وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم:القانون العام

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجريمة الإلكترونية في التشريع الجزائري

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق

التخصص: القانون الجنائي والعلوم الجنائية

من إعداد الطالب(ة):

مرابطن حياة

تحت إشراف الأستاذ(ة):

د/ يوسفـي محمد

أعضاء لجنة المناقشة

الأستاذ(ة)	درعي العربي	رئيسا
الأستاذ(ة)	يوسفي محمد	مشرفا مقررا
الأستاذ(ة)	بن عبو عفيف	مناقشا

السنة الجامعية: 2019/2018

نوقشت يوم:**2019/07/03**

شكر و عرفان

{ وَقَالُوا الْحَمْدُ لِلَّهِ الَّذِي هَدَانَا لِهَٰذَا وَمَا كُنَّا لِنَهْتَدِيَ لَوْلَا أَنْ هَدَانَا اللَّهُ }

(الأعراف/43)

بعد الحمد لله والثناء عليه وشكره على توفيقه لي في كتابة هذه المذكرة، والصلاة والسلام على سيدنا محمد وعلىآلهوصحبه أجمعين.

يسعدني أن أعرب عن عظيم امتناني وشكري لوالدي العزيزين على عنايتهما في نشأتي وتربيتي وعلى صبرهما وتشجيعهما لي على طلب العلم والمعرفة.

كما أتقدم بوافر الشكر وعظيم الامتنان إلى أستاذي الفاضل"**يوسفي محمد**"الذي تكرم بالإشراف على هذا البحث المتواضع، وما أسده إلي من إرشادات قيمة وتوجيهات نيرة كان لها الدور الواضح في إنجاز هذا البحث وتقويمه.

كما أود أن أتقدم بوافر الشكر إلى رئيس اللجنة واللجنة المناقشة إلى ما سيقدموه لي من ملاحظات دقيقة ونصائح قيمة.

والشكر موصول إلى الأساتذة الأفاضل في كلية الحقوق والعلوم السياسية– من درسني ومن لم يدرسني على حرصهم على تعليمنا العلم النافع.

فجزى الله الجميع خير الجزاء، والله ولي التوفيق

الإهـــداء

نحمد الله تعالى الذي قدرنا على شرب جرعة ماء من هذا العلم الواسع، فالعلم لا يتم إلا بالعمل وإن العلم كالشجرة والعمل به كالشجرة.

فأهدي ثمرة جهدي التي طالما تمنيت إهدائها وتقديمها في أحلى طبق:

إلى التي حملتني وهنا على وهن،وقاست وتألمت لألمي،إلى من رعتني بعطفها وحنانها وسمعت طربال ليل من أجلي إلى "أمي الحبيبة".

إلى الذي عمل وكد وجد حتى وصلت إلى هدفي هذا، إلى المصباح الذي لايبخل إمدادي بالنور، إلى الذي علمني بسلوكه خصالا أعتز بها في حياتي" أبي الغالي".

إلى أخواتي سر فرحتي وسعادتي.

إلى زوجي العزيز

إلى جميع الزملاء والأصدقاء

إلى كل من ذكرهم قلبي ونسيهم قلمي.

إلى كل هؤلاء أهدي ثمرة جهدي.

يشهد عالمنا اليوم ازدهارا في المجال العلمي، والتكنولوجي ويعود الفضل فيها للثورة المعلوماتية التي حققت قفزة ملحوظة في مستويات التقدم التقني والعلمي بحيث شملت معظم نواحي الحياة،لاسيما وأنها أصبحت سلعة تباع وتشترى بين الدول،والسعي للتنافس على امتلاكها باعتبارها مصدر قوة اقتصادية،سياسية وعسكرية.

فالعصر الحديث جعلها ضرورة من ضروريات التقدم الإنساني والمحرك الأساسي لها في مختلف مجالات الحياة، لأن هذا التقدم واكبه من جهة أخرى تطور الفكر والعقل البشري الإجرامي،لأن استخدامه لا يقتصر بين جانب الخير وجانب الشر في هذه الثورة ،وإنما يقتصر على الإنسان الشرير الذي قد يوصف كمجرم لسعيه وراء أطماعه لتحقيق أغراضه المشروعة منها والغير مشروعة لاسيما وأن هذه الظاهرة الإجرامية المتزايدة قد دقت ناقوس الخطر عن حجم المخاطر والخسائر التي يمكن أن تخلقها خاصة وأنها جرائم ذكية تنشأ وتحدث في بيئة خاصة ألا وهي الإلكترونية الرقمية و مرتكبوها أشخاص متميزون وأذكياء ذوي الخبرة.

هذه الظاهرة الإجرامية ظاهرة تقنية تنشأ في الخفاء فأصبحت حكرا على الدول المتقدمة وتعددت إلى غير ذلك (الدول النامية) مما زاد من أهمية هذه التكنولوجيا و التي عرفت بعصر المعلومات،وهذا ما دفع بالدول للعمل على الحد منها والوقاية،من خلال قيام بمجلات نوعية وخلق وسائل شتى لمحاربتها بحيث أصبح تهديدها المباشر واضحا لهذا تكاثفت الجهود الدولية كالمنظومة الحقوقية لمواجهة الآثار الناجمة عن هذه الظاهرة و المترتبة على إساءة استخدام تقنية الاتصالات و المعلومات،ووضع سياسات جنائية تتنوع بين الوقاية والمواجهة من خلال سن مجموعة القوانين من أجل وضع حد لها.

فالجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان سلبي أو إيجابي فهي أيضا معنية بالمكافحة فكان لا بد من إيجاد

إطار قانوني مناسب لسد الفراغ الإجرائي ،لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية عن طريق تعديل قانون الإجراءات الجزائية لتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة،ومنها الجريمة الإلكترونية،ومنها الإجراءات التي تطبق على الجريمة الإلكترونية فقط.

هذه الأخيرة قد أحدثت انقلابا هاما في النظريات التقليدية بما فيه نظرية الإثبات الجنائي وتحديد ما إذا كانت النصوص الجنائية التقليدية نواجه الأفعال الغير مشروعة التي ترتكب عبر شبكة الانترنت.

من منطلق هذا نجد أن أهم خاصية تتميز بها الجريمة الإلكترونية أنها لا تترك أي أثر خارجي لأنها لا تحتاج إلى أي عنف و إنما هي أرقام وبيانات تتغير أو تمحى تماما من السجلات المخزونة في ذاكرة الحاسبات الآلية التي يصعب إثباتها وذلك باتفاق الفقهاء ولدارسين في مجال المعلوماتية هو عدم تناسب النصوص المنظمة لطرق الإثبات التقليدية مع طبيعة الجريمة الإلكترونية وتطورها بسبب سرعة إخفائها وطمس معالمها في زمن قياسي ومن أي مكان في العالم،ما استلزم على المشرعين تبني أنواع جديدة من الأدلة تسمى بالأدلة الرقمية مع حرصهم على توفير الغطاء التشريعي لها.

تباينت واختلفت الرؤى من التشريعات وأراء واختلافات في دراسة الفقهاء لهذه الظاهرة (الجريمةالإلكترونية) فهناك جانب من هؤلاء الفقهاء من اعتبرها امتداد للجرائم التقليدية ،فالجريمة في نظرهم مواكبة لتطور الإنسان في مختلف مناحي الحياة وبالتالي أي ظاهرة إجرامية مستهدفة تعتبر امتداد لهذا التطور ،وجانب أخر اعتبرها جريمة مستقلة بذاتها وذلك بانفرادها بمجموعة من الخصائص والسمات بالإضافة إلى أن المجرم الذي يقوم بهذه الجرائم تختلف عن نظيره في الجرائم التقليدية،وبالتالي تعتبر الجريمة الإلكترونية في نظر أصحاب

هذا الرأي أنها جرائم لا علاقة لها بالعالم التقليدي بل هي جرائم ترتكب في عالم مختلف ألا وهو العالم الافتراضي.

تكمن أهمية البحث أساسا في كون الجريمة الإلكترونية جريمة يمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال والتي تستخدم في جميع مجالات الحياة سواء من طرف الأفراد أو المؤسسات ،واتخاذ تدابير اللازمة لحماية المجتمع من هذه الجريمة ومكافحة المجرمين وهذا الصنف من الأشخاص (المجرم)

ولقد وقع اختيارنا لهذا الموضوع بناءا علي أسباب ذاتية وأخرى موضوعية تمثلت في كون الموضوع حيوي وجديد بالإضافة إلىوجود رغبة شخصية في دراسة جانب من جوانب الجرائم المستحدثة و إثراء المكتبة الجزائرية بمراجع في هذا الموضوع.

وعليه سنحاول من خلال هذه الدراسة أن نبين أبرز النقاط المهمة المتعلقة بهذه الجريمة الحديثة وذلك من خلال طرح الإشكال التالي:

مـــــا مفهوم الجريمة الإلكترونية؟

وما هي السبل القانونية الكفيلة للحد من الجريمة الإلكترونية وفقا للتشريع الجزائري ؟

واعتمدنا في دراستنا هذه على المنهج التحليلي كونه الأنسب لمثل هذه الدراسات من خلال تحليل مختلف المواد القانونية التي تتضمن إجراءات المتابعة في الجريمة الإلكترونية على وجه الخصوص

وللإجابة على الإشكال المطروح اتبعنا المنهجية التالية ،حيث قسمنا البحث إلى فصلين، الفصل الأول تناول الإطار العام للجريمة الإلكترونية من خلال التطرق إلى ماهية الجريمة الإلكترونية في المبحث الأول، والمجرم الإلكتروني في المبحث الثاني ليصل بنا الحديث إلى توضيح هذه الجريمة بين المتابعة وأساليب المكافحة في الفصل الثاني.بحيث

تطرقنا في المبحث الأول إلي إجراءات متابعة الجريمة الإلكترونية ،أما المبحث الثاني إلي التدابير التشريعية و الأفاق المستقبلية لمكافحة الجريمة الإلكترونية

أحاط بالجريمة الالكترونية،شأنها في ذلك شأن كل ظاهرة جديدة كثير من التساؤلات التي تتعلق بتحديد مفهومها وخصائصها والتمييز بينها وبين ما يقترب منها من ظواهر وبتحديد حجم هذه الظاهرة ومعرفة العوامل المختلفة التي تتدخل في هذا التحديد والحقيقة إن تحديد مفهوم الجريمة الإلكترونية وتحديد حجمها هو خطوة أولى للتعرف على هذه الظاهرة من جمع جوانبها القانونية.

وعليه،سوف نحاول من خلال هذا الفصل إلقاء الضوء على تعريف الجريمة الإلكترونية وكذا خصائصها وبواعث ارتكابها وذلك في المبحث الأول،سنتطرق في المبحث الثاني إلى تدخل المجرم الإلكتروني المباشر في ارتكاب الجريمة الإلكترونية لنصل أخيرا إلى نظريات وأسس تصنيف الجريمة.

المبحث الأول: مـــــــاهية الجريمة الإلكترونية

تتعدد تعريفات الجريمة الالكترونية و تباينت فيما بينها ضيقا واتساعا وقد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة الجريمة الالكترونية وما يتبع ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها، لذلك سنحاول من خلال هذا المبحث دراسة ماهيتها من خلال تحديد مفهومها وصورها وما يترتب عنها من خطورة و هذا ما نتناوله[1]إتباعا.

[1]- محمود أحمد قرعان، **الجرائم الالكترونية**، ،دار وائل للنشر والتوزيع،الأردن، ط1، 2017،ص41.

المطلب الأول: مفهوم الجريمة الالكترونية و خصائصها

النظام الالكتروني لهذه التقنية يكون محلا للجريمة تارة،ويكون وسيلة لارتكابها تارة أخرى،فكلما كان البحث منصبا على الجرائم التي ترتكب ضد النظام الالكتروني كلما انطبق التعريف على محل الالكترونية بأنها [1]الجريمة المرتكبة ،وأن الفعل أن الحدث يشكل اعتداءا على النظام ألمعلوماتي.

الفرع الأول: مفهوم الجريمة الإلكترونية

أولا: تعريف الجريمة الإلكترونية

تتجه غالبية التشريعات الحديثة إلى عدم النص على تعريف عام للجريمة الالكترونية بحيث لا يوجد تعريف عام في القانون للجريمة،فالجرائم الالكترونية أو ما يسميها البعض بالجرائم المعلوماتية بذل الفقهاء جهودا حثيثة في محاولتهم لوضع تعريف جامع مانع لها ولكن لم يستقر ذلك إلى النتيجة المطلوبة و سوف نتناول بعض التعريفات التي وضعها الفقهاء لتعريف الجريمة الالكترونية كالأتي :

" بما أن هذه الجريمة مستحدثة فإنه قد تباينت التعاريف حولها ، فقد ذهب البعض في تعريف الجريمة الالكترونية أنها نشاط إجرامي يستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف تنفذ الفعل الإجرامي المقصود .

[1] –مرجع نفسه،ص42

وفي حين عرفها البعض الأخر بأنها فعل غير مشروع صادر عن الإرادة الآثمة يقرر لها القانون عقوبة أو تدبيرا احترازيا ، و نعتمد هذه الفئة (الجرائم الناشئة) عند الاستخدام الغير المشروع لشبكة الانترنت على المعلومة بشكل رئيسي

وقد تعرضت هذه التعاريف للانتقاد بسبب عدم شمولية تعريف الجريمة الالكترونية للفعل أو العمل الأساسي المكون لها.[1]

وعرفها البعض أيضا :

الفقيه الفرنسي Masse بأن جريمة الكمبيوتر يستخدم اصطلاح الغش ألمعلوماتي بأنها الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح ، و جرائم الكمبيوتر لدى الفقيه جرائم ضد الأموال .

وعرفها الفقيه الألماني تديمان Tièdement بأنها:" كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي".[2]

والفقيه David Thompson قال أن جريمة الحاسب الآلي جريمة يتطلب لاقترافها أن يتوافر لدي فاعلها معرفته بتقنية الحاسب بحيث ارتكز هذا الفقيه في تعريفه علي توافر المعرفة بتقنية المعلومات

[1] – خالد داودي، **الجريمة المعلوماتية**، دار الإعصار العلمي، ط1،2018،ص20.

[2] – غانم مرضي ألشمري، **الجرائم المعلوماتية،ماهيتها – خصائصها – كيفية التصدي لها قانونا**، دار العلمية الدولية للنشر والتوزيع،عمان، ط1،2016 ،ص25.

كما عرفها مكتب تقيم التقنية في الولايات المتحدة الأمريكية،من خلال تعريف جريمة الحاسب الآليcomputercrimeأنها:"الجرائم التي تلعب فيها البيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا"، وارتكز كذالك في تعريفه علي الوسيلة المرتكبة بها الجريمة

وعرفها خبراء المنظمة الأوروبية للتعاون و التنمية الاقتصادية ،بأنها كل سلوك غير مشروع و مناف للأخلاق أو غير مصرح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها .

كما عرفها خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD بأنها:" كل فعل أو امتناع من شأنه الاعتداء على الأمواج المادية أو المعنوية ،يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[1]

من خلال هذه التعاريف السابقة فقد تبنى الفقه الجزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي و شبكاته إذ عرف الجريمة الالكترونية بأنها :" جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ، أو

[1] – غانم مرضي ألشمري،المرجع نفسه،ص25.

داخل نظام حاسوب وتمثل في ناحية المبدئية ، جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية .[1]

فتعريف الجريمة عموما في نطاق القانون الجنائي أنه:" فعل غير مشروع صادر عن الإرادة الجنائية يقرر له القانون عقوبة أو تدابير احترازية تقوم على أساسين : عناصر الجريمة والسلوك ووصفه،والنص القانوني على تجريم السلوك و إيقاع العقوبة.[2]

ثـــــانيا: الطبيعة القانونية الخاصة للجريمة الإلكترونية

إن هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الالكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات و لغرض الحصول على معلومات معينة أو معالجة النصوص ، فهذه العمليات كلها و ثيقة الصلة بالجرائم محل البحث و عليه لا بد للجاني من فهمها فضلا عن أن الجاني قد يتعامل مع مفردات جديدة كالبرامج و المعطيات التي تشكل محل الاعتداء أو تستخدم وسيلة له .

وتكمن الطبيعة الخاصة لهذه الجرائم في فترة شبكة المعلومات على نقل و تبادل معلومات ذات طابع شخصي و عام في أن واحد مما يؤدي إلى اعتداء على الخصوصية

[1]– زبيخة زيدان،**الجريمة المعلوماتية في التشريع الجزائري و الدولي** ،دار الهدى ،الجزائر، دط، 2011 ،ص42.

[2]– محمد أحمد قرعان،المرجع السابق،ص47.

والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة أفراد و سعيهم إلى ربط حواسيبهم بالشبكة .

وبالتالي هذه الطبيعة الخاصة للأفعال المجرمة هل تدخل ضمن أحكام الخدمات البريدية أم التخابر الخاص أم يكون الهدف الأساسي للتحري عن نظام القانوني المناسب لطبيعة الجرائم الإلكترونية هو معرفة النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر الواقع و المعلومات فيها؟ ومن هذه النظام القانوني تتحدد المسئولية التي يف–ترض تطبيقها على الأشخاص المسئولين عند هذا النشر،ومن خلال المجال التي ترتكب فيه الجريمة الالكترونية و محل الاعتداء عليها تظهر لنا الطبيعة القانونية الخاصة للجريمة .

فالتكييف القانوني لهذه الجرائم تتخذ طبيعة خاصة إذا لم تكن القواعد التقليدية المخصصة لهذه الظواهر الإجرامية المستحدثة [1]، فتطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الإثبات و صعوبة إيجاد دليل مادي يدين مرتكب الجريمة لأنه من السهل محو أدلة الإدانة في وقت قصير لا يتجاوز لحظات وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال قد تكون البيانات التي يجري البحث عنها مشفرة و لا يعرف شفرة الدخول إلى أحد العاملين على الشبكة و من هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة.

[1] - بعرة سعيدة، **الجريمة الإلكترونية في التشريع الجزائري**،مذكرة مكملة من مقتضياتنيل شهادة الماستر في الحقوق،جامعة محمد حيضر،بسكرة،دفعة 2016/2015 ص 35.36

ومن صعوبة ملاحقة مرتكبي الجرائم المعلوماتية الذين يقيمون في دولة أخرى دون أن ترتبط هذه الدولة باتفاقية مع الدولة التي تحقق فيها السلوك الإجرامي أو جزء منه و في ضوء الاعتبارات السابقة يمكن القول أن هذه الجرائم تتمتع بطبيعة قانونية خاصة.[1]

ثـــــــالثا: أركان الجريمة الالكترونية

تتمثل أركان الجريمة الالكترونية مثل الجريمة العادية في الركن الشرعي والمادي والمعنوي .

1 الركن الشرعي للجريمة الالكترونية :

إن الجريمة هي نتيجة أفعال مادية صادرة عن إنسان هذه أفعال تختلف حسب نشاطات إنسان وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو للجرم و العقوبة المقررة لارتكابه.[2]

فالقاعدة الأساسية الناتجة عن مبدأ الشرعية ،هي عدم رجعية القانون الجنائي بمعنى لا يمكن معاقبة شخص ارتكب فعلا لم يجرمه القانون و هذا ما نصت عليه المادة01 من قانون العقوبات " لا جريمة ولا عقوبة أو تدبير أمن بغير نص قانوني"[3]،ويتميز هذا المبدأ أن القاضي الجنائي عنده تفسيره لنصوص القانونية تفسيرها

[1] –بعرة سعيدة، مرجع نفسه، ص37

[2] – أحسن بوسقيعة، **الوجيز في القانون الجزائي** العام، ،دار هومه،الجزائر،ط10 ،2011،ص27.

[3] – المادة الأولى من قانون العقوبات الجزائري.

ضيقا ،بالإضافة إلى منع اللجوء إلى القياس بمعنى عدم لجوء القاضي الجنائي إلى قياس فعل لم يرد نص بتجريمه على فعل ورد نص بتجريمه فيقرر القاضي الجنائي الأول عقوبة و الثاني لتشابه بين الفعلين.

2 الركن المادي للجريمة الإلكترونية :

إن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية ،واتصال بالانترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته فيقوم بتحميل الحاسب ببرامج اختراق،أو أن يقوم بإعداد هذه البرامج بنفسه وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة،وتحميلها على الجهاز المضيف ، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.

فالركن المادي للجريمة الالكترونية يتكون من السلوك الإجرامي والنتيجة والعلاقة السببية علما انه يمكن تحقق الركن المادي دون تحقق النتيجة كالتبليغ عن الجريمة قبل تحقيق نتيجتها ،مثلا :(إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع علي الشبكة إلا انه لا مناص من معاقبة الفاعل).[1]

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل ايجابي مرتكب مثلا: (جريمة الغش ألمعلوماتي الركن المادي فيها هو تغير الحقيقة في التسجيلات الالكترونية أو المحررات الالكترونية).

[1] - أحسن بوسقيعة،مرجع سابق،ص28

3 الركن المعنوي للجريمة الإلكترونية:

يتضح الركن المعنوي للجريمة الإلكترونية من خلال توضيح الحالة النفسية للجاني و العلاقة التي تربط بين ماديات لجريمة وشخصية الجاني،فهذا المبدأ يقوم على صورتين أساسيتين الصورة الأولى متمثلة في الاعتداء على نظام المعالجة الألية وهذه الأخيرة تحتوي على نوعين من الاعتداءات،النوع الأول وهو الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال وهي فعل الإدخال والمحو والتعديل،أما الصورة الثانية متمثلة في الاعتداء على منتجات الإعلام الآلي و تحتوي هذه الصورة على فعل التزوير ألمعلوماتي.[1]

الفرع الثاني: مميزات الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بصفة عامة عن الجريمة التقليدية في عدة نواح ، سواء كان هذا التميز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى أثار هذه الجريمة حدود الدولة الواحدة .

[1] – أحمد خليفة ،**الجرائم المعلوماتية**،،دار الفكر الجامعي،الاسكندرية،ط2،2006،ص78.

أولا: خصوصية الجريمة الإلكترونية

تتسم الجريمة المعلوماتية بصعوبة اكتشافها و إثباتها و يرجع ذلك إلى عدة أسباب من بينها:

- وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام من فقد ثقة عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.
- في مقابل انخفاض نسبة جرائم الإلكترونية في مواجهة الجرائم التقليدية ترتفع الخسارة لناتجة عن الجرائم لمعلوماتية بصورة كبيرة بالمقارنة بغيرها من الجرائم ، فعلى سبيل المثال في الولايات المتحدة الأمريكية توصل مكتب التحقيقات الفيدرالية FBI على أن متوسط الخسائر التي تحققها الجريمة المعلوماتية يبلغ حوالي 500.000 دولار في حين لا تزيد الخسائر التي تخلفها جرائم السرقة العادية عن 3500 دولار.[1]
- في المقابل فإنه وعلى غرار الآراء التي تتجه إلى القول بأن الجريمة الالكترونية لا يوجد شعور حقيقي بعدم الأمان في مواجهتها أو أنه لا يوجد شعور عام بعدم

[1]- خالد داودي،المرجع السابق،ص27

أخلاقية هذه الأفعال،فإننا لانتفق مع هذه الآراء،إذن الجريمة الالكترونية لا تختلف عن غيرها من الجرائم من حيث اعتداءاتها على المصالح .[1]

ثـــــــانيا: الطبيعة المتعدية الحدود (الدولية) للجريمة الإلكترونية

يمكن القول أن من أهم خصائص التي تميز الجريمة الإلكترونية هي تخطيها للحدود الجغرافية ومن اكتسابها طبيعة دولية،فالقدرة التي تتمتع بها الحاسبات الآلية في نقل ;تبادل كميات كبيرة من لمعلومات بين أنظمة يفصل بينها ألاف الأميال.

ولقد أثارت الطبيعة الدولية للجرائم الإلكترونية تساؤلات مهمة تتعلق بتحديد الدولة التي يختص قضائها بملاحقة الجريمة،فهل هي الدولة التي وقع بها النشاط الإجرامي أو تلك التي توجد بها المعلومات محل الجريمة ، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب،كما أثارت هذه لطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة لذلك بات من الضروري إيجاد وسائل مناسبة لتشجيع التعاون الدولي .

ونجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثير من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم،وإن كان مشرعنا قد خطى خطوة إلى الأمام في هذا المجال بصدور قانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات والذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في

[1] –خالد داودي،المرجع السابق،ص28.

المواد،من المادة 394 مكرر إلى غاية 394 مكرر 7 الخاص بالمساس بالأنظمة المعالجة لآلية المعطيات .[1]

المطلب الثاني: أنواع و دوافع ارتكاب الجريمة الإلكترونية

الفرع الأول: صور الجرائم الإلكترونية

الجريمة باعتبارها إحدى صور إفرازات المجتمع يصلها ما يصل المجتمع من تطور ومرجع ذلك أن مرتكب الجريمة وضحيتها عضوان في المجتمع ويتأثران بحياته وثقافته وتطوره فأقصى ما يصل إليه المجرم من براعة و دراية نتيجة لهذه الثقافة والتعليم يحاول استخدامها في جريمته ، فالجريمة محصلة كل ذلك.

قد يستخدم الانترنت كوسيلة لارتكاب الجرائم التقليدية وهي نوعان أحدهما له طابع سياسي والأخر له طابع جنائي بحث و ذلك على النحو التالي:

أولا : قيادة الجماعات إرهابية عن بعد:

حيث يمكن من خلال شبكة الانترنت بث الأفكار المتطرفة سواء كانت سياسية أو دينية عنصرية التي تسيطر على وجدان الأفراد وتفسد عقائدهم واستغلال معاناتهم في تحقيق مأرب خاصة تتعارض مع مصالحة المجتمع.

[1]– خالد داودي، مرجع سابق ، ص 29.

ثـــــــانيا: تنسيق جهود عصابات الجريمة المنظمة

فقد كشفت باحثة بريطانية عن استغلال شبكة إنترنت في تجارة الرقيق الأبيض من خلال عقد صفقات لبيع فتيات،إذ يتم إرسال كتالوجات تتضمن مواصفات دقيقة عن فتيات مراهقات من أروبا شرقية وغيرها،وثمن المحدد للشراء كل فتاة وكيفية اتصال بالوسيط لإتمام الصفقة.

ثـــــــالثا: تهديد الأمن القومي و العسكري [1]

فقد وقعت في الأونة الأخيرة عدة حوادث تبين مدى امكانية تعرض المراكز العسكرية لحوادث القرصنة المعلوماتية بغية الحصول على معلومات مخزنة في ذاكرة الحاسبات الألية المستعملة فيها .

رابعا: السطو على أموال البنوك

إن السطو على أموال البنوك هو الهدف المفضل لقراصنة أنترنت الذين يتلاعبون في كشوف وحسابات العملاء ونقل الأرصدة من حساب لأخر،ونظرا لخطورة جريمة السطو والتي تعد بصدق أخطر من الجريمتين المجتمعتين أقر لها المشرع الأمريكي كجريمة جديدة مستقلة وشدد العقوبة عليها.

[1] - أحمد عبداللاه المراغي،**الجريمة الالكترونية و دور القانون الجنائي في الحد منها – دراسة تحليلية تأصيلية مقارنة–** ،د ب ن،ط1،2017،ص45 وما بعدها

خـــــــامسا: أسلوب التجسس

يقوم قراصنة الحاسب الآلي باستخدام البرامج التي تنتج لهم الاطلاع على البيانات ومعلومات الخاصة بالشركات والمؤسسات العاملة على شبكة انترنت وبالتالي يتمكنوا من الحصول على ما يردوا من معلومات مختلفة

ســـــادسا: غسيل الأموال القذرة

تعتبر جرائم غسيل أموال من هم وأخطر الجرائم اقتصادية ومالية النقدية وأخلاقية التي بدأت تتغلغل في اقتصاديات بعض الدول بأساليب حديثة،وإخفاء أنشطتها والمرور بها في غفلة من رجال الأمن والاقتصاد والقانون،وهو ما أدى في نهاية إلى سهولة إتمام عملية غسل الأموال.

ســـــــابعا: التهديد بالقتل

فقد أدانت إحدى المحاكم بفرنسا أحد الجناة بالحبس لمدة شهرين مع الإيقاف لأنه عبث برسالة تهديد بالقتل عن طريق البريد الإلكتروني إلى أحد رجال السياسة .[1]

ثـــــــامنا: القتل العمد

[1] – عبد الله معيظ العبيدي،**الحماية الجنائية للتعاملات الالكترونية في نظام المملكة العربية السعودية**– دراسة تحليلية مقارنة،رسالة ماجيستير،كلية الدراسات العليا،جامعة نايف للعلوم العربية للعلوم الأمنية،الرياض،2009،ص52.

مثال ذلك حالة الرجل الذي قتل زوجته بحيث دخل عن طريق الانترنت إلى شبكة المعلومات الخاصة بالمستشفى ثم قام بتغيير المعلومات الطبية الخاصة بالمجني عليه

تـــــــاسعا: نشر المطبوعات المخلة بالآداب العامة

انترنت إحدى وسائل الاتصال التي تسهل ارتكاب الجرائم ذات الصبغة الجنسية كما تنتج شبكة انترنت لمستخدميها مكنة تتخطي القيود المحلية المفروضة [1] عليهم وبالتالي يمكنهم الاطلاع على المواد التي فرضت الرقابة شروطا معينة بالنسبة للحد الأدنى للسن المسموح له بالاطلاع عليها،كالأفلام والصور المخنوقة من مطبوعات ...الخ

الفرع الثاني: بواعث ارتكاب الجريمة الالكترونية

للجريمة الالكترونية عدة دوافع على ارتكابها فبعضها يرجع إلى دافع شخصي ومنها ما يرجع إلى دافع خارجي ومنها ما يكون خاصا بالمنشأة،وكل هذه الدوافع قد تكون مصدرها هو الرغبة الإجرامية .

أولا: الدوافع الشخصية

1 **الدوافع المادية**:يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل وهو من بين أكثر الدوافع تحريكا للجناة اقتراف الجرائم المالية،فإن الدراسات

[1]- عمرو موسى الفقيهي،**الجرائم المعلوماتية – جرائم الحاسب الآلي و الانترنت في مصر و الدول العربية**،مكتب الجامعي الحديث،الاسكندرية،2006،ص102.

أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر وفيما بعد احتيال انترنت هو تحقيق الكب المالي ففي دراسة الفقيه Parker باركر[1] الصادرة في إحدى مجلات المتخصصة تبين أن :

34% من جرائم الغش المعلوماتي (اختلاس أموال)

23 % من أجل سرقة لمعلومات

19%من أجل الإتلاف

15%من أجل سرقة وقت الحاسوب بالأغراض شخصية

أما الدراسات الحديثة فسنجد هذا الدافع يسود على غيره و يعكس استمراره اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية.

2– الدوافع الذهنية أو النمطية:

غالبا مايكون الدافع لدى مرتكب الجرائم المعلوماتية هو الرغبة في إتلاف الذات دون أن يكون له نوايا آثمة ويرجع ذلك إلى وجود عجز في التقنية التي تترك القرصنة لمشيدي برامج النظام المعلوماتي لارتكاب الجرائم وعليه فإنه يرى البعض أن الدافع إلى ارتكاب الجرائم المعلوماتية يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح،إلا أنه في حقيقة الأمر تحقيق الربح دافعا أكثر تحريكا لجرائم الحاسوب من الرغبة في قهر النظام .

[1]– **باركر**: هو فقيه وباحث اهتم بالجريمة المعلوماتية بشكل عام والمجرم المعلوماتي بشكل خاص:

ثـــــانيا : الدوافع الخارجية :

1– دافع الانتقام و إلحاق الضرر برب العمل :

قد يكون انتقام مؤثرا في ارتكاب الجرائم ومثال ذلك قيام محاسب شاب يتلاعب بالبرامج المعلوماتية بإحدى المنشآت بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات وديون المنشأة باعثها الانتقام من المنشأة أو أرباب العمل.

وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيسي والغالب لفئة التي تحمل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة.

2–الرغبة في قهر النظام و التفوق على تعقيد وسائل التقنية:

يمثل مرتكبو هذه الجرائم إلى إظهار تفوقهم و مستوى ارتقاء براعتهم لدرجة إنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة،بحيث يتزايد شيوع هذا الدافع لدى فئة صغار السن،و إن هذا الدافع هو أثر الدوافع التي يجري استغلالها قبل المنظمات الجرمية لأجل استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة.[1]

[1]–خالد داودي ، مرجع سابق ، ص37 وما بعدها.

المبحث الثاني: المجرم الإلكتروني

لم يكن لارتباط الجريمة الالكترونية بالحاسب الآلي أثره على تميز الجريمة الالكترونية عن غيرها من الجرائم التقليدية فحسب وإنما كان له أثره في تمييز المجرم المعلوماتي عن غيره من المجرمين العاديين الذين جنحوا إلى سلوك الإجرامي النمطي،وهذا وما سوف نعرض له موضحين أهم سمات المجرم المعلوماتي ثم تصنيفات المجرم المعلوماتي على النحو التالي:

المطلب الأول: مفهوم المجرم الإلكتروني و صفاته

الفرع الأول: تعريف المجرم الالكتروني

لقد تنوعت الدراسات التي تحدد المجرم المعلوماتي وشخصيته والأفعال الإجرامية التي يقوم بها نوع مكن العقوبات التي يخضع لها ،كما يمكن أن نستخلص مجموعة من السمات التي يتميز بها المجرم الالكتروني التي يساعد التعرف عليها في مواجهة هذا النمط الجديد من المجرمين ويعد الأستاذ باركر واحد من أهم الباحثين الذين عنوا بالجريمة الالكترونية بصفة عامة والمجرم الالكتروني بصفة خاصة،[1]ويرى باركر أن

[1] - محمد الدايج ، **الجريمة الالكترونية في التشريع الجنائي الجزائري** ، مذكرة لنيل شهادة الماستر ، كلية لحقوق و العلوم السياسية ، جامعة مستغانم ، سنة2017/2016،ص33

المجرم الالكتروني و أن كان يتميز ببعض السمات الخاصة إلا أنه في النهاية لا يخرج عن كونه مرتكبا لفعل اجرامي يتطلب توقيع العقاب عليه.[1]

الفرع الثاني: الصفات الشخصية للمجرم الالكتروني

السمات المشتركة بين المجرمين التي تحدد المجرم الالكتروني وهي عديجة نذكر منها ما يلي :

1* مجرم متخصص : له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور أو الشفرات،ويسبح في عالم الشبكات ليحصل على كل غالي و ثمين من البيانات والمعلومات الموجودة على أجهزة الحواسيب ومن خلال الشبكات.

فقد تبين في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوي جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم ، دون ان يكون لهم أي نوع من الجرائم التقليدية الاخري ،مما بين ان المجرم الذي يرتكب الجريمة المعلوماتية هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

2* مجرم عائد للإجرام: يتميز المجرم المعلوماتي بأنه عائد للجريمة دائما فهو يوظف مهارته في كيفية عمل الحواسيب وكيفية تخزين البيانات و المعلومات والتحكم في الأنظمة الشبكات في الدخول غير مصرح به مرات و مرات،فهو لا

[1]– محمد الدايج ، **مرجع نفسه**، ص 34.

يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته و مهارته في الاختراق.

فقد تبين في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوي جرائم الكمبيوتر ،أي أنهم يتخصصون في هذا النوع من الجرائم ،دون أن يكون لهم أي نوع من الجرائم التقليدية الاخري ،مما تبين أن المجرم في الغالب متخصص في هذا النوع من الإجرام.

بحيث يعود الكثير من مجرمي المعلومات إلي ارتكاب جرائم أخري في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلي التعرف عليهم وتقديمهم إلي المحاكمة في المرة السابقة ويؤدي ذلك إلي العودة إلي الإجرام ،وقد ينتهي بهم الأمر كذلك في المرة التالية إلي تقديمهم إلي المحاكمة

3* مجرم محترف : له من القدرات و المهارات التقنية ما يؤهله لأن يوظف مهارته في الاختراق و السرقة و النصب و الاعتداء على حقوق الملكية الفكرية و غيرها من الجرائم مقابل المال.[1]

بحيث يتمتع في تنفيذ جرائمه إلي احترافية كبيرة ،حيث انه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر الذي يقتضي الكثير من الدقة و التخصص والاحترافية ،في

[1] - امير فرج يوسف،**الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر و الأنترنت**، ،دار الناشر مكتبة الوفاء القانونية،الإسكندرية،ط1، سنة2011م،ص53

هذا المجال للتوصل إلي التغلب علي العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية

4* مجرم ذكي:حيث يمتلك هذا المجرم من المهارات ما يؤهله أن يقوم بتعديل و تطوير في الأنظمة الأمنية ، حتى لا تستطيع أن تلاحقه و تتبع 26أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب.[1]

5*مجرم متكيف اجتماعيا:

التكيف الاجتماعي يحتوي على حقيقتين الأولى تتمثل في تكيف المجرمين المعلوماتين فيما بينهم وتعتبر هذه الخاصية امتداد لسمة التخطيط والتنظيم، مثل التكيف الاجتماعي بين مجموعة لها صفات مشتركة مثل " نوابغ صغار المعلوماتية "، ولا شك أنهم يتكيفون في أفكارهم،وهذه الروابط تتعدى النطاق المحلي إلى المجال الدولي .

أما الحقيقة الثانية، تكمن في تكيف المجرم المعلوماتي الذي لا يضع في نفسه في حالة عداء مع المجتمع الذي يحيط به، كما أن تكيف المجرم المعلوماتي مع نفسه يزيده الثقة بأنه خارج إطار الشبهات وهذا الشعور يدفعه إلى التمادي في ارتكاب جريمته[2].

المجرم المعلوماتي لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به بل أنه إنسان متكيف اجتماعيا، ذلك أنه أصلا مرتفع الذكاء ويساعده على ذلك عملية التكيف، وما الذكاء في رأي الكثيرين سوى القدرة على التكيف، ولا يعني ذلك التقليل من

[1]–امير فرج يوسف ،لمرجع نفسه ص 54.

[2]– امير فرج يوسف ،المرجع نفسه،ص55.

شأن المجرم المعلوماتي،بل أن خطورته الإجرامية قد تزيد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه .

المطلب الثاني : تصنيفات المجرم الإلكتروني

الفرع الأول: أنماط المجرم الإلكتروني

تتدرج الجرائم في مجال الحاسب الآلي من جرائم بسيطة إلى جرائم إرهابية و ذلك تبعا لشخصية المجرم الالكتروني،مما أدى إلى ظهور عدة أصناف من المجرمين يصعب حصرهم تحت طوائف محددة ،لكن هذا لا يعني عدم وجود محاولات في تحديد أصناف المجرمين وملامحهم،بل على العكس هناك عدة دراسات ونظريات حاولت وضع قواعد يصنف بها المجرمون كل على حسب خطورته الإجرامية و يمكن حصرها فيما يلي: [1]

أولا : صغار نوابغ المعلوماتية

يطلق لفظ صغار نوابغ المعلوماتية على المجموعات التي تميل للتحدي الفكري هم غالبا ما يكونون في مرحلة المراهقة وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة البنكية الشركات والمؤسسات المالية ،ويتميز هؤلاء المراهقين عن غيرهم من مرتكبي الجرائم التقليدية بأنهم لا يعتبرون أن ما يقومون به يعد جريمة لأنهم يعتقدون أن النظام غير قادر عل حماية نفسه ليس من الخطأ اقتحامه ولذلك فإنهم يعتبرون أنفسهم أبطالا لمساعدة المجتمع في تحديد نقاط الضعف الخاصة بالبرنامج الذي

[1]-اميرفرج يوسف، المرجع نفسه،ص56

تم اقتحامه ، كما يمكن لصغار النوابغ أن يتحولوا إلى فئة القراصنة بعد تطور خبراتهم و مهارتهم فيتم استئجارهم و استغلالهم .

ويثير مجرمو الحاسبات من هذه الطائفة جدلا واسعا،ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، على الأقل بمواصلتها العبث بالحاسبات،ظهرت دراسات و مؤلفات تدافع عن هذه الفئة لتخرجها من دائرة الإجرام إلى دائرة العبث وأحيانا البطولة[1].

ثـــــــانيا: القراصنة

تعرف هذه الطائفة بالمجرمين البالغين أو المخربين المهنيين تتراوح أعمارهم بين 25-45 عاما ودائما ما يكونون من المتخصصين في مجال التقنية الالكترونية،أي يتمتعون بمهارات ومعارف فنية في مجال الأنظمة الإلكترونية ، يوجد مصطلحان مترادفان لها(القراصنة) هما:

- **الهكرز** : وهو المقتحم التقليدي الذي يقوم بتلصص على الغير ويتاجر في قطاع المعلومات وإذا ما واجهته حماية لا يستطيع تخطيها فهو ليس له علاقة بتكنولوجيا المعلومات.
- **الكراكرز**: لفظ يطلق على الشخص المقتحم الخبير في مجال المعلومات يعتمد في عمله على كسر الحماية الموجودة حول الشبكات اقتحام البرامج و يستعين بالتالي

[1]-امير فرج يوسف، المرجع نفسه،ص57.

الهاكرز بالكراكرز إذا ما صادفه أي نوع من أنواع الحماية و لكن يلاحظ أنه جرت العادة على إطلاق لفظ الهاكرز على كلا نوعين الهاكرز و الكراكرز أو استخدام لفظ القراصنة عموما .[1]

ثـــــــالثا: الهواة و المبتدئون

يعتبر نمط الهواة و المبتدئين من الأنماط التي تتميز بخطورتها في ارتكاب الجرائم و تبرز خطورتها في أن المخاطر في أن المخاطر التني تحدث نتيجة تصرفاتهم قد لا يمكن تداركها ، فقد ينتج عن طريق قيام أحد الهواة و المبتدئين بالضغط على أحد الأزرار في لوحة المفاتيح فقط ملفات مهمة أو اتلاف أي من المعلومات التي قد لا يمكن استرجاعها مرة أخرى.

رابعا: المخربون

يرتكب أشخاص هذه الفئة الجرائم ليس طعما في الإشادة العقلية أو إثبات التفوق العملي مثل صغار النوابغ المعلوماتية و إنما عادة ما يكون أشخاص هذه الفئة من الغاضبين في أغلب الأحوال ممن هيئة معينة إلى المستخدمين من داخل الهيئة أي لديهم تصريح لاستخدام أنظمة الحاسب الآلي و يقومون بإتيان تصرفات غير مصرح بها تنتج عنها أفعال تخريبية،وإلى الغرباء عن الهيئة أي المستخدمون الذين ليس لهم تصريح

[1]– خالد ممدوح ابراهيم،**الجرائم المعلوماتية**، ،دار الفكر الجامعي،اسكندرية،ط1، ،2009،ص142.

بالعمل على لنظام غرضهم التخريب و في بعض الأحيان لتسلية بحيث ينتج عن هذه الأفعال نتائج تخريبية و قد يكون المكسب المادي هو هدف من عملية الدخول.

خـــامسا: المجرمون المحترفون

تعد هذه الفئة من أخطر الفئات التي ترتكب الجرائم لأن الهدف الذي تقوم عليه هذه الفئة ينحصر في نية ارتكاب الفعل الإجرامي وهذا هو مصدر الخطورة لأن المحترفين يرتكبون أنواع الجرائم المختلفة و بأساليب مختلفة لأنهم يكونون على درجة كبيرة من لمهارة و الإتقان و الغرض دائما هو المكسب أو الحصول على فائدة مادية أو معنوية و يلاحظ أن الأضرار التي ترتب على هذه الأفعال تكون بالغة الضرر هذا بعكس الفئات السابقة لأنه على الرغم من الخطورة الناجمة عن صغار نوابغ المعلوماتية إلا أن ليست دائما مؤثرة لأن أغلب الظن يكون قصدهم هو إثبات التفوق العلمي ، و ينطبق ذات الأمر على فئة المخربين فهم ليس دائما مجرمين لأنهم يعمدون إ'إلى الانتقام أو إلى تأمين المراكز الوظيفية لضمان استمرارهم.[1]

تتميز هذه الطائفة بسعة الخبرة و الكفاءة و الإدراك الواسع للمهارات التقنية ، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها،ولذلك فإن هذه الطائفة تعد الأخطر من بين مجرمي التقنية حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم و سخرتهم لارتكاب جرائم نظم المعلومات كما

[1]-خالد ممدوح ابراهيم، المرجع نفسه، ص 148.

تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي .

يتم تقسيم أفراد هذه الطائفة إلى مجموعات متعددة إما تبعا لتخصصهم بنوع معين من الجرائم أو تبعا للوسيلة المتبعة من قبلهم في ارتكاب الجرائم فمثلا نجد طائفة محترفي التجسس الصناعي و هم أولئك الذين يوجهون أنشطتهم إلى اختراق نظم المعلومات التابعة للشركات الصناعية و التجارية إما لحساب أعمال يقومون بها بذاتهم أو في الغالب لحساب منافسين آخرين في السوق و أحيانا لحساب مجموعات القرصنة الدولية [1].

فنجد مثلا طائفة مجرمي الاحتيال و التزوير، وهؤلاء هم الطائفة التي تكون أغراضها متجهة إلى تحقيق مكسب مادي والاستيلاء على أموال الآخرين وضمن هذه الطائفة أيضا، ثمة تقسيمات عديدة فمنهم محتالو شبكات الهاتف و محتالو الانترنت وغير ذلك،وحتى في الطائفة الفرعية تتوفر تخصصات لبعضهم كأن يوجه الشخص أنشطته الاحتيالية إلى قطاع المزادات البضاعة و المنتجات على الانترنت أو في ميدان الاستيلاء على أرقام بطاقات الائتمان والاتجار بها، إلى جانب المعرفة التقنية المميزة والتنظيم العالي والتخطيط للأنشطة المنوي ارتكابها [2].

[1]–خالد ممدوح ابراهيم، المرجع نفسه،ص149.

[2]– أيمن عبد الله الكافي،جرائم نظم المعلومات – دراسة مقارنة – المرجع السابق، ص110.

خلاصة الفصل:

تتحدث هذه الدراسة عن مفهوم الجريمة الإلكترونية والسبل الكفيلة لمحاربتها كونها من أخطر الجرائم المهددة لمجتمعنا اليوم فهي جريمة ترتكب بواسطة نظام حاسوبي أو شبكة حاسوبية، المتمثلة في جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية .

أما في نطاق القانون الجنائي فهي فعل غير مشروع صادر عن الإرادة الجنائية يقرر له عقوبة أو تدابير احترازية، إلا أن المشرع الجزائري ألقي اهتمامه البالغ في التنظيم والتصدي لهذه الجريمة من خلال التعديلات التي أدخلتها ببعض القوانين.

شكل الانفجار المعلوماتي الذي نشهده،والتطور المتسارع والمتلاحق لهذه التكنولوجيا تنوعا في الأنشطة الإجرامية تفرغ في جنباتها أجراس الخطر لتنبه مجتمعات العصرالراهن لحجم المخاطر وهول الخسائر الناجمة عنها،فعدم كفاية التشريعات الخاصة بها وصعوبة التكييف القانوني لها وإجراءات متابعتها من أهم الصعوبات التي تعتري بالنسبة لمكافحة هذه الجريمة .

من خلال هذا الموقف ارتأينا أن تكون نقطة الانطلاق من عنوان هذا الفصل، فنتعرض في المبحث الأول إلى إجراءات المتابعة والجزاءات المترتبة عن مواجتها لننتقل إلى التدابير التشريعية وأساليب المكافحة في المبحث الثاني

المبحث الأول :إجراءات متابعة الجريمة الإلكترونية

المطلب الأول: إجراءات متابعة الجريمة الإلكترونية

إن الجريمة الالكترونية تعتبر كأي جريمة من الجرائم المنصوص[1] عليها في قانون العقوبات والقوانين الأخرى فلذلك تتسع الجريمة الإلكترونية بدعوى عمومية وهذه الدعوة تتم بمراحل سنوضحها من خلال الفروع الآتية.

[1] زبيخة زيدان،**الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى،عين مليلة،الجزائر،دط،2012 ص116-117

الفرع لأول: مرحلة جمع الأدلة :

تعد هذه المرحلة من اختصاص ضابط الشرطة القضائية وهما نوعان ،النوع الأول هم الذين يتمتعون باختصاص عام ويختصون بإجراءات الاستدلال بشأن الجرائم المنصوص عليها في قانون العقوبات،أما النوع الثاني فهم ذوي الاختصاص النوعي المحدود بخصوص نوع معين من الجرائم التي حددها القانون على سبيل الحصر هؤلاء المشار إليهم في المادة21 من قانون الإجراءات الجزائية، وسلطتهم كذلك محددة لا تمتد إلى مرحلة التفتيش ودخول المنازل والمعامل والمباني أو الأماكن المحاطة بأساور إلا بحضور أحد ضباط الشرطة القضائية ومن بين هؤلاء رؤساء الأقسام المهندسون وأعوان الغابات وحماية الأراضي، وتعد محاصرتهم ذات حجية وقوة إثبات كما استقر عليه القضاء الوطني[1].

أولا: الإجراءات التقليدية لجمع الدليل: تنقسم بدورها لإجراءات مادية و إجراءات شخصية

1 **الإجراءات المادية** : تتمثل هذه الإجراءات في :

أ – المعـايـنة:

[1]فراح ميسور ،**الجريمة الإلكترونية**، مذكرة تخرج لنيل شهادة ماستر ،كلية الحقوق والعلوم السياسية،جامعة الإخوة منتوري،قسنطينة، 2014،ص33.

يقصد بالمعاينة فحص المكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته كمعاينة مكان ارتكاب الجريمة أو أداة ارتكابها أو محلها أو معاينة جسم أو ملابس الجاني أو المجني علية لإثبات ما بالجسم من جراح أو ما على الثياب من دماء أو ما بها من مزق أو ثقوب.

هناك تعريف آخر للمعاينة وهي بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها، كذلك جميع الأشياء الأخرى التي تفيد في كشف الحقيقة واتخاذ ما يلزم من الإجراءات.[1]

ولقد أشارت قوانين الإجراءات الجزائية إلى إجراء المعاينة باعتباره إجراء من إجراءات التي تمتلكها السلطات التحقيقية بمختلف فئاتها وطوائفها، وهذا ما ورد في نص المادة 79 من قانون الإجراءات الجزائية الجزائري " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة .....الخ "

فالهدف من المعاينة هو لغرضين أثنين يتمثل الأول في جمع الأدلة الناتجة عن الجريمة والثاني إتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة حتى تكون لديه فكرة واضحة لا لبس فيها ولا غموض عن كيفية وقوع الجريمة[2].

[1] محمد أمين الرومي، **جرائم الكمبيوتر و الأنترنت** ،الإسكندرية، دار المطبوعات الجامعية، 2003، ط1،ص 201.
[2] المرجع نفسه، ص 202.

قد تكون المعاينة إجراء تحقيق أو استدلال تستهدف إظهار الحقيقة في واقعة يبلغ أمرها إلى السلطات المختصة , بحيث لا تتوقف طبيعتها على صفة من يجريها بل على ما يقتضيه أجراؤها من مساس بحقوق الأشخاص , فإذا تم إجراء المعاينة في مكان عام كانت إجراء استدلال , أما إذا اقتضت دخول حرمة مسكن خاص كانت إجراء تحقيق.

إن انتقال المحقق الجنائي لإجراء المعاينة متروك للسلطة التقديرية له فلا يقوم به إلا إذا كانت مصلحه من ورائه , وهذا ما قضت به أحكام المواد 42 , 79 , 80 من قانون الإجراءات الجزائية الجزائري على أن المعاينة تجري إما من طرف قاضي التحقيق وذلك بعد إخطار وكيل الجمهورية الذي له الحق في مرافقته , وكما يمكن تمديد اختصاص قاضي التحقيق إذا اقتضت ضرورة الحالة إلى دوائر اختصاص محاكم المجاورة , ويمكن أن يتم إجراء المعاينة من طرف ضباط الشرطة القضائية الذين عليهم إخطار وكيل الجمهورية فور وصول خبر الجريمة إلى علمهم وانتقالهم بدون تمهل إلى أماكن الواقعة الإجرامية .[1]

وللمعاينة أهمية بارزه في مجال التحقيق الجنائي لكونها مصدراً أصيلاً من مصادر الأدلة المادية والفنية الراسخة والثابتة التي تكون دائماً محل ثقة سلطات التحقيق والقضاء

[1] خالد ممدوح ابراهيم , **الجرائم المعلوماتية** , دار الفكر الجامعي الإسكندرية , مصر , الطبعة الأولى ,2009 , ص118

ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة , وبكل ما يحتويه من تفصيلات سواء تعلقت بمكانه أو وصفه من الداخل أو الآثار الموجودة به .[3]

وباعتبار المعاينة من أهم إجراءات التحقيق الجنائي فإن أهميتها تتجسد سواء من الناحية القانونية أو الفنية، فمن الناحية القانونية تبدو أهميتها من عدة اتجاهات منها تأكيد وقوع الجريمة أو نفيها , أي صدق أقوال الواقعة وكذلك تحديد الوصف القانوني لها , كما تساعد القاضي في تكوين اقتناعه , أما من الناحية الفنية فهي تساعد المحقق على تحديد وقت ارتكاب الواقعة الإجرامية ومعرفة علاقة الجاني بالمجني عليه وتحديد الأسلوب الإجرامي الذي استعان به الجاني.[1]

ب – التفتيش: يهدف التفتيش إلى جمع الأدلة من مكان وقوع الجريمة والتفتيش لغتاً هو من مصدر فتش أي بحث وسأل وفتش الرجل عن شيء أي تصفحه. ويقصد بالتفتيش قانونا : هو البحث في مكان ما بهدف البحث عن الأشياء .

وهناك عدة تعريفات فقهية للتفتيش وقد عرفه الفقه الفرنسي بأنه " بحث بوليسي أو قضائي عن عناصر الدليل في الجريمة ما ويكون وفقاً لقواعد قانونية خاصة بحيث يمكن أن ينفذ بالمسكن الخاص بأي أو في أي مكان أخر توجد فيه أشياء يكون اكتشافها مفيداً في إظهار الحقيقة .

[1] لطروش فيروز ، بن عزوز حاتم ، **الجريمة الالكترونية** في الجزائر من جريمة فردية إلى جريمة منظمة ، جامعة عنابة ، ص324.

مما لا شك فيه أن الطبيعة التقنية الرقمية قد زادت من الصعوبات التي تواجه القائمين على التفتيش في الجرائم الإلكترونية , فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكات الحاسب الآلي في أماكن قد تكون على مسافات بعيدة عن الموقع المادي الذي يتم فيه التفتيش، كما قد يكون الموقع الفعلي للبيانات والمعلومات ضمن الاختصاص القضائي لدولة أخرى وهو ما يصعب عملية التفتيش , وسوف نميز في هذه الخطوة بين احتمالين أثنين في تفتيش الشبكات :

- **الاحتمال الأول:** أن يكون الحاسب الآلي للمشتبه فيه أو المتهم متصلاً بحاسب أخر أو منظومة معلوماتية متواجدة في موقع أخر داخل الدولة نفسها :

وتتحقق هذه الفرضية حينما يقوم المتهم بتحويل عبر الانترنت معلومات أو بيانات متعلقة بجريمة إلكترونية من حاسبه إلى حاسب أو منظومة معلوماتية مملوكه للغير متواجدة في مكان أخر وتخزينها فيها , ففي هذه الحالة تواجه سلطات التحقيق مشكلة تجاوز الاختصاص المكاني من ناحية والاعتداء على حرمة خصوصية الغير من ناحية أخرى وذلك عند ممارسة التحقيق بتفتيش جهاز له علاقة بجهاز المتهم داخل الدولة[1].

- **الاحتمال الثاني:** اتصال الحاسب الآلي للمتهم أو المشتبه فيه بحاسب أخر أو منظومة معلوماتية متواجدة في إقليم دولة أجنبية:

[1] لطروش فيروز ، لمرجع نفسه، ص 325.

يتحقق هذا الاحتمال حينما يقوم المجرم الإلكتروني بتخزين بيانات أو معلومات تفيد في إثبات الجريمة في حاسب أو منظومة معلوماتية متواجدة خارج إقليم الدولة التي تقييم فيها عن طريق شبكة الانترنت بهدف عرقلة سلطات البحث والتحري من الوصول إلى الدليل وفي مثل هذه الحالة تواجه سلطات التحقيق مشكلة كبيرة تتمثل في مدى جواز تمديدها لإجراءات البحث والتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الأذن بالتفتيش والدخول في المجال الجغرافي لدولة أخرى وهو ما يسمى بالتفتيش العابر للحدود ، وقد أتفق الفقه الجنائي على أنه لا يمكن اللجوء إلى هذا الإجراء إلا في إطار اتفاقيات تعاون خاصة ثنائية أو جماعية تجيز وتنظيم هذا الامتداد أو على الأقل الحصول على الأذن الصريح من الدولة الأجنبية وإلا يعد اختراق مباشر ويشكل انتهاكاً فعلياً لسيادة الدولة .[1]

ج – الضبط: إن الضبط في قانون الإجراءات الجزائية هو وضع اليد شيء ليتصل بجريمة وقعت في كشف الحقيقة عنها وعن مرتكبيها.

فالضبط في الجريمة الإلكترونية يختلف عن ضبط الجرائم الأخرى من حيث المحل لأن الجريمة الإلكترونية يرد الضبط على الأشياء ذات طبيعة معنوية وهي البيانات

[1] محمد أمين الرومي، **جرائم الكمبيوتر و الانترنت**، الإسكندرية، دار المطبوعات الجامعية، ط1، ص201.

والمراسلات والاتصالات الإلكترونية من جهة ولها طبيعة مادية كالورق والكمبيوتر وملحقاته والأقراص الصلبة الخارجية والمرنة وأقراص الليزر البطاقات الممغنطة.[1]

والعلاقة التي تنشأ عن هذا الارتباط بين التفتيش والضبط، هو أن الضبط لا يجوز أن يقع على شيء إلا بعد وصفه دليلاً من أدلة الجريمة التي يجري التفتيش بشأنها ولذلك فأنه يباشر من أجل الوصول للحقيقة المطلقة، بمعنى أنه مدام التفتيش يستهدف ذات الحقيقة فيتعين أن يباشر الضبط فيما يتعلق بها من أدلة سواء كانت للإدانة أم للبراءة، لأن ما يضبط في الحالتين يحقق العدالة الجنائية .

وبخصوص الطبيعة القانونية التي تكتسي على الضبط فقد يكون من إجراءات الاستدلال أو التحقيق، ويتم تحديد هذه الطبيعة بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص وأقتضى الأمر تجريده من حيازته كان الضبط في هذه الحالة بمثابة إجراء تحقيق، أما إذا كان الاستيلاء عليها من دون الاعتداء على حيازة قائمة فأنة يكون بمثابة إجراء استدلال[2]

[1]:زبيخة زيدان،المرجع السابق ص117

[2]: مرجع نفسه ،ص118

2-**الإجراءات الشخصية:**وسوف نتطرق في هذه المجموعة التي تتميز بطبيعة شخصية لأنها غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل وتتمثل هذه الإجراءات في: عملية التسرب، الشهادة،والخبرة التقنية استجواب المتهم.[1]

أ – عملية التسرب:

جاءت المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري تعرف التسرب بأنه يقصد بالتسرب ضباط أعوان الشرطة القضائية المكلف بتنسيق العملية لمراقبة الأشخاص المشتبه فيهم لارتكابهم جناية أو جنحة باتهامهم أنه فاعل معهم أو شريك لهم.

يسمح لضباط الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14[2] ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريض على ارتكاب الجرائم.

ب – الشهادة في الجريمة الإلكترونية:

الشاهد في الجريمة الإلكترونية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي والذي يكون لديه معلومات جوهرية لازمة للدخول في نظام المعالجة الآلية للبيانات فلذلك نجد أن الشاهد المعلوماتي ينحصر في عدة طوائف تتمثل

[1]– المرجع السابق،ص 120.

[2]– المادة 65 مكرر من قانون الإجراءات الجزائية .

في:مشغلة الحاسب الآلي ،خبراء البرمجة، المحللون،مهندسو الصيانة والاتصالات،مديرو النظم.

ج – الخبرة في الجريمة الإلكترونية :

لا بد أن يكون الخبير صاحب مقدرة وإمكانيات علمية وفنية في مسألة موضوع الخبرة ويستطيع القيام بدوره والقيام بهذا الأخير عليه أن يبين المكان المحتمل لأدلة الإثبات وشكلها وهيئتها والآثار الاقتصادية والمالية المترتبة دون إتلاف الأدلة أو الأجهزة أو تدميرها.

د – استجواب المتهم:

الاستجواب ما هو إلا مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق ومطالبته بإبداء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليماوذلك قصد محاولة كشف الحقيقة واستظهارها بالطرق القانونية.[1]

ومسألة تعيين خبير تشكل صعوبة لأجل الاستعانة بالخبير المناسب باعتبار الخبرة في مجال الإلكترونية تتطلب شروط تتلاءم مع التطورات الطارئة في مجال تكنولوجيا المعلومات خاصة المسائل الفنية والعلمية , ولكي يكون الشخص خبيراً قضائياً في مجال الجرائم الإلكترونية لا بد من أن يكون مؤهلاً علمياً ومهنياً ومتحصلاً على شهادات

[1] مولود ديدان، **قانون الإجراءات الجزائية**، دار بلقيس، ، الجزائر،دط، 2014 ، ص 42 وما يليها.

ودراسات عليا في هذا المجال , وأن يخضع للتدريب العلمي والقانوني بشكل مستمر كم أجل مواكبة كل جديد يطرأ على تخصصه.

وبالإضافة أنه يجب أن يكون ملمابالجوانب التقنية والفنية ، ونذكر منها :

- المعرفة بتركيب الجهاز وصناعته وطرازه وأنظمة تشغيله الرئيسية والفرعية وملحقاته وكلمات المرور وأكواد التشفير ..... وغيرها .
- طبيعة البيئة التي يعمل في ظلها من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزينوالوسائل المستخدمة [1].
- المواضيع الرقمية المحتمل تواجد فيها أدلة إثبات والصور والأشكال التي تتخذها
- الكيفية التي يمكن بواسطتها عزل النظام المعلوماتي دون تلف أو تغيير أو إفساد الأجهزة.
- التمكن من تحويل أدلة الإثبات غير المرئية إلى أدلة إثبات مقروءة والمحافظة على الأدلة المستخرجة بصورة النسخ أو المطبوعات بشكل يمكن للقاضي أن يستوعبها.

لذلك يجب اختيار الخبير بعناية ودقة وذلك يكون بناءاً على نوع الجريمة المرتكبة وطبيعة أدلتها , وحتى لا يكون سبباً في فقدان الأدلة لعدم الاختصاص الدقيق وقد تحتاج الجريمة إلى أكثر من خبير حيث لا يوجد خبير واحد قادر على التعامل

[1] زليخة زيدان،المرجع السابق،ص 123.

- مع كافة أنواع الجرائم الإلكترونية , وبالتالي تكون الخبرة فردية والتي تعتبر من أهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والانترنت فالمؤسسات الكبرى المتخصصة في هذا المجال جاهدة على الاستعانة بأشخاص ثبتت كفاءتهم في مجال الإلكتروني والانترنت وهذا ما يطلق عليه بالخبرة الخاصة.[1]

ثانيا : الوسائل العلمية التي يلجأ إليها الخبير لاكتشاف الدليل الإلكتروني .

يعتمد الخبير في شرح ملابسات الجريمة الإلكترونية واستخلاص الدليل على مجموعة من الوسائل والتي تتمثل في غالبيتها أدوات فنية، ونذكر منها على سبيل المثال لا الحصر ما يلي :

1 – عنوان برتوكول الانترنت IP والبريد الإلكتروني وبرامج المحادثات : ويقصد بعنوان الانترنت المسئول عن تراسل كم من البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها ويشبه عنوان البريد العادي حيث يسمح للشبكات بنقل الرسالة وهو موجود بكل جهاز الإلكترونية مرتبط بشبكة الانترنت ويتكون عنوان الانترنت من أربعة خانات [أجزاء] حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود خدمة .

[1] زبيخة زيدات، لمرجع السابق،ص 124.

ثـــــانيا: الإجراءات الحديثة لجمع الدليل الإلكتروني: وتنقسم هذه الخبرة إلى :

1- الإجراءات المتعلقة بالبيانات الساكنة:

أ -**التحفظ المعجل على البيانات المخزنة** : ويقصد به توجيه السلطة المختصة لمزودي سيطرته،في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية.

ب -المقصود بمزودي الخدمات: هو من يقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات الإلكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود.[1]

2-الإجراءات المتعلقة بالبيانات المتحركة:

أ – حرمة الاتصالات الإلكترونية الخاصة:

نتيجة للتطور التكنولوجي الذي أدى إلى إفراز أجهزة لمراقبة ذات تقنية إلى مراقبة الأحاديث التي تمس بحق الإنسان في خصوصيته وما يتفرغ عنه من سرية الأحاديث الخاصة،وهو لصرف الصلة بالإنسان.[2]

---

[1] – عبد الرحمن خلفي، **الإجراءات الجزائية في التشريع الجزائري و المقارن**، دار بلقيس للنشر، د ط، 2015،ص 296.

[2] – المرجع نفسه،ص 297.

فلذلك أقرت معظم التشريعات على توفير قدر كبير من الحماية الجنائية على سرية الاتصالات الخاصة للأفراد،حيث عاقب المشرع الجزائري لأول مرة اعتراض الاتصالات السلكية واللاسلكية دون إذن بذلك بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل لقانون العقوبات الجزائري حيث تنص المادة 303 مكرر من قانون العقوبات على أنه:" يعاقب بالحبس من 06 أشهر إلى 03 سنوات وبغرامة تقدر ب 50.000 إلى 300.000 دج كل من تعمد المس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت .[1]

ب – اعتراض الاتصالات الإلكترونية بناءا على إذن:

مما لا شك فيه أن الحماية التي يكفلها المشرع للاتصالات العادية لا يقتصر نطاقها على هذا النوع من الاتصالات فحسب بل تمتد هذه الحماية إلى الاتصالات الإلكترونية عبر الانترنت من باب أولي بحسبان أن الغاية من وراء هذه الحماية هي حماية الحياة الخاصة للإنسان بحماية مستودع أسراره الشخصية، فإذا اقتضت ضرورة التحقيق اعتراض هذه الاتصالات و تسجيلها فستتبع – حينها – نفس الضمانات المقررة للمحادثات التلفزيونية ،مع مراعاة خصوصية هذه الاتصالات الحديثة.[2]

[1] – المادة 303 مكرر من القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 المعدل لقانون العقوبات الجزائري.

[2] – عبد الفتاح عبد اللطيف الجبارة ، **الإجراءات الجنائية في التحقيق** ، دار الحامد للنشر والتوزيع ،ط1، 2015 ص 25.

الفرع الثاني: مرحلة التحقيق في الجريمة الإلكترونية

التحقيق الجنائي يكون في جميع الجرائم التقليدية و المستحدثة و باعتبار أن الجرائم الالكترونية حديثة المنشأ تخضع لشخص المشتبه فيه للتحقيق من طرف السلطات المختصة .

فإن عملية التحقيق الجنائي تمر بمرحلتين المرحلة الأولى تسمى التحقيق الأولي المرحلة الثانية تسمى التحقيق الابتدائية فالمرحلة الأولى هي مرحلة جمع الاستدلالات التى يباشرها أعضاء الضبط القضائية وذلك حسب المادة 12 الفقرة الثالثة من قانون الإجراءات الجزائية والتي تنص بأنه " يناط بالضبط القضائي مهمه البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها تحقيق قضائي "،والمرحلة الثانية تدخل في اختصاص قاضي التحقيق وهذا حسب المادة 38 من نفس القانون حيث انه تنص على أنه"يناط لقاضي التحقيق إجراءات البحث والتحري ولا يجوز له أن يشترك في الحكم في قضايا نظرها بصفته قاضياً للتحقيق وإلا كان ذلك الحكم باطلاً "[1]

تعتبر هذه المرحلة هي المرحلة الثانية بعد مرحلة جمع الاستدلالات، فهي مرحلة من اختصاص قاضي التحقيق الذي يتعين بمقتضى قرار من وزارة العدل.

[1]– المادة 38 من قانون الإجراءات الجزائية.

أولا: سلطات قاضي التحقيق و حدود الدعوى الجنائية أمامه

يعد القيام باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة وبالتحري عن أدلة الاتهام و أدلة النفي المادة 68 قانون الإجراءات الجزائية.

كما يجوز لقاضي التحقيق أن يأمر بإجراء فحص طبي كما له أن يعهد إلى الطبيب بإجراء فحص نفساني المادة 68 من قانون الإجراءات الجزائية.

يستطيع القاضي سماع أقول كل من يشير إليهم في الشكوى باعتبارهم شهودا طبقا لنص المادة 73 من نفس القانون، وعلى القاضي الانتقال إلى مكان وقوع الجريمة للقيام بالمعاينات اللازمة طبقا لأحكام المادة 79 من القانون السابق.[1]

و يتم استدعاء كل شخص يرى فائدة من سماع شهادته بواسطة أحد أعوان القوة العمومية عملا بنص المادة 88 من قانون الإجراءات الجزائية[2].

[1] المواد من 68 إلى 79 من قانون الإجراءات الجزائية.

[2] المادة 88 من قانون الإجراءات الجزائية الجزائري.

ثـــــــانيا: اتصال قاضي التحقيق و استئناف أوامره

يتصل قاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية و ذلك بموجب إجراء تحقيق رسمي للطلب الافتتاحي لإجراء التحقيق إما عن طريق شكوى جزائية مقدمة من المضرور و هذا ما أكدته المادة 38 الفقرة 3 من قانون الإجراءات الجزائية والتي نصت صراحة على أنه:" ...يختص بالتحقيق في الحادث بناءا على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67إلى غاية 73.

أما الجهات التي تستأنف أوامر قاضي التحقيق هي :

1/ **النيابة العامة** :لوكيل الجمهورية أو أحد مساعديه استئناف جميع أوامر قاضي التحقيق دون استثناء وذلك طبقا لنص المادة 170 من قانون الإجراءات الجزائية الوكيل الجمهورية الحق في أن يستأنف أمام غرفة الاتهام جميع أوامر قاضي التحقيق.[1]

كما نصت أيضا المادة 171 من القانون السابق :" يحق الاستئناف أيضا للنائب العام في جميع الأحوال و يجب أن يبلغ استئنافه للخصوم خلال عشرين يوما التالية لصدور

[1] – المادة 170 من قانون الإجراءات الجزائية.

أمر قاضي التحقيق ولا يوقف هذا الميعاد ولا رفع الاستئناف بتنفيذ الأمر بالإفراج المؤقت".[1]

2-**استئناف المتهم** :المتهم لا يجوز له إستئناف جميع أوامر قاضي التحقيق بحيث يرفع الإستئناف بعريضة تودع لدى قلم مكتب المحكمة في ظرف ثلاث أيام من تبليغ إلى المتهم طبقا للمادة 168 ق إ ج

2 **إستئناف المدعي المدني** :أجاز المشرعالجزائري للمدعيالمدني الحق في إستئناف أوامر قاضي التحقيق التي لها علاقة بحقوقه المدنية ،وبمفهوم المخالفة لايجوز له إستئناف الأوامر المتعلقة بالجانب الجزائي مثل الحبس المؤقت والإفراج والرقابة القضائية .

الفرع الثالث: مرحلة المحاكمة في الجريمة الإلكترونية

أولا: اختصاص المحكمة

1 **الاختصاص المحلي في الجريمة الإلكترونية :**

طبقا لنص المادة 37 من قانون الإجراءات الجزائية يتحدد الاختصاص المحلي للجريمة في ثلاث ضوابط في مكان إقامة المتهم أو محل ضبطه.[2]

[1] – المادة 171 من قانون الإجراءات الجزائية.

[2] – المادة 37 من قانون الإجراءات الجزائية.

ففي نطاق الجرائم فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث فيروس ويحقق النتيجة في تدمي المعلومات في مكان أخر فإن الاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة.

ومتى كانت الجريمة الإلكترونية أيا كان نوعها فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية إذا ارتكبت خارج الإقليم الوطني وإذا كان مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية وذلك في إطار التعاون الدولي[1].

كما نصت أحكام المرسوم التنفيذي رقم 06ـــــ348 المؤرخ في5اكتوبر 2006 علي تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق الي دائرة اختصاص محاكم أخري، ويتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة وكذا محكمة قسنطينة، ومحكمة ورقلة وقسم محكمة وهران.[2]

2 الاختصاص النوعي في الجريمة الإلكترونية :

يتحدد الاختصاص النوعي للمحكمة بالفصل في المسائل المعروضة عليه تبعا لنوع الجريمة التي ينظر فيها،حيث تختص محكمة الجنايات بالفصل في الجنايات والجرائم

[1] عبد الرحمن خلفي، المرجع السابق،ص 66.

[2] المرسوم التنفيذي، رقم 06ـــــ348 المؤرخ في أكتوبر2006، المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، جريدة عدد63 ص.29

الموصوفة بأفعالإرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الاتهام حسب المادة 248 من قانون الإجراءات الجزائية كما تختص المحاكم بالنظر في الجنح و المخالفات فيما عدا الاستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 قانون الإجراءات الجزائية.[1]

المادة 248 من قانون الإجراءات الجزائية الجزائري ،كما تختص المحاكم في النظر في الجنح والمخالفات في ماعدا الاستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 قانون الإجراءات الجزائية.[2]

ثـــــانيا: تشكيلة المحكمة و الإجراءات المتابعة

1 / تختلف تشكيلة المحكمة الجزائية بحسب قسم ونوع قسم الجنح الخاصة بالجريمة الإلكترونية على مستوى المحكمة يتشكل من فرد ويساعده كاتب ضبط وبحضور وكيل الجمهورية أو مساعديه.

أما الغرفة الجزائية على مستوى المجلس القضائي فالتشكيلة فيها ثلاثية أي تتشكل من رئيس غرفة ومستشارين بالإضافة إلى كاتب ضبط وبحضور نائب عام أو أحد مساعديه.

[1] – المادة 248 من قانون الإجراءات الجزائية .

[2] -القانون رقم 04ـــــ14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 155/66 المتضمن قانون الإجراءات الجزائية ،جريدة عدد 71 ص5

أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبط والنيابة العامة أو من يمثلها.

2/ أما من ناحية الإجراءات فتستهل المحكمة جلستها بالإعلان أولا عن افتتاحها بالقول باسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم

والضحية والشهود والمسئول المدني والتأكد من حضورهم أو غيابهم، والتأكد من هويتهم والمادة القانونية المتابع بها[1].

إذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة وذلك بشروط: ترك المتهم حرا،إخضاع المتهم لتدابير أو أكثر من تدابير الرقابة القضائية.

أما إذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق فإنه يساق بواسطة القوة العمومية لحضور الجلسة ويخطره رئيس الجلسة بأن له الحق في اختيار محام الدفاع عنه.

ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها بالتفصيل من طرف القاضي وبعدها يقوم القاضي بسماع الشهود.

وبعد انتهاء من تحقيق تعطى الكلمة للطرف المدني فقط دون المطالعة بالعقوبات الجزائية،لتقوم بعد ذلك النيابة العامة بالمرافعة و تقديم التماساتها،ليقوم دفاع المتهم بتقديم

[1] – مولود ديدان، المرجع السابق،ص 51.

مرافعته وتقديم التماساتها،ويكون بعدها لنيابة العامة والمدعى حق الرد على موافقة محام المتهم و تعطى الكلمة الأخيرة بعدها للمتهم ومحاميه.

ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه نفس الجلسة أو يحدد تاريخ لاحق منطق بالحكم.[1]

المطلب الثاني: العقوبات المقررة على الجريمة الإلكترونية

العقوبات المقررة على ارتكاب الجريمة الإلكترونية سواء تعلق الأمر بالشخص الطبيعي والمعنوي أدرجها المشرع الجزائري في قانون العقوبات وخصص لها القسم السابع مكرر وسماه بالأنظمة المعالجة الآلية للمعطيات وخصص له 08 مواد اختلفت ما بين عقوبات أصلية وأخرى تكميلية.

الفرع الأول :العقوبات المقررة للشخص الطبيعي

أولا: العقوبات الأصلية

وتنقسم إلى جريمة بسيطة التي تمثلت في الدخول و البقاء الغير مصرح به حيث جاء في أحكام المادة 394 مكرر:" يعاقب بالحبس من ثلاثة أشهر إلى سنة وغرامة مالية من

[1] – امولود ديدان ، لمرجع السابق،ص 52.

50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الإلية للمعطيات.[1]

وجريمة مشددة تتمثل في الدخول والبقاء حيث نصت المادة 394 كرر 1 – 2 – 3 على تضاعف العقوبة إذا ترتب على ذلك تغيير في المعطيات أو حذفها المنظومة ولقد حدد العقوبة بالحبس من 06 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج.

وأخيرا إلى الاعتداء العمدي على المعطيات:

واستنادا لنص المادة 394 مكرر 2 فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من شهرين إلى 03 سنوات أو بغرامة مالية من 1.000.000 دج إلى 5.000.000 دج.[2]

ثـــــانيا: العقوبات التكميلية

من خلال نص المادة 394 مكرر نجد أنه إضافة إلى العقوبات توجد مجموعة من العقوبات التكميلية وهي كالتالي:

[1] – ينظر المادة 394 من قانون الإجراءات الجزائية .

[2] – ينظر المادة394 مكرر1 – 2 –3 من قانون الإجراءات الجزائية.

1 -**المصادرة :** يقصد بها مصادرة الأجهزة و البرامج و الوسائل المستخدمة للارتكاب الجرائم الماسة بالنظام و ذلك لبيعها أو حجزها مع مراعات حقوق الغير .

2 **الإغلاق:** يقصد المشرع بها موقع الانترنت أو الموقع الإلكترونية التي تعتبر وسيلة لارتكاب الجرائم أو تساعد في ارتكابها.

3 **إغلاق المحل أو مكان الاستغلال:**يشترط فيه توفر عنصر العلم بمعنى إذا ارتكبت الجريمة بعلم صاحبه أو مشاركا فيه أو لم يقم بالإخبار عنه أو بمنعه فتكون عقوبته بإغلاق المقهى الإلكتروني.

الفرع الثاني: العقوبات المقررة للشخص المعنوي

جاء في أحكام المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي أن عقوبة الشخص المعنوي تتأسس على مبدأ المسائلة بمعنى يسأل الشخص المعنوي عن هذه الجرائم سواء كان فاعلا أصليا أو شريكا أو متدخلا ،كما يسأل عن الجريمة التامة أو الشروع فيها شريطة أن تكون الجريمة لمصلحة الشخص المعنوي أو كانت بواسطة أحد أعضائه أو ممثليه ويكون منصوب عليها قانونا.أما فيما يخص المشرع الجزائري فقد نظم عقوبة الشخص المعنوي من خلال التعديل الأخير لقانون العقوبات وذلك من خلال نص المادة 18 مكرر من القانون 15/04[1] المتضمن قانون العقوبات الذي ينص:

[1] – ينظر المادة 18 مكرر من قانون 14/05.

1/ الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب الجريمة.

2/ واحدة أو أكثر من العقوبات الآتية :

- ✓ حل الشخص المعنوي
- ✓ غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 05 سنوات
- ✓ الإقصاء من الصفقات العمومية لا تتجاوز 05 سنوات
- ✓ المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية مباشرة أو غير مباشرة لمدة لا تتجاوز 05 سنوات
- ✓ مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- ✓ نشر أو تعليق حكم الإدانة
- ✓ الوضع تحت الحراسة القضائية لمدة لا تتجاوز 05 سنوات.

نصت المادة 394 مكرر 4 [1]من قانون العقوبات على الغرامة المالية المطبقة على الشخص المعنوي،يعاقب الشخص المعنوي الذي يرتكب أحد الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 05 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

المبحث الثاني: التدابير التشريعية و تطبيقات عن أساليب مكافحة الجريمة الإلكترونية

[1] – ينظر المادة 394 مكرر4 من قانون الإجراءات الجزائية .

لا بد من الاعتراف أن الإسهام في اقتراح حلول للإشكالات التي يطرحها موضوع الجريمة الإلكترونية مهمة جدا تعترضها صعوبة منهجية كبرى مصدرها اتساع و تشعب الجوانب التي تتعلق بالمعلوماتية .

المطلب الأول: الحلول التشريعية

تتمثل هذه الحلول التشريعية في تدابير وقائية تتخذها الدولة وسنتها القوانين من أجل مكافحة هذه الجريمة وحماية المجتمع، يتطلب الأمر اللجوء أولا إلى الحلول قصيرة المدى ثم الحلول طويلة المدى.

الفرع الأول: الحلول التشريعية قصيرة المدى

إن هذه الحلول تتمثل في إصدار السلطة المختصة بعض المراسيم التنظيمية لمقاهي الانترنت دون احتكار المعلومة فيمكن في إجراءات استعجاليه فرض بعض الأمور على أصحاب مقاهي الانترنت:[1]

- وضع البرامج اللازمة لمنع الدخول إلى المواقع المخلة بالحياء و هذا من أهم الظواهر التي برزت في مجتمعنا في ظل غياب التربية السليمة مما يؤدي للانحلال الخلقي لشبابنا،وحتى المراهقين الذي أصبح من السهل عليهم دخول أي

[1] – أمير يوسف فرج ،**الجريمة الإلكترونية و المعلوماتية و الجهود الدولية و المحلية لمكافحة جرائم الكمبيوتر** ،مكتبة الوفاء القانونية،الإسكندرية، ط 1، 2011،ص 380.

موقع يشاءون، بالإضافة إلى المواقع الإباحية هناك مواقع إرهابية ومواقع العنف كتعليم القتل،لذلك لا بد من اتخاذ تدبير عاجل.

- وضع برامج للحماية من الفيروسات وهذا كله بمراسيم تنظيمية ويمكن للدولة أن تدعم هذه العملية بتخفيض أسعار هذه البرامج.
- إصدار مراسيم من أجل تنظيم تكوين محققين ورجال شرطة وقضاة على التقنية الإلكترونية و المعرفة الكافية لجرائم الانترنت.
- تعريض أشخاص أو مقاهي الانترنت لغرامات مالية أو إغلاق المقهى إذ تثبت أنه يسمح للمراهقين أو حتى الشباب بالدخول للمواقع السابقة.[1]
- النوعية القانونية والتعريف بمدى خطورة الجرائم الإلكترونية .[2]
- أما من ناحية المواد المدنية والتجارية فإنه :

*يمكن للمحامات لعب دور مهم لتكيف بعض السلوكيات والمعلومات مع محاولة تكيف بعض المنازعات التجارية الإلكترونية، قياسا علي التجارة العادية لحين صدور تشريع منظم للتجارة الإلكترونية

*اعتماد حرية الإثبات في المجال التجاري

*يجب علي المشرع أن يوقع بعض المعاهدات والإتفاقيات لمكتفحة الجريمة الإلكترونية ومسايرتها بسن قوانين تنظيمية

[1]HTTP//DROIT.MOONTADA.COM/T622.TOPIC:

[2] – أمير يوسف فرج، المرجع السابق،ص 381.

فرع الثاني: الحلول التشريعية طويلة المدى

يعد الطابع الافتراضي لشبكة الانترنت يلزمه تعديلات عديدة من التشريعات الحالية بالإضافة إلى استحداث أخرى، وذلك بالاستفادة من الدول الأخرى التي سبقتنا في مجال التشريع لتجريم هذه السلوكات مادامت هذه التشريعات لا تخالف النظام العام

والآداب العامة تحت ما يقال لا يمكن معاقبة شخص من دون نص قانوني.[1]

1-الركن الشرعي:إذلابد من سن نصوص قانونية تتناسب والتطور الحالي،ومن الملاحظ أنه رغم زيادة انتشار الجرائم الإلكترونية و فعاليتها إلا أن المشرع لم يضع لحد الآنالإطار القانوني لأي من هذه الظواهر،لذا وجب على المشرع أن يعدل أو يصدر قوانين جديدة وسن تشريع جديد يتضمن الجرائم الإلكترونية من بينها العقد الإلكتروني والتوقيع الإلكتروني ...الخ.

2-القانون التجاري:ولقد عالجت معظم التشريعات موضوع التجارة الإلكترونية، وتكاد تتفق جميعها في بنائها الذي يعتمد على القانون النموذجي للتجارة الإلكترونية الذي وضعته لجنة اليونسترال [2]لكي تتيح تفعيل هذه التشريعات ووضعها موضع التطبيق ،إذ ليسثمة تنظيم لسلطات توثيق المعاملات الإلكترونية وليس ثمة تشريعات للمعايير الأمنية أو المعايير القياسية لخدمات التقنية وليس ثمة حسم لكثير من المشكلات الرئيسية في

[1] – عبد الرحمن خلفي ،المرجع السابق.ص67

[2]–**اليونسترال:** هي لجنة التجارة في الأمم المتحدة عام 1966.

ميدان التجارة الإلكترونية كمسائل الضرائب على الانترنت والدفع عن طريق بطاقة الائتمان ومسائل الخصوصية وغيرها[1]

المطلب الثاني: تطبيقات عن أساليب مكافحة الجريمة الإلكترونية

في إشارات مختصرة سنحاول الإطلاع على مدى ملائمة التشريعات ومدى نجاحها بشأن مكافحة الجريمة الإلكترونية وحماية المعلومات،فبين غافل ومواكب للتطور هو حال دول العالم.

قبل ظهور هذه السلوكيات المجرمة في بعض الدول المتقدمة لم تخضع قوانين العقوبات إلى أي تعديل يتيح تجريم مختلف صور جرائم الكمبيوتر أو يتيح المساواة بين المعلومات،سوى تعديل بعض العقوبات أو الغرامات المالية.

الفرع الأول: الأساليب الدولية

إن الولايات المتحدة الأمريكية والدول الأوربية 2001 من الدول التي ساهمت في التطور الواضح في مجال المعلوماتية بحيث:

رسمت سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الانترنت إذ يستلزم التدخل الحكومي والدولي نظرا للخطورة الجسيمة للأمر.

الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكب الجريمة

[1]:امير فرج يوسف،المرجع السابق،ص382

والاستدلال عليه بأقل وقت ممكن.

أما فرنسا تعتبر من بين الدول التي صادقت على تعديل القوانين حيث غيرت الغرامات المالية وحددت مدة السجن ،ويتضح من هذاالتغيير أن التكييف الجنائي لهذه السلوكيات المجرمة قد كيفه المشرع الفرنسي بجنحة أو جناية.[1]

ففي المادة 226 الفقرة 16 [2]من قانون العقوبات الفرنسي أصبحت الغرامة تقدر ب 45000 أورو ومدة السجن 03 سنوات حيث نصت على أنه:" كل فعل عن قصد أو عن غير قصد يرمي إلى المعالجة الآلية للمعلومات الاسمية بدون احترام الشكليات الأولية المقررة يعاقب عليها ب 45000 أورو السجن لمدة 03 سنوات".

الفرع الثاني: الأساليب المحلية

لقد فتحت الجزائر مجالا واسعا للانترنت وأدخلت عدة تقنيات حديثة تجدر الإشارة هنا إلى أن بعض مصالح البلديات تسعى حاليا إلى فتح بريد إلكتروني لاستخراج الوثائق.

[1] - le traitement judicaire de la cybercriminalité guide méthodologique ministère de la justice française p07 -

[2] – ينظر المادة 226 الفقرة 16 من قانون العقوبات الفرنسي.

فلقد أدخل استغلال شبكة الانترنت في نظام الخصوصية بعد أن كانت محتكرة من طرف مركز البحث في الإعلام العلمي والتقني بموجب مرسوم تنفيذي رقم 257 – 98 المؤرخ في 25 أوت 1998 [1]وقد ورد هذا المرسوم ما يلي:

***المـــــادة الأولى:** ضبط هذا المرسوم شروط وكيفيات إقامة خدمات"أنترنت " واستغلالها

***المـــــادة الثانية:** تعرف خدمات الأنترنت مايلي:

– خدمات " الواب" الواسعة النطاقWord. Vide WEPخدمات تفاعلية للإطلاع أو احتواء الصفحات متعددة الوسائط MultiMedia

– البريد الإلكتروني [2] Email: خدمات تبادل الرسائل الإلكترونية.

– تلنات [3]Telanat: خدمات النفاد إلي حواسب متابعة بصيغة المحاكاة الطرفية

– NEWGROUPS :خدمات تسمح بتبادل المعلومات بين مجموعة من المستعملين ذوي اهتمام مشترك حول موضوع معين

وغيرها من مختلف الخدمات التي يصعب حصرها وذكرها كلها.

- كما اورد اجراءا وقائيا في المادة 8/14 من هذا المرسوم مايلي :

[1] – مرسوم تنفيذي رقم 257– المؤرخ في 25 أوت 1998.

[2] – **البريد الإلكتروني:** خدمات تبادل الرسائل الإلكترونية

[3] – **تلنات:** خدمات النفاذ إلى حواسب متباعدة بصيغة المحاكاة الطرفية

– المحافظة علي سرية كل المعلومات المتعلقة بحياة مشتريكيها الخاصة ،وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون.

– تسهيل النفاذ إلي خدمات الإنترنت حسب الإمكانيات المتوفرة إلي كل الراغبين في ذلك.

– احترام قواعد حسن السير بالامتناع خاصة عند استعمالأية طريقة غير مشروعة سواء اتجاه المستعملين أو اتجاه مقدمي الخدمات "الانترنت "

الفرع الثالث :الآفاق المستقبلية لمكافحة الجريمة الإلكترونية في الجزائر :

أكد فاروق قسنطيني[1] ،رئيس اللجنة الوطنية للترقية وحماية حقوق الإنساعلي صعوبة تطبيق القوانين المعاقبة علي الجريمة الإلكترونية في الجزائر لقلة خبرتها في هذا الشق ،وغياب المختصين والخبراء القادرين علي تشخيص الجريمة قبل عرضها علي المحكمة للفصل فيها،وقال القسنطيني في تصريح للسلام:"أن استصدار الجزائر قوانين لمعاقبة مرتكبي الجرائم الإلكترونية غير كاف،مع عدم تهيئة الأسس التقنية،الكفيلة بتصنيف درجات هذه الجرائم وحدّة إضرارها قبل إصدار العقوبة،فهذا فضلا عن غياب التواصل الدائم بين القضاة والمختصين في

[1] قسنطيني ، تطبيق العقوبات في قضايا الجريمة الإلكترونية صعب في الجزائر ،صحيفة السلام الإلكترونية ليوم 24 -0 -2014

الاتصالات، ما أفرزه شبه تذبذب وغموض في شأن العقوبات في مثل هذه الجرائم."

وفي هذا الصدد وفي السياق ذاته أوضح أن القانون الجزائري،يعاقب في الغالب مرتكبي هذه الجرائم بالسجن قصير المدى أو بالغرامة المالية "بحكم أن جل الجرائم الإلكترونية المرتكبة في الجزائر تصب أو تصنف قانونيا كسرقة" ،مبرزا أن المعدل العام لهذه الجرائم في الجزائر متوسط مقارنة بباقي دول العالم،محذّرا من تنامي هذه الجرائم في السنوات الأخيرة من المستوي الوطني،مع بداية مرحلة إدمان الجزائر علي الانترنت،وما يصاحبها من خدمات إلكترونية، ودعا الحكومة إلي ضرورة استحداث استراتيجيات عقابية وتقنية لحماية ضحايا هذه الجرائم،خاصة فئة الأطفال ورجال المال كونهم الأكثر عرضة لها.[1]

وكانت الجزائر ضمن مجموعة من الدول المدرجة في مشروع إعداد بحث لتحديد لآلية تطور الهجمات الإلكترونية خلال السنوات الثمانية المقبلة، من طرف منظمة "التحالف الدولي لحماية أمن الانترنت" والذي يتضمن تقديم إرشادات لحكومات الدول والسلطات المحلية حول أفضل السبل المتاحة لمواجهة هذه الهجمات.[2]

فقد رأى المشرع بأنه من الضروري سن قانون للحد من هذه الجرائم خاصة مع إرتفاع النداءات المطالبة بذلك.

[1]:الجزائر معينة بالمشروع الدولي لمكافحة الجرائم الإلكترونية، قسم الشروق أون لاين ليوم 23-02-2012

[2]-WWW.ECHOROUK ONLINE.COM/ARA/ARTICLES

فقد قال الوزير هيشور: أصبحنا نرى ارتكاب أعمال غير قانونية وغير أخلاقية وغير مرخصة من مواقع بعيدة، بحيث زكي هذا المسعي مؤتمر أوراق العمل الوطني الأول في 28/03/2008 المنعقد في عين الدفلى،والذي تبنى دراسة توصي بتشريع يعاقب مجرمي الأنترنت بالإضافة إلي الملتقى الوطني الأول حول الجرائم الإلكترونية 12/12/2008.

وقد سعت السلطات الأمنية الجزائرية إلي الإستعانة بالمرصد الفرنسي لمتابعة جرائم الأنترنت من خلال إيجاد مرصد جزائري شبيه ويعتزم مناقشته في البرلمان قريبا، ينص القانون علي إنشاء مرصد مراقبة للتحكم في جرائم الكمبيوتر.[1]

[1] - WWW.ECHOROUK ONLINE.COM/ARA/ARTICLES

خلاصـــة الفـــــصل:

نستخلص من خلال هذه الدراسة أن الجريمة الإلكترونية متميزة عن باقي الجرائم ليس فقط في تعريفها وخصوصيتها ،بل تعدى الأمر ذلك حتى في إجراءات التحقيق فيها وحجية إثباتها بالنظر إلى صعوبة إثبات إثباتها كما سبق التطرق إليه.

ولم يغفل المشرع الجزائري إلى خطورة هذه الجريمة خطورة مرتكبها،فبادر بسن مختلف النصوص القانونية التي جاء في أحكامها عقوبات مشددة لمرتكبي الجرائم الإلكترونية بغض النظر عن كون الفاعل شخصا طبيعيا أو معنويا وذلك بهدف تحقيق الردع والحد من هذه الجرائم التي دخلت إلى مجتمعاتنا كفيروس خبيث إنتقلت عدواه إلى بقاع العالم وتفشت فيه وأضحى من الصعب اليوم التخلص منها .

في لختام هذه الدراسة المتعلقة بالجريمة الإلكترونية والذي لا أعتبره محاول الإلمام بالموضوع وما يطرحه من إشكالات عديدة ومبادئ جديدة،يمكن أن نقول أن هذه الجريمة تتميز باختلاف تعاريفها وتطورها وإرهاقها للمجتمعات الحديثة عرفنا أنها جريمة مستحدثة يكون الحاسب الآلي فيها أداة لارتكاب الجريمة فهي ليست مجرد نبيذ قديم في زجاجة جديدة" كما وصفها جملة من الإعلاميين الغربيين في المراحل الأولى لظهورها ولكنها في الحقيقة جرائم جديدة في طبيعتها و مضمونها،نطاقها وتأثيراتها،أدواتها و حتى في خصوصية وتميز وطبيعة مرتكبيها.

ومن خلال هذا البحث توصلنا إلى جملة من النتائج التالية:

1. بالنظر لحداثة هذا السلوك الإجرامي(الجريمة الإلكترونية) فإنه لا يوجد لحد الآن إجماع فقهي موحد على تعريف لها مما أدى بالقول أن الجريمة الإلكترونية تقاوم التعاريف.
2. رغم اجتهاد وتدارك المشرع الجزائري الفراغ القانوني في مجال الإجرام المعلوماتي إلا أنه لم يستطع التصدي لهذه الجريمة.
3. المشرع الجزائري عدل قانون العقوبات في عام 2006 بموجب قانون 06ـــ23 المؤرخ في 20 ديسمبر 2006 وذلك لازدياد الوعي بخطورة هذا النوع من المستحدث من الإجرام باعتباره يؤثر علي الاقتصاد الوطني بالدرجة الأولي وشيوع ارتكابه ليس

فقط من الطبقة المثقفة بل من قبل جميع مستويات التعليم والأعمار نتيجة تبسيط وسائل التكنولوجيا والمعلومات وانتشار الانترنت كوسيلة لنقل المعلومات.

4. المشرع الجزائري لم يخصص قانونا خاصا قائم بذاته للتحكم بهذه الجريمة وحسن سيرها.
5. في ظل قصور الحماية الجنائية للجرائم لمعلوماتية أصبحت هناك ضرورة لتكاثف الجهود الدولية وتوافق السياسات الجنائية في مواجهة هذه الجرائم بوضع اتفاقيات دولية ونصوص تشريعية.

في ضوء النتائج التي أظهرتها الدراسة نستخلص بعض التوصيات و الاقتراحات تتمثل في:

- ضرورة إعطاء تعريف موحد للجريمة الإلكترونية
- على المشرع أن يضع نصوصا قانونية واضحة خالية من الغموض كون أنها ستؤطر ظواهر اجتماعية جديدة مستقبلا.
- وضع إجراءات و القيام ببعض التعديلات على النصوص القائمة لمواكبة هذه الجرائم المتطورة.
- عقد دورات تدريبية التي تعتني بمكافحة الجرائم الإلكترونية
- بإعتبار الأسرة هي أساس المجتمع يجب أن يتم توعية الأولياء وتوفير الوسائل التي من شأنها أن تساعدهم للقيام بدورهم كاملا كمراقب أولي.

- توعية المجتمع حاصة فئة الشباب وخلق له ثقافة اجتماعية جديدة بأن هذه الجرائم ما هي إلا أعمال غير مشروعة ويتعرض مرتكبها لعقوبات جزائية.
- يتعين إدخال مادة الأخلاقيات الأنترنت ضمن المناهج الدراسية في التعليم ماقبل الجامعي.
- تعزيز التعاون بين المؤسسات الدولية المعنية بمكافحة مثل هذه الجرائم.
- اشتراك الإعلام بمختلف وسائله السمعية والبصرية للتوعية بمخاطر هذه الجرائم والطرق المتبعة من طرف المجرمين لاصطياد ضحاياهم، كما يجب أن تكون هذه الحصص دورية وتمس جميع فئات المجتمع وتبسيط لهم المعلومة، كي تصل بسهولة ويتم إستعابها والعمل بها مستقبلا.
- يجب إنتاج وتوفير الأدوات التي من شأنها أن تعطي الحماية اللازمة لمتصفحي الإنترنت خاصة ماتعلق منها بالبرامج الخاصة، أو الأنظمة العامة.
- الإستعانة ببرامج أمن قوية ضد الفيروسات
- الأخذ بالتجارب السابقة بالنسبة للدول المتطورة والتي ساهمت بشكل كبير في محاربة الجريمة الإلكترونية كالولايات المتحدة الأمريكية وكندا..

قائمة المصادر والمراجع

أولا: القوانين والمراسيم

1. القانون رقم 04ـــ14 المؤرخ في 10نوفمبر 2004 المعدل والمتمم للأمر 155/66 المتضمن قانون الإجراءات الجزائية ، جريدة عدد 71.

2. المرسوم التنفيذي، رقم 06ـــــ348 المؤرخ في أكتوبر2006، المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، جريدة عدد63.

ثـانيا:الكتب

1. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ،دار هومة، الجزائر،ط10،2011
2. أحمد خليفة، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط2،2006
3. أحمد عبد الله المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها دراسة تحليلية تأصيلية مقارنة، ط1، سنة2017
4. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، دار الناشر، مكتبة الوفاء القانونية، الإسكندرية، سنة2011
5. خالد الداودي، الجريمة المعلوماتية، ط1، دار إعصار العلمي، ط1، سنة2018
6. خالد ممدوح ابراهيم، الجريمة المعلوماتية ،دار الفكر الجامعي،الإسكندرية، ط1،سنة2009

7. زبيخة زيدان،الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى،عين مليلة الجزائر، دط، سنة2011

8. عائشة بن قارة مصطفي،حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن،دار الجامعة الجديد،كلية الحقوق، جامعة الإسكندرية، ،دط، سنة2006

9. عبد الرحمان خلفي،الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس لنشر، دط، سنة2015

10. عبد الفتاح عبد اللطيف الجبارة،الإجراءات الجنائية في التحقيق، ،دار الحامد للنشر والتوزيع،ط1، سنة 2015

11. عمرو موسي الفقيهي،الجرائم المعلوماتية (جرائم الحاسب الآلي والأنترنت في مصر والدول العربية)،مكتب الجامعي الحديث،الإسكندرية، دط، سنة2006

12. غانم مرضي الشمري،الجرائم المعلوماتية،ماهيتها خصائصها،كيفية التصدي لها قانونيا، ، دار العلمية الدولية لنشر والتوزيع، عمان، ط1، سنة2016

13. محمد أمين الرومي، جرائم الكمبيوتر والانترنت، ط1،دار المطبوعات الجامعية،الإسكندرية، دط، سنة2003

14. محمود أحمد قرعان، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، الأردن، ط1، سنة2017

15. مولود ديدان، قانون الإجراءات الجزائية، ، دار بلقيس، الجزائر، دط، ديسمبر2014

ثـالثا: البحوث والدراسات العلمية

1. بحث مقدم، الملتقي ألمغاربي حول القانون والمعلومات في إطار مواجهة الجريمة المعلوماتية في التشريع الجزائري، أكتوبر، سنة2004
2. بعرة سعيدة،الجريمة الإلكترونية في التشريع الجزائري، مذكرة مكملة من مقتضايات نيل شهادة ماستر في الحقوق، جامعة محمد خيضر،بسكرة دفعة2016/2015
3. عبد الله معيض العبيدي،الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)، رسالة ماجستر،تخصص سياسة جنائية جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، سنة2009
4. فرج ميسور،الجريمة الإلكترونية،مذكرة تخرج لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، قسنطينة، سنة 2014
5. لطروش فيروز، بن عزوز حاتم، الجريمة الإلكترونية في الجزائر من جريمة فردية إلى جريمة منظمة، مذكرة لنيل شهادة ماستر، جامعة عنابة، سنة 2015
6. محمد الدايج، الجريمة الإلكترونية في التشريع الجنائي الجزائري، مذكرة لنيل شهادة ماستر في الحقوق، جامعة مستغانم، سنة 2017/2016

رابعا: المراجع الإلكترونية

1- HTTP//DROIT.MOONTADA.COM/T622.TOPIC

2- HTTP//ESSALAM ONLINE.COM/ARA/PERMALINK

- WWW .ARABCIA.NET

3- WWW.ECHOROUK ONLINE.COM/ARA/ARTICLES

4-le traitement judicaire de la cybercriminalité guide méthodologique

ministère de la justice française

مـلخص المذكرة

تتحدث هذه الدراسة عن مفهوم الجريمة الإلكترونية، والسبل الكفيلة لمحاربتها، بتحديد حجم هذه الظاهرة ومعرفة العوامل المختلفة التي تتدخل فيها، وأهم المخاطر وهول الخسائر الناجمة عنها وهو الأمر الذي استلزم تدخل المشرع الجزائري من أجل التصدي لمثل هذه الظواهر ومعاقبة مرتكبيها .

الكلمات المفتاحية:1/ الجريمة الإلكترونية 2/ جريمة منظمة
3/ التحقيق 4/ المجرم المعلوماتي
5/ المعلوماتية 6/المشرع