الجمهورية الجزائرية الديمقراطية الشعبية

جامعة محمد بوضياف - المسيلة -

كلية الحقوق والعلوم السياسية

قسم الحقوق

دروس في تقنيات الاعلام والاتصال

مقدمة لطلبة السنة أولى ماستر قانون أعمال

الدرس الثالث:

الأهداف التعليمية للدرس:

يستهدف الدرس من خلال هذه المادة التعليمية تحقيق الغايات التالية:

- احاطة الطالب بطبيعة الجرائم السيبرانية .
- أن يتعرف الطالب الفرق بين الجريمة السيبرانية والجريمة العادية.
- التفريق بين المصطلحات القريبة من مصطلح الجريمة السيبرانية.
- أن يتمكن من التعرف على أهم مراحل تطور الجريمة السيبرانية.

الطبيعة القانونية للجرائم السيبرانية:

مع تطور التقنية التي يسرت طرق التواصل وانتقال المعلومات بين مختلف العالم بقاراته الخمس، وسهلت حركة المعاملات بمختلف أنواعها خاصة منها الاقتصادية، سعى الأفراد وكذا

الدول لاستغلال هذه القفزة العلمية في سبيل تيسير اشباع الحاجيات وتوفير الخدمات في اقل وقت وتكلفة ممكنة.

وفي المقابل ومع تطور التكنلوجيا الرقمية تطورت معها أشكال وأنواع الجرائم السيبرانية كأكبر خطر يهدد المعاملات الرقمية، حيث تعاني المجتمعات في الآونة الأخيرة من خرق للمعاملات -الشخصية والتجارية- الرقمية وما ينجم عنها من انتهاك للحقوق والخصوصيات الإلكترونية للمتعاملين.

الجريمة السيبرانية والجريمة التقليدية:

تتكون الجريمة السيبرانية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة(crime)والإلكترونية (cyber) ويستخدم مصطلح الإلكترونية للدلالة على فكرة الحاسب أو التقنية في عصر المعلومات.

أما الجريمة التقليدية فهي السلوكيات والأفعال التي جرمها القانون، أي هي كل الأفعال التي ترتكب ضد الأفراد أو المجموعات بدافع الجريمة، ويقر لها القانون عقوبة، وتكون بقصد إيذاء الضحية أذى مادي او معنوي، أذى مباشر او غير مباشر.

تتشابه الجريمة الالكترونية مع الجريمة التقليدية في أطراف الجريمة: من مجرم ذي دافع لارتكاب الجريمة، وضحية والذي قد يكون شخص طبيعي أو شخص اعتباري، وأداة ومكان الجريمة، وهنا يكمن الاختلاف الحقيقي بين نوعي الجريمة ففي الجريمة الالكترونية الأداة ذات تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجانى إليه انتقالا فيزيائيا، ولكن في الكثير من تلك الجرائم فان الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجانى ومكان الجريمة.

ضبط مفهوم الجريمة السيبرانية:

إن جرائم الكمبيوتر والانترنت، أو ما يسمى Cyber Crimes هى ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التى يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل علي المستويات

الاقتصادية والاجتماعية والثقافية والأمنية.إذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، إلا أن هناك دولا عربية كثيرة أضحت مهتمة بتلك الظواهر، ومفهومها القانوني، وسمات المجرم المعلوماتي.

أولا: التعريف التقني الفنـــــي

الجريمة الالكترونية عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي.كما يعرفها البعض الآخر: بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها[1].

كما يعرفها البعض الآخر: على أنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" كما تعرف بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك تعرف بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا"[2]

فقد أنقسم أنصار تعريف الجريمة من الجانب التقني والفني فالبعض استند إلى موضوع الجريمة والبعض الآخر إلى وسيلة الجريمة.

وعموما يقصد بالجريمة الإلكترونية: هي الجريمة ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني مرتبط بأي شكل بالأجهزة الإلكترونية يتسبب في حصول المجرم على فوائد مع تحميل الضحية خسارة ودائماً يكون هدف هذه الجرائم هو سرقة وقرصنة المعلومات الموجودة في الأجهزة أو تهدف إلى ابتزاز الأشخاص بمعلوماتهم المخزنة على أجهزتهم المسروقة.

والجريمة الالكترونية عبارة عن نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي.

ثانيا: التعريف القانوني للجريمة السيبرانية

يعرفها أحمد صياني بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها وهذا التعريف يعتبر جامع مانع من الناحية الفنية للجريمة الالكترونية حيث انه لارتكاب الجريمة يتطلب وجود أجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة[3].

و لقد عرف الدكتور عبد الفتاح مراد جرائم الانترنت على أنها :" جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي و نظم المعلومات سواء لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط عير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الالكتروني كما تسمى كذلك في هذا الإطار بالجرائم السيبيرية أو السيبرانية لتعلقها بالعالم الافتراضي[4] .

و هي " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة الى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر" [5].

أما بالنسبة لبعض الفقه المصري ، فهي تنشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال أو الأشياء المعنوية وهناك فريق أخر يرى أن الجريمة المعلوماتية هي " عمل أو امتناع يأتيه إضرارا بمكونات الحاسب ،وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا ". كما عرفها آخرون بأنها " كل فعل إيجابي أو سلبي عمدي يهدف إلى الإعتداء على تقنية المعلوماتية أية كان غرض الجاني".[6]

أما المشرع الجزائري لم يعرف الجريمة الإلكترونية وإنما تبنى للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة[7] ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة إستنادا إلى قانون العقوبات الجزائري المعدل والمتمم لم يعرف جرائم الانترنت، بل اكتفى بالعقاب على بعض الأفعال ، تحت عنوان " الجرائـم الماسة بنظـام المعالجـة الآلية للمعطيات"[8] .

الفرع الثاني: أهم المصطلحات الرديفة للجريمة السيبرانية

للجريمة الإلكترونية لها مسميات عدة منها[9]:

-1 -جرائم الحاسوب والإنترنت

-2-جرائم التقنية العالية

-3-الجريمة الإلكترونية

-4-الجريمة التكنولوجيا الحديثة

-5-جرائم أصحاب الياقات البيضاء

ومثل تلك الجرائم قد تهدد أمن الدولة وسلامتها المالية والقضايا المحيطة بهذا النوع من الجرائم كثيرة وأبرز أمثلتها الاختراق أو القرصنة وانتهاك حقوق التأليف ونشر الصور الإباحية للأطفال ومحاولات استمالتهم لاستغلالهم جنسيا والتجارة غير القانونية (كتجارة المخدرات) كما تضم انتهاك خصوصية الآخرين عندما يتم استخدام معلومات سرية بشكل غير قانوني.

ولا تقتصر الجرائم الإلكترونية على أفراد أو مجموعات وإنما قد تمتد إلى مستوى الدول لتشمل التجسس الإلكتروني (وأبرز أمثلته ما كشفته تسريبات المتعاقد السابق مع وكالة الأمن الوطني الأميركي إدوارد سنودن، الذي كشف مخططات أميركية عديدة للتجسس ليس على الأفراد فحسب بل على اتصالات دول أخرى، والسرقة المالية وغيرها من الجرائم العابرة للحدود.

وأحيانا توصف الأنشطة التي تتعلق بالدول وتُستهدف فيها دولة أخرى واحدة على الأقل بأنها تقع في إطار "الحرب الإلكترونية"، والنظام القانوني الدولي يحاول تحميل الفاعلين المسؤولية عن أفعالهم في مثل هذا النوع من الجرائم من خلال المحكمة الجنائية الدولية[10].

المطلب الثاني: تطور الجريمة السيبرانية

بتنامي معدلات الجريمة وتطور أشكالها و تهديدها المباشر فقد دق ناقوس مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن هذه الجرائم التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة.

فهي جريمة تقنية تنشأ في الخفاء و توجه للنيل من الحق في المعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت ، وتظهر مدى خطورتها في الإعتداءت التي تمس الحياة الخاصة للأفراد وتهدد الأمن والسيادة الوطنيين وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري.

الفرع الأول: مراحل تطور الجريمة السيبرانية

مر تطور الجرائم السيبرانية بثلاثة مراحل تبعا لتطور التقنية واستخدامات الحاسوب[11].

1 -المرحلة الأولى: بظهور استخدام الكمبيوتر و ربطه بالشبكة في الستينات إلى السبعينيات ،ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة و تدمير أنظمة الكمبيوتر و التجسس ألمعلوماتي ،و شكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة جرمية مستجدة ؟و هل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟ ، فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني و مع توسع الدراسات تدريجيا و خلال السبعينات بدأ الحديث عنها كظاهرة إجرامية جديدة.

2 – المرحلة الثانية: في بداية الثمانينات، تأكد مفهوم جديد لجرائم الكمبيوتر والانترنت حيث ارتبطت هذه الأخيرة بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر و زرع الفيروسات الالكترونية التي تقوم بعملية تدمير كلي للملفات أو البرامج،و شاع إصطلاح "الهاكرز " المعبر عن مقتحمي النظم وكذا المجرم المعلوماتي المتفوق.

3- المرحلة الثالثة : حيث شهدت فترة التسعينات تناميا هائلا في حقل الجرائم الالكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيلات لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة وخطيرة في ذات الوقت[12].

بحيث نمت الإنترنت بشكل مذهل خلال هذه الفترة ، بعد ما كانت مجرد شبكة أكاديمية صغيرة وتحولت الى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات ، وفي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كان الاهتمام ببناء الشبكة وتوسيع نشاطها ، دون مراعاة تحديات أمن المعلومات ، فالاهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة، وهذه الثغرة التي شجعت تنامي الجريمة الإلكترونية و تسببت في أضرار بالغة ، وهو ما أدى الى لفت النظر الى حاجة شبكة الإنترنت الى توفير

معايير من الأمن ، وبدأ التفكير مليا في الثغرات ونقاط الضعف، وعليه قد يكون الكمبيوتر هدفا للجريمة، وغايته المعلومات المخزنة و السيطرة على النظام دون التصريح و السرقة و الاعتداء على الملكية الفكرية ....الخ.

كما قد يكون الكمبيوتر محل للجريمة ، كحالة استغلال الكمبيوتر للاستلاء على أموال الغير بإجراء تحويلات غير شرعية كما أن الكمبيوتر قد يعد أداة للجريمة، كحالة تخزين البرامج المنسوخة أو في حالة استخدامه لنشر المواد غير قانونية.[13]