جامعة عمار ثليجي – الأغواط
كلية الحقوق والعلوم السياسية
قسم الحقوق

الموضوع :

التحقيق في الجرائم الالكترونية

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في الحقوق

تخصص القانون الجنائي والعلوم الجنائية

اعداد الطالبة : **اشراف الأستاذ:**

- خديجة بج أ/ راضية عيمور

أعضاء لجنة المناقشة

الاسم واللقب	الصفة
د. عطالله خضرون	رئيسا
أ– راضية عيمور	مشرفا ومقررا
د. علي غريبي	ممتحنا

السنة الجامعية : 2025/2024

شكر

قبل كل أحد، وبعد كل أحد الشكر للواحد الأحد، الفرد الصمد، الذي أمدنا بالقوة والعون والسداد لإنجاز هذا العمل، وندعوه عز وجل أن يجعله خالصا لوجهه الكريم، كما أتقدم بالشكر الجزيل للأستاذ المشرف عطاالله خضرون، الذي لم يبخل عليا بأي معلومة أو توضيح في شتى مراحل إعداد هذه المذكرة.

كما أتوجه بالشكر لأعضاء لجنة المناقشة، وأساتذتنا بقسم (الحقوق) على المجهودات المبذولة لإصالنا إلى ما نحن عليه.

كما أشكر جميع من سعى معي لإتمام هذه المسيرة وكانو لي عوننا شكرا لكم.

اهداء

بسم الله الرحمن الرحيم

" يرفع الله الذين أمنوا منكم و الذين أوتو العلم درجات و الله بما تعملون خبير."

صدق الله العظيم.

الحمد لله

حبا و شكرا و امتنا على البدء و الختام. وصلاة وسلام على سيدنا محمد صلى الله عليه وسلم

اهدي بكل حب تخرجي إلى نفسي العظيمة القوية التي تحملت كل العثرات رغم الصعوبات.

إلى من لا ينفصل اسمي عن اسمه ذالك الرجل العظيم الذي مهدى لي طريق العلم سندي ومأمني أبي الغالي.

إلى التي علمتني الأخلاق قبل الحروف إلى الجسر الصاعد بي إلى الجنة، إلى التي تعجز كل الكلمات عن وصفها إلى التي كانت النور في عتمتي، إلى التي كان دعاؤها سر نجاحي إلى المضحية من أجلي ورافقتني في كل أوقاتي، إلى التي تعبت بدون مقابل لإتمام مسيرتي الدراسية إلى معلمتي ودكتورتي الأولى سيدتي العظيمة أمي الحبيبة متعها الله بالصحة والعافية.

إلى أخي وسندي والكتف الذي استند عليه ادامك الله ضلعا ثابتا.

إلى أختي داعمي الأول ووجهتي التي أستمد منها القوة إلى من رزقت بها سندا إلى من ازالت من طريقي أشواك الفشل، إلى التي كانت سبب نجاحي بعد الله أدامكي الله نورا لا ينطفئ.

إلى جميع من عرفتني بهم الحياة، إلى كل من وقعت عليه عيني من أهل الخير.

إلى زملائي الذين شاركوني مقاعد الدراسة.

إلى كل من كان له الفضل في وصولي إلى هذه المرحلة أهدي لهم تخرجي.

مقدمة

إن من أبرز خصائص العصر الحديث أنه أصبح مجتمع معلوماتي بحيث تطورت فيه وسائل تبادل المعلومات والتكنولوجيا عبر منظومة إلكترونية، وظهور الانترنت والتي بدورها ساهمت في تعزيز التواصل الحضاري والثقافي وكسر الحواجز بين الشعوب.

لقد كان للتطور الإلكتروني الكبير الذي تحقق في القرن العشرين أثر كبير على ربط العالم بشبكة إلكترونية جعلته خلية مترابطة، وككل ظاهرة جديدة رافقتها موجات كبيرة من الاختراق والتعديات وجرائم لم تكن تعرف من قبل ليست كالجرائم التقليدية، استعملت فيها تكنولوجيا المعلومات وهذه الجرائم أطلقت عليها تسمية الجرائم الإلكترونية أو المعلوماتية والتي انتشرت بشكل واسع، وهذا ما أدى إلى نشوء نصوص تشريعية وقوانين للحد من الاختراقات ووضع قواعد تنظم استعمال تكنولوجيا المعلومات، فالتقدم التكنولوجي لا يمكن أن يسير بمعزل على أي تقدم قانوني يواكبه ويكفل حمايته ويضع الحلول لما قد يطرأ من مشكلات بسبب استعماله، ففي هذه الحالة يمكن للتقدم التكنولوجي أن يصبح أداة للبناء وأساس لكل تطور، ويمكن أن يكون محفزا للوصول إلى المعلومات، أما إذا أسيئ استعماله يصبح أداة جريمة، فلا يقف القانون على مجرد تنظيم العلاقة المترتبة على التقدم التكنولوجي الناتج عن الثورة المعلوماتية بل أنه في ذات الوقت يحمي السلوكيات التي تحيط باستخدام التكنولوجيا، وهو ما يوجب على القانون أن تمتد نصوصه على الأنشطة الجديدة التي تفرزها التكنولوجيا حتى تحدد الجريمة في نصوص منضبطة وواضحة، والجزائر كغيرها من دول العالم التي تهددها الجرائم الإلكترونية فسعت إلى محاربتها عن طريق وضع ترسانة من القوانين والتي بدورها حددت إجراءات المتابعة والتحقيق في هاته الجرائم، وهذا التحقيق يعتبر نشاط قانوني يتعلق بإجراءات ضبط الجرائم والبحث عن مرتكبيها وجمع الاستدلالات التي يتطلبها التحقيق والدعوى الجنائية، وهذه المهام

أسندت إلى الضبطية القضائية من خلال أجهزة ومصالح مختصة مكافحة هذا النوع من الجرائم.[1]

إن أهمية الدراسة تكمن في أهمية الموضوع في حد ذاته، فيما يكتسبه من غموض أمام انتشار ظاهرة الجريمة الإلكترونية، والتزايد المستمر للنشاط الإجرامي عبر النظم المعلوماتية وتزايد درجة خطورة هذا النشاط وارتفاع مستوى التهديدات، ذلك أن التحقيق الجنائي في الجرائم الإلكترونية موضوع جديد ومستحدث وبالتالي مكافحة هاته الجرائم يشكل تحدي حقيقي بالنسبة للأجهزة المختصة، لان الجريمة الإلكترونية لها خصوصيات كصعوبة إثبات الدليل الإلكتروني.

ومن الأسباب التي دفعتنا إلى اختيار هذا الموضوع فتتمثل في الاهتمام الشخصي بالموضوع حيث أن تفشي هذه الجريمة أصبح يشكل خطرا كبيرا مما جعلها هاجسا وخطرا على المستوى العلمي، لما تلحقه هذه الجرائم من أضرار ما يستوجب إقامة أجهزة كفيلة بالإشراف على مكافحة هذه الجريمة واكتشاف دور المحققين في متابعة المجرمين المعلوماتيين والحد من هذه الظاهرة الخطيرة.

كذلك من الأسباب التي جعلتنا نختار هذا الموضوع هو دراسة تكنولوجيات الإعلام والاتصال والمحتويات التي تحملها والسلوكيات التي تنتجها والجريمة الإلكترونية كأحد مفرزات هذه التكنولوجيات تستوجب دراستها كظاهرة مستحدثة، والوصول إلى حلول لمكافحتها.

عند دراستنا لهذا الموضوع والبحث فيه واجهتنا العديد من الصعوبات ولعل أهمها:

أنه موضوع جديد ومتشعب يتطلب الكثير من الإلمام من كل الجوانب و ندرة في المصادر والمراجعو ندرة المعلومات من الأجهزة المختصة في مكافحة الجرائم الإلكترونية بسبب سرية التحقيقات وذلك لدواعي أمنية.

[1] خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية،دار الفكر الجامعي، الإسكندرية، مصر، 2010، ص 30.

إن التطور الكبير الذي عرفته تكنولوجيا المعلومات أدى إلى تحول في المجال الإجرامي، بحيث انتقل من الكلاسيكية إلى الحداثة، مما صعب مهمة المحققين في إيجاد سبل كافية واليات لردع الجريمة الإلكترونية، وهذا بسبب وجود نصوص قانونية غير كافية وكذلك قلة الدراسات والبحوث في هذا المجال، وبالتالي توسع الهائل في التطور للجريمة الإلكترونية وإجراءات التحقيق الجنائي، ومن هنا يمكن طرح الإشكالية التالية:

ما مدى نجاعة النصوص المكرسة من طرف المشرع الجزائري في مجابهة الجرائم الإلكترونية والحد منها؟

وتم الإعتماد على المنهج الوصفي الذي يعتمد على وصف الجريمة الإلكترونية وتحليلها، وكذلك التحقيق الجنائي والكشف عن إجراءات متابعة المجرمين الإلكترونيين من طرف الأجهزة المختصة لردع ومكافحة الجرائم الإلكترونية.

ولدراسة هذا النوع من المواضيع يجب تسليط الضوء على ظاهرة الجريمة الإلكترونية، ومختلف آليات وإجراءات التحقيق الجنائي فيها، وتم ذلك من خلال فصلين:

الفصل الأول تطرقنا فيه إلى إجراءات التحقيق في الجريمة الإلكترونية وذلك لمجابهة هذا النوع من الجرائم من طرف الضبطية القضائية والقضاء، وقد اعتمدنا على مبحثين، المبحث الأول تحت عنوان دور جهاز الضبطية القضائية في مجابهة الجريمة الإلكترونية، أما المبحث الثاني تحدثنا فيه عن الإجراءات التي يباشرها قاضي التحقيق في الجرائم الإلكترونية، أما الفصل الثاني فتناولنا فيه التحقيق في الجرائم الإلكترونية من خلال القانون رقم (09_04)، وهذا من أجل التعرف على مختلف الآليات والإجراءات المتخذة من طرف الهيئات المختصة في التحقيق، حيث اعتمدنا على مبحثين كذلك، المبحث الأول تناولنا فيه آليات المتابعة في الجرائم الإلكترونية، أما المبحث الثاني فتطرقنا إلى الوحدات المختصة التي تتولى إجراءات البحث

والتحقيق في الجريمة الإلكترونية، والذي يحدد القواعد الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفصل الأول:

إجراءات التحقيق في الجريمة الالكترونية

إن كون الجرائم المعلوماتية حديثة النشأة ويمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال والتي تستخدم في جميع مجالات الحياة سواء من طرف الأفراد أو المؤسسات إذ تجعل التعامل معها صعبا ومعقدا مما يحتم إيجاد طرق جديدة وتابعة لمكافحتها.

والجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا فهي أيضا معنية بالمكافحة، فكان لابد من إيجاد إطار قانوني مناسبا لسد الفراغ الإجرائي، لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المعلوماتية عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل وإجراءات خاصة تتماشى مع طبيعة الجرائم المستحدثة ومنها الجريمة المعلوماتية، وفيها إجراءات تطبق فقط على الجريمة المعلوماتية ، التي تم النص عليها في قانون جديد يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته 04/09 المؤرخ في أوت 2009، لذا سنتناول في هذا الفصل آليات مجابهة الجريمة الإلكترونية في التشريع الجزائري.

المبحث الأول: دور جهاز الضبطية القضائية في مجابهة الجريمة الإلكترونية

كافح المشرع الجزائري جرائم المعلوماتية من خلال قانون الإجراءات الجزائية، ومن خلال قانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث نص قانون الإجراءات الجزائية على مجموعة من إجراءات التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والتي تتمثل فيما يلي على إجراء التفتيش والتسرب، [1]

المطلب الأول: إجراءات التفتيش للضبطية القضائية في الجرائم الإلكترونية

يعتبر التفتيش من اخطر الحقوق التي منحت للمحقق وذلك لمساسها بالحريات التي تكفلها الدساتير عادة، ولذا نجد المشرع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشرها وتأذن بمباشرتها والأحوال التي تجوز فيها مباشرته وشروط اتخاذ هذا الإجراء بما يمثل ضمانات الحرية الفردية أو حرمة المسكن.

إن الأنظمة الجنائية عرفت في مراحل تطورها أنواعا من الإجراءات تنطوي على انتهاك لحقوق الأفراد الأولية في سبيل تتبع الجناة ومحاكمتهم ومنها القبض والتفتيش فإذا ما تخلت يد العدالة عن التعرض لحقوق الأفراد لأصبحنا إزاء فوضى إجرامية، ومن ثم يجب أن يتاح للقائمين على تنفيذ القانون نوع من السلطة في إنكار الحريات الشخصية بالقدر الذي يحول دون تسلط الإجرام على مقدرات الناس وإنما لاينبغي أن يتجاوز هذا القدر، إذ لا فارق بين أن تنتهك حريات الأفراد بمعرفة أشخاص يعملون تحت ستار القانون أو بمعرفة مجرمين يرتكبون جرائمهم بمنا عن سطوة القانون ومن هذه الإجراءات التفتيش.[2]

---

[1] سعيدان نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادةالماجيستير، جامعة باتنة، 2012_2013،ص147.

[2] خالد ممدوح إبراهيم، مرجع سابق، ص 80.

ويعرف التفتيش على انه: عبارة عن إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة.

وموضوع التفتيش في الجريمة الإلكترونية: إذا كانت الجريمة واقعة على مكونات المادية للكمبيوتر، فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش، أما إذا كانت الجريمة واقعة على برنامج الكمبيوتر وبياناته، فان الصعوبات تبرز على اعتبار أن بإمكان الجاني التخلص من البيانات التي يستهدفها التفتيش عبر إرسالها من خلال نظام معلوماتي من مكان إلى أخر، أو إلى نظام معلوماتي أخر وعلى اعتبار أن التفتيش عن هذه البيانات، يستوجب الكشف عن الرقم السري pass ward للمرور إلى ملفات البيانات، وهذا الرقم السري يعرفه المتهم، ولا يمكن إجباره على البوح بها والإفصاح عنه.

إن من أخطر الإجراءات التي تجريها الضبطية القضائية في إثبات الجريمة، إجراءات التفتيش سواء ما تعلق بشخص المتهم أو مسكنه لأنه ماس بحريته وسكينته ولخطورة ما يسفر عنه من أدلة تكشف وجه الحقيقة، وقد حرص الدستور الدائم في جمهورية مصر العربية على تقرير حرمة الأشخاص والمساكن وجعلها مصونة لا يجوز المساس بها إلا بأمر قضائي مسبب أو في حالة تلبس.[3]

الفرع الأول: تفتيش وضبط الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في حالة تلبس الجريمة:

ويكون ذلك وفقا للقواعد التالية:

أولا: الحصول على إذن مسبق من قبل السلطة القضائية:

[3] خالد ممدوح إبراهيم، مرجع سابق، ص 181.

نصت المادة 44 ق.إ.ج: لا يجوز لضابط الشرطة القضائية الانتقال إلى مسكن الأشخاص الذين يظهر بهاما ساهموا في الجناية أو بها مايحوزون أوراقا أو أشياء لها علاقة لأفعال الجناية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادرا من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستضهار إذن الأمر قبل الدخول إلى المنزل والشروع في التفتيش.

ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها او التحقيق في إحدى الجرائم المذكورة في المادتين 37 و 40 من هذا القانون.[4]

يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان، تنجز هذه العملية تحت الإشراف المباشر للقاضي الذي أذن بها والذي يمكنه عند الاقتضاء أن ينتقل إلى عين المكان للسهر على احترام أحكام القانون.[1]

إذا اكتشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإن ذلك لا يكون سببا بطلان الإجراءات العارضة.

ثانيا: حضور صاحب المسكن أثناء عملية التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

يخضع التفتيش والضبط في الجرائم الماسة بأنظمة المعالة الآلية للمعطيات وبعض الجرائم المنصوص عليها على سبيل الحصر في المادة 3/47 قانون الإجراءات الجزائية، لقواعد خاصة تختلف عن القواعد العامة المقررة في البندين 1 و 2 من المادة 1/45 قانون الإجراءات الجزائية، وتختلف هذه القواعد حسب حالتين:

1/ الحالة الأولى:

[4] المادة 44 من الأمر رقم 66_155: المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[1] سعيدان نعيم، مرجع سابق، ص .150

إذا تعلق الأمر لتحقيق التمهيدي في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة لتشريع الخاص لصرف، فإن ضابط الشرطة القضائية بموجب الفقرة الأخيرة من المادة 45 منها لم يعد مقيدا عند إجراء تفتيش المساكن والمحلات لشرط المتعلق بضرورة حضور المشتبه فيه أو من ينوبه أو شاهدين إذا حصل التفتيش بمسكنه، وكذلك الأمر إذا حصل التفتيش في مسكن شخص أخر يشتبه به يحوز أوراقا أو أشياء لها علاقة بالجريمة.[2]

2/ الحالة الثانية:

أصبح ضباط الشرطة القضائية إذا تعلق التحقيق التمهيدي الذي يجريه بجريمة متلبسا أوتحقيق متعلق بإحدى أنواع الجرائم السالفة الذكر، يمكنه بموجب المادة 47 مكرر المستحدثة في قانون الإجراءات الجزائية أن يجري التفتيش بعد الموافقة المسبقة من وكيل الجمهورية بحضور شاهدين مسخرين من غير الموظفين الخاضعين لسلطته أو بحضور ممثل يعينه صاحب المسكن محل التفتيش، إذ كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا في مكان أخر وأن الحال يقتضي عدم نقله إلى ذلك المكان بسبب مخاطر جسيمة قد تمس لنظام العام أو لحتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله، ولضابط الشرطة القضائية وحده مع الأشخاص الحاضرين عملية التفتيش، الحق في الإطلاع على الأوراق أو المستندات قبل حجزها، غير أنه عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر، وتغلق الأشياء والمستندات المحجوزة ويختم عليها إذا أمكن ذلك، فإذا تعذرت الكتابة عليها فإنها توضع في وعاء أو كيس يضع عليه ضابط الشرطة القضائية شريطا من الورق ويختم عليه بختمه.

[2] علي عشاني، بن بعلاش خاليدة، الأحكام الموضوعية والإجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة أبحاث قانونية وسياسية، المجلد 6، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل، 2018، ص 703.

ثالثا: توقيت التفتيش والضبط في المعلومات

إذا كان قانون الإجراءات الجزائية قد وضع قاعدة قانونية عامة تحدد بدقة الميقات الذي يجوز فيه دخول المساكن وتفتيشها وإجراء الحجز لها، وهو بين الساعة الخامسة صباحا والساعة الثامنة مساء المحددة في المادة 1/47 من قانون الإجراءات الجزائية، فإنه وضع استثناء لتلك القاعدة، وهو جواز دخول المساكن وتفتيشها في أي وقت من اليوم ليلا ونهارا، دون التقيد بذلك الميقات القانوني، هذه الاستثناءات وردت في المواد 1/47، 2/47، 3/47 ق إ ج.[1]

وفيما يخص لاستثناء الوارد في المادة 3/47 قانون الإجراءات الجزائية فالأمر يتعلق بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب وكذا الجرائم المتعلقة لتشريع الخاص لصرف، فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناء على إذا مسبق من وكيل الجمهورية المختص، أو أن يقوم قاضي التحقيق بعملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو أمر ضباط الشرطة القضائية المختصين للقيام بذلك (المادة 4/47 قانون الإجراءات الجزائية)، لأن الغرض من الإسراع في الإجراء والقيام به خارج الميقات المحافظة على الدليل نظرا للطبيعة الخاصة لهذا النوع من الجرائم التي يستفيد فيها المشتبه فيه من التطور التكنولوجي، ولا تمس هذه الأحكام لحفاظ على السر المهني المنصوص عليه في الفقرة الثالثة من المادة 45 من قانون الإجراءات الجزائية (م6/47).[2]

[1] وردة شرف الدين، سامية بلجرف، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري،مجلة المنار للبحوث والدراسات القانونية، المجلدة 1، العدد 3، كلية الحقوق والعلوم السياسية جامعة يحي فارس بالمدية، 2017، ص 31.

[2] تابري مختار، السلطة القائمة على التحقيق في الجريمة الالكترونية، مجلة القانون العام الجزائري والمقارن، المجلدة 8، العدد 1،جامعة جيلالي اليابس سيدي بلعباس، الجزائر، 2022، ص 358.

الفرع الثاني: التفتيش والضبط في الجرائم المعلوماتية في مرحلة التحقيق الابتدائي

نصت المادة 64 قانون الإجراءات الجزائية أنه لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر فيذلك في المحضر مع الإشارة إلى رضاه، مع ضرورة التقيد لأحكام المنصوص عليها في المواد 44 إلى 47 قانون الإجراءات الجزائية . غير أنه عندما يتعلق الأمر بتحقيق في إحدى الجرائم المنصوص عليها في المادة 3/47 قانون الإجراءات الجزائية فإنه تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر قانون الإجراءات الجزائية.[1]

المطلب الثاني: إجراءات التسرب للضبطية القضائية لمواجهة الجرائم الإلكترونية

استحدث المشرع الجزائري في قانون الإجراءات الجزائية اختصاصين جديدين، الأول اعتراض المراسلات وتسجيل والتقاط الصور والثاني التسرب، فتعرف المادة 65 مكرر 12 التسرب على أنه " يقصد لتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة أنه فاعل معهم أو شريك لهم أو خاف "، حيث تتم هذه الإجراءات وفقا للقيود والشروط المقررة في الأحكام المقررة قانونا، والتي تتمثل فيما يلي:[2]

_ أن تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم الموصوفة الإرهابية وجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية

[1] سعيداني نعيم، مرجع سابق، ص 151.

[2] سعيداني نعيم، مرجع سبق ، ص 153.

للمعطيات وجرائم تبيض الأموال والجرائم المتعلقة لتشريع الخاص لضرف وجرائم الفساد والتهريب، عملا بحكم المادتين 65 مكرر 5، 65 مكرر 11 من قانون الإجراءات الجزائية.

_ يجب أن يتم الإذن بعملية التسرب من طرف وكيل الجمهورية أو من طرف قاضي التحقيق، بعد إخطار وكيل الجمهورية.

_ يجب أن يكون الإذن المسلم مكتوبا ومسببا وذلك تحت طائلة البطلان، مع ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تمم العملية تحت مسؤوليته، ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر ويمنك أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية. ويجوز للقاضي الذي رخص إجرائها أن مر في أي وقت، بوقفها قبل انقضاء المدة المحددة، وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.[1]

لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشرو عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات، ويعاقب كل من يكشف هوية ضباط أو أعوان الشرطة القضائية لحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة مالية من 50.000 ألى 200.000 دج.

وإذا تسبب الكشف عن الهوية في أعمال العنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (5) إلى عشر (10) سنوات والغرامة من 200.000 دج إلى 500.000 دج.

وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون عقوبة الحبس من عشر (10) سنوات إلى عشرين (20) سنة والغرامة المالية من 500.000 إلى 000000 1 دج دون

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة تخرج لنيل شهادة الماجيستير في القانون، جامعة مولود معمري تيزي وزو، تاريخ المناقشة 2013/30/06، ص 100.

الإخلال، عند الاقتضاء، بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات[2].

_إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة إجراءات التسرب مواصلة إجراءات التسرب للوقت الضروري الكافي لتوقيف عملية المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا تتجاوز ذلك مدة أربعة (4) أشهر، وفي هذه الحالة يتعين إخبار القاضي الذي رخص جراء عملية التسرب تلك في أقرب الآجال، فإذا انقضت مهلة الأربعة (4) أشهر تلك دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، أمكن لهذا القاضي أن يرخص بتمديدها لمدة أربعة (4) أشهر على الأكثر.

_ يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية.

ومن خلال قانون الوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال:

نص هذا القانون أيضا على جملة من الإجراءات المستحدثة والخاصة لتحري والتحقيق عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومنها طبعا الجرائم الماسة لتوقيع الإلكتروني، كمراقبة الاتصالات الإلكترونية، تفتيش النظم المعلوماتية، حجز المعطيات المعلوماتية، جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، التحفظ العاجل للبيانات المعلوماتية المخزنة وسنتكلم بمزيد من التفاصيل عن كل إجراء فيما يلي:

الفرع الأول: مراقبة الضبطية القضائية للاتصالات الإلكترونية

يقصد بـا لاتصالات الإلكترونية حسب المادة 2 ومن القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: أي تراسل أو

[2] سعيداني نعيم، مرجع سابق، ص 155.

إرسال أو استقبال علامات أو إشارات أو كتابة أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.[1]

وقد نص المشرع الجزائري في المادة 04 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على مراقبة الاتصالات الالكترونية.

الفرع الثاني: تفتيش النظم المعلوماتية

_ نص المشرع الجزائري في المادة 5 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على ضرورة توافر حالات على سبيل الحصر، تجيز للسلطات القضائية وضباط الشرطة القضائية القيام بتفتيش المنظومة المعلوماتية في إطار قانون الإجراءات الجزائية، وهي:[1]

1/ للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة من الدولة.

2/ في حالة توافر المعلومات عن احتمال اعتداء على منظومة معلوماتية نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

3/ لمقتضيات التحري والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة ما الأبحاث الجارية.

4/ في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

[1] صغير يوسف، مرجع سابق، ص 101.

[1] سعيداني نعيم، مرجع سابق، ص 177.

الفرع الثالث: حجز الضبطية القضائية للمعطيات المعلوماتية

نظمه المشرع الجزائري في نص المادة 06 و 07 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[5]

وتتمثل شروط إجراء الحجز فيما يلي:

_ عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم النسخ كل المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

_ ويجب على السلطة التي تقوم لتفتيش والحجز للسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

_ غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

_ إذا استحال إجراء الحجز وفقا لما هو منصوص عليه فيما سبق، لأسباب تقنية، لذا يتعين على السلطة التي تقوم لتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم استعمال هذه المنظومة.

[5] أنظر المادة 6 و 7 من القانون 09_04 مؤرخ في 14 شعبان 1430 الموافق غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادر بتاريخ 05أوت 2009.

_ على السلطة التي تباشر التفتيش أن أمر اتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكيف أي شخص مؤهل لاستعمال الوسائل التقنية المناسبة لذلك.

_ تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة، إلا في الحدود الضرورية للتحري أو التحقيقات القضائية.[1]

_ في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس من الدولة، تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة الإعلام والاتصال ومكافحتها حصر إجراءات الحجز.

المبحث الثاني: الإجراءات التي يباشرها قاضي التحقيق في الجرائم الإلكترونية

لقد خص المشرع الجزائري قاضي التحقيق بسلطات واختصاصات واسعة في سبيل تحقيق الهدف من إسناد مهمة التحقيق إلى قاضي تحقيق مستقل عن جهة المتابعة وجهة الحكم، وقد خولته المادة 68 من قانون الإجراءات الجزائية،[2] سلطة اتخاذ أي إجراء يراه ضروريا للكشف عن الحقيقة، كاستجواب المتهمين، وسماع الشهود والتفتيش وإجراء الخبرات وغيرها من الاختصاصات، وقد اتجهت إدارة المشرع إلى منحه سلطات جديدة لم يكن يتمتع بها في سبيل مواجهة الأنواع الجديدة من الجرائم المعلوماتية، وهو ما سنطرق إليه من خلال ما يلي:

المطلب الأول: إجراءات المعاينة في الجريمة الإلكترونية

مع تزايد استخدام الكمبيوتر والإنترنت والشبكات الداخلية والخارجية تزايدت نسبة الجريمة المرتكبة باستخدام هذه التقنيات الجديدة، سواء كانت هذه الجريمة تمت عبر الكمبيوتر، أم

[1] صغير يوسف، مرجع سابق، ص .110

[2] أنظر المادة 68: من الأمر رقم 66_155 الذي يتضمن ق.إ.ج المعدل والمتمم.

الجريمة تمت على الكمبيوتر، بمشتملاته المادية والمعنوية، إلى استخدام الكمبيوتر والانترنيت ماداموا يشعرون أن أجهزة إنفاذ القانون ورجال القضاء والنيابة والمحامين ورجال البحث الجنائي شبه عاجزون عن ضبطهم واستخلاص دليل إدانتهم سواء أكانت دليلا حسيا أم رقميا.

وعلى الرغم من أن التعامل في مسرح الجريمة المادية إلى مسرح الجريمة الإلكتروني أو الرقمي، ذلك أن التطبيقات أو البرنامج والبيانات المرقمة عنصران أساسيان يتحكم على أجهزة إنفاذ القانون وخبراء الأدلة الجنائية جمعها واستخلصها.

يراعي سرعة إجراء معاينة مكان الحادث والتحفظ على أدلة الجريمة والاثار المتخلفة عنها ووصف مكان الجريمة وكيفية ارتكابها وكيفية وصول الجاني إلى مكانها وهروبه منها ويتم حصر الأشياء المختلف عن الجريمة ومكان العثور عليها وتثبت هذه المعاينة في المحضر ويرفق به رسم تخطيطي بمكان الحادث.[1]

والمقصود بالمعاينة مسرح الجريمة الإلكترونية هو مناضرة وفحص ووصف المكان أو الشيء، أو الشخص الذي له علاقة بالجريمة واثبات حالته، حيث ينتقل قاضي التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة ماديا وكل ما يلزم إثبات حالته. فالمعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوافق طبيعتها على صفتها بمن يجريها بل على مدى ما يقتضيه إجرائها من مساس بحقوق الأفراد، فإذا جرت المعاينة في مكان عام مثل مقهى الانترنت كانت إجراء استدلال وإذا اقتضت دخول مسكن له حرمة خاصة كانت إجراء تحقيق.

حيث أصبح قضاة التحقيق عاجزون على ضبط واستخلاص دليل إدانة المجرم المعلوماتي، ويتطلب مسرح الجريمة سواء كان ماديا أو معنويا (الكتروني) إجراءات خاصة تختلف عن

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 142.

الإجراءات التي سبق وقد عرضناها في مرحلة البحث والتحري عن الجريمة المعلوماتية وذلك باختلاف الجهة القضائية في هذه المرحلة ألا وهو قاضي التحقيق.[2]

الفرع الأول: الانتقال إلى المعاينة (انتقال قاضي التحقيق للمعاينة)

إن من أعمال قاضي التحقيق الانتقال إلى أماكن وقوع الجريمة للمعاينة وضبط ما قد يعثر عليه من أثار وسماع ما قد يجده من شهود في عين المكان قبل أن يقع التأثير عليهم من المتهم أو من أطراف أخرى وهو ما قرره المشرع الجزائري في المادة 97 من قانون الإجراءات الجزائية، [1] وتتم المعاينة في الجريمة المعلوماتية المرتكبة عبر الإنترنت كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية إلا أن الانتقال هناك لا يكون إلى العام المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني.

وحتى تكون المعاينة صحيحة لابد على قاضي التحقيق أن ينتقل إلى مكان وقوع الجريمة بصحبة كاتبه بعد إخطار وكيل الجمهورية المختص إقليميا بجميع الإجراءات اللازمة، وحتى يستطيع قاضي التحقيق أن ينتقل إلى عالم الفضاء الالكتروني لمعاينته، عدة طرق تتمثل في:

_ الانتقال إلى العالم الافتراضي من المكتب بالمحكمة من خلال الكمبيوتر الخاص به

_ اللجوء إلى مقهى الإنترنت.

_ يجوز له اللجوء إلى مقر عمل مزود بخدمة الإنترنت providder server internet.[1]الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة.

كما يستطيع قاضي التحقيق أيضا الانتقال إلى العالم الافتراضي للمعاينة من خلال مقر مكتب الخبير التقني المختص، وبالتالي يتضح مما سبق أن هناك عوائق ومشكلة أمام قاضي

[2] سعيداني نعيم، مرجع سابق، ص .180.

[1]انظر المادة 97 : من الأمر رقم 66_155 الذي يتضمن ق.إ.ج المعدل والمتمم.

[1]يقصد مزود بخدمة الإنترنت: وهي شركة التي توفر لعملائها إمكانية الوصول إلى الإنترنت.

التحقيق من خلال الانتقال إلى العالم الافتراضي، حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال آثار الجريمة.

الفرع الثاني: الخطوات الواجب إتباعها قبل الانتقال إلى مسرح الجريمة المعلوماتية

يجب على المحقق الجنائي (قاضي التحقيق) قبل الانتقال إلى معاينة مسرح الجريمة المعلوماتية إتباع الخطوات التالية:

_ توفير معلومات مسبقة عن مكان الجريمة، ومالك المكان، نوع وعدة أجهزة الكمبيوتر.

_ قطع التيار الكهربائي عن موقع المعاينة لشل فعالية الجاني من القيام بأي فعل من شأنه التأثير عليه أو محو آثار الجريمة.

_ إعداد فريق بحث من المختصين والفنيين.

الفرع الثالث: شروط صحة معاينة مسرح الجريمة

حتى تعطي المعاينة ثمارها للكشف عن الغموض والتواصل إلى الجاني لابد أن يراعي قاضي التحقيق ما يلي:

1/ سرعة الانتقال إلى مكان الجريمة:

فور تلقي المحقق أو قاضي التحقيق البلاغ عن وقوع الجريمة من الجرائم المعلوماتية والتأكد من صحة الواقعة، عليه أن ينتقل إلى مكانها، وذلك ضمانا لعدم التغيير شكل مسرح الجريمة عن الوضع والحالة التي تركها الجاني عليه،

والحصول على شهادة الشهود.[1]

2/ السيطرة على مكان وقوع الجريمة:

[1] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، طبعة 1، دار الجامعة الجديدة للطباعة والنشر، بيروت، 1999، ص 58.

بمجرد وصول قاضي التحقيق البلاغ عن مكان وقوع الجريمة من أجل معاينتها لابد من أن يتبع مجموعة من الإجراءات التالية:

_ منع تواجد أحد بداخل مسرح الجريمة حتى لا يؤثر ذلك على الآثار والأدلة التي تم العثور عليها في المسرح.

_ التأكد من عدم لمس أية آثار أو أدوات بداخل مسرح الجريمة.

_ إخطار الخبراء لرفع الآثار والبصمات.[2]

المطلب الثاني: إجراءات التفتيش والاستجواب وضبط الأدلة في الجريمة الإلكترونية

يقوم قاضي التحقيق في مجال الكشف والبحث والتحري عن الجريمة المعلوماتية وكشف الغموض عنها والقبض على فاعلها باتخاذ الكثير من الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه، ومن بينها:

_ التفتيش.

_ استجواب المتهم.

_ سماع شهود (شاهد الكتروني).

_ ضبط الدليل الالكتروني.

الفرع الأول: التفتيش في الجريمة الإلكترونية

تطرقنا في المبحث الأول إلى التفتيش، مفهومه وضوابطه في الجريمة المعلوماتية غير أن أوجه الإختلاف في الجهة أو السلطة المختلطة ففي المبحث الأول فإن الضبطية القضائية هي المختصة بالقيام بالتفتيش في مجال الجريمة الإلكترونية[1] على خلاف هذا الفرع فإن قاضي التحقيق في هذه الحالة هو المختص وهو ما سنطرق إليه فيما بعد:

[2] خالد ممدوح ابراهيم، مرجع سابق، ص 159.

[1] للتفصيل أكثر: الإحالة إلى المبحث الأول من الفصل الأول من إجراءات التفتيش للضبطية القضائية في الجريمة الإلكترونية.

وقد خولت المواد من 79 إلى 81 ق.إ.ج.ج لقاضي التحقيق الاختصاص، الانتقال إلى منازل المتهمين أو المشتبه فيهم أو الذين بحوزتهم أشياء لها علاقة بالجريمة لتفتيشها والحصول على الأدوات المستعملة في الجريمة.

وبالتالي نجد أن جميع الإجراءات الخاصة بالتفتيش في الجريمة المعلوماتية في مرحلة جمع الاستدلالات هي نفسها الإجراءات في مرحلة التحقيق القضائي مع بعض الاختلافات البسيطة المتعلقة بجهاز التحقيق (قاضي التحقيق).

وحتى يكون التفتيش الذي يقوم به قاضي التحقيق سواء بنفسه (أو بواسطة ضابط الشرطة القضائية كما بينا سابقا) لابد من احترام مجموعة من القيود والشروط الآتية:

_ وقوع الجريمة فعلا وان يتحصل على فائدة وراء التفتيش من أجل كشف الحقيقة.

_ أن يكون هناك اهتمام قائم ضد شخص معين من أجل القيام بعملية التفتيش.

_ أن تكون الواقعة المرتكبة جناية أو جنحة.

_ أن يكون المنزل أو المحل المراد تفتيشه معروفا ومحددا.[2]

لابد ان يتم التفتيش من قبل قاضي التحقيق وذلك بعد إخطار وكيل الجمهورية الذي يمكن مرافقته حيث يكون مصحوبا بكاتب التحقيق.[1]

فإذا حصل التفتيش في منزل المتهم أو مسكن المتهم أو مسكن شخص آخر يشتبه أن يحوز أشياء لها علاقة بالجريمة فعلى قاضي التحقيق أن يقوم بهذه العملية بحضور المتهم أو صاحب المسكن فإن تعذر حضوره أو كان هاربا يتعين على قاضي التحقيق إحضار شهدين لا يكون لهما صلة بالمتهم وذلك طبقا للمادة 82، 08 ق.إ.ج.ج[1](من الساعة الخامسة صباحا إلى

---

[2]عبده جميل غصوب، الوجيز في قانون الإجراءات الجزائية طبعة 1، المؤسسة الجامعية للنشر والتوزيع، بيروت، 2011، ص 298.

[1] أنظر المادة 79: من الأمر رقم 66_155 الذي يتضمن ق.إ.ج المعدل والمتمم.

[1]أنظر المادة 80، 83: من الأمر رقم 66_155 الذي يتضمن ق.إ.ج المعدل والمتمم.

الساعة الثامنة ليلا)[2] وغير أن قاضي التحقيق خرج عن القاعدة العامة في ميعاد التفتيش في الجرائم المعلوماتية حيث يجوز له القيام بعملية التفتيش ليلا أو نهارا طبقا لنص المادة 74 فقرة 4 ق.إ.ج.ج.[3]

الفرع الثاني: استجواب المتهم من طرف قاضي التحقيق والشهادة الالكترونية

هناك مشكلة صعبة للمحقق الجنائي حين يقوم باستجواب المجرم المعلوماتي أو في محاولة الحصول على اعتراف منه ذلك إن المجرم الالكتروني هو من نوعية خاصة غير معروفة من قبل حيث يصعب الإمساك به كما أن المجرم ذكي ومتمرس بتفاصيل الكمبيوتر والشبكات والبرمجة وتشير المعلومات إلى أن اغلب مرتكبي الجرائم المعلوماتية يقيمون في دول العالم الثالث المختلفة في كل شيئا لا في مجرميها الالكترونيين الأذكياء.

ولا شك إن ذكاء الجرم المعلوماتي يجب أن يقابله من جهة أخرى محقق شديد الذكاء ولذلك سوف نعرض في هذا المقام إلى أصول وفن الاستجواب والاعتراف في نطاق الجرائم المعلوماتية.

الاستجواب في الجريمة المعلوماتية يعتبر من أهم إجراءات التحقيق في كشف الحقيقة يمكن الاستجواب السلطة المناط بها التحقيق من طرح الأسئلة الدقيقة والولوج في موضوع الدعوى والتعرف على أدق التفصيلات فيما يتعلق بالجريمة.

أولا: استجواب المتهم من طرف قاضي التحقيق:

الاستجواب هو مناقشة المتهم بالتهم والوقائع المنسوبة إليه ومواجهته بالأدلة القائمة ضده والمتهم حر في الإجابة عن الأسئلة الموجهة عليه ولا يعد امتناعه قرينة ضده، وهو وسيلة

[2] أنظر المادة 47: من الأمر رقم 66_155 الذي يتضمن ق.إ.ج المعدل والمتمم.

[4] خالد ممدوح إبراهيم، مرجع سابق، ص .241

تمحيص للمتهم أو لنفيها عنه فهو طريق من طرق تقصي الحقيقة ومصدر من مصادر الإثبات وليس وسيلة إثبات.[1]

إذا اعتبر الاستجواب ذو طبيعة مزدوجة فهو أداة اتهام ووسيلة دفاع في آن واحد بحيث يسمح للمتهم أن يحاط بالتهم والوقائع المنسوبة إليه وبكل ما يوجد بالملف من أدلة التي تساعد على كشف براءته.

_ استجواب المتهم في الموضوع:

أي مواجهة قاضي التحقيق المتهم بالتهم المنسوبة إليه ومناقشته فيها مناقشة تفصيلية ومواجهته بالأدلة القاطعة ضده ولابد ان يكون الاستجواب بحضور المحامي طبقا لنص المادة 105 ق.إ.ج.ج 101، 102 ق.إ.ج.ج .

_ الاستجواب الإجمالي للمتهم: يكون في مسائلة جنائية (جنايات) وهو إجراء وجوبي إذا تعلق التحقيق بقضية ذات طابع جنائي، يهدف إلى تخليص الوقائع وإبراز الأدلة التي سبق جمعها.

القواعد التي يلتزم بها المحقق في الاستجواب:

يعتبر الاستجواب إجراء من الإجراءات العامة في التحقيق لأن نجاح المحقق في إسناد الواقعة إلى الجاني واعترافه بارتكابها.

وحتى يكون الاستجواب صحيحا لابد ان يتضمن مجموعة من الإجراءات وهو ما سنتناوله بالتفصيل في ما يلي: [2]

1/ القواعد التي يلتزم بها المحقق قبل إجراء الاستجواب:

[1] أحسن بوسقيعة، التحقيق القضائي، دار هومة للطباعة والنشر، الجزائر، 2006، ص 45.

[2] خالد ممدوح ابراهيم، مرجع سابق، ص 240.

قبل أن يقوم المحقق بإجراء الاستجواب والمواجهة عليه أن يستعد لها وذلك بإتباع القواعد العامة التالية:

الإلمام الكامل بفهم أقوال الشهود وسائر المتهمين أن يحدد النقاط الجوهرية التي سيتم اتضاحها من المتهم.فهم فحوى التقارير الفنية التي وضعها الخبراء عن نتائج عملهم في الآثار المستخلصة، وضع خطة لنفسه يسير عليها في استجواب المتهم.[1]

2/ القواعد التي يلتزم بها المحقق الجنائي عند البدء في الاستجواب:

على المحقق عند البدء في الاستجواب أن يراعي اتخاذ وإتباع القواعد التالية:

_ إذا أعلن المتهم عم محاميه لابد من دعوة المحامي لحضور الاستجواب.

_ تفتيش المتهم.

_ عدم إكراه المتهم على الاعتراف بأي شكل من أشكال التعذيب.

كما يختلف الاستجواب عن السؤال في أن الثاني لا يتطلب مناقشة المتهم عن التهمة المسندة إليه تفصيليا ومواجهته بالأدلة ويمكن لمأمور الضبط القضائي، فالاستجواب من إجراءات التحقيق في حين أن السؤال من جمع الاستدلالات.

ثانيا: الشهادة الالكترونية (سماع الشهود) (الشهادة الالكترونية)

أما بالنسبة لشهادةالشهود فهي من أهم الأدلة يمكن لمحكمة الموضوع إن تأخذ بتا في القضاء الذي تصدره على المتهم سواء بالإدانة أو بالبراءة فالشهادة هي من أسهل الأدلة التس يمكن الحصول عليها لما يحدث عملا من ان يشاهد الواقعة احد الأشخاص أو أن يسمع نتائجها أو قد تكون ناتجة عن استعمال احد الحواس إلا أنها من الأهمية كذلك في خطورة تقيمها والاعتماد عليها حيث أنها من الدلائل التي يمكن اصطناعها أو الكذب فيها وينطبق هذا على الشهادة سواء التي أبديت امام جهات التحقيق أو تلك التي ابديت أمام المجكمة.

[1] خالد ممدوح ابراهيم، مرجع سبق، ص 243.

كما يمقوم المحقق الجنائي في مجال الكشف عن غموض الجريمة المعلوماتية وفاعلها باتخاذ الكثير من الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه ومنها ضبط الأدلة الإلكترونية.

_ الشهادة الالكترونية: إن مصطلح الشهادة الإلكترونية يطلق على نوع من الشهادة التي لا يكون فيها الشاهد حاضرا فقد تتم مثلا عن طريق الوسائل الإلكترونية أو الرقمية من خلال شبكة الإنترنت.

وقد أعطى قانون الإجراءات الجزائية لقاضي التحقيق الحرية في تحديد الأشخاص الذين يرى الفائدة من سماع شهادتهم، سواء كان هؤلاء الأشخاص قد ورد ذكرهم في البلاغ عن الجريمة أو الشكوى منها أو أي شخص آخر وذلك تطبيقا للمواد 88، 97، ق.إ.ج.ج .[1]

الفرع الثالث: ضبط الدليل في مجال الجريمة المعلوماتية

الضبط كقاعدة عامة لا يرد على أشياء مادية فلا صعوبة في ذلك، وبالتالي يضبط الدليل في الجريمة المعلوماتية على المكونات المادية للكمبيوتر، فترفع البصمات مثلا وغيرها، فلا صعوبة في ذلك، وإنما تكمن الصعوبة في ضبط الوسائل الفنية أو المعنوية المستخدمة في إتلاف البرامج

[1] أنظر المواد 88و 97: من الأمر 66_155 الذي يتضمن ق.إ ج. المعدل والمتمم.

خلاصة الفصل:

وفي الأخير وبعد ما تناولا في هذا الفصل إجراءات البحث والتحقيق في الجريمة المعلوماتية، حيث بين الجهاز المكلف بالبحث والتحري عن الجريمة المعلوماتية بالإضافة إلى الإجراءات العامة التي تخضع لها الجريمة المعلوماتية والتي تشترك فيها مع الجريمة التقليدية نوعا ما، حيث قسمناها إلى إجراءات مادية تقتصر فقط على المعاينة التقنية، التفتيش المعلوماتي الذي يخضع تارة لأحكام قانون الإجراءات الجزائية، (المكونات المادية) وتارة إلى قانون 04/09 تارة أخرى (المكونات المعنوية) وأخرى شخصية تتمثل في: الخبرة، وشهادة شاهد إلكتروني، من أجل توضيح إلتزاماتها، وأخرها التسرب وهو من أساليب التحري الخاصة التي جاء بها تعديل قانون الإجراءات الجزائية، والذي قرر هذا الأخير إلا على الجرائم الخطيرة.

وإجراءات الخاصة لا تطبق إلا على الجرائم الموصوفة بالخطيرة والتي من بينها الجرائم المعلوماتية، تتمثل في مراقبة الاتصالات الإلكترونية وحفظ المعطيات المتعلقة بحركة السير والتي جاء بها قانون 04/09 وكذا أسالب التحري الخاصة، وهذا كله أثناء مرحلة التحقيق التمهيدي.

أما أثناء التحقيق الابتدائي أو القضائي فقد عرفت الجريمة المعلوماتية في هذا المجال خصوصية خاصة في مجال كتابة محضر التحقيق وكذا ضمانات المتهم أثناء مرحلة التحقيق.

والشخص المسؤول عن التحقيق هو قاضي التحقيق وصلاحياته في مجال الجريمة المعلوماتية وكذا وجود عدة صعوبات أخرى تتعلق بالمحقق وأخرى بالتحقيق. تختلف الجريمة المعلوماتية عن بعضها البعض في مجال الاختصاص ففي حالة ما إذا ارتكبت الجريمة المعلوماتية بواسطة المكونات المادية للحاسب الآلي فهذه الجريمة تعود اختصاصها إلى المحاكم الجزائية العادية، أما في حالة ارتكاب جريمة على نظام المعالجة الآلية (على المكونات المعنوية) ففي هذه الحالة فإن القطب الجزائي هو المختص في هذه الجريمة نظرا لصعوبة اثباتها، أثناء مرحلة جمع الاستدلالات والتحقيق ونظرا لخطورة الفعل المرتكب، ونقص الخبرات للقضاة في المجال المعلوماتي أمام المحاكم العادية، هذا في مجال مكافحة الجريمة المعلوماتية على المستوى الداخلي (مرحلة المحاكمة).

الفصل الثاني:

التحقيق في الجريمة الإلكترونية من خلال القانون 09_04

الجريمة الإلكترونية يرتكبها جناة ذوي صفات معينة أهمها الدراية الفنية بعمل الحاسب الآلي، وكلها تقدم الجاني في فهم تكتيك العمل في الحسابات الآلية، وكيفية تصميم البرامج كلما استطاع أن يرتكب جريمته دون أن يتم الاهتداء إليه، لأنه لا يترك أي أثار يمكن أن يستدل عليه من خلالها، هذا ما يصعب على المحققين الكشف عن هاته الجرائم وإلقاء القبض على مرتكبيها وللتعرف أكثر على الآليات والإجراءات التي تتخذ للكشف عن هذه الجريمة، جاء القانون رقم 09_04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وسوف نحاول من خلال هذا الفصل استعراض أبرز الهيئات والوحدات المختصة في مجال مكافحة الجرائم المعلوماتية والتي ما تسند إليها عادة مهام الوقاية ومكافحة الجرائم المعلوماتية، لهذا تم التطرق للوحدات المختصة التي تتولى إجراءات البحث والتحقيق في الجرائم الإلكترونية، ولعل أن أبرز آليات المتابعة في الجرائم الإلكترونية في المبحث الأول، إضافة إلى الوحدات المختصة التي تتولى إجراءات البحث والتحقيق في الجريمة الإلكترونية في المبحث الثاني.

المبحث الأول: آليات المتابعة في الجريمة الإلكترونية

لم يشذ المشرع الجزائري عن القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية لكنه أرسى قواعد جديدة ذات طبيعة خاصة كان من اللازم أن تلد مع تطور الحاصل في حقل الجريمة المعلوماتية كظاهرة حديثة وبهذا الصدد جاء القانون رقم 09_04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومنها منصت عليه المادة 3 منه مما تتطلبه مستلزمات التحريات أو التحقيقات القضائية وهي وضع ترتيبات تقنية هدفها ما يلي:

_ مراقبة الاتصالات الإلكترونية.

_ تجميع تلك الاتصالات الإلكترونية.

_ تسجيل الاتصالات الإلكترونية.

_ القيام بإجراءات التفتيش للمنظومة الإلكترونية في حينها. [1]

_ القيام بإجراءات الحجز داخل المنظومة المعلوماتية.

المطلب الأول: مراقبة الاتصالات الإلكترونية

يبدو أن المشرع الجزائري لم يستثن المراسلات العادية كذلك والتي تتم عن طريق وسائل الاتصال السلكية واللاسلكية كما ورد في المادة 65 مكرر 5 من قانون الإجراءات الجزائية إذ نصت على أنه في الجرائم المعلوماتية يجوز لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

وإذا كانت هذه الأخيرة متعارف عليها ومقصود منها جميع المراسلات أو الرسائل والبرقيات والمحادثات السلكية واللاسلكية والمحادثات السلكية واللاسلكية المرسلة عن طريق البريد فإن فقهاء القانون يعتبرونها محمية قانونا ضد كل اطلاع عليها كونها تتعلق بحقين:

[1] زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري الدولي، دار الهدى، عين مليلة الجزائر، 2011، ص 120.

الحق في الملكية والذي يتمتع به المرسل إليه منذ وقت تسليمه للرسالة والحق في الحياة الخاصة بما تتضمنه من أسرار تتعلق بالحياة الخاصة للمرسل أو المرسل إليه.

وقد اهتم المشرع الجزائري من جهة أخرى بمبدأ الحق في حماية المراسلات في ظل أحكام القانون رقم 03/2000 المؤرخ في 2000/08/05 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية حين أشار في المادة 105 منه فقرة أخيرة إلى ما يلي لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات.

وفيما يتعلق بالبريد الإلكتروني فانه يتضمن برامج متخصصة للكتابة والتراسل ولتخزين الرسائل الإلكترونية وتختلف هذه البرامج حسب نوعيتها.

نص القانون رقم 09_04 المؤرخ في 2009/08/05 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 04 منه ما يلي:

أ/ للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.[1]

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

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

د/ في إطار تنفيذ طلبات المساعدة القضائية.

_ الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

[1] المادة 4 من القانون 09_04 الدي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

مكن المشرع الجزائري ضابط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة. [2]

والتقاط الصور يكون بالتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص، ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة.

أما تسجيل الأصوات فيتم عن طريق رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية.

إن ما يهم هو ان مثل هذه الإجراءات يمكن له المساس بالحرية الشخصية، خصوصا إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون رقم 04/09 المؤرخ في أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكافحتها. أنه: "مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني، ويكون الثاني برضا المعني أو بطلب من صاحب الشأن، ويخضع لتقدير الهيئة القضائية بعد تسخير المصالح البريد والمواصلات.

[2] خلفي عبد الرحمان ، محاضرات في القانون الإجراءات الجزائية، دار الهدى، عين مليلة، الجزائر، 2010، ص 72_73.

ويعد هذا الإجراء الحديث من أهم إجراءات التحقيق، مكن المشرع ضابط الشرطة القضائية ممارسته للكشف عن الجرائم التي حددها على سبيل الحصر في المادة 65 مكرر 5 بموجب قانون الإجراءات الجزائية، تباشره الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع في القريب العاجل، بمعنى أنها إجراءات للتحري والتحقيق.

_ المشرع على الرغم من إقراره أساليب تحري خاصة قد تمس بحرمة الحياة الخاصة إلا أنه يعاقب على اللجوء لاستعمالها بطرق غير مشروعة،[1] وهو ما سنشير إليه على النحو التالي:

وهي مباشرة التحري بإذن من وكيل الجمهورية:

لم يسمح المشرع بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، [2]إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته، وهذا ما قررته المادة 04 من القانون 04/09 التي جاء فيها: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن من السلطة القضائية."

المطلب الثاني: القواعد الإجرائية

1_ تفتيش المنظومات المعلوماتية:

وهي التي أوردها القانون رقم 09_04 والمشار له في المادة 5 منه ما يلي:

[1] المادة (303 مكرر) من الأمر رقم 156/66 معدلة ومتممة بموجب المادة (33) من القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006.

[2] خلفي عبد الرحمان، مرجع سابق، ص 76.

يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 الدخول بغرض التفتيش ولو عن بعد إلى:

أ _ منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب _ منظومة التخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة 1 من هذه المادة، إذا كانت هناك أسباب تدعو إلى الاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وان هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا لذلك.

إذا تبين مسبقا بان المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل.[1]

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية التي تتضمن قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها:

نص القانون رقم 09_04 في المادة 5 منه انه لا يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى:

أ _ منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب _ منظومة معلوماتي.

[1] زيدان زيبحة، مرجع سابق، ص 135.

يلاحظ إذن التفتيش في الوضعيات المشار لها يأخذ منحنيين فهو إما أن يكون عملا من أعمال التحقيق تقوم به السلطات القضائية المختصة، وإما يكون من أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطة المختصة، وفي كلتا الحالتين فان المستهدف هنا هو جهاز الكمبيوتر بمكوناته المادية والمعنوية، فالحاسوب كما هو معروف يتكون من مكونات مادية وهي مجموعة وحدات لكل منها وظيفة معينة، وهي متصلة ببعضها البعض في شكل نظام متكامل منها وحدات الإدخال، ومهمتها استقبال البيانات المعلوماتية والغير المعالجة وأيضا لها داخل جهاز الكمبيوتر لكي تمرر إلى وحدة الذاكرة للمعالجة أو التخزين، و وحدة الذاكرة هي التي تقوم بتخزين البرامج والمعلومات وبما يحتويه من ذاكرة رئيسية وعشوائية وذاكرة القراءة ثم وحدة الحساب والمنطق، وتتكون من مجموعة دوائر حسابية ومنطقية وسجلات لتنفيذ العمليات، وتنقسم إلى وحدة المعالجة المركزية و وحدة الذاكرة ثم وحدة التحكم و وحدة الذاكرة المساعدة، و وحدة الإخراج والمحتوى على أجهزة الشاشة والطابعة ومشغلات الأقراص وهي التي تستغل المعلومات المعالجة وتمريرها وإخراجها للمستخدم، أما المكونات المعنوية للجهاز الكمبيوتر والتي تسما أيضا بالكيانات المنطقية وهي مجموعة البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات. [1]

الشروط الشكلية للتفتيش:

يستخلص من نص المادة 5 من القانون 09_04 إن التفتيش في مجال الجرائم المعلوماتية يدرجه المشرع الجزائري في إطار قانون الإجراءات الجزائية.

إن طبيعة الاختلاف بخصوص موضوع التفتيش في مجال المعلوماتية والذي يختلف كلية عن التفتيش العادي يتوقف أساسا على طبيعة المكان الذي يحتوي أجهزة الكومبيوتر ومكوناته وفيما إذا كان خاصا أما عاما هذا فضلا عن تحديد الإقليم فيما إذا كان وطنيا أم أجنبيا فعندما

[1] زيدان زيبحة، مرجع سابق، ص .136

تصرح المادة 5 بالقول بأنه: يجوز للسلطة المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش لو عن بعد.

إن التفتيش يكون في الأصل بصفة مباشرة بالانتقال إلى مسكن المتهم أو المكان الذي تتواجد فيه الأجهزة المقصودة أو في الأماكن العامة حال حيازة شخص لجهاز الحاسوب الآلي أو احد مكوناته المادية كوسائط التخزين مثل الأقراص المرنة والأقراص الصلبة والأقراص المضغوطة والأشرطة الممغنطة فواضح بان القانون أحال هذه الإجراءات على القواعد العامة في قانون الإجراءات الجزائية.

وفقا لأحكام المادة 44 من قانون الإجراءات الجزائية لاسيما بعد التعديل الذي حصل بموجب القانون 06_22 في 2006/09/20 وهي:

1 _ وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.[1]

2 _ الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.

3 _ أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.

4 _ حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.

5 _ في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين لسلطته.

أما التفتيش في الأماكن العامة وهي التي يرتديها العامة في كل وقت ولا تتمتع بحرمة المنزل ومن الضروري التمييز بين نوعين من الأماكن العامة (الأماكن العامة بطبيعتها والأماكن العامة بالتخصيص).

[1] المادة 44 من القانون رقم 17_07 مؤرخ في 27 مارس 2017، المتضمن قانون الإجراءات الجزائية، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 20، الصادر يوم 29 مارس 2017.

فالأولى لها صفة العامة على وجه دائم مثل الشوارع والحدائق العامة أما الثانية فيرتاده الجمهور في أوقات محددة كالمقاهي والمطاعم، ويمكن دخولها خلاف للاماكن الخاصة وتفتيشها إذا تم غلقها لانتهاء فترة العمل وانصراف العامة فهذه الحالة تأخذ طابع الخصوصية كذلك الشأن فيما يحتويه من مكاتب أو غرف خاصة لصاحبها.

تفتيش المنظومة المعلوماتية عن بعد:

أجاز القانون الجزائري رقم 09_04 القيام بتفتيش المنظومة المعلوماتية عن بعد ويقتضي ذلك الدخول إليها دون إذن صاحبها والولوج إلى الكيان المنطقي للحاسوب فالتفتيش هنا يستهدف أشياء معنوية وفنية وليست مادية كالبرامج وقواعد البيانات ولان هذه قد تكون وسيلة لارتكاب جريمة أو تخزين معلومة بشأنها سيما إذا كانت هذه المعلومات غير مرتبطة بعد بأية دعامة مادية وان كان المشرع الجزائري قد أجاز إفراغ أو نسخ تلك المعلومات المشكوك فيها أو التي من شانها الإفادة في الكشف عن الجريمة أو مرتكبيها نسخها على دعامة تخزين الكترونية تكون قابلة للحجز.[1]

_ دواعي المراقبة الالكترونية وتفتيش المنظمة المعلوماتية:

1 _ وقوع الجريمة سواء كانت جناية أو جنحة وهذا ما يستخلص من أحكام المادة من القانون الإجراءات الجزائية.

2 _ توجيه الاتهام لشخص أو لمجموعة أشخاص ممن يظهر أنهم ساهموا في الجريمة كما أشير إليه في المادة 44، وخلافا لذلك كله فان التشريع الجزائري خرج عن القواعد العامة بخصوص الجريمة الإلكترونية وجعل من التفتيش المنصب على المنظومة المعلوماتية إجراء وقائي في مواجهة ما يقدم عليه المجرم المعلوماتي واستعمال الرقابة التقنية لوسائل الاتصالات الالكترونية قد تكون مسبقة لارتكاب أي جرم ودون توجيه الاتهام لأي شخص وقد وضحت ذلك

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة لنيل الماجستير، كلية الحقوق جامعة الجزائر، 2012، ص 132.

المادة 5 من القانون رقم 09_04 حين أشارت بالقول بان التفتيش المنظومة المعلوماتية جائز في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 5 من نفس القانون.

2 _ حجز المعطيات المعلوماتية:

تنص المادة 6 من القانون رقم 09_04 على أنه: عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وانه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.[2]

المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة،

كما ألزمت المادة 10 من نفس القانون مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش وحفظ المعلومات طبقا للمادة 11 التي من شأنها تمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

وقد حدد هذا القانون المادة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما اوجب في مادته 12 على مقدمي الخدمات التزامات خاصة هي:

_ واجب التدخل الفوري لحسب المعطيات المخلفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.

_ وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وان يخبروا المشتركين ليهم بوجودها.

[2] زيدان زيبحة، مرجع سابق، ص 138.

3 _ حفظ المعطيات المتعلقة بحركة السير:

تنص المادة 11 على ما يلي: مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ:[1]

أ _ المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ب _ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج _ الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

د _ المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.[2]

هـ _ المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها، أما بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة _ ا _ من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

المبحث الثاني: الوحدات المختصة التي تتولى إجراءات البحث والتحقيق في الجريمة الإلكترونية.

سنحاول من خلال هذا المبحث اعتراض ابرز الهيئات والوحدات المتخصصة في مجال مكافحة الجرائم المعلوماتية، والتي ما تسند إليها عدة مهام الوقاية ومكافحة الجرائم المعلوماتية، نظرا لتشكيلتها البشرية الخاصة والتي تضم محققين من نوع خاص تجتمع لديهم صفة ضابط شرطة قضائية إضافة إلى المعرفة الواسعة بمجال النظم المعلوماتية والإجرام المعلوماتي، مما يسمح لهم ويؤهلهم لتولي مهام البحث والتحقيق في ميدان الجرائم المعلوماتية، سواء تمثلت في

[1] المادة 11من القانون 09_04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016، ص 171.

شخص وكيل الجمهورية أو قاضي التحقيق نظرا لقلة خبرتهم بميدان النظم المعلوماتية وعلى تحكمهم في تقنيات البحث والتحقيق بواسطة وسائل معلوماتية خاصة تتطلب المعرفة والدقة في مجال استخدامها، ولعل أن أبرز هذه الهيئات والوحدات هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إضافة إلى تلك الأجهزة الأمنية سواء التابعة لسلك الأمن الوطني أو التابعة لقيادة الدرك الوطني.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

إن إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها يعود إلى 2009/08/05، بحيث جاء في نص المادة 13 من القانون على انه تنشا الهيئة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته حيث صدر بعد ذلك المرسوم الرئاسي رقم 15_268 المؤرخ في: 2015/10/08، والذي تضمن في فصوله تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[1]

أولا: تعريف الهيئة.

الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل، مقرها بالجزائر العاصمة، تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم: 09_04 المؤرخ في شعبان عام 1430 الموافق ل: 5 غشت 2009، تحت رقابة السلطة القضائية، طبقا لأحكام التشريع الساري المفعول، لا سيما منها قانون الإجراءات الجزائية والقانون رقم: 09_04.

[1] ربيعي حسين، مرجع سابق، ص 171.

ثانيا: اختصاصات الهيئة.

بينت الفقرة الثانية من المادة 4 من المرسوم الرئاسي 15_261 المهام الأساسية التي تكلف بها الهيئة وهي الوقاية من الجرائم المعلوماتية، ومكافحتها من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية، ومن بين ابرز مهام الهيئة نجد: [1]

1 _ اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

2 _ تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

3 _ مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.

4 _ ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة وذلك تحت سلطة قاضي مختص.

5 _ تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مسارها من اجل استعمالها في الإجراءات القضائية.

6 _ المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا المعلومات.

7 _ تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية.

8 _ تنفيذ الطلبات الصادرة عن الدول الأجنبية وتطوير سبل التعاون والتبادل معها.

---

[1] المرسوم الرئاسي رقم 15_261، المؤرخ في: 08 أكتوبر 2015، المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم: 53 المصدر يوم 08 أكتوبر 2015.

9 _ المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

ثالثا: تشكيلة الهيئة وتنظيمها.

1/ اللجنة المديرة:

يرأس اللجنة الوزير المكلف بالعدل تتشكل من الأعضاء التالية: الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، قائد الدرك الوطني، مدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا.

تمارس اللجنة المديرة وتكلف بالقيام بالمهام التالية:

_ توجيه عمل الهيئة والإشراف عليه ومراقبته.[1]

_ دراسة كل مسالة تخضع لمجال اختصاص الهيئة لا سيما فيما يتعلق بتوفر اللجوء للمراقبة الوقائية للاتصالات الالكترونية.

_ ضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه.

_ قيام اللجنة بشكل دوري بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة.

_ تتولى عملية اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[1]

_ دراسة مشروع النظام الداخلي للهيئة وميزانيتها والموافقة عليه.

_ دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه وإبداء الرأي في كل مسألة تتصل بمهام الهيئة.

---

[1] ربيعي حسين، مرجع سابق، ص .173.

[1] ربيعي حسين، مرجع سبق ذكره، ص .173.

_ تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة.

2/ المديرية العامة:

يتولى إدارتها مدير عام يعين بموجب مرسوم رئاسي وتنهى مهامه بنفس الطريقة حيث يمتلك المدير العام العديد من الصلاحيات حتى يتمكن من القيام بمهامه على أكمل وجه تتمثل أهمها في:

_ العمل على حسن سير الهيئة الوطنية عن طريق ضمان تنفيذ برنامج عملها.

_ تنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها.

_ تحضير اجتماعات اللجنة المديرة.

_ تمثيل لدى السلطات والمؤسسات الوطنية والدولية ولدى القضاء وفي جميع أعمال الحياة المدنية.

_ ممارسة السلطة السليمة على مستخدمي الهيئة والعمل على احترام قواعد حماية السر في الهيئة والقيام بإجراءات التأهيل وأداء اليمين.

_ إعداد تقرير سنوي لنشاطات الهيئة وعرضه على اللجنة المديرة للمصادقة عليه.

_ العمل على ضمان التسيير الإرادي والمالي للهيئة.

3/ مديرية المراقبة الوقائية واليقظة الإلكترونية:

لم ينشر الأمر الرئاسي 15_261 إلى تشكيلة هذه المديرية، غير انه ومن خلال تحليل نص المادة 18 منه يمكن لنا تحديد تشكيلتها في مجموعة من ضباط وأعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، من سلك الأمن الوطني وكذلك الدرك الوطني والمصالح العسكرية للاستعلام والأمن، يعينون بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل والدفاع والداخلية، يساعدهم مستخدمي الدعم التقني والإداري من نفس الأسلاك.

تعمل هذه المديرية على انجاز المهام التالية:

أ _ تنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية والقيام بإجراءات التفتيش والحجز داخل الأنظمة المعلوماتية إذا ما تعلق الأمر بجرائم الإرهاب أو الجرائم التخريب أو الجرائم الماسة بأمن الدولة بناء على رخصة مكتوبة من السلطة القضائية وتحت رقابة القاضي المختص.

ب _ إرسال المعلومات المحصل عليها إلى السلطات القضائية ومصالح الشرطة القضائية.[1]

ج _ تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات التي تسمح بتحديد مكان تواجد مرتكبي الجرائم المعلوماتية والتعرف عليهم.

د _ جمع ومركزة كل المعلومات واستغلالها من اجل الكشف عن الجرائم المعلوماتية.

هـ _ المشاركة في حملات التوعية حول مخاطر تكنولوجيا الإعلام والاتصال.

و _ تزويد السلطات القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المعلوماتية.

إذن وبالنظر إلى تشكيلة والمهام الملحقة بهذه المديرية فانه يمكن وصفها بأنها المركز العملياتي للهيئة بما أنها تتولى الجانب التقني الخاص بإنجاز الأعمال المتعلقة بالبحث والتحقيق في الجرائم المعلوماتية، ولعل أن ما يزيد من دورها الفعال هو تنصيبها على رأس مركز العمليات التقنية وكذلك الملحقات مما يبرز دورها الفعال في تسيير وتأطير الأعمال المتعلقة بالوقاية أو بمكافحة الجرائم المعلوماتية.[1]

4/ مديرية التنسيق التقني:

[1] المادة 18 من المرسوم الرئاسي 15_261، المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[1] ربيعي حسين، مرجع سابق، ص .175

لم ينص المرسوم الرئاسي رقم 15_261 على تشكيلة مديرية التنسيق التقني مما يترك المجال للقول بان تشكيلتها تكون بناء على قرارات مشتركة بين وزراء العدل والدفاع والداخلية على شكل مديرية المراقبة الوقائية واليقظة الإلكترونية، غير أنها تختلف عنه من حيث المهام الموكلة إليها، فتتمثل مهامها أكثر في الدور الوقائي والإعلامي من خلال توليها:

أ _ انجاز الخبرات القضائية في مجال اختصاص الهيئة.

ب _ تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي.

ج _ إعداد الإحصائيات الوطنية للإجرام المعلوماتي.

د _ تسيير المنظومة المعلوماتية وإدارتها.

5/ مركز العمليات التقني:

يتم تزويده بالمنشآت والتجهيزات والوسائل المادية وبالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الإلكترونية يتبع المركز مديرية المراقبة الوقائية واليقظة الإلكترونية حيث يتم تشغيله من طرفها.

6/ الملحقات الجهوية :

يتم تشغيلها من طرف مديرية المراقبة الوقائية واليقظة الإلكترونية التي تكون تابعة لها.

لقد اقتنع المشرع الجزائري بضرورة تفعيل دور الهيئة في مجال الوقاية ومكافحتها الجرائم الإلكترونية ولو بشكل متأخر، نظرا لتوسع تطبيقات تقنية المعلوماتية في المجتمع الجزائري على الصعيدين الحكومي والاجتماعي، وهو ما ينبئ بتنامي الإجرام المعلوماتي وازدياد حجم التهديدات التي يشكلها على سلامة الأنظمة المعلوماتية وامن المعطيات المخزنة والمتداولة عبرها.[1]

رابعا: سير الهيئة.

[1] ربيعي حسين، مرجع سابق، ص .177

تجتمع الهيئة بناءا على استدعاء من رئيسها أو بناءا على طلب احد أعضائها إذ تقوم بإعداد نظامها الداخلي والمصادقة عليه حيث يتم تزويدها بقضاة وضباط وأعوان الشرطة القضائية من المصالح العسكرية للاستعمال والأمن والدرك الوطني يتم تحديد عددهم بموجب قرارات مشتركة بين وزير العدل والدفاع والداخلية كما تزود بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح العسكرية للاستعمال والأمن والدرك الوطني كما يمكن لها الاستعانة بأي خبير أو أي شخص يمكن تعيينه في أعمالها شرط التزامهم بالسر المهني وواجب التحفظ وخضوعهم لإجراءات التأهيل.

المطلب الثاني: الأجهزة الأمنية.

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام.[1]

اولا: الوحدات التابعة لسلك الأمن الوطني.

تضع مدرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجرائم المعلوماتية، والتي تعتبر نتاج التطور الحاصل على المستوى الدولي والوطني في مجال التكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات.

[1] محمد سعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحث والدراسات، العدد الثاني، ديسمبر 2017، المركز الجامعي إليزي، الجزائر، ص 34_35.

توجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي كالآتي:

_ المخبر المركزي للشرطة العلمية بالجزائر العاصمة.

_ المخبر الجهوي للشرطة العلمية بقسنطينة.

_ المخبر الجهوي للشرطة العلمية بوهران.

في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط الشرق، الغرب، الجنوب، لتقوم فيما بعد بتعميم الخلايا على جميع مصالح الأمن ولايات الوطن.[1]

1- على المستوى المركزي

بادرت المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية بغية خلق وحدات تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها، ولذلك قامت المديرية العامة للشرطة القضائية بإستحداث مصلحة مختصة في مكافحة الجريمة المعلوماتية سمية بنيابة مديرية مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالإضافة إلى نيابة مديرية الشرطة العلمية والتقنية، هذه الأخيرة التي تضع لخدمة هذا الهدف مصالح عملية مختصة بذلك، تتولى أعمال البحث والتحري والتحقيق بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذه الوحدة هي المخبر المركزي للشرطة العلمية والكائن مقرة بالجزائر العاصمة.

يتولى كل مخبر المركزي، مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها، ولأجل ذلك يضم المخبر دائرة تقنية وتتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة

[1] سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52، ديسمبر 2019، ص 53.

عن الجرائم التي تستعمل فيها الأسلحة والقذائف بمختلف أنواع، وكذلك جرائم التزوير، إضافة إلى الجرائم المعلوماتية، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى.[2]

2- على المستوى الجهوي

قامت بإنشاء مخابر جهوية للشرطة العلمية في كل من ولايتي قسنطينة ووهران، على كل مستوى كل مخبر مصلحة تسمى دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية، تتولى هذه المصلحة أعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية، وذلك تحت تسمية دائرة الأدلة الرقمية والأثار التكنولوجية والتي لم تكن عند استحداثها سنة 2004 سوى قسم، غير أن الإرتفاع الملحوظ لعدد الناتجة عن الجرائم المعلوماتية، بسبب الإنتشار المتزايد لتقنية المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية هي:

1 _ قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.

2 _ قسم إستغلال الأدلة الناتجة عن الهواتف النقالة.

3 _ قسم تحليل الأصوات.

تضم الدائرة في صفوفها ثمانية 08 أعضاء محققين أربعة 04 منهم عناصر شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية، والبقية هم أعوان شبيهون، يحمل كل منهم شهادة جامعية في تخصص الإعلام والاتصال، إضافة إلى إلمامهم بالجانب القانوني، ومما يزيد في فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث والتحقيق في الجرائم المعلوماتية

[2] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، في العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح، ورقلة، تاريخ المناقشة 2019/07/02، ص 38.

هو خضوعهم بصفة دورية لدورات تكوينية لأجل الإطلاع على كل المستجدات القانونية منها والتقنية في مجال الإجرام المعلومات.[1]

ومن مهام هذه المخابر ضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية في مجال تحريات الإلكترونية، وذلك من خلال القيام بعمليات البحث عن المعطيات المشبوهة والمعلومات الرقمية على مختلف أشكالها: ملفات، رسائل إلكترونية، برامج، صور،... هذا البحث يتم عن طريق استعمال برامج ووسائل خاصة تمكن من استرجاع كل المعطيات المحذوفة، والإطلاع على محتوى كل الوسائط الرقمية.[2]

تلعب الدائرة دورا مهما للغاية في الكشف عن أسرار الجرائم المعلوماتية، من خلال مختلف الإجراءات التي تباشرها إما أثناء مرحلة البحث والإستدلال، أو أثناء مرحلة التحقيق القضائي.

فأما أثناء مرحلة البحث والتحري فإن أعضاء الدائرة عادة ما يستجيبون للطلبات التي يقدمها لهم عناصر الشرطة التابعون لفرق مكافحة الجرائم المعلوماتيةالموزعة على كل المديريات الأمن الوطني، أو طلبات وكيل الجمهورية أو قاضي التحقيق التي تردهم في شكل إنابة قضائية، من أجل دعمهم ومساعدتهم أثناء مرحلة المعاينة لمسرح الجريمة وكذلك لحجز الأدلة المتواجدة عليها.

أما أثناء مرحلة التحقيق القضائي فإن دور الدائرة لا يتعدى لأن يكون دور خبير، وذلك من خلال إعادة تقارير خبرة بناء على طلبات وكيل الجمهورية وبالخصوص قاضي التحقيق، كنتيجة لقيام المحققين بأعمال تحليل الأدلة المحجوزة والعمل على إستخراج الأدلة الإلكترونية منها، كتحليل محتوى الأقراص الصلبة للحاسوب المستعملة في الجريمة، أو حواسيب الضحايا، وكذلك كل دعامات التخزين الإلكتروني بمختلف أنواعها وأشكالها، وكذلك المواقع التي تم

[1] حسين ربيعي، مرجع سابق، ص 180.

[2] عمار حشمان، مرجع سابق، ص 39.

اختراقها وإستهدافها وصولا إلى تحديد الموقع الجغرافي وعناوين المجرمين، وذلك بالإستعانة بوسائل مادية خاصة متطورة ذات جودة عالية.[1]

3- على المستوى المحلي

في سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية، انشأت المديرية العامة للأمن الوطني سنة 2016 ما يقارب 48 فرقة لمكافحة الجرائم المعلوماتيةعلى مستوى مصالحها بأمن والولايات، يتمثل دورها في تلقي الشكوى والبحث والتحقيق في الجرائم المعلوماتية وتقريب الإدارة من المواطن.

ثانيا: الوحدات التابعة لدرك الوطني

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن الوطني والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية نذكر منها:

_ المصالح والمراكز العلمية والتقنية.

_ هياكل التكوين.

_ المصلحة المركزية للتحريات الجنائية.

_ المعهد الوطني لعلم الإجرام.

يوجد يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام التابع لقيادة العلمية للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وإنجاز المقاربة الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصور وذلك لتسهيل استغلالها بالإضافة إلى

[1] حسين ربيعي ، مرجع سابق، ص 181.

مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني.

الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى انواع الجرائم بما فيها الجريمة المعلوماتية حيث يوجد بهذا المركز قسم الإعلام الآلي والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.[1]

فقد تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف وذلك حسب الإختصاص والصلاحيات وطبيعة الجريمة إلى ثلاث 03 مسويات مركزية، جهوية، محلية.

1- على المستوى المركزي

تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم المعلوماتية ودعم أعمال البحث والتحقيق بشأنها من خلال الهيئات التالية:

أ _ مديرية الأمن العمومية والإستغلال:

وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العملي، في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

ب _ المصلحة المركزية للتحريات الجنائية:

وهي هيئة ذات إختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيات الإعلام والاتصال.[2]

ج _ المعهد الوطني للأدلة الجنائية وعلم الإجرام:

[1] سعيد بوزنون، مرجع سابق، ص 53_54.

[2] عمار حشمان، مرجع سابق، ص 42.

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاءه بمرسوم رئاسي رقم 183_04 بتاريخ: 26 جوان 2004، في إطار عصرنة قطاع الدرك الوطني، وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، يعد المعهد بمثابة هيئة مختصة في إجراء الخبرات والمعاينة وذلك بمختلف دوائره، الإعلام الآلي والإلكترونيك، التي أوكلت لها مهام تحليل الأدلة الخاصة بالجرائم المعلوماتية، وإن الخدمة الأساسية التي يقدمها هذا المعهد في هذا الشأن:

_ القيام بالخبرات العلمية أو اللازمة في توجيه التحقيقات القضائية بطلب من القضاة بما فيها تلك المتعلقة بالجرائم المعلوماتية.

_ مساعدة المحققين للسير الحسن للمعاينات، عن طريق دعمهم الأفراد المؤهلين أثناء الحاجة.

_ تنفيذ مناهج الشرطة العلمية والتقنية لجمع وتحليل الأدلة المأخوذة من مسرح الجريمة.

_ ضمان المساعدة العلمية في التحريات المعقدة كحال التحريات الخاصة بالجرائم المعلوماتية.

_ المشاركة في الأبحاث والتحاليل المتعلقة بالوقاية للتقليل من جميع أشكال الإجرام بما فيها المعلوماتي.

تعتبر مشاركة ومساهمة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المكلفة بالتحليل والخبرات في ميدان علم الإجرام في وضع سياسة مكافحة الإجرام.[1]

د _ مركز الوقاية من الجرائم الإعلام الآلي والجرائم المعلوماتية:

أنشأ هذا المركز حديثا ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية، [2] إذ يوفر المساعدة التقنية للمحققين ويساهم في توجيه

[1] عمار حشمان، مرجع سابق، ص 43.

[2] بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16 و 17 نوفمبر 2015، كلية الحقوق جامعة بسكرة، ص 29.

التحقيقات المرتبطة بالتكنولوجيا الإعلام والاتصال، فهو هيئة تقنية تعمل تحت وصاية مديرية المن العمومي والإستغلال لقيادة الدرك الوطني ويحقق المهام التالية:

_ ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت.

_ القيام بمراقبة الإتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.

_ مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال والبحث عن الأدلة في شبكة الأنترنت.

_ المشاركة في العمليات التحري والتسرب عبر شبكة الأنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.

_ المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

إذن تعتبر هذه الهيئات التابعة لدرك الوطني مسؤولة عن تنفيذ إجراءات البحث والتحقيق بشأن الجرائم المعلوماتية، وذلك على نطاق وطني بحيث تعتبر هيئات دعم وإسناد ونقاط وصل بين مختلف الوحدات الأخرى المتخصصة والتي توجد كذلك على مستويات أدنى منها الجهوية والمحلية.

2- على المستوى الجهوي

تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بمهمة تنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية وكذلك دعمها بالوسائل الخاصة للتحريات والأبحاث المعقدة كالجرائم المعلوماتية.

يلعب الدرك الوطني دورا هاما في ميدان الشرطة القضائية نظرا لانتشار وحداته على مستوى كامل التراب الوطني، ونظرا للوسائل المادية الموضوعية تحت تصرفه وعدد أفراده

الهائل، والصلاحيات التي خولها لهم القانون، وهم في الواقع حسب الرتب والوظائف ضباط وأعوان الرطة القضائية.

3- على المستوى المحلي

يحوز الدرك الوطني على فصائل للأبحاث التي ينتمي إليها أفراد ذوو خبرة وإختصاص واسعين في ميدان الشرطة القضائية، هذه الفصائل مكلفة خصوصا بمكافحة الأشكال الخطيرة للإجرام المنظم كالجرائم المعلوماتية، وذلك عن طريق القيام بتحقيقات تتطلب تحريات معقدة، هذه الوحدات المختصة تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني، وهو ما سمح بإنشاء خلية متخصصة لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال في كل مجموعة ولائية، وهو ما يسمح بتطبيق سياسة فعالة في مكافحة الجرائم المعلوماتية من خلال توفير الخلايا المتخصصة في مجال أعمال البحث والتحقيق في هذا النوع من الجرائم.[1]

خلاصة الفصل:

مما سبق تم التطرق في هذا الفصل إلى القانون رقم 09_04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وإلى آليات المتابعة في الجرائم الإلكترونية متمثلة في مراقبة الاتصالات الإلكترونية وتسجيل الاتصالات الإلكترونية والقواعد الإجرائية، ثم بعد ذلك تم التطرق إلى الوحدات المختصة التي تتولى إجراءات البحث والتحقيق في الجريمة الإلكترونية والتي تتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والأجهزة الأمنية سواء الأمن الوطني أو الدرك الوطني سواء على المستوى الوطني أو الجهوي أو المحلي، التي تمكن المحقق من التعرف على الجاني وتوقيفه وتقديمه أمام النيابة العامة لأخذ جزاءه.

[1] عمار حشمان، مرجع سابق الذكر، ص 45.

الخاتمة

إن الجريمة الإلكترونية ظاهرة عالمية اتضحت موازاة مع التطور الهائل الذي عرفه المجال التكنولوجي حيث أصبحت ترتكب في بيئة رقمية تقنية، فقد حاولت مختلف التشريعات درء هذه الجرائم من خلال استحداث نصوص تشريعية وقوانين خاصة، والتي أقرت بإجراءات واليات التحقيق الجنائي في الجرائم المعلوماتية، والتي تتبعها السلطات والهيئات المخولة للمتابعة والتحري وضبط المجرمين المعلوماتيين، والجزائر على غرار الدول العالم تهددها الجرائم الإلكترونية فحاولت التصدي لها والقضاء عليها من خلال قانون العقوبات رقم 04_15 (المعدل والمتمم) تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وكذلك قانون الإجراءات الجزائية، وهذا لم يحقق ما كان مرجوا، مما أدى بالمشرع إلى استحداث قانون خاص بهذه الجرائم وهو قانون 09_04 المؤرخ في 2009/08/05 والذي يحدد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فقد اقر على مجموعة من الإجراءات كمراقبة الاتصالات الإلكترونية وتفتيش وحفظ المعطيات وحجزها، وكذلك بين التزامات مقدمي الخدمات بمساعدة السلطات المكلفة بالتحقيق، وأكد أيضا على وجود الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالإضافة إلى مختلف الهيئات الأخرى كجهازي الأمن الوطني والدرك الوطني.

ومن خلال ما سبق نستخلص النتائج التي توصلنا إليها:

1 _ صعوبة التحقيق الجنائي في الجرائم الإلكترونية كون الدليل الإلكتروني سهل المحو والتخلص منه من طرف مجرمي المعلوماتية.

2 _ ضعف المنظومة القانونية التي تعالج الجرائم الإلكترونية، والدليل على ذلك التعديل المستمر للقوانين.

3 _ نقص التكوين والتأطير للمحققين.

ومن بين الاقتراحات التي تم استخلاصها نستنتج الآتي:

1 _ استحداث قوانين جديدة أكثر مواكبة للتطور المستمر للتكنولوجيات الحديثة، وسد الفراغات القانونية التي ترتكتها القوانين السابقة.

2 _ فرض رقابة أكثر على الإنترنت (وسائل الاتصال الاجتماعية خصوصا).

3 _ حجب بعض المواقع الإلكترونية، خاصة الخطيرة منها كالإرشاد بالأعمال الإرهابية والتي تدعو إلى الانخراط في منظمات إرهابية.

4 _ التنظيم الدوري والمستمر للأيام الإعلامية والملتقيات والندوات لتنوير الرأي العام بالمخاطر الكبيرة والخطيرة التي تخلفها الجرائم الإلكترونية على الفرد والمجتمع والدولة.

5 _ الدعوة والحث على الاستعمال الحسن لشبكة الإنترنت.

6 _ التكوين الدوري والمستمر للمحققين في مجال مكافحة الجرائم الإلكترونية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: المصادر:

القوانين:

أ- النصوص التشريعية :

1 _ القانون رقم 09 _04 المؤرخ في 5 أوت 2009، الذي يحدد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادر بتاريخ 05 أوت 2009.

ب- النصوص التنظيمية:

2 _ المرسوم الرئاسي رقم: 15_261 المؤرخ في 08 أكتوبر 2015، المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 53 الصادر يوم 08 أكتوبر 2015.

ثانيا: المراجع:

أ / الكتب:

1 _ أحسن بوسقيعة، التحقيق القضائي، دار هومة للطباعة والنشر والتوزيع، الجزائر، .2006

2 _ خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، .2010

3 _ زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011.

4 _ عبد جميل غصوب، الوجيز في قانون الإجراءات الجزائية، ط 1، المؤسسة الجامعية للنشر والتوزيع، بيروت، .2011

5 _ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، ط 1، دار الجامعة الجديدة للطباعة والنشر، بيروت، 1999.

ب / المذكرات والأطروحات:

1 _ حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتي، مذكرة لنيل الماستر، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، .2016

2 _ عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل الماستر، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرياح، ورقلة، 2019.

3 _ نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة لنيل الماستر، كلية الحقوق، جامعة الجزائر، .2012

4 _ نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية، مذكرة لنيل الماستر، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، .2013

5 _ يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل الماستر في القانون، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

ج / المقالات:

1 _ سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، العدد 52، الجزائر، ديسمبر .2019

2 _ علي عثماني، خالدة بن بعلاش، الأحكام الموضوعية والإجرائية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة أبحاث قانونية وسياسية، المجلد 6، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل، .2018

3 _ مختار تابري، السلطة القائمة على التحقيق في الجريمة الإلكترونية، مجلة القانون العام الجزائري والمقارن، المجلد 8، العدد 1، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، 2022.

4 _ وردة شرف الدين، سامية بلجرف، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية، المجلد 1، العدد 3، كلية الحقوق والعلوم السياسية، جامعة يحي فارس بالمدية، 2017.

د / المحاضرات:

1 _ عبد الرحمان خلفي، محاضرات في القانون الإجراءات الجزائية، دار الهدى، عين مليلة، الجزائر، .2010

2 _ بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16،17 نوقمبر 2015، كلية الحقوق، جامعة بسكرة.

فهرس
المحتويات

مقدمة:	01
الفصل الأول: إجراءات التحقيق في الجريمة الإلكترونية.	05
المبحث الأول: دور جهاز الضبطية القضائية في مجابهة الجريمة الإلكترونية.	07
المطلب الأول: إجراءات التفتيش للضبطية القضائية في الجرائم الإلكترونية.	07
المطلب الثاني: إجراءات التسرب للضبطية القضائية لمواجهة الجرائم الإلكترونية.	12
المبحث الثاني: الإجراءات التي يباشرها قاضي التحقيق في الجرائم الإلكترونية.	17
المطلب الأول: إجراءات المعاينة في الجريمة الإلكترونية.	17
المطلب الثاني: إجراءات التفتيش والإستجواب وضبط الأدلة في الجريمة الإلكترونية.	21
الفصل الثاني: التحقيق في الجرائم الإلكترونية من خلال القانون (09_04).	28
المبحث الأول: آليات المتابعة في الجرائم الإلكترونية.	30
المطلب الأول: مراقبة الإتصالات الإلكترونية.	30
المطلب الثاني: القواعد الإجرائية.	33
المبحث الثاني: الوحدات المختصة التي تتولى إجراءات البحث والتحقيق في الجريمة الإلكترونية.	39
المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.	40
المطلب الثاني: الأجهزة الأمنية.	46
الخاتمة.	55

الملخص باللغة العربية:

الجريمة الالكترونية من الجرائم التي تتطلب لارتكابها وسائل ذات تقنية عالية وعليه فإجراءات التحقيق فيها تتمتع بنوع من الخصوصية نظرا لطبيعة الجريمة الالكترونية حيث توجد في معظم البلدان المتضررة منها أجهزة خاصة بالتحقيق فيها وعندما يتحصل المحقق على بلاغ بوقوع جريمة الالكترونية يمكن أن يستدعي المتهم و الشاهد لاستجواب المتهم و الإستماع لأقوال الشاهد والشاهد في الجريمة الالكترونية هو شخص فني و صاحب خبرة وتخصص في تقنية و علوم الحاسوب والانترنت وعند الانتقال إلى مسرح الجريمة يقوم المحقق بتفتيش كل ما يستدعيه الأمر للكشف عن الحقيقة بما في ذلك النظم المعلوماتية.
الكلمات المفتاحية : الجرائم المعلوماتية ، إجراءات التحقيق ، النظم المعلوماتية

Summary in English:

Electronic crime is one of the crimes that require high-tech means to be committed. Therefore, the investigation procedures enjoy a kind of privacy due to the nature of electronic crime, as there are special devices in most affected countries to investigate it. And listening to the statements of the witness and witness in the electronic crime is a technical person with experience and specialization in technology and computer sciences and the Internet. When moving to the crime scene, the investigator inspects everything that is needed to reveal the truth, including information systems.

Key words: electronic crime, investigation procedures, information systems