الفصل الأول

الجريمة المعلوماتية

المبحث الأول: مفهوم الجريمة المعلوماتية

المبحث الثاني: الجريمة المعلوماتية في التشريع الجنائي الجزائري

تمهيد:

الجريمة المعلوماتية جريمة حديثة نسبيا وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، ونتيجة لحداثة هذه الجريمة فقد كانت هناك اتجاهات مختلفة في تعريفها، كما أنها اتسمت بمجموعة من الخصائص تميزها عن غيرها من الجرائم الأخرى، وجلبت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية.

وعليه سوف نحاول من خلال هذه الفصل تحديد مفهوم الجريمة المعلوماتية في المبحث الأول ثم نتعرض بعد ذلك إلى الجريمة المعلوماتية في التشريع الجزائري في المبحث الثاني.

المبحث الأول: مفهوم الجريمة المعلوماتية

لقد اختلفت المصطلحات التي اطلقت على الافعال غير المشروعة التى تقع نطاق المعلوماتية.[1]

حيث نجد أن هناك من أطلق عليها جريمة الغش المعلوماتي، والبعض الآخر أطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي وآخرون يفضلون تسميتها بالجريمة المعلوماتية.

كما أن هناك جانب يرى أن هذه الجريمة ناشئة أساسا عن التقدم التكنولوجي ومدى التطور الذي يطرأ عليه، فهو متجدد بصفة دائمة ومستمرة خاصة في مجال تكنولوجيا المعلومات ويفضل أن يطلق عليها اصطلاح «جرائم التكنولوجيا الحديثة ».[2]

إلا أننا سوف نعمد في هذه الدراسة الى إطلاق «الجريمة المعلوماتية » على الجرائم المتعلقة بالحاسوب والانترنت.

فاصطلاح الجريمة المعلوماتية عام ويشمل التقنيات الحالية والمستقبلية المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الانترنت. [3]

[1] – أحمد خليفة الملط ، الجريمة المعلوماتية ، ط02، دار الفكر الجامعي ، الإسكندرية ، 2006، ص83.

[2] – نهلا عبد القادر المؤمني ، جرائم المعلوماتية ، ط01 ، دار الثقافة للنشر والتوزيع ، عمان ، 2008، ص46-47.

[3] – أحمد خليفة الملط ، المرجع نفسه، ص83.

المطلب الأول: تعريف الجريمة المعلوماتية وخصائصها

تعد الجريمة المعلوماتية إفرازا ونتاجا لتقنية المعلومات فهي ترتبط بها وتقوم عليها فكلما تطورت هذه التقنية كلما تنوعت وازداد حجم الجرائم التي اتسع نطاقها في المجتمع، والسياسة الجنائية الحديثة استدعت محاولة إعطاء تعريف جامع ومانع للجريمة المعلوماتية حيث نجد أن هذه الأخيرة قد أثارت ضجة في الأوساط الفقهية بخصوص تحديد مفهومها حيث أعطى الفقهاء والدارسون لها عددا ليس بالقليل من التعريفات وكانت هناك محاولة لحصر خصائص الجريمة المعلوماتية والتي تتسم بلون وطابع قانوني يميزها عن غيرها من الجرائم بمجموعة من الخصائص.[1]

الفرع الأول: تعريف الجريمة المعلوماتية

تعددت محاولات الفقهاء في تعريف الجرائم المعلوماتية والتي يمكن تصنيفها الى عدة فئات كما يلي:

أولا: التعريفات التي تستند الى أداة ارتكاب الجريمة.

التعريفات التي انطلقت من وسيلة ارتكاب الجريمة أصحابها ينطلقون من أن الجرائم المعلوماتية تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة ومن هذه التعريفات نجد[2] :

[1] – أمير فرج يوسف، الجريمة الإلكترونية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت ، الطبعة الأولى ، دار الوفاء القانونية، 2011، ص63.

[2] – أيمن عبد الله فكري ، جرائم نظم المعلومات ، دون طبعة ، دار الجامعة الجديدة ، الإسكندرية ، 2007، ص 83.

تعريف Tiedemann «هي كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي» وانتقد هذه التعريف للأسباب التالية:

1- أنه تعريف بالغ العمومية والاتساع لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع ولما كانت الجريمة بوجه عام سلوك غير مشروع فكل جريمة عالجتها القوانين الجنائية التقليدية يمكن أن تدخل ضمن نطاق الجريمة المعلوماتية وهذا أمر غير مقبول.

2- تعريف غير منطقي لأنه لم يبين أنه خاص ببعض الجرائم التي لا يتصور وقوعها إلا بواسطة الحاسب الآلي، فلو فعل ذلك لكان تعريفه قد حد من نطاق عموميته وجعله أقرب للتعريفات العلمية.

3- مجرد استخدام الحاسب الآلي لا يضيف الى السلوك غير المشروع جديد ولكن استخدام البيانات والمعلومات والبرامج هو الذي يمكن أن يضيف الى الجريمة المعلوماتية سمات خاصة بها.

وهناك من يعرفها «الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي» وانتقد هذا التعريف لأنه ينظر الى الحاسب الآلي كما لو أنه شخص طبيعي يساهم في قيام الجريمة.[1]

[1] – أيمن عبد الله فكري، المرجع السابق ، ص83- 84.

ويعرف جون فورستر الجريمة المعلوماتية «أنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية».

أما مكتب تقييم التقنية بالولايات المتحدة الأمريكية فقد عرفها بأنها «الجريمة التي تلعب فيها البيانات، الكمبيوتر والبرامج المعلوماتية دورا رئيسيا».[1]

وقد تعرض هذه الاتجاه القائل بتعريف «الجريمة المعلوماتية استنادا الى وسيلة ارتكابها» لنقد مفاده أن تعريفاتهم بنيت على معيار واحد فقط، إضافة الى أن الوسيلة لم تكن موضوع اعتبار لدى المشرع الجزائي عند التجريم فالوسائل أغلبها متساوية والتكوين القانوني للجريمة وتوافر أركانها مجتمعة هو موضع اعتبار عند انطباق نص التجريم.[2]

ثانيا: التعريفات التي تستند الى محل أو موضوع الجريمة

يرى واضعوا هذه التعريفات بأن الجريمة المعلوماتية ليست هي التي يكون النظام المعلوماتي أداة ارتكابها بل هي التي تقع على النظام أو داخل نطاقه ومن ذلك نجد تعريف Resenblatt الذي يعرفها بأنها « كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه».[3]

---

[1] – أمين فرج يوسف، المرجع السابق ، ص63.

[2] – محمود أحمد عبابنة، جرائم الحاسوب وابعادها الدولية ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان ، 2009، ص18.

[3] – أحمد خليفة الملط ، المرجع السابق، ص86.

وانتقد هذا التعريف لأنه بدأ صحيحا وانتهى معيبا فبعد أن بين أن جريمة الحاسب تعتبر من الجرائم المحصورة في إطار نشاط معين وهو ما يتوافر ومبدأ الشرعية الجنائية لكنه انتهى الى توسع غير مقبول بنصه على أي نشاط غير مشروع يتعلق بالمعلومات التي يمكن أن تحول عن طريق الحاسب ليبقى الباب واسعا أمام التفسيرات بما يتعارض ومبدأ المشروعية في تحديد النشاط الإجرامي [1] وتعرف كذلك بأنها « أي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات ».

أو«الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة الى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية ».[2]

ولم يقتصر الأمر على قيام الفقه بمحاولة وضع تعريفات بل ساهمت الهيئات والمؤسسات المهتمة بدراسة الجريمة المعلوماتية بوضع تعريف لها ومن بينها نجد تعريف خبراء منظمة التعاون الاقتصادي والتنمية «كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو ونقلها ».[3]

ومن أنصار هذا الاتجاه في الفقه العربي نجد الدكتورة "هدى قشقوش" التي أشارت الى أن جرائم الحاسب الآلي هي مجموع الجرائم التي تتصل بالمعلوماتية فهذه الجرائم وفقا لرأيها هي جرائم الاعتداء على الأموال المعلوماتية وهي عبارة عن الأدوات المكونة للحاسب

[1] – أيمن عبد الله فكري، المرجع السابق، ص 86.

[2] – أمين فرج يوسف، المرجع السابق، ص65.

[3] – أيمن عبد الله فكري، المرجع نفسه، ص 87.

الالكتروني وبرامجه ومعداته وقد تعرض هذا الاتجاه الذي يستند في تعريف الجريمة المعلوماتية إلى موضوعها لنقد مفاده «أنه تبنى معيار موضوعي أدى الى إيراد تعريفات عامة ومطلقة لا تحدد الأفعال المتصلة بالجرائم المعلوماتية بصورة دقيقة، ذلك لأن الأخذ به يؤدي الى اعتبار بعض الأفعال من الجرائم المعلوماتية، مع أنها ليست كذلك في حقيقة الأمر».[1]

ثالثا: تعريف الجريمة المعلوماتية وفقا لأداة ارتكابها وموضوعها.

توجد تعريفات تعتمد على أكثر من معيار، فيعرف جانب من الفقه جرائم نظم المعلومات وفق معايير قانونية متعددة – أولها– تحديد محل الجريمة وثانيها وسيلة ارتكابها.

وتبعا لذلك يرى أصحاب هذا الجانب من الفقه ومن بينهم الأستاذ Thomas في مؤلفه «المرشد القانوني لنظرية وحماية وتسويق البرمجيات حيث يعرفها بأنها" أي ضرب من النشاط الموجه» ضد أو المنطوي على استخدام نظام الحاسوب "وكما أسلفنا فتعريف – النشاط الموجه ضد– ينسحب على الكيانات المادية إضافة إلى المنطقية "المعطيات والبرامج".

ويعرف الفقيه –Mass– الجريمة المعلوماتية بأنها «تلك الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح».

[1] – محمود أحمد عبابنة، المرجع السابق، ص18.

ويعرفها الفقيهين الفرنسيين Stanc–Vivant بأنها «مجموعة الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب».[1]

وفي تعريف آخر جاء به خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية بأنها «كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية».

وقد انتقد هذا التعريف وذلك لإدراجه للأموال المادية حيث أن هذه الأموال من الممكن حمايتها بموجب نصوص قانون العقوبات .

أما التعريف الذي جاء به الخبير الأمريكي Parker هو أن الجريمة المعلوماتية «هي فعل إجرامي أيا كانت صلته بتقنية المعلومات، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل ».[2]

رابعا : التعريفات التي تستند على سمات الجاني الشخصية

وضعت العديد من التعريفات للجريمة المعلوماتية التي تقوم على أساس سمات شخصية لدى مرتكب الفعل وهي تحديدا سمة الدراية والمعرفة التقنية ومن هذه التعريفات نجد:

[1] – أمين فرج يوسف ، المرجع السابق ، ص67– 68.

[2] – محمود أحمد عبابنة ، المرجع السابق ، ص17– 19.

تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث حيث عرفها بأنها أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها وكذلك تعريف" david" أية جريمة يكون متطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب ، كما عرفها الأستاذ (Solory) بأنها «أية فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا».

أما "sheldon " فيقول بأنها «واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب».[1]

كما تعرف كذلك بأنها « الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب ونظم المعلومات لارتكابها والتحقيق فيها ومقاضاة فاعليها »[2] أو هي «الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني».[3]

نخلص في الأخير بأنه على الرغم من تعدد التعريفات ضيقا واتساعا إلا أننا نرى أن التعريف الأنسب هو ذلك الذي يعرف الجريمة المعلوماتية بأنها «كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية . والعلة من اختيار هذا التعريف هو استناده الى أكثر

[1] – أيمن عبد الله فكري ، المرجع السابق ، ص 89-90.

[2] – محمد طارق عبد الرؤوف ، جريمة الاحتيال عبر الانترنت ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، 2011، ص 30.

[3] – أيمن عبد الله فكري ، المرجع نفسه، ص 89.

من معيار لتحديد تعريف الجريمة المعلوماتية فالمعيار الأول تمثل في إيراد التعريف للسلوك كل (فعل أو امتناع) والمعيار الثاني موضوع الاعتداء الأموال المعنوية.[1]

الفرع الثاني: خصائص الجريمة المعلوماتية

إن ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت أضفى عليها مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية ونذكر منها:

أولا: الجريمة المعلوماتية تقع في بيئة المعالجة الآلية للبيانات.

تقع الجرائم المعلوماتية في غالبية الأحيان في بيئة المعالجة الآلية للبيانات حيث تكون المعلومات محل الاعتداء عبارة عن نبضات الكترونية فنحن أمام ظاهرة إجرامية ذات طبيعة خاصة لها صلة بما يعرف بالقانون الجنائي المعلوماتي.

ووقوع هذه الجرائم في بيئة المعالجة الآلية للبيانات تستلزم التعامل مع بيانات مجمعة ومجهزة لدخول الحاسب بغرض معالجتها الكترونيا بما يمكن المستخدم من إمكانية كتابتها في الحاسب الذي تتوافر فيه إمكانيات لتحديدها وتعديلها ومحوها وتخزينها واسترجاعها وطباعتها وهذه العمليات وثيقة الصلة بارتكاب الجرائم.[2]

ثانيا: طبيعة المال الذي يرد عليه الاعتداء.

يتكون الحاسب الآلي من كيانين مادي ومعنوي غير أن صور الاعتداء على الكيان المادي تخرج عن وصف جرائم الحاسب الآلي استنادا الى أنها لا تختلف في الأحكام عن

[1] – محمود أحمد عبابنة، المرجع السابق، ص 18.

[2] – هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية، القاهرة ، 1992، ص15.

صور الاعتداء على شيء مادي .فالجانب المهم في الحاسب الآلي هو كيانه المعنوي أو ما يسمى بالمال المعلوماتي حيث يذهب البعض الى أن هذا الأخير يتميز عن غيره من الأموال بما يلي :

- أنه مال غير قابل للنفاذ بمعنى أنه لا ينفذ بالاستعمال.
- أنه مال لا يفقد قيمته بالاستعمال ولكن يفقدها متى ما ظهرت معارف أو برامج جديدة.
- أنه مال يمكن استعماله في آن واحد بواسطة أطراف عديدة دون أن يفقد قيمته فقيمة المعلومات لا تتغير باتساع نطاق استخدامها.
- أن نفقات نقله من طرف إلى آخر لاتكاد تذكر لأنها ضئيلة للغاية أو لا يمكن مقارنتها بنفقة إنتاجها.[1]

ثالثا: الجريمة المعلوماتية متعدية الحدود.

لقد أذابت شبكة الإنترنت الحدود الجغرافية بين دول العالم ولم تعد جريمة تخضع لنظام إقليمي محدود وإنما أصبحت تقع في بلد وتمر عبر بلد آخر، وتتحقق نتيجتها في بلد ثالث وكل ذلك في ثواني محدودة[2]، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بإمكان ارتكاب جريمة عن طريق حاسوب موجود في دول معينة بينما يتحقق الفعل الإجرامي في دولة أخرى، وهذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها

[1] – محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان ، 2004، ص 162– 163.

[2] – محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دون طبعة، دار النهضة العربية ، القاهرة، ص37.

جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة وكذلك حول تحديد القانون الواجب تطبيقه. إضافة الى إشكاليات تتعلق بإجراءات الملاحقة القضائية وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

ولقد كانت القضية المعروفة باسم مرض نقص المناعة المكتسبة من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية.

وتتلخص وقائع هذه القضية التي حدثت عام 1989 بقيام أحد الأشخاص بتوزيع عدد كبير من النسخ[1] الخاصة بأحد البرامج الذي هدف في ظاهره الى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)، إذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس وفي 03 فيفري 1990 تم إلقاء القبض على المتهم جوزيف بوب في الولايات المتحدة الأمريكية وتقدمت بريطانيا بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة (بريطانيا) ووافق القضاء الأمريكي على تسليمه وكانت هذه هي المرة الأولى التي يسلم فيها متهم في الجريمة المعلوماتية.[2]

[1] – نهلا عبد القادر المؤمني، المرجع السابق، ص 51.

[2] – المرجع نفسه، ص 51– 53 .

رابعا: صعوبة اكتشاف الجريمة

تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة فمن المفترض أن اكتشافها يتم عن طريق الفحص الدقيق أو عن طريق الشكوى التي يقدمها المجني عليه ويمكن رد الأسباب التي تقع وراء الصعوبة في ذلك إلى:[1]

- أنها جريمة هادئة لا عنف فيها.
- أنها جريمة فنية لا تترك أثرا كالآثار التي يتركها اقتحام مكان للسرقة مثلا.
- أنها جريمة تعتمد على تغيير الأرقام والبيانات أو محوها من ذاكرة الحاسب الآلي وبالتالي فلا يستطيع القارئ العادي أن يعرف البيانات التي كانت مثبتة قبل تغييرها أو محوها فيكون من العسر اكتشافها، كما أن التغيير والمحو لا يتمان علنا وإنما بطريقة خفية لا تترك أثرا كتابيا يدل على السلوك الإجرامي الذي يتم بمجرد النبضات الالكترونية التي تقضي إلى نقل المعلومات.

فلا شك بأنه كلما تقدم الإنسان في فهم تكنيك العمل في الحسابات الآلية كلما استطاع أن يرتكب جريمته دون أن يخلف أية آثار يمكن الاهتداء إليه من خلالها.

كما أن هذه الجريمة سواء وقعت داخل الحدود أو امتدت الى الخارج من خلال استخدام شبكات الاتصال لا تترك أية أدلة على حدوثها، لذلك يحجم رجال الأعمال عن

[1] – نهلا عبد القادر المؤمني، المرجع السابق، ص 53.

الإبلاغ عنها خوفا على سمعتهم، بالإضافة الى أنه يمكن تدمير المعلومات التي تستخدم كأدلة إثبات في بضعة أجزاء من الثانية.[1]

خامسا: صعوبة إثبات الجريمة المعلوماتية.

تعتبر هذه الخاصية من أهم الخصائص المميزة لجرائم الانترنت عن غيرها من الجرائم وخصوصا تلك التقليدية، نظرا لكونها ترتكب بواسطة أو على الانترنت ومن قبل شخص ذي دراية فائقة بها، وما ينجم عن ذلك من سهولة إخفاء معالم الجريمة و التخلص من آثارها وبالتالي صعوبة التحقيق فيها وتتبع مرتكبيها والقبض عليهم على غرار الجريمة التقليدية والى جانب الأسباب السابقة ، فانه تعود صعوبة إثبات الجرائم المعلوماتية إلى:

- صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- الحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها وهذا ما يعرقل عمل المحقق الذي تعود التعامل مع الجرائم التقليدية.
- أنها تعتمد على قمة الذكاء والمهارة في ارتكابها.
- أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها فهؤلاء يعتمدون على التخفي عبر دروب الانترنت تحت قناع فني.

[1] – محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، الطبعة الأولى، دار الجامعة الحديثة، 2001، ص 97-98.

- يلعب البعد الزمني (اختلاف المواقيت بين الدول) والمكاني (إمكانية تنفيذ الجريمة عن بعد) والقانوني (أي قانون يطبق) دورا مهما في تشتيت جهود التحري والتنسيق الدولي يتعقب مثل هذه الجرائم.[1]
- عدم ملائمة الأدلة التقليدية في القانون الجنائي في إثبات الجرائم المعلوماتية، ومن ثم يلزم البحث عن أدلة جديدة حديثة ناتجة عن ذات الحاسب ومن هنا تبدأ صعوبات البحث عن الدليل وجمع هذه الدليل.[2]

سادسا: أسلوب ارتكاب الجريمة المعلوماتية.

لا تتطلب جرائم الانترنت عنفا لتنفيذها، بل تنفذ بأقل جهد ممكن وتعتمد على الخبرة في المجال المعلوماتي بشكل أساسي عكس الجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة، إذن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج الى عنف بل كل ما تحتاج هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال الغير مشروعة.[3]

[1] – نبيلة هبة هروالة، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص 40.

[2] – محمد عبد الله أبو بكر سلامة، موسوعة الجرائم المعلوماتية، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2006، ص97.

[3] – نهلا عبد القادر المؤمني، المرجع السابق، ص 57– 58.

المطلب الثاني :المجرم المعلوماتي ودوافعه

يتمتع نشطاء الإنترنت بصفات وخصائص تميزهم عن غيرهم وذلك انعكاس حتمي لما تتطلب عمليات استخدام هذه الشبكة من قدرات تقنية وفنية هائلة، بيد أن ذلك لا يعني حصر مرتكبي جرائم الإنترنت في طبقة أو فئة معينة أو جنس معين فمرتكب الجريمة قد يكون من البالغين أو الأحداث والمتعلمين منهم أو المثقفين ومن الفقراء أو الأغنياء ومن الرجال أو النساء وهذا ما جعل المجرم المعلوماتي محلا لعديد من الأبحاث والدراسات.[1]

الفرع الأول: المجرم المعلوماتي

أولا: سمات المجرم المعلوماتي.

01-المجرم المعلوماتي يتمتع بقدر من المهارة والمعرفة والذكاء

المجرم المعلوماتي ليس كغيره من الجناة التقليديين بل يتمتع بمزايا ومهارات خاصة ودراية ومعرفة بتكنيك تشغيل الحاسب الآلي والقدرة على اختراق النظم الحمائية و الكودات السرية للبرامج والمعلومات والبيانات من أجل إشباع النية الإجرامية لديه أو لإظهار تفوقه على الآلة، أو بدافع اللهو والترف أو لتحقيق الربح فنحن لسنا بصدد سارق عادي

[1] – علي جبار الحسناوي، جرائم الحاسوب والانترنت ، بدون طبعة ، دار اليازوري العلمية للنشر والتوزيع ، عمان ، 2009، ص48.

أو محتال أو خائن للأمانة بمفهومه التقليدي بل أمام شخص يتمتع بمستوى عال من الذكاء الذي يسخره في السيطرة على الحاسب الآلي وجعله وسيلة سهلة في يده.[1]

02- المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي:

يقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي التي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة [2]، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات وقد تتمثل هذه السلطة في الحق في استعمال الأنظمة المعلوماتية، أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة .

03-المجرم المعلوماتي يبرر ارتكاب جريمته:

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم، أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.[3]

---

[1] – بلال أمين زين الدين ، جرائم نظم المعالجة الآلية للبيانات ، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية ، 2008، ص40.

[2] – نهلا عبد القادر المؤمني، المرجع السابق ، ص 80.

[3] – المرجع نفسه ، ص78.

04-المجرم المعلوماتي إنسان اجتماعي :

يتميز المجرم في مجال المعالجة الآلية للبيانات بالإضافة إلى الذكاء بأنه إنسان اجتماعي يبتعد عن السمات التقليدية للمجرم التقليدي، الذي قد يوصف بالعنف والتأثر بعوامل نفسية وذهنية تدفعه إلى بؤرة الإجرام أو كوابت غريزية تؤدي به إلى أفعال الاعتداء حيث نجد المجرم المعلوماتي قد يتجه إلى ارتكاب جريمة المعالجة الآلية للبيانات بدافع اللهو أو الترف أو بمجرد إثبات ضعف الأنظمة الأمنية للبرامج والنظم.[1]

ثانيا: فئات مجرمي المعلوماتية.

إن التطور والتغير السريع في أنماط الجريمة المعلوماتية وصورها يصعب علينا وضع تصنيف ثابت لطوائف مجرمي المعلوماتية ولكن يمكن لنا وفقا لما توصلت إليه الدراسات والأبحاث التي تناولت مجرمي المعلوماتية أن تبين بعض هذه الأنماط لهؤلاء المجرمين ولكن لا بد من الإشارة أولا إلى أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة وعليه يمكن حصر أنواع الجناة في جرائم الحاسب الآلي في عدة فئات كالتالي:[2]

[1] – بلال أمين زين الدين ، المرجع السابق ، ص 40.

[2] – نهلا عبد القادر المؤمني ، المرجع السابق ، ص 81.

الفئة الأولى : صغار مجرمي المعلوماتية

وهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية وتتمثل أفعالهم في الانتهاك غير المسموح به في ذاكرات الحاسبات الآلية،[1] ولقد تعددت أوصافهم في الدراسات الاستطلاعية والإحصائية وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح "المتلعثمين" الدال حسب تعبير أحد الفقهاء على "الصغار المتحمسين إلى الحاسب وبشعور من البهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسب" ويسميهم البعض بالمجانين[2] ومن الأمثلة الشهيرة للجرائم المعلوماتية التي ارتكبت من هذه الفئة ما حدث من العصابة الشهيرة التي عرفت باسم "عصابة 414" والتي نسب إليها ارتكاب 60 فعل تعد في الولايات المتحدة الأمريكية على ذاكرات الحاسبات الآلية نجم عنها أضرار كبيرة لحقت بالمنشآت العامة والخاصة.[3]

ويثير مجرموا الحاسبات من هذه الطائفة جدلا واسعا، ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة ظهرت دراسات تدافع عنها وتخرجها من دائرة الإجرام إلى دائرة العبث وأحيانا البطولة، فهناك اتجاه لا يرى إصباغ أية صفة إجرامية على هذه الفئة استنادا إلى أن صغار السن لديهم ببساطة ميل للمعلوماتية والتحدي والرغبة في الاكتشاف، كما أنهم

[1] – سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، بدون طبعة، دار الفكر الجامعي، الإسكندرية، 2007 ، ص 52.

[2] – أيمن عبد الله فكري، المرجع السابق، ص112.

[3] – سامي علي حامد عياد، المرجع نفسه، ص52.

لا يدركون ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إلى أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية.[1]

واتجاه يناصر هذه الفئة ويعتبرها ممن تقدم خدمة لأمن المعلومات ووسائل الحماية ويصفهم بالأخيار ويتمادى هذا الاتجاه في تقديره لهذه الفئة بالمطالبة بمكافأتهم باعتبارهم لا يسببون ضررا للنظام ولا يقومون بأعمال الاحتيال وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات .

أما الاتجاه الأخير يرى أن هذه الطائفة تصنف ضمن مجرمي المعلوماتية مثل غيرهم من المجرمين حيث أن أفعالهم المتمثلة في انتهاك الأنظمة واختراق الحواجز الأمنية في البيئة الالكترونية تعد أفعالا خطيرة من الناحية العملية ، كما أن مجرم هذه الفئة قد يتحول من مجرد هاوي صغير إلى محترف لأعمال السلب.[2]

الفئة الثانية: القراصنة

هناك صنفان من القراصنة :

المتطفلون" الهاكرز": وهم الأشخاص الذين يشعرون بالفخر لمعرفتهم بأساليب عمل النظام أو الشبكات حيث يسعون للدخول عليها بدون تصريح وهؤلاء عادة لا يتسببون بأي أضرار مادية إذ يتحدون إجراءات أمن النظم والشبكات ولا تتوافر لديهم دوافع حاقدة أو تخريبية.[3]

---

[1] – أيمن عبد الله فكري، المرجع السابق، ص 113.

[2] – نهلا عبد القادر المؤمني، المرجع السابق، ص 82.

[3] – أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، بدون طبعة، دار المطبوعات الجامعية، 2009، ص 68.

- **المحترفـون"الكريكرز"** : طائفـة الكريكـرز لا تختلـف عـن طائفـة الهـاكرز مـن الناحيـة التجريمية مع العلم أن بين الاصطلاحين تباينا جوهريا" فالهاكرز" متطفلون يتحدون إجراءات أمن النظم والشبكات لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، أما الكريكرز فـإن اعتـداءاتهم تعكـس ميـولا إجراميـة خطـرة تتبنـي عنهـا رغبـاتهم فـي إحـداث التخريـب فاصطلاح "الكريكرز" مرادف للهجمات الحاقدة والمؤذية والسمة المميزة لهذه الطائفة تبادلهم للمعلومات فيما بينهم وتحديدا التشارك في وسائل الاختراق وآليات نجاحها واطلاعهم بعضهم بعض على مواطن الضعف في نظم المعلومات والشبكات.[1]

الفئة الثالثة: الموظفون العاملون في مجال الأنظمة المعلوماتية

وهم غالبا الموظفون الساخطون على منظماتهم التي يعملون بها فيعمدون إلى تخريب الجهـاز أو إتلافـه أو حتـى سـرقته مـن خـلال عملهـم علـى أجهـزة منظمـاتهم أو مـن خـلال الـدخول عليهـا مـن اتصـالات خارجهـا وتكمـن خطـورة هـذا الشـخص فـي قدرتـه علـى معرفـة معلومات حساسة وخطيرة كونه يعمل داخل تلك الجهة، ولذلك فإن حرب التجسس بين الدول تعتمد على عناصر يعملون داخل الجهة الأخرى تعد من أخطر أنواع التجسس حيث تفرض الـدول أشـد الأحكـام صـرامة علـى مـن يمـارس ذلـك والتـي تصـل إلـى الإعـدام فـي كثيـر مـن الدول.[2]

[1] – أيمن عبد الله فكري، المرجع السابق، ص 107– 108.

[2] – عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، بدون طبعة، ص46.

الفئة الرابعة: مجرمو المعلوماتية في إطار الجريمة المنظمة

لقد ساعدت أجهزة التقنية المعلوماتية جماعات الجريمة المنظمة في تسوية أعمالها وتسهيل تنفيذها، إذ وجدت هذه الأخيرة في شبكة الانترنت وسيلة لا تضاهى للقيام بعمليات غسيل الأموال على نطاق واسع وكذلك لتدعيم تجارة الرقيق الأبيض وتجارة الأعضاء البشرية عبر إنشاء مواقع خاصة بهذه الأعمال وذلك بالاستعانة بأصحاب الكفاءات وأصحاب الخبرة والموهوبين في مجال تقنية المعلومات.[1]

الفئة الخامسة: مجرموا المعلوماتية أصحاب الآراء المتطرفة

تتألف هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي ويتركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه، وبدأ اهتمام هذه الجماعات وخاصة تلك التي تتمتع بدرجة عالية من التنظيم يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة المعلوماتية.

فهذه الجماعات تدافع عن قضية أو معتقد معين ولا تهدف ابتداء إلى تحقيق الربح المادي، وفي هذا تختلف هذه المنظمات المتطرفة عن المنظمات الإجرامية المنظمة حيث تهدف هذه الأخيرة إلى تحقيق مصالحها الشخصية المباشرة وتحديدا تحقيق الربح المادي.

[1] – نهلا عبد القادر المؤمني، المرجع السابق، ص 86-87.

إذ قامت جماعات تنتمي إلى منظمات إرهابية دولية من اليمين المتطرف واليسار مثل جماعة الألوية الحمراء الايطالية ومنظمة (Leclodo) وهي منظمة فرنسية متخصصة في تدمير نظم المعلومات المنتشرة في أوربا عام 1978.

وقد تعرضت وزارات وجامعات ومؤسسات مالية لهجمات الألوية الحمراء ومن هنا أيقنت المنظمات الإرهابية أن باستطاعتها بمجهود بسيط أن تلحق أضرارا ضخمة داخل أي مشروع عن طريق تدمير المركز المعلوماتي له.[1]

الفرع الثاني: دوافع المجرم المعلوماتي

يمارس المجرمون الالكترونية الرقميون نشاطهم الإجرامي الالكتروني بدوافع معنوية أو مادية غير سوية وتتمثل هذه الدوافع في :[2]

01- تحقيق مكاسب مالية:

أحيانا يكون الهدف من ارتكاب الجرائم المعلوماتية الرغبة في تحقيق الثراء الشخصي، وقد تبين من خلال تحقيق أجرته إحدى المجلات المتخصصة بخصوص الأمن المعلوماتي أن الغالبية من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال[3]، فإذا كانت بعض الجرائم التقليدية (كالسرقة والاختلاس) يكون الدافع إلى ارتكابها

[1] – نهلا عبد القادر المؤمني، المرجع السابق، ص 85- 86.

[2] – مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، طبعة أولى، مطابع الشرطة، القاهرة، 2008، ص151.

[3] – سامي علي حماد عياد، المرجع السابق ، ص57.

هو تحقيق النفع المادي فإن النفع المادي الذي يمكن تحقيقه عن طريق جرائم الحاسب الآلي أكثر وأكبر من النفع الذي تحققه هذه الجرائم.[1]

02- الولع في جمع المعلومات وتعلمها:

فهناك من يقوم بارتكاب جرائم الكمبيوتر بغية الحصول على الجديد في المعلومات فيرى قراصنة الكمبيوتر أن الحصول على المعلومة يجب أن لا يكون عليه أي قيد فالقرصان يكرس كل جهده في تعلم كيفية اختراق المواقع الممنوعة، وغالبا ما يكون القراصنة مجموعات يكون الهدف منها التعاون وتبادل المعلومات وتقاسم البرامج والأخبار، ويفضل القراصنة أن يكونوا مجهولين حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول فترة ممكنة.[2]

03- الرغبة في تحدي وقهر النظام التقني المعلوماتي:

إن اختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبها ووسيلة تغطي أوقات فراغه[3] فالدافع في هذا الفرض لا ينبني عن خطورة إجرامية كامنة في نفس مقترف هذه الأفعال إذ أنهم عادة لا يكونون من معتادي

[1] – محمد حماد مرهج الهيتي، جرائم الحاسوب ، طبعة أولى ، دار المناهج للنشر والتوزيع ، عمان ، ص 143.

[2] – محمد أمين الرومي، جرائم الكمبيوتر والانترنت ، بدون طبعة ، دار المطبوعات الجامعية ، الاسكندرية ، 2004، ص24.

[3] – نهلا عبد القادر المؤمني، المرجع السابق ، ص 91.

الإجرام بل يتمثل في رغبة هؤلاء بتحدي النظام التكنولوجي المعتمد للحاسب الآلي بكل مكوناته ومعطياته ومحاولة اختراقه عن طريق الوصول إلى المعلومات.[1]

فمجرمو المعلوماتية يتملكهم شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية ففي :

بعض الأحيان وجد أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي.[2]

04-الرغبة في الانتقام :

قد يكون الهدف من ارتكاب الجريمة المعلوماتية الحقد والكراهية فقد دفع الانتقام بمحاسب شاب إلى أن يتلاعب ببرامج الكمبيوتر الخاصة بشركة التي يعمل بها ، حيث برمجها على أن تختفي كل البيانات الخاصة بديون الشركة بعد مضي 06 أشهر من تاريخ تركه للعمل وحدث ما أراد بالفعل، فبعد أن ترك العمل ومرت 06 أشهر اختفت البيانات الخاصة بديون الشركة نهائيا من على جهاز الكمبيوتر.[3]

[1] – محمود أحمد عبابنة، المرجع السابق، ص25.

[2] – نهلا عبد القادر المؤمني، المرجع السابق ص 92.

[3] – محمد أمين الرومي، المرجع السابق، ص24-25.

05- دوافع سياسية :

لقد سخرت شبكة الانترنت في الصراعات السياسية الدائرة اليوم إذ شهدت السنوات القليلة الماضية محاولات دولية لاختراق شبكات حكومية في مختلف دول العالم، فالتجسس عبر الإنترنت يتم يوميا من قبل أجهزة المخابرات .

كما أن الأفراد كذلك قد يتمكنون من اختراق الأجهزة الأمنية الحكومية و خير مثال على ذلك عندما استطلاع 03 إخوة من قرية كفر قاسم الفلسطينية اختراق شبكة المخابرات الإسرائيلية الموساد وجهاز الأمن الإسرائيلي، واستطاعوا أن يتنصتوا على عدد من المكالمات والحصول على بعض المعلومات السرية وتقديمها للسلطة الفلسطينية علما أن الإخوة الثلاثة فاقدي لنعمة البصر.[1]

[1] – محمود أحمد عبابنة، المرجع السابق، ص26.

المبحث الثاني : الجريمة المعلوماتية في التشريع الجنائي الجزائري

إن استخدام شبكة الانترنت في جميع النشاطات المهنية والاقتصادية وحتى الحياة الخاصة بالأشخاص أدى إلى ظهور صور جديدة للاعتداءات وهذا بسبب التطور التكنولوجي والمعلوماتي[1] إذ تشير الإحصائيات إلى وقوع ما بين 200 –250 اعتداء يوميا على الأنظمة المعلوماتية في الجزائر وإن تفاقم الاعتداءات على أنظمة المعالجة الآلية للمعلوماتية خاصة مع ضعف الحماية الفنية استدعى تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي[2]، فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ: 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي[3]، أما على المستوى الوطني فقد استدرك المشرع الجزائري الفراغ القانوني من خلال إصداره للقانون 15/04 المتعلق بالمساس بالأنظمة الآلية لمعالجة المعطيات الذي عدل بموجبه قانون العقوبات في الفصل الثالث من الباب الثاني من الكتاب الثالث بالقسم السابع مكرر بعنوان "المساس بأنظمة المعالجة الآلية[4] للمعطيات" ويشمل المواد 394 مكرر إلى 394 مكرر 07 وعليه سوف نحاول في هذا المبحث معرفة صور الجريمة المعلوماتية في التشريع الجنائي الجزائري

[1] – بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاء ، مجلس قضاء قسنطينة ، 2012/2011.

[2] – فشار عطاءالله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم بالملتقى المغربي حول القانون والمعلوماتية، جامعة زيان عاشور بالجلفة، كلية الحقوق والعلوم السياسية .

[3] – الاتفاقية الدولية حول ، الإجرام المعلوماتي ، بتاريخ ، 2001/11/08، من طرف المجلس الاوروبي وتم وضعها للتوقيع منذ تاريخ ، 2001/11/23.

[4] – القانون 15/04 المؤرخ في ، 2004/11/10 المعدل والمتمم للأمر 156/66 المؤرخ في ، 08جوان 1966 المتضمن قانون العقوبات، الجريدة الرسمية رقم ، 71 بتاريخ ، 2004/11/10 .

في مطلب أول ثم بعد ذلك الجزاء المقرر لهذه الجرائم في التشريع الجنائي الجزائري في مطلب ثان.

المطلب الأول: صور الجريمة المعلوماتية في التشريع الجنائي الجزائري

تتخذ الجرائم المعلوماتية عدة أشكال تتعدد بتنوع صور الاعتداء على الاعلام الآلي والتي يمكن إجمالها في صورتين :

01- الاعتداءات على أنظمة المعالجة الالية للمعطيات

02- الاعتداءات على منتوجات الاعلام الالي.

لكن تجدر الاشارة إلى أن المشرع الجزائري على الرغم من استدراكه للفراغ القانوني الموجود في هذا المجال بإصداره للقانون 15/04 إلا أنه ركز فقط على الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل الاعتداءات الماسة بمنتوجات الاعلام الالي والمتمثلة في التزوير المعلوماتي وعليه سوف تكون دراستنا في نطاق الصورة الأولى فقط.[1]

الفرع الأول: جرائم الاعتداء على المنظومة المعلوماتية

إن الصورة الغالبة لتحقيق غاية المجرم المعلوماتي في نطاق الشبكة تتمثل في فعل الدخول غير المشروع لنظام المعلومات أو البقاء فيه بدون إذن ومن ثم قيام الجاني بارتكاب فعله الذي قد يكون مجرم فيشكل أحد جرائم المعلوماتية.

[1]- آمال قارة، الجريمة المعلوماتية،(أطروحة ماجستير)، جامعة الجزائر، كلية الحقوق، 2001-2002 ، ص41.

أولا: جريمة الدخول غير المشروع.

جاءت في المادة 394 مكرر/1" يعاقب بالحبس من ثلاثة أشهر (03) إلى سنة (01) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ".

بنص المادة الذي يعتبر الركن الشرعي للجريمة فإننا نستنتج أن الركن المادي يتخذ صورة الدخول ولا يقصد بالدخول هنا الدخول بالمعنى المادي أي الدخول إلى مكان أو منزل أو حديقة وفي نفس الاتجاه. إلى جهاز الحاسب الآلي وإنما يجب أن ينظر إليها كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة، إلى ملكة التفكير لدى الإنسان في الدخول إلى المعطيات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات.[1]

ويتحقق فعل الدخول متى كان الجاني قد دخل إلى النظام كله أو جزء منه ولم يحدد المشرع وسيلة الدخول والطريقة التي يتم بها الدخول إلى النظام ولذلك تقع الجريمة بأي وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[2] والدخول المجرد في ذاته غير معاقب عليه حتى ولو لم يترتب على الدخول أي ضرر أو فائدة للجاني وإن الدخول المعاقب عليه هو الدخول غير المشروع في ذاته[3]، بينما يتمثل الركن المعنوي في

1 – آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، ط2، دار هومة ، الجزائر ، 2007 ، ص107.

2 – علي عبد القادر القهوجي، جرائم التعدي على نظام المعالجة الآلية للمعطيات، بحث مقدم لمؤتمر القانون، كلية الشريعة والقانون، جامعة الإمارات، ماي 2000، ص50.

3 – المرجع نفسه ، ص51.

صورة القصد الجنائي (العلم زائد الإرادة)، فيجب أن تتجه إرادة الجاني إلى فعل الدخول وهو يعلم بأنه ليس له الحق في ذلك.[1]

ثانيا: جريمة البقاء غير المشروع في المنظومة المعلوماتية.

نجد المادة 394 مكرر (1) سابقة الذكر قد تحدثت كذلك على جريمة البقاء التي احتوتها الفقرة الثانية ونجد أن المشرع الجزائري لا يشترط أن ترتكب جريمة البقاء على كامل النظام بل يكفي البقاء في جزء منه لتكتمل أركانه، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على النظام.[2]

وفعل البقاء غير المشروع في نظام معالجة الآلية للبيانات كان الهدف من تجريمه هو تجريم البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات فالجاني لم يقصد الدخول إلى النظام ولكن حين تبين دخوله كان يمكن له أن يغادر النظام ومع ذلك يبقى داخل النظام وتنصرف إرادته إلى ذلك حيث يعاقب الجاني عن جريمة عمدية لأن إرادته انصرفت إلى البقاء داخل النظام رغم علمه أن دخوله غير مشروع وينصرف الحكم السابق كذلك إلى حالة الشخص المسموح له بالدخول إلى جزء من النظام المعلوماتي ثم يدخل إلى مكان آخر غير مصرح به.[3]

---

[1] – خالد عبد الله القائفي، التحقيق الجنائي الرقمي والمعروف باسم العلوم الجنائية للأجهزة الرقمية أو digital forensics وعملية التحقيق والاثبات بالأدلة والبراهين على ارتكاب الجريمة الالكترونية منشور يوم 2010/12/22 على الموقع، WWW.min-mag.com.

[2]– علي عبد القادر القهوجي، المرجع السابق، ص133.

[3] – عبد الفتاح بيومي الحجازي، الجريمة في عصر العولمة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ص83.

كما قد يجتمع فعل دخول غير مصرح به وفعل البقاء داخل نظام المعالجة ويتحقق ذلك في حالة ما إذا لم يكن للجاني الحق في الدخول إلى هذا النظام وبرغم من ذلك يدخل إليه فعلا ضد إرادة صاحبه أو من له الحق في السيطرة ثم يبقى داخل هذا النظام بعد ذلك.[1]

ويثار التساؤل حول الوقت الذي تنتهي فيه جريمة الدخول وتبدأ جريمة البقاء؟

ذهب رأي في الفقه إلى جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج، وإن كان الدخول في نظر هذا الرأي يفترض بالضرورة البقاء فترة قصيرة من الزمن تنتهي عندها جريمة الدخول وبعد تلك اللحظة تبدأ جريمة البقاء داخل النظام، وتنتهي بانتهاء حالة البقاء ويؤخذ على هذا الرأي أنه لا يحدد لحظة بداية جريمة البقاء بطريقة حاسمة، لهذا ذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه المتدخل أن بقاءه داخل النظام غير المشروع، وأخذ على هذا الرأي أيضا صعوبة إثبات علم المتدخل وذهب رأي ثالث إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع، فإذا لم ينسحب يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام. وهذا الرأي وإن أمكن توفيره فنيا فإنه لن يكون متاحا له بالنسبة للشركات أو المؤسسات الكبيرة فقط.

والرأي الصائب في مثل هذه الظروف هو الذي يعتبر أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبرم فيها الجاني التجوال داخل النظام، أو يستمر في التجول بداخله

[1] – بردال سمير، الجريمة المعلوماتية في التشريع الجزائري، مقال منشور في مجلة فصلية تصدر عن معهد الحقوق للمركز الجامعي بغليزان، العدد الثاني، 2010، ص187.

بعد انتهاء الوقت المحدد لأن الفرض يتعلق بدخول غير مشروع، أي مع علم الجاني أن ليس له حق في الدخول، فإذا دخل وظل ساكنا تعد جريمة الدخول إلى النظام، أما إذا بدأ التجول فإن جريمة البقاء داخل النظام تبدأ منذ تلك اللحظة لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله فيه غير مشروع أو أن مبدأ استمراره فيه غير مشروع ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام. [1]

ثالثا: جريمة تخريب نظام اشتغال منظومة المعالجة الآلية للمعطيات.

تناول المشرع الجزائري هذه العقوبة بموجب الفقرة الثالثة من نص المادة 394 مكرر حيث نصت "... إذا ترتبت على الأفعال أعلاه تخريب نظام الإشغال للمنظومة عقوبة الحبس من 06 أشهر إلى سنتين (02) والغرامة من 50.000 دينار جزائري إلى 150.000 دينار جزائري".

ويقصد بالأفعال المذكورة أعلاه كل من فعل الدخول والبقاء غير المشروع في كل أو جزء المنظومة وفعل الحذف أو التغيير الذي يلحق بمعطيات المنظومة لذلك تعد جريمة تخريب نظام اشتغال المنظومة المعلوماتية نتيجة إجرامية لجريمة الدخول أو البقاء غير المشروع في كل أو جزء من المنظومة المعلوماتية وما يترتب عنها من حذف أو تغيير المعطيات لذا فلا يمكن تصور وقوع جريمة تخريب نظام اشتغال منظومة معلوماتية إلا بعد ارتكابه لجريمة دخول أو بقاء غير مشروع في

[1] – آمال قارة، المرجع السابق، ص112– 113 .

كـل أو جـزء مـن المنظومـة المعلوماتيـة ثـم قيامـه بتغييـر أو حـذف معطيـات المنظومة.[1]

الفرع الثاني: جرائم الاعتداء على المعطيات التابعة للمنظومة المعلوماتية

إن صورة الإتلاف المعلوماتي المعنوي عبر شبكة الانترنت تتمثل في الاعتداء على سير نظام المعالجة الآلية للبيانات بمختلف التصرفات التدليسية المتمثلة في الدخول غير المشروع إلى النظام المعلوماتي والبقاء فيه.[2]

وبما يترتب عليه من إتلاف للبيانات والبرامج أو بما يؤدي إليه من تعطيل أو إفساد نظام التشغيل ويقع الإتلاف على النظام المعلوماتي سواء كان ذلك بالدخول العمدي للنظام المعلوماتي أو باستخدام الجاني الطرق التقنية والفنية للإتلاف كالفيروسات أو كان ذلك نتيجة خطأ أثناء التواجد بالنظام.[3]

أولا: صور الاعتداء على المعطيات التابعة للمنظومة المعلوماتية.

نظرا للطبيعة الخاصة التي تتسم بها المكونات المعنوية للنظام المعلوماتي نجد أن النشاط الإجرامي في هذه الجرائم يتمثل في أفعال الإدخال أو المحو أو تعديل، ويكفي توافر إحداها لقيام الجريمة فلا يشترط اجتماعه معا حتى يتوفر النشاط الإجرامي فيها ومن ثمة تقييم الركن المادي للجريمة، لكن القاسم المشترك لهذه الأفعال جميعها هو انطوائها على

[1] – بردال سمير، المرجع السابق ، ص 189.

[2] – محمد أمين الشوابكة، جرائم الحاسوب والانترنت ، الطبعة الأولى ، مكتبة دار الثقافة للنشر والتوزيع ، عمان ، 2004، ص222.

[3] – المرجع نفسه ، ص 222.

تلاعب في المعلومات التي تضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل أخرى قائمة.[1]

1- جريمة إدخال المعطيات في نظام المعالجة الآلية:

تنص المادة 394 مكرر 1 من قانون العقوبات " يعاقب بالحبس من ستة 06 أشهر إلى ثلاثة سنوات وبغرامة من 500.000دج خمسمائة ألف دينار جزائري إلى 2.000.000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريقة الغش المعطيات التي تضمنها" ويقصد بفعل الإدخال إضافة وإدراج معطيات جديدة في نظام المعالجة الآلية للمعطيات[2] سواء كان ذلك خاليا أو كان يوجد عليه معطيات من قبل وتتحقق هذه الحالة عندما يريد الحامل الشرعي لبطاقة السحب الممغنطة سحب مبلغ من النقود من حسابه الخاص يفوق حسابه الأصلي كما يتحقق فعل الإدخال في كل حالة يقوم فيها الجاني استخدام برنامج حامل للفيروس قادر على إضافة معطيات جديدة للنظام كبرنامج حصان طروادة، ويكون التدخل في المعطيات إما بإدخال المعلومات الوهمية في النظام المعلوماتي أو بتزوير المعطيات الموجودة.[3]

[1] – عبد الفتاح بيومي الحجازي، المرجع السابق، ص91.

[2] – بردال سمير، المرجع السابق، ص 191.

[3] – المرجع نفسه، ص 191.

2- جريمة تعديل معطيات المنظومة المعلوماتية:

تنص المادة 394 مكرر 1 "يعاقب بالحبس من (06) أشهر إلى 03 سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج أو عدل بطريقة الغش المعطيات التي يتضمنها"

وتقع هذه الجريمة على الكيان المنطقي للكمبيوتر، وهو مجموعة البرامج المخصصة للقيام بالمعالجة عن طريق الحاسب الآلي ويكون ذلك إما بتعديل البرامج أو بخلق برنامج جديد.

أ – **تعديل البرنامج:** يعد البرنامج كيانا ماديا يمكن رؤيته عبر شاشة الحاسب الآلي كترجمة إلى أفكار، كما يمكن الاستحواذ عليه عن طريق تشغيله في الحاسب ويأخذ هذا الفرض إحدى الصور الآتية:

- **التلاعب في البرنامج:** ويتم ذلك ببرمجة الجهاز الآلي والنظام المعلوماتي بشكل يؤدي إلى اختفاء البيانات بعضها أو كلها.
- **اختلاس نتائج الحساب أو الإدارة:** ويتم ذلك عن طريق إعادة نسخ المعطيات عن بعد أو عن طريق عملية النقل الالكتروني للبيانات وذلك بإتباع أسلوب التجسس المعلوماتي عن طريق بث برامج خاصة بالتقاط البيانات المتبادلة عبر شبكة الانترنت.
- **تغيير نظام الاشتغال:** ويكون ذلك بتزويد برنامج نظام التشغيل بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة كلمة السر أو مفتاح الشفرة أو أداة الربط بحيث تتيح الوصول إلى جميع المعطيات التي يتضمنها الحاسب الآلي.

ب- خلق برنامج جديد: وفي هذه الحالة إما يكون البرنامج وهميا أو أن يكون برنامج ناقص من الناحية الفنية.

- **خلق برنامج وهمي:** أي اصطناع برنامج مخصص فقط لارتكاب فعل الغش المعلوماتي.
- **إعداد برنامج ناقص من الناحية الفنية:** وفي هذا الغرض يقوم الجاني وهو غالبا المبرمج بإدخال فجوات في برنامج الحاسب الآلي حتى يتمكن من تنفيذ التعديلات الضرورية بإدخال كودات إضافية أو إحداث مخارج بسيطة.[1]

3- جريمة إزالة معطيات منظومة:

بنص المادة 394 مكرر 1 من قانون العقوبات الجزائري، فإن النشاط الإجرامي لهذه الجريمة يتمثل في محو كل أو جزء من المعطيات المسجلة على دعامة موجودة داخل نظام المعالجة الآلية للمعطيات أو التحطيم لتلك الدعامة. ويتحقق فعل الإدخال والمحو والتعديل عن طريق برامج غريبة بالتلاعب في المعطيات وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة أو برنامج الفيروسات بصفة عامة، وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل مذكورة على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر.[2]

[1] – محمد أمين الشوابكة، المرجع السابق، ص 237.

[2] – آمال قارة، المرجع السابق، ص 122.

ثانيا: الطرق الفنية لإتلاف البيانات والبرامج داخل نظام المعالجة الآلية للمعطيات.

يحدث إتلاف البيانات والمعلومات الموجودة داخل نظام معلوماتي بعدة أساليب قريبة الشبه تتمثل هذه الأساليب في ثلاثة أنواع هي: الفيروسات، برامج الدودة، القنابل المنطقية والزمنية وسنتعرض لكل منها على النحو التالي:

1- برنامج الفيروس: سنعرض الفيروس المعلوماتي بوصفه إحدى الوسائل التي يتم عن طريقها تعطيل أو تدمير أو نسخ البرامج أو البيانات المعلوماتية.

أ- **طبيعة برنامج الفيروس:** يعرف الفيروس المعلوماتي بأنه عبارة عن برامج للحاسب يهدف الى إحداث أكبر ضرر بنظام الحاسب [1]، وله القدرة على الالتصاق ببرنامج أو ملف آخر لا يكون قد تمت إصابته من قبل وذلك بعد فحصه والتأكد من عدم إصابته ويقوم الفيروس بالانتشار بين برامج الحاسب المختلفة بغية التعديل في تكوين البرامج المصابة أو تدمير ملفات بأكملها أو جزء منها، كما يستطيع إعادة نسخ نفسه في البرنامج الذي يصيبه العدوى.[2]

ب- **خصائص برنامج الفيروس:** برنامج الفيروس يتميز بالخصائص التالية :

-**القدرة على الاختفاء** :برنامج الفيروس له القدرة على الاختفاء حيث يستخدم عدة وسائل منها دخوله لذاكرة الحاسب كملفات مختفية داخل ملفات أخرى وكذلك عن طريق الاستقرار

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص145.

[2] – أيمن عبد الحفيظ، الاتجاهات الأمنية والفنية لمواجهة الجريمة المعلوماتية ، مطابع الشرطة ، 2005، ص 59.

في أماكن معينة لا يستطيع المستخدم ملاحظتها مثل: ساعة الحاسب كما يقوم برنامج الفيروس بإخفاء أي آثار دالة على وجوده.

- **خاصية الانتشار**: يتميز برنامج الفيروس بالقدرة الكبيرة على الانتشار مستخدما في ذلك وسائل الاتصال الحديثة مثل شبكة الحاسب مهما كانت المسافة بين هذه الأجهزة .
- **خاصية التدمير**: بمجرد تلقي برنامج الفيروس إشارة البدء في عمله كوقت معين تشير إليه ساعة الحاسب أو بمجرد تشغيل برنامج معين فانه يبدأ في تدمير البرنامج بأكمله عن طريق إزالة البيانات أو التعديل فيها.[1]

ج- أعراض الإصابة بالفيروس :تتمثل هذه الأعراض فيما يلي :

- بطء تشغيل الجهاز.
- توقف النظام عن العمل.
- نقص شديد في سرعة الذاكرة المؤقتة.
- ظهور حروف غريبة عند الضغط على مفاتيح معينة.
- تغيير في حجم الملفات وعددها.
- تشغيل القرص أكثر من المعتاد.
- عرض رسالة خطأ فجائية وغير عادية .

[1] – أيمن عبد الحفيظ، المرجع نفسه ، ص61.

- سماع صوت صفارة مع ظهور رسومات على شاشة مصحوبة بتوقف الجهاز.[1]

د- **أنواع الفيروسات وأشهر نماذجها** : تتعدد أنواع الفيروسات ويمكن تقسيمها من حيث تكوينها وأهدافها إلى:

- **فيروس عام العدوى** : ينتقل الى أي برنامج أو ملف.
- **فيروس محدد العدوى** : يستهدف نوعا معينا من النظم لمهاجمته ويتميز هذا النوع عن السابق بأنه أبطء في الانتشار وأصعب في الاكتشاف.[2]
- **فيروس عام الهدف:** وهو ما تندرج تحته الغالبية العظمى من الفيروسات التي تم اكتشافها حتى الآن ويتميز بسهولة إعداد واتساع مدى تدميره.
- **فيروس محدد الهدف:** وهو لا يؤدي الى تعطيل عمل البرنامج بل إلى تغيير الهدف منه، ولا يقتصر هدفه على مجرد التلاعب في البرنامج أو تعديله ويحتاج هذا النوع من الفيروسات الى درجة عالية من المهارة والدراية التامة بالتطبيق المستهدف[3]، ويمكن الإشارة في هذا المجال إلى أهم نماذج الفيروسات التي تم رصدها والتعامل معها:

---

[1]- وليد الكشباطي، جرائم اختراق الأنظمة المعلوماتية، مقال منشور يوم 12 يوليو 2009، على الموقع، http :www.algerie .droit.Fb.bz

[2]- أيمن عبد الحفيظ، المرجع السابق، ص62.

[3]- أحمد خليفة الملط، المرجع السابق، ص 541- 542.

فيروس الإبطاء، الفيروسات النائمة، الفيروسات التطويرية، فيروس حصان طروادة، الفيروس الإسرائيلي، فيروس مايكل أنجلوا، فيروس ناسا.[1]

2- **برنامج الدودة :** هو فيروس يصيب جزءا محددا من نظام المعالجة الالية للمعطيات وهو الجزء الخاص بنظام التشغيل و يهدف هذا البرنامج الى شغل اكبر حيز ممكن من سعة الشبكة ومن ثم العمل على تقليل وخفض كفاءتها واحيانا تتعدى هذا الهدف لتبدا بعدها بالتكاثر و الانتشار في التخريب الفعلي للملفات والبرامج ونظم التشغيل.[2]

3-**برنامج القنبلة المعلوماتية :** وهو عبارة عن برنامج او جزء من البرنامج ينفذ في لحظة محددة او كل فترة زمنية منتظمة ويتم وضعه في شبكة معلومات بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع. [3]

الفرع الثالث : جرائم الاعتداء على المعطيات خارج المنظومة المعلوماتية

جرمت المادة 394 مكرر 2 من قانون العقوبات الجزائري الأعمال التالية:

- تصميم أو تجميع أو بحث أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السالفة الذكر.

1 – أنظر حول أنواع الفيروسات، نهلا عبد القادر المؤمني، المرجع السابق، ص129-130.
2 - نهلا عبد القادر المؤمني ,المرجع السابق,ص131.
3 - احمد خليفة الملط,المرجع السابق,ص55.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي.[1]

أولا: تصميم أو بحث أو تجميع أو توفير أو نشر أو اتجار في المعطيات المستعملة في نظام المعالجة.

لم يكتفي المشرع بتجريم الأفعال المتعلقة بالدخول أو البقاء عن طريق الغش أو الأفعال المتعلقة بتجميع المعلومات بهدف السطو على المنظومة بل قام بتجريم حتى الأفعال التي تهدف إلى استغلال المعلومات المتحصلة عليها من عملية السطو[2]، حيث تنص المادة 394 مكرر 2 "يعاقب بالحبس من شهرين 02 إلى ثلاثة 03 سنوات وبغرامة مالية من 1.000.000 إلى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

تصميم أو بحث أو تجميع أو توفير أو نشر أو اتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها بهذا القسم ".والملاحظة أن المشرع يستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل النظام المعالجة الآلية للمعطيات، أو أن يكون قد تم معالجتها آليا فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص أو تلك

[1] – أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة 15، دار هومة للنشر والتوزيع، 2012 ، ص 495.

[2] – طويجني كمال الدين، محاضرة بعنوان " الجريمة المعلوماتية في التشريع الجزائري " ملقاة للقطب الجزائي المتخصص بسيدي محمد ، في 03-05-2011.

المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية[1] ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات الجزائري.[2]

ثانيا: حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات. جرمت المادة 394 مكرر 02 كل من أفعال الحيازة أو الإفشاء أو الاستعمال لأي غرض كان المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي.[3]

وهذه الأفعال المذكورة يجب أن تكون عمدا أو بطريق الغش أي بتوافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش.[4]

المطلب الثاني: الجزاء المقرر لهذه الجرائم في التشريع الجنائي الجزائري

سنتناول فيما يلي الجزاءات التي قررها المشرع الجزائري لهذا النوع من الإجرام الحديث وطبقا للمادة 13 من الاتفاقية الدولية للإجرام المعلوماتي فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن

عقوبات سالبة للحرية.[5]

---

[1] – فشار عطاءالله ، المرجع السابق ، ص10.

[2] – المرجع نفسه ، ص 10.

[3] – أحسن بوسقيعة ، المرجع السابق ، ص 495.

[4] – فشار عطاءالله، المرجع نفسه، ص11.

[5] – آمال قارة، المرجع السابق، ص 126.

الفرع الأول: العقوبات المطبقة على الشخص الطبيعي والمعنوي

أولا: العقوبات المطبقة على الشخص الطبيعي.

بحكم المواد 394 مكرر، 394 مكرر01، 394 مكرر02، 394 مكرر06 فإنه في حال قيام جريمة من الجرائم السابقة ويكون الجاني شخصا طبيعيا تطبق عليه عقوبة أصلية وأخرى تكميلية.

أ- **العقوبات الأصلية:** تعاقب المادة 394 مكرر من قانون العقوبات الجزائري على جريمة الدخول أو البقاء في المنظومة المعلوماتية بالحبس من 03 أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج.

- وتعاقب المادة 394 مكرر01 من قانون العقوبات الجزائري على جريمة الإدخال أو المحو أو التعديل التي تقع على نظام المعالجة الآلية بالحبس من 06 أشهر إلى 03 سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج .

- وتعاقب المادة 394 مكرر02 بالحبس من شهرين إلى 03 سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا عن طريق الغش بـ :

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو اتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى الجرائم المذكورة أعلاه.

2- حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم المذكورة.[1]

ب-العقوبات التكميلية: نصت المادة 394 مكرر 03 من قانون العقوبات على العقوبات التكميلية إلى جانب العقوبات الأصلية والمتمثلة في:

1- المصادرة: وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسنة النية.

2- إغلاق المواقع: والأمر يتعلق بالمواقع التي تكوم محلا لجريمة من الجرائم العامة بالأنظمة المعلوماتية.

3- إغلاق المحل أو مكان الاستغلال: إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك المقهى الالكتروني التي ترتكب منه مثل هذه الجرائم شرط توفر عنصر العلم لدى مالكها.[2]

ثانيا: العقوبات المطبقة على الشخص المعنوي

مبدأ مسائلة الشخص المعنوي ورد في المادة12 من الاتفاقية الدولية للإجرام المعلوماتي، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا، كما يسأل عن الجريمة التامة أو الشروع فيها كل ذلك يشترط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه .

[1] - أحسن بوسقيعة ، المرجع السابق، ص 496.

[2] - المرجع نفسه، ص 497.

وتنص المادة 394 مكرر04 "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 05 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي ".

الفرع الثاني: عقوبة الاتفاق الجنائي والشروع في الجريمة

لقد عاقب المشرع الجزائري على جريمة الاتفاق الجنائي والشروع في جريمة المساس بأنظمة المعالجة الآلية للمعطيات كسلوكين لم يتحقق فيهما الركن المادي وهذا حفاظا على حقوق الأفراد وحماية حرياتهم.[1]

أولا: عقوبة الاتفاق الجنائي.

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وتبنى المشرع الجزائري في 394 مكرر5 من قانون العقوبات الجزائري مبدأ المعاقبة على الاتفاق الجنائي بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار حيث نصت المادة 394 مكرر 05 على "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية، يعاقب بالعقوبة المقررة بالجريمة ذاتها "[2].

[1] – آمال قارة، المرجع السابق ، ص 129.

[2] – المرجع نفسه ، ص 130.

ثانيا: عقوبة الشروع في الجريمة.

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وتبناه المشرع الجزائري في المادة 394 مكرر 07 من قانون العقوبات الجزائري، فالجريمة الماسة بالأنظمة المعلوماتية لها نص جنحي ولا عقاب على الشروع في الجنح إلا بنص وهذا ما نصت عليه المادة 394 مكرر 07 بقولها: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"[1] يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنص عقوبة الجريمة التامة، ومن خلال استقراء نص المادة تستنتج أن الجنحة الواردة بنص المادة 394 مكرر 05 من قانون العقوبات الجزائري مشمولة بهذا النص، أي أن المشرع الجزائري بهذا يكون قد تبنى فكرة الشروع في الاتفاق الجنائي.[2]

الفرع الثالث: ظروف التشديد

أولا: جريمة الدخول والبقاء إذا حدث تغيير أو حذف.

نصت المادة 394 مكرر 2-3 من قانون العقوبات" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة "إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 06 أشهر إلى سنتين وغرامة من"50.000 دج

[1] – فشار عطاءالله، المرجع السابق، ص13.

[2] – آمال قارة، المرجع السابق ، ص 133.

إلى150.000 دج "[1] وهذه المادة نصت على ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام ويتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتوي عليها النظام وإما عدم صلاحية النظام لأداء وظائفه، ويكفي لتوافر هذا الظرف وجود علاقة السببية بين الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة .[2]

ثانيا: المساس بأنظمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام.

تضاعف العقوبات المقررة للغش المعلوماتي إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد، وهذا ما تؤكده نص المادة 394 مكرر 03 بقولها "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد "[3].

[1] – أحسن بوسقيعة، المرجع السابق، ص 496.

[2] – فشار عطاءالله، المرجع السابق، ص12.

[3] – أحسن بوسقيعة، المرجع نفسه، ص 496.