وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون إعلام الآلي وإنترنت

الموسومة بـ:

إجراءات البحث والتحري في الجرائم الإلكترونية

إعداد الطالبين:

- هشام عابد
- بيضياف سفيان

تحت إشراف الدكتورة:

غرس الله كريمة

لجنة المناقشة:

الاسم واللقب	الرتبة	الصفة
دكدوك هودة	أستاذ محاضر " أ"	رئيسا
غرس الله كريمة	أستاذ محاضر " ب"	مشرفا ومقررا
كوسة حليمة	أستاذ محاضر " ب"	ممتحنا

السنة الجامعية 2024/ 2025

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): عابد هشام ..... الصفة: طالب، أستاذ، باحث ..... طالب .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 116523833 والصادرة بتاريخ 2018/11/18 .....

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: إجراءات البحث والتحري في الجريمة الالكترونية .....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: ..... 26 ماي 2025

توقيع المعني (ة)

ملحق بالقرار رقم .....1082..... المؤرخ في ..... 2020 ماي 27 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله.

السيد(ة): بدرناف سفيان ..... الصفة: طالب. أستاذ. باحث ..... طالب .....

الحامل(ة) لبطاقة التعريف الوطنية رقم 105655476 والصادرة بتاريخ 2017/07/28 .....

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج. مذكرة ماستر. مذكرة ماجستير. أطروحة دكتوراه).

عنوانها: إجراءات البحث والتحري في الجريمة الالكترونية .....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: .....

2025 ماي 28

توقيع المعني (ة)

الإدارة الترقيمية

فعل المحمود نبيل

قائمة المختصرات:

ج، ر، ج، ج: الجريدة الرسمية للجمهورية الجزائرية

ص: الصفحة

ص، ص: من الصفحة إلى الصفحة

د، س، ن: دون سنة نشر

ط: طبعة

شكر وتقدير

قال الله تعالى* يرفع الله الذين امنوا منكم والذين اتو العلم درجات *

الحمد لله الذي انشا وبرى وخلق الماء وثرى، الرحمن على العرش استوى

والصلاة والسلام على من بكى على امته المبعوث في ام القرى سيدنا محمد

صلى الله عليه وسلم

نحمد الله سبحانه عزوجل حمدا كثيرا ونشكره على منحنا الصحة والعافية والذي

بقدرته وفقنا الى إتمام هذا العمل

كما نتوجه بالشكر الخالص والتقدير الى كل من اعاننا في انجاز هذه المذكرة،

كما نخص بالشكر والعرفان

الاستاذة المشرفة **الدكتورة: غرس الله كريمة** بأسمى عبارات الائتمان والشكر

والتقدير لقبولها بالأشراف علينا في انجاز هذا العمل، واثرائها لنا بالتوجيهات

القيمة والمتواصلة

والى أعضاء لجنة المناقشة على قبولهم اجراء المناقشة ومجهودهم في قراءة

المذكرة

واثراء المناقشة بملاحظاتهم القيمة.

والى كامل الطاقم الجامعي من عمال وأساتذة وعلى رأسهم عميد كلية الحقوق

والعلوم السياسية برج بوعريريج

مقدمة

مع انتقال البشرية إلى الألفية الثالثة، انطلقت في رحلة جديدة من التطور الفكري والمعرفي غير المسبوق، مدفوعة بالثورة العلمية والتكنولوجية التي اجتاحت مجالات الاتصالات والمعلومات. هذه النهضة العلمية الشاملة فتحت آفاقًا غير عادية في مختلف جوانب الحياة، حيث أزالت الحدود الجغرافية بين الدول والشعوب، وقللت المسافات وطوت الأبعاد بفضل سرعة نقل المعلومات ودقتها، وإمكانيات تجميع البيانات وتخزينها ومعالجتها ثم تبادلها بين مختلف الأطراف سواء داخل الدولة أو بينها وبين دول أخرى، أصبحت الكرة الأرضية تبدو كقرية صغيرة متصلة.

على الرغم من الفوائد المتعددة والمزايا الكبيرة التي أصبحت واقعًا ملموسًا في مختلف جوانب الحياة اليومية بفضل تقنيات وأدوات تكنولوجيا المعلومات والاتصال، فإن الاستخدام المتزايد لهذه التقنيات قد أدى في المقابل إلى ظهور بعض الآثار السلبية التي تشكل تهديدًا جديًا للأمن والاستقرار المجتمعي، ويعود ذلك إلى سوء استغلال هذه التكنولوجيا واستخدامها بطرق غير قانونية تتسبب في الإضرار بمصالح الأفراد والمجتمعات، وقد أسفر هذا الوضع عن نشوء شكل جديد من الجرائم، لم يكن مألوفًا في السابق، أصبح يُعرف اليوم بـ"جرائم تقنية المعلومات" أو "الجرائم الإلكترونية".

تُعتبر الجرائم الإلكترونية من أكثر الجرائم تعقيدًا وخطورة في العصر الحديث، حيث تمثل أحد أشكال الجريمة المنظمة المستحدثة. وتتسم هذه الجرائم بخصوصية طبيعتها المعقدة، سواء من حيث تكوينها وأركانها أو الأساليب الحديثة المستخدمة في ارتكابها، وكذلك البيئة التي تنشط فيها وخصائص مرتكبيها، هذه المميزات الفريدة جعلت التعامل مع النشاطات الإجرامية الإلكترونية باستخدام النصوص القانونية التقليدية أمرًا صعبًا، مما دفع المشرِّع الجزائي إلى تحمل مسؤولية إصدار تشريعات خاصة للتصدي لهذا النوع من الجرائم ومواجهتها بشكل فعّال، ولا يقتصر الأمر على تعديل القواعد الموضوعية فقط، بل يمتد ليشمل تحديث القانون الجنائي الإجرائي، الذي كان يعتمد سابقًا

على نصوص تعالج الجرائم التقليدية، لم تواكب خصوصية الجرائم الإلكترونية وما تثيره من تحديات إجرائية أمام الجهات المعنية بالتحري والتحقيق، مما تطلب وضع إجراءات بحث وتحري تتماشى مع خصوصيتها، بما يُمكن الجهات المختصة كرجال الشرطة القضائية والمحققين من الكشف عن هذه الجرائم وتحديد مرتكبيها وجمع الأدلة بسرعة ودقة. ومن أجل تحقيق ذلك وجب العمل على تحديث الإجراءات الجنائية التقليدية وابتكار إجراءات جزائية جديدة تواكب طبيعة الجرائم الإلكترونية. هذه الإجراءات لابد أن تكون مدعومة بتقنيات حديثة تضمن تحقيق توازن بين الاستفادة الضرورية من التكنولوجيا المتقدمة وبين توفير الحماية الجزائية للأفراد والمجتمع من تأثيراتها السلبيۃ.

من هنا تتجلى أهمية دراسة موضوع البحث والتحري في الجرائم الإلكترونية، والتي تعود أساسًا إلى حداثة هذا المجال وما يتميز به من طابع علمي بحت وجديد على تصور رجال القانون. فهذا الموضوع لم يحظَ بعد بالاهتمام الكافي من البحث والدراسة على مستوى الفقه الجنائي، حيث إن أغلب الدراسات القانونية المتعلقة بالجرائم الإلكترونية ركزت على الجانب الموضوعي فقط، مما أدى إلى ندرة وقلة المراجع التي تناولت الجانب الإجرائي. هذا النقص دفعنا إلى التركيز عليه لتعزيز النقاش القانوني وإثرائه في هذا المجال. وعليه، يمكن صياغة إشكالية الدراسة بالشكل التالي:

ما هي الآليات والإجراءات التي اعتمدها المشرع الجزائري لمواجهة الجريمة الإلكترونية؟

ويتفرع من هذا السؤال الرئيسي عدة تساؤلات فرعية، منها:

- ما المقصود بالجريمة الإلكترونية؟
- كيف يمكن تعريف البحث والتحري في الجرائم الإلكترونية؟
- ما هي الإجراءات الخاصة بالبحث والتحري في مجال الجرائم الإلكترونية؟

اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي الذي يهدف إلى وصف الظاهرة محل البحث وتحليل المواد المتعلقة بها. وجاء ذلك انطلاقًا من اهتمام الدراسة بأساليب البحث والتحري في الجرائم الإلكترونية وطرق كشفها من الناحيتين الفنية والقانونية.

ولمعالجة الإشكالية المطروحة، قمنا بتقسيم الخطة إلى فصلين على أساس تقسيم ثنائي. في الفصل الأول، استعرضنا الإطار المفاهيمي للجريمة الإلكترونية وإجراءات مكافحتها، حيث تضمن مبحثين: الأول تناول ماهية الجريمة الإلكترونية، بينما خصص المبحث الثاني للبحث والتحري عن هذه الجريمة. أما الفصل الثاني فتناول خصوصية البحث والتحري عن الجرائم الإلكترونية، وقسمناه إلى مبحثين أيضًا: المبحث الأول ركز على أساليب البحث والتحري المتعلقة بالجرائم الإلكترونية، بينما تناول المبحث الثاني مشروعية هذه الأساليب وأبعادها القانونية.

الفصل الأول

الإطار المفاهيمي للجريمة الالكترونية وإجراءات التصدي لها

تمهيد:

موضوع الجريمة الإلكترونية يمثل واحدة من أبرز القضايا التي تشغل المجتمع العالمي، وهو ما يؤرق الدول كافة بما فيها الجزائر. فقد أصبحت هذه الجريمة تتعدى على حقوق الأفراد بأساليب متنوعة، مما دفع المشرع الجزائري إلى ضرورة تحديث النصوص القانونية المتعلقة بالجوانب الموضوعية والإجرائية، بهدف مواجهة العواقب السلبية الخطيرة التي تنجم عنها. في هذا السياق، يتناول الفصل الحالي النقاط التالية: أولاً: التطرق إلى مفهوم الجريمة الإلكترونية من خلال مطلبين: – المطلب الأول: تعريف الجريمة الإلكترونية وخصائصها. – المطلب الثاني: الأحكام الموضوعية المتعلقة بالجريمة الإلكترونية. ثانياً: البحث والتحري عن الجرائم الإلكترونية، وذلك عبر مطلبين أيضاً: – المطلب الأول: تعريف عملية البحث والتحري عن الجرائم الإلكترونية. – المطلب الثاني: تحديد الضوابط والإجراءات المؤطرة لهذه العملية.

المبحث الأول: ماهية الجريمة الالكترونية.

تُعتبر الجريمة الإلكترونية من الظواهر المستحدثة التي ارتبطت ارتباطًا وثيقًا بتكنولوجيا المعلومات والاتصالات الحديثة، وقد أحاط مفهوم الجريمة الإلكترونية بشيء من الغموض، حيث تعددت المحاولات الأكاديمية والقانونية لوضع تعريف دقيق وشامل لها. على الرغم من ذلك لم يتم التوصل إلى توافق فقهي بشأن صياغة تعريف محدد، بل إن بعض الباحثين رجّحوا عدم السعي إلى تعريف جامع، نظرًا لأن هذا النوع من الإجرام يُنظر إليه باعتباره امتدادًا للجريمة التقليدية، لكن باستخدام وسائل إلكترونية.

كما أن حداثة الجرائم الالكترونية واختلاف الثقافات والنظم القانونية بين الدول صعب من إيجاد مصطلح موحد للدلالة عليها، وهو ما أدى إلى عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، حيث يتم استعمال العديد من المصطلحات والعبارات للتعبير أحيانا على نفس الجريمة كالجريمة المعلوماتية والجريمة المتصلة بوسائل الإعلام والاتصال.[1]

سوف نحاول من خلال هذا المبحث التطرق لتعريف الجريمة الالكترونية لننتقل فيم بعد إلى الأحكام الخاصة بالجريمة الالكترونية.

المطلب الأول: مفهوم الجريمة الالكترونية:

تعد الجرائم الإلكترونية تحديًا كبيرًا في عصرنا الحالي نظرًا لارتباط حياتنا اليومية بالتكنولوجيا والاعتماد المتزايد على الشبكات الرقمية.

[1]-عبد الصديق الشيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 04، العدد 1، السنة 2020، ص 192

الفرع الأول: تعريف الجريمة الالكترونية:

تباين النظم القانونية والثقافية بين الدول أدى إلى تعريف الجريمة الإلكترونية أحيانًا ضمن إطار ضيق وأحيانًا أخرى ضمن نطاق أوسع.

لذا سوف نتطرق إلى التعريف الفقهي الضيق لهذه الجريمة ثم التعريف الموسع والتعريف التشريعي.

أولا: التعريف الضيق للجريمة الالكترونية:

تعددت التعاريف بشأن الجريمة الالكترونية، فلا يوجد مصطلح محدد للدلالة على هذه الظاهرة، يطلق عليها البعض الجريمة المعلوماتية وآخرون جرائم الحاسب الآلي، ويطلق عليها البعض الآخر الجريمة الإلكترونية، أو الجريمة الرقمية على أساس لغة الحاسب الآلي.[1]

إن الوسيلة المستخدمة في الجريمة وإنما ركزوا على موضوع الجريمة، فهذه الجريمة ليست الجريمة التي يستخدم الحاسب الآلي كأداة في ارتكابها، بل تقع على الحاسب الآلي أو في داخل نظامه.[2]

لا يوجد مصطلح قانوني موحد للدلالة على ظاهرة الإجرامية الناشئة في البيئة الكمبيوتر وفيما يعد بيئة الشبكات، بل تباينت هذه المصطلحات حيث رافق هذا التباين مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات.[3]

---

[1]-حمزة خضري، حمزة عشاش: "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط الجزائر، جوان 2020، ص 168-176

[2]-بثينة حبيباتي، الطبيعة الخاصة للجريمة المعلوماتية، دراسات مجلة وأبحاث، مجلد جامعة زيان عاشور، الجلفة، الجزائر، مجلد 12، عدد 03 جويلية 2020، ص 608.

[3]- عائشة بن قارة مصطفى، حجية الدليل الإليكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير كلية الحقوق، جامعة الإسكندرية، سنة 2009، ص 26.

فظهرت عدة محاولات لتعريفها تعريفا ضيقا من بينها:

ما ذهب إليه الفقيه (MERWE) حيث يرى أن الجريمة المعلوماتية (جريمة الحاسب) هي: "الفعل الغير المشروع الذي يتورط في ارتكابه الحاسب الآلي وهي الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية[1]."

في أخرى ذهب (Tièdement) إلى أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعطيات[2].

فيما ذهب الفقيه (Rosblat) إلى تعريفها "بأنها كل نشاط غير مشروع موجه لنسخ أو تغيرات أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تحول طريقه."

أو أنها كما جاء في التعريف (Dauid Tompson) هي "الجرائم يكون متطلبا لاقترافها أن يتوافر لدى معرفة بتقنية الحاسب".[3]

وعرف (Leslie dball) الجريمة المرتبطة بالحاسب بأنها "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية".

[1]- MARWE VANDER، computer crimes and other grimes against information Technology in south Africa، "R.ID.P", 1993;p554.

[2]- Klaus Tiede man, Fraude et autres délits d'affaires commis a l'aide d'ordinateurs électroniques, Rev, drpén, crim, 1984, p 612.

[3]- هشام رستم، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة بحث مقدم إلى لجنة العلمية بمصر لمنع الجريمة المعلوماتية ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيط، العدد 17، سنة 1995 ص 107 و 108.

والواقع أن هذه التعريفات لم تتمكن من الإحاطة بجميع جوانب ظاهرة الإجرام المعلوماتي، ولهذا وُجِّهت إليها انتقادات لأنها ركزت على وسيلة ارتكاب الجريمة. لذلك، فهي لا تعتبر شاملة أو حصرية.

ومن أفضل التعريفات التي تدور حول الوسيلة هو تعريفها بأنها: تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب، أي أنها الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا.

إن تعريف الجريمة على معيار شخصي وهو مدى معرفة الجاني بتقنية المعلومات والإلمام بها، وحيث أن قصور هذه التعاريف واضحة لأن شخصية الجاني لا تكفي لوحدها لتعريف الجريمة الإلكترونية حيث يمكن لأي شخص عادي غير مؤهل بتقنيات الحاسب الآلي ارتكاب جريمة الغش المعلوماتي أو السرقة المعلوماتية[1].

ثانيا: التعريف الموسع للجريمة الالكترونية:

وهو ما ذهب إليه الفقيهان (MICHEL & REDO) تشمل: استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج الغير المصرح به لحاسب المجني عليه أو بياناته كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع البطاقات الائتمان، وانتهاك ماكينات الحساب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إليكترونية، وتزيف المكونات المادية والمعنوية للحاسب.

[1]- رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، كتاب أعمال المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، مركز جيل البحث العلمي طرابلس، لبنان، 24 مارس 2017، ص 95-99.

وتناول رأي من الفقه تعريف الجريمة المعلوماتية بأنها: عمل أو امتناع يأتيه الإنسان أضرارا بمكونات الحاسب وشبكات الإتصال الخاصة به التي يحمها قانون العقوبات ويفرض له عقابا.

ويمتاز هذا التعريف بأنه يحتوي على كل صور الإعتداء الإيجابية والسلبية التي تقع أضرار بمكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به.

أنه يتضمن الأثر الجنائي المترتب على العمل أو الامتناع غير المشروعين ويتمثل في الجزاء الجنائي بكافة صوره وأنواعه.[1]

بعد عرضنا لتعريف الجريمة المعلوماتية نضيف: أن شبكة الإنترنيت بوصفها نتاج تطور النظم المعلوماتية كأداة للربط والإتصال بين مختلف شعوب العالم، تشكل أداة لارتكاب الجريمة المعلوماتية أو مجالا لها وذلك بإساءة استخدامها أو استغلالها على النحو غير المشروع، ولذلك ينبغي على الجهات التشريعية مواجهتها بتشريعات حاسمة لمكافحتها وتقديم مرتكبيها للعدالة.[2]

ثالثا: التعريف التشريعي للجريمة الإلكترونية:

من المعلوم أن المشرع الجزائري وإلى وقت قريب أغفل تنظيم مجال الجريمة الالكترونية قانونا إلا أنه ما فتئ أن تدارك ذلك الفراغ القانوني من خلال سن قواعد قانونية لمواجهة هذه الجريمة، وذلك ما تجلى في القانون رقم 04-15 المتضمن تعديل قانون العقوبات الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية

[1]- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعية الجديدة للنشر، الإسكندرية، سنة 2009، من 157 و158.

[2]-جميل عبد الباقي الصغير، الأنترنيت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنيت، دار النهضة العربية، القاهرة، 2001، ص 04.

للمعطيات ثم تلاه بالقانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

ومما يجب الإشارة إليه، أن مصطلح نظام المعالجة الآلية للمعطيات تعبير ذا طابع فني تقني يصعب على القانوني إدراك مغزاه ببساطة، فضلا على أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلي[1].

ولذلك فالمشرع الجزائري على غرار الكثير من التشريعات لم يعرض نظام المعالجة الآلية للمعطيات وأوكل بذلك المهمة لكل من الفقه والقضاء.

ولمزيد من التفصيل نتطرق إلى تعريف ذلك من خلال القانونين 04-15 و 09-04 على التوالي:

أ-**تعريف الجريمة الالكترونية حسب القانون 04-15:** بالرجوع إلى قواعد القانون 04-15 من المادة 394 مكرر 1 ثم المادة 394 مكرر 2 نجد أنه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات حيث حددها في المادة 394 مكرر بالآتي:

- الدخول وابقاء بالغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك . - حذف أو تغيير المعطيات المنظومة إذا ترتب عن الدخول أو ابقاء غير المشروع بعرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكرر 1 فقد أشارت إلى ما يلي:

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

[1]-محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، 2018، ص 438.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[1].

ب–تعريف الجريمة الالكترونية حسب القانون 09–04: حددت المادة (02) منه الجريمة الإلكترونية بقولها: "يقصد في مفهوم هذا القانون بما يأتي:

– **الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:** 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.

– **منظومة معلوماتية** : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

– **معطيات معلوماتية** : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها[2].

الفرع الثاني: خصائص الجريمة الالكترونية:

تتسم الجرائم الإلكترونية بمجموعة من الخصائص التي لا تتواجد في الجرائم التقليدية، وعلى النحو ذاته، يتميز مرتكبو هذه الجرائم بصفات خاصة تفرقهم عن المجرمين العاديين. ويمكن توضيح ذلك من خلال النقاط التالية:

أولا: الجريمة الالكترونية عابرة للحدود (الزمان والمكان):

[1]- القانون رقم 04-15 المؤرخ في 10 نوفمبر يعدل ويتمم الأمر 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج . ر ، ج. ج.د.ش، العدد 71 الصادر في 10 نوفمبر 2004.

[2]-القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج، ر، العدد 47، الصادرة في 16 أوت 2009.

المقصود بذلك أن هذا النوع من الجرائم لا يعتد بالحدود الجغرافية للدول ولا بين القارات فمع انتشار شبكة الاتصالات بين دول العالم وأقاليمه أمكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر، حيث أن الجريمة الالكترونية تتسم غالبا بالطابع الدولي ذلك لأن الطابع العالمي لشبكة الأنترنت وما رتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط On line ، يسهل ارتكاب الجريمة من دولة الى دولة أخرى فالجريمة الالكترونية لا تعترف بالحدود بين الدول والقارات ولذلك فإن جريمة عابرة للقارات فهي تعبر شكلا جديدا من اشكال الجرائم العابرة للحدود الإقليمية.[1]

وتتميز الجريمة الالكترونية عن الجريمة التقليدية في كون أن الجريمة الالكترونية لا تعترف بالحدود الجغرافية، وذلك لأن شبكة الأنترنت ألغت كل الحدود المتعارف عليها في العالم.

في حين أن الجرائم التقليدية هي جرائم داخلية تقع كاملة في نطاق إقليمي محدد وينطبق عليها القانون الجنائي المختص لذلك الإقليم.[2]

ثانيا: صعوبة إثبات الجريمة الالكترونية:

فالجرائم الالكترونية تتصف بالخفاء أي عدم وجود آثار مادية يمكن متابعتها وهي خطيرة وصعبة الاكتشاف، أو هي صعبة في تحديد مكان وقوعها، أو مكان التعامل معها بسبب اتساع نطاقها المكاني، وضخامة البيانات.[3]

[1]-خالد ممدوح إبراهيم، الجرائم المعلوماتية،ط2، دار الفكر الجامعي الاسكندرية، مصر، 2019، ص 77.

[2]-هبة نبيلة هروال، جرائم الانترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013، ص 45.

[3]-خالد ممدوح إبراهيم، المرجع السابق، ص 79.

ويعد إثبات الجريمة الالكترونية من الصعوبة بمكان حيث يصعب تتبعها واكتشافها فهي لا تترك أثرا يقتفي، حيث تعتبر مجرد أرقام، فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها كما أنها تفتقر إلى الدليل المادي التقليدي مثلا ومن جهة أخرى، فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي للتعامل معها[1].

وتتميز عن الجريمة التقليدية في كونها تتميز بطابع خاص لا نظير له في الجرائم الأخرى خاصة التقليدية، يتمثل في صعوبة اكتشافها وإثباتها نظرا لأسباب تتمثل في:

- **فضاء الجريمة:** أي أن الجريمة الالكترونية في الغالب تكون منتشرة وخفية لا يلاحظها المجني عليه وذلك لأنها لا تترك أي أثر خارجي بعد ارتكابها لانعدام الدليل المرئي الملموس[2].

- **صعوبة الاحتفاظ بآثار الجريمة:** حيث تعتبر الأدلة فيها غير مرئية فهي عبارة عن نبضات الكترونية تنساب عبر أجزاء الحاسوب والشبكة، وهذا ما يساعد الجاني في محو الأدلة وتدميرها في زمن قصير كما أن الدليل في هذه الجرائم غالبا ما يكون مرمزا أو مشفرا حيث لا يمكن للشخص قراءتها دون اللجوء الى الأدلة وبظهورها على شاشة الحاسوب.

ثالثا: قلة الإبلاغ عن الجريمة الالكترونية:

ويرجع السبب في ذلك لأن أغلب الجرائم يتم اكتشافها بمحض الصدفة وذلك لأنها تبقى عادة في طي الكتمان وهذا ما يعبر عنه علماء الإجرام بالرقم الأسود أو الرقم الخفي.

[1]-هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي، مجلة الأمن والقانون، دبي الإمارات العربية المتحدة، العدد الثاني، 1999، ص 11.

[2]-هبة نبيلة هروال: المرجع السابق، ص 48.

ومن بين أسباب اختفاء هذه الجرائم إحجام المجني عليه عن الإبلاغ عنها إذ نجد أن أغلب الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك تكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها خاصة إذا كان المجني عليه عبارة عن مؤسسة مالية كالبنوك والمؤسسات الادخارية حيث تخشى مجالس إدارتها عادة من أن تؤدي اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها.[1]

في المقابل فإن الجرائم التقليدية يكون الإبلاغ عنها بكثرة لأنها من السهل اكتشافها كما أن المجني عليه في الجريمة التقليدية يتحتم عليه الإبلاغ عن الجرائم وإلا سيتابع بجريمة عدم التبليغ.

رابعا: نقص خبرة الشرطة والقضاء:

يستلزم لكشف جرائم الأنترنت والاهتداء إلى مرتكبيها وملاحقتهم قضائيا استراتيجيات تحقيق وتدريب خاصة أي خبرة فنية تتلاءم مع طبيعة هذا المجرم، وتسمح بتفهم مواجهة الخصوصيات التي يقوم ويرتكز عليها هذا الأخير والأساليب التي تستخدم في ارتكابه.

لهذا وجدت أجهزة العدالة نفسها غير قادرة على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع المستحدث والفريد من الإجرام أي أنها أصبحت فاشلة في مواجهته[2]، وتختلف عن الجريمة التقليدية أن رجال الشرطة والقضاء مختصون ومدربون وذوي خبرة في هذا المجال حيث يعتمد على القدرة البدنية.

[1]-هشام فريد رستم، الجوانب الإجرامية لجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، آسيوط، مصر، 1994، ص 25.

[2]-هبة نبيلة هروال، المرجع السابق، ص 50.

الفرع الثالث: دوافع ارتكاب الجريمة الالكترونية:

الدافع، الباعث، والغرض أو الغاية هي تعبيرات تحمل دلالات اصطلاحية محددة في مجال القانون الجنائي، وترتبط بما يُعرف بالقصد الخاص في الجريمة. أما بالنسبة للجريمة الإلكترونية، فهي تنطوي على عدة دوافع مختلفة تدفع إلى ارتكابها. بعضها يرتبط بدوافع شخصية، بينما ينشأ البعض الآخر بسبب دوافع خارجية، وهناك دوافع تتعلق بالمؤسسات أو المنشآت. وغالبًا ما تكون جميع هذه الدوافع متأصلة في الرغبة الإجرامية.

أولا: الدوافع الشخصية:

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

أ-الدوافع المادية:

يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل وهو من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم الالكترونية ذلك أن من خصائص هذه الجرائم الحجم الربح الكبير الممكن تحقيقه في 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.[1]

وحسب الدراسات الحديثة فسنجد أن هذا الدافع يسود على غيره ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية، وفي مقدمة هذه الدراسات

[1]-خالد داودي، الجريمة المعلوماتية، ط1، دار الاعصار العلمي للنشر والتوزيع، عمان، الاردن، 2008، ص 37-38.

المسحية والإحصائية الدراسات والتقارير الصادرة عن مركن احتيال المعلومات الوطني في الولايات المتحدة الأمريكية N.F.I.C

وهناك فئة من مرتكبي الجرائم الالكترونية يرجع ارتكابهم لها إلى 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 أثمة ويرجع ذلك إلى 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.[1]

ومع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها إذ يظهر السعي إلى 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

[1]-أحمد خليفة ملط، الجرائم المعلوماتية، ط1، دار الفكر الجامعي الاسكندرية، مصر، 2006، ص 89-90.

المؤشرات، فإن الأمر يؤول في النهاية الى ارتكابه الجريمة الكترونية، هذا وتتعدد المؤثرات التي تدفع الانسان الى اقتراف مثل هذا السلوك سواء كان بدافع الانتقام، جنون العظمة التعاون والتواطؤ على الأضرار والتهديد.[1]

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 الضغوطات 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 اظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجاد وغالبا 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،

[1]-خالد داودي، المرجع السابق، ص 39.

وإن هذا الدافع هو أكثر الدوافع التي يجري استغلالها قبل المنظمات الجريمة لأجل استرجاع محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداد معقدة أو استئجارهم للقيام بالجريمة هذا وإن كان العل الواحد.[1]

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

حيث أنها غالبا ما تقيد مجهول وفي حالة اكتشافها فمن الصعب إقامة الدليل عليه ومحاكمته، ولكن في الغالب يحجم المجتمع عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة في كفاءته على عكس الجرائم الالكترونية قد تقيد ضد المجهول أو ضد المعلوم.[2]

المطلب الثاني: الأحكام الخاصة بالجريمة الالكترونية:

الفرع الأول: أنواع وأشكال الجريمة الالكترونية:

يصعب حصر أنواع الجرائم الإلكترونية بشكل كامل، نظرًا لتعدد أشكالها وتزايدها المستمر مع زيادة استخدام العالم للحواسيب وشبكة الإنترنت. فمن المعروف أن معظم هذه الجرائم تهدف في الأساس إلى الحصول على المعلومات، سواء أكانت محفوظة على أجهزة الكمبيوتر أو منقولة عبر الإنترنت. كما أن هناك جرائم تهدف إلى الاستيلاء على الأموال، وأخرى تستهدف أفراداً أو جهات معينة بشكل مباشر[3].

[1]-خالد داودي، المرجع السابق، ص 41.
[2]-هبة نبيلة هروال، مرجع سابق، ص 58.
[3]-خالد ممدوح إبراهيم، المرجع السابق، ص 77.

حيث قسمها الفقه الى طائفتين رئيسيتين هما:

أولا: الجرائم الموجهة ضد نظم 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، ونعرض لها على نحو ما يلي:

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 أموالا منقولة تصلح محلا للاعتداء عليها بالجرائم الموصوفة بوقوعها على المال، وبجرائم الإتلاف والتخريب ولا يربطها بالمعلوماتية سوى أن الأجهزة المادية محل الجريمة تستخدم في تشغيل النظام المعلوماتي[1].

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.[2]

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

[1]-هدى حامد قشقوش، المرجع السابق، ص 15.

[2]-خالد ممدوح إبراهيم، المرجع السابق، ص116.

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 مجموعة 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.[1]

ج-الجرائم الواقعة على المعلومات المسجلة بالنظام المعلوماتي:

ينصب هذا النوع من الجرائم على المعلومات باعتبارها هي المحور الأساسي 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 وإتلافها.

ثانيا: الجرائم الواقعة بواسطة النظام المعلوماتي:

تتنوع الجرائم الواقعة بواسطة النظام المعلوماتي إلى 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[2]:

[1]-هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص 15.

[2]-فريحة حسين، الجرائم الالكترونية والأنترنت، مقال منشور بمجلة المعلوماتية، السعودية، العدد 36، أكتوبر 2011، ص 4.

أ-الجرائم الالكترونية الواقعة على الأشخاص:

معظم الجرائم التي ترتكب في مجال المعلوماتية تستهدف إما أشخاص وإما جهات بعينها وغالبا ما تكون تلك الجرائم هي جرائم مباشرة، ترتكب في صورة ابتزاز أو تهديد أو تشهير[1]، ومن أهم جرائم الأشخاص جرائم صناعة ونشر الإباحة، جرائم التهديد و المضايقة والملاحقة، انتحال الشخصية والتغرير والاستدراج، السب وتشويه السمعة.[2]

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[3]، كالسطو والسرقة والتحويل الالكتروني غير المشروع للأموال وجريمة غسيل الأموال الكترونيا وقرصنة الحسابات البنكية بطريقة غير مشروعة.

ج-الجرائم الواقعة على أمن الدولة:

وهي من أخطر الجرائم الالكترونية وأهمها الإرهاب الإلكتروني والتجسس الالكتروني الذي يهدد الأسرار العسكرية والاقتصادية للدول مما يسهل خلق الفوضى والمساس بأمنها الداخلي.[4]

---

[1]-حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، جامعة 20 أوت 1955، سكيكدة، الجزائر، ص 221.

[2]-صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري، تيزي وزو، الجزائر، 2013، ص 50-51.

[3]-حكيم سياب، المرجع السابق، ص 221.

[4]-خالد ممدوح إبراهيم، المرجع نفسه، ص 115.

الفرع الثاني: أركان الجريمة الالكترونية:

تُعتبر الجريمة عبر الإنترنت جريمة تُمارس في الفضاء الافتراضي، مما يُضفي عليها طابعًا مميزًا وخصائص فريدة. ومع ذلك، فإن هذا لا ينفي وجود تشابه بينها وبين الجرائم التي تُرتكب في العالم الواقعي أو المادي، حيث تشترك في وجود فعل غير مشروع يقوم به الجاني. وبناءً على هذا التشابه، سنُناقش الأركان الأساسية التي تستند إليها هذه الجريمة.

أولا: الركن الشرعي:

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبني على ذلك عدم جواز ملاحظة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجرائية، وعلى القضاة التقيد بمدلول النص والالتزام بمضامينه[1].

يترتب على إهمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة، تتمثل في عدم رجعية القاعدة الجنائية أي بمفهوم المخالفة تتطبق القواعد الجنائية بأثر فوري ولا مجال لإهمالها بأثر رجعي، إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم[2].

[1]-أسامة أحمد المناعة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014، ص 45.

[2]-حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت 2014، ص 57.

إن الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين:

- مطابقة الفعل لنص التجريم.

- ألا يخضع الفعل المرتكب لسبب من أسباب الإباحة.

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة[1].

ثانيا: الركن المادي:

يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور والقانون وقد ذهب الدكتور رضا فرح إلى تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر:

أ-السلوك الإجرامي:

هذا السلوك يوجد بصورتين فقد يكون بفعل إيجابي، إذ يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة، كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع، وفي الجريمة المعلوماتية يمكن أن تجده بنوعيه السلوك الإيجابي أو السلبي. لا ننسى التطور الكبير في محتوى وطبيعة هذا

[1]-بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص 94-95.

السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الفاعل، وهذا السلوك الذي طورته أيضا عقلية الفاعل الذكية، والتي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا أوجدت بلا شك صعوبات كثيرة.[1]

ب-النتيجة الإجرامية:

يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث، فالسلوك قد أحدث تغييرا ملموسا، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى.[2]

ج-العلاقة السببية بين الفعل والنتيجة:

تتمثل العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجح إلى إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق الرابطة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت غير عمدية فإن نفي رابطة سببية يؤدي إلى انتفاء المسؤولية كلية عنها ذلك أنه لا شروع في الجرائم غير العمدية.[3]

ثالثا: الركن المعنوي:

يقوم الركن المعنوي للجريمة المرتكبة عبر الانترنت على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود عبر الانترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن

[1]-أسامة أحمد المناعة، جلال محمد الزغبي، المرجع السابق، ص 51-52.

[2]-بلعلبات إبراهيم، المرجع السابق، ص 18.

[3]-أسامة أحمد المناعة، جلال محمد الزغبي، المرجع السابق، من 58-59.

تتوفر النتيجة الجريمة المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة المجرمة من العمل غير المشروع الذي يبين الشبه في ارتكابه وهو عالم بالآثار الضارة الناشئة عنه.[1]

يختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع المحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي[2].

وفي جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعية العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع.[3]

الفرع الثالث: أطراف الجريمة الالكترونية:

لابد للجريمة الالكترونية كغيرها من الجرائم أن يكون لها طرفان فاعل ومجني عليه:

[1]-خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنات، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2011، ص 73-74.

[2]-حنان ريحان مبارك المضحاكي، المرجع السابق، ص 107.

[3]-أحمد خليفة الملط، المرجع السابق، ص 112-113.

أولا: الفاعل في الجريمة الإلكترونية:

إلى جانب توفر الشروط العامة التي يجب أن تتوافر في مرتكب الجريمة الإلكترونية، مثل السلوك المنحرف والعلم والإرادة بما يترتب على هذا السلوك، يُشترط أيضًا أن يمتلك هذا الشخص مستوى معينًا من المعرفة والخبرة في مجال الحاسوب وتقنية المعلومات. لذا، أطلق عليه البعض اسم المجرم 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[1]، لا يمكن تصور أن يكون مرتكب هذا النوع من الجرائم سوى فرد يتمتع بخصائص طبيعية وخبرة متعمقة في مجال علوم الحاسوب، سواء كان مستخدمًا عاديًا، مبرمجًا محترفًا، هاويًا، أو حتى متخصصًا في الجرائم المرتبطة بالحاسوب وتقنية المعلومات. ومن أبرز ما يميز هذا النوع من الأشخاص هو امتلاكهم معرفة واسعة وخبرة كافية في المسائل المعلوماتية وآليات عمل وتشغيل أنظمة الحاسب الآلي. يُعد هذا شرطًا أساسيًا، إذ تتبع الجرائم المعلوماتية غالبًا من استخدام تقنيات متقدمة تعتمد على أساليب تدميرية غير مباشرة، تتجلّى في التلاعب بالبيانات والكيانات المنطقية.

يختلف الجاني في جرائم الأنترنت عن مثيله في الجرائم التقليدية في: فالجاني في هذه الجرائم يسمى إما مجرما تقنيا أو هاكر 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

[1]-عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية (دراسة مقارنة)، رسالة ماجستير، القانون العام، جامعة الشرق الأوسط عمان الأردن، 2014، ص 32.

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 الاختراق برامج جاسوسية[1].

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[2]، 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 09-04.

فإن الضحية في الجرائم الإلكترونية وفي الجريمة بصفة عامة قد يكون شخصا طبيعي أو شخصا معنويا أنتهك حق من حقوقه المحمية قانونا، فلحقه جراء ذلك ضرر معنوي أو مادي، مع الملاحظ أن هذه الضحية أو المجني عليه قد يكون سببا في ارتكاب السلوك الإجرامي، إما لجهله بالجريمة وارتكابها أو لعدم احتياطه في أخذ تدابير الحماية الأمنية

[1]-هبة نبيلة هروال، المرجع السابق، ص 59.

[2]-بلال محمد الزعبي، أسامة أحمد مناعسة، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، دار الثقافة، عمان، الأردن، 2010، ص 77.

اللازمة لمنظومته المعلوماتية، أو حتى بسبب عدم القيام أو التخاذل في واجب الرقابة والتوجيه لأطفاله حيث يستخدم الشبكة وباقي الأجهزة المتصل بها[1].

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 فالأكيد أنها لن تفصح عن نفسها في حالة اختراق موقعها الإلكتروني لوجود ثغرة أمنية أو سرقة كلمات السر أو فك التشفير وغيرها من أساليب ارتكاب الجريمة ولن يقوم بذلك حتى مقدم الخدمات إلا في حالات معينة إلى تعفيه من المسؤولية القانونية[2].

[1]-دلال مولاي ملياني، 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، ص 41.

[2]-بلال محمد الزعبي، أسامة أحمد مناغسة، المرجع السابق، ص 78.

المبحث الثاني: البحث والتحري عن الجريمة الالكترونية.

إذا وقعت جريمة ما ونما إلى علم السلطات العامة نبأ ارتكابها فإن تلك السلطات تبدأ في التحرك وتتخذ مجموعة من الإجراءات التمهيدية بهدف تجميع أكبر قدر ممكن من المعلومات حول الجريمة وظروف ارتكباها، وتتمثل هذه الإجراءات في التحري الذي يقوم بها الضبطية القضائية ولا تبدأ إجراءات هذه المرحلة إلا بعد وقوع الجريمة، وهي تقوم على التحري عن الجرائم والبحث عن مرتكبيها وجمع الاستدلالات اللازمة للتحقيق في الدعوى.[1]

حيث أسند المشرع الجزائري هذه العملية للضبطية القضائية وأعمال البحث والتحري تشكل مرحلة من المراحل الإجرائية التي تعقب وقوع الجريمة.

المطلب الأول: مفهوم البحث والتحري:

سنحاول في هذا المطلب وضع تعريف للبحث والتحري من المنظور اللغوي والفقهي والقانوني مع تبيان الأجهزة المسؤولة عن التحري.

الفرع الأول: تعريف البحث والتحري:

أولا: التعريف اللغوي:

التحري لغة هو طلب ما هو أحرى أي ما هو أجدر وأفضل للاستعمال، ويعني أيضا البحث والتفتيش، يقال فلان يتحرى الأمر أي يتوخاه ويقصده، ويقال تحر بالشيء وتحرى منه وتحرى فيه أي قصد أفشله واجتهد وحقق في طلبه.

[1]-عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الاسلامي والقانون الوضعي، دار الجامعة الجديدة للنشر، الاسكندرية، 2006، ص 14.

ورد الفعل تحرى في اللغة العربية بمعنى طلب ما هو أحرى بالاستعمال في غالب الظن أو طلب أحرى الأمرين أي أولهما، أو طلب الأمر بمعنى قصده وفضله، والتحري في اللغة بمعنى الخليف والجدير والمناسب والأخرى بمعنى الأولى والأجدر والأخلف[1].

وقد ورد في بعض المراجع أن معنى التحري يفيد التقصي وهو البحث والاستقصاء والتحقيق بدقة ودراسة.

ثانيا: التعريف الاصطلاحي:

أ-التعريف الفقهي:

لفظ التحري لفظ فقهي استخدمه الفقه في كتاباته، فقد ذهب جانب من الفقه إلى القول بأن جوهر التحريات هو جمع البيانات كلها والمعلومات الصالحة للتنقيب عن الجرائم ومعرفة مرتكبيها وظروفها من سائر المصادر المتاحة لمأمور الضبط أو لمن يعاونه من مساعديه.

ويعرفها جانب آخر من الفقه إلى عدم استخدام أي 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[2].

[1]-عادل عبد العال خراشي، المرجع السابق، ص 15.

[2]-زوليخة زوزو، مشروعية أساليب التحري الحديثة، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد 8، الجزء 2، جوان 2017، ص 758.

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"[1]

ب-التعريف القانوني:

تنص الفقرة الثانية من المادة 12 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"[2].

هذا النص يتطابق في محتواه مع نص الفقرة الأولى من المادة 14 من قانون الإجراءات الجزائية الفرنسي ونفس المنحى ملاحظة بالنسبة لأغلب التشريعات العربية .مما سبق يمكننا أن نستخلص العناصر الأساسية للبحث والتحري والتي تتمثل في :

1. أنها مجموعة من الإجراءات الجزائية.
2. ينفذها أعضاء الضباط القضائي.
3. تبدأ بعد ارتكاب الجريمة وتنتهي بتحريك الدعوى القضائية.
4. مضمونها معاينة الجرائم وجمع الأدلة عنها والبحث عن مرتكبيها.
5. تستهدف التمهيد لتحريك الدعوى العمومية ومباشرتها والسير في التحقيق القضائي[3].

[1]-حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء القانون الجزائري، دراسة مقارنة، ط1، منشورات السائحي، الجزائر، 2017، ص 18.

[2]-المادة 12 الفقرة 3 من الأمر رقم 66-155 المؤرخ في 8 جوان 196 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم 11-02 المؤرخ في 23 فيفري 2011، ج..ر، ج.ج.د،ش، العدد 12 المؤرخ في 23 فيفري 2011.

[3]-حمزة قريشي، المرجع السابق، ص 19.

وقد نهج نفس المنهج المشرع المصري في نص المادة 24 من قانون الإجراءات الجنائية، فإن المشرع قد أشار بمعنى عام وشامل بقوله في مجال تحديد اختصاصات مأمور الضبط القضائي ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على جميع الإيضاحات والتحريات وفق النص نفس المادة توضيح كافة الأمور المتعلقة بالجريمة أي كل من شأنه تحديد الجريمة ورسم معالمها.

الفرع الثاني: خصائص البحث والتحري في الجريمة الالكترونية.

تمثل مرحلة التحقيق الابتدائي، أو ما يُعرف بمرحلة جمع الاستدلالات، عنصراً جوهرياً في إطار البحث والتحري عن الجرائم. وتكتسب هذه المرحلة أهمية خاصة عند التعامل مع الجرائم الإلكترونية، باعتبارها الأساس الذي تُبنى عليه الدعوى القضائية برمتها. إذ إن المعلومات والأدلة الرقمية التي يتم جمعها مباشرة بعد وقوع الجريمة قد لا تظل متوفرة بعد مرور فترة وجيزة، وذلك يعود إلى الطبيعة التقنية والمتغيرة لهذه الجرائم.

ففي كثيرا من الجرائم المعلوماتية لم يترك الجاني ورائه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإعجاب والإحباط معا[1].

أولا: خصائص التحقيق:

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة .وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع

[1]-محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت: الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2011، ص 230.

والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته[1].

ذلك أن الفكر البشري المتعلق بالجرم الإلكتروني يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يكون متغيرا أو متطورا أيضا، وذلك كنتيجة طبيعية لمواجهة المجرم الإلكتروني.

1- أسلوب التحقيق الابتدائي في الجريمة الإلكترونية:

التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم للمحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمضاهاة البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي والهدف من التحقيق الابتدائي هو التأكد أولا من وقوع الجريمة يعاقب عليها القانون، ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وما هي الوسائل التي استعملت في ارتكابها، ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي يختلف عن غيره بالنسبة للجرائم الأخرى[2].

أ/ وضع خطة عمل التحقيق: يبدأ المحقق عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوفرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو الآتي:

[1]-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009، ص 56.

[2]-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009، ص 56.

– وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة .

– التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب التعامل مع هذه الجرائم.

– عمل دراسة جادة لكافة الإجراءات التحقيق خطة مسبقة التي يتم وضعها ومناقشتها من طرف العاملين في فريق التحقيق[1].

– تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في انجاز العمل من أجل ضمان مستوى جيد من الأداء.

– تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطار الفردية التي قد تنتج عن قلة الخبرة أنقص المعرفة، والتي تساعد في التقيد بالمستوى المطلوب والتي تضمن الخطوات التي يقوم بها المحقق خلال مراحل التحقيق.

ب/ تشكيل فريق التحقيق: إن التحقيق الابتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المضبوطات هي مجرد حاسب شخصي واحد ولذلك فإنه يفضل أن يتعاون عدة محققين في انجاز مهمة التحقيق والعثور على الأدلة، ويجب أن يتشكل فريق التحقيق من فنيين أخصائيين ذوي خبرة في مجال الحاسوب الأنترنت ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي

[1]-محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 72.

الإلكتروني وفي شكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والانترنت ليتمكنوا من فك التعقيدات التي تفرقها ظروف وملابسات كل جريمة[1].

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما تطلبه من مهارات وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا ومن الناحية العملية غالبا ما يتكون فريق التحقيق من:

- خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادثة وكيفية التعامل مع هذه الجرائم.

- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.

- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.

- خبراء التصوير والبصمات والرسم التخطيطي[2].

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة الحماية المعطيات المعلوماتية، وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك[3].

[1]-عبد الله حسين محمود، إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003، ص 612.

[2]-عبد الله حسين محمود، مرجع سابق، ص 613.

[3]-أنظر المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المعدل والمتمم في 2019.

2-العناصر الأساسية للتحقيق الابتدائي في مجال البرمجة الإلكترونية:

نقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي[1]

أ/ الإجراءات التي يجب مراعاتها قبل البدء في التحقيق:

- تحديد نوع نظام المعالجة الأولية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات.

- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.

- إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه.

- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.

مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة .

- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار الجريمة.

[1]-عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى، ص 84.

– فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها لطمس البيانات.

– التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتقليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك[1] .

– إبعاد الموظفين عن أجهزة الحاسوب الآلي بعد الحصول منهم على كلمة السر وكذا الثغرات في حالة وجودها.

– تصوير الأجهزة المستهدفة من أمام والخلف لإثبات بأنها كانت تعمل.

ب/ الإجراءات التي يجب مراعاتها أثناء التحقيق:

– عمل نسخة احتياطية من الأقراص الصلبة قبل استخدامها والتأكد فنيا من دقة النسخ.

– نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

– العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها .

– حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.

– العمل على فحص وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس المعلومات.

[1]-عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى، ص 84.

– أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص وتحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة المعلومات والملفات الممسوحة، وكذلك معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب[1].

الفرع الثالث: طبيعة وأهمية البحث والتحري عن الجريمة الالكترونية.

أولا: طبيعة البحث والتحري:

أغلب فقهاء القانون الجنائي لا يعدون مرحلة البحث والتحري والاستدلال من مراحل الخصومة وإنما يعدونها مرحلة ممهدة ومساعدة السلطات التحقيق، فهي لا تدخل في إطار الدعوى الجنائية وإن كانت ضرورية لها[2]، ويترتب أموري الضبط القضائي القائمين بهذه المرحلة أن يتحدوا أيا من الإجراءات التي تدخل في نطاق مرحلتي التحقيق الابتدائي والنهائي إلا في حالات استثنائية، ويعلق الفقه على ذلك بأن مرحلة الاستدلال مجرد مقدمة لمرحلة التحقيق، وأن الضبطية القضائية ليس لها أن تتوغل في أعماق الدعوى الجنائية مثلما تفعل سلطة التحقيق.

وإذا كان أغلب الفقه والقضاء لا يعد هذه المرحلة من مراحل الدعوى الجنائية، إلا أننا نجد أن بعضا من الفقه يعتبرها أساس الدعوى الجنائية ونحن نتفق مع هذا الرأي فيما ذهب إليه، إذ أن هذه المرحلة تعد مرحلة هامة وخطيرة في بناء صرح الدعوى الجنائية كما أن محاضر جمع الاستدلالات هي الأداة التي يتم بمقتضاها تحريك الدعوى الجنائية في الجنح والمخالفات وقد استند في هذا الرأي فيما ذهب إليه الى الاعتبارات الآتية[3]:

[1]-سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق و العلوم السياسية، جامعة باتنة، 2013، ص 112-114.

[2]- محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، ط11، مطبعة جامعة القاهرة، 1976، ص 203.

[3]- عادل عبد العال خراشي، المرجع السابق، ص 30.

أ-الاعتبار التشريعي:

إن إجراءات التحريات الأولية مباشرتها أعضاء الضبط القضائي ولا سيما الموظفين الذين يتصفون بصفة مأمور الضبط القضائي (ضابط الشرطة القضائية)، حيث أن هناك تداخل بين الضبط الاداري والضبط القضائي، إذ يتفقان في الهدف الذي يسعيان إليه وهو المحافظة على النظام العام إلا أنها يختلفان من حيث السلطة المختصة بإجراء كل منهما.

إن تنفيذ مهام الموظفين الذين يتصفون بضباط الشرطة القضائية تكون بواسطة الضبط الاداري والضبط القضائي، ونظرا الى أن أعضاء الضبط القضائي ليسوا من أعضاء الهيئة القضائية بل يعتبرون موظفين إداريين فإن التحريات التي يباشرونها هي مجرد استدلالات وهي مرحلة تمهيدية للتحقيق وقبل ذلك ضرورية تساعد النيابة على الفصل في الملف سواء بالحفظ أو تحريك الدعوى العمومية والبيانات التي تتضمنها محاضر التحريات الأولية لا يمكن اعتبارها أدلة يستطيع القاضي تسبيب أحكامها عليها وهذا هو المنحى الذي سار عليه الاجتهاد القضائي في الجزائر[1].

ب-الاعتبار القضائي:

فقد اعترف القضاء لمحاضر الاستدلال بقيمتها القانونية في الإثبات، فقضت محكمة النقض أعمالا لذلك بأن: "من المقرر أن للمحكمة أن تأخذ باعتراف المتهم ولو كان واردا بمحضر أوفي تحقيق اداري متى اطمأنت إلى صدقه ومطابقته للواقع ولو عمل عنه في مراحل التحقيق الأخرى دون بيان السبب".

[1]- حمزة قريشي، المرجع السابق، ص 21.

ج-الاعتبار العملي:

فهو مستمد من الواقع وطبيعة عمل النيابة العامة والتكوين المهني المأموري الضبط القضائي، فقد جرت النيابة العامة -لكثرة الأعباء الملقاة عليها والزيادة المطردة في عدد القضايا وخاصة الجنح والمخالفات-على التصرف في غالبية الجنح أن لم يكن كلها، وجميع المخالفات بناء على محضر الاستدلال، أما من ناحية طبيعة التكوين المهني لمأموري الضبط القضائي فيعرض عليهم الميل الى اتخاذ الإجراءات القسرية في جمع الأدلة وتقديمها الى سلطة التحقيق دون الالتجاء الى الوسائل العادية أو العلمية في الحصول على الأدلة مما يدفعهم إلى إهدار الحريات الفردية.

فكل هذه الاعتبارات أدلة واضحة على أن مرحلة التحري مرحلة أساسية من مراحل الدعوى الجنائية وليست مرحلة تمهيدية لها كما ذهب أغلب الفقه[1].

ثانيا: أهمية البحث والتحري عن الجريمة الالكترونية.

يسود اعتقاد لدى الكثير من مأموري الضبط القضائي أنه لا أهمية تذكر الأعمال التحري والاستدلال التي يجرونها، لأن هذه الأعمال متبوعة بإجراءات تحقيق أخرى، في مرحلة التحقيق الابتدائي تلك التي يقوم بها قاضي التحقيق أو النيابة العامة، الأمر الذي يجعلهم بمنأى عن الدقة والعناية وعدم الاهتمام بالمحافظة على الحقوق والحريات الفردية بالإضافة إلى ما يسود في الاعتقاد بأن الدعاوى التي تحال بناء على محضر الاستدلالات الى محكمة قليلة وأن قيمة هذه المحاضر في المحاكمة محدودة إلا لم تكن منعدمة.

وللتصدي لذلك يمكن القول بأن هذه المرحلة تعد من أخطر مراحل الدعوى ذلك لأن أغلب القضايا التي تطرح على المحاكم لا تتضمن أوراقها سوى محضر جمع

[1]- عادل عبد العال خراشي، المرجع السابق، ص 32-31.

الاستدلالات الذي يباشره مأمور الضبط القضائي فصلا عن أن سلطة الاتهام غالبا ما تكتفي في هذه القصايا بما دون في محضر الاستدلالات لتقديم الدعوى إلى المحكمة[1].

وأهمية هذه المرحلة تظهر من الدور الذي تقوم به في الكشف عن الجرائم الأمر الذي جعلها محل اهتمام العديد من المؤتمرات الدولية والإقليمية فقد أكد المؤتمر الدولي السادس لقانون العقوبات الذي عقد في مدينة روما عام 1953 أن البوليس القضائي يقوم بعمل لا غنى عنه في التحري عن الجرائم وكشفها[2]، وتتمثل أهمية البحث والتحري في:

1-أهمية البحث والتحري لجهات التحقيق والاتهام:

تعطي مرحلة البحث والتحري صورة واضحة عن وقوع الجريمة وكيفية حدوثها والظروف التي رافقتها ومحاولة كشف غموضها وملاحقة مرتكبيها وهي بذلك تساعد سلطة الاتهام في تحريك الدعوى الجنائية وتسهل لها القيام بعملها، كما تعد هذه المرحلة بمثابة الضوء الذي ينير الطريق لسلطة الاتهام وبقدر قوة هذا الضوء ونقائه تكون الرؤية واضحة أمام تلك السلطات، فالنيابة العامة لا تبدأ التحقيق إلا إذا وجدت دلائل كافية على وقوع الجريمة[3].

كما تظهر أهمية هذه المرحلة في أن بعض إجراءات التحقيق لا يجوز مباشرتها إلا إذا توافرت دلائل جدية تبرر اتخاذها، وهذه الدلائل قد تستخلصها سلطة التحقيق من الاستدلالات التي يجمعها مأمور الضبط القضائي ومتى قررت كفايتها كان لها أن تأذن بمباشرة بعض هذه الإجراءات فالقبض كإجراء من إجراءات التحقيق لا يجوز لمأمور الضبط مباشرته خارج نطاق حالة التلبس إلا بناء على إذن من النيابة العامة[4]

[1]- عادل عبد العال خراشي، المرجع السابق، ص 35.

[2]- محمود محمود مصطفى، المرجع سابق، ص 206.

[3]- عبد العالي خراشي، المرجع السابق، ص 36.

[4]- محمود محمود مصطفى، المرجع السابق، ص 206.

وتظهر أهمية هذه المرحلة في المحافظة على أدلة الجريمة وآثارها، لأن هذه الآثار والأدلة هي التي تقود إلى 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[1].

تتمثل أهمية البحث والتحري في توضيح الملابسات والظروف التي وقعت فيها الجريمة، والإسراع بجمع الأدلة والمستندات والعلامات والآثار التي تسهم في تأكيد حدوث الجريمة وربطها بشخص محدد.

وتحرير الأعمال والإجراءات التي ينفذها رجال الضبط القضائي في محاضر يكون بها ملف القضية وتتضمن كل العناصر الأولية التي يعتمد تحليلها وكيل الجمهورية[2].

2-أهمية البحث والتحري للقضاء:

لا تقتصر أهمية هذه المرحلة على دور سلطة التحقيق والاتهام فقط، بل تتجاوز ذلك لتشمل أهمية كبيرة بالنسبة للقضاء. ويتجلى ذلك من الناحيتين العملية والقانونية. فمن الناحية العملية، يعد عمل رجال الضبط القضائي العاملين في هذه المرحلة هو العنصر الأساسي الذي يحدد مدى نشاط الأجهزة القضائية. فكلما كان نشاطهم مكثفًا، كان الكشف عن الجرائم أكثر فعالية. إذ يتحملون مسؤولية البحث عن الجرائم المرتكبة، وفي حال تقاعسهم عن أداء واجبهم، تبقى بعض الجرائم طي الكتمان، مما يمنع العدالة من الوصول إليها.

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

[1]- المرجع نفسه، ص 36.

[2]-أحمد قريشي، المرجع السابق، ص 22.

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 تكمئن 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 يبني حكمه على دليل له أصل في أوراق الدعوى[1].

المطلب الثاني: ضوابط البحث والتحري عن الجريمة الالكترونية.

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعوانها حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية[2].

حدد المشرع الجزائري في نص المادة 14 من قانون الإجراءات الجزائية صفة القائمين بالتحري والاستدلال وهم ضباط الشرطة القضائية، أعوان الضبط القضائي والموظفين والأعوان المنوط بيهم قانون بعض مهام الضبط القضائي[3]، 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[4].

[1]-عبد العالي خراشي، المرجع السابق، ص 37.

[2]- عز الدين عثماني، إجراءات التفتيش والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، جامعة تبسة، العدد 04 جانفي 2018، ص 50.

[3]- المادة 14 من قانون الإجراءات الجزائية المعدل والمتمم بموجب الأمر رقم 15/02 ج.ر، ج، ج.د.ش، العدد 40.

[4]- عبد العالي خراشي، المرجع السابق، ص 106.

الفرع الأول: الأجهزة المكلفة بالبحث والتحري في الجريمة الالكترونية.

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 في مجال معين وباعتبارها الأقدر من غيرها على كشف الجرائم الواقعة ضمن حدود اختصاصها الفني أو التقني[1]، والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال الضبط القضائي.

ومن أجل إشراك مزودي خدمات الأنترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم الالكترونية يلزم القانون 09-04 هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها[2].

أولا: تشكيل الضبطية القضائية:

إن أعضاء الضبطية موظفون منحهم القانون صفة الضبطية القضائية مكلفون خلال مرحلة التحقيق التمهيدي بالكشف عن وقوع الجريمة وجمع الاستدلالات عنها وعن المساهمين فيها باعتبارهم فاعلين أصليين وشركاء فيها ليتم تحرير محاضر بشأنها وتقديمها أمام الأجهزة المختصة.

[1]- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09-04، رسالة مقدمة لنيل شهادة الماستر في القانون الجنائي، كلية الحقوق والعوم السياسية، جامعة ورقلة، 2012/2013، ص 66.

[2]- عز الدين عثماني، المرجع السابق، ص 52.

ويقصد بهم جميع الموظفين الذين خولهم القانون مباشرة إجراءات البحث والتحري وهؤلاء الموظفون يستمدون صفتهم واختصاصهم من نص القانون ومن ثم كان بيان المشرع لهم بيانا واردا على سبيل الحصر[1].

وقد حدد لنا القانون الإجراءات الجزائية الجزائري الضبطية القضائية وتتمثل في:

أ-**ضباط الشرطة القضائية:** يتمتع بصفة ضابط الشرطة القضائية حسب القانون الإجراءات الجزائية الجزائري.

- رؤساء المجالس الشعبية البلدية.

- ضباط الدرك الوطني الموظفون التابعين للأسلاك الخاصة والمراقبين ومحافظي وضباط الشرطة للأمن الوطني.

- ذو الرتب في الدرك، ورجال الدرك الذين أمضوا في سلك الدرك 03 سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني بعد موافقة لجنة خاصة[2]

- مفتشو الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة 03 سنوات على الأقل وعينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية بعد موافقة خاصة.

ويتبين من خلال نص المادة أن هناك 03 فئات ممن يتمتعون بصفة ضباط الشرطة القضائية وهي:

[1]- عبد العالي خراشي، مرجع سابق، ص 107.

[2]- المادة 15 من قانون اجراءات الجزائية المعدل والمتمم بموجب الأمر رقم 15/02 المرجع السابق..

الفئة الأولى: هي الفئة التي تتمتع بصفة ضباط الشرطة القضائية بحكم القانون وهم رؤساء المجالس الشعبية البلدية وضباط الدرك الوطني ومحافظو وضباط الشرطة القضائية.

الفئة الثانية: هي الفئة التي يجب لكي تتمتع بصفة ضباط الشرطة القضائية تعيينهم بقرار مشترك من وزير الدفاع ووزير العدل المصالح الأمن العسكري في الملفات.

الفئة الثالثة: وهي الفئة التي لا تخول لها صفة الضبطية إلا بعد تجاوز امتحان وموافقة لجنة خاصة وتعيينهم بقرار مشترك أما وزير الدفاع ووزير العدل ذوي الرتب في الدرك والدركين الذين قضوا في الخدمة 03 سنوات أو وزير الداخلية ووزير العدل (مفتشي الأمن الوطني والضباط التابعين للقطاع العسكري الذين تم تعيينهم بموجب قرار مشترك بين وزير العدل.[1]

ب-أعوان الضبط القضائي: وقد حددهم قانون الإجراءات الجزائية في المادة 19:

- موظفي مصالح الشرطة وذو الرتب في الدرك الوطني والدركيين ومستخدمو مصالح الأمن العسكري (الملفات) الذين ليس لهم ضباط شرطة قضائية.

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

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

[1]- عبد العالي خراشي، مرجع سابق، ص 108.

– رؤساء الأقسام والأعوان التقنيون في الغابات وحماية الأراضي الذين حددتهم المادة 23[1] يجور أثناء ممارستهم مهامهم أم يطلبوا مساعدة القوة العمومية.

– موظفون وأعوان الإدارات والمصالح العمومية الذين يباشرون بعض مهام الضبط الفضائي .– الولاية (المادة 28 من قانون الإجراءات الجزائية).

ثانيا: دور مقدمي خدمات الأنترنت في البحث والتحري عن الجرائم الالكترونية:

إن تكنولوجيا الاعلام والاتصال متنوعة خاصة ما يتعلق منها بخدمات الاتصال السلكية واللاسلكية كالهواتف النقالة والشبكات الرقمية المتمثلة في الأنترنت وهو ما يجعل عملية توصيل الخدمات المتنوعة لهذه التكنولوجيا الى مستعمليها يتطلب توافر مجموعة من الفاعلين على رأسهم مقدمي الخدمات المنصوص عليهم في القانون 09-04، حيث يلزمهم القانون بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، ويوضح المعطيات الملزمين بحفظها وتشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات المستعملة في الاتصال، والخصائص التقنية وتاريخ وزمن ومدة كل اتصال والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه وعناوين المواقع المطلع عليها[2]

وعرفهم القانون 09-04 على أنهم:

أي كيان عام أو خاص يقحم مستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصالات.

[1]- ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، رسالة تكميلية لنيل شهادة ماستر في القانون، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2015/2016، ص 3-4.

[2]- عز الدين عثماني، المرجع السابق، ص 52-53.

وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها[1].

الفرع الثاني: الوسائل المستخدمة في التحري وجمع الأدلة:

عند القيام بالتحقيق في جريمة ما فإنه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة وقواعد فنية تحقق الشرعية، وسهولة الوصول إلى الجاني وحيث أن للجرائم الالكترونية طابعها الخاص المميز لها فإن البحث والتحري فيها يحتاج إلى معرفة تامة وإدراك وسائل وقوع الجريمة وبالتالي حل لغزها والوصول إلى الجاني، وفي سبيل ذلك يعتمد المحقق على مجموعة من الوسائل المختلفة.

أولا: الوسائل المادية:

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

– عناوين IP والبريد الالكتروني وبرامج المحادثة.

– البروكسي (PROXY) حيث يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها الإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة (CASHE MEMORY).

– برامج التتبع حيث تقوم هذه البرامج بالتعرف على محادثات الاختراق التي تتم مع تقديم بيان شامل بها الى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث

[1]- المادة 02 الفقرة 02 من القانون رقم 09-04.

وتاريخ حدوثه وعنوان IP الذي تمت من خلاله عملية الاختراق واسم الشركة المزودة الخدمة الأنترنت المستضيفة للمخترق.

– وأرقام مداخلها ومخارجها على شبكة الأنترنت ومعلومات أخرى ومن الأمثلة على هذه البرامج (HACKTRACER VL.2).

–نظام كشف الاختراق (INTRASION DETECTION SYSTEM) ويرمز له اختصارا بالأحرف IDS وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجرى حدوثها على أجهزة الحاسبة الالكترونية أو الشبكة مع تحليلها بحثا عن أية إشارة قد تحل على وجود مشكلة قد تهدد أمن الحاسبة الالكترونية أو الشبكة.

ويتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسبة الالكترونية أو الشبكة ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع[1].

وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها.

– أدوات تدقيق ومراجعة العمليات الحاسوبية.

[1]- عز الدين عثماني، المرجع السابق، ص 54-55.

– أدوات فحص ومراقبة الشبكات، هذه الأدوات تستخدم في فحص بروتوكول ما وذلك المعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات أدوات ARP وظيفتها تحديد مكان الحاسبة الالكترونية فيزيائيا على الشبكة[1]

ثانيا: الرسائل الإجرامية:

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثانية والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها :

1. اقتفاء الأثر: يمكن تقصي الأثر بطرق عدة سواء عن طريق بريد الكتروني ثم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.
2. الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.
3. الاستعانة بالذكاء الاصطناعي، من خلال استنساخ النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الالكترونية وفق برامج صممت خصيصا لهذا الغرض[2].
4. مراقبة الاتصالات الالكترونية لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الاتصالات الالكترونية، على عكس بعض التشريعات التي عرفتها مثل التشريع الأمريكي والكندي.

[1]-خيرت علي محرز، المرجع السابق، ص 81.

[2]- عزالدين عثماني، المرجع السابق، ص 55.

الفرع الثالث: قواعد الاختصاص:

إن أعضاء الضبطية القضائية وهم يمارسون صلاحياتهم في إجراء التحريات اللازمة بشأن الجريمة لمعرفة مرتكبيها مقيدين في ذلك بنطاق إقليمي يسمى بالاختصاص المحلي وبنوع معين من الجرائم ويسمى الاختصاص النوعي.

أولا: الاختصاص المحلي:

يقصد به المجال الإقليمي الذي يباشر فيه ضباط الشرطة القضائية مهامهم في البحث والتحري عن الجريمة، ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة ولذلك يتعين أن يكون مكان وقوع الجريمة أو محل إقامة المتهم محل القبض عليه[1].

- **امتداد الاختصاص المحلي:**

يجيز القانون تمديد الاختصاص المحلي لضباط الشرطة القضائية في حالة الاستعجال أو بناء على طلب من السلطة القضائية وهو ما نصت عليه المادة 16/02 من ق. إ. ج (دائرة المجلس) وكذا تحديد الاختصاص المحلي لضباط الشرطة القضائية في الجرائم الستة الخطيرة إلى كافة التراب الوطني[2]

ثانيا: الاختصاص النوعي:

يقصد به اختصاص عضو 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.

[1]- ابتسام بغو، المرجع السابق، ص 5-6.

[2]- انظر المادة 16 من قانون الإجراءات الجزائية الجزائرية.

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[1].

نستنتج مما تم تناوله في هذا الفصل المتعلق بالإطار المفاهيمي للجريمة الإلكترونية أن التكنولوجيا المعلوماتية أصبحت جزءًا لا يتجزأ من حياة الناس اليومية، حيث تعتمد غالبية الدول على التقنية في مختلف المجالات. ومع الانتشار الواسع لهذه التكنولوجيا، ساهمت في بروز الجريمة الإلكترونية وظهور فئة جديدة من المجرمين تُعرف بـ "مجرمي المعلوماتية". ما يميز هؤلاء عن المجرمين التقليديين هو الذكاء، المعرفة العميقة، والخطورة العالية في مجال المعلوماتية، بالإضافة إلى التحديات المرتبطة بصعوبة تعقبهم.

وسنتطرق في الفصل الثاني إلى الإطار القانوني للبحث والتحري من خلال دراسة إجراءات التحري التقليدية والمستحدثة وموقف المشرع الجزائري منها وكذا دراسة مشروعية هذه الإجراءات، وفي الاخير سنحاول معرفة الجهود التي قامت بها الدول لمكافحة الجريمة الالكترونية.

[1]-ابتسام بغو، المرجع السابق، ص 5-6.

الفصل الثاني

خصوصية البحث والتحري عن الجريمة الالكترونية

لقد أثارت ظاهرة الجرائم الإلكترونية العديد من التحديات فيما يتعلق بالقانون الجنائي الموضوعي، حيث أظهرت عدم قدرتها على مواكبة تطور وتعقيد هذه الظاهرة وما تتميز به من خصائص فريدة. وفي المقابل، ظهرت مشكلات أخرى ضمن نطاق القانون الجزائي الإجرائي، خاصة أن الجرائم الإلكترونية غالبًا ما ترتبط بالبيانات الناتجة عن المعالجة الآلية للمعلومات والكيانات الرقمية غير الملموسة، مما يجعل عملية جمع الأدلة وتأكيدها أو ضبطها بالوسائل التقليدية مهمة صعبة. لذلك، يصبح من الضروري أن تمتلك الجهات المختصة بالتحقيق معرفة عميقة بأساسيات عمل الحواسيب وتقنيات تشغيلها، بالإضافة إلى امتلاك المحققين خبرة بفهم البيئة الرقمية المتمثلة في الحواسيب وشبكة الإنترنت، مع توفر المعرفة الكافية بشأن إجراءات الضبط والتفتيش وكشف الأدلة وحفظها بشكل سليم.

تشكل إجراءات التفتيش والضبط التي تنفذها أجهزة الضبط القضائي، سواء في الجرائم التقليدية أو الإلكترونية، مساساً بحقوق الأفراد وحرياتهم. ولهذا، فإنه من الضروري أن تُنفذ بصورة سليمة ومتوافقة مع القانون، إذ إن الاعتماد على أساليب غير مشروعة يترتب عليه بطلان تلك الإجراءات.

المبحث الأول: أساليب البحث والتحري في الجريمة الالكترونية.

الجرائم الالكترونية نوع من الاجرام الحديث ويعد التشريع اللبنة الأولى والأساسية التي يمكن من خلاله مكافحة هذه الجريمة، فلا جريمة ولا عقوبة إلا بنص[1]، لذا نجد دولا كثيرة حاولت وضع قوانين للتصدي لهذه الظاهرة الإجرامية، إلا أن النصوص القانونية مهما كثرت وتعددت تبقى غير كافية في ظل غياب القواعد الإجرائية والمؤسساتية، فهذه القواعد مجتمعة هي التي يمكن من خلالها تجسيد القانون على أرض الواقع وإعطائه

[1]- دلال مولاي ملياني، المرجع السابق، ص 174.

الديناميكية التي يحتاجها لمكافحة الجريمة والقبض على مرتكبيها[1]، حيث في هذا المبحث سوف تتناول فيه أساليب البحث والتحري في ظل قانون الإجراءات الجزائية وفي ظل قانون 09-04.

المطلب الأول: أساليب البحث والتحري في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والإتصال.

لأجل التطرق لمختلف الأساليب المنظمة بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والإتصال في هذا المطلب فقد تم تقسيمة إلى 3 فروع. خصص الفرع الأول للتفتيش الالكتروني، والفرع الثاني خصص للحجز أو الضبط الالكتروني، والفرع الثالث للمراقبة. الالكترونية.

الفرع الأول: التفتيش في الجريمة الالكترونية.

يعد التفتيش وسيلة قانونية تهدف إلى البحث عن الأدلة التي يمكن أن تسهم بشكل فعال في كشف الحقيقة وتوضيح الملابسات. وقد أولى المشرع الجزائري أهمية خاصة لهذا الإجراء، حيث عمل على تنظيمه وتطويره من خلال أحكام القانون 09-04، وذلك ليواكب طبيعة الجرائم المرتبطة بالإنترنت التي تتسم بطابعها غير المادي وغير المحسوس. وتمثل هذه الخطوة استجابة ضرورية للتحديات التي تفرضها هذه النوعية الحديثة من الجرائم، والتي تتطلب أدوات وأساليب تحقيق تتلاءم مع طبيعتها المعقدة والمتغيرة باستمرار.

يعرف التفتيش على أنه البحث في مستودع السر عن اشياء تفيد في الكشف عن الجريمة وقعت ونسبتها الى مرتكبيها، "وهو إجراء من إجراءات التحقيق التي تهدف إلى

[1]-شنتير خضرة، الآليات القانونية لمكافحة الجريمة الالكترونية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أحمد دراية أدرار، 2020/2021، ص 42.

البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص. وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة"، وعرفه البعض الآخر بأنه: " البحث عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون التفتيش سند من القانون[1]"

من خلال هذه التعريفات 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[2].

نطاق تفتيش مكونات النظام المعلوماتي في جرائم الأنترنت:

المنظومة المعلوماتية تتألف من مجموعة من العناصر المتكاملة التي تشمل الجوانب المادية، كالأجهزة والمعدات الإلكترونية، والجوانب غير المادية أو المعنوية، مثل البرمجيات والأنظمة التشغيلية. بالإضافة إلى ذلك، فإنها تضم شبكات الاتصال الإلكترونية التي تسهّل تبادل البيانات والمعلومات، بجانب منظومات تخزين متقدمة تُستخدم لحفظ واسترجاع المعلومات بكفاءة. هذه المنظومات، بمكوناتها المختلفة، تكون عادة محط اهتمام وتحليل خلال عمليات التفتيش بهدف استخراج الأدلة الجنائية الإلكترونية الضرورية لإثبات الحقائق أو كشف الجرائم ونسبتها إلى مرتكبيها[3].

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط1، دار الفكر الجامعي، الاسكندرية، مصر، 2009، ص 182.

[2]- دلال مولاي ملياني، المرجع السابق، ص 214.

[3]- دلال مولاي ملياني، المرجع السابق، ص 215.

تفتيش مكونات النظام المعلوماتي المادية والمعنوية

تفتيش مكونات النظام المعلوماتي المادية:

ليس هناك خلاف حول تفتيش المكونات المادية للنظام المعلوماتي بحثا عن شيء يتصل بالجريمة وقعت يفيد في كشف الحقيقة عنها وعن مرتكبيها يخضع للإجراءات القانونية الخاصة بالتفتيش بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات، حيث أن لصفة المكان أهمية وطبيعته أهمية قصوى، فإذا كانت موجودة في مكان خاص كمسكن المتهم واحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانونا.[1]

أما لو وجد شخص يحمل مكونات الكمبيوتر المادية أو حائز لها في مكان عام فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.

فالتشريع الإجرائي الجزائري، يتضمن نصوص قانونية تنطبق من حيث الأصل على تفتيش المكونات المادية للنظام المعلوماتي[2]، ومن النصوص القانونية التي يمكن تطبيقها في هذا المجال نص المادة 64 من ق. إ. ج ج والمواد (37) و (40) و (42) من المواد (44) الى (47) من ق. إ. ح. ج[3]

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي، المرجع السابق، ص 195.

[2]- دلال مولاي ملياني، المرجع السابق، ص 216.

[3]- انظر المادة 64 والمواد 44 إلى 47 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155، ج.ر، ج.ج،د.ش، العدد 84 الصادرة في 24 ديسمبر 2006.

تفتيش مكونات النظام المعلوماتي المعنوية:

التفتيش على مكونات النظام المعلوماتي، الذي يتمثل في المعلومات المُعالجة آلياً، يُعتبر ممارسة شائعة تهدف إلى الكشف عن الجرائم المتعلقة بالاعتداء على نظم المعالجة الآلية. وتعد عملية فحص البرمجيات نموذجاً عملياً لهذه الإجراءات، حيث تُستخدم كوسيلة رئيسية لكشف وجود برامج غير معتمدة تعمل في البيئات الرقمية بشكل غير قانوني أو تسهم في تحقيق أهداف غير مشروعة، مثل برمجيات المسح المصممة للكشف عن الثغرات أو "الأبواب المفتوحة" في الأنظمة. وتُعد هذه البرمجيات دليلاً واحتمالاً قوياً على ارتكاب جريمة الدخول غير المشروع إلى نظام المعالجة الآلية، خاصة إذا ما اقترنت باعتراف شفهي يؤكد تورط الشخص في هذا الفعل الجُرمي.

حيث أجاز المشرع الجزائري تفتيش المعطيات المعلوماتية وذلك بموجب المادة 05 من القانون رقم 09-04 السالف الذكر، وقد أجازت هذه المادة للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من نفس القانون التي من بينها توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني وللوقاية من هذه الجرائم الدخول بعرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المحزنة فيها وكذا منظومة تخزين المعطيات[1].

تفتيش المنظومة المعلوماتية عن بعد في الجرائم الإلكترونية.

إن التفتيش في نطاق الجرائم الالكترونية لا يخرج عن إحدى الحالتين:

[1]- دلال مولاي ملياني، المرجع السابق، ص 218.

حالة جهاز متصل بجهاز المتهم داخل الدولة.

تتمثل المشكلة في هذه الحالة عندما تقوم سلطة التحقيق بتفتيش جهاز متصل بجهاز المتهم ويقع داخل الدولة وكذا تجاوز الاختصاص المكاني لسلطة التحقيق من ناحية والاعتداء على خصوصيات الغير من ناحية أخرى[1]، ونظرا لوجود قصور في نصوص قانون إ.ج.ج لسنة 2006 تم مواجهة هذا القصور بأن سمح للسلطات القضائية المختصة تمديد التفتيش عن المعطيات المبحوث عنها بسرعة إلى أي منظومة معلوماتية أو جزء منها تقع داخل الإقليم الوطني وهذا ما نصت عليه الفقرة الثانية من المادة 05 من القانون رقم 09-04 وما يدخل ضمن نطاق الاستعجال في تمديد الاختصاص خوفا من العبث بالأدلة الرقمية[2].

حالة جهاز متصل بجهاز المتهم خارج الدولة.

في هذه الحالة فإن الإشكالية تثار بصورة أكبر في حالة أن يكون الجهاز المطلوب تفتيشه والمتصل بجهاز المتهم بنهاية طرفيه يقع خارج الدولة ففي الغالب يعمد مرتكبي الجرائم الإلكترونية إلى تخزين البيانات الخاصة بهم والتي تعد أدلة لإدانتهم في جرائم تم ارتكابها من قبلهم خارج الدولة[3]، وبالنسبة للقانون الجزائري فقد تلافي مشكلة التفتيش عن بعد خارج الإقليم الوطني بموجب الفقرة الثالثة من المادة 05 من القانون 09-04 التي نصت على أنه إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن

[1]- فاير محمود راجع غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، كلية الحقوق جامعة الجزائر 1، 2010/2009، ص 312.

[2]- دلال مولاي ملياني، المرجع السابق، ص 219.

[3]- فايز محمود راجع غلاب، المرجع السابق، ص 314.

الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[1].

شروط التفتيش في الجرائم الالكترونية :

القواعد الموضوعية للتفتيش: وتتضمن عدة شروط وهي:

– 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 أمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة.

– أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به .

القواعد الشكلية للتفتيش:

– أن يتم التفتيش بأسلوب إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة.

– أن يكون أمر التفتيش مسببا أي يجب أن يتضمن الاسباب التي أدت إلى إجراءه.

– تكوين فريق التفتيش يجب أن يتضمن خبراء مسرح الجريمة من الفنيين والمختصين في مجال الحاسوب والأنظمة الالكترونية وبالإضافة الى رجال الشرطة وأن يتكون الفريق

[1]- لفقرة الثالثة من المادة 05 من القانون 09-04 السابق ذكره.

من المشرف على التحقيق، فريق التفتيش العملي من خبراء الحاسوب، فريق الأمن والحماية من رجال الشرطة[1].

الفرع الثاني: الضبط والحجز في الجرائم الالكترونية.

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[2].

حيث نظم المشرع الجزائري الضبط في المادة 06 من القانون 09-04 والتي تتمكن من خلالها السلطة التي تباشر التفتيش من ضبط أو حجز المعطيات تكون مفيدة في كشف الجرائم أو مرتكبيها[3].

والضبط يعني وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبيها[4].

أ. إجراءات الضبط في الجريمة الالكترونية.

نص المشرع الجزائري على حجز المعطيات في المواد 06 إلى 09 من القانون 04-09 فوفقا للمادة 06 عندما تكتشف السلطة التي تباشر التفتيش معطيات تفيد في كشف الجرائم أو مرتكبيها يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية

[1]- خالد حياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2011، ص 154-155.

[2]- دلال مولاي ملياني، المرجع السابق، ص 228.

[3]-خضرة شنتير، المرجع السابق، ص 101.

[4]- خالد عياد الحلبي، المرجع السابق، ص 168.

تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون إ. ج. ج وإذا استحال الحجز لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات أو نسخها ويجب عليها السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية[1].

ب. صعوبات عملية حجز البيانات المعالجة الكترونيا:

– حجم الشبكة التي تحتوي على المعلومات المعالجة الكترونيا والمطلوب ضبطها من ذلك البحث في نظام الكترونى 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[2].

ولضمان الحفاظ على البيانات محل البحث ومقارنتها بالنسخة المخرجة من الجهاز في حالة بحدها من المتهم فقد أعطى القانون البلجيكي للنيابة العامة سلطة الأمر بغلق هذه

البيانات لمنع الوصول إليها أو إلى النسخة المستخرجة منها لدى من يستعملون النظام[3].

[1]- صالح شنين، إجراءات التحري والتحقيق في جرائم تكنولوجيا الاعلام والاتصال في التشريع الجزائري، مجلة الدراسات القانونية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، العدد 01، ص 283.

[2]- منير محمد الجنبيهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات، ط1، دار الفكر الجامعي، الاسكندرية، 2018، ص 116.

[3]-خضرة شنتير، المرجع السابق، ص 64.

الفرع الثالث: المراقبة الالكترونية للاتصالات في الجرائم الالكترونية.

تتمثل المراقبة في كشف الجرائم قبل وقوعها وتلعب دورا كبيرا في الكشف عن الجرائم الالكترونية وهي وسيلة هامة من وسائل الإرشاد الجنائي، ويقصد به المراقبة الأمنية التي محلها الاتصالات الالكترونية التي عرفها المشرع الجزائري في إطار القانون 04-09 وهي التي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية[1].

وقد استعمل المشرع الجزائري مصطلح مراقبة الاتصالات الالكترونية بالرغم أن معظم أحكام قانون 09-04 هي مستمدة من اتفاقية بودابست والتي استخدمت مصطلح اعتراض معطيات المحتوى[2].

أ. محل مراقبة الاتصالات الالكترونية.

إن محل المراقبة هو ذلك الهدف الذي تتم مراقبته وتتبع حكاته وتصرفاته في نطاق المراقبة الالكترونية محل المراقبة هو الحاسوب الرقمي أو الموقع عبر شبكة الأنترنت أو البريد الالكتروني بما يحتويه من مراسلات الكرتونية 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 عرفتها المادة الثانية من القانون 09-04، 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

[1]- المادة (02) من القانون 09-04، المرجع السابق.

[2]- دلال مولاي ملياني، المرجع السابق، ص 209.

هي كل المعطيات المعالجة باستثناء ما تعلق بمعطيات المرور، فمعطيات المحتوى هي محل المراقبة الالكترونية ذلك بأن أدرجها المشرع في المادة الرابعة من القانون 09-04 أما معطيات المرور فقد خصها المشرع بإجراء حفظ المعطيات المتعلقة بحركة السير المادة 11 من القانون 09-04.

أ. 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[1]

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 جسدته المادة الثالثة من القانون السالف الذكر[2]، بالإضافة إلى التقيد بالغرض المرجو من المراقبة حيث أنه قبل اللجوء إلى المراقبة لابد من وجود دلائل على إمكانية وقوع الجريمة أو وجودها بالفعل على أن تكون هناك وقائع فعلا منسوبة إلى 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

1- دلال مولاي ملياني، المرجع السابق، ص 210-211.

2- المادة 3 من القانون 09-04، المرجع السابق.

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[1] .

الشروط الخاصة:

– الإذن المكتوب إذ لا يجوز إجراء المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة وهو الشرط المشترك بين جميع الجرائم التي يمكن اللجوء فيها لإجراء المراقبة كأسلوب وقائي إذا تعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة أو كإجراء قضائي إذا تعلق الأمر بالاعتداء على منظومة معلوماتية تهدد النظام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات والتحقيقات القضائية التي لا يمكن المتابعة فيها إلا عبر اللجوء الى المراقبة الالكترونية أو في إطار تنفيذ طلبات المساعدة القضائية الدولية.

– مدة الإجراء الشرط الثاني وهو تحديد المدة المتعلقة بالجرائم المتعلقة بالإرهاب والتخريب والماسة بأمن الدولة بستة أشهر قابلة للتجديد وهو الشرط الذي استثنى باقي حالات مراقبة الاتصالات الإلكترونية كما جعل المشرع النائب العام لدى مجلس قضاء الجزائر مختصا يمنح ضباط الشرطة القضائية المنتمون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته الإذن بإجراء مراقبة الاتصالات[2].

[1]- دلال مولاي ملياني، المرجع السابق، ص 211.
[2]- المادة 04 والمادة 13 من القانون 09-04، المرجع السابق.

المطلب الثاني: أساليب البحث التحري في ظل قانون الإجراءات الجزائية (الحديثة).

نظرا لخطورة الجريمة الالكترونية وصعوبة اكتشاف المجرم الالكتروني وإيجاد الآلية المناسبة للتحقيق التقليدي، قام المشرع الجزائري باستحداث آليات تحقيق خاصة بموجب قانون الإجراءات الجزائية الجديد المعدل والمتمم بالقانون 06-22[1] وهي التسرب أو الاختراق الإلكتروني واعتراض المراسلات وتسجيل الأصوات، هذا ما سنتناوله في هذا المطلب.

الفرع الأول: اعتراض المراسلات السلكية واللاسلكية.

استحدث المشرع الجزائري بموجب القانون رقم 06-22 المؤرخ في 20/12/2006 المعدل والمتمم لقانون الإجراءات الجزائية من خلال الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وقد ضمنه ستة مواد من المادة 65 مكرر الى المادة 65 مكرر 10 وتناول من خلالها المقصود بهذا الإجراء وضمانات استخدامه.

أ. مفهوم إجراء اعتراض المراسلات السلكية واللا سلكية:

ومن خلال نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية نجد أن المشرع الجزائري يقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللا سلكية، وهذه المراسلات هي عبارة عن

[1]- فلاح عبد القادر،أيت عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، المجلد 4 العدد 2، 2019، ص 1699.

بيانات قابلة للإنتاج والتوزيع التحرين الاستقبال والعرض[1]، حيث استثنى المراسلات الالكترونية لأنه يمكن أن تتم خارج النطاق السلكي واللا سلكي وقد أفرد لها مواد قانونية خاصة في إطار القانون 09-04 لمراقبة الاتصالات الالكترونية مما لا يدعو للشك أن المراسلات المقصودة هنا هي المتعلقة بالهاتف الثابت والنقال ولكن بعد رقمنة كل وسائل الاتصال والاعلام يعصب التفرقة بين ما هو رقمي وما هو غير ذلك، لذلك وعلى هذا الأساس جمع المشرع كل الاتصالات في خندق واحد بموجب المادة 5 من المرسوم رقم 15-261.[2]

واعتراض المراسلات هو نوع من أنواع المراقبة الالكترونية، وهو القيام باعتراض كل المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللا سلكية التي يقصد بها التنصت التليفوني.

ب. الشروط والضمانات المقررة لاعتراض المراسلات السلكية واللا سلكية.

مما لا شك فيه أن أسلوب اعتراض المراسلات السلكية واللاسلكية دون علم أصحابها بقدر ما يفيد في كشف الحقيقة ويسهل إثبات كثير من الجرائم الغامضة كتلك المتعلقة بالجرائم المعلوماتية، فهو من جانب آخر يمثل انتهاكا لحرمة الحياة الخاصة للأفراد واعتداء على سرية مراسلاتهم واتصالاتهم التي كفلتها الدساتير والتشريعات العقابية، والمشرع الجزائري في هذا الصدد أعطى لسلطات البحث والتحري امكانية اعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل[3]، لكن بشروط وتتمثل هذه الشروط في :

[1]- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة مقدمة لنيل شهادة الماستر تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج الحضر، باتنة، الجزائر، 2012/2013، ص 177-178.

[2]- دلال مولاي ملياني، المرجع السابق، ص 179.

[3]- نعيم سعيداني، المرجع السابق، ص 179.

1. ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ: طبقا للمادة 65 مكرر 5 من قانون الإجراءات الجنائية 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 ضمانة لازمة لمشروعية هذا الإجراء.

2. تحديد طبيعة المراسلة ومدة الاعتراض: وهذا ما يفهم صراحة من نص المادة 65 مكرر 7 التي نصت على أنه يجب أن يتضمن الإذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصالات أو المراسلات المطلوب اعتراضها، كما أن المشرع قد استوجب ألا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا لمقتضيات التحري والتحقيق وهي نفس المدة التي حددها المشرع الفرنسي في المادة 100 من قانون الإجراءات الجزائية الفرنسي.

2. طرق اعتراض المراسلات الإلكترونية.

يعتبر البريد الالكتروني أهم وسيلة تقنية في مجال التراسل الإلكتروني ومن ثم فعملية الاعتراض تنصب عليه، ومن المعلوم أن كل رسالة الكترونية يظهر فيها معلومات عامة مثل تاريخ إنشاء الرسالة وتاريخ تلقيها وكذا عنوان المرسل وعنوان المرسل إليه ولكن هذه المعلومات ليست كافية لمعرفة المرسل إذ بإمكان هذا الأخير إطلاق رسالته من صناديق بريد مسجلة بأسماء وهمية، كما أن هناك وسائل تتيح للمرسل أن يرسل رسالته دون أن يظهر فيها عنوان بريده الالكتروني الصحيح لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية رسائل البريد الالكتروني والتي يطلق عليها مصطلح Email-Header وهي أول خطوة للبدء في البحث والتحري عن مرسل الرسالة الإلكترونية وهذه الحاشية لا تظهر بصورة مباشرة وإنما يتطلب الأمر من المستخدم إجراء بعض الخطوات للحصول عليها أو من خلال IP يمكن من خلالها

الاستدلال على صاحب الرسالة ويصبح بعد ذلك من السهل الحصول على المزيد من المعلومات عن المرسل وذلك بإدخال رقم IP في بعض المواقع التي يقوم بالكشف عن مصدر الرسالة والمكان الجغرافي الذي أرسلت منه وكذا مزود الخدمة الذي يتعامل معه مرسل الرسالة ويكون بذلك من السهل تمام اعتراض هذه المراسلات والاطلاع على محتواها دون علم مرسلها[1].

الفرع الثاني: تسجيل الأصوات والتقاط الصور.

أولا: التسجيل الصوتي:

ثاني إجراء من الإجراءات الخاصة التي سنها المشرع الجزائري إجراء التسجيل الصوتي الذي يتم فيه اللجوء إليه بالإضافة إلى شرط للجرائم الخاصة لابد من شروط معينة.

أ. مفهوم التسجيل الصوتي:

التسجيل الصوتي يشمل تسجيل الأحاديث الشخصية وتسجيل الأصوات، فالحديث عبارة عن كل صوت له دلالة التعبير عن مجموعة من المعاني والأفكار[2]، 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 المعنى، أما تسجيل الصوت فهو إفراغ الأحاديث الخاصة في وعاء يحفظها مخصص لإعادة سماعها في وقت لاحق ونقله من مكان لآخر[3]، وهو التعريف المرتبط باعتراض المراسلات باعتبار أنه لا يمكن اعتراض

[1]- نعيم سعيداني، المرجع السابق، ص 181-182.

[2]- علي أحمد عبد الزغبي، المرجع السابق، ص 264.

[3]- دلال مولاي ملياني، المرجع السابق، ص 183.

هذا الأخير دون تسجيل[1]، 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[2].

ب. معيار إضفاء صفة الخصوصية على الأحاديث.

الأحاديث نوعان أحاديث عامة وهي التي لا حظر على مراقبتها بحيث يجوز مراقبتها دون شرط، والأحاديث الخاصة هي التي تحظر التشريعات مراقبتها إلا بتوافر ضمانات معينة منصوص عليها قانونا.

1. موقف الفقه

فالبعض اعتمد المعيار الشخصي أي موضوع الحديث ذاته والبعض الآخر أخذ بالمعيار الموضوعي أي طبيعة المكان الذي يدور فيه الحديث.

المعيار الشخصي (طبيعة الحديث)

ذهب أنصار هذا الاتجاه الى الاعتداد بموضوع الحديث ذاته كمعيار للتفرقة بين الحديث العام والحديث الخاص المباشر، فالعبرة هنا ليس بخصوصية المكان أو عمومه وإنما بخصوصية الحديث أي يقصد ذوي الشأن، وهذا القصد يستشف من موضوع الحديث ومن هيئة المتحدثين ودرجة علو صوتهم.

[1]- أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، رسالة لنيل شهادة الماجستير تخصص قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، الجزائر 2014-2015، ص 60.

[2]- دلال مولاي ملياني ، المرجع السابق، ص 183.

المعيار الموضوعي (طبيعة المكان)

ذهب أنصار هذا الاتجاه أنه يجب الأخذ بطبيعة المكان الذي يدور فيه الحديث كمعيار للتفرقة، حيث يتخذ من مكان حدوثه قرينة على طبيعة وبالتالي يعتبر الحديث عاما إذا جرى في مكان عام متاح لكل من يرغب أن يستمع لما يدور فيه ويكون الحديث خاصا إذا ما تم في مكان خاص[1].

2. موقف المشرع الجزائري

بالرجوع إلى 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"[2]، يلاحظ أن المشرع الجزائري قد مسح هذه المسألة وأخذ بالمعيار الشخصي أي بالطريقة التي يتم بموجبها تبادل أطراف الحديث وليس بالمعيار الموضوعي أي المكان الذي يوجد فيه الشخص.

ثانيا: التقاط الصور

أ. تعريف التقاط الصور: التقاط الصور عن طريق وضع الترتيبات والمعدات التقنية اللازمة دون أخذ موافقة[3]، ويقصد بإجراء التقاط الصور تثبيت الصور على مادة حساسة وتثبيت الصورة

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

[1]- أمينة ركاب، المرجع السابق، ص 63-64.
[2]- المادة 65 مكرر الفقرة 03 من قانون الإجراءات الجزائية.
[3]- دلال مولاي ملياني، المرجع السابق، من 186.

الوضعية التي كانوا عليها وقت التصوير، وهي تربط الزمان والمكان والأشخاص في وقت واحد وقد تمتد الى الدليل المادي للجريمة والى محيطها[1].

ب. معيار التقاط الصور

وكحال التسجيل الصوتي اختلف الفقه في تحديد طبيعة المكان الخاص الذي يدخل التقاط الصور ضمن التجريم والإباحة.

1. موقف الفقه

المعيار الموضوعي (معيار طبيعة المكان)

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.[2]

المعيار الشخصي (معيار حالة الأشخاص)

يأخذ أنصار هذا الرأي بحالة الخصوصية لا بطبيعة المكان لتحديد مدلول المكان الخاص فحسب رأيهم فإن الوضع الذي عليه الاشخاص هو الذي يصبغ ويحدد ما إذا يعتبر المكان خاصا أولا وعليه متى توافرت حالة الخصوصية فإن المكان يعد خاصاً ويعتبر المكان عاما حتى انتقلت حالة الخصوصية.

[1]- أمينة ركاب، المرجع السابق، ص 66.
[2]- دلال مولاي ملياني، المرجع السابق، ص 187.

2. موقف المشرع الجزائري

من خلال الرجوع إلى نص المادة 65 مكرر 5 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 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 إلى الأماكن الخاصة التي تعد مستودعات أسرار المعنيين بالمراقبة في سبيل اكتشاف الحقيقة واستبيان المجرم[1]

الفرع الثالث: التسرب أو الاختراق

التسرب يُعد إحدى التقنيات المستحدثة التي تنطوي على درجة عالية من الخطورة في مجال أمن الضبطية القضائية، ويتطلب تنفيذه مستوى عاليًا من الجرأة والكفاءة والدقة في العمل. وقد قام المشرع الجزائري بإدراج هذه التقنية ضمن التعديلات التشريعية التي طرأت على قانون الإجراءات الجزائية في عام 2006. بناءً على ذلك، سوف نسعى في هذه الدراسة إلى تناول مفهوم التسرب بشكل منهجي وتوضيح الشروط التي تحكم تطبيقه لضمان الامتثال للقواعد القانونية وتحقيق أهدافه المرجوة.

أولا: تعريف التسرب

يعرفه البعض بأنه تقنية من تقنيات البحث والتحري الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم وكشف

[1]- أمينة ركاب، المرجع السابق، ص 68.

أنشطتهم الإجرامية وذلك بإخفاء الهوية الحقيقية ولتقديم المتسرب لنفسه على أنه فاعل أو شريك[1].

ويعرف البعض بأنه أكثر رسائل التحري تعقيدا وخطورة لأنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بمناورات وتصرفات توحي بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة ولكنه في حقيقة الأمر يخدعهم ويتحايل عليهم فقط، ويوهمهم بأنه فاعل وشريك لهم وذلك حتى يطلع على أسرارهم من الداخل ويجمع ما يستطيع من أدلة إثبات ويبلغ السلطات بذلك فتتمكن من ضبط المجرمين ووضع حد للجريمة[2]

وتعرفه المادة 65 مكرر 12 بأنه: " قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"[3].

ويلاحظ أن المشرع الجزائري قد عرف التسرب على غير العادة والتي أصبحت – أي تعريف المصطلحات في نص قانوني –قواعد أرساها المشرع في ظل تطور التقنية حيث يلجأ الى عملية التسرب في جرائم خاصة دون سواها والمتضمنة جرائم الأنترنت[4]، وما يلاحظ أن المشرع الجزائري قد استعمل مصطلح التسرب في قانون إ. ج ومصطلح الاختراق في قانون مكافحة الفساد.

[1]- عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية، ط1، دار الهدى، الجزائر، 2012، ص 74-75.
[2]- وردة شرف الدين، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية، مجلة الفكرة، جامعة محمد خيضر بسكرة، الجزائر، العدد 15، 15 جوان 2017، ص 545.
[3]- دلال مولاي ملياني، المرجع السابق، من 195.
[4]- المادة 65 مكرر 12 الفقرة 02 من قانون الإجراءات الجزائية

ثانيا: شروط التسرب

حتى يكون التسرب ناجحة ونتائجها مقبولة كأدلة أمام القضاء فرض لها المشرع مجموعة من الشروط والتي إذا لم تتوفر لا يمكن اللجوء الى عملية التسرب أساسا، فبحسب المادة 65 مكرر 11 يمكن القيام بالتسرب إذا اقتضت ذلك ضرورات التحري أو التحقيق في إحدى الجرائم المبينة في المادة 65 مكرر 5 من قانون إ.ج والتي عمدت الجرائم على سبيل الحصر[1] في الجرائم المتلبس بها أو التحقيق الابتدائي في جرائم محددة وهي جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أو جرائم تبييض الأموال أو جرائم الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد[2].

وعلى اعتبار الجريمة الإلكترونية إحدى تلك الجرائم التي نصت عليها المادة السالفة الذكر فالتسرب فيها جائز إذا فرضت ذلك ضرورة التحقيق والتحري وأثبتت الجهة القائمة بالتسرب عدم نجاعة الاساليب العادية للتحقيق والتحري في جمع الأدلة خاصة الالكترونية، ويجب الحصول على إذن من طرف وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية حسب الأحوال مسلم إلى جهة مختصة متمثلة في ضباط الشرطة القضائية، فلا يمكن بأي حال من الأحوال مباشرة عملية التسرب والكشف عن الجرائم السالفة الذكر إلا بعد الحصول على إذن من وكيل الجمهورية المختص إقليميا أو قاضي التحقيق بعد إخطار وكيل الجمهورية[3]، يجب أن يكون الإذن المسلم مكتوب ومسببا 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

[1]- وردة شرف الدين، المرجع السابق، ص 546.

[2]- خضرة شنتير، المرجع السابق، ص 135.

[3]- دلال مولاي ملياني، المرجع السابق، ص 200.

التي لا يمكن أن تتجاوز أربعة (04) 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[1].

[1]- وردة شرف الدين، المرجع السابق، من 546.

المبحث الثاني: مشروعية أساليب البحث والتحري والجرائم الالكترونية

المطلب الأول: موقف المشرع الجزائري من إجراءات البحث والتحري عن الجريمة الالكترونية.

الفرع الأول: الجدل الفكري حول مشروعية أساليب البحث والتحري الخاصة بالجريمة الالكترونية.

يُعَدُّ استخدام أساليب البحث والتحري المتعلقة بالجرائم الإلكترونية من القضايا التي أثارت جدلاً حول مشروعيتها، حيث انقسم الفقه بين مؤيد ومعارض لاستخدام التكنولوجيا الحديثة وفقًا لما يلي:

أ-الرأي المعارض

فقد انتقد المعارضون بشدة أساليب البحث والتحري الخاصة وذلك من وجهين:

أ-1-من حيث حجيتها:

فهي وسائل غير مضمونة لأنها لا تعكس دائما الحقيقة، نظرا لإمكانية تغيير أو حذف أي مقاطع أو صور عن بعضها البعض، أو على العكس من ذلك تركيبها بشكل يغير الحقيقة، وينطبق هذا الأمر على الصوت والصورة.

أ-2-من حيث مشروعيتها:

يقضي دستور (1996) في المادة 39 منه " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة."

كما يقضي قانون العقوبات بحرمة الرسائل البريدية والبرقيات ويعاقب على فضها أو تسهيل ذلك، كما يجرم ويعاقب على المساس بحرمة الحياة الخاصة للمواطن فيما يتعلق بالمكالمات والصور من خلال المواد: المادة 137 (قانون رقم 06-23 مؤرخ في 20 ديسمبر 2006)، المادة 303 (قانون 06-23 مؤرخ في 20 ديسمبر 2006)، المادة 303 مكرر (قانون 06-23مؤرخ في 20 ديسمبر 2006).[1]

لذا يرى بعض الفقهاء أن الاتحاد الجديد للسياسة الجنائية التي جاء بها المشرع الجزائري بموجب القانون رقم 06-22 المعدل والمتسم القانون الإجراءات الجزائية لم يوازن بين حماية الصالح العام وحق الأفراد في احترام حياتهم الخاصة وهذا ما جسدته السلطات الواسعة المفتوحة الضباط الشرطة القضائية تحت غطاء مقتضيات التحري والتحقيق التي تتضمن مساسا صارخا لحقوق الأفراد يقدم له من الجريمة وحرياتهم الشخصية المكفولة حمايتها دستوريا، لقد اهتم المشرّع بوضع جميع القوانين والإجراءات اللازمة لضمان تنفيذ المهمة بأفضل صورة ممكنة. إلا أنه لم يولِ اهتماماً كافياً للإنسان الذي تُهدَر حقوقه بعد إثبات براءته. لذا كان من الأجدر أن يتضمن التشريع نصوصاً تضمن تعويضاً ينسجم مع حجم الأضرار التي لحقت به، مع التأكيد على أن أي تعويض يُقدّم له يجب أن يكون كافياً لإنصافه وتحقيق العدالة له.

ب-الرأي المؤيد:

ويرى المؤيدون أن الفائدة العملية والعلمية لهذه الوسائل جعل الكثير من التشريعات تعتمد عليها في سبيل الكشف عن الجريمة والبحث عن المجرمين بل اعتمد على هذه الوسائل حتى الدول التي تتغنى بحماية حقوق الإنسان، ونادت بضرورة استخدامها الاتفاقيات الدولية في ظل التطورات الخطيرة التي يشهدها الإجرام المنظم وجرائم المخدرات وتبييض الأموال والفساد وغيرها، والجزائر ليست في منأى عن هذا التطور

[1]- وردة شرف الدين، المرجع السابق، من 546.

الحاصل في مفهوم الجريمة وفي سبيل الوقاية بالطرق المستحدثة. ولكن لا بد من تأطير هذه الإجراءات ووضع الآليات اللازمة لتطبيقها، مع إعطاء ضمانات كافية بغية احترام الحريات الفردية وحقوق الإنسان مع جعلها تتم تحت إشراف القضاء وسلطته، مع تطبيق مجال تطبيقها[1].

وبالرجوع إلى الاتفاقيات الدولية الخاصة بحقوق الإنسان، ورغم حرصها على الحفاظ وعدم المساس بالحقوق الخاصة بالفرد كسرية مراسلاته ومكالماته الهاتفية وحرية التعبير بأي وسيلة كانت إلا أنها نصت من جانب آخر على مجموعة من الشروط والضمانات يمكن للسلطات القضائية للدول الأعضاء بموجب قوانينها الداخلية مراعاتها عند تقرير بعض الإجراءات للتحري والتحقيق إذا كانت الجرائم المرتكبة تمس بالنظام العام والأمن القومي والاقتصاد الوطني، ونفس النهج انتهجته اتفاقية بودابيست لمكافحة جرائم المعلوماتية، إذ الزمت المادة 15 الدول الأعضاء أن تضمن حماية كافية لحقوق الإنسان وحرياته وعلى الخصوص الحقوق الناشئة عن الالتزامات التي تعهدت بها في ظل الاتفاقيات الدولية لحقوق الإنسان المنظمة إليها، ومن جهة أخرى، وضعت هذه المادة مجموعة من الشروط والضمانات تقتضي على السلطات القضائية الداخلية للدول الأعضاء مراعاتها عند تقرير الإجراء المعني بشأنه.

كما أن التعديل الدستور الجزائري في 2016 نص في المادة 46 على أنه: ''لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر مغلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم. حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه''.

[1]- وردة شرف الدين، المرجع السابق، من 546.

وبإسقاط ما سبق بيانه على التشريع الجزائري لا سيما قانون الإجراءات الجزائية وقانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يمكننا القول بأن المشرع عند تقريره لإجراءات حديثة للتحري عن بعض الجرائم ومنها المعلوماتية، نظرا لثبوت عدم كفاية الإجراءات التقليدية لمكافحة هذا النوع المستحدث من الإجرام. كمراقبة الأشخاص والأشياء والأموال اعتراض المراسلات والتقاط الصور وتسجيل الأصوات. والتسرب والمراقبة الإلكترونية نقول انه حاول إمساك مسطرة العدالة من النصف بحيث أراد الحفاظ على حق الجماعة في توقيع العقاب وعدم إفلات المجرمين منه ومن الجهة الأخرى قرر مجموعة من الضمانات والشروط التي يجب إتباعها من قبل الضبطية القضائية عند التحري عن الجرائم للحفاظ على الحرية الفردية إزاء هذه الإجراءات مما أضفى على هذه الإجراءات الخاصة والحديثة طابع المشروعية.

الفرع الثاني: ضوابط مشروعية أساليب البحث والتحري.

تنقسم هذه الضوابط إلى قسمين: ضوابط موضوعية وضوابط شكلية.

أولا: الضوابط الموضوعية: تتمثل الضوابط الموضوعية فيما يلي:

أ. أن تتعلق بفئة معينة من الجرائم

لا يرخص بأساليب التحري الخالصة إلا بالنسبة للجرائم المحددة حصرا في القانون حيث أن المشرع الجزائري اشترط لمشروعية هذه الأساليب ولضمان عدم التعدي على حقوق الاشخاص أن يتعلق الأمر بالجرائم المحصورة في ثمانية فئات السالفة الذكر والتي نصت عليها المادة 65 مكرر 5 من قانون الإجراءات الجزائية[1].

[1]- عبد الرحمان خلفي، المرجع السابق، ص 70.

ويشترط لصحة إذن القاضي المختص أن يذكر في الإذن الجريمة التي تبرر اللجوء الى اتخاذ إحدى هذه التدابير حيث نصت المادة 65 مكرر 7 من قانون الإجراءات الجزائية على أنه يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 اعلام الجريمة التي تبرر اللجوء إلى هذه التدابير وقد جاء هذا النص بصيغة الوجوب، مما جعل كل إذن لا يتضمن الإشارة الى الجريمة المعاقب عليها إذنا باطلا لا يعتدي به.

ب. الإشراف القضائي على أساليب البحث والتحري

السلطة الوحيدة المؤهلة للإذن بالأساليب الخاصة هو وكيل الجمهورية يعتبر المؤهل الوحيد 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 أساليب التحري من تلقاء نفسه ودون إذن مسبق من وكيل الجمهورية، والفقه والقضاء متفقان على أن هذه الإجراءات محظورة على ضابط الشرطة القضائية دون الاذن له بذلك حتى ولو تعلق الأمر بحالة التلبس بالجريمة، ويمتنع على ضابط الشرطة القضائية أن يندب غيره للقيام بإحدى الأساليب الخاصة لأن الندب لا يكون إلا من طرف وكيل الجمهورية.[1]

ج. أن يكون الأساليب 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 أن أساليب التحري إجراءات استثنائية تمليها الضرورة تتضمن اعتداء جسيما على حرمة الحياة الخاصة للأفراد ولا نتاج إلا استثناء وللفائدة المنظرة منها والتي تتعلق بكشف غموض الجريمة أو

[1]- عبد الرحمان خلفي، المرجع السابق، ص 70.

العمل على ضبط الجناة[1]، لذلك يجب أن تفشل جميع وسائل البحث والتحري التقليدية في كشف هوية الجناة وضبطهم وفي حالة ما إذا ظهر عدم ضرورة الأساليب الخاصة لكشف الحقيقة أضحت غير مشروعة مما يترتب عليه بطلان الدليل المستمد منها وتقدير هذه الضرورة في مرحلة التحري متروك لسلطة وكيل الجمهورية تحت رقابة محكمة الموضوع وفقا لظروف كل جريمة[2].

ثانيا: الضوابط الشكلية

تتمثل الضوابط الشكلية فيما يلي:

أ. أن يكون المندوب ضابط شرطة قضائية مختص

يجب أن يكون الشخص المندوب ضابط شرطة قضائية مختص محليا ونوعيا فلا يجوز ندب عون ضبطية فضائية لانتقاء صفة الضبطية القضائية عنه، أو ندب ضابط شرطة قضائية غير مختص محليا، ويطرح التساؤل حول مدى شرعية الإجراء الذي يتم من طرف الضحية نفسه، فهل يأخذ بالدليل المستقى من هذا الإجراء في هذه الحالة أم لا؟

يرى البعض أن التسجيلات التي تتم من طرف الأفراد فيما بينهم لا تعد من قبل الإجراءات الجنائية مما تتضمنه من أقوال أو تصريحات لا تعد اعترافا كونها لم تصدر في خصومة جنائية أمام إحدى السلطات، بل تطبق عليها أحكام ما يقدمها الأفراد من

[1]-عبد الرشيد معمري، ضوابط مشروعية أساليب التحري الخاصة المجلة الأكاديمية للبحث القانوني، جامعة خنشلة، 2015، العدد 1، ص 473-475.

[2]-محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق، جامعة عين الشمس، مصر، 2011، ص 113.

أشياء مادية لتأييد ادعاءاتهم، يورى البعض الآخر أن المحادثات الهاتفية التي تنطوي في ذاتها على وقوع الجريمة لا تصلح في ذاتها لتكون محلا لحق يحميه القانون[1].

ب. صدور الإذن من وكيل الجمهورية المختص محليا

يجب أن يكون وكيل الجمهورية ذا اختصاص محلي وفقًا للقواعد العامة للاختصاص المحلي الواردة في المادة 29 من قانون الإجراءات الجزائية، بالإضافة إلى الالتزام بالقواعد الخاصة المتعلقة بتمديد اختصاصه المحلي. يتضمن ذلك تمديد نطاق اختصاصه إلى دائرة اختصاص محاكم أخرى، وذلك استنادًا إلى المرسوم التنفيذي رقم 06/348 الصادر بتاريخ 8 أكتوبر 2006، وكذلك المادة 40 الفقرة الثانية من قانون الإجراءات الجزائية.

وتثير مسألة التصنت الهاتفي على المكالمات الهاتفية التي تتم في الخارج مشكلة في الاختصاص المحلي، فهل يجوز الاعتراض عليها من داخل الإقليم الوطني؟ في فرنسا لا يمكن أن يؤذن بالاعتراض على الخط الهاتفي موجود في الخارج، إلا في حالة ما إذا مرت مراسلات محل الاعتراض بمراكز عبور دولية موجودة في فرنسا[2].

ج. تسبيب الإذن

أساليب التحري تمس بحرمة الحياة الخاصة لذا يستوجب تسبيب الإذن المرخص بها حتى تكون صحيحة رغم عدم اشتراط المشرع لهذا التسبيب، فالإذن يجب أن يكون محددا للأسباب التي كانت وراء إصداره أي تحديد عناصر الربط بين إذن الاعتراض والتسجيل والتصوير والجريمة[3].

[1]-محمد أمين الخرشة، المرجع السابق، ص 116.

[2]-عبد الرشيد معمري، المرجع السابق، ص 477.

[3]-محمد أمين خرشة، المرجع السابق، ص 87.

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 كتحديد 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[1]، فالدخول مسموح به خارج المواعيد المحددة في المادة 47 الفقرة الأولى من قانون إ.ج أي أن الدخول إلى هذه الأماكن جائز ليلا ونهارا ولا يحتاج الأمر إلى إصدار إذن مسبق بالدخول حسب القانون الجزائري كما لا يحتاج الدخول الى رضا وعلم الأشخاص الذين لهم حق الأماكن (مادة 65مكرر 5 من قانون إ.ج) كون أساليب الاعتراض والتسجيل والالتقاط تتم في سرية وخلسة 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.

هـ. تحديد مدة أساليب التحري

من ضمانات حماية الحرية الشخصية والحفاظ على راحة وأمن واطمئنان الأشخاص تحديد مدة زمنية للقيام بالإجراءات الخاصة فلا يمكن إطلاق مدتها دون تجديد.

[1]-فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الانسانية، جامعة منتوري قسنطينة، الجزائر، عدد 33 2010، ص 254.

وقد 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 أحسابها 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[1].

الفرع الثالث: نطاق تطبيق أساليب البحث والتحري في التشريع الجزائري

يتم إعمال أساليب التحري الخاصة من قبل الشرطة القضائية بخصوص التحقيق في حالات مختلفة نصت عليها المادة 65 مكرر 5 من قانون الإجراءات الجزائية، حيث تشمل حالة التلبس بالجريمة والتحقيق التمهيدي في جرائم معينة بالإضافة إلى الإنابة القضائية، وسنقتصر في دراستنا لهذا الموضوع على الحالة الأولى والثانية باعتبار أن الإنابة القضائية تتعلق بمرحلة التحقيق القضائي[2]

أولا: حالة التلبس بالجريمة

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

[1]-عبد الرشيد معمري، المرجع السابق، ص 479.480.

[2]-حاج أحمد عبد الله، أساليب التحري الخاصة وحجيتها في الإثبات الجنائي مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة أدرار، المجلد 8، العدد 05، 2019، ص 347.

أ. ارتكاب الجريمة في الحال:

والمقصود من ذلك مشاهدة الجناية أو الجنحة أثناء وقوعها وفي وقت اقترافها، والمشاهدة غالبا ما تكون عن طريق الرؤية، غير أن الرؤية ليست بشرط لازم لثبوت حالة التلبس بل يكفي لثبوتها أن يكون الشاهد قد حضر ارتكاب الجريمة وأدرك وقوعها سواء بحاسة البصر أو الشم أو السمع[1]

ب. مشاهدة الجريمة الالكترونية عقب ارتكابها:

يقصد بهذه الحالة مشاهدة آثار الجريمة التي تنبئ من ارتكابها منذ زمن يسير ويعبر بعض الفقهاء عن هذه الحالة بأن الجريمة تكون وقتئذ مازالت ساخنة فنراها لم تخمد بعد ودخانها لا يزال يشاهد ويعني ذلك ألا يكون قد انقضى وقت طويل بين ارتكابها واكتشافها.

ج. حيازة المجرم لأشياء تدل على مساهمة في الجريمة الالكترونية:

تقوم هذه الحالة إذا وقعت الجريمة الالكترونية وشوهد الجاني في وقت قريب جدا من وقوعها حائز الشيء أو الأشياء تكون أما قد استعملت ف ارتكاب الجريمة أو تحصلت من ارتكابها[2].

[1]-جيلالي بغدادي، التحقيق، دراسة مقارنة نظرية وتطبيقية، ط1، الديوان الوطني للأشغال التربوية، الجزائر، 1999، ص 28.

[2]-اسحاق ابراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، الطبعة 93، ديوان المطبوعات، الجامعية، الجزائر، 1993، ص 78-79.

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 والتي نصت عليها على سبيل الحصر، وهي:

أ. جرائم المخدرات:

يقصد بها الجرائم المتعلقة بالمخدرات والسلائف الكيميائية التي تدخل في تحضير المخدرات، مع استثناء تلك المتعلقة بالحيازة والاستهلاك لكونها لا يتوفر فيها عنصر التنظيم الذي يميز الجريمة المنظمة، وتضمن القانون رقم 04-18 المتعلقة بمكافحة المخدرات على الإجراءات الوقائية من أجل الحد من انتشار هذه الآفة والمقصود من إجراءات الوقاية هو منع وقوع الإصابة أهلا ومنع وقوع التعاطي المؤدي للإدمان[1]

ب. الجريمة المنظمة العابرة للحدود الوطنية

يقصد بها كل الجرائم العابرة للحدود الوطنية كتهريب المخدرات الأسلحة الهجرة غير الشرعية الإتجار بالبشر الح، وتشمل الشبكات المتخصصة وليست حالات الجرائم التقليدية العابرة للحدود كالهجرة الغير شرعية بصفة فردية.

ج. الجرائم الماسة بالمعالجة الآلية للمعطيات:

نص عليها المشرع في القسم السابع مكرر من قانون العقوبات المعدل بالقانون رقم 06-23 المؤرخ في 20/12/2006 بالمواد 394 مكرر إلى 394 مكرر 07 وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

[1]-اسحاق ابراهيم منصور، المرجع السابق، ص 78-79.

د. جرائم تبييض الأموال:

تبييض الأموال من الجرائم المساعدة للجريمة المنظمة منصوص ومعاقب عليها في القسم السادس مكرر المستحدث في قانون العقوبات المادة 389 مكرر وما يليها، كما نص على ذلك الأمر 05-01 المتعلق بالوقاية من الفساد ومكافحته[1].

هـ. الجرائم الإرهابية:

هي كل الجرائم الموصوفة بالأفعال الإرهابية والتخريبية المذكورة ضمن القسم الرابع مكرر من قانون العقوبات المنصوص والمعاقب عليها بالمادة 87 مكرر كما تم تعريف الإرهاب على أنه كل فعل من أفعال العنف أو التهديد به أيا كانت دوافعه أو أغراضه يقع تنفيذ المشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس .

و. الجرائم المتعلقة بالتشريع الخاص بالصرف:

حدد المشرع الجزائري المدلول القانوني الجريمة الصرف وهذا بموجب نص المادة 01 من التشريع الخاص بالصرف "تعتبر مخالفة أو محاولة مخالفة للتشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من والى الخارج".

وقد أفراد المشرع الجزائري قانون خاص يقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج بهدف ضبط إطار التصرف المشروع بخصوص حركة رؤوس الأموال من وإلى الخارج[2].

[1]-زوليخة زوزو، المرجع السابق، ص 761.
[2]-عبد الله حاج أحمد، المرجع السابق، من 350.

المطلب الثاني: أجهزة البحث والتحري والاختصاص القضائي والتعاون الدولي

الفرع الأول: البحث والتحري في الجريمة الالكترونية

نظرا لتفاقم الظاهرة الإجرامية المعلوماتية من يوم الآخر ونظرا إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم، كان من الضروري تطوير أجهزة الشرطة القضائية لتواكب التطور الحاصل في مجال الجريمة الإلكترونية (المعلوماتية)، لهذا عمدت معظم الدول إلى استحداث وحدات خاصة لمكافحة هذا النوع من الجرائم كما تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الإنتربول واليوروبول.

أما في الجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى وحدات قضائية تابعة لسلك الأمن والدرك الوطني.

أولا: الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم الإلكترونية .

الهيئات المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تستند مهام الوقاية ومكافحة الجرائم الإلكترونية بالنظر إلى تشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لديهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية والمجرم الإلكتروني[1].

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

وقد استحدثها المشرع الجزائري بموجب قانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام

[1]-ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة، ، الجزائر، 2016/2015 ، ص 171.

والاتصال ومكافحتها وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015[1]، ومن مهامها تفعيل التعاون القضائي والأمني الدولي وغدارة وتنسيق العمليات الوقائية والمساعدة التقنية للجهات القضائية والأمنية 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[2]

الهيئة الوطنية تعد سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتظم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

تنظم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين المصالح 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.

[1]-المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 53، في 08/10/2015.

[2]-فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، دراسة منشور بكتاب أعمال الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017 طرابلس.

للإشارة هنا تمكنت الجزائر ممثلة 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 توقيف 58 شخصا متورطا في قضايا إرهاب الكتروني تمت إحالتهم على القضاء. هذا 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 لتجميده عبر مواقع الأنترنت ومنصات التواصل الاجتماعي خاصة الفيسبوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية داعمة وتدعو للمشاركة في منتديات إرهابية على جانب اتصالات محلية ودولية[1].

ب. جهازي الأمن الوطني والدرك الوطني .

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين

[1]-أمال بن صوليح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر، مداخلة الملتقى الدولي حول "الإجرام السيبيرالى المفاهيم والتحديات"، 12-11أفريل 2017.

من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام[1].

أ-الوحدات التابعة لسلك الأمن الوطني:

تضع مديرية الأمن الوطني في إطار تحديد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات[2].

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

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية بقسنطينة.
- المخبر الجهوي للشرطة العلمية بوهران.

في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى

[1]-محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية مجلة ايليزي للبحوث والدراسات، العدد الثاني، ديسمبر 2017 المركز الجامعي اليزي، الجزائر، ص 34-35.

[2]-يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، تخصص جنائي، جامعة محمد بوضياف، مسيلة، 2017/2016، ص 20.

ولايات الوسط الشرق العرب الجنوب، لنقوم فيما بعد بتعميم الخلايا على جميع مصالح الأمن ولايات الوطن[1]

ب-الوحدات التابعة للقيادة العامة للدرك الوطني:

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

- المصالح والمراكز العلمية والتقنية .
- هياكل التكوين.
- المصلحة المركزية للتحريات الجنائية.
- المعهد الوطني لعلم الإجرام.

يوجد بالعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع لقيادة العلمية للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وإنجاز المقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رئيس والتابع لمديرية الأمن العمومية للدرك الوطني[2].

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

[2]-يوسف جفال، مرجع سابق، ص 21.

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

ثانيا: الهيئات القضائية الجزائية المتخصصة.

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون رقم 04-14 المؤرخ في 21 نوفمبر 2004[2]، وتختص هذه الجهات القضائية بموجب المواد 37-40-329 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار معالجة مثل هذه الجرائم[3].

ولقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000 والذي انصب على دراسة ثلاث نقاط أساسية دعم حقوق الإنسان وتسهيل حق اللجوء على القضاء وإعادة الاعتبار لنظام التكوين والتأهيل، بإحداث تغييرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائري بشقيه الموضوعي والإجرائي في مواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد مخاطر التقنية المعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة

[1]-سعيدة بوزنون، مرجع سابق، ص 53-54.

[2]-القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 155-66 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية الصادر بالجريدة الرسمية، عدد 71، بتاريخ 10 نوفمبر 2004.

[3]-بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، 2016، ص 52.

مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت السنوات الأخيرة تزايد في العلميات الإرهابية وتزايدا في أعمال المنظمات الإجرامية واستعمالها القضائي الافتراضي للاستفادة من خصائص الجريمة المعلوماتية [1]

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل المثال لا الحصر وتصف بأنها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف[2].

الفرع الثاني: الاختصاص القضائي في الجريمة الالكترونية

إن من أهم المشاكل التي تعترض أي تقدم في سير العملية الإثباتية وإجراءاتها 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[3].

[1]-محمد بوعمرة، سيد علي بنينال، مرجع سابق، ص 35.

[2]-كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع المجلة الأكاديمية للبحث القانوني، المجلد 11، عدد 01-2015، ص 117.

[3]-دلال مولاي ملياني، المرجع السابق، ص 248.

إذن كيف عالج المشرع الجزائري هذه المسألة وما هي الحلول التي تبناها من أجل إنجاح عملية التحري عن الجريمة الالكترونية من خلال تحديد قواعد الاختصاص القضائي الداخلي والقواعد الإجرائية المستحدثة في إطار الاختصاص القضائي الدولي في إطار القانون 09-04.

أولا: الاختصاص القضائي الداخلي

الاختصاص القضائي الداخلي أو المحلي أو الإقليمي تمديد القضاء المختص في الفصل في الدعوى الجزائية دون وجود نزاع في الاختصاص، حيث يقوم ذلك وفق معايير عندها المشرع الجزائري في المادة 37 الفقرة الأولى من قانون إن 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 الاشخاص حتى ولو حصل هذا القبض لسبب آخر"، أي يتحدد الاختصاص القضائي بمكان وقوع الجريمة أو المكان الذي يتم فيه المتهم أو المكان الذي يقبض فيه المتهم حتى ولو كان القبض قد وقع 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[1]"

ولما كانت جرائم الأنترنت جرائم لا تعترف بالحدود المادية الواقعية، والجرائم الماسة بالمعالجة الآلية للمعطيات من صورها فإنه عندما ترتكب الجريمة في إقليم الدولة

[1]-المادة 37 القانون رقم 04-14 المؤرخ 10 نوفمبر سنة 2004، ج.ر، ج ج.د.ش، العدد 71 ليوم 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 155-66 المتضمن قانون الإجراءات الجزائية.

الجزائرية هذا الاختصاص القضائي الجزائري وبسبب طبيعة هذه الجرائم التي أوضحنا أهم خصائصها في الفصل الأول من هذه الأطروحة قد مدد الاختصاص القضائي ليشمل كل إقليم الدولة حيث مدد الاختصاص للجرائم الالكترونية ومن بينها جرائم المعالجة الآلية للمعطيات، بموجب نص المادة 37 و 47 و 80 و 329 من قانون إ.ج على أن هذا التمديد يشتمل السلطات المختصة وكيل الجمهورية وفق المادة 37 من قانون إ.ج وضباط الشرطة القضائية المادة 40 مكرر 1 واختصاص قاضي التحقيق طبقا للمادة 40 من قانون إ.ج واختصاص المحاكم وفق المادة 329 من نفس القانون حيث أجاز تمديد الاختصاص إلى دائرة محاكم أخرى عن طريق التنظيم بموجب المرسوم التنفيذي رقم 06-348[1]، وعليه فإن الاختصاص القضائي في الجرائم يتحدد حسب:

أ. ضرورة التحقيق

إن وجود دلائل قوية لارتكاب الجريمة الالكترونية يجيز لقاضي التحقيق تمديد الاختصاص حيث يدخل في نطاق محاكم أخرى مجاورة .

- أن يكون هناك ضرورة للانتقال خارج نطاق اختصاصه المكاني.
- أن يخطر وكيل الجمهورية في نطاق الاختصاص الذي يعمل في نفس دائرة اختصاصه
- إخطار وكيل الجمهورية في نطاق الاختصاص الذي تم التمديد إليه .
- توضيح الأسباب التي أدت الى تمديد الاختصاص.

لذلك فإن قواعد الاختصاص من النظام العام وهذا لارتباطها بحسن سير العدالة فهي تحد الأهلية الإجرائية لجهات القضاء لنظر الخصومة[2].

[1]-دلال مولاي ملياني، المرجع السابق، ص250.
[2]-سامح أحمد البلتاجي موسى، المرجع السابق، ص 395.

ب. التمديد لا يتم إلا في جرائم معينة

وهي جرائم تشمل تمديد وكيل الجمهورية واختصاصات في التحقيق والمحكمة ويدعم هذا التمديد ما جاء به المادة 5 من القانون 09-04 والتي تشملت بتمديد الاختصاص حيث يتعلق الأمر بمسرح الجريمة الافتراضي بمعنى أن المشرع قد حاول الجمع بين المسرحين العادي أو التقليدي والمسرح الافتراضي، فقد نصت المادة 5 من القانون السالف الذكر على ما يلي: " ... إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك"[1]، إن هذه المادة إضافة جيدة خصوصا أن هذه المادة والمواد السابقة الذكر تجمع بين تمديد الاختصاص في المسرحين الإجراميين العادي والافتراضي وبذلك يتسنى للجهات المختصة التوصل إلى أفضل النتائج عندما يتعلق الأمر بالتحري عن الجريمة الالكترونية.

ثانيا: الاختصاص القضائي الدولي

إن ما يثير الإشكال في تمديد الاختصاص في جرائم الأنترنت هو امتداد مسرحها إلى أكثر من إقليم دولة فإن كان بإمكان التصدي الى اتساع نطاق الجريمة داخل الدولة باعتبارها وحدة واحدة هو ما لا يمكن تصوره إذا تعلق الأمر بامتداد مسرح الجريمة الى أكثر من إقليم دولة، ذلك أن أهم خصائص جرائم الأنترنت أنها عابرة للحدود وهو ما يصطدم بمبدأ أصيل في تطبيق القانون الجزائي مبدأ الإقليمية طبعا دون انتهاك سيادة الدولة في تحصيل الدليل الجنائي الالكتروني والمبادئ الاحتياطية، فالطبيعة التقنية

[1]-المادة 5 من القانون 09-04، المرجع السابق.

للمنظومة المعلوماتية المرتبطة بتكنولوجيا الاعلام والاتصال تؤدي الا محال الى أن إقليم أكثر من دولة مسرحا لجريمة من جرائم الأنترنت[1].

أ. مبدأ الإقليمية في جرائم الأنترنت

تعتب المحاكم الجزائرية صاحب الاختصاص الأصيل بالنظر في الجرائم المتعلقة بالأنترنت والتي تقع على إقليمها كل السلوك الإجرامي أو جزء منه دون الأخذ بعين الاعتبار شخص المتهم وهو المبدأ المجسد في المادة 3 الفقرة الأولى من قانون العقوبات الجزائري، هذا المبدأ الذي يعد مظهرا من مظاهر سيادة أي دولة.

ويقصد بمبدأ إقليمية القانون الجزائي أن القانون الجزائي الدولة ما يطبق على كل جريمة ترتكب على إقليم هذه الدولة سواء كان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية وسواء كان الجاني عليه مواطنا أم أجنبيا، ويجب التذكير بأن المحكمة المختصة وكذا سلطة التحقيق المختصة وفقا لمبدأ الإقليمية الذي يسود معظم التشريعات المقارنة هي محكمة المكان الذي وقعت فيه الجريمة أو جزء منها أي وقع منه الركن المادي أو جزء منه[2].

والأصل أن عناصر الركن المادي لأي جريمة يكون في نطاق جغرافي واحد أي إقليم دولة واحدة بداية من وقوع السلوك الإجرامي إلى تحقيق النتيجة الإجرامية غير أن الجرائم الالكترونية قد يتجزأ فيها الركن المادي قد يتوزع على أكثر من منظومة معلوماتية التي تكون ضمن إقليم دولة غير دولة ارتكاب السلوك الإجرامي كالتلاعب بالبيانات والمتاجرة بها أو تخريبها الذي يتم في نطاق إقليم دولة ولكن النتائج لا تتحقق إلا بإقليم

[1]-عادل عزام سقف الحيط، المرجع السابق، من 349.

[2]-مريم عراب، الاختصاص القضائي في الجرائم المعلوماتية، مجلة حوليات، كلية الحقوق والعلوم السياسية، جامعة وهران 2، العدد 03، 22/12/2015، ص 277.

دولة أخرى، وهنا تكون أمام ما يعرف بتنازع القوانين[1]، وفي هذا الصدد انقسم رأي الفقهاء الى ثلاثة اتجاهات:

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

وفقا 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 الإجرامية 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، وتجدر الإشارة الى أن معظم الدول لجأت الى مبدأ إقليمية النص الجنائي لحل مشكلة الاختصاص القضائي في الجرائم الالكترونية [2].

3. المذهب المختلط

أمام الانتقادات التي تعرض لها كلا الاتجاهين السابقين برز اتجاه ثالث مفاده أن الجريمة تعد واقعة في مكان حصول النشاط الإجرامي (العمل التنفيذي) وكذلك المكان الذي تحققت فيه النتيجة الإجرامية أو الذي المتوقع أو من المنتظر تحققها فيه، وهذا الاتجاه حضي بموافقة أغلب الفقد ويعد مبرره في أن الركن المادي للجريمة يقوم على

[1]-دلال مولاي ملياني، المرجع السابق، ص 252.

[2]-المرجع السابق، ص 277.

ثلاثة عناصر وهي الفعل أي النشاط الإجرامي، والنتيجة وعلاقة سببية ما يعني أن الجريمة وقعت في كل مكان تحقق فيه عنصر من عناصر الركن المادي للجريمة.

ب. المبادئ الأخرى في مسألة الاختصاص في الجريمة المعلوماتية

تعمد الدولة إلى حماية مصالحها على إقليمها الوطني وهذا الأصل ولكن حين تشكل الاعتداءات تهديدا لمصالحها وخارج حدود إقليمها لابد من أعمال مبادئ استثنائية حماية لمصالحها ومواطنيها وبالمقابل دون الاعتداء على سيادة الدولة الأخرى .

1. مبدأ العينية

يقصد به تطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة والمرتكبة خارج إقليمها أيا كانت جنسية مرتكبها وهذا المبدأ يفرضه حرص الدولة على حماية مصالحها الأساسية[1].

ولما لم يكن بإمكان مبدأ الإقليمية حماية كل المصالح المتعلقة بالدولة وحماية كامل سيادتها أوجبت الضرورة الملحة لمجابهة العجز الذي يكتنف مبدأ الإقليمية خصوصا في جرائم الأنترنت التي تتحقق أركانها على أكثر من إقليم افتراضي، حيث أن مبدأ العينية له ما يبرره إذا تعلق الأمر بحماية المصالح الوطنية خارج إقليم الدولة حتى وإن كان افتراضي وهو حال مسرح الجريمة في الجرائم الالكترونية.

وهو ما جعل المشرع الجزائري إضافة الى المادة 588 من قانون إ.ج العمل بمبدأ العينية يضيف المادة 15 من القانون 09-04 والتي تنص على أن المحاكم الجزائرية وحدها تختص بالنظر في جرائم تكنولوجيا الإعلام والاتصال ولكن بشروط:

* أن يتعلق الأمر بجرائم تكنولوجيا الاعلام والاتصال .

[1]-مريم عراب، المرجع السابق، ص 278-279.

* 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 القرار 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[1].

الفرع الثالث: التعاون الدولي في الجريمة الالكترونية

تعرف الجريمة الالكترونية أنها ذات بعد دولي عابر للحدود الوطنية وأن من بين الإجراءات المهمة التي تساعد في إثبات الجريمة والحد من الإشكالات المطروحة من هذه الناحية، فإن مكافحتها لا يتحقق إلا بوجود تعاون دولي على المستوى الجزائي الجنائي كما أن التحقيقات المتبادلة في الجريمة الإلكترونية وملاحقتها قضائيا تؤكد أهمية المساعدة القانونية المتبادلة بين الدول، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود لأن جهاز الشرطة في هذه الدول أو تلك لا يمكنه

[1]-مريم عراب، المرجع السابق، ص 280.

تعقب المحرمين وملاحقتهم إلا في حدود الدولة فيقف الجهاز الشرطي عاجزا ولذلك أصبحت الحاجة ماسة الى وجود كيان دولي يأخذ على عائقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين[1].

أولا: تعريف التعاون القضائي الدولي

ويعني تبادل العون والمساعدة لتحقيق هدف معين والأصل أن يتم التعاون الدولي في صورة مساعدة قضائية تتم عن طريق المساعدة القضائية اللازمة في التحري والتحقيق وتبادل المعلومات مع السلطات المختصة والأجهزة بمختلف الدول عن طريق الحصول على مختلف التسجيلات للاتصالات الالكترونية وغيرها[2].

ويعرف التعاون القضائي الدولي بأنه كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم[3].

حيث أن المشرع الجزائري قد أوجد استثناء فالأصل أن هذه المساعدة تتم عن طريق التمثيل الدبلوماسي أو ما يعرف بالقنوات الدبلوماسية كما هو منصوص عليه في المادة 721 من قانون إ.ج، لكن ومواكبة للتطور السريع والمستمر وفي حالة الاستعجال وهذا في محاولة الى إراحة عوائق التعاون الدولي ومن بينها المساعدة القضائية بتسيير الاتصال وتنسيق العمل على أساس احترام السيادة والمعاملة بالمثل يتم جمع الأدلة ومن

[1]-غانم مرضي الشمري، الجرائم المعلوماتية: ماهيتها، خصائصها، كيفية التصدي لها قانونا، الدار العلمية الدولية للنشر والتوزيع، عمان، الأردن، 2016، ص 98.

[2]-دلال مولاي ملياني، المرجع السابق، ص 270.

[3]-غانم مرضي الشمري، المرجع السابق، ص 98.

بينها الأدلة الجنائية الالكترونية بالطرق السريعة والتي تتجسد في الفاكس والبريد الالكتروني ولكن بشروط معينة [1].

ويتخذ التعاون القضائي صورا عدة منها:

أ. تبادل المعلومات

وهو يستعمل تقديم البيانات والمعلومات والوثائق والمواد التي من شأنها تسهيل مهمة المحاكمة وقد يشمل ذلك التبادل السوابق القضائية للجناة[2]، وأن مكافحة الجرائم لا تتحقق إلا من خلال تعاون دولي حقيقي، وقد تبلور هذا النوع من التعاون منذ إنشاء المنظمة الدولية للشرطة الجنائية (الأنتربول) وتقوم هذه المنظمة بتشجيع التعاون الدولي بين أجهزة الشرطة في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة[3].

ب. نقل الإجراءات

ويقصد بذلك قيام دولة ما بناء على اتفاقية أو معاهدة باتحاد إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت شروط معينة من أهم هذه الشروط التجريم المزدوج والمقصود به (أن يكون الفعل المنسوب إلى الشخص بشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات المطلوب اتحادها) بمعنى أن يكون الإجراءات المطلوب اتحادها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة، وقد أقرت العديد من الاتفاقيات الدولة كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية .

2. الإنابة القضائية الدولية

[1]-المادة 16 من القانون 09-04 المرجع السابق.

[2]-غانم مرضي الشمري، المرجع السابق، ص 99.

[3]-محمد لموسخ، تنازع الاختصاص في الجرائم الالكترونية مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، الجزائر، العدد 2، ديسمبر 2009، ص 153.

يقصد بالإنابة القضائية طلب اتحاد إجراء قصائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة الى الدولة المطلوب إليها لضرورة ذلك الفعل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام بنفسها وأن تنفيذ طلب الإنابة غير ملزم للدول المنابة لأن أساسها اعتبارات المجاملة الدولية.

وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تصنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى كسماع الشهود أو إجراء التفتيش وغيرها من الإجراءات، ويكون التنسيق في موضوع الإنابة القضائية عبر البعثات الدبلوماسية والتي تتميز بالبطء والروتين في إجراءاتها[1].

ولم نجد في القانون الجزائري ما يشير إلى تنظيم مسألة الإنابة القضائية مما يتطلب الرجوع الى الأحكام التي تنظمها في الاتفاقية الدولية التي انظمت إليها الجزائر ومن بين الاتفاقيات التي أبرمت في مجال الإنابة القضائية تلك التي عقدت بين الجزائر ومصر في 15/07/1964 وكذا التوقيع على اتفاقية جامعة الدول العربية المتعلقة بالتعاون القضائي في المواد الجنائية بتاريخ 09/07/1953، ما يلاحظ أنه غالبا ما يتم استبعاد تنفيذ أحكام الإنابة القضائية في المجال السياسي والضريبي والعسكري لأنها مجالات من شأنها المساس بالسيادة والنظام العام والمصالح الأساسية للدول غير أن هذا النظام يبقى معيب لارتباطه بالطرق الدبلوماسية والتي تتسم بالبطء وكثرة الشكليات والبروتوكولات وهو ما يتعارض مع وطبيعة جرائم البيئة التي تتميز بالسرعة والتغير وتأخر ظهور نتيجتها الإجرامية أحيانا وهذا من شأنه ضياع أدلة وبيانات أو اختفاءها والتي قد تشكل دليل مهما لإدانة المتهم[2]

[1]-غانم مرضي الشمري، المرجع السابق، ص 99-100.

[2]-محمد لموسخ، المرجع السابق، ص 155.

ثانيا: جهود المنظمة الدولية للشرطة الجنائية (الأنتربول)

وهي تسمى باللجنة الدولية للشرطة الجنائية (ICPO) ومقرها بباريس في فرنسا وقد غير اسمها ليصبح المنظمة الدولية للشرطة الجنائية، وتضم في عضويتها أكثر من 182 دولة عضو وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف.

ولقد مرت جهود المنظمة في هذا المجال بمراحل عديدة الى أن تم إنشاء عدة مراكز اتصالات إقليمية في كل من (طوكيو، نيوزيلندا نيروبي، أذربيجان، بيونس أيرس) لتسهيل مرور الرسائل ويضاف الى ذلك مكتب إقليمي فرعي في بانكوك.

وعلى المستوى العربي نجد أن مجلس الوزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء[1].

[1]-غانم مرضي الشمري، المرجع السابق، ص 97.

خلاصة الفصل:

وفي الختام، يتضح من خلال دراسة هذا الفصل المخصص للإطار القانوني للبحث والتحري أن إجراءات التحري في الجرائم الإلكترونية تتميز بطبيعتها الخاصة، وتتطلب الالتزام بمجموعة من الشروط، أهمها الالتزام بالنص الإجرائي المناسب. يهدف هذا التقيد إلى ضمان صحة الإجراءات وتجنب بطلانها، بالإضافة إلى الحفاظ على حريات الأفراد وصون كرامتهم.

في إطار التصدي للجريمة الإلكترونية، تتضافر الجهود التشريعية في مختلف الدول بهدف إيجاد حلول نهائية للتحديات المتعلقة بمبدأ إقليمية النص الجنائي والمبادئ الإجرائية المرتبطة باختصاص الجهات المعنية بتنفيذ إجراءات التحري.

الخاتمة

تمثل الجرائم المعلوماتية إحدى أخطر الصور الجنائية وأكثرها تعقيدًا، وقد نتجت عن التطور السريع في مجالي التكنولوجيا والاتصالات. إذ ساهمت الثورة المعلوماتية بشكل مباشر في ظهور نوع جديد من الجرائم يستهدف البنية التحتية التكنولوجية، ويُلحق ضررًا جسيمًا بالأنظمة المعلوماتية والبرمجيات.

على هذا الأساس، أضحى من الضروري وضع إطار قانوني يضمن حماية جنائية شاملة للبيانات والأنظمة المتصلة بالحواسيب. وقد فرضت الجرائم المعلوماتية على المجتمع الدولي ضرورة تكيف أنظمته القانونية مع هذا الشكل غير التقليدي من الإجرام، الذي يتميز بخصوصيات عدة، أهمها طابعه العابر للدول، مما يجعل تأثيره غير مقتصر على المكان الذي نشأ فيه. وفي هذا السياق، سعت الجزائر إلى مجابهة هذه الظاهرة عبر سن تشريعات واتخاذ آليات إجرائية وموضوعية تهدف إلى الحد من تأثيرها السلبي.

لقد أدى التطور التقني الهائل في مجال تكنولوجيا المعلومات وشبكات الاتصالات، لا سيما الحواسيب والإنترنت، إلى ترسيخ هذه الأدوات كجزء أساسي من حياة الأفراد اليومية. ومع ذلك، رافق هذا التطور بروز عدد متزايد من الجرائم المرتبطة بها، مما جعلها تشكل تهديدًا كبيرًا للدول، خاصة بالنظر إلى طبيعتها العابرة للحدود. ولهذا السبب، سارعت العديد من الدول إلى اتخاذ تدابير احترازية متعددة، سواء من خلال إبرام اتفاقيات دولية وثنائية أو عبر صياغة قوانين وطنية تهدف إلى مواجهتها. وفي هذا الإطار، استجابت الجزائر لهذه المستجدات عبر وضع إطار قانوني متكامل لمكافحة الجرائم الإلكترونية، أبرزها القانون رقم 09-04 الخاص بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها. وتأتي هذه المنظومة في سياق دعم قانوني العقوبات والإجراءات الجزائية القائمة.

وتتمثل خصوصية الجريمة المعلوماتية في كونها ظاهرة جنائية مستحدثة أثارت تباينات واضحة بين الفقهاء والقضاء في تعريفها وتوصيفها بدقة. بالإضافة إلى ذلك، تتميز هذه الجرائم بعدة خصائص فريدة، أبرزها أنها بطبيعتها عابرة للحدود، فضلاً عن السمات الخاصة بمن يمارسونها. كما تتصف هذ الجرائم بأنها متنوعة الأشكال والأنماط وتختلف طرق ارتكابها وأساليب تنفيذها. وتشمل هذه الجرائم النوعين التقليدي والفني. فبينما ترتكب الجرائم التقليدية باستخدام أجهزة الكمبيوتر وشبكات الإنترنت كوسائل، نجد الجرائم الفنية تستهدف مكونات أنظمة المعالجة المعلوماتية مثل نظم التشغيل وبرامج الحماية.

النتائج:

استناداً إلى ما تم طرحه، يمكن تلخيص النتائج التي توصلنا إليها على النحو التالي:

1. تعتبر الجريمة المعلوماتية من الجرائم المستحدثة التي تحدث في العالم الافتراضي، والذي رغم طبيعته غير المادية، إلا أنه يحمل وجوداً فعلياً وحقيقياً.

2. تمتاز الجريمة المعلوماتية بأنها تتجاوز الحدود الزمنية والمكانية، وتعد من بين أخطر أنواع الجرائم نظراً للاختلاف الجوهري بينها وبين الجرائم التقليدية.

3. لا تنطبق الأساليب التقليدية في متابعة وإثبات الجريمة المعلوماتية، حيث تتطلب تقنيات فنية وتقنية متطورة تتناسب مع البيئة الافتراضية التي تنشأ فيها مثل هذه الجرائم.

4. يمتاز المجرم المعلوماتي بذكاء عالٍ ومهارة تقنية متقدمة، مما يجعل الجريمة المعلوماتية هادئة بطبيعتها، إذ تعتمد بشكل كبير على المهارات الذهنية دون الحاجة إلى مجهود بدني.

5. نظراً لخطر الجريمة المعلوماتية، قامت الدول والهيئات الدولية بالسعي إلى وضع أطر قانونية للتصدي لها، ومن أبرزها اتفاقية بودابست لعام 2001. وفي السياق الجزائري، عمل المشرع على مواكبة هذا التطور من خلال تعديل قانون العقوبات بموجب القانون رقم 04/15، إضافة إلى القانون رقم 04/09 الذي يخص القواعد المتعلقة بالوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحته.

ورغم ذلك يبقى المشرع الجزائري لم يتدارك كل الثغرات والنقائص بعد في نصوصه القانونية لذا فإننا سنقترح بعض التوصيات التالية:

التوصيات:

1. العمل على إصدار قوانين صارمة تهدف للحد من هذه الجرائم، مع تشديد الرقابة على الأجهزة والبرامج المستخدمة.

2. مراجعة الإجراءات القانونية الحالية لتتناسب مع طبيعة الجرائم المعلوماتية، إما عن طريق تعديلها أو استحداث إجراءات جديدة.

3. إدراج نص قانوني يُجرّم سرقة المال المعلوماتي والمعنوي مثل البرامج والمعلومات ضمن التشريع الجزائري.

4. تضمين الدليل التقني أو الإلكتروني كوسيلة إثبات جنائي في هذه النوعية من الجرائم، مع تعديل القواعد الإجرائية لتسهيل الحصول عليه واعتماده قانونياً.

5. تعزيز التعاون الدولي بين الدول لمكافحة هذه الظاهرة الإجرامية، عبر توقيع اتفاقيات جماعية وثنائية، خاصة في مجالات التعاون القضائي والأمني.

6. التركيز على تأهيل وتدريب مختصين من الأجهزة القضائية وجهات الضبط القضائي لمواجهة الجرائم المعلوماتية بفعالية وكفاءة.

قائمة المصادر

والمراجع

قائمة المصادر والمراجع:

قائمة المراجع

أولا: باللغة العربية

أ – الكتب

1-أحمد خليفة ملط، الجرائم المعلوماتية، ط1، دار الفكر الجامعي الاسكندرية، مصر، 2006

2-أسامة أحمد المناعة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014

3-اسحاق ابراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، الطبعة 93، ديوان المطبوعات، الجامعية، الجزائر، 1993

4-بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، 2016

5-بلال محمد الزعبي، أسامة أحمد مناعسة، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، دار الثقافة، عمان، الأردن، 2010

6-بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007

7-جيلالي بغدادي، التحقيق، دراسة مقارنة نظرية وتطبيقية، ط1، الديوان الوطني للأشغال التربوية، الجزائر، 1999

8-حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء القانون الجزائري، دراسة مقارنة، ط1، منشورات السائحي، الجزائر، 2017

9-حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت 2014.

10- خالد حياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2011

11- خالد داودي، الجريمة المعلوماتية، ط1، دار الاعصار العلمي للنشر والتوزيع، عمان، الاردن، 2008

12- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط1، دار الفكر الجامعي، الاسكندرية، مصر، 2009

13- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعية الجديدة للنشر، الإسكندرية، سنة 2009

14- عادل عبد العال خراشي، ضوابط التحري والاستدلال عن الجرائم في الفقه الاسلامي والقانون الوضعي، دار الجامعة الجديدة للنشر، الاسكندرية، 2006

15- عبد الباقي الصغير، الأنترنيت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنيت، دار النهضة العربية، القاهرة، 2001

16- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى

17- عبد الله حسين محمود، إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003

18- عز الدين عثماني، إجراءات التفتيش والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، جامعة تبسة، العدد 04 جانفي 2018

19- غانم مرضي الشمري، الجرائم المعلوماتية: ماهيتها، خصائصها، كيفية التصدي لها قانونا، الدار العلمية الدولية للنشر والتوزيع، عمان، الأردن، 2016

20- فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، دراسة منشور بكتاب أعمال الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017 طرابلس.

21- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية مجلة ايليزي للبحوث والدراسات، العدد الثاني، ديسمبر 2017 المركز الجامعي اليزي، الجزائر.

22- محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت: الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2011

23- محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، ط11، مطبعة جامعة القاهرة، 1976.

24- منير محمد الجنبيهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات، ط1، دار الفكر الجامعي، الاسكندرية، 2018.

25- هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

26- هشام فريد رستم، الجوانب الإجرامية لجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، آسيوط، مصر، 1994.

ب –البحوث الجامعية:

- **أطاريح الدكتوراه :**

1. أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، رسالة لنيل شهادة الماجستير تخصص قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، الجزائر 2014-2015.
2. دلال مولاي ملياني، 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.

3. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة، ، الجزائر، 2016/2015 .
4. شنتير خضرة، الآليات القانونية لمكافحة الجريمة الالكترونية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أحمد دراية أدرار، 2020/2021
5. عائشة بن قارة مصطفى، حجية الدليل الإليكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير كلية الحقوق، جامعة الإسكندرية، سنة 2009
6. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية (دراسة مقارنة)، رسالة ماجستير، القانون العام، جامعة الشرق الأوسط عمان الأردن، 2014.
7. فاير محمود راجع غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، كلية الحقوق جامعة الجزائر 1، 2010/2009.
8. محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق، جامعة عين الشمس، مصر، 2011.
9. هبة نبيلة هروال، جرائم الانترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013.

- **مذكرات الماجستير:**

1. سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق و العلوم السياسية، جامعة باتنة، 2013.
2. صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

3. محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

- **مذكرات الماستر:**

1-ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، رسالة تكميلية لنيل شهادة ماستر في القانون، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2015/2016.

2-أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09-04، رسالة مقدمة لنيل شهادة الماستر في القانون الجنائي، كلية الحقوق والعوم السياسية، جامعة ورقلة، 2012/2013.

3-يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، مسيلة، 2017/2016.

المجالات:

1. أمال بن صوليح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر، مداخلة الملتقى الدولي حول "الإجرام السيبيرالى المفاهيم والتحديات"، 12-11أفريل 2017.

2. بثينة حبيباتي، الطبيعة الخاصة للجريمة المعلوماتية، دراسات مجلة وأبحاث، مجلد جامعة زيان عاشور، الجلفة، الجزائر، مجلد 12، عدد 03 جويلية 2020

3. حاج أحمد عبد الله، أساليب التحري الخاصة وحجيتها في الإثبات الجنائي مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة أدرار، المجلد 8، العدد 05، 2019

4. حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، جامعة 20 أوت 1955، سكيكدة، الجزائر

5. حمزة خضري، حمزة عشاش: "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط الجزائر، جوان 2020
6. رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، كتاب أعمال المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، مركز جيل البحث العلمي طرابلس، لبنان، 24 مارس 2017
7. زوليخة زوزو، مشروعية أساليب التحري الحديثة، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد 8، الجزء 2، جوان 2017
8. سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر 2019
9. صالح شنين، إجراءات التحري والتحقيق في جرائم تكنولوجيا الاعلام والاتصال في التشريع الجزائري، مجلة الدراسات القانونية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، العدد 01
10. عبد الرشيد معمري، ضوابط مشروعية أساليب التحري الخاصة المجلة الأكاديمية للبحث القانوني، جامعة خنشلة، 2015، العدد 1
11. عبد الصديق الشيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 04، العدد 1، السنة 2020
12. فريحة حسين، الجرائم الالكترونية والأنترنت، مقال منشور بمجلة المعلوماتية، السعودية، العدد 36، أكتوبر 2011
13. فلاح عبد القادر ،أيت عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، المجلد 4 العدد 2، 2019.

14.فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الانسانية، جامعة منتوري قسنطينة، الجزائر، عدد 33 2010

15.كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع المجلة الأكاديمية للبحث القانوني، المجلد 11، عدد 2015-01

16.محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، 2018

17.محمد لموسخ، تنازع الاختصاص في الجرائم الالكترونية مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، الجزائر، العدد 2، ديسمبر 2009

18.مريم عراب، الاختصاص القضائي في الجرائم المعلوماتية، مجلة حوليات، كلية الحقوق والعلوم السياسية، جامعة وهران 2، العدد 03، 22/12/2015

19.هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي، مجلة الأمن والقانون، دبي الإمارات العربية المتحدة، العدد الثاني، 1999

20.هشام رستم، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة بحث مقدم إلى لجنة العلمية بمصر لمنع الجريمة المعلوماتية ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيط، العدد 17، سنة 1995

21.وردة شرف الدين، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية، مجلة الفكرة، جامعة محمد خيضر بسكرة، الجزائر، العدد 15، 15 جوان 2017.

المحاضرات:

1. عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية، ط1، دار الهدى، الجزائر، 2012

- **النصوص التشريعية:**

الأوامر:

1-الأمر رقم 66-155 المؤرخ في 8 جوان 196 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم 11-02 المؤرخ في 23 فيفري 2011، ج..ر، ج.ج.د،ش، العدد 12 المؤرخ في 23 فيفري 2011.

القوانين

1-القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 155-66 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية الصادر بالجريدة الرسمية، عدد 71، بتاريخ 10 نوفمبر 2004

2-القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155، ج.ر، ج.ج،د.ش، العدد 84 الصادرة في 24 ديسمبر 2006.

3-قانون الإجراءات الجزائية المعدل والمتمم بموجب الأمر رقم 15/02 ج.ر، ج، ج.د.ش، العدد 40.

4-القانون رقم 04-15 المؤرخ في 10 نوفمبر يعدل ويتمم الأمر 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج . ر ، ج. ج.د.ش، العدد 71 الصادر في 10 نوفمبر 2004.

5-القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج، ر، العدد 47، الصادرة في 16 أوت 2009

المراسيم:

1-المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 53، في 08/10/2015.

ثانيا: باللغة الأجنبية

1- Klaus Tiede man, Fraude et autres délits d'affaires commis a l'aide d'ordinateurs électroniques, Rev, drpén, crim, 1984

2- MARWE VANDER، computer crimes and other grimes against information Technology in south Africa، "R.ID.P", 1993

فهرس

المحتويات

فهرس المحتويات	
العنوان	الصفحة
شكر وعرفان	
إهداءات	
مقدمة	01
الفصل الأول: الإطار المفاهيمي للجريمة الالكترونية وإجراءات التصدي لها	
المبحث الأول: ماهية الجريمة الالكترونية	06
المطلب الأول: مفهوم الجريمة الالكترونية.	06
المطلب الثاني: الأحكام الخاصة بالجريمة الالكترونية	19
المبحث الثاني: البحث والتحري عن الجريمة الالكترونية	30
المطلب الأول: مفهوم البحث والتحري	30
المطلب الثاني: ضوابط البحث والتحري عن الجريمة الالكترونية	44
الفصل الثاني: خصوصية البحث والتحري عن الجريمة الالكترونية	
المبحث الأول: أساليب البحث والتحري عن الجريمة الالكترونية	55
المطلب الأول: أساليب البحث والتحري في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال	56
المطلب الثاني: أساليب البحث والتحري في ظل قانون الإجراءات الجزائية	67
المبحث الثاني: مشروعية أساليب البحث والتحري والجرائم الالكترونية	78
المطلب الأول: موقف المشرع الجزائري من أساليب البحث والتحري	79
المطلب الثاني: أجهزة البحث والتحري والاختصاص القضائي والتعاون الدولي	89
خاتمة	110
قائمة المصادر والمراجع	
فهرس المحتويات	

ملخص:

تولي التشريعات الجزائرية أهمية كبيرة لإجراءات البحث والتحري في الجرائم الإلكترونية، نظرًا لتعقيداتها وطبيعتها التقنية. ينص قانون الإجراءات الجزائية المعدل بموجب القانون رقم 06-22 على تمكين الضبطية القضائية من استعمال وسائل تقنية متطورة للكشف عن مرتكبي هذا النوع من الجرائم. تشمل هذه الإجراءات المراقبة الإلكترونية، واعتراض المراسلات عبر الوسائط الرقمية، والتفتيش الإلكتروني للأجهزة والأنظمة المعلوماتية. كما أتاح المشرع إمكانية الاستعانة بخبراء تقنيين لتحليل الأدلة الرقمية. يتم تنفيذ هذه الإجراءات تحت إشراف النيابة العامة أو قاضي التحقيق ضمانًا لاحترام الحقوق والحريات. وتسهم هذه التدابير في تعزيز فعالية مكافحة الجريمة الإلكترونية وضمان العدالة.

الكلمات المفتاحية: الجريمة الإلكترونية، اعتراض المراسلات، التفتيش الإلكتروني، الضبطية القضائية، التعاون الدولي.

Abstract :

Algerian legislation attaches great importance to investigation and research procedures in cybercrimes, given their complexity and technical nature. The Code of Criminal Procedure, amended by Law No. 06-22, empowers judicial police to use advanced technical means to detect perpetrators of this type of crime. These procedures include electronic surveillance, interception of correspondence via digital media, and electronic inspection of information devices and systems.

The legislature also allows for the use of technical experts to analyze digital evidence. These procedures are carried out under the supervision of the Public Prosecutor or the investigating judge to ensure respect for rights and freedoms. These measures contribute to enhancing the effectiveness of combating cybercrime and ensuring justice.

Keywords: *cybercrime, interception of correspondence, electronic inspection, judicial police, international cooperation.*