وزارة التعليم العالي والبحث العلمي
جامعة الجيلالي بونعامة – خميس مليانة -
كلية الحقوق والعلوم السياسية
قسم الحقــوق

مذكرة لنيل شهادة الماستر

تخصص إدارة أعمال

الموضوع:

ضمان أمن وسلامة المعلومات (الحماية)

من إعــداد الطالبين:
- عبايدية عبد الرؤوف
- حاج جيلاني محمد رفيق

تحت إشراف:
الأستاذ: شكرين ديلمي

لجنة المناقشــة:

- الأستاذ: عبد المطلب فيصل ..... رئيسا
- الأستاذ: شكرين ديلمي ..... مشرف ومقرر
- الأستاذ: بونوة عبد القادر ..... عضوا مناقشا

المـوسـم الـجـامـعـي

2015 ـ 2016

شكـــر وتـــقـــديـــــر

بسم الله الرحمان الرحيم

"ولئن شكرتم لأزيدنكم"

فالحمد لله حمدا كثيرا أن منّ علينا بتوفيق منه ويسّر لنا هذت العمل بتذليله أسبابه.....

وكللّ بفضل منه مجهوداتنا بغنيمة النجاح.....

فكانت خطانا وبحمده ثابتة على الدرب.....

وبعده تعالى..... بالشكر والعرفان..... وأسمى عبارات الامتنان.....

إلى أهم الأسباب التي جعلت من هذا الجهد بثمر بثمار النجاح.

إلى السند الحقيقي الذي أمدنا من وقته ومن جهده الكثير.....

إلى الأستاذ الفاضل: شكرين ديلمي

إلى كل أساتذة كلية الحقوق بجامعة خميس مليانة.

إلى من ساعدنا في إتمام هذه المذكرة.

إهـــداء

آهدي عملي هذا:

إلى آمي،

إلى آمي،

إلى آمي الحبيبة

منبع الحنان والتسامح والتضحية والصبر والثبات.

آمي، التي كانت دعواتها النور الذي آهتدي به

صانها الله ورعاها، وآطال في عمرها.

إلى الذين تكتمل سعادتي بوجودهم.

إلى آختي الغالية على قلبي كوثر نورة

إلى كل إخوتي الذين ساندوني بتشجيعاتهم ونصائحهم.

إلى آبي رحمه الله

إلى كل الآهل والآقارب عزيزي هجيرة

إلى من ساعدني في إتمام هذه المذكرة مكتب خدمات الإعلام الآلي زكرياء "رضا"

إلى كل عمال إدارة كلية الحقوق خاصة عزيزي توفيق ومخاطرية محمد

بجامعة خميس مليانة

إلى كل من ساعدنا في إتمام هذه المذكرة من قريب آو من بعيد

عبد الرؤوف

إهـــداء

آهدي عملي هذا:

إلى آمي،

إلى آمي،

إلى آمي الحبيبة

منبع الحنان والتسامح والتضحية والصبر والثبات.

آمي، التي كانت دعواتها النور الذي آهتدي به

صانها الله ورعاها، وآطال في عمرها.

إلى آبي الغالي

إلى الذين تكتمل سعادتي بوجودهم.

إلى أختي التي ساندتني بتشجيعاتها ونصائحها.

إلى كل الأهل والأقارب

إلى كل من ساعدنا في إتمام هذه المذكرة من قريب آو من بعيد

محمد رفيق

مقدمة

مقدمة

بدأت صناعة الحاسبات الآلية في الانتشار منذ حوالي خمسين عاما وفي خلال هذه الفترة القصيرة أصبح للحاسبات الآلية دور رئيسي في الثورة الصناعية الثانية التي نعيش في ظلها الآن بقول أن أهم تكنولوجيا التي عرفها هذا القرن بل ربما عرفتها البشرية على مر عصورها كانت تكنولوجيا لبات الآلية، حيث أدى ظهور الحاسبات الآلية إلى تغيير شكل الحياة في العالم وأصبح الاعتماد عليها يزداد يوما بعد يوم سواء في المؤسسات المالية أو المرافق العامة أو المجال التعليمي أو الأمني أو غير ذالك.

فهذه الحاسبات مع ما تتصل به من أجهزة اتصالات أصبحت موجودة في كل المجالات وبدونها فإن مجالات عديدة كالصناعة والتجارة والطب والدفاع والتعليم والبحوث... الخ.

كانت ستصبح أقل كفاءة مما عليه الآن بحيث أصبح من الصعب إن لم يكن من المستحيل أن ت المختلفة بأداء أعمالها دون الاعتماد بشكل أساسي على الحاسبات الآلية ولا شك أن اتصال الحاسبات الآلية بوسائل الاتصال قد ضاعف من أهه الاتصال قد أثمر عن أوجه أخرى للتقدم في هذا المجال لعل أبرزه على الإطلاق هو ظهور الشبكات المعلوماتية.

حيث مهدت الثورة الصناعية منذ منتصف القرن الماضي تطورات وتغيرات من خلال التقدم التقني في مجال الحاسبات الآلية ليزوغ ثورة جديدة هي ثورة المعلومات.

فقد عرفة القرن العشرين تطورا مذهلا في مجال الاتصال وشكلت الشبكة المعلوماتية الدولية أعن التي امتدت عبر كامل أنحاء المعمورة وربطت بين شعوبها فأصبحت وسيلة تعامل بين أفراد مختلف الطبقات والمجتمعات.

هذه الثورة الحقيقية للمعلومات كانت وراء ما يطلق عليه صناعةمعلومات حيث ظهرت منافذ استثمارية جديدة تمثلت في مؤسسات وشركات ومشروعات فردية منها ما يهتم بتصنيع الحاسبات ومنها ما يتصدى لإعداد برامج لازمة لمعالجة المعلومات آليا وأخرى تتولى إعداد الكوادر الفنية المتخصصة في تشغيلها.

فقد أصبح النظام المعلوماتي في نهاية القرن الماضي من لوازم الحياة الضرورية والمتطورة على المستوى العام أو الخاص وإالمذهل التقني والتكنولوجي الذي يمكن وصفه بالثورة المعلوماتية التي أبهرت العالم بمزاياها فأصبحت قرية صغيرة في انتشار شبكة الانترنت بسرعة فائقة عزز فكرة الحق في المعلومات كمبدأ مقرر للدول والأفراد معا.

ولا يخفى أن كل تطور تقني تكون له انعكاساته حيث بات التطور التقني المعلوماتي سلاح ذو حدين فا على الرغم من التغيرات الايجابية التي أحدثتها إلا أنها وفي الوقت ذاته أتاحت الفرصة لظهور أنواع جديدة ومستحدثة من الجرائم الفنية والتي تحمل طابع هذه التقنية المعلوماتية هي نماذج من الجرائم المستحدثة.

حيث دخل في قاموس الجرائم نوعا جديدا يطلق عليها لدى البعض جرائم المعلوماتية ولدى البعض الأخر جرائم الالكترونية أو الانترنت وبعض يرى أنها جرائم الكمبيوتر وهي جرائم إساءنية الحديثة أي تلك الأعمال التي تتم عن طريق الانترنت.

وإذا كانت الشبكةتعتبر خزينة المعرفة وسيل المعلومات فإنها تعد أيضا أد المستوى لارتكاب الجريمة ففي هذه البيئة الضخمة المزدحمة تضعف قبضة الأمن والمراقبة والتحكم وتزداد عمليات التجسس على المعلومات وسرقتها حتى أنها تشكل تهديدا بالغا لسائر المنظمات الخاصة التي تعتمد أعمالها على الحاسبات

والشبكاية وترفع مخاطر إساءة استخدام الحاسبات والتلاعب في البرامج والمعلومات المخزنة آليا بقصد الحصول على أموال أو أصول أو خدمات.

ومما يزيد من خطورة الأمر أنه بجانب صعوبة السيطرة على شبكة الانترنت وعلى الجرائم التي ترتكب من خلالها فإنه يصعب اكتشاف هذه الجرائم أو تحديد مصدرها كما يصعب إيقافها بالنظر إلى سرعة نشر المعلومات وتسجيلها أوتوماتيكيا على الحاسبات في الخارج ولذلك فان الجرائم المعلوماتية غالبا ما تقيد ضد المجهول.

ومن أجل ذلك يجب اعند هذه الظاهرة الجديدة لتفكيك معانيها وتحديد صورها ومرتكبيها وطرق قمعها.

ومنه نطرح الإشكالية حول ماهية الطرق الكفيلة لضمان أمن وسلامة المعلومات؟

وهذا يدفعنا إلى طرح التساؤلات التالية:

- ما هي الجرائم المعلوماتية ؟
- هل تتميز الجرائم المعلوماتية بصفات تختلف عن الجرائم التقليدية ؟
- هل للمجرم المعلوماتي سمات تميزه عن المجرم العادي ؟
- ما هي الدوافع من وراء ارتكاب الجريمة المعلوماتية ؟
- ما هي أبرز الأنماط الأكثر شيوعا للجريمة المعلوماتية ؟
- على أي أساس تحظى المعلومة بالحماية ؟
- ما هي طرق حماية المعلومات ومكافحة الجرائم المعلوماتية ؟
- ما هي سبل مكافحة الجرائم المعلوماتية ؟
- ما موقف المشرع الجزائري من هذا النوع من الجرائم ؟
- ما هي أهم الاتفاقيات والمعاهدات الدولية في مجال مكافحة الجرائم المعلوماتية؟

أهمية البحث:

ترجع أهمية هذه الدراسة إلى أنها من الموضوعات الحديثة التي تـرتبط بتطـور وسائل التكنولوجيا الحديثة.

إن اختيار موضمان أمن وسلامة المعلومات لما يكتسيه من أهمية كبيرة في طور التقني لوسائل الاتصالات الحديثة، حيث يستوجب انتهاج دراسة تقنية وسياسة تشريعية لحمايتها ومما زاد من أهمية هذا الموضوع ظهور صـور إجراميـة مسـتحدثة متعلقة بالاعتداء على المعلومات على شبكة الانترنت وهذا ما دفع المختصين الفنيين في أمن المعلومات والمشرعين مكافحة الجرائم المعلوماتية.

وهذا ما سنتطرق إليه في موضوعنا من خلال تقديم مفهوم هذا النوع من الجـرائم وصورها وسبل مكافحتها.

أهداف البحث:

- تقديم مفهوم للجريمة المعلوماتية.
- التعف على كيفية حماية المعلومات وسبل مكافحة الجرائم المعلوماتية.
- التعرف على سبل مكافحة الجرائم المعلوماتية على المستوى الدولي.
- بيان موقف المشرع الجزائري إزاء هذا النوع من الجرائم.

الفصل الأول:
الجرائم الواقعة على المعلومات

المبحث الأول: ماهية المعلومات وطبيعتها القانونية.

إن تعريف المعلوماد الرغم مما قد يبدو من أنه لا يثير صـــعوبة حيـــث إن المعلومات تحيط بنا من كل جانب كما بكافة مجالات الحياة، إلا انه يمكن القول المعلومات قد اكتسبت بظهور تكنولوجيا الحاسبات الآلية بعدا جديدا أضفى عليها أهمية تفوق مما كانت عليها قبل ذلك، واكسبها شكلا جديدا بل تسمية جديدة حيث أصبح يشـــار إليها بالمعلوماتية إشارة إلى ارتباطها بهذه التكنولوجية الجديدة وللتعرف على المعلومـــات سوف نحاول من خلال هذا المبحث أن نقدم مفهوم للمعلومات فـــي المطلـــب الأول ثـــم نتطرق إلى الانترنت كوسيلة لتبادل المعلومات في المطلب الثاني وأخيرا الطبيعة القانونية للمعلومات في المطلب الثالث.

المطلب الأول: مفهوم المعلومات

الفرع الأول: تعريف المعلومات[1]

إن تعريف المعلومات على الرغم مما قد يبدو من انه لا يثير صـــعوبة، حيـــث أن المعلومات تحيط بنا من كل جانب، كما أنها تتعلق بكافة جوانب ومجالات الحياة، إلا أنـــه يمكن القول أن المعلومات قد اكتسبت بظهور التكنولوجيا وتقنياتحاسبات الآليـــة بعـــد جديدا أضيفي عليها أهمية تفوق ما كانت عليه من قبل ذلك، وأكسبها شكلا جديـــدا، بـــل وتسميه جديدا حيار أليها بالمعلوماتية أشارة إلى ارتباطها بتقنية وتكنولوجيـــا المعلومات.

أولا: التعريف بالمعلومات:

المعلومات information كلمة شاع استخدامها مند الخمسينات من القرن الماضـــي فـــي مجالات مختلف وسياقات شتي، مما جعل لها في الاســـتعمال الـــدارج مفـــاهيم متنوعـــة ومتعددة، وهيث اللغة مشتقة من كلمة (علم)، ودلالتها فيها تدور بوجه عام حـــول

[1]- أ. محمد الله أبو بكر سلامة، موسوعة الجرائم المعلوماتية، جرائم الكمبيوتر والانترنت، المكتبة العربي الحديث، الإسكندرية، ط 2005، ص 81.

المعرفة التي يمكن نقلها واكتسابها، وقريب مدلك إشارتها في اللغة الفرنسية إلى فحوي عمليات الاتصال الذي يستهدف نقل وتوصيل إشارة أو رسالة، والإعلام عنها، و'اتخاذ وظيفتها في نقا المعارف transfert de connaissances محورا تدور حوله مدلولاتها، وأصلها أيضا في اللغة الانجليزية والفرنسية والألمانية والروسية هو كلمة informatio اللاتينية الدلالة بحسب الأصل على شيء للإبلاغ والتوضيح أو على عملية الإبلاغ أو النقل أو التوصيل، وهو نفس ما يعنيه تعبير xinxi المقابل لها بالغة الصينية.

أما عن التعريف الاصطلاحي للمعلومات، فإن هناك مئات من التعريفات التي عرضها للمعلومات باحثون من تخصصات وثقافاتـختلفة، حتى ليكاد يكون مستحيلا – كما يقول البعض – فهم و إدراك المعني المراد بمصطلح "المعلومات" إذا ما استخدم فـي الاتصال العلمي بغير تحديد.

ويمكن تعريف المعلومات بطة عامة بأنها : مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل و الاتصال communication أو للتفسير والتأويل interpretation، أو للمعالجـة processing سواء بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة، بحيث يمكن تغيرها، وتجزئتها، وجمعها، أو نقلها بوسائل وأشكال مختلفة. (1)

ويري بعض الفقه إن أكثر ما يحظى من تعريفات للمعلومات هو ما ينطلق من تحديده لمفهومها من اختلافها في المعنى والدلالة مع البيانات التي تستعمل في الكثير من الأحيان مرادفا أو مكملا للمعلومات و وفقا لهذا الفقه فان البيانات تعتبر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض والتي لم تخضع بعد لعمليةفسير أو تجهيز للاستخدام والخالية تبع لذالك من المعنى الظاهر في أغلب الأحيان أي أنها بإيجاز الحقائق أو الرسائل أو الإشارات أو المفاهيم التي تعرض بطريقة صالحة لإبلاغ أو التوصيل أو التسيير أو المعالجة

(1)- أ. محمد الله أبو بكر سلامة، نفس المرجع، ص 82.

بواسطة إنسان أو أدوات أو معدات آلية أما المعلومات فهي المعني الذي يستخلص من البيانات عن طريق العرف أو الاتفاق أو الخبرة أو المعرفة وقد أخذت التوصية الصادرة عن منظمة التعاون لاقتصادي والتنمية عم 1992 الخاصة بحماية أنظمة الحسابات الآلية وشبكة المعلومات بالتفرقة التي سردها هذا الرأي حيث عرفة البيانات بأنها مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلا محددا يجعلها قابلة للتبادل أو التفسير أو المعالجة بواسطة الأفراد أو بوسائل الكترونية أما المعلومات فهي المعنى المستقي أو المستخلص هذه البيانات غير أن رأي آخر قد لا يجد جدوى من التميز بين المعلومات و البيانات في مقام دراسة المعلوماتية فمن الناحية، فان الذي يعنيها من هذه الدراسة هو حماية المعلوه بصفة عامة، وطالما أن المعلومات هي المعني لص من البيانات فإن الحماية القانونية تشملها معا،ومن ناحية آخري، قد لا تكون المعلومة مفهومة لدي متلقيها، وهو ما يجعلها تخرج عن دائرة المعلومات وفقا لهذه التفرقة، ورغم ذلك يكون الوصول إليها والتلاعب بها على قدر كبير من الخطورة، فالذي يعنيها لومات بغض النظر عن محتواها، ولذا يفضل هذا الرأي استخدام المعلومات والبيانات في مقام هذه الدراسترادفين، ونحن نميل إلى هذا الرأي الآخر ونؤيده.

ثانيا: التعريف بالمعلوماتية أو تقنية المعلومات: [1]

با في مقدمة هذا المؤلف أن مصطلح المعلوماتية يشير إلى المعلومات المعالجة والمبرمجة آليا، وأن الباحثين قد اختلفوا فيما بينهم حول تقصي المصدر التاريخي لهذا المصطلح، فمنهم من عزى اقتراح مصطلح، وفقا لوجهة نظر هذا الفريق من عزي اقتراح مصطلحمعلوماتية إلى الأستاذ Drefus الذي يعتبر صاحب الفضل في اقتراح هذا المصطلح، وفقا لوجهة نظرا هذا الفريق من الباحثين، حيث استخدمه عام 1962 لتيز المعالجة الآلية للمعلومات، ومنهم من عزى استخدامه لأول مرة إلى الأستاذ

[1]- أ. محمد الله أبو بكر سلامة، نفس المرجع، ص 83.

A.I.Mikhailov مدير المعهد الاتحادي للمعلومات العلمية والتقنيـة (vinnti) بالاتحـاد السوفياتي سابقا، الذي استعمله كوصف لعلم المعلومات العلمية science of scientific information.

ثم زاد استخدامه بعد ذلك على المستوي الجغرافي واسع بمفاهيم متباينـة، حتـى أحصى له بعض من الباحثين أكثر من ثلاثين تعريفا مختلفا في الكتابات المتخصصة فـي علم المعلومات.

وللأكاديمية الفرنسية تعريف المعلوماتية صاغته في جلستها بتاريخ 2 افريل 1952 تجري عباراته على أنها: (علم التعامل العقلاني على الأخص بواسطة آلات أوتوماتكيـة، مع المعلومات ارها دعامة للمعارف الإنسانية، وعمادا الاتصالات في ميدان التقنيـة والاقتصاد والاجتماع)، ولمنظمة الأمم المتحدة للتربية والعلوم والثقافة (اليونيسكو) تعريف موسع وأكثر حدثة لتقنية المعلومات أو المعلوماتية، يدرج في مفهومها الفـروع العلميـة والتقنية والهندسية وأساليب الإدارة الفنية المستخدمة في تداول و معالجة المعلومات وفـي تطبيقها، والمتعلقة كذالك بالحسابات الآلية و تفاعلها مع الإنسـان والآلات، ومـا يـرتبط بذالك من مور اجتماعية واقتصادية وثقافية، كما عرفت التوصية الصادرة عـن منظمـة التعاون الاقتصادي والتميعلوماتية أو نضم معلومات بأنها (تشمل الحسـابات الآليـة ووسائل الاتصال وشبكات المعلومات والبيانات والمعلومات التي يمكن تخزينها ومعالجتها واسترجاعها ونقلها بواسطة هذه السابات أو وسائل الاتصال أو شبكات المعلومات بمـا ذالك برامج الحسابات الآلية و جميع القواعد اللازمة لتشغيل هذه الأنظمة والحفـاظ عليها). [1]

[1]- أ. محمد الله أبو بكر سلامة، نفس المرجع، ص 84.

وعند كثرين تعي المعلوماتية أو تقنية المعلومات (التزاحم والالتحام بين تقنيات الحاسبات والاتصالات والاستعمال المتزايد للالكترونيات في العمليات الصناعية والتجارية بدءا بالإنسان الآلي المبرمج بالحاسوب حتى بطاقة الائتمان التي يحتفظ بها المستهلك في جيبه).

والتي إ ة نائلة عادل محمد فريد وبحق أن مفهوم المعلوماتية يمكن ببساطة في العلاقة بين المعلومات وبين التقنية الحديثة التي تستخدم من اجل معالجة هذه المعلومات وبعبارة أخرى فان المعلوماتية ببساطة هي (المعلومات المبرمجة آليا والتي تستخدم التقنية الحديثة في الحلبات الآلية وأنظمتها في التعامل معها). [1]

الفرع الثاني: أنواع المعلومات

أنواع المعلومات تقسم المعلومات إلي ثلاث طوائف هي، المعلومات الاسمية والمعلومات المتعلقة بالمصنفات الفكرية والمعلومات المباحة .

أما الطائفة الأولي وهى المعلومات الاسمية، فتنقسم إلي مجموعتين هما:

أ. المعلومات الشخصية:

نقصد بالمعلومات الشخصية المعلومات المتعلقة بأحد الأشخاص وذلك من حيث اسمه، لقبه، موطنه، جنسيته، وضعه الاجتماعي... كل شيء يتعلق بحياته الخاصة.

وبما أنه ذكرنا أنها تتعلق بالحياة الخاصة للشخص فهذا يوحي بالخصوصية ولا يجوز للغير أن يطلع على هذه المعلومات في أي نظام معلوماتي بدون الحصول على إذن من المعني بالأمر فصاحب الشيء هو مالكه ولا يجوز للغير التعدي عليه.

وهذا الأمر أكدت عليه نصوص القانون الفرنسي رقم 17 الصادر في 6 يناير سنة 1978 بشأن نظم المعلوماتية والحريات. [2]

---

[1]- أ. محمد الله أبو بكر سلامة، نفس المرجع، ص 85.

[2]- Loi N°17-78 du Janvier 1978 relative à l'informatique aux fichiers et aux libertés (J.O du 7 Janvier 1978)

ب. المعلومات الموضوعية:

المعلومات الموضوعية هي المعلومات المنسوبة إلى شخص ما معبرا عن رأيه اتجاه الغير.

ومثل ذلك مقالات الصحف، الملفات الإدارية للعاملين لدى جهةعينة فهذه المعلومات لا تتعلق بالشخص القائل أي الصادرة عنه وإنما تتعلق بشخص آخر.

مثلا: الصحفي الذي يكتب مقالا عن الأشخاص له حق على هذا المقال، ولكن في نفس الوقت يجب عليه عدم التعدي على الشخص محل المقال. ومن هذه النقطة نجد أن التشريعات أثمت جرائم القذف وغيرها.

المعلومات الخاصة بالمصنفات الفكرية:

يقصد بهذه المعلومات "كل عمل مبتكر أدبي أو فني أو علمي أيا كان نوعه أو طريقة التعبير عنه أو أهبته أو الغرض من تصنيفه -."أنواع المعلومات تقسم المعلومات إلي ثلاث طوائف هي، المعلومات الاسمية والمعلومات المتعلقة بالمصنفات الفكرية والمعلومات المباحة.

فهذه المعلومات يتمتع مؤلف مالية وأدبية عليها. وهذه الحقوق تتمثل في حق الأبوة، حق الاستئثار بالاستغلال لهذه المعلومات أو المصنف.

ونتاج القول أن هذه المعلومات أو المصنفات الفكرية محمية بتشريعات الملكية الفكرية الأدبية والفنية والملكية الصناعية ولا يجوز التعدي عليها بأي شكل من الأشكال.

المعلومات المتاحة أو الشاغرة: [1]

المعلومات المباحة هي المتاحة لكافة الناس للحصول عليها ومن غير إذن، وذلك لأنها بدون مالك ومثال ذلك النشراتجوية وتقارير البورصة. فهذه المعلومات تنقضي بالاستعمال الأول. لكن يمكن لهذه المعلومات أن تتمتع بالحماية التشريعية والجنائية في

[1]– رشدي محمد علي محمد عبد علي، الحماية الجنائية للمعلومات على شبكة الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ص 25.

حالة قيام أحد الأشخاص ببذل مجهود فكري وذهني في جمعها وصياغتها وذلك إعمالا لقاعدة "الجمع والصياغة"، وكذلك احتراما لما يبذل من مجهود في الجمع والصياغة.

المطلب الثاني: الانترنت كوسيلة لنشر وتبادل المعلومات

الفرع الأول: تعريف الانترنيت

هي شبكة عالمية من الروابط بين الب تسمح للناس بالاتصال والتواصل بعضهم مع بعض واكتساب المعلومات من الشة الممتدة إلى جميع أرجاء الأرض بوسائل بصرية وصوتية ونصية مكتوبة، وبصورة تتجاوز حدود الزمان والمكان والكلفة وقيود المسافات، وتتحدى في الوقت نفسه سيطرة الرقابة الحكومية.

ويعرفون آخرون الانترنيت كذلك بأنه شبكة دولية للمعلومات تتفاهم باستخدام بروتوكولات تتعاون فيها بينها لصالح جميع مستخدميها وتحتوي على العديد من الإمكانيات مثل البريد الإلكتروني، وإقامة المؤتمرات بالفيديو وقوائم البريد بالإضافة إلى الملايين من مجموعة والعديد من الملفات المتاحة لنقلها واستخدامها بطريقة شخصية وكذلك آلات البحث المرجعي[1].

الفرع الثاني: لمحة تاريخية عن الانترنت

على الرغم من انتشار الانترنت وتعدد استخداماته مازالت شبكة الانترنت في مهدها، وتتوالى على أسماعنا أنباء عن قرب ظهور جيلها الثاني الذي سيفوق الجيل الأول بقدر كبير سواء من حيث السرعة أو الإمكانيات الفنية حيث سيوفر مسارات أوسع بكثير لتدفق المعلومات وذلك باستخدام الألياف الضوئية ذات السعة الهائلة.

وقد أدى ظهور الانترنت إلى انتشار وازدهار مجالات كثيرة لم يكن لها أن تنتشر شبكة الانترنت ومنها تزايد النمو في مجال التمويل الالكتروني للبنوك E-Finance حيث يتضمن التمويل الالكتروني جميع أنشطة التمويل التي يمكن تنفيذها

(1)- www.tutgate.net/156.html، Date:14/05/2011 Heure:10:10

من خلال شبكة الانترنت أو الشبكات العامة، مثل شبكات الربط الفوري بين مجموعة من البنوك والتي ساعدت على انتشار المنتجات والخدمات المثل التأمين وخدمات وخدمات الرهن العقاري Mortgage والسمسرة والنقود الرقمية Digital Money والدفع الالكتروني.

إن انتشار استعمال شبكة الانترنت قد حمل معه تيارين مختلفين من الحماس والقلق الحماس من أجل فتح باب جديد لحرية الاتصال بأشخاص لا يمكن الاتصال بهم في الواقع بسهولة وإمكانية عقد صفقات تجارية،أما القلق فمن أجل احتمال عدم تأمين الاتصالات أو انتهاك السرعبر شبكة الانترنت أو القيام بأعمال القرصنة أو انتهاك حق الخصوصية The Right of Privacy والاطلاع على البيانات الشخصية وحسابات البنوك أو استخدامه في تجارة مشبوهة كالمخدرات وتجارة السلاح وعمليات بيع الأطفال استخدام شبكة الانترنت في النشاط التخابري والأضرار بأمن الدولة.

ذلك أنه يسهل عبر الشبكانكترونية الوصول إلى معلومات سرية وتتصل اتصالا وثيقا بخصوصية الإنسان وهو أمر بالطبع يثير القلق والحيرة ويزيد من حدته أن هذه المعلومات إذا ما تم تجميعها والربط بينها واستكمالها يمكن أن تظهر جوانب بمجرد كشفها وظهورها فإنه يضر كشفها بمصالح بعض الأفراد بل وبأمن واستقرار الدولة نفسها.

وبرغم ذوئ نجد أن الانترنت ساعد على تقريب المسافة وإزالة الحواجز بكافة أشكالها بين طرفي المعاملات الالكترونية بما في ذلك حاجز اللغة، حيث أصبح من السهل أريصل أي منهما إلى الآخر مباشرة ودون تدخل وسيط بينهم. [1]

وقد ظهرت النواة الأولىشبكة الانترنت في أواخر الستينات من القرن الماضي وبالتحديد عام 1969 عندما طلبت وزارة الدفاع الأمريكية (البنتاجون) من خبراء الكمبيوتر إيجاد أفضل طريقة للاتصال بعدد غير محدود من أجهزة الكمبيوتر دون

[1]– د. خالد ممدوح إبراهيم، أمن المعلومات الالكترونية، الدار الجامعية، ط 2008، ص 12.

الاعتماد على كمبيوتر واحد ينظم حركة السير، وكان الدافع هو الخوف من أن الاعتماد على شبكة تدار مركزيا سيكون هدفا سهلا لهجوم نووي مباغت يقضى عليها ولذلك عمل البنتاجون على البحث عن تكنولوجيا جديدة للاتصالات فقام بتمويل وإعداد شبكة تعد من أهم شبكات الكمبيوتر.

وكان الدافع هو تحقيق هدف استراتيجي وهو إرسال تعليمات التصويب من خلال مركز التحكم إلى قواعد الصواريخ ولو بعد تدمير جزء من شبكات هذا المشروع الذي أعدته وزارة الدفاع الأمريكية والذي يطلق عليه اختصار مشروع أربانت Advanced Project Agency (ARPANET) Research أي مشروع شبكة وكالة الأبحاث المتقدمة كما سمى أيضا مشروع شبكة العمود الفقري وكان هذا المشروع قاصرا على وزارة الدفاع الأمريكية للأغراض الأمنية والعسكرية إذا ما تعرضت لأيجوم أو دخلت في مواجهات مسلحة أو حرب نووية. [1]

طور مشروع أربانت في عام 1972 وأصبح يضم شبكة اتصالات بين أربعين جهاز كمبيوتر ولقد تحقق لهذه الشبكة الانطلاق والتوسع عندما تبنتها المؤسسة العلمية القومية National Science Fondation (NSF) عام 1980 وذلك بهدف السماح بدخول المجتمع العلمي كافة إلى المعلومات المخزنة على الشبكة وأصبحت أربانت تسمى نيسف نت NSFNET وأصبحنا نسمع ونقرأ الآن عن مصطلح الطريق السريع للمعلومات Information Super Highway والآن يزداد اتساع شبكة الانترنت وأصبحت تضم أكثر من 2500 شبكة في كافة أنحاء العالم وجاوز مستخدموها أربعين مليونا وقد انفصلت الشبكة العسكر الشبكة الأم عام 1983 والذي هو يعتبر تاريخ ميلاد شبكة الاتصالات الدولية حيث سمح لمختلف الأفراد استخدامها بعد عدة سنوات، إذ تم توصيل جميع شبكات الاتصال بمشرع أربانت ARPANET مستخدمين نفس بروتوكولات

[1]– د. خالد ممدوح إبراهيم، مرجع سابق، ص 13.

نصالات ونظام التشغيل NT أو نظام UNIX ولكن معظم الكمبيوترات الرئيسية لشبكة انترنت ترتبط فيما بينها بنظام التشغيل يونكس UNIX.

وفي عام 1986 توسعت شبكة الانترنت وشملت المئات من الجامعات والمعاهد والأكاديميات ثم انتقلت إلى التطبيقات الكمبيوترية التجارية، وكونت آلاف من الشبكات وقد نشأ الانترنت من ترابط هذه الشبكات وفي عام 1990 بدأ مقدمو خدمة البريد الالكتروني تقديم معلومات عن أسعار البورصات العالمية وأسعار سوق المال وكذلك قدموا بيانات معلومات عن أعمال البنوك ومن هنا أصبح الانترنت يستخدم في أغراض أخرى غير الأغراض العلمية وت الاتصالات الالكترونية عبر شبكة الانترنت وصار الانترنت بعد أن كان حكرا على مجموعة من العلماء والباحثين فقد يستخدم في الأغراض التجارية وبصفة خاصة بعد انتهاء الحرب الباردة بين الولايات المتحدة الأمريكية والاتحاد السوفيتي السابق.

ولقد نشأ عن استخدام الانترنت تكوين ممى بعالم الفضاء Cyber Space أي المكان الخيالي أو الافتراضي أو الفضاء المصطنع الالكتروني حيث يتم تبادل المعلومات والبيانات في هذا الفضاء المصطنع الكترونية،ومصطلح الفضاء المصطنع الالكتروني جديد على قواميس اللغة العربية ولا عجب في ذلك إذ أنه لم يبرز في الغرب إلا في السنوات الأخيرة فقط، وقد أدى ظهور عالم الفضاء المصطنع إلى ظهور نظام تبادل البيانات الكترونيا والذي أصبح حقيقة واقعية فرض نفسه وخصوصا في مجال التجارة الالكترونية. [1]

[1]– د. خالد ممدوح إبراهيم، مرجع سابق، ص 14.

الفرع الثالث: مميزات شبكة الانترنيت

1. سرية تبادل المعلومات

فكل جهاز كمبيوتر في شبكة الإنترنت له رقم خاص به Address و بالتالي يمكن أن يرسل أي شخص رسالة إلى هذا الرقم و يضمن أن تخزن داخل هذا الجهاز فقط ولا يستطيع أي شخص آخر معرفة محتويات الرسالة إلى صاحب الجهاز المرسل إليه، وكذلك يستطيع المرسل معرفة إذبال و قراءة الرسالة أم لا و تاريخ ذلك وكذلك يستطيع المرسل إليه الرد على الرسالة. [1]

2. سرعة و ضمان انتشار المعلومات

ومن مميزات شبكة الإنترنيعة و انتشار المعلومات، فنجد أنه لكي يرسل الشخص خطابا إلى أي مكان فأن ذلك يستغرق أمامه وقت يفقد في البريد، ولاستخدام الفاكس يستغرق ذلك دقائق و من الممكن أن تصل مات مشوهة أو غير مقروءة افترضنا أن المعلومة سوف تبلغ إلى مليون شخص في أماكن مختلفة فأن ذلك سوف يستدني إرسال ملون خطاب أو فاكس مع عدم ضمان وصول المعلومات إلى المبلغين.

وإذا افترضنا أيضا أن هؤلاء المليون شخص يعلمون أن المعلومات تكون موجودة في جهاز كمبيوتر معين و تجدد كل ساعة بأحدث المعلومات فإنهم جميعا سوف يتصلون بهذا الكمبيوتر و يقرءون المعلومات أول بأول بدوبجهد أو تعب.

وكل ما المرسل أو مبلغ المعلومة أن يكتبها و يخزنها في المكان المتفق عليه كما لو كان يكتب أي سند على جهاز الكمبيوتر.

[1]- د. سلميان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007، ص 21.

وهذا ما يحدث بالفعل الآن فجميع وكالات ومصادر الأنباء في العالم مثل NASA CNN تضع جميع المعلومات والأحداث و النشرات الجوية و التنبؤات على أجهزة الكمبيوتر فورا و يستطيع ملايين الناس الاتصال بها و معرفة الأخبار فورا بدون انتظار مواعيد نشرات الإذاعة والتلفزيون، كذلك شركات الطيران و المصانع الكبرى و المحلات العالمية تضع جميع المعلومات عن المواعيد والسلع المعروضة و أسعارها على أجهزة الكمبيوتر المتصلة بشبكة الإنترنيت ليتمكن الناس في العالم كله من التعرف في ثوان وفي ي وقت بدون التقيد بالإذاعة أو النشرات الصحفية المحددة المواعيد أو الطبعات.

3. تبادل المستند

فأي مستند ممكن تخزينه على الكمبيوتر سواء به خطاب أو مذكرة أو كتاب من ألف صفحة أو صورة أو تسجيل صوت أو فيديو أو رسم هندسي.... إلخ كل ذلك ممكن إرساله أو استقباله على جهاز كمبيوتر آخر في الشبكة، و مثال على ذلك إذا قامت شركة هندسية في أي دولة بعمل تصميم لمبنى ضخم في مصر فبدلا من إرسال الرسومات بالبريد أو الشحن و تعرضها للتلف و ير يمكن إرسالها إلى جهاز الكمبيوتر في مصر لتصل في ثوان و يتم طباعتها من الكمبيوتر في مصر و كذلك إذا تم اكتشاف أخطاء في التصميم يمكن الطريقة و التعديل في دقائق، أيضا من الممكن أن يشترك عدة مهندسين أو باحثين منة أماكن مختلفة في بلدان مختلفة في عمل تصميم احد أو تأليف كتاب أو بحث واحد و يتم تبادل الأفكار العمل عبر الإنترنيت.

4. سهولة الاستعمال

فأن جهاز كمبيوتر مهما كان نوعه أو حجمه أو سرعته يمكن أن يستعمل في شبكة ترنيت طالما أمكن ربطه بخط تليفون، يتساوى في ذلك جميع الأجهزة المعروفة القديمة و الحديثة بجميع ماركاتها و طرازها مثل BM، Apple ، Macintosh Unix ، HB FBC و غيرهم. [1]

[1]– د. سلميان أحمد فضل، نفس المرجع، ص 22-23.

5. الحديث و المشاورة و عقد المؤتمرات

فيمكن الحديث الفوري مع الآخرين سواء واحد أو اثنين أو أكثر و ذلك عن طريق أن يقوم كل واحد بكتابة ما يريد وسل فورا إلى الآخرين و يرد عليه الآخرين فورا بنفس الطريقة و يمكن استعمال برامج الاتصال الحديثة لنقل الصوت و الصورة عبر الشبكة ليسمع الآخرين و يراهم و هم يتحدثون معه في نفس الوقت من جميع بلاد العالم.

6. تعتبر شبكة الإنترنيت بما تمثله من تقدم تقني من أهم أدوات التواصل بين الشعوب و يمكن استغلال هذا التواصل في نقل التقدم التكنولوجي و العلمي من الدول المتقدمة للدول النامية

7. تعتبر الشبكة وسيطا في عملية تدريب العاملين بمختلف المصانع والشركات و تعريفهم بأحدث العمل في المصانع و الشركات المشابهة فيدول المتقدمة.

الفرع الرابع: استخدامات الانترنت

تقدم شبكة الانترنت خدمات جليلة لكل المستخدمين يمكن إجمالها في الآتي:

1. البريد الالكتروني مع كل أنحاء العالم.
2. الحصول على الرسائل العلمية والكتب والمعلومات الخاصة بالعلوم وملخصاتها.
3. مشاهدة الأحداث العالمية فور وقوعها وتفاصيلها بصورة أفضل.
4. مشاهدة الأفلام والأحداث الرياضية والعلمية والثقافية
5. قراءة الصحف اليومية والمجلات الأسبوعية
6. على شراء السلع بصورة فورية عبر الشبكة والتجارة الالكترونية
7. متابعة أسواق الأموال والأسهم والسندات
8. إنشاء نوادي صحافة من خلال الشبكة
9. نشر ثقافات الشعوب والدول على نحو يزيل الخطأ واللبس الثابت عن بعض الشعوب والطوائف والأديان
10. نشر التراث والآداب والفنون والآثار

11. الدعاية التجارية والسياحية
12. نقل التكنولوجيا من دولة إلى أخرى
13. إتباع سياسة التعليم عن بعد. [1]

المطلب الثالث: طبيعة المعلومات باعتبارها محل يمكن الاعتداء عليها

الفرع الأول: الشروط التي يجب توافرها في المعلومة محل الحماية

بصفة عامة هناك شروط يجب توافرها في المعلومة حتى تتمتع بالحماية وتتمثل هذه الشروط في الآتي:

- أن تكون المعلومةمحددة ومبتكرة، حيث أنه لا يمكن إطلاق لفظ (معلومة) على كم غير محدد من البيانات والمعلومات، بل يجب أن تكون محددة بوضوح لا يخلق أي لبس بخصوص مداها وتفاصيلها، وأن تكون مبتكرة بحيث أنها ليست معروفة أو متاحة للجميع أو يسهل الوصول إليها بواسطة العامة.
- أن يتوافر في المعلومة السرية والاستئثار، أي أن المعلومة حصر على عدد محدود من الأشخاص، أما خاصية الاستئثار فتعني أن المعلومة تخص أحد الأشخاص بحيث يكون مستأثرا بها، ومن ثم تتوافر هذه الصفة إذا كان الوصول إليها غير مصرحا به إلا بإذن مالك المعلومة.
- المعالجة الآلية للمعلومات يشترط بعض الفقهاء، لكي تتمتع المعلومة بالحماية الجنائية أن تكون معالجة آليا. ونقصد بالمعالجة الآلية للمعلومات، تلك العمليات المتعددة التي تتم بصفة آلية على معلومات لكي تتحول إلى معطيات عن طريق معالجتها داخل نظام آلي. [2]

---

[1]– د. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دراسة في الظاهرة الإجرامية المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2008، ص 18.

[2]- www.lawtechntea.com/2015/12/is.it.the.end.of.government-non-disclosure.agreements/ 26 ديسمبر 2015. الساعة 14:15.

الفرع الثاني: الطبيعة القانونية للمعلومات

هل تعد المعلومة التي تواجه بعيدا عن دعامتها المادية من قبيل المال.

حيث يرى أنصار المذهب التقليدي أو المبدأ أن للمعلومة طبيعة ذاتية خاصة ويرى الجانب الآخر من الفقه وهم أنصار المفاهيم الحديثة أن المعلومة مجموعة مستحدثات من الأموال وسنعرض كل من وجهتي نظر والأسانيد التي إليها استند إليها كلا منهما في تكوين عقيدته ووجهة نظره.

أولا: الطبيعة الذاتية للمعلومة

مؤدى هذا الرأي أن الأشياء التي تعد من قبيل الأموال هي الأشياء القابلة لتملك ويستخلص من هذه الحقيقة أن الأشياء التي تكون قابلة وحدها كمحل للحق الاستشاري التي هي تعد من قبيل الأموال وأن المعلومات التي نقابلها اقتراضا هي من قبيل الأشياء معنوية وأن الحق الاستشاري الذي من شانه أن يتقدم بالنسبة إليها لا يمكن من خلال هذا التحليل التقليدي إلى أن يكون من قبيل حقوق الملكية الأدبية أو الفنية أو الصنعية إلى أن المعلومة المختزنة لا تنتمي إلى المعلومات الأدبية أو الفنية أو الناعية الأمر الذي يؤدي إلى رفحق الإقامة في هذه المجالات وهكذا تستبعد بالضرورة من نظام مجموعة من الأموال.

ثانيا: المعلومات مجموعة مستحدثة من الأموال

كما رأينا سابقا أن التحليل التقليدي قد استبعد المعلومة من مجموعة الأموال و حدد ذلك أن المعلومة ليس لها الحق في الإقامة في مجال قانون الملكية الأدبية.

إلا أن بعض الفقهاء المهتمين بالمشاكل الناشئة عن تزايد الظاهرة المعلوماتية قد قاموا بإطلاق وتطبيق وصف الحال على المعلومة و من أهم العلماء و الفقهاء الذين طبقوا ذلك الوصف الأستاذين، vivant catala، وسوف نوضح الأسانيد التي استند إليها كل منهما على من اختلافهما في الأسلوب. [1]

[1]– سامي علي، علي حام عياد، الجريمة المعلوماتية وإجرام المعلومات، دار الفكر الجامعي، ط 2007، ص 27.

فتعد المعلومة طبقا للأستاذ atal واستقلال عن دعامتها المادية من قبيل المال للحيازة و لتدعيم هذا الوصف فقد أشار بان المعلومة قابلة للحيازة عندما لا يحظر السوق وهي قيمة تقوم وفقا لسعر السوق وأيضا منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها وأن المعلومة ترتبط بصاحبها عن طريق علاقة قانونية وهي علاقة الملك بالشيء الذي يملكه وأنها تنتهي إلى مؤلفها بسبب علاقة التبني التي تربط بينهما.

هكذا اعتمد الأستاذ catal من اجل إخفاء و صف المال على المعلومة على قيمتها الاقتص وعلاقة التبني التي تربط بينها و بين المؤلف ولا تعد هاتان الحجتان من قبيل الحجج المألوفة استخدامها لأجل الاعتراف بالمال و لكن تستحق التأييد.

ويؤكد الأستاذ vivant هذا الرأي مستندا إلى صحيتين أولهما مستمدة من الأستاذين ripert ; planionet ; و مضمونها " أن فكرة الشيء أو المال الذي يغلب عليه الطابع المعنوي محل الحق يجوز أن تستند إلى مال معنوي بحيث يكون هذا المال من قبيل الأموال الاقتصادية أو جدير بحماية القانون"

والحجة الثانية خاصة بالأستاذ vivant و مضمونها " أن كل الأشياء المملوكة ملكية معنوية والتي يعترف بها القانون ترتكز على الإقرار بان للمعلومة قيمة عندما نكون بصدد براعة اختراع أو علامات أو رسومات أو نماذج أو من قبيل حق المؤلف و منشئ ة هو الذي يقدم ويكشف ويطلع الجماعة على شيء ما بغض النظر عن الشكل أو الفكرة فهو يقدم لهم المعلومة بمعنى أوسع و لكنها خاصة به و يجب ان تعامل هذه الأخيرة بوصفها مالا و تصبح محلا للحق فلا يوجد ما يسمى بالملكية المعنوية بدون لاعتراف بقيمة المعلوماتية"

و يستخمن ذلك أن المعلومة باعتبارها مالا فهي مجموعة تندرج في نطاق القانون الوضعي و يضيف vivant قائلا أن المال المعلوماتي ليس شيء مستحدثا. [1]

[1]– سامي علي، علي حام عياد، نفس المرجع، ص 28-29.

ومن وجهة نظره أيضا أن المعلومة هي حتما من قبيل المال بسبب قيمتها الاقتصادية، فان هذا المال ليس مجال مستحدث لأنه يدخل في مجموعة قائمة من قبل خاصة بالأموال المعلوماتية والتي وفقا لرأيه متاحة و معترف بها عن طريق الملكية الأدبية و حينئذ يفهم انه يقرر و يحسم على فكرة أن المعلومة يمكن أن تكون محلا لعقد بيع طالما أن الإبداع يرتب بصاحبه بل يمكن علاوة على ذلك نقل حق الانتفاع بالمعلومة و استها و على نحو ما أشار إليه الأستاذ catala عندما نوه بان المعلومة ترتبط بصاحبها عن طريق علاقة التبني التي تربط بينهما.

و يضيف أن لصاحب المعلومة أن يتنازل عنها بموجب عقدا و يفيد استخدامها أو أن يرفقه و يبدو من خلال هذين الشرطين أن المعلومة هي بمثابة مال و لكنها ملا مبتكرا بسبب الحقائق الذاتية لحق الملكية الذي استند عليه.

ونعرض هنا إجابة على التساؤل: المعلومات هل هي مال شيء ذو قيمة كيان معنوي هل لأنها تتصل غالبا بوعاء تفرغ فيه ترتبط عضويا بوعائها لذا فهي شيء مادي بالنظر للوعاء المفرغة فيه ؟

المعلومات ذات الطبيعة المعنوية تستقل تماما من حيث الأصل عن الوعاء المفرغة فيه وتعد النظرة قاصرة أن اتجهت نظرية قانون الكمبيوتر نحو حماية المعلومات وفق وعائها والمعلومات الشائعة من حيث الأصل وحصيلة تراكم معرفي بشري ومن هنا ينشئ لكل فرد الحق في الوصول إليها ويتعيرحق انسيابها و تدفقها وهذا هو جوهر وأساس فكرة الحق في المعلومات لكن المعلومات فيما اتجهت إليه أنشطة تقنية المعلومات:

أولا: أما أنها أمست بذاتها ذات قيمة اقتصادية عالية تزداد يوما بعد يوم لذا وصفت وتوصف بأنها مال فإنها قابلة لتمتلك وهو ما يفرز مفهوم الحق في ملكية المعلومات. [1]

[1]– سامي علي، علي حام عياد، ، ص 30.

ثانيا: أو أنها أي المعلومات قد تتصل بشخص دون غيره عندما تتعلق ببياناتـه الاسـمية أو الشخصية ولكنها تستخدم من الغير وبالذات السـلطات لأغـراض تتصـل بالنشـاط الاجتماعي والاقتصادي والسياسي للدولة من هنا تنشئ المعلومات حقا في السيطرة عليها وحق في استخدامها ضمن قيود وضوابط وهنا تبدأ وتنتهي حدود الحق في الخصوصـية المعلوماتية أو في حماية البيانات الشخصية.

ثالثا: والمعلومات قد تكون الخلق الإبداعي للفكرة أو الابتكار في تنظيم الحقائق و الأوامر فتكون أمام مصنفات وليدة الأداء الإبداعي لعقول المؤلفين و المختـرعيمثـل وعـاء المعلومة فتكون لذلك وبما انطوت عليه من عناصر تتطلبها نظام الملكية الفكرية مادة حق الملكية الفكرية وموضعها للاستئثار المعنوي وللاستغلال المادي فتخلق في ذلك الحق في الملكية الفكرية لمصنفات المعلوماتية والقانون ليس بوسعه أن يكون عملية تنظيم إلا لحق يعترف به ويكلفه القانون وليس ثمة حماية إلا حيث تتوفر المصلحة التي يحميها القانون.

لهذا كان وجود الحماية القانونية مرتبطا بالاعتراف بالحق في المعلومات انسيابها وتدفقها وقدرة الفرد على الوصول لكن هذا الحق يثير إشـكالية نطـاق السـيطرة علـى المعلومات عبر ما سيوفره الاعتراف بهذا الحق من مكنات وسلطات قانونية هذه السيطرة التي تتعارض جوهريا مع مفهوم الحق في الشيوع المعلومات من الشمولية تمتد للأفكـار والحقائق كان وراء دعوات عدم إخضاع الحق فيها لأية قيود لكن الحقيقة ا ما ارتبط بهذا الحق من حقوق أخرى كالحق في ملكية المعلومات والحق فيما يتصل بهـا مـن حقـوق فكرية والحق في الخصوصية إنما هي ليست قيودا علىالحق بالمعلومات بقدر مـا هـي تنظيم لإمكانات والسلطات التي تقع في نطاق الحق في المعلومـات وتنظـيم المصـالح المعترف بها قانونا في نطاق هذا الحق إذن المعلومات كيان معنـوي يتعـين الاعتـراف بحمايتها بهذه الصفة وبما يتصل بها من سلوكيات وأداء وأنشطة استثمار تماما. [1]

[1]– سامي علي، علي حام عياد، نفس المرجع، ص 31.

كما تم الاعتراف بالمال المادي وخضع لقواعد ونظريات في الحقلين المدني والجزائي وأساس حماية المعلومات توفيرالقانوني المشابه (من حيث شموليته ونطاقه وفعاليته) لذلك الذي وفرته التشريعات للمال المادي والحق في المعلومات يوجب إقرار مبادئ كفالة حرية الوصول للمعلومات.

إقرار قواعد بشأن حقيقة يتعين أن يحميها القانون وهي حق الأفراد في المعلومات وحقهم في سلامة ومشروعية التعامل مع بياناته الشخصية وحقهم في ثمرة الإبداع في عقولهم المتصلة بنطاق المعلومات و المفرغة ضمن مصنفات تحميها قواعد الملكية الفكرية وحق مالكي المعلومات (بأشكالها المختلفة) المصنفة أو الخاصة بنشاطهم الاستثماري والتجاري وإدارتهم للمعلومات التي تمثل رأس المال الفعلي لمشروعاتهم وحق الفرد في سلامة ما يتعامل معه من معلومات سواء المرسلة منه أم المستقبلة أم نظامه التقني في المعلومات الحق في ملكية المعلومات الحق في الملكية الفكرية للمعلومات الحق في الخصوصية المعلوماتية الحق في إدارة المعلومات الحق في امن التعامل المرتكز على المعلومات.

ونظرا لان المعلومات: كيان معنوي لهذا ذات القيمة الاقتصادية للمال المادي يتعين أن تخضع لأحكامه والتعامل تماما كما يعامل فتحيطها حماية ذات الحقوق المقررة على المال المادي و يتعرف لهل بذات المصالح التي يتعرف بها القانون المادي.

وفي نطاق الحماية الجنائية يتعين الإقرار بصلاحية المعلومات كمحل لحماية من أنشطة الاعتداء كافة تماما كما المال المادي المحمي ضمن نصوص و قواعد حماية الأموال و يتعين الاعتراف لمحيط المعلومات ووعائها التقني بالصفة المقبولة لخضوعه للتصرفات التي ترتكب في بيئة المحرر الكتابي والمستندات الخطية ويتعين المساواة بين السلوكيات المادية في انتهاك السرية وبين السلوكيات المعنوية في انتهاك الخصوصية.[1]

[1]– سامي علي، علي حام عياد، نفس المرجع، ص 32.

المبحث الثاني: الجريمة المعلوماتية

إن الجريمة المعلوماتية باعتبارها مستحدثة أثارت ضجة في الأوساط الفقهية من حيث مفهومها والأفعال الإجرامية التي تدخل في نظامها لذالك سنطرق في هذا المبحث لبيان مفعولها ل ومن ثم تنتقل لمرتكبيها في مطلب ثاني وأخيرا لطبيعتها القانونية في مطلب ثالث.

المطلب الأول: مفهوم الجريمة المعلوماتية

الفرع الأول: تعريف الجريمة المعلوماتية

لعل المشكلة الأولى والأساسية التي تعترض ظاهرة الجريمة المعلوماتية هي عدم وجود تعريف مجمع عليه لهذه الجريمة، فلقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا كبيرا من أجل الوصول إلى تعريف مناسب.

يتلاءم مع طبيعة الجريمة المعلوماتية إلا أن كثيرا من هذه المحاولات قد باءت بالفشل حتى أنه قد قيل إن اعلوماتية تقاوم التعريف. ولقد دعا ذلك كثيرا من هؤلاء إلى تفادي مثل هذا التعريف بحجة أن الجريمة المعلوماتية ما هي إلا جريمة تقليدية ارتبطت بأسلوب جديد على أنه إذا كان ذلك صحيحا في بعض الحالات فإن كثيرا من جرائم الحاسب الآلي تتميز بسمات خاصة تجعل من الصعب تطبيق التعريفات التقليدية عليها. ولاشك أن عدم الاتفاق على تعريف متفق عليه لجرائم الحاسب الآلي إنما يؤدي إلى إثارة عدد من النقاط العملية يتمثل أهمها في: صعوبة تقدير حجم هذه الظاهرة، وتعذر إيجاد الحلواللازمة لمواجهتها، وكذلك صعوبة تحقيق التعاون الدولي لمكافحتها.

إن المحاولات التي بذلت من أجل تعريف الجريمة المعلوماتية متعددة وإن كانت لا تخرج جميعها عن أحد الاتجاهين: الأول، اتجاه يضيق من مفهوم الجريمة المعلوماتية، بحيث تقل الحالات التي يمكن أن يتصف فيها النشاط الإجرامي بها. [1]

[1]– د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، مصر، ص 28.

والثاني، على العكس، يوسع من مفهوم هذه الجريمة حتى أنه يمكن القول إنه يدخل في عدادها –الكثير من الأحيان– أفعالا لا يمكن أن تعد من قبيل جرائم الحاسب الآلي.

وسوف نحاول فيما يلي إلقاء الضوء على الاتجاهين، ثم نبين موقفنا منهما.

أولا: الاتجاه الذي يضيق من مفهوم الجريمة المعلوماتي.

ويعرف أنصار هذا الاتجاه المعلوماتية، بأنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، لملاحقته وتحقيقه من ناحية أخرى. وطبقا لهذا التعريف يجب أن تتوافر معرفة تكنولوجيا الحاسبات الآلية بدرجة كبيرة ليس فقط من أجل ارتكاب الجريمة المعلوماتية ولكن أيضا من أجل التمكن من ملاحقتها والتحقيق فيها على نحو صحيح، أي أن مرتكب الجريمة المعلوماتية والقائمون على ملاحقتها على درجة كبيرة من العلم بهذه التكنولوجيا، وقد أخذت وزارة العدل الأمريكية بهذا التعريف في تقرير صادر عنها عام 1989 يتعلق بجرائم المعلوماتية.

والأخذ بالتعريف المتقدم في رأينا يضيق على نحو كبير من الجريمة المعلوماتية، حتى أن البعض يرى أن الجريمة المعلوماتية في ظل هذا الاتجاه سوف تصبح أشبه بالخرافة، فهذا التعريف يحصر الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، وهو إن تحقق في بعض الأحوال فإنه لا يتحقق في كثير منها، ففي كثير من برتكب الفعل دون الحاجة إلى هذا القدر من المعرفة، ورغم ذلك لا يمكننا إنكار أن هذه الأفعال تدخل في جرائم المعلوماتية. فإتلاف البيانات المخزونة داخل نظام الحاسب الآلي، على سبيل المثال، لا يتطلب قدرا كبيرا من العلم بتكنولوجيا الحاسبات الآلية، وعلى الرغم من ذلك يعد الفعل مجرما في كثير من التشريعات كقانون العقوبات الفرنسي باعتباره من جرائم المعلوماتية. [1]

[1]– د. نائلة عادل محمد فريد قورة، نفس المرجع ، ص 29.

ويذهب أنصار هذا الاتجاه إلى أن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية تتكفل بها النصوص التقليدية للقوانين الجنائية، فلا حاجة لنا في هذه الحالة إلى نصوص جديدة للتعامل مع هذه الأفعال، وذلك على خلاف الجرائم التي يتوافر لها هذه المعرفة فهي بحاجة إلى نصوص خاصة تتلاءم مع طبيعتها التي تختلف عن غيرها من الجرائم التقليدية.

وفي تضييق آخر لمفهوم الجريمة المعلوماتية، يرى البعض أن الجريمة المعلوماتية ليست هي التي يكون الحاسب الآلي أداة لارتكابها، بل هي التي تقع على الحب أو داخل نظامه فقط. فيعرفون جريمة الحاسب بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه.

ولاشك أن هذا التعريف يضيق بدوره من مفهوم الجريمة المعلوماتية، إذ يخرج من نطبير من الأفعال غير المشروعة التي يستخدم الحاسب كأداة لارتكابها.

والأمثلة على ذلك عديدة وأهمها الاحتيال المعلوماتي كما سنبين تفصيلا فيما بعد.

ثانيا: الاتجاه الذي يوسع من مفهوم الجريمة المعلوماتية.

على عكس الاتجاه السابق، يذهب فريق آخر من الفقهاء إلى التوسيع من مفهوم هذه الجريمة. وتتباين مواقف الفقهاء أنصار هذا الاتجاه حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية.

فمن يذهب فريق من الفقهاء بعضها إلى تعريف الجريمة المعلوماتية بأنها كل سلوك إجرامي يتمعدة الحاسب الآلي، أو هي كل جريمة تتم في محيط الحاسبات الآلية. يماثل هذا التعريف ما ذهبت إليه مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 عند تناولهم موضوع الإجرام المرتبط بالمعلوماتية [1]

[1]– د. نائلة عادل محمد فريد قورة، نفس المرجع ، ص 30.

حيث ذهبوا إلى تعريف الجريمة المعلوماتية بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها.

ولاشك أن الاتجاه المتقدم ينطوي على توسع كبير لمفهوم الجريمة المعلوماتية، حيث إن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يسبغ عليه وصف الجريمة المعلوماتية. ومن جانبنا نرى صعوبة قبول هذت التوجه، فالحب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائقة الحاسب ذاته أو الأقراص والأسطوانات الممغنطة على سبيل المثال، فلا يمكن إسباغ وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد أن الحاسب أو أي من مكوناته المادية كانوا محلا لفعل الاختلاس.

إلا أن هناك تعريفات أخرى في إطار الاتجاه الموسع كانت أكثر تحديدا في تعريف الجريمة المعلوماتية، ومن ذلك تعريف الجريلوماتية بأنها: كل تلاعب بالحاسب الآلي ونظامه من أجل الحصول بطريقة غير مشروعة :مكسب أو إلحاق خسارة بالمجني عليه. وكذلك التعريف الذي بين مظهرين للسلوك الإجرامي في جرائم المعلوماتية: الأول يتعلق باستخدام الحاسب الآلي من أجل ارتكاب جريمة أخرى بغرض الحصول على مكسب مادي، أما الثاني فيتمثل في الاعتداء على الحاسب الآلي بغرض إلحاق الضرر بالمجني عليه.

الفرع الثاني: سمات الجريمة المعلوماتية:

1. تقع الجريمة في بيئة المعالجة الآلية للبيانات، حيث يستلزم لقيامها التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي بغرض معالجتها الكترونيا ،بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة والتي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها وطباعتها وهذه العمليات وثيقة الصلة بارتكاب الجريمة، ولابد من فهم الجاني لها أثناء ارتكابها في حالات التزوير والتقليد[1].

[1]– د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 93.

2. إثبات تلك الجرائم يحيط به كثير من الصعوبات التي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثراً خارجياً، فلا يوجد جثث لقتلى أو أثاراً لدماء وإذا اكتشفت جريمة فلا يكون ذلك إلا بمحض الصدفة، والدليل على ذلك أنه لم يُكتشف منها إلا نسبة 1% فقط، والذي تم الإبلاغ عنه للسلطات المختصة لا يتعدى 15 % من النسبة السابقة.

3. أدلة الإدانة فيها غير كافية إلا في حدود 20% فقط، ويرجع ذلك إلى عدة عوامل ة في عدم وجود أي أثر كتابي، إذ يتم نقل المعلومات بالنبضات الالكترونية،كما وأن الجاني يستطيع تدمير دليل الإدانة ضده في أقل من ثانية.

4. إحجام الشركات والمؤسسات في مجتمع الأعمال عن الإبلاغ عما يُرتكب داخلها من جرائم تجنباً للإساءة إلى السمعة وهز الثقة فيها.

5. هذه الجرائم لا تعرف الحدود بين الدول والقارات حيث أن القائم على النظام المعلوماتي في أي دولة يمكنه أن يحول مبلغاً من المال لأي مكان في العالم مضيفاً له صفر أو بعض الأصفار لحسابه الخاص، بل يستطيع أي شخص أن يعرف كلمة السر لي شبكة في العالم ويتصل بها ويغير ما بها من معلومات.

6. الرغبة في استقرار حركة التعامل ومحاولة إخفاء أسلوب الجريمة حتى لا يتم تقليدها من جانب الآخرين، كل ذلك يدفع المجني عليه إلى الإحجام عن مساعدة السلطات المختصة في إثبات الجريمة أو الكشف عنها، حتى في حالة الضبط لا يتعاون مع جهات التحقيق خوفاً مما يترتب على ذلك من دعاية مضادة وضياع الثقة، حيث يكون المجني عليه في مثل هذه الحالة بنك أو مؤسسة مالية. [1]

[1]– د. أحمد خليفة الملط، نفس المرجع، ص 94.

الفرع الثالث: محل الجريمة المعلوماتية

محل الجرائم المعلوماتية

سنتناول في هذا الفرع إيضاح محل الجريمة المعلوماتية الذي يتمثل في النظام المعلوماتيوقوع الجرائم منه أو عليه. وسنتعرض لها في هذا الفرع من خلال عنصرين هما: أولا: الجرائم الواقعة على نظام المعلوماتي، ثانيا: الجرائم الواقعة باستخدام النظام المعلوماتي

أولا: الجرائم الواقعة على النظام المعلوماتي

محل الجرائم المعلوماتية يمكن أن يكون على النظام المعلوماتي من خلال مكوناته المادية والمنطقية (البرامج) والمعلومات المدرجة بالنظام ولذلك سوف نبين هذه الجرائم من خلال المطالب الآتية:

- الاعتد على المكونات المادية للنظام المعلوماتي
- الاعتداء على المنات المنطقية (البرامج) للنظام المعلوماتي
- الاعتداء على المعلومات المدرجة بالنظام المعلوماتي

أ. الاعتداء على المكونات المادية للنظام المعلوماتي

يتضح من خلال تعرضنا للاعتداء على المكونات المادية للنظام المعلوماتي، إننا نتحدث عن الاعتداء على الأجهزة والمعدات الملحقة به من اسطوانات وشرائط ممغنطة وكابلات وخلافه، وفي مثل هذه الحالة من الاعتداء لا نخرج عن أن نكون بصدد جرائم عادية أي تقليدية لا يربطها بالنظام المعلوماتي سوى الأجهزة وملحقاتها محل الجريمة والتي تستخدم في تشغيل النظام المعلوماتي مع احتفاظها دائما بصفات أي شيء مادي. [1]

[1]– د. أحمد خليفة الملط، نفس المرجع، ص 171.

وفي هذه الحالة يمكن أن تكون هذه المكونات محلا للسرقة أو محلا للإتلاف العمدي ويتحقق ذلك عن طريق إتلاف المكونات بالضرب بآلات حادة أو ثقيلة أو إشعال الحرا بشحنات ناسفة أو استخدام قنبلة غاز أو مواد ملتهبة أو العبث بمفاتيح التشغيل أو محو بطاقات التعريف بما فيها من معلومات مخزنة أو خربشة الشريط أو مسح البرامج وإخفاء البطاقات أو إلقاء السجائر على اسطوانات التشغيل أو إفسادها مغناطيسيا بتعريضها إلى أي مجال مغناطيسي متلف ويترتب على هذا الإتلاف خسائر كبيرة.

ومن أمثلة ذلك، ما حدث من تنظيم الألوية الحمراء، بايطاليا حيث قامت مجموعة من المتخصصين لديهم في التكنولوجيا بتدمير مركز المعالجة الآلية لأحد الشركات بالديناميت مما أدى إلى خسائر بلغت قيمتها مليون دولار. وأيضا خسرت شركة ايطالية أربعة أنظمة خاصة بها بلغت قيمتها أربعة مليون دولار.

وحدث في فرنسا أيضا حالات إتلاف لمعدات مؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية وقدرت الخسائر بحوالي خمسة ملايين فرنك فرنسي وأن صور الإتلاف كثيرة في هذا المجال

رأى يرى أنه يعد من الجرائم الواقعة على المكونات المادية للنظام المعلوماتي سرقة وقت الماكينة أو الآلة. وهذه الجريمة تتم عادة من قبل العاملين بالنظام حيث أنهم يلجئون في بعض الأحيان إلى استخدام النظام المعلوماتي في أعمال خاصة بهم وهكذا تكون واقعة السرقة منصبة على أيشاء مادية بمعنى الكلمة ولكن على وقت الجهاز الذي يمكن تقويمه ماليا.

جريمة سرقة وقت الماكينة "الآلة" من الجرائم الشائعة في فرنسا في كثير من مراكز البحث فمن الممكن أن ينتقل باحث من أجل توفير نفقات سفره إلى مركز آخر أو أن يستعير كلمة السر أو الشللوصول إلى بنك المعلومات الخاص به. [1]

[1]– د. أحمد خليفة الملط، نفس المرجع، ص 172.

ويعتبر هذا الوقت من الأجور المكلفة جدا وقد يؤدي على إحداث خسائر مالية كبيرة يفوق بكثير بور المستخدمين بالمنشأة، وكذلك يدخل ضمن المكونات المادية ما يكون محلا للسرقة أو خيانة الأمانة.

والحقيقة أن خطورة واقعة ت المكونات المادية لا تكمن في الشيء المسروق فقط لضآلة قيمتها المادية بالمقارنة بما تحتويه هذه المكونات من معلومات وبيانات تقدر خسائر بأموال طائلة.

ب. الاعتداء على كونات المنطقية (البرامج) للنظام المعلوماتي

يقصد بالبرامج كل ما تم إعداده بواسطة مبرمجون وخبراء متخصون في التخطيط والبرامج لخدمة أهداف معينة، والجرائم المعلوماتية تزداد خطورتها حينما تقع على البرامج وليس على المكونات المادية لها وذلك لقيمة ما تحتويه هذه البرامج من معلومات وبيانات. ويستلزم هذا النمط من الجرائم معرفة فنية عالية في مجال البرمجة ومن المتصور أن تقع هذه الجرائم في حالتين الأولى على البرامج التطبيقية والثانية على برامج التشغيل ونوض من خلال فرعين الأول: - الاعتداء على البرامج التطبيقية، الثاني:

- الاعتداء على برامج التشغيل

- **الجرائم الواقعة على البرامج التطبيقية**

يرى الفقه أن هذ من الجرائم نسبة تقدر بحوالي 15 % من مجموعة حالات الجرائم المعلوماتية وتأخذ الصورة الغالبة لهذه البرامج قيام المجرم المعلوماتي أولا بتعديل البرامج ثانيا التلاعب فيه وذلك لتحقيق أكبر قدر ممكن من الاستفادة المادية.

- **تعديل البرنامج**

هدف الرئيسي لتعديل هذه البرامج هو اختلاس النقود، وتكثر تلك الجرائم في مجال الحسابات. [1]

[1]- د. أحمد خليفة الملط، نفس المرجع، ص 173.

- وهناك أمثلة كثيرة لذلك، من أهمها قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بوسيلته الخاصة بحيث يقوم بضافة 10 سنت لمصاريف إدارة الحسابات الداخلية على كل عشرة دولارات، دولار واحد على كل حساب يزيد عن عشرة دولارات قيد المصاريف الزائدة في حساب خاص به أسماه Zzwick حصل على مئات الدولارات كل شهر. وكان بالإمكان أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل له وفقا للترتيب الأبجدي وحينئذ اكتشف عدم وجود ما يدعى Zzwick.

- وهنا مثال آخر لموظف مفصول تسبب في إفلاس المشروع الذي كان يعمل به من قبل انتقاما من المسؤولين عنه، بأن قام ببرمجة النظام المعلوماتي للمنشأة التي كان يعمل بها بحيث يؤدي خلال ستة شهور إلى اختفاء كل البيانات المتعلقة بديون المشروع.

- وهناك نظام أكثر خطورة وانتشار يطلق عه سلامي (Salami) وتقوم فكرة هذا النظام على اقتراف الاختلاس عن طريق استقطاعات لمبالغ زهيدة وعلى فترات زمنية طويلة ومتباينة من خلال صفقات عديدة يترتب عليها تحقيق فائدة كبيرة وبمبالغ طائلة وفي حالة اكتشافها فإن المجني عليه يرى أنها لا تستحق تكبد عناء الإبلاغ والشكوى، وقد قام أحد المستخدمين الأمريكيين ويدعى E.Royce بإحدى المنشآت التجارية الكبرى بها وحقق خلال ست سنوات ما يقر من 2 مليون دولار.[1]

- وهناك تقنية أخرى على قدر من البراعة تتمثل في استقطاع بعض السنتيمات من الإيداعات الدورية" وعلى سبيل المثال جبر الكسور عن طريق الخطأ" وتحويلها إلى حسابات خاصة وقد أطلق عليها مصطلح الحلاقة Perruque بسبب استقطاع

[1]– د. أحمد خليفة الملط، نفس المرجع، ص 174.

سنتيم بسنتيم على نمط الحلاق الذي ينجز عمله شعره بشعره، وهي تطبق في البنوك التي تمنح فوائد على الحسابات الجارية،وقد قام مستخدم بإحدى شركات التأمين باستخدام تلك الطريقة في تحويل مبالغ كبيرة لحسابه الشخصي.

- **التلاعب في البرنامج**

أ. قد يصل الأمر بقيام أحد المبرمجين ذوي النوايا السيئة إلى زرع برنامج فرعي Un-sous Program غير مسموح به في البرنامج الأصلي ويسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي،ويمكن دفن هذا البرنامج الصغير في مكونات البرنامج الخاص بالمنشأة...ولصغره ودقته لا يحدث اكتشافه إلا بالصدفة.

ومثال لذلك ما حدث بأحد البنوك بزرع برنامج فرعي بمنشأة للكيانات المنطقية بإدارة الحسابات يتجاهل كل عمليات السحب التي تتم بمعرفة المبرمج سواء عن طريق بطاقات أو شيكات حسابية ويتحمل البنك هذه المسحوبات في باب ميزانية الإدارة، واكتشف بمحض الصدفة أيضا من خلال هذه الطريقيروس "حصان طروادة" عندما حدث عطل بأحد النظم المعلوماتية مما استلزم معالجة يدوية لكل الحسابات.

ب.وهناك أيضا تقنية معروفة تحت مصطلح(Bombe logique) قنبلة منطقية وهي قريبة الشبه من القنبلة الزمنية والتي تسمح بتحريك أحداث مستقبلية في تاريخ محدد أو طبقا لوقوع أحداث معينة... وقد استوحى Thery Berton هذه التقنية وشيد على أساها قصة واقعيطلق عليها Software الحرب الناعمة وتدور أحداثها حول شاب أمريكي يعمل مهندس، أسس نموذج لشركة خدمات معلوماتية بالولايات المتحدة يكون غايته وصف الحرب الناعمة الدائرة بين الولايات المتحدة الأمريكية والاتحاد السوفيتي (سابقا) [1]

[1]– د. أحمد خليفة الملط، نفس المرجع، ص 175.

- **الاعتداء على برنامج التشغيل**

تعتبر برامج التشغيل هي البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بالي التعليمات الخاصة بالنظام، والجريمة في هذه الحالة تتحقق بتزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصها بواسطة شفرة تتيح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي.....

وتأخذ الجرائم الواقعة على برامج التشغيل إحدى صورتين ا لي: – المصيدة والثانية: – تصميم برنامج وهمي وسنتناول هاتين الصورتين من خلال ما تعرض له الباحثون.

– **المصيدة**

تعني أن يتضمن أي برنامج عند إعداده من المبرمجين أخطاء وعيوب قد لا يكتشف البعض منها عند استخدامه فهم يتركون ممرات خالية وفواصل وأكواد في البرنامج حتى يستطيعون بعد ذلك تنفيذ التعديلات الضرورية بإدخال أكواد إضافية أو إحداث مخارلة ويمكن أيضا الولوج إلى داخل النظام المعلوماتي والوصول إلى كل المعلومات التي تحويها الذاكرة، وقد يصل الأمر أحيانا ببعض المبرمجين من ذوي النوايا السيئة والذين لهم دراية بأهمية هذا النظام التقني الموجود بين أيديهم بأن يتغاضوا عن هذه المصيدة ولا ينبهوا إليها أي شخص لكونهم هم المؤتمنين على السر.

فيمكنهم ذلك في أي لحظة أن يستخدموا البرنامج وفقا لأهوائهم واستغلالهم له من الناحية الفنية، ويمكن بهذه الوسيلة أن يصبح مرتكب هذا العمل الإجرامي هو المهين على النظام ويترتب عليه نتائج سيئة بالنسبة لصاحب العمل المعتدى عليه. [1]

[1]– د. محمد سامي الشوا، الجرائم الواقعة على شبكة الانترنت، دار النهضة القاهرة، ص 28.

- **تصميم برنامج وهمي**

يقوم المبرمجون من خلال برامج تشغيل النظام المعلوماتي وضع برنامج مصمم خصيصا لارتكاب الجريمة ومراقبة تنفيذها والتي يرى الخبراء والباحثون أنها لا تكتشف إلا صدفة وهناك مثال واضح على ذلك فقد قامت إحدى شركات التأمين الأمريكية- في- مدينة لوس أنجلوس بواسطنا والحاسب الآلي الخاص بها بتصميم برنامج وهمي يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عدهم 64.000 وثيقة تأمين.

وقد تقاضت الشركة من اتحاد شركات التأمين عمولات نظيرها، وأقتصر دورها فقط على إدارة الحسابات وإمعانا في التضليل وبغرض إعطاء العقود الوهمية مظهرا مشابها للحصر قامت الشركة المذكورة بتنشيط الملفات المختلفة لأصحاب الوثائق عن طريق تغيير الموطن والوظيفة وبعض الإقرارات الأخرى.

ونحن نرى أن الجرائم المعلوماتية التي تقع على المكونات المنطقية للنظام المعلوماتي تشكل جرائم خطيرة وسريعة ومتطورة بل إنها في تزايد مستمر طبقا لازدياد متخدام تلك التقنية وتحتاج إلى ردع وهو ما سنوضحه تفصيليا فيما بعد.

ج. الاعتداء على المعلومات المدرجة بالنظام المعلوماتي

المعلومات هي المحور الأساسي الذي تدور حوله المعلوماتية التي تمثل المعالجة الآلية للبيانات والمعلومات ونظرا لما لها من اقتصادية كبيرة باعتبارها أساس عمل النظام المعلوماتي فتعد هدفا للجرائم المعلوماتية من ناحية التلاعب فيها أو إتلافها و، هذا من خلال فرعين الأول: - التلاعب في المعلومات الثاني: - إتلاف المعلومات. [1]

[1]- د. محمد سامي الشوا، نفس المرجع، ص 29.

- **التلاعب في المعلومات**

يعد التلاعب في المعلومات وفقا لآراء الخبراء من أكثر جرائم الغش في أوربا ويتم هذا في المعلومات الموجودة داخل النظام المعلوماتي بطريقتين التلاعب المباشر، غير المباشر.

- **التلاعب المباشر:** وتتم هذه الحالة عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي والذيتسند إليه وظيفة المحاسبة والمعلومات المالية ويأخذ هذا التلاعب عدة صور من أهمها:

1-**ضم مستخدمين غير موجودين بالعمل** وتظهر هذه الحالة في المنشآت التي تضم عددا كبيرا من العاملين المؤقتين، ودائمي التغيير للظروف الاقتصادية والمالية وقائمة الطلبات، حيث يقوم المسؤول بالدفع بأسماء عدد من هؤلاء الموظفين الوهميين إلى الإدارة المركزية الخاصة باستئجار المستخدمين ويترتب على ذلك الحصول على مرتباتهم...

ومثال لذلك استطاع أحد المسؤولين عن القسم المالي بإحدى الشركات الفرنسية اختلاس أكثر من مليون فرنك فرنسي ووضعه في حسابه الخاص وحساب شركاءه في العمل الإجرامي، ثم قام بمحو آثار هذا العمل الإجرامي الذي ارتكبه.

2-**الإبقاء عاملفات مستخدمين تركوا العمل** وهو نمط جديد من أنماط التلاعب في مراكز المعلومات حيث يستطيع المسؤول عن الإدارة المالية المعلوماتية الإبقاء على ملفات العاملين الذين تركوا العمل دون حذفهم من المنشأة ويحصل من ذلك على مبالغ مالية شهرية. [1]

3-**اختلاس النقود ويتم ذلك** عن طريق عمل تحويلات لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك وتسجيلها وإعادة ترحيلها وإرسالها لحساب آخر في بنك آخر، ومثال لذلك ضبط مستخدم يعمل لدى فرع مصر في

[1]- د. محمد سامي الشوا، نفس المرجع، ص 30.

تابع لبنك Indo-Suej بفرنسا قام بعمل تحويلات لمبالغ تقدر بحوالي سبعة ملايين فرنك وتم ضبطها بمعرفة شرطة مرسيليا ووجهت له تهمة الاختلاس.

- **التلاعب غير المباشر:** ويحدث ذلك عن طريق التدخل الغير مباشر لدى المعلومات المسجلة بالنظام المعلوماتي وغالبا ما تتم باستخدام أحد وسالتخزين أو بواسطة التلاعب عن بعد باستخدام أدوات معينة ومعرفة الأرقام والشفرات الخاصة بالحسابات.

ويتخذ ذلك عدة وصر منها :

-**التلاعب في الشرائط الممغنطة:** وهي إحدى طرق التلاعب في المعلومات بطريق غير مباشر حيث يمكن أن ترسل معلومات لإحدى الشركات بشأن طلب دفع مقابل لأي تعاملات مالية ويمكن أن تتم الموافقة عليها وإرسالها بمبالغها وتتدرج هذه العمليات أيضا تحت عمليات النصب.

ومثال على ذلك أخفقت ،نصب تقدر بحوالي 21 مليون فرنك فرنسي بسبب خطأ لمعلوماتي مبتدئ وتتلخص وقائع الدعوى في قيام أحد الموظفين بأحد فروع الشركة الفرنسية (Isovertst Gobain) بإرسال شريط ممغنط احتوى على 139 إذن دفع وعند معالجته بالبنك بالقسم المعلوماتي تم رفض نسخه لعيب في طول الشريط وألقى القبض على المتهم الذي لو نجحت محاولته لحقق مبالغ طائلة، وكان بالإمكان وفقا لآراء الخبراء أن يكتب لهذه المحاولة النجاح إذا توافر لدى المزيف المعرفة التقنية اللازمة في مجال المعلومات.

2-**التلاعب في المعلومات:** عن بعد وتتمثل هذه الصورة في استخدام المجرم كلمة السر أو مفتاح الشفرة أوأداه ربط بالمركز المعلوماتي لأي جهة ويمكن لهذه الجريمة أن تتم على مسافات بعيدة بحيث يستطيع الجاني لتسلل إلى المعلومات المخزنة بالنظام المعلوماتي والحصول على المنفعة المالية التي يريدها. [1]

[1]- د. محمد سامي الشوا، نفس المرجع، ص 30.

ومثالا لذلك قيام طالب أمريكي بالدخول غير المشروع فـ أحد الأنظمة المعلوماتية، وأصبح مالكا لها لفترة من الزمن بعد تغيير مفتاح الشفرة وترتب على ذلك أن رفض هذا النظام أن يمد أصحابه ومستخدميه الشرعيين بالخدمات المعلوماتية لبضعة ساعات.

ويشير ذلك إلى مدى جسامة هذه الاعتداءات، وقد لجأ بعض الجناة في الجرائم المعلوماتية إلى الهجوم بواسطة معلومات محمولة بواسطة شبكات اتصالات بعدية بالتقاط أذونات تحويل عن طريق وسائل الكترونية مصطنعة وتزويدها بالأمر بالدفع لحساب آخر.

- **إتلاف المعلومات**

إن المعلومات التي تخزينها النظام المعلوماتي تمثل هدفا أساسيا بالنسبة للجناة الذين يحاولون الاستيلاء عليها بشتى الطرق وقد تتعرض هذه المعلومات للإتلاف. كما سبق أن بينا ضمن المكونات المنطقية للنظام المعلوماتي بطرق الإتلاف العادية من حريق أو ضرب أو سرقة، كما يمكن للمسؤولين عن حفظ المعلومات أن يتلفوا المعلومات المكلفين داخل النظام المعلوماتي وتشكل هذه العمليات عنصرا هاما من عناصر جرائم التزويد في مجال المعلومات والتي سنعرض لها في دراستنا من خلال جرائم الغش المعلوماتي في الباب الثالث وتأخذ جرائم إتلاف المعلومات إحدى صورتين أولا: -

استبدال المعلمات ثانيا:- محو المعلومات.

وسيتم إيضاح هذه الصور فيما يلي :

- استبدال المعلومات من الأمور السهلة أيضا في جرائم إتلاف المعلومات، استبدال رقم بآخر أو إحلال رقم مكان آخر، وهو نوع من جرائم التزويد على درجة كبيرة من الخطورة لأنه في حاله نجاحه يستمر فترة طويلة من الزمن ويتولد عنه مكاسب كبيرة. [1]

[1]- د. محمد سامي الشوا، نفس المرجع، ص 31.

فهناك مجموعة من المستخدمين الإداريين استطاعوا خلال سنوات بسيطة مضاعفة رواتبهم عن طريق م المعلوماتي. وهناك البعض الآخر الذي تقاضى ساعات إضافية لم يتم تنفيذها على الإطلاق وذلك عن طريق استبدال قوائم الحسابات بساعات عمل.

وفي ألمانيا الشرقية قام مسكتب القوى العاملة مختص بتوزيع الإعانات العاملين بتحويل مبلغ 500.000 مارك لحسابه في شكل مرتبات بإزالة الرقم الأول للمبالغ المحولة من المنفذ الخاص بمراقبة النظام المعلوماتي.

وهناك ما يطلق عليه عمل ممارسة Bluff وتتمثل في استخدام النظام المعلوماتي من أجل طبع فواتير مصطنعة يقوم العملاء بتسديدها منخدعين في الثقة التامة التي يستلهموها من استخدام النظام المعلوماتي وإذا اعترضوا يتلقوا خطابا بصيغة تقليدية تقبلوا عذرنا " فقد أخطأ نظامنا.

وهناك أيضا قضية شهيرة في إسرائيل تتلخص وقاعها في قيام شخص يدعى "Vladimir Loriblitt وهو مهاجر روسي يعمل بوزارة المالية بإدخال فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي اصطنعها.

وفي الواقع أنه بإمكان أي شخص يشغل منصبا على قدر من الأهمية في مراكز المعلومات بالمنشآت والبنوك ولديهفي استخدام النظام المعلوماتي أن يحصل على كل ما يريده من معلومات ويوعها إلى مصلحته الخاصة.

- محو المعلومات بينا فيما سبق أن من خصائص الجرائم المعلوماتية هي قدرة المتهم على محو ما لجريمته من آثار خلال فترة وجيزة جدا لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو بالبرمج عن طريق الفارة. [1]

وهناك أمثلة كثيرة للجرائم التي ارتكبت وتم محو معالمها بعد ارتكابها مثل ذلك:

قيام شخصان باختلاس 21.000 دولار وهي عبارة عن مبالغ مرسله من شركات التأمين إلى إحدى المراكز الجامعية حيث قام المحللون بمحو كل الحسابات القائمة في

[1]– د. محمد سامي الشوا، نفس المرجع، ص 32.

سجلات النظام المعلوماتي الخاص بالمركز وجعلها غيرابلة للتحصيل. كما تم الكشف في مدينة دالاس الأمريكية عن أربعة من موظفي البلدية استبعوا (281) مخالفة من السجلات المدنية مقابل نسبة مئوية محددة بلغ مجموعها 16.300 دولار.

مما سبق يتضح أن "النظام المعلوماتي" بالرغم من أهميته كتقنية حديثة في عالم تكنولوجيا المعلومات إلى أنه مصدر خصب للجرائم التي تقع عليه والتي غالبا ما تكون من المسؤولين عن إدارة المراكز المعلوماتية في جميع المنشآت والبنوك المواقع المالية داخل الوزارات والحكومات.

ثانيا: الجرائم الواقعة باستخدام النظام المعلوماتي

أ. الجرائم الواقعة على الأشخاص الطبيعية

في هذا المطلب نبين الجرائم التي تقع على الأشخاص باستخدام النظام المعلوماتي واليت تعرض لها المشرع المصري في بعض التشريعات الخاصة اقترافها وستتناول هذا من خلال فرعين **الأول:** – الجرائم الواقعة على حقوق الملكية الفكرية والأدبية **والثاني:** – الجرائم الواقعة على حرمة الحياة الخاصة.

- **الجرائم الواقعة على حقوق الملكية الفكرية**

النظام المعلوماتي يمكن أن يكون وسيلة فعالة للاعتداء على حقوق الملكية الفكرية والأدبية أو ما يسمى بحقوق المؤلفين. وهنا يجب علينا عدم الخلط بين الاعتداء على حقوق الملكية الفكرية بصفة عامة وبين الاعتداء على الملكية الأدبية والفكرية التي تنصب على البرامج والمعلومات المسجلة التي تمثل النظام المعلوماتي ذلك أن الاعتداء هنا صب على العناصر غير المادية لهذا النظام. مثال ذلك استخدم النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برام معلوماتي آخر أو حالة تخزين هذه المعلومات على نظام معلوماتي معين ثم يقوم المسؤول عن التخزين باستخدام هذه المعلومات أو التفريط فيها بدون إذن صاحبها. [1]

[1]– د. محمد أبو العلا عقيده، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، القاهرة، ص 503.

- **الجرائم الواقعة على حرمة الحياة الخاصة**

النظام المعلوماتي يمكن أن يستخدم في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد، ويتحقق ذلك إذا قام شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه، أو أن يكون تجميع هذه المعلومات بعلم الشخص المعني ولكن قام المكلف بحفظها باطلاع الغير عليها بدون إذن صاحبها، ويقوم البعض حاليا بعمل معالجات معلوماتية لبعض المعلومات الشخصية والاحتفاظ بها لدى النظام المعلوماتي الخاص به باعتباره الخزينة التي يحتفظ فيها الشخص بأسراره المكتوبة من أبياته وسيرته الذاتية ومذكرات عن حياته الشخصية وأسرار يهمه الاحتفاظ بها باعتبار النظام المعلوماتي إحدى وسائل التقنية الحديثة لحفظ المعلومات إلا أنه يمكن أن تخترق هذه المعلومات مرتهزة أخرى ويتم الاطلاع عليها.

وللحياة الخاصة وما تحتويه حقوق حماية دستورية ونة في كافة دساتير الدول وقوانينها، وقد عنى الدستور المصري بذلك وحرص على حماية الحياة الخاصة للمواطنين وفنص عليه في المادة 45 الفقرة الأولى حيث قرر أن "لحياة المواطنين الخاصة حرمه يحميها القانون"

ونص في الفقرة الثانية على "المراسلات والبرقيات والمحادثات التليفونية وغيرها من وسائل الاتصال لها حرمه، وسيرتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محدودة وفقا لأحكام القانون، ونص الدستور أيضا علة حرمه المسكن في المادة 44" للمساكن حرمه فلا يجوز دخولها ولا تفتيشها إلا بأمر قضائي مسبب وفقا لأحكام القانون".[1]

[1]– د. محمد أبو العلا عقيده، نفس المرجع، ص 504.

وقد حرص المشرع المصري أيضا على حماية حرمه الحياة الخاصة بأن نص في قانون العقوبات بالمادة (309) مكرر، (309) مكرر (أ) حيث نص في المادة (309) مكرر على أن "يعاقب بالحبس مدة لا تقل عن سنة كل من اعتدى على حرمه الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه"

أ. استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون

ب. التقط أو نقل من الأجهزة أيا كان نوعه صورة شخص في مكان خاص فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضا هؤلاء يكون مفترضا.

ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عليه، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها

م 309 مكرر أ يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلا أو مستندا متحصلا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن، ويعاقب بالسجن مدة لا تزيد عن خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عبالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها. [1]

[1]– د. أحمد ملط، جرائم المعلوماتية، مرجع سابق، ص 186.

ب. الجرائم الواقعة على النظم المعلوماتية الأخرى

لا تستلزم هذه الجرائم تدخلا لإتلاف الوظائف الطبيعية للنظام المعلوماتي ولا تعديل على المعلومات التي تم معالجتها بل تقتصر في الغالب الأعم على الولوج المادي من جانب البعض في مركز المعالجة المعلوماتية أو استخدام أداة الكترونية مصنعة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى.

وقد تأخذ صور أخرى كإساءة استخدام البطاقات الائتمانية وسوف نبين ذلك في فرعين:

1. الولوج غير المشروع للمعلومات المعالجة آليا

يستلزم القيام بمثل هذا العمل الإجرامي وجود المجرم المعلوماتي داخل أحد المراكز المعلوماتية حيث أن كل ما يهمه**لغرض** هو الولوج إلى المعلومات التي تمت معالجتها بأي من الأنظمة المعلوماتية، والاطلاع غير المصرح به على تلك المعلومات المخزنة في ذاكرات النظم المعلوماتية ويأخذ هذا الولوج إحدى صورتين الأولى الولوج المباشر وية الولوج غير المباشر.

- **الولوج المباشر**

يستطيع الجاني الاستيلاء على المعلوماتخزنة لدى الأنظمة المعلوماتية بعدة طرق:

1-باستخدام آلة طباعة لاستخراج المعلومات المكتوبة على ورق.

2-باستخدام شاشة النظام والاطلاع بالقراءة على ما هو مكتوب عليها.

3-باستخدام مكبر صوت أو سماعات لالتقاط المعلومات والبيانات المعالجة.

ويعد هذا النوع من أكثر الأفعال التي ترتكب وأسهلها من حيث التنفيذ وهناك صور عديدة لمقل هذه الجرائم تتمثل في أنه حدث في لوس أنجلوس أن قام أحد المتخصصين بمعرفة شفرة إحدى الشركات المتخصصة في تصنيع أجهزة سلكية ولاسلكية والاتصال عن طريق هاتف تليفوني بمركز المعلومات لترسل له أجهزة مما تصنعه.[1]

[1]- د. أحمد ملط، جرائم المعلوماتية، مرجع سابق، ص 188.

وقد نجحت العملية نجاحا كبيرا لدرجة قيامه بعمل مشروع لبيع الأجهزة التي حصل عليها بطريق مشروع، وهناك حالة أخرى قام بها موظف سابق بأحد البنوك الفيدرالية الأمريكية كان يعمل في النظام المعلوماتي الخاص بالبنك حيث تمكن من الحصول على كلمة السر من زميل سابق له ونجح في التقاط المعلومات المالية المخزنة في النظام ونقلها لرئيسه لي العمل الآخر لكي يستفيد منها. ونجح طالب جامعي بالتقاط معلومات خاصة بطلبيه بضاعة باستخدام النظام المعلوماتي واستولى على معدات توازي قيمتها مليون دولار من إحدى الشركات بولاية كاليفورنيا وقد تمكن عن طريق وساطة شركة أنشئت خصيصا لهذا الغرض من بيع هذه المعدات المختلسة.

وقد يتحقق الولوج المباشر بدون التدخل في الكيان المنطقي أو في المعلومات مثل ذلك حالة العامل الذي شاهد بطاقة الدفع الخاصة به تمر من خلال آلة الطباعة فقام بوضع إصبعه على زر (كرر-Repeat) إلى ـن ضاعف مرتبه مائتين مرة.[1]

- **الولوج غير المباشر**

أدى ظهات مستحدثة لها صلة بالنظام المعلوماتي مثل شبكات الاتصال البعيدة وأيضا المعالجة عن بعد إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للولوج والاستفسار عن بعد من المراكز المعلوماتية إلا أن المعلومات أثناء حركتها وبثها تكون مهددة في كل لحظة بالالتقاط أو التسجيل غير المشروع.

ويأخذ هذا الولوج الأشكال الآتية:

1-توصيل خطوط تحويلية لالتقاط المعلومات المتواجدة ما بين النظام المعلوماتي والنهائية الطرفيال المعلومات المختلسة إلى النهاية الطرفية عن طريق إشارات الكترونية.

2-تسجيل ثم حل شفرة الإشعاعات الالكترومغناطيسية المنبثة بواسطة أجهزة الكترونية، لالتقاط الإشعاعات الصادرة عن النظام المعلوماتي، وهناك مثال ذلك

[1]- د. أحمد ملط، جرائم المعلوماتية، مرجع سابق، ص 189.

قيام شخص باختلاس أموال عن طريق التقاط أمر بتحويل مرسلمن بنك إلى آخر بعدها تمكن من تزييف الرسالة بأمر أدفع نفس المبلغ لحساب قام بفتحه باسمه.

3-الولوج غروع عن طريق نهاية طرفيه بعيدة، عن طريق نظام معلومـــاتي ومعرفة كلمة السر أو مفتاح الشفرة المناسب.

2. إساءة استخدام البطاقات الائتمانية

تعتبر الجرائم المتعلقة بإساءة استخدام البطاقات الائتمانية من الجرائم المعلوماتيـة الخطيرة خصوصا في المجتمعات التي تتسم نظمها البنكية بدرجة عاليـة ن التطـــور والحداثة وتمنح فيها البطاقات الائتمانية وتستخدم بأقل قدر ممكن من لإجراءات وتتعـــدد صور إساءة استخدام بطاقات الائتمان من خلال حالتين الأولى إســاءة اســتخدام العميـل للبطاقات الائتمانية والثانية إساءة استخدام الغير للبطاقات الائتمانية وسوف نوضح صـور استخدام كل منها وما يوجد لذلك من أمثلة: [1]

- **إساءة استخدام العميل للبطاقات الائتمانية**

تضع العقود المبرمة بين البنك والعميل المصدر إليه البطاقات الائتمانية شـروط معينـة تكون ملزمة للطرفين، ويتعين على العميل مراعاتها عند استخدام البطاقات الائتمانية، من حيث مدة الصلاحية وإلغاء البطاقة وسحبها إلا أن جـرائم إســاءة اســتخدام البطاقــات الائتمانية من قبل العميل.

تأخذ عدة صور أهمها:

1-إساءة استخدام بطاقة تنتهي مدة صلاحيتها، حيث أنه مــن المعلــوم أن للبطاقــة الائتمانية مدة محددة هي غالبا سنة بعدها يجب على العميل إعادتها للبنــك إلا أن العمل يستمر في استخدامها بعد فترة انتهاءها

2-إساءة استخدام بطاقة تم إلغاؤها، فقد يقوم البنر البطاقة بالغاها أثنـــاء مـــدة صلاحيتها ويتم إخطار العميل بذلك إلا أنه يستمر في استخدامها بدلا من إرجاعها

[1]– د. أحمد ملط، جرائم المعلوماتية، مرجع سابق، ص 189.

3-إساءة استخدام بطاقة أثناء مدة صلاحيتها يمكن أن يقوم العميل بإساءة استخدام بطاقة الائتمان أثناء مدة صلاحيتها بالشراء بأكثر من قيمتها من التجار ويتعرض التاجر لتحمل الزيادة أو يتحملها البنك.

4-إساءة استخدام بطاقة الائتمان في السحب لأوراق البنكنوت من أجهزة التوزيع الآلي مستغلا بعض الثغرات التي تعاني منها آلات السحب.

5-إساءة استخدام بطاقة الائتمان بعد الإبلاغ بصياغتها أو سرقتها فقد يقوم صاحب طاقة بإبلاغ البنك بضياع أو سرقة البطاقة الخاصة به ثم يقوم على الفور بسحب ما بها من أموال قبل أن يتم التحفظ عليها من البنك وتعتبر هذه الحالة من أكثر الحالات خطورة.

- **إساءة استخدام الغير للبطاقات الائتمانية**

يمكن للغير أن يرتكب جرائم إساءة استخدام البطاقات الائتمانية من خلال حالتين:

1-حالة سرقة البطاقة أو فقدها، وتعتبر سرقة البطاقات الائتمانية أو فقدها من أهم المشكلات القانونية التي تثير التعامل ببطاقات الائتمان حيث يقوم السارق باستخدام للحصول على السلع والخدمات من الغير أو يقوم بسحب مبالغ بموجبها من أجهزة التوزيع الآلي.

2-حالة السحب باستخدام بطاقة مزورة حيث ظهرت فكرة تزييف البطاقات الممغنطة كوسيلة يتحايل بها الجاني على أجهزة التفتيش الآلي للمواصلات حتى يمكن المرور منها بدون دفع أجره كما يستخدمها الجاني في أجهزة التوزيع الآلي للنقود.

وبالرغم مما يتم حاليا من خلال البنوك من عمليات لتلك البطاقات إلا أنها مازالت حتى الآن تشكل مصدرا من مصادر الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي الموضوع لدى البنوك. [1]

[1]- د. أحمد ملط، جرائم المعلوماتية، مرجع سابق، ص 191.

ج. الجرائم الواقعة على الأسرار

يقصد بالجرائم الواقعة على الحق في الأسرار تلك الجرائم التي تقع باستخدام النظام المعلوماتي في إفشاء الأسرار سواء ما كان منها متعلقا بأسرار عامة وهي التي تخص الدولة ونظام الدفاع عنها ومنها ما تكون أسرار خاصة وما يطلق عليها الأسرار المهنية.

فجريمة إفشاء الأسرار المعلوماتية قد تقع نتيجة لسرقة المعلومات ويكون القصد منها التش أو جماعة معينة، وقد يكون الدافع بيعها للحصول على عائد مادي لمن يهمه الأمر وقد تكون تحت تأثير الرشوة كما لو وقعت من العاملين بنظام المعالجة الآلية للبيانات (المعلوماتية)، وقد تكون تحت تهديد، وقد يستخدمها أصحباها أيضا للضغط على صاحبها من أجل القيام بعمل أو الامتناع عن عمل.

فلهذه الجريمة صور متعددة وقد تسبب لصحابها أضرارا مادية وأدبية كبيرة لذلك حرص المشرع المصري على حماية هذه الأسرار من خلال القوانين التي صدرت بشأنها

وف نتعرض لذلك من خلال فرعين الأول:-الجرائم الواقعة على أسرار الدولة، والثاني:-الجرائم الواقعة على الأعمال المهنية

3. الجرائم الواقعة على أسرار الدولة

المعلومة هي المعرفة، فالشيء يعرف بالحصول على معلوماته، والسر يعتبر معلومة أو خبر، والإفشاء هو نقل المعلومات أي هو نوع من نقل الأخبار، واطلاع الغير عليها بدون رضاء صاحبها التي يرغب في حفظها في حيز الكتمان وهي الرغبة التي يحترمهوهي علله تجريم إفشاء الأسرار،فهي صوره من صور الحماية الجنائية للإرادة. [1]

[1]- د. أحمد ملط، جرائم المعلوماتية، مرجع سابق، ص 191.

وقد يكون السر وصل إلى المؤتمن عليه عن طريق وظيفته أو طبيعة عمله، فقد أوجب عليه المشرع عدم إفشاء هذه الأسرار التي وصلت إليه بحكم وظيفته وبناءا على ذلك حمى المشرع الإرادة وجرم إفشاء هذه الأسرار، كتجريمه لإفشاء الأسرار المتعلقة بالحياة الخاصة ويعتبر استخدام النظام المعلوماتي في الجرائم الواقعة على أسرار الدولة، والتي تمثل كافة الأسرار سواء كانت اقتصادية أو مالية أو عسكرية أو سياسية، من أخطر أنواع الجرائم المعلوماتية في الوقت الحاضر، والنصوص الموجودة حاليا بقانون العقوبات المصري كالعقوبات المصري كتسول إليه نفسه ارتكاب مثل هذه الجرائم.

وقد تعرض لها المشرع المصري في قانون العقوبات في الكتاب الثاني الجنايات والجنح المضرة بالمصلحة العمومية وبيان عقوبتها من خلال الأول الجنايات والجنح المضرة بأمن الحكومة من جهة الخارج خاصة حينما يكون إفشاء هذه الأسرار متعلقا بأسرار الدفاع.

4. الجرائم الواقعة على الأسرار المهنية

بينا أن المعلوماتية وهي المعالجة الآلية للبيانات أي المعلومات التي توجد داخل النظام المعلوماتي يجب أن تكون سرية بطبيعتها وهو ما يفترض توافر الثقة فيمن توكل إليه، كما يجب أن يعلم الموظف المكلف بحمايتها أثناء مباشرته مهنته أو وظيفته قيمة هذه السرية، وقد ثار خلاف حول تحديد تلك المعلومة السرية، فذ البعض إلى أن السر هو ما خون العلم به إلا لصاحبه أو ما يؤتمن عليه بحكم الوظيفة أو المهنة لطبيعته السرية وما لا يخصص للإفشاء بعلم الغير به.

وذهب البعض الآخر إلى أن السر هو واقعة أو صفة ينحصر نطاق العلم بها في عدد محدد من الأشخاص إذا كانت تعد مصلحة يعترف بها القانون لشخص أو أكثر في أن يظل العلم بها محصورا في ذلك النطاق. [1]

[1]– د. أحمد ملط، جرائم المعلوماتية، مرجع سابق، ص 192.

ولا يكتفي لوصف إحدى الوقائع بالسرية أن تكون أبلغت صارحه للغير بل يكتفي أن تكون وصلت إلى علم الأمين عليها أثناء حماية مهنه أو وظيفته سواء من خلال ما أبلغ إليه صراحة أو ما فهمه أو سمعه من الوقائع بل تشمل السرية المعلومة ولو كانت مجهولة لصاحبها مثل المرض فيلتزم الطبيب بالمحافظة على الأسرار التي يقررها له المريض والتشخيص أو المرض الذي يكتشفه أثناء الفحوص الطبية عليه.

وكذلك يلتزم المحامي بحفظ أسرار موكله في الدعاوي المودعة لديه وقد تكون هذه المعلومات مشرفة أولا تخجل صاحبها ولبضا الإفشاء عنها فالمجني عليه يودع سره لدى من يعلم أنه مؤتمن عليه مفترضا الثقة فيه بسبب وظيفته أو مهنته التي تتطلب ذلك إذا كانت المعلومة لعدد كبير من الناس أو عامة انتة صفة السرية. فهذه المهنة لابد وأن تكون محلا للثقة العامة من قبل المجتمع في عمومة ولا يكفي أن تكون محلا للثقة الخاصة من قبل فرد من الأفراد. [1]

ويرجع السبب في ذلك إلى حماية إرادة المجني عليه في الاحتفاظ بسرية المعلومات الخاصة والتي يرغب في عدم إفشائها أو علم الغير بها كصورة من صور الحماية الجنائية للإرادة. وهناك أثناء على ذلك فقد سمح القانون بإعطاء وتبادل بعض المعلومات الشخصية إلى بعض الأجهزة الإدارية مثل "الضرائب أو الصحة أو النيابة أو القضاء أو الشرطة" يتبادل هذه المعلومات أو الاطلاع عليها دون وضع ضمانات وفي الأحوال المصرح بها قانونا.

[1]– د. أحمد ملط، جرائم المعلوماتية، مرجع سابق، ص 193.

المطلب الثاني: المجرم المعلوماتي

الفرع الأول: صفات المجرم المعلوماتي

أولا: المجرم المعلوماتي هو إنسان اجتماعي بطبعه

يختلف الإجرام المعلوماتي عن الإجرام التقليدي من حيث أن المجرم في هذا الشأن يحيا وسط المجتمع ويمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى. أي أنه إنسان اجتماعي. وتطبيقا لذلك فكثير من جرائم المعلوماتية ترتكب بدافع الكبرياء (مستخدم طردمن عمله فيلجأ إلى ارتكاب جريمته) أو بدافع النصب أو الحسد أو بدافع اللهو أو لإظهار مدى ما يتمتع به من قدرة على التفوق في مواجأمن الأنظمة المعلوماتية.

وبالتالي فإنه يكتفي بالتفاخر بين أقرانه أو لمجرد الحصول على منفعة مالية من وراء جرائمهم.

ثانيا: المجرم المعلوماتي هو إنسان محترف وذكي

ومرة أخرى يختلف الإجرام المعلوماتي عن الإجرام التقليدي الذي يميل عادة إلى العنف، ومع ذلك إذا كانت الجرائم المقصور وقوعها في بيئام المعلوماتي تتفق أحيانا مع الإجرام التقليدي من حيث تتطلب العنفبيل ارتكابها، إلا أن الإجرام المعلوماتي يتميز بأنه ينشأ من تقنيات التدمير الناعمة.[1]

وبمعنى آخر يكفى أن يقوم المجرم المعلوماتي بالتلاعب في بيانات وبرامج الحاسب الآلي لكي يمحو هذه عطل استخدام البرامج. وليس عليه سوى أن يلجأ إلى زرع الفيروسات في هذه البرامج أو باستخدام القنابل المنطقية أو الزمنية أو برامج الدورة لكي يشل حركة النظام المعلوماتي ويجعله غير قادر على القيام بوظائفه

[1]– د. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص 18.

الطبيعية. وقد يصل الأمر إلى حد احتراف الإجرام مما يشكل خطرا كبيرا على المجتمع سواء كان فردا أو جماعة منظمة أو غير ذلك.

الفرع الثاني: فئات المجرم المعلوماتي:

أولا: صغار نوابغ المعلوماتية:

يطلق لفظ صغار نوابغ المعلوماتية على المجموعات التي تميل للتحدي الفكري وهم غالبا ما يكونون في مرحلة المراهقة وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة البنكية والشركات والمؤسسات المالية .

ومن هؤلاء ام مراهق يبلغ من العمر أربعة شعر عاما باقتحام أنظمة جهاز الحاسب الآلي الخاصة بالقوات الجوية الأمريكية وحصل منها على معلومات عسكرية خطيرة مما أحدث ارتباكا خطيرا داخل تلك القاعدة، ترتب عليه اتخاذ قرارات تكلف تنفيذها الكثير من الوقت والجهد والمال.

ن أشهر الجرائم التي ارتكبت في الولايات المتحدة الأمريكية جريمة مراهق عمره سبعة عشر عاما يدعى" دينيس موران". وهذه القضية تحولت إلى قضية رأي عام لافها عن الجرائم الأخرى فيما كبدته من خسائر،وقد اختار "دينيس موران" لنفسه اسما حركيا هو "كوليو".[1]

وقد قام "كوليو" بشن سلسلة من الهجمات الالكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية شبكة الانترنت، ومنذ نهاية سنة 1999 وحتى بداية سنة 2000 استطاع "كوليو" أن يحول حياة المسؤولين ن هذه المواقع إلى الجحيم، حيث دأب على مهاجمة موقع (DARE ORG) المسؤول عن مواجهة مخاطر الإدمان، ونفذ عمليات تخريبية عليه.

[1]- د. أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، الدار الجامعية، ص 28.

ويتميز هؤلاء المراهقون عن غيرهم من مرتكبي أنم التقليدية- على الرغم من التشابه أحيانا في أساليب ارتكاب الجرائم وفي حجم الخسائر الناجمة عن هذه الأفعال- في أنهم لا يعتبرون أن ما يقومون به يعد جريمة لأنهم يعتقدون أن النظام غير القادر على حماية نفسه ليس من الخطأ اقتحامه، ولذلك فإنهم يعتبرون أنفسهم أبطالا لمساعدة المجتمع في تحديد نقاط الضعف الخاصة بالبرنامج الذي تم اقتحامه.

ويعمل صغار نوابغ المعلوماتية في مجموعات، ومنهم كذلك من يعمل بمفرده ولكن على الرغم من ذكائه أنهم ضعفاء في دراستهم أو قد لا يذهبون إلى المدرسة على الإطلاق،ويميلون إلى العزلة ويكون لديهم أصدقاء قليلون من خارج المجال،وقد يصور لهم خيالهم الخصب أنهم يحاربون من أجل الحقيقة أو العدالة أو الحرية أو ضد النظام متقمصين،خصية "روبين هود"

ويمكن لجماعات صغار نوابغ المعلوماتية أن تتحول إلى فئة القراصنة لأنه عندما يصبحون على درجة عالية وكبيرة من الخبرة والمهارة يتم استئجارهم واستغلالهم في أعمال ذات أهداف إجرامية.

ويتحول بذلك هؤلاء المراهقين إلى هدف الحصول على الربح المادي حيث تتركز أغلب جرائمهم في سرقات الاعتماد عن طريق شبكة الانترنت، وبالتالي ينخرطون في السلك الإجرامي وتقوم في حقهم المسؤولية الجنائية عن أفعالهم.

ثانيا: القراصنة

تغير معنى لفظ القرصنة مع ظهور شبكة الانترنت عما كان عليه في الماضي لأنه لم يعد معنى القرصنة سفك الدماء والقتل وعمليات التالتدمير باستخدام الأسلحة ولكن للفظ القرصنة مدلول آخر ارتبط بالتطور التكنولوجي. [1]

[1]- د. أيمن عبد الحفيظ، نفس المرجع، ص 28.

وأصبح في إمكان شخص لا يزيد وزنه على بضعة كيلو جرامات وتتوارى عضلاته خجلا من ضعفه أن يردع العالم بأسره وأن يستولى على الملايين من الأموال.

وفي سنة في مجال الحاسب الآلي وشبكة الانترنت يوجد مصطلحات مترادفان لها هما.

1-الهاكرز:

ويطلق لفظ الهاكرز على المقتحم التقليدي الذي يقوم بالتلصص على الغير ويتاجر في قطاع المعلومات وإذا ما واجهته حماية لا يستطيع تخطيها فهو ليس له علاقة بتكنولوجيا المعلومات.

2-الكراكر:

أما لفظ الكراكر فيطلق على الشخص المقتحم الخبير في مجال المعلومات واستخدام الحاسب الآلي ويعتمد عمله على كسر الحماية الموجودة حول الشبكات وأجهزة الحاسب الآلي ولذلك فإن الكراكر يستطيع اختراق الشبكات واقتحام البرامج.

ويستعين بالتالي الهاكرز بالكراكر إذا به أي نوع من أنواع الحماية، ولكن يلاحظ أنه جرت العادة على إطلاق لفظ الهاكرز على كلا النوعين الهاكرز والكراكر أو استخدام لفظ القراصنة عموما.

ويعتبر الهاكرز في أغلب الأحيان نسخة ذكية وعقلانية من المجرمين، وهم عادة ما يشعرون بأنهم مستبعدون من المجتمع.

وبفضل القراصنة العمل عادة في جماعات عن العمل الفردي وغالبا ما يكون دافعهم لارتكاب الجريمة إماعلى المال أو بغرض الشهرة، أو إثبات تفوقهم العلمي ومدى ما يتمتعون به من ذكاء. [1]

[1]- د. أيمن عبد الحفيظ، نفس المرجع، ص 29.

وقد تم في سنة 1995 إلقاء القبض على أعظم هاكرز في التاريخ وهو يدعى "كيفين ميتنيك"، حيث قام على مدار عشرين عاما بارتكاب عدد كبير من الجرائم الالكترونية حيث كان بإمكانه الدخول إلى أي نظام معلوماتي مرتبط بأجهزة الكمبيوتر وتعلم كيفية كسر كلمة المرور بسلاسة فائقة.

وأتيحت له بذلك فرصة التبحر في مجال المعلومات والبيانات ليستولى على كل ما يريد، وكذلك يدمر ما يشاء، بالإضافة إلى قدرته على زرع أي نوع من الفيروسات بدءا من الفيروسات الخفيفة التي لا يترتب عليها سوى إزعاج الكمبيوتر والمستخدمين وانتهاء بالفيروسات الشديدة التي قد تتسف قاعدة البيانات وتدمر شبكة الاتصالات.

ولم تسلم كذلك أجهزوتر الخاصة بالشخصيات البارزة من غزوات القراصنة. وتعتبر جريمة القرصان "جاي ساينزو" هي أحدث وأخطر الجرائم التي ارتكبها القراصنة في الفترة الأخيرة، حيث أظهر هذا القرصان مهارته في اقتحام موقع شركة(اون لاين) وهي أكبر شركة أمريكية متخصصة في توفير خدمات الانترنت والتي تخدم نحو ثلاثة وعشرون مليون مستخدم.

حيث قام من خلال عمله بالشركة ولفترة محدودة بجمع معلومات عن الشركة واستطاع باستغلك المعلومات –عقب فصله من الشركة– تدمير جزء كبير من قاعدة البيانات الخاصة بالشركة من خلال موقعها الالكتروني.

ثالثا: الهواة والمبتدئون

يعتبر نمط الهواة والمبتدئين من الأنماط التي تتميز بخطورتها في ارتكاب الجرائم على الرغم من سلامة القصد لديهم في عدم اري من الجرائم، وهذا مرجعه لأن عدم الدراية والخبرة في استخدام الحسابات الآلية يترتب عليه الوقع في الكثير من الأخطاء التي يترتب عليها حدوث تلك الجرائم. [1]

[1]– د. أيمن عبد الحفيظ، نفس المرجع، ص 30.

وتبرز خطورة هذا النمط في أن المخاطر التي تحدث نتيجة تصرفاتهم قد لا يمكن تداركها، فقد ينتج عن طريق قيام أحد الهواة والمبتدئين بالضغط على أحد الأزرار في لوحة المفاتيح فقد ملفات مهمة أو الإتلاف أي من المعلومات التي قد لا يمكن استرجاعها مرة أخرى.

ويمكن أن يترتب كذلك عن محاولة الهواة والمبتدئين القيام باي تصرف خاطئ مع أنظمة الحاسب الآلي حدوث جرائم في صورتها التامة والتي تتميز بالخطورة لأن من الجرائم ما يرتكب بمجرد حدوث الفعل بصرف النظر عن القصد الجنائي، وخير مثال ، جريمة الدخول غير المشروع في أنظمة الحاسب الآلي، حيث تعتبر هذه الجريمة تامة بمجرد الدخول إلى أنظمة الحاسب الآلي .

ويخشى أيضا من نمط الهواة التحول من م اللهو والعبث إلى القصد الجنائي لديه، بحيث يتحول من مجرد هاو أراد الاطلاع والدخول في عالم مجهول استهوته النتائج التي تحدث من مجرد الضغط على بعض أزرار الحاسب الآلي إلى مجرم له خطورته، فالهاوي الذي يقوم بتقليد عملة ورقية وتظهر الورقة في صورة أشبه بالعملة الحقيقية قد يتطور به الأمر إلى أن يصبح من محترفي جرائم تزييف العملة.

رابعا: المخربون

يرتكب أشخاص هذه الئم ليس طمعا في الإشادة العقلية أو إثبات التفوق العملي مثل صغر نوابغ المعلوماتية وإنما عادة ما يكون أشخاص هذه الفئة من الغاضبين في أغلب الأحوال من هيئة معينة وقد يكونون غاضبين من الحياة بوجه عام ويمكن تقسيم فئة المخربين إلى المستخدمين من داخل الهيئة أو من الغرباء عن الهيئة. [1]

[1]– د. أيمن عبد الحفيظ، نفس المرجع، ص 33.

1. **المستخدمون:**

تحدد طبيعة المستخدمين بأنهم الذين يكون لديهم تصريح لاستخدام أنظمة الحاسب الآلي ويقومون بإتيان تصرفات غير مصرح أو مسموح بها تنتج عنها أفعال تخريبية سواء لحقت هذه التصرفات بأجهزة الحاسب الآلي ذاتها أو بالبرامج التي تحتويها هذه الأجهزة.

وقد تتولد هذه الأفعال نتيجة الإهمال من هؤلاءلمستخدمين، ثمل: إلقاء القائمة التي تحتوي على المعلومات في صناديق المهملات مما يجعل أي شخص يمكنه الاستيلاء على هذه القائمة من معرفة طبيعة المعلومات داخل أجهزة الحاسب الآلي ومن ثم تفتح الطريق لارتكاب الجريمة .

نموذج تطبيقي:

قيام الموظف الذي يعرف كيف يصل لداخل أنظمة الحاسب الآلي بالتصفح في ملفات المرتبات عن طريق معرفة كلمة السر التي يمكن معرفتها بسهولة لكونه موظفا بذات الهيئة ويكون هذا الموظف قد تعرض من قبل لجزاء أو خصم من مرتبه ومن ثم يتولد لديه الرغبة في الانتقام .

ويكون رد فعله هو ارتكاب إحدى الجرائم من مهاجمة أصول الأموال الخاصة بالمنشأة وقيامه إما بمسح أي من الملفات أو زرع أي من الفيروسات داخل أنظمة الحاسب الآلي أو إحداث أي تعديل في البيانات مما يكلف الهيئة أموالا طائلة نتيجة فقدها هذه البيانات أو المات أو عند محاولة إصلاح تلك الأنظمة نتيجة هذه الأفعال التخريبية .

وقد يعمد هؤلاء المستخدمون إلى إدخال أحد البرامج التخريبية والتي لها صفة التدمير على أجهزة الحاسب الآلي ولا تعمل هذه البرامج إلا في حالة عدم وجود اسم هذا اة تأمينية يلجأ إليها الموظف لضمان عدم الاستغناء عنه أو التسبب في مشكلات فنية بالأجهزة حتى يتم الإبقاء عليه. [1]

[1]– د. أيمن عبد الحفيظ، نفس المرجع، ص 34.

وقد حدث سنة 1981 تدمير جميع الملفات بمخازن أحد مستودعات الجيش الأمريكي بكوريا الجنوبية بغرض إخفاء سرقة حدثت بهذا المستودع وتكلفت إعادة كتابة وتنظيم هذه الملفات مرة أخرى حوالي مائة مليون دولار.

وفي سنة 1983 في الولايات المتحدة الأمريكية حدثت أخطر أعمال التخريب شهرة وتتمثل في تعديل قاعدة بيانات خاصة بنظام حاسب كبير يخص إحدى كبريات شركات التأمين بقصد إنشاء أسماء وهمية يعاد التأمين عليها وقد اشترك مديرو هذا النظام في التخريب وقد تكلف إصلاحه حوالي ألف مليون دولار.

2. الغرباء:

ويندرج تحت هذه الفئة المستخدمون الذين ليس لديهم تصريح بالعمل على النظام وفي أغلب الأحوال يكون التخريب هو هدف هؤلاء الدخلاء أو الغرباء أي أنهم يقومون بالدخول على أنظمة الحاسب الآلي بغرض ارتكابالتخريب أو قيد يكون دخولهم بغرض التسلية وينتج عن هذه الأفعال نتائج تخريبية وقد يكون المكسب المادي هو هدف هؤلاء من عملية الدخول.

ولاشك أن عملية الدخول على أنظمة الحاسب الآلي من الغرباء يكون لها تأثير بالغ الضرر وأن الأفعال التخريبية الناتجة قد تكلف الهيئة ملايين لمحاولة إصلاح تلك الأنظمة التي أفسدتها العمليات التخريبية .

وتشهد الإحصائيات التي أجرها معهد (Stanford research) سنة 1999 على أن نسب مرتكبي هذه الجرائم من المستخدمين والغرباء تتراوح كما يلي:

أ. **المحللون:** وتقدر نسبتهم بحوالي 25 % من مرتكبي الجرائم من المستخدمين

ب. **المبرمجون:** وتقدر نسبتهم بحوالي 18% وهم الذين يكون لديهم أفكار معلوماتية تتجاوز مجرد الولوج إلى أنظمة الحاسب الآلي. [1]

ج. **الصرافون:** وتقدر نسبتهم بحوالي 16% من مرتكبي الجرائم.

[1]– د. أيمن عبد الحفيظ، نفس المرجع، ص 35.

د. **المشغلون:** وتقدر نسبتهم بحوالي 11% من مرتكبي الجرائم.

ه. **الأشخاص الغرباء:** وتقدر نسبتهم بحوالي 11% من مرتكبي الجرائم.

خامسا: المجرمون المحترفون

تعد فئة المجرمين المحترفين من أخطر الفئات التي ترتكب الجرائم لأن الهدف الذي تقوم عليه هذه الفئة ينحصر في نية ارتكاب الفعل الإجرامي وهذا هو مصدر الخطورة لأن المجرمين المحترفين يرتكبون أنواع الجرائم المختلفة وبأساليب مختلفة لأنهم يكونون على درجة كبيرة من المهارة والإتقان والغرض دائما هو المكسب أو الحصول على فائدة مادية أو معنوية.

ويلاحظ أن الأضرار التي تترتب على هذه الأفعال تكون بالغة الضرر هذا بعكس الفئات السابقة لأنه على الرغم من الخطورة الناجمة عن صغار نوابغ المعلوماتية إلا أن الغرض من ارتكاب جرائمهم على الرغم من كونها بالغة الأثر في أحيان كثيرة إلا أنها ليست دائما مؤثرة لأن أغلب الظن يكون قصدهم هو إثبات التفوق العلمي.

وينطبق ذات الأمر على فئة المخربين فهم ليسوا دائما مجرمين لأنهم يعمدون إلى نام من الهيئة نتيجة فصلهم أو يعمدون إلى تأمين المراكز الوظيفية الخاصة بهم في الهيئات أو الجهات التي يعملون بها لضمان استمرارهم في عملهم أي أن دافعهم لارتكاب الجريمة ليس دائما بغرض إجرامي ممال دائما مواجهة هذه الأفعال.

أما المجرمون المحترفون فهم– عادة –فئة شديدة الخطورة ومواجهتهم تتسم دائما بالصعوبة بن أخطر هؤلاء الفئات "فئة ذوي الياقات البيضاء"،حيث يقومون بارتكاب جرائم السرقة والنصب والاحتيال من على بعد باستخدام شبكات الحاسب الآلي في تحويل مبالغ مالية من أي من الجهات. [1]

[1]– د. أيمن عبد الحفيظ، نفس المرجع، ص 36.

وتعد أخطر جرائم هذه الفئات جريمة التجسس سواء في المجال الصناعي أو التجاري أو في المجال السياسي أو العسكري لأن المعلومات التي يحصلون عليها من أي من الجهات المختصة أو من الدول يكون لها بالغ الأثر بالإضرار بتلك الدولة حيث يترتب على نقل المعلومات عن عدد القوات العسكرية وحجم المعدات جعل الدولة في مركز أقوى لأنها سوف تستعد بما يتناسب مع تلك القوات والعتاد، وذات الحال عن المجال التنافسي في التجارة أو الصناعة.

وتوضح الدراسات التي أجرها معهد (Stanford research) على سبعمائة جريمة معلوماتية، ومن خلال الدعاوي التي تم تحريكها في هذا الشأن سواء في الولايات المتحدة الأمريكية أو في أوروبا أن مرتكبي هذه الأفعال هم من الجيل الحديث من الشباب الذين تتراوح أعمارهم بين خمسة وعشرين إلى خمسة وأربعين عاما.

ويلاحظ أن فئة صغار نوابغ المعلوماتية إذا لم يراع توجيهها التوجيه السليم يتولد لديهم الرغبة في تحقيق مكاسب مادية نتيجة التقدم التكنولوجي الذي يصلون إليه من خلال استخدام أجهزة الحاسب الآلي والسعي إلى التقدم العلمي واثبات تفوقهم في هذا المجال، ويأتي على رأس هؤلاء المم الجماعات المنظمة لأن أفراد هذه الجماعات يتلاعبون في تحويلات النقود باستخدام حيل ومخططات لتحقيق مكاسب مادية كبيرة.

وتعد أخطر فئات المجرمين على الإطلاق هي الجماعات الإرهابية التي أصبحت تستخدم أجهزة الكمبيوتر في الاحتفاظ بالمعلومات وفي تلقي الأوامر من الجهات الخارجية التي تقود تلك الجماعات من الخارج وبالتالي يحقق لهم الحاسب الآلي وسيلة مهمة للاختفاء بالولايات المتحدة الأمريكية في الحادي عشر من سبتمبر 2001م، فجانب الخسائر المالية الكبيرة نتيجة توقف أعمال كثيرة عن الاستمرار ولاسيما في الأسواق المالية الماسم البورصة يوجد على جانب آخر الكثير من الهيئات والمصالح على مستوى العالم قد تأثرت تأثرا بالغا في حجم الخسائر نتيجة تلك الهجمات الإرهابية [1].

[1]– د. أيمن عبد الحفيظ، نفس المرجع، ص 37.

وبدأت سائر المنظمات الإجرامية في ارتكاب الأنواع المختلفة من الجرائم باستخدام الحاسب الآلي لتحقيق ذات الأهداف السابقة ومن هؤلاء-بالطبع-مرتكبو جرائم المخدرات في عملية تبادل المعلومات وتحديد الأسعار، حيث لا تتم المقابلة إلا عند التسليم فقط.

ويضمن بالتالي هؤلاء المجرمون تحقيق أعلة معدلات التأمين ولاسيما إذا استخدموا جميعا أنظمة التشفير في عملية الاتصال حتى يظلوا دائما به عن أعين رجال الأمن.

الفرع الثالث: دوافع ارتكاب الجرائم المعلوماتية

كما سبق و أوضحنا فان مرتكبي أفعال الغش المعلوماتي تختلف قليلا عن مرتكبي الأفعال الإجرامية التقليدية ونجد نفس الاختلاف في الأسباب في العوامل التي تدفع إلى اقتراف الفعل الغير المشروع.

فدائما أمل الربح و روح الكسب هي الدافع لارتكاب الجريمة المعلوماتية، وغالبا مال تقسم شخصية المجرم المعلوماتي بالنشاط و المخاطرة و الذهن المتقد الذي يسعى إلى خداع الآلة وسنتناول فيما يلي الأسباب المحرضة التي ندفع إلى بعض مستخدمي الحاسبات الآلية إلى استغلالها على النحو الغير المشروع وهي:

1. الشغف بالكترونيات

مثال: عامل طلاء يدعى Ronald تمكن بفضل الآلة المسروقة التوصل إلى أسلوب طالعة وقام بالسطو على صانع الموزعات الآلية ولكن القي القبض عليه قبل أن يستفيد من نزعتمستخدمة و نسب إليه جريمة سرقة الآلة. [1]

[1]- د. سامي علي حامد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي الإسكندرية، 2007، ص 56.

ومن الملاحظ على وجه الدقة أن بعض مرتكبي أفعال الغش المعلوماتي ليسو على جانب كبير من الخطورة الإجرامية و كل ما يهمهم هو تحقيق انتصارات تقنية دون أن تكون نوايا آثمة و أن كان هو يمنع من أن تكون هناك بواعث أخرى آثمة وغير شريفة تحض على ارتكاب أفعال الغش المعلوماتي.

2. السعي إلى الربح

الرغبة في تحقيق الثراء الشخصي تذائما هي الدافع إلى الغش الأكثر انتشارا وقد تبين من خلال تحقيق أجرته إحدى المجلات المتخصصة بخصوص موضوع الأمن المعلوماتي أن الغالبية من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال وقد يكون ذلك نتيجة الخسائرضخمة لألعاب القمار أو من إدمان المخدرات فالأمل في تحقيق الربح هو السبب الرئيسي والأساس الذي يسالتعدي المعلوماتي والتي ليست لها في ذاتها قيمة معتبرة سوى تقوية و معالجة أنظمتها المعلوماتية.

3. الدافع الشخصية و المؤثرات الخارجية

طبيعة الإنسان كمخلوق ضعيف سيكولوجيا من الممكن في بعض المواقف أن يستسلم للمؤثرات الخارجية فمجرد إظهار جنون العظمة قد يكون هو الدافع لارتكاب فعل الغش المعلوماتي، فنرى المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام قد يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته التقنية لإدارة المنشاة إلى ارتكاب فعل الغش المعلوماتي وقد يعترف به.

وفي نطاق المنافسة والتجسس خاصة ومجالات الأعمال التجارية عامة نرى أعمال الغش المعلوماتي تمارس تحت تهديد آو ضغط من الغير فهذا ما يدفع بعض المنشات بل بعض الدول إلى الاتصال بالأفراد الذين يشغلون المراكز المرموقة كي يعملوا للحد المنشات المنافسة بهدف الاطلاع على بعض المعلومات الأساسية مثل الرشوة، الإغراء، الخداع عند اللزوم الإكراه أو التهديد وقد يفضلون زرع جواسيس خاصة بهم.[1]

[1]– د. سامي علي حامد، نفس المرجع، ص 57-58.

4. أسباب خاصة بالمنشاة

من أهم التهديدات العظمى التي تؤثر على الأنظمة المعلوماتية هو أن يعهد بكل مسؤولية المركز إلى شخص واحد بمفرده فنرى الثقة العمياء لمحللي ومبرمجي الحاسب الآلي إلى استخدام النظام إلى مصلحتهم الخاصة فإذا سمحت اختصاصات شخص بالولوج في مفتاحين إلكترونين من ثلاثة أساسية للتحكم في التحويلات الالكترونية للنقود من البنك إلى بنك آخر وقد تمكن بفضل قدراته إلى الوصول إلى المفتاح الثالث واستطاع أن ينتقل الحال 10 مليون دولار إلى حساب بنكي فتح باسمه في سويسرا ولكن يجب ألا نغض الطرف عن أن التسامح والتساهل الذي يهيمن ائما على إجراءات المراقبة وممارسة التفتيش بعد من العوامل التي تساعد على الغش المعلوماتي فيجب دائما المعرفة الجيدة والكاملة للمنتظر ويلاحظ أن هناك بعض حالات الغش غير المعلن عنها الجرائم المعلوماتية عندما يعملون فإنهم يفضلون عدم إفشاء سمعتهم التجارية ومكانتهم المرموقة.[1]

5. التحدي الذهني

إذ قد ترتكب هذف قهر النظام المعلوماتي، الذي يرى الجاني في تعقيد أجهزته وأنظمته الأمنية، وما أحيط حوله من هالة عن قدراته، موضوعاً يستفز مهاراته وإمكاناته ويثير رغبة التحدي لديه. [2]

6. دوافع أخرى:

الدوافع المذكورة أعلاه تعد أبرز دوافع ارتكاب الجريمة المعلوماتية، لكنها ليست كل الدوافع، فمحرك أنشطة الإرهاب الالكتروني وحروب المعلومات على سبيل المثال السياسية والإيديولوجية، في حين أن أنشطة الاستيلاء على الأسرار التجارية

---

[1]– د. سامي علي حامد، نفس المرجع، ص 58.

[2]– أمال قارة، الجريمة المعلوماتية، رسالة ماجستير مقدمة لكلية الحقوق الجزائر، 2002، ص 26.

تحركها دوافع المنافسة، والفعل الواحد قد يعكس دوافع متعددة خاصة إذا ما اشترك فيه أكثر من شخص انطلق كل منهم من دوافع خاصة به وتختلف عن غيره.

المطلب الثالث: الطبيعية القانونية للجريمة المعلوماتية

عند حديثنا عن الجرائم المعلوماتية يجب علينا أن نتحدث عن ذلك من خلال الحديث أكثر الصور الاختلاف كل منهتكييفها عن الأخرى و ذلك من خلال الفروع التالية:

الفرع الأول: جرائم الحاسب الآلي جرائم أموال

لعل هذه الصورة من أكثر صور جرائم المعلوماتية وقوعا ولعلها أيضا من أكثرها تأثيرا على الاقتصاد الوطني وعلى الأمن المالي للأفراد المتعاملين لوسائل المعلوماتية.

ويمكن لنا القول بأنها تنقسم إلى قسمين أو شكلين الأول منهما هي تلك الجرائم نواع الحاسب الآلي لمختلف أنواع الجرائم الممكن وقوعها من خلاله.

والشكل الثاني:هي تلك الجرائم التي تقع على الحاسب الآلي نفسه بمكوناته المادية والمعنوية وهذين ان بالمال بصورة أو أخرى وذلك حين تسلم بأن الجانب المعنوي للحاسب الآلي وما أشتمل عليه هو مال بالمعنى الفني والقانوني.

وفي هذه الحالة من الممكن أن تكون الكثير من جرائم الأموال التقليدية جرائم أموال معلوماتية أيضا، فقد تكون الجريمة المعلوماتية جريمة سرقة وقد تكون جريمة احتيال.

وقد تكون أيضا جريمة إساءة ائتمان (خيانة الأمانة). وقد تكون جريمة إتلاف مال المال الغير.إذا سلمنا بمالي المعلومات. [1]

---

[1] - www.lawjo.net/vb/showthred.php?29853 - الإجراءات-الجزائية-الخاصة-في-الجرائم-المعلوماتية

Date : 20/04/2016 Heur : 13:20.

الفرع الثاني: جرائم الحاسب الآلي جرائم أشخاص

من الممكن وقوع جرائم أشخاص من خلال النظام المعلوماتي ولكن هذا الشكل لا يجد الكثير من التطبيقات العلمية على أرض الواقع إذ ينحصر أثارها في مجموعة ضيقة من جرائم الأشخاص و ذلك في جرائم الذم والقدح والتحقير وجريمة إفشاء الأسرار سواء تجارية أو الشخصية وكذلك جرائم التهديد والتحريض وجرائم الاعتداء على الحياة الخاصة عبر الانترنيت.

الفرع الثالث: جرائم المعلوماتية جرائم أمن دولة وجرائم مخلة بالثقة العامة والآداب العامة

نظرا المعلوماتية للطبيعة الخاصة التي تتمتع بها جرائم أمن الدولة وإمكانية وقوع الكثير منها عن طريق الوسائل المحكية أو المقروءة فهي بذلك تعد جريمة ملائمة لتقع عبر الوسائل معلوماتية سواءا فيما يخص أمن الدولة اأو الخارجي. مثل جرائم جرائم الإتصال العدو وجرائم إثارة الفتن والحض عليها والجرائم الماسة بالوحدة الوطنية وتعكير صفو الأمة. أما الجرائم المخلة بالثقة العامة والآداب العامة فهي أيضا قابلة للوقوع عبر الوسائل المعلوماتية ومثل ذلك جرائم التزوير وتقليد الأختام وتزويراق البنكية والمصكوكات وإنتحال الشخصي. [1]

[1] - www.lawjo.net/vb/showthred.php?29853 - الإجراءات-الجزائية-الخاصة-في-الجرائم-المعلوماتية

Date : 20/04/2016 Heur : 13:20.