وزارة التعليم العالي والبحث العلمي
جامعة يحي فارس بالمدية
كلـــية الحقوق والعلوم السياسية

إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية

مذكرة التخرج لنيل شهادة الماستر في الحقوق

تخصص القانون الجنائي والعلوم الجنائية

من تقديم الطالبين:

-سحنين طارق
-بوسماحة صارة

تحت إشراف الأستاذ:

-د.عزوز عبد الحميد

أعضاء لجنة المناقشة

الدكتور كربوش سليم ..... رئيسا
الدكتور عزوز عبد الحميد ..... مشرفا ومقررا
الدكتور بوصوار ميسوم ..... عضوا مناقشا

السنة الجامعية : 2021/2020

تشكرات

بسم الله الرحمن الرحيم

إن الاعتراف بالجميل لأهل الفضل واجب و أكيد

بصدد إنجاز هذا العمل ، نشكر الله سبحانه و تعالى

الذي وفقنا لإتمام هذا العمل.

نتقدم بالشكر الجزيل إلى كافة الأساتذة الذين أشرفوا على تعليمنا

خاصة الدكتور عزوز عبد الحمد

إلى كل من ساعدنا و لو بابتسامة صغيرة صادقة،

إلى كل هؤلاء شكرا جزيلا و جزأكم الله خيرا إنشاء الله.

إهداء

إلى من قال فيهما الله عز و جل: "و اخفض لهما جناح الذل من الرحمة و قل ربي ارحمهما كما ربياني صغيرا"

إلى الذين جعلهم الله سندا لي في هذه الحياة إخوتي

إلى أساتذتي الذين ساهموا بشكل كبير في تحصيلي العلمي

إلى أستاذي المشرف الذي أراد أن يبث الأمل فينا والذي أراد أن يصنع منا الكثير

طارق

إهداء

إلى من قال فيهما الله عز و جل: "و اخفض لهما جناح الذل

من الرحمة و قل ربي ارحمهما كما ربياني صغيرا"

إلى الذين جعلهم الله سندا لي في هذه الحياة إخوتي

إلى أساتذتي الذين ساهموا بشكل كبير في تحصيلي العلمي

إلى أستاذي المشرف الذي أراد أن يبث الأمل فينا والذي أراد

أن يصنع منا الكثير

صارة

مقدمة

مقدمة:

يشهد العالم اليوم ازدهارا في المجال العلمي و التكنولوجي ، و يعود الفصل فيها للثورة المعلوماتية التي حققت قفزة ملحوظة في مستويات التقدم التقني و العلمي ، فالعالم اصبح يعرف اليوم بالقرية صغيرة . و مع تقدم العلوم بدأ كم المعلومات يتزايد و يتكاثر . فأصبح من اللازم استخدام اساليب علمية و تقنية متطورة لمواجهة هذه الظاهرة . مثل الحاسبات الالكترونية و المستحدثات التقنية الاخرى المختلفة كأقراص فيديو .

ان عصر الثورة المعلومات التي يشهدها عالمنا اليوم يعتمد اعتمادا اساسيا على الحاسب بما يتميز بقدرات هائلة للتخزين و الاسترجاع و طرح الحلول لأعقد المشكلات ، فالحاسب جهاز الكتروني يستطيع ترجمة اوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات ادخال بيانات او اخراج معلومات او اجراء عمليات حسابية او منطقية . و يتكون الحاسب من المكونات المادية و المكونات المنطقية . كما اصبحت تقنية الحاسوب تستعمل في ارتكاب العديد من الجرائم تارة و كموضوع للجريمة تارة اخرى و اصبح هذا النوع من الجرائم يرتكب في وسط افتراضي غير متعارف عليه و لا يشبه الوسط التقليدي للجرائم التقليدية .

و تعتبر الجرائم الالكترونية من اخطر و اعقد الجرائم على الاطلاق و تعتبر من اعقد الاشكاليات الجديد للجريمة المنظمة . فهي جريمة تقنية سهلة الارتكاب تنشأ في الخفاء و في بيئة افتراضية دون ان تخلف اي آثار محسوسة ، و ترتكب هذه الجريمة عن طريق مجرمين اذكياء يمتلكون ادوات المعرفة الفنية للتعامل في مجال المعالجة الالية للمعطيات و يتمتعون بمهارات و خبرات تقنية عالية زيادة على ذلك تعتبر جريمة عابرة للحدود تتم عبر شبكة اتصال لا متناهية غير مرئية .

فالمشرع الجزائري كغيره من التشريعات حاول وضع اطر قانونية ملائمة و ادخال تحديدات على القوانين السارية المفعول بها تتلائم مع الوضع الجديد لتحديد شروط استعمال هذه الوسائل في مختلف

المعاملات من خلال نصوص جزائية لحماية الانظمة المعلوماتية و ردع اساءة استعمالها سواء محليا او دوليا في اطار الاتفاقيات الدولية . كما امتدت التعديلات الى نطاق القانون الجنائي الاجرائي الذي صيغت نصوصه لتنظيم الاجراءات المتعلقة بجرائم تقليدية التي لا توجد صعوبات كثيرة في اثباتها او التحقيق فيها و جمع الادلة المتعلقة بها . و المشرع الجزائري جاء بمجموعة من الاجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية و الجرائم المعلوماتية عن طريق تعديل قانون اجراءات جزائية بتقنين وسائل و اجراءات خاصة تتماشى مع طبيعة الجرائم المستحدثة و منها اجراءات تطبق على الجريمة المعلوماتية فقط التي تم النص عليها في القانون الجديد المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته 04/90 المؤرخ في 5 اوت 2009 .

و تكمن اهمية موضوعنا اساسا في كون الجريمة المعلوماتية جريمة جديدة حديثة النشأة و بالتالي لا يكفي تطبيق الاجراءات المطبقة على الجرائم التقليدية ، حيث ان القواعد الاجرائية المنصوص عليها في قانون اجراءات جزائية لا يمكن ان تطبق عليها لأنها تقع في عالم افتراضي و يمتد تأثيرها ، الى جميع الاصعدة لارتباطها بالتطور التكنولوجي للإعلام و الاتصال التي تستعمل في جميع مجالات الحياة سواء من طرف الافراد او المؤسسات اذ تجعل التعاملات معها صعبا و معقدا مما يحتم الى ايجاد اجراءات اخرى جديدة

و عليه من اسباب اختيارنا لهذا الموضوع هو معرفة القواعد الاجرامية الحديثة التي جاء بها المشرع الجزائري بتعديل قانون اجراءات جزائية و كذلك القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها .

و هذا ما يدل على الصعوبات و المعوقات الملقاة من خلال البحث و الدراسات المقدمة و دور المشرع في محاولته للتماشي مع مختلف التشريعات ، لتصدي لهذا النوع من الجرائم و تحقيق الحماية القانونية اللازمة .

و يمكن طرح الاشكالية التالية :

ما هي اجراءات المعاينة و التفتيش و الحجز داخل المنظومة المعلوماتية ؟

كما يمكن طرح مجموعة من الاشكاليات الفرعية :

ماهي الاجراءات التقليدية المتبعة للتفتيش و الحجز داخل المنظومة المعلوماتية ؟

ماهي اجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية ؟

و منه للإجابة هن هذه الاشكالية تم الاعتماد على علم المنهج الوصفي و ذلك من خلال وصف بعض المفاهيم العامة الخاصة بالجريمة المعلوماتية و آليات التحقيق فيها، مع الاستعانة بالمنهج التحليلي من خلال دراسة و تحليل الاجراءات الخاصة بالمعاينة و التفتيش و الحجز.

و للإجابة على هذه الإشكالية تم إتباع خطة ذات فصلين :

الفصل الاول بعنوان : الإجراءات العامة والمألوفة ومدى سريانها على الجريمة المعلوماتية (إجراءات التقليدية)، اما الفصل الثاني فاقترحنا له العنوان التالي: الاجراءات المستحدثة للتحري والكشف عن الجرائم داخل المنظومة المعلوماتية (الاجراءات الحديثة)

الفصل الأول

الإجراءات العامة والمألوفة ومدى سريانها على الجريمة المعلوماتية (إجراءات التقليدية)

تمهيد:

إنَ للضبطية القضائية دور كبير في مجال محاربة ومكافحة الجريمة الواقعة داخل النظام المعلوماتي، ويكمن دورها الرئيسي في حماية أمن المجتمع من الجرائم الواقعة في النظام المعلوماتي بصفة خاصة، والجرائم بصفة عامة، فالشرع الجزائري كغيره من التشريعات حدد جهات أو وحدات مختصة تعمل في هذا المجال، تكون هذه الوحدات مزودة بالخبراء والتقنيين الخاضعين لتكوين متخصص، حيث تنظم لهم أدوات متخصصة لهم في مجال مكافحة الجرائم المعلوماتية، حيث سنتطرق في هذا الفصل إلى مبحثين، المبحث الأول سنتناول فيه معاينة محل الجرائم الواقعة داخل وخارج النظم المعلوماتي، والمبحث الثاني التفتيش والحجز في النظم المعلوماتي.

المبحث الأول: معاينة محـل الجرائم الواقعة داخل وخارج النظم المعلوماتيــة.

تعتبر المعاينة من أهم مراحل التحقيق كما تعتبر من المراحل الأولية للاستدلال على ملابسات الجريمة، كما لها أهمية ودور كبير في الجرائم الالكترونية والغاية من المعاينة ضبط ما استعمل في ارتكاب الجريمة أو نتج عنها وسنتطرق في هذا المبحث إلى مفهوم النظم المعلوماتية (المطلب الأول) ومفهوم المعاينة (المطلب الثاني)، والقواعد الإجرائية لمعاينة مسرح الجريمة الالكترونية (المطلب الثالث)

المطلب الأول: مفهـوم النظم المعلومـاتية

لقد عرف حجم المعلومات ازديادا كبيرا مع مرور الوقت وكثرت بشكل سريع مما استدعى إلى الاعتماد على تقنية المعلوماتية، التي تهدف إلى حل ومعالجة المعلومات بطريقة سريعة ومواكبة للعصر عن طريق علوم الحاسوب وعلوم الاتصال، وسنتطرق في هذا المطلب إلى تعريف النظم المعلوماتية (الفرع الأول) ومكونات النظم المعلوماتية (الفرع الثاني).

الفرع الأول: تعريف نظم المعلوماتية

القد تكفلت نصوص أحكام الاتفاقيات الدولية إضافة إلى نصوص التشريعات الوطنية بتعريف نظم المعلوماتية، فغرفت بودابست لمكافحة الجرائم المعلوماتية في مادتها الأولى النظم المعلوماتية بأنها " كل آلة بمفردها أو مع غيرها مع الآلات المتصلة أو المرتبطة والى يمكن أن تقوم بمفردها أو مع مجموعة عناصر أخرى تنفيذ لبرنامج معين بأداء معالجة آلية للبيانات المعلوماتية، ويعني هذا الأخير كل تمثيل للواقع أو المعلومات أو المفاهيم تحت أي شكل، وتكون مهيئة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة يجعل الحاسوب يؤدي المهمة[1].

[1]– ربعي حسين، **أليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه في الحقوق، جامعة باتنة 01، الجزائر، السنة الجامعية 2016/2015، ص 11.

أما على مستوى التشريعات الوطنية فقد عرفها نظام مكافحة الجرائم السعودي في مادته الأولى بأنها "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية"، أما الشرع الأردني فقد تولى أيضا ابداء تعريف صريح للنظم المعلوماتية بقوله بأنَ نظم معالجة المعلومات هي ذلك النظام الالكتروني المستخدم لانشاء رسائل المعلومات وارسالها وتسليمها ومعالجتها أو تحزينها أو تجهيزها على أي وجه آخر وذلك وفق ما ورد في نص المادة 02 من قانون المعاملات الأردني رقم 05 لسنة 2001[1].

وهو الرأي الذي جاء به المشروع الجزائري بالقول بأن النظم 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"[2].

وبالعودة لمضمون التعاريف السابقة يمكن لنا أن نقترح تعريفا خاصا بالنظم المعلوماتي بأنها عبارة عن مجموعة من الحواسيب المنفردة أو المتصلة ببعضها البعض أو بواسطة شبكات داخلية أو خارجية تعمل بصفة آلية وفق برامج مصممة خصيصا لأجل تحقيق معالجة آلية للمعلومات[3].

[1]– ربيعي حسين، **المرجع السابق**، ص12.

[2]– المادة 02 من القانون المؤرخ في 14 شعبان 1430 الموافق ل 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة في 25 شعبان 1430 الموافق ل 16 أوت 2009.

[3]– ربيعي حسين، مرجع سابق، ص 12.

الفرع الثاني: مكـونات النظم المعلومـــات

لقد تم التطرق في هذا الفرع الى المكونات المادية للنظم المعلوماتية و شكل الاتصال كعنصر للنظم المعلوماتية .

أولا: المكـونات الماديـة للنظم المعلوماتية

أ) . التعريف الاصطلاحي للحاسوب:

يعرف الحاسوب بأنه آلة تقوم بأداء العمليات الحسابية واتخاذ القرارات المنطقية على البيانات الرقمية بوسائل الكترونية وذلك تحت تحكم البرامج المخزنة فيه[1].

كما يعرفه بأنه عبارة عن جهاز الكتروني يتكون من عنصرين مادي ومعنوي، يشمل الأول كل المكونات المادية في حين يشمل الثاني البرامج حيث يتم تشغيله على ضوء برنامج يتم تخزينه على ذاكرته ومن ثم يقوم باستقبال البيانات ومعالجتها على نحو المطلوب منه بغية الوصول إلى نتائج محددة.

ب) . التعريف الفقهي للحاسوب:

أما من ناحية الفقه فقد عرفه الفقه المصري بأنه "جهاز الكتروني يستطيع أن يقوم بأدق العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعة كبيرة قد تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وذلك على درجة عالية من الدقة وله القدرة عل التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة لها[2].

[1]– خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، الطبعة الأولى، دار الثقافة والتوزيع، عمان، الأردن، 2011، ص 39.

[2]– ربيعي حسين، مرجع سابق، ص 13.

ج) . التعريف القانوني للحاسوب:

للحاسوب نصيب من التعاريف القانونية، فقد عرفه المشرف السعودي في نص المادة الأولى من نظام مكافحة الجرائم المعلوماتية السعودي بأنه "أي جهاز الكتروني ثابت أو منقول سلكي يحتوي على نظام معالجة البيانات أو تخزينها أو ارسالها أو استقبالها أو تصفحها يؤدي وضائف محددة بحسب البرامج والأوامر المعطاة له.

أما من ناحية التشريع الجزائري فنجد أنَ القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها، لم يتطرق لتعريف الحاسب بالرغم من أنه يعتبر الوسيلة والقطعة الأساسية لأي نظام معلوماتي.

فإنَ فالحاسوب وفي مجال نظم المعلوماتي يعتبر الدعامة الأساسية وللتعامل مع المعلومات وذلك نظرا للسرعة والقدرة الهائلة التي يتمتع بها في هذا المجال وذلك لتوافر عدة خصائص مادية وأخرى منطقية تجعل منه فريدا من نوعه في هذا المجال.

1. المكونات المادية للحاسوب:

يقصد بالمكونات المادية للحاسوب الهيكل المادي المكون لنظم الحاسوب ويتكون أساسا من الوحدات الرئيسية التالية:

1. أ . وحدات الإدخال:

تستعمل هذه الوحدات لإدخال المعلومات أو الأوامر أو المعطيات أو البرامج المراد معالجتها إلى ذاكرة الحاسوب، وقد تكون في شكل وسائل إدخال مباشرة online، وتمثل غير مباشر off line وكغرفة الأقراص المدمجة، الماسح الضوئي[1].

[1]– نهلا عبد القادر، **الجرائم المعلوماتية**، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 24.

1. ب . وحدة المعالجة المركزية:

وتعتبر مركز الأنشطة في الحاسوب وتحتوي على دوائر كهربائية تترجم وتنفذ تعليمات برامج التشغيل.

1. ج . وحدة الذاكرة:

هي الوحدة التي تتم فيها عمليات التخزين المعلومات الواردة للجهاز أو النتائج الآنية من وحدة المعالجة المركزية.

1. د . وحدة الإخراج:

وهي الأجزاء والوحدات التي يتم من خلالها إخراج البيانات المعالجة من وحدة المعالجة المركزية على الخارج ومن أهم وحدات إخراج الشاشة والطابعة[1].

2. المكونات المنطقية للحاسوب:

تتكون هذه المكونات المنطقية في تطبيق العملية التي أجري أقل الكيان المادي للحاسوب وتتمثل في جملة البيانات والمعلومات، إضافة إلى برمجيات الحاسوب ولقد عرف القانون الأمريكي الصادر سنة 1988 الخاص لحماية حق المؤلف البرنامج software بأنها مجموعة من التوجيهات أو التعليمات التي يمكن للحاسب استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة، كما يعرفها العاملون في مجال الحاسوب بأنها الأوامر المرتبطة منطقيا والموجهة إلى الحاسوب بعد توجيهها إلى اللغة الوحيدة التي يفهمها وهي لغة الأرقام الثنائية[2].

[1]– ربعي حسين، مرجع سابق، ص14.

[2]– المرجع نفسه ، ص15.

ثانيا: شكـــل الاتصال كعنصر للنظم المعلومــاتية

يتكون النظام المعلوماتي في جملة من المكونات منها المتعلقة بالحاسوب من ماديات وبرمجيات ومنها ما يتعلق بشبكات الاتصال، وعليه فإنَ الجريمة المعلوماتية غلبا ما تنصب على استغلال هذه المكونات من حواسيب وشبكات اتصال باعتبارها القناة الرئيسية للوصول إلى المعلومات المخزنة والمتداولة بهدف الاعتداء عليها.

1. مفهوم شبكة الاتصال:

لشبكة الاتصال في مجال النظم المعلوماتية تعريف خاص يقصد به "أداة بين حاسوبين أو أكثر وهذه الرابطة قد تكون أرضية بالأسلاك والكابلات، كما يمكن أن تكون لا سلكية أو بالأشعة تحت الحمراء أو بالأقمار الصناعية، وشبكة يمكن أن تكون مقتصرة جغرافيا على منطقة صغيرة فتسمى شبكة محلية، كما يمكن أن تغطي منطقة كبيرة فتكون متسعة النطاق، ويمكن أن تكون متصلة ببعضها البعض.

وتعد شبكة الانترنت شبكة عالمية لأنها تتكون من العديد من الشبكات المتصلة ببعضها البعض[1].

2. تعريف شبكة الأنترنت:

تعتبر الأنترنت أكبر شبكة حواسيب موسعة تغطي جميع أنحاء العالم تتصل بين حواسيب شخصية وشبكات محلية أخرى عامة، يمكن لأي شخص حول العالم أن يصبح عضو في هذه الشبكة من منزله أو مكتبه او من أي مكان آخر بشكل يمكنه من الوصول إلى قدر هائل من المعلومات ويكفيه لذلك حاسوب مكتبي أو محمول وتقنية المودم[2].

[1]– ربعي حسين، مرجع سابق، ص16.

[2]– نهلا عبد القادر، مرجع سابق، ص 34.

فشبكة الانترنت عبارة عن وسيط ناقل للمعلومات من أجهزة الحاسوب المتصلة به بواسطة أنظمة التحكم في البيانات وبرتوكولات وعناوين خاصة TCPIIP حيث يتصل مستخدموها عن طريق الخط الهاتفي المتصل محول الإشارة المودم medeme الذي يقوم بتحويل الإشارة الرقمية ونقل الرسالة بين المرسل والمرسل إليه مرورا بالخادم.

إذن فشبكات الاتصال تعتبر عنصرا مهما في تكوين النظام المعلوماتي فلا جدوى من الحاسوب المنعزل من الشبكة في مفهوم النظام المعلوماتي مادام عاجزا عن التواصل مع باقي الحواسيب الأخرى، وفير قادر على إرسال أو استقبال المعلومات خصوصا وأن العالم اليوم يتمتع بأكبر نظام معلوماتي توفره له شبكة الانترنيت، هذه الأخيرة التي تقدم خدمات عديدة كتبادل المعلومات، البريد الإلكتروني، التعاقد عن بعد...إلخ. من خدمات أخرى أصبح الإنسان غير قادر على الاستغناء عنها نظرا لما تساهم به هذه الأخيرة من تذليل للصعوبات والعقوبات، غير أنها أصبحت المنفذ المنفصل لمجرمي المعلوماتية لأجل تحقيق أهدافهم الإجرامية، نظرا لاتصالها بأغلب الأهداف الإجرامية[1].

الفرع الثاني: تعريف المعلومـات

عرفها الفقه بأنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير والتأويل أو للمعالجة بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة حيث يمكن تغيرها وتجزئتها وجمعها ونقلها بوسائل وأشكال مختلفة ويذهب البعض إلى التفرقة بين المعلومات والبيانات (dgtg) وهي ما يطلق عليها بالتداخلات، وهي في حقيقتها عبارة عن مجموعة من الأرقام والكلمات أو الرموز التي لا علاقة لبعضها البعض، حيث أنها بعد معالجتها

[1]– ربعي حسين، مرجع سابق، ص35.

processing داخل الجهاز و الحصول على المخرجات output تكون في صورة معلومات infmgtion.

وتنقسم المعلومات إلى ثلاث طوائف: وهي المعلومات الاسمية وهي بدورها تنقسم إلى معلومات شخصية ومعلومات موضوعية، والمعلومات الخاصة بالمصنفات الفكرية، وهي المعلومات المحمية بين المؤلف أو الملكية الصناعية والتجارية والمعلومات المباحة، وهي التي يتاح للجميع الحصول عليها لأنها بدون مالك مثل: نشرات الأحوال الجوية أو تقارير اليومية للبورصة.

وعليه مما سبق يمكن تعريف المعلومات بأنها كل ما يصلح لتقديمه فائدة أو كل ما يصلح أن يكون محلا للتبادل أو التصرف فيه إلكترونيا سواء بالتخزين أو الإرسال بأي شكل كان من رموز أو صور أو بيانات يتم إرسالها وتبادلها عبر النظم المعلوماتية، يهدف إلى أمر معين ويكون ذا قيمة ما أغلبية ثقافية مالية اجتماعية[1].

المطلب الثاني: مفهــوم المعاينة

تعتبر المعاينة من أهم إجراءات التحقيق من أجل الحصول على دليل فيمكن للنيابة العامة أن تقوم به في غيبة المتهم، إذا تعذر حضوره فسنتطرق في هذا المطلب إلى تعريف المعاينة وأهميتها (الفرع الأول) ومعاينة مسرح الجريمة الإلكترونية (الفرع الثاني)، والتحليل الجنائي لمعلومات الجهاز (الفرع الثالث).

الفرع الأول: تعريف المعاينة وأهميتها.

لقد تم التطرق في هذا الفرع الى تعريف المعاينة مع تحديد أهميتها .

[1]– بن فريدية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، أطروحة دكتوراه في الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2015/2014.

أولا: تعريف المعاينة.

تأتي المعاينة بمعنى النظر في اللغة، وعاين الشيء رآه بعينه ودلالتها في اللغة تشير بمعنى الواسع إلى الرؤية والمشاهدة ودلالتها القانونية والخاصة في المجال الجنائي التي تعتمد على حاسة البصر، وتبعا لذلك تعني المعاينة رؤية أماكن ارتكاب الوقائع الجنائية، كما تتصرف إلى فحص جسم المجني عليه والمتهم وإثبات ما يوجد بها من أثار وعرفها جانب من الفقه بأنها مشاهدة واثبات الحالة في مكان الجريمة، وفي حالة لتجاوز جوهر المعاينة لمجرد الرؤية والمشاهدة وعدم انحسارها أو اعتمادها على حاسة النظر.

عرف بعض الفقه المعاينة بأنها إثبات مباشر ومادي لحالة الأشخاص والأماكن ذات الصلة بالحادث عن طريق رؤيتها أو فحصها حسيا مباشرا.

وبعض الفقه عرفها بأنها إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة ومرتكبها.

يتبين لنا من خلال المفاهيم والدلالات السابقة أنَّ جوهر المعاينة هو ملاحظة وفحص حسي مباشر لمكان أو شخص او شيء له علاقة بالجريمة لإثبات حالته والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة.

يجوز الالتجاء إلى المعاينة في كافة الجرائم، وهي إجراء هادف غايته كشف وصيانة العناصر المادية التي تتعلق بالجريمة وتفيد التحقيق الجاري بشأنها، فإذا انعدمت بالنسبة للتحقيق جدواها وفائدتها لم تكن ثمة مجال أو مقتضى لإجرائها، ولا تجدي في كشف الحقيقة بشأن المعاينة، مثل جريمة التصوير المعنوي، وجريمة القذف السب التي تقع بالقول في غير العلانية وغيرها[1].

[1]– صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، مذكرة لنيل شهادة الماجيستر في القانون، جامعة مولود معمري تيزي وزو، الجزائر، سنة 2013، ص 82-83.

ثانيا: أهمية المعاينة

تكمن أهمية وجدارة المعاينة عقب وقوع جريمة من الجرائم التقليدية في أنها تتبؤ مكانة الصدارة على ما عداها من الإجراءات الاستقصائية الأخرى، بحكم مركز المحورية لدورها في تصوير كنبضة وقوع جريمة وظروف وملابسات ارتكابها وتوفير الأدلة المادية من المادة التي تجمع عن طريقها وتمحيص وتقديم الأدلة الأخرى والتنسيق بينهما في ضوء المعلومات التي منها بما يكفل في ذات الوقت التخطيط السليم لعمليات البحث والتحقيق الجنائي وتطويرها.

إلا أنَ دورها في مجال كشف غموض الجرائم الأنترنيت، وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها إلى نفس الدرجة من الأهمية، ويمكن رد ذلك إلا أن هناك الدوام تقريبا مسرحا للجريمة التقليدية، جرت عليه الأحداث، وتركت آثارها المادية التي تنبثق من الأدلة، والمعاينة في مسرح الجريمة يتيح المجال أمام الباحث والمحقق الجنائي للكشف عن طريق معاينة الأثار المادية التي خلفها ارتكاب الجريمة والتحفظ على الأشياء التي تفيد في التحقيق الجاري بشأنها، بينما لا يعود عادة مسرح مماثل للجريمة المرتكبة عبر الأنترنيت وأقرب تشبيه لمسرحها قد يكون الموقع أو المكتب الذي توجد فيه المعدات والأنظمة المعلوماتية التي كانت محلا للجريمة أو أداتها[1].

يقلل مثل هذا المسرح إلى حد كبير من فرص إفصاحه عن الحقائق المراد التوصل إليها من وإزاء معاينة لسببين رئيسيين:

أولهما أن الجرائم التي تقع بواسطة المعلوماتية قلما يتخلف عن ارتكابها أثار مادية.

[1]– عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنيت**، دراسة متعمقة في جرائم الحاسب الآلي والانترنيت، بهجات للطباعة والتجليد، مصر، 2009، ص 220.

ثانيهما أن عدد كبير من الأشخاص يكون قد تردد على مكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا ، التي تقتضي عادة بين ارتكاب الجريمة و اكتشافها مما يفسح المجال لحدوث تغيير أو تلف أو عبث بأثار المادية أو زول بعضها و هو ما يلقي ظلالة من الشك على الدليل المستقى من المعاينة[1]

وينبغي لتفادي كل هذا وحتى يكون للمعاينة في الجرائم المتعلقة بشبكة الأنترنت فائدة في كشف الحقيقة عنها وعن مرتكبها مراعات عدة قواعد وإرشادات فنية أبرزها ما يلي:

1- تصوير الحاسب والأجهزة الطرفية المتصلة به على أن يتم تسجيل وقت وتاريخ التقاط كل صورة.

2- العناية الملاحظة الطريقة التي يتم بها إعداد النظام.

3- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجزاء عمليات المقارنة والتحليل حين عرض الأمر في بعد عن المحكمة.

4- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختيارات للتأكد من المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطسية يمكن أن يسبب في محو البيانات المسجلة.

5- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة الغير سليمة وفحصها ويرفع عليها البصمات ذات الصلة بالجريمة.

6- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومساهاة ما قد يوجد عليها من بصمات.

[1]- الصغير يوسف، مرجع سابق ص 85

7- قصر مباشرة المعاينة على الباحثين و المحققين الذين تتوفر لهم الكفاءة العلمية و الخبرة الفنية في مجال الحاسبات[1] .

الفرع الثاني: معاينة مسرح الجريمة:

تتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة غير أن الانتقال هنا يختلف بحسب طبيعة الجريمة الإلكترونية المرتكبة ولمعاينة مسرح هذه الجرائم يجب التفرقة بين حالتين:

أولا: معاينة الجرائم الواقعة على المكونات المادية للجهاز:

تتم المعاينة في جهاز الإعلام الآلي كشاشة العرض ومفتاح التشغيل والأقراص وغيرها من مكونات الجهاز ذات الطابع المادي المحسوس، فهي لا تثير أي مشكلة، حيث يمكن لضباط الشرطة القضائية معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

ثانيا: معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها:

المكونات المادية هي برامج الجهاز وبياناته وهذه المكونات تثير صعوبات كثيرة تحول دون فاعلية المعاينة أو فائدتها وهذه الصعوبات يمكن تلخصها فيما يلي:

. نقص وقلة الأثار المادية التي تقع على المكونات المادية للجهاز.

. تردد عدد كبير من الأشخاص على مسرح الجريمة خلال فترة زمنية قصيرة والتي غالبا ما تكون طويلة، وكذلك بين اقتراف الجريمة والكشف عنها[2].

[1]- الصغير يوسف، مرجع سابق ص 85، 86.

[2]- ماجد ياقوت، **أصول التحقيق**، دراسة مقارنة، الطبعة الثالثة، منشأ المعارف الإسكندرية، بدون سنة النشر، ص 70.

الفرع الثالث: التحليل الجنائي لمعلومات الجهاز.

تم التطرق في هذا الفرع الى مفهوم التحليل الجنائي و كيفية المحافظة على الادلة الرقمية المتحصل عليها من مسرح الجريمة .

أولا: مفهوم التحليل الجنائي:

هو استخدام تقنيات العلم والتكنلوجيا في عمليات التحقيق الجنائي للقضايا المخالفة للقانون وتتضمن فحص الجهاز أو المنظومة المعلوماتية وتحليل العمليات واسترجاع البيانات والملفات من أجل الحصول على دليل رقمي يستخدم في التحقيقات القانونية[1].

التحليل الجنائي الرقمي انسب أن يتم وفق معايير وإجراءات قانونية معتمدة من قبل المحكمة، وأهم هذه الإجراءات هو المحافظة على الأدلة الرقمية التي اكتشفها بدون أي تعديل أو أخريب أو توثيق كامل العمليات من لحظة الوصول لمكان الجريمة والعمليات التي تمت في مخبر التحليل الجنائي لحين وصول الدليل الرقمي إلى المحكمة التحليل الجنائي هو علم وهذا يعني أنك تتبع مبادئ علمية أثناء القيام بعملية التحقيق الجنائي الرقمي[2].

المطلب الثالث: إجراءات معاينة مسرح الجريمة

إنَ التشريع الجزائري وكغيره من التشريعات جاء لمجموعة من القواعد التي تعد وجوبية للقيان بالمعاينة، فأجاز المعاينة في الجنح وتكون وجوبية في الجنايات.

[1]– جميل حسين طويلة، **التحليل الجنائي الرقمي**، مكتبة النور، سوريا، ص10.

[2]– مرجع نفسه، ص11.

الفرع الأول: إخطار وكيل الجمهورية

لا يمكن معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إلا بعد إخطار وكيل الجمهورية بدائرة الاختصاص من قبل ضباط الشرطة القضائية[1].

وعملا بنص المواد 18، 32، 42، 63 من قانون إجراءات جزائية بالإضافة إلى نص 42 و49 من قانون القضاء العسكري من واجبات ضباط الشرطة القضائية، إذا ما عملوا بأي جريمة بأن يقوموا بإخطار وكيل الجمهورية سواء كان مدنيا أو عسكريا باعتباره المسؤول المباشر عن الشرطة القضائية على أن يكون الاخطار مسبوقا بتأكيد ضباط الشرطة القضائية من وقوع الجريمة فعلا[2].

الفرع الثاني: أوقات المعاينة

بالرجوع الى نص المادة 47 من قانون إجراءات جزائية، نرى بأن المشرع الجزائري جعل إجازات المعاينة و التفتيش و الحجز سواء كان المحل السكني أو غير سكني في كل الأوقات سواء تعلق الأمر بالنهار أو الليل دون تأخر في هذه الإجراءات وهذا عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كما يجوز لضباط الشرطة القضائية الاستعانة بأشخاص مؤهلين لذلك[3].

---

[1]– أحمد خريط، **الوجيز في الإجراءات الجزائية**، الطبعة الثانية، دار هومة، الجزائر، 2015، ص38.

[2]– حمزة أياة، **معاينة مسرح الجريمة ودوره في الكشف عن الحقيقة**، مذكرة لنيل شهادة الماستر في القانون الجنائي، كلية الحقوق، علي محمد الحاج، البويرة، سنة 2014، ص1.

[3]– انظر المادة 47من الأمر رقم 66–115 مؤرخ في 8 يونيو سنة 1966 يتضمن ق إجزائية معدل ومتمم لاسيما بالقانون 18–13 مؤرخ في 11 يوليو 2018.

الفرع الثالث: رضا صاحب المسكن

تطبقا للمادة 64 من قانون إجراءات جزائية لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المشبه فيها إلا بالرضا الصريح من الشخص الذي ستتخذ لديه هذه الإجراءات أو أن يكون هذا الرضا صريح، وكذلك أيضا بخصوص الجرائم الواقعة على النظم المعلوماتية [1].

ولنجاح المعاينة في الجرائم المعلوماتية يجب إتباع ومراعاة القواعد فنية وتتمثل فيما يلي:

- تفادي ضياع الوقت في التحقيق حول جرائم لا يمكن اكتشافها أو أن الأدلة اللازمة للاكتشاف وإثبات التهمة قضي عليها.
- ضرورة وجود نوع من التعامل بين المحققين وخبراء الحاسب الإلكتروني العاملين في المؤسسة المعين عليها.
- مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإلكتروني وغيرها من الحقوق.
- العناية بإصدار الأوامر القضائية الخاصة بالتفتيش والضبط وأجهزة الحاسب الآلي الإلكتروني وملحقاته وبرامجه.
- مراعاة حفظ الأدلة الجنائية بالطرق المناسبة كل حالة على حدا وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي طبق عليها.

- والاستعانة بتقنيات المتطورة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية لاسيما أنَ هذه التقنيات أثبتت جدارتها ونجاحها في جميع الأدلة الجنائية وصناعة البنية الاتهامية[2].

[1]– أنظر المادة 64 من قانون إجراءات جزائية السالف الذكر.

[2]– فهد عبد الله العبيد العازمي، **إجراءات الجنائية المعلوماتية**، دار الجامعة الحديثة، دار النشر الإسكندرية، 2016، ص 340.

المبحث الثاني: التفتيش والحجز في النظم المعلوماتي

يهدف التفتيش والحجز في النظم المعلوماتية إلى الكشف عن الجريمة ومرتكبها وذلك من خلال ضبط الأدلة المادية المتعلقة بالجريمة وذلك من خلال حفظ الوسائط الإلكترونية (الأسطوانات والأقراص) والحجز يكون من خلال وضع اليد والحجز للدعائم المادية المخزنة فيها البيانات الإلكترونية، وللجريمة المعلوماتية إجراءات تطبق على الجرائم التقليدية في حالة التفتيش والحجز، وسنتناول في هذا المبحث القواعد الاجرائية للتفتيش والحجز، وسنتناول أيضا بعض البرامج المستخدمة أثناء المعاينة والتفتيش والحجز.

المطلب الأول: تعريف التفتيش والحجز.

يتم التطرق في هذا المطلب الى تعريف التفتيش بالاضافة الى تعريف الضبط في البيئة الرقمية .

الفرع الأول: تعريف التفتيش

تعددت التعريفات الفقهية التي تناولت مصطلح التفتيش، فقد عرفه البعض بأنه "إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة، وهو ينطوي على مساس حق المتهم في سرية حياته الخاصة"كما عرفه آخرون بأنه "إجراء من إجراءات التحقيق

بهدف إلى التوصل إلى أدلة جريمة ارتكبت فعلا، وذلك بالبحث عن الأدلة في مستودع سواء أجري على شخص المتهم أو في منزله دوم التوقف عن إرادته[1].

أما الفقه الفرنسي عرفه بأنه "بحث بوليسي أو قضائي عن عناصر الدليل عن جريمة ما ويمكن وفقا لقواعد قانونية خاصة أن ينفذ في السكن الخاص بأي شخص أو في مكان آخر حيث يمكن أن توجد أشياء يكون اكتشافها مفيدا في إظهار الحقيقة.

[1]– ابن فردية محمد، مرجع سابق، ص 128.

وعليه يمكن القول بأن التفتيش عبارة عن إجراء من إجراء التحري والتحقيق يقوم به موظف قضائي، أو تحت سلطة القضاء بموجب إجراءات محددة في قانون الإجراءات الجزائية بهدف الحصول على الدليل الجنائي، ومن ثم تقديمه إلى القضاء[1].

الفرع الثاني: تعريف الضبط في البيئة الرقمية

يقصد بالضبط في البيئة الرقمية وضع اليد على شيء يتصل بجريمة معلوماتية وقعت، يفيد في كشف الحقيقة عنها وعن مرتكبها، ترد على منقولات يصطلح عليها بالمنقولات المعلوماتية والتي تتمثل في مكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، كما يمكن نقل المعالجة إلكترونيا أو المعلومات من حاسب معين إلى حواسب أخرى سواء عن طريق شبكات الاتصال المرتبطة بينها أو عن طريق الأقراص والشرائط الممغنطة، وهو ما يطلق عليها المراسلات الالكترونية، وإذا كناقدون توصلنا إلى إمكانية التفتيش في المكونات المعنوية للحاسوب وبالتالي إباحة ضبطها[2].

المطلب الثاني: القواعد الإجرائية للتفتيش والحجز داخل المنظومة المعلوماتية

يعتبر التفتيش إجراء من إجراءات التحقيق التي تهدف إلى الحصول والبحث عن الدليل وكل ما يفيد في كشف ملابسات الجريمة وذلك وفق قواعد إجرائية وتتمثل في إجراء الإذن، إجراء التفتيش والحجز بحضور أشخاص معنيين قانونيا، مواعيد التفتيش والحجز، ورضا المشتبه فيه بالتفتيش.

[1]– بن فردية محمد، مرجع سابق، ص 128– 129.

[2]– مرجع نفسه، ص 142.

الفرع الأول: إجراء الإذن

تنص المادة 44 من قانون إجراءات جزائية الجزائرية على ضرورة أن يكون التفتيش بناءا على إذن مكتوب صادر من وكيل الجمهورية، أو قاضي التحقيق مع وجوب استظهار هذا الإذن قبل الدخول وشروع التفتيش في نظم الحاسوب الآلي.

إنَ التفتيش نظم الحاسوب الآلية يتطلب مذكرة قضائية تجيز التفتيش أنظمة الكمبيوتر، فإجزاء التفتيش دون تلك الذكرة مسألة تثير الكثير مع بعض المعارض خاصة في ظل ما يتقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد[1].

الفرع الثاني: إجراء التفتيش والحجز بحضور أشخاص معنيين قانونيا

من بين هذه الأشخاص من بين هذه المشبه، المتهم القائم بالتفتيش والشاهدين فالأصل في التفتيش وكما عرفته القواعد الخاصة بالتفتيش يتم هذا الإجراء بحضور المتهم أو من يجوز أن يمثله، يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين للسلطة، إلا أن المشرع الجزائري استثنى على هذه القواعد في نص المادة 45 من قانون إجراءات جزائية الجزائري على أنه لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الأولية للمعطيات إذ يمكن تفتيش المنظومة المعلوماتية بدون حظور المتهم أو المشاهدين[2].

[1]– أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، ص 62.

[2]– – ناصر جوادي، إجراءات التحري الخاصة في ضل قانون الإجراءات الجزائية، دار العلوم، الطبعة الثالثة، الجزائر 2011، ص 47

الفرع الثالث: مواعيد التفتيش والحجز

كقاعدة عامة بخصوص الجرائم التقليدية فإن تفتيش الأماكن الخاصة لا يكون قبل المساعدة الخامسة صباحا إلا ولا يعد الساعة الثامنة مساءا والعبرة يساعده للدخول إلى المنزل إلا إذا طلب صاحب المنزل ذلك واجهت نداءات من داخل المنزل فهو سبب من أسباب الاتاحة الجزائية للدخول إلى المنازل.

غير أن تفتيش المنظومة المعلوماتية لا يخضع لهذه القواعد إذ نص المشرع على أنه يجوز إجراء التفتيش والحجز في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في كل ساعة من ساعات النهار والليل بناء على إذن سبق من وكيل الجمهورية المختص وهذا ما نصت عليه المادة 47 فقرة 3 من قانون إجراءات جزائية كونها حالة من حالات الاستثنائية التي أقرها القانون[1].

استثنى المشرع الجزائري هذه الضمانات على طائفة من الجرائم المذكورة في هذه من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والملاحظة أن المشرع غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ حريتهم الخاصة لاسيما حرمة المسكن باعتبار مستودع أسرارهم، إلا أن ما يبرر ويقل من خطورته الطبيعة الخاصة لهذه الجرائم خاصة الجريمة الالكترونية وطبيعة الدليل لإثباتها فهو قابل للمحو والتعديل في أقل من ثانية لأن مرتكبها ذو دراية بالأمور التقنية وما يوجد من الصعوبة إذا كان هذا الدليل الإلكتروني هو الوحيد في الدعوى الجنائية، أما بالنسبة للأماكن العامة فإذا وجد الشخص في هذه الأماكن و هو يحمل معه ما هو مكونات الحاسوب

[1]– ناصر جوادي، مرجع سابق، ص 48.

سالفة الذكر أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها التفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[1].

الفرع الرابع: تحرير محضر التفتيش

باعتبار أن التفتيش من أعمال التحقيق لابد من تحرير محضر يثبت فيه ما أسفر التفتيش عنه من أدلة والقانون لم يتطلب شكلا خاصا وبالتالي لصحة محضر التفتيش نظم الحاسوب لا يشترط سوى ما يستجوبه القواعد العامة في المحاضر عموما، بأن يكون مكتوبا باللغة الرسمية وأن يكون مؤرخا وموقعا عليه، كما يجب أن يتضمن كافة الإجراءات المتبعة من طرف الشخص المتخصص في الحاسوب والانترنت الذي

الاستعانة به في مجال الخبرة الفنية الضرورية [2].

المطلب الثالث: إجراءات تفتيش نظم الحاسوب المادية والمعنوية

يعتبر التفتيش إجراء من إجراءات التحقيق الابتدائي، يهدف إلى لبحث عن أدلة الجنائية أو جنحة ثبت ارتكابها في محل، وذلك من أجل الكشف والوصول إلى الحقيقة وينقسم التفتيش في الجريمة لإلكترونية إلى تفتيش نظم الحاسوب المادية والتفتيش في نظم الحاسوب المعنوية، وستطرق إليهما في فرعين متتاليين، التفتيش في نظم الحاسوب المادية (الفرع الأول) التفتيش في نظم الحاسوب المعنوية (الفرع الثاني)

[1]– ليندا بن طالب، **التفتيش في الجرائم المعلوماتية**، مجلة العلوم القانونية والسياسية، العدد 22، جوان، 2017، ص 494.

[2]–المرجع نفسه ص 494.

الفرع الأول: التفتيش في نظم الحاسوب المادية

تخضع عملية تفتيش المكونات المادية للكمبيوتر لنفس القواعد والإجراءات القانونية المرسومة له في قانون إجراءات جزائية إذ ما تعلق بجريمة معلوماتية بهدف الكشف عن الحقيقة والوصول إلى مرتكبها ولكن يتوقف جواز تفتيش تلك المكونات على المكان التي تكون موجود به، بحيث إذا كانت موجودة في مكان خاص كمسكن المتهم فلا يجوز تفتيشها إلا طبقا للقواعد الخاصة بإجراء التفتيش، طبقا لما هو منصوص عليه في قانون الإجراءات الجزائية، كما يجب التميز بينهما إذا كانت تلك المكونات المادية متصلة بكمبيوتر آخر وبنهاية طرفية آخر في مسكن آخر غير مسكن المتهم ففي هذه الحالة يجب مراعاة الضمانات المقرر لتفتيش تلك الأماكن[1].

أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الإلكتروني المادية أو كان مسيطرا عليها أو حائز لها، فإن تفشيها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في التشريعات المختلفة[2].

الفرع الثاني: التفتيش في نظم الحاسوب المعنوية

كانت ولاتزال هذه المكونات تؤرق الكثير من المحققين رغم التطور العلمي الذي وصلنا إليه ورغم التدريبات التي تخضع لها هذه الجهة المكلفة بالتحقيق إلى أن هذا التطور في هذا المجال لا يطال فقط رجال الضبط القضائي المكلفين بالتحقيق وإنما يستفيد منها أيضا الهاكرز، ويتم تفتيش المكونات المعنوية عن طريق فحص نظام التشغيل، ولعل أهم إحدى الطرق التي ساهمت فيها شركات صنع معالجة الكمبيوتر يجعل المعالجة بمثابة أداة لتسجيل هوية مالك الكمبيوتر إلى جانب أنه محرك هذا الجهاز

[1]– خالد عطية، عارف فراج، **مكافحة الجريمة المعلوماتية**، دراسة مقارنة بين التشريع الجزائري والفلسطيني، مذكرة لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، جامعة المدية، ص 79، 80.

[2]– فهد عبدالله العبيد العازمي، مرجع سابق ص 265.

المحققين يعتمدون عليه للاستغناء المعلوماتي ، وقد يحرك كذلك تفتيش الشبكة المعلوماتية رغم أن هذا الاحتواء صعب قليلا ويحتاج لوقت وجهد فيلجأ المحققون إلى الشريكات المسؤولة عن تزويد المنطقة بالأنترنت ويضيف نطاق البحث حول المنطقة التي وقع فيها الاعتداء ويفحصون كل نشاطات الأشخاص الذين يقطنون فيها أو الأشخاص الذين لهم صلة بالمجني عليه[1].

أثار تفتيش المكونات المعنوية للحساب الآلي خلاف كبير في الفقه بشأن جواز تفتيشه، فذهب رأي إلى جواز ضبط البيانات الالكترونية بمختلف أشكاله ويسند هذا الرأي إلى القوانين الإجرائية عندما تنص على إصدار الإذن بالضبط أي شيء لذلك يجب تفسيره بحيث يشمل بيانات الحاسوب المحسوسة والغير محسوسة، وذهب رأي إلى عدم انطباق المفهوم المادي على بيانات الحساب المحسوسة وغير المحسوسة، وذهب رأي إلى عدم انطباق المفهوم المادي على بيانات الحساب الغير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور الصرحي بالنص صراحة على أن تفتيش الحساب الآلي لابد أن يشمل المواد المعالجة عن طريق الحاسب الآلي، أو بيانات الحاسب الآلي، بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد ترتكز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحساب يوجد في المقابل هذين الرأيين بوجود رأي آخر يأتي بنفسه عن البحث عن ما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الحساب الآلي أم لا، فذهب إلى

[1]– الدكتور كبير بعقيقي، الدكتور فيصل ماصيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 04-09، مجلة العلوم القانونية والسياسية، العدد 02، جوان 2018، ص 46.

النظر في ذلك يجب أن يسند إلى الواقع العملي الذي يتطلب أن يقع الضبط عن بيانات الحساب الآلي إذا اتخذت شكلا ماديا[1].

المطلب الثالث: إجراءات معاينة مسرح الجريمة الالكتروني .

بعض البرامج المستخدمة أثناء المعاينة والتفتيش والحجز إضافة إلى القواعد الإجرائية الخاصة بالتفتيش والحجز، وإجراء تفتيش نظم الحاسوب المادية والمعنوية من خلال ما تطرقنا إليه في المطلبين السابقين، فقد خصصنا المطلب الثالث لبعض البرامج والتقنيات المستخدمة أثناء التفتيش والمعاينة والحجز داخل المنظومة المعلوماتية، حيث وجب على الجهات المختصة والمكلفة بالبحث والتحري عن الجريمة ومرتكبيها، ‘استخدام برامج تساعدها في الكشف عن الجريمة المعلوماتية في جانبها التقني، حيث سنتطرق إلى تقنية فحص البروكسي (الفرع الأول) برنامج التتبع المعلوماتي (الفرع الثاني) نظم كشف الاختراق (الفرع الثالث).

الفرع الأول: تقنية فحص البروكسي (proxy):

البروكسي هو وسيط العامل بين الشبكة والمستخدم تستخدمه الشركات المقدمة لخدة الاتصال لأجل إدارة الشبكة وضمان أمنها وتوفير حزمة الذاكرة الجاهزة cash memory.

يعمل البروكسي على طلب تلقي المستخدم للبحث عن صفحته ما فيحقق البروكسي ضمن الذاكرة الجاهزة عما إذ جرى تنزيل الطلب من قبل بإعادة إرسالها إلى المستخدم دون الحاجة إلى طلبها من الشركة العالمية للمعلومات واب من أجل تزويد المستخدم ومن مزاياه أن ذاكرته هذه يمكن أن تحتفظ بتلك

[1]–صغير يوسف، المرجع السابق، ص70.

المعلومات والعمليات وهو ما ينتج لضباط الشرطة القضائية فحصها واستخلاص الدلائل ضد المتهم وذلك من خلال تلقي أثار بمساعدة مزود الخدمات[1].

الفرع الثاني: برنامج تتبع المعلومات

تقوم برامج تتبع المعلومات على شاكلة برنامج hachiracer بالتعرف على محاولات الاختراق ومن قام بها وإشعار الجهة المتضررة بذلك، وهذه البرامج عادة ما تكون ساكنة في خلفية المكتب عندما ترصد أي محاولة للقرصنة أو الاختراق وتسارع بغلق منافذ الدخول للمخترق، ثم تبدأ بعملية مطاردة واقتناء أثره وصولا إلى تحديد عنوانه الإلكتروني (ip) و اسم الشركة المزودة بخدمة الانترنت معلومات أخرى[2].

الفرع الثالث: نظام كشف الاختراق ntrlision.petection

وهو النظام الذي يرمز له ب ips وهو نظام يعتمد على مجموعة من البرامج التي تولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب والشبكة من خلال مقارنة نتائج التحليل مع الصفاة المشتركة للاعتداءات المعلوماتية، ففي حال استئناف، يبادر لتسجيلها في مسجلات حاسوبية خاصة registre وهي السجلات التي يسعى لها ضباط الشرطة القضائية لتحليل أسلوب ارتكاب الجريمة وربما مصدرها[3].

[1]– ربعي حسن، مرجع سابق، ص 229.

[2]– مرجع نفسه ص 229.

[3]– نفسه ص 230.

الفصل الثاني:

الاجراءات المستحدثة للتحري والكشف عن الجرائم داخل المنظومة المعلوماتية (الاجراءات الحديثة)

تمهيد

إن الإجراءات المستحدثة للتحري والكشف عن الجرائم داخل المنظومة المعلوماتية، جاءت بعدما أصبحت الإجراءات المنصوص عليها في قانون إجراءات جزائية لم تعد تجدي نفعًا، فالمشرع الجزائري وكغيره من التشريعات ومع مواكبة التطور التكنولوجي قام بإصدار تشريع جديد وهو القانون 04/09 الصادر في 14 شعبان 1430 الموافق لـ 5 غشت سنة 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وهو جاء مكملاً للقواعد العامة المنصوص عليها في قانون إجراءات جزائية.

المبحث الأول: الإجراءات الواردة في قانون إجراءات جزائية وقانون 09-04

نظرًا لتطور الوقت وتماشيًا معه وتراجع أساليب البحث والتحري التقليدية في مكافحة الجريمة المعلوماتية المستحدثة أصبح من الضروري البحث عن أساليب وطرق مستحدثة، تتماشى مع التطور الذي عرفته هذه الجرائم من أجل تسهيل الكشف عن الجريمة وتحديد مرتكبها وتقديمهم إلى الجهات المختصة من أجل المحاكمة، حيث قام المشرع الجزائري من خلال استحداث إجراءات خاصة للحصول على الدليل في بعض الجرائم، ومنها الجريمة المعلوماتية من خلال ما جاء في القانون 06-22 المؤرخ في 20-12-2006 المعدل لقانون الإجراءات الجزائية، وكذلك استحدث المشرع القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وسنتطرق في هذا المبحث إلى الإجراءات الواردة في قانون إجراءات جزائية (مطلب أول)، والإجراءات الواردة في القانون 09-04 (مطلب ثاني).

المطلب الأول: الإجراءات الواردة في قانون إجراءات جزائية

إن القانون 06-22 المؤرخ في 20-12-2006 المعدل لقانون إجراءات جزائية، استحدث مجموعة من الإجراءات، من أجل مواجهة بعض الجرائم المستحدثة من بينها الجريمة المعلوماتية وهي إجراءات خاصة، سنتطرق إليها من خلال مطلبنا هذا على النحو التالي: الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور. الفرع الثاني: التسرب.

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

سنتطرق في هدا الفرع الى (اعتراض المراسلات السلكية واللاسلكية).(وضع الترتيبات التقنية)

أولا: اعتراض المراسلات السلكية واللاسلكية

تعد الاتصالات التي يجريها الشخص أيا كانت نوعيتها عنصر من عناصر الحق في الحياة الخاصة، فلا يجوز لغير الشخص الموجه إليه هذه المراسلات الاطلاع عليها، لأن الاتصال مهما كانت وسيلته يعتبر مستودعًا لسر الإنسان وخصوصياته، فالتصنت على المحادثات التي يجريها الشخص على شبكة الانترنت أو الاطلاع على رسائله الإلكترونية سواء بكشف كلمة السر أو باعتراض هذه المراسلات يعد انتهاكًا للخصوصية ومساسًا بحرمة الحياة الخاصة، يترتب عنه مسؤولية جزائية لمرتكب هذا الفعل[1].

وقد ضمن الدستور الجزائري سرية المكالمات الهاتفية وكل الاتصالات بأشكالها المختلفة، وذلك ما جاءت به نص المادة 46 من الدستور الجزائري لسنة 2016 بنصها على: <<لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون>>[2]

1-المقصود باعتراض المراسلات:

تم تعريف اعتراض المراسلات بأنه: <<إجراء تحقيقي يباشر خلسة ويهتك سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانونًا بهدف الحصول على دليل غير مادي للجريمة ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، وهو ما يعد وسيلة هامة من الرسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية في مواجهة الإجرام الخطير وتتم عبر وسائل الاتصال السلكية واللاسلكية، ويختلف اعتراض المراسلات عن وضع الخط الهاتفي تحت المراقبة الذي يتم برضا

[1] عقد القادر عميمر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري، أطروحة دكتوراه، علوم في القانون العام، تخصص قانون جنائي وعلوم جنائية، جامعة الجزائر 1، السنة الجامعية 2019-2020، ص 261.

[2] المادة 46 من الدستور الجزائري.

صاحب الشأن>>، ولم يتطرق المشرع الجزائري لتعريف اعتراض المراسلات بتاريخ 16-02-1989 بأنه: <<تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفي لشخص ما مع اللجوء إلى تسجيل المكالمات في أشرطة مغناطيسية>>[1].

2- شروط اعتراض المراسلات:

أ-ضرورة الحصول على إذن مسبق:

يتم إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط صور بقصد التحري والتحقيق عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإذن من وكيل الجمهورية المختص وتباشر تحت مراقبة وكيل الجمهورية، وبالرجوع إلى المادة 4 من القانون 09-04 الذي جاء فيه أنه لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطات القضائية المختصة.

يحرر ضابط الشرطة القضائية عند مباشرة التحريات والتحقيقات محضر عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط الصور وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط أو التسجيل الصوتي أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها بعد أن يصنف وينسخ ضابط الشرطة القضائية المراسلات أو الصور أو المحادثات المسجلة أو المقيدة في إظهار الحقيقة في محضر يودع بملف، وتنسخ وتترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم مسخر لهذا الغرض[2].

ب- كتمان السر المهني:

يسمح الإذن لضباط الشرطة القضائية المأذون له أو النائب باعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور دون المساس بالسر المهني، وجسد المشرع الجزائري هذه

[1] عبد القادر عميمر، مرجع سابق، ص 262.
[2] ناصر جوادي، مرجع سابق، ص 70.

الحماية من خلال تعيين الأشخاص المؤهلين للاطلاع على الأسرار وفرض عقوبات على من يفشي أسرار الناس مخالفة للقواعد الإجرائية الجزائية ووضع قواعد وضبط الإجراءات الواجب على أعضاء الشرطة القضائية اتباعها[1].

3- نطاق إجراء اعتراض المراسلات السلكية واللاسلكية:

إن الإذن المسلم من طرف وكيل الجمهورية لغرض وضع الترتيبات التقنية يسمح بالدخول إلى المحلات السكنية أو غيرها خارج المواعيد القانونية وبغير علم أو رضا الأشخاص الذين لهم الحق على تلك الأماكن وهو خروج عن القواعد العامة المحدد في المادة 47 من قانون إجراءات جزائية، ويباشر هذا الإجراء تحت المراقبة المباشرة لوكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي يتم بناءًا على إذن من قاضي التحقيق وتحت مراقبته المباشرة.

ويؤهل الإذن المشار إليه ضباط الشرطة القضائية لتسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية بالجوانب التقنية للعمليات وكذا مترجم لترجمة المكالمات التي تتم باللغات الأجنبية.

كما يلزم القانون ضباط الشرطة القضائية المأذون لهم بإجراء هذه العمليات تحرير محضر كل عملية اعتراض، وتسجيل المراسلات، وكذا عن عمليات وضع الترتيبات التقنية والالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري كما يجب على ضباط الشرطة القضائية وصف أو نسخ المراسلات أو الصور أو المحادثات المسجلة والمفيد في إظهار الحقيقة على محضر يودع بملف القضية.

[1] جميلة محلق، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاتصال والإدارة القانونية، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، العدد 42، ص 181.

وفي حالة اكتشاف جرائم أخرى أثناء تنفيذ عمليات اعتراض الاتصالات السلكية واللاسلكية غير تلك التي تم ذكرها ضمن الجرائم المحددة في الإذن فإن ذلك لا يؤدي إلى بطلان إجراءات الكشف والضبط بل تأخذ حكم الواقعة الملتبس بها طبقًا لأحكام المادة41 من قانون إجراءات جزائية ويحدد قانون إجراءات جزائية الإذن سواء الممنوح من طرف وكيل الجمهورية أو قاضي التحقيق لمدة أقصاه 4 أيا مقابلة للتجديد حسب مقتضيات التحري أو التحقيق[1].

ثانيا: وضع الترتيبات التقنية

يسمح الإذن بوضع الترتيبات التقنية دون موافقة المعنيين ودون علمهم أذ يجوز لضباط الشرطة القضائية ولأي عون مؤهل مسخر من طرفه دخول المساكن لوضع أجهزة الاعتراض والتنصت والتصوير والتسجيل دون التقيد بالزمن المحدد في المادة 47 ق إ ج، ودون العلم ورضا صاحب المسكن وذلك يعد خروجًا صريحًا من المشرع عن شروط التفتيش وهناك من يرى إجراء مراقبة المكالمات الهاتفية إجراء من نوع خاص إجراء يماثل التفتيش لكنه ليس في الحقيقة تفتيشا.2

1- وضع الترتيبات التقنية بغرض التقاط وتثبيت وتسجيل الأصوات

يعد تسجيل الأصوات من الوسائل العلمية الحديثة التي أدرجت والتي عرفها البعض بأنه نوع من استراق السمح يسلط على الأحاديث الخاصة والمحادثات التلفونية، خلسة دون علم صاحبها بواسطة أجهزة إلكترونية أسفر عنها النشاط العلمي الحديث وفي حين عرفها البعض الآخر بأنه: <<حفظ الأحاديث الخاصة على المادة المخصصة لإعادة الاستماع إليه>>[2].

يتم تسجيل الأصوات والتنصت الهاتفي عن طريق الدخول على الخط المراد مراقبته لاسلكيًا بواسطة سماعة تلفونية يمكن توصيلها بأجهزة تسجيل، حيث يتم ربط سلكي هذه السماعة إلى سلك دائرة

[1] عبد القادر عميمر، مرجع سابق، ص 263.

[2] مرجع نفسه، ص 264.

المشترك في مكان ما هذا النوع من التنصت الهاتفي هو طريقة قديمة يسهل اكتشافها بسبب ما تحدثه سماعة التنصت من تغيرات تطرأ على التيار بسبب التداخل.

كما يمكن التقاط وتسجيل محادثات مشتركة مغناطيسيًا دون وجود اتصال سلكي مباشر مع الخط المشترك، وذلك عن طريق سلك آخر خارجي يوضع بجانب سلك المشترك يتداخل معه مغناطيسيًا وتوصل به سماعة المتنصت، وظهر مؤخرًا جهاز جديد أطلق عليه (TX)يسمح بالدخول إلى الخط الهاتفي من بعيد دون أن يشعر أحد بذلك، ويستطيع تحويل الخط إلى جهاز إرسال ينقل جميع المكالمات التي تجري من خلاله[1].

ولقد ثار جدول حول مدى إمكانية الاعتماد على الدليل المستمد من أجهزة التسجيل كدليل في الإثبات الجنائي، فقد تردد القضاء في الأخذ بالأحاديث المسجلة أو طرحها في مجال الإثبات الجنائي، ولم يكن الخلاف في جانب القضاء فحسب بل كان هناك اختلاف في الفقه حول مشروعية الدليل المستمد من أجهزة التسجيل وظهرت في ذلك ثلاث اتجاهات.

الاتجاه الأول: يرى أن تسجيل المحادثات إجراء غير باطل وأنه يمكن الاستعانة بالأجهزة الحديث لخدمة القضاء وتحقيق العدالة، وبأنه ليس هناك انتهاك لحركة الانسان طالما أن هذه المحادثات صدرت منه طوعًا واعتيادًا دون تأثير أو إكراه.

الاتجاه الثاني: يرى أصحاب هذا الاتجاه بأن التسجيل الذي يقع خلسة هو إجراء باطل بطلانًا مطلقًا لأنه يشكل تعديًا على حقوق وحريات الإنسان، وأكثر من ذلك فإنهم يرون بأنه إجراء باطل حتى لو كان بإذن القاضي.

[1] روابح فريد، الأساليب الإجرائية الخاصة للتحري والتحقيق في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه، قانون عام، قانون جنائي والعلوم الجنائية، كلية الحقوق، الجزائر، 2016، ص 306-307.

الاتجاه الثالث: وهو الاتجاه الذي يرجح بين الرأيين السابقين حيث يرى أنصار هذا الاتجاه بأنه إذا كان الحديث في مكان عام مثل النوادي أو الأسواق أو المقاهي فيكون التسجيل في هذه الحالة مشروعًا، وأما إذا كان الحديث في مكان خاص كأن يتم في مسكن الشخص أو في سيارته فهنا يكون التسجيل باطلاً[1].

2- وضع الترتيبات التقنية بغرض التقاط الصور في الأماكن الخاصة:

تعد عملية التقاط الصورة إحدى الآليات المستحدثة التي اعتمدها المشرع الجزائري لمكافحة بعض الجرائم الخطيرة ومنها الجريمة المعلوماتية خروجًا عن الأصل العام الذي يمنع التقاط الصورة خلسة دون رضا صاحبها لما يترتب عن ذلك من تحدي على حق الخصوصية.

والمقصود بالحق في الصورة يقصد ه الانتشار الذي يتيح للشخص منع غيره من أن يرسمه او أن يلتقط له صورة من دون إذن منه صريح أو ضمني وما يستتبع ذلك من حقه في الاعتراض عن نشر صورته على الجمهور، ويعد الحق في الصورة من أبرز مظاهر الحياة الخاصة للفرد. وقد تم الاعتراف بهذا الحق في منتصف القرن التاسع عشر كحق من حقوق الإنسان وكفلت حمايته المواثيق ودساتير الدول ومنها الدستور الجزائري كما جرم قانون العقوبات الجزائري انتهاك الحق في الصورة[2].

[1] عبد القادر عميمر، مرجع سابق، ص ص 264-265.

[2] مرجع نفسه ، ص 265.

الفرع الثاني: التسرب

سنتترق في هدا الفرع الى (تعريف التسرب).(شروط صحة التسرب)

أولا: تعريف التسرب:

1-لغة: الولوج والدخول بطريقة مختفية إلى مكان معين أو جماعة معينة ويبعث في اعتقادهم أن المتسرب ليس شخصًا غريبًا عنهم، وإنما هو عضو منهم ومن خلال ذلك يمكن له معرفة انشغالهم وأهدافهم الإجرامية ونواياهم المسبقة قبل ارتكاب الجريمة[1].

2- التعريف القانوني للتسرب: يعد التسرب طريقة من الطرق الأمنية الحساسة والخطيرة في نفس الوقت وتستوجب العملية تحضيرًا دقيقًا وتنظيمًا متناهيًا ماديًا ومعنويًا للتوغل ضمن الوسط الإجرامي المستهدف، للتعرف على الجريمة وعناصرها وتحديد دور كل واحد من المجموعة البشرية، والوقوف على نواياهم وأهدافهم الإجرامية، عن طريق الملاحظة والتسجيل لأدق تحركاتهم، وعلى الضباط او العون المتسرب التعمق في البحث والتحري لتحديد أدق خصوصيات وتفاصيل نشاط وعمل هذه الجماعات[2].

ونصت المادة 65 مكرر 12 من قانون إجراءات جزائية الجزائري بأنه: <<يقصد بالتسرب قيام ضباط 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 .....>>[3]

ومن خلال هذا التعريف نلاحظ أن هذا الإجراء يقتضي التواجد في الوسط الإجرامي موضوع عملية التحقيق والاحتكاك المباشر مع المشتبه فيهم عن طريق التنكر والخداع، وكسب ثقة المشتبه فيهم من أجل

[1]..مجراب. الدوادي، الأساسي الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة دكتوراه علوم في القانون، كلية الحقوق، جامعة الجزائر 1، السنة الجامعية 2015-2016، ص 325.

[2]4. المرجع نفسه ، ص 325.

[3] القانون رقم 06-22، السالف الذكر.

الحصول على معلومات دقيقة وتحديد نقاط قوة وضعف الجماعة موضوع المراقبة والتحقق واكتشاف أعضائها ووسائل التواصل بينهم وامتدادات هذه المجموعة، ويمكن للعضو المتسرب أن يكون فاعلاً أصليًا في الجريمة من خلال القيام بالأفعال المادية للجريمة مما يوحي بأنه يمثل مركزًا مباشرًا في تنفيذ العمل الإجرامي، دون أن تشكل هذه الأفعال تحريضًا لأنه لا يجوز قانونًا للعون المتسرب ان يكون بأي حال من الأحوال فاعلاً معنويًا، أو محرضًا وإلا تعرض هذا الإجراء للبطلان طبقًا لأحكام المادة 65 مكرر 2/12[1].

ثانيا: شروط صحة عملية التسرب:

إن المشرع الجزائري قيد عملية التسرب بشروط شكلية وأخرى موضوعية:

1-الشروط الشكلية: من بين الشروط التي تتطلبها عملية التسرب التي حددها قانون إجراءات جزائية الجزائري نذكر منها ما يلي:

- صدور إذن بالتسرب من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية المختص، أي لا يمكن ضباط الشرطة القضائية القيام بهذا الإجراء بدون أخذ الإذن والموافقة من طرف قاضي التحقيق أو وكيل الجمهورية بالإضافة إلى إعلام وكيل الجمهورية المختص إقليميًا لجهة إجراء عملية التسرب.
- أن يوجه الإذن لضباط الشرطة القضائية أو أحد أعوانها تحت مسؤولية ضباط الشرطة القضائية المكلف بتنسيق عملية التسرب وأن يكون هذا الإذن مكتوبًا ومسببا.
- أن يتضمن الإذن بالتسرب الجريمة التي تبرر اللجوء إلى هذا الإجراء.

[1] عبد القادر عميمر، مرجع سابق، ص 268-269.

أن تحديد مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر ويمكن أن يتم تجديد هذه العملية بعد انتهاء المدة المحددة ضمن نفس الشروط الشكلية والزمانية، كما يمكن للقاضي المرخص له أيقاف عملية التسرب في أي وقت قبل انقضاء المدة المحدّدة[1].

الشروط الموضوعية: وتتمثل فيما يلي:

- تحرير تقرير عن كل عملية التسرب، يقوم ضابط الشرطة القضائية بتحرير تقرير عن كل عملية تسرب وإرساله إلى الجهة القضائية المختصة التي منحت الإذن بالتسرب لكي تتمكن من مراقبة العملية.
- الحفاظ على سلامة المتسرب يجب على ضباط الشرطة القضائية المنسق لعملية التسرب اتخاذ الإجراءات الضرورية والاحتياطات اللازمة لحماية أمن وسلامة الضابط أو العون المتسرب عن قرب، وكذا الأشخاص المسخرين في العملية في كل مرحلة من مراحل المهمة.
- عدم الكشف عن هوية المتسرب ضمان عدم الكشف عن هوية الضابط والأعوان المتسربين التزامًا بالنص القانوني[2].

ثالثا: آثار التسرب

يقوم ضابط الشرطة القضائية المنتدب باعتباره المسؤول عن عملية التسرب بتحرير تقارير عن العمليات التي يقوم بها المتسرب ويحيلها على قاضي التحقيق على أساس أنه المنسق بين هذا الأخير والمسرب.

ومن خلال النصوص المنظمة لعملية التسرب نلاحظ أن المشرع لم يشر إلى ما إذا كان ضابط الشرطة القضائية مسؤولاً عن عملية التسرب يقوم بتحرير محضر حول العملية ونشاط المتسرب أم لا. ولا إلى مصير الأدلة والأشياء المتحصل عليها نتيجة عملية التسرب. ولا موقف القانون من الجرائم التي يتم

[1] عبد القادر عميمر، المرجع السابق، ص 273.

[2] .مجراب الدوادي، مرجع سابق، ص 344.

اكتشافها عرض أثناء أدائها المتسرب لمهامه ولا إمكانية الطعن في الإذن بالتسرب عن طريق الاستئناف، فكل ما أشار إليه المشرع الجزائري هو إيداع الإذن أو الرخصة التي تم بها تنفيذ عملية التسرب في ملف الإجراءات بعد الانتهاء من العملية، وكذا سماع ضباط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته دون سواه كشاهد عن العملية[1].

المطلب الثاني: الإجراءات الواردة في القانون 09-04

إن القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية من جهة، ومن القواعد الوقائية لاتي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها من جهة أخرى، وقد أخذ المشرع الجزائري بعين الاعتبار أحكام الاتفاقيات الدولية ذات الصلة بالموضوع، وذلك من خلال تجانسها مع النصوص القانونية الأخرى، وتتمثل الإجراءات التي جاء بها هذا القانون 09-04 في مجال البحث والتحري عن الجريمة المعلوماتية وإثباتها في آلية مراقبة الاتصالات الإلكترونية وتجميع وتسجيل مضمونها التي سنتناولها في الفرع الأول من هذا المطلب، والفرع الثاني، سنتطرق فيه إلى توسيع الإجراءات الخاصة بالاختصاص الإقليمي.

الفرع الأول: مراقبة الاتصالات الإلكترونية وتجميعها

المشرع الجزائري لم يعترض لتعريف المقصود بالمراقبة الإلكترونية مثله مثل باقي التشريعات، إلا أن الفقه قد تصد لذلك وعرفه بأنه إجراء مراقبة شبكة الاتصال، أو هو العمل الذي يقوم بموجبه المراقب باستخدام التقنية الإلكترونية لجميع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصًا أو مكانًا أو شيئًا حسب طبيعة مرتبطة بالزمن لتحقيق غرض أمني أو لأي غرض آخر، فإجراء مراقبة الاتصالات

[1] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائية في المواد الجزائية، كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة، الجزائر، العدد 33، جوان 2010، ص 250.

الإلكترونية هو إجراء يدخل كذلك في إطار التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية[1].

ويقصد بالمراقبة بوجه عام تعمد الاتصال والتسجيل على المحادثات الخاصة، أما المحادثات العامة فلا قيد على مراقبتها وتسجيلها سواء علم أصحابها ذلك أو مل يعلموا لأن ذلك ليس بحرمتهم وخصوصياتهم مادامت هذه المحادثات عامة، وقد استخدم عدد من المصطلحات من طرف الفقه والقانون للدلالة على المراقبة الإلكترونية، ومن بين هذه المصطلحات، الاعتراض، الالتقاط، في حين استخدمه المشرع الجزائري في القانون 09-04 مصطلح مراقبة الاتصالات الإلكترونية والذي يقصد به اعتراض المحادثة وقطع الطريق عنها ومنعها من الوصول إلى وجهتها[2].

ثانيا: حالات اللجوء إلى المراقبة الإلكترونية والعمليات الإجرائية لها 1

1-حالات اللجوء للمراقبة الإلكترونية:

نص القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في نص المادة 9 على ما يلي:

<<مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقًا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية>>[3] من الواضح ان مراقبة

[1] بن بادة عبد الحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، العدد 23، جامعة زيان عاشور، الجلفة، الجزائر، جوان 2015، ص 86.

[2] عبد القادر عميمر، مرجع سابق، ص 275.

[3] المادة 3 من القانون 09-04، السالف الذكر.

الاتصالات حددها القانون على سبيل الإسناد وفي حالات محددة حصريًا في المادة 4 من القانون المشار إليه.

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني او مؤسسات الدولة أو الاقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث يكون من الصعب الوصول إلى نتيجة تهم لأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ طلبات المساعدة القضايا الدولية المتبادلة وما يلاحظ أن المشرع ونظرًا لما يترتب على تطبيق هذه التدابير ميدانيًا من مساس بحرية الحياة الخاصة وخصوصياتها[1].

وقد نصت المادة 303 مكرر من قانون العقوبات على ما يلي: <<يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 50.000 إلى 300.000دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

- بالتقاط أو تسجيل أو نقل صورة لشخص من مكان خاص بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقرر للجريمة التامة.

[1] ربيعة ريدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار هومة للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011، ص127-128

ويضع صفح الضحية حدا للمتابعة>>[1]

ثالثا: خصائص مراقبة الاتصالات الإلكترونية

لمراقبة الاتصالات الإلكترونية عدة خصائص نذكر منها:

1-مراقبة الاتصالات الإلكترونية ذات طابع تقني: يعد الطابع التقني من أبرز خصائص المراقبة الإلكترونية، وذلك لما يتطلبه هذا الإجراء من وجود أجهزة تقنية خاصة حتى يتمكن مباشرة المراقبة، فالتعقب الإلكتروني للاتصالات والتقاط وتخزين المحادثات والرسائل الصادرة والواردة يتطلب وضع الخادم المعلوماتي المزود للخدمات تحت المراقبة إذا تم الاشتباه في احتواء هذه الاتصالات على معلومات مجرمة أو متعلقة بجرائم خطيرة، وهذا يتطلب وضع ترتيبات خاصة بذلك حسب ما جاء في المادة الثالثة من القانون 09-04[2].

2- مراقبة الاتصالات الإلكترونية ذات الطابع الوقائي: من بين الخصائص التي يتميز بها إجراء مراقبة الاتصالات الإلكترونية أنه ذو طابع وقائي أملته طبيعة وخصوصية الجريمة المعلوماتية والتهديد الذي أصبحت تشكله ضد أمن الأشخاص وممتلكاتهم، وهو ما جعل المشرع يرخص باللجوء إلى هذا الإجراء بغرض وقف ارتكاب الجريمة وضبط الأدلة المتعلقة بها، ومن ضوابط القيام بهذا الإجراء أن تكون هناك شبهات قوية ودلائل توحي بارتكاب جريمة وضرورة وجود أسباب مبررة للقيام به كما يجب مراعاة خصوصية المشتبه فيه وعدم إفشاء المعلومات التي تظهر عنها هذه المراقبة[3].

[1] المادة 303 من الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 المتضمن قانون العقوبات، المعدل والمتمم لاسيما بالقانون رقم 16-02 مؤرخ في 19 يونية سنة 2016.

[2] عبد القادر عميمر، مرجع سابق، ص 277.

[3] مرجع نفسه، ص ص 277-278.

الفرع الثاني: توسيع الإجراءات الخاصة بالاختصاص الإقليمي

بالرجوع إلى قانون الإجراءات الجزائية والقانون 04-09 نجد بأن المشرع الجزائري نظم أحكام جديدة خاصة بالاختصاص في مجال الجريمة المعلوماتية والتي تتماشى والتطور الذي لحق هذه الجريمة.

أولا: الاختصاص المكاني في الجرائم المعلوماتية على المستوى الداخلي

تعتبر الجريمة المعلوماتية نوعًا خاصًا من الجرائم فهي لا تعترف بمبدأ الإقليمية ولا بالحدود الجغرافية فهي بمفهومها وطابعها الدولي قد قبلت مفاهيم الاختصاص الإقليمي للنص الجنائي وكذلك الإجرائي، فهي قد تقع في آن واحد وعلى مستوى عدة دول، وذلك بسبب الطابع اللامادي للمعلومات وللمعطيات محل الجريمة الذي نتج عنه مبدأ عدم اشتراط وقوع الجريمة المعلوماتية ضمن نطاق الاختصاص الإقليمي للنص الجنائي حتى ينشأ الحق في المتابعة والتحقيق، وهي كلها معطيات أثارت إشكاليات ماسة بالمسائل الإجرائية[1].

يمارس عدة وفق أحكام الفقرة 1 و2 من المادة 16 ق 06-22 من قانون إجراءات جزائية الجزائري، ضباط الشرطة القضائية أعمال البحث والتحري ضمن اختصاصهم المحلي المحدد وفق الحدود التي يباشرون فيها وظائفهم العادية، وفي حالة الاستعجال يباشرون مهام في دائرة اختصاص المجلس القضائي الملحقين به، وفي حالة قدم لهم قاضي التحقيق المختص ضمن حالة الاستعجال طلب مباشرة أعمال البحث والتحري على المستوى الوطني فلهم ذلك، أما بالنسبة للجريمة المعلوماتية، وفق ما تنص عليه الفقرة الرابعة من نفس المادة، فإن عمل واختصاص ضابط الشرطة القضائية يمتد على مستوى الإقليم الوطني من أجل متابعة أعمال البحث والمعاينة وذلك تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميًا مع إعلام وكيل الجمهورية المختص إقليميًا.

[1] ربيعي حسين، مرجع سابق، ص 201.

بالنسبة لوكيل الجمهورية فإن اختصاصه الإقليمي محدد وفق النطاق الإقليمي للاختصاص الأقطاب المختصة، وذلك وفق ما تفرضه قواعد المرسوم التنفيذي 06-348 المؤرخ في 5 أكتوبر 2006 المعدل والمتمم بموجب المرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016، إذن فنطاق اختصاصه الإقليمي في مجال أعمال البحث والتحري في الجرائم المعلوماتية إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية، بقوة القانون، بحيث لا يتمتع في هذا الشأن بسلطة الملائمة في تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المادة 144 مكرر، 144 مكرر2، من قانون العقوبات الجزائري.

وبالرجوع إلى المواد سالفة الذكر نجد أن المادة 144 مكرر تنص على أنه <<يعاقب بغرامة 000 100 إلى 000 500ج كل من أساء إلى رئيس الجمهورية عبارات تتضمن إهانة أو سب أو قذف سواء كان ذل عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية أخرى لبث الصوت والصورة أو بأي وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.

تباشر النيابة العامة إجراءات المتابعة التلقائية.

وفي حالة العود تضاعف الغرامة>>.

أما المادة 144 مكرر 2: فقد قيدت النيابة العامة في إجراءات المتابعة بتلقائية الدعوى الجزائية ضد كل من أساء إلى الرسول صلى الله عليه وسلم أو بقية الأنبياء أو بأية شعيرة من شعائر الإسلام سواء عن طريق الكتابة أو الرسم أو التصريح أو بأية وسيلة أخرى.

تباشر النيابة العامة إجراءات المتابعة تلقائيًا.

بالنسبة لقاضي التحقيق يجوز له حسب نص الفقرة الثالثة والرابعة من المادة 47 ق 06-22 من قانون الإجراءات الجزائية أن يباشر عمليات التفتيش والحجز ليلاً ونهارًا وفي أي مكان على امتداد التراب

الوطني إذا ما تعلق الامر بالجرائم المعلوماتية وهو ما يعني بالضرورة أن اختصاص كل من وكيل الجمهورية وقاضي التحقيق الإقليمي إذا ما تعلق الأمر بالجرائم المعلوماتية هو اختصاص وطني، وفي مجال تمديد الاختصاص الإقليمي دون عناء التنقل إلى مكان تنفيذ الإجراءات أجاز القانون ما يعرف بالتفتيش عن بعد والذي ينطوي على الدخول إلى المنظومة المتخصصة وكذلك ضباط الشرطة القضائية بعد إعلام السلطة القضائية (الفقرة 2 المادة 5 القانون 09-04 المتعلق بمكافحة الجرائم المعلوماتية) وهو الإجراء الذي يسمح بربح الوقت والجهد من خلال اختصار الإجراءات المتعلقة بتمديد نطاق الاختصاص وتعويضه بإجراءات ذات طابع تقني وفني تهدف إلى إحراز الأدلة بأسرع وقت ممكن[1].

ثانيا: الاختصاص المكاني في الجرائم المعلوماتية في المستوى الخارجي

إن أعمال بحث التحقيق قد تتعدى في بعض الأحيان نطاق الاختصاص الإقليمي الوطني لتمتد إلى إقليم دولة أخرى، فقد تتبع القواعد الخاصة في سبيل ضمان شرعية الإجراءات هي الالتجاء إلى قواعد التعاون الدولي لمكافحة الجرائم المعلوماتية، فإذا تبين أن المعطيات المتحصل عليها والتي يمكن الدخول إليها من المنظومة الأولى، مخزنة وموجودة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقًا للاتفاقيات الدولية ذات الصلة وفقًا لمبدأ المعاملة بالمثل[2].

وقد نصت المادة 16 من القانون 09-04 على ما يلي: <<في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني يمكن في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية

[1] ربيعي حسين، مرجع سابق، ص 203.

[2] أنظر المادة 5 فقرة 3 من القانون 09-04 السالف الذكر.

المذكورة في الفقرة الأولى. أعلاه إذ وردت عن طريق وسائل الاتصال السريع بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كفاية للتأكد من صحتها>>[1]

ومن أمثلة التشريعات المقارنة التي أقرت بذلك التشريع الهولندي في مادته 125 فقرة 1 على إمكانية إجراء تفتيش داخل الأنظمة المعلوماتية المتزايدة في دولة أخرى بشرط أن يكون هذا التدخل مؤقتًا ويهدف إلى كشف بيانات ضرورية لإظهار الحقيقة.

إذن فما يمكن قوله في شأن أحكام الاختصاص النوعي والمكاني التي تحكم عمل الجهات المختصة بالبحث والتحقيق في الجرائم على المستوى الوطني، هو أنه بالرغم مما تحمله من ضمانات شرعية إجرائية، كضمان لحقوق وحريات الأفراد إلا أنها تبقى غير متكاملة من حيث مفهومها وأحكامها الواردة في كل من قانون الإجراءات الجزائية وقانون مكافحة الجرائم المعلوماتية 09-04 الذي يحدد القواعد الخاصة بالتفتيش عن بعد دون ذكر مراعاة قواعد الاختصاص الإقليمي المبينة في قانون الإجراءات الجزائية[2]، وهذا الأخير الذي يضع شروطًا وقواعدًا عامة تطبق على المستوى الوطني وبدون شرط إعلان السلطة القضائية عكس القانون 09-04 الذي جعل من مسألة تحديد الاختصاص الإقليمي لأجل التفتيش عن بعد بضرورة إعلام السلطة القضائية، وهما إجراءان مختلفان إحداهما تفتيش مادي منصوص عليه في قانون إجراءات جنائية والآخر تفتيش رقمي منصوص عليه في القانون 09-04 وهو ما يفتح باب التعارض في تطبيق نصوص القوانين فإلى أي قانون نلجأ أولا وبأيهما نعمل بدءًا وهي كلها عوائق تمنع رجال البحث والتحقيق من تأدية مهامهم بالسرعة المطلوبة في مواجهة الجرائم المعلوماتية وهو ما يمنح للجاني فرصة إتلاف الدليل والإفلات من العقاب[3].

---

[1] المادة 126 من القانون 09-04 السالف الذكر.

[2] ربيعي حسين، مرجع سابق، ص 204.

[3] مرجع نفسه، ص 204-205.

المبحث الثاني: القواعد المتبعة للتفتيش والحجز داخل المنظومة المعلوماتية

إن التفتيش في الجريمة التقليدية لا يختلف عن الجريمة المعلوماتية، فيعتبر التفتيش من بين إجراءات التحقيق الذي يهدف من خلاله إلى الوصول إلى الأدلة من أجل الوصول إلى الحقيقة، ونسب الفعل المجرم إلى مرتكب الجريمة، ويقوم بالتفتيش سلطة مختصة وذلك بالدخول على المنظومة المعلوماتية من خلال نظم المعالجة الآليات للمعطيات، من أجل البحث عن الأفعال والسلوكات المرتكبة وغير المشروعة بالتفتيش، حجز الأدلة التي ضبطها، حيث سنتناول في هذا المبحث التفتيش والحجز داخل المنظومة المعلوماتية (المطلب الأول)، وطرق البحث على الدليل الرقمي والتعامل معه أثناء التفتيش والحجز (المطلب الثاني) بالإضافة إلى موقف المشرع الجزائري من مشروعية الدليل.

المطلب الأول: قواعد التفتيش والحجز داخل المنظومة المعلوماتية

إن المشرع الجزائري كغيره من التشريعات جعل لأنظمة معالجة المعطيات حماية ووقاية جنائية لازمة لعدم المساس بها، حيث قام المشرع الجزائري بوضع مجموعة من القواعد الموضوعية لحماية المتعاملين في هذا المجال من جهة أخرى، ونظرًا للتطور الذي اقتحم المجال المعلوماتي. قام المشرع الجزائري بإصداره للقانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وقام باستحداث قواعد خاصة بالتفتيش والحجز، تكمل القواعد المنصوص عليها في قانون إجراءات جزائية الجزائري، حيث سنحاول في هذا المطلب قواعد التفتيش داخل المنظومة المعلوماتية (فرع أول) وقواعد الحجز داخل المنظومة المعلوماتية (فرع ثاني).

الفرع الأول: قواعد التفتيش داخل المنظومة المعلوماتية

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق يهدف إلى البحث عن الأدلة لإثبات وقوع جريمة ما في مكان معين، حيث أنهُ ونظرً لخطورته تشترط أغلب التشريعات الحصول على رخصة

التفتيش من الجهة القضائية المختصة، إذا كان الالتزام بقواعد التفتيش في الجرائم التقليدية لا يثير إشكالات كبيرة فإن الأمر ليس كذلك بالنسبة للجرائم الإلكترونية، خاصة وأن نظم المعالجة الآلية تكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات اتصال متطورة[1].

كما يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون إجراءات جزائية وفي الحالات المنصوص عليها في المادة 4 من القانون 09-04 بغرض التفتيش ولو عن بع إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها.
- منظومة تخزين المعلومات.

في الحالات المنصوص عليها في الفقرة "أ" من هذه المادة إذا كانت هناك أسباب تدعوا للاعتقاد بأن المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقًا بذلك إذا تبين مسبقًا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقًا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يمكن بمساعدة السلطات الأجنبية المختصة طبقًا للاتفاقيات الدولية ذات الصلة وفقًا لمبدأ المعاملة بالمثل[2].

[1] عبد الصديق شيخ، الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة المدية، الجزائر، المجلد 4، العدد 1، 2020، ص ص 198-199.

[2] ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان، الجزائر، 2017، ص 111.

<<يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها، وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها>>[1]

وعليه مما سبق نجد أن المشرع الجزائري ومن خلال هذه المادة قد فصل في العديد من الإشكالات الإجرائية فزيادة على ما هو منصوص عليه في قانون إجراءات جزائية، السابق عرضه فقد أضاف المشرع الجزائري محلين للتفتيش وهما:

- المنظومة المعلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- ومنظومة تخرين المعلومات.

وبالتالي وضع نهاية لجدال فقهي لا تزال عديد الدول تتخبط فيه، كما نص صراحة على إمكانية التفتيش عن بعد إلا أنه حصر إمكانية تمديد التفتيش في الشبكة على الحالة "أ" أما المادة 4 للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب، أو الجرائم الماسة بأمن الدولة، يتنافى وطبيعة الجرائم المتصلة بتكنولوجيا المعلوماتية فالأحرى أن تكون إمكانية تفتيش في الشبكة في حال ما إذا كانت هناك أسباب تدعوا للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى[2].

إضافة إلى ما سبق فإننا نرى أن المشرع الجزائري بالغ في احترام سيادة الدولة الأخرى من خلال منع التفتيش في الأنظمة المعلوماتية التابعة لإقليمها إذ نص في المادة 5 الفقرة 3 من القانون 09-04 إذا تبين مسبقًا بان المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقًا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقًا للاتفاقيات الدولية ذات الصلة وفقًا لمبدأ المعاملة بالمثل.

[1] الفقرة 4 من القانون 09-04 السالف الذكر.
[2] ناني لحسن، مرجع سابق، ص 112.

في حين كان من الواجب التفصيل في طبيعة المعطيات المبحوث عنها والواقعة خارج التراب الوطني، فإن كانت متاحة للجمهور جاز الحصول عليها دون إذن مسبق أو في إطار التعاون الدولي[1].

الفرع الثاني: قواعد الحجز داخل المنظومة المعلوماتية

إن الضبط في المجال المعلوماتي هو وضع اليد على المكونات التي تفيد كشف الحقيقة في جريمة وقعت وجار التحقيق فيها، المادية للحاسوب والأدلة المعلوماتية المخزنة في الحاسوب محل التفتيش أو في الشبكة أو في الحاسوب الخادم ولاتي يطلق عليها تسمية المنقولات المعلوماتية، لإمكانية نقل البيانات المعالجة إلكترونيًا أو المعلومات من حاسب معين إلى حواسيب أخرى سواء عن طريق شبطة الاتصال التي تربط بينها أو عن طريق الأقراص والشرائط الممغنطة، فمكونات الحاسب الآلي يصدق عليها وصف الشيء المنقول[2].

تدخل المشرع الجزائري في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في المادة 6 منه بنصها <<عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية>>.[3]

---

[1] ناني لحسن، مرجع سابق، ص ص 112-113.

[2] بن طالب لندا، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراه علوم في القانون، جامعة مولود معمري، تيزي وزو، الجزائر، 23-01-2019، ص 65.

[3] المادة 6 من القانون 09-04 السالف الذكر.

كما يعتبر الحجز هو عملية تتبع التفتيش فيعتبر أيضًا تحرير المضبوطات عملية إجراء الضبط وعليه فإن المشرع الجزائري قضى بضرورة اتباع بعض الإجراءات الخاصة للمحافظة على سلامة المضبوطات من العبث وذلك كالتالي:

– منع المشرع من خلال المادة 7 من القانون 09-04 السالف الذكر الوصول إلى المعلومات المتحصل عليها والتي تم ضبطها، وذلك عن طريق ترميزها أو تقييدها عن طريق أي وسيلة إلكترونية أخرى تمنع الدخول على هذه المعلومات وهو ما نصت عليه أيضًا المادة 19 في فقرتها الثالثة من اتفاقية بودابست، غير أنه وفقًا لهذه الأخيرة يتم اللجوء إلى هذا الإجراء في حالة ما إذا المعطيات تتضمن خطر او ضرر بالمجتمع.

– ضبط الدعائم الأصلية للمعلومات وعدم الاقتصار على ضبط نسخها.

– عدم ثني القرص لأن ذلك يؤدي إلى ثقة وفقدان للمعلومات المستعملة عليه.

– عدم تعرض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية والرطوبة[1].

كما أن حجز المضبوطات الإلكترونية يستلزم اللجوء إلى وسائل وطرق تقنية ومن بين هذه الطرق والوسائل نذكر منها:

– طريق النسخ وتتم من خلال نسخ المضبوطات الإلكترونية باستخدام برامج معدة خصوصًا لهذا الغرض مثلا كبرنامج (Laplink)، حيث يتم أخذ نسخة من تلك البيانات أو المضبوطات الإلكترونية، ومن ثم يتم لصقها وخزنها باسم معين، على إحدى وسائل النقل (DVD، CD،Flash Memory) الخاصة بالجهة القائمة بالضبط وتبقى بعدتها إلى حين انتهاء التحقيق أو المحاكمة، على أن يفضل على رأي البعض

[1] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه، العلوم في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2017-2018، ص 293.

حفظ نسخة أخرى من تلك المضبوطات لدى المحضرين بالمحكمة، كي تكون بديلاً للأولى في حالة تلفها أو ضياعها[1].

– طريق التجميد: وتتم من خلال تجميد التعامل بالكمبيوتر أو النظام المعلوماتي الذي تتواجد بداخله المضبوطات الإلكترونية، أو على الأقل تجميد القسم الصلب الذي يحمل تلك المضبوطات، وذلك من خلال برامج معدة خصيصًا لهذا الغرض، ومن ثم يتم ضغط الملفات أو المضبوطات الإلكترونية من خلال برامج الضغط، حيث تقوم هذه الأخيرة بتقليصها حجن تلك الملفات أو المضبوطات وتضغطها بداخل ملف أو عدة ملفات صغيرة الحجم بصيغة (Zip) أو (Rdt) ومن دون أن يؤثر ذلك على سلامة الملفات، بحيث تبقى محتفظة بكامل خواصها الأصلية ومن ثم يتم حفظ تلك الملفات المضغوطة على أقراص ليزرية (DVD،CD) أو على أقراص ميموري، ومن ثم يتم فتح الملفات المضغوطة على أي كمبيوتر آخر من خلال برامج خاصة من مثل برنامج(wnrar)[2].

كما يتعين على مقدمي خدمة الانترنت تقديم المساعدة وذلك حسب ما جاء في المادة 11 من القانون 09-04 كما حدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة (1) ابتداء من تاريخ التسجيل[3].

[1] رابحي عزيزة، مرجع سابق، ص 294.
[2] مرجع نفسه، ص 294-295
[3] أنظر المادة 11 من القانون 09-04 السالف الذكر.

الفرع الثالث: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (المختصة بالبحث والتحقيق في الجرائم المعلوماتية)

سنتطرق في هدا الفرع الى (التعريف بالهيئة واختصاصاتها).(تشكيل الهيئة وطبيعة عملها)

أولا: التعريف بالهيئة واختصاصاتها

1-التعريف بالهيئة: تعتبر الهيئة كما يصطلح عليها في صلب نصوص المرسوم الرئاسي حسب أحكام المواد من 01 إلى 04 منه بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة، تتولى الهيئة المهام المنصوص عليها في المادة 14 من القانون 09-04 وذلك تحت سلطة الرقابة القضائية وطبقًا لأحكام قانون الإجراءات الجزائية[1].

وتنص المادة 14 من القانون 09-04 على <<مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بـ "تتولى الهيئة المذكورة في المادة 13 أعلاه خصوصا المهام الآتية:

أ- تنشيط وسبق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

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

ج- تبادل المعلومات مع نظيراتها فيا الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم>>[2]

[1] ربحي حسين، مرجع سابق، ص 172.

[2] المادة 14 من القانون 09-04 السالف الذكر.

اختصاصات الهيئة: بينت الفقرة الثانية 02 من المادة 04 من المرسوم الرئاسي 15-261 المهام الأساسية التي تكلفت بها الهيئة وهي على سبيل الحصر مهام الهيئة الهدف منها هو الوقاية من الجرائم المعلوماتية، ومكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث والتحقيق ومد يد الون لمصالح الشرطة القضائية، وأبرز مهام هذه الهيئة هي:

- اقتراح عناصر الاستراتيجية الوطنية للرقابة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.
- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية.
- تطور التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها[1].

ثانيا: تشكيل الهيئة وطبيعة عملها

تشل العينة من لجنة مديرية إضافة إلى مديرية عامة، تشكل اللجنة المديرية من الوزير المكلف بالعدل رئيسًا إضافة إلى الوزير المكلف بالداخلية والوزير المكلف بتكنولوجيا الإعلام والاتصال وقائد الدرك الوطني، وكذلك المدير العام للأمن الوطني، وممثلين أحدهما عن رئاسة الجمهورية والآخر عن وزارة الدفاع، يكملهما قاضيان من المحكمة العليا، أما المديرية العامة فيرأسها مدير عام يعين بموجب مرسوم رئاسي، وتتجلى مهام هذه المديريات في ضبط برامج عمل الهيئة ودراسة مشروع الميزانية، وتقديم

[1] ربيعي حسين، مرجع سابق، ص 172-173.

تقارير خاصة بنشاط الهيئة وبالتالي فهي لا تسهم في الإجراءات الخاصة بالوقاية أو مكافحة الجرائم المعلوماتية[1].

المطلب الثاني: طرق الحصول والتعامل مع الدليل الرقمي في الإثبات الجنائي

بعد عمليات التفتيش عن الجريمة ومرتكبها وعن الأدلة القائمة في هذه الجريمة تأتي عملية التحقيق من الأدلة الرقمية بحيث يجب أن يمر الدليل الرقمي لمراد حجزه بمراحل حتى يتم اعتباره دليل رقمي معتمد في الإثبات وذلك من خلال القيام بجمع الدليل وفحصه وتحليل ومراجعة الأدلة.

الفرع الأول: مفهوم الدليل الإلكتروني

سنتترق في هدا الفرع الى (تعريف الدليل الالكتروني).و(خصائص الدليل الالكتروني)

أولا: تعريف الدليل الإلكتروني:

يعرف الدليل الإلكتروني بأنه الوسيلة المبحوث عنها في التحقيقات بغرض إثبات صحة واقعة تهم الجريمة أو ظرف من الظروف المادية أو الشخصية وهي تلك الواقعة التي يستمد منها القاضي البرهان للنطق بالحكم[2].

كما يمكن تعريف الدليل الإلكتروني بأنه الدليل الذي يجد لها أساس في العالم الافتراضي ويقود على الجريمة فهو وذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الانترنت، فكلما كان هذا المزج في موضوع الدليل بالمعالجة الآلية للمعلومات فإنه يعد هنا دليلا تقنيًا، وهو أيضًا الدليل المؤذ من أجهزة الكمبيوتر ويكون في شكل مجالا أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام

[1] ربيعي حسين، مرجع سابق، ص 173-174.

[2] عبير بعقيق، فيصل نصيغة، مرجع سابق، ص 37.

برامج وتطبيقات وتكنولوجيا خاصة، ويعرف الدليل الجنائي أيضًا بأنه هو الوسيلة التي يستعين بها القاضي للوصول إلى اليقين القضائي الذي يقيم عليه حكمه في ثبوت الاتهام المعروض عليه[1].

ثانيا: خصائص الدليل الإلكتروني

1-الدليل الرقمي دليل علمي: لبيان مدة كون الدليل الرقمي دليلا علميًا فقد أورد عمر أبو بكر بن يونس بهذا الصدد <<إذا كان الدليل العلمي له منطقة خاصة والذي يجب أن لا يخرج عليه من حيث عدم تعارضه مع القواعد العلمية السليمة والدليل الرقمي وإلا فقد معناه>> بعبارة أخرى مواكبة التطور الذي يشهده العلمي الرقمي وعدم الاكتفاء بقواعد معينة فقط.

لذا فإنه وعند عرضه كدليل أمام هيئة المحكمة يأخذ القاضي برأي الخبراء والتقنين بخصوص تلك المعلومات، وفي الوقت نفسه يقدم له محضرًا به كافة الإجراءات المعمولة من قبل رجال الضبطية القضائية[2].

2- الدليل الرقمي دليل تقني: فهو مستوحى من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية، فهي لا تكشف الوسيط التي تم بواسطتها ارتكاب الجريمة كما هو الحال في الدليل العادي وإنما تنتج التقنية نبضات رقمية، تصل إلى درجة في شكلها وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان، يتميز الدليل بصعوبة محوه، أو تحطيمه إذ حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلية التي تحتوي ذلك الدليل[3].

---

[1] رابحي عزيزة، مرجع سابق، ص 265-266.

[2] عبير بعقيقي، مرجع سابق، ص 37-38

[3] نور الهدى محمودي، مشروعية الوسائل العلنية الحديثة في الإثبات الجنائي، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق، علم الإجرام وعلوم العقاب، جامعة باتنة 1، الحاج لخضر، الجزائر، 2017-2018، ص 174.

ثالثا: أنواع الدليل الإلكتروني

اختلف في تقسيم الدليل الإلكتروني فمنهم من قسم الدليل الإلكتروني إلى نوعين أدلة أعدت لتكون وسيلة إثبات، وأدلة لم تعد لتكون وسيلة إثبات، ومنهم من قسمها على أساس طبيعة الجريمة والوسيلة المستعملة فيها إلى أربعة أنواع:

- الأدلة الرقمية الخاصة بأجهزة الكمبيوتر وشبكتها.
- الأدلة الرقمية بالخاصة بالبروتوكولات وتبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
- الأدلة الرقمية الخاصة بالشبكة المعلوماتية العالمية[1].

الفرع الثاني: جمع الدليل والحصول عليه

إن علوم الأدلة الجنائية من شأنها أن تقدم منظورًا علميًا لتحليل أي شكل من أشكال الأدلة الرقمية، وتساهم علوم التحليل السلوكي للأدلة الرقمية في الربط المحدد بين المعارف التكنولوجيا وبين الطرق العلمية والقانونية لاستخلاص الدليل الرقمي. وعلى ذلك فإن هذه العلوم مجتمعة تساهم فيما يلي:

- الكشف عن الدليل الرقمي.
- إجراء الاختبارات التكنولوجية والعلمية على الدليل الرقمي لاختباره والتحقق منه.
- أصالته ومصدره كدليل يمكن تقديمه لجهة الحكم.
- تحديد الخصائص الفريدة للدليل الرقمي.
- عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.

[1] نور الهدى محمودي، مرجع سابق، ص 175.

– استخدام الخوارزميات للتأكد من أن الدليل لم يعبث به أو تعديله[1] من خلال قيام مجرمي الإنترنت بحماية مواقعهم وأجهزتهم بكلمات سرية أو رموز وشفرات لإعاقة المحاولات الهادفة إلى الوصول إليها أو الاطلاع عليها أو استخدامها، بالإضافة إلى أنه حينما يتوجه أفراد الضبطية القضائية من أجل القبض على الجاني وتحرير الأدلة ومنها جهاز الكمبيوتر المستخدم في الاتصال بالشبكة وما يحويه من برامج ومعلومات إذ تثور مشكلة معرفة الرقم السري والذي بدونه لا يعمل جهاز الكمبيوتر وفي هذه الحالة لا يجوز لأجهزة التفتيش إجبار المتهم على الإفشاء على الرقم السري لأن ذلك يعد إجراء غير قانوني، وكذلك قد يتمكن الجاني من تدمير البيانات الموجودة والمخزنة في جهاز الكمبيوتر في ثوان أثناء إجراء التفتيش، ففي هذه الحالة تكون هناك صعوبة في جمع الأدلة المادية التي تثبت ارتكاب جرائم الانترنت[2].

وعادة ما توجد الأدلة الرقمية في مخرجات الطابعة والتقارير والرسوم وفي أجهزة الكمبيوتر وملحقاته وفي الأقراص المرنة والصلبة وأشرطة تخزين المعلومات وفي أجهزة المودم والبرامج وأجهزة التصوير ومواقع الويب والبريد الإلكتروني ولذلك تستخدم عدة طرق أو أدوات تساهم في جمع الأدلة الرقمية منها: برنامج إذن التفتيش وهو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها، ويكن لهذا البرنامج أن يصدر اتصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل[3].

– برنامج معالجة الملفات مثل Xtreeprogold وهو برنامج يمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

---

[1] ناني لحسن، مرجع سابق، ص 115–116.

[2] بن بارة عبد الحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، جامعة غرداية، الجزائر، المجلد الثاني، العدد 23 جوان 2015، ص 90.

[3] ناني لحسن، مرجع سابق، ص 116–117.

– برنامج النسخ مثل Laplink وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي Parallelpor أو على التوالي Serial port وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم[1].

– برنامج كشف الديسك AmdDiskviewdisk ويمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة.

– برنامج اتصالات مثل lantasticفهذا البرنامج يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما يريد من معلومات وحفظها في جهاز نسخ المعلومات ثم القرص الصلب.

وهذه أهم التقنيات العلمية المعتمدة في جميع الأدلة الرقمية والتي يجب أن يقوم بها الخبراء في هذا المجال نظرًا لعملية ودقة هذه الأدلة، ومن وجهة نظر جهات التحقيق فإن جمع الأدلة الإلكترونية، يمكن أن تشكل صعوبة نسبية فبالرغم من أن ملفات الولوج Log file تبدو متشابهة للملفات العادية ويمكن جمعها من أي ملف آخر وهي تحتوي على كمية هائلة من المعلومات قد تفيد البحث والتحقيق الجنائي[2].

كما أنه يجب الحصول على دليل بصورة مشروعة فلا يجوز للقاضي الجنائي أن يسند في حكمه إلا أي دليل تم الحصول عليه بطرق غير مشروعة مثل الإكراه أو إفشاء سر مهني في غير الأحوال المقررة قانونًا أو خيانة أمانة وغيرها من الطرق غير المشروعة، ولابد أن يكون الدليل صحيحًا لا يشوبه بطلان يتقرر بمخالفة إجراءات القانون، لأن مشروعية الخصومة الأدلة تعتبر حدًا لا يمكن للقاضي أن

[1] ناني لحسن، مرجع سابق، ص 117.

[2] نور الهدى محمودي، مرجع سابق، ص 186–187.

يتجاوزه، نظرًا لما تقوم عليه الخصومة الجنائية من مبدأ حرية المتهم وتعزيز قرينة براءته وليس فقط إطلاق حرية القاضي في الإثبات ممثلا سلطة الدولة في العقاب[1].

الفرع الثالث: موقف المشرع الجزائري من الدليل الإلكتروني

سنتطرق في هدا الفرع الى موقف المسرع الجزائري من الدليل الالكتروني في ظل التشريع الجزائري

نصت المادة 212 من قانون إجراءات جزائية فقرة أولى <<يجوز أثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعًا لاقتناعه الخاص>>[2].

كما نصت المادة 307 من قانون إجراءات جزائية أيضًا <<أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكون اقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم>>.

ومن خلال هذين النصين القانونيين يتضح جليًا أن المشرع الجزائري قد تبنى كقاعدة عامة نظام الاقتناع الشخصي للقاضي الجزائري، إلا واستثناء نجده أخذ بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط إثباتها أدلة قانونية محددة مسبقًا وعلى سبيل الحصر.

وبتحليل المادة 212 من قانون الإجراءات جزائية نجدها تكرس قاعدتين تكمل إحداهما الأخرة، فقاعدة الاقتناع الحر للقاضي الجزائر من جهة وقاعدة حرية اختيار وسائل الإثبات الجزائي من جهة أخرى[3].

---

[1] رابحي عزيزة، مرجع سابق، ص 269.

[2] المادة 212 الفقرة الأولى من قانون إجراءات جزائية، السالف الذكر.

[3] سعيداني نعيم، آليات البحث والتحري من الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، علوم جنائية، كلية الحقوق، جامعة باتنة، الجزائر، 2012-2013، ص 225-226.

خاتمة

الخاتمة

خاتمة:

بعد ان فرغنا بحمد الله وتوفيقه من دراسة موضوعنا تحت عنوان اجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية فلا ريب أن هذه الجرائم أصبحت تشكل نمطا خطيرا في وقتنا الحالي نظرا لكون الإثبات فيها صعب المنال ، لاعتبار أدلتها الرقمية خفية وغير مرئية فقد أصبح العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية ، حيث أصبحت حياتنا اليومية تستدعي اللجوء إليها فقد مكنت طرق المعالجة الآلية للمعطيات المجتمعات من تجاوز فكرة الحدود الإقليمية ، باعتبار التكنولوجيا عابرة للحدود ، وقد عرف هذا التطور التكنولوجي الإجرام المعلوماتي وذلك نتيجة الاستخدام بالقصد الجنائي للمعلوماتية أو الحاسوب الذي ينتج عنه عدة أضرار مختلفة ، وذلك من خلال تهديد أمن المعطيات من جهة ومن جهة أخرى تمس بحرية الأفراد وممتلكاتهم ومؤسساتهم .

فالمشرع الجزائري كغيره من التشريعات خصا الجريمة المعلوماتية بخصوصية من الناحية الإجرائية من خلال اعتمادنا على قانون اجراءات جزائية الجزائري الجديد وكذلك القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته ، حيث وجدنا أن قانون إجراءات جزائية الجزائري ينص على القواعد العامة والمألوفة التي تطبق على الجرائم التقليدية وكذا على المعلوماتية ، أما بالنسبة للقانون 04/09 الذي وضع لمتابعة الجريمة المعلوماتية من خلال بعض الاجراءات الخاصة متمثلة في حجز المعطيات وحفظها ومراقبة الاتصالات الالكترونية وإجراء التسرب.

لقد تم توصلنا من خلال بحثنا أن هناك بعض الاجراءات مشتركا بين الجرائم التقليدية والجرائم المعلوماتية كالمعاينة والتفتيش الالكتروني وضبط الدليل الالكتروني .

ويمكن القول أن المشرع الجزائري لم يوفر اجهزة او الية تشريعية قادرة على الاطلاع بالآثار الخطيرة ، الناتجة من الجرائم الواقعة داخل المنظومة المعلوماتية ،سواءا على مستوى النصوص التشريعية

أو على مستوى طبيعة الإطارات البشرية ، ومنه يتبين لنا أيضا أن تحقيق العدالة مزال بحاجة إلى التدريب الفني والتقني للتعامل مع الجرائم المعلوماتية وتكييفها قانونيا .

ومن خلال هذه النتائج نخلص الى مجموعة من التوصيات :

- التوعية بشكل دائم عن مخاطر الجريمة المعلوماتية وأساليب المجرمين في ارتكابها عن طريق وسائل الاعلام .
- وجوب الاهتمام بتدريب الخبراء المحققين والقضاة على التعامل مع الجرائم المعلوماتية .
- عقد دورات مكثفة للإطارات العاملة في حقل البحث والتحري حول الجرائم الماسة بأنظمة المعالجة الالية للمعطيات وتطبيقات الحاسوب .
- ضرورة التعاون الدولي لمواجهة الجرائم المعلوماتية وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرم صور هذه الجرائم .
- إنشاء وحدات امنية مخصصة في مكافحة الجريمة المعلوماتية .
- ضرورة قيام الوحدات الامنية (ضباط الشرطة القضائية) بمعاينة وتفتيش وحجز تقني للأجهزة قبل الحجز عليها تفاديا لأي تغيير للمعطيات والبيانات .

قائمة المراجع

قائمة المراجع

قائمة المصادر والمراجع

-القوانين:

1. قانون رقم 16-01 المؤرخ في 26 جمادى الاولى عام 1437 الموافق ل 6 مارس سنة 2016 . يتضمن التعديل الدستوري الجريدة الرسمية الجمهورية الجزائرية العدد 14 بتاريخ 7 مارس 2016.
2. الامر رقم 66-155 مؤرخ في 8 يونيو سنة 1966 يتضمن قانون الاجراءات الجزائية معدل متمم لاسيما بالقانون رقم 18-13 مؤرخ في 11 يوليو سنة 2018.
3. الامر رقم 66-155 مؤرخ في 18 صفر 1386 الموافق ل 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل والمتمم لاسيما بالقانون رقم 16-02 مؤرخ 19 يونيو سنة 2016.
4. القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق ل 5 اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 47 الصادر في 25 شعبان 1430 الموافق ل 16 اوت 2009.

الكتب

1. احمد حزيط، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية ، النشر الجامعي الجديد تلمسان الجزائر 2017.
2. امال قارة ، الحماية الجزائرية للمعلوماتية في التشريع الجزائري الطبعة الاولى دار هومة .
3. جميل حسين طويلة ، التحليل الجنائي الرقمي ، مكتبة النور سوريا .
4. خالد عياد الحلبي ، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، الطبعة الاولى الطبعة الاولى ، دار الثقافة والتوزيع عمان الاردن .

قائمة المراجع

5.زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي دار هومة للطباعة والنشر والتوزيع عين مليلة الجزائر 2011.

6.عبد الفتاح بيومي عجازي ، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت دراسة معمقة في جرائم الحاسب الالي والانترنت بهجات للطباعة والتجليد مصر 2009.

7.فهد عبد الله العبيد العازمي ، الاجراءات الجنائية المعلوماتية ، دار الجامعة الجديدة للنشر ، الاسكندرية 2016.

8.ماجد ياقوت ، اصول التحقيق ، دراسة مقارنة ، الطبعة الثالثة منشأ المعارف الاسكندرية .

9.ناصر حوادي ، اجراءات التحري الخاصة في ظل قانون اجراءات جزائية الجزائري ، دار العلوم ، الطبعة الثالثة الجزائر 2011 .

10.ناني احسن ، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية ، النشر الجامعي الجديد ، تلمسا ن، الجزائر 2017.

11.نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الثانية دار الثقافة للنشر والتوزيع ، عمان الاردن.

الرسائل الجامعية

1.بن طالب لندا ، الدليل الالكتروني و دورة في الاثبات الجنائي اطروحة لنيل شهادة الدكتوراه في القانون ، جامعة مولود معمري ، تيزي وزو الجزائر 2013.

2.بن فزية محمد ، الاثبات الجنائي للجرائم المعلوماتية ، بالأدلة الرقمية اطروحة دكتوراه في الحقوق ، جامعة الجزائر 1، الجزائر 2017-2018.

قائمة المراجع

3. حمزة نجاة، معاينة مسرح الجريمة ودوره في الكشف عن الحقيقة مذكورة لنيل شهادة الماستر في القانون الجنائي ، كلية الحقوق اكلي محمد الحاج ، البويرة 2014.

4. خالد عطية ، عارف فراج ، مكافحة الجريمة المعلوماتية ، دراسة مقارنة في التشريع الجزائري و الفلسطيني ، مذكرة لنيل شهادة ماستر في الحقوق ، تخصص القانون الجنائي والعلوم الجنائية جامعة يحيى فارس ، المدية .

5. ربعي حسين ، اليات البحث والتحقيق في جرائم المعلوماتية ، اطروحة دكتوراه في الحقوق ، جامعة باتنة 1 الجزائر ، 2015-2016.

6. رابحي عزيزة ، الاسرار المعلوماتية وحمايتها الجزائية ، اطروحة مقدمة لنيل شهادة دكتوراه في القانون الخاص جامعة ابو بكر بلقايد، تلمسان ، الجزائر 1-2016.

7. روابحي فريد ، الاساليب الاجرائية الخاصة للتحري والتحقيق في الجريمة المنظمة ، اطروحة لنيل الدكتوراه ، قانون جنائي والعلوم الجنائية ، كلية الحقوق الجزائر 1-2016.

8. سعيداني نعيم ، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة لنيل شهادة ماجيستر في العلوم القانونية و العلوم الجنائية . كلية الحقوق جامعة باتنة . الجزائر 2012-2013

9. صغير يوسف ، الجريمة المرتكبة عبر الانترنت . مذكرة لنيل شهادة ماجيستر في القانون . جامعة مولود معمري تيزي وزو . الجزائر 2013 .

10. عبد القادر عميمر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري أطروحة دكتوراه ، في القانون العام . تخصص قانون جنائي و علوم جنائية جامعة الجزائر 1 ، 2019 - 2020

11. مجراب الداودي . الاساليب الخاصة للبحث و التحري في الجريمة المنظمة . اطروحة دكتوراه .علوم في القانون ، كلية الحقوق الجزائر 1 2015 –2016

12. نور الهدى محمودي ، مشروعية الوسائل العلمية الحديثة في الاثبات الجنائي . أطروحة مقدمة لنيل شهادة الدكتوراه .العلوم في الحقوق علم الاجرام و علم العقاب ، جامعة باتنة 1 . الجزائر 2017 – 2018 .

المقالات و المجلات

1. الدكتور عبير بعقيقي ، الدكتور فيصل نسيغة، الاثبات في الجرائم المعلوماتية على ضوء القانون 04/09 مجلة العلوم القانونية و السياسية العدد 2 جوان 2018 .

2. بن بارة عبد الحليم ، اجراءات البحث و التحري عن الجريمة المعلوماتية ، مجلة الحقوق و العلوم الانسانية ، جامعة غرداية الجزائر المجلد الثاني العدد 23 جوان 2015

3. بن بارة عبد الحليم ، اجراءات البحث و التحري عن الجريمة المعلوماتية ، مجلة الحقوق و العلوم الانسانية ، جامعة زيان عاشور الجلفة ، العدد 23 جوان 2015

4. جميلة محلق ، اعتراض المراسلات ، تسجيل الاصوات و التقاط الصور في قانون اجراءات جزائية الجزائري ، مجلة التواصل في الاتصالات و الادارة القانونية ، كلية الحقوق و العلوم السياسية ، جامعة باجي مختار عنابة العدد 42

5. عبد الصديق شيخ ، الوقاية من الجرائم الالكترونية في ظل القانون 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، مجلة معالم للدراسات

القانونية و السياسية . كلية الحقوق و العلوم السياسية جامعة المدية ، الجزائر ، المجلد 4 العدد 1 ، 2020

6. فوزي عمارة ، اعتراض المراسلات و تسجيل الاصوات و التقاط الصور و التسرب كإجراء تحقيق قضائي في المواد الجزائية ، كلية الحقوق و العلوم السياسية ، جامعة منصوري ، قسنطينة ، الجزائر العدد 33 ، جوان 2016

7. لندابي طالب ، التفيش في الجريمة المعلوماتية ، مجلة العلوم القانونية و السياسية العدد 16 ، جوان 2017 .

الفهرس

الفهرس

الفهرس:

المحتويات	الصفحة
شكر	–
إهداء.....	–
مقدمة.....	02
الفصل الأول الإجراءات العامة والمألوفة ومدى سريانها على الجريمة المعلوماتية (إجراءات التقليدية)	
تمهيد.....	06
المبحث الأول: معاينة محـل الجرائم الواقعة داخل وخارج النظم المعلوماتيـة.....	07
المطلب الأول: مفهـوم النظم المعلومـاتية.....	07
الفرع الأول: تعريف نظم المعلوماتية.....	07
الفرع الثاني: مكـونات النظم المعلومــاتية.....	09
ثانيا: شكــل الاتصال كعنصر للنظم المعلومـاتية.....	12
الفرع الثاني: تعريف المعلومـات.....	13
المطلب الثاني: مفهـوم المعاينة.....	14
الفرع الأول: تعريف المعاينة وأهميتها	14
أولا: تعريف المعاينة.....	15
ثانيا: أهمية المعاينة.....	16
الفرع الثاني: معاينة مسرح الجريمة:.....	18
أولا: معاينة الجرائم الواقعة على المكونات المادية للجهاز:.....	18
ثانيا: معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها:.....	18
الفرع الثالث: التحليل الجنائي لمعلومات الجهاز.....	19
أولا: مفهوم التحليل الجنائي:.....	19

المطلب الثالث: إجراءات معاينة مسرح الجريمة.....	19
الفرع الأول: إخطار وكيل الجمهورية.....	20
الفرع الثاني: أوقات المعاينة	20
الفرع الثالث: رضا صاحب المسكن.....	21
المبحث الثاني: التفتيش والحجز في النظم المعلوماتي.....	22
المطلب الأول: تعريف التفتيش والحجز.....	22
الفرع الأول: تعريف التفتيش.....	22
الفرع الثاني: تعريف الضبط في البيئة الرقمية.....	23
المطلب الثاني: القواعد الإجرائية للتفتيش والحجز داخل المنظومة المعلوماتية.....	23
الفرع الأول: إجراء الإذن.....	24
الفرع الثاني: إجراء التفتيش والحجز بحضور أشخاص معنيين قانونيا.....	24
الفرع الثالث: مواعيد التفتيش والحجز.....	25
الفرع الرابع: تحرير محضر التفتيش.....	26
المطلب الثالث: إجراءات تفتيش نظم الحاسوب المادية والمعنوية.....	26
الفرع الأول: التفتيش في نظم الحاسوب المادية.....	27
الفرع الثاني: التفتيش في نظم الحاسوب المعنوية.....	27
المطلب الثالث:اجراءات معاينة مسرح الجريمة الالكترونية.....	29
الفرع الأول: تقنية فحص البروكسي (proxy):.....	29
الفرع الثاني: برنامج تتبع المعلومات.....	30
الفرع الثالث: نظام كشف الاختراق ntrlision.petection.....	30
الفصل الثاني: **الاجراءات المستحدثة للتحري والكشف عن الجرائم داخل المنظومة المعلوماتية (الاجراءات الحديثة)**	

الفهرس

تمهيد	32
المبحث الأول: الإجراءات الواردة في قانون إجراءات جزائية وقانون 09-04.....	33
المطلب الأول: الإجراءات الواردة في قانون إجراءات جزائية.....	33
الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور	34
أولا: اعتراض المراسلات السلكية واللاسلكية.....	34
ثانيا: وضع الترتيبات التقنية	37
الفرع الثاني: التسرب.....	40
أولا: تعريف التسرب:.....	40
ثانيا: شروط صحة عملية التسرب:.....	41
ثالثا: آثار التسرب.....	42
المطلب الثاني: الإجراءات الواردة في القانون 09-04	43
الفرع الأول: مراقبة الاتصالات الإلكترونية وتجميعها.....	43
ثانيا: حالات اللجوء إلى المراقبة الإلكترونية والعمليات الإجرائية لها.....	44
ثالثا: خصائص مراقبة الاتصالات الإلكترونية.....	46
الفرع الثاني: توسيع الإجراءات الخاصة بالاختصاص الإقليمي.....	47
أولا: الاختصاص المكاني في الجرائم المعلوماتية على المستوى الداخلي.....	47
ثانيا: الاختصاص المكاني في الجرائم المعلوماتية في المستوى الخارجي.....	49
المبحث الثاني: القواعد المتبعة للتفتيش والحجز داخل المنظومة المعلوماتية.....	51
المطلب الأول: قواعد التفتيش والحجز داخل المنظومة المعلوماتية.....	51
الفرع الأول: قواعد التفتيش داخل المنظومة المعلوماتية.....	51
الفرع الثاني: قواعد الحجز داخل المنظومة المعلوماتية.....	54
الفرع الثالث: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (المختصة بالبحث والتحقيق في الجرائم المعلوماتية).....	57

الفهرس

أولا: التعريف بالهيئة واختصاصاتها.....	57
ثانيا: تشكيل الهيئة وطبيعة عملها.....	58
المطلب الثاني: طرق الحصول والتعامل مع الدليل الرقمي في الإثبات الجنائي.....	59
الفرع الأول: مفهوم الدليل الإلكتروني.....	59
أولا: تعريف الدليل الإلكتروني:.....	59
ثانيا: خصائص الدليل الإلكتروني.....	60
ثالثا: أنواع الدليل الإلكتروني.....	61
الفرع الثاني: جمع الدليل والحصول عليه.....	61
الفرع الثالث: موقف المشرع الجزائري من الدليل الإلكتروني.....	64
خاتمة.....	66
قائمة المصادر والمراجع.....	69
الفهرس.....	75