تاريخ الاستلام:.2021/05/02.تاريخ القبول: 2021/07/08

الجريمة الالكترونية و إجراءات مواجهتها في التشريع الجزائري

Electronic crime and measures to confront it in the Algerian legislation

معزوز ربيع *
المركز الجامعي علي كافي
تندوف(الجزائر)
maazouz.rabie@yahoo.fr

زروقي عاسية
جامعة غرداية
(الجزائر)
Zerrouki.assia@univ-ghardaia.dz

ملخص: إن التطور الحاصل في تكنولوجيا الحاسب الآلي وظهور الشبكة العالمية للإنترنت بقدر ما سهلت الحياة واختصرت الوقت والجهد وما قدمته للبشرية من تسهيلات وخدمات وإيجابيات غيرت نمط الحياة للشعوب وساهمت في تطورها ورقيها، بقدر ما أساء البعض استخدام هذه التكنولوجيا وتطويع الانترانت وغيره من الوسائل التكنولوجيا لارتكاب نوع جديد من جرائم التكنولوجيا الحديثة، والتي تتم عبر معدات وأجهزة إلكترونية أو باستخدام شبكة الإنترنت لارتكابها.

كلمات مفتاحية: جريمة، الكتروني، تقنيات، تشريع جزائري، مكافحة.

Abstract:
The development in computer technology and the emergence of the Internet as much as it facilitated life and shortened the time, effort and facilities, services and pros it provided to humanity changed the lifestyle of peoples and contributed to their development and sophistication, to the extent that some misused this technology and adapted the Internet and other means of technology to commit a new type of modern technology crime, which is carried out through electronic equipment and devices or using the Internet to commit it.

Keywords:Crime, electronic, techniques, Algerian legislation, combat.

*المؤلف المرسل.

.مقدمة:

إنّ التطور الحاصل في تكنولوجيا الإعلام والاتصال وظهور شبكة الإنترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام، لأنه بقدر ما أحدث آثارا إيجابية وغيّر نمط حياة المجتمعات وساهم في التطور والرقي في جميع المجالات لاسيما المعاملات الإلكترونية، بقدر ما كان له أثر سلبي على حياة الأشخاص ومصالح الدول، تجلى في تطويع الانترنت والوسائل الإلكترونية لتكون عالما من عوالم الجريمة[1]، مما أدى إلى بروز الجريمة الإلكترونية أو المعلوماتية أو التقنية، وما استتبعه ذلك من مصطلحات جديدة كالإثبات الإلكتروني والمجرم الإلكتروني وغيرها.

والجريمة الالكترونية باعتبارها من الجرائم المعلوماتية المعاصرة العابرة للحدود الوطنية تثير في مجملها الكثير من الإشكاليات في عدّة نواحي، كصعوبة اكتشافها وكذا إثباتها نظرا لغياب الدليل المادي الذي يدين مرتكبها، لاسيما أن هذا الأخير يتسم بطابع الحيلة والدهاء ويستعمل تقنيات معلوماتية عالية الكفاءة، مما يؤدي إلى اختراق الشبكات وأجهزة الحاسب الآلي المرتبطة بالإنترنت، حيث يتم اختراق نظام الأمن بالشبكة والدخول إلى الجهاز للكشف عن محتوياته أو إتلافها والتلاعب بالمعلومات المخزنة فيه[2] من طرف المجرم الالكتروني بكل سهولة ويسر ودون أن يبذل الكثير من الجهد، وهذا راجع كون المجرم المعلوماتي يتسم بالذكاء الحاد، فضلا عن معرفته سبل الإفلات من العقاب.

تبعا لذلك، ونظرا لحداثة الجرائم الالكترونية، وتطورها مع تطور كل تقنية حديثة كما أسلفنا، الأمر الذي تطلب من المشرع الجزائري مواكبة التطور الحاصل على الصعيد التقني، من خلال استحداث نصوص تشريعية لمكافحة الجرائم الناتجة عن هذه التقنيات، ووضع حد لها وبالتالي العمل على تحليلها إن لم يكن في الإمكان القضاء عليها، وهكذا نجد أن المشرع الجزائري أدرج الفصل السابع مكرر من قانون العقوبات بمقتضى تعديله بموجب القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004، حيث استحدث بموجبه جرائم المساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 مكرر إلى 394 مكرر7 ق ع، وقد ضمنه مجموعة من القواعد الموضوعية حدد من خلالها الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء وعقوبة.

هذا بالإضافة إلى القانون رقم 09-04 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وبمقتضاه وسع المشرع من مفهوم الجريمة الإلكترونية لتشمل إلى جانب جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، الجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية.

وعلاوة على هذه الآليات الإجرائية التي تضمنها القانون 09-04، فقد تضمن قانون الإجراءات الجزائية الجزائري مجموعة من الآليات الخاصة بالتحريات والتحقيقات في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مثل الآلية المتعلقة باعتراض المراسلات (المواد من65 مكرر 5 إلى المادة 65 مكرر 10 من قانون الإجراءات الجزائية الجزائري).

وبالنظر إلى خصوصية الجريمة الإلكترونية وخطورتها، نظرا لإمكانية اختلاف دولة المجرم الإلكتروني عن دولة المجني عليه وموضوع الجريمة، فقد توجد هذه العناصر في دول مختلفة كما هو الحال مثلا في جريمة سرقة خطوط الاتصالات الدولية وخطوط الانترنت والهاكرز وغيرها،ومثل هذه الحالات تحتاج لمعالجة من خلال تدخل المشرع الداخلي بسن نصوص قانونية،بالإضافة إلى ضرورة وجود تعاون دولي واتفاقيات دولية لمكافحة الجرائم الالكترونية.**وعليه تتمثل إشكالية الدراسة فيما يلي:ما هو مفهوم الجريمة الالكترونية؟ وما هي الإجراءات المتبعة للكشف عنها عبر مختلف مراحل الدعوى الجزائية؟.**

وقد تم الاعتماد على المنهج التحليلي باعتباره يخدم هذه الدراسة، وذلك بتحليل النصوص القانونية ذات الصلة بموضوع البحث،إضافة إلى المنهج الوصفي الذي ساهم بوصف هذه الجريمة ومفهومها وصفا يتناسب مع طبيعتها.

وتبعا للأهمية التي يتناولها موضوع الجريمة الالكترونية باعتبارها جريمة تطورت بتطور الوسائل التكنولوجية،نظرا للمخاطر التي تطرحها هذه الجريمة يستدعي تناولها بالدراسة والتحليل حتى يتمكن الباحث وكذا كل من له علاقة بالحقل القانوني التعرف على هذه الجريمة وإجراءات مواجهتها،وهذا ما سيتم معالجته في هذه محورين، المحور الأول بعنوان ماهية الجرائم الالكترونية، أما الثاني فنعرض فيه إجراءات المتابعة في الجرائم الالكترونية.

المحور الأول:ماهية الجريمة الالكترونية

إن ظاهرة الجرائم الالكترونية أو الجرائم التقنية العالية ظاهرة إجرامية مستحدثة نسبيا، ففي ظل انتشار الجريمة الالكترونية أصبحت المجتمعات تعاني من انتهاك الحقوق والخصوصية الالكترونية،وقد جاء تطور هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا التي يسرت سبيل التواصل وانتقال المعلومات بين مختلف الشعوب والحضارات وسهلت حركة المعاملات[3] ،إلا أن هذا التقدم المذهل والمميز لا يخلو من العيوب لأن استخدامه لا يقتصر على الإنسان الخير بل الإنسان الشرير الذي قد يوصف كمجرم لسعيه وراء أطماعه واقتناصه الفرص لتحقيق أغراضه غير المشروعة، وبالتالي لن يتوان عن استغلال التقنية لتطوير قدراته الإجرامية باستخدام شبكة المعلومات كوسيلة سهلة لتنفيذ العمليات الإجرامية[4].

أولا:تعريف الجريمة الالكترونية وخصائصها

نحاول ضبط تعريف للجريمة الإلكترونية ثم نتعرض إلى خصائصها

1/ تعريف الجريمة الالكترونية: الجريمة الالكترونية عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي،كما يعرفها البعض الأخر "بأنها تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها[5].

كما عرفها البعض على أنها"تلك الأعمال غير المشروعة التي تكون شبكة الانترنت أو إحدى تطبيقاتها إما وسيلة لها أو ضحية مستهدفة من قبل الفاعل أو الفاعلين"[6]، أو هي "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر شبكة الانترنت،أو تثبت عبر محتوياتها"[7]، كما يمكن تعريفها بأنها"جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت" أو "كل ما يمكن ارتكابه من أفعال غير مشروعة يعترف القانون بأنها جرائم" أو بأنها "تلك الجرائم التي لا تعرف الحدود الجغرافية و التي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الانترنت،وبواسطة شخص على دراية فائقة بهما"[8].

أو هي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية،أو داخل نظام حاسوب،وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية"[9].

وهكذا يستفاد من التعاريف المتقدمة أن الجريمة الإلكترونية محلها هو الحاسب الآلي، فيقدم على القيام بأحد الأفعال غير المشروع مستهدفا النظام المعلوماتي أو البيانات والمعلومات التي يتضمنها الجهاز. ومن هنا نصل إلى القول أن الجريمة الالكترونية من الجرائم المستحدثة وتكون وسيلة ارتكابها الحاسب الآلي ويكون للعلم ولتكنولوجيا الحاسبات الآلية قدرا كبيرا.

2/ خصائص الجريمة الالكترونية: تعتبر الجريمة الالكترونية عبر الانترنت من بين الجرائم المستحدثة التي أتى بها التطور في مجال الاتصالات، فهي تختلف عن الجريمة التقليدية في العالم المادي،فهي تتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل وهي على النحو التالي:

أ. خفاء الجريمة الإلكترونية وسرعة ارتكابها:تتسم الجرائم الناشئة عن استخدام الانترنت بأنها خفية مستترة في أغلبها،لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة،لأن الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة،كإرسال الفيروس المدمر وسرقة الأموال والبيانات الخاصة وإتلافها، والتجسس وسرقة المكالمات[10] وغيرها من الأفعال غير المشروعة.فالجرائم الالكترونية في أكثر صورها

خفية لا يلاحظها المجني عليه، أو يدري حتى بوقوعها، والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمر ليس في كثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبيها.

ب. اعتبارها أقل عنفا في التنفيذ: لا يتطلب هذا النوع من الجرائم في تنفيذها إلى مجهود كبير أو العنف فهي تتم بأقل جهد مقارنة بالجرائم التقليدية التي تتطلب نوعا من الجهد العضلي الذي قد يكون في صورة ممارسته للعنف والإيذاء، ولهذا نجد هذا النوع من الجرائم يتميز بطابعه الهادئ فكل ما يحتاج إليه المجرم هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني، فمن هذا المنطلق تعد الجريمة المرتكبة من الجرائم النظيفة فلا آثار فيها لأي عنف،وإنما مجرد أرقام وبيانات يتم تغييرها من السجلات في ذاكرة الحاسبات الآلية وليس لها أثر مادي[11].

ج. جريمة عابرة للحدود: بعد ظهور شبكات المعلوماتية لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المتخلفة،فالقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين الأنظمة يفصل بينهما آلاف الأميال أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة الإلكترونية الواحدة في آن واحد[12].

فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب هذه الجريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دول أخرى.

د. امتناع المجني عليهم عن التبليغ: لا يتم في الغالب الأعم الإبلاغ عن الجرائم الإلكترونية، إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، لذلك نجد أن معظم الجرائم تم اكتشافها بالصدفة بل وبعد وقت طويل من ارتكابها.

هـ. سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه:تكون البيانات والمعلومات المتداولة عبر شبكة الانترنت على هيئة رموز مخزنة على وسائل تخزين ممغنطة،لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمر صعب، لاسيما وأن الجاني يتعمد إلى عدم ترك أثر لجريمته وهذا ما يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك،إذ يتم عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح لجهاز الحاسوب.

و. نقص الخبرة لدى الأجهزة الأمنية والقضائية وعدم كفاية القوانين السارية: تتميز الجرائم الالكترونية بالكثير من السمات التي تختلف عن غيرها من الجرائم،الأمر الذي أدى إلى تغيير شامل في آلية التحقيق وطرق جمع الأدلة المتبعة من الجهات التي تقوم بعملية التحقيق،وإضافة أعباء تتعلق بكيفية الكشف عن هذه الجريمة وأدلتها، ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلب لاكتشافها والبحث عنها، وتستلزم أسلوب خاص في التحقيق والتعامل،الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي ضد هذه الظاهرة[13].

ثانيا ـ خصوصية الجريمة الإلكترونية

إن دراسة الجريمة الالكترونية بشكل خاص تدخل ضمن قسم من أقسام قانون العقوبات،وهو القسم الخاص وهو ذلك الفرع الذي يدرس كل جريمة على حده متناولا كل عناصرها الأساسية، والعقوبة المقررة لها[14]، فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة، وإن هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الالكترونية للبيانات،سواء كان بتجميعها أو تجهيزها أو في إدخالها إلى الحاسب الآلي المرتبطة بشبكة المعلومات ولغرض الحصول على معلومات معينة،كما قد ترتكب هذه الجرائم في مجال الكلمات أو معالجة النصوص، وهذا النوع الأخير من الجرائم لا يعدو أن يكون طريقة أوتوماتيكية للمستخدم من تحرير الوثائق والنصوص على الحاسب مع توفير إمكانيات التصحيح والمسح والتخزين والاسترجاع والطباعة[15].

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 الاعتداء أو تستخدم وسيلة له[16].

وتكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل المعلومات 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.

من هنا يثور التساؤل عن الطبيعة الخاصة للأفعال المجرمة، هل تدخل ضمن أحكام خدمات البريد أم التخابر الخاص؟، أم يكون الهدف الأساسي للتحري عن النظام 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 الأشخاص المسؤولين عن النشر،من خلال المجال التي ترتكب فيه الجريمة الالكترونية ومحل الاعتداء عليها تظهر لنا الطبيعة القانونية الخاصة للجريمة لاستخدامها في ارتكاب جرائم مختلفة،لأن الإجرام المعلوماتي يتعلق بالمعالجة الآلية للبيانات وإدخال المعلومات ونقلها،ومن ثم يتحتم ضمه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارنة عاجزة عن مواكبة التطور المعلوماتي وما يحويه من فراغ تشريعي في هذا المجال[17].

أما من حيث التكييف القانوني، فتتخذ هذه الجرائم طبيعة خاصة ذلك أن القواعد التقليدية ليست مخصصة لهذه الظواهر الإجرامية المستحدثة، ومن تمّ فإن 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 خاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال، فقد تكون البيانات التي تجرى للبحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة،و من هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة[18]. ومن العراقيل التي تطرحها هذه الجرائم أيضا هو صعوبة ملاحقة مرتكبي الجرائم الالكترونية الذين يقيمون في دولة أخرى دون أن ترتبط بهذه الدولة باتفاقية مع الدولة التي تحقق فيها السلوك الإجرامي أو جزء منه، وفي ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة[19].

ثالثا . مراحل تطور الجريمة الالكترونية:ظهرت الجرائم الالكترونية في حقل الجرائم التقنية العالية في نهاية الثمانينات،وكان ذلك من خلال العدوان الفيروسي، وبالأخص جريمة "دودة موريس"المؤرخة واقعتها في نوفمبر 1988، ولقد أطلق مصطلح جرائم الانترنت في المؤتمر المنعقد في استراليا في الفترة 16 /27 فيفري 1998، وتجدر الإشارة إلى أن الكثير من الباحثين يستخدمون مصطلح غير دقيق للتعبير عن الجرائم الإلكترونية[20]، إذ نجد البعض يستخدم مصطلح الإجرام المعلوماتي، ومنهم من يستخدم مصطلح جرائم التكنولوجيا المتقدمة أو مصطلح الغش المعلوماتي، في حين أنه يجب استخدام المصطلح الدقيق والمتماشي مع طبيعة تلك الجرائم الالكترونية، ذلك أن الإجرام المعلوماتي وإن كان يقصد التعبير عن الجرائم الواقعة عن طريق جهاز الكمبيوتر، إلا أن هذا لا يعني من جهة أخرى أن الاعتداء على المعلومة يتحقق دائما باستخدام الكمبيوتر،وخصوصا باستخدام الانترنت،ذلك لأن الوسائل التقليدية هي دائما ما تكون أداة لارتكاب تلك الجريمة،وبالتالي فالجريمة الالكترونية قد تكون أشمل من جرائم الانترنت وذات الشأن بالنسبة لمصطلح الغش المعلوماتي وكذا جرائم التكنولوجيا المتقدمة[21].

ولقد لاحظ مؤتمر القانون والانترنت المنعقد في لشبونة "البرتغال"في 2001/01/26 أنه يجب عدم الالتفات إلى مثل هذه المصطلحات غير الدقيقة،واعتماد مصطلح cyber crim دون غيره للتعبير عن جرائم الانترنت مع الأخذ بعين الاعتبار التمييز بين تلك الجرائم التي يمكن ارتكابها عبر الانترنت[22].

ومرت جرائم الانترنت بتطور تاريخي تبعا لتطور التقنية واستخدامها، ولهذا مرت بثلاث مراحل هي:

أ ـ المرحلة الأولى:من شيوع استخدام الحواسيب من الستينات إلى السبعينات من القرن الماضي اقتصرت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير الكمبيوتر،وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم شيء عابر أم ظاهرة إجرامية مستحدثة، وإن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة،لكن مع تزايد استخدام الحواسيب الشخصية في السبعينيات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، و بدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة[23].

ب ـ المرحلة الثانية:في الثمانينات حيث طفا على السطح مفهوم جديد للجرائم الالكترونية ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر ونزع الفيروسات الالكترونية التي تقوم بعملية تدميرية الملفات أو البرامج،وشاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم،لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محظورا في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقي،لكن هؤلاء المغامرون أصبحوا أداة إجرام،وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة له القدرة على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية والاجتماعية والسياسية والعسكرية.

ج ـ المرحلة الثالثة: شهدت التسعينيات تناميا هائلا في حقل الجرائم الالكترونية وتغيير في نطاقها ومفهومها، وكان ذلك بفضل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات، حيث ظهرت أنماط تقوم على فكرة تعطيل تقني ومنعه من القيام بعمله المعتاد،وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة ساعات في خسائر مالية بالملايين،ونشطت جرائم الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت وظهرت الرسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على الأحقاد أو المساس بكرامة واعتبار الأشخاص، أو المروجة لمواد غير قانونية أو غير المشروعة[24].

المحور الثاني:إجراءات المتابعة للجريمة الالكترونية

إن الجريمة الالكترونية تعتبر كأي جريمة من الجرائم المنصوص عليها في قوانين العقوبات والقوانين الأخرى، لذلك تتمتع الجريمة الالكترونية بدعوى عمومية وهذه الدعوى تتم بمراحل وهي كالآتي:

أولا: إجراءات جمع الاستدلالات في الجريمة الالكترونية:إن هذه المرحلة من اختصاص ضباط الشرطة القضائية،وهم نوعان النوع الأول الذين يتمتعون باختصاص عام ويختصون بإجراءات الاستدلال بشأن الجرائم المنصوص عليها في قانون العقوبات،أما النوع الثاني فهم ذو الاختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر، هؤلاء المشار إليهم في المادة 21 من قانون الإجراءات الجزائية الجزائري وسلطتهم كذلك محددة، لا تمتد إلى مرحلة التفتيش ودخول المنازل،المعامل والمباني والأماكن المحاطة بأساور إلا بحضور أحد ضباط الشرطة القضائية، ومن بين هؤلاء رؤساء الأقسام المهندسون وأعوان الغابات وحماية الأراضي، وتعد محاضرهم ذات حجية وقوة إثبات كما استقر عليه القضاء الجزائري، وما يهمنا في هذه الدراسة ضباط الشرطة القضائية ومجال اختصاصهما فيما يتعلق بالجريمة الالكترونية[25].

أ ـ الإجراءات التقليدية لجمع الدليل الالكتروني:ونتطرق فيه لإجراءين هما الإجراءات المادية والإجراءات الشخصية:

1ـ الإجراءات المادية: تتمثل هذه الإجراءات في المعاينة والتفتيش والضبط:

1-1 ـ المعاينة: هي رؤية بالعين لمكان أو شخص أو شيء لإثبات حالة وضبط كل ما يلزم لكشف الحقيقة،وتعتبر المعاينة إجراء من الإجراءات التي تقوم بها سلطة التحقيق بتعيينها أو تنتدب ضباط الشرطة القضائية للقيام بها،كما يمكن للمحكمة أن تقوم بإجراءات المعاينة إذا رأت ذلك ضروري لكشف الحقيقة من تلقاء نفسها أو بناءً على طلب من الشخص المعني، بعد موافقة القاضي المختص بناء على طلب على عريضة[26].

فالسؤال المطروح هو حول كيفية إجراء المعاينة التقنية لمسرح الجريمة الإلكترونية عند العلم بوقوعها، فأول خطوة يقوم بها مأموري الضبطية القضائية هو الانتقال إلى مسرح الجريمة، ويبقى التعامل في هذا الإطار مع مسرح الجريمة الالكترونية على أنه مسرحان هما:

-المسرح التقليدي: يقع خارج البيئة الالكترونية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية، ويترك فيها الجاني عدة آثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

ـ المسرح الافتراضي:يقع داخل البيئة الالكترونية لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت في ذاكرة الأقراص الصلبة الموجودة بداخله،ونظرا لاختلاف مسرح الجريمة الالكترونية عن غيره من الجرائم بإتباع عدة قواعد فيه قبل الانتقال إلى مسرح الجريمة الالكترونية والمتمثل:

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

ـ وجود خريطة توضح الموقع الذي سيتم معاينته وتفاصيل المبنى أو الطابق موضوع البلاغ، وعدد الأجهزة والخزائن والملفات ويتحدد ذلك من خلال مصادر سرية لجهات الأمن.

ـ تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج.

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

ـ تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حده، حتى لا تتداخل الاختصاصات.

ـ أن تتم هذه المعاينة وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.

ـ تأمين عدم انقطاع التيار الكهربائي لأن معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي[27].

1-2 ـ التفتيش في البيئة الالكترونية:تتفق جل التشريعات على تعريف التفتيش بأنه إجراء من إجراءات التحقيق غايته ضبط أدلة الجريمة موضوع التحقيق، وكل ما يفيد الحقيقة في شأنها، أما عن شروط التفتيش تخضع للقواعد العامة ومواعيده القانونية، أما عن الميعاد القانوني لإجراء التفتيش في الجرائم الالكترونية طبقا لنص المادة 47 من قانون الإجراءات الجزائية الجزائري أنه من الساعة الخامسة صباحا إلى الثامنة مساء، غير أنه يجوز التفتيش في كل ساعة من ساعات الليل أو النهار إذا طلب صاحب المنزل ذلك ووجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا كحالة الطوارئ وغيرها[28].

وبالنسبة للشروط الموضوعية للتفتيش يمكن حصرها في ثلاثة شروط أساسية:**السبب**:والذي يهدف من خلاله الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث المتمثل في وقوع جريمة ما أو جنحة أو جناية،واتهام شخص أو أشخاص معينين في كشف الحقيقة لدى المتهم أو في مسكنه أو شخص غيره أو مسكنه.

محل التفتيش: وهو الحاسب والشبكة التي تتمثل في مكوناتها الخادم والمزود الآلي والمضيف والملحقات التقنية.

السلطة المختصة بالتفتيش:الأصل في التشريع المصري تمنح للنيابة العامة سلطة الاختصاص بالتفتيش على خلاف التشريع الفرنسي والجزائري اللذان أخذ بنظام الفصل بين سلطتي الاتهام والتحقيق، أما الاستثناء يمنح لضباط الشرطة القضائية هذا الاختصاص في حالة التلبس والانتداب.

1-3 ـ الضبط: إن الضبط في قانون الإجراءات الجزائية هو وضع على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها،والضبط في الجريمة الالكترونية يختلف عن ضبط الجرائم الأخرى، من حيث المحل لأن الجريمة الالكترونية يرد الضبط على أشياء ذات طبيعة معنوية وهي البيانات والمراسلات والاتصالات الالكترونية من جهة، ولها طبيعة مادية كالورق والكمبيوتر وملحقاته والأقراص الصلبة الخارجية والمرئية وأقراص الليزر والبطاقات الممغنطة[29].

2 ـ الإجراءات الشخصية: وسميت كذلك، لأنه غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل، وتتمثل هذه الإجراءات في عملية التسرب، الشهادة، والخبرة التقنية واستجواب المتهم.

2-1-التسرب: جاءت المادة 65 مكرر من قانون الإجراءات الجزائية الجزائري تعرف التسرب بأنه "قيام ضباط وأعوان الشرطة القضائية المكلف بتنسيق العملية،بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم خاف"،وسُمح لضباط الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة،وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14، ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريض على ارتكاب الجرائم(30).

أما عن مواصفات الإذن بالتسرب وطبيعته حددتها المادة 65 مكرر 15 من قانون الإجراءات الجزائية وهي:

ـ أن يسلم فقط لضرورة التحري أو التحقيق القضائي.

ـ أن يكون مكتوبا ومسببا.

ـ أن يذكر في الإذن طبيعة الجريمة التي ينص عليها الإذن.

ـ يذكر في الإذن هوية ضابط الشرطة القضائية،الذي تتم عملية التسرب تحت مسؤوليته.

ـ يحدد فيه المدة المقررة للعملية والمحددة بأربعة أشهر، وهي قابلة للتجديد لمدة أربعة أشهر أخرى كلما دعت ذلك الضرورة.

ـ أن تودع الرخصة أي الإذن في ملف الإجراءات بعد الانتهاء من عملية التسرب.

2-2-الشهادة في الجريمة الالكترونية: يطلق على الشاهد في الجريمة الالكترونية اسم الشاهد المعلوماتي، لأنه هو الشخص المعني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي يكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات، لذلك نجد أن الشاهد المعلوماتي ينحصر في عدة طوائف تتمثل في مشغل الحاسب الآلي، خبراء البرمجة، المحللون، مهندسو الصيانة والاتصالات، مديرو النظم، وللشاهد التزامات لابد بها مثل طبع ملفات البيانات المخزنة في ذاكرة الحاسوب الآلي أو الدعامة الأخرى على أن يقوم بطبعها وتسليمها إلى سلطات التحقيق والإفصاح عن كلمات المرور السرية، والكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة(31).

2-3 ـ الخبرة في الجريمة الالكترونية: لابد أن يكون الخبير صاحب مقدرة وإمكانيات علمية وفنية في المسألة موضوع الخبرة، ويستطيع القيام بدوره وللقيام بذلك عليه أن يبين المكان المحتمل لأدلة الإثبات وشكلها وهيئتها والآثار الاقتصادية والمالية المترتبة على التحقيق في الجريمة الالكترونية، وكيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها.

2-4- استجواب المتهم في الجريمة الالكترونية: الاستجواب ما هو إلا مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق والمطالبة بإبداء رأيه في الأدلة القائمة ضده،قصد محاولة كشف الحقيقة واستظهارها بالطرق القانونية،وقد أحاط المشرع الاستجواب بضمانات خاصة وذلك في القسم الخامس من الباب الثالث الكتاب الأول من قانون الإجراءات الجزائية الجزائري.

3- الإجراءات الحديثة لجمع الدليل الالكتروني: من بين الإجراءات الحديثة لجمع الدليل الالكتروني نجملها فيما يلي:

أ ـ الإجراءات المتعلقة بالبيانات الساكنة: ـ حيث يجب التحفظ المعجل على البيانات المخزنة أو الساكنة، ويقصد بهذا الإجراء توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته في انتظار اتخاذ الإجراءات القانونية كالتفتيش أو الأمر بتقديم بيانات معلوماتية.

وفي هذا الشأن استوجبت المادة 16 من اتفاقية بودابست على كل دولة طرف السماح لسلطاتها المختصة أن تأمر أو تفرض بطريقة أخرى مزود الخدمة التحفظ العاجل على البيانات المعلوماتية المخزنة بما في ذلك البيانات المتعلقة بالأمور المخزنة على وجه الخصوص ومعرفة للفقد أو التغيير، وذلك في مدة عشرين يوما كحد أقصى قابلة للتمديد.

ب- الإجراءات المتعلقة بالبيانات المتحركة واعتراض الاتصالات الالكترونية:الأصل هو حرمة الاتصالات الالكترونية الخاصة فقد أقرت معظم التشريعات على توفير قدر كبير من الحماية الجنائية على سرية الاتصالات الخاصة للأفراد،حيث عاقب المشرع الجزائري لأول مرة على اعتراض الاتصالات السلكية واللاسلكية دون إذن بذلك بموجب قانون العقوبات في المادة 303 مكرر منه، والتي قضت أنه "يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك :. بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية،بغير إذن صاحبها أو رضاه.

. بالتقاط أو تسجيل أو نقل صورة لشخص من مكان خاص،بغير إذن صاحبها أو رضاه،كما يعاقب على شروع في هذه الجرائم بنص عقوبات الجريمة التامة.

. اعتراض الاتصالات الالكترونية بناء على إذن من السلطة المختصة يعد ضمانة لازمة لمشروعية الاعتراض على الاتصالات السلكية واللاسلكية،كما حددت المادة 65 مكرر من قانون الإجراءات الجزائية الجرائم التي يجوز فيها اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات[32].

ثانيا . إجراءات التحقيق في الجرائم الالكترونية:

تعتبر هذه المرحلة هي المرحلة الثانية بعد مرحلة الاستدلالات بحيث يتصل قاضي التحقيق بملف الدعوى، إما عن طريق وكيل الجمهورية بموجب إجراءات تحقيق رسمي للطلب الافتتاحي لإجراء تحقيق، أو عن طريق شكوى جزائية مقدمة من المضرور طبقا لنص المادة 38/3 من قانون الإجراءات الجزائية الجزائري، وما دامت الجريمة الالكترونية تختلف عن الجريمة التقليدية فلا يمكن أن يحقق فيها أي قاضي تحقيق وإنما لابد أن يكون له صفات خاصة وهي:

أ ـ أن يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة، وأن يميل إلى تصميم البرامج أكثر من تشغيلها، وكذا معرفة جديد هذه البرامج.

ب ـ أن يستطيع تصميم وتحليل البرامج أو أنظمة التشغيل بسرعة.

أما عن اختصاص قاضي التحقيق في جميع الجرائم ويكون ذلك وجوبيا في الجنايات وجوازيا في الجنح إذا كان هناك نص، واختياريا في المخالفات طبقا لنص المادة 66 من قانون الإجراءات الجزائية التي تفيد أن التحقيق الابتدائي وجوبي في مواد الجنايات، أما مواد الجنح فيكون اختياري ما لم يكن ثمة نصوص خاصة،كما يجوز إجرائه في مواد المخالفات إذا طلبه وكيل الجمهورية، ويختص قاضي التحقيق في المحاكم الجهوية في الجرائم التي اختصها المشرع بالنظر في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب وجرائم الصرف طبقا للمرسوم التنفيذي 06-348 المؤرخ في 10/5 /2006[33].

وبالنسبة للاختصاص المحلي لقاضي التحقيق فتنص المادة 40 من قانون الإجراءات الجزائية يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها،أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض حصل لسبب أخر، كما يمكن تمديد اختصاص قاضي التحقيق إلى أكثر من محكمة طبقا لنص المادة 40 مكرر 2 استنادا لتعليمات وكيل الجمهورية لدى الجهة القضائية.

مراقبة الاتصالات الالكترونية: طبقا لنص المادة 4 من القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

*كذلك لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

*كذلك في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، ولا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

كما يجوز استئناف أوامر قاضي التحقيق من طرف:

1 . **النيابة العامة:** لوكيل الجمهورية أو أحد مساعديه استئناف جميع أوامر قاضي التحقيق دون استثناء طبقا لنص المادة 17 من قانون الإجراءات الجزائية، ويكون هذا الاستئناف بناء على تقرير لدى قلم كتاب المحكمة،ويجب أن ترفع في ثلاثة أيام من تاريخ صدور الأمر[34]،كما يجوز للنائب العام الطعن في أوامر قاضي التحقيق في ظرف 20 يوما على أن لا يكون لهذا الطعن أثر موقف في حالة الاستئناف،ويفرج على المتهم رغم استئناف النائب العام ما لم يكن وكيل الجمهورية قد استأنفه بالطبع،ويجب تبليغ النائب العام عند استئناف الخصوم في الدعوى،وذلك خلال عشرين يوما التالية لصدور الأمر حتى لا يفاجئ الخصوم بقرار غرفة الاتهام في غير صالحهم.

2 . **استئناف المتهم:** إن المتهم لا يجوز له استئناف جميع أوامر قاضي التحقيق ويرفع الاستئناف بعريضة تودع لدى قلم ضبط المحكمة في ظرف ثلاثة أيام من تبليغ الأمر إلى المتهم.

3 . **استئناف المدعي المدني:** أجاز المشرع الجزائري للمدعي المدني الحق في استئناف أوامر قاضي التحقيق التي لها علاقة بحقوقه المدنية، وبمفهوم المخالفة لا يجوز استئناف الأوامر المتعلقة بالجانب الإجرائي مثل الحبس المؤقت والإفراج والرقابة القضائية[35].

ويرفع الاستئناف خلال ثلاثة أيام من تاريخ تبليغ الأمر المراد استئنافه إلى المدعي المدني،وذلك بتقديم عرضة لدى قلم ضبط قاضي التحقيق طبقا لنص المادة 173 /3 من قانون الإجراءات الجزائية[36].

ثالثا . إجراءات المحاكمة في الجريمة الالكترونية:

مرحلة المحاكمة هي آخر مرحلة للدعوى العمومية بحيث من خلالها يتم الوقوف على مدى صحة الوقائع المنسوبة للشخص المتهم بارتكابها،فبالنسبة للاختصاص المحلي للجريمة الالكترونية طبقا لنص المادة 37 من قانون الإجراءات الجزائية يحدد بثلاثة ضوابط هي مكان وقوع الجريمة، محل إقامة المتهم أو مكان الذي تم فيه القبض على المتهم[37].

وفي نطاق الجرائم الالكترونية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان آخر، فالاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة،وتعد الجريمة الالكترونية إذا تمت عن طريق شبكة الانترنت جريمة مستمرة حيث تعتبر أنها ترتكب في جميع الأماكن التي امتدت الجريمة فيها[38].

ومتى كانت الجريمة الالكترونية أيا كان نوعها،فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيا الإعلام والاتصال إذا ارتكبت خارج الإقليم الوطني أو إذا كان مرتكبها أجنبي وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية أو الإستراتيجية للدولة وذلك في إطار التعاون الدولي[39].

أما عن الاختصاص النوعي للمحكمة للنظر في القضية المعروضة أمامها،فنقول أنه بالنظر للطبيعة التقنية المعقدة للجرائم الالكترونية تفرض على رجال القضاء تكوينا يمكنهم من متابعة هذه الجرائم فقد خصها المشرع مع بعض أنواع الجرائم المتعلقة بالمتاجرة بالمخدرات،الجريمة المنظمة العابرة للحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بإجراءات خاصة، إذ جعل الاختصاص ينعقد إلى دائرة اختصاص أخرى، وهذا ما نصت عليه المادة 37 و40 والمادة 329 من قانون الإجراءات الجزائية، ونصت على إنشاء الأقطاب المتخصصة ذات اختصاص إقليمي موسع لدى كل من الجزائر العاصمة، قسنطينة، وهران، ورقلة[40].

وما يمكن استنتاجه في الأخير أن الجريمة الالكترونية تخضع للقواعد العامة في إجراءات المحاكمة في متابعة الشخص المتهم، وإنما تخضع لنفس إجراءات الجريمة التقليدية من حيث تشكيلة المحكمة وكذا القواعد العامة من حيث علنية الجلسات وشفوية المرافعات،حضور أطراف الخصومة وإلزامية تدوين التحقيق النهائي.

الخاتمة:

من خلال هذه الدراسة توصلنا إلى نتيجة هامة مفادها أن الجريمة الالكترونية هي إحدى المشكلات والتحديات الراهنة في هذا العصر،وهو ما أنتجته الحضارة التقنية والثورة المعلوماتية والتي امتدت آثارها إلى جميع أنحاء العالم، وانتشر خطر الجرائم الالكترونية إلى مختلف القطاعات الحياتية الاقتصادية منها والاجتماعية والسياسية وحتى الشخصية. ومن هنا نصل إلى مجموعة من النتائج:

- أنه لم يتفق على تعريف جامع مانع للجريمة الالكترونية.
- كما تبين من خلال هذه الدراسة خصائص الجريمة الالكترونية،أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية.
- قصور القوانين التقليدية عن مجابهة هذه الجرائم المستحدثة نظرا لطابعها الخاص والمتميز.
- بالنسبة للإجراءات الجزائية المتبعة عبر مختلف مراحل الدعوى العمومية، مازالت لم تصل إلى درجة المستوى المطلوب لأجل القضاء على هذه الجرائم ومجابهتها بالشكل المطلوب،خصوصا أمام تنامي هذه الجرائم.

أما عن الاقتراحات:

- من الضروري على المشرع الجزائري أن يضع نصوصا قانونية خالية من الغموض بحيث أنها ستؤطر ظواهر اجتماعية جديدة مستقبلا.
- ضرورة عقد دورات تدريبية التي تعنى بمكافحة الجرائم الالكترونية.
- ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم، وبالتعاون مع التقنيين من أصحاب الخبرة.
- ضرورة مراعاة احترام حقوق الإنسان والمواطن خاصة،وحتى تتكامل يجب أن يكفلها المشرع الجزائي بحماية قانونية رادعة وهذا بالتصدي لمواقع ووسائل اختراق المواقع بمختلف صورها.

قائمة الهوامش:

(1)حفوظة الأمير عبد القادر، غرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني الموسوم بآليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 2017/03/29، ص. ص. 83.

(2)ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية (الاتجاهات الدولية في مكافحة الجريمة الإلكترونية)، مجلة دراسات وأبحاث، المجلد 01، العدد 01، جامعة زيان عاشور، الجلفة، 2009/09/15، ص. 241.

(3)عوض محمد عوض، مبادئ قانون الإجراءات الجزائية، المكتبة القانونية، دار المطبوعات ، 1999، ص 404.

(4)قسول مريم، مبدأ مشروعية الأدلة العلمية في المواد الجنائية، دراسة مقارنة ، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، الجزائر، 2016، ص 179.

(5)محمد أبو العلا عقيدة، مراقبة الاتصالات الهاتفية، ط.د، دار النهضة العربية، 2008، ص 15.

(6)مروك نصر الدين، محاضرات في الإثبات الجزائي، ج1، النظرية العامة للإثبات، دار هومة للطباعة والنشر، الجزائر، 2003، ص 337.

(7)أحمد بوجمعة شحاته، مشروعية مراقبة الاتصالات الهاتفية وقوتها في الإثبات الجنائي، مجلة المحاماة المصرية، العدد 43، يناير، 1990، ص 34.

(8)قسول مريم، المرجع السابق، ص 178.

(9)قدري عبد الفتاح الشهاوي، ضباط التحريات والاستدلالات والاستخبارات، دار المعارف، الإسكندرية، 2003، ص 95.

(10)محمد عبيد،الكعبي،جرائم الانترنت و سبل مكافحتها،ط1،دار النهضة العربية،مصر، 2010، ص 123.

(11)حسن صادق المرصفاوي، المحقق الجنائي، منشأة المعارف، الإسكندرية، 1991، ص 85.

(12)محمد أبو العلا عقيدة، المرجع السابق، ص 22.

(13)قسول مريم، المرجع السابق، ص 180.

(14)سامي صادق الملا، اعتراف المتهم (دراسة مقارنة)، دار النهضة العربية، مصر، 1969، ص 113.

(15)قسول مريم، المرجع السابق، ص 181.

(16)محمد أبو العلا عقيدة، المرجع السابق، ص 31.

(17)محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ج2، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 432.

(18) Cerdars (J), les écoutes téléphoniques aux etats unie et en Iramce, Ren pev,crim.1991, p19-59.

(19)ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي (دراسة مقارنة)، مكتبة دار الثقافة للنشر والتوزيع، الأردن ، 1996، ص 581.

(20)موسى مسعود أرحومة، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة قانونية، جامعة قاريوس، العدد 17، دون سنة النشر، ص 299.

(21) قسول مريم، المرجع السابق، ص 184.

(22) عائشة بن قارة مصطفى،حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري و المقارن،دار الجامعة الجديدة،كلية الحقوق،جامعة الإسكندرية،مصر،2006، ص 87.

(23) موسى مسعود أرحومة ، المرجع السابق، ص 335.

(24) أمال قارة،الحماية الجزائية للمعلوماتية في التشريع الجزائري،ط1،دار هومة ،الجزائر،2007،ص100.

(25) ينظر المادة 21 من القانون 66/ 155 المتضمن قانون الإجراءات الجزائية الجزائري، المؤرخ في 8 يونيو 1966، المعدل عدة مرات آخرها بالأمر 02/15 المؤرخ في 23 يوليو سنة 2015، الجريدة الرسمية للجمهورية الجزائرية، العدد 40.

(26) عائشة بن قارة،المرجع السابق،ص159.

(27) ينظر المادة 65 مكرر من قانون الإجراءات الجزائية الجزائري.

(28) عبد الرحمان خلفي،الإجراءات الجزائية في التشريع الجزائري و المقارن،دار بلقيس للنشر،الجزائر،2015،ص298.

(29) مولود ديدان،قانون الإجراءات الجزائية،دار بلقيس،الجزائر2014، ص 79.

(30) جميل عبد الباقي،الجوانب الإجرائية للجرائم المتعلقة بالانترنت،دار النهضة العربية،مصر،2001، ص 63.

(31) ينظر المادة 15 من القانون 04/09 المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.

(32) أمال قارة ،المرجع السابق،ص105

(33) ينظر المادة 173 فقرة 3 من قانون الإجراءات الجزائية الجزائري.

(34) نجيمي جمال،قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، ج 1،دار هومة ،الجزائر،2016، ص101.

(35) مروك نصر الدين،محاضرات في الإثبات الجنائي، ج 2،الكتاب الأول،المرجع السابق،ص 135

(36)ممدوح خليل بحر، المرجع السابق، 1996، ص 465

(37)نجيمي جمال،المرجع السابق،ص105.

(38)عمر محمد أبو بكر بن يونس،الجرائم الناشئة عن استخدام الانترنت،دار النهضة العربية،مصر،2011،ص06.

(39). عبد الرحمان خلفي،المرجع السابق ،ص230 .

(40)عائشة بن قارة،المرجع السابق،ص162.