المستوى : السنة أولى ماستر(تخصص القانون الجنائي و العلوم الجنائية)
محاضرات : الجريمة المعلوماتية : للدكتورة : خلدون عيشة

المحور الأول : مفهوم الجريمة المعلوماتية :

المعلوماتية هي علم المعالجة الآلية للمعلومات ، و لمعرفة ماهية الجريمة المعلوماتية يجب التعرض لمفهوم كل من المعلومات و المعلوماتية.

مفهوم المعلومات : هي جمع كلمة معلومة و لا يوجد في وقتنا الحاضر إجماع في الفقه أو القانون على تعريف جامع و مانع للمعلومة ،فقد عرفها القانون الفرنسي رقم 652/82 الخاص بالإتصالات السمعية و البصرية بأنها "رنين صور الوثائق أو الوسائل من أي نوع." كما عرفها بعض الفقه بأنها "تلك التي تضيف شيئا ما إلى النموذج العقلي و إلى الإنطباع الذهني الذي نعرفه عن العالم الخارجي في لحظة معينة."

مفهوم المعلوماتية : هي طاهرة إجتماعية و علمية نشأت و إزدهرت مع تقدم الحضارة الإنسانية ، تستعمل كوصف للوقت الحالي و تتكون من مقطعين الأول كلمة المعلومات و الثاني كلمة آلي أو أتوماتيك التي تعني المعالجة الآلية للمعلومات.

و قد عرفتها الأكاديمية الفرنسية في جلستها المنعقدة في 1976/04/06 بأنها:" علم التعامل العقلاني ، بواسطة آلات أتوماتيكية مع المعلومات ، كونها دعامة للمعارف الإنسانية و عمادا للإتصالات في ميادين التقنية و الإقتصاد و الإجتماع."

تعريف الجريمة المعلوماتية:

لقد تعدد المصطلحات المستخدمة للدلالة على هذه الجريمة و تحديد مفهومها ، فهناك من يطلق عليها إسم جرائم الحاسبات أو إساءة إستخدام الحاسبات أو الجرائم المرتبطة أو المتعلقة بالحاسبات أو الجرائم الإلكترونية و جرائم الكمبيوتر و جرائم المعلوماتية التي تعتبر التسمية الأقرب لهذا النوع من الجرائم .

و كلها مصطلحات إنعكست على تعريف هذه الجريمة التي إختلف الفقه حول إعطائها تعريف جامع و مانع ، حيث عرفها البعض على أنها أي جريمة ضد المال مرتبطة

بإستخدام المعالجة الألية للمعلومات ، و أيضا تعرف على أنها الإعتداءات غير القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربـح .

-كما عرفت بأنها مجموعة من الأعمال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب ، أنها مجموعة الجرائم المتعلقة بعلم المعالجة المنطقية للمعلومات .

فالملاحظ على تعريفات هذه الجريمة أنه هناك منها ما تعتمد على معيار أداة إرتكاب الجريمة و أخرى تعتمد على معيار أ و محل هذه الجريمة و ثالثة تعتمد على معيار توافر المعرفة بالتقنية المعلوماتية و رابعة تمزج بين معياري موضوع الجريمة و أداة إرتكابها.

و هناك من رجح تعريف منظمة التعاون الإقتصادي و التنمية الخاص باستبيان الغش المعلوماتي عام 1982 و الوارد في تقرير بلجيكا الذي بين بأنها عبارة عن " كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات."

و كتعريف شامل للجريمة المعلوماتية فهي عبارة عن كل عمل أو امتناع عن عمل غير مشروع يتم بواسطة الحاسوب أو أي جهاز معالجة آلية للمعطيات المعلوماتية سواء كان الجهاز أداة لإرتكاب الجريمة أو محل لإرتكاب الجريمة في مجال إلكتروني أو معلوماتي مغلق أو مفتوح على شبكات المعلوماتية أو محيط لإرتكاب الجريمة والتي يجب أن تتوفر لدى فاعلها الأصلي المعرفة الكافية لإرتكابها.

وفيما يخص التعريف القانوني للجريمة المعلوماتية فلم يضع المشرع الفرنسي لها تعريف واضح و شامل و ترك ذلك للفقه ، و كذا المشرع الجزائري الذي أعطى لها تعريف عام خال من أي دقة مكتفيا مؤخرا من خلال القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، بنصه على أنها :" كل الجرائم سواء المتعلقة بالمساس بالأنظمة أو غيرها من الجرائم الأخرى التي ترتكب أو يسهل إرتكابها بإستعمال منظومة معلوماتية أو أي نوع آخر من نظم الإتصال الإلكتروني."

أطـراف الجريمة المعلوماتية (أشخاصها) :

لكل جريمة طرفين أساسيين هما الجاني و المجني عليه ، بحيث يتميز الجاني في الجريمة المعلوماتية بصفات خاصة تتضح من خلال :

الطرف الأول : المجرم المعلوماتي (الفاعل الأصلي)

قد يكون شخص طبيعي أو شخص معنوي يتصف بكونه مجرم غير عادي ، و إنما مجرم ذا مهارات تقنية و معرفة عالية بنظام الحاسوب و وسائل التكنولوجيا الحديثة الأخرى بعكس المجرم التقليدي الذي يعتمد على القوة العضلية أكثر من الذكاء.

كما يتصف المجرم المعلوماتي بأنه يملك سلطة ما على النظام المعلوماتي المستهدف العبث به تجعله مسيطرا و متحكما نوعا ما ، بحيث تكون هذه السلطة مباشرة مثل من يملك الشفرة الخاصة بالدخول إلى النظام المعلوماتي الحاوي على المعلومات ، و قد تكون سلطة غير مباشرة مثل من يملك التصريح بالدخول إلى غرفة الأنظمة المعلوماتية المتمثلة في الحاسبات الآلية و أدواتها دون الحق في الولوج إلى نظام معلوماتي معين.

كما يتميز بأنه إنسان إجتماعي كثير الخطورة الإجرامية ، و هو الأمر الذي جعل البعض يرى بأن صفة الذكاء لدى هذا المجرم المعلوماتي ماهي إلا القدرة على التكيف مع المجتمع.

كما ذهب البعض للقول بأن أغلب مجرمي المعلوماتية لا يشعرون بالمسئولية عن أفعالهم الإجرامية ، فهم يعدونها مباحة و لا يستحقون العقاب عليها، فهي سلوكات مقبولة و شائعة يقبل أغلب العاملين في المؤسسات على القيام بها سواء لتحقيق الربح الشخصي أو لمجرد التسلية و تمضية الوقت أو بسبب المنافسة التي تدفعهم لإرتكاب هذه الجرائم كنوع من الإثارة و المزاحمة.

و قد يكون المجرم المعلوماتي فاعلا أصليا أو شريكا في إرتكاب الجريمة ، فصفة الفاعل الأصلي قد ترتبط بأحد العاملين أو المستخدمين في منشأة تدار بالنظام المعلوماتي بغض النظر عن المستفيد من إرتكاب هذه الأعمال.

و بما أن الجريمة المعلوماتية تتطلب الدقة و التنفيذ للعمليات الغير مشروعة فإنه يستلزم وجود مشاركة أو مساعدة أشخاص آخرين سواء كانوا فنيين أو مجرد وسطاء يساعدون في حدوث و إنجاح العملية غير المشروعة.

-تصنيف مجرمي المعلوماتية :

يصنف مجرمي المعلوماتية إلى ثلاث طوائف هم المخترقون و المحترفون و الحاقدون .

الطائفة الأولى : المخترقون : تضم نوعين من المتطفلين هم :

1/ الهاكرز: تتألف هذه الطائفة من مراهقين و شباب في حالة دراسة أو عاطل عن العمل تتراوح أعمارهم مابين 18 و 35 سنة بارعين في إستخدام الحاسب الآلي و برامجه ،

يتصدون إجراءات أمن نظام الشبكات بدافع التصدي و إثبات الذات دون أن تتوفر لديهم أي دوافع حاقدة أو تخريبية.

2/ الكراكرز: طائفة إستفادت كثيرا من التقنيات المطورة من قبل فئة الهاكرز بإستخدامها في إعتداءات ذات ميولات إجرامية ، بحيث يقومون بالتسلل إلى نظم الحاسوب للإطلاع على معلوماته المخزنة أو لإلحاق الضرر أو العبث بها أو سرقتها.

و السمة المميزة لهم تبادلهم المعلومات فيما بينهم و تنظيم مؤتمرات لمخترقي الكمبيوتر تضم مجموعة من الخبراء للتشاور حول وسائل كل من الإختراق و تنظيم عملهم.

الطائفة الثانية: المحترفون : هم أخطر طائفة من بين مجرمي الكمبيوتر و الإنترنت تتراوح أعمارهم مابين 25 و 40 سنة ، تهدف إعتداءاتهم إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم لإرتكاب جرائم الحاسوب ، كما تهدف إلى تحقيق أغراض سياسية أو التعبير عن موقف فكري أو نظري أو فلسفي .

و هم أفراد يتسمون بالتكتم فلا يتبادلون المعلومات بشأن أنشطتهم ، و يطورون معارفهم دون الكشف عن طرقهم التقنية لإرتكاب جرائمهم.

الطائفة الثالثة : الحاقدون : هم طائفة غير محددة الأعمار و لا تتوفر لديهم نفس أغراض و أهداف الجريمة المتوفرة لدى الطائفتين السابقتين ، و إنما تحركهم الرغبة بالإنتقام من صاحب العمل كونهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة ، أو الإنتقام كغرباء من المنشأة المستهدفة في نشاطهم .

و رغم عدم إكتسابهم المعرفة التقنية الإحترافية إلا أنهم يسعون للإحتراف في أنشطتهم التي يغلب عليها إستخدام تقنيات الفيروسات و البرامج الضارة و تخريب النظم و تعطيل النظام أو موقع الإنترنت المستهدف.

كما يتميز أعضاء هذه الطائفة بعدم التفاعل بينهم و إخفاء نشاطاتهم التي تعتبر الأسهل إكتشافا مقارنة بنشاطات المحترقين و المحترفين.

<u>الطرف الثاني : المجني عليه في الجريمة المعلوماتية:</u>

قد يكون شخص طبيعي أو معنوي و يسمى بالضحية المعلوماتية نسبة للمصطلح المعتمد من قبل الجمعية العامة للأمم المتحدة في قرارها رقم 40/34 الصادر في 1985/11/29 .

و بتزايد إستخدام الأشخاص الطبيعيين للنظام المعلوماتي و شبكاته فإنهم يكونون عرضة لوقوع عدد كبير من الجرائم المعلوماتية عليهم و المتمثلة في النصب المعلوماتي و السرقة المعلوماتية و الإتلاف المعلوماتي .

و غالبية هذه الجرائم تقع على الأشخاص المعنوية سواء كانت العامة المتمثلة في مؤسسات الدولة و التي يتم إختراقها لأخذ معلوماتها و أسرارها و مشروعاتها ، أو الخاصة المتمثلة في المؤسسات المالية كالمصارف و شركات التأمين و الإقتراض التي يخترق مركزها الحسابي و الإداري و المالي و إستثماراتها.

و قد يكون محل هذه الجرائم المعلوماتية الحصول على المعلومات التي تسهل للمجرم المعلوماتي الحصول على الأموال عن طريق مقايضتها أو بيعها لغير أصحابها الشرعيين .

و غالبا ما يلجأ المجني عليه سواء كان أشخاص طبيعية أو معنوية إلى التكتم على ما لحقهم من جريمة معلوماتية لسببين، الأول رغبة منهم في الحفاظ على مركزهم الإجتماعي و سمعتهم التجارية و بالتالي عدم إظهار ضعف حماية أجهزتهم المؤدية إلى ضعف الثقة بالمؤسسة و عزوف العملاء عنها.

أما السبب الثاني فيتمثل في عجزهم عن الإثبات المادي للجريمة و بالتالي تحملهم المسؤولية في إفشاء المعلومات.

<u>دوافع و أسباب إرتكاب الجرائم المعلوماتية:</u>

للجريمة المعلوماتية دوافع و أسباب لا تختلف عن ما هو موجود في الجريمة التقليدية و تتمثل في :

<u>أولا الدوافع الذاتية :</u>

1/ الرغبة في الإنتقام : تعتبر سبب أو دافع أدى بالموظف العام أو العامل الذي تعرض إلى الفصل التعسفي من شركة أو منظمة حكومية يملك المعلومات الكافية حولها إلى إرتكاب جريمة معلوماتية في حقها لجعلها تتكبد خسائر مالية كبيرة.

2/الطمع و حب الثراء السريع : هي الدوافع التي تجعل الفرد يقوم بالقرصنة أو السرقة أو الإختلاس عن طريق الحاسوب للحصول على المال لتلبية حاجياته الأساسية و الوصول للثراء الغير مكلف.

<u>ثانيا : الدوافع النفسية :</u>

1/ الرغبة في إثبات الذات و التفوق على الوسائل التقنية : تتوفر عند مرتكب جرائم الحاسوب و الإنترنت الذي يصبو إلى أخذ صورة الإنسان الذكي و المتفوق القادر على تحطيم ألة الكمبيوتر و التفوق عليها.

2/ دوافع سياسية و إيديولوجية : يتميز العصر الحالي بظهور الكثير من المنظمات التي تتبنى بعض الآراء و الأفكار السياسية أو الدينية أو الإيديولوجية ، و التي تدافع عنها بإرتكاب أفعال إجرامية ضد معارضيها مثل مناداة أحد التجمعات في أواخر الثمانينات بضرورة الإعتراف بحق جديد للإنسان يتمثل في حق التواصل بين مختلف الأطياف الإنسانية عبر العالم دون قيود.

<u>الطبيعة القانونية للجريمة المعلوماتية :</u>

الجريمة المعلوماتية هي جريمة مستحدثة مرتبطة بالتطور الهائل في مجال التقنية العالية ، إختلف الفقه حول طبيعتها الخاصة حيث أكد البعض بأن دراستها تدخل في نطاق دراسة القسم الخاص لقانون العقوبات المختص بدراسة كل جريمة على حدة بتحديد عناصرها الأساسية و عقوبتها.

و أكد البعض الآخر بأنها ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي ، ففي معظم حالات إرتكاب الجريمة ندخل في مجال المعالجة الإلكترونية للبيانات ، و القانون الجنائي عاجز عن مواجهة هذا التطور المعلوماتي لعجز نصوصه و للتطور السريع المتلاحق في حقل المعلوماتية .

إن التحري على النظام القانوني لطبيعة الجرائم المعلوماتية عبر شبكة المعلومات يهدف أساسا لمعرفة ماهية النصوص القانونية الوضعية الواجب تطبيقها على خدمات نشر المواقع و المعلومات فيها ، و كذا المسؤولية المفترض تطبيقها على الأشخاص المسؤولين على هذا النشر.

فهذه الجرائم تختلف كثيرا عن الجرائم التقليدية من عدة نواحي في مقدمتها مسألة الإثبات لكون الأدلة تمحى فيها في لحظات ، فقد تكون المعلومات المراد البحث عنها مشفرة و لا يمكن الدخول إليها إلا من خلال أرقام معروفة عند أصحابها.

و كذا من الصعب ملاحقة جناة هذه الجرائم المقيمين في دولة أخرى لا تربطها أي إتفاقية بالدولة التي تحقق فيها السلوك الإجرامي أو جزء منه.

خصائص الجريمة المعلوماتية : تختلف عن الجريمة التقليدية بما يأتي:

1-عدم وجود مفهوم مشترك للجريمة المعلوماتية :

من خصائص هذه الجريمة عدم وجود لا مفهوم مشترك و لا تعريف قانوني موحد لها ، و هذا بسبب عدم وجود تنسيق دولي في مجالها و عدم وجود معاهدات دولية ثنائية أو جماعية لمواجهتها ، و كذا إختلاف الفكر القانوني حول حماية المعلومات و مشروعيتها التي تعتبر أمر نسبي من دولة إلى أخرى ، فمثلا المخدرات التي تحرم تجارتها في بعض الدول مثل مصر و الجزائر فإنه في الدول الإسكندنافية يصرح بها في حدود الإستعمال الشخصي فقط.

2-وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات :

هي أحد خصائص هذا النوع من الجرائم و التي تعتبر الشرط الأساسي الواجب توافره حتى يمكننا البحث في قيام أو عدم قيام أركان الجريمة المعلوماتية الخاصة بالتعدي على نظام معالجة البيانات ، و هذا لأنه في حالة تخلف هذا الشرط لا وجود للجريمة المعلوماتية.

3-الجرائم المعلوماتية عابرة للحدود :

هي جرائم عابرة للحدود الوطنية والإقليمية و القارية لا تعترف بالمجال الجغرافي للدول، بحيث يمكن أن يكون الجاني في دولة و المجنى عليه في دولة أخرى و الضرر المحتمل وقوعه في بلد ثالث .

4- جرائم المعلوماتية صعبة الاثبات :

حيث يصعب فيها الحصول على أثر مادي لإستخدام الجاني لوسائل فنية و تقنية معقدة و سريعة يسهل التخلص منها في ثواني .

5- الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية:

لأنها لا تحتاج لأدني مجهود عضلي بل تعتمد على المهارات الذهنية و التفكير العلمي و المعرفة التقنية للحاسوب.

6- الباعث على إرتكاب الجريمة المعلوماتية يختلف عن الجرائم التقليدية :

باعث الجريمة المعلوماتية يتمثل في الرغبة في مخالفة النظام العام و الخروج عن القوانين أكثر من إستهداف الحصول على الربح بعكس الجريمة التقليدية التي تهدف إلى الربح ، الذي يتحقق في الجريمة المعلوماتية أحيانا و لكن بشكل كبير.

7-قلة الإبلاغ عن وقوع الجريمة المعلوماتية :

لا يتم في الغالب الإبلاغ على هذا النوع من الجرائم بسبب خشية الضحية من التشهير به و خاصة إذا كانت مؤسسة تتخوف من فقد زبائنها أو لعدم إكتشاف الضحية لها ،لذا فإنها جرائم تساهم الصدفة في إكتشافها و لكن بعد مرور وقت كبير من إرتكابها ، و بالتالي هناك فرق كبير بين عدد الجرائم المعلوماتية المرتكبة و العدد الذي تم إكتشافه.

8- قوانين الجريمة المعلوماتية حديثة:

حيث لم يظهر قانونها إلا سنة 1988 في فرنسا إنطلاقا من القانون المتعلق بالغش المعلوماتي، أما في الجزائر فأول نص تشريعي في مجال الإجرام المعلوماتي لم يظهر في قانون العقوبات إلا في 2001/07/26 بموجب القانون رقم 09/01 إنطلاقا من مجموعة من المواد خاصة المادة رقم 144مكرر، التي أدرج فيها المشرع لأول مرة مصطلح وسيلة إلكترونية أو معلوماتية التي تسمح بتجريم الأفعال في محيط المعلوماتية والانترنت إضافة للمواد رقم 144مكرر1 و 2 و المادة 146 .

ثم جاء قانون رقم 15/04 المؤرخ في 2004/11/10 و الذي أدخل لقانون العقوبات القسم السابع مكرر تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات" والذي تناول المواد 394 مكرر إلى 394 مكرر 7 .

9-القوانين المتعلقة بالجرائم المعلوماتية قليلة التطبيق :

على المستوى الكمي بالنسبة للقوانين فإن المعالجة التشريعية في كل من فرنسا و الجزائر بقيت نظرية و قليلة التطبيق من قبل المحاكم.

أما على المستوى النوعي فإن المحاكم في بداية الأمر إمتنعت عن وضع إجتهادات قضائية لتكملة نقائص النصوص القانونية بخصوص هذا النوع من الجرائم.

10- وسائل إرتكاب الجريمة المعلوماتية مستحدثة:

أي أن إرتكاب الجريمة المعلوماتية يستلزم توفر جهاز الحاسوب أو أي جهاز بامكانه المعالجة الآلية للمعطيات المعلوماتية كأجهزة فك الرموز المقرصنة التي يمكن استعمالها

لسرقة الأموال من أجهزة التوزيع الآلي للنقود أو استعمالها للدخول الإنسيابي في أنظمة المعلوماتية المحمية قانونا .

11- الاختصاصات الاستثنائية لضباط الشرطة القضائية في الجرائم المعلوماتية :

يعود اختصاص المحاكمة الخاصة بالجريمة المعلوماتية في الجزائر في الأقطاب المتخصصة المتواجدة في أربع جهات هي قسنطينة ، الجزائر العاصمة(سيدي أمحمد) ، وهران ، ورقلة .

أيضا للشرطة القضائية اختصاصات استثنائية متعلقة بجرائم المعالجة الآلية للمعلومات إنطلاقا من قانون رقم 22/06 الذي أضاف سلطة مراقبة الأشخاص و الأموال و الأشياء و اعتراض المراسلات و تسجيل الأصوات و الصور و القيام بعملية التسرب .

محاور أنـواع الجرائم المعلوماتيـة(الواقعة على الأموال و الأشخاص و الحاسوب) :

تعددت محاولات الفقه الخاصة بتحديد أنواع الجرائم المعلوماتية و ذلك لصعوبة حصرها بدقة ، نظرا لحداثة هذه الجريمة و عدم وجود تعريف لها عام و متفق عليه و عدم تحديد مجاله المتغير بتطور التكنولوجيا الوثيقة الصلة بهذه الجريمة.

و قد ذهب الفقه الراجح إلى تقسيم الجرائم المعلوماتية إلى طائفتين رئيسيتين بالإعتماد على محل الجرائم المعلوماتية التي تنصب على معطيات الحاسوب و تطال الحق في المعلومات ، بالإضافة إلى الإعتماد على الدور الذي يلعبه الحاسوب في الجريمة التي يستخدم لإقترافها وسائل تقنية تقتضي إستخدامه.

و بهذا تقسم الجرائم المعلوماتية إلى نوعين : الجرائم الواقعة بإستعمال النظام المعلوماتي و الجرائم الواقعة على النظام المعلوماتي:

أولا : الـجرائم المعلوماتية الواقعـة باستعمال النـظام المعلوماتي :

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية بحيث يعد الحاسب الآلي هو الوسيلة المستعملة في تنفيذها و مضاعفة جسامتها، يهدف من خلالها المجرم المعلوماتي لتحقيق الربح أو الشهرة باعتدائه على أموال الغير و التدخل في حياتهم الخاصة مستعملا النظام المعلوماتي لتنفيذ جريمته .

1/ الجرائم الواقعة على الأموال :

كثيرة و متعددة تتم بواسطة النظام المعلوماتي و من أهمها ما يلي :

أ/غش الحاسب الآلي(التحايل المعلوماتي):

التحايل المعلوماتي مصطلح حديث النشأة تعددت تعريفاته المختلفة منها ما ذهب إليه البعض بأنه " الإحتيال الذي يرتكب بإستخدام الحاسوب ، و أنظمة الإتصالات بهدف الربح المالي."

كما عرف بأنه " أي سلوك إحتيالي أو خداعي مرتبط بالكمبيوتر ، يهدف شخص بواسطته إلى كسب فائدة أو مصلحة مالية."

و حول أساليب إرتكاب غش الحاسب الآلي فإنه بعد إزدياد إعتماد المصارف على أنظمة التحويل الإلكتروني للأموال زادت فرص إرتكاب جرائم هذا النوع من الغش بشكل كبير و تعددت أساليبه التي يمكن حصرها في ثلاثة صور من التلاعب في كل من البيانات المدخلة و في البرامج و في المعطيات.

ب/ السرقة الواقعة على البنوك :

تتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات و المعلومات الشخصية للمجني عليهم و استخدام شخصيتهم للقيام بعملية التحويل الالكتروني لأموال البنوك سواء إلى حساب الشخص الذي قام بالتحويل أو إلى جهات أخرى .

ج/ عملية السرقة الالكترونية :

مثل الاستيلاء على ماكينات الصرف الآلي و البنوك بحيث يتم فيها نسخ البيانات الالكترونية لبطاقة الصراف المالي ثم استعمالها لصرف أو إنشاء صفحة انترنت مماثلة لموقع أحد البنوك الكبرى أو المؤسسات .

د/ جريمة غسيل الأموال :

تمارس عبر شبكة المعلوماتية عن طريق توسيع مقترفي جريمة غسيل الأموال لنشاطهم الغير مشروع لغسيل الأموال مع تفادى الحدود الجغرافية والقوانين المضيقة لهذه العملية و سهولة نقل هذه الأموال و استثمارها من أجل إكسابها الشرعية.

و يعتبر خبراء صندوق النقد الدولي حجم الأموال التي غسلها سنويا ما بين 620 مليار دولار إلى 1600 مليار دولار ولأن الأجهزة المصرفية هي الوسيلة الأكثر فعلية لإضفاء

الشرعية على هذه الأموال فإن أصحابها يقومون بتحويلها إلى المصارف من أجل اجراء عمليات مصرفية متطورة في ظل التطور الاليكتروني في أنظمة المعلومات .

هـ/ الاستعمال غير المشروع للبطاقة الائتمانية :

لقد أدى التطور التكنولوجي إلى إفراز العديد من البطاقات التي أحدثت إنقلابا في أعمال عملية الدفع منها البطاقات المصرفية و المستخدمة لتسديد أثمان المشتريات أو لتوفير خدمة الإتصال الهاتفي ، و بطاقات النقد و بطاقات الإعتماد و الدين و الهاتف و التسليف.

و من أبرز هذه البطاقات تلك الخاصة بالإئتمان و التي عرفت بأنها " بطاقة مستطيلة من البلاستيك ، تحمل إسم المؤسسة المصدرة لها و شعارها و توقيع حاملها أو رقمها و إسم حاملها و رقم حسابه، و تاريخ إنتهاء صلاحيتها ، و يستطيع بواسطتها أن يحصل من فئة من التجار المتعاملين بها على ما يحتاجه من سلع و خدمات دون أن يضطر إلى الوفاء بثمنها فورا و إنما يكتفي بتقديمها للتجار لتدوين بياناتها (بصورة يدوية أو إلكترونية) ، و من ثم خصم قيمتها من الجهة المصدرة لها."

و قد رافق استعمال البطاقة الائتمانية سهولة الاستيلاء عليها بإعتبارها نقود الكترونية أما بسرقة أرقام البطاقات ثم بيعها إلى آخرين من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الحاسوب الضحية الذي قد يتفضل بتقديم معلوماته لغير الذي يقوم بسرقتها من أجل الحصول على السلع والخدمات أوسحب مبالغ مالية بموجبها من أجهزة الحاسوب .

و/ جريمة قرصنة البرمجيات :

هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات و بيعها للآخرين بسعر أقل كما يمكن نسخ المؤلفات العلمية و الأدبية

و ذلك بالطرق الالكترونية المستحدثة.

ي/ جريمة القمار عبر الانترنت :

عملية القمار كانت مسبقا تتم على نفس الطاولة و بحضور المعنيين بها إلا أنه حاليا أصبح القمار يتم في كازينوهات افتراضية و هي عبارة عن مواقع ويب مصممة على طراز كازينوهات موجودة على شبكة الانترنت ، و يتم فيها القمار بكل أنواعه و له عائدات مالية كبيرة فمثلا الولايات المتحدة الأمريكية عائدها من 3.1 مليار دولار أمريكي في سنة 2001

إلى 24 مليار دولار أمريكي سنة 2010 لذا حاول رجال التشريع الأمريكي تحريك مشروع قانون يمنع القمار عبر الانترنت .

ل/ جريمة تجارة المخذرات عبر الانترنت :

رغم أن لشبكة الانترنت نتائج ايجابية إلا أنها ساهمت بشكل كبير في ترويج للمخدرات عن طريق بيعها و التحريض على استخدمها و صناعتها بمختلف أنواعها .

2/ الجرائم الواقعة على الأشخاص :

رغم أن دساتير الدول أكدت على حماية الحياة الخاصة للأفراد فإن النظام المعلوماتي يستعمل أيضا في الاعتداء على الأشخاص إنطلاقا من الجرائم المعلوماتية المتمثلة في :

أ/الجرائم المعلوماتية الواقعة على الحياة الخاصة:

حماية الحياة الخاصة حق دستوري تكفله كل الدول لمواطنيها و رغم هذا تتعرض للإنتهاك و الإعتداء من قبل مستعملي الحاسب الآلي ، الذي رغم ماله من قدرة كبيرة على تخزين المعلومات سواء العامة أو الخاصة بالأفراد فإنه يسهل الحصول عليها عن طريق إفشائها ، و بالتالي يمكن أن يستخدم النظام المعلوماتي في الإعتداء على حرمة الحياة الخاصة كأن يقوم أحد الأشخاص بإعداد ملف يحتوي معلومات شخص آخر بدون علمه أو إذنه ، أو أنه يجمع معلومات بطلب من صاحبها إلا أنه بعد حفظها يجعل الغير يطلع عليها دون إذن صاحبها ، أو يخترق معلومات سرية مكتوبة أو سيرة ذاتية و مذكرات حياة شخصية للغير.

ب/ الجرائم الواقعة على الحقوق الملكية الأدبية و الفنية :

تتم عن طريق استعمال نظام المعلوماتي وذلك بالسطو على المعلومات المخزنة فيه دون إذن صاحبها ،فهي إعتداء على الجانبين المادي و المعنوي للمؤلف و قد تتعلق أيضا بالمساس ببراءة الاختراع .

ج/ جريمة التهديد :

تتم عن طريق الضغط على إرادة الإنسان و تخويفه مما سيلحقه من أضرار و هذا عن طريق إلزامه بالقيام بعمل معين أو الامتناع عنه، و قد أصبحت الانترنت أحسن وسيلة لهذا التهديد لما تحتويه من وسائل مثل البريد الاليكتروني ، الويب ، .. الخ

د/جريمة انتحال الشخصية :

تتم بإستخدام شخصية فرد معين للإستفادة من ماله أو سمعته أو مكانته أو سلطته، و تتميز بسرعة الانتشار خاصة في الأوساط التجارية بحيث تتم عن طريق جمع أكبر قدر ممكن من المعلومات المأخوذة من الشخص المطلوب بعد استدراجه عن طريق معرفة اسمه و عنوانه الشخصي و رقم البطاقة الانتمائية الخاصة به للتمكن من الوصول لماله و سمعته...

هـ/ جريمة انتحال شخصية أحد المواقع :

تتم عن طريق اختراق أحد المواقع للسيطرة عليه من خلال تركيب برنامج حساب جديد باسم الموقع المشهور.

و/ جريمة السب و القذف :

تهدف إلى المساس بشرف وسمعة الغير و تتم عن طريق المطبوعات و الرسوم أو الكتابات التي تمر عبر البريد الالكتروني أو الصوتي و صفحات الويب، بواسطة نشر معلومات مغلوطة عن الضحية سواء كان شخص طبيعي أو معنوي من أجل توصيل المعلومات لأكبر عدد ممكن من مستخدمي شبكة الانترنت .

ن/ جريمة التشهير و تشويه السمعة :

يقوم فيها المجرم المعلوماتي بنشر معلومات قد تكون سرية أو مغلوطة عن الضحية سواء كان فردا أو مؤسسة تجارية أو سياسية باستعمال عدة وسائل، منها انشاء موقع على شبكة الانترنت يحوي المعلومات المطلوب نشرها و ارسالها الكترونيا إلى اكبر عدد من المستخدمين.

فهي جرائم تستعمل لتشويه السمعة و الكذب على الرموز السياسية و الفكرية وحتى الدينية لتشكيك الناس في مصداقيتهم من أجل الابتزاز .

<u>ثانيا: الجرائم المعلوماتية التي تتم على النظام المعلوماتي(الحاسوب) :</u>

تستهدف هذه الجرائم المكونات المادية للنظام المعلوماتي أو مكوناته المنطقية (البرامج) أو المعلومات المدرجة فيه

<u>1/ جرائم الاعتداء على المكونات المادية لنظام المعلوماتي :</u>

المكونات المادية للنظام المعلوماتي هي تلك الأجهزة و المعدات الملحقة به و المستخدمة في تشغيله كالاسطوانات و الشرائط والكابلات ، و لطبيعتها المادية يكون الاعتداء عليها

عن طريق جرائم عادية و تقليدية كأن تكون محلا للسرقة أو خيانة الأمانة أو الإتلاف ألعمدي بحرقها أو ضربها بأدوات ثقيلة و حادة ، أو العبث بمفاتيح التشغيل و إفساد الشرائط و اسطوانات التشغيل مغناطسيا بتعريضها إلى أي مجال مغناطيسي متلف.

و قد أدرج بعض الفقه ضمن هذه الطائفة من الجرائم سرقة وقت الحاسوب ، حيث يلجأ العاملين بالنظام المعلوماتي لإستخدامه في أعمال خاصة بهم ، فتصب السرقة على وقت الجهاز و ليس على الأشياء المادية.

2/جرائم الاعتداء على المكونات المنطقية للنظام المعلوماتي (البرامج) :

هي جرائم تتطلب مهارة فنية عالية في مجال البرمجة وتقع على البرامج التطبيقية أو برامج التشغيل .

أ/الجرائم المعلوماتية الواقعة على البرامج التطبيقية:

يحدد فيها الجاني البرنامج أولا ثم يقوم بالتلاعب فيه لتحقيق أكبر إستفادة مالية ، و هذا من خلال قيامه بما يلي :

*** تعديل البرنامج :**

هدفه الرئيسي اختلاس النقود و يكثر استعماله في مجال الحسابات ، مثاله قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل البرنامج عن طريق إضافة دولار واحد على كل حساب يزيد عن عشر دولارات ،ثم قيامه بقيد هذه المصاريف الزائدة في حساب خاص به يتحصل على إثره على مئات الدولارات خلال كل شهر، و لم يكتشف هذا الفعل المجرم إلا بمناسبة محاولة البنك بمناسبة تأسيس شركة جديدة مكافأة أول و آخر عميل يتبع لهذه المؤسسات فكشف أمر وجود حساب غير موجود في الأصل .

*** التلاعب في البرامج :**

يأخذ عدة أشكال و صور فقد يتم عن طريق ما يسمى بالقنبلة المنطقية المتمثلة في برنامج أو جزء من برنامج ينفذ في كل لحظة أو كل فترة زمنية منتظمة يوضع في شبكة معلوماتية بغرض تسهيل عمل غير مشروع، أو عن طريق قيام أحد المبرمجين بزرع برنامج فرعي غير مسموح به في البرنامج الأصلي مما يسهل له عملية الدخول الغير مشروع في العناصر الضرورية لأي نظام معلوماتي مع ملاحظة صعوبة اكتشافه بسبب صغره و دقته .

ب/ الجرائم المعلوماتية الواقعة على برامج التشغيل :

برامج التشغيل هي البرامج المسؤولة عن عمل النظام المعلوماتي حيث تقوم بتنظيم و ضبط ترتيب تعليماته الخاصة ، جريمته تتم بتزويد البرنامج بتعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسهل الحصول على معلومات النظام و تتم في شكلين :

*** المصيدة :**

تتم بإعداد المبرمج لبرنامج به عيوب و أخطاء عمدا للدخول إليه بسهولة ، فهي ممرات خيالية و فواصل و تفرعات في البرنامج تمكنه من تنفيذ التعديلات الضرورية تمكنه من الخول للنظام المعلوماتي و الوصول إلى معلومات الذاكرة .

***/ تصميم برنامج وهمي :**

يتم بقيام المبرمج بوضع برنامج يصعب إكتشافه مخصص لإرتكاب الجريمة و مراقبة تنفيذها ، مثل قيام إحدى شركات التأمين الأمريكية في مدينة لوس أنجلوس بواسطة مبرمجيها بتصميم برنامج وهمي يحتوي وثائق تأمين لأشخاص وهميين بلغ عددهم 46 ألف شخص بهدف تقاضي هذه الشركة مبالغ طائلة خاصة بالتأمينات .

3/ جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي :

للمعلومة المعالجة آليا أهمية كبيرة كونها أساس عمل النظام المعلوماتي و ذات قيمة إقتصادية ، لذا تتعرض للتلاعب و الإتلاف بالشكل التالي:

أ/التلاعب في المعلومات: يتم بطريقة مباشرة أو غير مباشرة .

***التلاعب المباشر :**

يتم عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي وله عدة صور، مثل ضم مستخدمين غير موجودين بالعمل خاصة في المنشآت التي تضم عددا كبيرا من العمال المؤقتين ودائمي التغيير من أجل الحصول على مرتباتهم ، أو بطريقة الإبقاء على ملفات لعمال تركوا العمل من أجل الحصول على مبالغ مالية شهرية .

***التلاعب غير المباشر :**

يتم بالتدخل الغير المباشر لدى المعلومات المسجلة للنظام المعلوماتي باستخدام أحد وسائط التخزين ، أو بالتلاعب عن بعد بالمعلومات عن طريق استخدام أدوات معينة و معرفة أرقام و شفرات الحسابات.

و تكمن خطورة هذا التلاعب في تمكن الجاني من التسلل إلى المعلومات مخزنة بالنظام المعلوماتي والحصول على المنفعة المالية المطلوبة من مسافات بعيدة .

ب/ إتلاف المعلومات:

يتعلق هذا الإتلاف بالمعلومات المخزنة في النظام المعلوماتي وله عدة صور بحيث يتم بالطرق العادية كالحريق أو الضرب أو السرقة أو عن طريق استبدال المعلومات أو محو المعلومات، الذي يشكل أحد أنواع جرائم الغش أو التزوير المعلوماتي المتميزة بدرجة عالية من الخطورة لما ينجم عنه من حصوله على مبالغ مالية كبيرة بسبب صعوبة اكتشافه الذي يتم إلا بعد مرور فترة زمنية طويلة .

كما يمكن اتلاف المعلومات عن طريق محوها الذي يتم بسرعة فائقة من طرف المجرم المعلوماتي المتخصص ، مثل قيام شخصان باختلاس مبلغ يقدر ب 61 ألف دولار مرسلة من شركات التأمين إلى أحد المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز الجامعي وجعلها غير قابلة للتحصيل.