وزارة التعليـم العالـي والبحث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

المرجع: ...01...

قسم: قانون خاص

مذكرة نهاية الدراسة لنيل شهادة الماستر

إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق

التخصص: قانون قضائي

من إعداد الطالب:

بن نعوم خالد أمين

تحت إشراف الأستاذة:

دة. بلباي إكرام

أعضاء لجنة المناقشة

الأستاذ..... بن عبو عفيف.....رئيسا.

الأستاذة.....بلباي إكرام.....مشرفا مقررا.

الأستاذة.....خراز حليمة.....مناقشا.

السنة الجامعية: 2019/2018

نوقشت يوم:**2019/06/23**


بسم الله الرحمن الرحيم
١٤٢٠

كلمة شكر

بداية نتوجه بالشكر الجزيل وحمدنا الكثير لله سبحانه وتعالى على توفيقه لنا في إنجاز هذا العمل المتواضع مصداقا لقوله تعالى:(لئن شكرتم لأزيدنكم) فالحمد لك ربّنا على ما وهبتنا.

لنتقدم بعد ذلك بالشكر الكبير إلى الأستاذة المشرفة بلباي إكرام التي كانت سندا لي في كل مرحلة من مراحل بحثنا هذا، وبما قدّمته لي من توجيهات قيمة ونصائح مفيدة كانت دعما ساقنا إلى نور النجاح.

وإلى كل من ساعدنا من قريب وبعيد في إنجاز هذا البحث، لنخلص في نهاية هذه الكلمة بالتوجه بالشكر والتقدير لامتنان الكثير إلى جميع معلّمينا وأساتذتنا بدءا بأولئك الذين علّمونا أولى الحروف إلى من سلّمونا الأمانة حتى نكون خير خلف لخير سلف.

لكل هؤلاء أسمى عبارات الشكر والتقدير

إهداء

قال الله عز وجل:(وقضى ربك ألا تعبدوا إلا إيّاه وبالوالدين إحسانا) سورة الإسراء

عملا بقوله تعالى أهدي ثمرة جهدي هذا:

إلى التي ربتني وسهرت الليالي من أجلي وحملت عني هموم الدنيا وغرست في نفسي جذور المحبة والوفاء وحلمت كي تراني ناجح في دراستي أمي الغالية.

إلى من حمل مرارة الشقاء وعلمني معنى الصبر والتحدي والاعتماد على النفس في سبيل دربي والدي محمد حفظه الله تعالى.

إلى جميع إخوتي: أحلام، رفيق أنار الله عز وجل طريقهم.

إلى أغلى مخلوقين في الدنيا جدي وجدتي أطال الله في عمرهما

إلى من قدم لي العون والمساعدة وبالأخص أستاذتي المحترمة بلباي إكرام

إلى كل أصدقائي اللذين لا أعرف للحياة طعما بدونهم

إلى عائلة بن نعوم وعائلة مكي كبيرا وصغيرا وخاصة الجدة عائشة والجد الحنون جيلالي

إلى الساهرين على حمل مشعل النور ليضيئوا للأجيال القادمة طريق الهدى وإلى كل طلبة تخصص قضائي وأساتذتي وعمال قسم قانون العام وقانون الخاص

إلى كل هؤلاء أهدي ثمرة عملي

- خالد أمين -

قائمة المختصرات

ج.ر.ج.ج: جريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

ق.إ.ج: قانون الإجراءات الجزائية.

ق.ع: قانون العقوبات.

ص: صفحة

ص ص : من الصفحة إلى الصفحة

الإنسان و منذ نعومة أظافره يسعى بكل الأشكال إلى الوصول إلى المعرفة و الحقيقة اليقينية. هذا كون الضروريات و الحاجات و المتطلبات الفرد لا تعرف السكون و هكذا هو طبع الإنسان منذ بداية العصور مروراً بكل مراحل التطور و الإزدهار وكذا مراحل الإنحطاط و التدهور . حيث دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من التطور الفكري و المعرفي الهائل غير المعهود، وذلك بفضل الثورة العلمية التكنولوجية و الرقمنة في جميع المجالات خاصة منها مجال الاتصالات والمعلومات التي اقتحمت بقوة هذه المرحلة التي وفرت مناخا خصبا لنهضة علمية تكنولوجية شاملة غير مسبوقة في كافة مجالات الحياة، الاقتصادية، الاجتماعية، الثقافية، والعلمية، تهاوت أمامها الحدود السياسية و الحواجز بين الدول و الشعوب، وضاقت معها الأماكن وتقلصت فيها المسافات، واختزلت وطوت فيها الأبعاد، بما تتميز به من عنصري السرعة والدقة ، مما أهل لحقبة جديدة بالغة الأهمية أحدثت تأثيرا في بنية المجتمع وذلك نتيجة لاكتساح جميع النواحي التي تتطلبها الحياة البشرية، مما جعل منها مصدرا أساسيا للأشخاص وكذا المؤسسات للإعتماد عليه في كافة شؤونهم نظرا للسرعة والدقة في تخزين المعلومات ومعالجتها في وقت قصير . حيث في هذه الفترة عرفت المعلوماتية تطورا مذهلا، كما ساعد اقترانها بالتكنولوجيات أخرى على تعميم استعمالها وتعدد وظائفها. فالحديث اليوم لم يعد عن الحاسوب وقدراته في اختزال الوقت وتخزين المعلومات أو انجاز العمليات المعقدة، وإنما عن تكنولوجيا الإعلام والاتصال والفضاء الافتراضي الذي نشأ نتيجة ارتباط المعلومات بمختلف المواصلات السلكية واللاسلكية . حيث أصبحت هذه الوسيلة ليست حكرا فقط على الدول المتقدمة، وإنما تعدت إلى غيرها من الدول النامية مما زاد من أهميتها، حيث عرفت بما يسمى بعصر المعلومات الذي أضحت فيه الكرة الأرضية قرية صغيرة تسبح في فضاء الكتروني. وهو ما دعا بالكثير من المفكرين إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في أواخر القرن التاسع عشر، ففي حين كان الهدف من الثورة الأولى إستبدال الجهد البدني للإنسان بالماكنة أو الآلة ، فإن هدف الثورة الثانية إحلال الآلة محل النشاط الذهني للإنسان ،

و مما لا شك أن هذه الأخيرة قد انعكست بصورة إيجابية على كثير من جوانب الحياة المعاصرة، بسبب ما توفره من الوقت والجهد والتكلفة عن الإنسان تجعل حياته اليومية أكثر سهولة و تيسير، الأمر الذي أدى إلى تضاعف الطلب على التقنيات التي تقوم عليها هذه الثورة والمتمثلة في الحواسيب الآلية والشبكات المعلوماتية، وتوسع ميادين استعمالها وازدياد الاعتماد عليها بشكل مفرط في كل القطاعات العامة أو الخاصة . فهنالك أكثر من 8.6 مليار شخص يستخدمون الهاتف النقال ومع التغلغل المتزايد للمعلومات وتكنولوجيا الاتصال في مختلف النشاطات البشرية، ، وذلك لكون جميع الدول والمنظمات والمؤسسات خاصة المالية المرتبطة ارتباط وثيق بها من أجل ممارسة أعمالهم ونشاطاتهم وتقديم مختلف الخدمات لزبائنهم . و رغم من المزايا والفوائد الجّمة التي تحققت ومازالت تتحقق يوما بعد يوم في كل مناحي الحياة بفضل تقنيات وسائل تكنولوجيات المعلومات والاتصال، إلا أن الاستخدام المتنامي لهذه التقنيات انطوى، في الوقت ذاته، على بعض الجوانب السلبية التي تمثل تهديدا خطيراً للأمن والاستقرار في المجتمع، جراء سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات والمؤسسات،الأمر الذي أدى بأصحاب النوايا الإجرامية إلى الاتجاه إلى الاستعمال غير الشرعي لهذه المنظومات المعلوماتية، من أجل ارتكاب أعمالهم الإجرامية المختلفة، من جهة الانتفاع بها، ومن جهة أخرى التملص من المسؤولية الجزائية ، حيث ظهر شكل جديد من الإجرام لم يكن معهودا من قبل وهو ما يعرف بالإجرام أو الجرائم المعلوماتية.

ولا جدال في اعتبار الجرائم الإلكترونية من أخطر و أعقد الجرائم على الإطلاق و تأتي في مقدمة الأشكال الجديدة للجريمة المنظمة، وخطورة هذه الجرائم نابعة من طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها وحداثة أساليب ارتكابها والبيئة التي تجري فيها وخصوصية مرتكبيها و وسائل كشفها. فهي جريمة تقنية سهلة الارتكاب، تنشأ في الخفاء وفي بيئة افتراضية دون أن تخلف أي أثار محسوسة، ويقترفها مجرمون أذكياء يمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات ويتمتعون بمهارات و خبرات تقنية عالية، فضلا

على أنها جرائم عابرة للحدود تتم عبر شبكة اتصال لا متناهية غير مرئية بإمكان أي شخص الولوج إليها حول العالم وغير تابعة لأية سلطة حكومية، وقد أدت هذه الخصائص التي تميز الجريمة الإلكترونية إلى صعوبة التعامل مع النشاطات الإجرامية المستحدثة وتكييفها على أساس النصوص الجنائية التقليدية، وهو ما جعل من المجتمع الدولي(التشريعات الآخرى) والملتقيات الدورية و الدراسات تتدخل من أجل تحديد و ظبط المفاهيم و المصطلحات المتعلقة بها و وضع حد لإنتشارها من خلال الإتفاقيات الدولية والمؤتمرات القارية والتعاون القضائي بين الدول الأعضاء لإسقاط وضبط الجناة.

فكان لابد من وضع أطر قانونية ملائمة جديدة و إدخال تعديلات على القوانين السارية المفعول بما يتلاءم مع الوضع الجديد، لتحديد شروط استعمال هذه الوسائل في مختلف المعاملات، من خلال نصوص جزائية لحماية الأنظمة المعلوماتية، وردع إساءة استعمالها سواء محليا أو دوليا في اطار الاتفاقيات الدولية ،كما امتدت التعديلات إلى نطاق القانون الجنائي الإجرائي، الذي صيغت نصوصه لتنظم الإجراءات المتعلقة بجرائم تقليدية التي لا توجد صعوبات كثيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها،على غرار الصعوبات التي يطرحها هذا النمط الجديد من الإجرام(الجريمة المعلوماتية). فالتقدم العلمي والتكنولوجي لا يمكن أن يسير أو يعمل وحده بمنعزل عن أي تقدم قانوني يواكبه ويحافظ عليه ويكفل حمايته.
و الجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لهذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا فهي أيضا معنية بالمكافحة و مسايرة التطور، 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 وطبيعة الجرائم المستحدثة ومنها إجراءات تطبق فقط على الجريمة المعلوماتية فقط ، التي تم النص عليها في القانون الجديد المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته 04/09 المؤرخ في 05أوت 2009.

تكمن أهمية البحث أساسا في كون الجرائم المعلوماتية جريمة جديدة تتسم بصبغة علمية بحتة جديدة غريبة في تصورنا على رجال القانون، حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها ويرجع هذا للتقنيات و الوسائل المستعملة لارتكابها ، لاسيما أنّ هذا الموضوع يتسم بالحداثة وندرة المراجع و المؤلفات التي تعرضت للجانب الإجرائي التي يمكن الاعتماد عليها كون أغلبية الدراسات السالفة ركزت على الجانب الموضوعي فقط . بالإضافة إلى كون الجرائم المعلوماتية حديثة النشأة ويمتد تأثيرها إلى جميع الأصعدة لإرتباطها بتطور تكنولوجيا الإعلام والاتصال والتي تستخدم في جميع المجالات الحياة سواء من طرف الأفراد أو المؤسسات إذ تجعل التعاملات معها صعبا ومعقدا مما يحتم إيجاد طرق جديدة لمكافحتها ، على الرغم من الصعوبات العديدة التي واجهتنا في إعداد المذكرة نظرا لصعوبة الموضوع وتشعبه.

ومن أسباب إختيار موضوع "**إجراءات التحقيق الجريمة المعلوماتية في ظل التشريع الجزائري**" يرجع في حقيقة الأمر إلى العديد من الأسباب بعضها شخصي والآخر موضوعي فالأسباب الشخصية : تكمن في إهتمامي بمجال المعلوماتية و إجراءات المتابعة في جريمة المعالجة الآلية للمعطيات التي تختلف كل الإختلاف عن إجراءات التحقيق التقليدية بالإضافة إلى أنّه موضوع جديد ، ورغبتي الشديدة في الغوص في مجال إجراءاتها الفني والتقني. أما الأسباب الموضوعية: فتكمن فيما يطرحه موضوع الحماية الإجرائية للجريمة المعلوماتية من إشكاليات قانونية التي لا بد من الوقوف عندها نظراً لحداثتها و من جانب تجريم الأفعال و الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات والقواعد الإجرائية الحديثة التي جاء بها المشرع بتعديل قانون الإجراءات الجزائية الجزائري وكذا قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته وغيرها من القوانين التنظيمية.

وهذا إذا دّل إنما يدل على مجموعة الصعوبات و المعوقات المتلقاة من خلال البحث و الدراسات المقدمة ودور المشرع في محاولته للتماشي مع باقي التشريعات لمسايرة الركب و

التصدي لهذه الجرائم و تحقيق الحماية القانونية اللازمة لكل فرد و المعطيات التي تسبح في العالم اللامرئي(الإفتراضي) ومنه يمكننا الخروج بإشكاليات فرعية تخص :

_ما مفهوم الجريمة المعلوماتية، المصطلحات العلمية و التقنية منها، المتعلقة بإفتعالها.

_ما مدى تجريم المشرع للأعمال المعالجة الآلية للمعطيات.

_ما هي الأجهزة و الهيئات الوطنية المسخرة من طرف الدولة لمتابعة هذه الجرائم.

وطرح إشكالية شاملة والمتمثلة في :

___ ماهي إجراءات التحقيق والبحث و التحري في الجريمة المعلوماتية في ظل التشريع الجزائري؟

ومنه للإجابة عن هذه الإشكالية اعتمدنا على المنهج الوصفي التحليلي، وصفي لأن دارستنا سترتكز على وصف المفاهيم العامة الخاصة بالجريمة المعلوماتية وآليات التحقيق في الجرائم الالكترونية في ظل التشريع الجزائري لاستخلاص الدليل والعقبات التي تعتريها، وتحليلي لأننا سنستعرض أهم العقبات القانونية التي تطرحها المواجهة الإجرائية للجريمة الالكترونية، ثم مناقشتها وتحليلها بشكل مفصل والغوص في جزئياتها، من ثمة تقديم الحلول المناسبة على ضوء ما توصل إليه الفقه و التشريع . ونتبع في ذلك خطة تتضمن فصلين:الفصل الأول الجريمة المعلوماتية بين المفاهيم و التجريم، في المبحث الأول تناولنا ماهية الجريمة المعلوماتية، والمبحث الثاني تجريم و متابعة الأعمال الإلكترونية . وأما الفصل الثاني فتطرقت فيه للآليات التحقيق في الجريمة المعلوماتية في ظل التشريع الجزائري. من خلاله حاولنا دراسة مدى سريان الإجراءات العامة و المآلوفة على الجرائم الإلكترونية في المبحث الآول والمبحث الثاني الإجراءات المستحدثة والخاصة بالجرائم المعلوماتية.

الفصل الأول

الجريمة المعلوماتية بين المفاهيم والتجريم

الفصل الأول: الجريمة المعلوماتية بين المفاهيم والتجريم.

لقد تغير المنظور الحالي للجريمة عن ذلك المفهوم التقليدي خاصة بعد تطور أساليب ارتكابها،حيث أصبحت ترتكب بسهولة فائقة وأصبح المجرمون يفلتون من العقاب،لصعوبة اكتشافها من جهة وكذا صعوبة إثباتها من جهة آخرى،وذلك بعد ظهور الحاسب الآلي الذي يقوم بالمعالجة الآلية للمعطيات وتخزينها وتسهيل عمليات تراسلها عبر مختلف الشبكات.

بحيث اتسعت هذه الظاهرة بظهور الشبكة العالمية للآنترنت لتصبح إجراماً لا حدود له على مستوى العالم الإفتراضي بشكل كبير و مروع يمس جميع الاشخاص أياً كانت صفتهم،ونظراً لخطورة هذه الجرائم التي ترتكب على هذه الشبكة والتي أصبحت ملجأً غير ممسوس بالنسبة للجناة الفعليين أي المجرمين الذين يستعملون التقنيات المعلوماتية لتنفيذ عملياتهم في هذا الفضاء،و الذي إختلف فيه الفقهاء و التشريعات من أجل تأطيره و وضع قوانين واضحة تحكمه وهذا راجع لحداثة هذا النوع من الجرائم والمجرمين و حتى السبل المستحدثة لتحقيق الجرم.

وعلى إثر هذه الحداثة و التقنيات و الفنيات المستعملة في الجرائم المعلوماتية لقيت اهتماما كبيراً من طرف الدول الغربية و العربية وغيرها من الدول التي تعاني من هذه الجرائم،و حتى لا تبقى مكتوفة الأيدي فلابد من دراسات وبحوث لتحصيل معلومات تساعد على الحد من الظاهرة و مكافحتها بسبل قانونية و البحث و التحري فيها و إسقاط الجناة و توفير الحماية القانونية و الفنية اللازمة للأشخاص التي تستعمل هذه الشبكات لمصالحها الخاصة و العامة، و هذا ما سنحاول معالجته من خلال هذا الفصل الجريمة المعلوماتية بين المفاهيم و التجريم في مبحثين:

- المبحث الأول:ماهية الجريمة المعلوماتية.
- المبحث الثاني:تجريم ومتابعة الأعمال الإلكترونية.

المبحث الأول :ماهية الجريمة المعلوماتية.

الجريمة الإلكترونية ظهرت لأول مرة في الدول المتقدمة التي اكتسبت التكنولوجيا العالية لمعالجة المعطيات ثم إنتشرت إلى باقي الدول الأخرى لهذا سنتطرق في هذا المبحث إلى دراسة الجريمة الإلكترونية في التشريعات المقارنة قبل ذلك سنتطرق لتحديد مفهومها والمصطلحات المتعلقة بهذا النوع من الجرائم و طبيعتها القانونية و اركانها في التشريع الجزائري.

المطلب الأول :مفهوم الجريمة المعلوماتية.

للتطرق إلى الجريمة الإلكترونية لابد من تعريف مصطلحات المتعلقة بهذه الجريمة أولا ثم تعريف الجريمة الإلكترونية في تشريعات المقارنة تعريفا فقهيا وقانونيا،سنقسم هذا المطلب إلى فرعين ندرس في الفرع الأول تعريف المصطلحات المتعلقة بالجريمة الإلكترونية والفرع الثاني تعريف الجريمة الإلكترونية [1].

الفرع الأول :تعريف الجريمة المعلوماتية في باقي التشريعات الدولية.

1-مصطلحات الجريمة المعلوماتية:

هناك مجموعة من المصطلحات المتعلقة بمصطلح الجريمة الإلكترونية منها:

أولا الحاسب الآلي :الحاسوب هو عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما،وذلك بتنفيذ ثلاث عمليات أساسية هي:إستقبال البيانات المدخلة للحصول على حقائق مجردة،ومعالجة البيانات إلى معلومات و إجراء الحسابات والمقارنات ومعالجة المدخلات، وإظهار المعلومات المستخرجة للحصول على نتائج[2].

[1]-نهلا عبد القادر المومني ، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي،دار الثقافة للنشر والتوزيع 1429 .هـ 2008 م ، الطبعة الأولى، الإصدار الأول 2008 ، ص20

[2]-نفس المرجع، ص20.

ومن تعريفات التي أعطيت للحاسب الآلي أنه مجموعة من الأجهزة المتكاملة تعمل مع بعضها البعض بهدف تشغيل مجموعة من البيانات المدخلة وفقا لبرنامج موضوع مسبقا للحصول على نتائج معينة."

كما يعرف أيضا بأنه مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال أداء[1] التعليمات المخزنة وهو آلة حاسبة إلكترونية ذات سرعة عالية ودقة كبيرة يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على النتائج مطلوبة[2] .

ونظام الحاسوب يمكن تعريفه أيضا أنه :مجموعة من الأجهزة المترابطة والتي تعمل معا من خلال مجموعة من الأوامر والبيانات لتحقيق حل المسألة معينة[3] .

ثانيا المعلومات : تأخذ عدة معاني مختلفة نذكر منها

1- المعلومات هي المعنى الذي يستخلص من البيانات عن طريق العرف أو الإتفاق أوالخبرة أو المعرفة.

2- تعرف المعلومات: وقد اقترح **الأستاذ Cattala** بأنها رسالة ما يعبر عنه في شكل يجعلها قابلة للنقل أو الإبلاغ للغير[4] .

3- عرف **المشرع الأمريكي** المعلومات في قانون المعاملات التجارية الإلكترونية لسنة 1999بالفقرة العاشرة من المادة الثانية بأنها تشمل البيانات والكلمات والصور والأصوات و الرسائل وبرامج الكمبيوتر الموضوعة على الأقراص المرنة وقواعد البيانات أوما شابه ذلك.

4- وفي **فرنسا** ووفقا للقانون رقم82 - 652 الصادر في 26 يوليو 1982تعرف المعلومات بأنها صوت أو صورة أومستند أو معطيات أو خطايا أيا كانت طبيعتها.

---

[1]- خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، دار الجامعية ، الإسكندرية ، عنوان 84 شارع زكرياء غنيم،الإبراهيمية ،الإسكندرية ، 2008 ، ص20 .

[2]- خالد ممدوح إبراهيم ، المرجع السابق، ص14 .

[3]- نهلا عبد القادر المومني ،المرجع السابق ، ص2 .

[4]- سامي على حامد عياد ، الجريمة المعلوماتية وإجرام الأنترنت ، ماجستير في القانون ، دار الفكر الجامعي ، 30 شارع سوتير الإسكندرية ، 2008 ، ص2 .

5- ومن القوانين العربية التي عرفت المعلومات **القانون الأردني** للمعاملات الإلكترونية رقم 85 لسنة 2001 حيث المادة الثانية من هذا القانون بأنها البيانات أو النصوص أو الصور أو الأشكال أو الأصوات أو الرموز أو برامج الحاسوب أو قواعد المعلومات التي أنشات أو أرسلت أو استلمت أو خزنت بوسائل الإلكترونية[1] .

ثالثا المجرم المعلوماتي : هوالشخص الذي يتمتع بالمهارة والمعرفة والذكاءعند إرتكابه للجريمة يبررها بمبررات مختلفة لأنه يخاف من كشف جريمته .ومن الدوافع التي تدفع المجرم المعلوماتي لإرتكاب جريمة الرغبة في التعلم وقهر النظام المعلوماتي وإثبات الذات والرغبة في الإنتقام والمتعة والتحدي وهناك دوافع مادية مثل تحقيق الربح[2] وكسب المال و هناك دوافع أخرى كالتنافس السياسي والإقتصادي والتسابق العسكري بين الدول[3].

2-تعريف الجريمة الإلكترونية.

أولا تعريف اللغوي : المعلوماتية يقصد بها المعالجة الآلية وتعني تكنولوجيا التجميع للمعلومات Informatique ،وهي ترجمة للمصطلح الفرنسي Traitematique وهو معالجة وإرسال المعلومات بواسطة الكمبيوتر، وقد إستعمل مصطلح Télématique ويعني المعالجة الالية للبيانات ومصطلحAutomatisme des données في اللغة الإنجليزية وإن كان ليس لها أصل في إتصالات ، وهي تعادل مصطلح القاموس الإنجليزي Telematics ، مستمدة من اللغة الفرنسية [4].

ثانيا التعريف الإصطلاحي:

يلاحظ عدم وجود إتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة ، فهناك من يطلق عليها ظاهرة الغش المعلوماتي ، أو الإختلاس المعلوماتي ، أو الجريمة المعلوماتية،

[1]- خالد ممدوح إبراهيم ، المرجع السابق ، ص26 .
[2]- نهلا عبد القادر المومني ، المرجع السابق ، ص 77-80.
[3]- نهلا عبد القادر المومني ،المرجع السابق ، ص 77-80.
[4]- خالد ممدوح إبراهيم ، المرجع السابق ، ص43 .

فلهذا نجد بعض الفقهاء وضعوا تعريف الجريمة المعلوماتية في مجالين : مجال واسع ومجال ضيق[1] .

أ _ التعريف الواسع : هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية فعرفوها كالأتي : « كًل فعل أو امتناع عمدي ، ينشأ عن الإستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الإعتداء على الأموال أو الأشياء المعنوية » (الخبير الأمريكيParker)مفهوما واسعا للجريمة المعلوماتية أنها : كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق بالمجني عليه ، أو مكسب يحققه الفاعل[2].

يعرف **الأستاذVivan**الجريمة المعلوماتية بأنها : مًجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب [3].

جرائم الكمبيوتر فهو مصطلح شامل أشمل من المصطلح السابق ويقصد فيه كل الجرائم التي يستخدم فيها الكمبيوتر، سواء كأداة للجريمة أو كان هدفاً في الجريمة ويدخل في ضمنها جرائم معلوماتية وجرائم الإنترنت ، كما يدخل الإعتداء على الشبكات المحلية خاصة بالهيئات والمنشآت الخاصة والعامة . الجريمة الإلكترونية هي ببساطة إستخدام التقنيات الرقمية لإخافة الآخرين[4].

ب _ تعريف الضيق : تعرف الجريمة المعلوماتية على أنها : " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لإرتكاب الجريمة من ناحية و لملاحقته وتحقيق معه من ناحية أخرى".

يرى **الأستاذ Mass** أن المقصود بالجريمة المعلوماتية هي: " الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح[5].

---

[1]- محمد العريان ، الجرائم المعلوماتية ، كلية الحقوق جامعة الإسكندرية ، دار الجامعة الجديد للنشر ، الإسكندرية ، الطبعة 2004، ص43 .

[2]- نهلا عبد القادر المومني ، المرجع السابق ، ص49 .

[3]- نفس المرجع ، ص49 .

[4]- أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الأنترنت ، دار المطبوعات الجامعية ، الأسكندرية ، 2009 ، ص106 .

[5]- نهلا عبد القادر المومني ، المرجع السابق ، ص48 .

الفقيه الألمانيTiedmann أن " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بإستخدام الحاسب .فهو يرتكز في تعريفه على وسيلة إرتكاب الجريمة.

يعرفها **مكتب تقييم التقنية** في الولايات المتحدة الأمريكية من خلال تعريف جريمة الحاسب أنها :الجرائم التي تلعب فيها البيانات والبرامج المعلوماتية computer crime دورا رئيسيا . وإرتكز كذلك في تعريفه على الوسيلة المرتكبة بها الجريمة.

يعرف **david thompson** جريمة الحاسب بأنها : أي جريمة يكون متطلبا لإقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب و إرتكز هذا الفقيه في تعريفه على توافر المعرفة بتقنية المعلومات[1]

أما بالنسبة للفقه المصري ، فهي تنشأ عن الإستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الإعتداء على الأموال أو الأشياء المعنوية[2] وهناك فريق أخر يرى أن الجريمة المعلوماتية هي " عمل أو إمتناع يأتي بأضرار بمكونات الحاسب وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا ." وقد عرفها **محمد علي العريان** بأنها " كل فعل إيجابي أو سلبي عمدي يهدف إلى الإعتداء على تقنية المعلوماتية أيً كان غرض الجاني [3]".

يعتبر الإقتراح المقدم من قبل **مجلس الشيوخ الفرنسي** بشأن نطام المعالجة الآلية عند تبنيه للقانون 19-88 المعدل والمتمم مؤرخ في 05\01\1988 المتعلق بالغش المعلوماتي والدي تم إدماجه في القانون العقوبات الفرنسي لتجريم بعض جرائم الحاسب الألي و هو ما يعرف **بقانون Godfrain** ، يعتبر أهم تعريف يمكن الإعتماد عليه في تحديد مفهوم المعالجة الآلية للمعطيات ، بحيث إقترح هدا المجلس التعريف التالي: " نظام المعالجة تتكون كل منها ذاكرة ، برامج ، معطيات ، أجهزة إدخال وإخراج ، أجهزة ربط ، يربط بينهما مجموعة من العلاقات

[1]- سامى علي حامد عياد ، المرجع السابق ، ص38 -40.
[2]- سامى علي حامد عياد ، المرجع السابق ، ص38 -40.
[3]- نشناش منية ، مداخلة حول الركن المفترض في الجريمة المعلوماتية ، جامعة بسكرة2015 / 2016 ، ص3 ،2.

تتحقق عن طريق نتيجة معينة وهي معالجة المعطيات ، مع ضرورة أن يكون هذا المجموع أو المركب محميا بأجهزة أمان[1]."

ويلاحظ على هذا التعريف أنه إشترط على نظام المعالجة الآلية للمعطيات أن تتوافر على شرطين لا قائمة له ولا حماية قانونية بدونهما هما:

ضرورة وجود علاقات تربط مابين العناصر الداخلة في تكوين النظام ، وتوحدهما نحو تحقيق هدف واحد محدد هو المعالجة الآلية للمعطيات هذا مع الملاحظة أن العناصر الأدبية والمعنوية التي يتكون منها المركب والتي وردت في تعريف مجلس الشيوخ ،إنما وردت على سبيل المثال وهنا يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال مستقبلا ضرورة توافر النظام على أجهزة أمان تحقق له حماية فنية كشرط للتمتع بالحماية الجنائية[2].

تعريف القانوني:

إن غالبية المشرعين تجنبوا الخوض في مسألة وضع تعريف تشريعي لنظام المعالجة الآلية للمعطيات و أوكلوا مهمة ذلك إلى الفقه والقضاء، إلا أن بعضهم من جهة أخرى إتجهوا إلى وضع تعاريف لنظام المعلومات وليس لنظام المعالجة الآلية للمعلومات ، ومن بين التشريعات التي عرفت النظام المعلوماتي نذكر:

أ _قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة1996 :

حيث عرف هذا القانون من خلال نص المادة 2 الفقرة، نظام المعلومات على أنه:

"النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو إستلامها أو تخزينها لتجهيزها على أي وجه أخر "[3].

[1]- محمد علي العريان ، المرجع السابق ، ص45

[2]- قانون إمارة دبي رقم 02 لسنة 2002 متعلق بالمعاملات والتجارة الإلكترونية ، صادر بتاريخ .12 فبراير2002

[3]- :نشناش منية ، المرجع السابق ، ص3

ب _قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكتروني رقم 02 لسنة2002

حيث عرف هذا القانون هو الأخر من خلال نص المادة 2 الفقرة 6 ، بصدد تعريف المصطلحات أيضا نظام المعلومات الإلكتروني على أنه" : نظام إلكتروني لإنشاء أو إستخراج أو إرسال أو إستلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونيا[1]. "

و ما يلفت الانتباه من خلال هذه التعاريف أنها تنصب على أنظمة المعالجة الآلية للمعلومات في حد ذاتها أكثر من نظام المعلومات باعتباره نطاق أوسع، كذلك أنها انصبت في مجرى واحد معتمد في تعريف نظام المعلومات على تعداد الوظائف التي يقوم بها أوينجزها هذا النظام والتي تمثل طرق المعالجة المعلوماتية ومعبرة " المعالجة الآلية " مجرد وظيفة من تلك الوظائف[2]

على رغم من أن فكرة المعالجة الآلية أوسع من فكرة المعالجة المعلوماتية ، أضف إلى ذلك خلوها من الإشارة إلى الشرطين اللذين أشار مجلس الشيوخ الفرنسي إلى ضرورة توافرهما في النظام.

الفرع الثاني: تعريف المشرع الجزائري للجريمة الإلكترونية

إن الجريمة الالكترونية تتمتع بخطورة إجرامية لم يشهد لها العالم مثيلا في الجرائم التقليدية ، فلهذا ظهر اختلاف في تعريف قائما من هذه التعاريف مايلي:

" بأنها الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال. "

وهناك من يعرفها على أنها " كل عمل أو امتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية والمعنوية ، وشبكات الاتصال الخاصة به ، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها".

أو أنها " استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي و الهاتف النقال ، أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة و أمور غير أخلاقية لا يرتضى بها المجتمع[3].

[1]- قانون إمارة دبي رقم 02 لسنة 2002 متعلق بالمعاملات والتجارة الإلكترونية ، صادر بتاريخ .12 فبراير2002 .

[2]-نشناش منية ، المرجع السابق ، ص3 .

[3]- زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ، ط1 ، 2011 ، ص 43.

تبنى الفقه الجزائري تعريف **المؤتمر العاشر للأمم المتحدة** لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية ، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[1].

أ- **التعريف الأكاديمي.**

كل فعل إجرامي متعمد كانت له صلة بالمعلوماتية ، يترتب عنه خسارة تلحق بالصحية أو مكسب يحققه الجاني ، كما يمكن الاعتماد في التعريف الواسع للجريمة المعلوماتية على:

1-على ما تكون المعلوماتية موضوعاً للإعتداء عندما تقع الجريمة على المكونات المادية للأجهزة والمعدات المعلوماتية.

2-عندما تكون المعلوماتية أداة ووسيلة للإعتداء عندما يستخدم الجاني جهاز معلوماتي لتنفيذ جريمته[2].

ب- **التعريف القانوني:**

تبنى المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث[3].

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات[4]، حيث أنه عرف من خلال نص المادة 2 من القانون رقم09 -04 المتضمن القواعد الخاصة

[1]- زبيخة زيدان ، المرجع السابق ، ص44 .

[2]- المقدم عز الدين عز الدين ، الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية، بسكرة في11\2015 .

[3]- قانون رقم09 -04 المؤرخ في 14 شعبان 1430 سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح ر ع 47 صادر بتاريخ16 /2009/08، ص5.

[4]- نفس المرجع ، ص5.

للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، مسميا إياه": المنظومة المعلوماتية " وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة ، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات ، تنفيذا لبرنامج معين[2] "

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية بأشكال جديدة من الإجرام التي لم تشهدها الجزائر من قبل وهذا ما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم04- 156المؤرخ في العاشر من نوفمبر2004 المتمم للأمر رقم 66-156المتضمن قانون العقوبات والذي افرد القسم السابع مكرر منه تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات [3]، والذي تضمن 08 مواد من المادة 394 مكرر وحتى المادة 394 مكرر07 وفقا المشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها ،وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات[4] .

أما فيما ينص الشرط الثاني لمجلس الشيوخ الفرنسي والمتعلق بضرورة توافر النظام على حماية فنية فيبدو ان النظام المشرع قد حسم موقفه إلى جانب الفقه الذي لا يشترط هذا الشرط لحماية نظام المعالجة الآلية للمعطيات الجنائية.

ج_موقف المشرع الجزائري من الجريمة الإلكترونية:

من خلال ما تقدم من تعريفات الجريمة الالكترونية في التشريع الجزائري نستنتج موقف المشرع من هذه الجريمة ، المتمثل في أن التقدم التكنولوجي وإنتشار وسائل الاتصال الحديثة أدى إلى بروز إجرام فني في حلة و أشكال مستجدة ، مما دعى إلى النص على معاقبة هذا النوع من الجرائم ، تسعى من خلالها إلى توفير حماية الجزائية للأنظمة المعلوماتية وأساليب المعالجة

[1]- المادة 2 الفقرة ب قانون رقم 09-04 ،المرجع السابق.
[2]- نشناش منية ، المرجع السابق ، ص4 .
[3]- عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، كلية الحقوق جامعة الإسكندرية ، 2006 ، ص27.
[4]- نشناش منية ، المرجع السابق، ص4

الآلية للمعطيات ، وبالتالي قام المشرع الجزائري بتعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال و كان ذلك بموجب القانون رقم10/04 المؤرخ في 2004/11/10 المتمم و المعدل للأمر156/66 المتضمن لقانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات ، فقد أثار المشرع الجزائري إستخدامه لمصطلح للدلالة على كلمة المعلومات والنظام الذي يحتوي عليها ويخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة إرتكابها وحصرها فقط في صور الأفعال التي تشكل إعتداء على النظام المعلوماتي ، أي الجرائم التي يكون النظام المعلوماتي محلا لها[1] .

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها ، فقام بحماية هذه المعطيات من أوجه عدة.

ثم في مرحلة لاحقة اختار المشرع الجزائري التعبير عن الجريمة المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 04-09 الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها[2].

ونجد المشرع الجزائري تطرق إلى تعريف جريمة المساس بأنظمة المعالجة الآلية وجرم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات في المادة 2 من قانون رقم09 /04 في مواد من 394مكرر إلى 394 مكرر 7 من قانون العقوبات[3].

المطلب الثاني:الأركان و الطبيعة القانونية للجريمة المعلوماتية.

لابد للجريمة أن تتوافر على مجموعة من الأركان تقوم بتحققها و تزول بزوالها كغيرها من الجرائم ،حسب ما جاء به المشرع الجزائري من خلال النصوص القانونية التي تعرف و تحدد الجريمة المعلوماتية عن غيرها من الجرائم فسنحاول استخلاص أركان الجريمة المعلوماتية ،

[1]- سعيد نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية، جامعة الحاج لخضر باتنة 2012-2013 ، ص41 .

[2]- نفس المرجع ، ص41 .

[3]- نفس المرجع ، ص41 .

لكن قبل التطرق الى الآركان علينا تحديد الطبيعة القانونية لهذه الجريمة لكي تكون دراستنا سلسة و ممنهجة و هذا ما سنراه خلال الفرعين التاليين.

الفرع الأول: الطبيعة القانونية.

إن دراسة الجريمة الالكترونية بشكل خاص تدخل ضمن قسم من أقسام قانون العقوبات وهو قسم الخاص وهو ذلك الفرع الذي يدرس كل جريمة على حداها متناولا كل عناصرها الأساسية والعقوبة المقررة لها ، فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة[1]. "إن هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواءاً كان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة ، كما قد ترتكب هذه الجرائم في مجال المكالمات أو معالجة النصوص وهذا النوع الأخير من الجرائم لا يعد أن يكون بطريقة أوتوماتيكية من تحرير الوثائق والنصوص على الحاسب مع توفير إمكانيات التصحيح والمسح والتخزين والاسترجاع والطباعة".[2] فهذه العمليات كلها هي وثيقة الصلة بالجرائم محل البحث وعليه لابد للجاني من فهمها فضلا عن أن الجاني قد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل الإعتداء أو تستخدم وسيلة له[3]. تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى الاعتداء على الخصوصية والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة.

وبالتالي هذه الطبيعة الخاصة للأفعال المجرمة هل تدخل ضمن أحكام خدمات البريد أم التخابر الخاص أم يكون الهدف الأساسي للتحري عن نظام القانوني المناسب لطبيعة الجرائم المعلوماتية هو معرفة النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر المواقع والمعلومات فيها ، ومن هذا النظام القانوني تتحدد المسؤولية التي يفترض تطبيقها على

[1]- محمد زكي أبو عامر وعلي عبد القادر القهوجي،قانون العقوبات القسم الخاص ، دار النهضة العربية القاهرة1993،ص9.
[2]- أ حمد السمدان ، النظام القانوني لحماية برامج الكمبيوتر ، مجلة الحقوقي ، الكويت ، 1987 ، ص164.
[3]- جميل عبد الباقي ، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت ، دار النهضة العربية ، القاهرة ، 2001 ، ص92.

الأشخاص المسؤولين عن هذا النشر ، ومن خلال المجال التي ترتكب فيه الجريمة المعلوماتية والمحل الاعتداء عليها تظهر لنا الطبيعة القانونية الخاصة للجريمة[1].

إن التطور المعلوماتي يفتح المجال لاقتناء وسائل الكترونية تمكن المتجاوزين لاستخدامها في ارتكاب جرائم مختلفة لأن الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيها يتعلق بالمعالجة الآلية لبيانات وإدخال المعلومات ونقلها ومن ثم يتحتم ضمه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارنة عاجزة عن مواكبة التطور المعلوماتي أوبما يحويه من فراغ تشريعي في هذا المجال[2].

أما من حيث تكييف القانوني فتتخذ هذه الجرائم طبيعة خاصة إذا لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة ، إن تطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الإثبات وصعوبة إيجاد دليل مادي يدين مرتكب الجريمة لأنه من السهل على الجاني محو أدلة الإدانة في وقت قصير لا يتجاوز لحظات وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال قد تكون البيانات التي تجري البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة و من هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة[3]. ومن صعوبة ملاحقة مرتكبي الجرائم المعلوماتية الذين يقيمون في دولة أخرى دون أن ترتبط هذه الدولة باتفاقية مع الدولة التي تحقق فيهاالسلوك الإجرامي أو جزء منه وفي ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة[4].

إن للجريمة الالكترونية خصائص كثيرة سنحاول حصرها و إبرازها في مايلي:

أولا: الجرائم الإلكترونية من الجرائم عابرة للحدود.

وسعت شبكات المعلومات عملية الاتصال وتبادل معلومات بين الدول والأنظمة التي يفصل بينها آلاف الأميال ، ومع القدرة التي يتمتع بها الحاسب أدى ذلك إلى إمكانية إرتكاب الجريمة

[1]- طوبي ميشال عيسى ، التنظيم القانوني لشبكة الإنترنت ، دار صادر للمنشورات بيروت ، ط1، 2000 ، ص383.
[2]- مجلة جامعة بابل ، العلوم الإنسانية ، المجلد 14 ، العدد6 ،2007، ص91.
[3]- نفس المرجع ، ص9 .
[4]- هلال عبد الله أحمد ، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ،ط.1، ص22 .

الإلكترونية في أماكن متعددة من العالم وفي وقت واحد ، كما يمكن أن يكون المجني عليه في غير الدولة التي يقيم فيها الجاني[1].

إن الجريمة المعلوماتية هي شكل من أشكال الجرائم العابرة للحدود ، فمسرح الجريمة لم يعد محليا بل أصبح عالميا إذ أن الفاعل لا يتواجد ماديا على مسرح الجريمة وهذا التباعد في المسافات بين الفعل المرتكب من خلال الحاسوب والفاعل وبين المعلومات التي كانت محل الاعتداء ، فالجاني يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الآلي الموجود في بلد آخر وهذا الفعل قد يضر شخصا ثالثا في بلد آخر[2].

ومن خلال هذه الخاصية الدولية يثار إشكال حول الإختصاص القضائي في محاكمة المجني عليه بمعنى بمعنى آخر ما هي الدولة المختصة بمحاكمة الجاني ؟ هل هي الدولة التي ارتكب على إقليمها النشاط إجرامي أم التي يوجد فيها المجني عليه ؟[3].

ثانيا: صعوبة إكتشاف وإثبات الجرائم الإلكترونية.

و مايكسبها هذه الخاصية هو عدم ترك الجاني آثار تدل على إجرامه ، فالجرائم التي تتم بواسطة إدخال الرموز و الأرقام ، هي رموز دقيقة ويصعب إكتشافها وإثباتها لهذا عادة ما يتم إكتشافها بالصدفة وغالباً ما يتم معاقبة مجرمين وذلك لعدم وجود أدلة قائمة في حقه [4].

فالجريمة المعلوماتية لا تترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية[5].

وصعوبة اكتشاف وإثبات الجرائم المعلوماتية راجع لعدة أسباب منها وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى

[1]- خالد ممدوح ، المرجع السابق ، ص 82.
[2]- سعيد نعيم ،المرجع السابق ، ص32 .
[3]- نفس المرجع ، ص32 .
[4]- معتوق عبد اللطيف ، المرجع السابق، ص24.
[5]- سعيد نعيم، المرجع السابق، ص34.

خبرة فنية يصعب على المحقق التقليدي التعامل معها ، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات[1]

ويصعب في جرائم المعلوماتية العثور على دليل مادي للجريمة وذلك راجع إلى إستخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان ، وهذا السلوك المادي في إرتكابها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به[2].

ثالثا : تتطلبها لوسائل تقنية و فنية خاصة.

إن الجريمة المعلوماتية تستلزم لقيامها توفر الحاسب الآلي وكذلك شبكة الانترنت كوسائل لإرتكاب الجريمة و أدواتها الرئيسية أماكن المعرفة التقنية فتكون ضرورية بحسب درجة خطورة الجريمة المعلوماتية[3] .

رابعا : تتطلب خبرة وتحكما في تكنولوجيا المعلوماتية عند متابعتها .

الجريمة المعلوماتية لها طبيعة تقنية وبذلك لا يستطيع رجال الضبطية القضائية التعامل بإحترافية ومهارة أثناء البحث والتحري ، لذلك لابد أن يكون المحقق متخصص في جريمة المعلوماتية حتى لا يتسبب في إتلاف الدليل الالكتروني[4].

خامسا : الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية.

إن هذه الجريمة تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي ، وفي الواقع ليس هناك شعور بعدم الأمان تجاه المجرمين في مجال المعرفة المعلوماتية لأن مرتكبيها ليسوا محترفي الإجرام[5] .

---

[1]- نفس المرجع ، ص 31

[2]- هشام محمد فريد ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، أسيوط ، ط 1، 1994، ص 82.

[3]- معتوق عبد اللطيف ، المرجع السابق، ص 15

[4]- المرجع نفسه، ص15

[5]-معتوق عبداللطيف،المرجع السابق، ص15.

سادسا : دافع إرتكاب الجريمة المعلوماتية.

يختلف الدافع في الجريمة التقليدية عن الدافع الباعث في الجريمة المعلوماتية فقد يكون الدافع مخالفة النظام العام والخروج على القوانين وقد يكون ماديا يراد به إكتساب مبالغ طائلة أو الإهانة وتشهير والتأثر لكن دون الإحتكاك المباشر بالمجني عليه.[1]

الفرع الثاني: أركان الجريمة الإلكترونية.

سنتناول في هذا الفرع أركان الجريمة الالكترونية الأساسية والمتمثلة في الركن الشرعي والمتمثل في نصوص القانونية والركن المادي والمتمثل في السلوكات المادية المجرمة والركن المعنوي المتمثل في القصد الجنائي للجريمةالإلكترونية.

1_الركن الشرعي للجريمة الالكترونية:

كون الجريمة حاصل تحصيل مجموعة من السلوكات والأفعال المادية الصادرة عن الإنسان، هذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه[2].

القاعدة الأساسية الناتجة عن مبدأ الشرعية وهي عدم رجعية القانون الجنائي بمعنى لا يمكن معاقبة شخص ارتكب فعلا لم يجرمه القانون[3] وهذا ما نصت عليه المادة 1 من قانون العقوبات "لا جريمة ولا عقوبة أو تدبير أمن بغير نص قانوني "[4].

ويتميز هذا المبدأ أن القاضي الجنائي عند تفسيره لنصوص القانون أن يفسره تفسيرا ضيقا ، بالإضافة إلى منع اللجوء إلى القياس بمعنى عدم لجوء القاضي الجنائي إلى قياس فعل لم يرد نص بتجريمه على فعل ورد نص بتجريمه فيقرر القاضي الجنائي للأول عقوبة الثاني للتشابه بين الفعلين.[5]

[1]- جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، دار النهضة العربية ، القاهرة ، 1992 ، ص62

[2]- أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومه ، الجزائر ، ط10 ،2011، ص27.

[3]- أحمد خليفة الملط ،الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط2، 2006، ص78.

[4]- مولود ديدان ، قانون العقوبات ، المرجع السابق ، ص4 .

[5]- أحمد خليفة الملط ، المرجع السابق ، ص 10

إن ظهور شبكة الانترنت أدى إلى تطور ظاهرة الإجرام بشكل خطير في تفشي جريمة الإلكترونية وازداد هذا الوضع خطورة خاصة حين أصدر المجلس الأوربي سنة 1989[1]

وقد اختلفت في اختيار التقنية التشريعية المناسبة ، فمنها من قام بإدماج النصوص العقابية المتعلقة بالإجرام المعلوماتي في قانون العقوبات التقليدي ، ومنها من قام بوضع قانون جنائي مستقل للمعلوماتية يدخل في القانون الجنائي التقني[2].

تستمد الجرائم المعلوماتية شرعيتها من مختلف التشريعات الوطنية الصادرة بشأن الجريمة المعلوماتية فقد بذلت هيئة الأمم المتحدة جهودا كبيرة إضافة إلى جهود المجلس الأوربي لإقتناع الدول بوضع تشريعات لتصدي ومواجهة ومكافحة جرائم الالكترونية وتعزيز التعاون الدولي في هذا المجال.

واجه المشرع عدة عراقيل عند تنظيمه لمجال الحماية الجنائية من مخاطر جرائم المعلوماتية وكان أول العراقيل هو إمكانية تطبيق النصوص التقليدية على هذا النوع الجديد من الجرائم ؟ أم ذلك إخلال بمبدأ الشرعية ؟ ووقوع في التفاسير المخلة بمبادئ القانون الجنائي ؟.

وللإجابة على هذا الإشكال ظهر اختلاف المشرعين بين ضرورة وضع نصوص جديدة خاصة بالجرائم الالكترونية وبين تكييف النصوص القديمة مع هذه الجرائم الحديثة الخصوص من يقول لا فائدة من تطبيق التشريع خاص بجرائم عادية ترتكب بوسائل بتقنية متطورة ، والبعض الآخر يرى في ذلك إخلالا بالبنيان القانوني حيث أن المشرع يتطلب في الجرائم التقليدية سلوكا محددا وتتحقق مع الركن المادي للجريمة تختلف عن سلوكات المطلوبة في الجرائم الإلكترونية[3].

وهناك من يقول إن الجرائم المعلوماتية ماهي إلا جرائم عادية ترتكب بواسطة الحاسب الآلي فالمطلوب من المشرع توقيع العقاب على ارتكاب هذه الجرائم بنصوص تقليدية، وعلى المشرع

[1]- معتوق عبد اللطيف، المرجع السابق ، ص 25

[2]-نفسه ، ص25

[3]– نفس المرجع، ص25.

فقط الإلمام بمصطلحات تقنية حتى لا يتم المساس بجريمة تبادل المعارف والحفظ على الحق في احترام الحياة الخاصة[1].

بالنسبة للمشرع الجزائري أورد قسما خاصا للمساس بأنظمة المعالجة الآلية للمعطيات وهو القسم السابع مكرر بمحتوى المادة 394 مكرر إلى 394 مكرر7 بمقتضى القانون 04-10 المؤرخ في2004/11/15 ، ولم يكتف المشرع الجزائري بذلك بل فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون 23-06 المؤرخ في 2006/12/20والذي مس المادة 303وإقراره بالمادة 303 مكرر إلى 303 مكرر03 وهذا تصديا للاستخدام السيئ لوسائل التكنولوجيا الحديثة.[2]

2_ الركن المادي:

إن الركن المادي للجريمة الالكترونية يقوم على صورتين أساسيتين : الصورة الأولى :متمثلة في الاعتداء على نظام المعالجة الآلية وهذه الأخيرة تحتوي على نوعين من الاعتداء وهو الدخول والبقاء غير مشروع في نظام المعالجة الآلية وتنطوي تحت هذا النوع ثلاث أفعال فعل الدخول والبقاء والعرقلة أو التعطيل ، أما النوع الثاني : متمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال وهي فعل الإدخال والمحو والتعديل ، أما الصورة الثانية متمثلة في الاعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي ومن خلال ما تقدم سنتطرق أولا إلى دراسة الدخول والبقاء غير المشروع في نظام المعالجة آلية ، ثم نتطرق ثانيا إلى الاعتداء العمدي على نظام المعالجة الآلية.

الصورة الأولى: الإعتداءات على أنظمة المعالجة للمعطيات.

أولا : الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات نصت المادة 394 مكرر من قانون العقوبات الجزائر على أنه " يعاقب بالحبس من ثلاث (3)أشهر إلى سنة

[1]- نفس المرجع، ص25.

[2]- نفس المرجع ، ص25

(1) ، وبغرامة من 10.000دج إلى 50.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة(6) أشهر إلى سنتين (2) والغرامة من 50.000 إلى 150.000 دج "[1].

ونستخلص من خلال هذين النصين وجود صورتين لفعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات الصورة الأولى تتمثل في الصورة البسيطة وهي مجرد الدخول أو البقاء غير المشروعين في النظام ، والصورة الثانية هي الصورة المشددة تتحقق بتوفر ظروف المشددة وهي : _حذف أو تغير معطيات المنظومة بعد الدخول أو البقاءغير المشروعيين. تخريب نظام اشتغال المنظومة بعد الدخول أو البقاء غير المشروعين[2] .

1_الصورة البسيطة : يتمثل النشاط الإجرامي في هذه الصورة في الأفعال التالية:

أ /فعل الدخول : يتحقق فعل الدخول بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضاء صاحبها ، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات[3].

يمكن أن نميز ثلاث صور المحل هذه الجريمة وهي الصورة الأولى تتمثل في المعلومات في ذاتها والثانية أنظمة المعالجة الآلية للمعطيات التي ترتبط فيما بينها من خلال شبكة الاتصال ، والثالثة شبكات المعلومات.

فهذا التباين والاختلاف حول محل ركن المادي لهذه الجريمة أورد ثلاث اتجاهات هي:

_الإتجاه الموسع : يجمع بين الصور الثلاث ويتخذها جميعا كمحل الجريمة وهي المعلومات الواسعة للمعالجة الآلية وشبكات المعلومات . وتبنى هذا الاتجاه المشرع الفرنسي واقتدى به المشرع الجزائري كذلك.

[1]- مولود ديدان ، قانون العقوبات، المرجع السابق ، ص120 .
[2]- نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي ، الإقتصادية ، المنشورات الحلبي الحقوقية ، ط1 ،2005، ص233.
[3]- نائلة عادل محمد فريد قورة ، المرجع السابق ، ص.322.

إن جريمة دخول غير مصرح إلى نظام المعالجة الآلية للمعطيات يعد في التشريع الجزائري جريمة شكلية لأنها لا تشترط تحقق النتيجة ، يكفي الوصول إلى المعلومات المخزنة بداخل النظام ، فبمجرد الوصول إليها تقوم الجريمة[1] يرتكب فعل دخول بأية طريقة أو وسيلة كانت لأن المشرع الجزائري لم يحددها[2].

ويستوي أن يتم الدخول بطريق مباشر يستطيع الجاني للوصول إلى المعلومات المخزنة لدى الأنظمة المعالجة الآلية باستخدام شاشة النظام والإطلاع بالقراءة على ماهو مكتوب عليه وباستخدام آلة طباعة مرفقة بجهاز الحاسب الآلي استخراج قائمة البرامج الموجودة داخل النظام المعلوماتي أو بطريق غير مباشر ويكون ذلك بالإلتقاط المعلوماتي بعد إلتقاط المعلومات المتواجدة في الحاسب الآلي والتقاط الإشعاعات الالكترومغناطيسية المنبعثة من الجهاز المعلوماتي[3] .

ب/فعل البقاء:

معنى البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام ، ويتحقق هذا البقاء غير المشروع عند دخول شخص في نظام بتصريح ولكن تجاوز المدة المسموح له بالبقاء ، أو يكون ذلك الدخول خطأ أو سهوا في نظام آخر ولم ينسحب فورا ولا يقطع وجوده ، أو يقوم بطبع نسخة من المعلومات في حين سمح له بالرؤية فقط هنا تقوم جريمة البقاء غير المشروع في نظام المعالجة آليا للمعطيات.[4] يجتمع فعل البقاء مع فعل الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات ، مثل أن لا يكون للجاني حق الدخول ويدخل عن طريق الغش ويبقى عد ذلك ، حيث نصت المادة 394 مكرر من قانون العقوبات الجزائري على فعل البقاء غير المشروع ، على غرار القانون الفرنسي في المادة 1/323 من قانون العقوبات الفرنسي يصعب تطبيق النص في قراءته الأولى لأنه

[1]- نفس المرجع ، ص 324
[2]- أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومه الجزائر ، ط2 ، 2007، ص100
[3]- نائلة عادل محمد فريد قورة ،المرجع السابق ، ص 322
[4]- أمال قارة، المرجع السابق ، ص 110

ينص فقط على الدخول غير مرفق بإدراج الجزء الخاص بالبقاء غير المشروع ومن صياغة النص أصبح يمكن تطبيقه[1].

نظرا لإختلاف الطبيعة القانونية بين فعل الدخول غير المصرح والبقاء غير المشروع كذا يمكن وضعها في نص قانوني واحد حيث يعد فعل الدخول غير مصرح والبقاء غير المشروع جريمة سلبية ومستمرة[2] .

2_الصورة المشددة:

نصت المادة 394 مكرر الفقرة 2 و 3 من قانون العقوبات الجزائري على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل للمعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائف نتيجة التخريب أو التعديل.

إن ظرف التشديد ظرف مادي تربط بينه وبين الجريمة العمدية الأساسية علاقة سببية لكي نقول أن الشرط متوفر.[3] وفي المادة 394 مكرر في الفقرة الأخيرة شدد المشرع عقوبة المحو وتعديل المعطيات كل واحد على حدى تخريب نظام اشتغال المنظومة من جهة أخرى ، وعقوبة هذه الأخيرة أشد للان عقوبة المحو أو التغيير هي ضعف عقوبة الدخول والبقاء غير المشروعين أما بالنسبة للمشرع الفرنسي فجمع بين طرفين في فقرة واحدة وفي عقوبة واحدة في المادة 1/323 قانون العقوبات الفرنسي [4].

ب_:الإعتداءات العمدية على نظام المعالجة الآلية للمعطيات:

نصت على هذه الصورة المادتان 5 و8 من الاتفاقية الدولية للإجرام المعلوماتي ، والمادة 2/323 من قانون العقوبات الفرنسي نصت على أنه " بمجرد إعاقة أو إفساد اشتغال نظام المعالجة الآلية للمعطيات".أما بالنسبة للمشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي

[1]- المرجع نفسه، ص110.
[2]- نائلة محمد فريد قورة ، المرجع السابق ، ص 348
[3]- أمال قارة ، المرجع السابق ، ص 113
[4]- نفس المرجع، ص114

على سير النظام وإكتفى بالنص على الإعتداء العمدي على المعطيات الموجودة داخل النظام ، وهذا راجع إلى تفسير أن الإعتداء على المعطيات قد يؤثر على صلاحية النظام ووظائفه[1].

و إختلف الفقه في الرأي حول ما إذا كان الاعتداء وسيلة أم غاية ؟

فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات ، ومع عدم وجود نص خاص بالاعتداءات العمدية على نظام المعالجة الآلية للمعطيات ، فإن الاعتداءات على سير النظام الناجمة عن الدخول المشروع للنظام تفلت من العقاب ، وتتمثل السلوكات الإجرامية في هذه الاعتداءات في فعل عرقلة أو تعطيل و الإفساد لنظام المعالجة الآلية للمعطيات عن أداء نشاطه العادي والمنتظم منه القيام به[2].

أولا :التعطيل (العرقلة):

إن المشرع لم يشترط الوسيلة التي يتم بها فعل التعطيل قد تكون وسيلة مادية أو معنوية سواء اقترنت الوسيلة المادية بعنف أم لا ، ككسر الأجهزة المادية للنظام أ وتحطيم الاسطوانة ، وتكون معنوية إذا وقعت على الكيانات المنطقية للنظام مثل البرامج والمعطيات بإتباع التقنيات التالية : كإدخال برنامج فيروسي ، استخدام قنابل منطقية تجعل النظام يتباطأ أداءه لوظائفه إلى غيرها من التقنيات.

ثانيا : الإفساد : يقصد بفعل الإسفاد وهو كل فعل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وبالتالي يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.[3]

ج_: الإعتداءات العمدية على المعطيات.

نصت على الاعتداءات العمدية على المعطيات المواد8 ،4، 3من الاتفاقية الدولية للإجرام المعلوماتي[4] كذلك المادة 323 من قانون العقوبات الفرنسي بنصها " كل من أدخل (بطرق الغش المعطيات بنظام المعالجة الآلية للمعطيات أ ومحا أو عدل ، ونصت على الاعتداءات

[1]- نفسه، ص114
[2]- أمال قارة ، المرجع السابق ، ص 113
[3]- علي عبد القادر القهوجي ،المرجع السابق ، ص7
[4]- أمال قارة ، المرجع السابق ، ص 120

تلك المعطيات بعقوبة الحبس تصل إلى 03 سنوات وبعقوبة الغرامة تصل 300 ألف فرنك فرنسي[1] ".

وبالإضافة إلى ذلك نصت المادة 394 مكرر 2 قانون العقوبات الجزائري على الاعتداءات العمدية بنصها " يعاقب بالحبس من شهرين 02 إلى ثلاثة (3) سنوات وبغرامة من 1000000إلى 5000000 دج كل من يقوم عمدا أو عن طريق الغش بما يلي:

تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أومرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

حيازة أو إفشاء أو نشر واستعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[2].

ومن هنا أن نشاط إجرامي لجريمة الاعتداء العمدي للمعطيات يتجسد في صورتين هما:

الصورة الأولى : الإعتداءات العمدية على المعطيات الموجودة

تتجسد هذه الاعتداءات العمدية على المعطيات في ثلاث أفعال هي : الإدخال والمحو والتعديل ، ولتوافر الركن المادي في هذه الجريمة لابد توافر الأفعال الثلاثة ولا يشترط اجتماع هذه الأفعال ، يكفي أن يصدر من الجاني إحدى هذه الأفعال لتوافر ركن المادي[3]

/**الإدخال** : يقصد بفعل الإدخال هو إضافة معطيات جديدة على الدعاية الخاصة سواء كانت خالية ، أم كانت يوجد عليها معطيات من قبل ، ونكون أمام فعل الإدخال في حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة أو التزوير[4].

/**فعل المحو** : يقصد بفعل المحو إزالة جزء من معطيات المسجلة داخل النظام ، وتحطيم تلك الدعامة أو نقل أ وتخزين جزء من معطيات في ذاكرة المختلفة.

---

[1]- المادة 323 من قانون العقوبات الفرنسي ، رقم 1195 97 ، المرجع السابق .

[2]- مولود ديدان ، قانون العقوبات ، المرجع السابق ، ص121 .

[3]- أمال قارة ، المرجع السابق ، ص ، 112

[4]- نفس المرجع ، ص121

/**فعل التعديل** : يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى ويتحقق ذلك عن طريق برامج تتلاعب في المعطيات سواء بالمحو الكلي أو جزئي وهي برامج الفيروسات وهي مختلفة الأنواع والأشكال[1] .

الصورة الثانية : المساس العمدي بالمعطيات خارج النظام.

نص المشرع الجزائري على صورتين للمساس العمدي بالمعطيات خارج النظام ، الصورة الأولى تتعلق بحماية المعطيات من استعمالها في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، والثانية : تتعلق بحماية المعطيات المتحصل غليها من هذه الاعتداءات وذلك في نص المادة 394 مكرر 2 قانون العقوبات المشار إليه سابقا.[2]

ويتضح من خلال هذا النص أن هناك فرق بين الصورتين المنصوص عليهما في المادة 394 مكرر 2 قانون العقوبات حيث أن الصورة الأولى تكون فيها المعطيات وسيلة للارتكاب هذه الاعتداءات ، فالحماية التشريعية هنا تخصها قبل ارتكاب الاعتداءات أما الصورة الثانية فتكون المعطيات هي المحصلة أو نتيجة لارتكاب الاعتداءات الماسة بالأنظمة والحماية التشريعية في هذه الصورة تهدف إلى الوقاية من ارتكاب جريمة أخرى ، تتمثل ف حيازة أو إفشاء أو نشر أو استعمال هذه المعطيات المتحصل عليها من إحدى هذه الاعتداءات لأي غرض كان[3] .

وتجدر الإشارة إلى أن المشرع الجزائري اقتدى بالمشرع الفرنسي الذي أخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير لكن هناك فرق بين نصوص قانون العقوبات الجزائري وقانون الفرنسي حيث أن نصوص العقوبات الجزائري الخاصة بالتزوير الذي يرد على محرر لذلك لا يمكن إقتداء بالمشرع الفرنسي الذي يجعل موضوع التزوير عامة مادية ولهذا الاختلاف لابد تعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي في قانون العقوبات الجزائري.

[1]- محاضرات ألقيت على طلبة ثانية ماستر جنائي ، سنة-2016/2015

[2]- نائلة عادل محمد فريدة قورة ،المرجع السابق ، ص 366.

[3]- أمال قارة ، المرجع السابق ، ص 133.

أولا: مفهوم منتجات الإعلام الآلي : قبل التطرق إلى مفهوم المنتجات لابد توضيح معنى المستند المعالج آليا والمستند المعلوماتي ، فالمستند المعالج آليا في الاصطلاح القانوني هو الدعامة المادية التي تم تحويل المعطيات المسجلة عليها لغة الآلة [1]أما بالنسبة للمستند المعلوماتي ، تعتبر مستندات معلوماتية الأوراق المعدة لتسطير المعلومات عليه في الأقراص الممغنطة التي لم يسجل عليها أي شيء بعد.

ثانيا:مدى خضوع منتوجات الإعلام الآلي لنصوص التزوير:

هل يمكن تطبيق نصوص التزوير في قانون العقوبات الجزائري على الاعتداءات الماسة بمنتوجات الإعلام الآلي ؟ وللإجابة على هذا الإشكال لابد التطرق إلى مايلي[2] :

1_مدى إنطباق وصف المحرر على منتوجات الإعلام الآلي:

إن مفهوم المحرر في نصوص التقليدية يختلف عن مفهومه في مجال المعالجة الآلية للبيانات لأنه يشترط أن يكون شكلا كتابيا وأن يكون منسوبا لشخص معين وأن يحدث المحرر أثاراً قانونية ، فلذلك لايمكن إسقاط معنى المحرر التقليدي على المحرر في مجال المعالجة وذلك لعدم توفر شرط الكتابة فجريمة التزوير عنصر قيامها الكتابة فأي تغيير في الوعاء المعلوماتي لا يعتبر تزويراً لإستيفاء هذا الشرط[3].

حيث أدرج التشريع الجزائري النصوص الخاصة بتزوير المحررات في الماد من 214 إلى 229 من قانون العقوبات التي تشترط المحو لتطبيق جريمة التزوير.[4]

2_مدى خضوع منتوجات الإعلام الآلي للنشاط الإجرامي لجريمة التزوير:

تقوم جريمة التزوير على فعل التغيير الحقيقة القانونية السبية وليست الحقيقة الواقعية المطلقة بمعنى إستبدالها بما يخالفها وإذا إنتفى هذا التغيير إنتفى التزوير معه ، ويقع فعل التغيير من خلال طرق التزوير المادية والمعنوية.ونستخلص إلى أن المشرع الجزائري رغم تداركه من خلال

[1]– أمال قارة ، المرجع السابق ، ص 133–134.

[2]– المرجع نفسه، ص136.

[3]– المرجع نفسه، ص137.

[4]– أمال قارة ، المرجع السابق ، ص 139

القانون 15/04 المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الإعتداءات الواردة على منتوجات الإعلام الآلي ، فلم يستحدث نصا خاصا بالتزوير المعلوماتي ، ولم يتبنى الإتجاه الذي تبنته التشريعات التي عملت على توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث[1].

3_الركن المعنوي:

الركن المعنوي للجريمة المعلوماتية يختلف باختلاف أشكالها وعليه ارتأينا التعرض للركن المعنوي لكل جريمة على حده.

أ_جريمة الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:إن جريمة الدخول والبقاء غير المشروع هي جرائم عمدية تتطلب قصدا جنائيا وذلك بنص المادة 394 مكرر قانون العقوبات الجزائري التي عبرت عن القصد الجنائي بنصها" كل من يدخل أو يبقى عن طريق الغش[2]." ، كما تطرق له المشرع الفرنسي في نص المادة1/323 « بعبارة(FRAUDULUSEMENT)وتعني هذه العبارة أن الفاعل له كامل العلم بأن الدخول أو البقاء غير مشروع«[3] ، ولتوافر القصد الجنائي لابد أن يكون الجاني محيطا علما بكافة عناصر الجريمة وله علم بأن الفعل الذي يقوم به ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات برامج ، وباعتبار محل الحق الذي يحميه المشرع.

بمعنى آخر أنه اتجاه إرادة الجاني إتجهت إلى فعل الدخول أو فعل البقاء و أن الجاني يعلم بأن ليس له الحق في الدخول إلى النظام والبقاء فيه . ولا يتوافر القصد الجنائي إذا كان الجاني يعتقد أن دخوله أو بقاءه داخل النظام مسموح به أي مشروع ، أو كان الجاني يجهل بوجود حظر الدخول أو البقاء ،[4] فإذا اعتقد الفاعل بناءا على أسباب معقولة بأنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي ، دون أن يتجه علمه إلى أنه

[1]– المرجع نفسه، ص140

[2]– مولود ديدان، قانون العقوبات ، المرجع السابق ، ص 120

[3]– نائلة محمد فريد قورة ، المرجع السابق ، ص 366

[4]– أمال قارة ، المرجع السابق ، ص 124.

يقوم بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات، فإن قصد الدخول أو البقاء لا يتوافر فيه[1] أما بالنسبة لنية الغش تبدو من خلال الغش الذي تم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام ، بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام ، وفي الحقيقة أن الدخول و البقاء بالغش لا يتضمن معنى خرق الجهاز الرقابي للنظام ، و إنما يظهر من خلال الولوج دون حق إلى النظام ، و أن الدخول للنظام غير مرخص به[2].

ب_جريمة الإعتداءات على سير نظام المعالجة الآلية للمعطيات: جريمة الاعتداءا على سير نظام المعالجة الآلية للمعطيات هي جريمة عمدية لأن أفعال العرقلة والتعطيل من الأفعال العمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يعتبر ظرف مشددا لجريمة الدخول والبقاء غير مشروع داخل النظام ، وعليه فالقصد الجنائي المفترض ينتج من طبيعة الأفعال المجرمة[3] .

ج_الإعتداءات العمدية على المعطيات:إن جريمة الاعتداءا العمدي على المعطيات جريمة عمدية يتخذ فيها القصد الجنائي بعنصري العلم والإرادة ، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل ، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات ، ويعلم أيضا أنه ليس له الحق في القيام بذلك و أنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته .

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه ، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.[4]

---

[1]– نائلة محمد فريد قورة ، المرجع السابق ، ص 366

[2]– أمال قارة ، المرجع السابق ، ص125

[3]–أمال قارة،نفس المرجع ، ص125.

[4]– نفسه، ص125–126

د_إستخدام المعطيات كوسيلة في إرتكاب الجرائم الماسة بالأنظمة المعلوماتية.

إن هذا الاستخدام يكون عمديا وذلك متمثل في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، ويكون هذا الاستخدام عن طريق الغش فلذلك يتطلب القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش[1].

المبحث الثاني: تجريم ومتابعة الأعمال الإلكترونية.

إن التطور المذهل و المتسرع لتكنولوجيا المعلوماتية و شبكات إتصالها أدى إلى ظهور نمط جديد الا وهو الجريمة المعلوماتية التي وفرت لها العصرنة الوسائل التقية و الفنية كما ساهمت شبكات الإتصال العالمية في عولمة هذا النوع من الإجرام و تنوع الأنشطة الإجرامية مما حتم على التشريعات و بالأخص المشرع الجزائري ملاحقتها وتجريم الأفعال المتعلقة بالمعالجة الألية للمعطيات وكل ما يتعرض له هذا النوع من المعطيات ، فمعظم التشريعات جرمت الأعمال الإلكترونية ولكنها تباينت وإختلفت إختلافا كبيرا وذلك راجع أساسا ألى إختلاف المستوى الرقمي أو التكنولوجي لكل دولة ، و توسع نطاقه و أنواعه فلذلك نصت عليه قوانين الدولة الجزائرية وكرسته في تشريعاتها.وهذا ما سنتطرق إليه من خلال هذا المبحث بتقسيمه إلى مطلبين,الأول يخص الأعمال الإلكترونية و مدى تجريمها في ظل القانون الجزائري و المطلب الثاني نتطرق فيه للأجهزة الحكومية المختصة في متابعة الجرائم المعلوماتية.

المطلب الأول: الأعمال الإلكترونية ومدى تجريمها في القانون الجزائري.

_____نصت المادة 38 من_**الدستور الجزائري** "على القانون أن يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بأمر قضائي".

_____نصت المادة 39 منه " لا يجوز انتهاك حرمة حياة المواطن الخاصة ، وحرمة شرفه، ويحميها القانون ". سرية المراسلات والاتصالات الخاصة بكل أشكال مضمونة.[2]

---

[1]– نفسه، ض126.

[2]–:مولود ديدان ، الدستور ، تعديل نوفمبر 2008 ، دار بلقيس الجزائر ، ص16

كما سنذكر مجموعة من القوانين على سبيل الحصر عملت على تجريم جل الاعمال المتعلقة بالنشطات و الخدمات التي تكون فيها المعطيات معالجة بصفة آلية ومنها:

_في القوانين:

_____قانون رقم20-03 المؤرخ في 2000/08/05 و الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية:

تسارع هذا القانون الى مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان اجراء التحويلات المالية عن الطريق الالكترونيات ذلك ما نصت عليه المادة 87 من هذا القانون بالقول " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني[1] ".

_____نصت المادة84 /2 منه بقولها " تطبق أحكام المادة 89 من هذا القانون عن استعمال حوالات دفع عادية أو الكترونية أو برقية[2] ".

_____نصت المادة 105 الفقرة الأخيرة على أنه " لا يمكن بأي حال من الأحوال انتهاك حرمة المراسلات".

_____المادة 127 رتبت منه جزاء كل من تخول له نفسه أو بحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهك حرية المراسلات بنصها:"كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم بإختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل في اختلاسها أو إتلافها يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30.000دج إلى 500.000 دج. ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق أو يختلس أو يتلف برقية أو يذيع محتواها"[3]، ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.

_____قانون رقم 08-01 : المؤرخ في 2008/1/23والمتم لقانون رقم : 83-01 المتعلق بالتأمينات:

---

[1]- المادة : 87 قانون رقم20-03 المؤرخ في 2000/08/05والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

[2]- المادة2/84 من القانون رقم 08-01 :المؤرخ في2008/01/23 والمتمم للقانون رقم : 83-01 متعلق بالتأمينات

[3]- المادة 127 من نفس القانون.

المادة 6 مكرر 1 نصت على أنه" البطاقة الالكترونية تسلم للمؤمن له إجتماعيا مجانا من طرف هيئات الضمان الاجتماعي وهي صالحة في كل التراب الوطني وهي تقدم لكل مقدم علاج أو مقدم خدمات مرتبطة بالعلاج وهذا الأخير يزود الكترونيا يسمى " المفتاح الالكتروني لهيكل العلاج " حسب نص المادة 65 مكرر[1].

نصت المادة 93 مكرر 2 منه على معاقبة كل من يسلم أو يستلم البطاقة الالكترونية بغرض استعمالها بطريقة غير مشروعة وجاءت كما يلي":دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 100.000دج إلى 200.000 دج. كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهن الصحة [2]."

نصت المادة 93 مكرر 3 على أنه" من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة وهي نفس العقوبة التي تطبق كذلك على كل من قام بتعديل أو نسخ وبطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو مهن الصحة.[3]

_____قانون09 –04 مؤرخ في 14 شعبان 1430 الموافق2009/08/05 للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها:

_نصت المادة 2 منه على مفهوم كل من : الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال. منظومة المعلوماتية ، معطيات معلوماتية ، مقدمو الخدمات، المعطيات المتعلقة بحركة السير و الإتصالات الإلكترونية.

---

[1]– زبيحة زيدان ، المرجع السابق ، ص77 –78.

[2]– المادة 93 مكرر2،من نفس قانون

[3]– المادة 93مكرر3 من نفس القانون

_نصت المادة 4 منه على مراقبة الإتصالات الإلكترونية في الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية.

_نصت المادة 5 منه على القواعد الإجرائية لتفتيش المنظومات المعلوماتية.

_نصت المادة 6 منه على حجز المعطيات المعلوماتية.

_نصت المادة 7 على الحجز عن طريق منع الوصول إلى المعطيات.

_نصت المادة 8 على المعطيات المحجوزة ذات المحتوى الإجرام.

_نصت المادة 9 على حدود إستعمال المعطيات المتحصل عليها.

_نصت المادة 10 على إلتزامات مقدمي الخدمات مساعدة السلطات.

_نصت المادة 11 على حفظ المعطيات المتعلقة بحركة السير.

_نصت المادة 12 على الإلتزامات الخاصة بمقدمي خدمة الإنترنت.

_نصت المادة 13 و 14 على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها[1].

الفرع الأول : :تجريم الأعمال الإلكترونية في قانون العقوبات الجزائري.

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 15-04 المؤرخ في 10نوفمبر 2004 المتمم للأمر رقم 66-165 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات " ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 7ونصت هذه المواد على ما يلي[2] :

_نصت المادة 394 مكرر على جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات محاولة ذلك بنصها " يعاقب بالحبس من ثلاثة أشهر إلى

[1]- القانون09-04 المرجع السابق.

[2]- ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري ، مذكرة مقدمة لإستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار ، الحقوق ، تخصص قانون جنائي ، سنة 2014 2013 ، ص71

سنة وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك . تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج[1] ".

_نصت المادة 394 مكرر 1 على إدخال أو إزالة أو تعديل بطريق الغش معطيات في نظام المعالجة الآلية بنصها " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000دج إلى 2.000.000 دج ، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل الغش المعطيات التي يتضمنها"[2].

_نصت المادة 394 مكرر 2 على أن " يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي :

1-تصميم أو بحث أو تجميع أو توفير أو نشر الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

-نصت المادة 394 مكرر 3 على أنه " : تضاعف العقوبة المنصوص عليها في هذا القسم ، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام ، دون الإخلال بتطبيق عقوبات أشد".

[1]- مولود ديدان ، قانون العقوبات ، المرجع السابق ، ص120

[2]- المرجع السابق، ص121

–نصت المادة 394 مكرر 4 على أنه " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات بالحد الأقصى للغرامة المقررة للشخص الطبيعي".[1]

_نصت المادة 394 مكرر 5 على فعل إشتراك في جريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم فإنه يعاقب بنفس عقوبة المقررة للجريمة في حد ذاتها وذلك بنصها " كل من شارك في مجموعة أو في إتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها".

_نصت المادة 394 مكرر 6 على " مع الإحتفاظ بحقوق الغير حسن النية ، بحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم ، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها[2]"

_نصت المادة 394 مكرر 7 على أنه " يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها [3]".

في عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون رقم 23–06 المؤرخ في 20 ديسمبر 2006 حيث مس ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من القانون15–04 وربما يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث عن الإجرام بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى وشيوع إرتكابه، ليس فقط من الطبقة المثقفة بل من قبل

[1]– نفس المرجع ، ص121.

[2]– نفسه ، ص121.

[3]– .مولود ديدان ، قانون العقوبات الجزائري ، ص120

الجميع بمختلف الأعمار والمستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وإنتشار الأنترنت كوسيلة لنقل المعلومات .[1]

الفرع الثاني: تجريم الأعمال الإلكترونية في قانون الإجراءات الجزائية الجزائري.

نجد أن المشرع نص على تمديد الإختصاص المحلي لوكيل الجمهورية في جرائم الإلكترونية في المادة 37 قانون الإجراءات الجزائية.

ونص على التفتيش في المادة 45 الفقرة7 ، ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة6 ، ونص على إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور من المادة 65 مكرر5 إلى 65 مكرر10 أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليه نفس إجراءات الجريمة التقليدية[2]،و سنتطرق لهذه الإجراءات بالتفصيل في الفصل ثاني من هاته الدراسة.

المطلب الثاني: الأجهزة المختصة في متابعة الجريمة الإلكترونية في التشريع الجزائري.

سنتطرق إلى ثلاث أجهزة حكومية مخصصة لمتابعة هذه الجريمة والمتمثل في:

الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

أنشأت بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها [3]و بموجب المرسوم الرئاسي رقم15-261 المؤرخ في 24ذي الحجة1436 الموافق ل 2015/10/08 يحدد تنظيم و تشكيل الهيئة و كيفيات سيرها.

---

[1]- ماشوش مراد ، المرجع السابق ، ص72.

[2]- مولود ديدان ، قانون الإجراءات الجزائية ، الأمر 02 11 ، دار بلقيس ،الجزائر، ص18 -21-22-33.

[3]- سالم عبد الرزاق ، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية ، بمحكمة سيدي .محمد ، ص11

ومن **مهام الهيئة الوطنية** : تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق عمليات الوقاية ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية.

هناك الحالات التي تسمح بمراقبة الاتصالات الالكترونية لأغراض وقائية كالوقائية من جرائم الإرهاب والجرائم الماسة بأمن الدولة بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد.

والوقاية من إعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني بإذن من السلطة القضائية المتخصصة.

الفرع الثاني : الهيئات القضائية الجزائية المتخصصة:

أ/_إنشاؤها : أنشئت بموجب القانون04 /14 المؤرخ في 10 نوفمبر 2004 المعدل للقانون الإجراءات الجزائية.

تختص الجهات القضائية طبقا للمواد 37- 329 - 40 من قانون إجراءات الجزائية المتخصصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1].

اختصاصا إقليميا موسعا طبقا للمرسوم التنفيذي رقم06 /348 المؤرخ في 2006/01/05.

إمكانية قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني حسب المادة 15 من القانون رقم09/04.

ب/_ توسيع صلاحية الضبطية القضائية:

عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية كما يمكن تمديد الاختصاص المحلي على كامل الإقليم الوطني حسب المادة 16 قانون إجراءات جزائية كما يمكن تفتيش المحلات السكنية وغير السكنية في كل ساعة من ساعات الليل والنهار بإذن من وكيل الجمهورية حسب المادة 47 قانون الإجراءات الجزائية.

[1]- مولود ديدان ، قانون الإجراءات الجزائية ، المرجع السابق ، ص18

ج/_أساليب التحري الخاصة:

إعتراض المراسلات الالكترونية المادة 65 مكرر 5 من قانون إجراءات الجزائية المدرجة بموجب القانون 22-06 المؤرخ في 2006/12/20[1]

-التسرب المادة 65 مكرر 11 من قانون الإجراءات الجزائية[2] .

-تفتيش المنظومة المعلوماتية المادة 5 من القانون رقم09 /04.

-حجز المعطيات المعلوماتية المادة 6 رقم09 /04.

-نسخ المعطيات على دعامة تخزين الكترونية.

-إمكانية منع الوصول إلى معطيات تحتويها المنظومة.

-منع الاطلاع على المعطيات التي يشكل محتواها جريمة[3].

الفرع الثالث : المعهد الوطني للأدلة الجنائية وعلم الجرائم.

أنشأ بموجب المرسوم الرئاسي رقم 04-432 المؤرخ في 2004/12/20 و تم تنظيم المصالح و الأقسام و المخابر فيه بموجب قرار وزاري مشترك مؤرخ في 2007/04/14 و الذي تضمن مصلحة الخبرات الخاصة بالدلائل التكنولوجية، يتكون المعهد الوطني للأدلة الجنائية وعلم الإجرام من احدي عشرة دائرة متخصصة في مجالات مختلفة ، جميعها تضمن إنجازه الخبرة ، التكوين والتعليم تقديم المساعدات التقنية ، البحوث ، الدراسات والتحاليل في علم الجريمة.

دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة و تحليل وتقديم كل دليل رقمي وتماثلي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة . أفراد الدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف ، التقنيات والطرق المستعملة في مختلف الخبرات العلمية ، لإنجاز المهام المنوطة بها ، تنقسم الدائرة إلى ثلاث مخابر وذلك حسب نوع المعلومات سمعية ، بصرية ،والإعلام الآلي.

---

[1]- سالم عبد الرزاق ، المرجع السابق ، ص15-16-18.

[2]- :مولود ديدان ، قانون الإجراءات الجزائية ، المرجع السابق ، ص33

[3]- سالم عبد الرزاق ، المرجع السابق ، ص18-19.

كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل وهذه المخابر هي :

1-مخبر الإعلام الآلي .

2 -مخبر الفيديو.

3-مخبر الصوت[1] .

أولا : مخبر الإعلام الآلي :.من مهامه : تحليل ومعالجة حوامل المعطيات الرقمية الهاتف، الشريحة ، القرص الصلب ، ذاكرة الفلاش.

-تحديد التزوير الرقمي للبطاقات البنكية.

ومن تجهيزاته : محطة ترميم وتصليح الأجهزة والحوامل المعطلة والشبكات الإعلامية(خبرات الإعلام الآلي والتجهيزات البيانية) ،محطة ثابتة ومحمولة لإجراء خبرات الإعلام الآلي.

جهاز إقتناء معلومات الهواتف والحواسب والقاعات التي يحتوي عيها : تتمثل في 7 قاعات (مكتب التوجيه، فصيلة الأنظمة المشحونة ، فصيلة تحليل المعطيات ، فصيلة الهواتف ، فصيلة اقتناء المعطيات ، قاعة موزع وقاعات تخزين)[2] .

ثانيا : مخبر الفيديو : يختص مخبر الفيديو ب مقارنة الأوجه وشرعية الصورة والفيديو وإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد وتحسين نوعية الصورة (فيديو – صورة) بمختلف التقنيات.

ومن تجهيزاته : جهاز فيديو بوكس وحوامل الفيديو الرقمية والممغنطة وحبكات إعلامية (كونيتك ستوديو ، ماكس ثلاثة أبعاد) وموزع لحفظ شرائح الفيديو.

أما بالنسبة للقاعات يحتوي مخبر الفيديو على 4 قاعات (قاعتان لتحليل ، قاعة التخزين وقاعة موزع)[3]

---

[1]- هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ،المعهد الوطني للأدلة الجنائية وعلم الإجرام ، جامعة بسكرة كلية الحقوق ، 2016 ، ص3

[2]- سالم عبد الرزاق ، المرجع السابق ، ص4 -6.

[3]- المرجع نفسهن ص7.

ثالثا : مخبر الصوت: ومن المهامه التي يؤديها : تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ومعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية.

ومن أجهزته : أجهزة الإزدواجية والسماع و حبكات إعلامية معالجة وتحسين التسجيلات الصوتية ، نسخ الأقراص المضغوطة وأجهزة التصليح و التعبير.

أما بالنسبة للقاعات فإنه يحتوي مخبر الصوت على 05 قاعات (03 قاعات للتحليل ، قاعة تخزين وقاعة موزع[1])

الفرع الرابع : المديرية العامة للأمن الوطني.

1/ جوانب التصدي للجريمة الالكترونية : تصدت هده المديرية للجريمة الإلكترونية من مختلف الجوانب منها:

الجانب القانوني : والمتمثل في النصوص القانونية الأتية:

___ القانون 22-06 المؤرخ في 2006/12/10 والقانون 05-03 من القانون المدني .

___ القانون 04-09 المؤرخ في 2009/08/05 وقانون العقوبات المواد من 394 مكرر إلى 394 مكرر 7.[2]

الجانب التنظيمي : ويتمثل في التكوين المتواصل والتخصيص

والتكوين الأولي وتدعيم مخابر الشرطة العلمية.تدعيم المصالح الولائية للشرطة القضائية وتدعيم وهيكلة مصالح الشرطة القضائية للتصدي للجريمة.

الجانب التوعوي:

لم تغفل المديرية العامة للأمن الوطني عن الجانب الوقائي التوعوي يظهر ذلك من خلال برمجتها المديرية العامة لخطوات إستباقية للتصدي للجريمة الالكترونية للتصدي للجريمة الالكترونية عن طريق تنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في

[1]- المرجع السابق، ص8.

[2]- حملاوي عبد الرحمان ، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ، جامعة محمد خيضر بسكرة كلية الحقوق ، 2016 ، ص2

الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

أما في إطار سياسة الشرطة الجوارية التي تنتجها قيادة المديرية ، قام الأمن الوطني بفتح موقع الكتروني خاص بالشرطة الجزائرية على الانترنت يستطيع من خلاله أي مواطن مهما كان مستواه العلمي أو الاجتماعي طرح انشغاله والتبليغ عن أي شيء يثير الشبهة[1] .

الجانب الدولي:

في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم ، لم تغفل المديرية العامة للأمن الوطني استغلال عضويتها الفعالة في هاته الأخيرة تتيح مجالات للتبادل INTERPOL المنظمة الدولية للشرطة الجنائية المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين ، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا

العمل الميداني للتصدي للجريمة الإلكترونية:

عالجت المديرية العامة للأمن الوطني على المستوى الوطني مجموعة من القضايا المتعلقة بالجانب الالكتروني نذكر منها[2]:

السنوات	عدد القضايا المعالجة	عدد الأشخاص المتورطين
2007	**31**	**31**
2008	**06**	**10**
2009	**29**	**21**
2014	**245**	/
2015	**409**	**347**

[1]– حملاوي عبد الرحمان ، المرجع السابق ، ص5–6.

[2]– نفس المرجع، ص6–7.

خلاصة الفصل:

في ظل عصر السرعة والثورة المعلوماتية لا يستطيع أحد أن ينكر أهمية الإنترنت ، لأنها أحد أهم دعائم تكنولوجيا الإتصال والمعلومات ، ولكن هناك على الجانب الأخر أثار سلبية من أهمها ظهور نمط جديد من الجرائم المعلوماتية ، ونتيجة لحداثة هذه الجريمة و غموضها فقد كانت هناك التشريعات المقارنة التي عرفت الجريمة الإلكترونية منذ فترة وبينت كيفية التصدي إلى هذا الشبح ، وكذلك المشرع الجزائري الذي عرفها كذلك وبين خصوصياتها وطبيعتها و العقبات الناتجة عنها كونها حديثة النشأة ، وهذه الجريمة كأي جريمة أخرى لها أركان تقوم بقيامها وتزول بزوال أحدها،وإضافة إلى ذلك تحدثت عن الركن المفترض لهذه الجريمة.

ـــ في هذا الفصل حاولنا قدر المستطاع التطرق لمفهوم الجريمة الإلكترونية في التشريعات المقارنة كما خصصت الشطر الثاني من هذا الفصل للتشريع الجزائري و مدى تجريمه لهذه التلاعبات الرقمية بالمعطيات الحساسة ، بالإضافة إلى الأجهزة المخولة لها قانوناً متابعة لجرائم المعلوماتية واكتساب خبرات و فنيات لمتابعة ومسايرة هذا النوع الفنان من الجناة.

الفصل الثاني

آليات التحقيق في الجرائم المعلوماتية

إذا كانت ظاهرة الإجرام الالكتروني قد أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي، بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم واحترام مبدأ الشرعية والتفسير الضيق للنصوص الجزائية، فقد أثارت في الوقت نفسه مشكلات أكثر في نطاق القانون الجزائي الإجرائي .وتزداد المشكلات الإجرائية في مجال الجرائم الالكترونية بتعلقها في العديد من الأحيان ببيانات المعالجة الآلية وكيانات منطقية غير مادية، ومن ثم يصعب الكشف عنها وإثباتها نظ ا ر للسرعة الفائقة والدقة غير المتناهية في تنفيذها، ناهيك عن إمكانية محوها و تمويه آثارها وإخفاء الأدلة المتحصل منها بسهولة عقب تنفيذها باستعمال تقنيات تكنولوجيا عالية.

ولقد امتد تأثير التقنية المعلوماتية إلى الجانب الإجرائي من القانون الجزائي بشكل أوسع مع مرور الوقت، لأن نصوص هذا القانون صيغت و وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية، ترتكب في عالم محسوس وملموس يؤدي فيه السلوك المادي الدور الأكبر والأهم على خلاف الجريمة الالكترونية التي ترتكب في مسرح إلكتروني افتراضي وغير مادي يختلف كليا عن المسرح التقليدي.

وأمام هذا الوضع أثير التساؤل حول مدى صلاحية تطبيق إجراءات التحقيق التقليدية على جرائم إلكترونية أرتكبت في عالم افتراضي غير ملموس، وهل هذا الأمر يجعل قانون الإجراءات الجزائية قاصراً عن الوفاء بمتطلبات الشرعية الجزائية في مواجهة هذا النمط الإجرامي الجديد وإذا كان الوضع كذلك، فهل يقتضي تدخل المشرع لتعديل قواعد قانون الإجراءات الجزائية القائمة واستحداث قواعد إجرائية خاصة تتناسب والطبيعة المميزة للجرائم الالكترونية، والتي من خلالها يمكن لسلطات تنفيذ القانون تجاوز المشكلات التي تواجهها أثناء عملية البحث والتحقيق في مثل هذه الجرائم.

وعلى اثر هذه التساؤلات سنقسم هذا الفصل إلى مبحثين الأول نتطرق فيه للإجراءات العامة و المألوفة و مدى سريانها على هذا النوع من الجرائم(الجريمة المعلوماتية) والثاني الإجراءات الخاصة و المستحدثة للتحقيق في الجريمة المعلوماتية.

المبحث الأول: الإجراءات العامة والمألوفة ومدى سريانها على الجريمة المعلوماتية

لم يكن لدى الدول خيار آخر للتصدي لظاهرة الإجرام الالكتروني في بداية ظهورها إلا الاعتماد على النصوص الجزائية القائمة بمختلف فروعها الموضوعية و الإجرائية، وذلك تفاديا لإفلات الجناة من العقاب من جهة، وعدم وجود قواعد قانونية أخرى تتلاءم و طبيعة هذه الجرائم المستحدثة من جهة أخرى .ولكن بعد التطور السريع الحاصل في مجال المعلوماتية وما صاحبه من انعكاسات على الجرائم في الوسائل المستعملة لارتكابها والمحل الذي تقع عليه ونوع الجناة الذين يرتكبونها، جعل هذه القوانين غير مواكبة لها، وبالتالي أضحت غير مجدية [1]. ومما لا شك فيه، أن المشرع حينما أراد توسيع نطاق تطبيق إجراءات التحقيق التقليدية لمتابعة الجرائم الالكترونية، فانه يقصد بها تلك الإجراءات التي تثير إشكالات و عقبات عملية تعود إلى خصوصية هذه الجرائم، كالتفتيش و الضبط و المعاينة و الخبرة، والتي هي في حاجة إلى تطوير و تحسين لكي تتناسب مع طبيعتها الخاصة و طبيعة الدليل الذي يصلح لإثباتها[2] أما غيرها من الإجراءات كسماع المتهم أو الشهود، الاستجواب والمواجهة، فإنها مستبعدة نظراً لعدم وجود أية صعوبات في اتخاذها .استرشادا بذلك، فإننا سوف نركز على دراسة الفئة الأولى من إجراءات التحقيق دون غيرها.

المطلب الأول: التفتيش وضبط الأدلة .

قد يتطلب التحقيق تفتيش الشخص المتهم أو منزله أوغيره لضبط الأشياء المتعلقة بالجريمة، و التفتيش كإجراء من إجراءات التحقيق الإبتدائي هو في الأصل من إختصاص سلطة التحقيق،المتمثلة في قاضي التحقيق و النيابة العامة كما تخول بعض المهام الميدانية لرجال الضبطية القضائية من أجهزة الأمن في الحالات المحددة قانوناً.كما يعتبر الضبط م إجراءات

[1]–**محمد قدري حسن عبد الرحمن**، جرائم الاحتيال الالكتروني، مجلة الفكر الشرطي، عدد 79 ، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011 ، ص159

[2]– **محمد قدري حسن عبد الرحمن**، مرجع سابق، ص172

جمع الأدلة ،و هو النتيجة الحتمية التي ينتهي بها التفتيش و الأثر المباشر الذي يفسر عنه،و يقصد بالتفتيش وضع اليّد على الأشياء المتعلقة بالجريمة و التي تفيد في الكشف عن حقائق و الملابسات هاته الأخيرة،بحيث يكون الضبط مأطر بقواعد ونصوص قانونيةلا يجب التعالي عنها و إلا أبطلت الإجراء،و هذا ما سنتطرق إليه بالتفصيل من خلال هذان الفرعين.

الفرع الأول: التفتيش

قد يتطلب التحقيق تفتيش شخص المتهم أو منزله أو غيره لضبط الأشياء المتعلقة بالجريمة، والتفتيش كإجراء من إجراءات التحقيق الابتدائي هو في الأصل من اختصاص سلطة التحقيق، المتمثلة في قاضي التحقيق والنيابة العامة [1] ،إلا أنه يخول استثناء لرجال الضبطية القضائية في حالات محددة قانونا.[2]

وقد أجمع الفقه الجنائي، على أن التفتيش كإجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا.[3]

يتبين من هذا التعريف، أن التفتيش ما هو إلا وسيلة للإثبات المادي، غايته هي ضبط الأدلة المادية الخاصة بالجريمة، مما يجعله يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي، ومعطيات شبكة الانترنت التي ليس لها أي مظهر مادي محسوس في العالم الخارجي ومن هنا يثار التساؤل عن مدى جواز إخضاع هذه المكونات المعنوية لعملية التفتيش؟

---

[1]- إسحاق إبراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائرية، ديوان المطبوعات الجامعية، الجزائر، . 1995، ص105

[2]-من بينها حالة التحقيق في جناية أو جنحة متلبس بها المنصوص عليها في المادة (41) من ق إ ج ج، وفي التحقيق الابتدائي المنصوص عليه في المواد (63) و ما يليها من ق إ ج ج .أنظر أمر رقم 66-155 مؤرخ في 08 يونيو سنة 1966المتضمن قانون الإجراءات الجزائية الجزائري، المعدل و المتمم

[3]- **عبد** الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، .الإسكندرية، 2006، ص192

وللإجابة عن هذا التساؤل، يقتضي الأمر منا الوقوف عند الضمانات و الضوابط التي يجب على المحقق احترامها والتقيد بها قبل وأثناء قيامه بعملية التفتيش، منها ما يتعلق بمحل التفتيش ومن ما هو إجرائي.

أ-محل التفتيش :

يقصد بمحل التفتيش، المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره و خصوصيته، والسر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة، كالمسكن أو سيارة أو رسائل، بالتالي فمحل التفتيش قد يكون أحد المواقع المذكورة مع مراعاة الإجراءات والشروط القانونية المقررة لكل موقع على حدة[1]

وكلما كان المحل في الجرائم الالكترونية هو الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية وحدات(Hard Ware) ، كوحدات المعالجة المركزية (processeur) ، وحدات الإدخال والإخراج و وحدات التخزين أو ما يسمى بوحدة التحكم (Unité De Contrôle) ، ومكونات أخرى منطقيي (Soft Ware كبرامج النظام الأساسية و البرامج التطبيقية و والبيانات المعالجة آليا، كما أن له شبكات اتصالات بعدية سلكية ولاسلكية متواجدة على مستوى المحلي و الدولي، فان الأمر يتطلب منا البحث في مدى قابلية جميع هذه المكونات للتفتيش؟

1- تفتيش المكونات المادية للحاسب

ليس هناك خلاف على أن الولوج إلى المكونات المادية للحاسوب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الالكترونية و مرتكبيها يخضع لإجراءات التفتيش المألوفة، لأن حكم تفتيش هذه الكيانات المادية يتوقف أساسا على طبيعة المكان الذي تتواجد فيه ما إذا كان عاما أو خاصا . فإذا كانت موجودة في مكان خاص كسكن المتهم أو أحد ملحقاته كان له حكمه،

[1]- **بكري يوسف بكري**، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية،2010 .ص.ص80-81.

بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن و ملحقاتها وبالإجراءات والضمانات المقررة قانونا.[1]

ففي القانون الجزائري تشترط المواد من 44 إلى47 من قانون الإجراءات الجزائية للقيام بإجراء تفتيش المسكن في الجرائم المتلبس بها، و هذا بالحصول مسبقا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار بهذا الإذن قبل الدخول إلى المسكن والشروع في التفتيش[2]، على أن يتم التفتيش نهاراً في الفترة الممتدة من الخامسة(5)صباحا إلى الثامنة(8) مساءا وبحضور صاحب المسكن أو ممثله وإن تعذر ذلك استدعى .ضابط الشرطة القضائية القائم بالتفتيش شاهدين من غير الموظفين الخاضعين لسلطته[3]

وينبغي التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة أم أنها متصلة بحواسيب أو أجهزة متواجدة في مكان آخر كمسكن الغير، ففي هذه الحالة يجب على المحقق مراعاة القيود و الضمانات التي يشترطها القانون لتفتيش هذه الأماكن[4]

أما إذ كانت المكونات المادية للحاسوب متواجدة في أماكن عامة، سواء أكانت عامة بطبيعتها كالحدائق العامة والطرق العامة، أم أماكن عامة بالتخصيص كمقاهي الانترنت ومحلات بيع وصيانة الحواسب، فإجراءات تفتيشها تكون وفقا للأصول الخاصة بتلك الأماكن .ويستوي الأمر، بالنسبة للمكونات الموجودة بحوزة شخص ما، فبغض النظر عن صفة هذا الشخص،

---

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، إسكندرية، 2009 ، ص19

[2]– تجدر الإشارة إلى انه إذا تعلق الأمر بتفتيش المساكن في إطار التحقيق الابتدائي، فتشترط المادة (64) من ق إ ج قبل البدء في التفتيش، الحصول على رضا صريح و مكتوب بخط اليد من قبل صاحب المسكن، وإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه.

[3]– ونشير في هذا الشأن، أن المشرع الجزائري بعد التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون رقم 22–06 المؤرخ في 20 ديسمبر 2006 استغنى بموجب الفقرة الأخيرة من المادة (45) و كذا الفقرة الثانية من المادة (47) والفقرة الثالثة من المادة (64) عن تطبيق كل الضمانات المقررة لتفتيش المساكن عندما يتعلق الأمر بالتفتيش في الجرائم الالكترونية، بحيث أصبح من الممكن القيام بتفتيش مسكن المتهم في جريمة الكترونية في أي ساعة من الليل أو النهار ودون حاجة إلى رضائه ولا لحضوره أثناء التفتيش.

[4]– أحمد بن ا زيد جوهر الحسن المهدي، تفتيش الحاسب الآلي وضمانات المتهم، مذكرة لنيل درجة ماجستير في القانون،كلية الحقوق، جامعة القاهرة، 2009 ، ص.ص118 –119.

مبرمجا كان أو عامل صيانة أو موظفا في شركة تنتج برامج الحاسب الآلي، فإن تفتيش هذه المكونات يخضع لأحكام تفتيش الأشخاص، وبالشروط والضمانات القانونية المحددة لذلك[1].

بناءاً على ما سبق، يتضح أن تفتيش المكونات المادية لجهاز الحاسب و ملحقاته مثل لوحة المفاتيح أو الشاشة أو الطباعة أو غيرها من الأشياء المادية المحسوسة، لا يثير أية مشاكل إجرائية أمام سلطات الاستدلال، إذ يسري عليه ما يسري على تفتيش الأشياء والأدوات المادية الأخرى من شروط وضمانات، كمراعاة وقت التفتيش و الإذن بالتفتيش و الأشخاص القائمين بالتفتيش، والأشخاص المطلوب حضورهم عند التفتيش، مع مراعاة الاختصاص المكاني . كما أن أجهزة القضاء المخول لها القيام بإجراء التفتيش سواء بصفة أصلية أو استثنائية يمكنها تفتيش المكونات المادية في الجريمة الالكترونية دون الحاجة إلى أن تكون متخصصة في الجوانب التقنية، مثلها مثل غيرها من المكونات المادية الأخرى.[2]

2- مدى صلاحية مكونات الحاسب المنطقية للتفتيش:

تعرف الكيانات المنطقية للحاسب بأنها" مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات[3] "

وإذا كان الأمر قد انتهى إلى صلاحية مكونات الحاسب المادية كمحل يرد عليه التفتيش، فان امتداد ذلك إلى المكونات غير المادية أو المنطقية هو محل جدل فقهي كبير حول مدى صلاحيتها لأن تكون محلا للتفتيش تمهيدا لضبط الأدلة كون التفتيش وسيلة للبحث وضبط الآثار المتعلقة بالجريمة وتقديمها إلى المحكمة كدليل إدانة، لذلك يثور الشك والتساؤل حول إمكانية اعتبار البحث عن أدلة الجريمة الالكترونية في نظم وبرامج الحاسب نوعا من التفتيش،

---

[1]- **بوكر رشيدة**، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، 2012، ص39

[2]- **فايز محمد راجح غلاب**، الجرائم المعلوماتية في القانون الجزائري و اليمني، أطروحة لنيل شهادة الدكتوراه في القانون، .فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر1 ، الجزائر، 2011 ، ص3

[3]- **عفيفي كمال عفيفي**، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، منشورات الحلبي القانونية، طبعة ثانية ،دمشق، 2007 ، ص61

باعتبار أن البيانات الالكترونية أو البرامج في حدّ ذاتها تفتقر إلى مظهر مادي محسوس في المحيط الخارجي، ويستشعر الفقه صعوبة المسألة بالنظر الى غياب الطبيعة المادية للمعلومات والبيانات، بما يجعلها تتنافى مع الهدف الذي يصبو إليه التفتيش ألا وهو البحث عن الأدلة المادية[1]

وإزاء هذا التشكيك سعى جانب من الفقه إلى إزالته و تجنبه على نحو يسمح بتضمين التفتيش بمعناه التقليدي، البحث والتنقيب في نظم وبرامج الحواسب عن أدلة الجريمة الالكترونية و حجتهم في ذلك هي أنه وإن كانت هذه النظم والبرامج عبارة عن نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية إلا أنها قابلة للتسجيل والتخزين والتحميل على وسائط و دعائم مادية معينة، ولها كيان مادي محسوس من خلال استشعارها وقياسها، لذلك فمن الممكن جدا إخضاعها لقواعد التفتيش التقليدية.

وعلى النقيض من ذلك، يرى جانب آخر من الفقه بأنه من غير الممكن إخضاع مكونات الحاسب المنطقية لقواعد التفتيش التقليدية، لأن هذه القواعد وضعت في وقت لم تكن نظم المعالجة الآلية والحواسيب موجودة وتطبيقاتها غير معروفة، بالتالي فطبيعة هذه المكونات تتطلب إحداث قواعد تفتيش جديدة خاصة بها، أو على الأقل تعديل قواعد التفتيش المألوفة بشكل يجعلها تتلاءم أحكامها مع متطلبات هذه التقنية الجديدة.

ولم يبق المشرع الجزائري مكتوف الأيدي تجاه المتغيرات التي تحدث في عالم التكنولوجيات الحديثة، بل قام بدوره باستحداث نصوص قانونية جديدة أجاز من خلالها تفتيش المكونات المنطقية والمعطيات المعلوماتية للحاسب، ومن بين هذه النصوص المادة 05 من القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تسمح للسلطات القضائية المختصة ولضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة04 من هذا القانون،

[1]- **علي محمود علي حمودة**، مرجع سابق، ص81

الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية.[1]

ثالثا :مدى قابلية شبكات المعلومات المتصلة بالحاسب الآلي للتفتيش:

يقصد بالشبكة المعلوماتية، اتصال جهازين أو أكثر من أجهزة الحاسب الآلي اتصالا سلكيا أو لاسلكيا أو بواسطة الأقمار الصناعية، وقد تكون هذه الأجهزة مرتبطة ببعضها البعض في موقع واحد فيطلق عليها الشبكة المحلية، أو موزعة على عدة أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف أو المجال المغناطيسي فتسمى الشبكة الممتدة أو شبكة الانترنت[2].

لذلك يثير إخضاع شبكات المعلومات المتصلة بالحاسب الآلي لعملية التفتيش صعوبات كبيرة، تتعلق بالدرجة الأولى بالطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، فقد يكون الموقع الفعلي لهذه المعلومات داخل اختصاص قضائي آخر في إقليم دولة واحدة أو في إقليم دولة أو عدة دول أخرى، وهو ما يزيد الأمر تعقيدا باعتبار الشبكة المعلوماتية ممتدة عبر أرجاء العالم [3].ومن هنا يثار التساؤل حول مدى جواز إمداد التفتيش إلى الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا كانت متواجدة في دوائر اختصاص مختلفة؟ ويمكن أن نتصور هنا حالتين مختلفتين هما كالتالي:

---

[1]- أنظر المادة (05) من القانون رقم(09-04)المؤرخ في 14 شعبان 1430 الموافق ل 05 غشت سنة / 2009 والمتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام و الاتصال و مكافحتها، ج ر عدد 47 ، صادر بتاريخ25 شعبان 1430 الموافق ل 16 أوت 2009

[2]يتم الاتصال أو نقل المعلومات بواسطة الشبكية وفق ثلاثة أشكال هي:

ا- اتصال أحادي الجانب(Simplex) وفيه يتم الاتصال بنقل المعلومات في اتجاه واحد فقط من جهاز الحاسب المستفيد إلى الجهاز المركزي .

-اتصال ثنائي النصفي للمعلومات(Half Duplex) وفيه يمكن تبادل الاتصال بين جهازين بإرسال المعلومات، شريطة أن لا يتم الإرسال من الطرفين في وقت واحد.

-اتصال ثنائي كامل للمعلومات (Full Duplex) وفيه يمكن تبادل الاتصال بين جهازين بارسال و استقبال المعلومات في الوقت نفسه.

[3]- **عادل عبد الله خميس المعمري**، مرجع سابق، ص 262.

-الحالة الأولى :اتصال حاسب المتهم بحاسب آلي آخر أو منظومة معلوماتية متواجدة في موقع آخر داخل إقليم الدولة نفسها

تتحقق هذه الفرضية حينما يقوم المتهم بتحويل عبر الانترنت معلومات أو بيانات متعلقة بجريمة إلكترونية من حاسبه إلى حاسب أو منظومة معلوماتية مملوكة للغير متواجدة في مكان آخر وتخزينها فيها . [1] ففي هذه الحالة تواجه سلطات التحقيق مشكلة تجاوز الاختصاص المكاني من ناحية، والاعتداء على حرمة خصوصية الغير من ناحية أخرى،لاسيما في الدول العربية التي لم تفصل قوانينها الإجرائية في هذه المسألة بعد.

ولم يتأخر المشرع الجزائري عن التشريعات الأخرى ، إذ نصّ في المادة 2/5 من القانون رقم 09- 04 لسنة 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه ..." **في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن 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 بذلك.[2]** "

والملاحظ هنا أن تمديد التفتيش إلى منظومة معلوماتية أخرى مشكوك فيها يكتسي طابعا خاصا، فهو يتم عن بعد وبشكل سريع تماشيا مع طابع السرعة الفائقة الذي يجري عليه نقل المعلومات، و واضح أيضا أن الولوج إلى منظومة المعلومات يتم هنا بمجرد الشك أو الاعتقاد بتواجد المعلومات محل البحث داخل هذه المنظومة أو تلك، لذلك أوجب المشرع أن يكتسي هذا الإجراء طابعه الرسمي ويقع تحت طائلة القانون، أن يكون الدخول إلى النظام المعلوماتي المقصود قانونيا ومتماشيا مع مقتضيات حماية الحياة الخاصة للأفراد، وهما الأمرين التي علّق المشرع تحقيقهما على شرط إبلاغ الجهات القضائية المختصة مسبقا بذلك .ولا شك أن الجهات

[1]- **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، 2001 ، ص113.

[2]- انظر المادة 02/05من القانون 09-04 مرجع سابق.

المختصة المقصودة في هذه المادة هي وكيل الجهورية وقاضي التحقيق باعتبارهما الجهة المؤهلة بمنح الإذن بالتفتيش.

ومما يتعين الإشارة إليه أيضا، أن المشرع الجزائري استطاع أن يتجاوز مسألة تفتيش المنظومة المعلوماتية عن بعد بصفة نهائية، حينما وسّع في التعديل لقانون الإجراءات الجزائية اختصاصات ضباط الشرطة القضائية في مجال التحقيق عن الجرائم المعلوماتية، وأجاز إمكانية قيام هذه السلطات بالتفتيش في أي وقت من الليل و النهار و في أي مكان على امتداد كافة التراب الوطني.[1]

-الحالة الثانية :اتصال حاسب المتهم بحاسب آخر أو منظومة معلوماتية متواجدة في إقليم دولة أجنبية

يتحقق هذا الاحتمال حينما يقوم المجرم الالكتروني بتخزين بيانات أو معلومات تفيد إثبات الجريمة في حاسب أو منظومة معلوماتية متواجدة خارج إقليم الدولة التي يقيم فيها، عن طريق شبكة الانترنت بهدف عرقلة سلطات البحث و التحري من الوصول إلى الدليل.

وفي مثل هذه الحالة تواجه سلطات التحقيق مشكلة كبيرة تتمثل في مدى جواز تمديدها إجراءات البحث والتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهت ها المختصة الإذن بالتفتيش والدخول في المجال الجغرافي لدولة أخرى ، وهو ما يسمي بالتفتيش العابر للحدود.

في هذا الإطار خول المشرع الجزائري لسلطات التحقيق والبحث الحق بتفتيش عن بعد الأنظمة المعلوماتية المتصلة أو جزء منها حتى ولو كانت متواجدة خارج الإقليم الوطني، وذلك بنصه في المادة 3/5 من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على انه..." **إذا تبين مسبقا أن هذه المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في**

[1]- أنظر نص المادة47 /2 و3 من قانون الإجراءات الجزائية الجزائري، مرجع سابق

منظومة معلوماتية تقع خارج الإقليم الوطني، فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل."

الملاحظ في هذه المادة، أن المشرع الجزائري لم يسمح للسلطات القضائية المختصة وضباط الشرطة القضائية بتوسيع نطاق التفتيش الالكتروني ليشمل المعطيات المخزنة في منظومة معلوماتية تقع خارج القطر الوطني، إلا في إطار المساعدة القضائية المتبادلة وفي نطاق الاتفاقيات الدولية المبرمة في مجال ملاحقة الإجرام المعلوماتي .كما انه وخلافا للتشريعات سالفة الذكر لم يضع أية حالة استثنائية تسمح بالخروج عن هذا الإطار .ولكن بالمقابل ونظراً للطابع الخاص لهذا النوع من الجرائم وما يتطلبه تعقبها من سرعة، أجاز المشرع لسلطات الاستدلال في حالة الاستعجال تقديم وقبول طلبات المساعدة القضائية الدولية عن طريق وسائل الاتصالات السريعة مثل الفاكس أو البريد الالكتروني شريطة التأكد من صحتها.[1]

و مع هذا ينبغي ألا تفسر المادة 3/5 أعلاه على أنها تمنع وبشكل مطلق تمديد التفتيش عن بعد لتطال نظم معلوماتية متواجدة في إقليم دولة أجنبية دون إذن أو رضا هذه الأخيرة، إنما يمكن السماح لذلك بناء على اتفاقيات دولية ثنائية أو جماعية ، ولكن بالطبع في حدود ما يسمح بها التعاون الدولي ووفقا لمبدأ المعاملة بالمثل بين الأطراف المتعاقدة.

ب- ضمانات التفتيش في البيئة الإ لكترونية:

رغم اعتبار التفتيش من الإجراءات الجوهرية في عملية التحقيق البحث عن حقيقة الجرائم إلا أن معظم القوانين الإجرائية حرصت على إحاطته بجملة من الضمانات القانونية، وذلك تفاديا لتعسف سلطات البحث والاستدلال وما يمكن أن يحدثه من اعتداء على حقوق وحريات الأفراد

---

[1]- وهو ما تضمنته المادة16 /02 من القانون 09-04 بنصها على أنه" **يمكن في حالة الاستعجال قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني، وذلك بقدر ما توفره هذه الوسائل من أمن كافية للتأكيد عن صحتها** ."

وتأكّد في نص المادة 36 من المر 06-09 الصادر في 2006/07/15 المتعلق بمكافحة التهريب على انه ... " **توجه طلبات المساعدة في مجال محاربة التهريب الصادرة عن السلطات الأجنبية كتابيا أو بالطريقة الالكترونية إلى الجهات المختصة ...وفي حالة الاستعجال القصوى، يوجه الطلب شفاهة مع مراعاة تأكيده بوثيقة مكتوبة أو الكترونيا في أقرب الآجال.**"

و حرمة مساكنهم وحياتهم الخاصة من جهة، وإحقاقا لحق الدولة ممثلة المجتمع في كشف غموض الجرائم ومتابعة مرتكبيها وتوقيع العقاب عليهم من جهة أخرى. ويمكن تقسيم هذه الضمانات إلي ضمانات موضوعية وأخرى شكلية أو إجرائية نذكرها على النحو التالي:

-**أولا :الضمانات الموضوعية للتفتيش الإ لكتروني** :تتمثل هذه الضمانات في الشروط الواجب توفرها حتى يكون التفتيش صحيحا، وتتلخص في ثلاثة شروط أساسية هي:

سبب التفتيش، محل التفتيش، والسلطة المختصة بالتفتيش.

أ_ سبب التفتيش :يعتبر عنصر السبب ضمانة قانونية لصحة و مشروعية إجراء التفتيش، يتحقق بوقوع جريمة ما يتم بموجبها توجيه الاتهام إلى الشخص أو الأشخاص المراد تفتيشهم بناء على أدلة أو قرائن قوية تفيد تورطهم في هذه الجريمة، عملا بمبدأ الشرعية الجزائية القاضي بأن" **لا جريمة و لا عقوبة إلا بالنص**"[1] . "إذ بدون وقوع جريمة، و توجيه اتهام إلى شخص أو أشخاص معينين وفقا لأدلة كافية، يكون التفتيش باطلا لانتفاء السبب الذي يبرره وتطبيقا لما سبق، فإن سبب التفتيش في الجرائم الالكترونية لا يتحقق إلا بتحقق العناصر الثلاثة التالية:

- **وقوع جريمة الكترونية تحمل وصف جناية أو جنحة:**

لا يجوز لهيئات التحقيق مباشرة إجراءات التفتيش إلا بعد التأكد من الوقوع الفعلي لجريمة الكترونية نص عليها القانون في نصوص التجريم والعقاب، وأي تفتيش في جريمة محتملة الوقوع مستقبلا ولو أيقنت التحريات والدلائل الجدية على أنها ستقع بالفعل يعدّ إجراء غير مشروع مآله البطلان.[2]

كمالا يكفي وقوع جريمة الكترونية للقول بمشروعية إجراء التفتيش طبقا للقواعد العامة،

---

[1]- **خالد ممدوح إبراهيم**، .مرجع سابق، ص209

[2]– نشير إلى أن المشرع الجزائري خرج عن هذه القاعدة من خلال المادة (05) من القانون 09-04 التي تجيز إمكانية اللجوء إلى تفتيش النظم المعلوماتية للوقاية من جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة (04) من القانون نفسه.

بل لابد أن تحمل هذه الجريمة بمنظور القانون وصف جناية أو جنحة [1] ، ويستثنى من ذلك المخالفات بسبب ضعف خطورتها التي لا تستحق انتهاك حرمة الحياة الخاصة للأشخاص وسرية اتصالاتهم وحرمة منازلهم من أجلها.[2]

والجدير بالذكر، أن مسألة وقوع الجريمة من عدمها تثير مشكلة كبيرة عندما يتعلق الأمر بتفتيش جرائم الحاسب الآلي وشبكات المعلومات، خاصة في الدول التي لم تسّن حتى الآن قوانين تصنف فيها هذه الجرائم، وتحدد وصفها القانوني، عناصر أو أركان كل جريمة وكذا العقوبات المقررة لها، مع العلم أن إجراء التفتيش لا يكون مشروعا إلا إذا بني على سبب جدي يتمثل في الوقوع الفعلي للجريمة، وأن وقوع هذه الأخيرة من عدمه يتوقف أساسا على مدى تحقق أركانها مجتمعة [3].فعلى سبيل المثال، ما ا زلت العديد من الجرائم المتعلقة بنظم المعالجة الآلية وشبكة الانترنت خارج نطاق التجريم في التشريع الجزائري مثل جرائم الاعتداء على المواقع الالكترونية و حجبها، وتدميرها، وجرائم الاستغلال الجنسي للأطفال وغيرها من الجرائم الإباحية، وتبعا لذلك فان اتخاذ أي إجراء من إجراءات التحقيق إزاء هذه الجرائم بما في ذلك التفتيش، قد يكون مصيره البطلان طالما لم يرتكز على سبب مقبول قانونا، ناهيك عمّا تتطلبه الإجراءات التقنية في حالة النص على تلك الجرائم من نصوص مع حداثتها.[4]

- **اتهام شخص أو أكثر بمساهمته في ارتكاب الجريمة الإ لكترونية:**

يشترط لقيام سبب التفتيش إلى جانب وقوع جريمة الكترونية تحمل وصف جناية أو جنحة، أن تتوفر في حق الشخص المراد تفتيشه أو تفتيش حاسبه أو مسكنه دلائل كافية توحي إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة بوصفه فاعلا أصليا أو ثانويا، مما يستوجب اتهامه بها . ومن هنا كان عدم اكتشاف قاضي التحقيق لهوية المتهم في الشكوى ضد مجهول سببا

[1]- وهذا تصديقا للمادة (66)من قانون الإجراءات الجزائية التي تنص على أنّ " **التحقيق الابتدائي وجوبي في مواد الجنايات .أما في مواد الجنح فيكون اختياريا ما لم يكن ثمة نصوص خاصة"...**

[2]- **نبيلة هبة هروال،** مرجع سابق، ص . 232

[3]- **هلال عبد الله احمد،** تفتيش نظم الحاسب الآلي وضمانات المتهم ألمعلوماتي، دار النهضة العربية، القاهرة،1997 .ص121

[4]- **رشاد خالد عمر،** المشاكل القانونية و الفنية للتحقيق في الج ا رئم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، 2013 .، ص69

لحفظ ملف القضية وإصداره لأمر بأن لا وجه للمتابعة وقد أجمع الفقه الجنائي على أن المقصود بالدلائل الكافية بصفة عامة هو " الشبهات المستمدة من الواقع والقرائن التي تنبئ عن اقتراف الشخص جريمة من الجرائم"[1]. أما في الجرائم الالكترونية فيقصد بها" مجموعة من المظاهر أو الإمارات المعينة القائمة على العقل والمنطق والخبرة الفنية والحرفية للمحقق والتي ترجح نسبة الجريمة الالكترونية إلى شخص معين باعتباره فاعلا أصليا أو شريكا."

وعلى هذا الأساس فسبب التفتيش في البيئة الالكترونية لا يتوقف على وقوع جريمة من الجرائم الالكترونية فقط، إنما لابد أن يكون ذلك الوقوع مقترنا بنسبتها إلى شخص أو أشخاص معينين إما بصفتهم فاعلين أصليين أو شركاء.[2]

- **توافر إمارات قوية توحي إلى وجود أدلة مادية تفيد في كشف الجريمة:**

لا يكفي وقوع جريمة من نوع جناية أو جنحة منصوص عليها في القانون، وتوجيه الاتهام إلى شخص أو أشخاص معينين بمساهمتهم في ارتكابها لقيام سبب التفتيش في الجرائم الالكترونية و إنما ينبغي أن تتوافر كذلك لدى المحقق أدلة قوية و قرائن كافية على وجود لدى شخص المتهم أو في الموقع المراد تفتيشه أجهزة أو أدوات استعملت في الجريمة أو أشياء متحصل منها، أو أية معلومات أو بيانات أو مستندات إلكترونية تفيد في استجلاء الحقيقة ويتم الحصول عادة على هذه القرائن والإمارات من خلال مختلف التحريات الجدية التي تجريها سلطات الضبط في مرحلة الاستدلال، بعدما يتم إخضاعها لتقدير السلطة المختصة بإصدار الإذن بالتفتيش التي تتأكد من مدى توفر هذه القرائن لمصداقية كافية تبرر اللجوء إلى إجراء التفتيش وينطبق على هذه الضمانة ما قيل في سابقتها بأنها لا تجدي في مجال الجرائم الالكترونية، بخلاف ما هي عليه في الجرائم التقليدية لأن التوصل إلى قرائن أو إمارات قوية كسبب لقيام

---

[1]- هذا ما نصت عليه المادة (163) من قانون الإجراءات الجزائية الجزائري " **إذا رأى قاضي التحقيق... انه لا توجد دلائل كافية ضد المتهم أو كان مقترف الجريمة مازال مجهولا، اصدر أمراً بأن لا وجه لمتابعة المتهم**"

[2]– وهو ما يستشف من المادة 44 من قانون الإجراءات الجزائي الجزائري بنصها على أنه " **لا يجوز لضباط الشرطة القضائية الانتقال الى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا**"...

التفتيش في جريمة الكترونية ليس بالأمر الهين، نظراً للصعوبات الكثيرة والعقبات الجمّة التي تواجه سلطات التحري والاستدلال في ذلك، كنقص خبرتها في تقنيات التحري في العالم الالكتروني الافراضي، مقابل ما تتسم به تلك الأدلة من طبيعة معنوية يمكن إخفاؤها، تغيرها وإتلافها بكل سهولة وبسرعة فائقة [1].وهو ما قد يشكل دافعا كافيا لإنتفاء سبب التفتيش الذي يعتبر شرطا جوهريا لصحة إجراء التفتيش.

ب_محل التفتيش :يشترط كذلك لصحة و مشروعية التفتيش في الجرائم الالكترونية أن ينصب على محل، ويقصد بالمحل هنا كل المكونات المادية والمعنوية وشبكات الاتصال المتعلقة بالوسائل الالكترونية.[2] وكما أسلفنا الذكر، فالمحل في الجرائم الالكترونية لا يكون قائما بذاته، بل يكون إما مقترنا بمكان معين كمسكن المتهم أ وبشخص معين مالك أو حائز كما هو الشأن في الحاسب المحمول أو الهاتف النقال، لذلك قبل مباشرة التفتيش يجب مراعاة طبيعة المكان الذي تتواجد فيه الوسائل الالكترونية المراد تفتيشها وكذا الضمانات القانونية المحاطة به، لأن حكم تفتيش هذه الوسائل يتوقف غالبا على طبيعة المكان الذي تتواجد فيه.

ويشترط في المحل الذي يقع عليه التفتيش، أن يكون معينا ويكون مما يجوز تفتيشه، فأما الشرط الأول، فهو نتيجة منطقية للمحافظة على حقوق وحرمات وحريات الأفراد، لذا لا يمكن القيام بتفتيش كل الحواسيب المتواجدة في شركة ما أو الحواسيب المحمولة أو الهواتف النقالة الخاصة بكل أفراد العائلة الواحدة وأما الشرط الثاني، فلأن القانون يستثني من التفتيش بعض الأشخاص و الأماكن مثل أشخاص ومساكن وسيارات أعضاء السلك الدبلوماسيوأعضاءالمجالس النيابية[3] ، وكذا مكاتب المحامين لتمتعهم بالحصانة [4] ، وعليه فأي

---

[1]- **رشاد خالد عمر**، مرجع سابق، ص 130

[2]- **علي محمود علي حموده**، مرجع سابق، ص94 وما يليها.

[3]-ارجع في هذا الشأن المادتين 29 و 30 من اتفاقية فيينا للعلاقات الدبلوماسية لسنة 1961 وكذا المادة (126) من القانون رقم 16 -01 مؤرخ في 6 مارس 2016 ، يتضمن التعديل الدستوري الجزائري، ج.ر عدد 14 ، صادر في 7 مارس 2016.

[4]- ا رجع المادة (45) من قانون الإجراءات الجزائية الجزائري، مرجع سابق

تفتيش لأجهزة الحواسيب أو الوسائل الالكترونية الأخرى الموجودة بحوزة هذه الفئة من الأشخاص أو في منازلهم أو على متن سياراتهم يعد منافيا للقانون و مآله البطلان.

كذلك الحال بالنسبة للتفتيش عن بعد عبر شبكات الاتصال أو التفتيش الالكتروني الذي لا يستلزم الاعتداء المادي لحرمة المكان أو الشخص المراد تفتيشه ، فهو يخضع لقواعد الحصانة مثله مثل التفتيش المادي، لان الاعتداء المعنوي على الحياة الخاصة يرتب عادة الآثار نفسها التي يرتبها الاعتداء المادي أو اخطر منها، وذلك نظراً للكم الهائل من المعلومات والبيانات التي تحويها الوسائل الالكترونية الشخصية، والتي يسهل الولوج إليها والإفشاء عنها والاعتداء على سريتها.

وتجدر الإشارة في هذا الشأن، إلى أن المشرع الجزائري استحدث نصوصا قانونية سمح من خلالها لسلطات التحقيق تفتيش الأنظمة المعلوماتية، أو جزء منها، والمعطيات المخزنة بتلك الأنظمة، وجعلها محلا للتفتيش الالكتروني، كما وسّع نطاق هذا المحل، بحيث لم يعد قاصراً على تفتيش الأجهزة الالكترونية تبعا لتفتيش المكان والأشخاص، بل جعله يمتدّ ليشمل التفتيش عن بعد داخل النطاق الإقليمي للدولة إلى نهاية طرفية أخرى التي يمكن الدخول إليها من المنظومة الأولى وذلك كلما استدعت ضرورة التحقيق إلى ذلك.[1]

ج_السلطة المختصة بالتفتيش: لكي يكون التفتيش في الجرائم الالكترونية أو غيرها من الجرائم صحيحا و منتجا لأثاره، لابد أن يتم من طرف سلطات التحقيق الأصلية،[2] مع مراعاة الاختصاص المحلي الذي يتحدد عادة إما بمكان وقوع الجريمة وإما بمكان إقامة المتهم أو مكان القبض عليه[3].

---

[1]– رجع المادة (05)من القانون رقم 09–04 المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق

[2]– يقصد بسلطات التحقيق الأصلية، السلطات القضائية التي تملك صلاحية مباشرة التحقيق بنفسها(أي بقوة القانون) ولا تحتاج إلى تفويض من غيرها.

[3]- تنص المادة (40) من ق إ ج ج " **يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على احد هؤلاء الأشخاص حتى ولو كان سبب القبض قد حصل لسبب أخر."...**

إلا أنه استثناءاً، يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية و ذلك وفقا للشروط و الإجراءات المنصوص عليها في القانون[1] ، وفي هذه الحالة يشترط لصحة إجراء التفتيش الذي يقوم به رجال الضبطية أن يكون بناء على إذن بالتفتيش صحيح صادراً من هيئة مختصة .وفي غياب هذا الإذن، أو عدم صحته تصبح عدم مشروعية التفتيش أمراً مؤكدا.[2]

وفي نطاق تفتيش الأجهزة الالكترونية يثار التساؤل حول ما إذا كان يجب تحديد محل التفتيش في الإذن بالتفتيش تحديدا دقيقا، كتحديد نوع الجهاز الالكتروني أو إحدى مكوناته مثل : (الذاكرة، الوحدة المركزية، القرص الصلب..) أو ملحقاته (كالطابعة ، جهاز المسح الضوئي (scanner)، الذي سوف يرد عليه التفتيش دون غيره، أم انه يكفي الحصول على الإذن بتفتيش المكان الذي تتواجد فيه تلك الأجهزة حتى يشملها جميعها أو بعبارة أخرى هل يجوز لضابط الشرطة القضائية بمقتضي الإذن بتفتيش مسكن المتهم الولوج إلى الأجهزة الالكترونية التي تصادفهم فيه والتغلغل في منظومتها المعلوماتية للبحث عن أدلة إثبات يمكن أن تكون محل ضبط.

والجواب هو أن موقف المشرع الجزائري إزاء هذه المسألة غير واضح وغير حاسم، لأن بالعودة إلى القواعد الخاصة بالتفتيش المذكورة في قانون الإجراءات الجزائية فهي تتعلق بالتفتيش التقليدي الذي ينصب عادة على الفضاءات والمكونات المادية وما في حكمها كالمسكن وملحقاته[3] ، أما في القواعد المتعلقة بالتفتيش الالكتروني الواردة في القانون رقم 09-04، فالمشرع لم يحسم أمره .وإنما اكتفى فقط بالإشارة إلى ضرورة قيام جهات التحقيق بإعلام السلطة القضائية المختصة مسبقا قبل تمديد التفتيش إلى منظومة معلوماتية أخرى مرتبطة بالجهاز المأذون بتفتيشه.[4]

[1]- راجع المادة 06/68 و المواد من 138) إلى (142 من قانون الإجراءات الجزائية الجزائري، مرجع سابق
[2]- ا رجع نص المادة (44) من قانون الإجراءات الجزائية الجزائري، مرجع سابق
[3]- رجع المادة (44) وما يليها من القانون الإجراءات الجزائية الجزائري، مرجع سابق.
[4]- انظر نص المادة (05) من القانون رقم(09-04) المرجع السابق.

ومن خلال هذا السكوت و طبقا لمبدأ حرمة الخصوصية التي يحميها المشرع، نفهم بأن المشرع الجزائري يميل إلى عدم جواز الولوج إلى النظام المعلوماتي وما يمكن أن يحتويه من معلومات و بيانات سرية وخصوصية الأشخاص، لتفتيشه دون إذن خاص من السلطة القضائية المؤهلة، ومؤدى ذلك أن ضابط الشرطة القضائية يحتاج في الغالب لتفتيش منظومة معلوماتية إلى **إذنين بالتفتيش**، الأول يخص المسكن الذي يتواجد فيه الجهاز الالكتروني، والثاني يتعلق بتفتيش مكونات الجهاز أو المنظومة المعلوماتية في حد ذاتها أو على الأقل يحتاج إلى **إذن واحد** يسمح بتفتيش الجهاز الالكتروني الخاص بالمتهم ومسكنه معا.

وعلى ضوء هذا الإبهام، يتعين على المشرع الجزائي الجزائري التدخل و سنّ نصوص قانونية واضحة تفصل في هذه المسالة، والحل في أ رينا هو الأخذ بما ذهبت إليه معظم تشريعات الدول المتقدمة، والمتمثل في جواز تفتيش مسكن المتهم وكل الأجهزة الإلكترونية بمكوناتها وملحقاتها وملفاتها المتواجدة فيه، مع إمكانية تمديد التفتيش عن بعد على جناح السرعة إلى أية منظومة معلوماتية أخرى مرتبطة بها، كل ذلك بموجب إذن بتفتيش واحد.

ثانيا-الضمانات الشكلية للتفتيش الإلكتروني:

إن الغرض من إحاطة التفتيش بضمانات شكلية إلى جانب الضمانات الموضوعية هو ليس تحقيق مصلحة القضاء في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة وضمان مشروعية هذه الأخيرة فقط ، إنما تعتبر كذلك بمثابة سياج أمني لحماية الحقوق والحريات العامة الفردية. ومع هذا فتطبيق تلك الضمانات في مجال التفتيش الالكتروني من شأنها أن تتحول إلى عقبات تحول دون تحقيق الهدف من إجراء التفتيش بدلا من كونها ضمانات في مجال التفتيش التقليدي وهو ما سوف نبرزه عند دراسة هذه الضمانات كل واحدة على حدى:

1-احترام الميقات الزمني لإجراء التفتيش:

إن فرض قيود زمنية لإجراء التفتيش يعدّ ضمانة إجرائية مهمة جدا لحماية الحريات والحقوق العامة للأفراد من أي اعتداء ، نجد أن المشرع الجزائري وضع قيودا زمنية على تفتيش المنازل

وما في حكمها، ولم يسمح به بمقتضى المادة (47) من قانون الإجراءات الجزائية إلا في الوقت المحصور بين الساعة الخامسة صباحا و الثامنة مساء[1] ، وفي الوقت نفسه أقرّ حالات استثنائية أجاز فيها الخروج عن هذا الميقات ليصبح إجراء التفتيش في أية ساعة من ساعات الليل و النهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها في المواد من (342) إلى (348) من قانون العقوبات المرتكبة في أماكن معينة، وفي حالة الرضى الصريح لصاحب المسكن وقد اشتمل هذا الاستثناء التفتيش في الجرائم الالكترونية، بحيث استغنى المشرع الجزائري نهائيا عن شرط الميقات الزمني وسمح لرجال الضبطية القضائية بإجراء التفتيش في مثل هذه الجرائم في كل ساعة من ساعات الليل و النهار كما جاء في الفقرة الثالثة من نص المادة (47) ق إ ج... " عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة... أو **الجرائم الماسة بالمعالجة الآلية للمعطيات** و... **فانه يجوز إجراء التفتيش...في كل محل سكني او غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية.**"

أعتقد أنّ استغناء المشرع الجزائري عن هذا الشرط بخصوص التفتيش في الجرائم الالكترونية راجع من جهة، إلى فطنته وإدراكه للطبيعة المميزة لهذه الجرائم من حيث إمكانية ارتكابها في أي وقت، وأدلة الإثبات فيها غير مرئية وسهلة المحو والإتلاف، بالتالي فتأخير التفتيش إلى الموعد القانوني وفق المبدأ العام قد يكون سببا في ضياع الأدلة ومن ثم عرقلة سير التحقيق . ومن جهة أخرى، إلى تراجع أهمية هذا الشرط أو الضمانة مع ظهور تقنية "**التفتيش عن بعد** " والذي يمكن إجراؤه في أي وقت ومن أي مكان في العالم، مع العلم أن تحديد الوقت قد يختلف من دولة إلى أخرى، فالوقت الذي يكون نهاراً في دولة معينة مثل كندا قد يكون ليلا في الجزائر.

[1]- انظر المادتين (1/47و2) و (82) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

2_إجراء التفتيش بحضور المتهم أو من ينوب عنه:

حرصا على تضييق نطاق الاعتداء على حرمة الحياة الخاصة للأفراد وحرمة مساكنهم المحفوظة قانونا، يسهر المشرع على عدم جواز إجراء التفتيش إلا بحضور المتهم أو من يقوم مقامه معتبرين ذلك من القواعد الأساسية التي يترتب عن مخالفتها البطلان.

وغني عن البيان أن الشخص الذي يستوجب القانون حضوره في الأصل هو المتهم وهذا الشرط يكون قائما حتما في تفتيش الأشخاص على اعتبار التفتيش يقع عليه[1] ، وفي هذا الإطار لم يشترط القانون حضور الشهود عند تفتيشه .أما عندما يتعلق الأمر بتفتيش المساكن وما في حكمها، فالمشرع الجزائري يقضي لإجراء التفتيش بحضور المشتبه به أو من يمثله ولم يتطلب حضور الشهود إلا في حالة تعذر حضور هؤلاء، وهو مقتضىالمادة1/45 ق إ ج بأنه " **إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في ارتكاب جناية فيجب أن يحصل التفتيش بحضوره، وإذا تعذر عليه الحضور وقت إجراء التفتيش، فإن ضابط الشرطة القضائية ملزم بأن يكلّفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته**".[2]

أما فيما يخص التفتيش في الجرائم، فالمشرع و إقراراً منه بخصوصية جرائم الاعتداء على نظم المعالجة الآلية للمعطيات وما يتطلبه الأمر من بسط نوع من السرية أثناء جمع الدليل التقني فيها، عاد بموجب الفقرة الأخيرة من المادة نفسها[3] ، واستثنى هذه

الجرائم من تطبيق أحكام المادة السابقة، وأصبح بإمكان الضبطية القضائية إجراء التفتيش في الجرائم المعالجة الآلية دون التقيد بشرط حضور المتهم أ ومن ينوب عنه أو حتى الشهود.

---

[1]- **بوكر رشيدة**، مرجع سابق، ص 414

[2]– انظر المادة (45)و المادة (83) من القانون الإجراءات الجزائية الجزائري، مرجع سابق

[3]– تنص الفقرة الأخيرة من المادة 45 من ق إ ج ج على أنه " **لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...بإستثناء الأحكام المتعلقة بالحفاظ على السر المهني.**"

وفي أ رينا، ما فعله المشرع الجزائري باستبعاد تطبيق أحكام المادة 45 ق إ ج على الجرائم المعلوماتية هو الصواب، وذلك نظراً للطبيعة التقنية المحضة التي تتميز بها هذه الجرائم و طبيعة الدليل الذي تتطلبه لإثباتها و ما يقتضيه من السرعة في استخلاصه قبل فقدانه والذي يتطلب أحيانا عدم إعلام المتهم بعملية التفتيش.

3_تحرير محضر التفتيش:

إضافة إلى الضمانات المتعلقة بالميقات الزمني للتفتيش والأشخاص المطلوب حضورهم، يشترط كذلك أن يحرر محضر بالتفتيش تدون فيه كل الخطوات والإجراءات المتخذة أثناء عملية التفتيش، وما أسفر عنها من أدلة لكي يكون حجة على الجميع.

ولا يستوجب القانون شكلا أو شروطا خاصة في محضر التفتيش، بل يكفي أن يتوفر فيه ما تستوجبه القواعد العامة في المحاضر عموما، كالكتابة باللغة الرسمية، تاريخ تحريره، توقيع محرره، ويتضمن كافة إجراءات التفتيش[1].

ومن الشروط الجوهرية التي ينبغي مراعاتها في محضر التفتيش، وجوب استعانة المحقق بكاتب يتم اصطحابه لتحرير المحضر و تدوين ما تم من إجراءات و التأشير عليه تحت طائلة البطلان ، وهو ما نصت عليه المادة 2/68 من قانون الإجراءات الجزائية الجزائري على أنه:

"وتحرر نسخة من هذه الإجراءات وجميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل"، وأكدت عليه المادة 79 من القانون نفسه بنصها على: " **يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضراً بما يقوم به من إجراءات**[2] "

ولا يختلف محضر التفتيش في مجال الجرائم الالكترونية عن غيره في محضر الجرائم التقليدية

---

[1]- **فايز محمد ا رجح غلاب**، مرجع سابق، ص 338

[2]– أنظر الفقرة 2 من المادة (68) و المادة(79) من ق.ا.ج.ج، مرجع سابق.

سوى انه بالإضافة إلى الشكليات السابقة لابد من إحاطة القائم بالتفتيش في الجرائم الالكترونية بتقنية المعلوماتية الرقمية، أو استعانته بأهل الخبرة الفنية والاختصاص في هذا المجال ليساعده في صياغة و تحرير محضر يغطي كل الجوانب الفنية للتفتيش.

وأشير إلى انه بالإضافة إلى شرط تحرير محضر التفتيش، حرص المشرع على تضمين نصوص تمنع فيها الاطلاع أثناء التفتيش على الأشياء والأوراق المختومة التي تمس الأسرار الشخصية للعائلة، وتفرض على القائم بالتفتيش اتخاذ الاحتياطات الضرورية لتفادي انكشاف مثل هذه الأسرار.

حيث نص القانون الجزائري على هذه الضمانة في المادة 84 من ق إ ج على الشكل التالي : "إذا اقتضى الأمر أثناء إجراء تحقيق و جوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع عليها قبل ضبطها مع مراعاة ما تقتضيه ضرورات التحقيق و ما توجبه المادة3/83 ق إ ج.

ويجب على الفور إحصاء الأشياء و الوثائق المضبوطة ووضعها في أحراز مختومة .ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا..."[1]

وأعتقد أن هذا القيد المتعلق بعدم جواز الاطلاع على الأشياء والأوراق المختومة أثناء التفتيش يمكن تطبيقه على محتوى أنظمة المعالجة الآلية للبيانات المشفرة والمحمية فنيا ضد الاطلاع غير المرخص، لان العلة من تقرير هذا القيد بالنسبة للأوراق المختومة هي نفسها بالنسبة لبيانات أنظمة المعالجة الآلية المشفرة، ألا وهي المحافظة على الأسرار الخاصة بالشخص المراد تفتيشه[2] ، فكما يضفي الختم والتغليف والتحريز على تلك الأراق مزيداً من السرية و الحماية فكذلك التشفير يضفي السرية على البيانات و برامج المعالجة الآلية.

[1]– انظر المادتين 83–84 من قانون الإجراءات الجزائية الجزائري، مرجع سابق

[2]– **محمد فريد رستم**، أصول التحقيق في جرائم الحاسوب، مرجع سابق، ص428

الفرع الثاني: ضبط الأدلة

يعتبر الضبط من إجراءات جمع الأدلة، وهو النتيجة الطبيعية التي ينتهي إليها التفتيش والأثر المباشر الذي يسفر عنه، ويقصد به وضع اليدّ على الأشياء المتعلقة بجريمة وقعت والتي تفيد في كشف الحقيقة عنها و عن مرتكبيها، و وضعها في أحراز مختومة وتقدم إلى الجهة القضائية المختصة كدليل إثبات[1] .

وتحصيل الأدلة في الجرائم الالكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته و الأقراص الصلبة و الأقراص والأشرطة الممغنطة و الطابعة و البرامج اللينة والمراشد، البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الانترنت مثل المودم، ففي هذه الحالة فلا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها لإجراءات الضبط والتحريز التقليدية[2] .وقد يرتبط الدليل الالكتروني بالمكونات المعنوية للحاسب، كمختلف البرامج والبيانات المعالجة آليا والمراسلات والاتصالات الالكترونية التي يجري تبادلها عبر شبكة الانترنت والبريد الالكتروني، وهنا تثير الطبيعة المجردة لهذه المكونات جدلا فقهيا واختلافا تشريعيا كبيراً حول مدى إمكانية ضبطها وفقا لقواعد الضبط المألوفة، مع العلم أن الضبط بمفهوم هذه الأخيرة لا يرد إلا على الأشياء المادية.[3]

تنبه المشرع الجزائري بدوره لهذا القصور، وتبني في القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05 إجراءات مستحدثة خاصة بضبط وتحريز المعطيات والبيانات المعلوماتية

---

[1]- **خالد عياد الحلبي**، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر و التوزيع، عمان، 2011 .، ص17

[2]– راجع في ذلك المواد 45 و 46 و 84 من القانون الإجراءات الجزائية الجزائري.

[3]– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، دار الفكر الجامعي، الإسكندرية، 2006،. ص 218

وغيرها من الأدلة الرقمية بما يتناسب وطبيعتها اللامادية، تحت عنوان" **حجز المعطيات المعلوماتية** [1] " وخصص لها عددا من المواد التي نذكرها على النحو التالي:

نصت المادة (06)على أنه " **عندما تكتشف السلطات التي تباشر التفتيش في منظومة معلوماتية معطيات محزنة مفيدة في الكشف عن الجرائم أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية**"...

أضافت المادة (07)فيما يخص الحجز عن طريق منع الوصول إلى المعطيات بأنه "**إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (06)أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.**"

أما بخصوص المعطيات المحجوزة ذات المحتوى المجرم فنصت الماد (08)على أنه " **يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل .باستعمال الوسائل التقنية المناسبة لذلك**[2] "،بالإضافة إلى هذه التدابير، وضع المشرع الجزائري على عاتق مقدمي خدمات الانترنت جملة من الالتزامات تساعد سلطات التحقيق على ممارسة مهام التفتيش و الضبط على الكيانات المعنوية للحاسب الآلي عندما تستدعي ذلك ضرورة التحقيق[3] .

---

[1]– تجدر الإشارة إلى أن المشرع الجزائري استعمل في هذا القانون 09–04 عبارة " **الحجز saisie**" للتعبير عن عملية الضبط كإجراء من إجراءات التحقيق بدلا من عبارة " **الضبط**"**saisie** التي اعتاد على استعمالها في قانون الإجراءات الجزائية، و هذا الاختيار أمر مقصود، لأن عبارة " **الحجز** "لا تتعارض مع الضبط المادي التقليدي من جهة، وهي أكثر تلاؤما و تماشيا مع الطبيعة المنطقية واللامادية للأدلة الالكترونية و الرقمية من جهة أخرى.

[2]- أنظر المواد (6-7-8) من القانون 09-04 المؤرخ في 2004/08/05يتضمن القواعد الخاصة للوقاية من الج ا رئم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

[3]– **أحمد مسعود مريم**، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال في ضوء القانون 09–04 مذكرة لنيل شهادة ماجستير في القانون الجنائي، كلية قصدي مرباح بجامعة ورقلة،2013، ص103.

ويتضح من خلال النصوص السابقة، بأن المشرع الجزائري أدرك خطورة الجرائم الالكترونية وأن الجزائر ليست بمنأى عنها، فقام بتلافي القصور الموجود في قانون الإجراءات الجنائية فيما يخص ضبط الكيانات المنطقية للحاسب أسوة بالاتفاقية الأوروبية وتشريعات الدول المتقدمة، واعتقد أن موقفه هذا ليس اختياراً بل حتمية لا مفرّ منها ما دام

أنه قد أجاز تفتيش هذه الكيانات كما – رأينا سابقا – وهو ما يقتضي بحكم المنطق القانوني والعقلي ضرورة إباحة ضبطها لأن الغاية من التفتيش هو ضبط كل ما يفيد في كشف الحقيقة، بالتالي لا يعقل أن ينظم المشرع مرحلة من م ا رحل التحقيق ويغفل عن الأخرى.

والجدير بالذكر، أنه رغم محاولة استحداث قواعد وإجراءات جديدة تواكب الطبيعة الخاصة للأدلة المستمدة من البيئة الرقمية والالكترونية وتسمح بضبطها وتحريزها بشكل سليم، إلا أن الواقع يثبت وجود صعوبات كثير ما ا زلت تواجه عملية ضبط هذه الأدلة ولعل أهمها مايلي:

–الحجم الهائل للمعلومات المعالجة الكترونيا التي تحتويها الشبكة المعلوماتية الواجب فحصها من طرف المحقق للوصول إلى استخلاص البيانات التي تصلح كأدلة جنائية وضبطها.[1]

–قد يكون محل الأدلة الالكترونية جزء لا يمكن عزله عن المنظومة أو الشبكة المعلوماتية،مما يتعين بالضرورة ضبط النظام أو الشبكة بأكملها لتحصيل الدليل، وهو الأمر الذي يترتب عنه التوقف عن العمل لمشروعات صاحب النظام مدة زمنية قد تطول أو تقصر، ففي هذه الحالة يضطر المحقق لإعمال مبدأ التناسب الذي يقضى باقتصار الضبط على الأدلة الضرورية التي تفيد كشف الحقيقة ولها علاقة بالجريمة.[2].

كما قد تكون هذه الأدلة في شبكات أو أجهزة تابعة لدولة أجنبية، مما يعيق أجهزة التحقيق الوطنية من الوصول إليها وضبطها دون تعاون ومساعدة أجهزة التحقيق التابعة لتلك الدولة [3]ومن الصعوبات التي تعيق الوصول إلى ضبط الدليل الرقمي كذلك، تلك الأحزمة الأمنية

[1]- **حسام محمد نبيل الشنراقي**، مرجع سابق، ص.ص 671–672

[2]– **فايز محمد ا رجح .غلاب**، مرجع سابق، ص34

[3]– **أحمد بن ا زيد جوهر الحسن المهندي**، مرجع سابق، ص224.

المفروضة من طرف مستخدم النظام للحد من الدخول والاطلاع على البيانات التي يحتويها هذا النظام .وما يزيد الأمر تأزما هو عدم معرفة المحقق الجنائي لكلمات السر أو شفرات المرور أو شفرات ترميز البيانات و ما يقابله من حق المشتبه به في الصمت و عدم الكشف عن هذه الشفرات تطبيقا لمبدأ عدم اتهام الشخص لنفسه.[1]

المطلب الثاني: المعاينة.

تعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة، ومن أهم إجراءات التحقيق على الإطلاق، نظراً لما يمكن أن توفره من أدلة إثبات، وتزداد أهميتها أكثر إذا تعلق الأمر بالجرائم الالكترونية، باعتبارها من الجرائم المستحدثة وغير مألوفة بالنظر إلى الطبيعة الخاصة للسلوك الإجرامي فيها، والذي يستوجب ابتكار تقنيات جديدة مناسبة بالمعاينة في هذا المجال وهو ما سنبحثه في الفرعيين التاليين:

الفرع الأول : مفهوم المعاينة

تعرف المعاينة بأنها إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في كشف الحقيقة [2].فهي بذلك تعد من إجراءات التحقيق الابتدائي التي يجوز لسلطات التحقيق اللجوء إليها من تلقاء نفسها كلما رأت في ذلك ضرورة لإجلاء الحقيقة، أو بناء على طلب من الخصوم[3] .والأصل أن تجرى المعاينة بحضور أطراف الدعوى الجزائية، غير أنه

[1]– نص المشرع الجزائري على حق المشتبه به في الصمت وعدم الإدلاء بأي إقرار أثناء التحقيق في المادة(100)من قانون الإجراءات الجزائية، انظر في هذا الشأن أيضا : **لجنة منع الجريمة والعدالة الجناية**، مرجع سابق، ص13.

[2]– **فهد عبد الله العبيد العازمي**، الإجراءات الجنائية المعلوماتية ، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق بجامعة القاهرة، 2012 ، ص 266.

[3]– تنص المادة (79)من قانون الإجراءات الجزائية الجزائري على "**ويجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها**"...

يجوز للمحقق إجرا ؤها في غيابهم نظراً لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة[1].

وللمعاينة أهمية بارزة في مجال التحقيق الجنائي لكونها مصدراً أصيلا من مصادر الأدلة المادية والفنية الراسخة والثابتة التي تكون دائما محل ثقة سلطات التحقيق و القضاء، ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة، فهي ناطقة بما أتاه شاهد على ما .فعله الجاني دون انحياز أو تعديل أو نقصان[2]

وحتى تأتي المعاينة بثمارها وتفي بأغراضها المنشودة، أحاطها المشرع بجزاءات جنائية توقع على كل من يتجرأ ويقوم بإحداث تغييرات على حالة الأماكن التي وقعت فيها الجريمة أو ينزع شيء منها قبل الإجراءات الأولية للتحقيق القضائي، باستثناء ما إذا كانت تلك التغييرات أو نزع الأشياء للسلامة والصحة العمومية أو ستلزمها معالجة .الضحية وفي هذا الشأن تنص المادة 43 من قانون الإجراءات الجزائية الجزائري على " :يحظر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، وإلا عوقب بغرامة من 200دج إلى 1000 دج."

وتتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة، وإذا كانت الجريمة واقعة على المكونات المادية للأجهزة الالكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص الممغنطة ، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعدّ أدلة مادية تدل على وقوع

[1]– **محمد أبو العلاء عقيدة** " التحقيق و جمع الأدلة في محال الجرائم الالكترونية "ص . 07 مقال منشور في الموقع التالي : www.osamabahar.com. تاريخ الإطلاع 2019/02/17. 16:44.

[2]– **عفيفي كامل عفيفي**، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة والقانون، دار النهضة العربية، القاهرة، 2013 ، ص44.

الجريمة وانتسابها لشخص معين، ثم ضبطها وضعها في أحراز مختومة تقدم للنيابة العامة [1].

أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الالكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الانترنت فيكون الانتقال للمعاينة هنا افتراضيا أو الكترونيا، ويمكن للمحقق إجراء المعاينة الافتراضية أو الالكترونية بالولوج والانتقال إلى مسرح الجريمة عبر الانترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه، أو من خلال مقهى الانترنت أو إحدى مقرات مزود .خدمات الانترنت.

ويلتزم المحقق عادة قبل البدء في المعاينة الالكترونية بجملة من التدابير الفنية والتحفظية التي تساعده في القيام بمهامه على أحسن وجه هي كالتالي:

-الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد ومواقع الأجهزة الالكترونية وشبكاتها وسائر ملحقاتها والنهايات الطرفية المتصلة بها المتوقع مداهمتها[2] .

-توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة التي يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتامين وحفظ المعلومات.

-تأمين التيار الكهربائي بشكل لا يتم التلاعب او التخريب عن طريق قطع التيار او تعديل الطاقة الكهربائية.

-التأكد من خلو المحيط الخارجي لمسرح الجريمة الالكترونية من أية مجالات لقوى مغناطيسية او ممرات اتصالات التي يمكن أن تتسبب في محو البيانات المسجلة أو إتلاف الآثار الأخرى للجريمة.[3]

-التحفظ على محتويات سلة المهملات ومستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.

---

[1]- **ياسر محمد الكومي محمود أبو حطب**، الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشاة المعارف، الإسكندرية، 2014 .، ص243

[2]- **ياسر محمد الكومي محمود أبو حطب**، مرجع سابق، ص 245

[3]- **سرحان حسن المعيني**، مرجع سابق، ص.ص41-42

إعداد فريق من المتخصصين و أهل الخبرة في مجال تكنولوجية الإعلام الآلي للاستعانة بهم عند الحاجة[1].

الفرع الثاني :نطاق إعمال المعاينة

يعتمد المحقق الجنائي لإجراء المعاينة الإلكترونية بحثا عن الأدلة الرقمية على فحص مجموعة مصادر الدليل في البيئة الإلكترونية التي ارتكبت فيها الجريمة المعلوماتية والمتمثلة عادة في مكونات أجهزة الحواسيب الخاصة بالجاني والمجني عليه وملحقاتها وكذا أنظمة الاتصال بالانترنت.

-**أولا:معاينة مكونات الحاسب** :تعتبر الحواسيب مصدراً غنيا بالأدلة الإلكترونية خاصة الحواسيب الشخصية التي تعد بمثابة أرشيف لسلوك الأفراد ونشاطاتهم ورغباتهم، لذلك فان عملية فحص هذه الحواسيب تمثل نقطة البداية في الكشف عن خفايا الجريمة الإلكترونية باعتبار هذه الأجهزة وسيلة تنفيذها أو محل وقوعها .والمعروف أن الحاسب الآلي يقوم في تركيبته على ثلاثة عناصر أساسية هي، القطع الصلبة (Hardware) والقطع المرنة او البرمجيات(Software)) وكذا المعطيات أو المعلومات أو البيانات (données Informatiques) وهو العنصر الذي يتوزع بين القطع الصلبة و البرمجيات[2] .لذلك فمعاينة هذا الحاسب يستلزم الفحص المادي والمعنوي لكل هذه العناصر نظراً للإرتباط الطبيعي بين بعضها البعض.

وقد تعتمد عملية الفحص هنا على طريقتين أساسيتين، الأولى هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكوناته وتقديم تقرير كامل إلى طالب الفحص، ومثل هذه العملية تتطلب من القائم بها معرفة تقنية ومهارة فنية عالية .أما الطريقة الثانية، فهي الفحص بواسطة

[1]- **محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، مرجع سابق، ص114.

[2]- **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص1009.

حاسب آلي آخر أو أجهزة تقنية عالية للبحث في جزئية او جزئيات عبر الحاسب[1] .وعادة ما تشمل عملية فحص مكونات الحاسب الآلي العناصر التالية:

1-معاينة القرص الصلب :يتم معاينة القرص الصلب للحاسب الآلي بالفحص الجزئي أو الكلي للبيانات الرقمية ذات الطابع الثنائي المتواجدة بداخله، والتي تتميز بعدم التشابه .الذي يتكون منه تفصيل هذه البيانات [2] فيما بينها رغم وحدة الرقم الثنائي(0-1) ولتحقيق ذلك، يقوم المحقق بنزع القرص من الحاسب الم ا رد فحصه بكل عناية وحذر من أي ارتجاج أو اصطدام بأي شيء تفاديا لإتلافه أو تعطيله أو فقد أية بيانات، ثم يقوم بفحص .وتحليل النسخ التي تصدر من القرص بنفسه أو بواسطة الخبير المختص[3]

والفحص الجزئي للقرص الصلب يسمح للمحقق التعرف على محتوى البيانات ثنائية الرقم التي يؤدي التعامل معها إلى الكشف عن القيمة الاسترادادية للبيانات المخزنة فيه سواء كانت محتويات مكتوبة أو مصورة أو مسجلة .وكذا استرجاع ما تم حذفه من بيانات ومعلومات وبرامج بالاستعانة ببرمجيات مخصصة لهذا الأمر .وكمثال على ذلك، نذكر حالة البحث في ملفات النسخ الإضافية التي تحتفظ بها نظم التشغيل من كل صفحة تمّ الولوج اليها عبر الانترنت، أو الملفات الخاصة بالإنزال(Download File) الموجودة في نظم التشغيل والتي مهمتها استقبال الملفات التي يتم تحميلها على الحاسب من خارجه عبر الانترنت[4] .

فعملية فحص القرص الصلب إذا، تساعد المحقق عادة على جمع البيانات والمعطيات المخزنة فيه بشكل آلي أو إ رادي التي كان يستخدمها الجاني، من معلومات أو صفحات وعناوين الانترنت أو رسائل البريد الالكتروني المرسلة والمتلقاة وكذا مجموعة البرامج الجاهزة

[1]- **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص1101

[2]- **حسين بن سعيد بن يوسف الغافري**، المرجع سابق، ، ص426.

[3]- **خالد ممدوح إبراهيم**، الجرائم المعلوماتية، مرجع سابق، ص 215

[4]- **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص102.

المتخصصة التي استعملها المشتبه فيه(، للتواصل مع أصدقائه) شركاء المشتبه فيه في الجريمة، ثم تحليليها و تحديد تاريخها من ثم مقارنتها مع وقائع الجريمة لاستخلاص الدليل.[1]

وتجدر الإشارة إلى أن عملية فحص القرص الصلب كي تكون مجدية لا بد من مراعاة مسائل عدة منها الكيفية التي يتم ضبط الحاسب و فصل القرص الصلب عنه، ومهارة الشخص القائم لاستخلاص البيانات دون العبث بمحتوياتها، وكذلك مراعاة شرط سلامة الحاسب الآلي، الذي يعني صحة حركة القطع الصلبة فيه لتجنب رفض المحكمة الاعتداد بالدليل المنبثق عنه، فشرط سلامة الحاسب مطعن رئيسي على كل دليل تم الحصول عليه، لذا يجب دائما التأكد من سلامة الحاسب في أداء وظيفته قبل أي إقرار بمشروعية الدليل من حيث التحصيل[2] .

2_معاينة البرمجيات :يتّبع المحقق في هذه العملية طريقتين هما، الفحص الداخلي للبرمجيات والفحص الخارجي لها .فأما الفحص الداخلي، فيتم من خلال البحث عن البناء المنطقي للبرمجية بما يكشف عن وجود مجهودا تجديديا في إعداده للعمل حين إنزاله في جهاز الحاسب الآلي، وذلك بتتبع الخطوات المنطقية التي تعبر عن هذا الجهد ولعل أكثر ما يسعى المحقق الوصول إليه في إطار الفحص الداخلي هو مصدر الملفات الموجودة داخل البرمجيات التي تفيد في ترتيب حدوث الجريمة الالكترونية، والتعرف على الكيفية التي تم الإعداد لها . علما أن النسخ عبر الانترنت يختلف عن النسخ باستخدام برمجيات المعالجة فالأول نسخ عبر العالم الافتراضي أما النسخ الثاني فيتم لاستخدام ،(Word Processing) .مصنف متداول في العالم المادي.[3] أما الفحص الخارجي، فيتم بواسطة البحث عن البناء المنطقي للبرمجية للتأكد مما إذا كانت هذه الأخيرة منسوخة أم لا، ثم مقارنة النسخة الأصلية بالنسخة محل الاشتباه للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة[4]

---

[1]- **علي حسن الطوالبة** ، مشروعية الدليل الرقمي المستمد من التفتيش الجنائي دراسة مقارنة ص 07 ، بحث منشور على موقع الانترنت التالي : www.policemc.gov.bh/reports/2009/...7.../633843953272369688.doc

[2]– المرجع نفسه، ص8.

[3]– **حسين بن سعيد بن يوسف الغافري**، مرجع سابق، ص427.

[4]– **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 131.

والجدير بالذكر هنا، أنه ينبغي عدم التعويل كثيراً على الدليل المحصل من معاينة برمجيات الحاسب الآلي عن طريق الفحص الداخلي أو الخارجي، لأن برمجيات الحاسب ليست ذات نظرة مثالية وغالبا ما يشوبها عيب أو قصور و لو جزئي في أداء وظيفتها، وهذا القصور من شأنه أن يؤثر في الحاسب فيجعله محل شك تهتز معه قيمة الدليل، كما له أثره في عملية تقويم الدليل المستمد من البرمجية ذاتها.

3-معاينة النظام المعلوماتي :لا يحتوي النظام المعلوماتي للحاسب على معلومات مكتوبة كما يعتقد معظم الناس، إنما يتكون من بيانات ثنائية الرقمية يتم إيداعها في الحاسب الآلي في شكل تخزين، ثم يقوم الحاسب بمعالجتها آليا و إبرازها على هيئة معل ومة موحدة كلما تم استدعاؤها من قبل مستخدم الحاسب، أما إذا لم يتم استدعاء معلومة محددة فان بياناتها تضل مخزنة على حالتها الأصلية داخل الحاسب[1] .لذلك فالمهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر الموجهة من طرف مستخدم الحاسب والاستجابة لها.

وعليه، فالمقصود بمعاينة النظام المعلوماتي للحاسب هو قيام المحقق بفحص و ضبط كافة المعلومات المخزنة في ذاكرة تخزين الحاسب على شكل ملفات والتي يمكن استردادها عبره بأية حركة استردادية ممكنة، ما دام موضوعها يشكل جريمة[2] .

وقد أكد المختصّون في مجال تكنولوجية الإعلام و الاتصال بان نظام التخزين في ذاكرة الحاسب يعد مصدراً مهما للدليل الالكتروني، لأنه يسمح للحاسب الآلي بالاحتفاظ بصفة آلية بنسخة كاملة مما اطلع عليه المشتبه فيه من مواقع و صفحات الانترنت أثناء إبحاره عبر العالم الافتراضي، كما أن هناك أنظمة وبرمجيات جديدة فور ربطها بذاكرة التخزين يمكن لها تتبع كل خطوات المشتبه فيه ومساره عبر شبكة الانترنت واسترجاع ما تم تصفحه لفترات طويلة من

[1] -**حسين بن سعيد بن يوسف الغافري**، السياسة الجنائية...، مرجع سابق، ص430

[2] - **خالد ممدوح إبراهيم**، مرجع سابق، ص222

الزمن قد تصل إلى ستة أشهر كاملة، ولو قام المشتبه به .بإغلاق الاتصال بشبكة الانترنت و حذف كل ما قام نظام التشغيل بتخزينه.[1]

ومع ذلك، فلا ريب أن كثرة التعامل بالحاسب الآلي والتردد عليه من أكثر من شخص يؤدي حتما إلى تكاثر محتوى النظام المعلوماتي مما يترتب عنه صعوبة فحصه بالنظر الى الحجم الضخم والكم الهائل من المعلومات الممكن تخزينها فيه[2] .ناهيك عن تنوع أشكال وأساليب تخزين البيانات، التي يصل مداها إلى حدّ تخزين البيانات بشكل آمن في الحاسب بواسطة نظام التشغيل او نظام إخفاء البيانات المعلوماتية، مما يتعذر الكشف عن الملفات التي تحتوي عناصر إجرامية حتى في حالة البحث الآلي للحاسب عنها، ويحول دون وصول المحقق إليها.

ثانيا معاينة أنظمة الإتصال بشبكة الانترنت :أحيانا لا يكفي معاينة مكونات الحاسب وحدها لاستخلاص الدليل الالكتروني، إنما يتطلب من المحقق فحص أنظمة اتصال الحاسب بشبكة الانترنت كذلك .ويقصد بأنظمة اتصال بشبكة الانترنت بالمفهوم الإجرائي، تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة الاتصال بالانترنت، لذلك فعملية فحص أو معاينة هذه الأنظمة يشمل بالأساس فحص مسار الانترنت أو ما يعرف ببروتوكول الانترنت، والنظام الأمني للشبكات، وكذا فحص الخادم.

1_فحص مسار الانترنت :تتم هذه العملية من خلال تتبع الحركة التراسلية للنشاط الممارس عبر الانترنت باستخدام نظام فحص الكتروني يسمى علم البصمات المعاصر أو علم بصمات القرن الواحد والعشرين،[3] وما يتم التوصل إليه بعد ذلك، هو عنوان رقمي وهو عبا رة . (Internet protocole adresse)أو باختصار (IP Adresse) يطلق عليه عن بروتوكول لعنونة البيانات والمواقع في شبكة الانترنت يتم بمقتضاه التعرف على الحاسب الآلي الموصول بشبكة الانترنت من خلال عناوين عددية ، علما أن لكل حاسب آلي عنوانه الوحيد الخاص به

---

[1]- **عمر محمد أبو بكر بن يونس**، مرجع سابق،ص1018.

[2]– **علي عدنان الفيل**، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي .الحديث ، القاهرة ، 2012 ، ص33.

[3]– **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص998

(IP Adresse)، و كل عنوان (IP) مكون من جزأين الأول يشمل أرقام الشبكة و الثاني يشمل أرقام مزود الخدمة. فالحاسب الآلي فور اتصاله بالانترنت يقوم تلقائيا باختيارالبروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات.

يشتغل البروتوكول (IP) بشكل متزامن مع بروتوكول آخر يدعى بروتؤكول التحكم بالنقل (Tramsmission control protocol TCP)للاتصال بين عدة أجهزة من الحواسيب طورت أساسا لنقل البيانات الرقمية عبر شبكة الانترنت ، ويرتكز البروتوكولان معاً (TCP/ IP) على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Pachets) بين مختلف أنظمة الاتصالات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها[1] .

وحزمة المعلومات، هي جزء من ملف معلوماتي حجم مصغر ثابت تحمل رقما خاصا ومعلومات تعريفية بكل من المرسل والمرسل إليه، وعند كل اتصال تتم قراءة جهة المقصد أو المرسل إليه ثم تتم إعادة الحزمة المارة عبرهما إلى الوصلات التالية الأقرب إلى جهة المقصد النهائية.[2]

تبرز أهمية الاستعانة بالمعلومات والمصادر والعناوين التي يمكن أن يحتويها نظام (TCP/ IP) للتحقيق عن الجريمة الالكترونية، في كونها تدّل بصفة جازمة عن مصدر الجهاز المستخدم في ارتكاب الجريمة، وتحدّ د الأجهزة التي أصابها الضرر من جراء الفعل الإجرامي و نوعية النشاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة، كما أنها تساعد بالاطلاع على جميع المراسلات و المحادثات ، وكل ما تمّ نقله أو تبادله أو معالجته من بيانات عبر شبكة الانترنت، وكذا الكشف عن مصدرها وتتبع مسارها إلى غاية نقطة وصولها، من ثم تحديد هوية المرسل والمرسل إليه اللذين قد يمثلان أول المشتبه فيهم.[3]

---

[1]- **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 382

[2]– **ممدوح عبد الحميد عبد المطلب** "استخدام البروتوكول(TCP/ IP) في بحث و تحقيق الجرائم على الكمبيوتر ،مقال منشور عبر الموقع التالي: www.arablawinfo.com تاريخ الاطلاع:2019/04/04 ، 11:22.

[3]– **حسين بن سعيد بن سيف الغافري**، مرجع سابق، ص421

لذلك أثبتت تقنية تتبع الحركة العكسية لمسار الانترنت جدواها للكشف عن المجرمين في أكثر من جريمة الكترونية.

1-فحص الخادم(serveur) : يعتبر الخادم من أهم نظم الاتصال بالانترنت، فهو جهاز الكتروني كبير مهمته ضمان حركة الاتصال بمواقع و صفحات الانترنت، ثم استقبالها وتخزينها فيه على هيئة رقمية .من هنا فان للخادم وضيفة مزدوجة، إذ يتولى من جهة ربط مستخدمي الانترنت بالمواقع والصفحات التي يريدون الاطلاع عليها، ويقوم من جهة ثانية باستضافة هذه المواقع والصفحات وتخزينها على شكل بيانات رقمية وهو ما يرشحه لأن يكون مصدراً غنيا جدا للأدلة الالكترونية الرقمية، يطلق عليه البعض موقع تخزين المعطيات الرقمية(Lieu de stockage des données numeriques).[1]

وللقيام بعملية فحص الخادم ينبغي على المحقق الالتزام بالضوابط المقررة لإجراء المعاينة وفق القانون المنفذ في النطاق الإقليمي الذي يوجد فيه، واتخاذ كافة التدابير التقنية والفنية اللازمة للمحافظة على مسرح الجريمة من أي عبث أو تعديل، مع ضرورة الاستعانة بأحدث وسائل وآليات الفحص الالكتروني[2] . بالإضافة إلى لزوم الأخذ بعين الاعتبار مبدأ الغاية من البحث و التفتيش وبالتالي خلق مفارقة بين الخادم العام وبين الخادم الخاص بفئة تراسلية معينة غير أن الأمر لا يقف عند هذه النقطة لأن تقنية الانترنت تجعل من الممكن القيام بفحص الخوادم عن بعد باستخدام تقنيات حديثة في هذا المجال تجعل التوصل إلى محتوى حركة الاتصال بالخادم ذات مغزى، وربما أفضل من مجرد القيام بفحص الخادم المادي.[3]

المطلب الثالث: الخبرة التقنية

أدى التطور التقني الهائل في عالم تكنولوجيا الإعلام والاتصال إلى احداث تغيير كبير في المفاهيم المتعلقة بالدليل الجنائي، مما أدى بدوره إلى تعاظم دور الإثبات العلمي للدليل وإعلان

[1]- **حسين بن سعيد بن سيف الغافري**، مرجع سابق، ص424.

[2]- **أحمد مسعود مريم**، مرجع سابق، ص75.

[3]- **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص1007.

انضمام الخبرة التقنية إلى عالم الخبرة القضائية، وأصبحت الاستعانة بخبراء مختصين لفحص الأدلة التقنية وتقويم عملية الإثبات الرقمي وتحليل الجريمة الالكترونية أمراً ملحا لا يمكن الاستغناء عنه إذ لا يعقل أن يفصل القاضي في قضايا تقنية المعلومات دون أن يستند إلى الخبرة التقنية في هذا المجال تحقيقا لمبدأ معروف هو" مبدأ التخصص" وإلا كان حكمه معيبا ومطعونا فيه .

الفرع الأول :دور الخبرة التقنية

تعرف الخبرة الفنية بأنها إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء، من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع جريمة أو نسبتها إلى المتهم [1]. فهي الإستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها بمعرفة فنية و دراية علمية لا تتوفر لديه.

وللخبرة الفنية دور كبير في إثبات الجريمة الالكترونية، لأنها تنير الدرب لسلطات التحقيق والقضاء و سائر الجهات المختصة بالدعوى الجزائية للوصول إلى الحقيقة و تحقيق العدالة الجنائية[2] ، لذلك ومنذ تفشي الج ا رئم الالكترونية، تستعين سلطات التحقيق والإستدلال و المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال التقنية الالكترونية من اجل كشف غموض الجريمة وتجميع أدلتها والتحفظ عنها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق.155

وقد تزايدت الحاجة إلى الخبرة الفنية للتحقيق عن الجرائم الالكترونية في الآونة الأخيرة نظراً للتحولات التكنولوجيا التي مست وسائل الإعلام والاتصال، اذ تعددت أنواع ونماذج الحواسيب وشبكات الاتصال بينها، وأصبحت العلوم والتقنيات المتعلقة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتشعبة، والتطورات في مجالها سريعة و متلاحقة لدرجة قد

[1] – **عبد الناصر محمد محمود فرغلي**، مرجع سابق، ص24.

[2] – **بوكر رشيدة**، مرجع سابق، ص424.

يصعب على المتخصص تتبعها واستيعابها .بل يمكن القول انه لا يوجد حتى الآن خبير يملك معرفة متعمقة في سائر أنواع الحاسبات و برامجها و شبكاتها، أو قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها .لذلك ترك المشرع للمحقق الحرية الكاملة وفي أية مرحلة من مراحل التحقيق ندب أي خبير يرى فيه الكفاءة الفنية اللازمة للاستعانة بخبرته[1] .كما أنه لا يوجد في القانون ما يلزمه بالاستجابة للمتهم ولا غيره من الخصوم إذا طلبوا ندب خبير، تنص الفقرة الثانية من المادة (143)من قانون الإجراءات الجزائية الجزائري على انه " **وإذا رأى قاضي التحقيق انه لا موجب لطلب الخبرة فعليه أن يصدر في ذلك قراراً مسببا**" ... ومع هذا، فإذا كانت الإستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمراً واجبا على جهة التحقيق أو الحكم، فهي أوجب في مجال استخلاص الدليل الرقمي لإثبات الجرائم الالكترونية، لتعلقها بمسائل فنية آية في التعقيد لا يكشف غموضها إلا بمتخصص بارع في مجال تخصصه، ذلك لأن الذكاء والفن لا يكشفه ولا يفهمه إلا ذكاء وفن مماثلين.[2]

وتبرز أهمية الاستعانة بالخبير الفني لإثبات الجرائم الالكترونية بشكل أكبر عند غيابه، فقد تعجز سلطات التحقيق والاستدلال عن إسقاط اللثام عن الجريمة وجمع الدليل بخصوصها لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل أو محوه بسبب الجهل أو الإهمال عند التعامل معه.

ولم يتخلف المشرع الجزائري ، اذ نص في المادة (05) الفقرة الأخيرة من القانون رقم 09-04المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنه " **يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية معطيات**

[1]- **سليمان احمد فضل**، مرجع سابق ، ص134

[2]- **فهد عبد الله العبيد العازمي**، مرجع سابق، ص640

المعلومات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها[1] "

واعتقد أن صياغة المشرع الجزائري لهذا النص بصيغة العموم " **كل شخص له دراية**" أمر مقصود حتى يوسّع دائرة المساعدة القضائية في مجال مكافحة الجرائم الالكترونية لتشمل إلى جانب الخبير، جميع المتخصصين والمعاملين في مجال تكنولوجيات الإعلام والاتصال، مثل مهندسي وذوي الشهادات العليا في الإعلام الآلي، ومقدمي خدمات الاتصالات الالكترونية، كمزودي خدمة العبور إلى الانترنت، مزودي خدمة الإيواء، مزودي خدمة الحوسبة و كل من له دراية في هذا المجال.

ولم يتوقف المشرع الجزائري عند هذا الحد، بل قامت بإنشاء هيئات وأجهزة متخصصة في مواجهة الجرائم الإلكترونية مزودة بوسائل متطورة وتقنيات عالية، وجعلت من مهامها الأساسية انجاز الخبرات التي تحتاج إليها السلطات القضائية، نذكر منها مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها الذي أنشأته قيادة الدرك الوطني في عام2009 والمعهد الوطني للبحث في علم التحقيق الجنائي الذي أنشأ بموجب المرسوم الرئاسي رقم 04-432 المؤرخ قي 20 ديسمبر 2004 وتم تنظيم المصالح والأقسام والمخابر فيه بموجب قرار وزاري مشترك مؤرخ في 14-04-2007 والذي تضمن مصلحة الخبرات الخاصة بالدلائل التكنولوجية .ونذكر كذلك القسم الخاص بالخبرة الرقمية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية المتواجد على مستوى المديرية العامة

للأمن الوطني وتمتد مصالحها الى بعض الولايات، والذي يتولى تقديم الخبرة الفنية المتميزة في القضايا ذات الطابع الرقمي .بالإضافة إلى إنشاء مؤخراً ثلاث مخابر جنائية جهوية بشمال البلاد تابعة للأمن الوطني تضمّ عدة أقسام متخصصة بما فيها قسم الأدلة الالكترونية والرقمية، والتي ستدعّم مستقبلا على حد تعبير ممثلة المديرية العامة للأمن الوطني **هودة رشيدة** ملازم

[1]- انظر المادة 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة تكنولوجيات الإعلام و الاتصال و مكافحتها، المرجع سابق.

أول للشرطة ورئيسة فرقة مكافحة الجرائم المعلوماتية لأمن ولاية وهران بثلاث مخابر مماثلة في الجنوب[1]

ونشير إلى أنه تم إنشاء مؤخراً بموجب المرسوم الرئاسي رقم15 - 261 المؤرخ في 08 أكتوبر 2015 هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها[2] ، وأسندت إليها مهمة تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في البحث والتحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية.[3].

الفرع الثاني :الجوانب القانونية و الفنية للخبرة

مما لا شك فيه أن الخبرة التقنية باعتبارها من إجراءات التحقيق تخضع لضوابط قانونية و أخرى فنية، وهذا ما سوف يتم إبرازه بالشكل التالي:

أولا: الجوانب القانونية للخبرة الإلكترونية : نظراً للدور البارز الذي تؤديه الخبرة الالكترونية في مجال الإثبات الجنائي، حرصت معظم التشريعات على تنظيمها و إحاطتها بمجموعة من الضوابط حتى يكون لنتائجها حجية أمام القضاء، ومن ضمن هذه الضوابط ما يتعلق بالخبير و منها ما يتعلق بالخبرة، فأما الضوابط الخاصة بالخبير، فهي كالتالي:

أ-اختياره الخبير من جدول الخبراء : الأصل أن يختار الخبراء حسب التخصص من الجداول التي تعدّ ها المجالس القضائية بعد استطلاع رأي النيابة العامة، ولكن استثناء في حالة عدم توفر الخبرة المطلوبة في جداول الخبراء يجوز لجهات التحقيق أن تختار بقرارمسبب خبراء ليسوا مقيدين في أي من هذه الجداول .[4]

---

[1]- أنظر القرار الوزاري المؤرخ في2007/04/14 المتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، جريدة رسمية عدد 36 ، صادر بتاريخ 03 جويلية 2009

[2]-مرسوم رئاسي رقم 15 -261مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015 ، يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، جريدة رسمية عدد 53 ، صادر بتاريخ 8 أكتوبر2015

[3]- أنظر الفقرة ب من المادة13من القانون رقم09-04 المؤرخ في 2009/08/05

[4]- أنظر نص المادة (144) من قانون الإجراءات الجزائية

كما ان عملية اختبار الخبير أمراً متروكا لجهات التحقيق، فبمفهوم نص المادة147 من قانون الإجراءات الجزائية الجزائري للقاضي أن ينتدب خبيراً واحداً أو آكثر ،متعددين حسب الحاجة، ولا تهم طبيعة الخبير سواء كان شخصا طبيعيا أو شخصا معنويا كمؤسسة متخصصة تعمل في مجال الخبرة التقنية[1] .واعتقد أن مثل هذا التوجه يتجاوب مع الحالة التي عليها الخبرة التقنية اليوم، سيما أمام ما يثيره مجال تقنية المعلومات من جدل واسع حول مقدمات التعامل معه، وكذا النتائج الممكن تحقيقها فيه.

مع هذا فرغم أن القانون لا يمنع جهات التحقيق من ندب خبير أو عدة خبراء حتى من غير المقيدين بالجدول، يبقي هذا التوجه قاصراً ويحتاج إلى تطوير في مجال الجرائم الالكترونية حتى يسمح بالاستعانة بخبراء الرقمنة والإعلام الآلي من الدول الأجنبية ولو عن بعد، وهو أمر تسمح به مقومات العالم الافتراضي باعتباره بيئة اتصالية رقمية عالمية ومعمول به لدى بعض الدول المتقدمة[2] .لان هذا الإجراء من شانه أن يعود بفائدة كبيرة على الدول لا سيما التي تعاني نقص الكفاءة في مجال تكنولوجيا الإعلام والاتصال والانترنت.

ب- أداء اليمين القانونية :أوجب المشرع الجزائري على ضرورة أداء الخبير لليمين القانونية قبل مباشرة مهامه وإلا كان عمله باطلا في المادة (145) من قانون الإجراءات الجزائية على الخبير في كل مرة يختار فيها وقبل أداء مهامه أن يحلف اليمين القانونية، غير انه إذا كان الخبير المعين مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى ما دام قد أدى اليمين عند تقييده بالجدول أول مرة.[3]

ولعل العبرة من حلف الخبير هي حمله على الصدق والأمانة في عمله، وبث الطمأنينة في نتائج خبرته التي يقدمها سواء بالنسبة لتقدير القاضي و الثقة ببقية أطراف القضية.

---

[1]- **بوكر رشيدة**، مرجع سابق، ص 426.

[2]-ا رجع **خالد ممدوح إبراهيم**، مرجع .سابق، ص29

[3]- تنص المادة (145) من قانون الإجراءات الجزائية علي مايلي " **يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الأتي بيانها :اقسم بالله العظيم بان أؤدي مهمتي كخبير على خير وجه و بكل إخلاص و ابدي رأي بكل نزاهة و استقلال ولا يجدد هذا القسم مادام الخبير مقيدا بالجدول**".

علاوة على ذلك، يتعين على الخبير بعد تفرغه من أبحاثه وفحوصاته إعداد تقرير مفصل حول المسألة محل البحث ويبين فيه خلاصة ما توصل إليه من النتائج، وعلى الخبير إيداع تقرير خبرته لدى كتابة الجهة القضائية التي أمرت بالخبرة خلال الآجال المحددة في أمر التعيين وإلا جازاستبداله بغيره ما لم يطلب الخبير تمديد هذه الآجال.[1]

وفي حالة تعدد الخبراء و لم يصلوا إلى نتائج مشتركة يقدم كل منهم تقريراً منفصلا . وتقريرالخبير لا يكون ملزما للنيابة العامة أو المحكمة، إلا أن عدم الموافقة على التقرير يجب أن يكون مسببا، وفي هذه الحالة يجوز طلب خبرة تكميلية من الخبير نفسه وتمكينه الاستعانة بفنيين من أصحاب الاختصاص إذا تطلب الأمر ذلك بموجب طلب يقدمه لقاضي التحقيق ويعينوا بأسمائهم ويؤدون اليمين، ويرفق تقريرهم بتقرير الخبرة[2].

و اذا توفرت الخبرة على الشروط المذكورة أعلاه تكون لها حجية نسبية أمام القضاء، لأن نتائج الخبرة ما هي في الواقع إلا استدلالات لإنارة قاضي الموضوع، وآراء الخبير تقدّ م دائما بصفة استشارية ولا تلزم المحكمة فإن شاء القاضي أخد بالخبرة وإن لم يشأ استبعدها[3] ، كما له أن يفاضل بين تقارير الخبرات ويأخذ منها بما يطمئن إليه ويطرح جانبا ما عداه ،فالكلمة الأخيرة تعود لقاضي الموضوع وحده عملا بمبدأ " **القاضي خبير الخبراء.**"

وتجدر الإشارة إلى انه وإن كان القاضي يملك سلطة تقديرية واسعة بالنسبة لتقرير الخبرة الذي يرد إليه، غير أن ذلك لا يمتد إلى المسائل الفنية البحتة التي يتعذّر عليه تفنيدها والرد عليها إلا بأسانيد فنية قد يصعب عليه فهمها واستنباطها بدون خبرة فنية أخرى.

ثانيا –الجوانب الفنية للخبرة الإلكترونية :نظراً للطبيعة الفنية و العلمية البحتة التي تتميز بها الجرائم الالكترونية، فان عملية تحري الحقيقة وتجميع الأدلة الرقمية فيها تعد من أصعب

---

[1]– أنظر المادة (148) من قانون الإجراءات الجزائية الجزائري

[2]– أنظر المادة (149)من قانون الإجراءات الجزائية الجزائري

[3]– وهو ما أكدته المادة (215) من قانون الإجراءات الجزائية الجزائري كما يلي " **لا تعتبر المحاضر و التقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك.**"

التحديات التي تواجه الخبير التقني، لذلك كان لازماً عليه اعتماد تقنيات ومهارات علمية مهمة والاستعانة بوسائل تكنولوجيا متطورة لرفع هذا التحدي.

أ-**الوسائل العلمية لانجاز الخبرة الإلكترونية** : يعتمد الخبير في شرح ملابسات الجريمة الالكترونية واستخلاص الدليل الرقمي الذي يساعده على الكشف عن المجرم الالكتروني على جملة من الوسائل العلمية، والتي تمثل في الغالب أدوات فنية تستخدم في بنية نظام المعلومات . ونذكر منها مايلي:

-**برتوكول الانترنت (IP)**:أو ما يسمى بعنوان الانترنت هو نظام يشبه عنوان البريد : العادي يعمل على تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها، فهو موجود بكل جهاز الكتروني مرتبط بشبكة الانترنت ويتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات، ويشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الأجهزة الالكترونية المرتبطة، والجزء الرابع يحدد الجهاز الذي تم الاتصال منه . وفي حالة وقوع جريمة الكترونية فيمكن للخبير إتباع المسار التراسلي للبحث عن رقم الجهاز المستعمل في ارتكاب الجريمة، ومن ثم تحديد موقعه (IP) للبرتوكول ومنه معرفة الجاني.

-**نظام البروكسي (PROXY)**: يشتغل هذا النظام كوسيط بين شبكة الانترنت ومستخدميها يضمن توفير خدمات الذاكرة الجاهزة، ويقوم هذا النظام على تلقي مزود البروكسي طلبا من

المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق نظام البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، ويقوم بإرسالها إلى المستخدم دون الحاجة إلىإرسال الطلب إلى الشبكة العالمية مرة اخرى، أما إذا لم يتم تنزيلها من قبل، فيقوم بتحويل ومن أهم مزايا هذا (IP) الطلب إلى الشبكة العالمية مستعينا في ذلك بأحد عناوين النظام أن الذاكرة المتوفرة لديه تحتفظ وتخزن كل عمليات التنزيل التي تمت عليه والتي يمكن أن تساعد الخبير

على اقتناء أدلة إثبات مهمة، مما يجعل دور البروكسي قويا و فعالا في عملية إثبات الجريمة الالكترونية.

-**برنامج(Trace route)** :يتم عادة ادراج هذا البرنامج ضمن نظم تشغيل الحاسب الرئيسية، ويعتبر ذا أهمية بالغة في الكشف الجنائي، إذ يحدد بدقة الأجهزة الالكترونية التي اشتركت في نقل البيانات على الانترنت بتحديد مساراتها وصولا إلى المرسل إليه، كما يمكنه أن يستدعى ويحيط بالملفات التي تم الولوج إليها وكافة عمليات الاختراق والعبور أو التجاوز خلال الإعداد للجريمة، وكافة المعلومات المتعلقة بدخول أشخاص مواقع معينة وتحديد مسارات تنقلاتهم فيها الى غاية خروجهم من هذه المواقع، وعليه فكل هذه المسارات تتضم عادة آثار أو أدلة رقمية يمكن الاستدلال بها على الجريمة[1] .

-**أنظمة كشف الاختراق (IDS)**: يكمن دور هذه الفئة من البرامج في مراقبة العماليات التي تحدث على الأجهزة الالكترونية المرتبطة بشبكة الانترنت وتسجيلها فور وقوعها في سجلات خاصة داخل هذه الأجهزة[2] ومن بين هذه الأنظمة برنامج(hack Tracer) الذي يتكون من شاشة رئيسية تقدم للمستخدم بيانا شاملا بعملية الاختراق التي تتعرض لها جهازه، يذكر فيه اسم وتاريخ الواقعة والعنوان (IP) الذي تمت من خلاله عملية الاختراق واسم مزود خدمة الانترنت المستضيف للمخترق ورقم المنفذ والبوابة الخاصة وبيانات الشبكة التي يتبعها مزود الخدمة للمخترق بما فيها أرقام هواتفها.

-**برامج مراجعة العماليات الحاسوبية واسترجاعها:** برامج تستعمل لمراقبة مختلف العماليات التي تجري على ملفات وأنظمة تشغيل حاسب معينسواءاً بحذفها أوتسجيلها في ملفات تسمى(Logs) أواسترجاع هذه الملفات في حالة محوها و ومن أمثلتها برنامج (Recover). وتأتي هذه البرامج إما مضمنة في أنظمة التشغيل أو كبرامج مستقلة يتم تركيبها على أنظمة التشغيل، وفي كلتا الحالتين لا بد من تفعيلها وإعدادها للعمل مسبقا قبل وقوع الجريمة

[1]- **سليمان بن مهجع العنزي**، مرجع سابق، ص99.

[2]- **ممدوح عبد الحميد عبد المطلب**، مرجع سابق، ص.ص15-16

الالكترونية حتى تتمكن من تسجيل كل المعلومات المتعلقة بهذه الجريمة والتي من شانها أن تساعد الخبير في استنباط الأدلة والقرائن المفيدة لإثبات الجريمة وانسبها إلى مرتكبها.[1]

-**برنامج الدمج وفك الدمج (pkzip):** يستعين الخبير الالكتروني بهذا البرنامج عادة لفك البرامج التي قام المجرم الالكتروني بدمجها قصد التعرف على طبيعة البيانات التي يحتويها وتحليلها، ودمج البرامج هي تقنية عالية يستعملها المجرم الالكتروني لإخفاء معلومات معينة لا يمكن الاطلاع عليها إلا بعد فك الدمج.

-**الذكاء الصناعي** :نقصد بالذكاء الصناعي تقنيات وبرامج الحاسب الآلي التي يستعين بها الخبير الالكتروني لحصر الأسباب والفرضيات المتعلقة بالجريمة، وجمع الأدلة الجنائية وتحليلها واستخلاص الحقائق منها، عن طريق عمليات حسابية يتم حلها بواسطة برامج الحاسب الآلي صممت خصيصا لهدا الغرض[2] ، كبرنامج (Xtree Progold) الذي يستخدم للعثور على الملفات المبحوث عنها في أي مكان على الشبكة أو الأقراص الصلبة أو الأقراص المرنة المضغوطة، وقراءة محتوياتها في صورتها الأصلية من اجل التحليل والتقوى.

المبحث الثاني: الإجراءات المستحدثة الخاصة بتحقيق الجريمة المعلوماتية.

إذا كانت الثورة المعلوماتية قد أثرت على نوعية الجرائم التي صاحبتها بظهور أنماط مستحدثة من الجرائم عرفت بالجرائم المعلوماتية، فإنها في المقابل أثرت على وسائل التحقيق في هذه الجرائم ، إذ أصبحت الطرق التقليدية التي جاءت بها نصوص قانون الإجراءات الجزائية غير كافية لاستخلاص الدليل بخصوص هذا النوع الإجرامي المستجد الذي يحتاج إلى طرق وتقنيات جديدة تتناسب مع طبيعته، يمكنها فك رموزه و ترجمة نبضاته و ذبذباته الى كلمات وبيانات محسوسة ومقروءة تصلح لان تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة.واعتباراً للطبيعة الخاصة للجرائم الالكترونية في عناصرها و وسائل وتقنيات ارتكابها، اضطر المشرع الجزائي إلى إعادة النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق

[1]- **حسين بن سعيد الغافري**، التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مرجع سابق، ص16

[2]- **حسن بن أحمد الشهري**، مرجع سابق، ص51

بمسالة التحقيق والإثبات، باعتبارها أهم موضوعات هذا القانون .لان الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية والفنية ، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية للتحقيق واستخلاص الدليل قادرة على القيام به .مما قد يؤدي في الغالب إلى إفلات العديد من المجرمين من العقاب.

وعلى ضوء ما تقدم، كان لازما على المشرع التدخل بقواعد إجرائية جديدة أكثر فعالية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الالكترونية الاعتماد عليها في الكشف عن المجرم المعلوماتي والوصول إلى دليل الإثبات فيها بسرعة و سهولة، وهي الإجراءات التي سوف نتناولها بشيء من التفصيل في هذا المبحث من خلال أربعة مطالب.

المطلب الأول: التسرب الإ لكتروني.

يعد التسرب من إجراءات البحث والتحقيق الجديدة التي أرساها المشرع الجزائري فقد تبني هذا الإجراء، مباشرة عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة بموجب المرسوم الرئاسي رقم 02-05 المؤرخ في 2002/02/02 بتحفظ واتفاقية مكافحة الفساد لسنة 2003 بتاريخ 2004/04/19.

وقد ورد النص على هذا الأسلوب لأول مرة بالجزائر بمناسبة صدور القانون 06-01المتعلق بالوقاية من الفساد ومكافحته في عام 2006 ، الذي نص في المادة 56 على أنه "**من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن اللجوء إلى التسليم المراقب وإتباع أساليب تحري خاصة كالترصد الإلكتروني أو الاختراق على النحو المناسب وبإذن من السلطة القضائية المختصة**[1] "

ولكن نظراً للغموض الذي انتاب هذا النص بخصوص المقصود بالاختراق أو التسرب و شروطه وآليات مباشرته، بقي هذا الإجراء جامدا وبدون مفعول إلى أن تم تعديله بموجب قانون

[1]- أنظر نص المادة (56) من القانون رقم 06-01 المؤرخ في 02/20/ 2006 ، يتعلق بالوقاية من الفساد ومكافحته، . ج رج ج عدد 14 ، صادر بتاريخ 2006/03/08.

06-22 ، المؤرخ في 2006/12/20 أين تم تحديد الإجراءات الجزائية و معالم إجراء التسرب من خلال تعريفه و تحديد ضوابطه والآثار المترتبة عنه، وهي النقاط التي سوف ندرسها بشيء من التفصيل من خلال الفرعين التاليين:

الفرع الأول :المقصود بالتسرب

تعرف المادة 65 مكرر 12 من القانون الإجراءات الجزائية الجزائري التسرب على انه:

"**قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلّف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك أو خاف**" ،انطلاقا من هذا التعريف، يتبين أن التسرب عملية معقدة جدا تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية [1] ، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية . لذلك اعتبار لهذه الضرورة تفطن المشرع الجزائري وجرد الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب.[2]

ليس هذا فحسب، بل أحاط المشرع المسرب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضائها، منها ما ورد في المادة65 مكرر16 من قانون الإجراءات الجزائية بأنه" **لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراء**" . [3] "وما تضمنته كذلك المادة 65 مكرر 17 من القانون نفسه بأنه " **إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب**

[1] - أنظر المادة 65 مكرر 14 من القانون الإجراءات الجزائية.

[2] -أنظر المادة 65 مكرر 14 فقرتها الأخيرة من القانون الإجراءات الجزائية.

[3]- وقد فرض المشرع الجزائري في الفقرات (1، 2 و3 من المادة 65 مكرر 16) من قانون الإجراءات الجزائية على من يكشف هوية المتسرب عقوبات صارمة تتفاوت درجتها حسب الضرر الذي يرتبه الكشف على المتسرب أو على احد أفراد أسرته قد تصل إلى 20 سنة حبسا و غرامة مليون دينار.

مواصلة النشاطات المذكورة في المادة 65 مكرر14 أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على أن لا يتجاوز ذلك 4 أشهر. "

وعلى هدى ذلك، لا يجوز اللجوء لعملية التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة 65 مكرر وهي : جرائم المخدرات، الجريمة المنظمة العابرة للحدود، جرائم تبييض الأموال وجرائم التخريب والإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1]

ويمكن تصور عملية التسرب في الجرائم الالكترونية في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي ومشاركته في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو انخراطه في مجموعات أو نوادي الهاكر، مستخدما في ذلك أسماء وصفات مستعارة وهمية ظاهراً فيها بمظهر طبيعي كما لو كان واحد مثلهم قصد استدارجهم والكشف عنهم وعن أعمالهم الإجرامية.

الفرع الثاني :الضوابط التي تحكم التسرب في الجرائم الإلكترونية.

نظراً للخطورة التي يشكلها إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه، فقد قيده المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي:

أولا–الضوابط الإجرائية: تتلخص الضوابط الإجرائية للتسرب الالكتروني في الإذن القضائي وكل ما يجب أن يتضمنه من أحكام، إذ لا يجوز للضابط أو عون الشرطة القضائية الغوص في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة والمتمثلة حسب أحكام المادة 65 مكرر 11 ق إ ج في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه . [2] على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لتفادي حدوث تجاوزات و تعسفات في استعمال هذا الحق.

[1] أنظر المادة 65 مكرر من القانون الإجراءات الجزائية.

[2] – تنص المادة 65 مكرر11 من قانون الإجراءات الجزائية على أنه ... " **يجوز لوكيل الجمهورية او لقاضي**

ولا يكفي أن يصدر الإذن بالتسرب من الجهة المختصة فحسب، بل لابد أن يكون مكتوبا وإلا كان هذا الإجراء باطلا، لأن الأصل في العمل الإجرائي الكتابة، وهو ما أكدته المادة 65 مكرر 15 ق إ ج بنصها " **يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر11 مكتوبا تحت طائلة البطلان.**"

كما يشترط أن يتضمن الإذن بالتسرب جملة من البيانات التي يتوقف على تحديدها صحة الإجراء ذاته، كذكر نوع الجريمة محل عملية التسرب واسم ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وتحديد المدة المطلوبة لهذه العملية، والتي يجب ألا تتجاوز أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن الشروط نفسها .و في الوقت ذاته يجوز للقاضي الذي أذن بهذا الإجراء أن يأمر بوقفه في أي حين قبل انقضاء الآجال المحددة.[1]

ثانيا-الضوابط الموضوعية :إلى جانب الضوابط الإجرائية المذكورة أعلاه أحاط المشرع عملية التسرب بضوابط أخرى موضوعية يمكن إيجازها في عنصرين أساسين هما:

-العنصر الأول: هو عنصر التسبيب، تضمنته المادة 65 مكرر 15 ق إ ج، ويتمثل في المبررات والحجج التي أقنعت الجهات القضائية المختصة لمنح الإذن بإجراء التسرب، وكذا الدوافع والأسباب التي جعلت ضابط الشرطة القضائية يلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكون ضمن موضوع طلبه الإذن.[2]

-أما العنصر الثاني: فيتعلق بتحديد نوع الجريمة التي ينصب عليها الإذن بالتسرب والتي يجب ألا تخرج عن نطاق الجرائم السبع التي حددتها المادة 65 مكرر5 على سبيل الحصر المشار إليها أعلاه.

التحقيق بعد إخطار و كيل الجمهورية ان يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب"

[1] -أنظر المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري.

[2] -**علاوة هوام** " التسرب كآلية للكشف عن جرائم في القانون الجزائري " مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر بباتنة، 2012 ، ص03.

والناظر إلى هذه الطائفة من الجرائم التي خصها المشرع الجزائري بإمكانية الأمر بإجراء عمليات التسرب بخصوصها، يجدها تندرج ضمن الجرائم الخطيرة جدا لسرعة انتشارها وامتداد آثارها خارج الحدود الوطنية، كما أنها تسخر عددا كبيراً من المجرمين الأذكياء، وقائمة على التخطيط واستخدام كل الوسائل محو آثار الجريمة وطمس معالمها . [1] مما يجعل الاستعانة بإجراء التسرب للكشف عن مثل هذه الجرائم والإطاحة بمرتكبيها أمراً مبرراً ومفيدا.

المطلب الثاني:اعتراض المراسلات والمراقبة الإلكترونية.

إن الإقدام الهائل للأفراد والمؤسسات على وسائل الاتصال الحديثة والاستخدام المفرط لشبكات المعلوماتية في الآونة الأخيرة ، جعل المشرع يدرك الصعوبات الكثيرة التي تثيرها محاولة مدّ نطاق إجراءات الاعتراض والمراقبة وفق النصوص التقليدية لتشمل المراسلات والاتصالات عبر الشبكات المعلوماتية، لذلك عمد المشرع إلى مراجعة قوانينه الإجرائية، بوضع نصوص صريحة تنظم هذه العملية. فتدخل بموجب قانون الإجراءات الجزائية 06-22 المؤرخ في2006/09/20 المعدل و المتمم فاستحدث لهذا الإجراء الفصل الرابع تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط صور" تناول فيه المقصود بهذا الإجراء، نطاقه وضمانات استخدامه ثم عززه بالقانون رقم 09-04 المؤرخ في2009/08/05 و سنبين كل ذلك في الفرعين التاليين :

الفرع الأول : مفهوم الاعتراض و المراقبة الإلكترونية

قد عرف المشرع الجزائري الإعتراض بالتفصيل في المادة 65 مكرر5 من قانون الإجراءات الجزائية، إذ اعتبر عملية مراقبة المراسلات بأنها " **اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للانتاج والتوزيع، التخزين، الاستقبال والعرض.**" نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل

[1] -**زورو هدى**، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة و .القانون، العدد الحادي عشرة، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، 2014 ، ص12

الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات ، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، أشكال، صور) أو الدعامة التي تنصب عليها (ورقية أو رقمية)، أو الوسيلة المستعملة لإرسالها سلكية كانت (كالفكس أو تليغرام) أم لاسلكية(البريد الالكتروني، الهاتف النقال)، باستثناء الكتب والمجلات والرسائل والحوليات .التي تعد مراسلات خاصة[1]و هذا ما آكدته المادة 02 فقرة 6 "من القانون رقم09- 04 التي عرفت الاتصالات الالكترونية بأنها " **أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة الكترونية**[2] "وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون علم أو موافقة المعنيين [3] ، وذلك لغرض التصنت و التقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل لمواجهة المتهم.[4]

ولعل من أهم المراسلات الالكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض والمراقبة والتي تمثل مصدراً غنيا لأدلة إثبات الجرائم الالكترونية، المراسلات عبر البريد الالكتروني، كون هذه التقنية من أكثر الوسائل الحديثة استخداما للاتصال عبر الانترنت و مجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون حواجز .

---

[1] –وهو ما يستكشف كذلك من خلال نص المادة 06/09 من القانون رقم 20–03 المؤرخ في 2000/08/05 لمحدد للقواعد العامة المتعلقة بالبريد و المواصلات التي اعتبرت المراسلات بانها " **كل اتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها الى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، و لا تعتبر الكتب و الجرائد و المجلات و اليوميات كمادة مرسلات**"

[2] –وهو التعريف الذي كرره المشرع الجزائري في المادة (05)من المرسوم الرئاسي رقم 15–261 المؤرخ في 2015/10/08 ، المحدد تشكيلة وتنظيم و كيفيات تسيير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جريدة رسمية عدد 53 ، صادر في 8 أكتوبر 2015

[3] – **مصطفى محمد موسى**، المراقبة الالكترونية عبر شبكة الانترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، دار الكتب و الوثائق القومية المصرية، القاهرة، 2003 ، ص1

[4] –**زيبحة زيدان**، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011 ، ص157

فهو بمثابة نظام تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، كما يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه بسهولة لأنه محاط بحماية فنية.[1]

ومن هنا، فعملية اعتراض ومراقبة البريد الالكتروني التي تجري بغرض ضبط ، المراسلات الالكترونية تنصب على ثلاثة عناصر أساسية وهي : الأول هو الوارد (IN) ويتم من خلاله مراقبة ومراجعة قائمة المراسلات الالكترونية التي وصلت المشتبه فيه.

والثاني الصادر (OUT)، وهو عكس الوارد يفيد في الكشف عن قائمة المراسلات التي أرسلت من طرف المشتبه فيه .أما العنصر الثالث فهو الحافظ و سلة المهملات (Trash) الذي يسمح بالاطلاع على المراسلات المحفوظة داخل البريد الالكتروني الخاص بالمشتبه فيه والمحذوفة منه والتي تحفظ بشكل آلي في سلة المهملات وينبغي التنبيه في هذا الصدد، الى أن المراسلات التي تصلح لأن تكون محلا لإجراء الاعتراض أو المراقبة لابد أن تتسم بالسرية و الخصوصية، ولا يتحقق هذا الأمر إلا بتوفرها على عنصرين جوهرين، يتعلق الأول بموضوع وفحوى المراسلة في حد ذاتها عندما ينصب على معلومات أو أفكار شخصية وسرية فيما تخبر به .أما العنصر الثاني، فهو شخصي ويتعلق بإرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالاطلاع على مضمون المراسلة.

وتجدر الإشارة إلى أن المشرع الجزائري لم يتبني في القانون رقم 09-04 مراقبة الاتصالات الاتصالات الالكترونية كإجراء تقتضيه التحريات والتحقيقات القضائية فقط مثلما هو في قواعد الإجراءات الجزائية، إنما أعطى تصريحا للجهات القضائية باستعمال هذا الإجراء التقني في إطار الوقاية من بعض الجرائم التي يُحتمل أن تشكل خطراً على أمن الدولة وهي كما حددتها المادة(04) ، الأفعال الموصوفة بجرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة، وجرائم الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو

[1] -نفس المرجع ص159

مؤسسات الدولة .[1] والمثير للانتباه أن المشرع سمح بإجراء عمليات المراقبة للاتصالات الالكترونية لأشخاص أو مجموعات بمجرد وجود احتمال تورطهم مستقبلا في ارتكاب إحدى هذه الجرائم، لأن الوقاية في اعتقاده لا تفرض القيام بأعمال تحضيرية لارتكاب هذه الأفعال وإنما مجرد تكهنات أو حتى قرائن بسيطة تنبئ بأن هؤلاء الأشخاص قد يقدمون على ارتكاب تلك الجرائم.

غير أن احتمال اكتشاف جريمة بنوع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال قبل وقوعها هو احتمال ضئيل جداً إن لم نقل منعدم، لأن أكثر ما يميزها أنها جرائم متبخرة ومجردة من أية مقدمات مادية ولا تكتشف إلا مصادفة، لذلك يثار التساؤل كيف للاحتمال الوارد في نص المادة 04 فقرة ب من القانون رقم 04-09 الذي يبرر اللجوء إلى المراقبة الالكترونية لمراسلات واتصالات الأفراد و انتهاك سريتها أن يتحقق، وإن كان هذا الأمر يدخل أيضا في إطار الوقاية من هذه الجرائم ؟ واعتقد أن هذا التخوف هو الذي جعل المشرع يشدد في الفقرة الأخيرة من المادة (04) أعلاه على أن تكون الترتيبات التقنية الموضوعة لمراقبة الاتصالات الالكترونية في هذه الحالة موجهة حرصاً لتجميع وتسجيل معطيات ذات صلة بالوقاية من تلك الأفعال ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

وحرصا منه على تحقيق هذا المبتغى،قام المشرع الجزائري بإنشاء هيئة وطنية خاصة أُوكّلَ إليها بالإضافة إلى مهام أخرى، مهمة تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مع السلطات القضائية ومصالح الشرطة القضائية، بما في ذلك جمع المعلومات والتزويد بها و من خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالإعمال الإرهابية والتخريب والمساس بأمن الدولة، تحت سلطة القاضي المختص، وكذا تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية.

[1] -أنظر نص المادة 04 من القانون رقم 09-04، مرجع سابق.

أضف إلى ذلك أنها تتولى تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال وتحديد مكان تواجدهم.[1]

الفرع الثاني :القيود الواردة على عملية اعتراض ومراقبة المراسلات

إذا كان أسلوب اعتراض المراسلات السلكية واللاسلكية دون علم أصحابها قد اثبت جدارته في كشف وإثبات الكثير من الجرائم الغامضة كتلك المتعلقة بالجرائم الالكترونية، فهو في الوقت نفسه يمثل انتهاكا خطيراً لحرمة الحياة الخاصة للإفراد، واعتداءاً صارخاً على سرية مراسلاتهم واتصالاتهم التي كفلتها الدستور والتشريعات العقابية بالحماية[2]. ولتحقيق التوازن بين ضرورة التحقيق التي تفرضها المصلحة العامة واحترام الحياة الخاصة التي تفرضها المصلحة الفردية، تمت إحاطة عملية الاعتراض بعدد من القيود القانونية التي تضمن عدم تعسف السلطات العامة وتصون الحرية الفردية والتي سنلخصها فيما يلي:

أولا: -الحصول على إذن السلطة القضائية المختصة :قيد القانون اللجوء إلى عملية اعتراض أو مراقبة المراسلات بشرط الحصول المسبق على إذن مكتوب ومسبب من الجهات القضائية المختصة المتمثلة عادة في وكيل الجمهورية أثناء مرحلة التحقيق الابتدائي [3] ، أو قاضي التحقيق في مرحلة التحقيق القضائي و إلا كان هذا الإجراء باطلا، فالسلطة القضائية وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية الإجراء.[4]

---

[1] – انظر المادة 05 من المرسوم الرئاسي رقم15-261 المؤرخ 8 أكتوبر2015 و المادة (14) من قانون09-04 للمزيد من التفاصيل حول مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ،أو إرجع للمبحث الثاني من الفصل الأول من المذكرة.

[2] نذكر منها المادة 2/46 من الدستور الجزائري 2016 التي تنص على سرية المراسلات والاتصالات **الخاصة بكل أشكالها مضمونة** .اما عن التشريعات العقابية نذكر المادتين 303 و 303 مكرر من قانون العقوبات الجزائري.

[3] –غير انه استثناء لهذه القاعدة عندما يتعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بأمن الدولة يكون **النائب العام لدى مجلس قضاء الجزائر هو المختص بمنح الإذن لإجراء عملية المراقبة**، أنظر الفقرتين 6 و 7 من المادة 04 من القانون 09-04

[4] –ورد هذا الشرط بالنسبة لعملية الاعتراض في المادة 65 مكرر 5 من قانون الإجراءات الجزائية بالشكل التالي": **إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم ... الجرائم الماسة بأنظمة المعالجة الآلية**

وحتى يكون الإذن صحيحا ومنتجا لآثاره، يجب أن يتضمن جملة من العناصر الأساسية وهي:

1-طبيعة الجريمة التي تبرر الإجراء :والتي ينبغي أن تكون من ضمن الجرائم التي يجوز فيها اللجوء إلى هذه العملية ، وإذا اكتشفت جرائم أخرى غير تلك الوارد ذكرها في الإذن فلا تبطل الإجراءات العارضة.

2-التعريف بالعملية :بمعنى تحديد المراسلات والاتصالات المطلوب اعتراضها وتسجيلها، تحديد الأماكن المقصودة (سكنية او غير سكانية، عامة او خاصة)، إلى جانب تحديد المدة التي تستغرقها التدابير التقنية اللازمة في عملية الاعتراض، والتي يجب أن لا تتجاوز أ ربعة أشهر قابلة للتجديد ضمن الشروط نفسها، حسب تقدير السلطة مصدرة الإذن لمقتضيات التحري والتحقيق[1] .

ولا يكفي الحصول على إذن مشمول بالعناصر المذكورة لإتمام عملية اعتراض المراسلات أو المراقبة، إنما لا بد أن تنفّذ هذه العمليات تحت الرقابة المباشرة للسلطات التي أذنت بها، وذلك من خلال قيام ضابط الشرطة القضائية المأذون له بإحاطتها علما بكل خطوات وتطورات عملية الاعتراض والمراقبة وإخطارها بشكل دوري ومستمر عن عمليات وضع الترتيبات التقنية لهذا الغرض، ساعة بداية وانتهاء هذه العمليات، على أن يد ون كل ذلك في محاضر مرقمة وبهذه الطريقة فقط نكون قد حققنا الغرض الحقيقي من هذه العمليات.[2]

ثانيا: تسبيب اللجوء إلى اعتراض أو مراقبة المراسلات :يقصد به المبرر الشرعي والضرورة الملحة التي تستدعى القيام بعملية اعتراض أو مراقبة المراسلات ، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء إلى

للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية ... و في حالة فتح تحقيق قضائي تتم العملية المذكورة بناء على إذن من قاضي التحقيق و تحت مراقبته المباشرة. " أما بالنسبة لإجراء المراقبة الالكترونية نص عليه في المادة6 من القانون 09-04 على النحو التالي ..." :**لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطات القضائية المختصة**"

[1] استثناء لهذه القاعدة إذا تعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بآمن الدولة تكون مدة الإذن بالمراقبة الالكترونية 06 أشهر قابلة للتجديد، انظر المادة 7 من القا 09-04

[2] أنظر نص المادة 65 مكرر 9 من قانون الإجراءات الجزائية.

هذه العملية، وفي هذا الشأن يشترط على وكيل الجمهورية أو قاضي التحقيق المختص قبل منح الإذن بتنفيذ العملية المذكورة تقدير جدواها وجدية دواعيها والفائدة المنتظرة منها في إظهار الحقيقة وكشف غموض الجريمة والجناة مسبقا، ثم موازنة كل هذه العناصر للتأكد مما إذا كانت كافية لخرق مبدأ حرمة الحياة الخاصة .فإذا ارتأى بأن التسبيب غير كاف رفض طلب الإذن.

والجدير بالذكر هنا هو انه إلى جانب إمكانية القيام بمراقبة الاتصالات الالكترونية في إطار التحريات والتحقيقات القضائية من اجل الوصول إلى أدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء، فقد أجاز المشرع الجزائري كذلك تطويع هذه التقنية لغرض الوقاية من احتمال وقوع جرائم خطيرة قد تهدد كيان الدولة كما قررته المادة ال ا ربعة 4 من القانون 09-04 [1].وهنا يصبح مفهوم الضرورة الملحة التي تستدعى القيام بإجراءات المراقبة الالكترونية مبهما وغير واضح، خاصة إذا تعلق الأمر بالجرائم التي تهدد النظام العام لأن مصطلح النظام العام غير محدد المعالم وقد تنجر عنه إخلالات كبيرة من شأنها المساس بحرية الأفراد.

ثالثا: تحديد الجرائم محل الاعتراض والمراقبة : إن الاستعانة بعملية اعتراض أو مراقبة المراسلات الالكترونية لغرض التحقيق غير مسموح في كافة الجرائم إنما مجال تطبيقها يتوقف عند نوع محدد فقط وهي كالتالي:

-الجرائم المذكورة على سبيل الحصر في نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية، وهي جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال أو الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد والجرائم الماسة بأنظمة المعالجة الآلية.[2]

---

[1] تنص المادة 4الفقرة1و2 من القانون 09-04 على أنه **يمكن القيام بعمليات المراقبة الاتصالات الالكترونية في الحالات الآتية-1 :للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة -2 .في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة و الاقتصاد الوطني.**".

[2] -أنظر نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية.

الجرائم المنصوص عليها في الفقرات أ، ب، ج، د من المادة (04)من قانون09-04 المتمثلة في الأفعال الموصوفة بجرائم الإرهاب أو التخريب، الاعتداءات على منظومة معلوماتية الماسة بأمن الدولة بما فيها تلك التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.[1]، وتجدر الإشارة إلى أن المشرع لم يحدد نوع الجرائم التي تندرج ضمن الفقرة ج من المادة 4 أعلاه، والتي يصعب وصول التحريات والتحقيقات القضائية الجارية في شأنها إلى نتيجة تهم هذه الأبحاث دون اللجوء إلى المراقبة الالكترونية .وهو ما يفتح المجال أمام جميع جرائم القانون العام لكي تكون محلا للمراقبة الإلكترونية كلما كان هذا الإجراء ضروريا.

رابعا: سرية الإجراءات وكتمان السر المهني :أي ينبغي أن تنفّذ عملية الاعتراض والمراقبة في سرية تامة و دون علم أو رضا المشتبه فيه أو صاحب الأماكن، مع مراعاة عدم المساس بالسر المهني المقرر بنص المادة 45 فقرة 4 ق إ ج ج.

وينبغي التنبيه كذلك، إلى أن المشرع الجزائري لم يشرط صراحة إلى كيفية وضع الأدلة المحصل من عملية اعتراض ومراقبة المواصلات (التسجيلات السمعية البصرية، البيانات الرقمية) في أحراز مختومة، مما يطرح التساؤل حول مدى اعتبارها من قبيل الأشياء المضبوطة التي تخضع لأحكام المادة (84)من قانون الإجراءات الجزائية وحكم المادة5/45 من القانون نفسه . [2] علما بأن هذه التسجيلات والبيانات تعتبر أدلة إثبات رقمية أصلية تقتضي الشرعية الجزائية حفظها بطريقة خاصة بوضعها في أحراز مختومة تضمن عدم التلاعب والعبث فيها بالحذف أو الإضافة، وضمّها إلى ملف الإجراءات مع المحاضر التي تصف أو تنسخ محتواها للكشف عن الحقيقة.

ومن ذلك كانت الحاجة إلى فتح المشرع المجال أمام سلطات التحقيق والاستدلال للاستعانة بذوي الاختصاص سواء عن طريق تسخير كل من لديهم دراية و مؤهلات في مجال سير تكنولوجيات الإعلام والاتصال من اجل تزويدهم بالمساعدة الفنية والتقنية الممكنة لتسهيل

[1] أنظر نص المادة 04 من القانون 09-04.

[2] –تنص المادة (84)من قانون الإجراءات الجزائرية على ..." **ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة**"...

وإنجاح أية عملية من عمليات التحقيق بما فيها المراقبة الالكترونية للاتصالات كما أو عن طريق ماهو منصوص في المادة 05 فقرة أخيرة من القانون رقم09-04. [1]

تكليف هؤلاء المختصين باستعمال الوسائل التقنية المناسبة والضرورية للحيلولة دون الوصول الى المعطيات التي تشكل محل الجريمة أو تحتوي أدلة لها، الموجودة داخل المنظومة المعلوماتية و منع الاطلاع عليها أو نسخها أو تهريبها أو تدميرها وفقا لما تقتضيه المادتين7 و 8 من القانون رقم09-04.

ويجب الاعتراف بأن تكريس المشرع الجزائري لإجراءات اعتراض المراسلات والمراقبة الالكترونية يعد خطوة جريئة تحسب له، على اعتبار أنها من اخطر إجراءات التحري والتحقيق عبر العالم الافتراضي نظراً لما تحمله من انتهاكات مباشرة لخصوصيات الإنسان هذا من جهة، ومن جهة أخرى لأن الفقه الجنائي لم يحسم الأمر بعد و يرى بأن المراقبة الالكترونية لا تزال محل نظر في القانون لضرورة الالتزام بما هو مقرر في القوانين والدساتير من ضمانات احترام الحق في الخصوصية.

المطلب الثالث:الحفظ والإفشاء العاجلان للمعطيات الإلكترونية.

يعد الحفظ والإفشاء العاجلان للمعطيات المعلوماتية من الإجراءات المستحدثة و الوقائية التي فرضت بموجب القانون على مزودي خدمة الأنترنت و هذا إستنشاداً بما إرتأت له أغلبية الدول الغربية لمتابعة الجريمة الإلكترونية و توقيع العقاب على الجاني، واسترشادا بذلك تضمن القانون الجزائري رقم09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وبالتحديد في المادة (10) عددا من الالتزامات تفرض على مزودي خدمات الانترنت بتقديم المساعدة بخصوص العمليات التي ينجزونها للسلطات المكلفة بالبحث والاستدلال لأغراض التحقيق من بينها :حفظ المعطيات المعلوماتية المتعلقة بالسير ووضعها

[1] أنظر المادة 505 من القانون رقم 09-04، المرجع السابق.

تحت تصرف القائمين بالتحقيق . [1] وهو ما سنحاول التفصيل فيه من خلال دراسة هاذين العنصرين في الفرعين التاليين:

الفرع الأول :الحفظ العاجل لمعطيات السير

سنتناول في هذا العنصر مفهوم الحفظ العاجل لمعطيات السير أولا ثم ضمانات المتهم أثناء هذه العملية ثانيا.

أولا –مفهوم الحفظ العاجل لمعطيات السير :اعتماد على ما سبق ذكره يمكن اعتبار الحفظ على المعطيات الالكترونية بأنه قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل قصد تمكين جهات الاستدلال من الاستفادة منها واستعمالها لأغراض التحقيق.[2]

فعملية الحفظ إذا هي من مهام مقدمي الخدمات [3] ، الغرض منها حماية المعطيات التي سبق وجودها في شكل مخزن من كل ما يمكن أن يتسبب في إتلافها أو تجريدها من صفتها أو حالتها الأصلية .ولا تهم الطريقة التي يتم من خلالها الحفظ على المعطيات الالكترونية ولا الوسيلة القانونية المقررة لذلك، فالأمر متروك لكل دولة لتقدير النماذج التي تراها ملائمة لوضع عملية الحفظ موضع التنفيذ، وينبغي التنويه في هذا الإطار إلى أن عملية الحفظ هنا لا تخص كل المعطيات الالكترونية بمختلف نماذجها [4] ، إنما تخص معطيات المرور فقط أو كما يسميها البعض حركة السير، التي عرفها المشرع الجزائري في المادة (02)الفقرة الأخيرة من

---

[1] تنص المادة (10) من القانون09-04 **في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ... و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة."...**

[2] –**بوكر رشيدة**، مرجع سابق، ص448

[3] عرفت الفقرة د من المادة (02) من القانون09-04 مقدم او مزود الخدمة بأنه –1 " :**أي كيان عام او خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام الاتصال –2 .و أي كيان آخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها** ."

[4] نشير إلى انه توجد عدة أنواع للمعطيات المعلوماتية محل التحري و التحقيق الجزائي فمنها : معطيات متصلة بالمرور ، معطيات المحتوى، و معطيات المشترك .أنظر :**هلال عبد ألاه أحمد**، مرجع سابق، ص.ص198-199.

القانون رقم 09-04 بأنها " **أية معطيات متعلقة بالاتصالات عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات، توضّح مصدر الاتصال، الوجهة المرسلة إليها، والطريق الذي يسلكه، ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة**"[1]

إلا أنه بالنظر إلى نص المادة 10فقرة1من القانون09-04فإن المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتوى الاتصالات بشرط أن يكون في **حينه**، وهو إجراء تسخير من طرف السلطات القضائية لمقدمي الخدمات المعنيين لجمع وتسجيل المعطيات المتعلق بمحتوى اتصالات أيا كانت (محادثات هاتفية أو مكالمات فيديو عبر مواقع الانترنت) أو مراسلات كتابية على شكل (SMS-MMS) .

ومن ضمن معطيات المرور التي يتعين على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية المختصة لأغراض التحقيق، تلك التي حددها المشرع الجزائري في المادة11من القانون09-04على النحو التالي:

_المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

_المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال (كرقم التسلسلي لجهاز الاتصال، و نوعه).

_الخصائص التقنية وكذا تاريخ و وقت و مدة الاتصال.

_المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

_المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم (كأرقام الهاتف مثلا او عناوين بروتوكول الانترنت ، تحديد مكانهم...)[2]

وإذا كان تحديد معطيات المرور قد يبدو أمرًا سهلا عندما تكون تلك المعطيات مرتبطة بمقدم خدمة واحد، فالأمر غير ذلك عندما ترتبط بأكثر من مقدم خدمة، فغالبا ما يساهم عدد من مقدمي خدمات في نقل اتصال معين، ويحتفظ كل واحد منهم بجزء من معطيات المرور أو

[1] 236-أنظر المادة (02)الفقرة الأخيرة من القانون) مرجع سابق.

[2] -أنظر المادة (11) من القانون09)

بعض أجزاء اللغز، مما يجعل تحديد مصدر هذا الاتصال ومنتهاه أمراً لا يستقيم إلا بجمع كل هذه الأجزاء و ضمها بعضها إلى البعض و اختبارها.[1]

لذلك عندما ترتبط معطيات المرور بأكثر من مقدم خدمة فالحفظ العاجل لهذه المعطيات يتم من خلالهم جميعا، سواء بناء على أمر منفصل لكل مقدم خدمة على انفراد، أو أمر واحد يشملهم جميعا يتم إخطارهم به بالتعاقب، أو بناء على أمر يضمّ كل مقدمي الخدمات، ثم يطلب من كل مقدمي خدمة يصله الأمر بالحفظ، أن يقوم بإخطار من يليه بفحوى هذا الأمر وهكذا.[2]

ثانيا –ضمانات المشتبه فيه أثناء عملية حفظ معطيات السير :نظراً لتعارض عملية التحفظ على المعطيات الالكترونية مع الحق في الخصوصية فقد قيدها القانون بجملة من الشروط و الالتزامات التي وضعها على عاتق مقدمي الخدمات أو أي كيان آخر يقع عليه عبئ الحفظ و هي كالتالي:

1–احترام المدة المقررة لعملية الحفظ : تعتبر عملية الحفظ تدبيراً مؤقتاً يتم اللجوء إليه بموجب أمر توجهه السلطات المختصة إلى مقدم خدمات الاتصال تلزمه بالحفظ على البيانات الالكترونية فترة معينة من الزمن و وضعها تحت تصرفها لغرض التحقيق، وتحديد مدة الحفظ يسمح بتعجيل إجراءات المتابعة الجزائية إن كان لها محل، لذلك، في حين حدد المشرع الجزائري مدة الحفظ بسنة واحدة وهو ما يستفاد من المادة (11) من القانون 09–04 التي تنص على أن ..." **تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل** ."... ومباشرة بعد انقضاء المدة المقررة لعملية الحفظ يجب على مزود الخدمة التدخل فوراً لسحب وإزالة كل المعطيات التي تم تخزينها أو على الأقل وضع ترتيبات تقنية تضمن عدم إمكانية الاطلاع على هذه المعطيات حفاظا على سريتها وخصوصيتها وإلا تعرض

[1] –**فايز محمد ا رجح غلاب**، مرجع سابق، ص427

[2] –**هلالي عبد ألاه أحمد**، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية...، مرجع سابق، ص2

لعقوبات إدارية [1] ، وأخرى جزائية قد تصل إلى عقوبات سالبة للحرية .بل انه عندما يؤدي إخلاله بالالتزامات المذكورة إلى عرقلة حسن سير التحريات القضائية .فان ذلك يعرضه للعقوبة المقررة في نص المادة 11 فقرة الأخيرة من القانون09-04 وهي الحبس من 6 أشهر إلى خمس 5 سنوات وبغرامة من 50.000 دج الى 500.000 دج.

2-الالتزام بكتمان سرية عملية التحفظ و المعلومات المتصلة بها :

بالإضافة إلى ضرورة احترام المدة المقررة لعملية الحفظ العاجل لمعطيات السير، يلتزم كذلك مقدمو الخدمات بالحفاظ على سرية كل الإجراءات والتدابير التي تفرضها هذه العملية طيلة المدة المقررة لها .ولعل الغرض من فرض هذا الالتزام هو ضمان حماية الحق في الخصوصية من جهة، وتجنب إحداث تغييرات في البيانات أو محوها من طرف أشخاص آخرين من جهة أخرى .و قد تطرق المشرع الجزائري بدوره على ضرورة تحلي مزودي الخدمات بكتمان سرية عملية الحفظ وكذا سرية المعطيات المخزنة طيلة فترة الاحتفاظ بها، وعدم الإفشاء بها إلا لسلطات التحقيق المختصة، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق[2]

و مما سبق فتقيد مزودي الخدمات بالالتزامات المذكورة أعلاه أثناء عملية حفظ المعطيات الالكترونية يجعلهم سندا مهما لجهات التحري والتحقيق في الحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها وملزمين في الوقت نفسه بوضعها تحت تصرف هذه الجهات إذا ما طلبتها.

---

[1] المعروف عند معظم الدول أن مقدمي خدمات الاتصالات الالكترونية والانترنت يخضعون في ممارسة نشاطهم إلى نظام الترخيص المسبق من الهيئات الإدارية المختصة، لذلك فان عدم التزامهم بمسح المعطيات المخزنة بعد انقضاء الفترة المقررة لعملية التحفظ من شانه أن يعرضهم إلى عقوبة إدارية تتمثل في سحب الرخصة . أنظر في هذا الشأن نص المادة 394مكرر 6 من قانون العقوبات الجزائري، مرجع سابق.

[2] تنص المادة 2/10 من القانون 09-04 على ما يلي: ... **و يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين و كذا المعلومات المتصلة بها و ذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق**

الفرع الثاني :الإفشاء العاجل لمعطيات السير.

يعد هذا الإجراء من الالتزامات المترتبة على مقدمي خدمات الانترنت في إطار مساعدة السلطات المكلفة بالبحث والتحقيق في الجرائم الالكترونية، فهي عملية مكملة لإجراء الحفظ العاجل لمعطيات المرور، كما أوضح المشرع الجزائري إجراء الإفشاء العاجل لمعطيات السير لغرض التحقيق وجعله التزاما على عاتق كل مقدمي الخدمات، وذلك من خلال نصه في المادة (10)من القانون09-04 على انه " **:في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ...** و **بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) أدناه، تحت تصرف السلطات المذكورة**[1] "...

بناء على ما سبق فكما تلزم سلطة التحقيق مقدمي الخدمات بالحفظ العاجل على معطيات المرور فإنها تلزمهم بالإفشاء السريع لها، أو لمن تعينه من قبلها عن تلك المعطيات المهمة المتعلقة بالمرور ووضعها تحت تصرفهم لفحصها قبل أن يتم التلاعب بها، قصد الوصول إلى تحديد هوية كل مقدمي الخدمة الآخرين، والطريق الذي بمقتضاه تم الاتصال .وبهذه الطريقة يكون بمقدور السلطة المكلفة بالبحث والتحري أن تكشف منبع الاتصال ومصبه، وهي المعلومات التي قد تقوده إلى معرفة هوية الأشخاص المتورطين في ارتكاب الجريمة الالكترونية .وتجدر الإشارة هنا إلى انه عند اللجوء لتلك الإجراءات يجب مراعاة الحدود والضمانات القانونية المتعلقة بالخصوصية، وحقوق وحريات الإنسان بشكل عام، بما يحقق التوازن بين إقامة العدالة و المحافظة على تلك الحقوق

ومما يحسب على هذا الإجراء رغم أهميته البالغة في عملية البحث و التحري في الجرائم الالكترونية، و رغم أن أي إخلال به من قبل مقدمي الخدمات يرتب مسؤوليتهم الجزائية.

[1] -أنظر نص المادة 10 من القانون 09-04 المؤرخ في 05-8-2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

خلاصة الفصل:

وفي الأخير وبعد ما تناولنا في هذا الفصل آليات التحقيق في الجريمة المعلوماتية، حيث بينا الإجراءات العامة او ما يسمى بالإجراءات التقليدية أي تلك المآلوفة على الجرائم التقليدية و البسيطة إن صحّ التعبير والتي تشترك فيها مع الجريمة التقليدية نوعا ما ، بالإضافة إلى الآليات الخاصة و المستحدثة لمسايرة هذا النمط المستجد و الآكثر خطورة من سابقاته التي تخضع لها الجريمة المعلوماتية ، حيث أدرجناها في إجراءات مادية(العامة والمآلوفة) التي تقتصر فقط على المعاينة التقنية، التفتيش بشتى أنواعه وضبط الأدلة في العالم الإفتراضي و كذا الخبرة و التي تخضع تارة لأحكام قانون الإجراءات الجزائية. (المكونات المادية) وتارة إلى قانون /09 04 تارة أخرى (المكونات المعنوية) وأخرى سنطلق عليها إسم الإجراءات الفنية أو التقنية وهي تلك المستحدثة من طرف المشرع ،فأولها التسرب وهو من أساليب التحري الخاصة النـي جاء بها تعديل قانون الإجراءات الجزائية و إجراء الإعتراض و المراقبة الإلكترونية و كذلك كل ما يتعلق بحفظ و تجميع و إفشاء بيانات حركة السير، والذي قرر تطبيق هذه الإجراءات خاصة إلا على الجرائم الموصوفة بالخطيرة التي تهدد النظام العام أو الإقتصاد و الأمن الوطني والمذكورة على سبيل الحصر قانوناً والتي من بينها الجرائم المعلوماتية.

الخاتمة

الخاتمة:

أضحى 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 ، نظرا لكون التكنولوجيا عابرة للحدود . وأمام هذا التطور فقد ارتبطت به الظهور ما يعرف بالإجرام المعلوماتي وذلك نتيجة الإستخدام بالقصد الجنائي للمعلوماتية أو الحاسوب الذي نتج عن هذا الآخير عدة أضرار يمكن حصرها، وذلك أنها تهدد أمن المعطيات من جهة وتمس بحرية الأفراد و ممتلكاتهم والمؤسسات من جهة أخرى .وإنّ الحماية الفنية مهما بلغت درجتها من التعقيد والصعوبة فهي لا تستطيع المقاومة أمام التطور التقني الذي تشهده تقنيات الإختراق وكذا عجز النصوص التقليدية في توفير الحماية خاصة من الناحية الإجرائية .

هذا ما دفع بالمشرع الجزائري لإنشاء قواعد قانونية تحمي حريات الآفراد ومكاسبهم المدرجة في شكل معطيات وقد حاولنا من خلال الفصلين كاملين الوقوف على مفاهيم الجريمة و تجريمها في نصوص قانونية لحل الآحكام الإجرائية الخاصة بمتابعة مرتكبي الجرائم المعلوماتية من أجل إقرار الحماية لها، فوجدنا ان للجريمة المعلوماتية خصوصية من الناحية الإجرائية من خلال اعتمادنا على قانون الإجراءات الجزائية الجزائري الجديد وكذا القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته . حيث وجدنا ان قانون الإجراءات الجزائية الجزائري ينص فقط علي القواعد العامة التي تطبق علي الجرائم التقليدية وكذا علي المعلوماتية أما بالنسبة للقانون 09-04 الذي وضع لمتابعة الجريمة المعلوماتية من خلال بعض الإجراءات الخاصة ممثلة في حجز المعطيات وكذا مراقبة الإتصالات الإلكترونية و حفظ المعطيات في هذا المقام وجدنا أن هناك بعض الإجراءات تعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المعلوماتية كالمعاينة على مسرح الجريمة مشتركا بين الجرائم في المسرح التقليدي(المادي و المحسوس) و المسرح الإفتراضي(غير المحسوس) وكذا التفتيش الإلكتروني وضبط الدليل الرقمي والمستحدث في الإجراءات الجديدة التي جاء بها تعديل

قانون الإجراءات الجزائية سنة 2006 التي تعرف بأساليب التحري حيث تطبق سواء كانت الجريمة معلوماتية أو تقليدية ومنها إجراءات لا تطبق إلا على الجرائم المعلوماتية بالإضافة إلى إجراءات خاصة جاء بها قانون 09-04 .ضبط الدليل الرقمي الكترونيا وكذا التسرب الرقمي و مراقبة الإتصالات الكترونية وكذا حفظ المعطيات و هي اجراءات جاء بها قانون 09-04 ، يتم التحقيق في الجريمة المعلوماتية تحت إشراف قاضي التحقيق الذي لا بد أن تتوافر فيه مجموعة من المؤهلات التي تؤهله من اجل متابعة التحقيق و متابعة المجرم المعلوماتي امام الأقطاب الجزائية المتخصصة و مكافحة الجريمة علي المستوي الدولي والعربي وتكريس التعاون الدولي من أجل مكافحتها خاصة في مجال الإجراءات الدولية ممثلة في المساعدة القضائية الدولية وكذا تسليم المجرم المعلوماتي . وقد لاحظنا في نهاية عرضنا هذا الموضوع أنه من الموضوعات الصعبة والمتشعبة خاصة فيما يتعلق بالجانب الإجرائي ولعل أهم المشكلات التي واجهتنا في إعداد بحثنا هذا . وبالرغم من وجود نصوص قانونية فأن مكافحة الجريمة المعلوماتية رهينة بالمعيقات الإجرائية في مجال المتابعة فإن أول إشكال أو عائق هو غياب القدرات التأهيلية والوسائل الفنية التي تنتج سرعة إدراك ما حصل وأن غياب التأهيل قد يؤدي إلى إتلاف الدليل وإفلات مرتكبي هذه الجرائم من العقاب بالإضافة إلى مشكلات في القانون الواجب التطبيق كون الجريمة المعلوماتية عابرة للحدود وإعادة النظر في مدي تطبيق القوانين من عدمها والإسراع لسن قواعد إجرائية خاصة تتلائم مع طبيعة الجريمة المعلوماتية حتى تكون أكثر فعالية و بالإضافة إلى تكثيف الجهود الدولية والإقليمية لمكافحة هذا النوع من الإجرام.

وكذا ضرورة تدريب وتأهيل أفراد الضبطية القضائية على كيفية التعامل مع هذا النوع من الجرائم وذلك بعقد دورات تكوينية بشكل دائم لتدريس الأنظمة المعلوماتية والجرائم التي تقع عليها في كليات الحقوق والمعاهد وتفعيل دور الأسرة في متابعة أبنائهم لوقايتهم من الآثار السلبية للإستخدام السيئ لشبكة الأنترنت بالإضافة الدعوة إلى ضرورة وجود تعاون دولي في مجال مكافحتها وتفعيله اكثر فآكثر.

قائمة المراجع

المؤلفات:

1- أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومه ، الجزائر ، ط 10،2011.

2- إسحاق إبراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1995 .

3- أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومه الجزائر ، ط2 ، 2007.

4- أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الأنترنت ، دار المطبوعات الجامعية ، الأسكندرية ، 2009 .

5- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية،2010

6- بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية،

7- جميل عبد الباقي ، القانون الجنائي والتكنولوجيا الحديثة ، دار النهضة العربية ، القاهرة ،1992 .

8- جميل عبد الباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت ، دار النهضة العربية ، القاهرة ، 2001 .

9- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية،2001 .

10- خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر و التوزيع، عمان،

11- خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، الإسكندرية ، 2008 .

12- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، إسكندرية، 2009 .

13- رشاد خالد عمر، المشاكل القانونية و الفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية،

14- زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ، ط1 ، 2011 .

15- عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الهدى. الجزائر.

16- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، دار الفكر الجامعي، الإسكندرية، 2006.

17- عفيفي كمال عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة،دار النهضة،2002.

18- محمد العريان ، الجرائم المعلوماتية ، كلية الحقوق جامعة الإسكندرية ، دار الجامعة الجديد للنشر ، الإسكندرية ، الطبعة 2004 .

19- محمد زكي أبو عامر وعلي عبد القادر القهوجي ، قانون العقوبات القسم الخاص ، دار النهضة العربية القاهرة ، 1993.

20- مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، دار الكتب و الوثائق القومية المصرية، القاهرة، 2003 .

21- مولود ديدان ، الدستور الجزائري تعديل نوفمبر 2008 ، دار بلقيس ،الجزائر،2009.

22- مولود ديدان ، قانون الإجراءات الجزائية ، الأمر02-11، دار بلقيس ،الجزائر.

23- نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الإقتصادية ، المنشورات الحلبي الحقوقية، ط1 ،2005.

24- هشام محمد فريد ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، أسيوط ، ط 1، 1994.

25- هلال عبد الله أحمد ، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ،ط.1.

26- هلال عبد الله احمد، تفتيش نظم الحاسب الآلي وضمانات المتهم ألمعلوماتي، دار النهضة العربية، القاهرة،1997

27- ياسر محمد الكومي محمود أبو حطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشأة المعارف، الإسكندرية.

الرسائل الجامعية:

1- أحمد بن ا زيد جوهر الحسن المهدي، تفتيش الحاسب الآلي وضمانات المتهم، مذكرة لنيل درجة ماجستير في القانون، كلية الحقوق ، جامعة القاهرة ، 2009 .

2- أحمد خليفة الملط ،الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط2، 2006.

3- **أحمد مسعود مريم**، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال في ضوء القانون 09-04 مذكرة لنيل شهادة ماجستير في القانون الجنائي، كلية قصدي مرباح ،بجامعة ورقلة ،2013.

4- حسين بن سعيد الغافري، التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت حملاوي عبد الرحمان ، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ، جامعة الجزائر،2014.

5- سامي على حامد عياد ، الجريمة المعلوماتية وإجرام الأنترنت ، ماجستير في القانون ، دار الفكر الجامعي ،الإسكندرية ، سنة الطبع2008 .

6- سعيد نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية، جامعة الحاج لخضر باتنة 2012-2013 .

7- طوبي ميشال عيسى ، التنظيم القانوني لشبكة الإنترنت ، دار صادر للمنشورات بيروت ، ط1، 2000 .

8- **فايز محمد راجح غلاب**، الجرائم المعلوماتية في القانون الجزائري و اليمني، أطروحة لنيل شهادة الدكتوراه في القانون، .فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر1 ، الجزائر، 2011 .

9- فهد عبد الله العبيد العازمي ، الإجراءات الجنائية المعلوماتية ، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق، مسيلة ،2013

10- ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري ، مذكرة مقدمة لإستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار الحقوق ، تخصص قانون جنائي ، سنة 2013 - 2014 .

11- نهلا عبد القادر المومني ، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي،دار الثقافة للنشر والتوزيع، سنة 2012.

12- هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ،المعهد الوطني للأدلة الجنائية وعلم الإجرام ، جامعة بسكرة كلية الحقوق ، 2016 .

المقالات والمجلات:

1- **زورو هدى**، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة و .القانون، العدد الحادي عشرة، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة،2014

2- **محمد قدري حسن عبد الرحمن** ، جرائم الاحتيال الالكتروني ، مجلة الفكر الشرطي ، عدد 79 ، صادر عن مركز بحوث،سنة2003

<u>الدوريات(الملتقيات):</u>

1- سالم عبد الرزاق ، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية ، بمحكمة سيدي محمد.

<u>المصادر القانونية:</u>

1- الدستور الجزائري لسنة 2016

2- اتفاقية فيينا للعلاقات الدبلوماسية لسنة 1961 و القانون رقم 16 -01 مؤرخ في 6 مارس 2016 ، يتضمن التعديل الدستوري الجزائري، ج.ر عدد 14 .

3- المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08 ، المحدد تشكيلة وتنظيم و كيفيات تسيير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جريدة رسمية عدد 53 ، صادر في 8 أكتوبر 2015

4- من المرسوم الرئاسي رقم15-261 المؤرخ 8 أكتوبر 2015 والقانون09-04 للمزيد من التفاصيل حول مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

5- المرسوم رئاسي رقم 15 -261 ، مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015 ، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحته.

6- القرار الوزاري المؤرخ في 2007/04/14 المتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، جريدة رسمية عدد 36 ، صادر بتاريخ 03 جويلية 2009 .

7- القانون 09-04 المؤرخ في 05-8-2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها

8- الأمر رقم 66-155 مؤرخ في 08 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية الجزائري، المعدل و المتمم.

9- القانون رقم 06-01 المؤرخ في 02/20/ 2006 ، يتعلق بالوقاية من الفساد ومكافحته، .ج رج ج عدد 14 ، صادرة بتاريخ 2006/03/08

10- القانون رقم 2000-03 المؤرخ في 2000/08/05

11- القانون 06-09 الصادر في 2006/07/15 المتعلق بمكافحة التهريب .

12- قانون رقم20-03 المؤرخ في 2000/08/05والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

13-القانون رقم 08-01 :المؤرخ في2008/01/23 والمتمم للقانون رقم : 83-01 متعلق بالتأمينات

المواقع الالكترونية:

1- **علي حسن الطوالبة** ، مشروعية الدليل الرقمي المستمد من التفتيش الجنائي دراسة مقارنة ص 07 ، بحث منشور على موقع الانترنت التالي www.policemc.gov.bh.

2- مجلة جامعة بابل ، العلوم الإنسانية ، المجلد 14 ، العدد6 ،2007.

3- **محمد أبو العلاء عقيدة** ، "التحقيق و جمع الأدلة في محال الجرائم الالكترونية"، مقال منشور في الموقع التالي : www.osamabahar.com. تاريخ الإطلاع 2019/02/17، 16:44.

4- **ممدوح عبد الحميد عبد المطلب** "استخدام البروتوكول(TCP/ IP) في بحث و تحقيق الجرائم على الكمبيوتر،مقال منشور عبر الموقع التالي: www.arablawinfo.com تاريخ الاطلاع:2019/04/04 ، 11:22.

الفهرس

مـلخص المذكرة

تعرضنا في هذه المذكرة إلى إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري بنوع من التفصيل من خلال الفصلين : فقد تناولنا في الفصل أول الجريمة المعلوماتية بين المفاهيم والتجريم،حيث لم تختلف التشريعات الآخرى عن التشريع الجزائري من حيث مفهومها وطبيعتها الخاصة وأركانها وكذلك مدى تجريم القوانين الوضعية وغيرها من القوانين والمراسيم الرئاسية والوزارية لإنشاء وتنظيم أجهزة متخصصة في متابعة الجرائم المتعلقة بالمعالجة الآلية للمعطيات كإنشاء مخابر المعالجة الآلية.والفصل الثاني آليات التحقيق في الجرائم المعلوماتية حيث منها ماهو تقليدي كالمعاينة والتفتيش وكذا ضبط الآدلة في البيئة الإفتراضية وكذا الخبرة التقنية والتعديلات التي أضفاها المشرع الجزائري في قانون إجراءات جزائية لمسايرة التقنيات المعلوماتية التي هي في تطور مستمر والخاصية المنفردة للوسائل المستعملة في إرتكابها.كما إستحدث المشرع إجراءات حديثة لمحاربة الجريمة وتوقيع العقاب على الجناة الأصليين وكذا الشركاء والمساهمين مهما كانت صفتهم وهذا ما أكدته مواد القانون رقم 09-04 المؤرخ في 2009/08/05 والذي أدرج إجراء التسرب وإعتراض المراسلات اللذان ظبطوا بقواعد تنظيمية إجرائية صارمة كونهما إجراءات حساسة تمس خصوصيات الأفراد بشكل مباشر،وكذا حفظ وإفشاء وتجميع المعطيات المتعلقة بحركة السير،وكلها إجراءات مستحدثة جاء بها تعديل قانون الإجراءات الجزائية الجزائري لسنة 2006 وكذا قانون 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها،مما إستوجب على المشرع الجزائري ضرورة تكييف الواقعة طبق المنظومة التشريعية والقانونية خاصة الإجرائية من خلال منح الصلاحيات وتمديد الإختصاص المحلي والإقليمي لوكلاء الجمهورية وقضاة التحقيق من أجل كشف خيوط وملابسات القضية وكذا التعاون دولياً في مجال مكافحتها عن طريق الإنضمام إلى الإتفاقيات الدولية والعربية.

<u>الكلمات المفتاحية</u>:1/المعالجة الألية للمعطيات. 2/التشريع الجزائري.

3/إجراءات التحقيق. 4/الإجراءات المستحدثة.