المحاضرة الثانية والثالثة

الجرائم الماسة بأنظمة المعالجة الالية للمعطيات

إن النهج التجريمي من قبل المشرع الجزائري المتبع في الجرائم الماسة بالمعالجة الالية للمعطيات كان واضحا وشاملا ، غير أن ما يطرح الإشكال بهذا الخصوص هو غياب تحديد معاني الركن المادي والمعنوي بشكل دقيق كما نبينه لاحقا ، مما قد يرتب أثارا إيجابية بالنسبة للمجرمين الذين تسمح لهم الثغرات القانونية بالإفلات من العقاب ، وعلى كل حال فإن جرائم التعدي على النظم المعلوماتية يمكن حصرها في الصور التالية :

- جرائم الاختراق (الفرع الأول)
- جرائم إتلاف المعطيات (الفرع الثاني)
- جرائم إساءة استخدام المعلوماتية (الفرع الثالث) .

الفرع الأول: جرائم الدخول والبقاء غير المشروع للنظم المعلوماتية - جرائم الاختراق

تعتبر هذه الجرائم الأكثر شيوعا في مجال الإجرام المعلوماتي ، والسلوك الإجرامي المحبب والمفضل لمجرمي المعلوماتية ، وسنتناول بالتفصيل كل صورة من هذه الصور الإجرامية على حدى وفق ما يلي :

الفقرة الأولى : طبيعة جرائم الاختراق المعلوماتي

تعرف جرائم الدخول والبقاء غير المشروع ، أو جرائم اختراق النظم المعلوماتية بشكل عام بأنها : القدرة على الوصول لهدف معين بطريقة غير مشروعة (بطريقة الغش) ، عن طريق ثغرات في نظام الحماية الخاص بالهدف ، وهي سمة سيئة يتسم بها المخترق ، لقدرته على دخول أنظمة الآخرين عنوة ودون رغبة منهم ودون علمهم بغض النظر عن الأضرار التي تحدثها ، وتعد هذه الأنشطة الجرمية الأكثر انتشارا .

ويعد الدخول والبقاء غير المشروع أو غير المصرح به للنظم المعلوماتية ، سابقة ضرورية كنشاط إجرامي لأجل ارتكاب جرائم معلوماتية أخرى كإتلاف المعطيات أو سرقتها ، أو التحايل الالكتروني أو التعدي على الأشخاص غير إن مرتكب هذا الفعل قد يقصده دون سواه وهو ما أثار خلافا بين الفئة حول مدى انطباق وصف الجريمة المعلوماتية على هذا النوع من السلوكيات ويمكن تلخيص موقف الفقه في الاتجاهات التالية :

أولا : الاتجاه الداعي إلى عدم تجريم هذا النوع من السلوكيات :

يرى أنصار هذا الاتجاه أنه ومن غير الداعي إلى تجريم مجرد الدخول أو البقاء داخل النظام المعلوماتي ، وخاصة إذا لم يكن الفاعل نية ارتكاب جرائم لاحقة

ثانيا : الاتجاه الداعي إلى ضرورة تجريم فعل الدخول والبقاء غير المشروع :

يرى أنصاره حتمية تجريم هذه السلوكيات حتى ولو لم يكن لدى الفاعل نية ارتكاب جرائم لاحقة ، مستندين في ذلك إلى حجم الخسائر المادية التي تترتب على مجرد حالة الدخول غير المشروع أو حتى محاولة ذلك ، مستهدفين بالخسائر التي لحقت بأحد المصانع الأمريكية المتخصصة في صناعة الأسلحة النووية والتي بلغت 100.00 دولار كتكلفة أبحاث بهدف منع أحد الأشخاص من الدخول إلى نظمها المعلوماتية بصفة متكررة .

ولعل أن هذا الاتجاه هو الأكثر شيوعا وعملا به من قبل أغلب التشريعات التي لا ترى في وجوب تحليل نية المخترق في ارتكاب جرائم لاحقة ، أمرا ضروريا لأجل تجريم الدخول غير المشروع كما هو عليه الحال في التشريع الجزائري حسب نص المادة 394 مكرر – ق 04 -05 قانون عقوبات جزائري تقابلها المادة 323 – 1 قانون عقوبات فرنسي .

الفقرة الثانية : أساليب ودوافع جرائم الاختراق المعلوماتي

يعتمد المجرم المعلوماتي أساليب معلوماتية متنوعة لأغراض إجرامية ، مدفوعا بأغراض ودوافع شخصية تنبأ عن ميولاته الإجرامية ، ويمكن ذكر أهم أساليب الإجرامية وحصرها في :

أولا – أساليبها : يعتمد هذا النوع من السلوكيات على مبدأ التواصل غير المصرح به مع نظام الحاسوب أو شبكة المعلومات ، من خلال استخدام وسيلة اتصال عن بعد أو خلال التواصل عبر نقاط الاتصال الموجودة على الشبكة للدخول إلى نظام حاسوب معين ، بغرض الاطلاع على البيانات أو البرامج المخزنة فيه ، ويتطلب ذلك عادة تجاوز أو كسر إجراءات الحماية المعلوماتية للنظام .

كما يعتمد المخترقون عادة على خطط أخرى لأجل تنفيذ أفعالهم وهي محاولة السيطرة على جدران الحماية (fire wall) وكذلك الهجوم على خادم الملفات العامة (serveur) ، وقد يستعمل المخترق طرق غير هجومية عن طريق الدخول كمستعمل عادي حائز على التصريح ، ثم الولوج إلى شبكة المنشأة ثم الاتصال بالخادم والحصول على المعلومات .

وعلى كل حال فإن محترفي هذه الأنشطة يسعون دائما للاطلاع على معلومات محمية ومشمولة بالسرية ، دون أن ننسى الأهداف اللاحقة التي يمكن أن تتجسد في إتلاف أو إزالة أو استغلال هذه المعلومات بشكل غير شرعي .

ثانيا : دوافعها : لجرائم الاختراق دوافع وأسباب عدة ولو أن العبث وقضاء وقت الفراغ يعد من أبرز عوامل نشوء هذه الظاهرة الإجرامية وبروزها للوجود ، غير أن خبراء الأمن المعلوماتي لخصوا دوافعها في ثلاث نقاط :

1. الدافع العسكري : إن الاعتماد شبه الكامل على أنظمة الحاسوب في المجال العسكري والصراع القائم بين الدول في مجال الدفاع فتح الطريق أمام ظاهرة الاختراق المعلوماتي بهدف التجسس لتوفير المعلومات السرية السياسية العسكرية والاقتصادية .
2. الدافع التجاري : كما هو الحال بالنسبة للصراع بين الدول ، تعيش الشركات التجارية حربا مشتعلة في مجال المنافسة وهو مايجعلها عرضة لمحاولات الاختراق يوميا .
3. الدافع الشخصي : ويشكل هذا الدافع نوعا من أساليب التباهي بالنجاح في إختراق أنظمة الحاسوب ، وهو الدافع المشترك عموما بين فئة طلاب الجامعات والمهتمين بمجال المعلوماتية .

الفقرة الثالثة : أركان جريمة الاختراق المعلوماتي

تقوم جرائم الدخول غير المشروع والبقاء ، على مبدأ عدم احداث اي تأثير سلبي على الانظمة المعلوماتية ، ويقوم بهذا النوع من الانشطة مايطلق عليهم المخترقون ذوي القبعات البيضاء ، الذين يقومون بالدخول بطريقة غير مشروعة لانظمة الحاسوب وشبكات المعلومات ومواقع الانترنت ، مستغلين الثغرات الامنية لتلك النظم ومخترقين اجراءات الامن المعلوماتي وذلك بهدف الوصول الى معلومات محاطة بالخصوصية والسرية ، وقد يتعدى ذلك إلى اتلاف المعلومات وهي جرائم تقوم على ركنين أحدهما مادي والاخر معنوي .

أولا الركن المادي :

لايقوم الركن المادي لفعل الدخول إلى النظام المعلوماتي على مدلول الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه ، بل هو الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول الالكتروني .

ويعتبر فعل الدخول غير المشروع في نظر الفقه الفرنسي إما عن طريق التسلل إلى داخل النظام من خلال الاستعانة بتقنيات المعلوماتية ، سواء في شكل برمجيات خاصة أو عن طريق الشبكة وتسخيرها لأجل عمليات الغش ، وتقوم هذه الجريمة بمجرد دخول الشخص إلى نظام معلوماتي عن طريق الغش أي بدون رخصة أو تصريح إي بدون وجه حق .

وتعتبر جريمة الاختراق شكلية أي أنها تحقق بمجرد تحقق السلوك الاجرامي ، إذ يلزم لتحققها نتيجة ما ، وقد يترتب عليها لاحقا من أضرار بالمعطيات المعلوماتية

والتي تعتبر في نظر العديد من التشريعات ظرفا مشددا للعقاب ولو لم يكن لدى الجاني النية في تحقيق أي نتيجة .

أما بالنسبة لجريمة البقاء غير المشروع داخل نظام معلوماتي فإنها عادة ماتكون نشاطا لاحقا للجريمة الدخول غير المشروع ، أو تعديا على الحق الممنوح بالدخول إلى النظام المعلوماتي من خلال تحديد مدة البقاء القصوى ، ويظهر ركنها المادي على أنه نشاط مكمل لجريمة الدخول غير المشروع ، ويقصد به الحالات التي يكون فيها الدخول إلى أنظمة المعالجة الالية للمعطيات مشروعا متبوعا ببقاء غير مشروع ويتجلى ذلك في حرمان الفاعل من حق البقاء داخل النظام المعلوماتي .

ويتحقق الركن المادي الجريمة البقاء غير المشروع عن طريق الصدفة ، أو الخطأ ، فقد يجد الشخص نفسه داخل النظام صدفة فيقرر البقاء وعدم قطع الاتصال به ، ويعتبر هذه الجريمة شكلية لاتشترط تحقيق أية نتيجة كما أنها جريمة مستمرة ما استمر البقاء بصفة غير مشروعة داخل النظام المعلوماتي .

ثانيا – الركن المعنوي : إن الركن المعنوي في الجريمة هنا ، هو عبارة عن القصد الجنائي بعنصرية ، العلم والارادة ، فالفاعل لابد له من أن يكون على علم بأنه يقوم بفعل الدخول او البقاء غير المشروع الى النظام المعلوماتي ، ولابد من ان تكون ارادته متجهة لارتكاب هذا الفعل .

ففعل الدخول غير المشروع أو البقاء داخل النظام المعلوماتي ، يشكلان جريمة إذا ما تم اقترافهما بطريق الغش (frauduleusement) وهو دليل على ضرورة توفر القصد الجنائي (العلم والارادة) ، وان الفاعل كانت له النية في اتيان فعل مخالف للقانون ، وقد أكد الفقه في فرنسا أن القصد الجنائي فيما يتعلق بهذا النوع من الجرائم يتجلى من خلال الولوج إلى النظام المعلوماتي والبقاء فيه بدون وجه حق ، أو بدون ترخيص من خلال حصر المسؤول عن النظام المعلوماتي لحق الدخول لاشخاص دون غيرهم ، وبالتالي فإن غياب الحق في الدخول أو البقاء هو تعبير عن إرادة القائم على النظام المعلوماتي .

وقد أكد ذلك المشرع الفرنسي بهذا الخصوص في نص المادة 323 قانون عقوبات فرنسي ، وهو ماسار عليه المشرع الجزائري الذي اعتبر هذه الجرائم عمدية إذا ما اقترفت بطريق الغش ، أي اللجوء الى استعمال اساليب تقنية من نوع خاص تسمح للشخص الممنوع من الدخول بالدخول والبقاء في مجال الكتروني محظور ، وذلك حسب ماجاء في نص المادة 394 مكرر ق 04 -05 قانون عقوبات

الفقرة الرابعة : المقررة لجريمة اختراق النظم المعلوماتية .

بالرغم من كون هذا النوع من الجرائم ذات طابع شكلي ، إلا أن أغلب التشريعات قابلتها بجزاءات عقابية حتى ولو لم يترتب عليها ضرر ، وهو حال المشرع الجزائري الذي نص عليها في مضمون المادة 394 مكرر ق 04 -05 قانون عقوبات .

والملاحظ من خلال إستقراء الفقرة التالية من نفس المادة وهو تشديد المشرع للعقوبة المقررة من خلال مضاعفتها إذا ماترتب عن الجريمة الأولى حذف أو تغير بمعطيات المنظومة المعلوماتية ، أما إذا ماترتب عنها تخريب للنظام المعلوماتي أي تعطيله عن أداء مهامه فإن العقوبة تكون بالحبس 06 ستة أشهر إلى سنتين 02 وغرامة من 50.000 دج إلى 150.000 دج ، كما نص المشرع في نص المادة 394 مكرر 03 ق 04 -05 على تشديد العقوبة بمضاعفتها إذا ما تعلقت الجريمة بمصالح الدفاع الوطني والمؤسسات والهيئات العامة ، والملاحظ أن المشرع الجزائري كان شديدا وصارما في تقرير العقوبة بالرغم من أن الجريمة شكلية ، وترجع العلة في ذلك إلى الغاية المرجوة ، وهي تحقيق مفهوم الردع من المنشأ ، أي وضع حد لهذا النوع من السلوكيات على اعتبار أنها بوابة الجرائم اللاحقة .

يقابل نص المادة 394 مكرر ق 04 -05 قانون عقوبات جزائري نص المادة 323-1 قانون عقوبات فرنسي التي تقر بعقوبة الحبس لمدة سنتين 02 دون تحديدها كحد أدنى أو أقصى ، وبغرامة قدرها 60.000 أورو لمجرد ارتكاب هذه الافعال ، وهي عقوبات مشددة مقارنة بما جاء في نص المادة 394 مكرر ق 04 -05 قانون عقوبات جزائري ، ويرجع السبب أساسا إلى مدى انتشار تقنية المعلوماتية في هذه الدولة وبالتالي مدى الضرر الذي قد تلحقه هذه السلوكيات بالسير الحسن للمؤسسات الفرنسية .

أما من ناحية التشريعات العربية المقارنة فإن المشرع السعودي قد نص في المادة 07 من قانون مكافحة جرائم المعلوماتية ، على عقوبات شديدة مقدارها 10 سنوات سجنا وبغرامة قدرها 05 ملايين ريال سعودي ضد كل شخص يرتكب مث هذه الافعال لاجل الحصول على بياغنات تمس الامن الداخلي أو الخارجي للدول أو اقتصادها الوطني .

إذن ما يمكن استخلاصه أن جرائم الاختراق المعلوماتي وبالرغم من طابعها الشكلي نظرا لارتباطها بمظاهر اجرامية لاحقة تعتبر اشد خطورة ، ضف الى ذلك طابع الخصوصية والسرية الذي يحيط بالمعلومات المتحصلة بطريق الغش والتي يمكن أن تستعمل ضد المصالح الحيوية للدولة .

الفرع الثاني : جرائم الاتلاف المعلوماتي – اتلاف المعطيات .

بعد تعرضنا لجرائم الدخول والبقاء غير المشروع داخل النظم المعلوماتية ، نستعرض نوعا آخر من الجرائم المعلوماتية يعرف بوصف جرائم الاتلاف المعلوماتي ، والتي تعتبر عادة نيجة حتمية للجريمة الاولى فما هي ياترى طبيعة هذه الجريمة .

الفقرة الأولى : تعريف جرائم الاتلاف المعلوماتي .

قد نلتبس ونحن نعرف جرائم اتلاف النظم المعلوماتية لما قد مايتبادر للذهن بأننا الجرائم التي تقع على الحاسوب بمكوناته المادية أو الشبكة المتصلة بها .

فالمقصود بهذه الاخيرة هي تلك الجرائم التي ينتج عنها اتلاف المكونات المادية كالاتلاف الذي يقع على الشاشة او الطابعة او الاقراص المضغوطة ، او اسلاك ربط الشبكة ، وهذه الصورة تنطبق عليها نصوص قانون العقوبات التقليدية التي تتناول بالتجريم فعل اغلاتلاف الذي يؤدي الى الحاق الضرر بالمال المنقول .

أما جرائم الاتلاف المعلوماتي فهي كما وضحتها المذكرة التفسيرية لاتفاقية بودابست لسنة 2001 بانها ، " تخريب نظم الحاسوب بهدف الاعاقة العمدية للاستخدام الشرعي للنظم المعلوماتية بما في ذلك نظم الاتصالات باستخدام او التاثير على بيانات الحاسوب " ، ومصطلح الاعاقة يرتبط بالافعال التي تحمل اعتداءا على حسن تشغيل نظام الحاسوب ، وهذه الاعاقة تكون ناجمة عن ادخال او نقل او محو او اتلاف او طمس او الاضرار بالبيانات المعلوماتية .

ولقد اورد المشرع الجزائري تعريفا لهذا النوع من الجرائم وذلك وفق مانصت عليه المادة 394 مكرر 01 ق 04 -05 قانون عقوبات جزائري ،وهو التعريف الوارد في نص المادة 323 -2 و 3 من قانون العقوبات الفرنسي ، ويمكن استخلاص من التعريفين ان طبيعة هذه الجرائم ترتكز على اسلوبين اساسيين هما : اعاقة سير النظم المعلوماتية و المساس بسلامة المعلومات .

الفقرة الثانية : الركن المادي لجريمة الاتلاف المعلوماتي

لجريمة الاتلاف المعلوماتي و على غرار الجرائم الاخرى الخاضعة لمبدأ شرعية الجرائم والعقوبات ، ركن مادي تقوم عليه الجريمة وذلك بالرغم من الطابع المنطقي لها وصور الركن المادي لهذه الجريمة هي :

أولا : إعاقة السير العادي للنظم المعلوماتية :

أولا نشير الى ان المشرع لم يتعرض في نص المادة 394 مكرر 01 ق 04-05 قانون عقوبات جزائري ، الى مفهوم اعاقة السير العادي للنظم المعلوماتية ، وهو السلوك الاجرامي الذي اولته اتفاقية بودابست اهمية بالغة وقد تجلى ذلك في نص القانون الفرنسي .

يقصد باعاقة سير عمل النظام المعلوماتي ،" ذلك الفعل الذي يسبب تباطؤا في عمل النظام او ارتباكا ، مما يؤدي الى تغير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت "

ويتحقق الركن المادي لهذا النوع من الجريمة من خلال وقوع اعتداء على نظام معلوماتي يسبب ارتباكا في عمله قد يكون دائما في حال استعمال الفيروسات ، او مؤقتا يهدف الى شل او تعطيل النظام كما هو الحال في حالة استعمال القنابل المنطقية ، او من خلال اغراق الخادم بالرسائل الالكترونية لاجل الحد من قدرته على التعامل مع المعلومة .

وعلى كل حال فانه يجب ان تكون الاعاقة دون وجه حق ، وبالتالي فان اولئك الذين تكون لهم الحق في اطار ممارسة انشطة تصميم الشبكات او تشغيلها وصيانتها واختبارها ، لاتعتبر انشطتهم غير شرعية اذا ما تسبب في اعاقة النظام .

ثانيا : المساس بسلامة المعلومات : ان المساس بسلامة المعلومات Atteintes a l'intégrité des donnés كسلوك مجرم محصور في فعل الادخال ، التعديل ، الحذف للمعطيات المعلوماتية المخزنة في ذاكرة الحاسوب ، أو على الشبكة هو ما أنفقت عليه اغلب التشريعات كما جاء في نص المادة 394 مكرر 01 ق 04 -05 قانون عقوبات جزائري ، المادة 323-3 قانون عقوبات فرنسي ، المادة 05 من نظام مكافحة الجريمة المعلوماتية السعودي ، ويقوم الركن المادي لهذه الجريمة من خلال :

1. حذف اي محو البيانات كليا وتدميرها الكترونيا ، كمحو الذاكرة الرئيسية للحاسوب ، او استعمال برمجيات خفية تعمل على محو محتوى الحاسوب او الشبكة .
2. تعديل البرامج والمعطيات المعلوماتية من خلال :
   أ. التلاعب بالبرامج اي بالنظام المعلوماتي بشكل يؤدي الى اخفاء البيانات كليا او جزئيا .
   ب. اختلاس البرامج ويكون عن طريق نسخها عن طريق اسلوب التجسس .
   ج. تغيير نظم عمل البرامج اي تزويدها بتعليمات اضافية تتيح الوصول الى جميع المعطيات التي يتضمنها الحاسوب .
3. ادخال برامج جديدة : اي اصطناع برنامج كامل او ناقص في الناحية الفنية يخصص لارتكاب فعل الغش المعلوماتي .

الفقرة الثالثة : الركن المعنوي لجرائم الاتلاف المعلوماتي .

يتحقق الركن المعنوي بتحقيق السلوك المادي المقترن وجوبا بالقصد الجنائي (الارادة العمدية) ، باستثناء الحالات المرخص لها ادخال تعديل او حذف جزء من النظام المعلوماتي ، ويعتبر قائما هذا الركن من لحظة ادخال او تعديل او حذف جزء من النظام المعلوماتي ، ويعتبر قائما هذا الركن من لحظة ادخال او حذف المعلومات المقترنة بارادة احداث تعديل على النظام المعلوماتي ، مهما كانت النتيجة المتوقعة على النظام .

أما فيما يخص عنصر العلم فانه يتحقق اذا ماكانم الفاعل يعلم بان المحل المعتدي عليه (النظام المعلوماتي) ملك للغير ، وان فعله بالادخال او الحذف والتعديل هو فعل من شانه احداث تلف او اعاقة للنظام المعلوماتي عن اداء مهامه بشكل طبيعي ، ولعل أن تمييز مصطلح " بواسطة الغش Frauduleusement " في نص المادتين 394 مكرر 1 ق 04-05 من قانون العقوبات الجزائري ، والمادة 323 – 2 و 3 من قانون العقوبات الفرنسي ماهو الا دلالة على تاكيد المشرع بضرورة توافر القصد الجنائي لاجل قيام المسؤولية الجنائية في مجال هذا النوع من الجرائم ، وبالتالي تستثني من نطاق التجريم نفس الافعال اذا لم تقترن بنية احداث الضرر .

الفقرة الرابعة : الوسائل الفنية لتنفيذ جرائم الاتلاف المعلوماتي .

تتنوع اساليب جرائم اتلاف المعلومات وانماطها ولايمكن حصرها ولا التنبؤ بمستقبلها ، نظرا للنسق المتسارع لتطورها و ازدياد معدل الاعتداءات المعلوماتية من يوم لاخر فقد افادت شركة kaspersky المختصة بالامن المعلوماتي في تقريرها السنوي ل 2014 بان منتوجاتها الخاصة بالحماية نجحت في التصدي ل 6.167.233.068 مليار هجمة الكترونية عن طريق البرامج الخبيثة ، وهو مايدل على تعدد وسائل تنفيذ الاعتداءات الالكترونية واتاحتها امام مجرمي المعلوماتية ويمكن حصر او تصنيف هذه الوسائل الى ثلاث طوائف رئيسية هي :

أولا الفيروسات الخاصة بالحاسوب : الفيروس هو " شفرة حاسوبية " ، أو برنامج ذو قدرة هائلة على التناسخ ، يستطيع الصاق نفسه ببعض الملفات والبرامج الحاسوبية ، كما يملك القدرة على الانتقال من حاسوب لاخر بواسطة الشبكة ، وللفيروس اثار مدمرة وفي احسن الاحوال فهي مزعجة ، وقد تتسبب الفيروسات في حذف كامل محتوى القرص الصلب للحاسوب ، أو تحذف بعض اجزاء نظم التشغيل المهمة أو تحتل مساحة مهمة على القرص الصلب للحاسوب فتعيق عمله .

عادة مايكون الفيروسات مرافقة ومخزنة على البرامج التطبيقية ، وبرامج التشغيل ، وتنشط في حالة نسخ البرامج من جهاز لاخر ، او عن طريق الشبكات (الانترنت) ، فتكون مخبئة في الرسائل الالكترونية ، وقد تكون عامة العدوى أي تنتقل من برنامج لاخر وتعطل نظام

تشغيل الحاسوب برمته ، أو محددة العدوى اي انها تستهدف نوعا معينا من النظم فتعطل عمل الحاسوب جزئيا .

ومن اشهر الفيروسات الموجهة ضد الانظمة والحواسيب هي :

1. فيروسات الابطاء : وتعمل على ابطاء الحاسوب عن العمل تمهيدا لتوقيفه .
2. الفيروسات النائمة : وهي فيروسات تظل منكمشة الى حين انطلاقها ، لاجل تدمير وتعطيل نظم تشغيل الحاسوب .
3. الفيروسات التطورية : وهي فيروسات لها القدرة على تغيير شكلها والتاقلم مع مضاد الفيروسات ، تعمل على تخريب وتعطيل النظام .
4. حصان طروادة : تختبئ هذه الفيروسات ضمن برامج تبدو بريئة وعندما يتم تشغيلها ينشط الجزء الماكر منها ، فتقوم بممارسة عملها وهو السيطرة على الجهاز واتلافه من خلال جمع المعلومات عن اسم المستخدم وكلمة السر وارسالها لصاحب الفيروس ، اثناء اتصال المستخدم بالشبكة كما يسمح بتصفح الجهاز والتحكم فيه عن بعد وبملفاته بشكل كامل .
5. ثانيا : برامج الدودة (worm soft wear) : هي عبارة عن برمجيات تقوم بالانتقال من حاسوب لباخر ، دون الحاجة الى تدخل الانسان من اجل تنشيطها ، فهي تعمل بصفة خاصية التنشيط الذاتي ، وبذلك فهي تختلف عن الفيروسات ، كما انها تلتصق بنظام التشغيل للحاسوب الذي تصيبه ، وتسبب عادة حركة الدودة تعطيل الحاسوب ، من خلال تجميد لوحة المفاتيح أو الشاشة ، كما تعبئ الذاكرة وتبطل من عمل الحاسوب .

ولعل أن اشهر انواع الدودة المعلوماتية هي دودة موريس ، التي اطلقها هذا الطالب الامريكي روبرت موريس – Robert Morris في جامعة كورنان عام 1988 عمدا بهدف اثبات ضعف شبكة الانترنت من حيث الامان ، وهو ماتسبب في تدمير 16 الف شبكة عبر الولايات المتحدة الامريكية ، اضافة الى تعطيلها لعدة ايام وقد حكم عليه بالحبس لثلاث 03 سنوات و 10500 دولار كغرامة و 400 ساعة عمل عقوبة النفع العام .

ثالثا : القنابل المعلوماتية : وهي نوع من البرامج الخبيثة تعمل على شكل قنبلة تقليدية ، غير أنها الكترونية ، وهي نوعان :

1. القنابل المعلوماتية المنطقية : هي عبارة عن برامج صغيرة الحجم ، يتم إدخالها بطرق الغش مع برامج اخرى تهدف الى تدمير وتغيير برامج ومعلومات النظام في لحظة محددة أو خلال فترات زمنية منتظمة بحيث تعمل على مبدأ التوقيت ، فتحدث دمارا أو تغيرا في المعلومات والبرامج عند إنجاز أمر معين في الحاسوب أو البرنامج من قبل المستخدم .

2. القنابل المعلوماتية الزمنية : عكس الاولى فهذه تحدث دمارا وتغيرا في لحظة زمنية محددة بالساعة واليوم والسنة ، ويتم إدخالها في برنامج معين وتنفذ في جزء من الثانية ، أو في ثواني أو دقائق معدودة وفقا لتاريخ محدد سلفا .

ففي فرنسا مثلا قام محاسب خبير في نظم المعلومات وبدافع الانتقام على اثر فصله من عمله بزرع قنبلة زمنية في شبكة المعلومات الخاصة بالمؤسسة وانفجرت بعد 06 اشهر من رحيله مما خلف تلفا كليا للبيانات المتعلقة بالشركة .

كل هذه تعتبر وسائل يستعين بها مجرمو المعلوماتية بهدف تحقيق اغراضهم الاجرامية التي تتمثل عادة في اتلاف المعلومات والنظم المعلوماتية على حد سواء ، وما ذكرنا لهذه الوسائل ماهو الا استشهاد باهمها واقربها الى فهمنا ، فهناك الالاف من الوسائل الحديثة والمستحدثة بما يفوق مجال اختصاصنا ويتعدى اطارنا القانوني لاجل وصفها .

الفرع الثالث : جرائم اساءة استخدام المعلوماتية .

تناولت اغلب التشريعات ، والاتفاقيات سواء الدولية او الاقليمية بتحديد المفاهيم المتعلقة بمحاربة الجريمة المعلوماتية باعتبارها سلوكا يهدد ويشجع على الاعتداء على المصالح العامة والخاصة ، في شاكلة الجرائم التقليدية (كالقتل ، السرقات ، الاعتداء على الغير ...) ، ومن المفاهيم التي تطرقت لها التشريعات هو المفهوم المتعلق بتجريم صور السلوكيات التي تعتمد على اساءة استخدام النظم المعلوماتية ، نظرا لما قد تقدمه هذه السلوكيات السلبية من تشجيع وتيسير للمجرمين المعلوماتيين في اتيان الافعال المجرمة المذكورة سالفا (الدخول والبقاء غير المشروع ، الاتلاف المعلوماتي) ، على اعتبار ان هذه الجرائم تعتمد على توفير المعلومات من خلال عرضها للبيع او اتاحتها بصفة مجانية على شبكة الانترنت او على وسائط تخزين خارجية ، لغرض استعمالها في اتيان الجرائم المعلوماتية .

الفقرة الاولى : تعريف جرائم اساءة استخدام المعلوماتية .

وجدت هذه الجرائم مجالا تعريفيا في نصوص القانون ، فقد عرفها المشرع الجزائري من خلال نص المادة 394 مكرر 02 ق 04 -05 قانون عقوبات جزائري . ولعل مفهومها يتضح بشكل افضل وفق نص المادة 09 من الاتفاقية العربية لمكافحة جرائم التقنية الحديثة بوصفها لجرائم اساءة استخدام وسائل تقنية المعلومات

وقد تعرضت اتفاقية بودابست قبل ذلك (2001) الى تجريم هذا النوع من السلوكيات باعتماد نفس الصياغة وذلك وفق ما جاء في نص مادتها السادسة (06) ، وما يمكن ملاحظته ان اغلب النصوص التشريعية قد نصت على تجريم افعال اساءة استخدام الحاسوب بالرغم من انه سلوك لايترتب عنه اي ضرر يمس بامن وسلامة النظم المعلوماتية ، باعتباره سلوك خارجي يتم بعيدا عنها ، غير انه ومن جهة

اخرى يتيح الاستفادة من الوسائل المادية او البرمجيات لارتكاب الجرائم المعلوماتية السالفة الذكر .

اما ما يمكن استخلاصه من خلال استقراء نص المادة 394 مكرر 02 ق . 04-05 قانون عقوبات جزائري مقارنة بالنصوص السالفة الذكر ، أن المشرع الجزائري لم يعتمد على الدقة بالشكل المناسب في توضيح مفهوم هذا النوع من الجرائم ، فنلحظ استعماله لاوصاف متعددة تفتقر للدقة ، كوصف فعل التجميع أو البحث عنها او تصميمها او تجميع الوسائل المادية او البرامج ؟ وذلك بالرغم من انه ربطها بفعل الغش غير انها تظل غامضة من حيث المفهوم القانوني .

فقد كان على الأحرى على المشروع الجزائري توظيف مصطلحات تقنية قانونية اكثر دقة وشمولية وتناسبا مع موضوع التجريم ، اسوة بما قدمه نظيره السعودي في نص المادة 06 من قانون مكافحة الجرائم المعلوماتية السعودي ، وقد نرجع سبب عدم دقة النص العقابي الجزائري من حيث تحديد معالم التجريم الى قدمه اساسا ، فتاريخ سن القانون يعود الى سنة 2004 اين كانت مفاهيم الجريمة المعلوماتية غير مستقرة بعد ، ولكنه لا يعتبر سببا كافيا يمنع المشرع الجزائري من التدخل مرة اخرى بوضع قوانين حديثة متماشية وتطور الجريمة المعلوماتية .

الفقرة الثانية : اركان جريمة اساءة استخدام المعلوماتية .

تقوم هذه الجرائم على توفير عنصرين اساسيين هما :

أولا : الركن المادي : يشكل هذا السلوك الاجرامي جريمة جنائية منفصلة ومستقلة ، تتمثل في ارتكاب افعال غير مشروعة ذات طبيعة خاصة ترتبط ببعض الاجهزة او البرامج او بيانات الدخول ، في صورة اساءة استخدامها بغرض اتاحة جرائم معلوماتية اشد واخطر ، ان ارتكاب هذه الجريمة يستلزم عادة وفي غالب الاحيان حيازة وسائل الولوج مثل ادوات وبرامج القرصنة او اي وسائل اخرى بغرض استعمالها لاغراض اجرامية ، الامر الذي يؤدي في النهاية الى خلق نوع من السوق السوداء لانتاج وتوزيع مثل هذه الادوات كما هو عليه الحال في الفضاء السيبرني الحديث المعروف ب (the dark net) ويمكن حصر الركن المتادي لهذه الجريمة في تحقق السلوكيات التالية :

- تصميم برامج تساعد على الدخول غير المشروع داخل النظام المعلوماتية .
- تصميم برامج تساعد على إتلاف المعلومات كبرامج الفيروسات .
- البحث وتجميع المعلومات والبرامج التي تساعد على ارتكاب الجرائم الأخرى .
- توفير ونشر كل ما من شأنه المساعدة على ارتكاب الجرائم المعلوماتية .
- الاتجار في كل وسائل ارتكاب الجرائم المعلوماتية .

ثانيا الركن المعنوي : تعتبر هذه الجرائم ذات طابع عمدي وهو مانستنتجه من نصوص قانون العقوبات الجزائري في نص المادة 394 مكرر 02 ق 04 -05 التي أكد فيها المشرع على ضرورة توفر عنصر القصد الجنائي من خلال استخدامه لعبارة " عمدا أو عن طريق الغش " وبالتالي فإنه تستبعد من مجال التجريم الحالات التي لا يتوفر فيها القصد الجنائي اي صور الخطأ .

وعلى كل حال فإنه يشترط لقيام هذه الجريمة ان ترتكب عمدا وبدون وجه حق اي يتوفر القصد الجنائي العام ، اضف الى ذلك يجب توفر نية خاصة او قصد جنائي خاص يتمثل في استخدام جهاز الحاسوب والشبكة لاجل ارتكاب الجريمة المشار اليها ، واستنادا ممن ذلك نخرج من دائرة التجريم الادوات والبرامج المصرح بها لاجل استخدامها من اجل اختبار او حماية جهاز الحاسوب .

الفقرة الثالثة : العقوبات المقررة لجرائم اساءة استخدام المعلوماتية :

أقر المشرع الجزائري بعقاب كل من يعتمد او يستعمل طريق الغش لاجل ارتكاب جرائم اساءة استخدام المعلوماتية بعقوبة الحبس من (02) شهرين الى (03) سنوات وبغرامة من 1.000.000 دج الى 5.000.000 دج وتضاعف هذه العقوبة اذا ما مست بامن الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للنظام العام ، دون الاخلال بمبدأ تطبيق عقوبات اشد اذا تعدت من حيث النتيجة او القصد ما كان مقررا بدءا .

والملاحظ انها عقوبات تقليدية تتراوح ما بين العقوبات البدنية والمالية لا يتعدى حدها الأقصى 03 سنوات الا في الحالة التي تمس فيها بالمصالح العليا للبلاد فانها تضاعف اي تصل لمدة اقصاها (06) ستة سنوات فالمشرع الجزائري حاول قمع هذه الجريمة باعتبارها نشاطا خطيرا يهدد امن وسلامة النظم المعلوماتية خصوصا تلك الخاضعة لتحكم مؤسسات الدولة ، واذا ما قارنها بما هو وارد في نص المادة 323 -3-1 قانون عقوبات فرنسية ، فإننا نلاحظ ان المشرع الفرنسي كان ذكيا في مجال قمع الجرائم وربطها بمدى تحقق النتيجة الاجرامية وامكانية تحقق جرائم لاحقة عنها ، وذلك حتى يغلق باب الاتاحة المعلوماتية اساسا ولا يترك مجالا للمناورة امام النص القانوني ويرجع السبب في ذلك الى اتقان النظام الخاص بمكافحة الجريمة المعلوماتية ودقته عكس التشريع العقابي الجزائري الذي يحتاج الى ثورة قانونية يشترك فيها الفنيون القائمون على مجال النظم المعلوماتية والقانونيون على حد سواء من اجل تحديد دقيق لمفاهيم هذه السلوكيات من الناحية الفنية والتقنية والقانونية اساسا .