المجال من نوع خاص يتماشى وخصوصية الجريمة الإلكترونية وقد تعمل بعض الدول على إعادة تأهيل بعض القراصنة من أجل الإستفادة من خبراتهم في الإختراق، وفي هذا الصدد يجب أن يتحلى الخبير بمؤهلات

[1] بعرة سعيدة، المرجع السابق، ص 82.

[2] صغير يوسف، المرجع السابق، ص 90.

ومقدرة فنية عالية، معرفة تركيب الكمبيوتر معرفة شاملة لشبكة الأنترنت، كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف[1].

– التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة دون أن يلحقها تدمير أو إتلاف مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على الحاسب أو النظام أو الشبكة[2].

واختيار الخبير في مجال الجريمة المعلوماتية يتحدد بنوعية الجريمة المرتكبة، نظرا لأن الحاسبات وشبكة الإتصال ذات نماذج متعددة، وبالتالي لا يوجد خبير لديه معرفة متعمقة مع كافة أنواع الحاسبات وبرمجياتها وشبكاتها، كما أنه ليس هناك خبير قادر على التعامل مع جميع أنواع الجرائم التي تكون هذه الوسائل الإلكترونية محلا لارتكابها أو أداة لها[3] فقد يستعان بأكثر من خبير ويجب على هذا الأخير أن يدرك أن أي خطأ في التفسير يؤدي إلى إتلاف أو محو الدليل الرقمي.

أما الشروط المتعلقة بتقرير الخبرة فإن الخبير بعد انتهائه من أبحاثه وفحوصاته يعد تقريرا يضمنه خلاصة ما توصل إليه من نتائج بعد تطبيق الأسس والقواعد العلمية الفنية على المسألة محل البحث وإن كان المشرع لم يوجب إتباع شكل معين في تقرير الخبرة فقد يكون شفويا وقد يكون كتابيا وفقا لما تحدده طبيعة المهمة.

ويشترط أيضا أن يقوم الخبير بإيداع تقرير خبرته خلال المدة المحددة له في أمر أو حكم الندب، فإن لم يودع تقريره خلال هذه المدة جاز للقاضي استبداله بغيره ما لم يقدم الخبير طلب بتمديد هذه المهلة وذلك نظرا لما تتسم به الإجراءات الجزائية من طابع السرعة خصوصا في الجرائم الرقمية[4].

[1] فضيلة عاقلي، أعمال المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، طرابلس، 24–25 مارس 2017، ص 12.

[2] صغير يوسف، المرجع السابق ، ص 91.

[3] معمش زهية وغانم نسيمة ، المرجع السابق، ص 36.

[4] جواحي عبد الستار، المرجع السابق، ص 73.

يتعين على الخبير في الجرائم الرقمية التنسيق مع المحقق الجنائي قبل محاكمة الجاني في هذه الجريمة على أن يشمل اللقاء كافة الخبراء الذين ساهموا مع سلطات الضبط أو التحقيق في تلقي البلاغ أو إجراءات الضبط والتفتيش أو فحص البرامج وجمع الأدلة الجناية، على أن يتم في هذا اللقاء حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بينة أو قرينة، وعلى المحقق أن يشرح لهؤلاء الخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة.

وتجدر الإشارة إلى أنه وإن كان للقاضي السلطة التقديرية في الخبرة إلا أن ذلك لا يمتد إلى مسائل فنية فلا يستطيع دحضها إلا عن طريق خبرة فنية أخرى[1].

الفرع الرابع: عمل الخبير و أساليبه:[2]

يتمثل دور الخبير في إبداء رأيه في المسائل الفنية التي يصعب على القاضي استنتاجها دون المسائل القانونية واستخراج الدليل الرقمي وذلك من خلال إتباع الخطوات التالية:

أولا: مرحلة ما قبل التشغيل والفحص

على الخبير الجنائي في الجرائم الرقمية أن يقوم بوضع نسخة لوسائط التخزين المضبوطة كالأقراص الصلبة للقيام بالفحص المبدئي وحماية الأصل من الفقدان أو التلف وعليه التأكد من صلاحية النظام للتشغيل و مدى مطابقة محتوى الأحراز المضبوطة أثناء التحقيق بما هو مدون عليها كما يقوم بتسجيل محتوى البيانات المضبوطة.....آلخ.

ثانيا: مرحلة التشغيل والفحص

أثناء هذه المرحلة يقوم الخبير باستكمال تسجيل البيانات التي لم يتم ضبطها من خلال قراءة جهاز الحاسب الآلي ويحدد أنواع البرمجيات كبرامج النظام ، برامج التطبيقات و أي من البرامج له علاقة بموضوع الجريمة التي تحقق فيها الصور في جرائم التزييف أو التعديل أو التلاعب، مع إبراز إذا كانت مستندات أو معلومات لها دلالة بموضوع الجريمة كبصمات

[1] صغير يوسف ، المرجع السابق ، ص 91.

[2] معمش زهية وغانم نسيمة ، المرجع السابق ، ص 40

الأصابع في جرائم التزوير و وجود رسائل تهديد في جرائم القتل وغيرها، كما يجب عليه اكتشاف المستندات أو النصوص المخبأة داخل الصور، وأن يقوم بتحويل الدليل الرقمي إلى مكونات مادية بواسطة طباعة الملفات أو تصوير محتواها أو وضعها في وعاء حسب البيانات المكتوبة[1]، ويجب أن يقوم باسترجاع الملفات التي تم محوها عن طريق استخدام أحد برامج إستعادة البيانات بالنسبة للملفات والسجلات المعطلة أو التالفة.

ثالثا: مرحلة تحديد مدى ترابط الدليل المادي والدليل الرقمي

يتم خلال هذه المرحلة فحص الدليل المادي المضبوط مع الدليل المستخرج من جهاز الحاسب الآلي والربط بينها ليصبح الدليل موثوق ويقيني حتى يتسنى قبوله أمام المحكمة.

رابعا: تدوين النتائج و إعداد تقريره

يقوم الخبير بتقديم تقرير موقع منه عما توصل إليه من نتائج وغالبا ما يرفق معه الملاحق الإيضاحية سواء كانت مصورة أو مسجلة، ويقدم الملف إلى جهة التحقيق أو جهة الحكم.

[1] معمش زهية وغانم نسيمة ، المرجع السابق ، ص 40

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 إلى خارج الحدود الوطنية لتشمل دول أخرى وتهدد أمنها واستقرارها وعليه أصبح من الصعب تتبع تحركات هاته الشبكات الإجرامية، مما استدعى المشرع إلى التدخل لمكافحة هذا النوع من الجرائم عن طريق تعديل القانون رقم: 06-22 المؤرخ في: 2006/07/20 المتضمن قانون الإجراءات الجزائية حيث أدخل أساليب البحث و التحري الخاصة التي تقوم بها جهات متخصصة بغية التحري في جرائم خطيرة مقررة في قانون العقوبات، كما استحدث المشرع القانون رقم: 09-04 المؤرخ في: 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

وعليه سوف نتطرق إلى هذه الأساليب من خلال ثلاث مطالب، بحيث يتضمن (المطلب الأول) إعتراض المراسلات و تسجيل الأصوات و التقاط الصور و(المطلب الثاني) مراقبة الاتصالات الالكترونية و(المطلب الثالث) نتناول فيه التسرب.

المطلب الأول: إعتراض المراسلات و تسجيل الأصوات و التقاط الصور

سعيا من المشرع لمكافحة الجرائم الخطيرة و مراقبة نشاطات الشبكات الإجرامية الذين يستعملون تقنيات حديثة تتسم بالسرعة و الفعالية قام بإدخال الوسائل التقنية في مجال البحث و التحري في التحقيقات الجنائية الخاصة بهذه الجرائم، و لقد نظم المشرع الجزائري كل من إعتراض المراسلات و تسجيل الأصوات و التقاط الصور في المواد من 65 مكرر5 إلي غاية 65 مكرر10 ق.إ.ج، بحيث يجوز لضباط الشرطة القضائية و أعوانهم القيام بهذه الأعمال إذا اقتضت ضرورة التحري في الجرائم المتلبس بها و في بعض الجرائم الأخرى عن طريق إذن من وكيل الجمهورية أو قاضي التحقيق.[1]

[1] السوفي نور الهدى، المرجع السابق، ص 42.

وعليه سنتناول هذا المطلب من خلال ثلاث فروع؛ (الفرع الأول) نتطرق فيه إلى تعريف إعتراض المراسلات و(الفرع الثاني) إلى تعريف تسجيل الأصوات وإلتقاط الصور و(الفرع الثالث) ندرس فيه إجراءات و شروط إعتراض المراسلات و تسجيل الأصوات والتقاط الصور.

الفرع الأول: تعريف إعتراض المراسلات

لم ينص قانون الإجراءات الجزائية على تعريف خاص لعملية إعتراض المراسلات بل إكتفى بتنظيمها في المواد المذكورة أعلاه، فقد عرفها الباب الثالث من القانون الفدرالي الأمريكي لسنة 1968 أنها "الإكتساب السمعي عن طريق السمع لمحتويات أية أسلاك أو أية اتصالات شفوية عن طريق إستخدام جهاز إلكتروني أو ميكانيكي أو جهاز آخر، و بصفة عامة فإن أي جهاز يمكن إستعماله لتسجيل الاتصالات يقع ضمن ما يقصده القانون"[1].

وعرفها إجتماع لجنة الخبراء للبرلمان الأروبي بستراسبورغ بتاريخ 2006/10/06 المتعلق بأساليب التحري التقنية وعلاقتها بالأفعال الإرهابية، بأنها "عملية مراقبة سرية للمراسلات السلكية و اللاسلكية وذلك في إطار البحث و التحري عن الجريمة و جمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في إرتكابهم أو في مشاركتهم في إرتكاب الجرائم"[2].

و يقال أيضا "يتمثل في إعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية و يقصد به التصنت التليفوني"[3].

وعرفها القضاء "بالتصنت على المكالمات و هو تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفي لشخص ما مع اللجوء إلى تسجيل المكالمات في أشرطة مغناطيسية"[4].

[1] حمزة قريشي، المرجع السابق، ص36.

[2] لوجاني نور الدين، "أساليب البحث و التحري الخاصة و إجراءاتها"، يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية، إليزي ، 2007/12/12، ص8.

[3] أحسن بوسقيعة، المرجع السابق ، ص113.

[4] مصطفاوي عبد القادر، أساليب البحث و التحري الخاصة و إجراءاتها، مجلة المحكمة العليا، العدد02، 2009 ، ص 70.

و يراد بها أيضا "تلقي أية مراسلة مهما كان نوعها مكتوبة أو مقروءة أو مسموعة وبغض النظر عن وسيلة إرسالها و تلقيها، سواء كانت سلكية أو لاسلكية من غير الشخص الموجه إليه أو الذي أرسلها"[1].

و يمكن القول أنها "إجراء تحقيق يباشر خلسة، وينتهك سرية الأحاديث الخاصة، تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها و يتضمن من ناحية استراق السمع إلى الحديث، و من ناحية أخرى حفظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض"[2].

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 و يخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك[3].

و قد حدد المشرع الجزائري في نص المادة 65 مكرر5 الفقرة 2 ق.إ.ج نوع المراسلات محل الإعتراض وهي المراسلات التي تتم عن طريق وسائل الإتصال السلكية و اللاسلكية.

وبما أن المشرع لم يتطرق إلى مفهوم إعتراض المراسلات فهل كان يقصد بها التنصت الهاتفي[4] فقط واستبعد بذلك الخطابات الخطية التي تتم عن طريق البريد حرصا منه على

---

[1] العدواني عبد الحميد،"إدارة التحريات و التحقيقات الأولية في الجرائم التي تدخل في إختصاص القطب القضائي الجزائي" الملتقى الجهوي حول مكافحة الإجرام الخطير، مجلس قضاء ورقلة، الأربعاء 2009/01/28، ص7.

[2] ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية– دراسة تأصيلية تحليلية و مقارنة للتنصت على المحادثات التليفونية و التي تجري عبر الأنترنات و الأحاديث الشخصية نظريا و علميا– دار المطبوعات الجامعية، الاسكندرية، ط1، 2009، ص 150.

[3] عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية ، دار هومه، الجزائر، بدون طبعة، 2012، ص73.

[4] التنصت :هو الاستماع إلى الأحاديث الخاصة خلسة بواسطة أجهزة مخصصة لذلك. أنظر: أكثر ياسر الأمير فاروق، نفس المرجع ، ص 145.

والتنصت نوعان: تنصت مباشر عن طريق توصيل سماعة الهاتف مباشرة بجهاز التسجيل وربط سلكي هذه السماعة إلى سلكي دائرة المشترك بالمركز الرئيسي للمكالمات الهاتفية و هو طريقة تقليدية يتم كشفها بسهولة . أما التنصت غير المباشر و يكون بالتقاط المحادثات الهاتفية لاسلكيا، أي دون اتصال سلكي بالخط هاتفي بل عن طريق استغلال المجال المغناطيسي المحيط بالسلك أو استخدام أجهزة متطورة مثل directionnel micro و هو جهاز على درجة من الحساسية يسجل المحادثات عن بعد مسافة بعيدة. أنظر أكثر: لوجاني نور الدين، المرجع السابق، ص 13.

ضمان حرية المراسلات بين الأفراد المكفولة دستوريا، أم أن الأمر يمتد إلى هذه المراسلات المتبادلة بالحاسب الآلي لكل من المتهم و الغير ممن يتبادلون معه المراسلات؟ هناك من يرى أن المشرع قصد أساسا التنصت الهاتفي، إذ كثيرا ما تتطلب إجراءات التحري و التحقيق اللجوء إلى مراقبة المحادثات الهاتفية، غير أنه وعلى اعتبار أن وسائل الإتصال الحديثة ساهمت بشكل كبير في تسهيل ارتكاب جرائم منظمة سواء عن طريق المكالمات الهاتفية أو المراسلات الإلكترونية المتبادلة عبر الشبكات المعلوماتية، فقد أجازت إتفاقية بودابست للجرائم الإلكترونية الإعتراض الشرعي لكل أشكال النقل الإلكتروني للبيانات سواء تم عبر التليفون أو الفاكس أو البريد الإلكتروني.... الخ وتشمل الإتصالات محل الإعتراض محتوى غير مشروع أو دليل على الأفعال الإجرامية الخطيرة التي يعرفها القانون الداخلي لكل دولة طرف في الاتفاقية، مما يستوجب ضرورة إعتراض المراسلات الإلكترونية المتبادلة عبر الحاسب الآلي أيضا لدرء خطر الجريمة وملاحقة الجناة، وهذا ربما ما قصده المشرع الجزائري صراحة من خلال اعتراض المراسلات السلكية واللاسلكية[1] وما اتجه إليه من خلال القانون04/09 حيث أجاز وضع الترتيبات التقنية لمراقبة الإتصالات الإلكترونية والقيام بالتفتيش والحجز داخل المنظومة المعلوماتية[2].

و ما اتجه إليه أيضا من خلال القانون 2000-03 المؤرخ في: 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، حيث أجاز اعتراض المراسلات المتبادلة عن طريق التلغراف، الفاكس، البريد الالكتروني(E.mail)، الرسائل القصيرة(sms)

[1] المقصود بالمواصلات السلكية و اللاسلكية طبقا للقانون 03/2000 المؤرخ في: 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية في المادة 08 فقرة 21 أنها " كل تراسل أو إرسال أو استقبال علامات أو إشارات كتابات صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطسية

[2] جميلة محلق، إعتراض المراسلات، تسجيل الأصوات، التقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد و الإدارة و القانون، جامعة باجي مختار عنابة، العدد 42 ، جوان 2015، ص178.

عن طريق الهاتف المحمول، الاتصالات المرئية....الخ، و إذا كان الحال كذلك فكل إشارة أو كتابة أو صورة مطلوب التقاطها أو مكالمة هاتفية يجوز أن تكون محل للاعتراض[1].

وعليه يمكن أن نقول وجب أن يتضمن أسلوب إعتراض المراسلات خصائص معينة هي التي تساعد في تحديد مضمونه و طبيعة العمل به و تتمثل في:

-أن يتم خلسة دون علم و رضا صاحب الشأن.

-يمس بالحق الشخصي في سرية الحديث.

-يستهدف الحصول على دليل غير مادي لأن الأحاديث و الأقاويل غير مادية.

-يستخدم فيه أجهزة قادرة على التقاط الأحاديث خاصة مع تطور التكنولوجيا أصبح هناك أجهزة مختلفة الأحجام و الأشكال[2].

الفرع الثاني : تسجيل الأصوات و التقاط الصور

لم يقدم المشرع تعريفا صريحا لتسجيل الأصوات و التقاط الصور، و بالرجوع إلى المادة 65 مكرر5 ق.إ.ج نستشف أن المقصود من تسجيل الأصوات هو "وضع الترتيبات التقنية دون موافقة المعنيين من أجل إلتقاط و تثبيت و بث و تسجيل الكلام المتفوه بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية"[3].

ويقصد به كذلك "حفظ الحديث على جهاز معد لذلك بهدف الاستماع إليه مرة أخرى"[4]. و التسجيل الصوتي الذي يهمنا في هذه الدراسة هو الذي يجريه رجال الضبطية القضائية من أجل التحري و التحقيق عن الجرائم الخطيرة السابقة الذكر.

[1] لوجاني نور الدين، المرجع السابق ، ص12.

[2] ياسر الأمير فاروق، المرجع السابق، ص151.

[3] احسن بوسقيعة، المرجع السابق، ص 113.

[4] نقادي عبد الحفيظ،" التسجيل الصوتي" المجلة الجزائرية للعلوم القانونية و الاقتصادية، كلية الحقوق الجزائر، العدد01، 2009 ، ص312.

و يمكن القول أنه "تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان خاص أو عام"[1].

أما التقاط الصور فنفس الأمر كذلك، لم يعرف المشرع الجزائري هذه العملية صراحة و قد أشار إليها "بالالتقاط، وهناك من عرفها أنها "تلك العملية التقنية التي تتم دون موافقة المعنيين من أجل التقاط صور لشخص أو عدة أشخاص وإن تواجدوا في مكان خاص"[2].

و يمكننا أن نعرف تسجيل الأصوات و التقاط الصور بأنها تسجيل المحادثات الشفوية بين الأفراد بصفة سرية أو خاصة في مكان عام أو خاص و كذلك التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص[3].

و تجدر الإشارة أن المشرع عندما جمع بين إعتراض المراسلات وتسجيل الأصوات 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[4].

الفرع الثالث : إجراءات و شروط إعتراض المراسلات و تسجيل الأصوات والتقاط الصور

حق الإنسان في الخصوصية وأن يعيش حياة هادئة من المبادئ القدسية التي كرسها الدستور في المادة 39 منه، إلا أن المشرع الجزائري ولضرورة التحقيق في بعض الجرائم الحساسة سمح بالقيام بمثل هذه العمليات،بحيث تكون مصلحة التحقيق و كشف المجرمين أولى بالرعاية من الحفاظ على أسرار الحياة الخاصة، وذلك من خلال المواد من 65 مكرر5 إلى غاية 65 مكرر10 ق.إ.ج حيث أتاح للضبطية القضائية حق إستعمال الأساليب و الوسائل التقنية في إطار البحث و التحري في الجرائم المستحدثة و لكن وفقا للشروط و الإجراءات التالية:

[1] جميلة محلق، المرجع السابق ، ص178.

[2] لوجاني نور الدين، المرجع السابق، ص 8.

[3] عبد الرحمان خلفي، المرجع السابق، ص 73.

[4] عباسي خولة، الوسائل الحديثة للإثبات في القانون الجنائي، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة، 2014، ص 42.

1- طبيعة الجريمة: بالرجوع إلى نص المادة 65 مكرر5 ق.إ.ج، تكون إجراءات التحري الخاصة في حالة التلبس أو التحقيق الإبتدائي في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، الجرائم الإرهابية، جرائم الصرف والفساد وإذا اكتشفت أثناء التحريات الخاصة جرائم أخرى غير مذكورة غي الإذن، فهذا لا يكون سببا لبطلان الإجراءات العارضة وفقا لأحكام المادة 65 مكرر2/6 ق.إ.ج[1].

2- الإذن من وكيل الجمهورية أو قاضي التحقيق: وهو شرط أساسي لمباشرة عمليات إعتراض المراسلات و تسجيل الأصوات و التقاط الصور، و يشترط لصحته ما يلي:

_ أن يكون مكتوبا و هذا كمبدأ عام من الأعمال المخولة للضبطية القضائية حسب نص المادة 18 ق.إ.ج[2].

_ أن يتضمن جميع المعلومات المكونة للجريمة و التي تسمح لوكيل الجمهورية أو لقاضي التحقيق بالتعرف على الإتصالات المطلوب إلتقاطها و الأماكن المقصودة من ذلك.

_ تحديد المدة الزمنية للعملية بأربعة أشهر قابلة للتجديد حسب مقتضيات التحري[3].

3- الرقابة القضائية: يجب خضوع هذه العمليات المسموح بها قانونا إلى رقابة وإشراف وكيل الجمهورية المختص ، كما أنه في حالة فتح تحقيق قضائي فإن هذه العمليات تكون بإذن من قاضي التحقيق وتحت رقابته[4].

[1] بن كثير بن عيسى، الإجراءات الخاصة المطبقة على الإجرام الخطير نشرة القضاة، مديرية الدراسات القانونية و الوثائق، العدد 63، ص 89.

[2] المادة 1/18 قانون الإجراءات الجزائية " يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم و أن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنايات أو الجنح التي تصل إلى علمهم"

[3] فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، كلية الحقوق والعلوم السياسية جامعة منتوري قسنطينة الجزائر، العدد 33 ، 2010، ص 241

[4] مصطفاوي عبد القادر، المرجع السابق، ص 74.

4- وضع الترتيبات التقنية: بعد الحصول على الإذن يسمح لضباط الشرطة القضائية بوضع الترتيبات التقنية في الأماكن الخاصة و العمومية و غيرها دون موافقة وعلم الأشخاص المعنيين و هذا للمحافظة على سرية العملية[1]، كما أجاز المشرع أن تكون هذه الترتيبات خارج الميقات القانوني، أي خارج المواعيد المحددة في نص المادة 47 ق.إ.ج.

5- الإطار المكاني للأساليب التقنية في التحري عن الجرائم: بالرجوع إلى المادة 65 مكرر 5 ق.إ.ج نجدها نصت على الأماكن التي يتم فيها إستعمال الوسائل التقنية وهي الأماكن العمومية، الأماكن الخاصة، المحلات السكنية[2].

6- المحافظة على السر المهني: يلزم على الضبطية القضائية أثناء أداء مهامهم أو وظيفتهم بكتمان السر المهني الذي اطلعوا عليه، سواء كان عن طريق تسجيل الأصوات أو التقاط الصور، خاصة إذا تعلق الأمر بأماكن يشغلها أشخاص ملزمون بكتمان السر المهني مثل مكاتب المحامين أو الموثقين[3]، أو إذا تعلق الأمر بأشخاص يحملون أسرار مهنية مثل القضاة، الأطباء.... الخ فحتمية عدم إستثناء هذه الأماكن من إجراء الإعتراض يستوجب اتخاذ التدابير اللازمة لضمان إحترام السر المهني الذي يخصها.

7- تسخير الأعوان المؤهلين و المكلفين بالمواصلات السلكية واللاسلكية: أجاز المشرع لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له باستعمال الوسائل الخاصة في البحث و التحري و لقاضي التحقيق أو ضباط الشرطة القضائية الذي ينوبه أن يكلف عون مؤهل وصاحب خبرة وكفاءة في مجال المواصلات السلكية واللاسلكية بالتكفل بالجوانب التقنية

[1] لوجاني نور الدين، المرجع السابق،ص 12

[2] الأماكن العامة : وهي التي يتم الدخول إليها و الخروج منها بحرية تامة كالأسواق – الأماكن الخاصة : هي الأماكن أو المحلات المعدة لنشاطات معينة كالفنادق و العيادات . المحلات السكنية: عرفتها المادة 355 من قانون العقوبات أنظر أكثر لوجاني نور الدين، نفس المرجع ، ص 9.

[3] براهيمي جمال، المرجع السابق، ص 141.

لعمليات إعتراض المراسلات وتسجيل الأصوات و هذا ما جاء في نص المادة 65 مكرر 8 ق.إ.ج [1].

8- تحرير محضر عن العملية: كمبدأ عام يجب على ضباط الشرطة القضائية تدوين وتحرير تقارير عن كل عملية، تطبيقا لنص المادة 65 مكرر 9 ق.إ.ج التي جاء فيها أنه يجب تحرير محضر يذكر فيه جميع تفاصيل العملية من بدايتها إلى نهايتها، و كذلك يذكر فيه تاريخ وساعة بداية العملية و تاريخ الانتهاء منها[2].

أما بخصوص نتائج التحريات التي تتعلق بمضمون المراسلات المسجلة و الصور الملتقطة فعلى المأذون له بهاته العملية أو المناب أن ينسخ أو يصف المحتوى الضروري والمهم لإظهار الحقيقة في محضر ليودع بالملف، أما إذا كانت المكالمات باللغة الأجنبية فإنه يتم الإستعانة بمترجم لترجمة محتوى المكالمات و نسخها[3].

9- ضبط التسجيلات ووضعها في أحراز: بما أن التسجيلات أو الأشرطة المصورة تعتبر أدلة إثبات مادية أصلية تقتضي الشرعية الإجرائية حفظها بطريقة خاصة و ذلك بوضعها في أحراز مختمة بما يضمن عدم التلاعب بها أو العبث في الحديث المسجل سواء بالحذف أو الإضافة و ضمها إلى المحضر، و هذا ما نستنتجه من خلال إستقراء نصوص المواد 18 و45 ق.إ.ج، و تجدر الإشارة هنا إلى أن المشرع الجزائري لم يشر إلى عرض هذه التسجيلات و الصور على المشتبه فيهم في مرحلة جمع التسجيلات، ويرجع ذلك إلى الطابع السري الذي تتميز به هذه الجرائم الخطيرة[4]، على عكس ما نجده في المادة 42 من نفس القانون حيث أوجب عرض الأشياء المضبوطة على المشتبه فيهم لتميزها بطابع العلنية.

[1] أنظر المادة 65 مكرر 8 من قانون الإجراءات الجزائية.

[2] عبد لله أوهايبة، شرح قانون الإجراءات الجزائية الجزائري، دار هومه للطباعة و النشر ، الجزائر، ط2، 2011، ص 280.

[3] أنظر المواد 65 مكرر 9 و 65 مكرر 10 ق.إ.ج.

[4] لوجاني نور الدين، المرجع السابق، ص 13.

المطلب الثاني : مراقبة الاتصالات الالكترونية

أكد المشرع الدستوري الجزائري على الحماية القانونية للحياة الخاصة للأفراد ، حيث لا يجوز إنتهاك حرمة المواطن و حرمة شرفه و سرية مراسلاته و إتصالاته الخاصة بأي شكل من الأشكال، و لكن نظرا للظروف الأمنية التي يعيشها المجتمع الدولي و خاصة مع تطور التكنولوجي الذي سهل عمل الشبكات الإجرامية، و حفاظا منه على الأمن العام و النظام العام تدخل المشرع عن طريق القانون 04/09 السالف الذكر و سمح بصفة إستثنائية للسلطات القضائية و في إطار قرار معلل بمراقبة الاتصالات الالكترونية.

وعليه سوف نتطرق من خلال هذا المطلب إلى مفهوم مراقبة الاتصالات الالكترونية (الفرع الأول) ونتطرق إلى حالات اللجوء إلى المراقبة الالكترونية (الفرع الثاني) ونعرج إلى الضمانات المقررة لتنفيذ مراقبة الإتصالات الالكترونية (الفرع الثالث).

الفرع الأول: مفهوم مراقبة الاتصالات الالكترونية

لم يتطرق المشرع الجزائري إلى تعريف مراقبة الإتصالات الالكترونية، بل إكتفى فقط بتحديد مفهوم الاتصالات الالكترونية.

أولا: تعريف المراقبة

1- لغة: "المراقبة تعني الملاحظة، فراقب الشئ حرصه أو رصده، و الرقيب هو الحارس أو الحافظ و المرقب آلة لرصد الفلك".

2- إصطلاحا: "المراقبة هي وضع الشخص أو وسائل نقل، أو أماكن أو مواد بصورة سرية تحت رقابة سرية أو دورية بهدف الحصول على معلومات خاصة بالنشاط، أو كشف شخصية الأفراد، و هي تفيد في منع إتمام الجريمة و جمع الأدلة عنها و التأكد من صحة المعلومات، ثم الحصول عليها بالفعل"[1].

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

ثانيا: تعريف الإتصالات الإلكترونية: عرفها المشرع الجزائري بموجب الفقرة (و) من المادة 02 من القانون 09-04 السالف الذكر على أنها «أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية».

وتعرف الإتصالات الإلكترونية في الفقه المقارن بأنها "الإتصالات التي تتم عن طريق جهاز الحاسب الآلي، والتي تتخذ شكل البريد الإلكتروني(E.mail)[1] أو شكل محادثة فورية (Instant message) والتي تتم عن طريق شبكة الأنترنت"[2].

وعليه يمكن تعريف مراقبة الإتصالات الإلكترونية أنها "عملية تتمثل في ترصد الرسائل الإلكترونية و إجراء فحوصات تقنية لها و ذلك بغية الوصول إلى مصدرها و معرفة صاحبها"[3]

الفرع الثاني: حالات اللجوء إلى المراقبة الإلكترونية

بعد إستقراء المادة 04 من القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها نجدها تتضمن حالات تطبيق الإجراء الجديد المتمثل في مراقبة الإتصالات الإلكترونية وقد جاءت على سبيل الحصر وهي كالآتي:

أولا: الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة: المراقبة الوقائية كأصل عام لا تطبق على المتابعة القضائية لجريمة مرتكبة وإنما تختص بكشف أي خطر أو تهديد لأمن الدولة بحيث تهدف إلى البحث عن أي معلومة سياسية أو إقتصادية أو عمومية أو عسكرية من شأنها أن تمس باستقرار الدولة، و الشخص الذي يخضع لهذا الإجراء التقني لا يعتبر متهم أو مشتبه فيه طبقا لأحكام قانون العقوبات، و لكن نشاطه يمكن أن يشكل خطرا على الأمن الوطني، لأن هذه الجرائم لم ترتكب و لكن المشرع سمح في إطار الوقاية منها بإجراء عملية مراقبة الإتصالات الإلكترونية لأشخاص أو مجموعات يحتمل توريطهم مستقبلا في القيام بأعمال إرهابية أو تخريبيه أو جرائم تمس بأمن

[1] يعرف بأنه إرسال و استقبال الرسائل الالكترونية عن طريق شبكة الانترنت

[2] ثابت دنيازاد، المرجع السابق، ص 207.

[3] قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة مكملة لنيل شهادة الماستر أكاديمي في القانون، تخصص قانون عام للأعمال، جامعة قاصدي مرباح ورقلة، 2014، ص56.

الدولة، ولا يشترط توافر أدلة قوية ضدهم بل يكفي فقط مجرد الشك في إمكانية ارتكابهم تلك الأفعال، و يتخذ هذا الإجراء خدمة للصالح العام للدولة و المواطن معا من جرائم محتملة الوقوع.

ثانيا: في حالة توافر معلومات تدل على احتمال وقوع إعتداء على منظومة حاسوبية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني: إن اكتشاف الجريمة قبل وقوعها و خاصة في الجرائم الإلكترونية يعتبر إحتمال ضئيل لأن هذه الجرائم يصعب اكتشافها و عادة ما يكون ذلك صدفة أو عن طريق تحريات في جرائم أخرى، وعليه يعتبر وفي إطار الوقاية من الجرائم الرقمية أن مجرد توافر معلومات عن إحتمال وقوع إعتداء على منظومة معلوماتية تمس بالمصالح السابقة الذكر يجعل من إجراء المراقبة الإلكترونية فعلا مشروعا.

ثالثا: لمقتضيات التحريات و التحقيقات القضائية: في حالة صعوبة الوصول إلى نتيجة تفيد التحقيقات والأبحاث الجارية دون اللجوء إلى مراقبة الإتصالات الإلكترونية، و يعتبر إجراء قضائي لأنه يتم في مرحلة البحث والتقصي عن الدليل ويمكن أن يطبق على كافة جرائم القانون العام بشرط أن تكون هناك صعوبة في الحصول على نتيجة تهم التحقيق دون اللجوء إلى المراقبة الإلكترونية[1].

رابعا: في إطار تنفيذ طلبات المساعدة القضائية الدولية: تتعلق بالجرائم التي ترتكب خارج الإقليم الوطني، بحيث من شأن مراقبة الإتصالات في التراب الوطني أن تفيد الدول المعنية بنتائج تتعلق بمعاينة الجرائم الماسة بتكنولوجيات الإعلام والإتصال وتقديم المعلومات الضرورية عن مكان تواجد مرتكبي هذه الجرائم و يكون ذلك في إطار الإتفاقيات الدولية و مبدأ المعاملة بالمثل[2] هذا ما أشارت إليه المادة 4/11 من المرسوم الرئاسي 261/15[3].

[1] جبار فطيمه، المرجع السابق، ص 18.

[2] ثابت دنيازاد، المرجع السابق، ص 211.

[3] أنظر المادة 4/11 من المرسوم الرئاسي 15-621 .

الفرع الثالث: الضمانات المقررة لتنفيذ مراقبة الاتصالات الالكترونية

ويتم تنفيذ عملية مراقبة الاتصالات الالكترونية عن طريق اتخاذ بعض الإجراءات وتتمثل في:

أولا: سرية الإجراءات: و تتم هذه العملية بسرية تامة أي دون علم و رضا المشبه فيهم، وكذلك يخضع الموظفون الذين يدعون إلى الاطلاع على معلومات سرية إلى أداء اليمين أمام المجلس القضائي قبل تنصيبهم و هم ملزمون بكتمان السر المهني[1].

ثانيا: التسخير: حيث يجوز لوكيل الجمهورية أو قاضي التحقيق أو لضابط الشرطة القضائية أن يسخر عون مؤهل لدى هيئة مكلفة بالاتصالات سواء كانت عامة أو خاصة للقيام بهذا الإجراء، كما يمكنه طلب المساعدة من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته لأن من مهام هذه الهيئة تقديم المساعدة للسلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال[2].

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 و وضع التدابير التقنية لمراقبة الاتصالات الالكترونية و ما أسفرت عنه من نتائج، كما يجب أن يذكر فيه تاريخ و ساعة بداية هذه العمليات و الإنتهاء منها و جميع الشروط الشكلية العامة في جميع المحاضر[3].

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

[2] جبار فطيمة، المرجع السابق، ص 19.

[3] ثابت دنيازاد,، المرجع السابق، ص 219.

رابعا: حماية المعطيات المتحصل عليها: نصت المادة 09 من القانون 09-04 السالف الذكر أنه لا يجوز استعمال المعطيات المتحصل عليها من عملية المراقبة إلا في الحدود الضرورية للتحقيقات القضائية و هو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار[1].

خامسا: الإذن: أشار المشرع الجزائري في نص المادة 04 من القانون 09-04 أنه في حالة ما إذا تعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو التخريب أو الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحته إذن لمدة 06 أشهر قابلة للجديد، وذلك بموجب تقرير يوضح و يبين فيه طبيعة الترتيبات التقنية المستعملة و الأغراض الموجة لها.

أما في غير هذه الجرائم الثلاث فانه يتم الأخذ بالقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، و هي صدور الإذن من وكيل الجمهورية أو قاضي التحقيق كل حسب اختصاصه، بهدف إعتراض المراسلات مع تحديد العناصر المهمة في الإذن و يسلم مكتوبا لمدة 04 أشهر قابلة للتجديد عند الضرورة[2].

سادسا: عدم المساس بالحرية الشخصية للفرد: بحيث ضابط الشرطة القضائية ملزم بالإجراءات التي وضعها القانون لحماية حقوق الأفراد و حرياتهم الشخصية، كما هو ملزم بالتقيد بالإذن المقدم له من قبل السلطة القضائية المختصة، وأي خروج على مضمون الإذن يترتب عليه مساس بالحرية الشخصية الذي يعرض ضابط الشرطة القضائية إلى العقوبة[3].

وتجدر الإشارة في الأخير أن المشرع الجزائري قد وضع إجراء مراقبة الاتصالات الالكترونية تحت سلطة القضاء، و ذلك ضمانة لعدم المساس بحريات الأفراد و الحياة الخاصة بهم، باعتبار أن القاضي يهدف إلى الموازنة بين ضرورات التحقيق و إلزامية حماية الأفراد

[1] أنظر المادة 9 من القانون 09-04.

[2] جبار فطيمة، المرجع السابق، ص 19.

[3] أنظر المادة 107 من قانون العقوبات.

المشتبه فيهم، لأن مجرد الاشتباه لا يجعل من الفرد مجرما و هذا ما يطلق عليه بضمانات المحاكمة العادلة.

المطلب الثالث: التسرب

لقد أدرك المشرع أن المواجهة الفعالة للجرائم الإلكترونية لا تكون فقط بإرساء قواعد قانونية ذات طبيعة ردعية، بل لابد من مصاحبة هذه الأخيرة قواعد قانونية إجرائية وقائية من شأنها أن تتفادى وقوع هذا النوع من الجرائم، وقد استدرك هذا الموقف عن طريق تقنين عملية التسرب في القانون 06-22 في الفصل الخامس من الباب الثاني للكتاب الأول من قانون الإجراءات الجزائية، حيث استحدث هذه العملية في البحث و التحري عن جرائم معينة ومنها الجريمة الإلكترونية.

وعليه سوف نتطرق في هذا المطلب إلى تعريف التسرب (الفرع الأول) و تنظيم عملية التسرب (الفرع الثاني) وإلى الإطار الزماني و المكاني لعملية التسرب في (الفرع الثالث) ثم الآثار المترتبة عن عملية التسرب و بطلان إجراءاته (الفرع الرابع).

الفرع الأول: تعريف التسرب

يعتبر التسرب تقنية جديدة من تقنيات التحري الخاصة يقوم بها ضابط أو عون الشرطة القضائية وهي من أخطر العمليات و أصعبها وسوف نتطرق إلى تعريف التسرب من خلال النقاط التالية:

أولا: التعريف اللغوي للتسرب

تسرب: تسربا (سرب) من الماء، دخل في البلاد: دخلها خفية كقولك "تسرب الجواسيس"[1]

و تعني كلمة التسرب بالفرنسية INFILTRATION

[1] المنجد للغة و الأعلام، دار المشرق، لبنان، طبعة 27 ، 1986، ص 329.

ثانيا: التعريف القانوني للتسرب

عرفه المشرع في المادة 65 مكرر12 ق.إ.ج على أنه "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

وأطلق عليه الإختراق أيضا في القانون رقم:06/01 المتعلق بالوقاية من الفساد و مكافحته في نص المادة 56 منه.

وعرفه المشرع الفرنسي في نص المادة: 81_706 الفقرة الثانية من قانون الإجراءات الجزائية الفرنسي على أنه: يقوم بالتسرب ضابط أو عون الشرطة القضائية يخول خصيصا بموجب شروط محددة قانونا ويتصرف تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة ويظهر أمامهم كأنه فاعل أو شريك أو خاف[1]، من خلال هذا نلاحظ أن المشرع الجزائري أخذ نفس التعريف الوارد في التشريع الفرنسي.

ثالثا: التعريف العملي للتسرب

يمكن تعريف التسرب أنه " تقنية من تقنيات التحري و التحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية و ذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم و كشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقة و تقديم المتسرب لنفسه على أنه فاعل أو شريك أو خاف"[2]، و عليه يعتبر التسرب من أخطر طرق التحري و جمع المعلومات ويقوم بها الضباط أو الأعوان أصحاب الخبرة والكفاءة و يستخدم فيها أساليب التنكر والإحتيال لكسب ثقة المشتبه فيهم و إيهامهم بأنه فاعل معهم أو شريك و تقديم المساعدة لهم، بقصد تحديد طبيعة و مدى

[1] « L'infiltration consiste، pour un officier ou un agent de police judiciaire spécialement habilite dans des condition fixées par décret et agissant sous la responsabilité d'un officier de judiciaire charge de coordonner l'opération ،a surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer، auprès de ces personnes comme un de leurs coauteurs complices ou receleurs. »

[2] لوجاني نور الدين، المرجع السابق، ص 15.

النشاط الإجرامي في الجرائم المذكورة حصريا في المادة 65 مكرر5 ق.إ.ج وهي جرائم المخدرات، والجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبيض الأموال والإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد، بإذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية وتحت رقابته، فالمشرع وضع قواعد و ضوابط تكفل نجاح و سلامة هذه العملية من خلال تقنين نصوص قانون الإجراءات الجزائية.

الفرع الثاني : تنظيم عملية التسرب

نظم المشرع عملية التسرب في المواد من 65 مكرر11 إلى غاية 65 مكرر18 ق.إ.ج، و وضع شروط شكلية وموضوعية تضمن نجاح عملية التسرب وهذا ما سنتطرق إليه بالتفصيل في هذا الفرع، كما سنشير أيضا إلى خصوصية التسرب في الجريمة الالكترونية.

أولا : الشروط الشكلية للتسرب

بالنظر إلى ما تتطلبه عملية التسرب من دقة و حذر، بسبب خطورتها على حياة المتسرب وجب توافر شروط شكلية تضمن صحة و مشروعية هذا الإجراء و هي كالتالي:

1- تحرير تقرير من طرف ضابط الشرطة القضائية: بالرجوع إلى المادة 65 مكرر13 ق.إ.ج والتي تنص على «يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب و كذا الأشخاص المسخرين طبقا للمادة 65 مكرر14 أدناه»، وعليه قبل مباشرة عملية التسرب وجب على ضباط الشرطة القضائية كتابة تقرير إلى وكيل الجمهورية، وهذا كمبدأ عام على أعمال الشرطة القضائية ويجب أن يتضمن التقرير العناصر التالية[1]:

أ **_طبيعة الجريمة:** طبقا لنص المادة 65 مكرر5 ق.إ.ج، يمكن لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته بمباشرة عملية التسرب إذا اقتضت

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

ضرورات التحقيق في الجريمة المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات، أو الجريمة المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أو الجرائم المتعلقة بالتشريع الخاص بالصرف، أو جرائم الفساد.

ب _السبب وراء إجراء عملية التسرب: يجب على ضابط الشرطة القضائية أن يذكر سبب ودواعي اللجوء إلى عملية التسرب، وغالبا ما يكون السبب مرتبط بضرورة التعمق في البحث والتحري في هذا النوع من الجرائم.

ج _تحديد عناصر الجريمة: بمعنى ذكر كل المعلومات المتعلقة بالجريمة و العناصر المكونة لها، فيتضمن التقرير هوية المشتبه فيهم من أسمائهم و ألقابهم ...الخ و الوسائل المستعملة في الجريمة من مركبات أو أماكن مرتاده، أي 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، فيجب عليه أن يذكر في تقريره جميع البيانات المتعلقة بهويته من الإسم واللقب و الرتبة و المصلحة[1].

2 _طلب الإذن بمباشرة التسرب: الإذن هو محرر رسمي صادر عن هيئة مختصة متمثلة في وكيل الجمهورية أو قاضي التحقيق، مسلم إلى ضابط الشرطة القضائية، وهو إجراء شكلي اشترطه المشرع طبقا لنص المادة 65 مكرر 15[2]، ونشير أن وكيل الجمهورية هو المسؤول الأول عن تقدم رخصة الإذن بصفته الممثل الأول للنيابة العامة، أو قاضي التحقيق بعد إخطار النيابة العامة و تكون العلاقة بين قاضي التحقيق و الضبطية القضائية في إطار التحقيق ضمن إنابة قضائية من طرف قاضي التحقيق إلى ضابط الشرطة القضائية[3].

و وجب توافر جملة من الشروط في الإذن وهي :

[1] مهدي شمس الدين، النظام القانوني للتسرب في القانون الجزائري، مذكرة مكملة لنيل شهادة الماستر في الحقوق قانون جنائي، جامعة محمد خيضر بسكرة، 2014، ص 65.

[2] حمزة قريشي، المرجع السابق، ص 123.

[3] بوطبة روميصاء، المرجع السابق، ص30.

- الكتابة : يجب أن يكون الإذن مكتوبا وإلا يقع تحت طائلة البطلان.
- التسبيب : أي ذكر مبررات اللجوء إلى هذا الإجراء و يترتب على تخلفه أيضا البطلان.
- ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء: يمنح الإذن للتعمق في البحث والتحري في الجرائم المنصوص عليها في المادة 65 مكرر5 السالفة الذكر.
- ذكر هوية ضباط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته: من إسم ولقب، الرتبة و المصلحة التابع لها....الخ.
- المدة الزمنية للتسرب: تقدر مدة التسرب بأربعة أشهر طبقا للمادة 65 مكرر5 ق.إ.ج، ويجب تحديد بداية و نهاية العملية، ويجوز للقاضي المختص تمديد المدة بحسب مقتضيات التحري أو التحقيق كما يجوز له أن يأمر بوقفها في أي وقت قبل انقضاء المدة المحددة قانونا، و تودع الرخصة في ملف الإجراءات بعد الإنتهاء من عملية التسرب[1].

وفي حالة ما إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب ولم يتم تمديدها، يجوز للعون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر14 ق.إ.ج من اقتفاء أو حيازة أو نقل أو تسليم أو إعطاء أموال أو منتجات أو وثائق أو معلومات متحصل عليها ...الخ، و إعطائه الوقت الكافي لتوقيف عمليات المراقبة في ظروف تضمن سلامته و أمنه دون أن يكون مسؤولا جزائيا، على أن لا يتجاوز ذلك مدة أربعة أشهر[2]، و في حالة إنقضاء هذه المدة دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف ملائمة تضمن سلامته، يمكن للقاضي أن يأمر بتمديدها أربعة أشهر على الأكثر[3].

ثانيا: الشروط الموضوعية للتسرب

ولابد لإتمام عملية التسرب توافر بعض الشروط الموضوعية و تتمثل في:

[1] فوزي عمارة، المرجع السابق، ص 248 و 249.

[2] عبد الرحمان كوداد، عملية التسرب على ضوء التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق تخصص علم إجرام، جامعة الطاهر مولاي سعيدة، 2017، ص 75.

[3] أنظر المادة 65 مكرر17 من قانون الإجراءات الجزائية

1- السلطة المختصة بمباشرة عملية التسرب: بالرجوع إلى نص المادة 65 مكرر12 ق.إ.ج يتضح أن المختص بإجراء عملية التسرب هو ضابط الشرطة القضائية المكلف بتنسيق العملية و مسؤولا عنها، و يقوم بالتحضير و التنظيم المحكم لها، و يتولى تنفيذ هذه العملية ضابط آخر أو عون شرطة قضائية ويعرف بالعون المتسرب، فالضابط يكون بمثابة همزة وصل بين المتسرب الذي كلفه الضابط بالعملية و قاضي التحقيق[1]، غير أن هذا الإجراء لا تكون له في مرحلة التحقيق أية قيمة قانونية إذا لم يكن تحت رقابة قاضي التحقيق، فبهذه الرقابة يصبغ الإجراء بطابع إجراءات التحقيق.

وعليه نستطيع القول أن عملية التسرب تقوم بوجود العون المتسرب الذي يقوم بتنفيذ العملية والضابط المنسق الذي يسهر على التنسيق بين المتسرب و الجهة الآذنة بالتسرب.

2- دوافع إجراء عملية التسرب: بما أن التسرب ينصب على جناية أو جنحة متعلقة بالجرائم المنصوص عليها في المادة 65 مكرر5 ق.إ.ج، فإنه يجب أن يكون هو الإجراء الوحيد أو الأنسب الذي يمكن بواسطته إظهار الحقيقة بعد أن أثبتت الإجراءات الأخرى عدم نجاعتها، فالمشرع الجزائري أجاز لوكيل الجمهورية أو قاضي التحقيق أن يأذن للقيام بعملية التسرب شريطة أن تقتضي ضرورات التحقيق والتحري ذلك، لأن التسرب أجيز لعملية معينة و لغرض خاص و بصفة إستثنائية، فتخلف هذه الأسباب يمنع القاضي من الإذن به، وإلا عد تعسفا فالتسرب الذي لا يلتمس من ورائه فائدة إظهار الحقيقة يعتبر تسربا تحكميا[2].

3- السرية لعملية التسرب: تعتبر السرية شرط أساسي لنجاح عملية التسرب وذلك حماية للشخص المتسرب و المصلحة العامة ومنه الوصول إلى كشف الحقيقة، ولم يكتفي المشرع بعدم علانية التحقيق وإنما فرض عقوبات جزائية على كل من يكشف هوية ضابط أو عون شرطة قضائية[3].

---

[1] فوزي عمارة، نفس المرجع، ص 246.

[2] نفس المرجع ، ص 247 .

[3] انظر المادة 65 مكرر16 من قانون الإجراءات الجزائية.

ثالثا: طرق التسرب في مجال الجريمة الرقمية

يمكن تصور عملية التسرب في مجال الجريمة الرقمية عند دخول ضابط الشرطة القضائية أو العون إلى العالم الإفتراضي و ذلك باختراقه لمواقع معينة أو مشبوهة و فتح ثغرات إلكترونية فيها في شكل إرسال فيروسات صديقة في بعض المواقع أو الصفحات التي تكون مشبوهة أو محل مراقبة، أو عن طريق إشتراكه في محادثات غرف الدردشة أو مواقع التواصل الاجتماعي facebook، حيث يتصل مباشرة مع المشتبه فيهم و الظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك أسماء أو صفات و هيآت مستعارة ووهمية سعيا منه للإستفادة منهم حول كيفية إقتحام الهاكر للموقع[1].

الفرع الثالث : الإطار الزماني و المكاني لعملية التسرب

نظرا لأن صفة العون المتسرب مخفية و هويته مستعارة حيث لا يتحرك بصفته الأصلية كضابط أو عون شرطة قضائية فإن المشرع لم يحدد له حيزا مكانيا يتحرك فيه، بل خول له الدخول إلى جميع الأماكن الخاصة بصفته المستعارة التي تترك له الحرية لدخول كل الأماكن التي تساعد في الكشف عن الحقيقة دون أن يترتب عن ذلك مسؤولية جزائية، كما لم يقيد المتسرب بحيز زمني معين يتحرك فيه، لأن ضرورات التحقيق تبرر عملياته طوال ساعات الليل و النهار، ومنه في عملية التسرب تسقط كل الحواجز الزمانية و المكانية المقررة في ظل قانون الإجراءات الجزائية[2].

الفرع الرابع: الآثار المترتبة عن عملية التسرب و بطلان إجراءاته

أولا: الآثار المترتبة عن عملية التسرب

بما أن العون المتسرب يعمل بهوية مستعارة، فمن البديهي أن يترتب عن ذلك آثار نذكر منها ما يلي:

[1] سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية و الإدارية، تخصص علوم جنائية، جامعة الحاج لخضر باتنة، 2013، ص177.

[2] أنظر المادة 65 مكرر 5 /4 ق.إ.ج.

1- أن يقوم ضابط الشرطة القضائية المنتدب و باعتباره المسؤول عن عملية التسرب بتحرير تقرير حول العملية ثم يحيلها إلى قاضي التحقيق على أساس أنه المنسق بين هذا الأخير والعون المتسرب.

وبالرجوع إلى النصوص القانونية التي تنظم عملية التسرب نلاحظ أن المشرع لم يشر إلى مصير الأشياء المتحصل عليها نتيجة عملية التسرب ولا إلى موقف القانون من الجرائم التي تم إكتشافها عرضا أثناء عملية التسرب، و كذلك لم يشر إلى إمكانية الطعن بالنقض في الإذن بالتسرب عن طريق الاستئناف[1].

2- بعد الانتهاء من عملية التسرب يتم سماع ضابط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته و بالتنسيق معه دون سواه كشاهد عن العملية، و هذا من باب الحماية غير المباشرة للعون المتسرب[2].

3- توفير الحماية للعون المتسرب من أي خطر قد يتعرض له أو يمتد إلى أفراد عائلته بعد العملية، وذلك من خلال فرض عقوبات نص عليها في المادة 65 مكرر16 ق.إ.ج التي تعاقب كل شخص يكشف الهوية الحقيقة للعون المتسرب[3].

4- إنعدام المسؤولية الجزائية للعون المتسرب عن بعض الأفعال المجرمة سواء من إقتفاء أو حيازة أو نقل و غيره من الأفعال التي نصت عليها المادة 65 مكرر14 ق.إ.ج[4]، وعليه عند اقتراف العون المتسرب هذه المخالفات أثناء عملية التسرب تعفيه من المسؤولية الجزائية لأنها أفعال مبررة قانونا[5].

غير أن المشرع لم يوضح القيمة الثبوتية لتصريحات المتسرب عن طريق المسؤول عن العملية بحث هل يمكن إعتبارها استدلالات أو شهادات مكتوبة فقط ؟ الأمر الذي يستدعي معه

[1] فوزي عمارة، المرجع السابق، ص 250.

[2] أنظر المادة 65 مكرر 18 ق.إ.ج.

[3] أنظر المادة 65مكرر 16 ق.إ.ج.

[4] أنظر المادة 65مكرر14 ق.إ.ج.

[5] مصطفاوي عبد القادر،المرجع السابق ، ص 67 و68.

تطبيق القواعد العامة للإثبات واعتبارها إستدلالات لا ترقى إلى دليل ما لم ترفق بدلائل أو عناصر ثبوتية أخرى[1].

ثانيا: بطلان إجراءات التسرب

كمبدأ عام يكون البطلان إما لسبب مخالفة الأحكام الجوهرية المتعلقة بصفة عامة بحقوق الدفاع و حق الخصوم، وإما بطلان قانوني يتولى المشرع تحديد حالاته و هذا ما نلتمسه من خلال المواد 65 مكرر12 و 65 مكرر15 ق.إ.ج التي تبين حالات بطلان إجراءات التسرب وتتمثل في:

-يتعرض العمل الإجرائي لضابط الشرطة القضائية في إطار عملية التسرب إلى البطلان عند مخالفة الشروط الشكلية أو الموضوعية المتعلقة بالإذن لمباشرة عملية التسرب باستثناء حالة عدم ذكر الجريمة و هوية ضابط الشرطة القضائية المسؤول عن عملية التسرب و المدة التي تستغرقها وهو ما يعني أن عدم مراعاة الشكليات المنصوص عليها في الفقرة الثانية والثالثة من المادة 56 مكرر15 السالفة الذكر لا يترتب عليه بطلان الإذن بالتسرب[2].

-إذا كان العون المتسرب محرضا على ارتكاب مخالفة غير الذي سمحت له قانونا[3].

[1] فوزي عمارة، المرجع السابق، ص 250.

[2] نفس المرجع المرجع ، ص 248.

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

الخاتمة

الخاتمــة

تبين لنا من خلال هذه الدراسة أن التحقيق في الجريمة الرقمية يختلف تماما عن نظيره في الجرائم المعروفة في العالم التقليدي و تتجلى هذه الخصوصية في عدم إمكانية تطبيق أحكام الجرائم التقليدية على الجرائم المرتكبة في العالم الافتراضي بأصلها و إنما تأخذ طابع خاص و ذلك نظرا للطابع المستحدث لهذه الجريمة المتسمة بالتشعب.

أيضا هذه الخصوصية للجرائم المرتكبة عبر الأنترنت جعلت مختلف الدول و الهيئات والمنظمات الدولية و الإقليمية تدرك مدى خطورتها و مدى التحديات التي تفرضها عليها مما أدى بها إلى المسارعة من أجل وضعها في إطار قانوني يمكن من خلاله وضع طرق ناجعة وفعالة لمكافحتها.

وتمثلت الجهود الدولية في عقد المؤتمرات و إبرام معاهدات و اتفاقيات دولية و إقليمية مثل إتفاقية بودابست سنة 2001 التي وضعت الأسس السليمة لمكافحة الجريمة المعلوماتية، وقد واكب المشرع الجزائري هذه الحركة التشريعية بعد الفراغ التشريعي الذي عانته الجزائر في هذا المجال بتعديل قانون العقوبات بالقانون رقم: 04-15 و بعدها إصدار القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها و إدراج تعديلات على قانون الإجراءات الجزائية بما يتلاءم وخصوصية التحقيق في الجرائم الرقمية، والتي تستهدف إظهار أركان الجريمة محل التحقيق، وتحديد وقت ومكان ارتكاب الجريمة المعلوماتية والوصول إلى دليل إدانة و تحقيق العدالة بين جميع أطراف الدعوى التي تستوجب العمل تحت ضمانات المحاكمة العادلة، والتحقيق في قضايا نظم المعلومات كما رأينا عادة ما يكون أكبر من أن يتولاه شخص واحد بمفرده فمن الأفضل أن يتعاون عدة أشخاص في إنجاز هذه المهمة فهناك محققون جنائيون ذوو خبرة طويلة، وهناك أخصائيون في الحاسب الآلي والشبكات ذو معرفة واسعة وغيرهم كل يعمل على شاكلته وباتباع آليات جاءت بها التعديلات الجديدة التي تتلاءم وطبيعة الجرائم الرقمية من أجل إثبات المسألة بدليلها.

وعلى ضوء الإشكالات التي ظهرت من خلال الدراسة خلصنا إلى جملة من النتائج نذكر منها ما يلي على سبيل المثال لا الحصر:

1-إن مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات التي تستهدف البيئة الإلكترونية و عليه فان محل الجريمة التقليدية يختلف تماما عن محل الجريمة الرقمية الذي يكون في شكل افتراضي.

2-من بين الوسائل التي تساعد المحقق في التحري عن الجرائم الالكترونية هي عناوين الانترنت,كبروتوكول الانترنت IP الموجودة بكل جهاز مرتبط بالانترنت و الذي يساعد على تحديد مكان الحاسب الآلي.

3-المحقق في الجريمة المعلوماتية يجب أن يكون على معرفة و دراية بالجوانب الفنية و كذا التقنية للحاسب الآلي والانترنت.

4-توسيع دائرة إختصاص كل من قضاة التحقيق و ضباط الشرطة القضائية في مجال متابعة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و البيانات.

5-تفتيش المنظومة المعلوماتية من أصعب إجراءات البحث و التحري عن الجريمة ومرتكبيها، الأمر الذي يتطلب خبرة واسعة و كفاءة عالية من قبل القائمين به، كما يتطلب في الوقت نفسه تعاونا دوليا فعالا لمحاصرة هذه الجرائم و ملاحقة مرتكبيها، لان التفتيش في البيئة الافتراضية يختلف كثيرا عن مفهومه التقليدي وإن كانت تحكمه في بعض جوانبه القواعد المألوفة في قانون الإجراءات الجزائية مثل تفتيش المساكن و المجال الذي توجد فيه أجهزة الإعلام الآلي.

6-وكما لاحظنا أيضا مشاركة عدة أطراف في عملية التفتيش والحجز عن المعطيات المعلوماتية مثل النيابة العامة، قاضي التحقيق و كذلك الضبطية القضائية و مقدمو الخدمات والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

7-المعاينة في الجريمة الالكترونية أقل أهمية منها في الجرائم العادية، لقلة الآثار المادية بينما الخبرة تعتبر من أهم إجراءات التحقيق في الجرائم الالكترونية وهذا ما تستدعيه طبيعة هذه الجريمة، كونها تعتمد بالدرجة الأولى على وسائل مستحدثة.

8-نتيجة لخصوصية هذه الجريمة لجأ المشرع إلى استحداث قوانين تتلاءم مع الطبيعة الخاصة لهذه الجرائم من خلال إصدار القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، إضافة إلى المرسوم الرئاسي رقم 261/15 المؤرخ في 2015/10/08 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الاتصال ومكافحتها.

9-تبين لنا أيضا أن الاتصالات الالكترونية والنظم المعلوماتية تعتبر أحد أوجه الحياة الخاصة للإنسان ومظهرا من مظاهر خصوصياته، وعليه فإن إجراءات استخلاص الدليل الرقمي من الممكن أن تؤدي إلى المساس بهذه الخصوصية والاطلاع على أسرار أشخاص قد لا تكون لهم أية صلة بالجريمة، لذلك اشترط المشرع اللجوء إلى هذه الآليات الخاصة في التحري إذا دعت الضرورة لذلك ولم تعد أساليب التحري التقليدية كافية لمحاربة هذا النوع من الجرائم المستحدثة.

10-كما أضاف المشرع في تعديله وسيلة جديدة والمتمثل في التسرب وهو إجراء خطير سبقته اليه بعض التشريعات منها التشريع الفرنسي وهو يهدف للكشف عن الجرائم الخطيرة والمتورطين فيها و تحديد هويتهم ومناطق نشاطهم و الوسائل التي يستعملونها و ضبط كل ماله علاقة بهذه الجرائم من أدلة أو قرائن.

11-إستحداث مراقبة الاتصالات الالكترونية بموجب القانون 04/09 السالف الذكر, حيث رأى المشرع أن إباحة مراقبة الاتصالات الالكترونية بكافة أشكالها للوقاية من هذه الجرائم و تفادي خطرها المدمر خير له من تركها تقع وينتج عنها أضرار و خسائر.

و عليه فان المشرع الجزائري من خلال كل هذه القوانين و الإجراءات حاول بشكل عام الموازنة بين اعتبارين متناقضين:

الاعتبار الأول: الحرص على مزيد من الفاعلية في البحث و التحري عن الحقيقة و الذي يمكن أن يتسبب في انتهاك حقوق الإنسان

الاعتبار الثاني: الحرص على إحترام حقوق الإنسان والذي يترتب عليه في بعض الأحيان غل يد العدالة للوصول إلى معاقبة الجناة.

ومنه يتضح أن المشرع حاول التوفيق بين ما تتطلبه ضرورات التحقيق و المصلحة العامة والحريات الفردية الخاصة.

و بناءا على هذه النتائج نستخلص مجموعة من الاقتراحات نذكر منها ما يلي:

1-إنشاء دورات تكوينية لتدريب و تأهيل قضاة التحقيق وضباط الشرطة القضائية في مجال نظم المعلوماتية والحواسيب، لان دور القاضي مهم في توجيه مسار القضايا، فإذا كان القاضي غير ملم بالجوانب التقنية الحديثة للحاسب الآلي و الانترنت، فانه لا يستطيع تقدير مدى خطورة المجرم ألمعلوماتي، وعليه يصدر أحكام غير متكافئة مع الجريمة المرتكبة.

2-نقترح إدراج المراسلات الالكترونية صراحة ضمن إجراء اعتراض المراسلات التي أضحت وسيلة فعالة في ارتكاب الجرائم الخطيرة في قانون الإجراءات الجزائية ليتماشى مع جاء في به المشرع في القانون 04/09 السالف الذكر.

3-دعوة المشرع إلى تعديل المادة 56 مكرر 18 من القانون 22/06 المعدل و المتمم لقانون الإجراءات الجزائية و جعلها تسمح لضابط الشرطة القضائية المسؤول عن عملية التسرب أو العون المتسرب الإدلاء بشهادته عن طريق الشاشة الالكترونية مع إمكانية تغيير الصوت والصورة.

4-استحداث جهاز على مستوى وزارة العدل لحفظ و متابعة الهوية الحقيقة للعون المتسرب، لأنه لا يكمن تصور ما يحدث له (العون المتسرب) إذا توفي رئيسه المسؤول عن العملية أو تم فصله أو قام نزاع بينه وبين المتسرب، ولذلك يستحسن أن تكون هناك جهة ثانية على دراية بهويته و متابعتها.

5-يتعين إتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم الالكترونية، وذلك خلال إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم.

6-التطرق إلى الضمانات المتعلقة بتنفيذ الإجراءات الخاصة، من هذه الضمانات نذكر مثلا

- إخطار الشخص بمراقبة أحاديثه بعد انتهاء عملية المراقبة
- تمكينه من الاطلاع عليها و مناقشتها و الاعتراض عليها خلال التحقيق الابتدائي
- خلو قانون إجراءات الجزائية من بيان مصير التسجيلات المتحصل عليها بعد إنهاء العملية.

وهكذا يكون البحث قد اكتمل بحمد الله وعونه ولا يسعنا سوى القول، إن كان فيه من الحسن والصواب فهو من الله سبحانه وتعالى، وإن كان فيه نقص أو قصور فهو منا، ولما لا ونحن بشر نجتهد ونخطي ونصيب فإن أصبنا فأجرنا على الله وإن أخطانا فندعوه ألا يحرمنا أجر المجتهدين، مصداقا لقول نبينا الكريم " **إذا اجتهد العالم فأصاب فله أجران و إن اجتهد وأخطأ فله أجر**.

تم بحمد الله

قائمة المصادر والمراجع

قائمــة المصـــادر و المراجـــع

أولا: المصادر

1. الدستور الجزائري لسنة 1996، الصادر بموجب المرسوم الرئاسي رقم: 96-438 المؤرخ في: 1996/12/07، ج.ر عدد 76، الصادرة في:1996/12/08 (المعدل و المتمم).

2. القانون رقم: 03/2000 ، المؤرخ في: 2000/08/05، المحدد للقواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، ج.ر عدد 48 الصادرة في: 2000/08/06.

3. القانون رقم: 09-04، المؤرخ في: 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام الآلي و الإتصال و مكافحتها، ج.ر عدد 47، الصادرة في: 2009/08/16.

4. الأمر رقم: 66-155 المؤرخ في: 1966/06/08، المتضمن قانون الإجراءات الجزائية الجزائري، ج.ر عدد 48، الصادرة في: 1966/06/10، المتمم حسب آخر تعديل له بالأمر رقم: 17-07، المؤرخ في: 2017/03/17.

5. الأمر رقم: 66-156، المؤرخ في: 1966/06/08، المتضمن قانون العقوبات الجزائري، ج.ر عدد 49، الصادرة في: 1966/06/11، المتمم حسب آخر تعديل له بالأمر رقم: 02/16، المؤرخ في: 2016/06/19.

6. المرسوم الرئاسي رقم: 15-261 ، المؤرخ في: 2015/10/08، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر عدد 53، الصادرة في: 2015/10/08.

7. المرسوم التنفيذي رقم:348/06 المؤرخ في:2006/10/05 المتعلق بالتنظيم القضائي، ج.ر عدد 63 الصادرة بتاريخ: 2006/10/08، المعدل والمتمم بالمرسوم رقم: 267/16.

8. إتفاقية بودابست لمكافحة الجرائم المعلوماتية و الموقعة في العاصمة المجرية بودابست في 23 نوفمبر 2001 المتعلقة بالإجرام الفضائي.

ثانيا: المعـاجم

1.المنجد للغة و الأعلام، دار المشرق، لبنان، طبعة 27، 1986، ص 329.

ثالثا: الكتــب

1. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، مصر، بدون طبعة ، 2008.

2. أحسن بوسقيعة، التحقيق القضائي، دار هومة للطباعة والنشر، الجزائر، ط 10، 2013.

3. بكرى يوسف بكرى، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، ط1 ، 2011.

4. حسن الجوخدار، التحقيق الإبتدائي في قانون أصول المحاكمات الجزائية،دار الثقافة للنشر و التوزيع، الأردن، ط1، 2008.

5. حمزة قريشي" الوسائل الحديثة للبحث و التحري في ضوء القانون الجزائري" (دراسة مقارنة) منشورات السائحي، الجزائر، ط 1، 2017.

6. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية،دار الفكر الجامعي، الاسكندرية، ط1، 2009.

7. زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، بدون طبعة، 2011.

8. عبد الله أوهايبة، شرح قانون الإجراءات الجزائية الجزائري، دار هومه، الجزائر، ط2، 2011.

9. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، دار النهظة العربية، مصر، ط1، 2009.

10. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر و الأنترنت، دار الكتب القانونية، مصر، بدون طبعة، 2004.

11. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الأنترنت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، لبنان ، ط1 ، 2007.

12. عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية، دار هومة للطباعة والنشر والتوزيع، الجزائر، بدون طبعة ، 2009.

13. علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة) ، دار الكتب و الوثائق القومية، مصر، بدون طبعة،2012.

14. علي شملال، الجديد في شرح قانون الإجراءات الجزائية، الكتاب الأول، الإستدلال والإتهام، دار هومة، الجزائر، ط 3، 2017.

15. عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية، دار هومه، الجزائر، بدون طبعة، 2012 .

16. غسان مدحت الخيري، أصول التحقيق الإبتدائي كحق من حقوق الإنسان، دار الراية للنشر والتوزيع، الأردن، ط1، 2013.

17. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ط1، 2009.

18. محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، دار الحامد للنشر والتوزيع، الأردن، ط1، 2014.

19. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر، الجزائر، ط2، 2009.

20. محمد حمدان عاشور، أساليب التحقيق والبحث الجنائي، أكاديمية فلسطين للعلوم الأمنية، الشؤون الأكاديمية قسم المنهاج، فلسطين، بدون طبعة، 2010.

21. ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية– دراسة تأصيلية تحليلية و مقارنة للتنصت على المحادثات التليفونية و التي تجري عبر الأنترنات و الأحاديث الشخصية نظريا و علميا– ، دار المطبوعات الجامعية، الإسكندرية، ط1، 2009.

رابعـا: البحوث الجامعية

أ- أطروحات الدكتوراه

1. صالح شنين، الحماية الجنائية للتجارة الإلكترونية، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق، الجزائر، 2013.

2. بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، جامعة الجزائر، كلية الحقوق، الجزائر، 2015.

ب- مذكرات الماجستير

1.أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضل القانون 09/ 04، مذكرة لنيل شهادة الماجستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم الإقتصادية، قسم الحقوق، الجزائر، 2013.

2.سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العالية، أكاديمية نايف العربية للعلوم الأمنية،الرياض،2003

3.سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية و الإدارية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013.

4.صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، الجزائر، سنة 2013.

5.صبايحية خديجة، جرائم السرقة و الإحتيال عبر الأنترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم الإسلامية، جامعة الجزائر، كلية العلوم الإسلامية،الجزائر، 2013.

6.طيبي الطيب، البحث والتحقيق في جريمة تبييض الأموال في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في الحقوق، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2012.

7.عبد الله بن حسين أل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية، رسالة مقدمة لنيل شهادة الماجستير، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية ، الرياض، 2014.

ج- مذكرات مـاستر

1.السوفي نور الهدى، التحقيق في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر أكاديمي في الحقوق، تخصص قانوني جنائي، جامعة قاصدي مرباح ورقلة، 2017.

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

3.بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2016.

4.جواحي عبد الستار، جرائم الحاسوب – دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري- مذكرة تخرج تدخل ضمن متطلبات الحصول على شهادة الماستر في العلوم الإسلامية، جامعة الشهيد حمه لخضر، كلية العلوم الإجتماعية و الإنسانية، قسم العلوم الإنسانية، الجزائر،2015 .

5.عباسي خولة، الوسائل الحديثة للإثبات في القانون الجنائي، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2014.

6.عبد الرحمان كوداد، عملية التسرب على ضوء التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق تخصص علم إجرام، جامعة الطاهر مولاي، سعيدة، 2017.

7.قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة مكملة لنيل شهادة الماستر أكاديمي في القانون، تخصص قانون عام للأعمال، جامعة قاصدي مرباح ورقلة، 2014.

8.معمش زهية وغانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في الحقوق، جامعة عبد الرحمان مريم بجاية،.كلية الحقوق والعلوم السياسية، قسم القانون الخاص، الجزائر، 2013.

9. مهدي شمس الدين، النظام القانوني للتسرب في القانون الجزائري، مذكرة مكملة لنيل شهادة الماستر في الحقوق قانون جنائي، جامعة محمد خيضر، كلية، قسم، بسكرة، 2014.

خامسـا: المقـالات

1. بن كثير بن عيسى،الإجراءات الخاصة المطبقة على الإجرام الخطير، نشرة القضاة، مديرية الدراسات القانونية و الوثائق، العدد 63، 2008.

2. براهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، جامعة مولود معمري تيزي وزو، العدد02، 2016.

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

4. جميلة محلق، إعتراض المراسلات، تسجيل الأصوات، التقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد و الإدارة و القانون، جامعة باجي مختار عنابة، العدد 42، جوان 2015.

5. جبار فطيمة، مراقبة الاتصالات الالكترونية بين الحظر و الإباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، جامعة مولود معمري بتيزي وزو، العدد 3، ديسمبر 2016.

6. .حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ط1، 2000.

7. فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، كلية الحقوق والعلوم السياسية جامعة منتوري قسنطينة ، العدد 33، جوان 2010.

8. مصطفاوي عبد القادر، أساليب البحث و التحري الخاصة و إجراءاتها، مجلة المحكمة العليا، العدد02، 2009.

9. نقادي عبد الحفيظ، " التسجيل الصوتي" المجلة الجزائرية للعلوم القانونية و الاقتصادية، كلية الحقوق، الجزائر، العدد01، 2009.

سادســـا: الملتقيــات

1.العدواني عبد الحميد،"إدارة التحريات و التحقيقات الأولية في الجرائم التي تدخل في إختصاص القطب القضائي الجزائي"، الملتقى الجهوي حول مكافحة الإجرام الخطير، مجلس قضاء ورقلة، الأربعاء 2009/01/28.

2.لوجاني نور الدين، "أساليب البحث و التحري الخاصة و إجراءاتها"، يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية، إليزي، 2007/12/12.

3.محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون و الكومبيوتر و الانترنت، مجلد 3، الفترة من01 إلى 03 ماي2000.

4. فضيلة عاقلي، أعمال المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، طرابلس 24-25 مارس 2017.

5.هشام محمد فريد رستم، الجرائم المعلوماتية: أصول التحقيق الجنائي الفني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة و القانون جامعة الإمارات العربية المتحدة، مجلد 2، الفترة من01 إلى03 ماي2000.

ســابعــا: المراجع الأجنبية

1.Code de procédure pénal Francis, section 2,de l’infiltration version en vigueur au 25/12/2011, depuis 01/10/2004, Cree pour loi n.2004_204 du 09/03/2004, art ,01 jorf 10/03/2004,en vigueur le 01/10/2004.

ثامنا: مواقع الأنترنت

1.حسين بن سعيد الغافري، التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الأنترنات، موقع المنشاوي للدراسات و البحوث على الموقع WWW.minshawi.com ، أطلع عليه بتاريخ: 2018/02/11.

2. وليد طه، التنظيم التشريعي للجرائم الإلكترونية في إتفاقية بودابست، بحث على الموقع Htt://leagueofarabstates.net أطلع عليه بتاريخ:2018/03/31.

الملاحق

الملحق رقم 01

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة العدل

مجلس قضاء ورقلة
محكمة ورقلة
نيابة ورقلة

وكيل الجمهورية لدى محكمة_ورقلة

إلى السيد /

قائد فصيلة الأبحاث للدرك الوطني

إذن بالتسرب

نحن وكيل الجمهورية لدى محكمة ورقلة

بعد الإطلاع على الطلب المقدم من طرف .....

بتاريخ .....تحت رقم .....

بعد الإطلاع على المواد 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية المعدل و المتمم.

نـأذن

.....ضابط الشرطة القضائية

.....بالتسرب

ضمن .....

تكون مدة التسرب لا تتجاوز أربعة أشهر تحدد طبقا للمعطيات الشكلية و القانونية المحددة بالمواد المذكورة أعلاه.

ورقلة في:.....

وكيل الجمهورية

الملحق رقم 02

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة العدل

مجلس قضاء ورقلة
محكمة ورقلة
نيابة ورقلة

وكيل الجمهورية لدى محكمة ورقلة

إلى السيد /

قائد فصيلة الأبحاث للدرك الوطني

إذن التنصت

نحن وكيل الجمهورية لدى محكمة ورقلة

بعد الإطلاع على الطلب المقدم من طرف .....

بتاريخ .....تحت رقم .....

بعد الإطلاع على المواد 65 مكرر 5 إلى 65 مكرر 9 من قانون الإجراءات الجزائية المعدل و المتمم.

نـأذن

.....ضابط الشرطة القضائية

.....بالتنصت

ضمن .....

تكون مدة التنصت لا تتجاوز أربعة أشهر تحدد طبقا للمعطيات الشكلية و القانونية المحددة بالمواد المذكورة أعلاه.

ورقلة في:.....

وكيل الجمهورية

الملحق رقم 03

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة الداخلية، الجماعات المحلية
والتهيئة العمرانية
المديرية العامة للأمن الوطني
أمـــن ولايـــة غرداييـــــة.

رقم: .....

محضـــر معايـنة إلـكترونية

قضية ضد :

الموضوع: محضـر معاينة إلكترونية

التكييف:

--/ **إنه في :** يوم الجمعة الموافق للحادي عشر من شهر جوان ----------
---/ **سنة :** الفين و سبعة عشر ----------
--------/**الساعة:** العاشرة صباحا. ----------
-----/ **نحن :** ..... ملازم أول للشرطة ، ضابط الشرطة القضائية ، رئيس فرقة مكافحة الجرائم المعلوماتية ، بالمصلحة الولائية للشرطة القضائية بامن ولاية غرداية ----------/ضابط الشرطة القضائية بدائرة :الاختصاص والمقيم بها----------
--/ استمرارا في التحقيق المفتوح في شكوى ..... بخصوص قضية السب و الشتم عبر وسائط إلكترونية و المساس بحرمة الحياة الخاصة للأشخاص و قرصنة حسابها عبر مواقع التواصل الاجتماعي – فيس بوك ،و بعد تقدم الشاكية لمصالحنا .----------
--/ لما سبق ذكره قمنا بمكتبنا وباستعمال وسائل المصلحة وبحضور و موافقة صاحبة الحساب / ..... بالولوج إلى حسابها بموقع الفايسبوك الحامل للرقم IP.....

--/ المعاينة جـــــــاءت نتائجها إيجابية مثلما هو مبين في الصور أسفل هذا:----- ----------
---

--/ دامت المعاينة حوالي نصف الساعة، وأغلق المحضر في حدود الساعة 09:30 صباحا من نفس اليوم .----------
--/ حرر هذا المحضر إثباتا للعملية والذي نمضيه في اليوم والساعة المذكورين أعلاه.----------

ضابط الشرطة القضائية

فهرس المحتويات

المحتوى	الصفحة
شكر و عرفان	-
إهــداء	-
قائمة المختصرات والكلمات المفتاحية	-
ملخص الدراسة	-
مقدمــة	1
الفصل الأول ماهية التحقيق الجنائي في الجرائم الرقمية	
المبحث الأول: الإطار المفاهيمي للتحقيق الجنائي في الجرائم الرقمية	11
المطلب الأول: المبادئ الأساسية للتحقيق الجنائي في الجرائم الرقمية	12
الفرع الأول: مفهوم التحقيق الجنائي في الجرائم الرقمية	12
أولا: تعريف التحقيق الجنائي في الجرائم الرقمية	12
ثانيا: خصائص التحقيق الجنائي في الجرائم الرقمية	14
الفرع الثاني: العناصر الأساسية للتحقيق الجنائي في الجرائم الرقمية	15
أولا: إظهار الركن المادي للجرائم الرقمية	15
ثانيا: إظهار الركن المعنوي للجرائم الرقمية	16
ثالثا: تحديد وقت ومكان ارتكاب الجريمة الرقمية	16
الفرع الثالث: ضمانات المتهم في مرحلة التحقيق الجنائي في الجرائم الرقمية	17
أولا: علانية التحقيق بالنسبة للخصوم	17
ثانيا: سرية التحقيق بالنسبة للجمهور	17
ثالثا: حق المتهم في محاكمة عادلة وسريعة	18
رابعا: حق المتهم في الإستعانة بمحام	18
المطلب الثاني: وسائل التحقيق الجنائي في الجرائم الرقمية	19
الفرع الأول: منهج التحقيق الجنائي في الجرائم الرقمية	19

أولا: تحديد خطة عمل التحقيق	19
ثانيا: تكوين فريق التحقيق	22
الفرع الثاني: الوسائل المادية للتحقيق الجنائي في الجرائم الرقمية	24
أولا: عناوين (IP و MAC والبريد الإلكتروني وبرامج المحادثة)	25
ثانيا: البروكسي Proxy	26
ثالثا: برامج التتبع	26
رابعا: نظام كشف الإختراق IDS	28
خامسا: أدوات الضبط	28
سادسا: الأدوات المساعدة بالتحقيق	28
سابعا: أدوات فحص ومراقبة الشبكات	29
الفرع الثالث: الوسائل الإجرائية للتحقيق الجنائي في الجرائم الرقمية	29
أولا: اقتفاء الأثر	30
ثانيا: الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته	30
ثالثا: الاستعانة بالذكاء الصناعي	30
رابعا: التوقيف خلال فترة التحقيق	31
خامسا: إظهار الحقائق	31
سادسا: إتباع القواعد الفنية لكشف الجريمة	34
المبحث الثاني: المحقق في الجرائم الرقمية	35
المطلب الأول: القائم بالتحقيق في الجرائم الرقمية	35
الفرع الأول: مفهوم المحقق في الجرائم الرقمية	35
أولا: تعريف المحقق في الجرائم الرقمية	35
ثانيا: خصائص المحقق في الجرائم الرقمية	36
الفرع الثاني: مساعدو المحقق في الجرائم الرقمية	40
أولا: رجال الضبطية القضائية	40
ثانيا: مقدمو الخدمات	40

ثالثا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال	41
رابعا: الخبراء	42
خامسا:القضاة و المحامون	42
المطلب الثاني: صلاحيات المحقق في الجرائم الرقمية	43
الفرع الأول: صلاحيات قاضي التحقيق في الجرائم الرقمية	43
أولا: الإختصاص المحلي	43
ثانيا: الإختصاص النوعي	44
الفرع الثاني: صلاحيات الضبطية القضائية في الجرائم الرقمية	45
أولا: تمديد الإختصاص الإقليمي للضبطية القضائية	45
ثانيا: تعزيز صلاحيات الضبطية القضائية	46
الفصل الثاني **آليات التحقيق الجنائي في الجرائم الرقمية**	
المبحث الأول: الآليات الإجرائية العامة للتحقيق الجنائي في الجرائم الرقمية	50
المطلب الأول: المعاينة في الجرائم الرقمية	50
الفرع الأول: تعريف المعاينة في الجرائم الرقمية	51
الفرع الثاني: محل المعاينة في الجرائم الرقمية	53
أولا: مسرح تقليدي	53
ثانيا: مسرح سيبراني أو إفتراضي	53
الفرع الثالث: إجراءات معاينة مسرح الجريمة الرقمية	54
المطلب الثاني: التفتيش والضبط في الجرائم الرقمية	57
الفرع الأول: التفتيش في الجرائم الرقمية	57
أولا: تعريف التفتيش في الجرائم الرقمية	58
ثانيا: شروط التفتيش في الجرائم الرقمية	60
ثالثا: مدى قابلية المنظومة المعلوماتية للتفتيش	67
رابعا: بطلان التفتيش في الجرائم الرقمية	73

الفرع الثاني: الضبط في الجرائم الرقمية	74
أولا: تعريف الضبط في الجرائم الرقمية	74
ثانيا: حجز المعطيات المعلوماتية	75
ثالثا: ضوابط الحجز في الجرائم الرقمية	77
المطلب الثالث: الخبرة في الجرائم الرقمية	78
الفرع الأول: تعريف الخبرة في الجرائم الرقمية	78
الفرع الثاني: أهمية الخبرة في الجرائم الرقمية	79
الفرع الثالث: شروط الخبرة في الجرائم الرقمية	81
الفرع الرابع: عمل الخبير و أساليبه	84
المبحث الثاني : الآليات الإجرائية الخاصة للتحقيق الجنائي في الجرائم الرقمية	86
المطلب الأول : إعتراض المراسلات و تسجيل الأصوات و التقاط الصور	86
الفرع الأول: تعريف إعتراض المراسلات	87
الفرع الثاني : تسجيل الأصوات و التقاط الصور	90
الفرع الثالث : إجراءات و شروط إعتراض المراسلات و تسجيل الأصوات والتقاط الصور	91
المطلب الثاني : مراقبة الاتصالات الالكترونية	95
الفرع الأول: مفهوم مراقبة الاتصالات الالكترونية	95
أولا: تعريف المراقبة	95
ثانيا: تعريف الإتصالات الإلكترونية	96
الفرع الثاني: حالات اللجوء إلى المراقبة الالكترونية	96
أولا: الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة	96
ثانيا: في حالة توافر معلومات تدل على احتمال وقوع إعتداء على منظومة حاسوبية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني	97
ثالثا: لمقتضيات التحريات و التحقيقات القضائية	97

رابعا: في إطار تنفيذ طلبات المساعدة القضائية الدولية	97
الفرع الثالث: الضمانات المقررة لتنفيذ مراقبة الاتصالات الالكترونية	98
أولا: سرية الإجراءات	98
ثانيا: التسخير	98
ثالثا: تحرير محضر بالعمليات التقنية التي تم القيام بها	98
رابعا: حماية المعطيات المتحصل عليها	99
خامسا: الإذن	99
سادسا: عدم المساس بالحرية الشخصية للفرد	99
المطلب الثالث: التسرب	100
الفرع الأول : تعريف التسرب	100
أولا : التعريف اللغوي للتسرب	100
ثانيا : التعريف القانوني للتسرب	101
ثالثا : التعريف العملي للتسرب	101
الفرع الثاني : تنظيم عملية التسرب	102
أولا : الشروط الشكلية للتسرب	102
ثانيا: الشروط الموضوعية للتسرب	104
ثالثا: طرق التسرب في مجال الجريمة الرقمية	106
الفرع الثالث : الإطار الزماني و المكاني لعملية التسرب	106
الفرع الرابع : الآثار المترتبة عن عملية التسرب و بطلان إجراءاته	106
أولا : الآثار المترتبة عن عملية التسرب	106
ثانيا: بطلان إجراءات التسرب	108
الخاتمة	109
قائمة المصادر والمراجع	115
الملاحق	-

ملخص البحث

لقد واجهت عملية التحقيق في الجريمة المعلوماتية صعوبات كثيرة في كشف غموض هذه الجرائم التي يتطلب لارتكابها وسائل ذات تقنية عالية، إضافة إلى ذكاء وخبرة المجرم في مجال الأنترنت و الحاسب الآلي، الأمر الذي قد يخلف آثار غير مادية فيصعب بذلك كشف الجريمة و القبض على الجاني، هذا الوضع دفع إلى ضرورة تطوير عملية التحقيق واستعمال أساليب ذي تقنية عالية لاستخلاص الدليل الرقمي، حيث أصبحت وسائل التحقيق المادية و الإجرائية تتميز بالطابع العلمي وذلك بالإستعانة بالأساليب العلمية واستخدام الانترنت لكشف هذا النوع من الجرائم، و أيضا الرفع من قدرات الجهات المختصة القائمة بالبحث و التحري، لأن التحقيق بصفة عامة يعتمد على ذكاء المحقق وفطنته وأن يحاول بكل جهده إظهار الحقيقة.

إضافة إلى أن الطابع الخاص للجريمة المعلوماتية أنتج نوع خاص من الأدلة من نفس طبيعتها بحيث يصعب إكتشافها و ضبطها عن طريق الآليات العامة للتحقيق المتمثلة في المعاينة والتفتيش والحجز والخبرة مما دفع بالمشرع الجزائري إلى ضرورة تطوير القوانين و إدخال تعديلات على مستوى قانون الإجراءات الجزائية، إضافة إلى استحداث قوانين جديدة تتلاءم وخصوصية هذه الجريمة التي تقوم في عالم افتراضي، فاستحدث بذلك آليات خاصة تتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، و أيضا التسرب و المراقبة الإلكترونية.

Summary:

Information crime investigation process has witnessed a set of hurdles to unveil the vagueness of such crimes that entail methods of high techniques, additionally to the criminal's smartness and experience in field of internet and computing, the fact that could have non-material consequences making it much harder to reveal the crime and to arrest the unsub, This situation has enforced the necessity for developing the investigation process and using highly technical methods to tease out the digital evidence. Physical and measuring methods of investigation are of scientific nature, using scientific methods and internet to reveal such crimes, along with increasing the abilities of specialized donors of research and investigation, because generally investigation depends on the investigator's intelligence and wit and deploying all efforts to reveal the crime.

In addition to the specificity of information crime, a new kind of evidences is emanated, the fact that harden the crime's detection and control merely by public mechanisms of investigation, being constatation, inspection, detention and expertise which led the Algerian legislator for the necessity to enforce the laws and bring about amendments on penal measures law, along with creating new laws fitting in with this crime's specificity happening in the virtual world, thus creating specific mechanisms for correspondences interception, voter registration and pictures taking along with electronic leakage and control.