جامعة محمد خيضر – بسكرة –

كلية الحقوق والعلوم السياسية

قسم الحقوق

الجريمة الالكترونية في التشريع الجزائري

مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق

تخصص: قانون جنائي

إعداد الطالبة:

بوحفص راوية

إشراف الأستاذة:

د.بوستة إيمان

السنة الجامعية:

2018/2017


بسم الله الرحمن الرحيم

﴿ قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا ۖ إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ﴾ ﴿٣٢﴾

الآية32 من سورة البقرة

﴿ ... وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلًا﴾ ﴿٨٥﴾

الآية 85 من سورة الإسراء

شكر وعرفان

أحمد الله حمدا يليق بجلاله وعظيم سلطانه على نعمته وعلى عونه لي في إنجاز هذا العمل المتواضع لعله يكون ثمرة جهدي البسيط

أتقدم بالشكر الجزيل إلى الذي أشرفت علي وتابعت هذا العمل بكل تواضع وصبر، فكانت الأستاذة بدروسها ونصائحها والأستاذة الفاضلة بسداد رأيها، إليها أسمى آيات التقدير والشكر.

الأستاذة الدكتورة

"بوستة إيمان".

كما لا يفوتني أن أشكر جميع أساتذتي الكرام

كلية حقوق خاصة وأساتذة جامعة محمد خيضر عامة

إهداء

إلى قلب ملاءته الطيبة و فاضت فيه وديان الود و الحنان إلى من جعل الله الجنة تحت أقدامها إلى ولذتي العزيزة أطال الله في عمرها

إلى أغلى هدية من عند الله إلى ذلك الذي دوما أنا محتاجة إلى أن أرتمي بين ذراعيه أبي الغالي أطال الله في عمره

إلى زوجي الغالي جمال الذي هو مصدر قوتي و سعادتي في الحياة أطال الله في عمره وكل عائلته الكريمة

إلى إخوتي الأعزاء إكرام أية حبيب عماد و كل فرد في عائلتي

إلى كل صديقاتي العزيزات الذين صادفتهم في مشوار حياتي

خاصة هناء إكرام أحلام رفيقة...

مقدمة

مقدمة:

إن التطور الذي يشهده عالمنا ويعيشه حاضرنا المتمثل في ظهور وسائل تكنولوجيا حديثة ومتطورة، بخاصة وما صاحبه من قفزة هائلة في مجال الاتصالات والانترنت، التي هي بمثابة موسوعة عالمية تقدم خدماتها لكافة المستفيدين في مختلف المجالات بحيث نتج عن الثورة التكنولوجية تلك ظهور نوع جديد من المعاملات تسمى بالمعاملات الالكترونية، حيث تختلف عن هذه المعاملات عن المعاملات التي نعرفها من حيت البيئة التي تتم فيها، نظرا لما يميز هذه الوسائل والشبكات من عنصري السرعة والدقة إلا أن هذا يبقي الجانب الايجابي لها فقط بحيث لا يمكننا نفي الانعكاسات السلبية التي أفرزتها هذه التقنية العالية المتمثلة في إساءة استخدام الوسائل الالكترونية والأنظمة المعلوماتية، وعدم استغلالها على نحو غير مشروع حيث أدى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجريمة اصطلح على تسميتها، الجريمة الالكترونية .

أهمية الموضوع:

وعليه يعد موضوع الجريمة الالكترونية من الموضوعات الهامة، التي باتت الحاجة لدراستها دراسة جيدة ومتائنية من قبل الباحثين و الدارسين القانون من الأمور الضرورية و الملحة في الوقت الراهن، ففي ضل تنامي معدلات الجريمة الالكترونية وانتشارها إما بالتعدي على المعلومة بالحذف أو التعديل او الحجب ...، وهو الأمر الذي دفعنا لإجراء دراستنا في هذا المجال القانوني.

أهداف الدراسة:

نظرا لتفشي الجريمة الالكترونية، في المجتمع وتزايدها وباعتبارها جريمة مستحدثة نسبيا، تهدف دراستنا الى توضيح والتعريف بها وتوصيفها وبيان خصائصها وتميزها عن الجريمة التقليدية من حيت المسرح و البيئة التي ترتكب فيها، فمرتكبيها ليسووا عاديين أنما يتمتعون

بمهارات فنية و تقنية لاسيما في مجال التكنولوجيات والشبكات، ولهذا سنت الدول و من بينها الجزائر مجموعة من القوانين والتشريعات للتصدي لها.

أسباب اختيار الموضوع:

إن اختياري لموضوع الجريمة الإلكترونية في التشريع الجزائري يرجع في حقيقة الامر إلى العديد من الأسباب بعضها شخصية وأخرى موضوعية.

أسباب الشخصية: هي الاهتمام بالاطلاع على هذا النوع من الجرائم المستحدثة بحيث لا يخفى علي أحد ما يشهده العالم من اعتداءات الواقعة بسبب هذه الجريمة وما خلفه هذا التطور التكنولوجي، وهذا ما جعله موضوع جديد ومواكب للحاضر.

أما الأسباب الموضوعية: فتكمن فيما يطرحه هذا الموضوع من إشكالات قانونية، ومدى مسايرة المشرع الجزائري لهذا الموضوع نظرا لحداثاته بتجريم اعتداءات الماسة بنظام المعالجة الآلية والقواعد الإجرائية الحديثة التي جاء بها قانون إجراءات الجزائية.[1]

وقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحاته، ومعرفة كيف تصدى المشرع الجزائر بالاعتداء على المعطيات في الجريمة الالكترونية وذلك بتعديل قانون العقوبات بإضافة القسم السابع مكرر، وكذا قواعد إجرائية من خلال تعديل قانون الإجراءات الجزائية، وقانون04/09.

الدراسات السابقة:

سوير سفيان، جرائم المعلومات، مذكرة ماجستير في العلوم الجنائية وعلم الاجرام2011/2010.

صالح شنين، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، رسالة دكتوراه في القانون،جامعة تلمسان،2013/2012.

[1] . الجمهورية الديمقراطية الشعبية، 22/06 مؤرخ في 20 ديسمبير2006، يعدل ويتمم الأمر 155/66 المؤرخ في 8 يونيو سنة 1966، المتضمن قانون إجراءات الجزائية الجريدة الرسمية عدد84، المؤرخ في 24 ديسمبر 2006.

سمية مزغيش، الجرائم المساس بالأنظمة المعلوماتية، مذكرة ماستر في الحقوق، جامعة بسكرة،2014/2013.

ولتسليط الضوء أكثر على الموضوع فالإشكالية الأساسية التي نطرحها تتمحور حول دراسة الجريمة الالكترونية ومدى مسايرة المشرع الجزائري لتطور وتشعب هذه الجريمة العابرة للحدود،و لذلك:

ما مدى مواكبة المشرع الجزائري لتطور الجريمة الالكترونية؟

وما هي الآليات الموضوعية و الإجرائية لمكافحتها و الوقاية منها؟

ويندرج تحت هذه الإشكالية إشكالات فرعية تتمثل في.

ما هي الخصائص التي ميزة الجريمة الالكترونية عن غيرها من الجرائم التقليدية؟

وما هي الأنواع التي تندرج من خلالها الجريمة الالكترونية؟

ما هي الأركان التي حدادها المشرع لكل شكل من أشكال الاعتداء في الجريمة الالكترونية؟ فيما تتمثل الجزاءات المقررة للجريمة الالكترونية في التشريع الجزائري؟ فيما تتمثل الخصوصية الإجرائية الجريمة الالكترونية ؟

ومن خلال هذا البحث سأحاول و بشكل مجمل تقديم صورة عامة عن الجريمة الالكترونية والعقوبات المقررة لها في التشريع الجزائري, وخصوصياتها من حيث الإجراءات. لهذا الأمر اتبعت المنهج الوصفي التحليلي نضرا لحداثة الموضوع وتشعبه، فالمنهج الوصفي يظهر من خلال قيامنا بوصف ظاهرة الجريمة الالكترونية، والمنهج التحليلي بحيث حولنا في هذا البحث شرح بعض المواد وتحديد بغض المفاهيم و الغوص في إجراءاتها.

ولقد حاولت حصر دراستي هذه ضمن خطة تتكون من فصلين، وكل فصل بيه مبحثين.

الفصل الاول يتمحور حول ماهية الجريمة الالكترونية و التي تتضمن الخصائص و كذا الانواع وبالإضافة الى الاشخاص مرتكبي الجريمة و دوافعهم.

أما الفصل الثاني فتناولت فيه الآليات الموضوعية من أركان وعقوبات وإجرائية من حيث التحقيق و المحاكمة.

الفصل الأول:
الإطار المفاهيمي للجريمة الإلكترونية

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية:

الجريمة الإلكترونية، جريمة حديثة نسبا، وذلك لارتباطها بتكنولوجيا متطورة وهي تكنولوجيا المعلومات، ونتيجة لحداثة هذه الجريمة فقد كانت هناك اتجاهات مختلفة في تسميتها فلم يتفق فقهاء القانون الجنائي في تحديد مصطلح دقيق، فمنهم من يطلق عليها الجريمة المعلوماتية ومنهم من يسميها جرائم الحاسب الآلي أو جرائم الكمبيوتر والإنترنت، ولقد كانت كذلك اتجاهات مختلفة في تعريفها، كما أنها اتسمت بمجموعة من الخصائص والسمات التي تميزها عن غيرها من الجرائم الأخرى، وكذلك للجريمة الإلكترونية طائفة جديدة من المجرمين تختلف عن الجرائم التقليدية، وعليه سوف ندرس في هذا الفصل مفهوم الجريمة الإلكترونية في المبحث الأول، وتصنيفات المجرم في الجريمة الإلكترونية.

المبحث الأول: مفهوم الجريمة الإلكترونية

إن التطور الذي يشهدها علمنا اليوم قد أوجد وسائل جديدة تسهل على الفرد حياته اليومية في مختلف معاملاته (الإقتصادية، التجارية، الاجتماعية ....) ومن انعكاسات الحاسب الآلي و الأجهزة الالكترونية بمختلف أنواعها أدى إلى طهور جرائم جديدة من بينها الجريمة الالكترونية كما يطلق عليها.

ومن خلال هذا المبحث سوف نحاول التطرق إلى تعريف الجريمة الإلكترونية وذلك في المطلب الأول، وكذلك إلى خصائصها في المطلب الثاني وإلى أهم أنواعها في المطلب الثالث.

المطلب الأول: تعريف الجريمة الإلكترونية

لقد اختلف الدارسون والفقهاء في إعطاء تعريف جامع مانع لهذا النوع من الجرائم الجريمة الإلكترونية، ففي مجال هذه الجريمة الناشئة من استخدام الحاسب الآلي أو الأجهزة الإلكترونية الأخرى، فمنهم من اعتمد في تعريفه على معيار الوسيلة، ومنهم من اعتمد على معيار موضوع الجريمة الإلكترونية، ومنهم من اعتمد على معيار التقنية وهناك اتجاه آخر اعتمد على جمع عدة معيار كأساس لتعريف الجريمة، وبذلك سنخص فرعا لكل معيار ونختمها بموقف المشرع الجزائري.

الفرع الأول: معيار الوسيلة

التعريفات التي انطلقت من الوسيلة التي ارتكبت بها الجريمة يرى أصحابها ان الجريمة الإلكترونية تتحقق باستخدام الكمبيوتر، ومن هذه التعريفات يعرفها الأستاذ جون فورستر وكذلك الأستاذ Ensiled. Ball أنها "فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ويعرفها تديماTiedemann بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا"[1].

[1] نسرين عبد الحميد نبيه، **الجريمة المعلوماتية والمجرم المعلوماتي**، منشأة المعارف، الإسكندرية، 2008، ص 58.

وكذلك تعرف على أنها "كل فعل أو امتناع من شأنه الاعتداء المادية أو المعنوية يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية" ولقد تبنيا هذا التعريف الأخير من قبل العديد من الباحثين والدارسين التي تحتوي على الطابع التقني الذي تتميز به الجريمة الإلكترونية[1].

ولقد تعرض هذا التعريف إلى عدة انتقادات، من بينها أنه الاعتماد على معيار واحد وهو الوسيلة المستخدمة فقط، بل تتطلب بقيام العمل الرئيسي أو الفعل الرئيسي المكون هما ولذلك لا يمكن أن يطلق على أي جريمة أنها من الجرائم الإلكترونية لمجرد استخدام الحاسب الآلي فيها كأداة أو وسيلة[2].

الفرع الثاني: معيار التقنية

يعتمد أنصار هذا الرأي أساسا على صفات أو سمات التي تكمن في شخص المجرم، أي على الشخص الذي يستخدم الحاسب لارتكاب هذه الجرائم، وهذا ما يميز الجريمة الإلكترونية عن الجرائم التقليدية، حيث أن الشخص المجرم في هذه الجريمة يتميز بصفة العلم والمعرفة التقنية، حيث لا يمكن أن ترتكب من شخص عادي ومن هذه التعريفات التي جاءت في هذا الصدد تعريف الفقيه: David. Chombson بأنها "أية جريمة يكون متطلبا لاقترافهما أن تتوفر لدى فاعلها معرفة بتقنية الحاسب" وكذلك تعريف A.SoLarz لها بأنها "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات" وعرفها آخرون بأنها: "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبة وللتحقيق فيه وملاحقته قضائيا"،وتعرفها وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفتها بأنها " أي جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها[3].

---

[1] فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، المؤتمر الدولي الرابع عشر الرابع عشر حول الجريمة الالكترونية، طرابلس، 2017، ص 4.

[2] عادل يوسف عبد النبي شكري، **الجريمة المعلوماتية والأزمة الشرعية الجزائية**، الجريمة المعلوماتية، جامعة كوفة، كلية الحقوق، العدد السابع، 2008، ص 113.

[3] يونس عرب، **إيجاز في المفهوم و النطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات**، مؤتمر الأمن العربي حول دليل أمن المعلوماتية و الخصوصية جرائم الكمبيوتر والإنترنت، أبو ظبي، 2002، ص 3.

ويعاب أيضا على هذه التعريفات أيضا، اعتمادها على شخص الجاني في تعريفها للجريمة الإلكترونية، ومدى امتلاكه لقدرات ومؤهلات لتعامل مع هذه التقنية المستحدثة، بحيث عند الرجوع إلى الواقع فإن هذه الجرائم ترتكب حتى من طرف شخص عادي غير مؤهل[1].

الفرع الثالث: المعيار الموضوعي :ومن بين التعريفات التي استندت على موضوع الجريمة أنها "نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقة"

وتعرف بأنها كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات" أو هي "نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات" أو هي "الجريمة الناجمة عن إحالة بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافية إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر"[2].

فالجريمة الإلكترونية حسب هذا الرأي هي التي تقع على الحاسب الألي أو داخل نظامه، بحيث أنهم لم يركزوا لا على الوسيلة المستخدمة ولا على توفر إمكانيات في الشخص لارتكاب هذه الجريمة[3].

لم يسلم هذا التعريف المعتمد على موضوع الجريمة من النقد، ولذلك قيل أنه وسع من نطاق هذه الجريمة، فهذه التعريفات لا تستند في الحقيقة إلى موضوع الجريمة بالمعنى القانوني، الذي هو محل الاعتداء فهي ركزت على نمط السلوك الإجرامي وأبرزتها متصلا بالموضوع لا بالموضوع ذاته[4].

---

[1] . نمديلي رحيمة، **خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة**، المؤتمر الدولي الرابع عشر حول الجريمة الالكترونية، طرابلس، 2017، ص 5.

[2]. نسرين عبد الحميد نبيه، مرجع سابق، ص ص 56، 57.

[3]. محمد خليفة ، **الحماية الجنائية لمعطيات الحاسب الألي** في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007، ص79.

[4]. نفس المرجع والصفحة

الفرع الرابع: أساس الجمع بين عدة معيار

يعتمد هذا المعيار على أكثر من معيار واحد، الأول هو محل الجريمة والثاني وسيلة ارتكاب الجريمة وفي كلا المعيارين الكمبيوتر أو الحاسب الألي دورا هاما حيث يعرفها الأستاذ .Thomrs.j.Smedinghsff بأنها "أي ضرب من النشاط الموجه **بصدد** أو المنطوي على استخدام نظام الحاسوب". وكذلك عمد أصحاب هذا الاتجاه إلى تعريف الجريمة عبر الأنترنت بأنها "الجريمة التي يستخدم فيها الحاسب الألي كوسيلة أو أداة لارتكابها أو تمثل إغراء بذلك بأنها، أو جريمة يكون الحاسب نفسه ضحيتها". وعرفت كذلك بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[1].

ومن الفقيه الفرنسي، يعرفها الفقيه Masse جريمة الكمبيوتر بأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الأرباح".

ويعرفها الفقهاء الفرنسيين Le stsnc.Vivant بأنها " مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب".

اتضح من خلال هذا التعريف الأخير أنه لا يتماشى مع المعيار القانوني، قد يكون صلح في نطاق العلوم الاجتماعية مثلا.

ورغم ما تعرض له هذا الاتجاه الذي جمع بين عدة معايير لتعريف الجرائم الإلكترونية، إلا أن هذا التعريف يعتبر الأنجح والأقرب من الناحية العلمية[2].

الفرع الخامس: موقف المشرع الجزائري من تعريف الجريمة الإلكترونية

بالرجوع إلى المشرع الجزائري نجده لم يعرف الجريمة الإلكترونية فالمشرع الجزائري اصطلح على الجريمة الإلكترونية تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك بموجب أحكام المادة 02 من القانون رقم 04/09 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام و الإتصال ومكافحتها[3]، على أنها "جرائم المساس بالأنظمة المعالجة الألية للمعطيات المحددة في قانون

---

1. نسرين عبد الحميد نبيه، مرجع سابق، ص ص 23،24 .

2. نمديلي رحيمة، مرجع سابق، ص 6.

3. الجريدة الرسمية للجمهورية الجزائرية،العدد47، المؤرخة في 05-08-2009 .

العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية".

ويمكننا أن نستخلص من خلال هذا التعريف أن المشرع الجزائري اعتمد عدة معايير لتعريف الجريمة الإلكترونية، منها معيار الوسيلة وهو نظام الاتصالات الإلكترونية، وكذلك معيار موضوع الجريمة وهو المساس بأنظمة المعالجة الألية للمعطيات، كما هو مبين في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر7[1]، حيث نجد أن المشرع ترك المجال واسع لأي جريمة ترتكب أو يسهل ارتكابها عن طريق الحاسب الألي أو نظام الاتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم حتى تلك الجرائم التي يكون للمنظومة المعلوماتية دورا فيها، وكذلك قد وسع في نطاق الجريمة كونها ترتكب في نظام معلوماتي[2].

المطلب الثاني: خصائص الجريمة الإلكترونية

تختلف وتتميز الجريمة الإلكترونية عن غيرها من الجرائم العادية أو التقليدية لان هذا النوع من الجرائم يرتبط بالحاسب الآلي أو تقنية المعلومات، وعليه سوف نتطرق إلى أهم سمات هذه الجريمة في الفرع الأول و سمات الخاصة ب المجرم في الفرع الثاني .

الفرع الأول: سمات الجريمة الالكتروني

وتتميز الجريمة الالكترونية بعدة خصائص أهمها.

أولا: عالمية الجريمة الالكترونية

مع ظهور شبكة الإنترنت أو الشبكة المعلوماتية كما يطلق عليها البعض أدى إلى تخطي كل فواصل والحدود الجغرافية وظهور ما يسمى بالفضاء لا منتهي أو العالم الافتراضي، وجعل العالم ككل قرية صغيرة، وهذا بدوره ما ساعدا على إضفاء صفة العالمية على الجريمة الإلكترونية وتميزها بالطابع الدولي في أغلب الأحيان حيث تكون آثار هذه

[1]. الجريدة السمية للجمهورية الجزائرية، العدد71،المؤرخة في 10 -11-2004.

[2] .نمديلي رحيمة، مرجع سابق، ص 6.

الأخيرة بتخطي حدود الدولة الواحدة، فنقل المعطيات أو البيانات التي تتم عن طريق الحاسب الآلي عبر شبكة الإنترنت فيمكن نقل كم هائل منها في بضع دقائق من دولة إلى أخرى أو عدة دول في آن واحد، وهذا ما سهل سرعة تنفيذ هذا النوع من الجرائم من جاني إلى مجني عليه تفصل بينهم مئات الكيلومترات ،وخاصة في المعاملات الإلكترونية التي تتم بين الأشخاص[1]

ثانيا: صعوبة إثبات واكتشاف الجريمة الإلكترونية

تتسم الجريمة الإلكترونية بصعوبة اكتشافها، لأن معظمها تتم في الخفاء ولا يلاحظها المجني عليه ولا يدري حتى بوقوعها ،حتى إنها لا تترك أثر في مسرح الجريمة وإن وجد فمن الصعب إثباته، فليس هناك شيء ملموس أو مادي فهي عبارة عن مجموعة من البيانات والمعطيات يتم تلاعب بها في عالم غير مرئي ونقل المعلومات عبر نبضات إلكترونية ،وما يزيد من صعوبات إثبات هذا النوع من الجرائم هي عدم إبلاغ الضحية أو المجني عليه.[2]

ثالثا: جريمة ناعمة و مغرية

الجريمة الإلكترونية على عكس الجرائم الأخرى لا تتطلب جهد عضلي في تنفيذها ،فهذه الأخيرة لا تكلف الجاني جهدا أبدا بل بضع دقائق وسوى أنامله لإتمامها، وإنما تحتاج منه توفر المعرفة بتقنية الحاسب الآلي أو الكمبيوتر ، والتعامل السليم مع شبكة الإنترنت ،ويتميز المجرم في هذه الجريمة بالتوافق مع المجتمع وأسلوبه الراقي في ارتكاب هذا النوع

---

1. سوير سفيان **جرائم المعلومات** .مذكرة ماجستير ،في العلوم الجنائية وعلم الإجرام ،كلية الحقوق والعلوم سياسية ،جامعة أبوبكر بلقاي تلمسان، سنة 2010، 2011 ص 20

-جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة**، دار البداية، الطبعة الاولى،عمان،2010، ص141.

2. مزيود سليم، **الجريمة المعلوماتية وواقعها في الجزائر وآليات مكافحتها**، المجلة الجزائرية للإقتصاد والمالية، جامعة المدية، العدد الأول، أفريل 2014ص120.

- محمد خليفة، مرجع سابق، ص34.

من الجرائم وتوفر لديه ثقافة عالية بهذه التقنية ، ويرتكب الشخص هذه الجريمة بدافع اللهو أو القرصنة أو تفوقه على الكمبيوتر أو لأجل مصلحة معينة ككسب الربح أو دافع الانتقام[1].

رابعا: جرائم فادحة الأضرار

أكدت دراسات الشركة العالمية المتخصصة في تقنيات حماية وآمن المعلومات " إنتل سكيور يتي" أن الخسائر التي كبدتها الجرائم الإلكترونية ضخمة، لاسيما أن الاعتماد على الحاسب الآلي في مختلف مجالات الحياة ،وبالأخص المجال الاقتصادي وإدارة المؤسسات المالية والبنوك و الشركات التجارية قد تؤدي إلى خسارة مبالغ مالية كبيرة بسبب هجوم إلكتروني واحد مقارنة مع الجرائم التقليدية[2].

خامسا: قلة الإبلاغ عن وقوع الجريمة الإلكترونية

لا يتم في الغالب الإبلاغ عن الجرائم الإلكترونية أو جرائم الإنترنت كما يطلق عليها البعض إما لعدم اكتشاف الضحية لها و إما خشية من التشهير ،ويعتبر هذا السبب هو الغالب ،حيث أن أغلب الجرائم الإلكترونية تم اكتشافها بصدفة، بل وبعد وقت طويل من ارتكابها، فرد على ذلك أن الجرائم التي اكتشفت كبيرة جدا إلا أن التي لم تكتشف أكبر وهو رقم خطير بالضرورة، وبعبارة أخرى أن الفرق بين عدد الجرائم الحقيقية وبين ما تم اكتشافه فرق كبير.[3]

الفرع الثاني: سمات الخاصة بالمجرم الإلكتروني

من أجل تحقيق الأهداف المرجوة من العقوبة، وجب التعرف على شخصية المجرم، أهم ما يميزه عن غيره من المجريمين حيث يتميز ب المهارة و الذكاء وأنه إنسان إجتماعي بطبعه

[1].فضيلة عاقلي، مرجع سابق، ص8.

[2]. محمد خليفة، المرجع السابق، ص38.

[3]. خالد ممدوح إبراهيم، **آمن الجريمة الإلكترونية**، الدر الجامعية، الإسكندرية، 2008، ص51.

أولا: المعرفة والمهارة والذكاء

تعني المعرفة التعرف على الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم و الكشف عنهم وتميز المعرفة بمفهومها السابق مجرما المعطيات ، حيث يستطيع المجرم ان يكون لديه تطورا كاملا عن الجريمة،كما يتمتع المجرم بقدر لا يستهان به من المهارة بتقنيات الحاسوب، وهذا ما يظهر من خلال العديد من القضايا[1]. حيث أن المجرمين لا يرتكبون إلا جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم فهم يجب أن يكونوا على إلمام كافي بمهارات فنية في مجال أنظمة الألي[2]، كما أنها من الجرائم التي تتطلب قدرا وافرا من الذكاء، ولا تحتاج إلى أدنى مجهود عضلي، ولا إلى سلوكيات مادية فيزيائية[3].

ثانيا: المجرم المعلوماتي إنسان اجتماعي

إن مرتكبي هذه الجرائم أفراد ذات مكانة في المجتمع ,وبتكيف المجرم مع مجتمعه تزيد ثقته بأنه خارج إطار الشبهات، وهذا الشعور يدفعه إلى تمادي في ارتكاب الجريمة فهي صعبة الاكتشاف كما وسبق أن قلنا، وإن اكتشفت فهي صعبة الإثبات[4]، كذلك نجد أن الذكاء يساعد على التكيف وما الذكاء في رأي الكثيرين سوى القدرة على التكيف، ولا يعني ذلك القليل من شأن هذا المجرم حيث تزداد خطورته الإجرامية كلما زاد تكيفه الاجتماعي، و

---

1. نائلة عادل قورة محمد فريد، **جرائم الحاسب الآلي الإقتصادية**، منشورات الحلبي الحقوقية، لبنان،2005، ص86

2. عبد العال الديربي، محمد صادق إسماعيل، **الجرائم الإلكترونية دراسة قانونية قضائية مقارنة**، المركز القومي، القاهرة 2012، ص57.

3 توح عبد الشاذلي، **أساسيات علم الإجرام والعقاب**، منشورات الحلبي الحقوقية، لبنان، 2009، ص144.

4. نائلة عادل قورة محمد فريد، مرجع سابق، ص97.

من جهة أخرى نجدهم لا يسعون إلى الحصول على منافع مالية، بل يكتفون بالتغافل بأنفسهم و أن يظهروا لضحاياهم ضعف أنظمتهم.[1]

المطلب الثالث: أنواع الجريمة الإلكترونية

ومن خلال هذا المطلب سوف نتطرق إلى أنواع الجرائم الإلكترونية الأكثر انتشارا، منها الجرائم الواقعة على الأشخاص وذلك في الفرع الأول والجرائم الواقعة على أمن الدولة في الفرع الثاني، والجرائم الواقعة على الملكية في الفرع الثالث.

الفرع الأول: الجرائم الواقعة على الأشخاص

لقد حمت مختلف التشريعات في قواعدها الدستورية الحياة الخاصة للفرد ،حيث أنه من الطبيعي لكل شخص حياة خاصة به وأسراره الشخصية التي لا يجوز الإطلاع عليها من غيره بحيث يمكنه أن يحتفظ بها في أي مكان يشأ ، وتكون الاعتداء عليها على الأشخاص في الجريمة الإلكترونية تلك المعلومات التي يتم الإعتداء عليها عن طريق الحاسب الآلي لشخص و الإطلاع على هذه المعلومات و الأسرار الموجودة في حاسب الشخص وهو جريمة قائمة في حد ذاتها بمجرد الدخول إلى نظام المعالج للمعلومات والإطلاع الغير المشروع على أسرار الشخص.[2]

ويكون كذلك الاعتداء على الأشخاص بالسب والقذف و التشهير والتحقير أو التهديد بالشخص عبر شبكة الإنترنت حيث يتم نشر أخبار أو معلومات صحيحة أو غير صحيحة أو مشوهة هذه إلى أشخاص آخرين بحيث يمكنهم الجاني بالإطلاع على المعلومات الخاصة بالمجني عليه على مواقع التواصل الاجتماعي أو البريد الإلكتروني.[3]

---

1. عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والانترنت في القانون النموذجي (دراسة متعمقة في مكافحة جرائم التقنية الحديثة)**، دار مونوجزفيك ، مصر، 2005، ص86.

2. خالد عيادي الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت**، دار الثقافة، عمان،2011 ص61.

3. نفس المرجع، و الصفحة.

وكذلك يمكن أن تكون عن طريق نشر الإباحة و الجنس سواء البالغين أو أطفال خاصة، و بحيث أن أكثر فئة معرضة للاستغلال الجنسي هي فئة الأطفال عن طريق الصور أو تسجيلات الفيديوهات الجنسية التي يستمر نشرها ونقلها من شخص إلى أخر عبر الأنترنت.[1]

الفرع الثاني: الجرائم الواقعة على الأموال

مع تزايد المعاملات الإلكترونية عبر شبكة الإنترنت أصبح البيع والشراء وكذا الإجار عبر هذه الأخيرة، والذي كان من نتاجه تطور وسائل الدفع و الوفاء، فوجدت وسائل السطو على المال بطريقة غير مشروعة كالتحويل الإلكتروني، السرقة، القرصنة حيث يتم سرقة المال من خلال اختلاس البيانات والمعلومات الشخصية للمجني عليهم، كدخول إلى حسابات المصرفية الخاصة بالعملاء في البنوك من قبل أحد الموظفين، وتحويل المال إلى حسابه ،وذلك باستخدام الجاني الحاسب الآلي و الإنترنت للوصول إلى المصارف والبنوك.[2]

وكذلك يدخل ضمن جرائم الاعتداء على الأموال في الجريمة الإلكترونية تجارة المخدرات عبر الأنترنت ،قرصنة البرمجيات وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية، وأيضا جريمة القمار عبر شبكة الإنترنت حيث وجدت لها كازينوهات افتراضية أو أندية القمار الافتراضي التي أصبحت فيها بعد مسرحا كذلك لجريمة غسيل الأموال.[3]

الفرع الثالث: جرائم ضد الملكية

يمكن أن يكون النشاط المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية والأدبية مثال ذلك استخدام النظام المعلومات في السطو على بنوك المعلومات التي

---

1. نمديلي رحيمة، مرجع سابق، ص9.

2. سورية ديش، **أنواع الجريمة الإلكترونية وإجراءات مكافحتها**، مجلة العلوم السياسية والقانون، جامعة جيلا لي ليابس، سيدي بلعباس، العدد الأول، 2017، ص 149.

3. نمديلي رحيمة، مرجع سابق، ص9.

تتضمنها برامج نظام معلوماتي أخرى أو حالة تخزين واستخدام هذه المعلومات أو التفريط فيها دون إذن من صاحبها، وذلك لأن استخدام معلومة معينة دون إذن من صاحبها يتضمن اعتداء على حقوق المعنوية إضافة إلى كونه اعتداء على قيمتها المالية كون أن المعلومة لمالها إضافة إلى قيمتها المادية كما يندرج أيضا ضمن الحقوق الفكرية كذلك براءات الاختراع باعتبارها تمثل فكرة المخترع تحتوي على حق معنوي وآخر مالي للمخترع.[1]

الفرع الرابع: جرائم ضد أمن الدولة

تعهد هذه الجرائم من اخطر الجرائم الإلكترونية خاصة الإرهاب المعلوماتي والجريمة المنظمة المعلوماتية، حيث تاحت الإنترنيت للكثير من المنظمات الإرهابية الترويج لأفكارها ومعتقداتها، وادت إلى ظهور جريمة أخرى أخطر منها التجسس الإلكتروني على الدول بالاطلاع على مختلف الأسرار العسكرية والاقتصادية بين الدول المتصارعة، كما تعطي الشبكة العنكبوتية فرصة للتأثير على المعتقدات الدينية وتقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة والمساس بأمنها داخلي وبنظامها العام.[2]

[1]. أحمد خليفة الملط، **الجرائم المعلوماتية** ،الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص184.

[2]. نمديلي رحيمة، مرجع سابق، ص9.

المبحث الثاني: مرتكبو الجريمة الإلكترونية

أصبحت الوسائل الإلكترونية حيز اساسي في الحياة اليومية للفرد ويرجع ذلك إلى التطور المستمر في مجالات الحياة التي تدخل ضمن مختلف الأنشطة الإقتصادية أو العلمية أو التجارية وغيرها، ومن نتائج المعاملات الإلكترونية بين الأشخاص العادين أو الذين يزاولن أنشطة تجارية أو صناعية في أساليب مستحدثة هذا أدى إلى ظهور مجرم إلكتروني يرتكب هذا النوع من الجرائم عكس المجرم التقليدي والذي سنتطرق إليه في المطلب الأول وأسباب انتشار هذا النوع من الجرائم في المطلب الثاني .

المطلب الأول: تصنيفات مرتكبو الجريمة الالكترونية

الإجرام التقليدي يتسم بالعنف وهو الوسيلة الوحيدة لاقتراف الجريمة وهذا ما يعكس شخصية المجرم أنه مجرم عنيف، عكس الإجرام الإلكتروني الذي يتسم بالنعومة وعدم بدل جهد كما سبق وإن نكرنا في خصائص هذا النوع من الجرائم حيث أن هناك فئات مختلفة ويطلق عليهم مجرمي التقنية حيث قسمت هاته الفئات .

الفرع الأول: طائفة المخترقون أو المتطفلون Crackers & Hackers

ويعرف المتطفلون بأنهم مجموعة من الناس الذين يحاولون التسلل إلى الحاسبات الإلكترونية أو الإنترنت لفرض إثبات مقدرتهم أو تحديهم أو لمجرد المزاج، وليس لغرض الكسب المادي كهدف أساسي،[1] فالمتطفلون أو الماكرون يتوفر لديهم في الغالب دوافع حاقدة ،بل لديهم دافع إثبات قدرتهم في اختراق المواقع والدخول الغير مشروع إلى تلك المواقع أو حجبها، حيث أن أفراد هذه الطائفة يرتكبون جرائم التقنية بدافع التحدي الإبداعي، ويتميز أغلب أفراد هذه الطائفة بأنهم صغار السن أو قليلي خبرة في المعرفة التقنية وبرغم من هذه الصفات فقد تمكن المجرمون من هذه الطائفة من اختراق مختلف أنواع نظم الكمبيوتر التابعة للشركات المالية والتقنية والبنوك والمؤسسات الحكومية ...الخ

1. قصعة خديجة ،جمال بن زروق، **تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الإلكترونية في العالم**، مجلة تاريخ العلوم، جامعة الجلفة، العدد السادس، 2015 ص249.

وتتميز هذه الطائفة بتبادل المعلومات فيما بينهم و إطلاع بعضهم البعض على مواطن الضعف في نظام الكمبيوتر والشبكات، وتكمن خطورة هؤلاء في إمكانية توفر فرصة استغلالهم من قبل منظمات وهيئات إجرامية تسعى للكسب المادي، وكذلك يمكن استغلالهم في جانب إجابي وهو مساهمتهم في تطوير الأمن في المؤسسات والقطاعات العامة والخاصة ،وتطوير خبراتهم في فحص و تدقيق مستوى أمن نظام الكمبيوتر.[1]

الفرع الثاني:طائفة محترفو الجرائم الإلكترونية

هؤلاء الأشخاص الذين يحترفون ارتكاب الجرائم الإلكترونية يتميزون بالتعسف وذات خطورة خاصة وسبب في ذلك ارتكابهم جرائم من نوع تقنية العالية، التي لا يرتكبها سوى أشخاص ذو مهارة عالية، من جهة وغموض شخصية مرتكبيها من جهة أخرى، ويتراوح أعمار هذه الفئة ما بين 25إلى 45 سنة، وتمثل هذه المرحلة من العمر مرحلة النضج حيث تزامن هذا النضج مع انتشار الوسائل الإلكترونية و التقدم التكنولوجي، ويكون أغلب مرتكبي هذه الأفعال من محلل والمبرمج و شخص يعمل في المنشأة ما أو مسؤول عن أنظمة معلوماتية، فهم يملكون المعرفة اللامة و التقنية الكافية للتلاعب بالحاسبات الآلية.

فقد أكدت دراسات من علماء النفس على عينة من شخصيات مرتكبي هذه الأفعال الغير مشروعة لديهم اتجاه إجرامي خطير ونية سيئة مثلا أعمال الجنس، حيث يقومون بتنفيذ أفعال أنفسهم أو بمشاركة أشخاص أخرين سواء كانوا فنين أو مجرد وسطاء واغلبهم يشغلون مراكز قيادة هامة، ويتمتعون بثقة كبيرة في مجال عملهم، بحيث يطلق عليها جرائم ذوى الياقات البيضاء وذلك لتشابه الكبير بينهم حيث أن هؤلاء ومن ذوى التخصصات العليا وقدرة من الذكاء.[2]

---

1. نسرين عبد الحميدة نبيه، مرجع سابق ص199, ص120.

– محمد علي الصريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2004، ص 64.

2. سامي على حامد عياد، **الجريمة المعلوماتية و إجرام الأنترنت**، دار الفكر الجامعي، الإسكندرية،2007، ص54.

الفرع الثالث: طائفة الحاقدون

تختلف هذه الطائفة عن الطائفتين السابقتين فهم لا تتوفر لديهم إثبات قدرة التغلب على التقنية وإثبات المهارة ولا يسعون إلى مكاسب مادية أو سياسية، بل يتوفر لديهم دافع الانتقام والثأر،حيث يتسم أفراد هذه الطائفة بقلة خبرة في مجال التقنية إلا أنهم يسعون بكافة الوسائل والطرق من آجل الوصول إلى غايتهم وهي لانتقام عن طريق هذه الأخيرة، ومن الوسائل التي يستعملونها وهي نشر الفيروسات والبرامج الضارة وتخريب وإتلاف النظام في كل أو بعض من معطياته، لم يحدد العمرية بشأنهم ،ونجد أن هذه الطائفة عكس طائفة الهاركز الذين يشهرون بالأعمال التي قاموا بها فهؤلاء يتعمدون إخفاء أعمالهم الإجرامية، كذلك أن هذه الطائفة تعد أقل خطورة من غيرها من مجرمي التقنية، وهم الطائفة الأسهل من حيث الكشف الأنشطة التي قاموا بارتكابها ولكن يمكننا القول أن بعض الأنشطة التي قاموا بها قد خلفت خسائر فادحة في بعض الأحيان.[1]

المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية

ويقصد بالدافع الباحث أو الغاية من ارتكاب الجريمة ويصطلح عليها في القانون الجنائي القصد الجنائي، وترتكب الجريمة الإلكترونية لعدة دوافع منها دوافع شخصية أو خارجية وهنا إلى أخرى خاصة بالمنشأة،وعليه سوف نتطرق لكل من هذه الدوافع كل فرع على حدى.

الفرع الأول: الدوافع الشخصية

ترتكب الجريمة الإلكترونية من طرف بعض الأشخاص نتيجة إحساسه بالقدرة على اختراق النظام فيندفع تحت رغبته القوية في تحقيق الذات ومن أجل تأكيد على قدرته الفنية على ارتكاب أحد جرائم الكمبيوتر،[2] كاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية

[1]. نسرين عبد الحميدة نبيه، مرجع سابق ص123.

[2] . محمد أمين الرمي، **جرائم الكمبيوتر والأنترنت**، دار المطبوعات الجامعية، الإسكندرية،2003، ص24.

المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبها وتسلية تغطي أوقات فراغه كذلك قد يكون الدافع وراء ارتكاب الجرائم الإلكترونية هو الرغبة في قهر الأنظمة الإلكترونية و التغلب عليها، إذ يميلوا إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة،كذلك يدخل ضمن الدوافع الشخصية الرغبة في تحقيق مكاسب مادية تكون هائلة في وقت زمني قصير جدا وهو من أكثر البواعث التي تؤدي إلى المجرمين على اقتراف جرائمهم ، حيث يتم ارتكاب هذا النوع من الجرائم عن طريق اختلاس من جهاز الحاسوب و استعمال بطاقة سحب إلى مزورة أو منتهية الصلاحية.[1]

الفرع الثاني: الدوافع الخارجية

قد يتأثر المجرم المعلوماتي ببعض المواقف قد تكون دافعة له على اقترافه للإجرام المعلوماتي، و لا يسعى في ذلك حينها لا للمتعة لا للتسلية ولا لتحقيق الربح ، وتمكن أهم الدوافع الخارجية بالشخص إلى الانتقام و إلحاق الضرر برب العمل، حيث لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل، يتعرضون على نحو كبير لضغوطات في نفسية ناجمة عن ضغط العمل و المشكلات المالية من طبيعة العمل المنفردة في حالات معينة وهذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح ،ولكن في حالات كبيرة أن القوة المحركة لبعض العاملين لارتكاب جرائم الحاسوب، باعتها الانتقام من المنشأة أو رب العمل، حيث يقومون مثلا بجرائم إتلاف البيانات أو محوها كذلك العبث بالبرامج،[2]وهناك أمثلة كثيرة كان دافع الجناة فيها إشباع الرغبة بالانتقام، وعلى سبيل المثال أن شاب يعمل محاسب في مؤسسة ما فقرر التلاعب في برامج الكمبيوتر الخاص بتلك الشركة التي يعمل بها، بحيث برمجة على أن تختفي كل البيانات الخاصة بديون الشركة بعد

1. نهلا عبد القادر المومني، **جرائم المعلوماتية**، دار الثقافة، عمان، 2008، ص ص90-92.
2. نسرين عبد الحميد نبيه، مرجع سابق ص130.

فوات ستة أشهر من تاريخ تركه للعمل ، وحدث ذلك بعد تركه للشركة بستة أشهر حذفت كل البيانات نهائيا على جهاز الكمبيوتر.[1]

الفرع الثالث: دوافع أخرى

الدوافع السابقة التي ذكرها من دوافع شخصية المتمثلة في الرغبة في تحقيق الربح أو إثبات قدرة التغلب على النظام ،ودوافع خارجية المتمثلة في الانتقام من رب العمل و إلحاق ضرر به تعد هي أبرز الدوافع ،ولكن ليست هي الوحيدة بل هناك دوافع أخرى لارتكاب هذا النوع من الجرائم المتمثلة في:

التنافس العسكري و الاقتصادي قد يكون دافعا رئيسيا كاختراق الأنظمة الحكومية والقيام بسرقة معلومات حساسة من أجهزة، الحواسب الخاصة بدولة ما، وقد يكون كذلك الدافع السياسي أو الإيديولوجي سبب في ارتكاب الفعل الإجرامي، بحيث وجدت بعض المجموعات تطلق على نفسها مجموعات الكراهية على الأنترنت تزدري كل القيم الدينية و الأخلاقية والاجتماعية وبصفة خاصة تلك المرتبطة بالأسرة، وهناك بعض من مواقع الإلحاد التي تطلب بإلغاء الدين والدولة والأسرة وتحرير الإنسان من تلك القيود.[2]

1. محمد أمين الرومي، مرجع سابق، ص ص24 25.

2. نهلا عبد القادر المومني، مرجع سابق، ص 93.

خلاصة الفصل الأول:

وعليه لقد تناولنا في هذا الفصل تعرف الجريمة الإلكترونية وأبرز المعيار التي اعتمدت في تعريفها للجريمة الإلكترونية، وكذلك لموقف المشرع الجزائري من تعريفها حيث أنه لم يعرفها بل اكتفى بالدلالة عليها بمصطلح المساس بأنظمة المعالجة الألية للمعطيات وتحديد أركانها في المطلب الأول، أما في المطلب الثاني فقد تناولنا أهم خصائص الجريمة والتي تتميز وتختلف عن الجرائم التقليدية، وأهم أنواع هذه الجريمة من حيث أنها قد تمس الأشخاص أو تكون ضد حكومة أو ملكية .....أخرى.

أما في المبحث الثاني فقد تعرفنا على الأشخاص الدين يرتكبون هذا النوع من الجرائم ومميزاتهم في المطلب الأول أما المطلب الثاني قد جاء فيه أهم الأسباب الدافعة لارتكاب هذه الجرائم و اللجوء إليها .

الفصل الثاني:
الأليات الموضوعية و الاجرائيةللجريمة الإلكترونية

الفصل الثاني: الآليات الموضوعية والإجرائية في الجريمة الإلكترونية

يتسم عصر المعلوماتية بازدياد الاعتماد على شبكات أجهزة الحواسب والإنترنت، مما يجعلها أكثر انفتاحا على المجتمع ونتيجة لهذه التطورات التكنولوجية ظهرت أنواع جديدة من الجرائم، والتي يمكن تسميتها بجرائم الحاسب الآلي أو الجرائم الإلكترونية ومن هنا فقد اتجهت جل التشريعات وأغلب الدول إلى وضع نصوص قانونية خاصة في هذا الشأن، أما بالنسبة للمشرع الجزائري ومسايرة منه لهذا التطور فقد أصدر مؤخرا نصوصا تجرمية للحد من الاعتداءات الصادرة ضد الأنظمة المعلوماتية، وذلك بموجب القانون رقم 04-15 المتضمن تعديل قانون العقوبات و عليه سوف نتطرق في هذا الفصل إلى أشكال وصور الاعتداء في الجريمة الإلكترونية وهذا في المبحث الأول، كذلك إلى خصوصية الجزائية و الإجرامية في الجريمة الإلكترونية وذلك في المبحث الثاني.

المبحث الأول: أشكال الاعتداء في الجريمة الإلكترونية

نتيجة لظهور الإجرام المعلوماتي أبرمت العديد من الاتفاقيات التي تجرم هذه الأفعال، وهو الأمر الذي دفع بالدول إلى سن تشريعات داخلية من أجل مكافحة هذا النوع من الإجرام، منها التشريع الجزائري حيث قام بتعديل قانون العقوبات وذلك بإضافة القسم السابع مكرر من الفصل الثالث الخاص بالجنايات و الجنح، تحت عنوان "المساس بأنظمة المعالجة الألية للمعطيات " من أجل المحافظة على سرية وسلامة المعطيات، وقد حدد من هذا النص ثلاثة جرائم من خلال المواد 394 مكرر الى مكرر 7 والتي سنتطرق إليها في كل مطلب :المطلب الأول يتناول جريمة الدخول و البقاء والمطلب الثاني جريمة الاعتداء القصدي على النظام و المطلب الثالث جريمة الاعتداء على المعطيات.

المطلب الأول: جريمة الدخول أو البقاء في النظام

لقد نص المشرع الجزائري على هذه الجريمة في نص المادة 394 مكرر وسبق التطرق لذكرها في تمهيد المبحث حيث نجد المشرع الجزائري جرم كل فعل دخول أو بقاء في كل أو جزء من النظام المعلوماتي، و انطلاقا من نص المادة أنه ولقيام هاته الجريمة لابد من توفر ركنين أولهما الركن المادي وذلك ما سنتطرق إليه في الفرع الأول و ثاني الركن المعنوي وذلك ما سنتطرق إليه في الفرع الثاني.

الفرع الأول : الركن المادي

وعليه يتضح أن لهذه الجريمة صورتين لركنها المادي، فهناك صورة بسيطة لفعل الدخول والبقاء الغير المشروع و هناك صورة مشده بفعل الدخول و البقاء غير مشروع.

أولا: الصورة البسيطة لجريمة الدخول إلى النظام أو البقاء فيه

وعلية سوف نتعرف على الصورة البسيطة لكل من الدخول و البقاء

1- **فعل الدخول:** يرى الفقه الفرنسي أن الدخول له مدلول معنوي ، حيث يشبه الدخول إلى النظام بمثابة الدخول إلى ذاكرة الإنسان، كما له مدلول مادي يتمثل في آن الشخص قد يكون حاول الدخول إلى النظام المعلومات، فلدى يتحقق هذا الأخير بأي صورة من صور التعدي، أي أن كان التعدي مباشرا أو غير مباشر فهو يتساوي.

كذلك نجد أن المشرع لم يحدد وسيلة الدخول إلى النظام، فإنه يمكن الدخول بأي وسيلة كانت، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها أو باستخدام برنامج أو شفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص أخر أو الدخول من خلال شخص مسموح له بالدخول.[1]

وتقع هذه الجريمة من أي إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم لا علاقة له بذلك أو يستطيع الاستفادة منه أم لا، ويشترط أن يكون من الذين لهم الحق في الدخول في هذا النظام، ويكون الدخول في مشروع كذلك متى كان مخالفا لإرادة صاحب النظام، كتلك الأنظمة المتعلقة بأسرار الدولة أو دفاعها، أو ما تعلق بحرمة الحياة الخاصة، وكذلك يتحقق بدخول الجاني إلى النظام كلة أو جزء منه حيث، أنه يكون مسموح له بالدخول إلى جزء معين في برنامج فيتجاوز إلى جزء أخر غير مسموح له بالدخول فيه، ولذلك يخرج من نطاق الدخول غير مشروع الدخول إلى برنامج منعزل عن نظام المعلومات التي حظر عليه الدخول فيه، كما أن الجريمة لا تقوم إذا اقتصر دور الجاني على مجرد قراءة الشاشة دون الولوج إلى داخل النظام،

[1]. عبد الفتاح بيومي حجازي، **التجارة الإلكترونية و حمايتها القانونية**، دار الفكر الجامعي، الإسكندرية 2004، ص ص28،29.

وعليه يتضح من خلال كل ما قدم أنه يتحقق الدخول الغير مشروع بمجرد تعدى الجاني إلى ما هو غير مسموح له الدخول أو الإطلاع عليه، أما إذا كان الولوج في دائرة ما هو مسموح به فهنا لا يمكننا التحدث عن قيام جريمة الدخول الغير مشروع.[1]

2- **فعل البقاء:** ويقصد بفعل البقاء " التواجد داخل نظام المعالجة الألية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام " حيث أن الركن المادي لفعل البقاء يتحقق بأن يظل الجاني باقي داخل النظام بعد المدة المحددة له داخله أو في حالة التي يضع فيها نسخة من المعلومات في الوقت الذي كان له مسموح له فيه الرؤية و الإطلاع فقط، ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، والتي يستطيع فيها الجاني الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو حصل على خدمة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل غير مشروعة.[2]

إذا اتجهت إدارة الجاني إلى البقاء داخل هذا النظام على الرغم من معرفته أنه غير مصرح له بالدخول، لاختلف عن الدخول الغير مصرح به إلى نظام الكمبيوتر، فالنتيجة الإجرامية فيكلا الحالتين واحدة وهي الوصول الى نظام غير مصرح للدخول إليه، فالمصلحة التي يهمها القانون هي نظام الكمبيوتر.[3] وقد يجمع الدخول غير المشروع معا وذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، تم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الإجماع المادي بين الجريمتين، ويكفي لقيام هذه الجريمة البقاء داخل النظام كله أو في جزء منه.[4]

وعليه يطرح الدكتور مسعود خثير الإشكالية التي تنور في هذا الصدد متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؟

---

1. خثير مسعود، **الحماية الجنائية لبرامج الكمبيوتر (أساليب وثغرات)**، دار الهدى، الجزائر، 2010، ص ص115-117.

2. عبد الفتاح بومي حجازي، **التجارة الالكترونية وحمايتها القانونية**،الكتاب الثاني، مرجع سابق، ص31.

3. خثير مسعود ، مرجع سابق ص117.

4. أمل قارة ،**الحماية الجزائية للمعلوماتية في التشريع الجزائري**، الطبعة الأولى، دار هومة، الجزائر ،2008، ص110.

ولقد اختلفت الآراء الفقهية حول هذا الموضوع حيث أن هناك رأي من الفقهاء يرون أن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج ويبقى مدة قصيرة من الزمن داخله، وبعد تلك اللحظة تبدأ جريمة البقاء وتنتهي بانتهاء حالة البقاء.[1]

حيث يؤخذ على هذا الرأي أنه لا يحدد لحظة بداية الجريمة البقاء بطرقة حاسمة،لهذا ذهب رأي أخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه المتدخل أن بقاءه داخل النظام غير مشروع، ويؤخذ على هذا الرأي أيضا صعوبة إثبات على المتدخل.

فالرأي لأصوب وراجح هو ما ذهب إليه فريق من الفقهاء في اعتبار أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام، أو يستمر في التجول بداخله يعد إنتهاء الوقت المحدد، لأن الفرض يتعلق بدخول غير مشروع أي مع علم الجاني أنه ليس له الحق في الدخول، فإذا دخل وظل ساكن تعتبر جريمة دخول ، أما إذا بدأ بالتجول تعتبر جريمة بقاء داخل النظام.[2]

ثانيا :الصور المشددة

وقد نص عليها المادة394 مكرر3/2 من قانون العقوبات[3]، وهو طرفين تشدد بهما عقوبة جريمة الدخول و البقاء داخل النظام كما يتضح من النص، حيث يتمثل هذان الطرفان

– عندما ينتج عن الدخول أو البقاء في عدم صلاحية النظام لأداء وظائفه، بحيث أنه إذا توفر هذا الظرف المشدد تكون هناك علاقة سببية بين الدخول و البقاء الغير مشروع وجود نتيجة ضارة[4].

وقد تكون النتيجة ضارة غير مقصودة، حيث إذا أنبت الجاني انتقاء العلاقة السببية بين السلوك الإجرامي والنتيجة الإجرامية كأن يحدث إلى التعديل أو المحو أو عدم صلاحية

---

[1]. خثير مسعود، نفس المرجع، ص117.

[2]. أمل قارة، مرجع سابق، ص112، 113.

[3] بنصها على ما يلي:"تضاعف العقوبة إذا ترتب على ذلك حذف أو تغير لمعطيات المنظمة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000دج إلى دج 150000."

[4] حابت أمال ، **التجارة الإلكترونية في الجزائر**،رسالة دكتوراه في العلوم الجنائية جامعة تيزي وزو ،كلية الحقوق و العلوم السياسية ،2015،ص 393.

النظام للقيام بوظائفه يرجع إلى قوة حاجة عن إدارة الجاني و حادث مفاجئ ينتفي بذلك السلوك الإجرامي وبذلك ينتفي القصد الجاني[1].

الفرع الثاني: الركن المعنوي

تعتبر هذه الجريمة جريمة الدخول أو البقاء من الجرائم العمدية حيث يتعين لقيامها توافر القصد الجنائي العام لدى الجاني بعنصريه العلم و الإرادة،[2] بحيث أن الجاني هنا يعلم أنه قد دخل إلى نظام ليس له حق الدخول فيه وكذلك يتعمد البقاء فيه، حتى ولو كان الدخول مشروع ومدة البقاء متجاوزة المدة المستحقة فهنا تكون جريمة و إما إذا إنتقى عليه فهنا لا تقوم جريمة[3].

[1] خثير مسعود،مرجع سابق، ص119.

[2]. عبد الفتاح بيومي حجازي،**التجارة الالكترونية وحمايتها القانونية**، مرجع سابق، ص37.

[3]. خثير مسعود، مرجع سابق، ص118.

المطلب الثاني: جريمة الاعتداء القصدي على النظام.

Atteintes nolotmtaires au fonctionnement de STAD

لقد نصت على هذا الشكل من الاعتداء المادتين 05و 08 من الاتفاقية الدولية للإجرام المعلوماتي، في حين أن المشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدى على سير النظام، واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام ،ويمكن رد ذلك لكون أن المشرع الجزائري قد أعتبر أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه،[1] وذلك من خلال نصه في الفقرة من المادة الثانية من القانون 09-04 على أن برامج سير نظام المعالجة الألية للمعطيات تدخل ضمن المعطيات المعلوماتية.[2]

وقد وقع الفقه معيارا للتفرقة بين الاعتداء على المعطيات والاعتداء على النظام على أساس ما كان الاعتداء وسيلة أم غاية، فإذا كان الاعتداء مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدى على النظام، أما إذا كان الاعتداء غاية فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات.[3]

على غرار المشرع الجزائري نجد أن المشرع الفرنسي قد نص عليها، وذلك بموجب نص المادة 2/323: "يعاقب كل من عطل أو أفسد نشاط أو وظائف المعالجة الألية للمعطيات بالحبس حتى ثلاثة سنوات وبالغرامة حتى ثلاثمائة ألف فرنك".[4]

وعلية سوف نتطرق في هذا المطلب الركن المادي في الفرع الأول و الركن المعنوي في الفرع الثاني.

---

[1]. أمل قارة، مرجع سابق، ص114

[2]. تنص الفقرة ج من المادة 02 من القانون 09-04 في تعريفها للمعطيات المعلوماتية بأنها:"أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة معلوماتية تؤدي وظيفتها."

[3]. أمل قارة، مرجع سابق، ص114.

[4]. ختير مسعود، مرجع سابق، ص120.

الفرع الأول: الركن المادي

ويتمثل السلوك المادي في هذه الجريمة أما في فعل التوقيف أو تعطيل النظام المعالجة الألية للمعطيات عن أداء نشاطه ، و أما في فعل الإفساد النشاط أو وظائف هذا النظام، ويكفي أن يكون فعل الإيقاف أو الإفساد على جزء من نظام الحاسوبي أو أحد أجهزته المادية لكي يعد سلوك مجرم.[1]

أولا: التعطيل أو التوقيف وتتمثل هذه العملية في إعاقة سير عمل نظام المعالجة الآلية للمعطيات، وقد يؤثر على عمل النظام بتباطؤه أو ارتكابه بحيث تأثر على أجهزة الكمبيوتر والبرامج على سواء، بحيث يحصل عمل التعطيل أو التوقيف بأي وسيلة كانت مثل كسر أحد أجهزته أو تحطيم أسطوانة، أو قطع شبكة الاتصال بأي وسيلة مادية، أما الإعاقة أو التعطيل بوسيطة معنوية يتمثل في إدخال فيروس عن البرامج، أو تعديل أو تغير كلمة السر أو تغير كيفية عمل النظام.[2]

ثانيا: الإفساد أو التعيب" ويقصد بالإفساد هنا كل فعل وإن كان لا يؤدي إلى التعطيل ،يؤدي إلى جعل نظام المعالجة الألية للمعطيات غير صالح للاستعمال السليم وذلك بأن بعض نتائج غير تلك التي كان من الواجب الحصول عليها". [3]

تتنوع وسائل التعيب أو الإفساد مثل استخدام القنبلة المعلوماتية التي يدخل عن طريقها مجموعة معطيات تتكاثر داخل النظام تجعله غير صالح للاستعمال، كذلك استخدام حصان الطروادة البرنامج الذي يقوم بتغير غيره محسوس في المعطيات أو البرامج، وتوجد الكثير من الفيروسات التي تغير في مخرجات النظام ،يمكن أن يتحقق الإفساد عن طريق إتلاف أو تخريب العناصر المادية للنظام.[4]

---

[1]. أمل قارة، مرجع سابق، ص115.

[2]. مسعود ختير،،مرجع سابق، ص115.

[3]. أمل قارة، مرجع سابق، ص119.

[4].نفس المرجع، و الصفحة.

الفرع الثاني: الركن المعنوي

تعتبر جريمة الاعتداء القصدي على النظام المعالجة الألية للمعطيات من الجرائم العمدية، بحيث أن الركن المعنوي فيها يتوفر على قصد جنائي بعنصرين العلم والإرادة بحيث تتجه إرادة الجاني إلى فعل الإفساد أو الإيقاف أو التعطيل مع علمه بأن نشاطه الإجرامي من شأنه أن يوصله إلى تلك النتيجة أو، وعليه إذا قام شخص وتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة خطأ في التشغيل أو التعامل مع تلك البيانات ينتفي قصده الجنائي ولا تقوم الجريمة في حقه.[1]

المطلب الثالث: جريمة الاعتداء العمدي على المعطيات

نجد أن المشرع الجزائري جرم هذا الفعل الاعتداء على المعطيات ليس ليحمي نظام البيانات من الناحية المادية أي البرامج والتطبيقات ، بل ليوفر الحماية للمعلومات الموجودة داخل النظام ذاته ضد أي نشاط إجرامي ، حيث نص المشرع الجزائري على هذه الجريمة من خلال نص المادة 394 مقرر 1 من قانون العقوبات.[2]

وعليه تناولنا في هذا المطلب الركن المادي و الركن المعنوي كل على حدى.

الفرع الأول: الركن المادي

ويأخذ الركن المادي في هذه الجريمة ثالثة صور ويكفي توفر أحدها لقيام الجريمة، بحيث لا يشترط اجتماعها معا حيث يتوفر النشاط الإجرامي بحيث تشترك هذه الأفعال في انطوائها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل أخر، وعليه فإن الاعتداء على المعطيات في نظام المعالجة ، أي البيانات التي أدخلت لمعالجتها وتحولت إلى معطيات عبارة عن رموز أو إرشادات تمثل تلك المعلومة، أي بيانات تمت معالجتها أي الجريمة تقع على المعطيات إلى البيانات التي تمت معالجتها، دون المعلومة ذاتها، بحيث أن المعلومة التي لم تعالج بصد لا تدخل ضمن نطاق الجريمة، كذلك يخرج من نطاق الجريمة المعلومات التي انفصلت عن النظام وسجلت على شريط أو قرص مدمج لأنها أصبحت خارج النظام، بحيث أن المشرع

---

[1]. ختير مسعود، مرجع سابق، ص122.

[2]. عبد الفتاح بيومي حجازي، **التجارة الإلكترونية و حمايتها القانونية**، ص ص44، 55.

هنا يحمي المعلومات المعالجة داخل النظام أو تلك التي في طريقها للمعالجة بأن اتخذت خطوة أو أكثر في مراحل معالجتها، أو المعلومة التي انفصلت عن النظام ثم أعيد إدخالها.[1]

وعليه سوف نبين فيما يلي المقصود بالأفعال المكونة لهذه الجريمة، مع العلم أنه لا يشترط لقيامها توفر كل هذه الأفعال بل يكفي لقيامها توفر فعل واحد كما وسبق وأن ذكرنا:

أولا : فعل الإدخال

ويقصد بفل الإدخال إدخال بيانات في نظام المعالجة لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات يقصد التشويش على صحة المعلومات الموجودة كالفيروسات، وغالبا ما تقع بمعرفة المسؤول عن القسم المعلوماتي، الذي يسند إليه وظائف المحاسبة والمعاملات المالية، حيث يكون هذا المسؤول في أفضل وضع يؤهله لارتكاب هذا النمط الغير مشروع من التلاعب، ومن أهم هو إدخال المعلومات المصطنعة اختلاس النقود عن طريق الغش المعلوماتي، وعليه يمكن لأي شخص يشغل مركزا في إحدى المنشات أو البنوك من القيام بما يشاء من أفعال غير مشروعة.[2]

ثانيا: فعل المحو

ويقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة الموجودة داخل النظام، أو تحطيمها، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

ثالثا: فعل التعديل

ويقصد بالتعديل تغير المعطيات الموجودة داخل النظام، واستبدالها بمعطيات أخرى ويتحقق هذا الفعل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو تعديلها، وذلك باستخدام برنامج الممحاة أو برامج الفيروسات بصفة عامة[3].

---

[1]. خثير مسعود، مرجع سابق، ص124.

– عبد الفتاح بيومي حجازي، **التجارة الإلكترونية وحمايتها القانونية**، ص ص46 47.

[2]. أمال قارة، مرجع سابق، ص122.

[3].نفس المرجع، والصفحة.

الفرع الثاني: الركن المعنوي

من خلال إستقراء نص المادة 394 مكرر 1 من قانون العقوبات المعدل و المتمم، يتبين أن جريمة التلاعب بمعطيات الحاسب الآلي هي جريمة عمدية يتخذ فيها ركن المعنوي صورة القصد الجنائي العام بعنصرية العلم والإرادة، فيكفي أن يعلم الجاني بأن نشاطه غير مشروع، وتتجه إرادته إلى فعل الإدخال أو المحو أو التعديل بهدف تغيير المعطيات.[1]

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجاني العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بصاحب النظام، بل تتوفر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي، لا أنه ليس عنصرا في الجريمة،[2] أي أن الجريمة لا تتطلب قصد جنائي خاص.

[1]. محمد خليفة, مرجع سابق, ص186.

[2]. خثير مسعود, مرجع سابق,ص125.

المبحث الثاني: آليات الجزائية والإجرائية للجريمة الإلكترونية

لقد نصت المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي بموجب أن تكون العقوبة المقررة نتيجة ارتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات سالبة للحرية كما نصت على وجوب تطبيق عقوبات على الشخص المعنوي بناء على مبدأ له مساءلته الشخص المعنوي الوارد في المادة 12 من نفس الاتفاقية، وهذا ما سنطرف إليه في المطلب الأول وما هي العقوبات التي نص عليها المشرع الجزائري لمعاقبة الشخص المعنوي والطبيعة كذلك عقوبة الاتفاق او المشروع في الجريمة الإلكترونية.

أما في المطلب الثاني سوف نتناول خصوصية الجرائم الإلكترونية من حيث الإجراءات التي تختلف عن الإجراءات المتبعة في الجرائم التقليدية.

المطلب الأول:الجزاءات المقررة للجريمة الإلكترونية

لقد نصت المواد الخاصة في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات الجزائري، من المادة 394 مكرر إلى 394 مكرر7 نجد أن المشرع الجزائري قد أقر جزاءات واجبة التطبيق عن هذا النوع من الجرائم، فمنها عقوبات تطبيق على الشخص الطبيعي وكذلك عقوبات تطبق على الشخص المعنوي وذلك ما سنتناوله فيما يلي:

الفرع الأول: العقوبات المطبقة على الشخص الطبيعي

من خلال هذا الفرع سوف نذكر العقوبات الأصلية و التكميلية للشخص الطبيعي.

أولاً: العقوبات الأصلية المطبقة على كل جريمة

ولهذه الجرائم الدخول و البقاء و التلاعب وكذا التعامل الغير مشروع عقوبات وهي كالأتي:

1-الدخول والبقاء:

أ- الدخول والبقاء بالغش(الجريمة البسيطة): تنص المادة 394 مكرر من قانون العقوبات المعدل و المتمم، على العقوبة المقررة هي الحبس 3 أشهر إلى سنة وغرامة مالية قدرها 50.000دج إلى 100.000دج.

ب- الدخول والبقاء بالغش(الجريمة المشددة): تنص المادة 394 مكرر فقرة 02و 03 من قانون العقوبات المعدل والمتمم تضاعف العقوبة التي ترتكب عن هذه الأفعال حذف أو تغيير لمعطيات العقوبة من06 أشهر إلى سنتين وغرامة من 50.000دج إلى 150.000دج.

2- جريمة التلاعب بالمعطيات

نصت عليها المادة 394 مكرر 1من قانون العقوبات المعدل و المتمم، حيث يعاقب بالحبس من 06 أشهر إلى 03 سنوات وبغرامة مالية تتراوح من 500.000دج إلى 2.000.000دج، كل من أدخل بطريقة الغش معطيات في نظام المعالج آلية أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها.

ويلاحظ أن عقوبة التلاعب بالمعطيات تفوق جريمة الدخول والبقاء غير المصرح بهما سواء كانت هذه الاخيرة في صورتها البسيطة أو المشددة لأن في صورتها البسيطة، لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو بالنظام معالجتها وحتى صورتها المشددة، وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي الإزالة أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجاني بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشددة[1].

[1]. نائلة عادل محمد فريد قورة، مرجع سابق، ص 228.

3-جريمة التعامل في معطيات غير مشروعة.

تعاقب المادة 394 مكرر5 من قانون العقوبات المعدل و المتمم، على جريمة التعامل في المعطيات غير مشروعة بعقوبة الحبس من شهرين إلى 3سنوات وبغرامة مالية من 1.000.000دج، إلى 5.000.000دج، بهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول والبقاء غير المصرح بهما سواء في صورتها البسيطة أو المشددة وبين جريمة التلاعب بالمعطيات (غير أن حدها لأدنى يقل عن كلتا الجريمتين).

ذلك أن حدها الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء في صورتيها (سنة أو سنتين) وتتساوى مع الحد الأقصى لجريمة التلاعب بالمعطيات (3سنوات)، غير أن حدها الأدنى يقل عن الجريمتين معاً، لأنه في جريمة الدخول أو البقاء البسيطة 3 أشهر وفي هذه الجريمة في صورتها المشددة وفي جريمة التلاعب وفي جريمة التلاعب هو 6أشهر.[1]

ثانيا: العقوبات التكميلية

نصت المادة 394 مكرر6 من قانون العقوبات المعدل و المتمم، على العقوبات التكميلية، التي يمكن الحكم بها إلى جانب العقوبات الأصلية وجاء فيها مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادر الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها هذا القسم علاوة على إغلاق المحل أو مكان الاستعمال إذا كانت الجريمة قد ارتكبت بعلم مالكها ويستخلص من نص هذه المادة العقوبات التكميلية التالي:

1- مصادر الأجهزة والوسائل والبرامج المستخدمة، وذلك مع الاحتفاظ بحقوق الغير حسن النية، وتجدر الإشارة إلى أن المشروع نص فقط عل مصادرة الأجهزة والبرامج والوسائل المستخدمة فقط وأغفل مصادرة الوسائل الموجهة لارتكاب الجريمة من المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الألية للمعطيات المنصوص عليها في الفقرة الأولى من المادة394 مكرر2 قانون العقوبات الجزائري، حيث أن عبارة "المستخدمة" الواردة في نص المادة 394 مكرر6

[1]. محمد خليفة مرجع سابق, ص219.

الخاصة بالعقوبات التكميلية تفيد صيغة الماضي وهذا ما نصت عليه المادة 394 مكرر6 من قانون العقوبات الجزائري التي تنص على العقوبات الجزائري التي تنص على العقوبات التكميلية، في فقرتها الثالثة على المصادرة فنجد أنها تناولت مصادرة الشيء الذي كان موجهاً للقيام.[1]

2- إغلاق المواقع التي تكون محلاً للجريمة من جرائم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

3- إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها وإضافة المشرع على المالك، ويعلم هذه الأخير خطورة الأفعال التي يقوم بها الجاني، كغلق نادي الإنترنت الذي ترتكب فيه هذه الجرائم ولكن المشرع لم يحدد المدة القصوى لغلق المحل أو مكان الاستغلال وهذا ما يطرح مشكلة في تنفيذ هذه العقوبة فمن جهة يعتبر إغلاق المحل كعقوبة تكميلية للشخص الطبيعي المسؤول جزائيا، ومن جهة أخرى لا يمكننا الرجوع إلى القواعد العامة للمسؤولية الجزائية للشخص المعنوي لتحديد المدى، وعليه يمكن توقيع جزاء خاص بالشخص المعنوي غلق المحل على الشخص الطبيعي.

فالعقوبة التكميلية الواردة في المادة 394 مكرر6 من قانون العقوبات الجزائري غير كافية في مواجهة الحالات العديدة التي يمكن أن يرتكبها الشخص الطبيعي فمثلاً تنص المادة على العقوبة التكميلية الخاصة بالموظف العمومي المصرح له بالدخول على النظام الآلية للمعطيات لكنه يبتعد ذلك أي ارتكاب جرائم أخرى متعلقة بالمنظومة المعالجة آلياً، وكذلك الشيء نفسه فيما يخص المحامين أو الأطباء إذا ارتكبوا جرائم أثناء تأدية مهامهم فإنهم يعاقبون بالعقوبات التالية:

-المنع لمدة أقصاها 5سنوات من الحقوق السياسية والمدنية

- المنع لمدة أقصاها 5سنوات من ممارسة الوظيفة العمومية أو النشاط المهني أو الاجتماعي إذا ارتكب الجريمة أثناء تأدية الوظيفة

[1]. أحسن بوسقيعة، **الوجيز في القانون الجزائري الخاص**، الجزء الأول، دار هومة، الجزائر، طبعة التاسعة، 2008، ص448.

– مصادرة الشيئي الذي أستخدم أو الموجه لارتكاب الجريمة أو عدة مؤسسات مقاولة التي استعملت في ارتكابها الأفعال المجرمة.[1]

ثالثا: الظروف المشددة

نصت المادة 394 مكرر فقرة2 و03 من قانون العقوبات المعدل و المتمم، على ظرف التشديد عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا الظرف عندما ينتج عن الدخول أو البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

– في الحالة الأولى تضاعف العقوبة المقررة في الفقرة الأولى من المادة 394 مكرر وفي الحالة الثانية تكون العقوبة الحبس ستة(6) أشهر إلى سنتين(5) والغرامة من 50.00دج إلى 150.00دج

هذا الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافر الجريمة.

نصت المادة 394 مكرر3، على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام.[2]

الفرع الثاني: العقوبات المطبقة على الشخص المعنوي

نصت المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي على أنه يسال الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلاً أصلياً أو شريك أو متدخلاً، كما يسأل عن هذه الجريمة التامة أو الشروع فيها بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه، هذا مع الإشارة إلى أن المسؤولية الجزائية للشخص المعنوي

1. أحسن بوسقيعة، مرجع سابق، ص149

2. نص المادة 394 مكرر 3" ضاعف العقوبات المنصوص عليها في هدا القسم، إدا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات اشد"

لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.[1]

كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائرية للشخص المعنوي وذلك من خلال نص المادة 18 مكرر من قانون 15،04 المتضمن قانون العقوبات.

وقد نصت المادة 394 مكرر 4 من قانون العقوبات أن عقوبة الشخص المعنوي الذي يرتكب إحدى الجرائم الماسة بالأنظمة المعلوماتية هو الغرامة التي تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.[2]

الفرع الثالث: عقوبة جريمة الاتفاق والشروع الجنائي

أ- عقوبة الاشتراك، حيث نصت عليه المادة 394 مكرر05 من قانون العقوبات المعدل و المتمم، إذ جاء فيها أن "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسداً بفعل أو عدة افعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

ويلاحظ من خلال هذا النص أن المشرع الجزائري لم يخرج عن القواعد العامة لعقوبة الشريك، حيث رصدهما نفس عقوبة الجريمة التامة، حيث أن الإشراك في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية يتمثل في كون أن مثل هذه الجرائم يتم عادة في إطار مجموعة، كما أم المشرع أراد توسيع نطاق العقوبة فأخضع الأعمال التحضيرية بالعقوبة المقررة للجريمة التي تم التحضير ها إذا تمت في إطار اتفاق جنائي، بمعنى آخر أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.[3]

ب- أما المشروع فنصت عليه المادة 11 من الاتفاق الدولية للإجرام المعلوماتي وتبناه المشرع الجزائري في المادة 394 مكرر7 قانون العقوبات المعدل و المتمم، فالجرائم الماسة

---

[1]. سوير سفيان، مرجع سابق، ص100.

[2].نفس المرجع،والصفحة.

[3]. أمال قارة، مرجع سابق، ص130.

بالأنظمة المعلوماتية لها وصف جنحة و يعاقب على الشروع في الجنح ،حيث نصت هذه المادة "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها."

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة تشمل اكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ لعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة. وعليه تضح المشرع الجزائري بهذا المنطلق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي.[1]

المطلب الثاني: الخصوصية الإجرائية في الجرائم الإلكترونية

بعد التطرق إلى الأفعال المكونة للجريمة الإلكترونية وأركانها والجزاءات المقررة لها سوف نعالج في هذا الفصل الآليات القانونية في مفهوم أصول التحقيق الجنائي في الجزائر الإلكترونية بما فيها جمع الأدلة والتفتيش وجمع الاستدلالات، وطرق متابعيها بما فيها الانتقال والمعاينة.

وذلك تماشياً مع مواد القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والذي يسمح باستعمال وسائل قانونية جديدة تتلاءم وخصوصية هذا النوع من الجرائم إضافة إلى الأشخاص المخولين قانونا لكيفية إثبات الجريمة لضباط الشرطة القضائية، والجهات المختصة جزائياً.

بحيث تناولت في الفرع الأول خصوصية الجرائم الالكترونية من حيث المتابعة والتحقيق والفرع الثاني من حيث المحاكمة.

الفرع الأول: خصوصية الجرائم الإلكترونية من حيث المتابعة والتحقيق

يقوم ضباط الشرطة القضائية والنيابة العامة بإجراءات المتابعة فور تلقي بلاغ أو دعوى عن وقوع جريمة الالكترونية، مع التحقيق في هذه الجرائم وكل ما لهم صلة بالموضوع محل البلاغ جمع الاستدلالات من خلال الانتقال والمعاينة والتفتيش وتلقي المراسلات ....، وهذا ما سيتم التطرف إليه من إجراءات المتابعة لضباط الشرطة القضائية، والتحقيق

1. آمال قارة، المرجع السابق،ص133

أولاً: خصوصيتها من حيث إجراءات المتابعة

إن لضباط الشرطة القضائية دور فعال في ضبط أدلة الجرائم ومرتكبيها وكشف كل ما يتعلق بها حالة وقوعها، أما بالنسبة للجرائم المستحدثة فإنها تلق المزيد من الأعباء على عاتق هذه السلطة، وكذلك الأمر بالنسبة للسلطات القضائية، وذلك نظراً لضعف خبرة كلا منهما في مواجهة هذه الجرائم، فمن المتصور أن يجد ضباط الشرطة القضائية أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات غير التقليدية من هذا النوع من الجرائم، وقد يفشل جهاز الضبط القضائي في تقدير أهمية الجريمة نظراً لنقص الخبرة والتدريب ولهذه الأسباب كانت أوليات السياسة الوطنية لمكافحة الجرائم المتصلة بتكنلوجيا الإعلام والاتصال تكوين وتأهيل سلك ضباط الشرطة القضائية وأعوانهم.[1]

فلقد أستحدث المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام ومكافحتها بموجب قانون رقم09-04 المتعلق بالوقاية من جرائم الاتصال والمعلومات ومكافحتها في المواد 13 و14 من هذا القانون وتتولى هذه الهية وفقا للمادة14 تنشيط وتنسيق عمليات بالوقاية من جرائم الإيصال والمعلومات ومكافحتها، ومساعدة السلطات القضائية، وأيضا تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل مفيد في التعرف على مرتكب الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم، كما أنشأت الجزائر مركز لمكافحة جرائم الإنترنت على مستوى الدرك الوطني في إطار مسايرتها للتطور التكنلوجي وما يصحبه من أنواع جرائم الإنترنت.[2]

ثانيا: خصوصية الجريمة الإلكترونية من حيث التحقيق

من الصعب التحقيق في الجرائم الإلكترونية بسبب تعقيداتها يستوجب الإلمام بأمور تقنية بحتة، تختلف الطرق العادية في مجال التحقيق وتوجيه الأسئلة والإسفسارات بحيث

---

1. عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي**، دار شتات للنشر والبرمجيات، مصر، 2000، ص232.

2. صلاح شنين، **الحماية الجنائية للتجارة الالكترونية**، دراسة مقارنة، رسالة دكتوراه في القانون الخاص، جامعة تلمسان،2012-2013، ص ص، 231-232.

تكون واقعية وذات مصداقية وهذا ما يجعلها ذات طبيعة خاصة، وهذا ما سنتناوله في ما يلي:

أولا: المعاينة

يجب على عضو الضبط القضائي في حدود اختصاصه إذا أخبر عن جريمة مشهودة أو اتصل عمله بها انتقال إلى مكان الجريمة كمعاينتها، وبدون إفادة المجني عليه ويسأل المتهم عن التهمة المسندة إليه، وربط كل ما يظهر أنه استعمل في ارتكاب الجريمة ويعاين آثارها المادية ويحافظ عليها ويثبت حالة الأشخاص والأماكن، وكل ما يفيد في اكتشاف الجريمة، وعند انتقال إلى محل الجريمة المشهودة عليه أن يمنع الحاضرين من مبارحة محلا لواقعة أو الابتعاد عنها، وعليه أن يحضر في الحال كل شخص يمكن الحصول منه على إيضاحات.[1] حيث أجمع أغلب الفقهاء بأنها إثبات حالة الأماكن والأشخاص،وكل ما يفيد في كشف الحقيقة عن الجريمة ومرتكبها.[2]

فالمعاينة من إجراءات التحقيق الابتدائي، حيث يجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة، وأهمية المعاينة عقب وقوع الجريمة من الجرائم التقليدية، حيث يتوجب المسرح الفعلي للجريمة أن يحتوي على آثار مادية فعلية، يهدف القيام بالمعاينة إلى التحفظ عليها تمهيدياً لفحصها، لبيان مدى صحتها في الإثبات، وهو ليس الحال في الجرائم الإلكترونية، حيث تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض آثارها إلى المحو أو التلف أو العبث به.[3]

ثانيا: التفتيش

لقد أجاز المشرع الجزائري تفتيش المنظومة المعلوماتية بموجب المادتين 45و47 من القانون رقم 22/06 المعدل والمتمم لقانون الإجراءات الجزائية إذ تنص المادة 45 أنه لا

---

1. محمد م صالح شنين، نفس المرجع، ص 232.

2. محمد مروان، **نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري**، جزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999،ص343.

3. صالح شنين، نفس المرجع، ص232.

يشترط حضور المشتبه فيه صاحب المسكن إذا تعلق الأمر بالتفتيش عن الجرائم المعلوماتية باستثناء الأحكام المتعلقة بالحفاظ على السر المهني وكذلك جرد الأشياء وحجز المستندات.
كما نصت المادة 47 من قانون العقوبات عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإنه يجوز إجراء التفتيش في كل محل كني أو غير سكني في كل ساعة من ساعات الليل أو النهار وذلك بناء على إذن مسيق من وكيل الجمهورية المختص.

– كذلك سمح المشرع الجزائري في المادة05 من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالدخول في منظومة معلوماتية بفرض التفتيش ولو عن بعد، وذلك في الحالات المنصوص عليها في المادة4.[1]

ويعرف التفتيش في اللغة، بأنه البحث عن مكان وجود شيء ما إما اصطلاحا، هو البحث عن شيء في مستودع سر،أما فقهاً، فقد تعددت التعريفات منها: هو إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن او الشخص، وذلك من أجل إثبات ارتكابها أو نسبتها إلى متهم،وفقا للإجراءات القانونية المقررة .[2]

وذهبت محكمة النقض إلى تعريفه أنه البحث عن الحقيقة في مستودع سر فيها.[3]

1– ضوابط التفتيش الإلكتروني

أن البحث عن الحقيقة لا ينبغي أن يكون طليقاً من كل قيد، لم يجب أن يخضع لضوابط معينة، وعليه يجب أن يخضع التفتيش في النظام المعلوماتي لضوابط أو لشروط منها موضوعية وأخرى شكلية سوف نتطرق إليها بإيجاز:

---

1. الحالات المنصوص عليها في المادة 04 هي: الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

2. طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتى النظام القانوني للحماية المعلوماتية**، دار الجامعة الجديدة، الإسكندرية،2009، ص ص364-367.

3. نفس المرجع، ص367.

أ- الضوابط الموضوعية

-وقوع جريمة الكترونية: والجريمة الإلكترونية هي كل فعل غير مشروع مرتبط استخدام الحاسوب.[1]

- تورط شخص أو أشخاص معينين في ارتكاب الجريمة الإلكترونية أو الإشتراك فيها: أي يجب أن تتوفر في شخص ما المراد تفتيشه دلائل كافية بأنه ساهم في إرتكاب جريمة كشريك أو فاعل أصلي.[2]

- توفر إمارات قوية أو دلالات على وجود أشياء أو أجهزة أو معدات إلكترونية تفيد في كشف الحقيقة لدى المتهم[3].

- أن يكون محل التفتيش هو لحاسوب بكل مكوناته المادية والمعنوية وشبكات الإتصال الخاصة به: بالإضافة إلى الأشخاص الذين يستخدمون الحاسوب محل التفتيش.[4]

ب- الضوابط التشكيلية

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

- أن يكون الامر بالتفتيش مسبباً: أي يجب أن يتضمن أمر التفتيش الأسباب التي أدت بالنيابة العامة إلى إجراء التفتيش.

- تشكيل فرقة التفتيش في الجرائم الإلكترونية تكون متخصصة بشكل ممتاز في مجال الحاسب الالي و الأنظمة الإلكترونية، وخبراء تقنيين وفنيين[5].

ثالثا: ضبط الدليل الرقمي

مم لا شك فيه أن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي تم الحصول عليها أثناء، فالضبط هو العثور على الأدلة الخاصة بالجريمة التي يباشر التحقيق

---

[1]. خالد عياد الحلبي، مرجع سابق، ص153.

[2]. عبد الله هلالي، **التفتيش في نظام الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة**، دار النهضة العربية، القاهرة 2006، ص120.

[3]. خالد عياد الحلبي، مرجع سابق، ص154

[4]. نفس المرجع، والصفحة.

[5]. نفس المرجع،ص ص153 155.

بشأنها والتحفظ على هذه الأدلة، والضبط هو الغاية من التفتيش ونتيجته المباشرة[1]، فقد اقرر المشرع الجزائري بآليات خاصة لحجز المعطيات الجريمة الإلكترونية وهذا ما نصت عليه المادة6 من قانون 04/09 بقولها: "عندما تكتشف السلطة التي تباشر التفتيش في المنظومة معلوماتية معطيات مجزئة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأمه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون قابلة للحجز ....."، بحيث أن المشرع أجاز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل المعطيات المبحث عنها من أجل جعلها قابلة لاستعمال الأغراض التحقيق بشرط ان لا يؤدي ذلك إلى المساس بمحتوى المعطيات.[2]

كذلك أقر المشرع الجزائري بموجب المادة 7 من القانون 04/09 "إذا استحال إجراء الحجز وفقاً لما هو منصوص عليه في المادة6 من نفس القانون، لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال تقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها الموصولة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".

وعليه نجد أن المشرع الجزائري قد أجاز بموجب المادة47 من قانون الإجراءات الجزائية الجزائري الضبط أو الحجز في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في محل سكني أو غير سكني، وفي كل ساعة من ساعات الليل أو النهار، إذن مسبق من وكيل الجمهورية المختص.

هناك بعض الإجراءات الفنية و الاستثنائية التي يجب مراعاتها في الجريمة الإلكترونية.

– تصوير الحالب الأجهزة المتصلة به وتسجيل وقت وتاريخ ومكان التقاط الصورة.

– العناية بملاحظة الطريقة التي تم بها إعداد النظام،والكابلات المتصلة بكل مكونات النظام.

---

1. محمد سعيد نمور، **أصول الإجراءات الجزائية شرح لقانون أصول المحاكمة الجزائية**، الطبعة الأولى، دار الثقافة ، الأردن، 2005، ص359.

2. المادة 6فقرة 3 من القانون 04/09 المتعلقة بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنلوجيا والإعلام والاتصال ومكافحتها.

– عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء الاختبارات للتأكد من خلو المحيط الخارج للموقع الحاسب من أي مجال لقوة مغناطيسية يمكن أن يمحو البيانات المسجلة.

– التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، ورفع البصمات ذات الصلة بالجريمة.

– التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

– ضرورة قصر عملية المعاينة على أعضاء الضبط القضائي ممن تتوفر فيهم الكفاءة العملية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات.

وتجد الإشارة إلى أن المشرع الجزائري أجاز المعاينة في الجرائم المعلوماتية المتلبس فيها في المادة 3/47، والتي تنص على آلية عندما يتعلق الأمر بجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإنه يجوز إجراء المعاينة في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك على إذن مسبق من وكيل الجمهورية المختص.[1]

الفرع الثاني: خصوصيتها من حيث المحاكمة

أن قواعد القانون الجنائي تخضع في تطبيقها من حيث المكان لمبدأ الإقليمية الذي يعني خضوع الجرائم التي تقع بإقليم الدولة معينة لقانونها، بحيث تصبح محاكمها هي صاحبة الولاية بنظر للدعوى الناشئة عنها، ويتحد الاختصاص المحكمة بمكان وقوع الجريمة أو إقامة المتهم أو القبض عليه، نجد أن المشرع الجزائري أخذ بإقليمية، القوانين و ذلك في نص المادة 3 من قانون العقوبات الجزائري، على أنه" يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أرضي الجمهورية الجزائرية كما تطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقاً لأحكام قانون الإجراءات الجزائية".

[1]. صالح شنين، مرجع سابق، ص233.

أولا: من حيث الاختصاص المحلي

تنص المادة 02/37 من قانون الإجراءات الجزائية، على أنه يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف[1]، كما أن المشرع أراد أن يواكب سياسة التخصص والنظر لوجود جرائم تحتاج إلى أقطاب قضائية لمعالجة جرائم معينة من بينها الجرائم الماسة بنظام المعالجة الآلية للمعطيات.

ولقد صدر مرسوم تنفيذي رقم 348/06 المؤرخ في 12 رمضان عام 1425هـ الموافق ل05 أكتوبر 2006، وقد أجاز المشرع تمديد الاختصاص بإصداره لهذا المرسوم الذي يعالج الأقطاب القضائية المختصة في هذه الجرائم التي يتمدد الاختصاص المحلي لها، ولقد نصت المادة 1 على تطبيق الأحكام في مواد 37و40و329 من الأمر 66-155 المتضمن قانون الإجراءات الجزائية.[2]

ثانيا: من حيث الإختصاص النوعي

لقد تم تعديل قانون الإجراءات الجزائية بموجب القانون 06-23 الصادر في2006/12/20 المتضمن قانون الجرائيةا الجزائية وجاء بإجراءات خص بها ضباط الشرطة القضائية وأعوانهم في مرحلة البحث والتحري تحت إشراف وكيل الجمهورية المختص.

وهذا تماسكاً مع الإجراءات الخاصة بالاختصاص النوعي والمحلي وكيل الجمهورية، أو قاضي التحقيق عندما يتعلق الأمر بالاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات كالتالي:

---

[1]. هو المرسوم التنفيذي رقم348/06 المؤرخ في 05أكتوبر 2006، الجريدة الرسمية،العدد63 مؤرخة في 2006/10/18، المتضمن تمديد الاختصاص المحلي لبعض المحاكم والوكلاء الجمهورية وقضاة التحقيق

[2].أنضر نص المادة،37 و40 و329، من الأمر 66-156، المؤرخ في 18 صفر 1386هـ، الموافق ل 1966/06/08، المتضمن قانون الإجراءات الجزائية.

أصبح اختصاص أعوان وضباط الشرطة القضائية يمتد إلى كامل الإقليم الوطني بموجب التعديل الأخير لقانون الإجراءات الجزائرية من خلال المادة 07/16، أما فيما يخص عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يعمل على الاشتباه فيهم بإركاب الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، وكذلك مراقبة وجهة أو نقل الأشياء أو الأموال أو المتحصلات من ارتكاب هذه الاعتداءات او التي قد تستعمل في ارتكابها وبعد إخبار وكيل الجمهورية المختص إقليمي وإن يتعرض،يتم تمديد الاختصاص لكافة الإقليم الوطني لضباط الشرطة القضائية تحت سلطتهم وأعوان الشرطة القضائية [1] ويخبر ضباط الشرطة القضائية فوراً وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويبلغونه بأصل ونسختين من إجراءات التحقيق الابتدائي، ويرسل هذا الأخير النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة التي مدد اختصاصها، وهذا ما نصت عليه المادة 40 مكرر1 من قانون الإجراءات الجزائية، ويطلب النائب العام طبقا للمادة 40 مكرر2 بالإجراءات فوراً إذا أعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة 40 مكرر من قانون الإجراءات الجزائية.

[1]. انظر المرسوم التنفيذي، رقم 06-338، المؤرخ في 5-10-2006،الجريدة الرسمية، العدد63 المؤرخة في 18-10-2006.

خلاصة الفصل الثاني:

تعرفنا في هدا الفصل إلى أشكال الاعتداء في الجريمة الإلكترونية و أركان كل جريمة على حدى بالتفصيل التي تمثل في جريمة الدخول والبقاء الغير مشروع في نظام المعالجة الألية للمعطيات وجريمة الاعتداء العمدي على سير النظام، وكل هذا في المبحث الأول.

أما المبحث الثاني فلقد تطرقنا إلى خصوصية الجريمة الإلكترونية من حيث الجزاءات المقررة الجرائم الاعتداء الماس بالأنظمة المعلوماتية التي نصت عليه قانون 15/04 معدل ومتمم لقانون العقوبات ابتداء من المواد394 إلى غاية 394 مكرر بما فيها عقوبات المطبقة على الشخص المعنوي و الشخص الطبيعي .

كذلك تناولننا خصوصية هذه الجريمة من حيث الإجراءات التي تختلف من حيث طبيعتها عن الإجراءات المتبعة في الجرائم التقليدية من المعاينة و التحقيق، يستوجب على ضباط الشرطة القضائية أن يكون على خبرة عالية في مجال التقنية كذلك من خلال منح صلاحيات من اختصاص محلي ونوي موسعا للقضاة والمحققين.

خاتمة

لقد أضحى العالم اليوم يعيش في زمن ساده تطور تكنولوجي أو ما يسمى بالثورة المعلوماتية حيث أصبحت حياتنا اليوم تستدعي اللجوء إليها فقد مكنت الوسائل الإلكترونية المجتمعات من تجاوز فكرة الحدود السياسية، نظر للإمكانيات المتاحة أمامها، لكن مع هذا التطور قد أرتبط به تطور هذا النوع من الجرائم وذلك نتيجة سواء استخدم هذه الوسائل .

ولقد حاولت من خلال الفصل الأول الوقوف على الإطار المفاهيمي للجريمة الإلكترونية و ذلك بالتعرف على أهم التعريفات المختلفة و أراء الفقهاء حول تحديد المعيار التعريف في الجريمة، ثم الخصائص التي تتميز بها الجريمة الإلكترونية عن غيرها، و أهم أنواع هذه الجريمة، كذلك من هم الأشخاص الذين يرتكبون هذا النوع من الجرائم، و الأسباب الدافعة لارتكابها .

أما في الفصل الثاني فقد تناولنا جل المواد المتعلقة بأحكام الموضوعية الخاصة أشكال الاعتداء في الجريمة الإلكترونية، وكذلك العقوبات التي أوجدها أو وضعها المشرع الجزائري لكل جريمة على حدى، وأهم القواعد الإجرائية المتبعة في هذه الجريمة بحيث لاحظنا تشعب في الموضوع و صعوبته وخصوصا ما تعلق بالقواعد الإجرائية حيث أن هذه الجرائم حديثة نسبيا لتستلزم دراسة مستقبلية محاولة وضع مبادئ عامة بكل ما يتعلق بجرائم ترتبط بالتطور الإلكتروني و المعلوماتي ووسائل الاتصال الحديثة وهذا ما يتطلب تدخلا تشريعيا من أجل وضع حماية قانونية متكاملة لسد جميع الثغرات في قانون العقوبات وبحيث تكون صالحة لمواكبة نظم المعلومات ولعل من أبرز النتائج التي أفرزتها هذه الجريمة تتمثل في :

النتائج:

- لقد توصلنا من خلال بحثنا هذا الى أنه لم يتم التوصل تعريف جامع مانع للجريمة الالكترونية، أو حتى إلى مصطلح موحد.
- قصور القوانين العادية أمام هذه الجريمة المستحدثة، رغم اجتهاد المشرع الجزائري للتصدي لهده الجريمة.

- ان المشرع الجزائري لم يخص الجريمة الالكترونية بقانون قائم بداته للتحكم فيها وفرض عقوبات صارمة وشديدة على مرتكبيها.

عدم الكفاية الاجرائية الخاصة بإجراءات المتابعة و التحقيق و المحاكمة.

- من أبرز التحديات التي أثارها الجريمة الإلكترونية هي التحديات الإجرائية في ميدان التحري و التحقيق والمحاكمة من حيث الاختصاص و القانون الواجب التطبيق خاصة و أن الجريمة الإلكترونية كما سبق و إن قلنا هي جريمة عالمية لا تعرف الحدود الدولية و إقليمية.
- كذلك أن موضوع مكافحة جرائم الإلكترونية يبقي يواجه الكثير من المعوقات الإجرائية، فإن مرحلة التحري و التحقيق ينعدم فيها حسن سير وغياب القدرة التأهلية و الوسائل الفنية التي تتيح سرعة اكتشاف الجريمة و غياب التأهيل قد يؤدي إلى إتلاف الدليل على الجريمة.
- كذلك قصور النصوص الإجرامية التقليدية للضبط و التفتيش لا تتلاءم و الجريمة الإلكترونية التي تتميز بسهولة إخفاء الدليل، كذلك نجد من أهم المشكلات التي تتعلق بالمحاكمة هي الاختصاص و ما يتعلق بمكان وقوع الجريمة إضافة إلى القانون الواجب التطبيق باعتبار أن الجريمة الإلكترونية جريمة عالمية .

المقترحات:

وفي الأخير وعلى ضوء ما انتهينا إلية فضلنا بان ندرج جملة من المقترحات فيما يلي:

- ضرورة التعاون الدولي لمكافحتها من خلال سن مجموعة من التشريعات الوطنية واتفاقيات دولية.
- ضرورة توفير خبرات قضائية مختصة بجرائم الانترنيت، وتخصيص تقنين من أصحاب الخبرة.
- إصدار المزيد من النصوص خاصة من شأنها الإحاطة بالوسائل لعلمية وبتيسير استعمالها في أطار التحقيق و التحريات لملاحقة المجرم الالكتروني و استخلاص الدليل الرقمي بسرعة.

قائمة المصادر والمراجع

المراسيم و القوانين

- ✓ **المراسيم**

1/ المرسوم التنفيذي رقم348/06 المؤرخ في 05أكتوبر 2006، الجريدة الرسمية العدد 63، مؤرخة في 2006/10/18، المتضمن تمديد الاختصاص المحلي لبعض المحاكم والوكلاء الجمهورية وقضاة التحقيق.

- ✓ **القوانين**

2/ القانون 15/04، المؤرخ في 10 نوفمبر 2004 يعدل و يتمم الأمر رقم156/66 مؤرخ في يونيو سنة 1966، والمتضمن قانون العقوبات، الجريدة الرسمية العدد 71، المؤرخة في 10 نوفمبر، سنة 2004.

3/ القانون 09-04 المؤرخ في 05-08-2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47 سنة 2009.

4/ المؤرخ في 8 يونيو سنة 1966، المتضمن قانون إجراءات الجزائية الجريدة الرسمية عدد84، المؤرخ في 24 ديسمبر 2006.

- ✓ **الكتب**

5/ أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، الجزء الأول، دار هومة، الجزائر، طبعة التاسعة،.2008

6/أحمد خليفة الملط، **الجرائم المعلوماتية** ،طبعة 2 دار الفكر الجامعي، الإسكندرية، 2006.

7/أمال قارة ،**الحماية الجزائية للمعلوماتية في التشريع الجزائري**، طبعة الأولى، دار هومة، الجزائر ،2008.

8/ توح عبد الشاذلي، **أساسيات علم الإجرام والعقاب، منشورات الحلبي الحقوقية**، لبنان، 2009.

9/ جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة**، دار البداية، الطبعة الاولى،عمان،2010.

10/ خالد عيادي الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، دار الثقافة، عمان،2011.

11/خالد ممدوح إبراهيم، **آمن الجريمة الإلكترونية**، الدر الجامعية الإسكندرية، 2008.

12/ ختير مسعود، **الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات**، دار الهدى، الجزائر، 2010.

13/ سامي على حامد عياد، **الجريمة المعلوماتية و إجرام الإنترنت**، دار الفكر الجامعي، الإسكندرية،2007.

14/ طارق إبراهيم الدسوقي عطية،**الأمن المعلوماتى النظام القانوني للحماية المعلوماتية**،دار الجامعة الجديدة، الإسكندرية،2009.

15/ عبد العال الديربي، محمد صادق إسماعيل، **الجرائم الإلكترونية**، دراسة قانونية قضائية مقارنة، المركز القومي، القاهرة، 2012.

16/ عبد الفتاح بيومي حجازي، **التجارة الإلكترونية و حمايتها القانونية**، دار الفكر الجامعي، الإسكندرية 2004.

17/ عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والانترنت في القانون النموذجي**، دراسة متعمقة في مكافحة جرائم التقنية الحديثة، دار مونوجزفيك،2005.

18/ عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي**، دار شتات للنشر والبرمجيات، مصر، 2000.

19/ عبد الله هلالي، **التفتيش في نظام الحاسب الآلي وضمانات المتهم المعلوماتي**، دراسة مقارنة، دار النهضة العربية، القاهرة 2006.

20/ محمد أمين الرمي، **جرائم الكمبيوتر والإنترنت**، دار المطبوعات الجامعية، الإسكندرية،2003 .

21/ محمد سعيد نمور، أصول الإجراءات الجزائية شرح لقانون أصول المحاكمة الجزائية، ط1 دار الثقافة ، الأردن، .2005

22/ محمد علي الصريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2004.

23/ محمد مروان، **نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري**، جزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999.

24/ نائلة عادل قورة محمد فريد، **جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان،**.2005

25/ نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، .2008

26/ نهلا عبد القادر المومني، **جرائم المعلوماتية**، دار الثقافة، عمان، 2008.

✓ **المذكرات**

27/ حابت أمال التجارة الالكترونية في الجزائر ،رسالة دكتوراه في العلوم الجنائية، كلية الحقوق و العلوم سياسية، جامعة تيزي وزو، كليةالحقوق و العلوم السياسية، 2015.

28/ سوير سفيان **جرائم المعلومات** .مذكرة ماجستير ،في العلوم الجنائية وعلم الإجرام ،كلية الحقوق والعلوم سياسية ، جامعة تلمسان،2012-2013.

29/ صلاح شنين، **الحماية الجنائية للتجارة الالكترونية**، دراسة مقارنة، رسالة دكتوراه في القانون الخاص، جامعة أبوبكر بلقايد تلمسان، سنة 2010، 2011

✓ **مقالات**

30/ سورية ديش، **أنواع الجريمة الإلكترونية وإجراءات مكافحتها** مجلة العلوم السياسية والقانون، جامعة جيلا لي ليابس، سيدي بلعباس، العدد الأول، 2017.

31/ قصعة خديجة ،جمال بن زروق، **تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الإلكترونية في العالم**، مجلة تاريخ العلوم، جامعة الجلفة، العدد السادس2008.

32/ مزيود سليم، **الجريمة المعلوماتية وواقعها في الجزائر وآليات مكافحتها**، المجلة الجزائرية للاقتصاد والمالية، جامعة المدية، العدد الأول، أفريل 2014.

- ✓ **مداخلات**

33/ عادل يوسف عبد النبي شكري، **الجريمة المعلوماتية والأزمة الشرعية الجزائية**، الجريمة المعلوماتية، جامعة كوفة، كلية الحقوق، العدد السابع، 2008.

34/ فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، المؤتمر الدولي الرابع عشر الرابع عشر حول الجريمة الالكترونية، طرابلس، 2017.

35/ نمديلي رحيمة، **خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة**، المؤتمر الدولي الرابع عشر حول الجريمة الالكترونية، طرابلس، 2017.

36/ يونس عرب، **إيجاز في المفهوم و النطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات**، مؤتمر الأمن العربي حول دليل أمن المعلوماتية و الخصوصية جرائم الكمبيوتر والإنترنت، أبو ظبي، 2002.

فهرس الموضوعات

ملخص البحث

بعد اتساع دائرة الجريمة الالكترونية في الوقت الراهن، عملت أعلب الدول جاهدة في التصدي لها و مكافحتها وعلية تتمحور دراستنا حول هذا الموضوع و السؤال الذي يتبادر لأذهاننا هل وفق المشرع الجزائري في التصدي للجريمة الالكترونية؟

لنصل في الأخير، أن المشرع الجزائري حاول ذالك من خلال نصوص مستحدثة بموجب القانون رقم 15/04 توفير الحماية من هذه الجريمة، أما بالنسبة للحماية الجزائية فقد وفرها من خلال تعديل قانون الإجراءات الجزائية وسن القانون المتعلقة بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصالات و مكافحتها.