فرقة مشروع البحث التكويني الجامعي P.R.F.U
الجرائم الالكترونية في المجتمع الجزائري، انعكاساتها، وسبل مواجهتها
رمز I05L02UN260120190001

الملتقى الوطني: الجرائم الإلكترونية في المجتمع الجزائري: تشخيص الواقع وتحديات الأمن
جامعة يحي فارس المدية
المنعقد بتاريخ 15 مارس 2022

إجراءات البحث والتحري في الجرائم الإلكترونية

Research and investigation procedures in cybercrime

د. ليندة بومحراث
جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة

ط.د عبد النور سعيداني
جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة

ملخص

لقد ساهمت التكنولوجيا الحديثة في القضاء على الأساليب التقليدية التي كان يستخدمها الإنسان قديما، فالحديث اليوم لم يعد مقتصرا فقط على توفير الوقت والجهد، وإنما حول تكنولوجيا الإعلام والاتصال وما أفرزته من تقنيات حديثة، لكن على الرغم من المزايا لهذه التقنية إلا أنها صاحبها في المقابل انعكاسات سلبية نتيجة سوء استخدامها، فبرز ما يسمى بالجرائم الإلكترونية والتي تعد من أخطر الجرائم، وللحد من انتشار مثل هذه الجرائم واحتوائها ومن أجل الوصول إلى الجهات القضائية المختصة وفك لغز هذه الأنواع من الجرائم كان لابد من اتباع إجراءات قانونية في مجال البحث والتحري والذي يتطلب بدوره مهارات تقنية وفنية وخبرة في مجال الحاسب الآلي والإنترنت.

الكلمات الدالة: الجرائم الإلكترونية؛ إجراءات البحث والتحري؛ المعاينة التقنية؛ جمع الاستدلالات؛ التسرب.

Abstract :

Modern technology has contributed to the elimination of the traditional methods used by humans in the past. Today's talk is no longer limited to saving time and effort, but rather about information and communication technology and the modern technologies it produced, but despite the advantages of this technology, it has repercussions in return. Negative as a result of its misuse, the so-called cybercrime emerged, which is one of the most dangerous crimes, and to limit the spread and contain such crimes and in order to reach the competent judicial authorities and decipher these types of crimes, it was necessary to follow legal procedures in the field of research and investigation, which in turn requires skills Technical and technical expertise in the field of computers and the Internet

Keywords : cyber crimes. Research and investigation procedures. technical inspection. collecting inferences. leakage.

مقدمة:

لقد تطورت الجريمة بتطور وسائل الاتصال الحديثة، خصوصا أنها أصبحت تقع في العالم الافتراضي، مما زاد الأمر تعقيدا وصعوبة على الجهات القضائية هذا من جهة، ومن جهة أخرى أن هذا النوع من الجرائم يتطلب تقنيات عالية من أجل فك ملابسات ارتكابها، وفي ظل الخروقات التي ترتبت عن تهديد الحياة الخاصة للأفراد، والخسائر الناجمة عن ولوج برامج وأنظمة الشركات والأشخاص المعنوية العمومية وخاصة منها الاقتصادية، كان لابد من وضع إجراءات قانونية خاصة في مرحلة البحث والتحري، تمنع أو تقلص من ارتكاب الجرائم الإلكترونية، هذا ما جعلنا نطرح الإشكال الرئيسي التالي:

هل إجراءات البحث والتحري الخاصة بالجرائم التقليدية استطاعت معالجة الجرائم الإلكترونية أم أن هذه الأخيرة تتطلب نوع خاص من الإجراءات من أجل التعرف على مرتكبيها ؟

وتندرج تحت هذه الإشكالية الرئيسية مجموعة من التساؤلات الفرعية أهمها:

- ما مفهوم الجرائم الإلكترونية؟.
- ما هي الجهات المختصة بإجراء البحث والتحري في الجرائم الإلكترونية؟.
- ما هي آليات المتابعة الإجرائية في مرحلة البحث والتحري للكشف عن الجرائم الإلكترونية؟.

خطة البحث:

المطلب الأول: مفهوم الجرائم الإلكترونية.

المطلب الثاني: الاجراءات العامة للبحث والتحري في الجرائم الالكترونية.

المطلب الثالث: الاجراءات الخاصة للبحث والتحري في الجرائم الإلكترونية.

جامعة يحيى فارس المدية ، طريق عين الذهب، المدية ، **البريد الإلكتروني:** colloqueprff@gmail.com

1.مفهوم الجرائم الإلكترونية:

نظرا لحداثة الجرائم الإلكترونية وارتباطها بوسائل الاتصال الحديثة كان لابد من إيجاد مفهوم لها، وبما أن مثل هذه الجرائم تقع على عدة أشياء مادية ومعنوية مما جعلها تصنف إلى عدة أنواع حسب ما تقع عليه، كما اتسمت بمجموعة من الخصائص تميزها عن غيرها من الجرائم، بالإضافة إلى أن المشرع حدد الأركان التي تقوم عليها الجرائم الإلكترونية.

1.1.تعريف الجرائم الإلكترونية:

لقد اختلفت التسميات المطلقة على الجرائم التي ترتكب بواسطة أجهزة الإعلام الآلي بين الفقهاء فمنهم من يطلق عليها جرائم الحاسب الآلي، والبعض يطلق عليها جرائم الكمبيوتر فيما يطلق عليها آخرون الغش المعلوماتي.

1.1.1.التعريف الضيق والموسع للجرائم الإلكترونية:

لقد اختلف فقهاء القانون حول تعريف الجرائم الإلكترونية فمنهم من ركز على الجانب المعنوي والذي يقصد به البرامج التي تنفذ عن طريق الحاسب الآلي، وهناك من ركز على الجانب موسع والذي يعني جميع السلوكيات غير المشروعة المرتكبة بواسطة الحاسب الآلي أيضا.

1.1.1.1.التعريف الضيق للجرائم الإلكترونية:

اختلف الفقه في تعريف الجريمة الإلكترونية من جهة نظر ضيقة، فمنهم من اعتمد معيار الوسيلة المستعملة، ومنهم من اعتمد معيار توافر المعرفة بتقنية الحاسب الآلي ومنهم من يرى أن الجريمة الإلكترونية هي التي يكون موضوعها المال المعلوماتي المعنوي[1].

1.1.1.1.1. معيار وسيلة ارتكاب الجريمة:

يرى البعض أن الحاسب الآلي هو أساس هذه الجريمة ويميزها عن غيرها من الجرائم بوسيلة ارتكابها. ومن أنصار هذا الرأي "**مارو**" الذي عرف الجريمة الإلكترونية بأنها: " **الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي**"[2].

2.1.1.1.1. معيار توفر المعرفة بتقنية المعلوماتية:

يستند أصحاب هذا الاتجاه إلى معيار شخصي يستوجب أن يكون الفاعل ملما بتقنية المعلومات واستخدام الحاسب الآلي[3]. ولذا عرفها دافيد تومسون بأنها:" **أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب**"[4]. وقد عرفها ستيرن سكجوبر (**STRIN SCKJOBR**) بأنها:" **أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه**"[5].

3.1.1.1.1.معيار موضوع الجريمة:

يرى آخرون أن تعريف الجريمة الإلكترونية إنما يرجع إلى موضوعها وغير متعلق بالوسيلة المستعملة أو الفاعل، حيث يرى هؤلاء أن الجريمة هي التي يكون موضوعها المال المعلوماتي المعنوي، دون النظر فيها إذا كان الحاسب هو الأداة المستعملة في ارتكابها من عدمه[6]. وعرفها فريق آخر من الفقه بأنها:" **كل فعل متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل**"[7].

جامعة يحيى فارس المدية ، طريق عين الذهب، المدية ، البريد الإلكتروني: colloqueprff@gmail.com

2.1.1.1.التعريف الموسع للجرائم الإلكترونية:

يوسع البعض مفهوم الجريمة المعلوماتية لتشمل إساءة استخدام الحاسب (Computer abuse) التي عرفوها: " **أي فعل متعمد مرتبط بأي وجه بالحسابات، يتسبب في تكبد أو إمكانية تكبد المجني عليها لخسارة، أو الحصول أو إمكانية حصول مرتكبه على مكسب"**[8]. ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها:"**كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر"**[9].

2.1.1. تعريف الجرائم الإلكترونية في التشريع الجزائري:

المشرع الجزائري لم يعرف الجريمة الإلكترونية وإنما تبنى للدلالة على الجريمة الإلكترونية، مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة، حيث يمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة، كما لم يتطرق قانون العقوبات الجزائري المعدل والمتمم لتعريف جرائم الإنترنت، بل اكتفى بالعقاب على بعض الأفعال تحت عنوان الجرائم الماسة بنظام المعالجة الآلية للمعطيات [10].

فقد تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية[11]. وهذا يظهر واضحا من خلال نص المادة الثانية (02)الفقرة الأولى من القانون رقم 09-04 الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي جاء فيها:" **جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"**[12] .

فقد جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، وهذا ما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات والذي أفرد القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 8 مواد من المادة 394 مكرر وحتى المادة 394 مكرر 7[13].

كما استحدث المشرع الجزائري القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و المتخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها[14].

ويقصد بمفهوم هذا القانون بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال[15].

2.1. أنواع الجرائم الإلكترونية:

توجد عدة تصنيفات للجرائم الإلكترونية وأبرز هذه الجرائم، الجرائم الواقعة على الأموال، أو على الأشخاص، أو على أمن الدولة.

1.2.1. الجرائم الواقعة على الأموال:

تنقسم الجرائم الواقعة على الأموال باستعمال الأنظمة المعلوماتية إلى ثلاث جرائم وهي: جرائم غسل الأموال والمخدرات، جرائم جرائم التجارة الإلكترونية، جرائم السرقة والنصب أو الاحتيال.

1.1.2.1. جرائم غسل الأموال والمخدرات:

سنفصل في جرائم غسل الأموال أولا ثم جرائم المخدرات.

1.1.1.2.1. جرائم غسل الأموال:

توجد عدة أساليب يلجأ إليها المجرمون فيما يخص غسيل الأموال، وتختلف حسب نوعية الأموال المقصود غسلها ومن بين هذه الأساليب نجد ما يلي:

– شراء الأصول مثل الطائرات، السيارات، القطارات و القوارب وتسجيلها بأسماء آخرين.

– النقود الإلكترونية وتعتبر هذه التقنية نتيجة التطور الهائل في المجالات الإلكترونية والمصرفية، حيث تمكن من استخدام البطاقات الذكية **(Smart Carde)**، دون مخاطرة أو تكاليف مرتبطة بعملية التبادل دون وسيط كما تتميز بسرعة الحركة والتغيير[16] .

2.1.1.2.1. جرائم المخدرات:

تختلف جرائم المخدرات على شبكة الأنترنت والحواسب الآلية حسب طريقة الاستعمال، فهناك من يستعمل الإنترنت للإنتاج وآخرون للبيع أو الاستخدام عبرها، ونذكر كالآتي:

1.2.1.1.2.1. إنتاج المخدرات على الإنترنت:

يوفر الوصول للإنترنت كميات كبيرة من المعلومات تتعلق بإنتاج المخدرات بما في ذلك من عمليات ووصفات ومكونات ومقادير، وهذه المعلومات متوفرة لصغار السن والمراهقين والمتعاطين. وإن هذه المعلومات ليست بالضرورة أن تكون دقيقة وصحيحة فالمعلومات الخاطئة قد تقود إلى اصابات خطيرة أو أمراض أو حتى أحيانا قد تؤدي للوفاة. كما أن أدوات الانتاج متوفرة عبر الإنترنت والمواد الكيماوية اللازمة لإنتاج المادة المخدرة متوافرة أيضا، وحتى أن هذه المواد والمعدات رخيصة الثمن[17].

2.2.1.1.2.1. استخدام المخدرات على الإنترنت:

تحتوي الإنترنت كميات هائلة من المعلومات تتعلق بآثار استخدام المخدرات وطرائقها والتحذيرات حولها، وعن أي نوع يفكر فيه المتعاطي أو أي فرد على الإنترنت حيث أن هناك العديد من المواقع تشجع على خلق ثقافة استخدام المخدرات و إغواء الشباب بمثل هذا الاستخدام خاصة عند ربطها بموضوع الإثارة الجنسية.

3.2.1.1.2.1. بيع المخدرات على الإنترنت:

تباع المخدرات سواء القانونية منها أو غير القانونية بشكل واسع على الإنترنت، وغالبا ما تتم الصفقات للمخدرات غير الشرعية عبر لوحات النقاش وغرف الدردشة بلغة مشفرة، وترسل المخدرات إلى عنوان المعني كما أنه يمكن تقديم المعلومات اللازمة لإنتاجها في المنزل[18] .

2.1.2.1. جرائم التجارة الإلكترونية:

تتعدد وتتنوع الجرائم الواقعة على التجارة الإلكترونية، وينحصر أغلبها في:

- الاعتداء على التوقيع الإلكتروني.
- السطو على أرقام البطاقات الائتمانية.
- الاعتداء على حقوق الإنترنت[19].

3.1.2.1. جرائم السرقة والنصب والاحتيال:

تتم جرائم النصب والاحتيال الإلكتروني بطرق وأشكال متنوعة ومدروسة للنصب والاستلاء على أموال الآخرين ولعل أبرزها ما تم عن طريق مواقع التواصل الاجتماعي خاصة (فيسبوك و تويتر) كونه أداة سهلة للتلاعب بالآخرين لسرقة أموالهم، وهذا ما أدى إلى وقوع الكثير من مستخدمي هذه المواقع فريسة الاحتيال والنصب عليهم، ومن أشهر حالات النصب عبر مواقع التواصل الاجتماعي الاحتيال في التسويق الإلكتروني، الاحتيال في عروض الوظائف، الاحتيال عبر التسول الإلكتروني، الاحتيال عبر أسئلة الامتحان[20] .

2.2.1. الجرائم الواقعة على الأشخاص:

من أبرز الجرائم الواقعة على الأشخاص بواسطة البرامج المعلوماتية، جرائم الاعتداء على حياة الخاصة عبر الإنترنت، وجرائم الذم والقذف والتحقير عبر الأنترنت.

1.2.2.1. جرائم الاعتداء على حياة الخاصة عبر الإنترنت:

لقد حاول بعض الفقهاء وضع تعريف للحق في الحياة الخاصة فقد عرف الفقيه (**Martin**) الحق بالحياة الخاصة بأنه:" الحق بالحياة الأسرية والشخصية والداخلية والروحية لشخص عندما يعيش وراء باب مغلق" [21].

وتعتبر الخصوصية من المبادئ العامة التي تقرها الدساتير أيضا لتضمن حماية حرمة الحياة الخاصة للمواطن، فجميع الأشخاص الحق في أن تظل أسرار حياتهم الخاصة مصانة عن العلن وتدخلات الغير وعلمه، و اعتداءاته عليها، وزادت أهمية حماية الحياة الخاصة إزاء تطور وسائل التواصل وانتشارها ليتم استخدام الوسائل المعلوماتية في هذا الجانب[22] .

2.2.2.1. جرائم الذم والقذف والتحقير عبر الإنترنت:

تعد جريمة السب والقذف والتعرض للحياة الشخصية للأفراد بغرض التشهير والخوض في أعراضهم، من أكبر الجرائم التي تم تجريمها في كافة القوانين، سواء في الدول العربية أو الدول الأجنبية، وترجع أسباب التجريم إلى تجريح الأشخاص في أعراضهم ومبادئهم وشرفهم ونسب أمور غير صحيحة إليهم بغرض التشهير بهم والخوض في أعراضهم وفي حياتهم الخاصة[23] .

والجرائم تتم إما عبر البريد الإلكتروني أو عن طريق شبكة الويب حيث ترتكب جريمة الذم والقدح إذا قام المعتدي بإسناد مادة للعلنية، أو بإسناده حكما أو صفة عامة في القدح إلى المعتدى عليه في أحد مواقع الشبكة الإلكترونية أو عن طريق مجموعات الأخباركما يلاحظ أن صور الذم والقدح يمكن أن تمارس من خلال مجموعات الأخبار في نشر التعليقات والمشاركة على مواضيع منشورة، وتتحقق علنية الذم والقدح إذا كانت رؤية ما يرد في الرسائل والتعليقات متاحة للجميع في مجموعات الأخبار أو عبر غرف الدردشة والمحادثة.

جامعة يحيى فارس المدية ، طريق عين الذهب، المدية ، **البريد الإلكتروني:** colloqueprff@gmail.com

3.2.1. الجرائم الواقعة على أمن الدولة:

لقد أصبحت عدة دول أمنها مهدد بفعل التطور التكنولوجيا الحاصل، وتنوعت الجرائم في هذا المجال بحسب طبيعتها، ومن بين أهم الجرائم الواقعة في على أمن الدولة، جريمة التجسس، جرائم الإرهاب، الجريمة المنظمة.

1.3.2.1. جريمة التجسس:

التجسس هو الاطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر وليس مسموحا لغير المخولين بالاطلاع عليها. وقد سهلت شبكة الإنترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية و الوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاث أهداف رئيسية وهي: التجسس العسكري، التجسس السياسي، والتجسس الاقتصادي، كما تستخدم العديد من الدول التجسس باستخدام التقنية المعلوماتية، وهذه الأنشطة تمارس من قبل دولة على دولة أو دول أخرى، أو من قبل الدول على مواطنيها، أو من قبل شركة على شركات أخري منافسة[24] .

2.3.2.1. جرائم الإرهاب:

يتم بث ثقافة الإرهاب عبر الإنترنت والوسائل الحديثة عن طريق تأسيس مواقع افتراضية تمثل المنظمات الإرهابية وهي مواقع آخذة في الازدياد مع ازدياد المنظمات الإرهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية احدى الهجمات التي ارتكبت، أو بيانات تنفي أو تعلق على أخبار صادرة من منظمات أو جهات دولية أخري. وتجند الجماعات الارهابية من خلال الإنترنت عبر وسائل وأنظمة الحواسيب الآلية عناصر ارهابية جديدة تساعدهم على تنفيذ أعمالهم الاجرامية، وهم في ذلك يعتمدون على فئة الشباب خصوصا ضعاف العقل والفكر[25] .

3.3.2.1. الجريمة المنظمة:

الجريمة المنظمة ليست وليدة التقدم وان كانت استفادت منه، فالجريمة المنظمة بسبب تقدم وسائل الاتصال والتكنولوجيات الحديثة أصبحت غير محدودة لا بقيود الزمان ولا بقيود المكان، وأصبح انتشارها على نطاق واسع وكبير كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة على وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية بسهولة، فقد اكتشفت هذه الجماعات أن استخدام شبكات الإنترنت والتكنولوجيا تستطيع أن تؤمن فرص جديدة وفوائد حية لأعمالهم وأرباح غير مشروعة عما يقومون به[26] .

3.1. خصائص الجرائم الإلكترونية:

تتميز الجريمة الإلكترونية بخصائص جعلتها تختلف عن الجريمة التقليدية، وذلك لتعلقها وارتباطها بشبكة الأنترنت ومن بين هذه الخصائص نجد مايلي:

1.3.1. صعوبة اكتشاف الجريمة:

الجريمة الإلكترونية من الجرائم التي ترتكب في الخفاء مما يزيدها صعوبة، حيث يتم نقل البيانات والمعلومات في شكل نبضات إلكترونية. كما أن هذه الجرائم في الغالب الأعم تكون منظمة، وترتب وتنفذ وتمس إقليم أكثر من دولة واحدة

لاستخدامها شبكة الاتصالات العالمية (الإنترنت)، أضف إلى ذلك امكانية تدمير الدليل في مدة قياسية، ومن بين الأسباب التي تؤدي إلى صعوبة اكتشافها صعوبات تعود الى الجاني وأخرى إلى المجني عليه[27].

1.1.3.1. صعوبات تعود إلى الجاني:

قد يكون المجرم في الجريمة الإلكترونية شخصا طبيعيا يعمل لحسابه الخاص ويهدف إلى تحقيق مصلحة شخصية له، ولكن في الغالب يقوم بهذا الفعل لحساب أحد الأشخاص المعنوية (شركة عامة أو خاصة) تستند في عملها على تكنولوجيا المعلومات، بغية السطو على أحد الأنظمة المعلوماتية أو اضرار بالغير[28] .

2.1.1.3.1. صعوبات تعود إلى المجني عليه:

المعتدى عليه في الجريمة الإلكترونية هو من يكون ضحية الاعتداءات غير المشروعة على مكونات الحاسوب، وقد يكون شخصا طبيعيا أو شركة أو مؤسسة تتعامل بمجال الحاسوب أثناء ممارسة الأعمال التجارية، والاقتصادية والسياسية التي ينبغي أن تستغل الحاسوب في إدارة أعمالها[29] .

توجه هذه الجرائم بصفة خاصة إلى البنوك والمواقع الإلكترونية للمؤسسات المالية، لأن القطاعات المستهدفة من الجريمة الإلكترونية هي التي تعتمد أكثر من غيرها على أجهزة الحاسوب وملحقاته وتعتبر تلك البنوك من أهم القطاعات وأكثرها تضررا[30].

2.3.1. صعوبة إثبات الجريمة:

الجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة. ما يجعل فكرة مسرح الجريمة في الجريمة الإلكترونية يتضاءل دوره في الافصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين:

– **الأول**: أن الجريمة المعلوماتية لا تخلق أثارا مادية.

– **الثاني**: أن كثيرا من الأشخاص يترددون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي فترة طويلة نسبيا، الأمر الذي يعطي مجالا للجاني أو للآخرين، أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت، الأمر الذي يولد الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية[31] .

2.الاجراءات العامة للبحث والتحري في الجرائم الالكترونية:

يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها[32].

إن الجريمة الإلكترونية كغيرها من الجرائم تتطلب إجراءات قانونية عامة من أجل فك ملابساتها، والتي تتمثل في الإجراءات المادية، والإجراءات الشخصية بالإضافة إلى إجراءات تقنية.

1.2. الإجراءات المادية:

تتضمن الإجراءات المادية المعاينة التقنية للوقوف على كيفية ارتكاب الجريمة، وكذا التفتيش المعلوماتي من أجل الحصول على الأدلة الكافية المتعلقة بالجريمة في حد ذتها.

1.1.2. المعاينة التقنية:

نصت المادة 79 من الأمر رقم 66- 155 المتضمن ق.إ.ج.ج والتي نصت على أنه:" **يجوز لقاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها...**".[33] .

كما يقصد بالمعاينة فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، كمعاينة مكان ارتكاب الجريمة أو أداتها، والمعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجرها بل على ما يقتضيه إجراؤها من مساس بحقوق الأفراد، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال، وإذا اقتضت دخول مسكن له حرمة خاصة كانت إجراء تحقيق[34].

1.1.1.2. إجراءات المعاينة التقنية:

تتمثل إجراءات المعاينة التقنية في الانتقال إلى مسرح الجريمة لمعاينته وتأمينه.

1.1.1.1.2. الانتقال إلى مسرح الجريمة:

تتم المعاينة في الجريمة الإلكترونية المرتكبة عبر الإنترنت أو بواسطة الحاسب الآلي كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية، إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني[35] .

ومن بين التدابير الفنية والتحفظية التي تساعد المحقق على المعاينة الإلكترونية هي كالآتي:

- الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد وموقع الأجهزة الإلكترونية وشبكاتها وسائر ملحقاتها والنهايات الطرفية المتصلة بها المتوقع مداهمتها.
- توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتأمين وحفظ المعلومات.
- التحفظ على محتويات سلة المهملات ومستندات الادخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.
- إعداد فريق من المتخصصين وأهل الخبرة في مجال تكنولوجيا الإعلام الآلي للاستعانة بهم عند الحاجة [36].

2.1.1.1.2. تأمين مسرح الجريمة:

من أجل ضمان حماية وتأمين لمسرح الجريمة الواجب مراعاة بعض الضوابط التالية:

- تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.
- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف، حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها وتأمينها.

– إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.

– أن تقتصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر فيهم الكفاءة العملية والخبرة الفنية في مجال الحواسيب[37] .

2.1.2. التفتيش:

التفتيش هو: "إجراء من إجراءات التحقيق تقوم به سلطة مختصة حددها القانون، يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة"[38] .

التفتيش في الجريمة الإلكترونية إجراء يحتاج إلى تقنيات خاصة، لأن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات الحاسوب ومجال إخفاء المعلومات فيها لأنه يسهل إتلافها جزئيا أو كليا، ويصعب تحديد مكان الدليل من حيث أنه داخل النظام أم على دعامة خارجية، وقد تكون الملفات مشفرة لا يظهر محتواها إلا بفك التشفير، وقد تكون البيانات التي تثبت حصول الفعل جزءا من نظام حاسوب يقع خارج الحدود في دولة أخرى، كل هذه الحقائق وغيرها يجعل تحديد السبب الموجب للتفتيش أمرا صعبا، ويجعل من تقديم وصف محدد لمحل التفتيش أمرا أكثر صعوبة[39].

1.2.1.2. الشروط القانونية للتفتيش في الجرائم الإلكترونية:

من أجل القيام بعملية التفتيش في الجرائم الإلكترونية لابد من توافر مجموعة من الشروط الشكلية والموضوعية.

1.1.2.1.2. الشروط الشكلية:

وهي شروط ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء حفاظا على الحريات الفردية من التعسف أو الانحراف في استخدام السلطة[40] وهي كالآتي:

1.1.1.2.1.2.الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في البيئة الإلكترونية:

يعتبر هذه الإجراء من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم، حيث أن ا لمتهم هو الشخص الذي يستوجب القانون حضوره عند إجراء التفتيش، إذ أن الإجراء المتخذ يمسه هو، غير أنه قد لا يتسنى للمتهم الحضور في حال كان محل التفتيش مسكنه، فمن أجل ذلك أجاز القانون له أن يُنيب عنه غيره ليجري التفتيش في حضوره، وإلا وجب استدعاء شاهدين في بعض الأحوال، كما يحق للمتهم أن يستعين بمحاميه عند إجراء التفتيش، ومن ثم يجوز للمحامي الحضور أيضا، كذلك إذا جرى التفتيش لدى غير المتهم وجب إتاحة الفرصة لحائز المكان في الحضور رعاية لمصالحه، ويخول المشرع للنيابة العامة أيضا حق الحضور أثناء التفتيش الذي يجريه قاضي التحقيق[41] .

2.1.1.2.1.2.موعد إجراء التفتيش في الجرائم الإلكترونية:

اختلفت التشريعات الإجرائية في وضع مبدأ موحد يخص الميعاد الزمني للتفتيش لنظم المعلوماتية، فمنها من حظر القيام بهذا الإجراء في أوقات معينة في الليل مثلا، وهنالك من قرنه بوقت معين حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المساكن، وهنالك من تركه على مطلقه يتم في أي ساعة من ساعات الليل والنهار وترك السلطة التقديرية في ذلك للقائم أو للسلطة المكلفة بالتفتيش[42].

أما عن المشرع الجزائري فقد تطرق إلى هذه الجزئية من خلال نص المادة 47 من ق.إ.ج.ج.، والتي جاء فيها: "عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

جامعة يحيى فارس المدية ، طريق عين الذهب، المدية ، البريد الإلكتروني: colloqueprff@gmail.com

وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".

3.1.1.2.1.2. محضر التفتيش في الجرائم الإلكترونية:

باعتبار أن التفتيش عمل من أعمال التحقيق، فينبغي تحرير محضر يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما، ثم ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسوب والإنترنت يرافقه للاستعانة به في صياغة مسودة محضر التفتيش[43]

2.1.2.1.2. الشروط الموضوعية:

وهي الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاث شروط أساسية هي السبب، المحل، والسلطة المختصة بالقيام بالتفتيش[44].

1.2.1.2.1.2. سبب التفتيش في البيئة الإلكترونية:

فالسبب هو وقوع الجريمة جناية أو جنحة، وتوافر أمارات قوية وقرائن على وجود دليل يفيد في كشف الجريمة لدى المتهم أو غيره وهذا السبب لا ينشأ إلا بعد وقوع الجريمة، واتجاه قرائن الاتهام ضد شخص، أو وجود أمارات قوية ضد آخر على حيازته ما يفيد في كشف الحقيقة[45].

2.2.1.2.1.2. محل التفتيش:

يشترط كذلك لصحة ومشروعية التفتيش في الجريمة الإلكترونية أن ينصب على محل بحيث يشترط أن يكون محددا أو قابلا للتحديد ويكون مشروعا يرد على محل جائز قانونا. كالمكونات المادية والمعنوية للكمبيوتر وملحقاته وبرامجه، الهاتف الذكي وشبكات الاتصال عن بعد، كما نشير إلى استثناء بعض الأشخاص والأماكن من التفتيش مثل أشخاص ومساكن وسيارات أعضاء السلك الدبلوماسي وأعضاء المجالس النيابية، ومكاتب المحامين لتمتعه بالحصانة، وعليه فأي تفتيش لها يعد منافيا للقانون ومآله البطلان[46] .

3.2.1.2.1.2. السلطة المختصة بالقيام بالتفتيش:

إن التفتيش إجراء قاصر على السلطة المختصة به وهي قاضي التحقيق والنيابة العامة، فالنيابة العامة توجه الاتهام وقاضي التحقيق يباشر الإجراءات بما فيها التفتيش. كما أنه يجوز لقاضي التحقيق القيام بإجراء التفتيش في أي مسكن يرى أنه توجد به أشياء من شأنها أن تفيد التحقيق وإظهار الحقيقة. وزيادة على ذلك له الحق في إنابة أحد ضباط الشرطة القضائية للقيام بهذا التفتيش (بشروط حددتها المواد من 138 إلى 142 من ق.إ.ج.ج) إذا استحال على قاضي التحقيق تنفيذه بنفسه[47].

2.2.1.2. إجراءات التفتيش:

يقع التفتيش على جانبين في الجرائم الإلكترونية على الجانب المادي وعلى الجانب المعنوي، وذلك من أجل فك ملابسات الجريمة.

1.2.2.1.2. تفتيش منظومة الحاسب الآلي المادية:

يتكون الحاسوب من كيانات مادية، تتمثل في وحدة المدخلات، ووحدة الذاكرة الرئيسية، ووحدة الحاسوب والمنطق، وحدة التحكم، وحدة المخرجات، ووحدات التخزين الثانوية، وفي الواقع أغلب الجرائم المعلوماتية تقع على معدات الحاسب، وشاشة العرض ومفاتيح تشغيلها وغيرها، وإن الولوج إلى هذا النوع من الكيانات للبحث عن شيء يفيد في كشف الحقيقة، والبحث عن مرتكبيها بشأن جريمة معلوماتية وقعت يخضع لإجراءات قانونية خاصة بالتفتيش ولا يثير أية صعوبة[48] .

2.2.2.1.2. تفتيش مكونات الحاسب الآلي المعنوية:

يقصد بها أنظمة الكمبيوتر والبيانات المخزنة فيه التي جرى التلاعب فيها أو تغييرها وغيرها من الوسائط التي تساعد على تخزين المعلومات[49]، فالبيانات والمعلومات المخزنة في الحاسب الآلي تصلح لأن تكون محلا للتفتيش، ويمكن ضبطها واستنساخها على الورق أو الأقراص، أو على أي دعامة أخرى كالفلاش ميموري (Flash Memory)، بحيث يمكن الاستناد إليها كدليل على ارتكاب المتهم الجريمة في مرحلة المحاكمة[50] .

2.2. الإجراءات الشخصية:

وهي مجموعة الإجراءات التي تتعلق بالشخص في حد ذاته، وتتمثل في الشهادة والخبرة بحيث يعتبران من أهم الأدلة في المواد الجنائية.

1.2.2. الشهادة:

يقصد بالشهادة " إقرار من الشاهد بأمر رآه أو سمعه أو أدركه بأي حاسة من حواسه".[51]، وللشهادة عدة شروط حتى يحتكم إليها القاضي كدليل إثبات ومن بينها مايلي:

1.1.2.2.التمييز:

هي القدرة على فهم ماهية الفعل وطبيعته وتوقع الآثار التي من شأنه احداثها. وهذه القدرة تنصرف إلى ماديات الفعل فتتعلق بكيانه وعناصره وخصائصه، وتنصرف كذلك إلى آثاره من حيث ما تنطوي عليه من خطورة على المصلحة أو الحق الذي يحميه القانون وما تنذر به من اعتداء عليه.

2.1.2.2. تحليف اليمين:

ألزم الشرع الشاهد أن يحلف اليمين قبل أداء الشهادة، وذلك كضمانة تضفي عليها الثقة كي تكون دليلا يستمد منه القاضي اقتناعه، وتعطي لها قيمتها القانونية من جهة، ومن جهة أخرى تجلب هذه المشكلة انتباه الشاهد إلى خطورة ما سيُدلي به، حيث تجعله حريصا على قول الحق.

3.1.2.2. حرية الاختيار:

ينبغي أن يكون الشاهد متمتعا بإرادة حرة عند الإدلاء بشهادته بمعنى أن لا تكون أقواله صادرة إثر تهديد أو إكراه وإنما يشترط أن تكون صادرة عنه بمحض إرادته.[52].

2.2.2. الخبرة:

تعرف بأنها "استشارة فنية يستعين بها القاضي و المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى دراية علمية لا تتوفر لدى السلطة القضائية المختصة"[53]. فالخبرة في الجريمة الإلكترونية إجراء يهدف إلى استخدام قدرات شخص سواء كانت فنية أو علمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن وقوع الجريمة[54] .

3.2. الإجراءات التقنية:

الإجراءات التقنية تتطلب جمع المعلومات والبيانات الخاصة بالجريمة أو ما يعرف بمرحلة جمع الاستدلالات التي تعتبر بمثابة المرحلة التمهيدية، وفي الوقت ذاته التقاط القرائن والأدلة.

1.3.2. جمع الاستدلالات:

"ينصرف مفهوم الاستدلال إلى تجميع المعلومات والبيانات الخاصة بالجريمة، وذلك عن طريق التحري والمراقبة والبحث عن الفاعلين بشتى الوسائل القانونية، كما يقصد بها ضبط الواقعة الإجرامية عن طريق التحري عنها، والبحث عن مرتكبيها بكافة الأساليب القانونية المشروعة، وجمع كل ما يمكن جمعه من المعلومات بشأنها[55].

2.3.2. ضبط الدليل الإلكتروني:

يعرف الضبط بأنه: "وضع اليد على شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبها، بهدف ضبط الأدلة والوثائق والأشياء التي تفيد في كشف الجريمة". كما يعرف الدليل الإلكتروني بأنه: " **الدليل الذي يوجد أساسا في العالم الافتراضي ويقود إلى الجريمة، فهو كل البيانات التي يمكن إعدادها أو تخزينها بشكل إلكتروني، بحيث تمكن الحاسب من إنجاز مهمة ما**"[56].

1.2.3.2. حجية الدليل الإلكتروني:

الدليل الإلكتروني دليل جنائي رقمي وحتى يتم قبوله كدليل إثبات يجب أن يتم الحصول عليه بطريقة مشروعة، وذلك من خلال أن يكون الإجراء المتبع في استخلاص الدليل الجنائي الرقمي مشروعا، عن طريق مراعاة القواعد الموضوعية والشكلية أثناء اتخاذ أي إجراء، حيث تتمثل القواعد الموضوعية في أن يكون الإجراء الذي يستهدف استخلاص الدليل الجنائي الرقمي عملا إراديا صادرا من شخص له صلاحية القيام به بناء على سبب معين، زيادة على ذلك يجب أن يكون المحل الذي يرد عليه الإجراء محددا أو قابل للتحديد وأن يكون مشروعا، وأما بالنسبة للقواعد الشكلية فيجب الالتزام باحترام كيفية مباشرة تنفيذ هذا الإجراء، ودائما ما تكون القواعد الشكلية محددة بموجب القانون[57].

3. الإجراءات الخاصة لمرحلة البحث والتحري في الجرائم الإلكترونية:

لقد استحدث المشرع الجزائري جملة من الإجراءات الخاصة بمرحلة البحث والتحري، وهذا تماشيا مع الأساليب المستجدة لارتكاب الجرائم.

1.3. اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

تعتبر عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من الأساليب التي اتخذها المشرع الجزائري من أجل حماية الأشخاص والممتلكات، وذلك كونها تتميز بطابع السرية.

1.1.3. اعتراض المراسلات:

يقصد بعملية اعتراض المراسلات والتي أشار إليها المشرع الجزائري من خلال نص المادة 65 مكرر 05 من ق.إ.ج.ج أنها: "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض" .

وبالتالي المراسلات حصرها المشرع الجزائري في الشكل الكتابي فقط، إلى أن جاء القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتهما، والذي جاء فيه من خلال نص المادة الثانية الفقرة السادسة "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[58].لذا يمكننا القول أن المراسلات تعني كل رسالة مكتوبة بأي شكل من الأشكال سواء مادية أو إلكترونية، وسواء كانت على دعامة ورقية أو رقمية، مرسلة بأي وسيلة لعدد معين ومحدد من المرسل إليهم، باستثناء الكتب والمجلات والجرائد والحوليات التي لا تعتبر من قبيل المراسلات الخاصة[59].

2.1.1.3. خصائص اعتراض المراسلات:

من بين خصائص اعتراض المراسلات نجد مايلي:

1.2.1.1.3. اعتراض المراسلات يتم خلسة بدون رضا وعلم صاحب الشأن:

اعتراض المراسلات هو إجراء يتم دون رضا وعلم صاحب الشأن، فلو كان صاحب الشأن عالم بالإجراءات المطبقة عليه لا تطبق بذلك خاصية الاعتراض، وكذا عند وضع الخط الهاتفي تحت المراقبة، لا يمكننا القول بأننا أمام إجراء الاعتراض، لهذا فهو سري[60].

2.2.1.1.3. تستهدف عملية اعتراض المراسلات الحصول على دليل غير مادي:

إن ضرورة البحث والتحري عن الجرائم تقتضي الوصول إلى شيئين وهما الحصول على أدلة مادية أو غير مادية. فالأدلة المادية هي التي تنبعث من عناصر مادية ناطقة بنفسها وتؤثر في اقتناع القاضي بحكم العقل والمنطق، في حين الأدلة القولية هي التي تنبعث من عناصر شخصية تتثمل فيما يصدر عن الغير من أقوال وتؤثر في اقتناع القاضي بطريق غير مباشر بتأكده من صدق هذه الأقوال[61].

3.2.1.1.3. استناد اعتراض المراسلات على أجهزة قادرة على التقاط الأحاديث:

أصبح استخدام الوسائل الحديثة الحصول على معلومات وأخذ نسخة منها دون الانتقال إلى مكان وجودها، كما أنها تستطيع أن تفصل الأصوات المسموعة وتميزها عن بعضها من أجل الوصول إلى الصوت المراد سماعه من بين تلك الموجودة في ذلك المكان، ويمكن للقائمين بها أن يجعلوا منها عملية فعالة ومفيدة، بالإضافة إلى إمكانية استنتاج الأدلة المادية على ارتكاب الجريمة وعلى كيفية أدائها دون علم وملاحظة المجرم بذلك[62].

2.1.3. تسجيل الأصوات:

يقصد به النقل المباشر والآلي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمله من عيوب في النطق إلى شريط تسجيل بحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي، بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه[63]. والمشرع الجزائري لم ينص في قانون الإجراءات الجزائية على تعريف التسجيل الصوتي، لكن أشار إلى ذلك من خلال نص المادة 65 مكرر 05 حيث جاء فيها: " **وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية** "[64]

1.2.1.3. طرق تسجيل الأصوات:

التسجيل الصوتي لايتم إلا بطريقتين: يكون إما عن طريق التسجيل المباشر أو التسجيل غير المباشر.

1.1.2.1.3. التسجيل المباشر:

يتم تسجيل الصوت مباشرة من المصدر دون وسيط في ذلك، مثال وجود جهاز التسجيل في نفس المكان الذي به الشخص، بحيث يتم رصد الصوت مباشرة فور خروجه من الشخص على شريط التسجيل.

2.1.2.1.3. التسجيل غير المباشر:

يقصد به إجراء التسجيل عن طريق وسيط ينقل الصوت من مصدره إلى المسجل، أو بالأحرى عدم وجود مصدر الصوت أمام جهاز التسجيل، أو آلة التقاط الصوت (الميكروفون) مباشرة، بل إن الصوت هنا ينقل عبر الهاتف، مثلا ليلتقطه جهاز التسجيل أو نقل الصوت، أو أن يتم التسجيل من تسجيل صوت آخر[65] .

3.2.3. التقاط الصور:

لم يشر المشرع الجزائري إلى مفهوم التقاط الصور وإنما أشار إلى ذلك في نص المادة 65 مكرر09 من ق.إ.ج.ج بمصطلح "الالتقاط"، في حين عرفها البعض بأنها: "تمثيل لشخص أو شيء عن طريق أحد الفنون من نقش أو نحت أو تصوير فوتوغرافي أو فيلم، ولم تقف الصورة عند حد تجسيد المادة لشخص ما بل تعدت ذلك إلى عكس شخصيته وانفعالاته"[66].

أما فيما يخص إجراءات التقاط الصور فالمشرع الجزائري لم ينص على شروط وإجراءات خاصة بهذه العملية، وهذا ما يفسر رغبة المشرع في الربط بين إجراء عملية التقاط الصور والأحكام المتعلقة باعتراض المراسلات وتسجيل الأصوات.

2.3. التسرب:

عرف المشرع الجزائري التسرب من خلال نص المادة 65 مكرر 12 من ق.إ.ج.ج. والتي جاء فيها: " **يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف**".

1.2.3. صور التسرب:

للتسرب عدة طرق نص عليها المشرع الجزائري في نص المادة 65 مكرر 12 من ق إ.ج.ج، ويتم ذلك من خلال الصور التالية:

1.1.2.3. المتسرب كفاعل:

الفاعل هو ما جاء بيانه في نص المادة 41 من قانون العقوبات كالتالي: "**يعتبر فاعلا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو اساءة استعمال السلطة الولائية أو التحليل أو التدليس الإجرامي**"[67].

2.1.2.3. المتسرب كشريك:

لقد جاء في نص المادة 42 من ق.ع.ج تعريف الشريك بأنه: " **يعتبر شريكا في الجريمة من لم يشترك اشتراكا مباشرا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك" فالعلم بالجريمة يشكل عنصرا أساسيا في الاشتراك**".

3.1.2.3. المتسرب كخاف:

عرف المشرع الجزائري الاخفاء في المادة 387 من قانون العقوبات على أنه:" **كل من أخفى عمدا أشياء مختلسة أو مبددة أو متحصلة من جناية أو جنحة في مجموعها أو جزء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر**".

4.1.2.3. التسرب في نطاق الجرائم الالكترونية:

يمكن تصور عملية التسرب في الجرائم الإلكترونية من خلال دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، كالمشاركة في غرف محادثات الدردشة أو حالات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو انخراطه في مجموعات ونوادي الهاكر، مستخدما في ذلك أسماء وصفات مستعارة وهمية ظاهرا فيها وكأنه واحد مثلهم قصد استدراجهم وللكشف عنهم وعن أعمالهم الإجرامية، كما يمكن تكييف عمل المتسرب على أنه شاهد [68].

2.2.3. شروط عملية التسرب:

تتمثل شروط عملية التسرب فيما يأتي:

1.2.2.3. تقرير ضباط الشرطة القضائية:

يقوم ضباط الشرطة القضائية قبل مباشرة عملية التسرب بكتابة تقرير إلى وكيل الجمهورية، وهذا كمبدأ عام على أعمال الشرطة القضائية. كما نصت المادة 65 مكرر 13* من ق.إ.ج.ج صراحة أن ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب هو المسؤول عن تحرير التقرير.

2.2.2.3. الحصول على الإذن:

لا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات المختصة والمتمثلة في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه، ولا يكفي صدور الإذن من الجهة المختصة فحسب، بل لابد أن يكون مكتوبا و إلا كان هذا الإجراء باطلا[69].

3.2.2.3. السرية في عملية التسرب:

أوجب المشرع الجزائري في عملية التسرب وأحاطها بالسرية الكاملة والمشددة وهذا ما نصت عليه المادة 65 مكرر 16 من ق.إ.ج.ج و التي تنص على: " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات"[70].

3.3. المراقبة الإلكترونية:

عرف الفقه إجراء المراقبة الإلكترونية على أنه: "مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر"[71]. والمراقبة الإلكترونية تشمل مراقبة مراقبة الاتصالات الإلكترونية أو مراقبة الأشخاص والأشياء والأموال.

1.3.3. مراقبة الاتصالات الإلكترونية:

لم يتطرق المشرع الجزائري إلى المقصود من مراقبة الاتصالات الإلكترونية، لكنه عرف الاتصالات الإلكترونية ويقصد بها: "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال"[72].

2.3.3. حالات اللجوء إلى المراقبة الإلكترونية للاتصالات:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[73].

2.2.3. مراقبة الأشخاص و الأشياء والأموال:

مراقبة الأشخاص أو ما يعرف بملاحظتهم وتتبعهم، تعني وضع هؤلاء تحت أعين رجال الضبطية القضائية لترصد تحركاتهم وتنقلاتهم والأماكن التي يتردد عليها المشتبه بهم واتصالاتهم بالأشخاص الآخرين، وكذلك يمكن مراقبة حتى نمط معيشتهم إن تطلب الأمر، وفي سبيل الكشف عن أفراد هذه الشبكات الإجرامية، يقوم رجال الضبطية القضائية بمراقبة وترصد حركة الأموال، وتتبع وجهتها مثل ما هو الحال في جريمة تبييض الأموال، وذلك بهدف المساهمة في الكشف عن عمليات إعادة توظيف الأموال الناتجة عن الجرائم وتمويل النشاطات الإرهابية بالجزائر والوقاية منها والردع عنها.

كما تنصب المراقبة على أشياء قد تستغل في ارتكاب الجريمة، حيث تكون هذه المواد محل تتبع وملاحظة رجال الضبطية القضائية لمعرفة الوجهة الحقيقية لهذه المواد بغية وضع اليد على التنظيم الاجرامي وتفكيكه[74].

خاتمة:

أولا: النتائج: من خلال هذه الورقة البحثية توصلنا إلى النتائج التالية:

– يرتبط مفهوم الجريمة الإلكترونية بكل الأفعال الغير مشروعة التي لها علاقة مع البيئة الرقمية، والتي تهدد حياة الإنسان أو ممتلكاته أو المؤسسات العمومية أو الخاصة.

– تختلف الجريمة الإلكترونية على الجريمة التقليدية، كونها تقع في عالم افتراضي يصعب الاحاطة بها وفك جميع ملابساتها.

– يتميز الجاني في الجريمة الإلكترونية بالذكاء العالي، وسرعة التنفيذ، ومسح آثار الفعل الغير مشروع.

– يشترط في مرحلة البحث والتحري اتخاذ كافة الإجراءات القانونية اللازمة والتي حددها المشرع الجزائري، والتي تتناسب مع طبيعة الجريمة الإلكترونية، وخاصة عنصر الخبرة.

– إجراءات البحث والتحري الخاصة بالجرائم الإلكترونية تتطلب وسائل تقنية حديثة، كتسجيل الأصوات والتقاط الصور والتسرب.

ثانيا: التوصيات: من جملة ما يمكن طرحه كتوصيات ما يأتي:

– ضرورة تكوين محققين مختصين في الجرائم الإلكترونية، يتمتعون بالكفاءة والمهارة اللازمة من أجل فك ملابسات مثل هذا النوع من الجرائم.

– تعزيز أساليب الرقابة على الشبكة المعلوماتية، حتى يضيق على كل من تسول له نفسه الاعتداء على حرمة الأشخاص أو ممتلكاتهم، أو تخريب واختراق الأنظمة والبرامج الخاصة بالأشخاص المعنوية.

– سن قوانين أكثر ردع على الجناة تصل عقوبتها إلى المؤبد أو الإعدام، لأن مثل هذه الجرائم لها آثار جسيمة على الفرد والمجتمع والدولة، وحتى على الأمن العالمي.

---

[1] – غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية، د.ط، الجزائر،2015م ص14.

[2] – محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة، ط.1، عمان الأردن، 2007، ص08.

[3] . سميرة معاشي، ماهية الجريمة الإلكترونية، مجلة المنتدى القانوني، ع7، جامعة بسكرة، ص276.

[4] – عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2013م، ص21.

[5] – سميرة معاشي، ماهية الجريمة الإلكترونية، مرجع سابق، ص277.

[6] – – غنية باطلي، الجريمة الإلكترونية، مرجع سابق، ص17.

[7] – أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)، دار الجامعة الجديدة، دط، الإسكندرية، مصر، 2007م، ص86.

[8] – سامي علي حامد عياد، الجريمة المعلوماتية واجرام الإنترنت، دار الفكر الجامعي، دط، الاسكندرية، مصر، 2007م، ص43.

[9] – فريال لعاقل، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر، كلية الحقوق، جامعة أكلي محند اولحاج، البويرة، الجزائر، 2015م، ص10.

[10] – فضيلة عاقلي، الجريمة الإلكترونية و إجراءات مواجهتها من خلال التشريع الجزائري، مركز جيل البحث العلمي، www.jilrc.com، 2022.02.12، 16.30.

[11] – فريال لعاقل، الجريمة المعلوماتية في ظل التشريع الجزائري، مرجع سابق، ص12.

[12] – المادة 02 الفقرة 1 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، ع47، ص05.

[13] – عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، دط، مصر، 2002م، ص01.

[14]- الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق ل 25 غشت 2021 المتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية.

[15] - المادة 211 مكرر 22 الفقرة الثالثة من قانون الإجراءات الجزائية.

[16] –ينظر: عبد الله بن مرزوق العتيبي، جريمة غسل الأموال وعلاقتها بالجرائم الحديثة، جامعة نايف للعلوم الأمنية، دط، الرياض، السعودية، 2009م، ص04-05.

[17] – ذياب موسى البداينة، الشباب والإنترنت والمخدرات، مركز الدراسات والبحوث، ط1، الرياض، المملكة العربية السعودية، 2011م، ص46.

[18] – ذياب موسى البداينة، الشباب والإنترنت والمخدرات، مرجع نفسه، ص47.

[19] – نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الإنترنت، دار نور، دط، د.م، 2017م، ص72.

[20] – زينب شاكر السماك، جرائم الاحتيال الإلكتروني www.annaba.org/arabic، 14 فيفري 2022م، 18:40.

[21] – آمنة بوشاقور، جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية، مذكر ماستر في القانون الجنائي للأعمال، كلية الحقوق، جامعة العربي بن مهيدي، أم البواقي، الجزائر، 2015م/2016م. ص23.

[22] – حنان ريحان مبارك المضاحكي، الجرائم المعلوماتية(دراسة مقارنة)، منشورات الحلبي الحقوقية، ط1، سوريا، 2014م، ص322.

[23] – ليلى لفويلي، الجريمة الإلكترونية، مذكرة ماستر في قانون العقوبات والعلوم الجنائية، كلية الحقوق، جامعة قسنطينة01، قسنطينة، الجزائر، 2012م، ص37.

[24] – . محمد أمين بالبحري، زينب بو العام، الجريمة الإلكترونية كجريمة منظمة عابرة للحدود، مذكرة ماستر، كلية الحقوق، جامعة منتوري، قسنطينة، 2014م/2015م، ص53.

[25] – يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2012م/2013م، ص 55.

[26] – يوسف صغير، الجريمة المرتكبة عبر الإنترنت، المرجع نفسه، ص56.

[27] – غنية باطلي، الجريمة الإلكترونية، مرجع سابق، ص34.

[28] – محمد عبد الله أبو بكر، موسوعة جرائم المعلوماتية – جرائم الكمبيوتر والإنترنت – ، المكتب العربي الحديث، دط، الإسكندرية، مصر، 2007م، ص49.

[29] – فاطمة الزهراء بخي، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، 2013م، ص18.

[30] – فاطمة الزهراء بخي، إجراءات التحقيق في الجريمة الإلكترونية، المرجع نفسه، ص19

[31] – عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، المرجع السابق، ص59.

[32] - المادة 211 مكرر 25 من قانون الإجراءات الجزائية.

[33] – المادة 79 من الأمر رقم 66- 155، المؤرخ في 18 صفر 1386هـ الموافق لـ 08 جوان 1966م المتضمن قانون الاجراءات الجزائية، ج.ر، ع84 ، ص38.

[34] – عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة الدكتور طاهر مولاي، سعيدة، الجزائر، 2016م، ص28.

[35] – ابتسام بغو، اجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة ماستر في القانون الجنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، الجزائر، 2015م/2016م، ص63

[36] – ينظر: بشير حماني، خصوصية التحقيق في الجريمة الإلكترونية، مذكرة ماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2019م، ص64-65.

[37] – ابتسام بغو، اجراءات المتابعة الجزائية في الجريمة المعلوماتية، المرجع السابق، ص65.

[38] – عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، دار الثقافة، ط1، الأردن، 2010م، ص500-501

[39] – خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، ط1، عمان، الأردن، 2011م، ص151.

[40] – عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، دط، الإسكندرية، مصر، 2010م، ص108.

[41] – ينظر: عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية أو الاستثنائية، المرجع السابق، ص515- 516.

[42] – عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، وهران، الجزائر، 2013م، ص194.

[43] – ينظر: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، المرجع السابق، ص112-113.

[44] – عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، المرجع نفسه، ص99.

[45] – عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، مرجع سابق، ص512- 513.

[46] – ينظر: جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018م، ص58

[47] – ينظر: المواد 81.82.83.84 من ق.إ.ج.ج.

[48] – راضية بن جاب الله، إجراءات التفتيش على ضوء قانون الإجراءات الجزائية الجزائري، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، المسيلة، الجزائر، 2013م، ص72.

[49] – خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، ط1، عمان، الأردن، 2011م، ص159.

[50] – أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، ع58، م29، الرياض، المملكة العربية السعودية، ديسمبر 2013م، ص90.

[51] – عماد محمد ربيع، حجية الشهادة في الإثبات الجزائي، دار الثقافة، ط1، عمان، الأردن، 1999م، ص109.

[52] – ينظر:عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، مرجع سابق، ص133.

[53] – يسعد روبيو، فرحات يايا، الخبرة القضائية ودورها في الإثبات، مذكرة ماستر في المهن القانونية والقضائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، 2019م، ص12.

[54] – ينظر: عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، المرجع السابق، ص383.

[55] – عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، المرجع نفسه، ص197

[56] – خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، المرجع السابق، ص229.

[57] – عبد المطلب طاهري، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، 2015م، ص20.

[58] – القانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق لـ05 أوت 2009م المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر، ع47

[59] – عبد المطلب طاهري، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، 2015م، ص20.

[60] – نصر الدين مروك، محاضرات في الاثبات الجنائي، دار هومة، ط3، الجزائر، 2009م، ص 132.

[61] – فوزي لواتي، التحقيق في جرائم المخدرات على ضوء أساليب التحري الخاصة، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر1، الجزائر، 2015م، ص18

[62] – ليدية سعدلي، كاهنة العيدي، تعزيز مكانة ضباط الشرطة القضائية ضمن استراتيجية مكافحة الفساد، مذكرة ماستر في القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، 2018م، ص09.

[63] – عبد القادر رويس، أساليب البحث الخاصة وحجيتها في الاثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية، ع 3، جوان 2017م، ص40.

[64] – ينظر : المادة 65 مكرر 05 الفقرة 02 من الأمر رقم 66-155، مرجع سابق، ص29.

[65] – وسام عواس، مشروعية وسائل البحث الجنائي الحديثة، شهادة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2014م، ص 104.

[66] – رشيد شميشم، الحق في الصورة، مجلة العلوم الانسانية، ع3، 2008م، ص127

[67] – المادة 41 من الأمر 66-156 المؤرخ في 18 صفر 1386هـ الموافق لـ 08 جوان 1966م المتضمن قانون العقوبات المعدل والمتمم بالقانون رقم 82-04 المؤرخ في 13 فيفري 1982م، ج.ر، ع07، ص318

[68] – ينظر: لامية وعلي، كاهنة سعودي، إجراءات مكافحة الجريمة الالكترونية، مذكرة ماستر في القانون الجنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، 2019م، ص99-100.

[69] – ينظر: جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص85- 86.

[70] – ينظر المادة 65 مكرر 16 من ق.إ.ج.ج.

[71] – بشير حماني، خصوصية التحقيق في الجريمة الالكترونية،المرجع السابق، ص73- 74.

[72] – ينظر: المادة 05 من المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015م الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، ع53، ص17.

[73] – ينظر: سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية، مجلة الباحث للدراسات الأكاديمية، ع9، جوان 2016م، ص394.

[74] – ينظر: ميليسة سليماني، نصيرة خلوات، خصوصيات المعاينة في الجرائم المستحدثة، مذكرة ماستر في القانون الجنائي والعلوم الإجرامية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2017م، ص55.54.53.