



وزارة التعليم العالي والبحث العلمي
جامعة عباس لغرور خنشلة
كلية الحقوق والعلوم السياسية
قسم الحقوق



أساليب البحث والتحري في الجريمة الإلكترونية

مذكرة مكملة لنيل شهادة الماستر في شعبة الحقوق
تخصص قانون جنائي

إشراف الأستاذ:

* تكواشت كمال

إعداد الطالبتين:

حامام ملاك

بوسالم سلوى

أعضاء لجنة المناقشة

اللقب والاسم	الرتبة العلمية	الجامعة الأصلية	الصفة
عمراوي خديجة	أستاذ التعليم العالي	خنشلة	رئيسا
تكواشت كمال	أستاذ التعليم العالي	خنشلة	مشرفا ومقررا
معمرى عبد الرشيد	أستاذ محاضر أ	خنشلة	عضوا مناقشا

السنة الجامعية: 2024 - 2025

سُبْحَانَكَ اللَّهُمَّ رَبَّ السَّمَاوَاتِ وَالْأَرْضِ
وَرَبَّ الْعَرْشِ الْكَرِيمِ

شكر وعرفان

بسم الله الرحمن الرحيم

الحمد لله بي العالمين، الذي بعثه لنم الصالحين، وكوفيته أتمنا هذا العمل فله الحمد
أولا وآخرا، ظاهرا وباطنا، أسأل الله العظيم أن يجعل هذا العمل خالصا لوجهه العظيم، وأن ينفع
به.

أتقدم بجزيل الشكر والامتنان إلى أستاذي الفاضل ومشرف هذا العمل الدكتور "كمال
تكواشت"، لما بذله من جهد وما أبداه من توجيه وما أكرمني به من صبر ومتابعة حتى
خرج هذا العمل إلى النور.

كما لا يفوتني أن أتوجه بالشكر والتقدير لأعضاء لجنة المناقشة الموقرة، على ما تفضلوا به
من وقت وجهد لقراءة هذا العمل ومناقشته، وعلى ملاحظاتهم القيمة التي أعتر بها كثيرا.
ولا يسعني إلا أن أعبر عن عظيم امتناني لكلية "الحقوق والعلوم السياسية"، التي
احتضنتني طيلة سنوات الدراسة، وكانت بيئة علمية محفزة، ومناورة للعلم
والمعرفة.

كما أخص بالشكر والتقدير لطاقم الإداري المحترم وعلى
رأسهم "كريم سطمبولي"، لما يبذلونه من جهود متواصلة في
خدمة الطلبة وتيسير شؤونهم.



الإهداء

أهدي هذا العمل لي:

أبي الحبيب الذي علمتني أن النجاح لا يأتي إلا بالجد والاجتهاد، أقول لك شكراً من القلب على كل ما قدمته لي، وعلى كل لحظة قضيتها في دمي و تشجيعي، أهديك هذا البحث الذي لولاك ما كنت ولا كان.

لي والدي الحبيبة التي كانت لي الأم الحنون والمعلمة الأولى، والتي كانت السند في كل الأوقات، أقول لك الشكر لا يكفي على ما قدمته لي، لكنني سأظل بارة ومحبة لك طوال حياتي يا أجدد ما فيهما.

لي أختي العزيزة ورفيقة دمي والسند في ضعفي، لي من أهدتني من قلبها حبا ومن فتحتها عما أهديك هذه المذكرة، عرفانا وامتنانا لكل ما قدمته لي وامت نورا لا ينطفئ.

أمينة

يوسف

لي أخي، سندي الذي لا يميل، ورفيقي في كل المراحل، لك كل الامتنان.

سلوى

ولا أنسى صديقتي العزيزة التي كانت عوناً وسنداً في كل مراحل هذا العمل.

لي صديقتي الغالية، أنتم أكثر من مجرد رفيقات في الدراسة، كنتم النور في درب التعب والضحكة الصاوقة وسط كل الضغط فشكراً لقلوبكم التي احتوتني، ورفقتكم التي لم تنسي، أهدكم عملي هذا

سلمى، إيناس، ريان

﴿ فَرِحِينَ بِمَا آتَاهُمُ اللَّهُ مِنْ فَضْلِهِ ﴾

الإهداء

لي من كانت وستبقى الحزن الدافئ، والدعاء الصادق، والنور الذي يهديني في كل درب... لي أُمي الغالية، كل
الحب والامتنان.

لي روح أبي الطاهرة، الذي ما زال صده يعيش في قلبي ونوره يضيء دمي، رحمك الله واسكنك فسحج جنته..
لي إخوتي وأخواتي، سندي الحقيقي في الحياة،

لي صديقاتي وصديقاتي، من زرعوا البهجة في أيامي وكنتم لي الضوء في اللحظات المعتمة.

لي رفيقتي في العمل، التي كانت لي أكثر من زميلة، بل رفيقة درب وكفاح.

ولي أستاذي المشرف، الذي لم يخل علي بعلمه وتوجيهه، لك مني كل التقدير والاحترام فقد كنت العون
والدليل.

لكم جميعاً أهدي ثمرة هذا الجهد، فبكم كان الطريق سهلاً، وبفضل وحنكم مضيئاً بثبات نحو ما نطمح إليه.



مقدمة:

إن الجريمة ظاهرة قديمة عرفها المجتمع منذ آلاف العصور وهي ناجمة عن التصرفات المطلقة للأشخاص التي أدت إلى تجاوز الحدود والتعدي على مصالح الغير ونتيجة لذلك وضعت بعض القيود على تلك التصرفات حماية للحريات وضمانا للحقوق، فاعتبرت المجتمعات أن كل فعل يمس حياة الفرد أو ماله أو سلامته فعل يجرم عليه ويستحق العقاب، ولقد تولت الدولة سلطة تجريم الأفعال ووضع العقوبات لها.

غير أنه وبطور الانسان في شتى المجالات تشكلت قفزة حضارية نوعية، وذلك بفضل عصر الثورة الرقمية حيث أصبح العالم أكثر ترابطا وتداخلا في أي وقت مضى مما أدى إلى نشوء فضاء إلكتروني واسع يمكن الأفراد والمؤسسات من التفاعل والتبادل المعلوماتي بسرعة فائقة، إلا أن هذا التقدم التكنولوجي على الرغم من فوائده الجمة أفرز تحديات أمنية كبيرة تمثلت في ظاهرة الجريمة الإلكترونية التي باتت تشكل تهديدا متزايدا للأفراد و الدول على حد سواء، فهذه الجريمة عرفت على أنها كل فعل غير قانوني يرتكب باستخدام الأجهزة الإلكترونية أو الشبكات المعلوماتية فهي تستهدف الأنظمة أو البيانات أو الأشخاص أو المؤسسات لأغراض إجرامية مثل السرقة أو الابتزاز أو التجسس أو التخريب.

ونظرا لطبيعة الجريمة الإلكترونية الخاصة فإنها تتطلب إجراءات وأساليب خاصة للبحث والتحري من أجل الوصول إليها وتحصيلها من طرف فنيين مختصين، وكل ذلك يستدعي اتخاذ أساليب تحي متخصصة تواكب طبيعة هذه الجرائم.

إن إجراءات البحث والتحري في القانون الجنائي العام هي الأساس في الجرائم الإلكترونية كما هو الحال في باقي الجرائم، فلما قام المشرع الجزائري على تجريم الأفعال الواقعة في الوسط الإلكتروني اعتمد على نصوص قانون العقوبات وكذلك قانون الاجراءات الجزائية، عاملا بإحداث تغييرات عليها، كما استحدث القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، فنلاحظ أن إجراءات البحث و التحري عن هذه الجرائم تتصف بالخصوصية من حيث طريقة كشفها و

التبليغ عنها و كذلك العناية بمسرح الجريمة ، و كيفية التحري عنها و تكوين فرق التفتيش و المعاينة ، وصولا إلى خصوصية التعامل مع الدليل الجنائي.

تعتبر أساليب البحث والتحري في الجرائم الإلكترونية موضوعا ذا أهمية علمية وعملية كبيرة وأن هذه الأخيرة تتميز بخصائص كونها جريمة عابرة للحدود ويصعب اثباتها فإن دراسة هذه الأساليب تساعد على فهم آليات وتقنيات ارتكاب الجرائم الإلكترونية وتكمن أهميتها في مساعدة الجهات الأمنية والقضائية على التعامل مع هذا النوع من الجرائم كما أنها تساهم في تطوير آليات الوقاية والحماية من الاختراقات والتهديدات الإلكترونية لذلك فإن التركيز على أساليب التحري تعد ضرورة ملحة لمواكبة تقنيات مكافحة الجرائم الإلكترونية.

وبالتالي فإن الهدف من هذه الدراسة هو:

- ❖ إعطاء نظرة شاملة حول الجريمة الإلكترونية والمجرم الإلكتروني.
- ❖ تحديد إجراءات التحري التقليدية والمستحدثة للتحري عن الجريمة الإلكترونية.
- ❖ تسليط الضوء على موقف المشرع الجزائري حول أساليب التحري الخاصة بالجريمة الإلكترونية

❖ وأيضا توضيح نطاق تطبيق أساليب التحري في التشريع الجزائري.

وعلى ضوء ما ذكرنا سابقا يمكن طرح التساؤل التالي:

✓ إلى أي مدى وفق المشرع الجزائري في وضع آليات قانونية تتصف بالمشروعية للبحث والتحري عن الجريمة الإلكترونية؟

وقد تفرع عن هذا التساؤل عدة تساؤلات فرعية:

✓ ما مفهوم الجريمة الإلكترونية؟ وما المقصود بالتحري عن الجريمة الإلكترونية؟

✓ ما هي أساليب البحث والتحري المعتمدة للكشف عن الجريمة الإلكترونية؟

✓ هل هذه الأساليب تتصف بالشرعية اللازمة لتطبيقها؟

وقد اعتمدنا في دراستنا هذه على كل من المنهج الوصفي والتحليلي، فمن جهة قمنا

بوصف الجريمة الإلكترونية من خلال تبيان مفهومها وكذلك خصائصها وأركانها، إضافة

إلى تعريف التحري والجهات المختصة فيه، ومن جهة آخر قمنا بتحليل النصوص القانونية الإجرائية لدراسة الإطار القانوني لتحري عن الجرائم الإلكترونية.

أما بالنسبة لأسباب اختيارنا لهذا الموضوع فتنقسم لأسباب ذاتية وأخرى موضوعية، حيث تمثلت أسبابنا الذاتية في:

❖ الفضول الكثير الذي أحدثته هذه الجرائم كونها جرائم مستحدثة ومنتشرة بكثرة في الزمن الحاضر، وكيفية التحري عنها والوصول إليها، وكذلك من أجل معرفة كل ما هو جديد في عالم تكنولوجيا الاعلام والاتصال.

أما الأسباب الموضوعية فتمثلت في:

❖ الحاجة المتزايدة لفهم الأدوات والأساليب التقنية المستخدمة في كشف الجرائم الإلكترونية بسبب تطورها المستمر

❖ تزايد معدلات الجرائم الإلكترونية وتهديدها لأمن الأفراد والمؤسسات، ما يدعو إلى البحث عن آليات التحري متخصصة وفعالة.

❖ تركيز أغلب الدراسات والأبحاث عن الجانب الموضوعي، وهذا ما دفعنا إلى دراسته من الناحية الإجرائية.

ولبلوغ أهداف الدراسة والإجابة على التساؤلات اعتمدت على دراسات أنجزت من قبل متمثلة في كتب قانون متخصصة وعلى مقدمتها كتاب نجاه بن مكي، محمد مدين المتخصص في الجريمة الإلكترونية وتحديات الأمن القومي إضافة لمجموعة من الكتب والبحوث القانونية التي تطرقت إلى موضوع الجريمة الإلكترونية بشكل عام أو خاص، فبالنسبة لدراسات السابقة فهناك مجموعة من الباحثين الذين تطرقوا إلى هذا الموضوع من جوانب مختلفة ومن بينها:

- دراسة هروال هبة نبيلة، جرائم الأنترنت، دراسة مقارنة، أطروحة دكتوراه تخصص القانون كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2013/2014.

-دراسة مولاي ملياني دلال، إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2017/2018.

ومن أهم الصعوبات التي واجهتنا في إتمام هذه الدراسة هي وجود مصطلحات تقنية غير مألوفة خارج مجال التخصص مثل المعلوماتية ومكونات الحاسوب وشبكات الانترنت، كما واجهنا صعوبة في وضع خطة مناسبة وذلك بسبب تعدد محاور الموضوع. ولمناقشة هذه الاشكالية تم الاعتماد على خطة ثنائية تكونت من فصلين: حيث تمحور الفصل الاول حول الإطار المفاهيمي للجريمة الالكترونية، و تم تقسيمه إلى مبحثين : فقد تطرقنا إلى مفهوم الجريمة الإلكترونية في المبحث الأول، أما المبحث الثاني تناولنا فيه مفهوم التحري في الجريمة الالكترونية، أما الفصل الثاني فعرض فيه الإطار القانوني للتحري عن الجرائم الالكترونية، درسنا الآليات الكلاسيكية والمستحدثة للتحري عن الجرائم الالكترونية في المبحث الأول، أما المبحث الثاني خصصناه لمشروعية آليات التحري عن الجرائم الالكترونية.

الفصل الأول:

الإطار المفاهيمي للجريمة

الالكترونية ومسألة التحري فيها

منذ منتصف القرن العشرين شهد العالم تطور في مجال الانترنت، حيث تعد التكنولوجيا الحديثة من أبرز سمات العصر الحديث، والسبب يعود الى ارتباطها بوسائل حديثة من أجهزة الكمبيوتر و شبكات الانترنت والمواقع الالكترونية ، وعلى الرغم من هذا التطور والتسارع في مجال التكنولوجيا فقد صاحبها جملة من الانعكاسات السلبية جراء هذا الاستخدام، ونفشت مع ذلك ظاهرة الجريمة الالكترونية التي يصعب اثباتها والتحري عنها، كونها شبكة تربط مجموعة من أجهزة الكمبيوتر المتصلة ببعضها البعض و تستطيع تبادل المعلومات فيما بينها ، التي ستكون محل دراستنا هذه، وسنتطرق في هذا الفصل الى ماهية الجريمة الالكترونية في المبحث الأول، اما المبحث الثاني سنتناول ماهية التحري عن الجرائم الالكترونية.

المبحث الأول: ماهية للجريمة الالكترونية:

يوصف العصر الحالي بأنه العصر الرقمي أو ما يسمى بالعصر الإلكتروني الرقمي، فهو تضمن تطورات تكنولوجيا هائلة وكبيرة ومعقدة تخدم جميع المجالات العامة والخاصة داخل الإطار الضيق للدول، مما يؤدي إلى خدمة المجتمع الدولي بأكمله فهذه التكنولوجيا تخدم جميع مجالات الحياة.

فهي تعرف بأنها فعل غير مشروع ترتكب باستخدام تكنولوجيا الاعلام والاتصال والتي تؤدي إلى أضرار كبيرة بالفرد والمجتمع، لذا قمنا بتقسيم هذا المبحث إلى مطلبين حيث تناولنا في المطلب الأول مفهوم الجريمة الالكترونية، أما المطلب الثاني تناولنا فيه الأحكام الخاصة بالجرائم الالكترونية (بوزيدي، 2017، صفحة 9).

المطلب الأول: مفهوم الجريمة الالكترونية:

ارتأينا ونحن نيمم وجهتنا لدراسة الجريمة الالكترونية من حيث أساسها النظري، أن ننطلق بداية من تعريف مصطلح الجريمة الالكترونية، مع تبيان خصائصها والأطراف المشتركة لقيامها.

الفرع الأول: تعريف الجريمة الالكترونية:

على الرغم من تنامي جهود التصدي لظاهرة الإجرام الإلكتروني إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة الإلكترونية، فقد ذهب جانب من الفقه إلى تناولها بتعريف ضيق وجانب آخر عرفها على نحو موسع.

أولاً: التعريف الفقهي للجريمة الإلكترونية:

أ. التعريف الضيق للجريمة الالكترونية:

يعرف أنصار هذا الاتجاه الجريمة لإلكترونية على أنها: "الجريمة التي يتم ارتكابها إذا قام شخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة، ومصلحة الأفراد الخاصة. " كما عرفت أيضاً بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحسابات الآلية بقدر كبير لازم ارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى " (حمزة، 2011\2012، صفحة 13).

حسب هذا التعريف يجب أن تتوفر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة، بل كذلك لملاحقتها، والتحقيق فيها.

وهذا التعريف يضيق بدرجة كبيرة من الجريمة الالكترونية، بمعنى يجب أن تتوفر على قدر كبير من العلم بهذه التكنولوجيا لدى الجناة والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم.

كما يرى الأستاذ "rosenblatt" بأن الجريمة الالكترونية هي "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو تحويلها عن طريقه." (حمزة، 2011\2012، صفحة 14).

حسب هذه التعاريف نرى أن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم، والجريمة الالكترونية هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.

ب. التعريف الواسع للجريمة الالكترونية: هناك تعريفات حاولت التوسع في مفهوم

الجريمة المعلوماتية وتم تعريفها كالآتي:

على عكس الاتجاه السابق، يرى فريق آخر من الفقهاء أن الجريمة الالكترونية هي جريمة تتم بواسطة الحاسوب أو أي جهاز الكتروني، وذلك باستخدام شبكات الانترنت من خلال اختراق البريد الالكتروني ومختلف مواقع التواصل الاجتماعي، بهدف إلحاق الضرر للفرد أو مجموعة من الأفراد، وحتى الدولة وذلك من أجل الأضرار بسمعتها، حيث يقوم بتسريب قضايا متستر عنها أو نشر معلومات لفائدة أطراف أخرى.

من هذه التعريفات الموسعة ما يقوله الفقيهان "Micel"and"Credol" أن سوء استخدام الحاسب الآلي أو جريمة الحاسوب تشمل استخدامه كأداة لارتكاب الجريمة، بالإضافة إلى حالات المتعلقة بالولوج غير المصرح به لحساب المجني عليه أو بياناته، كما تمتد جريمة الحاسوب لتشمل الاعتداءات المادية سواء كان هذا الاعتداء على الحاسوب ذاته أو على المعدات المتصلة به، كذلك الاستخدام الغير المشروع لبطاقات الائتمان و انتهاك ماكينات الحسابات الآلية، بما تتضمنه من شبكات التمويل الحسابات المالية بطريقة الكترونية و تزيف المكونات المادية و المعنوية للحاسب، بل وسرقة جهاز الحاسب في حد ذاته أو مكون من مكوناته (مدين، فن التحقيق و الاثبات في الجريمة الالكترونية، 2020).

ودائماً حسب أنصار هذا الاتجاه يري البعض أن الجريمة الالكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسوبيا، أو شبكة حاسوبية للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها، أو جعلها غير صالحة. أما بعض من الفقهاء يعرفونها بأنها كل نشاط إجرامي تستخدم فيه

التقنية الالكترونية بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الاجرامي المستهدف (مدين، فن التحقيق و الاثبات في الجريمة الالكترونية، 2020، صفحة 23).

ومن خلال هذه التعريفات يتضح لنا صعوبة قبول هذا التوجه لأن جهاز الحاسوب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه أو الأقراص المضغوطة على سبيل المثال، ومن ثم لا يمكن إعطاء وصف الجريمة الالكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة الالكترونية، كما قد ترتكب الجريمة ويستعمل الحاسب الآلي، ولا نكون أمام جريمة الكترونية.

ثانيا: التعريف التشريعي للجريمة الالكترونية:

أن أغلب المشرعين لم يخوضوا في وضع تعريف تشريعي جامع للجريمة الالكترونية لكن هناك بعض التشريعات التي أعطت تعريف لها نذكر منها:

أ. تعريف المشرع الأمريكي:

تبنى الخبير الأمريكي (parker) مفهوما واسعا للجريمة الالكترونية حيث يشير إلى أنها: كل فعل اجرامي معتمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.

كما جاء تعريفها بالقانون الأمريكي بأنها الاستخدام الغير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام الضار لأجهزة الكمبيوتر أو ملفات البيانات وتتراوح خطورة هذه الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة (متولي، 2011، صفحة 23).

ب. تعريف المشرع الجزائري:

بالنسبة للتعريف القانوني للجريمة الالكترونية فقد اصطلح المشرع على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وعرفها بموجب أحكام المادة 02 من القانون رقم 04-09 الصادر في 05 اوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47،

على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية."

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبني معيار دور نظام المعلوماتي في تحديد معالم الجريمة، فسمي الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما أنه بينها في قانون العقوبات رقم 15-04، الصادر في 10 نوفمبر 2004 المعدل والمتمم للأمر 66/156 الصادر في 08 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، في المادة 394 مكرر إلى المادة 394 مكرر 07 وترك المجال واسع لأي جريمة أخرى ترتكب على طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

وحسب المشرع الجزائري فإنه تتحقق الجريمة الالكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف قد تضمن نوع من التكرار كون أن مفهوم نظام الاتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية، من أمثلة الجريمة الالكترونية المرتكبة في الجزائر، قيام الجزائري "حمزة بن دلاج" بقرصنة حسابات بنكية عالمية حيث ألقى القبض عليه من طرف الشرطة الفيدرالية الامريكية.

ونلاحظ من هذا التعريف ما يلي:

أن المشرع اعتمد على الجمع بين عدة معايير لتعريف الجريمة الالكترونية أولهما هو معيار وسيلة الجريمة المتمثل في نظام الاتصالات الإلكترونية، وثانيهما معيار موضوع الجريمة وهو المساس بالأنظمة المعالجة الآلية للمعطيات، وثالث معيار وهو القانون الواجب التطبيق أو الركن الشرعي المنصوص عليه في قانون العقوبات.

كما أن المشرع الجزائري حدد نطاق الجريمة الالكترونية وذلك عن طريق اقراره بأن الجريمة الالكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه وهذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري (مختارية، 2017، صفحة 12).

الفرع الثاني: خصائص الجريمة الإلكترونية:

تميزت الجريمة الإلكترونية عن الجريمة التقليدية التي ترتكب في الواقع المادي الملموس، لذا نجد لها مجموعة من الخصائص أو السمات التي تجعلها تختلف عن غيرها من الجرائم، سواء من حيث الجريمة ذاتها، أو من حيث مرتكب الجريمة.

أولاً: السمات الخاصة بالجريمة الإلكترونية:

أ. الجريمة الإلكترونية عابر للحدود:

الجريمة الإلكترونية هي شكل من أشكال الجرائم العابرة للحدود حيث أنها لم تعد ترتكب محليا بل أصبحت إمكانية ارتكابها دوليا حيث أصبح الجاني يقوم بالجريمة عن طريق الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد آخر وهذا الفعل يضر شخصا ثالثا في بلد اخر (صبيح، 2022، صفحة 41).

ولاشك في أن ما يترتب على هذا الأمر من إشكاليات تتعلق أولاً بقواعد الاختصاص و ثانيا بنطاق سريان القانون ومن ثم تحديد القانون الواجب التطبيق فيما لو ظهرت الصلاحية لقانون أكثر من دولة، بالإضافة إلى متطلبات التحقيق و الملاحقة و الضبط و التفتيش (نجا، 2017، صفحة 21)، فعدم تحديد مكان الجناة يشكل صعوبة تضاف إلى الصعوبات المتعلقة بتعقب مرتكبي هذه الجرائم و محاسبتهم ،لاسيما إذا أخذنا بعين الاعتبار الاختلاف القائم بين التشريعات بشأن مكافحة هذا النوع من الجرائم (الهيبي، 2014، صفحة 99).

ب. صعوبة اكتشاف واثبات الجريمة الإلكترونية:

توصف الجريمة الالكترونية بأنها خفية ومستترة في أغلب الأوضاع، لأن الضحية قد لا يلاحظ رغم وقوعها في وجودة على الشبكة، وهذا لأن الجاني يتمتع بقدرات فنية تمكنه من

تنفيذ جريمته بدقة كإرسال فيروسات أو سرقة الأموال والبيانات الخاصة أو اتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم الأخرى.

كذلك نجد أن كل ما يكتشف في هذه الجريمة يرجع إلى الصدفة البحتة، والدليل على ذلك أن لا يكتشف إلا نسبة 1% فقط منها، و15% منها تم الإبلاغ عنها، وخمس النسبة الأخيرة هي التي تصدر فيها احكام الإدانة لمرتكبيها، وهذا ما يستدعي حاجة التحقيق الجنائي إلى خبراء في مجال المعلوماتية لإمكانية تسهيل اكتشافها، وهو ما قامت به الجزائر مؤخرا (نجا، السياسة الجنائية لمكافحة الجرائم المعلوماتية، 2017، صفحة 21).

نستنتج اثبات الجريمة الالكترونية من الصعوبة تحديد مكان وقوعها حيث يصعب تتبعها واكتشافها فهي لا تترك أثر يكتفي، بحيث تعتبر مجرد أرقام، فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها كما أنها تقتصر إلى الدليل المادي التقليدي مثلا ومن وجهة أخرى، فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي لتعامل معها.

ج. قلة الإبلاغ عن الجريمة الالكترونية:

ويرجع السبب في ذلك أن أغلب الجرائم يتم اكتشافها بمحض الصدفة وذلك لأنها تبقى عادة في طي الكتمان وهذا ما يعبر عنه علماء الإجرام بالرقم الأسود أو الرقم الخفي. ومن بين أسباب اختفاء هذه الجرائم حجب الجرم عليها وعدم الإبلاغ عنها، إذ نجد أن أغلب الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك تكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للأضرار بسمعتها ومكانتها خاصة إذا كان المجني عليه عبارة عن مؤسسة مالية كالبنوك والمؤسسات الادخارية حيث تخشى مجالس ادارتها عادة أن تؤدي اتخاذ إجراءات القضائية حيالها إلى تضؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها.

ثانيا: السمات الخاصة بالجناة:

أن الجرم الإلكتروني يختلف عن المجرم العادي فلا يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة فيرتكب هذا المجرم الالكترونية وراء شاشة الحاسوب بل لابد أن تتوفر فيه خصائص نذكر منه:

أ. المجرم الإلكتروني مجرم ذكي:

يختلف المجرم الإلكتروني عن المجرم العادي الذي عادة ما يميل إلى العنف مه ذلك فإن الجرائم التي يقتصر وقوعها في بيئة النظام الإلكتروني تتطلب تقنيات وتدابير ناعمة أي انه يكفي ان يقوم الجرم الإلكتروني بالتلاعب في البيانات وبرامج الحاسوب لكي يمحو هذه البيانات وليس عليه إلا أن يلجأ الى زرع الفيروسات في هذه البرامج لكي يشمل حركة النظام الإلكتروني ويجعله غير قادر على القيام بوظائفه الطبيعية مما يجعله يحترف الإجرام ويصبح خطرا عن المجتمع (محمد، 2019، صفحة 15).

ب. المجرم الإلكتروني يحترف ارتكاب الجريمة الإلكترونية:

هؤلاء الأشخاص الذين يحترفون الجريمة الإلكترونية هم شباب تتراوح أعمارهم ما بين 20 و40 سنة، ففي السنوات الأولى تمثل أن الشباب حدثي العهد بالمعلوماتية والحواسيب الآلية، ولم يكن لديهم الميل لارتكاب الأفعال غير المشروعة، أما المرحلة الثانية فهي تمثل نضوج هؤلاء الشباب ويتزامن هذا النضوج مع تطور التكنولوجيا، ومن ثم يتحول من مجرم هاوي إلى مجرم محترف في استخدام التكنولوجيا واحتراف ارتكاب الأفعال غير المشروعة (محمد، الجريمة الالكترونية وتحديات الامن القومي، 2019 ، صفحة 15).

ج. صعوبة تحديد هوية الجاني:

الجريمة الإلكترونية عند ارتكابها تكون خلف شاشات الحاسوب ولا تكون وجها لوجه كما في الجريمة العادية و هذا ما يجعل تحديد هوية الجاني صعبة للغاية ، و قد طرح هذا الموضوع في المؤتمر الدولي لجرائم الحاسوب المنعقدة في أوصلو عام 2000 حيث تناول موضوع عدم إمكانية البنية التحتية للإنترنت من التوصل الى تحديد شخصية مرتكب

الجريمة او المصدر الحقيقي لها رغم إمكانية توفر التعرف على عنوان ورقم الحاسب الآلي فقط المرتبط بالإنترنت والمستعمل كوسيلة لارتكاب الجريمة عن طريق عنوان (LP) الذي يشير الى رقم يعين الحاسب الآلي الموصول بالإنترنت لكن في المقابل فان هذا الرقم ليس موحدًا على المستوى العالمي (الهيئي، الجريمة المعلوماتية) (نماذج من تطبيقاتها) ، 2014، صفحة 82).

الفرع الثالث: أطراف الجريمة الالكترونية:

لكل جريمة أطراف والجريمة الإلكترونية كغيرها من الجرائم لابد أن يكون لها طرفان فاعل ومجني عليه:

أولاً: الفاعل في الجريمة الإلكترونية:

بالإضافة الى الشروط العامة الواجب توافرها في مرتكب الجريمة الالكترونية من سلوك منحرف، وعلم وإرادة في نتائج هذا السلوك، ينبغي أن يكون هذا الشخص على درجة معينة من العلم والخبرة العلمية في شؤون عالم الحاسوب وتقنية المعلومات وقد سماه البعض بالمجرم الإلكتروني أو المجرم المعلوماتي.

وبهذا المعنى لا يتصور أن يكون الجاني في الجريمة الإلكترونية إلا شخصا طبيعيا ذا أهلية وقدرة على أن يكون محلا لتوقيع العقوبة وهو الأمر الذي لا يتصور حدوثه إلا بالنسبة للشخص الطبيعي دون الشخص المعنوي كما لا يتصور أن يكون الجاني هذا إلا شخصا طبيعيا ذا خبرة ودراية في علم الحاسوب سواء كان مستخدما أو مبرمجا أو مجرد هاو أو محترف لجرائم الحاسوب وتقنية المعلومات، ولعل أهم ما يتميز به الشخص المذكور أن يتوافر لديه كشرط أساسي دراية بالمسائل المعلوماتية ومعرفة كافية بآلية عمل الحاسب الآلي وتشغيله باعتبار أن الإجرام المعلوماتي ينشأ من تقنيات التدمير الهادئة التي تتمثل بالتلاعب بالمعلومات والكيانات المنطقية.

يختلف الجاني في جرائم الإنترنت عن مثيله في الجرائم التقليدية في: فالجاني في هذه الجرائم يسمى إما مجرما تقنيا أو هاكرا أو مجرما معلوماتيا وهو يتمتع في غالب الأحيان بقدر كاف من العلم وبالمعرفة التقنية لدرجة تساويه في السمات مع مجرمي ذوي الباقات

البيضاء، ويختلف عليه في كونه يتمتع بشخصية منتقلة فهو من جهة مثال منفرد عن المجرم الذكي بامتلاكه الجبروت في الاختراق وارتكاب أفعال تقنية عبر العالم الافتراضي بطريقة لا يمكن للناس العاديين أو العامة القيام بها.

ومن جهة، فإن هؤلاء المجرمين يختلفون عن المجرمين التقليديين لأنهم يقضون أوقاتا طويلة على جهاز الحاسوب، كما أن سلاحهم ليس ناريا أو أداة حادة وإنما عقل وبرنامج وفيروسات لاختراق برامج جاسوسية (هروال، 2013، صفحة 59).

ثانيا: المجني عليه في الجرائم الالكترونية:

بتعدد أصناف المجرمين قد يتحدد أصناف الضحايا ولكن ليس بقدر تعدد المجرم الالكتروني، فالضحية قد يكون شخص طبيعي أو معنوي ويمكن أن يكون الضحية فرد عادي في المجتمع أو مؤسسة اقتصادية كشركات التأمين، أما الأخطر فهو أن تكون بالدولة أو الواقعة بالمجال العسكري من خلال عمليات التجسس، والتي لم يغفل عنها المشرع الجزائري وشملها بإجراءات خاصة للوقاية من جرائم تكنولوجيات الاعلام والاتصال، أي إجراء مراقبة الاتصالات الإلكترونية باعتبارها إجراء وقائيا في إطار الضبط الإداري وهذا بموجب المادة 04 من القانون 04-09 .

فإن الضحية في الجرائم الإلكترونية وفي الجريمة بصفة عامة قد يكون شخصا طبيعيا أو شخصا معنويا أنتهك حق من حقوقه المحمية قانونا، فالحقه جراء ذلك ضرر معنوي أو مادي، مع الملاحظ أن هذه الضحية أو المجني عليه قد يكون سببا في ارتكاب السلوك الإجرامي (الزعيبي و مناغسة، 2010، صفحة 77)، إما لجهله بالجريمة وارتكابها أو لعدم احتياطه في أخذ تدابير الحماية الأمنية اللازمة لمنظومته المعلوماتية، أو حتى بسبب عدم القيام أو التخاذل في واجب الرقابة والتوجيه لأطفاله حيث يستخدم الشبكة وباقي الأجهزة المتصل بها. ويختلف المجني عليه أو الضحية في الجرائم الإلكترونية عن المجني عليه في الجرائم التقليدية في الإبلاغ عن الجريمة حيث أن الضحية أو المجني عليه في الجريمة الإلكترونية له دور سلبي جدا أمام تكتم العديد وخوفهم على سمعتهم، لذلك فهم يحجمون عن الإبلاغ،

أما إذا كان المجني عليه والضحية مؤسسة اقتصادية تجارية استثمارية (الزعي و مناغسة، 2010، صفحة 78)، فالأكيد أنها لن تفصح عن نفسها في حالة اختراق موقعها الإلكتروني لوجود ثغرة أمنية أو سرقة كلمات السر أو فك التشفير وغيرها من اساليب ارتكاب الجريمة ولن يقوم بذلك حتى مقدم الخدمات إلا في حالات معينة التي تعفيه من المسؤولية القانونية.

المطلب الثاني: الأحكام الخاصة بالجرائم الإلكترونية:

للحديث عن الجريمة بصفة عامة سواء كانت جريمة تقليدية أو إلكترونية لابد من التطرق إلى أركانها والدوافع التي أدت إلى وقوعها بالإضافة إلى أنواع هذه الجريمة، وهذا ما سنتناوله في هذا المطلب:

الفرع الأول: أركان الجريمة الإلكترونية:

تنهض الجريمة على ثلاثة أركان أساسية؛ هما الركن المادي والركن المعنوي، والجريمة الإلكترونية كغيرها من الجرائم لها ركن مادي يمثل كيانها الملموس ويعبر عن ارادة الفاعل بصورة يمكن إثباتها، فلا بد أيضا من وجود ركن معنوي يعبر عن إرادة المجرم الإلكتروني. وكما يتطلب وجود الركن الشرعي وهو الصفة الغير المشروعة للفعل وهذا ما سنوضحه فيما يلي:

أولا: الركن المادي للجريمة الإلكترونية:

يقصد بالركن المادي للجريمة وجود فعل خارجي له طبيعة ملموسة تحركها الحواس والركن المادي كذلك بمعنى (الواقعة الإجرامية) التي يتكون منها السلوك المادي الخارجي الذي ينص القانون على تجريمه، أي كل ما يدخل في كيان الجريمة وتكون له طبيعة مادية فتلمسه الحواس، وهو ضروري لقيامها إذ لا يعرف القانون جرائم بدون ركن.

فالنشاط أو السلوك المادي في الجريمة الإلكترونية، يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الأنترنت، وكذلك معرفة بداية هذا النشاط والشرع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيحمل الحاسوب ببرامج اختراق أو أن يقوم بإعداد هذه البرامج بنفسه (إبراهيم، 2009 ، صفحة 98)، لذلك

وجب تحديد ومعرفة نقطة بداية السلوك الإجرامي أو الشروع فيه والنتيجة التي يحققها هذا السلوك.

أ. السلوك المادي في الجريمة الإلكترونية:

إن النشاط أو السلوك المادي عبر الأنترنت، هو محل تساؤلات عديدة لاسيما فيها ما يتعلق ببدايته أو الشروع في ارتكاب الجريمة، ومثل هذا النشاط يختلف عما هو الحال العالم المادي، فارتكاب الجريمة عبر الأنترنت يحتاج بالضرورة إلى منطلق تقني ومن دونه لا يمكن للشخص حتى الاتصال بالإنترنت سواء كان بقصد ارتكاب الجريمة أو لمجرد التصفح أو الدخول في الاتصال المباشر كالمحادثة وغيرها (إبراهيم، 2009 ، صفحة 99). ويتخذ السلوك في الجريمة الإلكترونية صورتين:

1) السلوك المادي الإيجابي:

هو السلوك الذي يتطلب مجهود بدني، يتمثل في العالم الخارجي من حركات عضوية يأتيها الجاني بهدف الاعتداء على المصلحة التي يحميها المشرع، ومثالا على ذلك في الجرائم الإلكترونية: كل الأفعال التي يرتكبها الجاني من تلاعب ببرامج وبيانات الحاسب الآلي، بهدف إتلاف البيانات أو سرقتها أو نسخها، أو أن يستخدم الجاني وسائل الاتصال بشكل غير قانوني، كاختراق شبكات الاتصال أو إجراء المكالمات المحلية والدولية بشكل غير مشروع.

2) السلوك المادي السلبي:

يتمثل هذا الفعل في السلوك أو موقف يتخذه المكلف بالقاعدة القانونية تفرض عليه أن يفعل ولا يفعل، وفي هذه الحالة يقوم المكلف بالحيولة دون جسمه كله أو بعضه وبين الحركة التي يطلبها القانون، أو قد يتحرك باتجاه مضاد لما أمره به. يقوم الفعل أو السلوك السلبي على امتناع أو إقدام شخص عن قيام بعمل يوجبه عليه القانون إذا كان باستطاعته القيام به، فلا يجوز للقاضي أن يمتنع عن الحكم بالدعوى ولا للشاهد أن يمتنع عن الإدلاء بشهادته أمام المحكمة بواقعة على علم بها ولا للموظف.

أما الامتناع في الجريمة الإلكترونية فيمكن التمثيل له بامتناع موظف في شركة ما على حماية البيانات والمعلومات المتعلقة بالشركة التي يعمل بها أو ألا يبلغ عن الجريمة الحادثة للحفاظ على حقوق الغير (الهيئي، الجريمة المعلوماتية (نماذج من تطبيقاتها)، 2014، صفحة 90).

ب. النتيجة الإجرامية في الجرائم الإلكترونية

النتيجة الإجرامية: هي العنصر الثاني من عناصر الركن المادي للجريمة ويمكن تعريفها على: أنها الضرر الذي ينتج عن السلوك الإجرامي سواء كان فعلا أو تركا أو هي الأثر الخارجي الذي يتولد عن السلوك ويحدث تغييرا يعتد به القانون.

تطرح مسألة النتيجة الإجرامية في الجرائم الإلكترونية مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين باختراق جهاز حاسب الي رئيسي وهو ما يعرف باسم "الخادم server" في أحد البنوك في فرنسا وهذا الجهاز الخادم موجود في الصين فمعرفة وقت حدوث الجريمة هل هو بتوقيت بلد المجرم أو توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين وهذا ما يثير أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن (الزعيبي و مناغسة، 2010، صفحة 51).

ج. العلاقة السببية للجريمة الإلكترونية:

حتى يتم الركن المادي بعناصره كافة، لا بد أن تكون هناك علاقة سببية بين السلوك الإجرامي الذي أتاها الجاني والنتيجة الحاصلة بحيث يمكن القول إن هذه النتيجة من ذلك السلوك فإذا انتفت العلاقة السببية فلا مجال لمساءلة الفاعل.

ولكي تكتمل الرابطة السببية في الجرائم الإلكترونية، يجب أن يكون الاتصال بالإنترنت واختراق موقع ما للتعدي على بياناته، بعدها يتم نشر هذه البيانات عبر المواقع الإلكترونية، فمثلا تثبت الرابطة السببية في جريمة حيازة صور إباحية خاصة بالأطفال في حاسوب بمجرد ثبوت نشر هذه الصور، فهنا تظهر الرابطة السببية بين حيازة الصور الإباحية وبين الترويج لها.

ثانيا: الركن المعنوي للجريمة الإلكترونية:

لاكتمال الإجرام في أي جريمة؛ لابد أن يصاحب السلوك أو النشاط المادي إرادة آثمة للجاني فلا يكفي لتقرير المسؤولية الجنائية أن يصد عن الجاني سلوك إجرامي بل لابد من توفر نية داخلية يضمورها الجاني في نفسه وتظهر في العالم الخارجي بشكل نشاط مادي وهي ما يسمى بالركن المعنوي للجريمة.

ويتضح الركن المعنوي في الجريمة الإلكترونية من خلال توضيح الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني فهذا المبدأ يقوم على صورتين أساسيتين الأولى تتمثل في الاعتداء على أنظمة المعالجة الآلية والتي تحتوي على نوعين من الاعتداءات: النوع الأول يتمثل في الدخول والبقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات، والنوع الثاني يتمثل في الاعتداء على منتجات الإعلام الآلي كالتزوير المعلوماتي.

فالركن المعنوي للجريمة الإلكترونية، يقوم على أساس مجسد في توافر الإرادة الآثمة لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون، مثل انتحال شخصية المزود عبر الأنترنت، وسرقة أرقام البطاقات الائتمان.

ثالثا: الركن الشرعي للجريمة الإلكترونية:

يقصد بالركن الشرعي النص القانوني الذي يضيفي عدم شرعية على النشاط الإجرامي وبالتالي لا يمكن متابعة أي شخص على أي فعل ما لم يكن لهذا الأخير نص يجرمه تطبيقا لمبدأ شرعية الجرائم والعقوبات الذي جاء في المادة الأولى من الأمر 156-66 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 الذي يتضمن قانون العقوبات المعدل والمتمم، ومفاده أن «لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون».

ومع تطور الأنظمة المعلوماتية برز نوع جديد من الأفعال الغير المشروعة والتي تنفرد بخصوصياتها عن غيرها من الأفعال السابقة في ظل الجرائم التقليدية لذلك حاولن العديد من الدول وضع نصوص عقابية للحد من الجرائم الإلكترونية تقاديا لإفلات المجرمين من جهة

ومن جهة أخرى لضمان حماية الشبكات المعلوماتية ومن بين هذه النصوص ما قضي به المشرع الجزائري في قانون العقوبات في القسم المخصص لهذا النوع من الجرائم تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات " من المادة 394 مكرر إلى المادة 394 مكرر 7.

بناء على ما تقدم يتضح أن الأركان الأساسية للجريمة الإلكترونية من دونها تنتفي الجريمة حيث تعتبر الجريمة الواقعة من نتائج التطور التكنولوجي من المستحدثات التي عجزت النصوص العقابية التقليدية على مواجهتها لذلك سعت معظم الدول العالم إلى سن قوانين وتشريعات جديدة لاحتواء هذا النوع من الجرائم قانونيا.

الفرع الثاني: أنواع الجريمة الإلكترونية:

من الصعوبة تمام حصر أنواع الجريمة الإلكترونية حيث أن أشكالها متعددة وهي تزداد تنوعا وتعدادا كلما زاد للعالم في استخدام الحاسب الآلي وشبكة الأنترنت، فمن المعروف أن أكثر تلك الجرائم يكون ضمن أهدافها الأساسية الحصول على المعلومات التي تكون إما محفوظة على أجهزة الحواسيب واما منقولة عبر شبكة الأنترنت وأخرى يكون هدفها الاستيلاء على الأموال وثالثة تستهدف الأفراد أو الجهات بعينها. حيث قسمها الفقه الى طائفتين رئيسيتين هما:

أولاً: الجرائم الموجهة ضد النظم المعلوماتية

الجرائم الموجهة ضد النظام المعلوماتي قد تقع على المكونات المادية لنظام المعلومات أو البرامج التي يحتوي عليها نظام المعلوماتية أو المعلومات المسجلة على نظام المعلوماتية، ونعرضها على النحو التالي:

أ. الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

تعتبر هذه الجرائم من قبيل الجرائم الواقعة في نطاق الجرائم التقليدية، فهذه الجرائم تقع ضمن الجرائم العادية التي تستهدف المال باعتبار مكونات الحاسوب المادية أموالاً منقولة

تصلح محلا للاعتداء عليها بالجرائم الموصوفة بوقوعها على المال، وبجرائم الإلتاف والتخريب ولا يربطها بالمعلوماتية سوى أن الأجهزة المادية محل الجريمة تستخدم في تشغيل النظام المعلومات.

ويدخل ضمن الجرائم الواقعة على المكونات المادية للنظام المعلوماتي جريمة سرقة وقت الماكينة كما اصطلح على تسميته بذلك الفقه الفرنسي *vol du temps-machine* أو سرقة وقت الآلة *vol du temps-ordinateur* أو جريمة سرقة الوقت والخدمات (إبراهيم، 2009 ، صفحة 166).

ب. الجرائم الواقعة على المكونات المنطقية للنظام المعلوماتي:

تتحقق جريمة التعدي على المكونات غير المادية للنظام المعلوماتي عندما تكون مكونات الكمبيوتر المعلوماتية الغير مادية مثل البرامج المستخدمة والبيانات المخزنة في ذاكرة الكمبيوتر محلا أو موضعا للجريمة، والمقصود بالبرنامج *logiciel* أو الكيان المنطقي أنه مجموعة من الأوامر التي تسمح بتشغيل جهاز الحاسب الآلي أو نظم المعلومات المخصصة لمعالجة المعلومات بهدف إنجاز عملية معينة أو إعطاء نتائج محددة.

وجرائم الاعتداء على برامج الكمبيوتر تأخذ شكلين الأول يكون في شكل الاعتداء على البرامج التطبيقية والثاني في شكل الاعتداء على برامج التشغيل، وفيما يتعلق بالبرامج التطبيقية يشكل هذا النوع من الجرائم نسبة تقدر بحوالي 15% من مجموع حالات الجرائم الالكترونية، أما بالنسبة لبرامج التشغيل تتحقق الجريمة في هذه الحالة بتزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تتيح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي.

ج. الجرائم الواقعة على المعلومات المسجلة بالنظام المعلوماتي

ينصب هذا النوع من الجرائم على المعلومات باعتبارها هي المحور الاساسي الذي تدور حوله المعلوماتية التي تمثل المعالجة الآلية للبيانات والمعلومات بل أن المعلومة هي أساس عمل النظام المعلوماتي ومن صور هذه الجرائم التلاعب في المعلومات واتلافها.

ثانيا: الجرائم الواقعة بواسطة النظام المعلوماتي

تتنوع الجرائم الواقعة بواسطة النظام المعلوماتي الى جرائم اقتصادية، أو قرصنة المعلومات، أو ذات طابع سياسي أو متعلقة بالأمن القومي أو قد تقع هذه الجرائم على أشخاص طبيعية أو اعتبارية وتتمثل هذه الجرائم في:

أ. الجرائم الالكترونية الواقعة على الأشخاص

معظم الجرائم التي ترتكب في مجال المعلوماتية تستهدف إما أشخاص واما جهات بعينها وغالبا ما تكون تلك الجرائم هي جرائم مباشرة، ترتكب في صورة ابتزاز أو تهديد أو تشهير، وعن طريق وسائل التواصل الاجتماعي مثل الفايسبوك، الفاير، الواتساب، ومن أهم جرائم الأشخاص جرائم صناعة ونشر الإباحة والجنس سواء للكبار البالغين أو الأطفال التي تتخذ أشكال مختلفة انطلاقا من الصور إلى التسجيلات المرئية والمسموعة التي تتم عبر الأنترنت.

ب. الجرائم الالكترونية المتعلقة بالأموال:

تستهدف أكثر تلك الجرائم تحديدا عناصر الخدمة المالية ويكون الطمع وراء ارتكابها هو الحصول والاستيلاء على تلك الأموال، وفكرة المكسب السريع التي تحرك مرتكبيها وقد ترتكب أحيانا لمجرد قهر نظام منشأة (مؤسسة) مثلا، وتخطي حواجز الحماية أو بدافع الانتقام من صاحب تلك المنشأة أو أحد عناصرها، كالسطو والسرقة والتحويل الالكتروني غير المشروع للأموال وجريمة غسيل الأموال الكترونيا وقرصنة الحسابات البنكية بطريقة غير مشروعة (إبراهيم، 2009 ، صفحة 76).

ج. الجرائم الواقعة على أمن الدولة:

وهي من أخطر الجرائم الالكترونية وأهمها الإرهاب الإلكتروني والتجسس الإلكتروني الذي يهدد الأسرار العسكرية والاقتصادية للدول مما يسهل خلق الفوضى والمساس بأمنها الداخلي (إبراهيم، 2009 ، صفحة 115).

ثالثا: أنواع الجرائم الالكترونية في التشريع الجزائري

تتناول المشرع الجزائري صور المساس بأنظمة المعالجة الآلية للمعطيات من خلال قانون العقوبات وهي:

* جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات بنص المادة 394 مكرر من قانون العقوبات حيث يعاقب على الدخول المجرد الى النظام أو البقاء غير المشروع في المنظومة المعلوماتية دون علم الضحية.

* جريمة التلاعب في بيانات نظم المعالجة الآلية للمعطيات من خلال نص المادة 323/3 من قانون العقوبات الجزائري، ولهذه الجريمة ثلاث صور هي المحو وفعل التعديل والإدخال.

وفيما يتعلق بجريمة إعاقة أو تحريف تشغيل نظم المعالجة الآلية للمعطيات فلم يرد نص خاص بها واكتفى المشرع بجريمة التلاعب في بيانات نظم المعالجة الآلية والتعطيل الذي يندرج ضمن إعاقة النظام المعلوماتي بأي وسيلة.

الفرع الثالث: دوافع ارتكاب الجريمة الالكترونية:

الدافع، الباعث، الغرض أو الغاية تعبيرات لكل منها دلالاته الاصطلاحية في القانون الجنائي، وتتصل بما يعرف بالصد الخاص في الجريمة.

وللجريمة الإلكترونية عدة دوافع على ارتكابها فبعضها يرجع الى دافع شخصي ومنها ما يرجع الى دافع خارجي ومنها ما يكون خاص بالمنشأة، وكل هذه الدوافع قد تكون مصدرها هو الرغبة الإجرامية، وسنعرض لكل دافع في النقاط التالية:

أولا: الدوافع الشخصية:

ويمكن رد الدوافع الشخصية لدى مرتكب الجرائم المعلوماتية الى دوافع مالية ودوافع ذهنية أو نمطية:

أ. الدوافع المادية:

يعتبر السعي الى تحقيق الكسب المالي في الحقيقة غاية الفاعل وهو من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم الإلكترونية ذلك أن خصائص هذه الجرائم حجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتكب بالحاسوب الذي يتبع تعزيز هذا الدافع بما تحققه من ثراء فاحش، والدليل على ذلك ما حدث في فرنسا سنة 1986 حيث كان العائد من ارتكاب جناية سرقة مع معمل سلاح هو 70000 فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية لمعطيات حصل منها الجاني على 670.000 فرنك فرنسي أي ما يعادل أكثر من 38 مرة (خالد، 2017 ، صفحة 37/38). وحسب الدراسات الحديثة فسنجد أن هذا الدافع يسود على غيره ويعكس استمرار اتجاه مجرمي التقنية الى السعي لتحقيق مكاسب مادية شخصية، وفي مقدمة هذه الدراسات المسحية والإحصائية الدراسات والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية N.F.I.C.

وهناك فئة من مرتكبي الجرائم الالكترونية يرجع ارتكابهم لها الى الديون الناتجة عن المشاكل العائلية والخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، فقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه الحالات فالغاية تبرر الوسيلة.

ب. الدوافع الذهنية أو النمطية:

غالبا ما يكون الدافع لدى مرتكب الجريمة الالكترونية هو الرغبة في إثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا آثمة ويرجع ذلك الى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم، وعليه فإنه يرى البعض "أن الدافع الى ارتكاب الجرائم الالكترونية يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح".

ومع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها إذ يظهر السعي الى تحقيق الربح دافعا أكثر تحريكا لجرائم الحاسوب من الرغبة في قهر النظام، إلا أن الدافع الأخير يتجسد في نسبة مرتفعة من جرائم الحاسوب خاصة ما يعرف بأنشطة « HACKERS » المتطفلين الداخليين على النظام والمتجسدة في جرائم التوصل مع أنظمة الحاسوب تحديدا عن بعد.

ثانيا: الدوافع الخارجية:

في بعض المواقف يتأثر الانسان ويستسلم للمؤثرات والدوافع الخارجية بارتكابه لبعض الجرائم الالكترونية ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات مع توافر هذه المؤثرات، فإن الأمر يؤول في النهاية الى ارتكابه لجريمة الكترونية، هذا وتتعدد المؤثرات التي تدفع الانسان الى اقتراف مثل هذا السلوك سواء كان بدافع الانتقام، جنون العظمة، التعاون والتواطؤ على الأضرار والتهديد (خالد، 2017 ، صفحة 39).

أ. دافع الانتقام وإلحاق الضرر برب العمل:

قد يكون الانتقام مؤشرا في ارتكاب تلك الجرائم، ومثال ذلك قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشآت بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات وديون المنشأة، ولقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية، ومن طبيعة علاقات العمل المنفردة في حالات معينة، هذه الأمور قد تدفع الى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب باعثها الانتقام من المنشأة أو رب العمل، وربما تحتل أنشطة زرع الفيروسات في نظام الكمبيوتر النشاط الرئيسي والغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة.

ب. الرغبة في قهر النظام والتفوق على تعقيد رسائل التقنية

يميل مرتكب هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجاد ما يجودون الوسيلة التي تحيطها، وبتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم الالكترونية الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات لإظهار تفوقهم على رسائل التقنية، وإن هذا الدافع هو أكثر الدوافع التي يجري استغلالها قبل المنظمات الجريمة، لأجل استرجاع محترفي الاختراق الى قبول المشاركة في أنشطة اعتداد معقدة أو استئجارهم للقيام بالجريمة هذا وإن كان العل الواحد (خالد، 2017 ، صفحة 41).

قد يعكس دوافع متعددة وخاصة فمحرك أنشطة الإرهاب الالكتروني وحروب المعلومات سياسة وايديولوجية، في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة وقد تتداخل وتشترك هاته الدوافع في الفعل الواحد فتتمازج دون إمكانية التفرقة بينهما.

وتتميز الجريمة الالكترونية عن الجريمة التقليدية في أنها جرائم يستعمل فيها العنف وتسفك الدماء عند ارتكابها عل عكس جرائم الأنترنت التي تعتمد على الذكاء، فهي كما سبق الذكر من جرائم الإغراء والحيلة فلا عنف فيها ولا سفك للدماء ولا آثار لاقتحام لسرقة أموال.

حيث أنها غالبا ما تقيد مجهول وفي حالة اكتشافها فمن الصعب إقامة الدليل عليه ومحاكمته، ولكن في الغالب يحجم المجتمع عن الإبلاغ عنها تجنباً للإساءة الى السمعة وهز الثقة في كفاءته على عكس الجرائم الإلكترونية قد تقيد ضد المجهول أو ضد المعلوم (هروال، 2013، صفحة 58).

المبحث الثاني: ماهية التحري عن الجرائم الإلكترونية:

في العصر الرقمي الذي نعيشه اليوم ،أصبحت التكنولوجيا جزء لا يتجزأ من حياتنا اليومية ، فقد سهلت التواصل ،وساهمت في تطوير التعليم وتيسير المعاملات المالية و الإدارية ، لكن في المقابل هذه الفوائد الكبيرة ظهرت تحديات جديدة و المتمثلة في الجريمة الإلكترونية التي بات تهدد الأفراد و المؤسسات وحتى الدول ومع تزايد هذه الجرائم و تعقيد أساليب مرتكبيها، حيث اصبح من الضروري تطوير آليات فعالة لمواجهتها وهنا يبرز دور التحري في الجريمة الإلكترونية كأداة أساسية لكشف الحقائق وجمع الأدلة و كذلك ملاحقة الجناة في هذا الفضاء الرقمي المعقد .

سنتناول في هذا المبحث موضوع التحري عن الجريمة الإلكترونية، حيث ينقسم إلى مطلبين المطلب الأول حول مفهوم التحري عن الجريمة الإلكترونية أما المطلب الثاني ندرس فيه ضوابط التحري عن الجريمة الإلكترونية.

المطلب الأول: مفهوم التحري

سأحاول في هذا المطلب وضع تعريف للتحري من المنظور اللغوي والفقهوي والقانوني مع تبيان الأجهزة المسؤولة عن التحري.

الفرع الأول: تعريف التحري

أولاً: التعريف اللغوي

التحري لغة: هو طلب ما هو أخرى أي ما هو أجدر وأفضل للاستعمال، ويعني أيضا البحث والتفتيش، يقال فلان يتحرى الأمر أي يتوخاه ويقصده، ويقال تحر بالشئ وتحري منه وتحري فيه أي قصد أفشله واجتهد وحقق في طلبه، ورد الفعل تحرى في اللغة العربية بمعنى طلب ما هو أخرى بالاستعمال في غالب الظن أو طلب أخرى الأمرين أي أولهما، أو طلب الأمر بمعنى قصده وفضله، والتحري في اللغة بمعنى الخليف والجدير والمناسب والأخرى بمعنى الأولى والأجدر والأخل (خراشي، 2006 ، صفحة 14).

وقد ورد في بعض المراجع أن معنى التحري يفيد التقصي وهو البحث والاستقصاء والتحقيق بدقة ودراسة (زوليكهزوزو، 2017).

ثانياً: التعريف الاصطلاحي:

أ. التعريف الفقهي

لفظ التحري لفظ فقهي استخدمه الفقه في كتاباته، فقد ذهب جانب من الفقه الى القول بأن جوهر التحريات هو جمع البيانات كلها والمعلومات الصالحة للتقريب عن الجرائم ومعرفة مرتكبيها وظروفها من سائر المصادر المتاحة لمأمور الضبط أو لمن يعاونه من مساعديه. ويعرفها جانب آخر من الفقه الى عدم استخدام اي من لفظي التحري والاستقصاء ويفضل استخدام لفظ الاستدلال، وهو يعني مجموعة الإجراءات التمهيدية السابقة على تحريك الدعوى الجنائية التي تهدف الى جمع المعلومات في شأن جريمة ارتكبت كي تتخذ سلطات التحقيق بناء عليها القرار فيما إذا كان من الجائز أو من الملائم تحريك الدعوى الجنائية.

ويعرفها الدكتور علي سالم عياد الحلي كما يلي: "مرحلة التحري والاستدلال هي إجراءات تمهيدية لإجراء الخصومة الجنائية ومستمر بعدها وضرورة لازمة لتجميع الآثار والأدلة والمعلومات بهدف إزالة الغموض والملابسات المحيطة بالجريمة وملاحقة فاعليها".

ب. التعريف القانوني

تنص الفقرة الثالثة من المادة 12 من الأمر رقم 155-66 المؤرخ في 8 جوان 196 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم 02-11 المؤرخ في 23 فيفري 2011، ج.ر، ج.ج.د.ش، العدد 12 المؤرخ في 23 فيفري 2021، من قانون الإجراءات الجزائية على ما يلي: "ويناط بالضبط القضائي مهمة البحث عن الجريمة المقررة في قانون العقوبات وجمع الأدلة فيها والبحث عن مرتكبيها ما دام لم يبدأ فيها بتحقيق قضائي".

مما سبق يمكننا أن نستخلص العناصر الأساسية للتحري والتي تتمثل في:

- * أنها مجموعة من الإجراءات الجزائية.
- * ينفذها أعضاء الضباط القضائي.
- * تبدأ بعد ارتكاب الجريمة وتنتهي بتحريك الدعوى القضائية.
- * مضمونها معاينة الجرائم وجمع الأدلة عنها والبحث عن مرتكبيها.
- * تستهدف التمهيد لتحريك الدعوى العمومية ومباشرتها والسير في التحقيق القضائي.

الفرع الثاني: طبيعة مرحلة التحري عن الجريمة الإلكترونية

تتسم الطبيعة القانونية للتحري عن الجريمة الإلكترونية في الجزائر بخصوصية نابعة من طبيعة هذه الجرائم ذاتها والتي تختلف عن الجرائم التقليدية في عدة جوانب يمكن تلخيص هذه الطبيعة القانونية في النقاط التالية:

أولاً: ازدواجية الطبيعة القانونية:

يعتبر التحري عن الجريمة الإلكترونية إجراء من إجراءات التحقيق الابتدائي التي تقوم بها الضبطية القضائية تحت إشراف النيابة العامة للكشف عن الجرائم وجمع الأدلة وتقديم مرتكبيها للعدالة وذلك وفقاً لقانون الإجراءات الجزائية الجزائري.

كما يتميز التحري في الجرائم الإلكترونية بطبعه الفني والدقيق حيث يتطلب التعامل مع أنظمة المعلومات وبيانات رقمية مما يستدعي خبرة وكفاءة خاصة من المحققين في مجال تكنولوجيا الإعلام والاتصال.

ثانياً: الخصوصية في الإجراءات:

يجيز القانون الجزائري للسلطات القضائية المختصة وضباط الشرطة القضائية المختصة وضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها قانوناً الدخول بغرض التفتيش ولو عن بعد إلى الأنظمة المعلوماتية ومحاملها وكل ما يتصل بها من معدات وبرامج ومعطيات.

كما يسمح القانون بضبط وحجز الأجهزة وكل ما يتعلق بها التي يحتمل أن تكون قد استخدمت في ارتكاب الجريمة التي أو نتجت عنها أو تشكل دليلا عليها، ويجب ان يتم ذلك وفقا لإجراءات قانونية تضمن سلامة الأدلة وحجيتها.

نظرا للطبيعة القانونية المعقدة لهذه الجرائم، غالبا ما تستعين جهات التحقيق بالخبراء المختصين في مجال المعلوماتية والأدلة الرقمية لتحليل البيانات واستخلاص الأدلة وتقديم الخبرة الفنية (زولبخة زوزو، 2017، صفحة 760).

ثالثا: الإطار القانوني المنظم:

القانون الخاص بمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال صدر في الجزائر هو القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 غشت سنة 2009، والمتضمن القواعد الإجرائية الخاصة بالتحري والتحقيق في هذا النوع من الجرائم، بما في ذلك تفتيش الأنظمة المعلوماتية وضبط الأدلة الإلكترونية.

ومع ذلك يخضع التحري عن الجرائم الإلكترونية أيضا للأحكام العامة المنصوص عليها في قانون الإجراءات الجزائية، فيما لا يتعارض مع الاحكام الخاصة الواردة في قانون مكافحة الجرائم الإلكترونية.

باختصار يمكن القول بأن الطبيعة القانونية للتحري عن الجريمة الإلكترونية في الجزائر تجمع بين كونها أجراء من إجراءات التحقيق الجنائي التقليدية، لكنها تتميز بنوع من الخصوصية نابعة من الجريمة الإلكترونية التقنية، مما يستلزم إجراءات وأدوات قانونية وتقنية متخصصة لضمان فعاليتها في الكشف عن هذه الجرائم وملاحقة مرتكبيها.

الفرع الثالث: أهمية التحري عن الجرائم الالكترونية:

- تعطي مرحلة التحري صورة واضحة عن وقوع الجريمة وكيفية حدوثها والظروف التي رافقتها ومحاولة كشف غموضها وملاحقة مرتكبيها وهي بذلك تساعد سلطة الاتهام في تحريك الدعوى الجنائية وتسهيل لها القيام بعملها.

- كما تظهر أهمية هذه المرحلة في أن بعض إجراءات التحقيق لا يجوز مباشرتها إلا إذا توافرت دلائل جدية تبرر اتخاذها.
- وتظهر أهمية هذه المرحلة في المحافظة على أدلة الجريمة وآثارها، لأن هذه الآثار والأدلة هي التي تقود الى الكشف عن غموضها، وهنا تظهر أهمية المحافظة عليها من الزوال والتخريب ومنع الحاضرين من لمسها أو الاقتراب منها أو إضافة أي شيء عليها حتى تبقى في حالة سليمة لحين وصول رجال النيابة العامة.
- ومن الناحية القانونية تعد هذه المرحلة إعداد وتحضيرا للدعوى الجنائية والمعلومات التي يمكن جمعها في هذه المرحلة يمكن أن تنتج عنها أدلة في الدعوى، ويبدو ذلك واضحا في محاضر التحري وما تحويه من إثبات فقد اعترف القضاء بقيمتها القانونية، فللمحكمة أن تستند في حكمها الى أن عنصر من عناصر الإثبات التي تضمنها محضر التحري وتطرح جانبا مالا تكمنن إليه وتجزئة، وإذا كان الأمر كذلك فإنه لا ينبغي إنكار أهمية إجراءات التحري المدونة في المحضر، لأنه إذا كان المبدأ هو حرية القاضي الجنائي في أن يأخذ أو لا يأخذ بما هو مدون في التحقيق الابتدائي أو محاضر جمع الاستدلالات إلا أنه من جهة أخرى يجب أن يبنى حكمه على دليل له اصل في أوراق الدعوى (خراشي، 2006 ، صفحة 37).

المطلب الثاني: ضوابط التحري عن الجريمة الالكترونية

إن وضع ضوابط واضحة وفعالة للتحري عن الجريمة الإلكترونية يمثل ضرورة حتمية لمواجهة هذا النوع المتنامي من الجرائم وحماية المجتمع من آثاره السلبية، يجب أن تكون هذه الضوابط متوازنة، بحيث تمكن السلطات المختصة من أداء مهامها بكفاءة مع ضمان احترام الحقوق والحريات الأساسية للأفراد في البيئة الرقمية، كما يجب أن تكون هذه الضوابط قابلة للتطوير والتحديث المستمر لمواكبة التحديات التقنية المتجددة التي تطرحها الجريمة الإلكترونية. ونظرا لأهمية التحري في هذا النوع من الجرائم قسمنا هذا المطلب الى ثلاث فروع:

الفرع الأول: الأجهزة المكلفة بالتحري في الجريمة الالكترونية

يناط بالتحري عن الجرائم الإلكترونية مجموعة من الأجهزة المتخصصة التي تملك الكفاءة التقنية والسلطة القانونية للتعامل مع هذا النوع من الجرائم المستحدثة، وتختلف هذه الأجهزة من دولة إلى أخرى وفقا للبنية التنظيمية والقانونية إلا أن هناك عددا من الجهات التي تتكرر مهامها في معظم الأنظمة، ومن أبرزها التي حدد المشرع الجزائري في نص المادة 14 من قانون الإجراءات الجزائية الجزائية المعدل والمتمم بموجب الأمر رقم 15/02 ج.ر، ج.ج.د.ش، العدد 40. صفة القائمين بالتحري والاستدلال وهم ضباط الشرطة القضائية، أعوان الضبط القضائي والموظفين والأعوان المنوط بيهم قانون بعض مهام الضبط القضائي، وأوردهم على سبيل الحصر ولم يجز لغيرهم مباشرة إجراءات التحقيق، كما حرص المشرع على ضرورة توافر صفات معينة في الشخص القائم بالتحري وذلك ضمانا لاحترام الحقوق الفردية في تلك المرحلة (خراشي، 2006 ، صفحة 106).

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الاستثناء الى بعض الجهات والهيئات الخاصة بحكم خبرتها، ومثال ذلك يلزم القانون 04-09 مزودي خدمات الأنترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم الالكترونية هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها.

أولا: تشكيل الضبطية القضائية

تتكون الضبطية القضائية من مجموعة مختصين وذوي صلاحيات قانونية وفنية، ويختلف أعضاؤها ومهامهم باختلاف الجهات المسؤولة قانونا وبحسب صلاحياتهم القضائية فالضبط القضائي هو المرحلة التي يتم فيها التحقيق والتحري في الجرائم الخاصة أو البسيطة بهدف ملاحقة مرتكبيها وخلال هذه المرحلة يضطلع أفراد الضبطية القضائية بمجموعة متعددة من المهام المعينة.

أ. ضباط الشرطة القضائية:

ضباط الشرطة القضائية هم الذين عدتهم المادة 15 من قانون الإجراءات الجزائية المعدل والمتمم بموجب الأمر رقم 15/02 ج.ر، ج.ج.د.ش، العدد 40. والتي تنص على ما يلي:

"يتمتع بصفة ضابط الشرطة القضائية:

أ. رؤساء المجالس الشعبية البلدية.

ب. ضباط الدرك الوطني.

ج. محافظو الشرطة.

د. ضباط الشرطة.

هـ. ذوي الرتب في الدرك، ورجال الدرك الذين أمضوا في سلك ثلاث سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني، بعد موافقة لجنة خاصة.

و. مفتشو الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الأقل وعينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية، بعد موافقة لجنة خاصة.

ز. ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل."

ب. أعوان الضبط القضائي:

وفقا لمادة 19 من القانون الاجراءات الجزائية " يعد من اعوان الضبط القضائي، موظفو مصالح الشرطة وضباط الصف في الدرك الوطني ومستخدمو المصالح العسكرية للأمن الذين ليست لهم صفة ضباط الشرطة القضائية " وفقا للمادة 20 من قانون الإجراءات الجزائية " يقوم اعوان الضبط القضائي الذين ليست لهم صفة ضباط الشرطة القضائية

بمعاونة ضباط الشرطة القضائية في مباشرة وظائفهم ويثبتون الجرائم المقررة في قانون العقوبات ممثلين ذلك لأوامر رؤسائهم مع الخضوع لنظام البيئة الذين ينتمون إليها.

ج. الموظفين والأعوان المكلفين ببعض مهام الضبط القضائي:

والموظفون والأعوان المكلفون ببعضهم مهام الضبط القضائي وقد حددتهم المادة 21-27 وهم:

- المهندسون والأعوان، الفنيون، التقنيون، المختصون في الغابات وحماية الأراضي واستصلاحها.

- رؤساء الأقسام والأعوان التقنيون في الغابات وحماية الأراضي الذين حددتهم المادة 23 يجوز أثناء ممارستهم مهامهم أم يطلبوا مساعدة القوة العمومية.

- موظفون وأعوان الإدارات والمصالح العمومية الذين يباشرون بعض مهام الضبط القضائي.

- الولاية (المادة 28 من قانون الإجراءات الجزائية)

ثانيا: دور مقدمي خدمات الأنترنت في التحري عن الجرائم الالكترونية:

قد استحدثها المشرع الجزائري بموجب قانون رقم 041-09 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 261-15 المؤرخ في 08 أكتوبر 2015 ومن مهامها تفعيل التعاون القضائي والأمني الدولي وتنسيق العمليات الوقائية والمساعدة التقنية للجهات القضائية والأمنية (نعيم، 2013، صفحة 107)، مع إمكانية تكاليفها بالقيام بخبرات قضائية في حال الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني الهيئة الوطنية، تعد سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل، وتظم أساسا أعضاء من الحكومة معنيين بالموضوع، ومسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء .

تضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين، وفقا لأحكام قانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعلومات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للاتصالات الإلكترونية، وذلك قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى تحت سلطة القاضي المختص.

للإشارة هنا تمكنت الجزائر الممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 100 جريمة إلكترونية منها 30 % على مواقع التواصل الاجتماعي.

هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016 وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بالتهديدات الإرهابية باسم تنظيم "داعش الإرهابي" لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة وتوقيف 58 شخصا متورطا في قضايا إرهاب إلكتروني تمت إحالتهم على القضاء (نعيم، 2013، صفحة 108).

وقد استطاعت الشرطة الجزائرية المتخصصة من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق، سوريا وليبيا كما تمكنت من فك شفرات الرسائل المتبادلة وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجنيدهم عبر مواقع الانترنت ومنصات التواصل الاجتماعي خاصة الفيس بوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية داعمة وتدعو للمشاركة في منديات إرهابية على جانب اتصالات محلية ودولية.

الفرع الثاني: الوسائل المستخدمة في التحري وجمع الأدلة

لم تعد الأدلة تعتمد فقط على الشهادات أو الوثائق الورقية، بل أصبحت الأدلة الإلكترونية تحتل مكانة محورية في التحقيقات، لما توفره من معلومات دقيقة يصعب إنكارها. لذلك يعد جمع الأدلة الرقمية وتحليلها بشكل قانوني وفني سليم من أهم المراحل في الوصول إلى الحقيقة وتحقيق العدالة في هذا العصر الرقمي. ولحل الجريمة والوصول لمرتكبيها يستخدم الباحثون مجموعة متنوعة من الأساليب:

أولاً: الوسائل المادية:

وهي الأدوات الفنية التي غالباً ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحري المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها.

أ. عناوين IP والبريد الإلكتروني وبرامج المحادثة:

عناوين IP هي المسؤولة عن نقل حزم البيانات عبر شبكات المعلومات وتوجيهها إلى وجهتها بنفس طريقة عناوين البريد الإلكتروني يمكن لأجهزة التوجيه والشبكات المرتبطة بها ترحيل الرسائل وهو أمر طبيعي حيث يمكن العثور عليها من قبل جميع الأجهزة المتصلة بالشبكة معلومات عالمية تتألف من أربعة أقسام كل جزء يتكون من أربعة أرقام أي 12 رقماً في المجموع والحقل الأكبر ويمثل الجزء الأول على الجانب الأيسر لمحدود المعلوماتية ويمثل الجزء الثاني مجهز للخدمة ويستخدم الجزء الثالث للاتصال بمجموعة من أجهزة الكمبيوتر ويستخدم الجزء الرابع في تحديد الجهات المرتبطة بنظام الحوسبة (عثماني، 2018، صفحة 53).

ب. برامج التتبع:

تعد برامج التتبع من الأدوات الفعالة في مجال التحري الإلكتروني حيث تتيح تتبع نشاط الأشخاص أو الأجهزة عبر الأنترنت أو من خلال تحديد مواقعهم الجغرافية وتستخدم هذه البرامج في قضايا الاختراق والابتزاز أو حتى الجرائم التقليدية التي ترتكب باستخدام وسائل

رقمية. حيث تقدم بيان شامل بها الى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP الذي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الأنترنت المستضيفة للمخترق.

ج. نظام جرة العسل Honeypot

هو نظام يعمل بشكل فعال لتعامل مع الهجمات على الشبكة يتم استخدام هذا النظام كطريقة لجذب المهاجمين وتحليل طريق الهجوم والتعرف على استراتيجياته بالتالي تعزيز أمان الشبكة واتخاذ تدابير مضادة فعالة كما يعتمد على خلق بيئة يظن فيها المهاجمون انها هدف سهل للهجوم، عندما يحاول المهاجمون اختراق النظام، Honeypot يتم تسجيل وتحليل كل الأنشطة التي يقومون بيها ويتم جمع المعلومات حول طريق الهجوم . المستخدمة والأدوات المستخدمة ونقاط الضعف المستهدفة، يتم استخدام هذه المعلومات لتحسين أمان الشبكة الأصلية وتعزيز الحماية من الهجمات المستقبلية.

د. نظام البروكسي:

البروكسي هو خادم وسيط يعمل بين المستخدم والأنترنت، يستخدم لتحسين الأداء وتوفير الحماية او إخفاء خزين هوية المستخدم وعند الحديث عن التحري الالكتروني وجمع الأدلة، فان البروكسي يلعب دورا مزدوجا فقد يستخدم من قبل الجناة لإخفاء آثارهم وقد يستخدم مقبل المحققين لتعقبهم او مراقبة انشطتهم. ويهدف تحسين إدارة الخدمة وأمانها وأدائها والفكرة الرئيسية للوكيل هي تلقي طلب المستخدم عبر خادم وكيل والبحث عن صفحة معينة في ذاكرة تخزين مؤقت محلية يتحقق البروكسي مما إذا كانت الصفحة موجودة في ذاكرة التخزين المؤقت وإذا كان الامر كذلك يرسلها مباشرة إلى المستخدم دون إرسال طلب جديد إلى الشبكة العالمية إذا لم تكن الصفحة موجودة في ذاكرة التخزين المؤقت المحلية يرسل الوكيل طلبا لشبكة العالمية لاسترداد المعلومات المطلوبة.

ثانيا: الوسائل الاجرائية:

في ظل التحولات الكبرى التي يشهدها العالم على المستويين التقني والأمني أصبح من الضروري تحديث أدوات التحري وجمع الأدلة بما يتماشى مع طبيعة الجريمة المعاصرة، التي باتت أكثر تعقيدا وتنظيما وقد فرض هذا الواقع على أجهزة انفاذ القانون تبني وسائل إجرائية حديثة تعتمد على التكنولوجيا المتطورة من بينها:

أ. **اقتفاء الأثر:** هو عملية جمع وتحليل الأدلة الرقمية للكشف عن أنشطة أو جرائم إلكترونية، يتم استخدامها للتحقيق في الاختراقات الإلكترونية وسرقة المعلومات وجرائم القرصنة وتهديدات الأمان الإلكتروني (عثماني، 2018، صفحة 55).

ب. **الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته:** وذلك بهدف تحليل كيفية اختراق النظام أو تعطيله أو استغلاله، فالمحققون يحتاجون إلى دراسة نظام المعلومات وعناصر بالإضافة إلى فهم تشغيل وإدارة وأمان نظام المعلومات مثل قواعد البيانات، كما يجب دراسة معلومات الملفات و المستخدمين والقيود الزمنية، فالإجراءات الأمنية تشمل استخدام كلمة المرور وتعيين أذونات المستخدم ومراقبة الأنشطة والموارد ومعالجة البيانات واستخدام سجلات الأحداث، كما يجب أيضا على المحقق فهم كيفية عمل تقارير جدار الحماية وكيفية التدخل في حالات تعذر الوصول إلى النظام.

ج. **الاستعانة بالذكاء الاصطناعي:** من خلال استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الالكترونية وفق برامج صممت خصيصا لهذا الغرض (عثماني، 2018، صفحة 55).

الفرع الثالث: قواعد الاختصاص:

تشير قواعد الاختصاص إلى مجموعة القواعد القانونية التي تحدد الجهة القضائية المختصة بالفصل في النزاع، فأعضاء الضبطية القضائية يمارسون صلاحياتهم في الكشف عن الجريمة ومعرفة مرتكبيها داخل نطاق إقليمي يسمى بالاختصاص المحلي، وكذلك نوع الجريمة ويسمى الاختصاص النوعي.

أولاً: الاختصاص المحلي

يقصد بيه المجال الإقليمي الذي يباشر فيه أعضاء الضبطية القضائية مهام البحث والتحري عن الجريمة الإلكترونية، ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة، ولذلك يتعين أن يكون مكان وقوع الجريمة أو محل إقامة المتهم محل القبض عليه.

أ. امتداد الاختصاص المحلي:

حسب ما جاء في المادة 16 من قانون الإجراءات الجزائية الجزائري: ان ضباط الشرطة القضائية يمارسون اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة. إلا انه يجوز لهم أيضا في حالة الاستعجال، أن يباشروا مهامهم في كافة دائرة اختصاص المجلس القضائي المحليين بيه، ويجوز أيضا في حالة الاستعجال ان يباشروا مهامهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونا، وكذا تحديد الاختصاص المحلي لضباط الشرطة القضائية في الجرائم الستة الخطيرة و المذكورة في المادة 16 من قانون الإجراءات الجزائية الجزائية (جرائم المخدرات، الجرائم المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف) الى كافة التراب الوطني.

ثانيا: الاختصاص النوعي:

يقصد به اختصاص أعضاء الضبطية القضائية بنوع معين من الجرائم دون غيرها من الجرائم، وقد ميز المشرع بين الاختصاص العام لبعض الفئات أعضاء الضبطية القضائية أي الاختصاص بالبحث والتحري بشأن جميع الجرائم دون تحديد نوع معين من الجرائم دون الأنواع الأخرى من الجرائم وهي الفئات المنصوص عليها في المادة 15 من ق. إ. ج فلهم الاختصاص العام بالبحث والتحري في جميع الجرائم أما الفئات الأخرى من الضباط المحددين في الفقرة 7 من المادة 15 والمواد 21 و 27 و 28 من قانون الإجراءات الجزائية فإنهم ذو اختصاص خاص وليس عام يتحدد بنطاق جرائم معينة.

خلاصة الفصل الأول:

إن التطور السريع والملحوظ الذي يشهده العالم اليوم في عالم الانترنت يتفرغ عنه ليس فقط تنوع الإيجابيات والخدمات التي تيسر الحياة، وإنما بقدر هاته الإيجابيات هناك من السلبيات، لعله كان من المتوقع أن تظهر الجريمة الالكترونية عاجلا أم آجلا، لكن وقتها لم يكن الإنسان غفل هذا لأنه فضل النظر للجانب المشرق من الأمور، وعليه فإن الجريمة الإلكترونية اليوم تشكل تحديا لجميع العاملين والمستهلكين وحتى المستثمرين في هذا القطاع، خاصة وإنها باتت جريمة يصعب تفقيها أو الوصل اليها.

فالجريمة الإلكترونية تشمل مجموعة واسعة من الأنشطة غير القانونية التي ترتكب عبر الإنترنت أو بمساعدة التكنولوجيا الرقمية من بين هذه الأنشطة الاحتيال الإلكتروني، السرقة الرقمية، القرصنة، نشر الفيروسات والبرامج الضارة، وانتهاك الخصوصية، يتميز مجرموا الإنترنت بذكائهم ومعرفتهم التقنية العالية، بالإضافة إلى خبرتهم الواسعة في استخدام الأدوات والبرامج المتقدمة تختلف الجريمة الإلكترونية عن الجرائم التقليدية في طبيعتها ووسائل ارتكابها فهي لا تحتاج إلى وجود مادي أو استخدام للقوة البدنية، بل تعتمد بشكل أساسي على الخبرة والمعرفة التقنية هذا يجعل مم عمليات التحقيق والتعقب أكثر تعقيدا وصعوبة فمثلا يمكن للمجرمين إخفاء هويتهم بسهولة واستخدام تقنيات التشفير لتجنب الكشف عنها في الفصل الثاني.

الفصل الثاني:

الإطار القانوني للتحري

عن الجرائم الالكترونية

إن أنشطة مكافحة الجريمة الإلكترونية أبرزت تحديات ومشكلات جمة تغاير في تحديات ومشكلات التي ترتبط بالجرائم الأخرى، كون أن الجريمة الإلكترونية يرتكبها جناة ذو صفات معينة أهمها الدراية الفنية بعمل الحاسب الآلي، وكل هذه الصفات تساعد الجاني في فهم تكتيك العمل في الحسابات الآلية وكيفية تصميم البرامج التي يستعملها في ارتكاب جريمته دون الاهتداء إليه، لأنه لا يترك أي آثار يمكن أن يستدل عليه من خلالها، مما يوجب على السلطة المختصة بالتحقيق الإلمام الواسع بمعطيات الحاسوب وطبيعته وتشغيله ويتعين على المحقق معرفة بيئة الحاسوب والأنترنت والمعرفة الكافية بمسائل الضبط والتفتيش وكشف الأدلة والتحفظ عليها.

إن إجراءات التفتيش والضبط التي تقوم بها أجهزة الضبط القضائي سواء في الجرائم العادية أو الجرائم الواقعة على الحاسوب تمس حقوق الناس وحررياتهم لذا وجب أن تتم هذه الإجراءات بصورة صحيحة وقانونية، لأن اللجوء الى الطرق الغير مشروعة يؤدي الى بطلان هذه الإجراءات، وهذا ما سنتطرق إليه في هذا الفصل، سنتناول الآليات الكلاسيكية والمستحدثة للتحري عن الجريمة الإلكترونية في المبحث الأول، أما المبحث الثاني سنتطرق فيه إلى مشروعية آليات التحري عن الجرائم الإلكترونية.

المبحث الأول: الآليات الكلاسيكية والمستحدثة للتحري عن الجريمة الإلكترونية

أضحى التحري عن الجريمة الإلكترونية يعتمد من جهة على الآليات الكلاسيكية المعروفة في مجال البحث الجنائي، مع تكييفها لمواجهة التعقيدات التقنية الحديثة، كما أنه يعتمد على الآليات المستحدثة التي فرضتها طبيعة الجريمة الإلكترونية.

حيث تتجلى أهمية دراسة هذه الآليات في كونها تمثل الركيزة الأساسية لكشف الجرائم الإلكترونية وضمان تقديم مرتكبيها للعدالة، مع المحافظة على المبادئ الدستورية والحقوق الأساسية للأفراد. لذا نسعى الى تسليط الضوء على مختلف الآليات الكلاسيكية والمستحدثة للتحري عن الجريمة الإلكترونية في هذا المبحث:

المطلب الأول: اليات التحري عن الجرائم الإلكترونية في القانون رقم 09-04

القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في ظل قانون 09-04 تتعلق بالتحري والتحقيق في الجرائم الإلكترونية وهي مرتبطة بالعمليات الجنائية والأمور القانونية من الأساليب التقليدية الأساسية في التحري والتحقيق والتي قد تُطبق طبقاً لهذا القانون وهذا ما سنتناوله في هذا المبحث مطلبين، المطلب الأول حول التفتيش والحجز، اما الثاني فكاف المعاينة ومراقبة الاتصالات الإلكترونية.

الفرع الأول: التفتيش والحجز في الجريمة الإلكترونية

التفتيش هو إجراء تقوم بيه سلطات الضبطية القضائية للبحث عن الأدلة المرتبطة بالجريمة الإلكترونية فالتفتيش لا يكون ماديا تقليديا بل يشمل الحواسيب والهواتف الذكية وغيرها من الأجهزة الإلكترونية وهو من الإجراءات التي ثمنها القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أما الضبط أو الحجز كما أطلق عليه المشرع في إطار القانون 09-04 إجراء جديد خاص بالمعطيات والذي يتناسب مع طبيعة اللامادية و اللامحسوسة لجرائم الأنترنت.

أولاً: التفتيش الإلكتروني:

أ. مفهوم التفتيش الإلكتروني

قبل الحديث عن مفهوم التفتيش يجدر بنا الإشارة أن المشرع الجزائري لم يضع تعريفا تشريعيا للتفتيش الإلكتروني في القانون 09-04 وإنما اكتفى فقط بتنظيم احكامه وضوابطه تركا ذلك للفقهاء، وبالرجوع للتعريفات الفقهية فإنه يقصد بالتفتيش بوجه عام «هو البحث عن أشياء تفيد في الكشف عن الجريمة وقعت ونسبتها إلى المتهم وفقا للإجراءات القانونية محددة».

أما التفتيش الإلكتروني فهو إجراء مستحدث نظرا لحدثة هذه الجرائم لكن يبقى التفتيش إجراء معروف منذ القدم، ومن بين اهم التعريفات التي أجمع عليها الفقهاء الجنائي هو: «الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، يستوي في ذلك أن يكون هذا المحل جهاز الحاسب الآلي أو أنظمة أو شبكة الأنترنت» كما عرفه المجلس الأوروبي بأنه: إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني من أجل الوصول إلى مرتكب وحيثياتها (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري) (أطروحة دكتوراه)، 2017/2018، صفحة 214).

انطلاقا من التعريفات السابقة يتضح بأن التفتيش ينطبق على الجرائم التي تترك آثار مادية وبالتالي فلا توجد مشكلات تعيق إجراؤه لأن من خلاله سيتم البحث عن الأدلة المادية الملموسة.

ب. ضوابط التفتيش الإلكتروني

يمكن تقسيمهم الى نوعين:

1) الضوابط الموضوعية للتفتيش

يقصد بالضوابط الموضوعية للتفتيش الإلكتروني تلك الشروط اللازمة لإجراء تفتيش صحيح والتي يمكن حصرها في أربعة شروط أساسية تتمثل في: سبب التفتيش، المحل المراد تفتيشه، السلطة المختصة بالتفتيش و صدور الإذن بالتفتيش.

• سبب التفتيش الإلكتروني:

التفتيش هو إجراء يتم عادة عند وقوع جريمة ويستند إلى وجود شخص معين مشتبه هو في ارتكاب الجريمة أو وجود أدلة ومؤشرات تشير إلى وجود جريمة أو تساهم في إثباتها، يهدف التفتيش إلى الحصول على أدلة تساعد في كشف الحقيقة وإثبات الجريمة أو الكشف عنها ويجب أف يستند التفتيش إلى مبررات محددة توضح السبب والهدف منه ومن بين هذه المبررات:

- وقوع جريمة معلوماتية وهي كل فعل غير مشروع مرتبط باستخدام الحاسوب لتحقيق أغراض غير مشروعة.
- تورط شخص أو اشخاص معينين في ارتكاب الجريمة الالكترونية أو الاشتراك فيها.
- توافر إمارات قوية أو قرائن على وجود اشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة " (الهام، 2018، صفحة 32).

• المحل المراد تفتيشه:

يفيد مكان التفتيش في الجرائم البسيطة على أنه المكان الذي تخزن فيه الأشياء المتعلقة بالجريمة أو أسرار الجريمة وفي هذه الحالة يكون مكان التفتيش هو المتهم أو شخص آخر غير المتهم أو محل إقامة المتهم ومحتوياته أو محل إقامة غير محل إقامة المتهم ومحتوياته أثناء ارتكاب الجريمة يجب فحص جميع مكونات الحاسوب سواء كانت مادية مثل الأجهزة والأقراص أو غير ملوسة مثل البرمجيات والبيانات ويشمل ذلك أيضاً شبكات الاتصالات الحاسوبية ، ولكن من المهم الإشارة إلى أنو عند فحص هذه الوحدات قد تكوف موجودة ككيانات مستقلة في موقع معين مثل المنزل أو المكتب أو قد تكون مرتبطة بمالكها أو أصحابها مثال الكمبيوتر المحمول وينبغي دراسة هذا الجانب العملي والوظيفي على سبيل المثال شبكات الحاسوب والاتصالات السلكية واللاسلكية (ليندا، 2017، صفحة 492).

• السلطة المختصة في التفتيش:

التفتيش هو الإجراء المتخذ بشأن الجرائم الجسدية أو الجرائم المرتكبة إلكترونياً يتعلق الأمر بفحص حقوق وحريات كل شخص، حيث يسمح القانون الجنائي بالسيطرة على بيئة التحقيق ويعتبر ذلك ضرورياً لإجراء المزيد من القضايا وتبسيط وتسريع التحقيق وكما يجوز لسلطات التحقيق تفويض الشرطة بمهام التحقيق للاستفادة من خبرة الشرطة وكفاءتها في القيام بهذا الإجراء فيما يتعلق بالتحقيقات المتعلقة بالإعلام الإلكتروني، يسمح القانون الجزائري لسلطات التحقيق بطلب مساعدة خبراء للقيام بهذا الإجراء وإجراء التدابير المتخذة لحماية البيانات ونظم المعلومات ذات الصلة ويتولى هؤلاء الخبراء مسؤولية تقدير المساعدة وتوفير المعلومات اللازمة لوكالة التحقيق للقيام بمهامها (الهام، 2018، صفحة 36).

• صدور الإذن بالتفتيش واحترام الميعاد:

في كثير من الأحيان يتم إصدار أمر تفتيش لمنزل المشتبه به ويغطي على هذا المذكرة جميع العناصر الموجودة في المنزل فهل يجوز لمأموري الضبط القضائي الدخول إلى البيئة والدخول إلى النظام للبحث عن أدلة قد تكون عرضة للاعتقال في هذه الحالة يتفق معظم الخبراء القانونيين على أن مذكرة التفتيش يجب أن تحدد المكان الذي سيتم تفتيشه والأشخاص أو الأشياء التي سيتم تفتيشها ومصادرتها أجهزة الكمبيوتر وأشرطة الفيديو الجنسية للأطفال، والأعمال الإلكترونية المزيفة، الغرض من هذا التعريف في أمر التفتيش هو تجنب مراقبة التفتيش بحيث يكون للشخص سلطة ممارسة أي سلطة تقديرية ومع ذلك هناك مشكلة في تنفيذ التحكم في جهاز الحاسوب (ليندا، 2017، صفحة 393).

حيث أوضح المشرع الجزائري أنو كقاعدة عامة ينبغي اتباع هذا الإجراء من الساعة الخامسة صباحاً إلى الساعة الثامنة مساءً، خلال المدة المحددة في المادة 47 من القانون الإجراءات الجزائية إلا في حالات خاصة ومع ذلك ونظراً لطبيعة المعلومات المراد التحكم فيها، فمن السهل تدميرها وحظرها وتعديلها عند علمهم بإجراء بحث مشبوه يعتقد العديد من الخبراء القانونيين أن السيطرة على نظام المعلومات لا ينبغي أن تكون محدودة وفقاً للحد

الزماني المطلوب ولكن يجب أن يتم ذلك في أي وقت من النهار أو الليل وقد تبني المشرع الجزائري الفكرة طبقاً للمادة 47 فقرة 3 من الأمر 66-155 المؤرخ في 18 صفر 1386 الموافق ل 8 يونيو سنة 1966 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم، ومن الممكن هنا إجراء المراقبة فيما يتعلق بجرائم المعلومات ليلاً أو نهاراً وعند الضرورة ويجب الحصول على إذن من الوكيل الجمهورية.

(2) الضوابط الشكالية لتفتيش في الجريمة الإلكترونية:

يقصد بها الشروط اللازمة للقيام بالتفتيش وهي إجراءات سابقة له

• ضرورة توفر الإذن واحترام ميعاد التفتيش:

في إطار الجرائم الإلكترونية يعد التفتيش الرقمي من أبرز الوسائل التي تلجأ إليها السلطات القضائية للكشف عن الأدلة الرقمية التي قد تكون مخزنة في أجهزة الحاسوب أو على الشبكات الإلكترونية، غير أن هذا النوع من التفتيش يثير إشكاليات قانونية تتعلق بحماية الحياة الخاصة وسرية المعطيات الشخصية.

لذلك يشترط القانون الجنائي أن يتم تفتيش الأجهزة الإلكترونية أو الولوج إلى البيانات المخزنة فيها بموجب إذن قضائي صريح ومسبق، مالم تكون هناك حالة تلبس تستوجب التدخل الفوري، كما يجب أن يتم هذا الإجراء تحت رقابة السلطة القضائية التي تحمي خصوصية الأفراد وتضمن مشروعية الدليل المستخرج

• أن يتم تحرير محضر خاص بعملية التفتيش:

يحرر محضر التفتيش لتوثيق عملية دخول الأجهزة الأمنية إلى الفضاء الرقمي أو الأجهزة الإلكترونية المشتبه فيها فيجب تسجيل هذه الأنشطة أثناء إعداد تقرير يوضح العملية والأدلة المتعمقة بالتدقيق كما يجب أن يتضمن تقرير التدقيق المعد وصفاً للعملية من البداية إلى النهاية وقائمة بالاعتقالات والاحتجازات التي تمت خلال ذلك ويجب أن يكون التقرير موقعاً من قبل الشخص الذي يقوم بالتفتيش والشخص الملزم قانوناً بالتوقيع عليه

(الهام، 2018، صفحة 39).

ويهدف المحضر إلى ضمان مشروعية الإجراءات وحماية الأدلة الرقمية حتى يمكن اعتمادها أمام القضاء وهذا ما جاءت بيه المادة 79 من قانون الإجراءات الجزائية حيث يتم التفتيش في الجريمة الالكترونية بأسلوب آلي الكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة أن يكون أمر التفتيش مسببا أي يجب أن يتضمن الاسباب التي أدت الى إجراءه.

ويتكون فريق التفتيش: من خبراء مسرح الجريمة من الفنيين والمختصين بشكل ممتاز بالحاسوب والأنظمة الالكترونية وبالإضافة الى رجال الشرطة وأن يتكون الفريق من: المشرف على التحقيق، فريق التفتيش العملي من خبراء الحاسوب، فريق الأمن والحماية من رجال الشرطة.

• إجراء التفتيش بالحضور الضروري لبعض الأشخاص المعنيين بالقانون:

يعتبر هذا الشرط من أهم الشروط الشكلية التي يطلبها القانون في الجرائم التقليدية، لكن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم 06-22 من المادة 45 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ومنه استغنى على ضمانة حضور الأشخاص المحددين في الفقرة الأولى من المادة (المشتبه فيه أو المتهم أو إذا كان هاربا أو منع من الحضور وجب حضور شاهدين من غير الموظفين الخاضعين لسلطة القائمة بالتفتيش) في جرائم معينة منها الماسة بأنظمة المعالجة الآلية للمعطيات، والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية إثناء جمع الدليل الإلكتروني، خاصة و أن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله و التلاعب فيه حتى عن بعد .

ثانيا: الضبط في الجرائم الإلكترونية:

أ. تعريف الضبط في الجريمة الإلكترونية

لما أقر المشرع الجزائري تفتيش المنظومة المعلوماتية كما سبق وأن فصلنا فبالضرورة كان لابد له أن يقر ضبط الاشياء المستخلصة من تفتيش البيئة الافتراضية بما يناسبها وهو

الحجز بأنواعه، والحجز هنا هو كل ما يتعلق بإجراءات التحقيق أي التفتيش عن بعد والضبط هنا يعد من إجراءات التحقيق حيث أن الضبط يعد في الأصل من إجراءات الاستدلال (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري) (أطروحة دكتوراه)، 2017/2018، صفحة (288).

في التشريع الجزائري نجد الحجز في الجريمة الإلكترونية مؤطر بنص المادة 06 من القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها التي تنص على أنه عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس ضروري حجز كل المنظومة، يتم نسخ المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية، تكون قابلة للحجز، والوضع في احراز وفقا للقواعد المقررة في قانون إجراءات الجزائية الجزائري.

ب. الشروط القانونية لإجراء الحجز الإلكتروني

تبني المشرع الجزائري في القانون 04-09 إجراءات مستحدثة بضبط وحجز المعطيات والبيانات المعلوماتية وغيرها من الأدلة الرقمية بما يناسب وطبيعتها اللامادية، حيث خصص مجموعة من المواد شكلت الشروط القانونية لهذا الاجراء وتتمثل هذه الشروط فيما يلي:

الشرط الأول: حجز المعطيات والبيانات الأولية:

حيث يشمل على الأشياء المادية، وعلى البيانات المعالجة الكترونيا أما بالنسبة لتحديد محل الحجز كل المعطيات المخزنة المفيدة في الكشف عن الجرائم أو مرتكبيها واستثناء يتم الحجز الجزئي أي اكتفاء بالمحتوى الذي يتعلق بالمجرم.

الشرط الثاني: الحجز عن طريق منع وصول المعطيات:

وهذا خوفا من ضياع أو اتلاف الأدلة الرقمية حيث أعط القانون السلطات المعنية قيام بهذا الاجراء، وجذا ما نصت عليه المادة 07 من القانون 04-09 السالف الذكر، كما نلاحظ من خلال المادة 09 أن المشرع حصر حالات اللجوء إلى الحجز عن طريق منع

الوصول في الحالة الواحدة كما نصت المادة 08 من نفس القانون على التحفظ على البيانات محل الجريمة أو أدواتها.

الشرط الثالث: وضع حدود لاستعمال المعطيات:

طبقا للمواد 07 و 08 و 09 من القانون 04-09 أنه عقب كل عملية تفتيش أو معاينة إيجابية، يتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، وتبقى المحجوزات تحت تصرفها إلى غاية انتهاء المحاكمة.

ج. صعوبات عملية حجز البيانات المعالجة إلكترونيا:

حجم الشبكة التي تحتوي على المعلومات المعالجة إلكترونيا والمطلوب ضبطها من ذلك البحث في نظام الكتروني لشركة متعددة الجنسيات.

- وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع جهات الشرطة والتحقيق في عملية التفتيش والضبط والتحفظ.

- يمثل التفتيش والضبط أحيانا اعتداء على حقوق الغير أو على حرمة حياته الخاصة فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق وتلك الحريات.

ولضمان الحفاظ على البيانات محل البحث ومقارنتها بالنسخة المخرجة من الجهاز في حالة بعدها من المتهم فقد أعطى القانون البلجيكي للنيابة العامة سلطة الأمر بغلق هذه البيانات لمنع الوصول إليها أو الى النسخة المستخرجة منها الموجودة لدى من يستعملون النظام.

الفرع الثاني: المعاينة والمراقبة الإلكترونية

بالإضافة الى التفتيش والضبط تأتي إجراءات تتعلق بالمعاينة والمراقبة:

أولا: المعاينة في الجريمة الإلكترونية:

عند التكلم على إجراءات التحري كلاسيكية للكشف عن الجريمة الإلكترونية، لابد من دراسة معاينة مسرح الجريمة الإلكترونية، ويقصد بهذه الأخيرة رؤية عين المكان أو الشخص

أو الشيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة ويعد مسرح الجريمة بمثابة الشاهد الصامت الذي إذ أحسن المحقق استنطاقه حصل على معلومات مؤكدة.

أ. معاينة مسرح الجريمة:

لمعاينة مسرح الجريمة الإلكترونية يجب التفرقة بين حالتين:

• معاينة الجرائم الواقعة على المكونات المادية للحاسوب Hardware

كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أي مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

• معاينة الجرائم الواقعة على المكونات غير مادية أو بواسطتها software

تلك الجرائم الواقعة على برامج الحاسوب وبياناته، تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته، وهذه الصعوبات تتلخص فيما يلي:

- قلة الآثار المادية المترتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب.

- الأعداد الكبيرة من الأشخاص الذي يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لإحداث تغييرات أو العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل المستقي من المعاينة.

فالمعاينة في الجريمة الإلكترونية ليست مسألة مرتبطة بالضرورة بالانتقال عبر العالم المادي بل قد تتم عبر العالم الافتراضي وهناك عدة طرق يستطيع بها عضو سلطة التحقيق أن ينتقل الى العالم الافتراضي للمعاينة ومن ذلك:

- من مكتبه بالمحكمة من خلال الحاسب الآلي الخاص به.

- كما يمكنه اللجوء الى مقهى الأنترنت وأيضا يمكنه اللجوء الى مزود خدمة الأنترنت الذي

يعتبر أفضل مكان يمكن إجراء المعاينة فيه (إبراهيم، 2009، صفحة 156/157).

- ويستطيع المحقق المعاينة في المسرح التقليدي ويقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة كالبصمات وغيرها وربما ترك متعلقات شخصية.

ب. الضوابط الواجب مراعاتها عند معاينة مسرح الجريمة

ولنجاح المعاينة في الجرائم المعلوماتية يوصي الخبراء بوجوب إتباع ومراعاة قواعد وإرشادات فنية أبرزها ما يلي:

- القيام بتصوير الحاسوب وما قد يتصل به من أجهزة طرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة بالتركيز على تصوير أجزائه الخلفية وملحقاته، ومراعاة تسجيل الزمان والتاريخ والمكان الذي التقطت فيه كل صورة.

- يجب ملاحظة واثبات الحالة التي تكون عليها توصيلات الكابلات (الخيوط الكهربائية للحاسوب)، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.

- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو البيانات المسجلة.

- وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.

- ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية مقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.

- التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.

- القيام بحفظ المستندات الخاصة بالإدخال، وكذا مخرجات الحاسوب الورقية التي قد تكون لها صلة بالجريمة، وذلك من أجل رفع البصمات التي قد تكون موجودة (نورة، 2012-2011، صفحة 131).

- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعلمية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها

- إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها.

- أن تتم هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية. والمعاينة وإن أنت في الجرائم إلا أن أهميتها تتضاءل في بعض الجرائم مثل جريمة السب.

ثانيا: المراقبة الاتصالات الإلكترونية:

تتمثل المراقبة في كشف الجرائم قبل وقوعها وتلعب دورا كبيرا في الكشف عن الجرائم الإلكترونية وهي وسيلة هامة من وسائل الإرشاد الجنائي، ويقصد به المراقبة الأمنية التي محلها الاتصالات الإلكترونية التي عرفها المشرع الجزائري في المادة 2 من القانون 04-09 وهي التي ترسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

يقصد بالمراقبة بوجه عام تعمد الاتصال والتسجيل على المحادثات الخاصة، أما المحادثات العامة فلا قيد على مراقبتها وتسجيلها سواء علم أصحابها ذلك أو لا يعلموا لأن ذلك ليس بحرمتهم وخصوصياتهم مادامت هذه المحادثات عامة، وقد استخدم عدد من المصطلحات من طرف الفقه والقانون للدلالة على المراقبة الإلكترونية، ومن بين المصطلحات، الاعتراض الالتقاط في حين استخدمه المشرع الجزائري في القانون 04-09 (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري (أطروحة دكتوراه)، 2017/2018، صفحة 209) مصطلح مراقبة الاتصالات الإلكترونية والذي يقصد به اعتراض المحادثة وقطع الطريق عنها ومنعها من الوصول إلى وجهتها.

أ. محل مراقبة الاتصالات الالكترونية

إن محل المراقبة هو ذلك الهدف الذي تتم مراقبته وتتبع حركاته وتصرفاته في نطاق المراقبة الالكترونية محل المراقبة هو الحاسوب الرقمي أو الموقع عبر شبكة الأنترنت أو البريد الالكتروني بما يحتويه من مراسلات الكترونية وحلقات نقاش وغرفة دردشة، وقد يكون محلها الهاتف النقال المتصل بشبكة الأنترنت وحتى ساعة اليد الذكية أو اللوح الرقمي، إذن محل المراقبة يشمل الاتصالات الالكترونية الخاصة والتي عرفت المادة الثانية من القانون 04-09، قد ميز المشرع بين نوعين من المعطيات المعالجة، المراقبة، النوع الأول المراقبة المتعلقة بحركة سير معطيات المرور، أما النوع الثاني المعطيات المتعلقة بمحتوى الاتصال فبالنسبة للنوع الأول عرفت المادة 02 من القانون 04-09 أما النوع الثاني والمتعلقة بالمحتوى فلم يرد تعريف لذلك ولو أنه بمفهوم المخالفة هي كل المعطيات المعالجة باستثناء ما تعلق بمعطيات المرور، فمعطيات المحتوى هي محل المراقبة الالكترونية ذلك بأن أدرجها المشرع في المادة الرابعة من القانون 04-09 أما معطيات المرور فقد حصرها المشرع بإجراء حفظ المعطيات المتعلقة بحركة السير المادة 11 من القانون 04-09.

ب. شروط مراقبة الاتصالات الإلكترونية:

لكي تتم مراقبة الاتصالات الالكترونية على الوجه الصحيح لابد أن يلتزم ضابط الشرطة القضائية المختص والمكلف بهذا الإجراء الذي لابد أن يكون من ذوي الكفاءة والخبرة في استخدام التكنولوجيا الحديثة للاتصال بشروط المراقبة التي تعتبر ضمانات في مقابل كفالة حماية الحق في الحياة الخاصة لذلك فالمادة تجيز التدخل في نطاق الحياة الخاصة للأفراد ولكن بشروط معينة (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري) أطروحة دكتوراه، 2017/2018، صفحة 210/211).

أ. الشروط العامة:

تتمثل في جدية الأسباب أي الجدية الكافية وهذا بغض النظر عن النتيجة التي توصل إليها أي نتيجة سلبية أو إيجابية، التقيد بالكشف عن النشاط الإجرامي وهذا بتحديد الهدف

من مراقبة الاتصالات والمتمثل في الوقاية من الجرائم أو الكشف عنها وهذا ما جسده المادة الثالثة من القانون السالف الذكر بالإضافة الى التقيد بالغرض المرجو من المراقبة حيث أنه قبل اللجوء الى المراقبة لابد من وجود دلائل على إمكانية وجود الجريمة أو وجودها بالفعل على أن تكون هناك وقائع فعلا منسوبة الى مشتبه فيه وأخيرا مشروعية الوسيلة، فاستخدام البرمجيات اللازمة لعملية المراقبة لابد أن تكون أصلية أي ليست مستنسخة عن البرامج الأصلية لكي يكون للدليل قيمة أصلية في الإثبات الجنائي والجدير بالذكر أن مراقبة الاتصالات الالكترونية كانت في الأصل إجراء وقائي لحماية الشبكات وبالتالي أساسها برمجيات المراقبة المستعملة من طرف مبرمجي الشبكة العالمية والتي تستخدمها المصالح المختصة في الضبط من أجل مراقبة الاتصالات على الشبكة (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري) (أطروحة دكتوراه)، 2017/2018، صفحة 211).

ب. الشروط الخاصة

- ضرورة صدور أمر من السلطة القضائية المختصة باللجوء إلى مراقبة الاتصالات الالكترونية والتفتيش: يُعد الحصول على إذن بمراقبة الاتصالات الإلكترونية من السلطة القضائية المختصة من أهم الضمانات التي يوفرها المشرع الجزائري أو التشريعات الأخرى المماثلة للأفراد ويجوز لقاضي التحقيق أو في بعض الحالات أو النائب العام لمجلس قضاء الجزائر قبل إصدار الإذن كما هو منصوص عليه صراحة في الفقرتين 2 و 3 من المادة 4 من القانون 04-09

- صدور إذن مكتوب من السلطة القضائية المختصة: وتنص المادة 4 من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وبمكافحتها في فقرتها الأخيرة على وجوب صدور إذن كتابي من السلطة القضائية المختصة.

- تحرير محضر بالعمليات التقنية التي تم القيام بها: بموجب أحكام القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

ومكافحتها وبالتالي يجب على ضباط الشرطة القضائية المأذون ليهم أو المفوضين مم طرف القاضي المختص إعداد تقارير عن جميع أعمال إنشاء الوسائل التقنية لمراقبة الاتصالات الإلكترونية ونتائجها وكذلك عن التحقيقات التي أجريت والأدلة التي تم الحصول عليها، كما يجب أن يتضمن التقرير أيضا تواريخ و أوقات بدء هذه المهام وإنجازاتها، فضلا عن المتطلبات الشكلية العامة في جميع التقارير و يجب أن يكون مكتوبا باللغة المراد بها ألا وهي العربية.

- تحديد الشخص المراد مراقبة اتصالاتهم الإلكترونية: يجب تحديد الاشخاص الذين ستم مراقبة اتصالاتهم الإلكترونية من خلال ذكر الاسم واللقب، يجب تحديد هوية الاشخاص الذين ستم مراقبة اتصالاتهم الإلكترونية من خلال ذكر الاسم واللقب ومكان الإقامة حيث لا يكون إجراء البحث ساري المفعول إلا إذا تم تحديد نظام المعلومات المراد البحث فيه بشكل صحيح ولا يلزم ذكر مكان وجوده سواء كان عاما او خاصا، إذا تم التعرف على مالكه وذلك لان نظام المعلومات الخاضع للتفتيش هو الذي يجب لن يكون مشمولا في تصريح البحث.

المطلب الثاني: اليات التحري المستحدثة عن الجرائم الإلكترونية

جاء دستور 1996 بعدة أساليب تحي مستحدثة من بينها أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وكذلك التسرب والاختراق في قانون الإجراءات الجزائية أصبح يمارس من قبل ضباط الشرطة، واعتمد المشرع الجزائري على ضوء القانون 22/06 لتفادي الفراغ القانوني وتم تقرير جملة من الإجراءات لمحاربة هذه الجريمة، حيث أجاز لوكيل الجمهورية أو قاضي التحقيق أن يأذن بهذا الأجراء عندما تقضي ضرورات التحري وهذا ما سنتطرق له في هذا المطلب:

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقط الصور

أولاً: اعتراض المراسلات في الجريمة الإلكترونية

أ. تعريف اعتراض المراسلات

قد عرف المشرع الجزائري الاعتراض بالتفصيل في المادة 65 مكرر 5 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 للإنتاج والتوزيع، التخزين، الاستقبال والعرض " (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري (أطروحة دكتوراه)، 2017/2018، صفحة 179).

نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلاً للاعتراض بتلك المراسلات التي تتم بواسطة وسائل 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) كالفاكس أو تلغرام أم لاسلكية (البريد الإلكتروني، الهاتف النقال)، باستثناء الكتب والمجلات والرسائل والحواليات والتي تعد مراسلات خاصة، وهذا ما أكدته المادة 02 الفقرة 06 من القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي عرفت الاتصالات الإلكترونية بأنها " أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة إلكترونية وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية.

فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون أو علم موافقة المعنيين، وذلك لغرض التصنت، والتقاط وتثبيت وبث وتسجيل البيانات المرسلّة أو

المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل المواجهة المتهم.

ب. الشروط الشكلية والموضوعية للاعتراض المراسلات:

- تحديد الجهة المختصة الموجه لها الاعتراض: يجب أن يوجه الاعتراض إلى الجهة المختصة (الجهة المرسله أو الجهة المشرفة على القرار) طبقا للمادة 65 مكرر 5 من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء الى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانا لازمة لمشروعية هذا الإجراء.

- تحديد الشخص المراد مراقبته وكذلك تاريخ المراسلة المعترض عليها: يشترط ذكر البيانات الشخصية للمعترض مثل الاسم الكامل او الاسم المعروف بيه والعنوان ورقم الهوية ووسائل الاتصال. كما يجب الإشارة بدقة إلى رقم المراسلة وتاريخها وموضوعها.

- تحديد طبيعة المراسلة ومدة الاعتراض: يلزم المشرع الجزائري في المادة 65 مكرر 9 من قانون الإجراءات الجزائية ضباط الشرطة القضائية المأذون لهم أو من ينوب عنهم من القضاة المختصين بإعداد تقرير عن اعتراض الاتصالات وتسجيلها، وعن الترتيبات التقنية لعمليات الاعتراض والتسجيل السمي والبصري والحصول عليها وتثبيتها وتسجيلها، كما يتم تدوين تواريخ وأوقات بدء هذه العمليات واتمامها في التقارير.

لا يفرض قانون الإجراءات الجنائية الجزائري أي قيود زمانية أو مكانية عمى الإجراءات ويستثنى من ذلك اعتراض الاتصالات في أي وقت من النهار أو الليل في الأماكن العامة أو الخاصة والقيد الوحيد المنصوص عليه صراحة في اللائحة يتعلق باتخاذ التدابير اللازمة لضمان احترام سرية الاتصالات ويشمل ضمان احترام السرية المهنية الاتصالات والمحادثات الهاتفية بيف المحامي وموكله، غير أن الالتزام بالسرية المهنية قد لا يكون واجب التطبيق إذا كان ذلك ينحرف عن دور الممارس ووظيفته عندما يتصرف كمتهم في

جريمة جنائية كما هو منصوص عليه في المادة 02 مكرر 2 من قانون الإجراءات الجزائية أو لأن المشرع يحمي احترام السرية المهنية فقط وليس كممارس، بالإضافة إلى هذه القيود المنصوص عليها بوضوح هناك قيد آخر لم يذكره المشرع وهو استبعاد السفارات والقنصليات الأجنبية من المواقع التي مم المحتمل أن تباشر فيها هذه التطبيقات (عمارة، 2010، صفحة 238).

ثانيا: تسجيل الأصوات والتقاط الصور

أ. تعريف تسجيل الأصوات والتقاط الصور

التسجيل الصوتي يشمل تسجيل الأحاديث الشخصية وتسجيل الأصوات، فالحديث عبارة عن كل صوت له دلالة التعبير عن مجموعة من المعاني والأفكار، كما يشمل التحدث بصوت مرتفع لذلك يخرج عن نطاق تسجيل الأصوات الأحاديث التي لا تتضمن اعتداء على الحق في حماية الحديث وتسجيله كما هو الحال في تسجيل الأحاديث الإذاعية والتلفزيونية أو الصحفية بعد موافقة المعني، أما تسجيل الصوت فهو إفراغ الأحاديث الخاصة في وعاء يحفظها مخصص لإعادة سماعها في وقت لاحق ونقله من مكان لآخر (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري (أطروحة دكتوراه)، 2017/2018، صفحة 138)، وهو التعريف المرتبط باعتراض المراسلات باعتبار أنه لا يمكن اعتراض هذا الأخير دون تسجيل، والذي لم يعرفه المشرع الجزائري بل وضح الجانب الفني منه في المادة 65 مكرر 5 الفقرة 3 من القانون الإجراءات الجزائية بقولها هو وضع الترتيبات الفنية.

اما النقاط الصور عن طريق وضع الترتيبات والمعدات التقنية اللازمة دون أخذ موافقة، ويقصد بإجراء التقاط الصور تثبيت الصور على مادة حساسة وتثبيت الصور يعني تركيزها بسرعة خاطفة ثم أخذها عن طريق جهاز معد لذلك، وعليه إجراء التقاط الصور هو عبارة عن معاينة مادية مرئية لحالة شخص أو عدة اشخاص على الوضعية التي كانوا عليها وقت التصوير، وهي تربط الزمان والمكان والأشخاص في وقت واحد وقد تمتد الى الدليل المادي للجريمة والى محيطه.

ب. موقف المشرع الجزائري من اعتراض المرسلات والتقاط الصور:

بالرجوع الى أحكام المادة 65 مكرر 5 الفقرة 03 من قانون إ. ج التي تنص على أن: "تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية "يلاحظ أن المشرع الجزائري قد مسح هذه المسألة وأخذ بالمعيار الشخصي الذي اعتداد بموضوع الحديث ذاته كمعيار للتفرقة بين الحديث العام والحديث الخاص المباشر، فالعبرة هنا ليس بخصوص المكان أو عمومته وإنما بخصوصية الحديث أي يقصد ذوي الشأن، وهذا القصد يستشف من موضوع الحديث ومن هيئة المتحدثين ودرجة علو صوته أي بالطريقة التي يتم بموجبها تبادل أطراف الحديث وليس بالمعيار الموضوعي أي المكان الذي يوجد فيه الشخص.

ومن خلال الرجوع الى نفس المادة من قانون إ. ج التي تنص على ما يلي: "التقاط صور لشخص أو عدة اشخاص يتواجدون في مكان خاص ..."، فيلاحظ أن المشرع الجزائري أخذ بالمعيار الموضوعي والذي يضع لطبيعة المكان وزنا في تحديد مدلول المكان الخاص، وهو كل مكان يمكن ارتباطه من قبل الجمهور سواء بمقابل أو بدون مقابل وينقسم الى ثلاثة أنواع: الأماكن العامة بطبيعتها وهي الأماكن التي تكون معدة منذ إنشائها لدخول الجمهور، الأماكن العامة بالتخصيص وهي الأماكن التي يسمح بارتباطها في أوقات معينة، الأماكن العامة بالمصادفة وهي بحسب الأصل تكون أماكن خاصة ويكون أمر ارتباطها مقصورا على أفراد وطوائف لتحديد مفهوم المكان الخاص أي بطبيعة المكان لا بحالة خصوصية التي يكون عليها الأشخاص على اختلاف إجراء تسجيل الأصوات الذي أخذ فيه المشرع بالمعيار الشخصي، حيث سمح المشرع أن يمد عين الكاميرا الى الأماكن الخاصة التي تعد مستودعات أسرار المعنيين بالمراقبة في سبيل اكتشاف الحقيقة واستبيان المجرم (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري (أطروحة دكتوراه)، 2017/2018، صفحة 187).

الفرع الثاني: التسرب أو الاختراق

ويعتبر أسلوب التسرب أو الاختراق تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط الشرطة القضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبّه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية، ويقدم المتسرب نفسه على أنه فاعل أو شريك.

أولاً: تعريف التسرب أو الاختراق

تناوله المشرع الجزائري في المادة 65 مكرر 12 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 بقوله: "يقصد بالتسرب قيام ضباط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهاهم أنه فاعل معهم أو شريك لهم أو خاف." هذا ويلاحظ أن المشرع سمى هذه العملية بالتسرب في قانون الإجراءات الجزائية في حين استخدم مصطلح الاختراق في المادة 56 من القانون رقم 01-06 المتعلق بالوقاية من الفساد ومكافحته، وهما مسميان لمسمى واحد ولهما نفس المدلول.

من خلال هذه المادة يتضح أن التسرب هو عبارة عن عملية ميدانية تستخدم أسلوب التحري لجمع الوقائع المادية والأدلة من داخل العملية الإجرامية وكذا الاحتكاك شخصيا بالمشتبه بهم والمتهمين وهذا ينطوي على خطورة بالغة تحتاج إلى دقة وتركيز وتخطيط سليم.

من ثم يمكن القول أن التسرب هو أكثر الوسائل تعقيدا وخطورة، لأنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بمناورات وتصرفات توحى بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة، لكنه في حقيقة الأمر يخدعهم ويتحايل عليهم فقط، حتى يطلع على أسرارهم من الداخل ويجمع ما يستطيع من أدلة إثبات، ويبلغ السلطات بذلك

فتمكن من ضبط المجرمين ووضع حد للجريمة (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري) (أطروحة دكتوراه)، 2017/2018، صفحة 195).

إذن ترتكز عملية التسرب على ضرورة الحصول على صورة حقيقية على الوسط المراد استكشافه لمعرفة طبيعة سيره وأهدافه وكذا معرفة تاريخ هذه الجماعة وكيفية نشأتها واختصاصات كل فرد من عناصرها، وأيضا الوسائل التي تعمل بها كوسائل النقل والاتصال وتحديد نقاط قوة وضعف هذه الجماعة، وبعد دراسة الوسط المستهدف يتم اختيار الأشخاص المناسبين لتولي مهمة التسرب.

ثانيا: شروط التسرب

اشترط المشرع في المادة 65 مكرر 11 من قانون الإجراءات الجزائية وجوب أن تقتضي ضرورات التحري أو التحقيق إجراء عملية التسرب، وبمفهوم المخالفة فإن وجود أدلة كافية تعزز الاشتباه أو تدعم الاتهام فإنه لا داعي للمخاطرة بإجراء عمليات تسرب وعليه فإن هذه الأخيرة تجرى عند الضرورة فقط المتمثلة في قلة أو صعوبة الحصول على أدلة وبراهين كافية لتحريك دعاوى عمومية.

كما اشترط المشرع في اللجوء إلى هذا الأسلوب ضرورة ارتكاب أنواع محددة من الجرائم التي تتسم بالخطورة والتعقيد، من ثم فإن الأمر بإجراء عمليات التسرب ليس مفتوحا لكل الجرائم بل هو خاص بمجموعة محددة من الجرائم المذكورة في المادة 65 مكرر 5 من قانون الإجراءات الجزائية، هذه الجرائم هي: جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، إذن فيما عدا هذه الأنواع المذكورة على سبيل الحصر لا يجوز استخدام هذا الأسلوب.

فلاحظ هنا أن المشرع الجزائري عدد هذه الجرائم على سبيل الحصر، وقد يرجع هذا للخطورة الإجرامية لهذه الأفعال وأثرها على السياسة العامة في الدولة واقتصادها، أما إذا كانت هذه الاعمال في غير هذه الجرائم فإجرائها باطل.

فلا يمكن بأي حال من الأحوال مباشرة عملية التسرب والكشف عن الجرائم السالفة الذكر إلا بعد الحصول على إذن من وكيل الجمهورية المختص إقليمياً أو قاضي التحقيق بعد إخطار وكيل الجمهورية (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري) (أطروحة دكتوراه)، 2017/2018، صفحة 200) ، يجب أن يكون الإذن المسلم مكتوب ومسبباً وذلك تحت طائلة البطلان مع ذكر الجريمة التي تبرر اللجوء الى هذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته، ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر ويمكن أن تتجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية ويجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.

ثالثاً: صور التسرب

استناداً لنص المادة 65 مكرر 12 من قانون الإجراءات الجزائية فإن عملية التسرب تتم وفق ثلاث صور هي:

أ. المتسرب كفاعل: من أجل التحري الفعال لهذا الإجراء الخطير سمح المشرع الجزائري للضابط أن ينتحل دور الفاعل الرئيسي مع أعضائها وذلك من خلا ارتكابه للسلوكيات الاجرامية المذكورة في المادة 65 مكرر 14 من قانون إجراءات الجزائية، والهدف من قيام الضابط بهذا الدور هو كسب الثقة الكاملة لأعضاء المنظمة الاجرامية والحصول على الأدلة الكاملة التي تساعد للوصول للحقيقة، غير أنه مقيد بشرط عدم قيامه بأعمال تحريضية واعما خارج القانون.

ب. المتسرب كشريك: المتسرب الذي يأخذ صورة الشريك يوهم المشتبه فيهم بأنه يريد تقديم المساعدة لهم ويقوم بمشاركتهم أو تقديم مسكن أو ملجأ ويسايرهم في السلوكيات الاجرامية إلى حين الإيقاع بهم متلبسين بجرمهم.

ج. المتسرب كخاف: سمح المشرع الجزائري للضابط أو العون المتسرب بعملية الاخفاء وذلك بصفة استثنائية وذلك من أجل مكافحة الاجرام وإجهاض مخططات الجماعات الاجرامي.

المبحث الثاني: مشروعية اليات التحري عن الجرائم الإلكترونية

مع التطور التكنولوجي المتسارع واتساع رقعة استخدام الإنترنت برزت الجرائم الإلكترونية كأحد التحديات الأمنية و القانونية الأبرز في الوقت الحالي فقد باتت تلك الجرائم ترتكب بوسائل متطورة يصعب معها كشف الجناة بالأساليب التقليدية ،مما استدعى تطوير أساليب التحري الإلكترونية لتكون أكثر فعالية ،غير أن هذا التطور يثير تساؤلات قانونية جوهرية تتعلق بمدى مشروعية الوسائل المستخدمة في جمع الأدلة الرقمية و ضرورة تحقيق التوازن بين حماية الأمن العام من جهة و صيانة الحقوق والحريات الفردية من جهة أخرى، ومن هنا تبرز أهمية دراسة مشروعية أساليب التحري في الجريمة الإلكترونية باعتبارها ضمانة أساسية لاحترام سيادة القانون في الفضاء الرقمي، وفي هذا السياق سنتطرق إلى موقف المشرع الجزائري من آليات التحري عن الجريمة الإلكترونية في المطلب الأول، أما المطلب الثاني سنتناول فيه الاختصاص القضائي في الجريمة الإلكترونية.

المطلب الأول: موقف المشرع الجزائري من أساليب التحري عن الجريمة الإلكترونية

موقف المشرع الجزائري من أساليب التحري الخاصة بالجريمة الإلكترونية يتسم بالحرص على التوفيق بين فعالية مكافحة هذا النوع من الإجرام المستحدثة وضمان احترام الحقوق الدستورية وخصوصا حماية الخصوصية والحرية الشخصية وقد تجلّى هذا الموقف من خلال:

ادراج المشرع الجزائري احكاما خاصة بمكافحة الجريمة الإلكترونية ضمن قانون العقوبات وكذلك قانون الإجراءات الجزائية وأيضاً في الدستور الجزائري المعدل في 2020 في نص المادة 47 التي تنص على "لكل شخص الحق في حماية حياته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت، لا مساس

بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية، حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي" كما جاء أيضا بالقانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

الفرع الأول: نطاق تطبيق أساليب التحري في الجريمة الإلكترونية

نطاق تطبيق أساليب التحري في الجريمة الإلكترونية يشمل مجموعة من الإجراءات الفنية والقانونية التي تهدف إلى الكشف عن مرتكبي الجرائم باستخدام الوسائط الإلكترونية، مثل الأنترنت أو الأجهزة الرقمية، حيث يتم إعمال هذه الأساليب من طرف الشرطة القضائية وهذا ما ورد في المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري، حيث تشمل حالة التلبس بالجريمة والتحقيق التمهيدي في جرائم معينة بالإضافة الى الإنابة القضائية.

أولاً: حالة التلبس بالجريمة:

حصر المشرع الجزائري التلبس في حالات معينة هذا ما نصت عليه المادة 41 و62 من قانون الإجراءات الجزائية وهي:

أ. ارتكاب الجريمة في الحال: المقصود بذلك هو ضبط الجاني أثناء قيامه بارتكاب الجريمة الإلكترونية أو فور الانتهاء منها مباشرة سواء كان ذلك من خلال الأنترنت أو أي وسيلة إلكترونية مع وجود دلائل فنية تثبت أنه في حالة تلبس رقمية، مثل ضبط شخص أثناء اختراقه نظاما إلكترونيا أو مشاهدة شخص ينشر محتوى غير قانوني على وسائل التواصل في الوقت الفعلي.

ب. مشاهدة الجريمة الإلكترونية عقب ارتكابها: يقصد بها أن يتم رصد أو اكتشاف آثار الجريمة مباشرة بعد وقوعها دون أن يشاهد الفعل الإجرامي أثناء التنفيذ، ولكن تكون المؤشرات والدلائل واضحة وحديثة تدل على ارتكاب الجريمة منذ وقت قريب، ومثال ذلك مشاهدة منشور إلكتروني مسيء نشر للتو من حساب معروف أو اكتشاف عملية اختراق حدثت منذ دقائق مع تتبع مصدر الاتصال.

ج. حيازة المجرم لأشياء تتدل على مساهمة في الجريمة الإلكترونية: تعني أن يعثر بحوزة شخص على أدوات أو بيانات رقمية تستخدم عادة في ارتكاب الجرائم الإلكترونية وذلك عقب وقوع الجريمة مباشرة، مما يعد قرينة قوية على مشاركته فيها، ومثال ذلك حيازة حاسوب أو هاتف يحتوي على برامج اختراق أو أدوات تجسس مثل key loggers أو أدوات ddos وهذا ما جاء في المواد من 41 إلى 62 من قانون الإجراءات الجزائية.

ثانيا: التحقيق التمهيدي في جرائم معينة

حدد المشرع الجزائري الاختصاصات الاستثنائية لضباط الشرطة القضائية في الحالات الخاصة بجرائم معينة، وذلك بموجب المادة 65 مكرر 5 من قانون الإجراءات الجزائية، فالتحقيق التمهيدي هدفه جمع الأدلة الأولية وتحديد هوية الفاعلين قبل البدء بالإجراءات القضائية الرسمية (زوزو، 2017، صفحة 761).

فالجرائم الماسة بالمعالجة الآلية للمعطيات: نص عليها المشرع في القسم السابع مكرر من قانون العقوبات المعدل بالقانون رقم 23-06 المؤرخ في 20/12/2006 بالمواد 394 مكرر الى 394 مكرر 07 وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

الفرع الثاني: ضوابط مشروعية أساليب التحري في الجريمة الإلكترونية

تعد أساليب التحري الجنائي من الوسائل الجوهرية التي تعتمد عليها الأجهزة الأمنية والقضائية في كشف الجرائم وتعقب مرتكبيها، بما يضمن تحقيق العدالة وصيانة النظام العام ومع تطور الجريمة وتعقيد صورها، تزايدت الحاجة إلى استخدام أساليب تحري أكثر فاعلية ودقة ما دفع المشرع إلى تنظيمها وتقييدها بضوابط قانونية تضمن التوازن بين مصلحة المجتمع في مكافحة الجريمة من جهة، وضمان حقوق الأفراد وحياتهم الأساسية من جهة أخرى، وتنقسم هذه الضوابط إلى قسمين:

أولاً: الضوابط الموضوعية: تتمثل فيما يلي:

أ. أن تتعلق بفئة معينة من الجرائم:

لا يرخص بأساليب التحري الخالصة إلا بالنسبة للجرائم المحددة حصراً في القانون حيث يجب أن يكون هناك نص قانوني يجيز استخدام هذه الأساليب أما المشرع الجزائري أما فاشتراط لمشروعية الأساليب الخاصة ولضمان عدم التعدي على حقوق الأشخاص، أن يتعلق الأمر بالجرائم المحصورة في ثمانية فئات وهي: جرائم المخدرات، الجريمة المنظمة العابرة لحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد (المادة 65 مكرر 1/5 إ ج ج) (معمرى، 2015، صفحة 473).

نستنتج أن المشرع الجزائري جعل أساليب التحري عن الجريمة الإلكترونية ضمن نصوص قانونية ولا يجوز استخدام وسائل أو أساليب غير منصوص عنها صراحة.

ب. أن يكون إذن مسبق من السلطة القضائية:

غالبا ما يشترط القانون الحصول على إذن مسبق من النيابة العامة أو القاضي المختص خاصة في الحالات التي تمس الحقوق والحريات الأساسية مثل التنصت أو المراقبة أو التفتيش، حيث نصت المادة 65 مكرر 7 من قانون الإجراءات الجزائية على أنه يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه ... الجريمة التي تبرر اللجوء الى هذه التدابير وقد جاء هذا النص بصيغة الوجوب، مما جعل كل إذن لا يتضمن الإشارة الى الجريمة المعاقب عليها إذنا باطلا لا يعتدى به.

ج. الإشراف القضائي على أساليب التحري:

السلطة الوحيدة المؤهلة للإذن بالأساليب التحري هو وكيل الجمهورية أثناء مرحلة التحري (مادة 65 مكرر 1 من ق. إ. ج) ويكون بذلك المشرع قد وضع ضمانة هامة لحماية حقوق الأشخاص مستوجبا صدور إذن من وكيل الجمهورية يتضمن الترخيص بالأساليب الخاصة، وأن تتم الإجراءات تحت رقابته المباشرة فلا يجوز لضابط الشرطة القضائية القيام

بإحدى الأساليب الخاصة من تلقاء نفسه ودون إذن مسبق من وكيل الجمهورية. والفقه والقضاء متفقان على أن هذه الإجراءات محظورة على ضابط الشرطة القضائية دون الإذن له بذلك، حتى ولو تعلق الأمر بحالة التلبس بالجريمة ويمتنع على ضابط الشرطة القضائية أن يندب غيره للقيام بإحدى الأساليب الخاصة، لأن النذب لا يكون إلا من طرف وكيل الجمهورية، ولا يحق له إلا تسخير الأعوان المؤهلين لدى إحدى المصالح أو الوحدات أو الهيئات العمومية أو الخاصة المكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية لعمليات الاعتراض والتسجيل الصوتي والمرئي (م 65 مكرر 8 إ ج ج). والقيام بإحدى هذه الترتيبات التقنية والدخول في المنازل لوضعها دون إذن مكتوب من وكيل الجمهورية المختص، يجعل الأدلة المستمدة باطلة وتبطل جميع الإجراءات التي بنيت عليها، حتى ولو اكتشفت عرضا جريمة متلبس بها، لأن ما بني على باطل فهو باطل. ونشير بأن إذن الاعتراض والتسجيل الصوتي والمرئي ليس له طابع قضائي وغير قابل للطعن ولا يوجد ضمن قانون الإجراءات الجزائية الجزائري ولا الفرنسي نص يوجب تبليغه إلى محامي الأطراف أو المتهم. وبالتالي لا يمكن التمسك ببطلانه وبطلان الإجراءات التالية له لعدم تبليغه للمتهم أو محاميه (معمرى، 2015، صفحة 475/474).

د. أن يكون لأساليب التحري فائدة في إظهار الحقيقة:

لابد أن تكون هناك فائدة حقيقة ترجى من وراء هذه الأساليب وهي ظهور الحقيقة وهو شرط ضروري رغم عدم النص عليه صراحة وعلى هذا الشرط، وتقدير هذه الضرورة في مرحلة التحري متروك لسلطة وكيل الجمهورية تحت رقابة محكمة الموضوع وفقا لظروف كل جريمة وحسب درجة أهميتها وخطورتها وصعوبة اكتشافها وحاجة التحري إلى معلومات عنها.

ثانيا: الضوابط الشكلية: تتمثل فيما يلي:

أ. صدور إذن من وكيل الجمهورية المختص محليا:

يجب أن يصدر إذن مكتوب من وكيل الجمهورية ويتضمن الترخيص بالأساليب الخاصة لضابط الشرطة القضائية، كما يجب أن يكون وكيل الجمهورية مختص محليا طبقا للقواعد العامة للاختصاص (مادة 29 ج ج)، وكذا طبقا للقواعد الخاصة بتمديد اختصاصه خاصة قواعد تمديد اختصاصه إلى دائرة اختصاص محاكم أخرى عن طريق المرسوم التنفيذي 348/06 المؤرخ في 2006/10/08 (المادة 40 فقرة 2 من قانون الإجراءات الجزائية).

ب. أن يكون المندوب ضابط شرطة قضائية مختص

يجب أن يكون الشخص المندوب ضابط شرطة قضائية مختص محليا ونوعيا فلا يجوز ندب عون ضبطية قضائية لانتقاء صفة الضبطية القضائية عنه، أو ندب ضابط شرطة قضائية غير مختص محليا.

ج. تسبب الإذن

الأساليب الخاصة تمس بجرمة الحياة الخاصة، لذا يستوجب تسبب الإذن المرخص بها حتى تكون صحيحة، رغم عدم اشتراط المشرع لهذا السبب. فالإذن يجب أن يكون محددا للأسباب التي كانت وراء إصداره، أي تحديد عناصر الربط بين إذن الاعتراض والتسجيل والتصوير والجريمة.

د. تحديد العناصر التي تسمح بالتعرف على الاتصالات والأماكن المقصودة

استوجبت المادة 65 مكرر 7 الفقرة 1 من قانون إ. ج أن يتضمن الإذن المذكور في المادة 65 مكرر 5 من قانون إ ج، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها لتحديد أرقام هواتف الأشخاص الذين يعدون طرفا في المحادثات يستدعي أن يكون الأشخاص مشتبه فيهم أو متهمين أو لهم علاقة بالجريمة بصفة مباشرة أو غير مباشرة، والأماكن السكنية أو الأماكن العامة والجريمة التي تبرر اللجوء الى هذه التدابير

ومدتها وتعيين كل هذه العناصر الغرض منه ضمان عدم المساس بالحياة الخاصة ومنع تعسف المشرفين عليها ولم يضع المشرع الجزائري قيودا زمنية لتنفيذ أساليب التحري، فالدخول مسموح به خارج المواعيد المحددة في المادة 47 الفقرة الأولى من قانون إ. ج أي أن الدخول الى هذه الأماكن جائز ليلا ونهارا ولا يحتاج الأمر الى إصدار إذن مسبق بالدخول حسب القانون الجزائري كما لا يحتاج الدخول الى رضا وعلم الأشخاص الذين لهم حق الأماكن (مادة 65 مكرر 5 من قانون إ. ج) كون أساليب الاعتراض والتسجيل والالتقاط تتم في سرية وخلصة عن الشخص الذي يكون محلا لها وبالتالي لا يمكن التمسك ببطلان إذن دخول المساكن لكونه قد تم ليلا أو لعدم موافقة ورضا من له حق على الأماكن (معمري، 2015، صفحة 479).

هـ. تحديد مدة أساليب التحري

قد حدد المشرع مدة أربعة أشهر كحد أقصى للأساليب الخاصة في المادة 65 مكرر 7 الفقرة الثانية من قانون إ. ج قابلة للتجديد حسب مقتضيات التحري وضمن نفس الشروط الشكلية والزمنية، ولا يبدأ حسابها من تاريخ المذكور في إذن القاضي بل من تاريخ الوضع الفعلي للترتيبات التقنية وفي حالة انتهاء المدة المعينة في الإذن ولم تظهر الحقيقة يمنع القيام بأي أسلوب من الأساليب المأذون بها طالما انتهت مدتها، غير أنه يمكن تجديدها لمدة أقصاها أربعة أشهر بموجب إذن مكتوب من وكيل الجمهورية المختص.

المطلب الثاني: الاختصاص القضائي والتعاون الدولي

إن من أهم المشاكل التي تعترض أي تقدم في سير العملية الإثباتية وأجراءاتها هو مشكل الاختصاص القضائي في الجرائم العادية والذي يبدو أكثر تعقيدا حينما يتعلق الأمر بجرائم ذات بعد دولي ومنها الجريمة الالكترونية، فمسألة الاختصاص القضائي على كل المستويات المحلي والدولي هو تنازع أكثر من جهة قضائية سواء وطنية أو دولية النظر في الجريمة الالكترونية (دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري) (أطروحة دكتوراه)،

(2017/2018، صفحة 248).

الفرع الأول: الاختصاص القضائي في الجريمة الالكترونية

أولاً: الاختصاص القضائي الداخلي:

يعد الاختصاص القضائي أحد المبادئ الأساسية التي يقوم عليها النظام القضائي، إذ يحدد إجراءات التحقيق والتحري، حيث يقوم ذلك وفق معايير عددها المشرع الجزائي في المادة 37 الفقرة الأولى من قانون إ. ج كما يلي: "يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر".

وفي الفقرة الثانية من المادة السالفة الذكر: "يجوز تمديد الاختصاص المحلي لوكيل الجمهورية الى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة المعالجة الآلية بالمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

حيث يمدد الاختصاص في الجرائم الالكترونية ومن بينها جرائم المعالجة الآلية للمعطيات ليشمل كامل إقليم الدولة، وذلك بموجب نص المواد 37 و 47 و 80 و 329 من قانون إ. ج على أن هذا التمديد يشمل السلطات المختصة وكيل الجمهورية وفق المادة 37 من قانون إ. ج وضباط الشرطة القضائية المادة 40 مكرر 1 واختصاص قاضي التحقيق طبقاً للمادة 40 من قانون إ. ج واختصاص المحاكم وفق المادة 329 من نفس القانون حيث أجاز تمديد الاختصاص الى دائرة محاكم أخرى عن طريق التنظيم بموجب المرسوم التنفيذي رقم 06-384.

فيحدد الاختصاص القضائي حسب ضرورة التحقيق، فإن وجود دلائل قوية لارتكاب الجريمة الالكترونية يجيز لقاضي التحقيق تمديد الاختصاص حيث يدخل في نطاق محاكم أخرى مجاورة، أو أن يكون هناك ضرورة للانتقال خارج نطاق اختصاصه المكاني. كما أن تمديد الاختصاص لا يتم في كل الجرائم، حيث يمتد الاختصاص في الجرائم

الخطيرة كالإرهاب والجريمة المنظمة وجرائم الماسة المعالجة الآلية بالمعطيات، فهو يشمل اختصاص وكيل الجمهورية في التحقيق والمحاكمة، وهذا ما جاءت به المادة 5 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التي تمدد الاختصاص حيث يتعلق الأمر بمسرح الجريمة الافتراضي بمعنى أن المشرع قد حاول الجمع بين المسرحين العادي أو التقليدي والمسرح الافتراضي.

ثانيا: الاختصاص القضائي الدولي:

أن الاتجاه الغالب اليوم لحل مشكلة الاختصاص القضائي في العالم الافتراضي، هو تطبيق المبادئ ذاتها المعمول بها لحل مشكلة الاختصاص الجزائي الدولي في الجرائم التقليدية وعلى رأسها مبدأ إقليمية القوانين، أي تطبيق القانون.

أ. مبدأ الإقليمية في جرائم الأنترنت:

يقصد بمبدأ إقليمية القانون الجزائي، أن القانون الجزائي لدولة ما يطبق على كل جريمة ترتكب على إقليم هذه الدولة، سواء أكان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية، وسواء أكان المجنى عليه مواطناً أم أجنبياً (عرب، صفحة 277).

وفي هذا الصدد انقسم رأي الفقهاء إلى ثلاثة اتجاهات لتحديد مكان وقوع الجريمة:

1. مذهب السلوك أو النشاط الإجرامي بوصفه معياراً لتحديد مكان وقوع الجريمة:

وفقاً لهذا المعيار ينعقد الاختصاص للمحكمة التي يقع في دائرة اختصاصها النشاط الإجرامي لأن الأخذ بالمعيار حصول النشاط الإجرامي هو أيسر في عملية الإثبات وجمع الأدلة، حيث أن السلطات المختصة في نظرها هي أقرب من مسرح الجريمة.

2. مذهب النتيجة الجرمية كمعيار لتحديد مكان وقوع الجريمة:

هذا الاتجاه يأخذ بمبدأ وحدة الجريمة وعدم الفصل بين عناصرها، كذلك يمتاز في نظر المدافعين عنه بأنه أكثر واقعية على اعتبار أن الضرر له مظهر خارجي ملموس على خلاف السلوك الإجرامي الذي قد لا يكون كذلك والذي قد يتخذ فعل إيجابي كما قد يكون

عبارة عن امتناع أي فعل سلبي، وقد تم تبنيه في بعض التشريعات المقارنة منها القانون الألماني (عرب، صفحة 278).

3. المذهب المختلط

ظهر اتجاه ثالث مفاده أن الجريمة تعد واقعة في مكان حصول النشاط الإجرامي (العمل التنفيذي) وكذلك المكان الذي تحققت فيه النتيجة الجرمية، أو الذي من المتوقع أو من المنتظر تحققها فيه، وهذا الاتجاه حضي بموافقة أغلب الفقه ويعد مبرره في أن الركن المادي للجريمة يقوم على ثلاثة عناصر، وهي الفعل أي النشاط الإجرامي والنتيجة وعلاقة السببية.

ب. المبادئ الأخرى في مسألة الاختصاص في الجريمة المعلوماتية:

حين تتشكل الاعتداءات التي تهدد مصالح الدولة داخل وخارج حدود إقليمها لابد من أعمال مبادئ استثنائية حماية لمصالحها ومواطنيها وبالمقابل دون الاعتداء على سيادة الدولة الأخرى:

1. مبدأ العينية:

يقصد بمبدأ العينية تطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة، والمرتبكة خارج إقليمها أيا كانت جنسية مرتكبها، وهذا المبدأ يفرضه حرص الدولة على حماية مصالحها الأساسية (عرب، صفحة 279).

فمثلا أن يقوم شخص أجنبي من خارج الدولة باختراق أنظمة الحكومة، أو سرقة معلومات أمنية أو بيانات استخباراتية فإن الدولة يمكنها ملاحقته جنائيا رغم أن الفعل خارج أراضيها، وهذا تطبيقا لمبدأ العينية.

وبالرجوع إلى نص المادة 15 من القانون رقم 04-09 السالف الذكر والمادة 588 من قانون الإجراءات الجزائية نجد أنها نصت على مبدأ العينية لقيامه يجب أن تتوفر الشروط التالية:

❖ أن يتعلق الأمر بجرائم تكنولوجيا الاعلام والاتصال.

- ❖ أن ترتكب الجريمة خارج الإقليم الوطني.
- ❖ أن يكون مرتكب الجريمة أجنبيا.
- ❖ أن يستهدف مؤسسات الدولة الجزائرية الدفاع الوطني المصالح الاستراتيجية للاقتصاد الوطني.

2. مبدأ الشخصية:

يقصد بمبدأ الشخصية ملاحقة القانون الوطني للأشخاص الذين يحملون جنسية الدولة أينما وجدوا ليحكم أفعالهم الإجرامية المرتكبة بالخارج ويطبق مبدأ الشخصية بطريقتين: إيجابية وسلبية، ويقصد بالطريقة الإيجابية تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها وهذا تجنبا لفرار المجرم الذي يسيء الى سمعة دولته، أما الطريقة السلبية فيقصد بها تطبيق القانون الجزائي على كل جريمة يكون المجني عليه حاملا لجنسية الدولة ولو ارتكبت الجريمة خارج إقليمها وأيا كانت جنسية الجاني وهذا لضمان حماية رعايا الدولة من الاعتداءات الجرمية عليهم (عرب، صفحة 280، 297).

الفرع الثاني: التعاون الدولي في الجريمة الالكترونية

تعد المساعدة القضائية المتبادلة في المسائل الجنائية أو ما يعرف بالتعاون القضائي الدولي من أهم صور التعاون الدولي في مكافحة الجريمة وأكثرها فعالية قذفي مجال تعقب مرتكبي الجرائم وملاحقتهم والقبض عليهم ومحاكمتهم.

قد نص المشرع الجزائري في القانون 09/01 على مبدأ المساعدة القضائية الدولية المتبادلة في المادة 81 منه معتبرا انه في إطار التحريات والتحقيقات القضائية الجارية لمعاقبة الجرائم الالكترونية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني.

وترتبط الجزائر بالعديد من المعاهدات والاتفاقيات الثنائية في مجال التعاون القضائي التي تتضمن أحكام متعلقة بتسليم المجرمين نذكر منها:

- اتفاقية تنفيذ الأحكام وتسليم المجرمين بين الجزائر وفرنسا.
 - اتفاقية تسليم المجرمين بين الجزائر وجمهورية نيجيريا الاتحادية.
 - اتفاقية تسليم المجرمين بين الجزائر وإيران.
 - اتفاقية تسليم المجرمين بين الجزائر والمملكة المتحدة وايرلندا الشمالية.
 - اتفاقية تسليم المجرمين بين الجزائر والصين.
 - اتفاقية تسليم المجرمين بين الجزائر والبرتغال.
 - اتفاقية تسليم المجرمين بين الجزائر وكوريا.
 - اتفاقية تسليم المجرمين بين الجزائر واسبانيا.
- وهناك عدة أشكال للتعاون الدولي القضائي في مكافحة الجريمة تتمثل فيما يلي:
- أولاً: تبادل المعلومات:**

يقصد بتبادل المعلومات تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم كما أن هناك مظهر آخر لتبادل المعلومات يتعلق بالسوابق القضائية للجناة (صغير، 2001، صفحة 127)، من خلالها تتعرف الجهات القضائية بدقة على الماضي الجنائي للفرد المحال إليها وقد جاء هذا في العديد من الاتفاقيات الوطنية والدولية لعل من أهمها:

- ما جاء على المستوى الشرعي الوطني حيث نصت المادة 82 من قانون 01/09 على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل.
- وما ورد في الفقرة الثانية من المادة الأولى في معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية وكذا ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية إذ أوجبت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي.

- أيضا ما ورد في المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية (خراشي، 2006، صفحة 235/234).

- وفي هذا الإطار أيضا صاغ اتفاق "شنجن" للاتحاد الأوروبي نظام متكامل لتبادل المعلومات.

ثانيا: نقل الإجراءات:

ويقصد بهذه الصورة قيام دولة ما بمقتضى اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد التحقيق في جريمة الكترونية ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من الشروط أهمها:

- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والمطلوب منها أن تكون الإجراءات المطلوب اتخاذها مقررّة في قانون الدولة المطلوب منها عن ذات الجريمة.
- أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصول إلى الحقيقة كأن تكون أدلة الجريمة موجودة بالدولة المطلوبة منها.

ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية منها: معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية وكذا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية.

ثالثا: الإنابة القضائية

تعد الإنابة القضائية الدولية في المسائل الجنائية من أهم أشكال التعاون القضائي الدولي، حيث تهدف إلى تفعيل الحماية القانونية استجابة إلى متطلبات العدالة الجنائية، وذلك بالوصول إلى استكمال كافة إجراءات التحقيق المختلفة حتى لو كانت خارج نطاق سلطة القاضي الوطني الإقليمية. هذا الدور الوظيفي للإنابة يصطدم بصعوبات في التنفيذ (صغير، 2001، صفحة 83)، تتعلق بسيادة الدولة والتي حاولت الاتفاقيات الدولية التغلب عليها

من خلال التوسع في موضوع الإنابة، وأيضاً طرق التنفيذ وخلصت هذه الدراسة إلى نتيجة مهمة هي أن الإنابة القضائية الدولية أصبحت صورة للتخفيف من غلو مبدأ الإقليمية للقوانين الجنائية حيث ساهمت في تطوير آليات المساعدة القضائية بين الدول في المسائل الجنائية فأصبح بإمكان القاضي الوطني التعويل على نتائج الإنابة القضائية الدولية التي تمت بواسطة سلطة قضائية أجنبية. وتستلزم الإنابة القضائية الدولية إرسال الملف الخاص بالدعوة الجنائية بمرافقاته من مستندات ووثائق ومحاضر التحقيق التي أجريت بمعرفة السلطة القضائية في الدولة المطلوب فيها اتخاذ بعض إجراءات التحقيق وهي في ذلك تتشابه إلى حد كبير مع النذب (الإنابة القضائية الداخلية).

خلاصة الفصل الثاني:

وفي الأخير، ومن خلال دراسة هذا الفصل المتعلق بالإطار القانوني للتحري، نخلص الى أن إجراءات التحري عن الجريمة الالكترونية هي إجراءات من نوع خاص يشترط لمباشرتها التقيد بمجموعة من الشروط أهمها شرط التقيد بالنص الإجرائي الملأئم حفاظا على سلامة الإجراءات من طائلة البطلان وكذلك حفاظا على حريات الأفراد وكرامتهم.

وفي سبيل مكافحة الجريمة الالكترونية يشترك تكاثف الجهود التشريعية في كافة الدول لوضع حلول نهائية لإشكالية مبدأ إقليمية النص الجنائي والمبادئ الإجرائية المتعلقة بالاختصاص الذي يحكم عمل الجهات المخول لها مباشرة إجراءات التحري.

الخاتمة:

في آخر المطاف، تعد هذه الدراسة حصيلة جهد قمنا بها لتصدي لموضوع إثبات الجريمة الإلكترونية، غير أنه لا يجب أن يكون الطابع التقني لمثل هذا النوع من الجرائم عقبة تمنعنا من محاولة التوسع في قاعدة النقاش حول الإجماع الإلكتروني.

ومنه إذا كانت الجريمة الإلكترونية أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي بحثاً عن إمكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الجرائم مع احترام مبدأ الشرعية، والتفسير الضيق للنصوص الجنائية، فقد أثارت في نفس الوقت العديد من المشكلات في نطاق القانون الجنائي الإجرائي، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو للتحقيق فيها وجمع الأدلة المتعلقة بها، غير أن المشكلات الإجرائية في مجال الجرائم الإلكترونية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونية وكيانات غير ملموسة، وبالتالي يصعب من ناحية كشف هذه الجرائم ومن ناحية أخرى يصعب جمع الأدلة بشأنها.

نتائج الدراسة:

- عدم وجود تعريف أو مفهوم موحد وشامل للجريمة الإلكترونية وكذا صعوبة حصرها لتعدد وسائل ارتكابها وكذا المجالات الواقعة عليها.
- تعرف الجريمة الإلكترونية على أنها: "الجريمة التي يتم ارتكابها إذا قام شخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة، ومصلحة الأفراد الخاصة"
- تعد الجرائم الإلكترونية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة، وذلك بسبب الاستعمال السيئ للثورة التكنولوجية.
- نقص الخبرة لدى رجال الضبط القضائي وأجهزة العدالة أو الأجهزة الأمنية بصفة عامة فيما يتعلق بثقافة الحاسب الآلي وأنظمة الاتصال وهذا راجع إلى غياب أو نقص وسائل التكنولوجيا والبنية التحتية الحديثة التي تساعد في الكشف عن الجرائم الإلكترونية وملاحقة مرتكبيها.

- إن المشرع الجزائري لم يتطرق الى بعض الجرائم الالكترونية وعلى رأسها الجرائم التقنية، ولذلك لا يمكن القياس عليها حسب نص المادة الأولى من قانون العقوبات.
- وبناء على النتائج المتوصل اليها، يمكننا الإجابة على الاشكالية التي سبق طرحها بأن المشرع الجزائري قد وفق نسبيا في مجال التحري عن الجريمة الالكترونية، مع وجود بعض النقاط التي يتعين عليه تداركها.

التوصيات:

- وعلى هذا الأساس حاولنا وضع جملة من الاقتراحات التي من شأنها المساهمة في تدعيم الآليات القانونية المتعلقة بالتحري عن الجرائم الالكترونية وهي كالتالي:
- ضرورة تكثيف الجهود الدولية في مجال التعاون لمواجهة خطر انتشار الجريمة الإلكترونية دوليا.
- تسخير كفاءات من ذوو الخبرة للتحقيق في مجال الجريمة الإلكترونية.
- ضرورة إنشاء أقسام أو إدارات أو جهات للضبط الجنائي والتحقيق متخصصة في مجال الجريمة الإلكترونية
- العمل على إثراء القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم الالكترونية ببعض المواد القانونية لتجنب الوقوع في أي ثغرة قانونية من شأنها فتح المجال للمجرمين للإفلات من العقاب.
- وضع آليات ردعية تتماشى مع التطورات الحاصلة من خلال فتح المجال لأصحاب الخبرات من خارج القطاع الأمني للمشاركة في مكافحة الجريمة الالكترونية.
- تخصيص قاضي مختص بالنظر في الجرائم الإلكترونية.

قائمة المصادر والمراجع

(1) المصادر

أ. المراسيم والقوانين:

1. القانون رقم 04-15 الصادر في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 الصادر في 08 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71
2. القانون رقم 09-04، الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47
3. الأمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 الذي يتضمن قانون العقوبات المعدل والمتمم
4. الأمر رقم 155-66 المؤرخ في 8 جوان 1996 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم 02-11 المؤرخ في 23 فيفري، 2011، العدد 12 المؤرخ في 23 فيفري 2021.
5. التعديل الدستوري الجزائري لسنة 2020 الصادر بالمرسوم الرئاسي رقم 251-20 المؤرخ في 27 محرم عام 1442 الموافق ل 15 سبتمبر، 2020 ج.ر، العدد 54 الصادر بتاريخ 16 سبتمبر 2020.

(2) المراجع

أ. الكتب

1. جلال محمد الزعبي، أسامة أحمد مناغسة: جرائم تقنية نظم المعلومات الالكترونية دراسة مقارنة، دار الثقافة، عمان، الأردن، 2010.
2. جميل عبد الباقي صغير، الجوانب الاجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية سنة 2002.
3. خالد داودي، الجريمة الالكترونية، دار الإعصار للنشر والتوزيع، عمان، 2017
4. خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، طبعة الأولى، الإسكندرية 2009،

- 5.رامي متولي، مكافحة الجرائم المعلوماتية، دار النهضة العربية، طبعة الأولى، القاهرة، 2011
- 6.عادل عبد العال إبراهيم خراشي، ضوابط التحري والاستدلال عن الجرائم، دار الجامعة الجديدة للنشر، الإسكندرية 2006
7. ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، تيزي وزوو، عدد 16، جوان 2017،
- 8.مختار به بوزيدي، ماهية الجريمة الإلكترونية الملتقى الوطني آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، الجزائر العاصمة، 29 مارس 2017
- 9.محمد حماد مرهج الهيبي، الجريمة المعلوماتية (نماذج من تطبيقاتها)، دار الكتب القانونية، الامارات 2014،
10. محمد مدين، الجريمة الإلكترونية وتحديات الامن القومي، المصرية للنشر والتوزيع، الطبعة الثانية، مصر القاهرة ، 2019
11. محمود مدين، فن التحقيق والإثبات في الجريمة الإلكترونية، دون دار النشر، طبعة الأولى، 2020
12. ميرفت محمد صبيح، مكافحة الجريمة الإلكترونية، دار اليازوري للنشر والتوزيع، دون طبعة، عمان 2022
13. نجاة بن مكي، السياسة الجنائية لمكافحة الجرائم المعلوماتية، دار الخلا ونية، الجزائر، 2017،
14. هبة نبيلة هروال: الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، دون طبعة، الإسكندرية، 2013،

ب. الأطروحات والرسائل العلمية

1. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الاجرام والعقاب، جامعة باتنة، 2011\2012
2. سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2013
3. طرشي نورة: مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة ال جزائر 2011/2012
4. مولاي ملياني دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أوبكر بالقايد، تلمسان، الجزائر، 2017/2018

ج. المجلات العلمية

1. الهام بن خليفة، التفتيش كأجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، الوادي المجلة الدولية للبحوث القانونية والسياسية، سنة النشر، 30/05/2018 المجلد 1، العدد 2 .
2. زوليخة زوزو، مشروعية أساليب التحري الحديثة مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، العدد 8، الجزء 2 جوان 2017 .
3. عبد الرشيد معمري، ضوابط مشروعية أساليب التحري الخاصة، المجلة الأكاديمية للبحث القانوني، جامعة خنشلة، العدد 1، 2015.
4. عزالدين عثمان، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، تبسة، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، 2018.

5. فوزي بن عمارة، اعتراض المرسلات وتسجيل الاصوات والتقاط الصور والتسرب كإجراءات تحقيقي قضائي في المواد الجزائية، قسنطينة، مجلة العلوم الانسانية، سنة 2010، العدد 33، جوان 2010،
6. مريم عراب، الاختصاص القضائي في الجرائم المعلوماتية، مجلة حوليات، كلية الحقوق والعلوم السياسية، جامعة وهران 2، العدد 03.

فهرس الموضوعات

الصفحة	العنوان
	الشكر والعرفان
	الإهداء
5 - 1	مقدمة
41 - 6	الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية ومسألة التحري فيها
7	المبحث الأول: ماهية للجريمة الإلكترونية
7	المطلب الأول: مفهوم الجريمة الإلكترونية
8	الفرع الأول: تعريف الجريمة الإلكترونية
12	الفرع الثاني: خصائص الجريمة الإلكترونية
15	الفرع الثالث: أطراف الجريمة الإلكترونية
17	المطلب الثاني: الأحكام الخاصة بالجرائم الإلكترونية
17	الفرع الأول: أركان الجرائم الإلكترونية
21	الفرع الثاني: أنواع الجريمة الإلكترونية
24	الفرع الثالث: دوافع ارتكاب الجريمة الإلكترونية
27	المبحث الثاني: ماهية التحري عن الجرائم الإلكترونية
28	المطلب الأول: مفهوم التحري
28	الفرع الأول: المقصود بالتحري
30	الفرع الثاني: طبيعة مرحلة التحري
31	الفرع الثالث: أهمية التحري عن الجرائم الإلكترونية
32	المطلب الثاني: ضوابط التحري عن الجريمة الإلكترونية
36 - 32	الفرع الأول: الأجهزة المكلفة بالتحري عن الجريمة الإلكترونية
39 - 36	الفرع الثاني: الوسائل المستخدمة في التحري وجمع الأدلة
40 - 39	الفرع الثالث: قواعد الاختصاص

41	خلاصة الفصل الأول
78 - 42	الفصل الثاني: الإطار القانوني لتحري عن الجرائم الالكترونية
44	المبحث الأول: الاليات الكلاسيكية والمستحدثة للتحري عن الجرائم الالكترونية
44	المطلب الأول: اليات التحري عن الجرائم الالكترونية في القانون رقم 09-04
51 - 44	الفرع الأول: التفتيش والحجز في الجريمة الالكترونية
57 - 51	الفرع الثاني: المعاينة والمراقبة الالكترونية
57	المطلب الثاني: اليات التحري المستحدثة عن الجرائم الالكترونية
61 - 58	الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والنقاط الصور
64 - 62	الفرع الثاني: التسرب والاختراق
65	المبحث الثاني: مشروعية اليات التحري عن الجرائم الالكترونية
65	المطلب الأول: موقف المشرع الجزائري من اليات التحري
67 - 66	الفرع الأول: نطاق تطبيق اليات التحري في الجرائم الإلكترونية
71 - 67	الفرع الثاني: ضوابط مشروعية اليات التحري
71	المطلب الثاني: الاختصاص القضائي في الجريمة الالكترونية
75 - 72	الفرع الأول: الاختصاص القضائي في الجريمة الالكترونية
78 - 75	الفرع الثاني: التعاون الدولي في الجريمة الالكترونية
79	خلاصة الفصل الثاني
82 - 80	خاتمة
87 - 83	قائمة المصادر والمراجع
90 - 88	فهرس الموضوعات
92	الملخص

وكان فضل الله عليك عظيمًا

وكان فضل الله عليك عظيمًا

عظم المراد فهان الطريق فجاءت

لذة الوصول لتتهون مشقة الطريق

الحمد لله ما تنأهى رب ولا ختم جهد ولا تم سعي إلا بفضل

تم بحمد الله

تخرجي



الملخص:

قام المشرع الجزائري بمكافحة الجريمة الإلكترونية على غرار باقي الدول من خلال تعديل قانون العقوبات وقانون الإجراءات الجزائية حيث تم تدارك النقص في المجال الإجرائي لإثبات هذا النوع من الجرائم بإصدار قانون 09/04، إذ تضمن قواعد إجرائية وأخرى وقائية. لذا كان الهدف من هذا البحث هو تحديد الجوانب الإجرائية، لاسيما ما يتعلق بإثباتها باعتبار أن أدلتها تختلف عن أدلة الجرائم التقليدية، إذ تتمثل في كميات ضخمة من البيانات المخزنة على أجهزة الحاسوب، ومن خلال دراستنا قمنا بتحديد الإجراءات التي يعتمد عليها المختصون في البحث والتحري لاستخلاص هذه الأدلة والكشف عن الجريمة وضبط مرتكبيها وذلك من خلال تناول الإجراءات التقليدية إلى جانب الأساليب المستحدثة والهيئات المختصة بها، بالإضافة إلى موقف المشرع الجزائري من هذه الإجراءات.

Summary:

The Algerian legislator, like many others around the world, has taken steps to combat cybercrime by amending both the Penal Code and the Code of Criminal Procedure. The procedural gap related to the proof of such crimes was addressed through the enactment of Law No. 04/09, which introduced both procedural and preventive rules.

The aim of this research is to identify the procedural aspects, particularly those related to evidence, given that the evidence of cybercrimes differs from that of traditional crimes. It often consists of massive amounts of data stored on computer systems. Through this study, we have identified the procedures used by specialists in investigation and inquiry to extract this evidence, uncover the crime, and apprehend the perpetrators – whether through traditional methods or newly developed techniques – while also addressing the competent authorities and the position of the Algerian legislator regarding these procedures.