جامعة أكلي محند أولحاج – البويرة

كلية الحقوق والعلوم السياسية

قسم: قانون الخاص

جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري

مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية

تخصص: القانون الأعمال

من إعداد الطالبين:

- محمد بوعمرة
- سيد علي بنينال

إشراف الأستاذ (ة):

د/ دليلة معزوز

أعظاء لجنة المناقشة:

- د/	جامعة البويرة	رئيسًا
- د/ دليلة معزوز	جامعة البويرة	مشرفًا ومقررا
- د/	جامعة البويرة	ممتحنًا

السنة الجامعية : 2019 / 2020

بسم الله الرحمن الرحيم

إهداء

إلى من لا يمكن للكلمات أن توفي حقهما، الوالدين الكريمين الأم والأب وبالأخص إلى أمي الحنونة رحمة الله عليها (بالنسبة للطالب بنينال سيد علي) وإلى الأخوة والأخوات التحية الخاصة وإلى كل الأهل والأقارب وجميع الأصدقاء والزملاء

نهدي لهم ثمرة جهدنا .

سيد علي

محمد

كلمة شكر

الحمد لله الذي أنار لنا درب العلم والمعرفة، والذي أعاننا على أداء هذا الواجب ووفقنا إلى إنجاز هذا العمل نتوجه بجزيل الشكر والإمتنان إلى كل من ساندنا من قريب أو بعيد على إنجاز هذا العمل وفي تذليل ما وجهناه من صعوبات

ونخص بالذكر الأستاذة المشرفة "دليلة معزوز"

التي لم تبخل علينا بتوجيهاتها ونصائصحها القيمة التي كانت عون لنا في اتمام هذا البحث

وقبل أن نمضي نقدم أسمى آيات الشكر والإمتنان والتقدير والمحبة إلى الذين حملوا أقدس رسالة في الحياة إلى الذين مهدوا لنا طريق العلم والمعرفة إلى جميع أساتذتنا الأفاضل

مقدمة

مقدّمة:

إن التطور الهائل الذي شهدته كل من مجال تقنية المعلومات ومجال الاتصلات والاندماج المذهل الذي حدث بينهم فيما بعد، كا ن المحور الأساسي الذي قامت عليه تقنية المعلومات إذ أصبحت جميع القطاعات المختلفة تعتمد في آداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية، لما تتميز به عنصرين السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة، داخل الدولة الواحدة أو بين عدة دول.

فبات يلق على هذا العصر عصر المعلومات فمنذ وقت ليس ببعيد كان كم من العلومات المتولدة عن التفاعلات البشرية محدودة إلى حد كبير، ولم يشكل حجمها أي مشكلة أمام عمليات تجميعها وتخزينها وإعادة استرجاعها إلا أنه ومع تقدم البشرية وتزايد معارف الإنسان وعلومها بدأ كم المعلومات يتزايد ويتكاثر وصارت الرق التقليدية لتجميع وتنظيم هذه المعلومات عاجزة عن تلبية إحتياجات المستفيدين منها بكفاءة وفعالية وأصبح من الضروري اللجوء إلى استخدام أاليب علية وتقنية متطورة لمواجهة هذه الظفرة، فكان أن ظهرت الحاسبات الإلكترونية وظهور مستحدثات تقنية كأقراص الفيديو الرقمية، وأقراص الليزر، ووسائل الإتصال، ذلك من أجل تسهيل التحكم في المعلومات ومعالجتها واسترجاعها.

وهو ما دعى بالكثير من رجال الإقتصاد والاجتماع إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية فإن كان هدف الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان، فهدف الثورة الثانية هو إحلال الآلة محل النشاط الذهني للإنسان.

وفي مرحلة لاحقة من مسار عصر تقنية المعلومات تم التوصل إلى فكرة الربط بين أجهزة الآعلام الآلي ووسائل الإتصال، المر الذي أثمر على ظهور شبكات المعلومات، ولعل أهمها على الإطلاق شبكة الأنترنت، وثم استتبع اتساع ونماء كل من تكنولوجية الاتصال والحاسبات من جهة والبرمجة من جهة أخرى والإندماج الذي حصل بينهما إلى الوصول إلى استحداث تقنية نظم المعالجة الآلية للمعلومات، وتضاعفت أهمية هذه التقنية والإعتماد عليها في نقل وتبادل المعلومات والصوت والصورة عبر أنحاء العالم لما تتميز به من شمول وسعة محتواها وما توفره من مال وجهد ووقت وأصبحت بذلك نظم المعالجة الآلية للمعطيات بسبب التقنيات التي تقوم عليها والمتمثلة في الحواسيب والشبكات المعلوماتية أكثر انتشارا في كل القطاعات والمجالات كالصناعة والتجارة وغيرها.

ولكن على الرغم من المزايا الهائلة التي تحققت كل يوم بفضل هذه التقنية على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة، إلا أن هذه الثورة التكنولوجيا المتنامية صاحبتها في المقابل حملة من الإنعكاسات السلبية جراء الإستخدام السيء وغير المشروع مما ألحق الضرر بمصالح الفرد والجماعة على

حد سواء، وعلى ضوء ذلك فإن هذه الظاهرة الإجرامية التقنية آثارت العديد من المشكلات في نطاق قانون الاجراءات الجزائية الذي وضعت نصوصه لتحكم الاجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في اثباتها والتحقيق فيها.

لقد قمنا بإختيار هذا الموضوع وجعلناه موضود دراستنا في هذه المذكرة نظرا للأهمية البالغة الجريمة الإلكترونية وما يشملها من إجراءات وآليات التحري والتحقيق، تظهر هذه الأهمية من خلال اعتبار أن موضوع الجزائم الإلكترونية حديث وكثير الإنتشار حاليا، كما أنه من الموضوعات التي تثير جدلا فقهيا لدى فقهاء القانوني الجنائي، إظافة إلى تعلق الموضوع بالوسائل الحديثة ذلك أنه كلما تطورت الوسائل الإلكترونية كلما تطور أسلوب ارتكاب هذا النمط من الجرائم، وهذا ما شكل عائقا أما القائمين على البحث والإثبات الجرائم الإلكترونية، حيث أن قواعد البحث والتحري وأسس الإثبات الجنائي في القوانين التقليدية لا تكفي، بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلائم مع طبيعتها الفنية.

إن الغاية المرجوة من هذه الدراسة تتمثل أساسا في تحديد جهاز التحقيق في الجريمة الإلكترونية وكذا طرق التحقيق في إستخلاص أدلة الإثبات الجنائية في الجرائم الإلكترونية، كما تهدف الدراسة إلى تقديم رؤية خاصة بالمسرح الرقمي وهو المسرح الإفتراضي غير المرئي، وقد تعرضت الدراسة أيضا إلى المشكلات التي تعيق تحديد الإختصاص المكاني في هذا النوع من الجرائم العابرة للحدود.

ولقد أفرزت الجريمة الإلكترونية تحديات واضحة للقوانين التي وضعت لمكافحتها، فقد تغيرت من صورتها المادية إلى أخرى معنوية مما أدى إلى إفلات كبير للمجرمي هذه الجرائم من العقوبات، كما استحدثت ثورة الإتصالات والمعلومات نوع جديد من الجرائم لم يتصور المشرع الوطني حدوثها أصلا، ومن هنا كان لابد من التشريعات الوطنية المختلفة أن تواكب هذا التطور الملحوظ في الجرائم الإلكترونية في قواعد قانونية غير تقليدية لمواجهة هذا الخطر، بالتالي ومن خلال مشكلة الدراسة يمكننا أن نتسائل عن:

أي مدى استطاعت أجهزة التحقيق في الجريمة الإلكترونية مواكبتها ومواجهتها في التشريع الجزائري ؟

هذه الإشكالية يمكن أن تتفرع منها عدة تساؤلات منها:

1- ما هي الجريمة الإلكترونية وما هو المجرم الإلكتروني ؟

2- ما المقصود بالتحري والضبط في الجرائم الإلكترونية ؟

3- ما هي الإجراءات المتعلقة بالتحقيق في الجريمة الإلكترونية ؟

4- كيفية ضبط الدليل الإلكتروني وحجيته لدى القاضي الجزائري ؟

وعلى هذا الأساس اعتمدنا على المنهج الوصفي التحليلي، الذي يقوم بوصف هذه الظاهرة وتحليل المواد التي تناولتها، ذلك لأن الدراسة تهتم بسبل التحقيق في الجرائم الإلكترونية وكشفها من الناحية الفنية والقانونية.

وحتى نتمكن من معالجة الإشكالية المطروحة إرتأينا إلى تقسيم الخطة إلى فصلين معتمدين على تقسيم ثنائي للخطة، ففي الفصل الأول سنتناول فيه مفهوم جهاز التحقيق للجريمة الإلكترونية والذي أدرجناه في مبحثين تناول كل منهما كيفية التحقيق في الجريمة الإلكترونية وكذا السلطات المخصصة بالتحقيق في الجريمة الإلكترونية، أما الفصل الثاني فتطرقنا إلى أجهزة التحقيق في الجريمة الإلكترونية وأدرجناه كذلك في مبحثين هما: المبحث الأول: مرحلة جمع الاستدلالات والتحقيق فيها، أما المبحث الثاني: مرحلة المحاكمة.

لا يفوتنا القول أنه تلقينا صعوبات كثيرة في اختيار موضوع البحث في حد ذاته كونه حديث ولم يسبق بحثه بوضوحا وتعمق، ولو أن هناك مراجع ومقالات تناولت الموضوع إلا أنها لم تعالجه من كل جوانبه أو أدرجته بشكل سطحي إظافة إلى أن الجرائم محل الدراسة ترتبط بالحاسب الآلي مما يتطلب الإلمام بمكوناته وبنظام المعالجة الآلية للمعلومات والشبكات الإلكترونية.

الفصل الأول:

مفهوم جهاز التحقيق الجريمة الإلكترونية في التشريع الجزائري.

تعد الجريمة الإلكترونية ظاهرة إجرامية حديثة نظرا لإرتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير من الغموض، لأجل ذلك فقد بدا لنا أنه وقبل الخوض في الإجراءات التي تطبق على الجرائم الإلكترونية، إذا يجب الإلمام الجريمة الإلكترونية وخصائصها وأيضا التطرق إلى الأجهزة المختصة في التحقيق في الجريمة الإلكترونية.

وعلى ضوء ذلك سنقسم الفصل الأول إلى الجريمة الإلكترونية وكيفية التحقيق فيها في المبحث الأول أما المبحث الثاني سيكون تحت عنوان السلطات المختصة في الجريمة الإلكترونية.

المبحث الأول: الجريمة الإلكترونية والتحقيق فيها في التشريع الجزائري.

أثيرت العديد من التساؤولات حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم، حيث ظهرت عددت آراء فقهية في محالة فهم المقصود بالجريمة الإلكترونية.

وقد تبنى المشرع الجزائري للدلالة على الجريمة الإلكترونية، مصطلح المساس بالأنظمة المعالجة الآلية للمعطيات، حيث يمثل نظام المعالجة الآلية للمعطيات المسئلة الأولية أو الشرط الأولي الذي يلزم تحقيقه.

وذلك فالمشرع الجزائري لم يبعرف نظام المعالجة فأوكل مهمة تعريفه لكل من الفقه والقضاء.

وعليه سنحاول من خلال هذا المبحث أن نتطرق إلى الجريمة الإلكترونية والتحقيق فيها، حيث يتضمن المطلب الأول التعريف بالجريمة الإلكترونية وخصائصها وأنواعها، أما المطلب الثاني سنتطرق إلى التحقيق فيها في التشريع الجزائري.

المطلب الأول: مفهوم الجريمة الإلكترونية.

ظاهرت تعاريف كثيرة حول تعرف الجريمة الإلكترونية ما بين مضيف لمفهومها وموسع كما تعددت المصطلحات المستخدمة للدلالة عليها فالبعض استخدم مصطلح جرائم استخدام الحسابات أو جرائم المعالجة الآلية للبيانات والبعض الآخر أطلق عليها اسم الإجرام المعلوماتي، وفيما يلي: تفصيل لمفهوم هذه الجريمة من حيث التعريف والخصائص.

الفرع الأول: تعريف الجريمة الإلكترونية:

تعتبر الجريمة الإلكترونية من الظواهر الحديثة لإرتباطها بتكنولوجيا الحديثة، ولقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، حيث لم يتفق الفقه على تعريف محدد

بل إذ بعض الفقهاء، ذهب إلى ترجيح عدم وضع تعريف بحجة أن مثل هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني[1].

أولا: تعريف الجريمة الإلكترونية لغة.

الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه وجرمه الرجل على قومه وإليهم، ذنب وجنى جنتئة[2].

ثانيا: تعريف الجريمة إصطلاحا:

معظم الفقهاء المؤلفين في هذا الباب يردون تعريف الجريمة في الفقه إلى ما قرره الموارديي في الأحكام السلطانية بقوله: " الجرائم محظورات شرعية زجر الله عنها بحد أو تعزير يعني إذا كانت ممن يتعمد ارتكابها، أما الإمام أبو زهرة فبعدها ذكر تعريف الماوردي وأيده ساق من بين نصوصه تعريف آخر للجريمة فقال " هي المعصية التي يكون فيها عقاب يقرره القضاء"[3].

ثالثا: تعريف الجريمة الإلكترونية فقها وقانونا.

أ- **التعريف الفقهي:** انقسم الفقه إلى عدة آراء منهم من ضيق من مفهوم الجريمة الإلكترونية ومنهم من وسع من مفهومها، الاتجاه الذي يضيق من مفهوم الجريمة الإلكترونية.

يذهب أنصار هذا الإتجاه إلى حصر الجريمة الإلكترونية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها ومن التعريفات التي وضعها أنصار هذا الإتجاه أن الجريمة الإلكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لإرتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى.

---

[1] _ خالد ممدوح، أمن الجريمة الإلكترونية، الدار الجامعية، الإلكترونية، الإسكندرية، 2008، ص 41.

[2] _ ضياء مصطفى عثمان، السرقة الإلكترونية، دار النفائس، عمان، الطبعة الأولى، 2011، ص 32.

[3] _ بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، 2014، ص9.

وفي هذا الإتجاه أيضا الجانب الفقهي بالنظر إلى معيار نتيجة الإعتداء، إذ يرى الأستاذ MASS أن المقصود بالجريمة الإلكترونية هي اعتداءات ترتكب بواسطة المعلومات بغرض تحقيق ربح.

كما عرف الأستاذ PARKER الجريمة الإلكترونية بأنها كل فعل إجرامي متعمد أيا كان صلة بالمعلوماتية ينشأ عنها خسارة تحلق بالمجني عليه أوكسب يحققه الفاعل[1].

الإتجاه الذي يوسع من مفهوم الجريمة الإلكترونية: عرف أصحاب الإتجاه الموسع الجريمة الإلكترونية بأنها سلوك إجرامي يتم بمساعدة الكمبيوتر أو هي جريمة تتم في محيط أجهزة الكمبيوتر، أو هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها، كما عرفها الفقيهان Michels&credo بأنها سوء استخدام الحاسب أو جريمة الحسابات تسهل استخدام الحاسوب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه البيانات الخاصة، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به، وأيضا الاستخدام غير المشروع أو سرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته[2].

ب-التعريف القانوني: أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة للتكنولوجيات الإعلام والإتصال فإنه يعرفها بأنها: « جرائم المساس بأنظمة المعالجة الآلية للامعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية ».

[1] _ محمد أمنية الشوايكة جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009، ص 8.

[2] _ سميرة معاشي، ماهية الجريمة الإلكترونية، مجلة المنتدى القانوني، العدد السابع، جامعة، بسكرة، ص 276.

وبهذا فقد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نضم المعلوماتية وشبكات الإتصال إما موضوعا للجريمة أو وسيلة أو دعامة للجرائم التقليدية. ولول هذه النضم المعلوماتية وشبكات الإتصال ما كان أن نسبغ صفة المعلوماتية على هذه الجرائم.

وعلى خلاف المشرع الفرنسي الذي لم يعطي تعرفا للجريمة الإلكترونية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب المادة 02 من القانون 09-04 على أنها: « جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية ».

ويلاحظ على هذا التعريف ما يلي:

- أن المشرع قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكترونية، وثانيها معاير موضوع الجريمة المساس بأنظمة المعالحة الآلية للمعطيات، وثالثا معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات[1].
- كما حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري.

الفرع الثاني: خصائص الجريمة الإلكترونية وأنواعها.

إذ ما نقصد به ذاتيه الجرائم الإلكترونية هو استقلاليتها وتميزها من غيرها من الجرائم سيما التقليدية منها، وذلك بمجوعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية

[1] _ بوظياف إسماهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، العدد 11، سبتمبر 2018، ص 352- 353.

والإجرائية التقليدية القائمة، وسوف نحاول أن تبرز أهم خصائص المجرم الإلكتروني والمجني عليه الجريمة الإلكترونية وأنواع المجرمين الإلكترونيين وصفاتهم[1].

أولا: خصائص الجريمة الإلكترونية.

الفرع الأول :خصائص الجرائم المعلوماتية

إن ما نقصد به من ذاتية الجرائم المعلوماتية هو استقلاليتها وتميزها عن غيرها من الجرائم سيما التقليدية منها، وذلك بمجموعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة، وسوف نحاول أن نبرز أهم هذه الخصائص فيما يلي:

أ- **الجريمة المعلوماتية متعدية للحدود (عابرة للوطنية):** إنه وبعد ظهور شبكات

المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال أسفر هذا الأمر إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، حيث يمكن أن ترتكب الجريمة من مجرم في دولة على مجني عليه في دولة أخرى في وقت يسير جدا.

فالجريمة المعلوماتية بهذا الشكل لا تعترف بالحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، ذلك أن قدرة تقنية المعلومات على إختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمالى الإجرامية التي يعتمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول

[1] _ سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، 2013، ص 31.

إلى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث، أو القيام بإعداد أحد البرامج الخبيثة (Vérus) في بلد ما ثم يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم. وتظهر هذه المشكلة بصفة خاصة في التعاملات البنكية عبر شبكات المعلومات الدولية، حيث أدى التوسع الكبير لإجراء التعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد دولي لهذه الجرائم ذلك أن ربط وسائل الإتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية والتي أصبحت تتم بواسطة وسائل إلكترونية، وبصفة خاصة من خلال التحويل الإلكتروني للأموال والتبادل الإلكتروني للمعلومات.

ومفاد ما سبق ذكره أن الجرائم المعلوماتية تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ومن الوجهة التقنية التباعد بين أداة الجريمة ومحلها، وهذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة أو خارجها ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعلومات محل الإعتداء.

ولقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة إشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي في محاكمة مرتكب هذه الجريمة، فهل هي الدولة التي وقع فيها النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب، بالإضافة إلى إشكالية مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها، إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية. وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل عام.

لذلك فقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجريمة المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم لمختلف الدول.

ومن أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لها بحزم، وأن يشمل هذا التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم

جمعها في دولة تقبل في محاكم دولة أخرى . ولكن ومع ضرورة هذا التعاون والمناداة به إلا أنه تقف أمام هذا المبدأ عقبات ومعوقات تحول دون تحققه وتجعله صعب المنال، من أهمها انعدام نموذج موحد للنشاط الإجرامي المكون للجريمة المعلوماتية، وأن كثيرا من القوانين لم يتم تعديلها بحيث

تتواءم مع هذه الجرائم حتى يتسنى إدراجها ضمن الإتفاقيات الدولية الخاصة بتبادل المساعدة الجنائية في مجال الجرائم المعلوماتية، بالإضافة إلى تنوع واختلاف النظم القانونية والإجرائية.

ب- صعوبة اكتشاف الجريمة المعلوماتية وإثباتها:

تقع الجريمة المعلوماتية في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أنها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والذي يتحقق أحيانا إن لم نقل في الغالب في غفلة من المجني عليهم. كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمر كشف الجريمة وإثباتها، وإذا ما قورنت حالات اكتشاف الجريمة المعلوماتية على ضوء ما يتم اكتشافه من الجرائم التقليدية فإن عددها قليل، فمعظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابه، ذلك أن هذا النمط الإجرامي لا يحتاج إلى عنف أو جثث أو اقتحام وإنما هي معلومات وبيانات تغير أو تعدل أو تمحى كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الآلي فلا تترك أثرا خارجيا مرئيا أو ملموسا فهي كما وصفها بعض الفقهاء بأنها جريمة هادئة بطبيعتها لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها. فالجريمة المعلوماتية من الجرائم المستحدثة التي لا تترك شهودا يمكن الإستدلال بأقوالهم ولا أدلة مادية يمكن فحصها وإنما تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية.

كما ذهب البعض للقول بأن صعوبة اكتشاف الجريمة المعلوماتية وكذا صعوبة إثباتها راجع أيضا إلى عدة أسباب، من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، إذ أنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات وذلك سواء لارتكابها أو التحقيق فيها أو لملاحقة مرتكبيها .فأحيانا نجد رجال الضبطية القضائية غير قادرين على التعامل

بالوسائل الإستدلالية والإجراءات التقليدية مع هذا النوع من الجرائم . بالإضافة إلى صعوبة الإحتفاظ الفني بدليل الجريمة المعلوماتية، إذ للمجرم المعلوماتي القدرة على تدمير الدليل في أقل من ثانية ويمكن اعتبار أنه من بين الأسباب أيضا التي تقف وراء صعوبة اكتشاف الجريمة المعلوماتية وإثباتها المجني عليهم أنفسهم، ذلك أن هؤلاء قد يلعبون دورا رئيسيا في ذلك من خلال الإحجام عن الإبلاغ عنها في حالة اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للإنتهاك أو تمنى بخسائر فادحة من جراء ذلك عن عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهزا للثقة في كفاءتها ويبدو ذلك أكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الإدخارية ومؤسسات الإقراض .حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه، وهو ما يؤثر سلبا على السياسة التي يمكن أن توضع لمكافحتها.

وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي انقاص حجم الإجرام المعلوماتي الخفي، ومن هذه الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم المعلوماتية على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم

به من جرائم في هذا المجال مع تقرير جزاء على الإخلال بهذا الإلتزام . وعرض ذات الإقتراح على لجنة خبراء مجلس أوروبا ولاقت الفكرة رفضا باعتبار أنه ليس مقبولا تحويل المجني عليه إلى مرتكب الجريمة.

ثانيا: أنواع الجريمة الإلكترونية.

نظرا لانتشار الجريمة الالكترونية بشكل كبير فقد تعددت أنواع هذه الجرائم وأهمها ما يلي:

الجريمة المادية: هي التي تسبب أظرارا مادية على الضحية أو المستهدف من عملية النصب وتؤخذ واحدة من الأشكال الثلاثة التالية:

- عملية السرقة الإلكترونية كالاستيلاء على ماكنات الصرف الآلي، والبنوك كتلك المنتشرة في الكثير من الدول وبها يتم نسخ البيانات الاكترونية لبطاقة الصراف الآلي ثم استخدامها لصرف أموال حساب الضحية.
- إنشاء صفة إنترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة.
- الرسائل البريدية الواردة من مصاغدر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج من الوعد بنسبة من المبلغ أو تلك التي توهم صاحب البريد الالكتروني بفوزه بأحدى الجوائز أو الينا صيب.

الجريمة الثقافة: هي استيلاء المجرم على الحقوق الفكرية ونسبتها لهم دون موافقة الضحية وتكون على إحدى الصور الآتية:

- قرصنة البرمجيات وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اصطرانات وبيعها للناس بسعر أقل.
- التعدي على القنرات الفضائية المشفرة واتاحتها عن طريق الانترنت من خلال تقنية Soft Copy .
- جريمة لنسخ المؤلفات العلمية والأدبية بالطرق الالكترونية المستحدثة.

الجريمة السياسية والاقتصادية:

تستخدم المجموعات الارهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتمويل بعض الأموال في سبيل تحقيق أهدافهم.

- الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات.
- نشر الأفكار الخاطئة بين الشباب كالإرهاب والادمان والزنة لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى.

الجريمة الجنسية:

هذا النوع من الجريمة يمكن أن يتمثل في إحدى الصور الآتية:

- الإبتزاز: من أشهر حوادث الابتزاز عندما يقوم أحد الشباب باختراق جهاز إحدى الفتيات أو الاستيلاء عليه وفيه مجموعة من صورها واجبارها على الخروج معه أو فضحها بما يملكه من صورها.
- التغرير والاستدراج: في العادة هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات عبر برامج المحادثة يكون مع علاقة معها ثم يستدرجها بالكلام ويوهمها بالزواج لكي تثق به ومن ثم يقوم بتهديدها بما يملكمه من صور وتسجيلات من صوتها إن لم تستجب لطلباته[1].

جرائم حسب الأفراد:

هي الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق غير شرعية، كحسابات البريد الإلكتروني وكلمات السر التي تخصهم وقد تصل إلى انتحال شخصياتهم وأخذ صور وملفات المهمة من أجهزتهم بهدف تهديدهم وينطوي تحت هذا القسم من الجرائم كل من:

- جرائم التشهير بهدف تشويه سمعت الأفراد.

[1] _ نواوي سليمة، دور الدرك الوطني في محاربة الجريمة الالكترونية، جامعة مسيلة، 2019/2018، ص 25-27.

- جرائم السب والشتم والقذف.
- جرائم المطاردة الالكترونية[1].

ثالثا: المجني عليه في الجريمة الإلكترونية.

المعتدي عليه في الجريمة الإلكتورنية هو من يكون ضحية الإعتداءات غيرالمشروعة على مكونات الحاسوب، وقد يكون شخصا طبيعيا، شركة، أو مؤسسة تتعامل بمجال الحاسوب أثناء ممارسة الأعمال التجارية، الاقتصادية والسياسية التي ينبغي أن يستغل الحاسوب في إدارة أعمالها، وحسب تقديرات بعض خبراء الصندوق الدولي للبنوك، فإنه من المستحيل أن تحدد على نحو دقيق نطاق الجريمة الإلكترونية التي لا يعلم ضحاياها عنها شيئا إلا عندما تكون النظم المعلوماتية المملوكة لهم هدفا للجريمة الإلكترونية، حتى في حالة عملهم بذلك فهم يفضلون عدم إفشاء الفعل لأنه لا يوجد من يريد الإعتراف بأنه تم إنتهاك نظامه المعلوماتي.

والجدير بالذكر أن سلبية المجني عليهم أو ضحايا الجريمة الإلكترونية، وخوفهم من الإبلاغ حفاظا على سمعتهم التجارية ومكانتهم المرموقة، غير معين على التمادي في إقتراف مثل هذه الجرائم، وتوجد هذه الجرائم بصفة خاصة إلى البنوك، وإلى المواقع الإلكترونية للمؤسسات المالية، لأن القطاعات المستهدفة من الجريمة الإلكترونية هي تعتمد أكثر من غيرها على أجهزة الحاسوب، وتعتبر البنوك من أهم تلك القطاعات وأكثرها تضررًا[2].

ثالثا: أنواع المجرمين الإلكترونين وصفاتهم. قد يكون الجاني في الجريمة الإلكترونية، إما شخص يعمل بمفرده أو ضمن منظومة بغض النظر عن هذه الأخيرة، فقد تكون تجارية، سياسية، أو عسكرية[3]، ويمكن تقسيم أنواع المجرمين إلى فئتين.

---

[1] _ بن سولة نور الدين، الجرائم الالكترونية في ضوء التشريع الجزائري، المجلد التاسع، العدد 1، مارس 2018، ص272.

[2] _ عبد الفتاح البيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص 96-97.

[3] _ عبد الفتاح مراد، المرجع السابق، ص 45.

الفئة الأولى: صغار نوابغ المعلوماتية.

ويقصد بهم البالغ المفتون بالمعلوماتية والحسابات الآلية، وكثيرا ما لفتوا النظر في الآونة الأخيرة، ويرتكب هؤلاء الأشخاص الجرائم بغرض التسلية والمزاج مع الآخرين دون أن يكون في نيتهم نيتهم إحداث أي ضرر بالمجني عليهم.

الفئة الثانية: المحترفون في الجريمة الإلكترونية.

ويتمتع أصحابها بخيرة ودراية أكبر ويتقسمون إلى:

فئة المتسللين الهوات Hackers: هم لا يهدفون في حربهم المعلوماتية إلا للمغارات وإظهار القدرات أمام الأقران فلا توجد عادة عندهم هؤلاء أطماع مالية.

فئة القراصنة الخبيثون MALICIOUSHACERS : هم أشخاص هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية، ويندرج تحت هذه الفئة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

فئة حلالي المشاكل الشخصية: هم الأكثر شيوعا يترتب على إجرامهم في الكثير من الأحيان خسائر كبيرة تحلق بالمجني عليهم، رغبة منهم في إيجاد حلول لمشكلات مادية تواجههم، والتي لا يتم حلها بالوسائل الأخرى وغالبا ما يكون المجني عليه المؤسسة التي يعملون بها.

فئة المجرمين المهنيين: وتظم مجرمي الجريمة الإلكترونية الذي يبتغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة، ويعمل المنتمون إلى هذه الفئة في أغلب الأحوال بطريقة منظمة بحيث ينطيق على أفعالهم وصف الجريمة المنظمة.

فئة أصحاب الدعوة المتطرفة:وتدخل في عدادها الجماعات الإرهابية أم المتطرفة، والتي تتكون بدورها مجموعة أشخاص لديهم معتقدات وأفكار اجتماعية سياسية أو دينية، يرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الإجرامية أحيانا[1].

[1] _ بخي فاطمة الزهراء، المرجع السابق، ص 23-25.

وقد بدأ اهتمام الجماعات الإرهابية وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم، يتجه إلى نوع جديد من النشاط الإجرامي، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة بأوروبا باسم THERED BRIGADES بتدمير ما يزيد من 60 مركز للحاسبات الآلية خلال الثمانينات لتلف الأنظار إلى أفكارها ومعتقداتها.

فئة الجناة المقصرية: تضم واحدة من أهم المشكلات التي تتصل بإساءة إستخدام الحاسبات الآلية وهي الإهمال، ولا شك في أن الإهتمام في مجال الحسابات الآلية يمكن أن يترتب عليه في كثير من الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح ففي نيوزيلدا مثلا: قام الاثنان من مبرمجي الحسابات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائر بهذا التغيير، مما أنجم عن مقتل 60 راكب بعد تحطم الطائرة إثر اصطدامها بأحد الجبال وتمت محاكمتها بتهمة القتل الخطأ[1].

المطلب الثاني: التحقيق في الجريمة الإلكترونية.

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل إسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.

والتحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم العادية من حيث الإجراءات وذلك لحادثة هذه الجريمة ومهارة مرتكبيها في الإجرام وحو الأدلة[2].

[1] _ بخي فطيمة الزهراء، المرجع السابق، ص 23-25.

[2] _ سعيد (أبي نعيم)، المرجع السابق، ص 102.

الفرع الأول: تعريف التحقيق الجنائي في الجريمة الإلكترونية.

لا يختلف التحقيق في الجريمة الإلكترونية عن الجرائم الأخرى وسنتناول تعريفه لغة واصطلاحا، ولكي يكتمل هذا التعريف يجدر التطرق إلى تعرف المحقق الذي هو بدوره القائم بجميع وكافة اجراءات التحقيق.

أولا: المقصود بالتحقيق الجنائي في الجريمة الإلكترونية.

يهدف التحقيق إلى جمع الأدلة والتنقيب عليها.

أ-تعريف التحقيق لغة: التحقيق مأخوذ من حقق يحقق تحقيقا، حقق الظن بالله صدقه، الأمر أحكمه- مع فلان- في قضيته: أخذ رأيه فيها.

ب-تعريف التحقيق اصطلاحا: عرف التحقيق بمعناه العام أنه: اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها.

وعرف التحقيق أنه: مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها الإحالة المتهم إلى المحاكمة، كذلك هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا، بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة[1].

وكذلك عرف التحقيق بأنه: " مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهذا التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت كتقدير لزوم محاكمة المدعي عليه أو عدم لزومها "[2].

[1] _ عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلة الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمينة، 2007، ص22.

[2] _ حسن الجوخندار، التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة عمان، الطبعة الأولى، 2008، ص11.

ثانيا: تعريف المحقق.

ذهب جانب من الفقه إلى تعريف المحقق بأنه: " كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، وتحقيقها ويسهم بدوره في كشف غوامضها وصولا إلى معرفة حقيقية الحادث وكشف مرتكبيه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة ".

كما عرف البعض المحقق أو الباحث الجنائي بأنه الشخص الذي يتولى ويتكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها أو اكتشافها بعد وقوعها، وضبط مرتكبيها والأدوات التي استعملت فيها.

وعرف المحقق بأنه: " ذلك الشخص الذي عهد غليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل إلى عمله من جرائم بهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة "[1].

أما المشرع الجزائري فقد وضع تعرفا لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية حيث جاء في نصها ما يلي: " يقوم قاضي التحقيق وفقا لقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الإتهام وأدلة النفي "

الفرع الثاني: خصائص التحقيق الجنائي في الجريمة الإلكترونية:

تعد مرحلة التحقيق الإبتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات، مرحلة هامة في سبيل البحث والتحري عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة الإلكترونية، لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوة برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب إرتكاب الجريمة مباشرة قد لا يبق متاحا بعد مرور وقت قصير على إرتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم،

[1] _ بخي فاطمة الزهراء، المرجع السابق، ص 40.

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 والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته[2].

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 الإبتدائي في الجريمة الإلكترونية:

التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى إكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم للمحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمظاهات البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي.

والهدف من التحقيق الإبتدائي 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

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

[2] _ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009، ص56.

هي الوسائل التي استعملت في ارتكابها، ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي يختلف عن غيره بالنسبة للجرائم الأخرى.

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

– 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 للتعامل مع هذه الجرائم.

– عمل دراسة جادة لكافة الإجراءات التحقيق خطة مسبقة التي يتم وضعها وناقاشها العاملون في فريق التحقيق.

– 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[1].

ب/ تشكيل فريق التحقيق: إن التحقيق الإبتدائي 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،

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

ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي 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 إستعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغض 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، المرجع السابق، ص 613.

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

2/ العناصر الأساسية للتحقيق الإبتدائي 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 الإبتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الإبتدائي[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 الإتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الإختراق 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.

– فصل خطوط الهاتف حتى لا يسيئ الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيؤون 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 هاتيفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتقليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.

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

– 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 معلومات.

– 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].

ثانيا: الخصائص الفنية للمحقق.

تلعب الأجهزة الفنية دروا أساسيا في صيانة أمن المجتمع وذلك إما بالقيام بدور وقائي يهدف إلى منع إرتكاب الجرائم والحيلولة دون وقوعها وتقليل فرص إقترافها، وإما القيام بدور قضائي في ضبط الجرائم ومرتكبيها بعد حدوثها.

ولقد أصاف ظهور الجرائم المعلوماتية النابعة من التطور الإلكتروني أعباء جديدة على أجهزة التحقيق لما يتطلب التصدي لهذه الجرائم من قدرات فيه لم يألفها رجال الضبطية القضائية ولم يتعودو عليها، ما يستلزم ضرورة توفير المهارات المطلوبة في هذا المجال.

[1] _ سعيداني نعيم، المرجع السابق، ص 112-114.

والمشكلة الأساسية التي تواجب المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فمتخصصوا الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربيين على تفهم دوافع الجريمة وجمع الأدلة التقديم المتهم للمحاكة، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول الجريمة الإلكترونية، ولكن من الناحية يتضح فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى، بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم[1].

وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة و مناقشة الشهود وغير تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلزمه عند مباشرته التحقيق في الجريمة الإلكترونية معرفة العديد من الجوانب الفنية يقوم بعمله على أحسن وجه ونذكره منها:

معرفة الجوانب الفنية والتقنية لأجهزة الأجهزة الحاسوب الانترنت والتي تتعلق بالجريمة المرتكبة ذلك أن إفتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقي قد يغطي إلى إتلاف وتدمير الدليل، على اعتبار أن جهله بأساليب ارتكاب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية وتدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات، وبالتالية فإن الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصيها وضبطها وصولا إلى مرتكبيها[2].

كما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والانترنت، وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم

[1] _ سعيداني نعيم، المرجع السابق، ص 115.

[2] _ جميل عبد الباقي صغير أدلة الإثبات الجنائي والتكنولوجي الحديثة، دار النهضة العربية، القاهرة، 2002، ص 115.

الافتراضي من اختراق للشبكات وإعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنها تعطي للمحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الإعتداء على الشبكة والمعوقات التي تحول دون ذاك[1].

المبحث الثاني: السلطات المختصة بالتحقيق في الجريمة الإلكترونية.

المطلب الأول: جهاز التحقيق الجنائي في الجريمة الإلكترونية وأقسامه.

نظرا لانتشار الجريمة الإلكترونية بشكل ملفت للإنتباه، ولأن أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النوع من الإجرام، أنشئت أجهزة خاصة بالتحقيق فيها.

الفرع الأول: تعريف جهاز التحقيق في الجريمة الإلكترونية.

جهاز التحقيق في الجريمة الإلكترونية هو عبارة عن الوظائف المتخصصة إلكترونيا وقانونيا، التي يصدر بها قرار إداري وتشغل بنوعين من الأفراد الضباط وضباط الصف والمدنيين وتحكم علاقاتهم الوظيفية التسلسل النظامي للرتب العسكرية وقانون الخدمة المدنية للمدنيين وقواعد الأمن ويستخدمون التقنية الإلكترونية وضبطها والتي يكون محلها التقنية الإلكترونية الرقمية ونظامها وبرامجها وشبكاتها[2].

الفرع الأول: أقسام جهاز التحقيق الجنائي في الجريمة الإلكترونية.

أصبحت الجرائم في عصر التقنية الحديثة أربعة أنواع، جرائم الإعتداء على النفس، جرائم الإعتداء على المال، جرائم الإعتداء على المصلحة العامة، والجرائم الإلكترونية بعد أن كانت ثلاثة أنواع فقط.

وعلى هذا الأسس قسمت الأجهزة التي تتولى التحقيق في هذه الجرائم إلى:

---

[1] _ حسين سعيد بن سيف الغافري، الجهود الدولية، في مواجهة جرائم الأنترنت، ورقة مقدمة للاتحاد العربي للتحكيم الإلكتروني، 2007، ص 02.

[2] _ محمد مصطفى موسى، التحقيق في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، 2009، ض286.

أولا: أجهزة الأمن العام:

وتختص بالتحقيق في جرائم الإعتداء على النفس والمال[1].

أ- الجرائم الواقعة على الأشخاص:

إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال على ذلك الإعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الإطلاع على البيانات والمعلومات الخاصة.

ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، ويقوم بنشرها على الانترنت، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإدارة على ذلك[2].

ب- الجرائم الواقعة على الأموال:

لقد صاحب ظهور شبكة الانترنت تطورات في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما إنجر عنه تطور وسائل الدفع والوفاء وأصبحت جزء لا يتجزء من هذه المعاملات.

وفي ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية وما أنجز عنه من تطور ووسائل الدفع والوفاء، وفي خضم التداول المالي عبر الانترنت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومنها:

- السطو على بطاقات الإئتمان والتحويل الإلكتورني وفي غير المشروع.

---

[1] _محمد مصطفى، المرجع السابق، ص286.

[2] _ يوسف خليل يوسف العطيفي، الجرائم الإلكترونية في التشريع الفلسطيني، غزة، 2013، ص13.

– القمار وغسل الأموال عبر الانترنت.

– جريمة السرقة والسطو على أموال البنوك.

– تجارة المخدرات عبر الانترنت[1].

ثانيا: أجهزة التحقيق في الجرائم المخلة بأمن الدولة.

وتنقسم إلى :

– أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الداخل وتتولها أجهزة متخصصة مثل مباحث أمن الدولة في مصر، فرنسا والكويت[2].

– أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الخارج وتتولاها أجهزة متخصصة مثل المخابرات العامة في مصر[3].

وقد اشتغل الكثير من الجماعات المتطرفة الطبعة الاتصالية للانترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا معنى آخر في استعمال الانترنت التي سمحت لهم في ارتكاب جرائم غاية الشلك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت الانترنت الكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على مختلف الأشرار العسكرية الاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون فيها نزاعات، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الانترنت[4].

---

[1] _ صغير يوسف، الجريمة الإلكترونية، عبر الانترنت، تيزي وزوو، 2013، ص44.

[2] _ محمد مصطفى، المرجع السابق، ص286.

[3] _ محمد مصطفى، المرجع السابق، ص287.

[4] _ بوظياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11 سبتمبر 2018، ص 258.

ثالثا: جهاز التحقيق في الجرائم الإلكترونية.

وهذا النوع من الأجهزة لم ينشأ بعد في كل الدول العربية وإن كانت بعض الدول قد أنشأته منذ أن استخدمت الحاسب الآلي وشبكات المعلومات، ويرجع السبب الرئيسي لإنشاء جهاز متخصص للتحقيق الجنائي في الجرائم الإلكترونية إلى تحقيق الضبط الإجتماعي الإلكتروني حماية للمجتمع من الجرائم الإلكترونية وذلك للحد منها وضبطها بعد وقوعها، وذلك بالعمل على الحصول على الدليل الإلكتروني من أجل إثبات الجريمة[1].

ويضاف إلى هذا السبب زيادة تفاعل المجرمين مع تقنية المعلومات، فقد وضح أن تقنية المعلومات ستزيد التفاعل بين الإرهابيين، ومهربي المخدرات والأسلحة وجماعات الجريمة المنظمة، فمن خلال عالم مرتبط شكليا سيكون هناك مدخل للمعلومات والتقنية والتمويل والخداع المعقد وتقنيات الأفكار الهدامة، وإذا تم استخدام تلك سواء عن طريق الدول أو فاعلين غير دوليين سيصبح ذبك بمثابة الخاصية الرئيسية لمعظم التهديدات من الداخل للدول.

أما الجزائر فلا زالت إلى الآن تفتقر لجهاز خاص بالتحقيق في الجريمة الإلكترونية إلا أنه انعقدت عدة ملتقيات حول مخاطر هذه الجريمة وناشدت بإنشاء جهاز خاص بالتحقيق في الجريمة الإلكترونية في الجزائر، منها الملتقى الوطني للجريمة الإلكترونية الذي يضم بدائرة قديل بمبادرة من نقابة المحامين لولاية وهران، حيث أختتم بمجموعة من التوصيات منها: أنه لابد من الإسراع في إنشاء الهئية الوطنية المكلفة بتنشيط وتنسيق عمل السلطات المكلفة بمكافحة الجريمة الإلكترونية، ومدها بالمساعدة والاستشارة اللازمة، وحث الخبراء غلى ضرورة الإسراع في إنشاء هذه الهيئة الوطنية التي ينص على استحداثها القانون رقم 04-09 الصادر في 05 أوت 2009 والخاص بالوقاية من الجرائم الإلكترونية ومحاربتها والمكافحة ضدها والقضاء عليها[2].

---

[1] _ محمد مصطفى، المرجع السابق، ص287.

[2] _ بخي فاطمة الزهراء، المرجع السابق، ص 50-51.

الفرع الثالث: معوقات وصعوبات التحقيق في الجريمة الإلكترونية.

يتسم التحقيق في الجريمة الإلكترونية بالعديد من المعوقات والصعوبات التي تؤثر على عملية التحقيق التي تؤدي بها إلى الخروج بنتائج تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون غير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضا على المجرم نفسه، حيث يشعر أن الجهات القضائية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق، لا تجاري خبرته وعلمه بالأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من الجرائم التي تكون أكثر فداحة وأشد ضررًا على المجتمع.

أولا: قلة خبرة القائمين بالتحقيق في الجرائم.

توجد معوقات للتحقيق في الجريمة الإلكترونية تتعلق بالسلطة القائمة بالتحقيق وتجمع لعدة أسباب نذكرها كالآتي:

أ-قلة خبرة القائمين بالتحقيق في هذه الجرائم:

لقلة المهارات الفنية المطلوبة للتحقيق في هذا النوع من الجرائم وتقص المهارات في استخدام جهاز الحاسوب والانترنت وعدم توافر المعرفة بأساليب ارتكاب الجريمة الإلكترونية، وقلة الخبرة في مجال التحقيق في جرائم الحاسوب والانترنت وقلة المعرفة باللغة الأجنبية لاسيما أن للعاملين في مجال الحاسوب مصطلحات عملية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم بينهم، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف الأولى لديهم تعرف بلغة المختصرات[1].

ب- الصعوبات التقنية لاستخدام بروتوكول TCP/IP في الإثبات:

هناك تحديات عند استخدام المحقق بروتوكول TCP/IP كدليل إلكتروني في الإثبات وهي:

[1] _ يوسف جفال، التحقيق في الجريمة الإلكترونية، 2017/2016، ص41-42.

– بروتوكول IP وحدة معلوماتية تحتوي على معلومات عن الحاسوب وليس عن الأشخاص، لذلك فمن الصعوبة إثبات أن شخصا محدد أحدث الفعل غير المشروع، ومع ذلك يمكن أي يستخدم كقرينة قضائية ضد مالك الجهاز غلى أن يثبت العكس.

– الجاني يعمد إلى استخدام عناوين ومعلومات غير صحيحة أو غير قانونية باستخدام حاسوبه الشخصي في ملف خدمات عامة لتجنب التعرف عليه، ويستخدم عنوان IP له مستخدمين كثر ويمكنهم استخدام نفس العنوان، وبعد مرور فترة زمنية يقوم بغلقّ الإتصال، وبعد فترة يعاود الاتصال مما يجعل النشاط الإجرامي غالبا موزعا على عدة عناوين.

– تكون المعلومات المحلية لمصدر عنوان IP غير حقيقية أو زائفة وهدا ممكن باستخدام مصدر زائف لمصدر IP بحيث يظهر بأن المعلومات جاءت من حاسوب محدد وفي الحقيقة جاءت من حاسوب آخر.

ج– ارتفاع تكاليف جمع الأدلة:

إن التحقيق في هذه الجرائم يحتاج إلى خبراء متخصصين وهؤلاء يحتاجون إلى دورات مستمرة متزامنة مع تطور التقنية الإلكترونية، وهذا الأمر مرتبط بالتكاليف باهظة، وكذلك التفتيش عن الأدلة يحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات شيئا[1].

ثانيا: عوائق تتعلق بالجريمة والجهة المتضررة منها.

المعوقات المتعلقة بالجريمة الإلكترونية تتمثل في:

– خفاء الجريمة وغياب الدليل المرئي وصعوبة التعرف عليه.

– الإعاقات المتعلقة بالوصول إلى الدليل لإحاطته بوسائل الحماية الفنية.

– سهولة محو الدليل أو تدميره في زمن فصير جدًا.

[1] _ يوسف جفال، المرجع السابق، ص42–43.

الجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدًا بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعمل بها فإنه يستهدف بالمحو السريع عدم استطاعة السلطات إقامة الدليل ضده، وبالتالي تملصه من مسؤولية هذا الفعل وإرجاعه إلى خطأ نظام الحاسوب الآلي أو الشبكة أو في الأجهزة.

أما المعوقات المتعلقة بالجهات المتضررة من جرائم الحاسوب والانترنت، وهي عدم إدراك خطورة جرائم الحاسوب والانترنت من قبل المسؤولين بالمؤسسات المجني عليها التي تعد من معوقات التحقيق، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالأنترنت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحاتها واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، وهذا يؤدي إلى الإحجام عن الإبلاغ عن الجريمة التي تعتبر من أهم وأخطر الإشكالات التي تتعلق بعملية الإبلاغ عن الجريمة الإلكترونية، حيث يحجم البعض عن إبلاغ السلطات المختصة بالجرائم التي ارتكبت بحقهم خاصة وإذا تعلق الأمر بالمؤسسات المالية أو ما شابهها[1].

المطلب الثاني: أجهزة التحقيق في الجريمة الإلكترونية.

نظرًا لتفاقم الظاهرة الإجرامية المعلوماتية من يوم لآخر ونظرًا 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 الانتربول واليوربول والأنريبول.

[1] _ يوسف جفال، المرجع السابق، ص 43-44.

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

الفرع الأول: 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].

أولا: 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 والاتصال ومكافحتها وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، [2] 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 الإستراتيجية للاقتصاد الوطني[3].

[1] _ ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، جامعة باتنة، 2015-2016، ص 171.

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

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

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.

تظم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين، وفقا لأحكام قانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعلومات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للإتصالات الإلكترونية.

وذلك قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى تحت سلطة القاضي المختص.

للإشارة هنا تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال 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 الفيس بوك والتويتر لصالح التنظيمات الإرهابية نتيجة

استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية داعمة وتدعو للمشاركة في منتديات إرهابية غلى جانب اتصالات محلية ودولية[1].

ثانيا: 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 من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام[2].

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 والإتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات[3].

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.

---

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

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

[3] _ يوسف جفال، التحقيق في الجريمة الإلكترونية، 2017/2016، ص20.

– 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 ولايات الوسط، الشرق، الغرب، الجنوب، لتقوم فيما بعد بتعيم 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 ومكلفحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني وهو قيد الإنشاء[2].

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

[2] _ يوسف جفال، المرجع السابق، ص21.

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].

الفرع الثاني: الهيئات القضائية الجزائية المتخصصة.

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون رقم 04-14 المؤرخ في 1à 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 غلى القضاء وإعادة الإعتبار 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 مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت السنوات الأخيرة تزايد في العلميات الإرهابية وتزايدًا في أعمال المنظمات الإجرامية واستعمالها القضائي الافتراضي للاستفادة من خصائص الجريمة المعلوماتية.

---

[1] _ سعيدة بوزنون، المرجع السابق، ص 53-54.

[2] _ القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 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.

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[1].

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم رقم 06-348 المؤرخ في 05-10-2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم بحيث شمل التقسيم إضافة بعض المجالس القضائية بمقتضى المادة 3-4-5- المعدلة للمواد 3-4-5 من المرسوم السابق وجاء التقسيم كالتالي[2]:

محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: الجزائر، الشلف، الأغواط، البليدة، تيزي وزوو، الجلفة، المدية، المسيلة، وبومرداس، البويرة، وعين الدفلى.

محكمة قسنطينة ويمتد اختصاصها للمجالس القضائية: قسنطينة، أم البواقي، باتنة، بجاية، تيسة، جيجل، سطيف، سكيكدة، عنابة، ثالمة، برج بوعريريج، الطارف، خنشلة، سوق أهراس، وميلة.

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

[2] _ سعيدة يوزنون، المرجع السابق، ص 54.

محكمة ورقلة ويمتد اختصاصها للمجالس القضائية التالية: ورقلة، أدرار، تمنراست، إليزي، بسكرة، الوادي، وغرداية.

محكمة وهران ويمتد الاختصاص بها إلى المجالس القضائية التالية: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسنمسلت، النعامة، عين تيموشنت، وغليزان.

بحيث يشمل اختصاص كل جهة فضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا، جنويا، شرقا، وغربا، وذلك لدى أربع محاكم تسمى أقطابا جزائية، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيه الجريمة الإلكترونية[1].

[1] _ سعيدة بوزنون، المرجع السابق، ص 55.

الفصل الثاني:
إجراءات التحقيق والمتابعة في الجريمة الإلكترونية.

تعتبر الجريمة الإلكترونية من الجرائم الحديثة النشأة، ولذلك فإن القواعد العامة لمكافحة الجريمة الإلكترونية غير صالحة وإنما استحدث قواعد وآليات جديدة خاصة فقط بالجريمة الإلكترونية نظرا لخصوصيتها من الناحية الإجرامية خاصة في مجال التحقيق، فيجب على المحقق في حالة وقوع أي جريمة لابد أن يستظهر أركانها الثلاث، الشرعي، والمادي والمعنوي للجريمة محل التحقيق.

أ/ إظهار الركن المادي: يتطلب النشاط أو السلوك الإجرامي في جرائم الأنترنت وجود بنية رقمية واتصال بالانترنت، وأيضا معرفة بداية هذا النشاط والشروع فيه نتيجته

ب/ إظهار الركن المعنوي للجريمة الإلكترونية: يتمثل في الحالة النفسية التي يكون عليها الجاني التي دفعت به لإرتكاب الجريمة والعلاقة التي تربط بين الشخص الجاني والفعل المرتكب أو المكون للجريمة ويتمثل أساسا في العلم و الإدارة المعروف باسم القصد الجاني العام.

ج/ علانية التحقيق من الضمانات اللازمة للعدالة الجنائية علاقة التحقيق في الإجراءات الجنائية وهي تختلف عن التحقيق الإبتدائي عنها في مرحلة المحكمة[1].

[1] _ خالد ممدوح إبراهيم، فن التحقيق الجاني في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2008، ص 59.

المبحث الأول: مرحلة جمع الاستدلالات والتحقيق فيها.

إن أهمية جهاز الشرطة القضائية في كشف عن الجريمة الإلكترونية والتعرف على المجرم الإلكتروني، تبعه استعداد المشرع الجزائري لأساليب التحري الخاصة المستعملة بما تناسب ومتطلبات ضبط الوجه الجديد للإجرام حتى يسمح للقضاء والشرطة أن يتكيف دورها في مهامها مع الإجرام الجديد مستمدة شرعيتها من المواثيق الدولية التي صادقت عليها الجزائر، وخاصة المادة 20 من اتفاقية باليرمو لمكافحة الجريمة المنظمة عبر الحدود الوطنية التي أدرجت الجريمة الإلكترونية كشكل من أشكال الجريمة المنظمات[1].

ما تجدر الإشارة إليه أن هذه الإجراءات لا يرخ ضبها إلا في بعض الجرائم المعنية من طرف المشرع الجزائري على سبيل الحصر لا المثال بما فيها الجريمة الإلكترونية التي استدركها المشرع بموجب تعديل قانون الإجراءات الجزائية، القانون رقم 06-22 والتي تتمثل في النقاط التالية:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية ولا سلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين من أجل إلتقاط وتثبيت وبث وتسجيل الكلام من طرف شخص أو عدة أشخاص يتواجدون في أماكن عمومية أو خاصة أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.
- جواز التسرب أو الاختراق للكشف عن الجريمة الإلكترونية حسب المادة 65 مكرر 12 من القانون 06-22 المتضمن قانون الإجراءات الجزائية.
- ولأنه إجراء غير مألوف وخطير في عمل سلطات الضبط القضائي أحاطه المشرع الجزائري بجملة من الضوابط أبعادها، الإذن القضائي بالسرب من قاضي التحقيق أو وكيل الجمهورية، المادة 65 مكرر 11، وأيضا احترام المدة القانونية للسرب.

[1] _ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، الطبعة 2، دار الفكر الجامعي، مصر، 2011، ص 76.

المطلب الأول: جمع الاستدلالات في الجريمة الإلكترونية.

المحقق أو المحتوى هو الشخص المكلف بإبراء التحري بواسطة الحاسب الإلكتروني عن المتحري عنه، سواء كان شخصا أو مكانا أو شيئا حسب طبعته، على المتحري أن يكون لديه استعداد وقدرة على إجراء مهامه وأن يميز من الحقائق والأقوال والآراء والاستنتاجات، حتى يتحوّل هذا الاستعداد لقدرات خاصة تساهم في قيام المتحري بمهامه بشكل سليم، من أهم السيمات التي يجب أن تتوفر في المحقق يمكننا أن نذكر، دقة الملاحظة في تتبع للمهتمين والشهود أثناء التعامل معهم، سرعة الأداء، كتمان السر حتى لا يضر بمصالح الغير الترتيب والدقة والتأني وبذل العانية، الصبر، قوة الذاكرة[1].

المتحري المهني هو مأمور الضبط القضائي المسؤول عن تلقي البلاغ وسماع الشهود وسؤال المتهمين، والمهارة الرئيسية التي يجب على المتحري تنميتها بالتدريب هي ترتكز في مهارات الإتصال التي أصبحت اليوم أساس أي تعامل أمني سواء على المستوى الشخصي أو العملي تنقسم هذه المهارة إلى 3 أقسام هي: الحديث إلى الغير، الإنصات، كتابة المحاضر.

وبما أن الحديث إلى الغير في مجال التحري يكون في حدود توجيه الأسئلة والإستفسارات، فيجب أن تكون مقنعة مليئة بالثقة، في حين أن كتابة المحاضر يجب أن تتميز بالوضوح والتسلسل المنطقي والإقناع لتصل إلى العدالة، كما أن الإنصات وحسن الإستعمال يساعد المتحري في اتخاذ القرارات المحبة.

الفرع الأول: تلقي البلاغات والشكاوي.

أولا: تلقي البلاغات في الجريمة الإلكترونية.

الأصل أنه يجب على رجال الشرطة قبول البلاغات أو الشكاوي التي تقدم إليهم سواء كانت كتابية أو شفهية، وعند وردها للقسم تقيد في دفتر خاص بتلقي البلاغات، كما يجب على

[1] _ مروك نصر الدين، محاضرات في الإثبات الجنائي، دار هومة، الجزائر، 2011، ص 81.

المتحري أو المتحقق إخطار رئاسته في حالة الجرائم الإلكترونية، وإخطار الجهات المختصة مثل: إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، ومن الأخطار الشائعة في هذا المجال، الامتناع عن قبول البلاغ أو الشكوى بدعوى عدم الاختصاص المكاني أو النوعي بها، في حين أن الواجب إتخاذ الإجراءات المقرة بشأنها، تم إخطار جهة الاختصاص وإحالة المحضر إليها.

ويقوم المتحري بجمع الأدلة وفحص البلاغ أو الشكوى إجراءات معينة تتمثل في المعاينة وجمع الأدلة والتحقيق[1].

كما يتم الإبلاغ عن الجريمة الإلكترونية عن طريق الانترنت أو ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق، كإبلاغها عن وجوه صفحات أو مواقع غير مشروعة بإرسال رسالة إلكترونية مثلا تتضمن التبليغ عنى وجود موقع منشور فيه صور الإستغلال الجنسي للأطفال.

والمعلومات التي يجب معرفتها من المبلغ والتي ينبغي أن يدونها المحقق عند تلقي البلاغ، يمكن الحصول عليها من خلال طرح أسئلة عن تاريخ وقت تلقي البلاغ، المعلومات الخاصة، طبيعة ونوع الجريمة الإلكترونية، محل البلاغ، إلى غيرها من الأسئلة المتعلقة بالجريمة.

ثانيا: الشكوى في الجريمة الإلكترونية.

قد يترتب على الجريمة ضرر خاص قد يصيب أحد الأفراد ماديا أو معنويا، فينشأ له حق تحريك الدعوى العمومية بتقديم شكوى أمام الجهة المختصة بالتحقيق حيث نص المشرع الجزائري في قانون الإجراءات الجزائية أنه يحق لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص وقد عرفت الشكوى بأنها البلاغ أو

[1] _ خالد عباد الحلي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، 2011، ص 79.

الإخطار الذي يقدمه المجني عليه أو ووكيله الخاص إلى السلطات المختصة طلبا تحريك الدعوى العمومية بشأن جريمة معينة.

ولقد خصصت العديد من المراكز لمعالجة هذه الشكاوي من بينها مركز نلقي الشكاوي عن جرائم الإحتيال عبر الأنترنت المؤسسة في فيرجينيا الغربية بالولايات المحتدة الأمريكية من طرف مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء من أجل مكافحة ظاهرة الإحتيال عبر الانترنت.

الفرع الثاني: الاستجواب وسماع الشهود في الجريمة الإلكترونية.

أولا: الاستجواب:

وهو أن يمثل أمام المحقق حتى يتحقق من هويته ومحيطه علما بكل الوقائع المنسوبة إليه وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخبر المتهم في أن له الحق في توكيل محامي وإن لم يقدر يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إذا ما طرأ تغيير عنوانه أن يخطر المحقق بذلك[1].

ثانيا: سماع الشهود في الجريمة الإلكترونية.

سماع الشهود هو إجراء من الإجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة، بحيث يستدعي أشخاص ليست لهم علاقة بالجريمة، إلا أن وجودهم ضروري للكشف عن الجرائم والقبض عن مرتكبها يختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية.

المطلب الثاني: التحقيق في الجريمة الإلكترونية.

عند تلقي المحقق البلاغ أو الشكوى بوقوع جريمة ما، فإنه ينتقل مباشرة إلى مكان وقوعها مع إخطار وكيل الجمهورية، وذلك بهدف التنقيب عن الأدلة وحمايتها إلا أنه تجدر الإشارة إلى

[1] _ خالد عياد الحلبي، المرجع السابق، ص 80.

أن مسرح الجريمة الإلكتروني بالإضافة إلى المسرح المادي يوجد مسرح إلكتروني متمثل في البيئة الإلكترونية التي يجد فيها المحقق صعوبة استخلاص الدليل منها، ممّا يدفعه بالاستعانة بالخبراء الفنيين في هذا المجال، في معاينة مسرح الجريمة أو القيام بالعمليات التفتيش والضبط وفحص آثار الجريمة، لا تشكل خللا فنيا أو قانونيا، كما هو الحال في التحقيق مع الشهود والمتهمين، إذ أن أخذ أقوال الشهود واستجواب المتهمين يعتمد على خبرات المحققين، ويعتبر الاستجواب مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق، ومطالبته له بإدلاء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما، وذلك قصد محاولة الكشف عن الحقيقة واستظهارها بالطرق القانونية.

تتولى سلطة مختصة إجراء الاستجواب، إذ يجب على جهات التحقيق أن تكون مؤهلة للتحقيق في الجرائم المعلوماتية حتى يمكن استيعاب واقعة التحقيق، إن طريقة توجيه الأسئلة وترتيب أولوياتها واستنتاج الحقائق من الطريقة التي يتحدث بها المتهم وقراءة لغة الجسد لديه، أمور مهنية لا يوفيها حقها إلا المحققون الذين اكتسبوا الخبرة والمعرفة العلمية[1].

يمكن القول بصفة عامة أنه لا يوجد حتى الآن خبير معلوماتي لديه المعرفة المتعمقة في سائر أنواع الحسابات وشبكاتها، كما لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم، ولهذا يتمتع مأمور الضبط القضائي وكذلك المتحري بحرية كاملة حتى يتمكن من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها هو أنها مناسبة، ولذلك لأي منهما أن يندب الخبير يأنس فيه الكفاءة الفنية اللازمة لحل هذه المسألة.

الفرع الأول: التفتيش وضبط الأدلة.

أولا: التفتيش:

تتميز الجريمة الإلكترونية عن غيرها من الجرائم كونها من الجرائم التي يصعب إثباتها لذلك يجيز المشرع الجزائري التفتيش في المنظومة المعلوماتية ضد كل جريمة يحتمل وقوعها

[1] _ محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2010، ص 102.

وتتقلص معه الضمانات التي يشترطها المشرع عادة في الجرائم العادة الأخرى، نظرا لسرعة ارتكابها ومحو آثارها وخطيها الحدود الوطنية.

وإذا كان التفتيش يقصد به البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها وكل ماله علاقة بها أو بفعالها، فإن عالم التقنية قد يتميز عن الجرائم العادية بكونه يتكون من شقين هما الكيانات المادية والتي تنطبق عليها القواعد العامة للتفتيش من حيث مكان تواجدها بحسب ما إذا كان مكان عام أو خاص[1].

كمسن المتهمة مثلا، أما إذ تعلق الأمر بتفتيش الكيانات المعنوية كالبرامج ونظم الشغل وقواعد البيانات وبعيدا عن الآراء الفقهية التي قيلت حولها فقد نص المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب بنصه على أنه : " إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأي عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على إمتداد التراب الوطني أو بأمر ضباط الشرطة القضائية للقيام بذلك".

ثانيا: ضبط الأدلة:

هو ضبط الأدلة أو الأشياء التي تفيد في ظهور الحقيقة في الجريمة التي وقعت، فالضبط في اغلب الأحيان هو غرض التفتيش وإن لم يكن له السبب الوحيد، فقد يتم الضبط استنادا لأسباب أخرى غير التفتيش من ذلك المعاينة وما يقدم المتهم والشهود لمأموري الضبط القضائي، لذا يرى جانب من الفقه أن الضبط ليس من إجراءات التحري بل من إجراءات الإستدلال خاصة إذا تم في مكان يجوز لسلطات الضبط دخوله مثل الأشياء التي يتم العثور عليها خارج المساكن أو في الطريق العام أو في الحقول أو غيرها.

والضبط لا يخرج من كونه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، سواء في ذلك أن يكون هذا الشيء عقارا أو منقولا الضبط حسب

[1] _ بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، 2012، ص 74.

الأصل لا يراد إلا على أشياء مادية فلا صعوبة بالتالي بضبط الأدلة في الجريمة الواقعة على المكونات المادية للكومبيوتر، كرفع البصمات مثلا عنها وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخة غير مشروع أو إتلافه بوسائل تقليدية كالكسر، الحرق، لكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس وفي ضبط البيانات الكمبيوتر لعدم وجود أي دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثواني معدودات ولعدم معرفة كلمة السر أو ثغرات المرور أو ترميز البيانات[1].

الفرع الثاني: المعانية وندب الخبراء في الجريمة الإلكترونية.

أولا: المعانية:

المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تسلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يري المحقق أن لها صلة بالجريمة، والأصل أن إجراء المعاينة متروك لتقدير المحقق، لا يقوم بها إلا إذا كمان هناك فائدة من ورائها، كما أن هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية ملتبس بها، يجب على القائمين بالمعاينة تأمين الأجهزة والمعدات التي يتم الإستعانة بها خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة وإخطاره مسبقا حتى يستعد من ناحية الفنية والعملية ويعد خطة مناسبة للمعاينة مع مراعاة ما جاء في القوانين الجنائية حول المعاينة تحقيقا لمبدأ الشرعية[2].

[1] _ عبد الفتاح بومي حجازي، المرجع السابق، ص 238.

[2] _ عبد الفتاح بومي حجازي، مكافة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، الطبعة الأولى، بدون سنة، ص 237.

ثانيا: ندب الخبراء:

تعتبر الخبرة من أهم الإجراءات التي تتخذ للتثبيت عن الأدلة التي تساعد عن الكشف عن الجريمة الإلكترونية، كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها[1].

الخبير هو كل شخص له إلمام بأي علم أو فن سواء كان اسمه مقيدا في جدول الخبراء أو على مستوى المحاكم أم لا، وهو كل شخص له دراية بمسألة من المسائل، وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه، فيمكنه أن يستشير فيها خبراء كما هو الحال في تقرير الصفة التشريعية في جرائم القتل أو تحليل المادة المطعومة في جريمة تسمم، أو فحص لخطوط الكتابة المدعي بتزويرها، ولما كان قاضي التحقيق هو المختص بالتحقيق، قد يتعرض في عمله لمسائل فنية يصعب عليه كرجل قانون البت فيها، حينئذ يجوز له ندب أهل الخبرة، حتى يخرج التحقيق في صورة موضوعية صادقة.

[1] _ ضريفي نادية، سلطات القاضي الجاني في تقدير الدليل الإلكتروني، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 219، ص 124.

المبحث الثاني : مـرحلـة المحـاكمـة

يتصل القاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي لطلب الإفتتاحي لإجراء تحقيق، وإما عن طريق شكوى جزائية مقدم من المضرور وهذا ما أكدته 3/38 من قانون الإجراءات الجزائية الجزائري على "... يختص بالتحقيق في الحادث بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و 73

ويتقيد القاضي التحقيق بالوقائع دون الأشخاص طبقا المادة 3/67 و4 من قانون الإجراءات الجزائية " ...ولقاضي التحقيق سلطة الإتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المجال تحقيقها إليه .فإذا وصلت لعلم قاضي التحقيق وقائع لم يشير إليها في طلب إجراء التحقيق تعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع [1]

المطلب الأول : إختصـاص المحكمة .

يختض القضاء الوطني في الفصل في الدعوي الجزائية كما يقوم بتحديد ايطارها الجغرافي او دائرة اختصاص مكاني تتحدد بمنطقة معينة من اقليم الدولة

الفرع الأول: الإختصـاص المحـلي فـي الجـريمة الإلكتـرونية

الفصل الثاني الجريمة الإلكترونية بين التجريم والمتابعة 93 .طبقا نص المادة 37 من قانون الإجراءاتيتحددد الإختصاص المحلي للجريمة في ثلاث ضوابط في أو المكان إقامة المتهم أو مكان الضبط، كما نصت أحكام المرسوم التنفيذي رقم 06 ــ 348 المؤرخ في 5 أكتوبر 2006 على تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دائرة إختصاص محاكم أخرى ، ويتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة وكذا محكمة قسنطينة ومحكمة ورقلة وقسم محكمة وهران وفي نطاق الجرائم الإلكترونية فإن

[1] _ بعرة سعيدة، مرجع سابق، ص92.

السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان اخر ، فإن الإختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة ، وتعد الجريمة الإلكترونية إذا تمت عن طريق شبكة الأنترنت جريمة مستمرة حيث تعتبر أنها إرتكبت في جميع الأماكن التي إمتدت الجريمة فيهاومتى كانت الجريمة الإلكترونية ، أيا كان نوعها ، فقد وسع المشرع الجزائري من إختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيات الإعلام والإتصال إذا إرتكبت خارج الإقليم الوطني ، أو إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإقتصادية الإستراتيجية للدولةوذلك في إطار التعاون الدولي[1].

الفرع الثاني- الإختصاص النوعي في الجريمة الإلكترونية.

يتحدد الإختصاص النوعي للمحكمة الفصل في القضية معروضة عليها تبعا لنوع الجريمة التي ينظر فيها ، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الإتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري ، كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الإستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 قانون الإجراءات الجزائية.

ولأن الطبيعة التقنية المعقدة للجرائم المعلوماتية تفرض على رجال القضاء لتكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع مع بعض أنواع الجرائم المتعلقة بالمتاجرة بالمخذرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبيض الأموال والإرهاب ، والجرائم المتعلقة بالتشريع الخاص بالصرف بإجراءات خاصة إذا جعل الإختصاص ينعقد إلى دائرة إختصاص أخرى وهذا مانصت عليه المواد 37 ، 40 ، والمادة 329 من قانون الإجراءات الجزائية أثر التعديل الذي جاء به القانون رقم 04 ـ 14 المؤرخ في 10نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 06 ـ 348 والمتعلق بالتنظيم القضائي حيث نص على

[1] _ بعرة سعيدة، مرجع سابق، ص93.

إنشاء أقطاب قضائية متخصصة ذات إختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة ، قسنطينة ، وهران ، ورقلة [1].

المطلب الثـانـي : تشكيلة المحكمـة.

تختلف تشكيلة المحكمة الجزائية بحسب قسم ونوع قسم الجنح خاصة بجريمة الإلكترونية على مستوى المحكمة يتشكل من فرد ويساعده كاتب ضبط وبحضور وكيل الجمهورية أو مساعديه. أما الغرفة الجزائية على مستوى المجلس قضائي فالتشكيلة فيها ثلاثية ، أي تتشكل من رئيس غرفة ومستشارين إثنين بالإضافة إلى كاتب ضبط وبحضور النائب العام أو أحد مساعديه .أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبطوالنيابة العامة أو من يمثلها [2]

الفــرع الأول : إجـــــراءات المحـــــاكمة.

تستهل المحكمة جلستها بالإعلان أولا عن إفتتاحها بالقول بإسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم ، ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها. ، وإذا كانت الدعوى غير مهيأة للحكم أمرتالمحكمةبتأجيلها إلى أقرب جلسة ، وفي هذه الحالة وطبقا لأحكام المادة 339 مكرر 6 المستحدثة بموجب الأمر 15 ـ 02 المؤرخ في 23 جويلية 2015 من قانون الإجراءات

الجزائية تتخذ المجكمة إحدى الإجراءات التالية:

ترك المتهم حرا . ـــ إخضاع المتهم لتدابيرأو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر 1 قانون الإجراءات الجزائية .ـــ وضع المتهم في الحبس المؤقت .ـــ مع الإشارة وأن هذه التدابير لا تقبل الإستئناف .

[1] _ بعرة سعيدة، مرجع سابق، ص93.

[2] _ مرجع نفسه، ص94.

وإذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب إجراءات المثول الفردي فإنه يساق بواسطة القوة العمومية لحضور الجلسة ويخطره رئيس الجلسة بأن له الحق في إختيار محام الدفاع عنه فإن طلب ذلك أمهاه القاضي مهلة لاتقل عن ثلاثة أيام لتحضي دفاعه .ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها بالتفصيل من طرف القاضي و بعدها يقوم القاضي بسماع الشهود .وبعد الإنتهاء من تحقيق تعطى الكلمة للطرف المدني فقط دون المطالبة بالعقوبات الجزائية ، لتقوم بعد ذلك النيابة العامة بالمرافعة وتقديم إلتماساتها في الشق الجزائي فقط وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم إلتماساتها ، ويكون بعدها لنيابة العامة والمدعى حق الرد على مرافقة محامي المتهم ، وتعطى الكلمة الأخيرة بعدها للمتهمومحاميهثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أويحدد تاريخ لاحق منطق بالحكم. [1]

الفـرع الثـاني : القـواعـد العـامة للمحـاكمة.

تنفيذ المحاكمة بمجموعة من المبادئ تنطبق على محكمة الجزائية لقسم الجنح على مستوى المحكمة أو الغرفة الجزائية سنحاول شرحها على توضيح الأتي بيانه :

أولا: عـلانـية الجـلسة : جل التشريعات تقر بمبدأ علانية الجلسة ، وذلك أن العلانية تسمح للجمهور بمراقبة عمل المحكمة ومنه الإطمئنان والشعور بالعدالة وهذا على التحقيق الأولي الذي تقوم به ضباط الشرطة القضائية وكذا التحقيق الإبتدائي الذي تقوم به الجهات التحقيق ، فكلاهم يتم في سرية ، إلا أن العلانية ليست في جميع الجلسات بل القاضي سلطة تقديرية في إخراج القصر من الجلسة ، كما يمكن أن تكون الجلسة سرية إذا كان في علانيتها خطر على نظامالعام والأداب العامة ، إلا أن هذا الحكم يجب أن يصدر في جلسة علنية ، ويحكم هذا المبدأ نص المادة 285 من قانون الإجراءات الجزائية الجزائري .

[1] _ بعرة سعيدة، مرجع سابق، ص95.

ثانيا: شفوية المرافعات: فأطراف الخصومة الحق في مناقشة كل دليل يعرض بالجلسة حتى يتمكن الجميع من الدفاع عن نفسه ولايتم الإكتفاء بالتحقيقات الأولية والإبتدائية التي سبقت المحاكمة .

ثالثا: حضور أطراف الخصومة: لا يجوز إجراء المحاكمة دون أطراف الخصومة لذلك أوجب المشرع حضور كل من الضحية والمتهم أما بالنسبة لنيابة فهي جزء من التشكيلة.

رابعا: تدوين التحقيق النهائي: لا يمكن للمحكمة أن تنعقد في حالة غياب أمين الضبط لأن دورخ يتجسد في تدوين كل ما يدور بالجلسة وفي الأخير نستنتج أن الجريمة الإلكترونية لم يخص لها إجراءات المتابعة خاصة بها وإنما تخضع نفس إجراء الجريمة لتقليدية [1]

[1] _ بعرة سعيدة، مرجع سابق، ص96.

الخاتمة

الخاتمة:

لقد أضحى العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية، حيث أصبحت حياتنا اليومية تستدعي اللجوء إليها، فقد مكنت طرق المعالجة الآلية المجتمعات من تجاوز فكرة الحدود الإقليمية، نظرًا لكون التكنولوجيا عابرة للحدود.

وأمام هذا التطور قد إرتبط به ظهور ما يعرف بالجريمة الإلكترونية، وذلك نتيجة للاستخدام السيئ للمعلوماتية أو الحاسوب، الذي نتج عن هذا الأخير عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن المعطيات منة جهة وتمس بحرية الأفراد والمؤسسات من جهة أخرى.

ولأن الحماية الفنية مهما بلغت درجتها من التعقيد والصعوبة، فهي لا تستطيع المقاومة أمام التطور التقني الذي تشهد تقنيات الإختراق، وكذا النصوص التقليدية في توفير الحماية الخاصة من الناحية الإجرائية ما ننع العديد من الدّول إلى إبرار اتفاقيات وسن قوانين داخلية من أجل توفير الحماية ومحاربة هذا النوع من الجرائم ومن هذه الدول الجزائر ولقد حاولنا الوقوف على مفهوم جهاز التحقيق وما يليها من الجريمة الإلكترونية في التشريع الجزائري وخصائصها وكذا أجهزة التحقيق في الجريمة الإلكترونية ومن خلال دراستنا توصلنا للنتائج التالية:

– أن قانون الإجراءات الجزائية الجزائري ينص فقط على القواعد العامة التي تطبق على الجرائم التقليدية وكذا على المعلوماتية من خلال بعض الإجراءات الخاصة الممثلة في حجز المعطيات أو البيانات وكذا مراقبة الاتصالات الإلكترونية وحفظ البيانات.

– أن بعض الإجراءات تعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية، كالمعانية على المسرح الجريمة وكذا التفتيش الإلكتروني وضبط الدليل الرقمي والمستحدث هو إجراءات جديدة جاء بها تعديل قانون الإجراءات الجزائية الجزائري سنة 2006 التي تعرف بأساليب التحري حيث جاء بإجراءات لا تطبق إلا على الجرائم الإلكترونية كإجراءات المحاكمة التي

يخص بها الأقطاب الجزائية المتخصصة وبالإضافة غلى إجراءات خاصة جاء بها قانون 09-04.

- بالرغم من وجود نصوص قانونية فإن مكافحة الجريمة الإلكترونية رهينة بالمعيقات الإجرائية في مجال المتابعات فإن أول إشكال أو عائق هو غياب القدرات التأملية والوسائل الفنية التي تتيح سرعة إدراك ما حصل، وأن غياب التأميل قد يؤدي إلى إتلاف الدليل وإتلاف مرتكبي هذه الجرائم من العقاب بالإضافة إلى مشكلات في القانون الواجب التطبيق كون الجريمة الإلكترونية عابرة للحدود.

- إن هذه الجريمة ومع تعدد أنماطها وإحتراف مرتكبيها، سواء كانت جرائم واقعة على النظام المعلوماتي أو بإستخدامه، فإن لها جوانب سلبية خطيرة تهدد أمن وسلامة الفرد والمجتمع وهي تتسم بالغموض حيث يصعب إتباعها والتحقيق فيها ممّا يضع مسؤولية كبيرة على ضباط الشرطة والقضاء.

- أغفل المشرع الجزائري الجرائم المالية بمنتوجات الحاسب الآلي، حيث لم ينص على جريمة التزوير المعلوماتي، واخضاعها للنصوص التقليدية الخاصة بتزوير المحرّر ولم يوسع من مفهوم المحرّر ليشمل التزوير المعلوماتي.

كما لم يقم بتحديد الجريمة المرتكبة باستخدام النظام المعلومات وترك المجال واسع ليدخل في نطاقها كل ما تفرزه التقنية الحديثة وتطوراتها من خلال هذه النتائج استطعنا وضع الاقتراحات التالية:

- ضرورة تدريس الجريمة الإلكترونية في كلية الحقوق فمثلا إدراجها في مقياس القانون الجنائي والإداري الإلكتروني في مقياس القانون الإداري والمحكمة الإلكترونية في مقياس قانون الإجراءات الجزائية.

- نرجو من المشرع الجزائري التوقف عن استيراد القوانين من البلدان الأجنبية والإهتمام أكثر بالأدمغة الجزائرية والإعتماد على خبرتها في وضع التشريعات الوطنية.

- الاستفادة من التجارب الدولية في هذا المجال لكسب المهارات اللازمة لمكافحتها.

الخاتمة:

– ضرورة تدريب وتأهيل أفراد الضبطية القضائية على كيفية التعامل مع هذا النوع من الجرائم بعقد دورات تكوينية بشكل دائم.

– لابد أن يكون التفتيش على المكونات المادية للحاسوب الآلي.

– المعاينة في الجريمة الإلكترونية يكون على مستويين وهما المسرح التقليدي والمسرح الافتراضي.

– ضبط الدليل الرقمي إلكترونيا وسماع الشهود الخاصين والعاملين بالجانب المعلوماتي.

– التسرب الرقمي.

– مراقبة الاتصالات الإلكترونية وحفظ البيانات.

– مكافحة الجريمة الإلكترونية على المستوى الوطني والدولي.

قائمة المراجع

قائمة المصادر والمراجع:

أولا: الكتب:

– أشرف عبد القادر قنديل، النظرية العامة للبحث الجنائي، وأثرها في اقتناع القاضي، دار الجامعة الجديدة، مصر، 2011.

– بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، 2012.

– جميل عبد الباقي أدلة الإثبات الجنائي والتكنولوجي الحديثة، دار النهضة العربية، القاهرة، 2002.

– حسن الجوخندار، التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة عمان، الطبعة الأولى، 2008.

– حسين سعيد بن سيف الغافري، الجهود الدولية، في مواجهة جرائم الأنترنت، ورقة مقدمة للاتحاد العربي للتحكيم الإلكتروني، 2007.

– خالد عباد الحلي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، 2011.

– خالد ممدوح إبراهيم، فن التحقيق الجاني في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2008.

– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009.

خالد ممدوح، أمن الجريمة الإلكترونية، الدار الجامعية، الإلكترونية، الإسكندرية، 2008.

– سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجتها في الإثبات الجنائي، دار الكتب القانونية، مصر، 2011.

– ضياء مصطفى عثمان، السرقة الإلكترونية، دار النفائس، عمان، الطبعة الأولى، 2011.

قائمة المراجع:

– عائشة بن قارة مصطفى، حجة الدليل الإلكتروني في الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010.

– عبد الفتاح بومي حجازي، مكافة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، الطبعة الأولى، بدون سنة.

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

– عبد الفتاح بيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006.

– علي حسن محمد الطوالية، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديثة، الأردن.

– فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الثالثة، دار الثقافة والنشر والتوزيع، الأردن، 2010.

– محمد أمنية الشوايكة جرائم الحاسوب والأنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009.

– محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2010.

– محمد طارق عبد الرؤوف، جريمة الإحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2011.

– محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، ديوان المطبوعات الجامعية، 1999.

– محمد مصطفى موسى، التحقيق في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، 2009.

– مروك نصر الدين، محاضرات في الإثبات الجنائي، دار هومة، الجزائر، 2011.

– نائلة عادل محمد فريد قورة، جرائم الحساب الآلي الاقتصادية، منشورات الحلبي الحقوقية لبنان، الطبعة الأولى، 2005.

– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، الطبعة 2، دار الفكر الجامعي، مصر، 2011.

– يوسف خليل يوسف العطيفي، الجرائم الإلكترونية في التشريع الفلسطيني، غزة، 2013.

ثانيا: الرسائل والمذكرات:

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

– عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلة الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمينة، 2007.

– بلهومي مراد، الحدود القانونية لسلطة القاضي الجزائي، في تقدير الأدلة، مذكرة لنيل شهادة الماجستير، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، 2011.

– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، 2013.

– بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر، 2014.

– بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة لنيل شهادة ماستر، 2016.

– ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، جامعة باتنة، مذكرة لنيل شهادة ماستر، 2015–2016.

– صغير يوسف، الجريمة الإلكترونية، عبر الانترنت، تيزي وزوو، 2013.

– نواوي سليمة، دور الدرك الوطني في محاربة الجريمة الالكترونية، جامعة مسيلة، مذكرة لنيل ماستر، 2019/2018.

ثالثا: المقالات والبحوث:

– آمال بن صوليح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر، مداخلة الملتقي الدولي حول " الإجرام الييبرالي المفاهيم والتحديات "، 11–12 أفريل 2017.

– بن سولة نور الدين، الجرائم الالكترونية في ضوء التشريع الجزائري، المجلد التاسع، العدد 1، مارس 2018.

– بن فريحة رشيد، التحري الجنائي في مسرح الجريمة الإلكترونية، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، العدد 42،صفر 2017.

– بن فريدة محمد، الدليل الجاني الرقمي وحجته أمام القضاء الجزائي، مقال في المجلة الأكاديمية للبحث القانون، الصادر عن كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة عبد الرحمن، بجابة، جانفي 2014.

– بوظياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11 سبتمبر 2018.

– سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر 2019.

– سميرة معاشي، ماهية الجريمة الإلكترونية، مجلة المنتدى القانوني، العدد السابع، جامعة، بسكرة.

– ضريفي نادية، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسة، المجلد 04، العدد 02، السنة 2019.

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

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

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

– محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، العدد الثاني، ديسمبر 2017، المركز الجامعي إليزي، الجزائر.

رابعا: النصوص القانونية:

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

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

– القانون رقم 08-19 المؤرخ في 11/15/ 2008، الجريدة الرسمية، عدد 63، المؤرخ في 2008/11/16، يتضمن الدستور الجزائري المعدل والمتمم.

– قانون رقم 09-04 المؤرخ في 2009/08/05، يتضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، الصادرة في 08/16/ 2009.

الفهرس

الفهرس:

الإهداء:.....

الشكر:.....

مقدّمة:.....

الفصل الأول: مفهوم جهاز التحقيق للجريمة الإلكترونية في التشريع الجزائري.

المبحث الأول: الجريمة الإلكترونية والتحقيق فيها في التشريع الجزائري.....3

المطلب الأول: التعريف بالجريمة الإلكترونية وخصائصها وأنواعها.....3

الفرع الأول: تعريف الجريمة الإلكترونية.....3

أولا: تعريف الجريمة الإلكترونية لغة.....4

ثانيا: تعريف الجريمة الإلكترونية اصطلاحا.....4

ثالثا: تعريف الجريمة الإلكترونية فقها وقانونا.....4

الفرع الثاني: خصائص الجريمة الإلكترونية.....6

أولا: خصائص المجرم الإلكتروني.....7

ثانيا: المجني عليه في الجريمة الإلكترونية.....11

ثالثا: أنواع المجرمين الإلكترونيين وصفاتهم.....13

المطلب الثاني: التحقيق في الجريمة الإلكترونية.....15

الفرع الأول: تعريف التحقيق الجنائي في الجريمة الإلكترونية.....16

أولا: المقصود بالتحقيق الجنائي في الجريمة الإلكترونية.....16

ثانيا: تعريف المحقق.....17

الفرع الثاني: خصائص التحقيق في الجريمة الإلكترونية.....17

أولا: خصائص التحقيق.....18

ثانيا: الخصائص الفنية للمحقق.....22

المبحث الثاني: السلطات المختصة بالتحقيق في الجريمة الإلكترونية...24

المطلب الأول: تعريف جهاز التحقيق وأقسامه.....24

الفرع الأول: تعريف جهاز التحقيق الجنائي في الجريمة الإلكترونية.....24

الفرع الثاني: أقسام جهاز التحقيق الجنائي في الجريمة الإلكترونية.....24

أولا: أجهزة الأمن العام.....25

ثانيا: أجهزة التحقيق في الجرائم المخلة بأمن الدولة.....26

ثالثا: الجهاز التحقيق في الجرائم الالكترونية.....27

الفرع الثالث: معوقات وصعوبات التحقيق في الجريمة الإلكترونية.....28

أولا: قلة خبرة القائمين بالتحقيق في الجرائم.....28

ثانيا: عوائق تتعلق بالجريمة والجهة المتضررة منها.....29

المطلب الثاني: أجهزة التحقيق في الجريمة الإلكترونية.....30

الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم الالكترونية.....31

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.....31

ثانيا: جهازي الأمن الوطني والدرك الوطني.....33

الفرع الثاني: الهيئات القضائية الجزائية المتخصصة.....35

الفصل الثاني: إجراءات التحقيق والمتابعة في الجريمة الإلكترونية.

المبحث الأول: مرحلة جمع الاستدلالات والتحقيق فيها.....40

الفهرس:

المطلب الأول: جمع الاستدلالات في الجريمة الإلكترونية.....41

الفرع الأول: تلقي البلاغات والشكاوي.....41

أولا: تلقي البلاغات في الجريمة الإلكترونية.....41

ثانيا: الشكوى في الجريمة الإلكترونية.....42

الفرع الثاني: الاستجواب وسماع الشهود في الجريمة الإلكترونية.....43

أولا: الإستجواب.....43

ثانيا: سماع الشهود في الجريمة الإلكترونية.....43

المطلب الثاني: التحقيق في الجريمة الإلكترونية.....43

الفرع الأول: التفتيش وضبط الأدلة.....44

أولا: التفتيش.....44

ثانيا: ضبط الأدلة.....45

الفرع الثاني: المعانية وندب الخبراء في الجريمة الإلكترونية.....46

أولا: المعاينة.....46

ثانيا: ندب الخبراء.....47

المبحث الثاني: مرحلة المحاكمة.....48

المطلب الأول: اختصاص المحكمة.....48

الفرع الأول: اختصاص المحلي في الجريمة الإلكترونية.....48

الفرع الثاني: اختصاص النوعي في الجريمة الإلكترونية.....49

المطلب الثاني: تشكيلة المحكمة.....50

الفرع الأول: اجراءات المحاكمة.....50

الفرع الثاني: القواعد العامة للمحاكمة.....51

أولا: علانية الجلسة.....51

ثانيا: شفوية المرافعات.....52

ثالثا: حضور أطراف الخصومة.....52

رابعا: تدوين التحقيق النهائي.....52

الخاتمة:.....54

قائمة المصادر والمراجع:.....58

الفهرس:.....64