جامعة عمار ثليـــــــــجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

عنوان المذكرة:

إجراءات الوقاية والمتابعة في الجرائم الالكترونية

مذكرة تكميلية لنيل شهادة الماستر التخصص: قانون جنائي وعلوم جنائية

إعداد الطالبين

*قلو عمر

*عرابة عبد القادر

تحت إشراف

يوسفي مباركة

لجنة المناقشة

الأستاذ: رئيســـا.

الأستاذ: مناقشـا.

الأستاذة: يوسفي مبـــــــــــــــاركة مشرفـة.

السنة الجامعية: 2021/2020

شكر وعرفان

نتقدّم بجزيل الشكر والعرفان للأستاذة المشرفة الدكتورة يوسفي مباركة التي كان لها الفضل بعد الله تعالى في انجاز هذا العمل وصبرت معنا رغم طول المدة، وفي هذا الصدد نقول:

" ان الصبابة نحونا ما نال العلم. والتهيب في الصدر من الفضول الذي نمى إليّنا كما إننا نقول ونجود على أنفسنا الآن بالحجة في ذلك إن طالبنا، أو بالعذر إن استوضحنا، فإذا كان تبرير التقصير غامضا عنك فهو أدرى عندنا، ونعوذ بالله من علم عاد كلاً وأورث ذلاً، وصار في رقبة صاحبه غلاً -وهذا ضرب من الاحتجاج المخلوط بالاعتذار....

نسأل الله تعالى رب الأولين أن يجعل اعترافنا بما نعرفه موصولاً بنزوعنا عما صارحنا به، إنه قريب مجيب. وماذا نقول وسامعنا يصدق أن زماناً أحوج مثلينا إلى ما بلغك، مع ما نجده من انكسار للمعالم وانطواء لتقلبات الحياة العلمية لتعاود العلل علينا.

ثم إننا ما أردنا أن نبرر تقصيرنا بالقلم ليس لطول جفائنا، وشدة التوائنا عمن لم يزل علنا الرأي مجتهداً ولكن هي الظروف التي كانت تنافسنا وتحيطنا في كل محطة".

كما نتقدّم بالشكر لمن قدموا لنا يد العون في انجاز هذا العمل سواء من قريب أو من بعيد

إهداء

إلى من جعل الله الجنة تحت أقدامها أمي الغالية

إلى سندي وفخري واعتزازي...

رحمها الله برحماته الواسعة

و أبي الغالي حفظه الله تعالى ما حييت...

إلى نور حياتي ومصدر قوتي أخوتي الأعزاء

إلى من لم يبخل علي بالدعاء...

إلى كل أفراد عائلتي

إلى زملائي في الجامعة والأصدقاء والأحباء أهدي لكم هذه العمل المتواضع وأخص بالذكر لقمان أخي الذي لم تلده أمي وسندي في الحياة...

قلو عمر

إهداء

إلى من قدما بسخاء دون مقابل

إلى من زرعا في قلبي بذرة الإيمان، وفي روحي شجرة الولاية ...

إلى من ثابرا في تنشئتي، وبذلا أقصى الجهد في تربيتي أحسن

تربية ...

إلى أبي الحبيب

معلمي ورائدي في الجدية والالتزام والإيثار

إلى الأم الغالية أطال الله في عمرها

إلى ينابيع المحبة التي لا تنضب

اخوتي الكرام

الى جميع افارد أسرتي

لكل هؤلاء أهدي ثمرة جهدي

عرابة عبد القادر

المقدمة

مقدمة:

تمخض عن الفكر الإنساني فيس العقدين الرابع والخامس من القرن الماضي عن ابتكار أعظم ما قدمته الحضارة الإنسانية ألا وهو الحاسوب، مما أهل لحقبة جديدة بالغة الأهمية أحدثت تأثيرا في بنية المجتمع حيث تطورت وذلك نتيجة لاكتساح جميع النواحي التي تتطلبها الحياة البشرية، مما جعل منها مصدرا أساسيا للأشخاص وكذا المؤسسات للإعتماد عليه في كافة شؤونهم نظرا للسرعة والدقة في تخزين المعلومات ومعالجتها في وقت قصير.

حيث في هذه الفترة عرفة المعلوماتية INFORMATIQUE تطورا مذهلا، كما ساعد اقترانها بالتكنولوجيات أخرى (الإلكترونيك، الرقمنة) على تعميم استعمالها وتعدد وظائفها ، فالحديث اليوم لم يعد عن الحاسوب وقدراته في اختزال الوقت وتخزين المعلومات أو انجاز العمليات المعقدة، وإنما عن تكنولوجيا الإعلام والاتصال ، والفضاء الافتراضي الذي نشأ نتيجة ارتباط المعلومات بمختلف المواصلات السلكية واللاسلكية .

حيث أصبحت هذه الوسيلة ليست حكرا فقط على الدول المتقدمة، وإنما تعدت إلى غير ذلك (الدول النامية) مما زاد من أهمية هذه التكنولوجيات حيث عرفت بما يسمى بعصر المعلومات ، ومع التغلغل المتزايد للمعلومات وتكنولوجيا الاتصال في مختلف النشاطات البشرية، إذ اعتبرت فضاء ا مفتوح ا لا حدود له مقارنة بالحدود الإقليمية للدول، وذلك لكون جميع الدول والمنظمات والمؤسسات خاصة المالية المرتبطة ارتباط وثيق بها من أجل ممارسة أعمالهم ونشاطاتهم وتقديم مختلف الخدمات لزبائنهم ، وهو الأمر الذي أدى بأصحاب النوايا الإجرامية إلى الاتجاه إلى الاستعمال غير الشرعي لهذه المنظمات المعلوماتية (الإلكترونية)، من أجل ارتكاب أعمالهم الإجرامية المختلفة ، من جهة الانتفاع بها، ومن جهة أخرى التملص من المسؤولية الجزائية.

وأمام هذا الزحف المتزايد للأنظمة المعلومات ظهر شكل جديد من الإجرام وهو ما يعرف بالإجرام او الجرائم الإلكترونية ، إذ أنه وبظهور هذا النوع الجديد من الإجرام جعل من المجتمع الدولي التدخل من أجل وضع حد لإنتشاره، فكان لابد من وضع أطر قانونية

ملائمة جديدة أو إدخال تعديلات على قوانين سارية المفعول بما يتلاءم والوضع الجديد، لتحديد شروط استعمال هذه الوسائل في مختلف المعاملات، من خلال نصوص جزائية لحماية الأنظمة الإلكترونية ، وردع إساءة استعمالها سواء محليا أو دوليا في اطار الاتفاقيات الدولية .

فالتقدم العلمي والتكنولوجي لا يمكن أن يسير أو يعمل وحده بمعزل عن أي تقدم قانوني يواكبه ويحافظ عليه ويكفل حمايته ويضع الحلول لما قد يطرأ من مشكلات بسبب استعماله، ففي هذه الحالة يمكن للتقدم التكنولوجي أن يصبح أداة للبناء وأساس لكل تطور ويمكن أن يكون أداة لارتكاب الجريمة إذا أسيء استخدامه ، وهو ما يوجب على القانون أن يمتد نصوصه إلى هذه الأنشطة الجديدة التي تفرزها التكنولوجيا حتى تتخذ الجريمة في نصوص منضبطة واحدة إذ أصبحت النصوص التقليدية لا يمكن أن تسرى أو تطبق على هذا النوع من الجرائم مما أدى إلى ظهور مشكلات إجرامية في هذا المجال.

والجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا فهي أيضا معنية بالمكافحة، فكان لابد من إيجاد إطار قانوني مناسبا لسد الفراغ الإجرائي، لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة ومنها الجريمة الإلكترونية ، ومنها إجراءات تطبق فقط على الجريمة الإلكترونية ، التي تم النص عليها في قانون جديد يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته 04/09 المؤرخ في أوت 2009.

تكمن أهمية البحث أساسا في كون الجرائم الإلكترونية جريمة جديدة وبالتالي لا يمكن تطبيق الإجراءات التي تطبق على الجرائم التقليدية لانها من الموضوعات التي لم تنل حظها (من البحث والتحقيق والمحاكمة) على المستوى الجزائي، حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها، بالإضافة إلى كون الجرائم الإلكترونية حديثة النشأة ويمتد تأثيرها

إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال والتي تستخدم في جميع المجالات الحياة سواء من طرف الأفراد أو المؤسسات إذ تجعل التعاملات معها صعبا ومعقدا مما يحتم إيجاد طرق جديدة وتابعة لمكافحتها ، على الرغم من الصعوبات العديدة التي واجهتنا في إعداد المذكرة نظرا لصعوبة الموضوع وتشعبه .

أهداف الدراسة:

التعرف على جرائم الإلكترونية وخصائصها وطرق إثباتها ، وكذا الصعبات التي تواجهها السلطات المختصة ، وأيضا إجراءات التحري والمتابعة والكشف عنها وآلية الحماية والوقاية من أخطارها ، وإلقاء الضوء على مدى مسايرة النظام القانوني الجزائري بصفة خاصة والقانون المقارن بصفة عامة ، لمستخدمي الأجهزة الإلكترونية التي هي في تطور رهيب ، ومعرفة السمات الخاصة بهذا النوع من الجرائم وبمرتكبيها ووسائل القضاء عليها.

أما من ناحية اسباب اختيارنا للموضوع إجراءات المتابعة والوقاية في الجريمة الإلكترونية يرجع في حقيقة الأمر إلى العديد من الاسباب بعضها شخصي والآخر موضوعي

فالأسباب الشخصية : يكمن اهتمامنا بمجال الجريمة الإلكترونية وما يتعلق بها من جرائم وكذا من إجراءات خاصة وإن إجراءات المتابعة فيها تختلف كل الاختلاف عن إجراءات المتابعة في الجرائم التقليدية بالإضافة إلى أنه موضوع جديد، ورغبتنا الشديدة في الغوص في مجال إجراءاتها وكذا مكافحتها والوقوف على حقيقة التعامل مع الجريمة الإلكترونية من الناحية الإجرائية .

أما الأسباب الموضوعية: فيكمن فيما يطرحه موضوع الحماية أو الوقاية للجريمة الإلكترونية من إشكاليات قانونية التي لا بد من الوقوف نظرا لحداثة الموضوع من الجانب الموضوعي لتجريم الافعال او الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، والقواعد الإجرائية الحديثة التي جاء بها تعديل الإجراءات الجزائية الجزائري وكذا قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته .

ولعل من أهم الصعبات التي واجهناها في دراستنا لموضوع البحث الظروف الراهنة التي يمر بها العالم بصفة عامة ، والتي جعلتنا غير قادرين على إعطاء الوقت الكافي لموضوع بحثنا من جهة ، وقلة المراجع المتخصصة في النظام الجزائري والتي تعالج موضوع بحثنا من جهة أخرى، بغض النظر عن بعض القوانين والمراسيم وكذا المجالات الجامعية والكتب القانونية لكن لا ترقى إلى المستوى المطلوب لإعطاء سياق متطور ويواكب هذا النوع من الجرائم.

و نظرا للأهمية البالغة التي تكتسيها مكافحة الجريمة المعلوماتية وما فرضته من تحديات خاصة في عصرنا الحالي الذي يعرف تطورا سريعا في مجال تكنولوجيات الإعلام والاتصال حيث أصبحت هذه آلأخيرة الركيزة التي تقوم عليها مختلف القطاعات سواء الخاصة أو العامة من أجل ذلك حاولنا في دراستنا هذه إلى محاولة المساهمة في وضع الخطوط العريضة بالتعرف على طرف التحقيق (ابتدائي أو قضائي) والمحاكمة والتعاون الدولي في هذا النوع من الجرائم بالإضافة إلى إلقاء نظرة على مستجدات في مجال الجريمة الإلكترونية ، خاصة إجراءات المتابعة إنه وبظهور الإجرام الإلكتروني أثار العديد من المشاكل خاصة الإجرائية في مجال الجريمة الإلكترونية باعتبار أن تلك الجرائم هي جرائم صعبة الكشف عنها و متابعة مرتكبها بالإضافة إلى أنها ترتكب على المسرح الإلكتروني غير مادي يختلف عن مسرح الجريمة التقليدي، مما يجعل قانون الإجراءات الجزائية قاصرا علي اجراءات المتابعة في الجرائم التقليدية فقط ؛على الأمر الذي أدى إلى تدخل المشروع تعديل قانون الإجراءات الجزائية واستحداث قانون خاص يتضمن جميع القواعد الإجرائية التي يمكن من خلالها لجهات البحث والتحقيق والقضاء التحري من أجل الوصول إلى الدليل المناسب لإثبات الجريمة الإلكترونية والتمييز بين إجراءاتها وإجراءات المطبقة على الجرائم التقليدية .

إلى أي مدى تقيد المشرع الجزائري بالإجراءات العادية للوقاية والمتابعة في الجرائم الإلكترونية؟ وهل تخضع الجريمة الإلكترونية لقواعد إجرائية عامة أم قرارلها أحكام خاصة؟

واعتمدنا في دراستنا هذه على المنهج التحليلي و الوصفي، كونه الأنسب لمثل هذه الدراسات من خلال تحليل مختلف المواد القانونية التي تتضمن إجراءات المتابعة في الجريمة الإلكترونية واختلافها عن النصوص الإجرائية التقليدية وكذا وصف وتحليل مختلف الاتفاقيات الدولية والعربية من أجل مكافحة هذا النوع من الإجرام الإلكتروني.

تطرقنا إلى عدة دراسات سابقة الي الجرائم الإلكترونية من الناحية الموضوعية فقط ؛مع وجود بعض الدراسات التي تطرقنا لها من الناحية الاجرائية ؛ ومن بين هذه الدراسات التى تم العتماد عليها في بحثنا هذا :

- سعيداني نعيم ، اليات البحث والتحري عن الجريمة المعلوماتية ، جامعة الحاج لخضر باتنة 2014/2013.
- نايري عائشة ، الجريمة الإلكترونية في التشريع الجزائري ، جامعة أحمد دراية أدرار 2017/2006.

ومن أجل معالجة الإشكالية التي سبق طرحها وجب تقسيم هذه الدراسة وفقا لخطة منهجية تتمثل في :

فصلين تطرقنا في الفصل الأول إلى مفهوم الجرائم الإلكترونية وإجراءات الوقاية منها ، قسم إلى مبحثين هما :

– المبحث الأول: مفهوم الجرائم الإلكترونية.

– المبحث الثاني: إجراءات الوقاية منها ، لكل مبحث مطلبين ولكل مطلب فروع.

أما الفصل الثاني تطرقنا فيه إلى إجراءات المتابعة في الجرائم الإلكترونية ، قسم إلى مبحثين هما :

– المبحث الأول: إجراءات وأجهزة التحقيق و التحري.

– المبحث الثاني: مرحلة المحاكمة.

لنختم جهدنا هذا بخاتمة لهذا الموضوع.

الفصل الأول

مفهوم الجرائم الإلكترونية وإجراءات الوقاية منها

تمهيد:

تعد الجريمة الإلكترونية ظاهرة إجرامية حديثة نظرا لارتباطها 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 الجهود الوطنية والتعاون الدولي لمكافحتها.

وعلى ضوء ذلك سنقسم الفصل الأول إلى الجريمة الإلكترونية مفهومها وانواعها وخصائصها والمبحث الثاني بالوقاية من الجريمة الالكترونية محليا ودوليا.

المبحث الأول: مفهوم الجرائم الالكترونية

يمكن تعريف الجرائم الإلكترونية بأنها "الجرائم التي تُرتكب ضد أفراد أو مجموعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب في الأذى الجسدي أو النفسي للضحية بشكل مباشر أو غير مباشر، باستخدام شبكات الاتصال الحديثة مثل الإنترنت (غرف الدردشة، البريد الإلكتروني...)، والهواتف الجوالة (الرسائل النصية القصيرة ورسائل الوسائط المتعددة) وعليه ستناول تعريف الجرائم الالكترونية"المعلوماتية" وأنواعها[1].

المطلب الأول: تعريف وأنواع الجرائم الالكترونية

مما لا شك فيه أن الجريمة بالمفهوم الوسع تعني كل مخالفة لقاعدة من القواعد تنظم سلوك الإنسان في الجماعة، أو هي سلوك إجرامي من خلال ارتكاب فعل يجرمه القانون، أو الامتناع عن فعل أمر به القانون، وعلى العموم فالجريمة هي ذلك السلوك المضاد للمجتمع والذي يضر بصالحه، هذا بوجه عام، فإذا ما تم هذا النشاط أو الفعل بواسطة الوسائل التكنولوجية الحديثة الممثلة في الكمبيوتر وباستخدام شبكات الاتصال الإلكترونية عبر وسائط تقنية علمية يمكن وصف النشاط أو الفعل حينئذ بالجريمة الإلكترونية، وقد أخذ تحديد مفهوم الجريمة الإلكترونية زخما واسعا[2].

الفرع الأول: تعريف الجرائم الالكترونية وخصائصها

لم ستوصل الفقه إلى تعريف جامع مانع للجريمة الإلكترونية، وبالتالي تعددت التعريفات بشأنها وفق المنظور الذي تبناه الفقيه، في هذا الإطـــار نشير الى:

[1] – على الساعة 12:22 مساءا ، اطلع عليه يوم 2021/04/11م https://www.aljazeera.net.

[2] – فريد روابح، محاضرات في القانون الجنائي العام،كلية الحقوق والعلوم السياسية، جامعة محمد دباغين سطيف،2019/2018م،ص100.

أولا: تعريف الجرائم الالكترونية

يصعب الاتفاق على تعريف موحد للجريمة المعلوماتية ، حيث اختلفت الاجتهادات في ذلك اختلافاً كبيرا ، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، و تباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى ، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة ، و يكون وسيلة لارتكابها تارة اخرى، فكلما كان البحث منصباً على الجرائم التي ترتكب ضد النظام المعلوماتي انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي ، أما إذا كان البحث منصباً على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة و كان :" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي[1] .

تجر الاشارة أيضاً إلى أن أهم عوامل صعوبة الاتفاق على تعريف هو أن التقنية المعلوماتية أصبحت تحل محل العديد من التقنيات السابقة كاهاتف و الفاكس و التلفزيون، فالمسألة لم تقتصر على معالجة البيانات فحسب، وإنما إلى وظائف عديدة مثل وظيفة النشر والنسخ ، وهو ما يحتم ضرورة التفرقة بين جرائم الإنترنت وشبكات المعلومات بالمعنى الفني عن بقية الجرائم الأخرى التي يستخدم فيها الإنترنت أو الحاسب الآلي كأداة لارتكابها.

فيقصد بجرائم الإنترنت وشبكات المعلومات الدخول غير المشروع إلى الشبكات الخاصة كالشركات والبنوك وغيرها وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات مثل تزييف البيانات أو إتلافها ومحوها، و امتلاك أدوات أو كلمات سرية لتسهيل ارتكاب مثل هذه الجرائم التي تلحق ضرراً بالبيانات والمعلومات ذاتها وكذلك بالنسبة للبرامج والأجهزة التي تحتويها وهي الجرائم التي تلعب فيها القنية المعلوماتية دوراً رئيسياً في مادياتها أو السلوك الإجرامي فيها.

[1] – هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة،أسيوط،1992 م، ص29.

أما الجرائم التقليدية الأخرى مثل غسيل الأموال، تجارة المخدرات، الإرهاب، الدعارة، الاستخدام غير المشروع للكروت الإلكترونية، ودعارة الأطفال Pornographie و جرائم التجارة الإلكترونية ، وكذلك جرائم السب و القذف ، هي جرائم تستخدم التقنية المعلوماتية كأداة في ارتكابها دون أن تكون جرائم معلوماتية بالمعنى الفني وإن كان يطلق عليها الجرائم الإلكترونية.[1]

نصل إلى أن الجرائم الإلكترونية (معلوماتية) لها انواع و أصناف عديدة ، وكما أسلفنا القول فإن الجريمة الإلكترونية تتميز بأنها تضم نوعين من الجرائم المستحدثة ، الأول أنواعا مسحدثة من الاعتداء على مصالح محمية جنائياً بالنصوص القانونية التقليدية ، أي أن في هذه الحالات فإن طرق الاعتداء فقط هي المستحدثة لأنها تتم عن طريق التقنية المعلوماتية بعد أن كانت ترتكب بالسلوك المادي الملموس، أما محل الاعتداء فهي المصالح المحمية أصلا حماية جنائية على مر الأزمان و العصور كالأموال و الشرف و الاعتبار، أما النوع الثاني فيضم أنواعاً أخرى من الاعتداءات بالطرق المستحدثة على مصالح مستحدثة لم تعرفها القواعد التقليدية كالشبكات المعلوماتية التي تتعرض للاختراق أو التعطل أو الإغراق.

وفي تعريفات اخرى في دول اخرى تعدَّدت ألفاظ ومفردات وصِيَغ ومصطلحات التعريف بالجريمة الإلكترونية تعدُّدًا يحمل صورة التنوُّع والثراء لا التنازع والتضاد، فأُطْلِقَ على الجريمة الإلكترونية هذا المسمَّى (crime-e)،وجرائم الكمبيوتر والإنترنت، وجرائم الحاسب الآلي (Computer Crimes)، وجرائم التقنية العالية (High-Tick)، والجرائم المعلوماتية (Information Crimes)، والجرائم الرقمية (Digital Crimes)، والسيبر كرايم

[1]– صالح أحمد البربري ، دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية - الموقعة في بودابست في 2021/04/14 – www.arablawinfo.com ص2.

(CyberCrime)، وجريمة أصحاب الياقات البيضاء (**WhiteCollar**)، والجرائم الناعمة[1] (SoftCrimes)، والجرائم النظيفة[2] (CleanCrimes).

وقديمًا عرَّف العلامة الماورديُّمن علماء المسلمين من أئمَّة الشافعيَّة سنة (450هـ) الجرائم بأنها: (محظورات شرعية، زجر الله تعالى عنها بحدّ أو تعزير) وحتى اليوم ما زال هذا التوصيف صالحًا ليشمل جرائم الإنترنت؛ لأنها في أفعال تستهدف محظورات، ولكن وِفْق أساليب جديدة.[3]

وقد تحدَّث الفقه القانوني المعاصر طويلًا حول التعريف العلمي القانوني للجريمة الإلكترونية، وتعدَّدت المدارس والاتجاهات في ذلك، ومن أحسن وأجمع وأشمل هذه التعاريف، تعريف منظمة التعاون الاقتصادي والتنمية (OCDE)؛ إذْ عَرَّفت الجريمة المعلوماتية في اجتماع باريس عام (1983م) بأنها: (كل سلوك غير مشروع أو غير أخلاقي أو غير مصرَّح به، يتعلَّق بالمعالجة الآليّة للبيانات أو نقلها).

وعَرَّف نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم م/ 17 وتاريخ: 1428/3/8هـ بناءً على قرار مجلس الوزراء رقم: (79) وتاريخ: 1428/3/7هالجريمة المعلوماتية بأنها:(أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام).[4]

---

[1]– ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، مجلة العدل، العدد 31 رجب 1427ه، ص45.

[2]– محمد علي العريان، الجرائم المعلوماتية، أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر20-19 نيسان/يونيو، ، المملكة المغربية2007 ص52.

[3]– فايز بن عبد الله الشهري، التحديات الأمنية لوسائل الاتصال الجديدة – دراسة الظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد20، العدد، ب.س39، ص153.

[4]– سميرة معاشي التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية،1432 هـ /2011م، ص63 .

ثانيا: خصائص الجرائم الالكترونية

تعتبر الجرائم الإلكترونية جرائم حديثة إذ أنها لم تظهر إلا بعد اتساع التغطية بشبكة الانترنيت والانتشار الواسع للحواسيب والوسائط الالكترونية ومختلف وسائل الاتصال الحديثة لا سيما الهواتف النقالة، لذلك فهي تنفرد بخصائص لا نجدها في غيرها من الجرائم وتميزها عن الجرائم التقليدية،[1] ومنها:

1/يتطلب ارتكاب الجريمة الالكترونية وجود جهاز الكتروني والتحكم بتقنية استخدامه

من خصوصية الجريمة الإلكترونية أن بعض حالات ارتكابها يتعمد مرتكبها التدخل في مجالات النظام المعلوماتي المختلفة منها مجال المعالجة الإلكترونية للبيانات ، ومجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية، في المجال الأول : يتدخل الجاني من خلال ارتكاب الجريمة الإلكترونية في مجال المعالجة الإلكترونية (الآلية) للبيانات ، سواء من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسب الآلي ، وذلك بغرض الحصول على المعلومات ، وفي المجال الثاني : يتدخل الجاني في مجال المعالجة الإلكترونية للنصوص والكلمات ، وهي طريقة أوتوماتيكية تمكن مستخدم الحاسب الآلي من كتابة الوثائق المطلوبة بدقة متناهية بفضل الأدوات الموجودة تحت يده ، وبفضل إمكانيات الحاسب الآلي تتاح إمكانية التصحيح والتعديل والمحو والتخزين والاسترجاع والطباعة ، وهي بذلك علاقة وثيقة بارتكاب الجريمة[2].

2/تعد الجرائم الإلكترونية جرائم عابرة للحدود:

أحدث التطور الذي شهدته التكنولوجيا ووسائل الاتصال ثورة شاملة امتدت لكل جوانب الحياة، حتى فيما يتعلق بالإجرام، حيث أصبح الجناة يسخرون التكنولوجيا الحديثة ووسائل

[1] – دوادي نعيمة، الجرائم الالكترونية ،خصائصها ومجالات إستخدامها وأهم سبل مكافحتها، مجلة محد اللغات ،المجلد 2 ،العدد 1 ، جامعة علي لونيسي، البليدة ،الجزائر،2020، ص53،54.

[2]– محمد على العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، 2004 ، ص37 .

الاتصال المتطورة في تحقيق مآربهم الإجرامية، وأفضل وسيلة في ذلك استخدام شبكة المعلوماتية أو الأنترنت، التي جعلت من العالم يعيش في قرية صغيرة. تسمى الجرائم المرتبطة بشبكة الأنترنت " الجرائم الإلكترونية "، وهي الجرائم الواقعة على الحاسوب الآلي تعّرف بأنها أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب.

الجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[1]، كما أنها تسمى الجريمة المعلوماتية أيضا بالجريمة الإلكترونية، وذلك نظرا للبيئة التي تتم فيها، أي البيئة الإلكترونية، وهي تشمل الجرائم المنصبة على استغلال البيانات المخزنة على الكومبيوتر بشكل غير مشروع، الجرائم التي يتم من خلالها اختراق الكومبيوتر لتدمير البرامج والبيانات الموجودة في الملفات المخزنة، الجرائم التي يكون جهاز الكومبيوتر محلا أو وسيلة لارتكاب الجريمة أو التخطيط لها.

وأخيرا الجرائم التي يتم فيها إساءة استخدام الكومبيوتر أو استعماله بشكل غير قانوني من قبل الأشخاص المرخص لهم باستعماله [2] والجرائم الإلكترونية لم تعد حبيسة النطاق الإقليمي للدولة الواحدة، بل أن مداها يشمل المستوى الإقليمي والدولي، لتصبح هذه الجرائم عابرة للحدود، تعّرف بأنها : " كل عمل أو امتناع يأتيه الإنسان، بواسطة نظام معلوماتي معين، إما اعتداء على حق أو مصلحة أو أية بيانات معلوماتية يحميها القانون، وإما إضرارا بالمكونات المنطقية للحاسب ذاته أو بنظم شبكات المعلومات المتصلة به، إذا كانت الواقعة تمس حدود أكثر من دولة "[3]

وجدت الجماعات الإجرامية المنظمة، بفضل تطور التكنولوجيا والاتصالات، المجال الخصب لارتكاب أنشطتها الإجرامية، فأصبحت جرائمها بلا حدود، حيث يمكن أن يكون المجرم في مكان ما، ويقوم بجريمته في مكان آخر، مما أسبغ على هذه الجرائم

[1] – أسامة أحمد المناعسة، جلال محمد الزغبي وصايل فاضل الهواوشة، جرائم الحاسب الآلي والأنترنت، ط الأولى، دار وائل للنشر والتوزيع، عمان الأردن،2001، ص78.

[2] – زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر، سنة 2011 ، ص 44 ، 45.

[3] – هلالي عبد اللاه أحمد، جرائم المعلوماتية عابرة للحدود (أساليب المواجهة وفقا لاتفاقية بودابست)، ط الأولى، دار النهضة العربية، مصر، 2007 ص 31.

ظاهرة العالمية[1]، خاصة وأن جرائم المعلوماتية من الجرائم العابرة للدول، التي لا تعترف بالحدود الجغرافية بل تعتبر الصورة الحقيقية للجرائم عبر الوطنية، الأمر الذي شجع الجناة على اللجوء إلى هذا النوع من الإجرام، الذي يتميز ببساطته وعفويته، إضافة إلى أنه يعد أقل خطورة من الإجرام المباشر[2]وهو ما قد يشير العديد من المشكلات العملية، لاسيما تلك المتعلقة بمتابعة الجناة والتحقيق في الجرائم[3].

البيانات والمعلومات وحتى الأموال، مما يجعل مكافحة هذه الجريمة بالوسائل التقليدية أمرا في غاية الصعوبة، لتعدد الأماكن التي تتعلق بالجريمة وتنازع قوانين الدول الواجبة التطبيق، واختلاف الإجراءات الجزائية من دولة لأخرى وصعوبة ملاحقة الجناة.[4]

3/جرائم هادئة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل والسرقة وغيرها من الجرائم، فالجرائم الإلكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسبات ، إلا أن البعض بشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفدرالي بالولايات المتحدة الأمريكية FBI نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف[5].

[1] – عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، ط الأولى، دار النهضة العربية، القاهرة مصر 2004 ، ص 219.

[2] – أسامة أحمد المناعسة وآخرون، مرجع سابق، ص 106.

[3] – محمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة (التجريم وسبل المكافحة)، مطبعة العشري، مصر، 2006 ص 153.

[4] – عبد الصديق شيخ المرجع السابق، ص195.

[5] – رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، العدد41، جامعة أحمد دراية أدرار،2018/2017، ص442.

3/جرائم صعبة الإثبات :

يعد إثبات الجريمة الإلكترونية من الصعوبة بمكان، حيث يصعب تتبعها واكتشافها، فهي لا تترك أثر يقتفى، حيث تعتبر مجرد أرقام، فمعظم الجرائم الإلكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كالبصمات مثلا ومن جهة أخرى، فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي للتعامل معها، زيادة على ذلك يعمد مرتكب الجريمة الإلكترونية إلى ممارسة التمويه عند ارتكابها والتضليل والتحايل بغاية عدم التعرف على مرتكبيها[1].

الفرع الثاني: أنواع الجريمة الالكترونية

نتطرق في هذا الفرع على أنواع الجرائم الالكترونية "المعلوماتية"

فقد قسمت هذه الجرائم إلى:

- ✓ الجرائم التي تستهدف عناصر المعطيات والنظم.
- ✓ الجرائم المرتبطة بالكمبيوتر "**التزوير والاحتيال.**"
- ✓ الجرائم المرتبطة بالمحتوى " **الأفعال الإباحية والأخلاقية**".
- ✓ الجرائم المرتبطة بحقوق المؤلف والحقوق المجاورة.[2]

وفي أنواع أخرى للجريمة المعلوماتية نذكر:

[1] – رحموني محمد، المرجع السابق، ص443.

[2] – عادل بوزيدة، الحماية الجزائية لأسماء نطاق المواقع الإلكترونية ،على ضوء قانون حقوق المؤلف والحقوق المجاورة، مجلة العلوم القانونية والسياسية ، جامعة العربي التبسي تبسة ،الجزائر،2018،عدد17، ص853و854.

1. الجرائم ضد الأفراد

وتسمى بجرائم الانترنت الشخصية مثل سرقة الهوية ومنها البريد الإلكتروني أو سرقة الاشتراك في موقع شبكة الإنترنت.

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة.

يصعب بداية حصر عناصر الحق في الحياة الخاصة فهي تتكون من عناصر ليست محل اتفاق بين الفقهاء فيمكن القول بأنها تشمل حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنية[1].

اما علاقة الحياة الخاصة بالتقنية المعلوماتية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الآونة الأخيرة لخدمة أغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية[2].

2. الجرائم ضد الملكية :

انتقال برمجيات ضارة المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها لتدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى ممتلكات شخصية.

[1] – ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائي ،دار النهضة العربية القاهرة 1983، ص 207.

[2] – أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دار النهضة العربية القاهرة 1994، ص 48.

3. الجرائم ضد الحكومات :

مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الانترنت وهي تتركز على تدمير الخدمات والبنى التحتية ومهاجمة شبكات الكمبيوتر وغالباً ما يكون هدفها سياسي بحت.

المطلب الثاني: التعريف القانوني للجرائم الالكترونية في التشريع الجزائري

تأثر المشرع الجزائري بغيره من التشريعات الأجنبية الأوروبية منها والعربية، فيما يخص القواعد التي أستند إليها أو أتى بها لمكافحة الجرائم المعلوماتية، حيث اتجه إلى خلق نصوص جديدة وخاصة تتعلق بهذا النوع من الإجرام، رغبة منه في تأمين أنظمة المعلومات من اعتداءات المجرمين ، إذ نجد أنه ضمن موضوع الجريمة المعلوماتية في قانون العقوبات أو بموجب نصوص خاصة على السواء.

ويعتبر نظام المعالجة الآلية للمعطيات الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الاعتداء على نظام المعالجة، فإذا تخلف هذا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .إن نظام المعالجة الآلية للمعطيات تعبير تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا على أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال الحاسبات الآلية، لذلك فالمشرع الجزائري على غرار المشرع الفرنسي لم يقم بتعريف نظام المعالجة الآلية للمعطيات بل أوكل مهمة تعريفه لكل والقضاء.

أما المشرع الجزائري فقد اصطلح على تسمية الجريمة الإلكترونية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وتبنى في ذلك التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي[1]، بموجب المادة الثانية من القانون 09- 04 المتضمن القواعد

[1] – المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر2000.

الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وعرفها على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية" أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ، «وبالتالي تكون الجريمة الإلكترونية أيضا، تلك الجرائم المرتكبة عن طريق أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض[1] أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا البرنامج معين ، والمرتكبة عن طريق أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية ،يلاحظ على هذا التعريف مايلي:[2]

- ✓ أن المشرع الجزائري قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكتروني، وثانيها معيار موضوع الجريمة والمتمثل في المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.
- ✓ كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة المعلوماتية، كونه أقر أن هذه الجريمة ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع نطاق محال الجرائم المعلوماتية في القانون الجزائري .وترتيبا على كل هذه التعاريف الفقهية والتشريعية يمكننا القول أن الجريمة المعلوماتية هي كل سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته و يحس بالأشخاص

[1] – ونوغي نبيل زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية المجلد الرابع، العدد الثالث، المركز الجامعي أحمد بن عبد الرزاق حمودة -سي الحواس – بريكة سبتمبر 2019، ص131.

[2] – المرجع نفسه، ص131.

أو الأموال أو أمن الدولة، وهي على غرار الجرائم التقليدية تعرف من خلال أركانها بتوافر القصد الجنائي لارتكاب هذه الجريمة والركن المادي للجريمة وركنها.[1]

المبحث الثاني: إجراءات الوقاية من الجرائم الإلكترونية

تزايدت خطط مكافحة الجرائم الإلكترونية وانصبت الجهود على دراستها المتعمقة وخلق آليّات قانونيّة للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية خاصة المنظمات والهيئات الإقليميّة الأوروبية. وإدراكًا لقصور القوانين الجنائيّة بما تتضمّنه من نصوص التجريم التقليديّة عن أن تحيط بالجرائم الإلكترونية، كان لا بد للعديد من الدول من وضع قوانين وتشريعات خاصّة، أو العمل على جبهة قوانينها الداخلية لجهة تعديلها من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم. وأظهر تحليل الجهود الدولية، واتجاهات القانون المقارن بشأن جرائم الكمبيوتر والإنترنت أنّ مواجهة هذه الجرائم تم في ثلاثة قطاعات مستقلة:

- ✓ حماية استخدام الكمبيوتر، أو ما يُعرَف أحيانًا بجرائم الكمبيوتر ذات المحتوى الاقتصادي.
- ✓ حماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية).
- ✓ حماية حق المؤلف على البرامج وقواعد البيانات (الملكية الفكرية للمصنفات الرقمية).

المطلب الأول: تقنين واستعمال وسائل الرقابة القبلية (التفتيش والحجز)[2]

أمام صعوبة تتبع والكشف عن الجرائم الإلكترونية التي تعرف على أنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة او غير

[1] – المرجع نفسه، ص132.

[2] – مواد الفصل 03، القواعد الإجرائية تفتيش المنظومات المعلوماتية ، من القانون 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها.

مباشرة في تدخل التقنية المعلوماتية، وأمام قصور القواعد التقليدية في مواجهة الجريمة كان لزاما على المشرع الجزائري التدخل بنصوص آمرة لتجريم الظاهرة من جهة وإصدار قوانين خاصة تتلاءم وطبيعة الجريمة ومستلزمات المكافحة التي تستدعي التعاون بين الجهات القانونية والمختصين في المعلوماتية زيادة على التعاون الدولي[1].

أولا: التفتيش

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق، يهدف إلى البحث عن الأدلة الإثبات وقوع جريمة ما في مكان معين، حيث أنه ونظرا لخطورته تشترط أغلب التشريعات الحصول على رخصة للتفتيش من الجهة القضائية المختصة.

إذا كان الالتزام بقواعد التفتيش في الجرائم التقليدية لا يثير إشكالات كبيرة، فإن الأمر ليس كذلك بالنسبة للجرائم الإلكترونية، خاصة وأن نظم المعالجة الألية تتكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات اتصال متطورة ومعقدة.

كما أن إجراء التفتيش في الجريمة الإلكترونية يحتاج إلى تقنيات ومهارات خاصة يختلف عن الجرائم التقليدية، فتفتيش الحواسيب و أجهزة الاتصال يتطلب دراية وتحكم دقيق في هذه الأجهزة وكيفية إخفاء المعلومات فيها، وهي عملية ليست بالبسيطة والسهلة وتتطلب وقت وجهد كبيرين، بل أحيانا لا بد من الاستعانة بالخبرات الفنية والتقنية المتخصصة سواء تعلق الأمر بتفتيش المكونات المادية والمعنوية للحاسوب أو تفتيش الشبكات المعلوماتية المتصلة بالحاسوب عن بعد، وكذلك مختلف وسائل الاتصال كالهواتف وغيرها من الأجهزة الإلكترونية لقد أجاز المشرع للسلطات القضائية[2] ولضباط الشرطة القضائية في إطار قانون

[1] – سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري مجلة العلوم الإنسانية، المجلد 30، العدد3، جامعة الاخوة متنوري قسنطينة1، الجزائر2019م، ص59.

[2] – عبد الصديق شيخ المرجع السابق، ص199.

الإجراءات الجزائية، وضمن حالات المراقبة المنصوص عليها في المادة 4 من القانون رقم 09-04، الدخول بغرض التفتيش ولو عن بعد في الحالتين التاليتين[1] :

- ✓تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- ✓تفتيش منظومة تخزين معلوماتية بالنسبة للحالة الأولى، فإذا كانت هناك أسباب تدعو إلى الاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى يمكن الدخول إليها انطلاقا من المنظومة الأولى، فيجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام الجهة القضائية المختصة بذلك أما إذا تبين مسبقا، بأن المعطيات المبحوث عنها التي يمكن الدخول إليها انطلاقا من المنظومة الأولى، هي مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فيمكن الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[2].

ثانيا: الحجز

عن طريق منع الوصول إلى المعطيات المعلوماتية. فبالنسبة لنسخ المعطيات فإنه وبالرجوع إلى نص المادة 06 من القانون 04/09 ،أجاز المشرع استخلاص الدليل عن طريق نسخ المعلومات المضبوطة وتخزينها في دعامات، مع الحرص على استعمال كافة الوسائل التقنية لتشكيل أو إعادة تشكيل المعطيات محل البحث وفحصها واستخلاصها، من أجل جعلها قابلة للاستغلال لأغراض التحقيق مع مراعاة عدم المساس بمحتوى المعطيات[3].

[1] – المرجع نفسه، ص198.

[2] – عبد الصديق شيخ، المرجع السابق، ص199.

[3] – المادة 06 الفقرة 3 من القانون 09-04 ،المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

أما الحجز عن طريق منع الوصول إلى المعطيات، فهو طريقة استثنائية، يتم اللجوء إليها في حالة عدم إمكانية إجراء الحجز عن طريق النسخ لأسباب تقنية، لذلك فإنه يتعين على السلطة التي تقوم بالتفتيش، استعمال التقنيات المناسبة، لمنع الوصول أو إلى نسخ المعطيات التي تحتويها المنظومة المعلوماتية الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة كما جاء في المادة 07 من القانون 09-04 ،المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 :أوت سنة 2009 ، كما يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة كما نصت المادة 08 من القانون 09 -04 ،المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009 ،(وفي كل الأحوال فإنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة، إلا في الحدود الضرورية للتحريات والتحقيقات القضائية (المادة 09 من القانون 09 -04 ،المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009[1]

المطلب الثاني: دور الهيئة الوطنية والتعاون الدولي في الوقاية منها

نتطرق في هذا المطلب على دور الهيئة الوطنية والتعاون الدولي في الوقاية منها من خلال الهيئات الاقليمية اي الوطنية و دورها و كذلك التعاون الدولي في الوقاية منها.

[1] – حليم رامي،إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاتر البحوث العلمية، المجلد 9 ،العدد 1 ، 202كلية الحقوق والعلوم السياسية، جامعة البليدة 2 ،ص 227-243.

اولا: دور الهيئة الوطنية

1: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تعد الرقابة من أهم آليات الوقاية من الجرائم الإلكترونية، حيث يمكن مراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها عند الحالات التالية :

- ✓ الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، إذ يختص النائب العام لدى مجلس قضاء الجزائر، بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته. إذنا لمدة ستة أشهر قابلة للتجديد، وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.
- ✓ تكون الترتيبات التقنية الخاصة بهذه الحالة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها، وهذا تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.
- ✓ عند توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- ✓ عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية، لمقتضيات التحريات والتحقيقات القضائية.
- ✓ عند تنفيذ طلبات المساعدة القضائية المتبادلة كما لا بد من الإشارة بأن المشرع قد منع عمليات المراقبة المنصوص عليها في المادة 4 من القانون رقم 09-04 السالف الذكر إلا بإذن مكتوب من السلطة القضائية المختصة[1].

[1] – عبد الصديق شيخ، المرجع السابق، ص198.

2/ جهازي الأمن الوطني والدرك الوطني .

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم الإلكترونية ، 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[1] .

3/ 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.

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

[2] – يوسف جفال، التحقيق في الجريمة الإلكترونية عبر الانترنت، تيزي وزو، 2017/2016، ص20.

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].

4 /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 ولإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، و المقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني وهو قيد الإنشاء· الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى

[1] – سعيدة بوزنون، المرجع السابق، ص53.

أنواع الجرائم بما فيها الجريمة الإلكترونية حيث يوجد بهذا المركز قسم الإعلام الآلي والإلكترو نيك الذي يختص بالتحقيق في الجرائم المعلوماتية[1].

5/الهيئات القضائية الجزائية المتخصصة

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون رقم 04 -14 المؤرخ في ،10نوفمبر 2004م [2]وتختص هذه الجهات القضائية بموجب المواد 37-40-329 م ن 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 دعم حقوق الإنسان وتسهيل حق اللجوء غلى القضاء واعادة على دراسة ثلاث نقاط أساسية :

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 مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدتها في أعمال المنظمات الإجرامية واستعمالها السنوات الأخيرة تزايد في العلميات الإرهابية وتزايد القضائي الافتراضي للاستفادة من خصائص الجريمة المعلوماتية.

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

[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، مذكرة لنيل شهادة ماستر، جامعة المسيلة، 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- 5-4-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، قالمة، برج بوعريريج، الطارف، خنشلة، سوق أهراس، وميلة.

[1] – كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11 عدد01 ،2015 ،ص117.

[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].

ثانيا: التعاون الدولي

إن مكافحة الجرائم الإلكترونية لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي و الجنائي، وفي إطار الجهد الدولي المنول، فإن هناك العديد من الهيئات والمنظمات الدولية التي تلعب دورا ملحوظا في إطار برام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة الجرائم الإلكترونية.

1/جهود الأمم المتحدة:

تبذل الأمم المتحدة جهودا لا يستهان بها في مجال محاولة التصدي للجرائم المعلوماتية وتؤكد على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون للحد من

[1] – سعيدة بوزنون، المرجع السابق، ص55.

انتشارها وتعاظم آثارها، وقد حظيت الجرائم المعلوماتية باهتمام مؤتمرات الأمم المتحدة، وأبرزها ما جاء في هذا المجال مايلي[1]:

عقد منظمة الأمم المتحدة المؤتمر الثالث عشر (10) لمنع الجريمة والعدالة الجنائية من 12 إلى 19 أفرين 2015بدولة قطر، وكان الموضوع الرئيسي للمؤتمر "دماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع للتصدي للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي، ومشاركة الجمهور" وقررت الجمعية العامة قرارها (67/184) النظر في ما يلي: إنشاء حلقات عمل من بينها تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، منها الجرائم المعلوماتية عقد منظمة الأمم المتحدة المؤتمر الثاني عشر من 12 إلى 19 أفريل 2010 بالبرازيل تحت عنوان "استراتيجيات شاملة التحديات عالمية نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، وتضمن جدول اعمال المؤتمر ثمانية بنود: من بينها جرائم الإنترنت، حيث دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية لدراسة شاملة لمشكلة الجريمة المعلوماتية وتدابير التصدي.[2]

2/جهود الاتحاد الدولي للاتصالات

يوفر الاتحاد الدولي للاتصالات الذي يضم 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية منبرا استراتيجيا للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة، وقد وضع الاتحاد الدولي للاتصالات مخططا لتعزيز الأمن الإلكتروني العالمي، ومن أهم أهدافه الرئيسية ما يلي:

[1] – خلف فاروق، الجريمة المعلوماتية بين الوقاية و المكافحة مداخلة بعنوان"الاليات القانونية لمكافحة الجريمة المعلوماتية" ،كلية الحقوق و العلوم السياسية، جامعو محمد خيضر ،بسكرة، ص04.

[2] – خلف فاروق، المرجع السابق، ص04.

- ✓ وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلا للتطبيق محليا وعالمية بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة[1] .
- ✓ وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهياكل التنظيمية والسياسات المتعلقة بجرائم الإنترنت.

3/جهود المنظمة الدولية للشرطة الجنائية الإنتربول:

وتهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأعضاء و على نحو فعال في مكافحة الجريمة، من تجميع البيانات والمعلومات المتعلقة المجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأعضاء .وتتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأعضاء، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت[2].

4/جهود المنظمة العالمية للملكية الفكرية:

تهدف إلى تشجيع النشاط الابتكاري، وتطوير إدارة الاتحادات في مجال حماية الملكية الصناعية وحماية المصنفات الأدبية والفنية، واهتمت بتوفير الحماية القانونية البرامج المعلوماتية وقواعد البيانات، وتم الاتفاق على توفيرها بواسطة الاتفاقيات العالمية وخاصة اتفاقية التربس "و "اتفاقية بيزن" اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصية تشريعات حقوق المؤلف كما يلزم الاتفاق الدولي الأعضاء في المنظمة بوجوب فرض إجراءات تنفيذية، وتدابير مدنية و إدارية، و عقوبات جنائية لمواجهة أي اعتداء على حقوق المؤلف وخاصة القرصنة، وتنص المادة 04 من منظمة العالمية للملكية

[1] – المرجع نفسه، ص05.

[2] – خلف فاروق، المرجع السابق، ص05.

الفكرية المعتمدة سنة 1996 على أنه "تمتع برامج الحاسوب بالحماية باعتباره مصنفات أدبية ونطبق تلك الحماية على برامج الحاسوب أيا كانت التعبير عنها"[1].

5/ جهود منظمة التعاون الاقتصادي والتنمية :

تضم هذه المنظمة في عضويتها 34 دولة وضعت المنظمة توصيات إرشادية بخصوص أمن نظم المعلومات، ومن مجمل أعمال منظمة التعاون الاقتصادي والتنمية حول الجرائم الإلكترونية حصل اتفاق على ضرورة أن يغطي قانون العقوبات في كل دولة الأفعال التالية:

- ✓ التلاعب في البيانات المعالجة آليا بما في ذلك محوها.
- ✓ التجسس المعلوماتي.
- ✓ التخريب المعلوماتي.
- ✓ قرصنة البرامج.
- ✓ الدخول غير المشروع على البيانات أو نقلها، واعتراض استخدام المعطيات أو نقلها[2].

6/اتفاقية الإجرام السيبيري (الإجرام عبر الانترنت) (2001م):

صدرت هذه الاتفاقية عن المجلس الأوروبي، ووُقِّعَت في العاصمة المجرية بودابست في 23 نوفمبر (2001م)، وقّعت عليها 30 دولة، ولأهمية هذه الاتفاقية انضمَّ إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في 22 سبتمبر (2006) م، ودخلت حيز النفاذ في الأول من يناير

[1] – اتفاقية إنشاء المنظمة العالمية للملكية الفكرية الموقعة في 14 جويلية 1967 والمعدلة في 28 سبتمبر 1979 لاسيما في المادة 04 منها الفقرة 01 " عمل على دعم اتخاذ الإجراءات التي تهدف الى تيسير الحماية الفعالة للملكية الفكرية في جمع أنحاء العالم والى تنسيق التشريعات الوطنية في هذا المجال."

[2] – خلف فاروق، المرجع السابق، ص06.

(2007م). واشتملت على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.[1]

7/جهود الاتحاد الأوروبي:

حرص المجلس الأوربي على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات, وذلك من خلال العديد من الجهود التي بذلت في هذا الشأن؛ وقد بدأ اهتمام هذا المجلس بالمعلوماتية بشكل عام وما يحيطها من مشكلات منذ مطلع السبعينات من القرن الماضي؛ وقد اتجه هذا الاهتمام بداية إلى العمل على حماية البيانات الشخصية حتى لا تؤدي الرغبة في زيادة فاعلية عمل الحاسبات الآلية لخدمة المجتمع في تهديد حق الأفراد في الخصوصية، في عام 1981 تم التوقيع على الاتفاقية الخاصة بحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيا.

وقد تضمنت تلك الاتفاقية عدة مبادئ تمثلت في الحد الأدنى من الاحتياطات التي يجب أن تتضمنها التشريعات الداخلية للدول أطراف المعاهدة لحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيا، و ضرورة الحصول على البيانات الشخصية من مصادر مشروعة، وأن تكون البيانات صحيحة ومتفقة مع الغرض الذي وضعت من أجله وأن تكون المعلومات حديثة، وأن تراعى القواعد الشكلية اللازم إتباعها للحيلولة دون إساءة استخدام البيانات الشخصية.

والواقع أن هذه المبادئ لا تختلف عن تلك الصادرة عن مجلس منظمة التعاون الاقتصادي والتنمية عام 1980 في شكل توصيات، وإن كان الاختلاف يمكن في عنصر الإلزام الذي تتميز به اتفاقية المجلس الأوربي باعتبارها اتفاقية قانونية تلزم الدول الأطراف فيها.

وقد أكدت الاتفاقية على اتخاذ التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع

[1] – علي حسن الطوالبة، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي ، دراسة مقارنة مجلة جامعة العلوم التطبيقية ، البحرين ، مركز الإعلام الأمني، 2009م،ص23.

التركيز على أهمية التعاون المحلي والإقليمي والدولي مع وجوب إقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الأساسية والسيادة[1].

ولأن الاتفاقية جاءت حصيلة جهود دولية وإقليمية فقد أكدت الاتفاقية على أهمية ما انجز من جهود في حقل جرائم الكمبيوتر من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوربي ومجموعة الدولة الصناعية (مجموعة الثانية) وبالنتيجة فإن مقدمة مشروع الاتفاقية قد ركزت على عناصر أساسية ثلاث :

الأول: يتمثل بأهمية التدابير التشريعية الموضوعية لمواجهة جرائم الكمبيوتر(نصوص التجريم الموضوعية)

الثاني: يتمثل بأهمية التدابير التشريعية الإجرامية المتلائمة مع طبيعة الكمبيوتر (النصوص الإجرائية).

الثالث : يتمثل أهمية التعاون الدولي والإقليمي في حقل مكافحة هده الجرائم والانطلاق مما انجز من جهود دولية واقليمية في هدا الحقل[2].

8/جهود اتفاقية المجلس الأوروبي:

اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام 1976، وفي العام 1996 أنشات اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء التعامل مع مشكلة الجريمة السيبرانية، عملت اللجنة بين عامي 1997 و2000 على الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر أفريل 2001، وتم التصديق على الاتفاقية من قبل 30 دولة بحلول العام 2010[3]، و اتفاقية جرائم الإنترنت في المعاهدة

[1] – ورقة عمل ،المركز العربي للبحوث القانونية والقضائية، ضرورة التعاون الإقليمي والدولي في مكافحة جرائم المعلوماتية، بيروت 2018/08/01م،ص10.

[2] – ورقة عمل ،المركز العربي للبحوث القانونية والقضائية، مرجع السابق ،ص10.

[3] – خلف فاروق، المرجع السابق، ص07.

الدولية الأولى التي تسعى لمعالجة الجرائم الإلكترونية عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى ومن أهم أهداف الاتفاقية:

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
- توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيا.
- جمع معلومات عن حركة البيانات، و عن إمكان وجود تدخل في محتواها.
- تضمن الاتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في تعليم المجرمين، المساعدة الدولية المتبادلة إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة[1].

9/جهود مجموعة الدول الثماني (20) :"G8"

اعتمد وزارة العدل والداخلية تبلدان الثمانية في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم تدريب الموظفين المكلفين تنفيذ القوانين، وتجهيزهم بالمعدات الضرورية التعامل الجرائم ذات التقنية العالية.

بالإضافة إلى ذلك دعت دول الثمانية إلى مواصلة العمل حتى التوصل إلى حلول دولية ناجحة، من خلال عقد اتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة ومن توصيات ال "G8" بالنسبة للجرائم الإلكترونية موجودة في اطار الباب "D" من المعاهدة.

[1] – توصيات عن مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، تقرير عن اجتماع الفريق العامل المعني بالتعاون الدولي، المعقود في فيينا يومي 27 و28 أكتوبر 2015،ص 02،03.

10/جهود الاتحاد الإفريقي:

طلب المؤتمر الاستثنائي لوزارة الاتحاد الإفريقي المسؤولين عن تكنولوجيا المعلومات والاتصالات المنعقد في جنوب إفريقيا من 02 إلى 05 نوفمبر 2009 من مفوضية الاتحاد الإفريقي القيام بالاشتراك مع لجنة الأمم المتحدة الاقتصادية لإفريقيا بإعداد اتفاقية حول التشريع القضائي على أساس احتياجات القارة والالتزام بالمتطلبات القانونية والتنظيمية للمعاملات الإلكترونية والأمن الإلكتروني وحماية البيانات الشخصية.

وكما أوصت بضرورة توفير الحماية القانونية لأنظمة المعلوماتية التي تعتبر ذو قيمة بالنسبة للمجتمع مما يجعل من الضروري سن التشريعات ضد الجريمة الإلكترونية. وفي اجتمع مجموعة من قادة الاتحاد الإفريقي مكون من 54 حكومة أفريقية في القمة 23 للاتحاد الإفريقي، ووافقوا على قواعد الأمن السيبراني [1].

[1] – المادة 29 من اتفاقية الاتحاد الأفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية من المخاطر التي تتعرض لها البيانات، في قمة 23 للاتحاد الإفريقي ،جوان 2014.

خلاصة

ان عصر المعلوماتية خلف ورائه آثاراً سلبية نجمت عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية في غير الغرض الذي خلقت من أجله، الأمر الذي أثر على حقوق الأفراد وحرياتهم حيث وفرت الأنظمة المعلوماتية وسيلة جديدة في أيدي مجرمي المعلوماتية لتسهيل ارتكاب العديد من الجرائم، كما أضحى النظام المعلوماتي ذاته محلاً للاعتداء عليه وإساءة استخدامه فالجريمة المعلوماتية، من أكبر التحديات التي نوجهها في عالمنا المعاصر وهذا ما سعى اليه المشرع الجزائري وكذلك التعاون الدولي.

الفصل الثاني

إجراءات المتابعة في الجرائم الإلكترونية

تمهيد:

لم تكتف التشريعات الحديثة بحماية معطيات الحاسب الالي بصفة عامة من خلال تجريم صور الاعتداء عليها أي حماية موضوعية وإنما نظرا لخطورة الاجرام الالكتروني في حد ذاته لكون محل الجريمة مجموعة معطيات هي عبارة في الحقيقة عن ذبذبات الكترونية يسهل على الجاني القيام بعمل اجرامي عليها دون ترك اثار ودون ان يستغرق هذا العمل وقتا طويلا وهو ما جعلها صعبة الاكتشاف والاثبات، ادى ذلك الي ظهور مشكلات اجرائية في هذا النطاق ، حيث ان المحقق او ضابط شرطية قضائية او القاضي نفسه في حيرة امام هذه الجرائم نظرا لقصور التشريع الاجرائي خاصة وان هذه الجرائم حديثة ولا يمكن تطبيق النصوص التقليدية من جهة وعدم القدرة الكافية والفنية لرجال القانون لاكتسابها.

لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الحاسة بالمعطيات أو بالأحرى الجرائم الإلكترونية ، ومن هذا المنطلق إرتأينا أن نقسم فصلنا هذا الى مبحثين:

المبحث الأول: إجراءات التحقيق والتحري في الجرائم الإلكترونية

والمبحث الثاني: مرحلة المحاكمة في الجرائم الإلكترونية

المبحث الأول: إجراءات وأجهزة التحقيق و التحري :

وضع المشروع الجزائري كغيره من التشريعات بعض القواعد والضوابط التي تستهدف متابعة مرتكبي الجرم المعلوماتي حماية لمعطيات الحاسب الالي خاصة في مرحلة جمع الاستدلالات، حيث ان أجهزة الشرطة تقوم بدور فعال ورئيس حال وقوع الجريمة، لمعاينة مكانها وضبط ادلتها والقبض على مرتكبيها والقيام بكل ما يفيد في كشف الحقيقة وذلك بعد مساعدة أجهزة التحقيق للتوصل الى حقيقة الواقعة ومعرفة مرتكبيها، وهو ما سنتناوله بالتفصيل.

المطلب الأول: أجهزة التحقيق و التحري:

إن الدعوة العمومية باعتبارها الوسيلة القانونية لاستفتاء حق الدولة في العقاب نبدأ إجراءاتها بمرحلة البحث والتحري أي مرحلة جمع الاستدلالات التي تهدف الى البحث عن الجريمة والكشف عن مرتكبيها، وان الإجراءات الجزائية المتخذة خلال هذه المرحلة تتولاها أجهزة الضبطية القضائية (مرحلة التحقيق الأولي) ومرحلة التحقيق الإبتدائي (قاضي التحقيق)، وفي كل أنواع التحقيق يكون لضباط الشرطة القضائية والقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية[1] .

الفرع الاول: 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 اصليين وشركاء فيها ليتم تحرير محاضر بشأنها وتقديمها امام الأجهزة المختصة[2] وقد حدد لنا قانون الإجراءات الجزائية الجزائري[3] اهداف الضبطية.

ونظرا لخصوصية الجريمة الإلكترونية كان محتما توفير كوادر، وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة الإلكترونية، وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني، بالنسبة لجهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة

---

[1]– خالد عياد الحلبي. إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ط. 1 دار الثقافة للنشر والتوزيع ، عمان 2011 .ص147.

[2]– أحمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري – الجزء 2 ، طبعة 05 ديوان ، المطبوعات الجامعية، الجزائر ص، 159.

[3]– المادة 15 من قانون إجراءات الجزائية المعدل والمتمم بموجب امر رقم 15 /02 ، الجريدة الرسمية العدد 40.

ووهران، تحتوي على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى فرق متخصصة مهمتها التحقيق في الجريمة الإلكترونية تعمل بالتنسيق مع هذه المخابر توجد على مستوى مراكز الأمن الولائي، أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني، قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني.[1]

الفرع الثاني: قواعد الاختصاص :

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

أولا: الاختصاص المحلي :

يقصد به المجال الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه في البحث والتحري عن الجريمة، ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة ولذلك يتعين ان يكون مكان وقوع الجريمة او محل إقامة المتهم او محل القبض عليه[2].

يجيز القانون تمديد الاختصاص المحلي لضابط الشرطة القضائية في حالة الاستعجال او بناء على طلب من السلطة القضائية، وهو ما نصت عليه المادة 2/16 من ق.إ.ج (دائرة المجلس) وكذا تحديد الاختصاص المحلي لضباط الشرطة القضائية في الجرائم الستة الخطيرة الى كافة التراب الوطني انظر المادة 16 من ق.إ.ج .ج[3].

ثانيا: الاختصاص النوعي :

يقصد به اختصاص عضو الضبطية القضائية بنوع معين من الجرائم دون غيرها ، وقد ميز المشروع بين الاختصاص العام، لبعض فئات أعضاء الضبطية القضائية أي

---

[1]– نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكر مقدمة لنيل شهادة الماستر، نخصص قانون الإداري، جامعة أدرار، 2017/2016، ص41.

2- أحمد شوقي الشلقاني، مبادئ الاجراءات الجزائية في التشريع الجزائري ، مرجع سابق ،ص 59.

[3]– المادة 16 من قانون الإجراءات الجزائية الجزائري.

الاختصاص بالبحث والتحري بشأن جميع الجرائم دون تحديد نوع معين من الجرائم دون الأنواع الأخرى[1]، وهي الفئات المنصوص عليها في المادة 15.إ.ق ج فلهم الاختصاص العام بالبحث والتحري في جميع الجرائم اما الفئات الأخرى من الضباط المحددين في الفقرة 7 من المادة 15 والمواد و 21،27،28 من ق.إ.ج.ج فانهم ذوو اختصاص خاص وليس عام يتحدد بنطاق جرائم معينة[2].

المطلب الثاني: إجراءات التحقيق و التحري :

يبدأ التحقيق في الجريمة الإلكترونية من خلال تلقي المحقق البلاغ عن وقوع الجريمة مرورا بالإجراءات التي يتخذها المحقق في كشف غموضها وضبط الفاعل وإسناد الاتهام قبله وتقديمه للمحاكمة، أما القواعد الفنية فهي تلك التي تحكم المحقق منذ تلقيه البلاغ حتى ضبط المتهم وتقديمه للمحاكمة بعد إسناد الاتهام إليه وهذه القواعد القانونية يحكمها كل من قانون العقوبات وقانون الإجراءات الجزائية .

ويقصد بالتحقيق في مجال القانون هو مجموعة الإجراءات التي تباشرها سلطة التحقيق عند وقوع جريمة أو حادث ما يهدف التنقيب عن الأدلة التي تفيد في كشف الحقيقة[3]. خاصة في الجريمة الإلكترونية وهو ما سنعرض له في ثلاثة فروع على النحو التالي :

الفرع الأول : مبادئ كتابة التحقيق والمبادئ الأساسية للتحقيق في الجرائم الإلكترونية

أولا: مبادئ كتابة التحقيق في الجرائم الإلكترونية :

لكتابة محضر التحقيق أصول وعناصر محددة، يجب أن يلتزم بها المحقق ويمكن القول بأن تلك العناصر هي: افتتاحية المحضر، ومقدمة المحضر، وموضوع المحضر وأقفال، والتوقيع ...، وجميع هذه الإجراءات هي إجراءات ملزمة بنص القانون بالتدوين المحضر، إذ يعد الصورة الحقيقية والواقعية للحادث وكيفية حدوثه .

[1]– عبد الله اوهايبية ، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 27.

[2]– نبيه صالح ،الوسيط في شرح مبادئ الاجراءات الجزائية،د ط،منشاة المعارف القانونية للنشر، عمان،ص30.

[3]- ابتسام بغو ، إجراءات المتابعة في الجرائم المعلوماتية ، مذكرة تكميلية لنيل شهادة ماستر في القانون تخصص قانون جنائي للأعمال ، جامعة أم الأبواقي ، 2016/2015 ، ص41.

1/ : افتتاح ومقدمة المحضر:

إن لافتتاح المحضر أهمية بالغة وتقدير الدليل الذي يستخلص من الأوراق، فهي أول بيانات تقع عليها العين هي من المقدمة الذي تعتبر ملخص عن الواقعة [1].

أ/ افتتاح المحضر:

حتى تكون الافتتاحية صحيحة لا بد أن يتضمن مجموعة من البيانات نوردها فيما يلي :

أ-1- الرقم القضائي للواقعة والتكييف القانوني لها :

إن أول ما يتصدر المحضر جمع الاستدلالات هو الرقم القضائي الخاص بالواقعة حسب ترتيب القيد بدفتر القضايا مقترن بالوصف القانوني والتكييف القانوني للواقعة (جناية،جنحة...).

وبالتالي لا بد أن يكون جميع الجنح والجنايات أو مخالفة أو شكوى عن وقوع جريمة معلوماتية لا بد أن تكون مقيدة برقم قضائي[2] .

أ-2- عنوان المحضر :

يتضمن عنوان المحضر تاريخ ووقت ومكان افتتاحه، وبيانات المحقق والإجراءات التي قام بها قبل بدء التحقيق، ونتناولها على النحو التالي :

*** تاريخ ووقت افتتاح المحضر :**

إن أول ما يكون في المحضر هو تاريخ افتتاحه ووقته، والتاريخ يثبت فيه أي أيام الأسبوع قد جرى التحقيق فيها واليوم والشهر والسنة بالتقويمين، الميلادي والهجري . وهذا التاريخ كثيرا ما يفيد في معرفة وقت حدوث الجريمة[3].

***مكان تحرير المحضر التحقيق :**

يجب ذكر مكان تحرير المحضر، فقد تتأثر المحكمة حسب الأحوال بين ما إذاكان التحقيق يجري في النيابة أو على مسرح الجريمة أو الشرطة، أو المستشفى[1].

---

[1]- المرجع نفسه ، ص42.

[2]- إجراءات المتابعة في الجرائم المعلوماتية ، مذكرة تكميلية لنيل شهادة ماستر في القانون تخصص قانون جنائي للأعمال، المرجع السابق ، ص43.

[3]- المرجع نفسه ، ص43.

*** بيانات المحقق :**

يثبت المحقق الذي يتولى تحرير المحضر اسمه وصفته وأهمية هذا البيان في تحديد ما إذا كان للمحقق حق مباشرة التحقيق من عدمه، ويتلو بيان اسم كتب التحقيق، سواء كان كاتب النيابة أو آخر انتدبه المحقق بعد أداء اليمين، مع إثبات الحلف على ما سبق بيانه.

*** الإجراءات السابقة على بدء التحقيق :**

ويقصد به إثبات جل وكل الإجراءات السابقة على بدء ومباشرة التحقيق من تلقيه للبلاغ وانتقاله إن انتقل ومضمون محضر الاستدلالات إن وجد . فيجب على المحقق إثبات البلاغ الذي تلقاه عن الحادث على الصورة التي وردت إليه، كساعة وصول البلاغ إليه وتأشيرة بذلك عليه .

ب/ مقدمة المحضر :

هي عبارة عن ملحص وافي عن الواقعة، ويراعى في مقدمة المحضر إثبات ذلك :

ب-1- طريقة تلقي البلاغ :

في بداية المقدمة لا بد على المحقق إثبات كيفية ورود البلاغ إليه، مثلا حضور المبلغ أو المعني عليه شخصيا، أو بصحبة المواطنين أو بلاغ تلفوني وغير ذلك من الطرق[2].

ب-2- ملخص بسيط عن الواقعة :

ويكون بعد ذلك إثبات ورود الأخبار عن الواقعة للمحقق كما بينا سابقا على المحقق أن يقوم بإثبات محضر مضمون الواقعة وكيفية حدوثها، ومناقشة الأطراف شفاهة[3].

2/ : موضوع المحضر:

هو ما يتضمنه المحضر من إثبات جميع ما قام به المحقق من إجراءات قانونية وفنية من أجل كشف الغموض عن الواقعة، قبض على مرتكبي (المجرم المعلوماتي أو الإلكتروني) الفعل، وضبط الأدلة من أجل إسناد الواقعة[1].

---

[1]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنيت، مرجع سابق، ص: 192.

[2]- محمد صبحي نجم ،الوجيز في قانون اصول المحاكمات الجزائية ط1 ،دار الثقافة للنشر والتوزيع، الاردن،2012، ص،27.

[3]- المرجع السابق، ص27.

ويمكن تقسيم هذه الإجراءات إلى قسمين :

** الإجراءات التي قام بها المحقق ويطلق عليها الأدلة المحسوسة أو المادية .

** الإجراءات المتعلقة بأطراف الواقعة.

أ- الأدلة المادية :

يقصد بها الحجج والبراهين التي تشير إليها دلالة العثور على الآثار والأجسام المتعلقة بالجريمة ومعاينتها، وفحصها والتي يمكن إدراكها بالحواس أو عن طريق استعمال أي وسيلة من الوسائل العلمية التي تستعمل لضبط الأدلة وخاصة الإلكترونية منها.

وتتمثل هذه الإجراءات لضبط الأدلة المادية من خلال قيام المحقق الانتقال إلى مكان ارتكاب الجريمة ومعاينتها[2] ومن أسفرت ونتج عنه من آثار ومدلولات بالإضافة إلى وضع خطة من فريق البحث من أجل تنفيذها من خلال القبض على المتهم تفتشه وغيرها[3].

ب - الإجراءات المتعلقة بأطراف الواقعة :

تتمثل الواقعة (الجريمة) من المبلغ، المجنى عليه، الشاهد المتهم المضبوطات ، لكننا لن نتعرض لهم وإنما إلى المبلغ والمتهم فقط .

ب- أ- المبلغ :

قد يكون المبلغ هو شخص آخر أو المجنى عليه في حد ذاته، أو أي شخص له صلة بأطراف القضية فقد يكون صديق أو قريبا أو جارا، بل قد يكون محاميا عن أحد أطرافه ، ويقصد به أيضا الشخص الذي يقوم بالابلاغ او الاخطار عن وقوع جريمة من الجرائم.

والمبلغ على اختلاف صورة السابقة، من العناصر الأساسية للمحقق في كشف الغموض عن الواقعة (الجريمة) وضبط الفاعل وإسناد الواقعة قبله ، ومن ثم فإنه ينبغي في مناقشة المبلغ وسؤاله على أن يحصل المحقق على كافة الإجابات التي تحقق الغرض المنشود وذلك

[1]- عبد الفتاح بيومي الحجازي ، اصول التحقيق والتاديبي ، د ط.دار الفكر الجامعي ،الاسكندرية،2005،ص،47.

[2]- محمد الهيتي.التحقيق الجنائي والادلة الجنائية المادية، ط1 ، دار المناهج للنشر والتوزيع ،عمان 2010،ص59.

[3]- محمد حماد مرهج الهيتي، الادلة الجنائية المادية،د ط، دار الكتب القانونية مصر 2008،ص، 28.

باستخدام كافة أدوات الاستفهام والتي بدأت من ما؟ كيف؟ متى؟ أين؟ لماذا؟ ما هو؟ ما هي؟ [1]مثال :

ما تفصيلات ما حدث؟.. لماذا تأخرت في الإبلاغ عن الجريمة؟ أين حدثت الواقعة؟[2]

ب – ب – المتهم :

المتهم او الجاني او المشته فيه وهو الشخص الذي ارتكب الجريمة في أي حالة (واقعة) لا يخرج عن حالتين :

اما منكر لارتكابه الجريمة. أو معترفا بها .

لذا ينصح بأن وقت مناقشة المتهم في حالة ارتكابه جريمة معلوماتية وسؤاله هو الوقت الحرج الذي لا تهاون فيه ولا استهانة .

ولذلك يجب أن يقتصر مناقشة المتهم على أحد المحققين ذوي الخبرة وليس أعوانهم وأن يكون يكون ذلك في غرفة التحقيق[3].

وسنعرض فيما يلي الحالات التي يكون عليها المتهم :

***استجواب المتهم في حالة اعترافه بارتكاب الواقعة**

تكون في شكل أسئلة، ويمكن صياغتها من طرف المحقق بذات الأسلوب السابق بيانه بالنسبة للمبلغ المجنى عليه والشاهد .

ويمكن صياغتها بأسلوب آخر وهو وضع خطه محددة لسؤال المتهم تتمثل في وضع أركان الواقعة وتفصيلاتها في شكل مجموعات، كل مجموعة فيها عدد من الأسئلة، وللمحقق أن يختار النموذج المناسب، وقد يكون كل نموذج يختلف عن الآخر إما باستخدام أدوات الاستفهام، وغيرها؟[4]

[1]– خالد ممدوح ابراهيم ،فن التحقيق الجنائي في الجرائم الاكترونية ، مرجع سابق،ص38.

[2]– مرجع نفسه ،ص 39.

[3]– مراد احمد العبادي ، اعتراف المتهم واثاره في الاثبات ، ط1 ، دار الثقافة للنشر و التوزيع، عمان،2010، ص56.

[4]– مرجع سابق، ص43.

***استجواب المتهم في حالة انكاره ارتكاب الواقعة**

وهي الحالة التي ينكر فيها المتهم ارتكاب الفعل الجرمي (جريمة الإلكترونية) محل التحقيق، فإنه يقع على المحقق عبئ أكبر في حالة اعتراف المتهم، إذ يجب عليه في حالة الإنكار أن يعد نفسه لمواجهة المتهم طالما كانت الأدلة كلها تقوى من إتهام ذلك الشخص، وبالتالي لا بد على المحقق أن يضع خطة لسؤاله ومناقشته واستجوابه حتى يصل إلى اعترافه بارتكاب الجرم الإلكتروني دون خدع أو عنف .

والمحقق في سبيل هذا الهدف لابد له أن يلتزم باتباع قواعد هامة في مناقشة واستجواب المتهم :

– إثبات أقوله الخاصة بالواقعة على وجه العموم وأن تدون إجابته كاملة دون تنقيح أو تغيير أو حذف .

– أن يسأل المتهم عن علاقته بأطراف الواقعة وصلته بهم وخاصة المجنى عليه .
– أن يسأل عن سبب إتهام المجنى عليه له بارتكاب الواقعة .
– يجب على المحقق تقديم إيضاحات من المتهم عن تفاصيل وجزيئات الواقعة .
– مواجهة المتهم بأقوال أطراف الواقعة الآخرين كالشهود أو المجني عليه أو متهم آخر .
– مواجهة المتهم بالدلة التي تم العثور عليها بمسرح الجريمة أو في حيازته .
– يجب أن يحدد المحقق مدى تعارض وتناقض واختلاف أقول المتهم ويقوم بمواجهتهبهذا التناقض .

3/ : توقيع المحقق على المحضر:

القانون أوجب على المحقق أن يوقع على المحاضر وكذلك الحال بالنسبة إلى الكاتب ويجب أن يتم التوقيع على كل صفحة من صفحات التحقيق .

هذا وفضلا عن نهاية المحضر وذلك إبعاد لأية شبهة كالتزوير على أنه بالنسبة للكاتب يكفي توقيعه مع المحقق في نهاية محضر التحقيق، لأن الثقافة القائمة بالمحضر مستمدة من توقيع عضو النيابة العامة[1].

[1]– خالد عياد الحلبي ، اجراءات البحث والتحقيق في جرائم الحاسوب و الانترنت، مرجع سابق ،ص70.

ثانيا : المبادئ الأساسية للتحقيق في الجرائم المعلوماتية وضماناته للمتهم ومعوقات التحقيق[1]:

تعتبر الجريمة الإلكترونية من الجرائم حديثة النشأة ولذلك فإن قواعد العامة لمكافحة الجريمة المعلوماتية (الإلكترونية) غير صالحة، وإنما استحدثت قواعد جديدة خاصة فقط بالجريمة الإلكترونية نظر لخصوصيتها من الناحية الإجرائية خاصة في مجال التحقيق[2]، فهي ترتكز على مبادئ أساسية للتحقيق في الجرائم الإلكترونية وضمانات المتهم وصعوبات التحقيق في مجال الجرائم الإلكترونية :

1/ : العناصر الأساسية للتحقيق في الجرائم الإلكترونية:

يجب على المحقق في حالة وقوع أي جريمة لابد له أولا أن يستظهر أركانها الثلاث الشرعي، والمادي والمعنوي للجريمة محل التحقيق.

فلا إشكال بالنسبة للركن الشرعي لأنه يتحدد بنص المادة، أما الركن المادي والمعنوي فهي الأساس، بالإضافة إلى تحديد مكان وقوع أو ارتكاب الجريمة المعلوماتية بالإضافة إلى علانية التحقيق وهو ما ستناوله فيما يلي :

1/ إظهار أركان الجريمة الإلكترونية:

ويقصد بها الركن المادي والمعنوي المكونان للجريمة وهو ما ستناوله :

– أ – إظهار الركن المادي للجرائم الإلكترونية

يتطلب النشاط أو السلوك الإجرامي في جرائم الأنترنيت وجود بيئة رقمية واتصال بالأنترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته فمثلا يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة فيقوم بتحميل الكمبيوتر ببرامج اختراق أو أن يقوم بإعداد هذه البرامج بنفسه وكذلك قد يحتاج إلى تهيئة صفحات تحمل في

[1]– أحمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري – الجزء 2 ، طبعة 05 ديوان ، المطبوعات الجامعية، الجزائر.

[2]– خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق ،ص52.

طياتها جرائم تدخل في نطاق أو مجال الجرائم المعلوماتية، كما يمكن أن يقوم بجريمة إعداد الفيروسات، أو تزوير إلكتروني وغيرها[1].

لكن ليست كل جريمة تستوجب وجود أعمال تحضيرية، إذ تجدر الإشارة أنه من الصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في مجال الجريمة المعلوماتية، إذ أنه في هذا المجال فالأمر يختلف بعض الشيء عن الجريمة التقليدية، فشراء برامج اختراق أو معدات لكشف الشفرات وكلمات المرور وحيازة صور دعارة للأطفال فهي كلها تشكل جريمة في قائمة في حد ذاتها وليست عمل تحضيري[2].

– ب – إظهار الركن المعنوي للجرائم الإلكترونية :

يتمثل الركن المعنوي في الحالة النفسية التي يكون عليها الجاني التي دفعت به لارتكاب الجريمة، والعلاقة التي تربط بين الشخص الجاني والفعل المرتكب أو المكون للجريمة، ويتمثل أساس في العلم والإرادة المعروف باسم القصد الجنائي العام، إلى جانب القصد الجنائي الخاص في بعض الجرائم .

2/ علانية التحقيق:

من الضمانات اللازمة للعدالة الجنائية، علانية التحقيق في الإجراءات الجنائية وهي من بين الضمانات الخاصة به، وهي تختلف عن التحقيق الابتدائي عنها في مرحلة المحكمة، غير أن المشرع قد يجيز في بعض الحالات أن يكون التحقيق سريا وهذه الحالة لا يمكن اللجوء إليها إلا عند الضرورة .

وبالتالي فقد تكون عبارة عن علانية نسبية وذلك حماية للشهود ونظرا لخطورة الإجراء خاصة في مجال الجرائم الإلكترونية[3].

[1]– احسن بوسقيعة، الوجيز في القانون الجزائي القسم العام، ط1، دار هومة للنشر والتوزيع ، الجزائر2010،ص30.

[2]– خالد ممدوح إبراهيم، فن التحقيق في الجريمة الإلكترونية، مرجع سابق، ص 59.

[3]– مرجع نفسه، ص54.

2/ : ضمانات المتهم في مرحلة التحقيق الجنائي :

إن الهدف من التحقيق الجنائي هو تجسيد العدالة لجميع أطراف المجتمع ككل وكذلك بالنسبة للمحقق فإنه يستهدف توفير الحماية الكاملة له في حالة اتخاذه جميع الإجراءات الصحيحة، وتوافر وكافة الضمانات مما يؤدي ذلك إلى شعور بدء إلى مع الاطمئنان، وتتمثل أهم هذه الضمانات في :

أ/ سرية التحقيق بالنسبة للجمهور وعلانية للخصوم :

وهي من الضمانات المتعلقة بالمتهم في مرحلة التحقيق، والتي أكدتها معظم الدول والغرض من ذلك وضع هو أن سرية التحقيق من شأنها عدم الإساءة والتشهير بالمتهم قبل إدانته والحكم عليه من قبل المجتمع الأمر الذي يؤدي إلى ترك أثر سلبي وسيء في النفوس لاسيما إذا تبين بعد ذلك براءته.

كما تحصل العديد من الفوائد بالنسبة للمجتمع، وذلك من خلال عدم انتشار الشائعات بين أفراد المجتمع[1].

وعلى خلاف مبدأ السرية المقرر بالنسبة للجمهور فإن المشرع أقر علانية التحقيق بالنسبة لأطراف الدعوى العمومية القائم على التحقيق بشأنها وذلك من أجل إحاطة المتهم بضماناته، وكيفية سير التحقيق في جميع المراحل وغيرها .

وقد يرد على هذه القاعدة العامة استثناءات تتمثل في أنه يمكن للمحقق في حالة الضرورة والاستعجال أن يباشر إجراءات التحقيق في غيبة الخصوم أنظر المادة 101 ق.إ.ج.ج[2]، لذلك وجب السماح للمحامي الاطلاع على التحقيق عند طلبه الأوراق المثبتة لإجرائه عند انتهاء الحالة الواجبة، لأنه من حق المتهم الاستعانة بمحامي والدفاع عن نفسه أنظر المادة 102ق.إ.ج.ج[3].

[1]– أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص 65.

[2]– المادة 101 قانون إجراءات الجزائية.

[3]– المادة 102من قانون الإجراءات الجزائية الجزائري.

ب/ حق المتهم في محاكمة عادلة وسريعة :

من ضمانات الأساسية للمتهم أثناء مرحلة التحقيق حقه في محاكمة عادلة[1] وسرعة إنجاز واتخاذ كل الإجراءات التحقيق خاصة فيما يتعلق بمدة الحبس وهي محددة في قانون العقوبات في المواد 399 مكرر وما يليها في حالة ارتكاب أحد هذه الأفعال التي تستوجب عقوبتها الحبس والغرامة، وبالتالي على القاضي احترام المواعيد المقررة في القانون وهو ما ستناوله فيما بعد[2].

3/ : صعوبات التحقيق في مجال الجرائم الإلكترونية :

إن التحقيق في الجرائم المعلوماتية وملاحقة مرتكبيها جنائيا يتسم بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق في بيئة رقمية قد تؤدي إلى وجود نتائج سلبية تنعكس على نفسية المحقق بفقده الثقة في نفسه وفي عمله، بالإضافة أنها تصعد من قيمة مكافحة هذا النوع من الجرائم[3].

ومن أهم المعوقات التي قد تواجه القائمين عل مكافحة الجرائم الإلكترونية والتحقيق فيها، عوائق تتعلق بالجريمة وعوائق تتعلق بالجهات المتضررة وهو ما سنتناوله بالتفصيل :

3-1/ عوائق تتعلق الجرائم الإلكترونية:

من الصعوبات المتعلقة بالجريمة الإلكترونية:

- خفاء الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه .
- افتقاد أكثر الآثار التقليدية .
- إعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية كاستخدام كلمات السر .
- سهولة محو الدليل أو تدميره في زمن قصير جدا.[4]

---

[1]– الحق في الدفاع هو حق دستوري لا يمكن حرمان منه طبقا لنص المادة 151 من الدستور الجزائري .

[2]– تنص المادة 10 من الميثاق العالمي لحقوق الإنسان، المعتمد بموجب قرار الجمعية العامة 217 ألف(3 .د) المؤرخ في 10 ديسمبر 1948 " لكل إنسان الحق في أن تنظر قضيته أمام المحكمة مستقلة، نزيهة نظرا عادلا...".

[3]– خالد عياد الحلبي ،إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت،مرجع سابق ،ص 220 .

[4]– خالد ممدوح ابراهيم ،فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق،ص65.

3-2/ عوائق تتعلق بالجهة المتضررة :

- عدم إدراك خطورة الجرائم الإلكترونية من قبل المسؤولين بالمؤسسات تعد إحدى معوقات التحقيق[1].
- الأحجام عن الإبلاغ عن الأشخاص الميسورين أو صغار السن خوفا من المجتمع المحيط بهم وخشية الفضيحة بعد معوقا من معوقات التحقيق .
- عدم الإبلاغ عن الجرائم (القابلية المعطيات الإلكترونية للتلاشي عن طريق المحو أو التغيير).

3-3/ عوائق تتعلق بجهات التحقيق :

- قد تكون شخصية (معوقات تتعلق بالمحقق) قد تتعلق هذه العوائق بالعامل البشري القائم بالتحقيق في الجريمة المعلوماتية، حيث نجد أن السلطات القائمة بالتحقيق تلعب دور مهم في البحث والتحقيق في الجرائم التقليدية،غير أنها في مجال مكافحة الجرائم المعلوماتية لا تكون بنفس الدرجة نظرا للطبيعة الخاصة التي تتميز بها البيئة الإلكترونية ، مثل: التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الأنترنت، عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الإلكترونية.
- صعوبات تتعلق بالنواحي الفنية كنقص المهارة المطلوبة للتحقيق في هذا النوع من الجرائم، نقص المهارة في استخدام الكمبيوتر والأنترنت، عدم توفر المعرفة بأساليب ارتكاب الجريمة الجرائم الإلكترونية.
- قلة الخبرة في مجال التحقيق في الجرائم الإلكترونية.[2]

الفرع الثاني : المحقق الجنائي في الجرائم الإلكترونية

يقوم المحقق الجنائي بأهم وأخطر المهام على الإطلاق وهي تحقيق العدل لذا فإنه يتعين أن يكون ذات صفات معينة، وعزيمة جبارة، وأن يكون شديد اليقظة والانتباه والحزم ذا قدرة على استخلاص المعلومات، وفي سبيل أدائه لمهامه، يجب عليه أن يبذل العناية الواجبة فيما يعرض عليه من تحقيقات وشكاوي والتزام النزاهة والحياء فيما يتخذه من إجراءات،

[1]- المرجع نفسه، ص67.

[2]- خالد إبراهيم عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، مرجع سابق، ص 224.

والحرص على إنزال حكم القانون صحيحا، وهو الأمر الذي يتطلب تحديد المحقق الجنائي وبيان صفاته وعيوبه.

ومما سبق فإننا نقسم هذا المطلب إلى 3 عناصر على التوالي حيث ستتناول فيه تحديد المحقق الجنائي وصفاته وعيوبه في نطاق الجرائم الإلكترونية.

أولا : تحديد المحقق الجنائي :

تعتبر مهنة المحقق الجنائي من أفضل وأمتع المهن كافة، حيث بدك المحقق الثقة والرضا ويملأ النفس بالطمأنينة وتتجه إرادته إلى إحراز العدالة وإبراز الحقيقة .

ومن هذا المنطلق سنتناول بيان تعرف المحقق الجنائي وتحديده :

1/ تعريف المحقق الجنائي :

المحقق الجنائي هو الشخص القائم بأعمال إجراءات التحقيق الجنائي ولا يختلف تعريف المحقق الجنائي في الجرائم التقليدية عن الجرائم الإلكترونية ، فالفرق يكمن في نوعية الجريمة وليس في المحقق.[1]

وقد ذهب بعض الفقه إلى تعريف المحقق بأنه "هو كل من عهد إليه القانون لتجرى الحقيقة في البلاغات والقضايا والجرائم المطلوب التحقيق فيها، ويسهم دوره في كشف غوامضها وصولا إلى معرفة حقيقة الحادث وكشف مرتكبيه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة

كما عرفه البعض الآخر بأنه هو يقوم بمباشرة التحقيق بمعناه القانوني .

ومن خلال التعريفات السابقة يتضح أن الاختلاف راجع إلى الاختلاف في زاوية الظر إلى عمل المحقق أو تحديده.[2]

[1]– يتم تعيين قضاة التحقيق بالمحاكم في الجزائر بموجب المادة 50 من القانون الأساسي للقضاة الصادر في 06 سبتمبر 2006 بمقتضى قرار من وزير العدل بعد استشارة المجلس الأعلى للقضاء .

[2]– محمد الهيتي،التحقيق الجنائي والادلة الجنائية، مرجع سابق ،ص 50.

2/ تحديد شخص المحقق :

يختلف تحديد شخص المحقق من دولة إلى دولة أخرى فمنهم من يوكل مهمة التحقيق إلى النيابة العامة ومنهم من يوكلها إلى قاضي التحقيق وهو ما أخذت به الجزائر، وسنتطرق فيما يلي إلى قاضي التحقيق أو الشخص المحقق في الجريمة الإلكترونية.

2 – أ / تعيين قاضي التحقيق :

يمارس مهام التحقيق في الجزائر قضاة التحقيق، ويتم تعيينهم بموجب القانون الأساسي للقضاء الصادر في 06 سبتمبر 2004 ،بمقتضى قرار من وزير العدل لمدة 3 سنوات قابلة للتجديد، وتنهى مهامه طبقا لنفس الأوضاع .

ثم أصبح يعين بموجب مرسوم رئاسي قبل أن يتم إلغاء المادة 39 من ق.إ.ج.ج بموجب القانون رقم 06/ 22 المؤرخ في 20 ديسمبر 2006، ولا تختلف كثيرا صلاحيات قاضي التحقيق سواء في الجرائم التقليدية أو في الجرائم الإلكترونية إلا في كون قاضي التحقيق في الجرائم الإلكترونية يمتد اختصاصه المحلي إلى أقطاب جزائية متخصصة أنظر المادة 40 فقرة 2 والمادة 40 مكرر ق إ.ج.ج ، وهو ما سنعرضه فيما يلي :

2 –ب / اتصال قاضي التحقيق بالجريمة الإلكترونية:

بعد وقوع الجريمة وقيام ضباط الشرطة القضائية بجميع إجراءات البحث وجمع الاستدلالات عن الجريمة الإلكترونية بأنها وقعت، يخطر وكيل الجمهورية قاضي التحقيق بضرورة التحقيق في الجريمة عن طريق النائب العام، حيث يقدم له التماسا لقاضي التحقيق بإجراء التحقيق في هذه الجريمة. ويفصل فيها قاضي التحقيق أنظر المادة 40 مكرر.ق.إ.ج.ج. بأمر :

- ✓ إما بالتخلي عن القضية لصالح قاضي التحقيق على مستوى القطب الجزائي أنظر المادة 40 فقرة 2 والمادة 40 مكرر ق.إ.ج.ج[1].
- ✓ إما رفضه للتخلي عن القضية .

[1] - المواد 40 فقرة 2 و40 مكرر من القانون الإجراءات الجزائية الجزائري.

وفور انتقال الاختصاص لقاضي التحقيق على مستوى القطب الجزائي المختص، ويتلقى ضباط الشرطة القضائية العاملين بدائرة اختصاص القطب التعليمات الخاصة أنظر المادة 40 مكرر ق.إ.ج.ج.[1]

وتبقى نفس الاختصاصات والأوامر الممنوحة للقاضي التحقيق في الجرائم التقليدية هي نفسها الصلاحيات والأوامر الممنوحة للقاضي التحقيق في جرائم المعلوماتية، غير أن الحبس المؤقت هو عبارة عن إجراء استثنائي لمدة زمنية محددة، فيكون في حالات محددة على سبيل الحصر تتمثل في :

- إذا لم يكن للمتهم موطن مستقر .

- إذا لم يقدم ضمانات كافية للمثول أمام العدالة أنظر المادة 123 فقرة ½ ق إ.ج.ج.

- عندما يخالف المتهم من تلقاء نفسه إجراءات الرقابة القضائية أنظر المادة 123 فقرة 2 بند 4 ق.إ.ج.ج.

- عندما يكون الحبس المؤقت الوسيلة الوحيدة للحفاظ على الحجج والدلة أو الشهود أنظر المادة 123 فقرة 2 بند 2 ق إ.ج.ج.

- يكون ضروريا لحماية المتهم أو وضع حد للجريمة أنظر المادة 123 فقرة 2 بند 3 ق إ.ج.ج.

- إذا كانت الجريمة تشكل جنحة معاقب عليها بالحبس مع الغرامة أقل من سنتين أو يساويها أنظر المادة 124 ق إ.ج.ج.

وتكون مدة الحبس المؤقت عندما تتوافر الشروط السابقة الذكر 20 يوما أي 4 أشهر أنظر المادة 125 ق إ.ج.ج[2].

[1] – المواد من 40 فقرة 2 والمادة 40 مكرر والمادة 123 من قانون الإجراءات الجزائية الجزائري.

[2] – المواد من 125،124،123 من قانون الإجراءات الجزائية الجزائري.

ثانيا: صفات المحقق الجنائي:

حيث يعطى للشخص فقه المحقق الجنائي لابد أن تتوافر لديه مجموعة من الصفات الخاصة التي تتوافر فيه من خلال أخلاقه، طباعه، تصرفاته حتى يكون مؤهلا للقيام بجميع صلاحياته ومهامه الموكلة له قانونا ، وتتمثل هذه الصفات والشروط في :

1/ أن يكون هدف المحقق الوصول إلى الحقيقة :

وهو الشرط الأساسي في نجاح المحقق في أداء عمله، وأن يكون اعتقاده هو الوصول إلى الحقيقة[1].

ويجب على المحقق أن يدرك دائما أنه في صراع دائم بينه وبين المجرم المعلوماتي، (الإلكتروني) فالأول يبحث عن الحقيقة، والثاني يجتهد من أجل تضليل العدالة .

وأن يتسم المحقق بفن التحقيق وهو الإبداع والتمكن والقدرة على تحليل الأمور، وفن التحقيق في الجريمة الإلكترونية ليس فقط قدرة المحقق على استبيان وإيضاح مدى توافر أركان الجريمة المعروضة، وعناصرها القانونية وإسناد التهم إلى المتهم، والقدرة على التحقيق في مدى صحة ما يبديه المجرم الإلكتروني ومناقشة الشهود وغيرها، ولابد له أن يتبع جميع إجراءات التحقيق وأن يكون سريع التصرف خاصة سرعة إخطار الخبير الجرائم الإلكترونية ، من أجل التصرف كونه غير قادر على معاينة الجريمة الإلكترونية إلا عن طريق ندب خبير الإلكتروني.[2]

2/ قوة الملاحظة وسرعة البداهة :

أي معرفة المحقق الجنائي الدقيقة لحقيقة أمر أدركته إحدى الحواس أو المعرفة السريعة لتفاصيل الأشياء[3]، حيث لا يدع أمر يمر دون أن يقف عنده بالتأمل والتفكير والتمحيص والتحليل من أجل إظهار الحقيقة وإزالة اللبس بالإضافة إلى عدم انحيازه إلى أي أحد من أطراف الدعوى الجنائية .

[1]– محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، طبعة دار هومة للنشر والتوزيع ، الجزائر 2008، ص13.

[2]– خالد إبراهيم ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 95.

[3]– محمد حزيط ، قاضي التحقيق في النظام القضائي الجزائري ، مرجع سابق، ص15.

3/ الهدوء وحفظ أسرار التحقيق :

لابد على المحقق الجنائي أن يضبط نفسه ولا يستسلم للغضب، وأن يتحلى بالصبر والمثابرة خاصة أثناء استجواب المتهم، وأن يتأنى في الحكم على الدليل أو الأخذ به من عدمه.

كما يجب على المحقق الالتزام بمبدأ سرية التحقيق وكتمانه لمجرياته ضمانا لسير القضية، لذلك يحظر على المحقق إذاعة أو نشر أسرار التحقيقات أو الشكاوى أو الأوراق المتداولة لديه أو عند زملائه المحققين ولا يطلع أحدا من غير ذوي الشأن.

و أن يكون المحقق على علم تام بأحكام قانون العقوبات والإجراءات الجزائية، وإلمامه بقوانين خاصة بالجرائم الإلكترونية (المعلوماتية)، وكذا أي قانون يتعلق بالمعاملات الإلكترونية وتكنولوجيا الإعلام والاتصال ومكافحتها كونه اللبنة الأساسية أو الميثاق الأساسي للجرائم الإلكترونية[1].

حيث كلما زادت معرفته ومعلوماته بالجانب المعلوماتي أدى ذلك إلى زيادة خبرته ودرايته بها، وهناك علوم أخرى لابد على المحقق الإلمام بها، على الكمبيوتر وعلم الأدلة الجنائية، والأدلة الرقمية وغيرها من العلوم التي تختص بمكافحة الجريمة الإلكترونية ، وكيفية استخلاص الدليل الرقمي[2] حيث تساهم هذه العلوم في :

- الكشف على الدليل الرقمي .
- تحديد الخصائص الفريدة للدليل الرقمي .
- إصلاح الدليل وإعادة تجميعه من المكونات المادية .
- عمل نسخة أًلية من التدليل الرقمي .
- جمع الآثار المعلوماتية الرقمية.[3]
- استخدام الخوارزميات Algorithm للتأكد من أن الدليل لك يتم العبث به أو تعديله .

[1]– نبيه صالح ،الوسيط في شرح مبادئ الاجراءات الجزائية،د ط، منشاة المعارف القانونية للنشر، عمان.ص86.

[2]– مرجع نفسه ، ص89.

[3]– فن التحقيق الجنائي في الجرائم الكترونية، مرجع سابق، ص 118.

وهذه كلها تساعد المحقق على معاقبة والقبض على المجرم المعلوماتي والتحقيق في الجرائم الإلكترونية.

ثالثا : عيوب المحقق الجنائي في نطاق الجرائم الإلكترونية:

تشوب أثناء عملية التحقيق عيوب تلحق بالمحقق الجنائي في جرائم المعلوماتية فقد تكون هناك عيوب تتعلق بأسلوب التحقيق، وقد تكون هناك عيوب ترجع إلى شخص المحقق أو عيوب ترجع إلى رؤساء المحقق،[1] وهو ما سنسرده فيما يلي :

1/ عيوب تتعلق بأسلوب التحقيق :

قد تشوب أعمال المحقق أثناء التحقيق في الجريمة المعلوماتية بعض العيوب التي من شأنها أنو تعرقل الوصول إلى الحقيقة ومنها :

1 – أ- عدم الانتقال الفوري لمعاينة مسرح الجريمة الإلكترونية:

قد لا ينتقل المحقق فور تلقي الأخطار بوقوع الجريمة الإلكترونية وذلك بسبب عدم درايته نقص الخبرة والتأهيل في المجال المعلوماتي، أو لكثرة أشغاله ، أو لتأخر المحقق في الوصول إلى مسرح الجريمة فقد يقوم شخص ما بإلغاء أو تحريف رسائل البريد الإلكتروني الموجودة على جهاز الكمبيوتر الخاص بالمتهم، أو تغيير الرقم السري الخاص بالكمبيوتر word Pass لمنع تشغيله، مما يؤدي إلى صعوبة اكتشاف الجريمة سيما أن خصائص الدليل الإلكتروني سهل محوه.[2]

1 – ب- إغفال الدقة في فحص وحصر الدلة التي خلفها المجرم المعلوماتي (الإلكتروني) :

من عيوب التحقيق أيضا إغفال المحقق للدقة الواجبة في فحص وحصر ووصف الأدلة التي خلفها المتهم على مسرح الجريمة أو إغفال ملاحظة ما وعدم تسجيلها اعتقادا منه أنها غير مهمة، ولكنها قد تكون ذات قيمة من أجل استظهار الحقيقة مثال ذلك: عدم ذكر اسم

[1]– مرجع سابق ، ص 128.

[2]– عبد العال الديري و محمد صادق اسماعيل ، الجرائم الاكترونية ، مرجع سابق، ص 327.

الدومين الخاص بالبريد الإلكتروني بالمتهم، والذي قد يكون مرتبط بجهة عمله أو جهة عمل المجني عليه.[1]

1- جـ - الإكتفاء باعتراف المتهم دون اثبات باقي أدلة الجريمة الرقمية:

قد يكتفي المحقق باعتراف المتهم المعلوماتي بارتكاب الجريمة الإلكترونية ، بغض النظر عن إثبات كافة الأثار المادية أو الدلة الإلكترونية التي خلفها المتهم على مسرح الجريمة، مثل إثبات وجود جهاز طابعة، أو وجود مساح ضوئي، أو عدم اثبات اتصال جهاز الكمبيوتر شبكة الأنترنت، في حين أن كل هذه الأجهزة لازمة لتأكيد صحة الاعتراف أو بإظهار كذبه، أو العدول عن اعترافه أمام المحكمة.[2]

1- د - إخلاء سبيل المجرم المعلوماتي قبل استكمال التحقيق:

قد يقوم المحقق بإخلاء سبيل المتهم قبل استكمال أو انتهاء إجراءات التحقيق سواء بضمان مالي أو بضمان محل إقامته، وهذا من شأنه التأثير على حسن سير التحقيق إذ قد يأثر المتهم على شهود الإثبات ليؤثر على شهاداتهم، أو يحتمل هروبه خارج البلاد إذا كان المتهم أجنبي أو يحمل جنسية دولة أخرى.[3]

1- هـ- عدم إعطاء الجريمة الإلكترونية التكييف القانوني الصحيح:

قد لا يستطيع المحقق أن يضع التكييف القانوني الصحيح للجريمة الإلكترونية وذلك بسبب حداثة الجريمة أو يكون المحقق حديث العهد ليست له خبرة في مجال المعلوماتية.[4]

2/ عيوب ترجع إلى شخص المحقق:

وهي عيوب ترجع إلى المحقق نفسه، ومن بين هذه العيوب:

2- أ - الإرهاق في العمل :

إنه ونظرا لعمل المحقق ورغبته في سرعة كشف الغموض عن الواقعة أو الجريمة وكشف الحقيقة وضبط فاعله، مما يجعل المحقق يصاب لإرهاق بدني وذهني، قد يؤثر على تفكيره

[1]- غنام محمد غنام ، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت ،د ط، دار الفكر الفكر والقانون ،المنصورة، 2010، ص89.

[2]- دور قانون العقوبات في مكافحة جرائم الكمبيوتر و الانترنت، مرجع نفسه ،ص90.

[3]- غنام محمد غنام، المرجع السابق، ص91.

[4]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الكترونية، مرجع سابق، ص 128.

وسيره في التحقيق. لذا لابد عليه متى شعر بذلك أن يتوقف عن التحقيق وأخذ راحة حتى لا يؤثر ذلك على التحقيق.[1]

2- ب - التأثر بالمركز الاجتماعي لأحد الخصوم:

وهو الأمر الذي يؤدي بالمحقق للتراخي عن عمله أو الانحياز لذلك الطرف، دون سواه لذلك لابد على المحقق حتى يبتعد عن هذا العيب لابد له أن يستمع لتوجيهات رؤساءه في ذلك المجال وأن يؤدي عمله على أكمل وجه.[2]

2- جـ - اعتناق المحقق بوجهة نظر مسبقة عن الوقعة :

من العيوب الذاتية والشائعة في الحياة العملية، هو تمسك المحقق برأي واحد أو محدد نحو تحديد الفاعل ظنا منه أنه السبيل الوحيد لتحقيق هذا الهدف ويسلك في سبيل ذلك كافة الطرق المؤيدة لوجهة نظره، إلا أن يتبين في نهاية المطاف من عدم صحته وبالتالي يكون قد ضاع من المحقق جهده والكثير من الوقت وقد يصاب بالإحباط.[3]

3/ عيوب ترجع إلى رؤساء المحقق :

هناك بعض العيوب التي تلصق بالمحقق الجنائي وذلك نتيجة أسباب تعود لرؤسائه، ومن تلك العيوب أو الأخطاء :

3- أ- استعجال الانتهاء من التحقيق :

قد يأمر رؤساء المحقق من المحقق إلى استعجال التحقيق من أجل الانتهاء منه في القضايا المتعلقة بالجرائم الإلكترونية ، وهو الأمر الذي يجعل بالمحقق بالإسراع في الإجراءات مما ينتج عنه تقديم المتهم بأدلة ناقصة أو غير صحيحة.[4]

---

[1]- محمد هماج مرهج الهيتي، جرائم الحاسوب، ط1، دائرة المطبوعات والنشر، عمان، 2006، ص210.

[2]- عبد العال الديري و محمد صادق اسماعيل، الجرائم الاكترونية، مرجع سابق، ص327.

[3]- خالد عياد الحلبي، إجراءات البحث والتحقيق في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص134.

[4]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم المعلوماتية، مرجع سابق، ص135.

3- ب- تنازع الاختصاص بين جهات التحقيق :

وهي من العيوب الخطيرة التي تضر بالمواطنين وتفيد المتهم أي كل جهة تحقيق تقول بأنها المختصة (تنازع إيجابيا) أو غير مختصة (تنازع سلبي)، ما يؤثر سلبا على القضية المعروضة نظرا لأن الجريمة المعلوماتية (الإلكترونية) صعبة الإثبات.[1]

3- جـ- عدم التخصص في نطاق التحقيق في الجريمة الإلكترونية:

عدم وجود أجهزة خاصة تقوم بالتحقيق في نطاق الجرائم الإلكترونية خلافا لبعض الدول كالولايات المتحدة الأمريكية توجد بها نيابة جرائم الحاسوب و الاتصالات ، تتشكل من مجموعة من أعضاء النيابة العامة لكنهم تلقوا تدريب مكثف على نظام المعالجة الآلية للمعطيات وتم منحهم مجموعة من الصلاحيات في مجال الاستعانة بغيرهم من خبراء سيما قسم الحاسوب، وكيفية التعامل **مع الدليل** الإلكتروني.[2]

الفرع الثالث : الإجراءات التي يباشرها قاضي التحقيق في الجريمة الإلكترونية:

لقد خص المشرع الجزائري قاضي التحقيق بسلطات واختصاصات واسعة في سبيل تحقيق الهدف من إسناد مهمة التحقيق إلى قاضي تحقيق مستقل عن جهة المتابعة وجهة الحكم، وقد خولته المادة 68 ق.إ.ج سلطة اتخاذ أي إجراء يراه ضروريا للكشف عن الحقيقة، كاستجواب المتهمين، وسماع الشهود والتفتيش وإجراء الخبرات وغيرها من الاختصاصات ، وقد اتجهت إرادة المشرع إلى منحه سلطات جديدة لم يكن يتمتع بها في سبيل مواجهة الأنواع الجديدة من الجرائم الإلكترونية.

وهو ما سنطرق إليه من خلال مايلي :

أولا - المعاينة في الجريمة الإلكترونية:

مع تزايد استخدام الكمبيوتر والإنترنت والشبكات الداخلية والخارجية تزايدت نسبة الجريمة المرتكبة باستخدام هذه التقنيات الجديدة، سواء كانت هذه الجريمة تمت عبر الكمبيوتر، أم

[1]- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص45.

[2]- محمد حماد، مرهج الهيتي، جرائم الحاسوب، مرجع سابق، ص219.

الجريمة تمت على الكمبيوتر، حيث أصبح قضاة التحقيق عاجزون على ضبط واستخلاص دليل إدانة في المجرم الإلكتروني.

ويتطلب مسرح الجريمة سواء كان ماديا أو معنويا (الكتروني) إجراءات خاصة تختلف عن الإجراءات التي سبق وقد عرضناها في مرحلة البحث والتحري عن الجريمة المعلوماتية وذلك باختلاف الجهة القضائية في هذه المرحلة ألا وهو قاضي التحقيق.[1]

1- الانتقال للمعاينة (انتقال قاضي التحقيق للمعاينة):

إن من أعمال قاضي التحقيق الانتقال إلى أماكن وقوع الجريمة للمعاينة وضبط ما قد يعثر عليه من آثار وسماع ما قد يجده من شهود في عين المكان قبل أن يقع التأثير عليهم من المتهم أو من أطراف أخرى وهو ما قرره المشرع الجزائري في أنظر المادة 79 من ق.إ.ج[2] ، وتتم المعاينة في الجريمة الإلكترونية المرتكبة عبر الإنترنت كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني.[3]

وحتى تكون المعاينة صحيحة لابد على قاضي التحقيق أن ينتقل إلى مكان وقوع الجريمة بصحبة كاتبه بعد إخطار وكيل الجمهورية المختص إقليميا بجميع الإجراءات اللازمة ، وحتى يستطيع قاضي التحقيق أن ينتقل إلى عالم الفضاء الالكتروني لمعاينته، عدة طرق تتمثل في:

- الانتقال إلى العالم الافتراضي من المكتب بالمحكمة من خلال الكمبيوتر الخاص به.
- اللجوء إلى مقهى الإنترنت.
- يجوز له اللجوء إلى مقر عمل مزود خدمة الإنترنت الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة، كما يستطيع قاضي التحقيق أيضا الانتقال إلى العالم الافتراضي للمعاينة من خلال مقر مكتب الخبير التقني المختص.[4]

---

[1]- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص59.

[2]- المادة 79 من قانون الإجراءات الجزائية الجزائري.

[3]- عبد العالي الديري، محمد صادق اسماعيل، الجرائم الالكترونية، مرجع سابق، ص264.

[4]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص156 و158.

وبالتالي يتضح مما سبق أن هناك عوائق ومشكلة أمام القاضي التحقيق من خلال الانتقال إلى العالم الافتراضي، حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال آثار الجريمة.[1]

2- الخطوات الواجب إتباعها قبل الانتقال إلى مسرح الجريمة الإلكترونية:

يجب على المحقق الجنائي (قاضي التحقيق) قبل الانتقال إلى معاينة مسرح الجريمة الإلكتروني إتباع الخطوات التالية :

- توفير معلومات مسبقة عن مكان الجريمة، ومالك المكان، نوع وعدة أجهزة الكمبيوتر .
- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل .
- قطع التيار الكهربائي عن موقع المعاينة لشل فعالية الجاني من القيام بأي فعل من شأنه التأثير على أو محو آثار الجريمة .
- إعداد فريق بحث من المختصين والفنيين.[2]

3- شروط صحة معاينة مسرح الجريمة الإلكترونية:

حتى تعطى المعاينة ثمارها للكشف عن الغموض والتوصل إلى الجاني لابد أن يراعي قاضي التحقيق ما يلي :

3- أ- سرعة الانتقال إلى مكان الجريمة :

فور تلقي المحقق أو قاضي التحقيق البلاغ عن وقوع الجريمة من الجرائم المعلوماتية والتأكد من صحة الواقعة، عليه ان ينتقل إلى مكانها، وذلك ضمانا لعدم التغيير شكل مسرح الجريمة عن الوضع والحالة التي تركها الجاني عليه، والحصول على شهادة الشهود.[3]

[1]- خالد عياد الحلبي، إجراءات البحث والتحقيق في جرائم الكمبيوتر والانترنت، مرجع سابق، 155.

[2]- نبيلة هروال هروال، الجوانب الإجرائية لجرائم الإنترنت، مرجع سابق، ص45.

[3]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، 1ط، دار الجامعة الجديدة للطباعة والنشر، بيروت، 1999، ص85.

3- ب- السيطرة على مكان وقوع الجريمة :

بمجرد وصول قاضي التحقيق البلاغ عن مكان وقوع الجريمة من أجل معاينتها لابد من أن يتبع مجموعة من الإجراءات التالية :

- منع تواجد أحد بداخل مسرح الجريمة حتى لا يؤثر ذلك على الآثار والأدلة التي تم العثور عليها في المسرح .
- التأكد من عدم لمس أية آثار أو أدوات بداخل مسرح الجريمة .
- التحفظ على كل ما له علاقة بالحادث من أشياء وأشخاص .
- اخطار الخبراء لرفع الآثار والبصمات.[1]

ثانيا: التفتيش في الجريمة الالكترونية:

تطرقنا في المطلب الأول إلى التفتيش، مفهومه وضوابطه في الجريمة الالكترونية غير أن أوجه الإختلاف في الجهة أو السلطة المختلطة ففي المبحث الأول فإن الضبطية القضائية هي المختصة بالقيام بالتفتيش في مجال الجريمة الالكترونية على خلاف هذا المطلب فإن قاضي التحقيق في هذه الحالة هو المختص وهو ما سنطرق إليه فيما بعد :

وقد خولت المواد من 79 إلى81 ق.إ.ج.ج[2] ، لقاضي التحقيق الاختصاص، الانتقال إلى منازل المتهمين أو المشتبه فيهم أو الذين بحوزتهم أشياء لها علاقة بالجريمة لتفتيشها والحصول على الأدوات المستعملة في الجريمة.[3]

وبالتالي نجد أن جميع الإجراءات الخاصة بالتفتيش في الجريمة الالكترونية في مرحلة جمع الاستدلالات هي نفسها الإجراءات في مرحلة التحقيق القضائي مع بعض الاختلافات البسيطة المتعلقة بجهاز التحقيق (قاضي التحقيق)، وحتى يكون التفتيش الذي يقوم به قاضي التحقيق سواء بنفسه (أو بواسطة ضابط الشرطة القضائية كما بينا سابقا) لابد من احترام مجموعة من القيود والشروط الآتية بيانها:[4]

---

[1]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص159 .

[2] - المواد من 79 إلى 81 من القانون الإجراءات الجزائية الجزائري.

[3]- أحمد شوقي الشلفاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، مرجع سابق، ص240.

[4]- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص118.

– وقوع الجريمة فعلا وان يتحصل على فائدة من وراء التفتيش من أجل كشف الحقيقة.
– أن يكون هناك اهتمام قائم ضد شخص معين من أجل القيام بعملية التفتيش.
– أن تكون الواقعة المرتكبة جناية أو جنحة.
– أن يكون المنزل أو المحل المراد تفتيشه معروفا ومحددا.[1]

كما تجدر الإشارة ان يتم التفتيش من قبل قاضي التحقيق وذلك بعد إخطار وكيل الجمهورية الذي يمكن مرافقته حيث يكون مصحوبا بكاتب التحقيق أنظر المادة 79 ق.إ.ج.ج[2]، فإذا حصل التفتيش في منزل المتهم أو مسكن المتهم أو مسكن شخص آخر يشتبه أن يحوز أشياء لها علاقة بالجريمة فعلى قاضي التحقيق أن يقوم بهذه العملية بحضور المتهم أو صاحب المسكن فإن تعذر حضوره أو كان هاربا يتعين على قاضي التحقيق إحضار شاهدين لايمتان بصلة للمتهم أنظر المادة 80 ،82، 83 ق.إ.ج.ج.[3]

(من الساعة الخامسة صباحا إلى الساعة الثامنة ليلا) وغير أنقاضي التحقيق خرج عن القاعدة العامة في ميعاد التفتيش في الجرائم المعلوماتية حيث يجوز له القيام بعملية التفتيش ليلا أو نهارا أنظر المادة 47 فقرة 4 ق.إ.ج.[4]

ثالثا – الاستجواب والشهادة وضبط الأدلة في الجريمة الالكترونية:

يقوم قاضي التحقيق في مجال الكشف والبحث والتحري عن الجريمة الالكترونية وكشف الغموض عنها والقبض على فاعلها باتخاذ الكثير من الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه، ومن بينها :

– استجواب المتهم .
– سماع شهود (شاهد الكتروني).
– ضبط الدليل الالكتروني .

[1]– عبده جميل غصوب، الوجيز في قانون الإجراءات الجزائية، ط1، المؤسسة الجامعية للنشر والتوزيع، بيروت، 2011،ص 298.

[2]– المادة 79 قانون الإجراءات الجزائية الجزائري.

[3]– المواد من 80 ،82، 83 من قانون الإجراءات الجزائية الجزائري.

[4]– المادة 47 فقرة 4 من قانون الإجراءات الجزائية الجزائري.

وهو ما سنطرق إليه فيما يلي :

1- استجواب المتهم :

الاستجواب هو مناقشة المتهم بالتهم والوقائع المنسوبة إليه ومواجهته بالأدلة القائمة ضده والمتهم حر في الإجابة عن الأسئلة الموجهة عليه ولا يعد امتناعه قرينة ضده، وهو وسيلة تمحيص للتهم أو لنفيها عنه فهو طريق من طرق تقصي الحقيقة ومصدر من مصادر الإثبات وليس وسيلة إثبات. إذ يعتبر الاستجواب ذو طبيعة مزدوجة فهو أداة اتهام ووسيلة دفاع في آن واحد بحيث يسمح للمتهم أن يحاط بالتهم والوقائع المنسوبة إليه وبكل ما يوجد بالملف من أدلة التي تساعد على كشف براءته.

ويختلف الاستجواب عن السؤال و أن الثاني لا يتطلب مناقشة المتهم في هويته، ومدى خطورته، اعمالا بالمواد .

- استجواب المتهم في الموضوع: أي مواجهة قاضي التحقيق المتهم بالتهم المنسوبة إليه ومناقشته في ها مناقشة تفصيلية ومواجهته بالأدلة القاطعة ضده ولابد ان يكون الاستجواب بحضور المحامي طبقا لنص المادة 57 /110، 101 ، 102،ق.ا.ج.ج.

- الاستجواب الإجمالي للمتهم: يكون في مسائلة جنائية (جنايات) وهو إجراء وجوبي إذ تعلق التحقيق بقضية ذات طابع جنائي، يهدف إلى تخليص الوقائع وإبراز الأدلة التي سبق جمعها.[1]

**** القواعد التي يلتزم بها المحقق في الاستجواب:**

يعتبر الاستجواب اجراء من الإجراءات العامة في التحقيق لأن نجاح المحقق في اسناد الواقعة إلى الجاني واعترافه بارتكابها ، وحتى يكون الاستجواب صحيحا لابد ان يتضمن مجموعة من الإجراءات وهو ما سنتناوله بالتفصيل فيما يلي:[2]

1- أ/ القواعد التي يلتزم بها المحقق قبل إجراء الاستجواب :

قبل أن يقوم المحقق بإجراء الاستجواب والمواجهة عليه أن يستعد لها وذلك بإتباع القواعد العامة التالية :

[1]- محمد حزيط، المرجع نفسه، ص103.

[2]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص240.

- ✓ الإلمام الكامل بفهم أقوال الشهود وسائر المتهمين أن يحدد النقاط الجوهرية التي سيتم ايضاحها من المتهم .
- ✓ فهم فحوى التقارير الفنية التي وضعها الخبراء عن نتائج عملهم في الآثار المستخلصة.
- ✓ وضع خطة لنفسه يسير عليها في استجواب المتهم.[1]

1- ب/ القواعد التي يلتزم بها المحقق الجنائي عند البدء في الاستجواب :

على المحقق عند البدء في الاستجواب أن يراعي اتخاذ وإتباع القواعد التالية :

• إذا إستعان المتهم عن محاميه لابد من دعوة المحامي لحضور الاستجواب و تفتيش المتهم..

• عدم إكراه المتهم على الاعتراف بأي شكل من أشكال التعذيب.

2- الشهادة الالكترونية (سماع الشهود) (الشاهد الالكتروني):

في هذا الجزء سنطرق إلى الشهادة الالكترونية:

2- أ/ الشهادة الالكترونية :

إن مصطلح الشهادة الالكترونية يطلق على نوع من الشهادة التي لا يكون فيها الشاهد حاضرا فقد تتم مثلا عن طريق وسائل الكترونية أو رقمية من خلال شبكة الإنترنت.[2]

وقد أعطى قانون الإجراءات الجزائية لقاضي التحقيق الحرية في تحديد الأشخاص الذين يرى فائدة من سماع شهادتهم، سواء كان هؤلاء الأشخاص قد ورد ذكرهم في البلاغ عن الجريمة او الشكوى منها، أو أي شخص آخر، وذلك تطبيقا للمواد 60،97،88،110 ق.إ.ج.[3]

2- ب/ ضبط الدليل في مجال الجريمة الالكترونية:

الضبط كقاعدة عامة لا يرد إلا على أشياء مادية، فلا صعوبة في ذلك، وبالتالي يضبط الدليل في الجريمة الالكترونية على المكونات المادية للكمبيوتر، فترفع البصمات مثلا

[1]- خالد ممدوح ابراهيم،المرجع نفسه، ص243.

[2]- عبد العالي الديري، محمد صادق اسماعيل، الجرائم الاكترونية، مرجع سابق، ص313.

[3]- المواد 60 ،88 ،97 ،110 قانون الإجراءات الجزائية الجزائري.

وغيرها، فلا صعوبة في ذلك، وإنما تكمن الصعوبة في ضبط الوسائل الفنية أو المعنوية المستخدمة في إتلاف البرامج وقد تم التطرق إليها أنواع الأدلة الالكترونية ، بالإضافة إلى العديد من الصلاحيات والسلطات المخولة لقاضي التحقيق التي تمارسها الضبطية القضائية في إطار الإنابة القضائية أو بناء على إذن منه وتتمثل في أساليب التحري الخاصة.

المبحث الثاني: مرحلة المحاكمة

تختلف الجريمة الإلكترونية عن بعضها البعض في مجال الاختصاص ففي حالة ما إذا ارتكبت الجريمة الإلكترونية بواسطة المكونات المادية للحاسب الآلي فهذه الجريمة تعود اختصاصها إلى المحاكم الجزائية العادية، أما في حالة ارتكاب جريمة على نظام المعالجة الآلية (على المكونات المعنوية) ففي هذه الحالة فإن القطب الجزائي هو المختص في هذه الجريمة نظرا لصعوبة اثباتها، أثناء مرحلة جمع الاستدلالات والتحقيق ونظرا لخطورة الفعل المرتكب، ونقص الخبرات للقضاة في المجال الإلكتروني أمام المحاكم العادية، هذا في مجال مكافحة الجريمة الإلكترونية على المستوى الداخلي (مرحلة المحاكمة).

المطلب الأول: اختصاص المحكمة (المحلي و النوعي) للجرائم الإلكترونية

لقد أبرزنا في الفصل أول كيفية نشأة الأقطاب الجزائية المتخصصة وماذا يقصد بها والقوانين التي تناولتها ، والتعديلات التي طرأت عليها إما بتوسيع نطاق بعض الأقطاب بإضافة مجالس قضائية جديدة إليها أو تحديد إقليمها[1]، بحيث يشمل اختصاص كل جهة فضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا، جنويا، شرقا، وغربا، ولذلك لدينا أربع محاكم تسمى أقطابا جزائية، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيه الجريمة الإلكترونية ، وإن كان ولابد من تبيين اخصاصها المحلي والنوعي في هذا النوع من الجرائم.

أصبحت الأقطاب الجزائية المتخصصة وهيكلتها أمرا مهما لابد منه بعد الفترة العسيرة التي مرت بها، وفي إطار دراستنا سنتطرق في الفرع الأول إلى الجانب البشري وهو الجانب

[1] – بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة لنيل شهادة ماستر، جامعة المسيلة، 2016، ص52.

الذي يمثلها ويقوم بتسيير أعمالها وكذا الجانب التقني، والهياكل القاعدية ثم نتناول إختصاصها (المحلي و النوعي) في الفرع الثاني:

الفرع الأول: هيكلة الأقطاب الجزائية المتخصصة[1]

1/ العنصر البشري:

ويعني هذا ابراز دور العنصر البشري الذي يتكون منه القطب، وبالتالي فالحديث يكمن هذا عن القضاة وكذا أمناء الضبط فنجد أن جميع المعالم الجزائية موجودة في النظام القضائي الجزائي حيث تتكون من :

- قضاة التحقيق .
- قضاة الحكم .
- أمناء الضبط .

وباعتبار أن الأقطاب الجزائية هي أجهزة تنتمي إلى القضاء الجزائي فهو يتكون من:

- وكيل الجمهورية .
- وكيل جمهورية مساعد .
- قاضيان للتحقيق على الأقل يشرفان على غرفة التحقيق .
- قاضي حكم يشرف على قسم تابع للقضاء الجزائي المتخصص .
- أمناء ضبط مكلفون بأعمال تنظيم الملفات ومساعدة القضاة.[2]

2/ التكوين التقني:

يقصد به خضوع القضاة والأمناء العاملين في القطب الجزائي إلى تأهيل خاص بهم من أجل التخصص والتعمق أكثر في مجال البحث والتحقيق في الجرائم والقضايا المعروضة عليها خاصة وأنها جرائم محددة على سبيل الحصر نظرا لخطورتها، ولذلك فهي تتطلب تكوين خاص ، فمنذ إنشاء وتأسيس هذه الأقطاب والنص عليها في القانون الجزائري فهي تعاني من عدم وجود تخصص فعلي في القضاة، يعني لا وجود لقضاة متخصصين في هذا

[1] – 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.

[2] – محمد امقرن، التنظيم القضائي الجزائري ،ط1، دار هومة للنشر والتوزيع ، الجزائر2009 ،ص25.

المجال، لذلك نجد أن الدولة تسعى دائما إلى جعل القضاة متخصصين من خلال الدورات التكوينية[1]، في اطار سياسية التكوين المستمر للقضاة في مجال الاقطاب الجزائية المتخصصة قامت وزارة العدل بتنظيم دورات تكوينية لفائدة القضاة العاملين بالمحاكم الجزائية المتخصصة بالمدرسة العليا للقضاء من 03 الي 07 ماي2008.

3/ التكوين القاعدي:

يقصد به توفر جميع المرافق والأجهزة التي تستكمل بها الأقطاب الجزائية عملها من اجل تفعيلها، وتتمثل في مدى توافر المقرات وجاهزيتها، ولابد ان تكون مستقلة .

الفرع الثاني: اختصاص الأقطاب الجزائية المتخصصة

بالرجوع إلى نص المواد 37،40،329 ق.إ.ج.ج في توسيع الاختصاص المحلي لكل من وكيل الجمهورية، قاضي التحقيق وكذا المحكمة إلى دائرة اختصاص المحاكم الأخرى تحدد عن طريق التنظيم وذلك بخصوص 6 جرائم مذكورة على سبيل الحصر. ومن بينها الجريمة الإلكترونية حيث تم انشاء محاكم أو أقطاب جزائية متخصصة ذات اختصاص إقليمي ومحلي موسع وهو ما سنعرضه من خلال ما يلي :

1- الاختصاص المحلي :

تتميز الأقطاب الجزائية المتخصصة بأنها ذات اختصاص محلي موسع طبقا لقانون الإجراءات الجزائية[2] ، فقد تم تمديد الاختصاص المحلي لوكيل الجمهورية وقضاة التحقيق ، وبصدور المرسوم التنفيذي رقم 06-3348 والذي تم بموجب تحديد وتعيين المحاكم ذات الاختصاص الإقليمي الموسع وكذا الجهات القضائية لهذه المحاكم اليها. كما قد تناولناها في الفصل الأول.

2- الاختصاص النوعي :

بمقتضى القانون 04/ 14 المؤرخ في /10/ 11 2004 المتضمن تعديل قانون الإجراءات الجزائية، وذلك في المواد 37 ،40 ،329 منه المذكورة سلفا، والمادة 01 من

[1] – كور طارق ، اليات مكافحة جريمة الصرف، ط2 ، دار هومة للنشر والتوزيع ، الجزائر2014.ص 155 .

[2] – المواد 37،40،329 من قانون الإجراءات الجزائية الجزائري.

[3] – كور طارق.اليات مكافحة جرائم الصرف.مرجع سابق.ص 161.

المرسوم التنفيذي رقم 06 – 348[1] المتعلق بتحديد وتعيين المحاكم ذات الاختصاص الإقليمي الموسع جاءت بالجرائم التي تخضع لاختصاص تلك المحاكم، وجاءت على سبيل الحصر– جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية ، جرائم تبييض الأموال،[2] جرائم الارهاب،[3] جريمة مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من والى الخارج،[4] و الجرائم الماسة بأنظمة المعالجة الالية للمعطيات المنصوص عليه في المواد 394 مكرر الى 394 مكرر07 ق.ع.ج .المعدل وكذا قانون 09/ 04 وهو موضوع بحثنا ودراستنا هذه .

المطلب الثاني: إجراءات المحاكمة والقواعد العامة لها

إجراءات مختلفة عن تلك المتعلقة بالجهات القضائية الكلاسيكية، وهذا يتطلب توافر هذه الجهات القضائية المتخصصة على نوع جديد من التنظيم وقواعد جديدة للسير والاتصال بالقضايا متى اتضحت معالم الجريمة من حيث التكييف القانوني للوقائع والطابع المميز للجريمة ولذلك لابد من اللجوء الى الجهة القضائية المتخصصة وتفادي إحالة الملفات البسيطة والعادية على الجهات القضائية المتخصصة، وهو الشيء الذي تتميز به فهي تنظر فقط في الجرائم الخطيرة، ومن خلال ذلك لابد أولا من التطرق الى كيفية اخطار واتصال القطب الجزائي بالقضايا في الفرع الأول . واجراءات المطالبة من طرف النائب العام في الفرع الثاني

الفرع الأول: اتصال القطب الجزائي بالقضايا

أولا: اخطار الأقطاب الجزائية المتخصصة:

---

[1]– المرسوم التنفيذي رقم 06 –348 المؤرخ في /05/ 10 2006 متعلق بتمديد الاختصاص المحلي لبعض المحاكم أو وكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية العدد 63.

[2] – المواد من 1 إلى 35 من القانون 05 –01 المؤرخ في 06 فبراير 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتها، وكذا قانون إجراء جزائية القسم السادس مكرر من قانون العقوبات .

[3] – المواد 87 مكرر إلى 87 مكرر–* 10 قانون العقوبات بموجب تعديله للأمر 95 /11 المؤرخ في 25 فبراير 1995 والتعديل الثاني بموجب القانون 06/23 المؤرخ في /20/ 12 2006.

[4] – الأمر 96 /22 المؤرخ في 19 يوليو 1996 المعدل والمتمم بالأمر 03/ 01 في المؤرخ2003/02/29 والأمر 03/10 المؤرخ في 09 يونيو 2010.

لكي يتم اتصال الأقطاب الجزائية المتخصصة بالقضية لابد من إجراءات حتى يعود لها الاختصاص للنظر فيها، وهذا لا يأتي الا من خلال اخطارها وذلك عن طريق اجراء المطالبة بممارسة النائب العام فهذا الاجراء الذي يقوم به النائب العام له أثرين :

- أ/ ناقل للاختصاص.

- ب/ تخضع الضبطية القضائية للأجهزة القضائية المتخصصة مباشرة من حيث الإدارة لوكيل الجمهورية، الاشراف للنائب العام المراقبة لغرفة الاتهام الانابة القضائية لقاضي التحقيق

وقد نصت مواد 40 مكرر 01 ،40 مكرر 02 ،40 مكرر03 ، 40مكرر 04 ،و 40 مكرر 05 ق.إ.ج.ج على كيفية سير هذه المحاكم ذات الاختصاص الإقليمي الموسع والكيفية التي تخطر بها بحيث لابد من اخبار واخطار وكيل الجمهورية لدى المحكمة العادية فورا من قبل الضبطية القضائية بالواقعة حصول او حدوث جريمة من جرائم الماسة بأنظمة المعالجة الالية للمعطيات (جريمة معلوماتية) بهذه الجريمة في دائرة اختصاصه، ويبلغونه عن طريق نسختين من محاضر التحقيق التي قاموا بها.[1]

ثم يرسل وكيل الجمهورية النسخة الثانية الى النائب العام لدى المجلس القضائي التابعة له المحكمة ذات الاختصاص المحلي الموسع حسب ما جاء في المرسوم التنفيذي 06 – 348 السابق ذكره ، كما جعل قانون الإجراءات الجزائية للنائب العام التابعة له المحكمة المختصة دورا محوريا واساسيا في اخطار المحكمة المختصة بملف الجريمة الإلكترونية .

اذ للنائب العام وحده صلاحية طلب ملف القضية من الجهات القضائية الداخلة ضمن اختصاص القطب الجزائي، اذ اعتبر هذا الأخير ان الجريمة تدخل ضمن اختصاص .

ثانيا: المطالبة بالإجراء من النائب العام

كما وسبق ذكره في الفرع الأول انظر المادة 40 مكرر 01 .ق.إ.ج.ج ، انه للنائب العام دور أساسي في مجال اخطار او المطالبة من القطب الجزائي الاختصاص في مجال

[1]– المواد من 40 مكرر 01 الى 40 مكرر 05 من القانون 04 –14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري .

الجريمة الإلكترونية وهو ما أكدته المادة 40 مكرر02 ، والمادة40 مكرر 03 حيث انه يجوز للنائب العام لدى المجلس القضائي مطالبة الإجراءات في جميع مراحل الدعوى[1].

الفرع الثاني: إجراءات المطالبة والتخلي عن القضية لصالح القطب الجزائي .

بعدما تصل القضية الى أروقة المحكمة فهي تسلك أحد الطرفين اما التمسك بها واما يتم التخلي عنها. أذ إ ن النيابة لها من يمكن لها التصرف في ملف الدعوى بالحفظ، الا انها قدمتها للقضاء اذ يصبح وحده صاحب الحق في الحكم وليس للنيابة العامة الحق في إعطاء طلبات شفوية او الكتابية حيث ان النيابة العامة لا يجوز لها التخلي عن حق المطالبة الذي خوله القانون لها وفقا لقانون الإجراءات الجزائية خاصة المادة 37 منه، كما انه على وكيل الجمهورية ابلاغ النائب العام لدى المجلس القضائي التابعة له القطب الجزائي المتخصص بنسخة من اجراء التحقيق.

وهو امر ضروري حتى يتمكن النائب العام لدى المجلس القضائي التابع له القطب الجزائي من تفعيل اجراء المطالبة بالملف فكما قلنا سابقا إذا كان وكيل الجمهورية يتبع النائب العام التابع للمجلس القضائي التابع له القطب الجزائي الذي يمارس فيه النائب العام صلاحياته .

غير ان الاشكال الذي يطرح في هذا الصدد في حالة ارتكاب او وقوع جريمة تقع في محكمة تابعة لمجلس قضائي اخر، وتدخل ضمن الاختصاص الموسع للقطب الجزائي. فيكون الإبلاغ من طرف النائب العام التابع له القطب الجزائي المتخصص من طرف النائب العام لدى المجلس القضائي الذي وقعت الجريمة في دائرة اختصاصه وبالتالي على وكيل الجمهورية التخلي عن القضية لصالح النائب العام لدى القطب الجزائي المتخصص عن طريق إبلاغه للنائب العام بالمجلس الذي بدوره يجب عليه ابلاغ القطب أنظر المادة 40 مكرر 03 فقرة 02 ق.إ.ج.ج[2].

أولا: دور النائب العام المحور ي في الإجراءات .

[1]– المواد من 40 مكرر 01 و40 مكرر 02 و40 مكرر 03 و40 مكرر03 فقرة 15 من القانون الإجراءات الجزائية الجزائري.

[2]– المادة 40 مكرر 03 فقرة 02 قانون إجراءات جزائية جزائري.

انه وباستقراء نصوص المواد 40 مكرر 01 الى 40 مكرر 03 ق.إ.ج ان للنائب العام التابعة له المحكمة الجزائية المتخصصة دورا محوريا واساسيا في اخطار القطب الجزائي بوقوع جريمة من الجرائم المعلوماتية (الجرائم المنصوص والمعاقب عليها في المواد 394 مكرر الى 394 مكرر 2 قانون عقوبات جزائري) التي تدخل في اختصاصها كما بينا سابقا أنظر المواد من 40 مكرر01 إلى 40مكرر 05 مع ارسال الملف للقطب للنظر فيه، كما يملك صلاحية المطالبة بملف الإجراءات في جميع مراحل الدعوى سواء كانت في مرحلة التحريات الأولية او في التحقيق القضائي، او كانت على مستوى غرفة الاتهام أنظر المادة 40 مكرر03 ق.إ.ج.ج، وفضلا عن ذلك تجدر الإشارة بالإضافة الى القيام بالإجراءات المذكورة أعلاه تطبق القواعد والإجراءات العادية المنصوص عليها في قانون الاجراءات الجزائية.

ثانيا: تخلي قاضي التحقيق عن القضية للنائب العام .

اعتبر قانون الإجراءات الجزائية الجزائري انه من الصلاحيات الأساسية لقاضي التحقيق متابعة ملف القضية (التحقيق) على مستوى المحكمة التي وقعت في دائرتها الجريمة، والتي اتضحت من معالم القضية فيما بعد ان هذه الجريمة هي من الجرائم الخطيرة المذكورة في المادة 37 ق.إ.ج [1]والتي تدخل من الاختصاص الموسع للقطب الجزائي، حيث يتجنب التحقيق فيها من خلال مطالة النائب العام بملف الدعوى لصالح القطب الجزائي المتخصص في أي مرحلة من مراحل الدعوى وهو ما أكدته المادة 40 مكرر 03 /02 ،حيث سيصدر قاضي التحقيق امرا بالتخلي عن الدعوى لفائدة قاضي التحقيق لدى القطب الجزائي المختص أنظر المادة 40 مكرر03 فقرة 02 ق.إ.ج.ج[2].

أي انه على قاضي التحقيق لدى المحكمة العادية في حالة صدور مطالبة من النائب العام بملف القضية يصدر القاضي التحقيق امر التخلي على القضية لصالح القطب الجزائي وفي حالة رفضه لإصدار امر التخلي عن القضية لصالح قاضي التحقيق بالقطب المتخصص يمكن للنائب العام ان يستأنف امر التخلي حسب القواعد العامة.

[1]– المواد 40 مكرر 03 و37 من قانون إجراءات جزائية جزائري.

[2]– المادة 40 مكرر03 فقرة 02 من قانون إجراءات جزائية جزائري.

خلاصة:

نظرا لخصوصيات التي تتميز بها جرائم المساس بالأنظمة المعلوماتية او المعالجة الالية للمعطيات او الجريمة الإلكترونية وتطورها السريع والمستمر، جعل من الدول ومنها الجزائر الى وضع الية قانونية جديدة للحد من خطورة هذه الجريمة على المجتمع ككل من خلال تمديد الاختصاص المحلي لبعض المحاكم لقضاة التحقيق ووكيل الجمهورية من خلال الية قضائية جديدة تعرف بالقطب الجزائي المتخصص من خلال عرض وجيز لكيفية سير وتنظيم هذه الهيئة وكذا هيكلتها بالإضافة الى قواعد اختصاص الأقطاب الجزئية المتخصصة النوعي أي تختص في نوع معين من الجرائم محددة على سبيل الحصر ومن بينها الجريمة الإلكترونية في نص المادة 37 ق.إ.ج.ج.

وكذا توسيع اختصاصها المحلي ليشمل بعض المجالس القضائية وحددها في أربعة اقطاب فقط. وهران، قسنطينة، الجزائر، ورقلة. بالإضافة الى عرض القواعد الإجرائية لتسييرها والدور الأساسي الذي يلعبه النائب العام هذا فيما يخص بالجهود الداخلية، اما بالنسبة للجهود الدولية فقد عمدت جميع الدول والهيئات الى الحد او التقليص من خطورة الاجرام الإلكتروني وتأثيره على العام للدول والمؤسسات، وكذا الأشخاص مما دفعها الى محاولة وضع أطراف قانونية من اجل مجابهة الجريمة الإلكترونية ومكافحتها سواء على المستوى الدولي المتمثل في الاتفاقيات الدولية.

بالإضافة الى جهود تبذل على المستوى العربي ممثلة في القانون العربي النموذجي، اما بالنسبة للمشروع الجزائري فقد واكب ولو بقدر قليل الحركية التشريعية التي فرضت نفسها عالميا في مجال مكافحة الجريمة الإلكترونية.

خاتمة

خاتمة

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

وأمام هذا التطور فقد ارتبطت به الظهور ما يعرف بالإجرام الإلكتروني (المعلوماتي) وذلك نتيجة الاستخدام السيئ للمعلوماتية أو الحاسوب الذي نتج عن هذا 51خير عدة أضرار يمكن حصرها، وذلك إنها تهدد أمن المعطيات من جهة وتمس بحرية الأفراد والمؤسسات من جهة أخرى.

ولأن الحماية الفنية مهما بلغت درجتها من التعقيد وصعوبة فهي تستطيع المقاومة أمام التطور التقني الذي تشهده تقنيات الاختراق وكذا عجز النصوص التقليدية في توفير الحماية خاصة من الناحية الإجرائية.

مادفع العديد من الدول إلى إبرام اتفاقيات وسن قوانين داخلية من أجل توفير الحماية الجنائية الإجرائية لها، ومن هذه الدول الجزائر.

وقد حاولنا من خلال الفصلين كاملين الوقوف على حل الأحكام الإجرائية الخاصة بمتابعة مرتكبي الجرائم الإلكترونية من أجل إقرار الحماية لها، فوجدنا ان للجريمة الإلكترونية خصوصية من الناحية الإجرائية من خلال اعتمادنا على قانون الإجراءات الجزائية الجزائري وكذا قانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته. حيث وجدنا ان قانون الإجراءات الجزائية الجزائري ينص فقط على القواعد العامة التي تطبق على الجرائم التقليدية وكذا على المعلوماتية اما بالنسبة

للقانون 09/04 الذي وضع لمتابعة الجريمة الإلكترونية من خلال بعض الإجراءات الخاصة ممثلة في حجز المعطيات وكذا مراقبة الاتصالات الإلكترونية وحفظ المعطيات.

في نفس الصدد وجدنا أن بعض الإجراءات تعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية كالمعاينة على مسرح الجريمة مشتركا بين الجرائم المسرح التقليدي و الافتراضي وكذا التفتيش الإلكتروني وضبط الدليل الرقمي والمستحدث إجراءات جديدة جاء بها تعديل قانون الإجراءات الجزائية سنة 2006 التي تعرف بأساليب التحري حيث تعتبر كل هذه الإجراءات تطبق سواء كانت الجريمة إلكترونية أو التقليدية ، ومنها إجراءات لا تطبق إلا على الجرائم الإلكترونية و هي إجراءات المحاكمة التي يخص بها الأقطاب الجزائية المتخصصة بالإضافة إلى إجراءات خاصة جاء بها قانون 04/09.

- لابد ان يكون التفتيش على المكونات المادية للحاسب الآلي.
- المعاينة تتم على مستويين في الجريمة الإلكترونية في المسرح التقليدي والمسرح الإفتراضي.
- ضبط الدليل الرقمي الكترونيا وكذا سماع الشهود الخاصين فقط والعالمين بالجانب المعلوماتي.
- مراقبة الاتصالات إلكترونية وكذا حفظ المعطيات و هي اجراءات جاء بها قانون 09-04 ان يتم التحقيق في الجريمة إلكترونية قاضي التحقيق الذي لابد ان تتوافر فيه مجموعة من المؤهلات التي تؤهله من اجل متابعة التحقيق.
- متابعة المجرم إلكتروني امام الأقطاب الجزائية المتخصصة.
- مكافحة الجريمة على المستويين الدولي والعربي.
- تكريس التعاون الدولي من اجل مكافحة هذا النوع من الجرائم خاصة في مجال الإجراءات الدولية ممثلة في المساعدة القضائية الدولية وكذا تسليم المجرم إلكتروني.

وقد لاحظنا في نهاية عرضنا هذا الموضوع أنه من الموضوعات الصعبة والمتشعبة خاصة فيما يتعلق بالجانب الإجرائي ولعل أهم المشكلات التي واجهتنا في إعداد بحثنا هذا .

وبالرغم من وجود نصوص قانونية فأن مكافحة الجريمة إلكترونية رهينة بالمعيقات الإجرائية في مجال المتابعة فإن أول إشكال أو عائق هو غياب القدرات التأهيلية والوسائل الفنية التي تنتج سرعة إدراك ما حصل وأن غياب التأهيل قد يؤدي إلى إتلاف الدليل وإفلات مرتكبي هذه الجرائم من العقاب بالإضافة إلى مشكلات في القانون الواجب التطبيق كون الجريمة إلكترونية عابرة للحدود.

– إعادة النظر في مدي تطبيق القوانين من عدمه.

– الإسراع لسن قواعد إجرائية خاصة تتلأم مع طبيعة الجريمة إلكترونية حتى تكون أكثر فعليه.

– بالإضافة إلى تكثيف الجهود الدولية والإقليمية لمكافحة هذا النوع من الإجرام.

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

– تدريس الأنظمة المعلوماتية والجرائم الواقعة في كليات الحقوق والمعاهد وتفعيل دور الأسرة في متابعة أبنائهم لوقايتهم من الآثار السلبية لاستخدام السيئ لشبكة الأنترنت.

– بالإضافة إلى ووجوب ضرورة وجود تعاون دولي في مجال مكافحتها.

وأخيرا لا يسعنا من خلال دراستنا هذه إلا القول بأن مجال المعلوماتية و الاعتداءات الواردة عليها متجددة و لا تحدها حدود ، لهذا لا بد أن يتم التصدي لهذا الموضع بالدراسة القانونية المستفيضة و المتخصصة و التي لا تزال ليومنا هذا لاسيما في الدول العربية عموما و الجزائر خصوصا دون المستوى المطلوب بالرغم من مخاطر وأضرار الزحف المعلوماتي و التي باتت حقيقة تهدد معها كل المصالح دون استثناء، و عليه نكون قد انهينا دراسة لهذا الموضوع دراسة متواضعة و الذي تم بعون الله و توفيقه.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

1 / الكتب:

– احسن بوسقيعة، الوجيز في القانون الجزائي القسم العام، ط1، دار هومة للنشر والتوزيع ، الجزائر2010،

– محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، طبعة دار هومة للنشر والتوزيع ، الجزائر 2008،

– هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة،أسيوط،1992 م

– ناول عبدالهادي، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، مجلة العدل، العدد 31 رجب 1427هـ.

– محمد علي العريان،الجرائم المعلوماتية، أعمال الندوة الإقليمية حول«الجرائم المتصلة بالكمبيوتر 20–19 نيسان/يونيو، ، المملكة المغربية2007.

– أسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة 1994.

– ممدوح خليل عمر ، حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية القاهرة 1983 .

– خالد عياد الحلبي. إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ط. 1 دار الثقافة للنشر والتوزيع ، عمان 2011.

– أحمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري – الجزء 2 ، طبعة 05 ديوان ، المطبوعات الجامعية، الجزائر.

– نبيه صالح ،الوسيط في شرح مبادئ الاجراءات الجزائية،د ط، منشاة المعارف القانونية للنشر، عمان.

– محمد صبحي نجم ،الوجيز في قانون اصول المحاكمات الجزايئة ط1 ، دار الثقافة للنشر والتوزيع، الاردن،2012.

– عبد الفتاح بيومي الحجازي ، اصول التحقيق والتاديبي ، د ط.دار الفكر الجامعي ،الاسكندرية،2005.

– محمد الهيتي.التحقيق الجنائي والادلة الجنائية المادية، ط1 ، دار المناهج للنشر والتوزيع ،عمان 2010.

– محمد حماد مرهج الهيتي، الادلة الجنائية المادية،د ط، دار الكتب القانونية مصر 2008.

– مراد احمد العبادي ، اعتراف المتهم واثاره في الاثبات ط1 ، دار الثقافة للنشر و التوزيع، عمان2010.

– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، 1ط، دار الجامعة الجديدة للطباعة والنشر، بيروت، 1999.

- عبده جميل غصوب، الوجيز في قانون الإجراءات الجزائية، ط1، المؤسسة الجامعية للنشر والتوزيع، بيروت، 2011.

2 / الدساتير و الاتفاقيات الدولية:

- الدستور الجزائري سنة 1996.

- الاتفاقية الأوروبية الموقعة في بودابست في 2021/04/14 في إطار دور الشرطة في مكافحة جرائم الإنترنت.

- الميثاق العالمي لحقوق الإنسان، المعتمد بموجب قرار الجمعية العامة للأمم المتحدة 217 ألف المؤرخ في 10 ديسمبر 1948.

- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر 2000.

3/ القوانين:

- القانون 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها.

- القانون 14/04 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 15 /02 المؤرخ في 230يوليو 2015 المعدل والمتمم لقانون الاجراءات الجزائية الجزائري .الجريدة الرسمية العدد .40

- قانون العقوبات بموجب تعديله للأمر 95 /11 المؤرخ في 25 فبراير 1995 والتعديل الثاني بموجب القانون 06/23 المؤرخ في /20/ 12 2006 و طبقا للأمر 96 /22 المؤرخ في 19 يوليو 1996 المعدل والمتمم بالأمر 03/ 01 في المؤرخ2003/02/29 والأمر 03/10 المؤرخ في 09 يونيو 2010.

- الأمر 96 /22 المؤرخ في 19 يوليو 1996 المعدل والمتمم بالأمر 03/ 01 في المؤرخ2003/02/29 والأمر 03/10 المؤرخ في 09 يونيو 2010.

- القانون الأساسي للقضاة الصادر في 06 سبتمبر 2006 الجزائر.

4/ الرسائل والمذكرات العلمية:

- اسميرة معاشي،التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية،1432 هـ /2011م.

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

– نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكر مقدمة لنيل شهادة الماستر، نخصص قانون الإداري، جامعة أدرار، 2017/2016.

– ابتسام بغو ،اجراءات المتابعة الجزائية في الجرائم المعلوماتية، مذكرة تكميلية لنيل شهادة ماستر، تخصص قانون الجنائي للأعمال، جامعة أم الأبواقي ،2016.

5/ مجلات:

– عادل بوزيدة، الحماية الجزائية لأسماء نطاق المواقع الإلكترونية ،على ضوء قانون حقوق المؤلف والحقوق المجاورة، مجلة العلوم القانونية والسياسية ، جامعة العربي التبسي تبسة ،الجزائر، ، 2018، عدد 17.

– فايز بن عبدالله الشهري، التحديات الأمنية لوسائل الاتصال الجديدة – دراسة الظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد20، العدد39.

– رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة،العدد41، جامعة أحمد دراية أدرار،2018/2017.

– ونوغي نبيل، زيوش عبد الرؤوف ، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية و الاجتماعية، المجلد الرابع، العدد 03، المركز الجامعي أحمد بن عبد الرزاق حمودة – سي الحواس – بريكة، باتنة ،سبتمبر 2019.

– دوادي نعيمة، الجرائم الالكترونية ،خصائصها ومجالات إستخدامها وأهم سبل مكافحتها، مجلة محد اللغات ،المجلد 2 ،العدد 1 ، جامعة علي لونيسي، البليدة ،الجزائر،2020.

– سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية ،المجلد 30،العدد3،جامعة الاخوة منتوري قسنطينة1 ،الجزائر 2019.

– 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 02، ديسمبر 2017 ،المركز الجامعي إليزي، الجزائر.

– علي حسن الطوالبه ، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي: دراسة مقارنة، مجلة جامعة العلوم التطبيقية–البحرين، ، مركز الإعلام الأمني، 2009.

6/ مداخلات:

- عبد الكريم الشامي، جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني ، ورقة عمل مقدمة للأمانة العامة لمجلس وزراء الداخلية العرب ،سبتمبر 2004.

- خلف فاروق، الجريمة المعلوماتية بين الوقاية و المكافحة ، مداخلة بعنوان"الاليات القانونية لمكافحة الجريمة المعلوماتية"، كلية الحقوق و العلوم السياسية، جامعو محمد خيضر ،بسكرة.

7/ المواقع الإليكترونية:

- https://www.aljazeera.net.
- www.arablawinfo.com.

الفهرس

قائمة المحتويات

الفهرس	الصفحة
مقدمة	6 -1
الفصل الأول: مفهوم الجرائم الإلكترونية وإجراءات الوقاية منها	7
المبحث الأول: مفهوم الجرائم الإلكترونية	9
المطلب الأول: تعريف وأنواع الجرائم الإلكترونية	9
الفرع الأول: تعريف الجرائم الإلكترونية وخصائصها .	16 - 9
الفرع الثاني: أنواع الجرائم الإلكترونية .	18 - 16
المطلب الثاني: تعريف القانوني للجرائم الإلكترونية في التشريع الجزائري	20 - 18
المبحث الثاني: إجراءات الوقاية من الجرائم الإلكترونية.	20
المطلب الاول: تقنين وإستعمال وسائل الرقابة القبلية (التفتيش والحجز)	20
الفرع الأول: التفتيش.	22 - 21
الفرع الثاني: الحجز.	23 – 22
المطلب الثاني: دور الهيئة الوطنية والتعاون الدولي للوقاية منها.	23
الفرع الأول: دور الهيئة الوطنية.	29 - 24
الفرع الثاني: التعاون الدولي.	36 - 29
الفصل الثاني: إجراءات المتابعة في الجرائم الإلكترونية.	38
المبحث الأول: إجراءات وأجهزة التحقيق والتحري .	40
المطلب الأول: أجهزة التحقيق والتحري .	40
الفرع الأول: تشكيل الضبطية الفضائية.	41 - 40
الفرع الثاني: قواعد الإختصاص.	42 – 41
المطلب الثاني: إجراءات التحقيق والتحري.	42
الفرع الأول: مبادئ كتابة التحقيق والمبادئ الأساسية للتحقيق في الجرائم الإلكترونية.	52 - 42
الفرع الثاني: المحقق الجنائي في الجرائم الإلكترونية.	61 - 52
الفرع الثالث: إجراءات التي يباشرها قاضي التحقيق في الجريمة الإلكترونية.	68 - 61
المبحث الثاني: مرحلة المحاكمة.	68
المطلب الأول: إختصاص المحكمة (المحلي و النوعي) للجرائم الإلكترونية.	68
الفرع الأول: هيكلة الأقطاب الجزائية المتخصصة.	70 - 69
الفرع الثاني: اختصاص الأقطاب الجزائية المتخصصة.	71 – 70
المطلب الثاني: إجراءات المحاكمة والقواعد العامة لها.	71
الفرع الأول: اتصال القطب الجزائي بالقضايا.	73 – 71
الفرع الثاني: إجراءات المطالبة والتخلي عن القضية لصالح القطب الجزائي.	74 - 73
خاتمة.	79 - 76
قائمة المصادر المراجع.	84 - 80
الفهرس	85