

جرائم تكنولوجيا المعلومات وآليات الحد منها

م . جعفر حسن جاسم الطائي jaffarjassem@yahoo.com

جامعة ديالى / الامانة العامة للمكتبة المركزية

تاريخ استلام البحث : ٢٠١٥/١٠/١٩ تاريخ قبول النشر : ٢٠١٥/١١/٤

الكلمة المفتاحية : تكنولوجيا المعلومات
Keyword : Information Technology

المستخلص :

يهدف البحث إلى التعريف بجرائم تكنولوجيا المعلومات و أنواعها و سمات و خصائص مرتكبي هذا النوع من الجرائم و الأسباب و الدوافع وراء انتشارها و قد استخدم الباحث في إعداد هذا البحث المهج الوصفي لملائمته طبيعة هذا البحث و قد توصل الباحث إلى جملة من النتائج من أهمها ضرورة العمل على إصدار قوانين جديدة تحد من انتشار هذه الظاهرة و ضرورة الاهتمام بالتربية الأسرية و المدرسية لغرض بناء جيل قادر على الاستعمال الايجابي لتكنولوجيا المعلومات.

Information technology crimes and the mechanism of its reduction.

Jaffar Hassen Jassem / central library

Abstract :

The study aims at defining the crimes of the information technology, their kinds and the features and characteristics of those who commit such crimes and the reasons and motives behind the spreaded crimes. The Researcher has used in the preparation of this research the descriptive method as it suits the purpose of the research. The researcher reached a number of recommendations to reduce the spread of such phenomenonsuch as: the necessity to work on issuing new IT laws to limitand the necessity to take good care of family and schools education to build new generation who is able to use information technology positively.

أولاً : إشكالية البحث :

لقد بات مؤكداً أن أحداً لا يستطيع أن يتجاهل التغييرات الجوهرية التي أحدثتها ثورة تكنولوجيا المعلومات في المجالات الاقتصادية والسياسية والاجتماعية ، الإيجابية منها والسلبية على حدٍ سواء ، وعليه فإن نظرة الناس نحو تكنولوجيا المعلومات أضحت مختلفة ، ففي الوقت الذي تبعت فيه على الإعجاب في نفوس العديدين من المستفيدين عند الاستفادة منها في علاج عدة مشكلات ، إلا أنها تبدو مروعة لاسيما عندما يتعلق الأمر بتهديد أمن وحياة المجتمعات الإنسانية ، ومن هنا تبدأ ملامح إشكالية البحث بالظهور .

فضلا عن ذلك ، فإن المجتمعات الإنسانية ولاسيما المتأخرة تكنولوجياً وبالذات في مجال تكنولوجيا المعلومات منها اعتادت ولا تزال معتادة على الجريمة التقليدية المتعارف عليها وهي بالتالي لم تقطن بعد للجرائم الحديثة أو المستحدثة وخاصة جرائم المعلوماتية والتي باتت تهدد حقوق المواطنين ولاسيما أولئك الذين لم تكن لديهم دراية ومعرفة بخفايا وشؤون تكنولوجيا المعلومات وتحديد الجانب السلبي أو المظلم منها ، وهذا هو الجزء المهم الآخر من إشكالية البحث .

إضافة إلى ذلك ، فإن تكنولوجيا المعلومات أصبحت أداة للربط والاتصال والتخزين والاسترجاع بين الناس في مختلف أرجاء الأرض ، وباتت تشكل أداة ليس للبحث عن المعلومة فحسب ، بل وتوظيف هذه المعلومة لأغراض الجريمة ، ولاسيما الجرائم المعلوماتية منها تحديداً؛ وذلك من حيث إساءة استعمال تكنولوجيا المعلومات ، والعمل على توظيفها سلبياً وبشكل غير قانوني ، لإشباع رغبات النفس الإنسانية المختلفة ، وكل تلك الرغبات الإنسانية غير المشروعة ولدت جرائم جديدة لم تكن مألوفة لدى المجتمع يمكن أن نطلق عليها جرائم تكنولوجيا المعلومات ، وهذا هو الجزء المهم من إشكالية البحث .

وزيادة على ذلك ، هو غياب وقصور القوانين المواكبة للتطورات التكنولوجية مما يساعد على انتشار جرائم تكنولوجيا المعلومات في العديد من دول العالم ولاسيما الدول النامية ومنها الوطن العربي ، إذ إن المشرع العربي لم يشرع قانوناً أو قوانيناً تواكب متغيرات العصر الرقمي مما يتيح لذوي النفوس الشريرة والضعيفة سواء من الداخل أو الخارج أن يرتكبوا جرائم عبر وسائل هذا العصر دون وجود رادع لهم ، وهذا الجزء المهم الآخر من إشكالية البحث .

علاوة على ما تقدم ، فإن إشكالية البحث تتمثل في الإجابة عن التساؤلات الآتية :

١- ما المقصود بجرائم تكنولوجيا المعلومات ؟ وهل باتت تمثل ظاهرة ؟ وما التسميات التي تطلق عليها ؟

٢- ما سمات وخصائص جرائم تكنولوجيا المعلومات ؟

- ٣- ما أسباب انتشار جرائم تكنولوجيا المعلومات ؟ وما مواصفات الذي يرتكبها؟
- ٤- ما الدوافع وراء ارتكاب جرائم تكنولوجيا المعلومات ؟ وما أنواع جرائم تكنولوجيا المعلومات ؟
- ٥- ما السبل اللازمة لمكافحة جرائم تكنولوجيا المعلومات؟ وما الصعوبات التي تقف عائقاً وراء مكافحتها بالطرق القانونية ؟

ثانياً: أهداف البحث :

يروم البحث إلى تحقيق الأهداف الآتية :

- ١- التعريف بماهية جرائم تكنولوجيا المعلومات وإظهار التسميات المرتبطة بها .
- ٢- كشف النقاب عن السمات والخصائص المتعلقة بجرائم تكنولوجيا المعلومات .
- ٣- إمطة اللثام عن الأسباب والدوافع وراء انتشار جرائم تكنولوجيا المعلومات .
- ٤- تسليط الضوء على أنواع جرائم تكنولوجيا المعلومات وكيفية مكافحتها .

ثالثاً : أهمية البحث :

تكمن أهمية البحث في أهمية الموضوع ذاته بوصفه يسلط الضوء على أهم الجرائم المستحدثة والمعاصرة ، ولاسيما تلك التي ترتبط بظاهرة تكنولوجيا المعلومات والتعريف بها لكونها نوعاً جديداً من الجرائم لم تألفها المجتمعات من قبل وخاصة العربية منها. فضلاً عن ذلك ، فإن أهمية البحث تتجلى بكشف النقاب عن أهم أنواع جرائم تكنولوجيا المعلومات والأسباب والدوافع وراء انتشارها وارتكابها ،ومن ثم تعريف الجهات الأمنية والقانونية ومن خلفهم المجتمعات الإنسانية بهذا النوع من الجرائم ، وكذلك تنبع الأهمية من خلال وضع الآليات والتصورات اللازمة في كيفية معالجة هذه الجرائم والصعوبات التي تحول دون معالجتها بشكل قانوني .

رابعاً : مفهوم جرائم تكنولوجيا والتسميات ذات العلاقة :

قبل تسليط الضوء على مفهوم جرائم تكنولوجيا المعلومات لابد من توضيح بعض المفاهيم ذات الارتباط بها ، منها :

- ١- **الجريمة في اللغة** : الجريمة هي الفعل الذي يستوجب عقاباً ، ويوجب ملاماً . أصل كلمة جريمة من جرم بمعنى كسب وقطع ، والجرم هو الذنب . وهي الكسب المكروه غير المستحسن وجرم يراد منها الحمل على فعل حمل أثماً (ابن منظور . لسان العرب).

٢- **الجريمة اصطلاحاً** : هي سلوك ينتهك القواعد الأخلاقية التي وضعت لها الجماعة جزاءات سلبية تحمل صفة الرسمية أو هي السلوك الذي تحرمه الدولة لما يترتب عليه من ضرر على المجتمع ، والذي تتدخل لمنعه بعقاب مرتكبيه (محمد - ١٩٩٤ . ص ٣٩)

٣- **تكنولوجيا المعلومات** : تعني تلك الأجهزة والمعدات والأدوات والأساليب والوسائل التي استعمالها الإنسان ويمكن أن يستعملها مستقبلاً في الحصول على المعلومات الصوتية والمصورة والرقمية ، وكذلك معالجة تلك المعلومات من حيث تسجيلها وترتيبها و تخزينها وحيازتها واسترجاعها وعرضها واستنساخها و بثها وتوصيلها في الوقت المناسب لطالبيها ، وتشمل كلاً من تكنولوجيا التخزين والاسترجاع وتكنولوجيا الاتصالات . (جعفر - ٢٠٠٨ ص ٢٩٠)

٤- **جرائم تكنولوجيا المعلومات** : لا بد من القول أن هناك العديد من التعريفات الصادرة من وجهات نظر قانونية واجتماعية ونفسية وفلسفية أحياناً ، وعليه يمكن أن نضع لها تعريفاً شاملاً يتمثل في أن جرائم تكنولوجيا المعلومات هي (كل فعل وعمل وكل سلوك غير مشروع أو غير أخلاقي أو غير مسموح به صادر عن إرادة جنائية يقوم به شخص ما له دراية ومعرفة بتكنولوجيا المعلومات المختلفة ويوجه ضد المصلحة العامة والخاصة ، وتشتمل تلك الجرائم من الناحية المبدئية جميع الجرائم التي يمكن أن ترتكب فيه أو عبر وسط إلكتروني ، ويقرر لها القانون عقوبة أو تدبيراً) (جعفر - ٢٠٠٧ ص ١١٠)

أما بخصوص التسميات المتعددة والمرتبطة بظاهرة جرائم تكنولوجيا المعلومات ، فيمكن القول : إنه ومما لا شك فيه أن ثمة تباين أو عدم ثبات حول التسميات التي أطلقت ولا زالت تطلق على هذه الظاهرة الإجرامية الجديدة التي باتت تهدد الدول قبل الأفراد ، وربما مرد هذا التباين يعود إلى نشأة وتاريخ وتطور تكنولوجيا المعلومات من جهة ، ومن ثم يعود إلى تطور وتمحور ظاهرة جرائم تكنولوجيا المعلومات من جهة أخرى ، واختلاف النظر بشأنها بين المختصين في مجال الإعلام وبين رجال القانون وعلماء الاجتماع وعلم النفس من جهة ثالثة .

لقد تعددت التسميات بشأن هذه الظاهرة الإجرامية ، فمرة تسمى جرائم الكمبيوتر والإنترنت ، ومرة ثانية جرائم التقنية العالية ، ومرة ثالثة الجريمة الإلكترونية ، ومرة رابعة الاحتيال المعلوماتي ، ومرة خامسة احتيال الحاسوب ، ومرة سادسة غش الحاسوب ، ومرة سابعة نصب الحاسوب ، ومرة ثامنة الغش المعلوماتي أو الجريمة المعلوماتية ، ومرة تاسعة جرائم الهاكرز ، والمرة العاشرة الاختراقات التقنية ، وما قبل الأخير السيبركرايم (cyber crime).

أمام هذا الواقع المتشظي من حيث تعدد التسميات المطلقة على هذه الظاهرة الإجرامية الجديدة على المجتمع الإنساني، لاسيما وأنها حدثت وسوف

تحدث في مجتمع المعلومات العالمي، أي الذي يستعمل تكنولوجيا المعلومات في معظم قطاعات الحياة فيه، لذلك تطلب ويتطلب الأمر وضع عنوان جامع شامل تنضوي تحته كل التسميات السابقة الذكر، وربما حتى التسميات اللاحقة إذا كانت تسميات جزئية . فنحن بدورنا أطلقنا عليها تسمية جديدة نكاد لم نلمسها في الأدبيات التي تناولت هذا الموضوع، تمثلت هذه التسمية ب(جرائم تكنولوجيا المعلومات) (جعفر - ٢٠٠٧ ص ١٠٨)

تعد جرائم تكنولوجيا المعلومات ظاهرة إجرامية مستجدة نسبياً تفرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن إلى حجم المخاطر وهول الخسائر الناجمة عنها بوصفها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة (بيانات ومعلومات والبرامج بكافة أنواعها) .

خامساً : سمات وخصائص جرائم تكنولوجيا المعلومات :

مثلما للجرائم العادية خصائص وصفات تتسم بها ، كذلك فإن الأمر ينطبق على جرائم تكنولوجيا المعلومات ، وتعد الجرائم التي ترتكب من خلال الحاسوب وشبكة الإنترنت هي جرائم ذات خصائص منفردة خاصة بها لا تتوافر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها ، وتلك الخصائص يمكن أن نذكرها بالشكل الآتي :

١- **الحاسب الآلي هو أداة ارتكاب الجريمة :** خاصية الحاسب الآلي هو دائماً أداة للجريمة في الجرائم التي ترتكب على شبكة الإنترنت وهي خاصية متفردة عن أي جريمة أخرى ؛ ذلك أن الحاسب الآلي هو الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الإنترنت (internet) وقيامه بتنفيذ جريمته أياً كان نوعها ، وعليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب على شبكة الإنترنت .

٢- **الجرائم ترتكب عبر شبكة الإنترنت :** تعد شبكة الإنترنت (internet) هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم ، كالبنوك والشركات الصناعية وغيرها من الأهداف التي غالباً ما تكون ضحية لتلك الجرائم .

٣- **مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي :** لاستعمال الحاسب الآلي من أجل ارتكاب أو تنفيذ جريمة ما على شبكة الإنترنت لا بد وأن يكون مستعمل هذا الحاسب الآلي على دراية ومعرفة فائقة ، وذو خبرة كبيرة في مجال استعماله ، ولذلك نجد أن معظم ممن يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب وأن الشرطة تبحث أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب الجرائم .

٤- **الجريمة لا حدود جغرافية لها :** شبكة الإنترنت ألغت أي حدود جغرافية فيما بين الدول وبعضها ، إذ يمكن التحدث فيما بين أشخاص ليس في بلدان مختلفة وإنما في قارات مختلفة في نفس الوقت على شبكة الإنترنت من الدردشة (shating)، وعليه فإنه أي جرائم ترتكب عبر شبكة الإنترنت فإنها

تتخطى حدود الدولة التي ارتكب فيها لتتعدى آثارها كافة البلدان على مستوى العالم. (منير - ٢٠٠٤ ص ١٤ - ١٥)

٥- جرائم الكمبيوتر والإنترنت : طائفة من الجرائم التي تتسم بسمات مخصوصة عن غيرها من الجرائم ، فهي تستهدف معنويات وليست ماديات محسوسة ، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي إن جاز التعبير.

٦- كما أنها تتسم بالخطورة البالغة نظراً لأغراضها المتعددة : ونظراً لحجم الخسائر الناجمة عنها قياساً بالجرائم التقليدية ، لارتكابها من بين عدة فئات تجعل من التنبؤ بالمشتببه بهم أمراً صعباً .

٧- صعوبة التحقيق والتحري في جرائم الكمبيوتر والإنترنت والمقاضاة في نطاقها : تنطوي على مشكلات وتحديات إدارية وقانونية تتصل ابتداءً بمعوقات ومتطلبات عمليات ملاحقة الجناة ، فإن تحققت مكنة الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم . ونظراً لأنها جرائم لا تحدها حدود وتعد من الجرائم العابرة للحدود ، فتثير لذلك تحديات ومعوقات في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش .

إن جرائم الكمبيوتر قد ترتكب عن طريق حاسب آلي في دولة ما، في حين يتحقق الفعل الإجرامي في دولة أخرى ، فجرائم الكمبيوتر والإنترنت ، لا تحدها حدود ولا تعترف ابتداءً في هذه المرحلة من تطورها بسبب شبكات المعلومات - بعنصر المكان أو حدود الجغرافيا ، وتتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ، ومن الوجهة التقنية ، بين الحاسوب أداة الجريمة ، وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدفة بالاعتداء ، و هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة ، لكنه وبفعل سيادة تقنيات شبكات النظم والمعلومات ، امتد خارج هذه الحدود - دون تغيير في الاحتياجات التقنية - ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محل الاعتداء .

الحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر المسائل التي تثير إشكالات في مجال جرائم الحاسوب وبشكل خاص الإجراءات والاختصاص والقانون الواجب والتطبيق . وهذا بدوره عامل رئيس في نماء دعوات تضافر الجهود الدولية لمكافحة هذه الجرائم . (الشبكة القانونية العربية - ٢٠٠٤) التي باتت واحدة من أهم سمات العصر ، بل واحدة من أهم ظواهره .

سادساً : أسباب انتشار جرائم تكنولوجيا المعلومات :

يمكن القول : إن تزايد عدد أنواع أجهزة تكنولوجيا المعلومات جعل من الجرائم المرتبطة بها هي الأخرى في تزايد ، بل وفي تنوع طرق ارتكابها ، ويقف وراء ذلك التنوع عدد من الأسباب .

إن من أهم أسباب انتشار جرائم تكنولوجيا المعلومات صعوبة اكتشاف هذه الجريمة ومقاضاة المتهم ؛ لأنه لا يوجد في أغلب الأحوال شاهد للقضية ولا دلائل يمكن استعمالها للتوصل إلى الجاني . وقد يستهان في هذه الجرائم أو يركن إلى السكوت عنها ، إذ إن كثيراً من المنشآت التي تخترق نظم معلوماتها لا تلاحق مرتكبي هذه الجرائم قضائياً مفضلة استقالتهم من أعمالهم – إن كانوا من داخل المنشأة – دون إثارة ضجة لئلا تشوه سمعة المنشأة . ويحاول العديد من مديري نظم المعلومات الإدارية التكتم على ما يحدث من جرائم ذات علاقة بالحاسب الآلي وعدم رفعها إلى المستويات الإدارية العليا في المنشأة ، وتحاول المستويات العليا أيضاً أن تخفيها عن مجلس الإدارة ، كما أن مجالس الإدارة يتجاهلون إذا وصلت إليهم ولا يوصلوها إلى المساهمين ، مما أدى إلى إفلات العديد من القراصنة من العدالة وتشجيعهم على ارتكاب جرائم أخرى .

مما يزيد الأمر صعوبة التطور التقني السريع الذي يساعد القراصنة على كسر الحواجز واختراق النظم باستعمال تقنيات وبرامج أكثر تطوراً لم تؤخذ في الحسبان عند وضع إجراءات الحماية .

لقد سهل انتشار شبكة الإنترنت في الآونة الأخيرة على مستوى عالمي اختراق نظم المعلومات المرتبطة بالشبكة من قبل قراصنة المعلومات الذين يقعون في أماكن بعيدة لم تكن تشكل خطراً في السابق لانعدام الوسيلة . ولاحظ " سكوت سارني " المسؤول عن مكافحة الجريمة على الإنترنت في وزارة العدل الأمريكية أن الكمبيوتر الموصول بشبكة الإنترنت أصبح سلاحاً لاقتراف هذه الجرائم في عالم بلا حدود ، وأضاف أن شبكة الإنترنت تسهل الجريمة أيضاً على غرار دعاة الأطفال . واعترف "دو غلاس بيرت" أحد المسؤولين في مركز الحماية من جرائم الحاسب الآلي التابع للشرطة الفدرالية الأمريكية بأنه لا يمكننا أن نتوقع كل شيء لأن تحديد الخطر أمر بالغ الصعوبة .

فضلاً عن ذلك ، أن غياب الأنظمة والقوانين الرادعة نظراً لحدوث هذه الجرائم على المجتمع أدت إلى انتشارها واستفحال خطرهما مما ينجم عن عدم إلحاق العقوبات المناسبة بمن يقبض عليه من القراصنة ، ويمكن أن يضاف على هذه الأسباب أيضاً ضعف الوعي بهذه الجرائم وأساليب ارتكابها وكيفية الحماية من أخطارها (صالح – ٢٠٠٠ ص ١٧٥ - ١٧٦) .

علاوة على ذلك ، يمكن أن نضيف عدداً آخر من الأسباب وراء انتشار جرائم تكنولوجيا المعلومات منها :

١- الفرص المتزايدة : إن ازدياد عدد مستعملي الحاسوب من ذوي المعرفة والمقدرة في اختراق البيانات نتيجة "لا مركزية المعالجة"، الشبكات، والاتصالات والدخول عن بعد إلى الحاسوب قد اتخذت فرصاً متزايدة للمزورين والمتلاعبين لتنفيذ أغراضهم لاسيما في ظل سيطرة ورقابة غير كفوءة في هذا المحيط الإلكتروني لمعالجة البيانات .

٢- صعوبة الاكتشاف : إن وجود كم كبير من البيانات المخزنة في الحاسوب يجعل إخفاء أي تزوير أو تلاعب عملية سهلة خاصة إذا تمكن مرتكب الجريمة من عدم ترك أي دليل خلفه ، الأمر الذي يترتب عليه صعوبة اكتشاف الجريمة .

٣- تحقيق أرباح كبيرة : نتيجة للأرباح الطائلة التي يمكن أن يجنيها مرتكب التزوير والتلاعب ، فإنها تشكل دافعاً قوياً لأصحاب النوايا السيئة في ارتكاب جريمتهم . في استبيان أجراه أحد الباحثين في أمريكا عام (١٩٩٥) بيّن أن معدل أرباح مرتكب جريمة الحاسوب وصلت إلى "٦٠٠.٠٠٠" ألف دولار مقابل "٣٠٠.٠٠٠" ألف دولار لمرتكب الجريمة في النظم اليدوي(سرحان - ٢٠٠١ ص ١١٥ - ١١٦).

٤- صعوبة الاحتفاظ بآثارها إن وجدت .

٥- إنها تحتاج إلى خبرة فنية وتقنية ويصعب على المحقق التقليدي التعامل معها .

٦- إنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها .

٧- إنها تعتمد على قمة الذكاء والمهارة في ارتكابها (منير - ٢٠٠٤ ص ١٩).

٨- الولوج في جمع المعلومات وتعلمها يقود إلى ارتكاب جرائم الحاسب الآلي .

٩- الدوافع الشخصية قد تدفع بعضهم لإرتكاب جرائم تكنولوجيا المعلومات نتيجة إحساسه بالقوة والذات وبقدرته على اقتحام النظام ومن أجل تأكيد قدرته الفنية على ارتكاب أحد جرائم الحاسوب .

١٠- المؤثرات الشخصية : من المعلوم أن البرامج والمعلومات المخزنة داخل جهاز الكمبيوتر لها قيمة مادية كبيرة ، لذلك تسعى بعض الشركات التجارية والصناعية إلى الحصول على هذه البرامج والمعلومات عن طريق سرقتها ، وغالباً ، ما يقوم بذلك مقابل رشوة الموظف أو خداعه أو إغرائه أو استغلال نقاط ضعفه .

١١- حب المغامرة والإثارة . (محمد - ٢٠٠٤ ص ٢٣ - ٢٦)

سابعاً : مواصفات مرتكبو جرائم تكنولوجيا المعلومات :

حدد "دون باركر" الخبير بجرائم الحاسوب ، مواصفات مرتكب جريمة الحاسوب ، وحددها في ثلاثة شروط يجب أن تتوافر جميعها في شخص واحد ، ولكن وبسبب التطورات التكنولوجية التي حصلت مؤخراً والتوسع في استعمال

الحاسوب فقد تزيد أعداد الذين يمتلكون هذه المواصفات ، والتي تمكنهم من اختراق الحاسوب وارتكاب جريمتهم في التزوير ، وقد حدّد "باركر" هذه الصفات بالآتي :

١- **المعرفة: (knowledge)** : مع انتشار استعمال الحاسوب الشخصي ازداد عدد مستعمليه ، ومعها ازداد عدد ذوي العلم والمعرفة ولاسيما المعرفة بنقاط الضعف في الأنظمة المطبقة عليه مما يشجع ويسهل ارتكاب جريمة الحاسوب .

٢- **القدرة على اختراق وسائل الخزن: (access)** : نتيجة للتوجه الحاصل نحو اللامركزية في المعالجة بواسطة الحاسوب فقد ازداد استعمال الشبكات ووسائل الاتصال من أجل التفاعل عن بعد مع الحاسوب الأمر الذي أدى إلى ازدياد أعداد المستعملين ، وتوفير المعرفة المناسبة فلن يجد المستخدم صعوبة في استغلال وسائل الاتصال من أجل الوصول إلى مواقع خزن البيانات وتنفيذ جريمته لا سيما إذا لم تكن وسائل الخزن محاطة بنظام كفؤ للحماية .

٣- **القابلية على استعمال الوسائل: (resources)** : مع تزايد وسائل الاتصال بالحاسوب وتزايد أعداد ذوي المعرفة به ، تهيأت الظروف لأصحاب النوايا السيئة في استغلال وسائل الاتصال هذه وغيرها من مصادر الحاسوب سواء ما يتعلق منها بالخزن أو المعالجة لتنفيذ جريمة الحاسوب .

قد يكون السؤال المهم هنا مفاده : من أين يتم ارتكاب الجريمة الإلكترونية ؟ من داخل البلد أم من خارج أسوار الوطن ؟ يمكنك أن يكون مرتكب الجريمة من داخل المؤسسة أو من خارجها ، وهذا يعني ممكن أن يكون المجرم من أبناء البلد أو من غيرهم (أجنبي) ، ففي استبيان أجري في الولايات المتحدة الأمريكية والتي تعد من أكثر الدول التي تعاني من جرائم الحاسوب ، وجد أن (٩٨%) من مجموع الجرائم نفذت من قبل أشخاص من داخل المؤسسة التي تعرضت للجريمة وهي تتمحور حول نوايا ودوافع مرتكبيها التي تشمل اختلاس الموجودات ، والسرققة وإتلاف البيانات ، والتضليل وتشويه الحقائق ، وأن درجة الضرر الذي يمكن أن تسبب به الجريمة تعتمد بشكل رئيس على خبرة مرتكبيها . (سرحان - ٢٠٠١ ص ١١٤-١١٥)

ثامناً : الدوافع وراء ارتكاب جرائم تكنولوجيا المعلومات :

مما لا شك فيه أن وراء كل فعل سواء كان يحمل في طياته جانب الخير أم الشر إلا وخلفه دافع أو غرض أو غاية ، ولهذا ولذاك فإن الدافع (الباعث) ، والغرض ، والغاية ، تعبيرات لكل منها دلالاته الاصطلاحية في القانون الجنائي ، تتصل بما يعرف بالقصد الخاص في الجريمة وهي مسألة تثير جدلاً فقهيًا وقضائياً واسعاً ، ذلك أن القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجرمي ، وان " الباعث لا أثر له في وجود القصد الجنائي " ، وإذا كان الاستعمال العادي للتعبيرات المشار إليها يجري على أساس ترادفها

في الغالب ، فإنها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية، فالباعث (الدافع) هو " العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء أو الانتقام" ، وهو إذن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو " يختلف من جريمة إلى أخرى ، تبعاً لاختلاف الناس من حيث السن والجنس ودرجة التعليم وغير ذلك من المؤثرات كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر .

بالنسبة لجرائم تكنولوجيا المعلومات ، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنضوية تحت المفهوم ، ويمكننا من خلال الحالات التطبيقية نبين الدوافع الرئيسية الآتية :

١- **السعي إلى تحقيق الكسب المالي** : يعد هذا الدافع (والذي يمثل في الحقيقة غاية الفاعل) من بين أكثر الدوافع تحريكاً للجناة لاقتراف جرائم الحاسوب ، ذلك أن خصائص هذه الجرائم وحجم الربح الكبير الممكن تحقيقه من بعضها ، لاسيما غش الحاسوب أو الاحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع .

منذ بدايات الظاهرة ، فإن الدراسات أشارت إلى أن المحرك الرئيس لأنشطة احتيال الكمبيوتر ، وفيما بعد احتيال الإنترنت ، هو تحقيق الكسب المالي ، ففي دراسة قيّمة عرض لها الفقيه (RARKER) يظهر أن (٤٣%) من حالات الغش المرتبط بالحاسوب المعلن عنها قد بوشرت من أجل اختلاس المال ، وهي النسبة الأعلى من بين النسب التي حققتها جرائم أخرى في هذه الدراسة ، وأن (٣٢%) سرقة معلومات ، و(١٩%) أفعال إتلاف ، و(١٥%) سرقة وقت الحاسوب (الألة) لأغراض شخصية .

٢- **الانتقام من رب العمل وإحاق الضرر به** : لقد لوحظ أن العاملين في قطاع التقنية أو المستعملين لها في نطاق قطاعات العمل الأخرى ، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفرة في حالات معينة . هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح ، لكنها في عدة حالات ، مثلت قوة محرّكة لبعض العاملين لارتكاب جرائم الحاسوب ، باعثها الانتقام من المنشأة أو رب العمل ، والدليل على ذلك ، ربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيس والتكنيك الغالبة للفئة التي تمثل الأحقاد على رب العمل المحرك لارتكاب الجريمة .

٣- **الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية** : يرى بعضهم " إن الدافع إلى ارتكاب الجرائم في الطائفة الأولى (جرائم الحاسوب) يغلب عليه الرغبة في قهر النظم أكثر من شهوة الحصول على الربح " ، ومع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها ، إذ يظهر في قهر النظام إلا أن الدافع الأخير يتجسد في نسبة معتبرة من جرائم الحاسوب لاسيما ما يعرف

بأنشطة (HACKERS) المتطفلين الدخيلين على النظام والمتجسدة في جرائم التوصل مع أنظمة الحاسب - تحديداً عن بعد - والاستعمال غير المصرح به لنظام الحاسوب ، واختراق مواقع الإنترنت .

٤- **يميل مرتكبو هذه الجرائم إلى تفوقهم ومستوى ارتقاء براعتهم ، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم (شغف الآلة) يحاولوا إيجاد ، وغالباً ما يجدون الوسيلة إلى تحطيمها (والأصوب التفوق عليها) .** ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي جرائم الحاسوب ، الذين يمضون وقتاً طويلاً أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات ، ولإظهار تفوقهم على وسائل التقنية ، ونكتفي بالقول : إن الدافع هذا أكثر الدوافع التي يجري استغلالها من قبل منظمات الجريمة (مجموعات الجريمة المنظمة) لجهة استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة .

٥- **دوافع أخرى :** كانت تلك أبرز دوافع ارتكاب جرائم تكنولوجيا المعلومات ، لكنها ليست كل الدوافع ، فمحرك أنشطة الإرهاب الإلكتروني ، وحروب المعلومات ، الدوافع السياسية والأيدولوجية ، في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة ، والفعل الواحد قد يعكس عدة دوافع خاصة ما إذا اشترك فيه أكثر من شخص انطلق كل منهم من دوافع خاصة تختلف عن غيره ، ويمكننا أخيراً أن نضع التصور - الرياضي - التالي لدوافع بعض الهجمات الشائعة في حقل جرائم تكنولوجيا المعلومات :

أ- حروب المعلومات والإرهاب الإلكتروني = دوافع سياسية أو فكرية .
ب- إنكار الخدمة للمواقع التجارية والخدمية = التحدي وقهر النظم + أفعال تأدية وأحقاد موظفين + التنافسية بأنشطة غير مشروعة .
ج- احتيال الكمبيوتر واحتيال الإنترنت = استيلاء على المال أو المنافع وتحقيق الربح .

د- الاستيلاء على المعلومات = التنافسية + ابتزاز الأفراد وتحقيق المكاسب + المنافع +

التأرية + الإعداد للهجمات ذات الدوافع المالية .
و- إتلاف المعطيات وتخريب الأنظمة = الأحقاد والدوافع التأرية + إخفاء الأنشطة الجرمية

الأخرى + التنافسية غير المشروعة + التحدي وتحديداً بالنسبة لبرامج الفيروسات . (جعفر - ٢٠٠٧ ص ١٦٦ - ١٦٩)

تاسعاً : أنواع جرائم تكنولوجيا المعلومات :

مما لا شك فيه أن جرائم تكنولوجيا المعلومات باتت تشكل اليوم ظاهرة جديدة في المجتمعات الإنسانية ، لاسيما مجتمع المعلومات العالمي ، ولذلك أصبح المجتمع أمام مسؤولية جديدة وخاصة أولئك المتخصصين في مجال أمن المجتمع من رجال القانون وعلم الاجتماع وعلم النفس ، ورجال الأمن ... الخ . وباتت المسؤولية الجديدة تملي عليهم معرفة أنواع أو أنماط جرائم تكنولوجيا المعلومات ، ولهذا وذاك يتطلب الأمر كشف النقاب عن أنواع جرائم تكنولوجيا المعلومات من خلال تسليط الضوء على أهم أنواعها، وفيما يلي تلك الأنواع :

- ١- جريمة الإرهاب الإلكتروني .
- ٢- جريمة تضليل العقول : الإعلام المزيف .
- ٣- جريمة التزييف والتزوير .
- ٤- جريمة العبث بالبرامج أو جرائم تعمد الأذى والتدمير .
- ٥- جرائم السرقة الإلكترونية .
- ٦- جريمة سرقة البيانات والأصول .
- ٧- جريمة السطو على بطاقات الإئتمان والتجارة الإلكترونية .
- ٨- جريمة الانتحال .
- ٩- جريمة السب والقذف . جرائم التجسس .
- ١٠- جرائم التجسس وتهديد الأمن .
- ١١- جريمة المساعدة على الانتحار .
- ١٢- جرائم الجنس والعرض عبر الإنترنت .
- ١٣- جريمة غسيل الأموال عبر الإنترنت .
- ١٤- جريمة تعاطي المخدرات عبر الإنترنت . (جعفر - ٢٠٠٧ ص ١٧٢ - ٢٠٨)

عاشراً : المشكلات التي تقف وراء صعوبة مكافحة جرائم تكنولوجيا المعلومات :

يعترف العديد من المهتمين بشؤون تكنولوجيا المعلومات ، لاسيما بالجانب المتعلق بارتكاب الجرائم ، يعترفون بصعوبة اكتشاف جرائم تكنولوجيا المعلومات ، وكذلك في الوقت ذاته يعترفون بصعوبة بالغة جداً في محاولة منعها . وعملية الاعتراف هذه نابعة من وجود العديد من المشكلات والصعوبات العملية والإجرائية التي تظهر عند ارتكاب أحد ما جريمة ما من جرائم تكنولوجيا المعلومات ، ومن هذه المشكلات :

- ١- يمكن أن تنقضي عدة أشهر أو حتى سنوات قبل اكتشاف الجريمة .
- ٢- القوانين التي تحكم جرائم الحاسوب ليست واضحة ولم يسبق اختبارها مثل أنواع الجرائم الأخرى .

٣- عادة ما تتردد المنظمات مثل البنوك ، وشركات بطاقات الإئتمان ، وبيوت الاستثمارات في الإعلان عن الجريمة . (نانسي - ١٩٩٨ . ص ٨٤١)

٤- صعوبة إثبات وقوع الجريمة : ففي العديد من الحالات يتم الفعل الإجرامي دون أن يعلم المجني عليه بحدوث اعتداء وقع عليه ، ومن ذلك أن يتم إدخال فايروس إلى الجهاز عن طريق الاتصال بشبكة الإنترنت .

٥- صعوبة التوصل إلى الجاني : كثيراً ما يقوم الجاني بالدخول إلى شبكة الإنترنت باستعمال اسم مستعار وغالباً ما يقوم بالدخول إلى الإنترنت عن طريق مقاهي الإنترنت وبالتالي يصعب معرفة الجاني وتحديد موقع اتصاله .

٦- صعوبة إلحاق العقوبة بالجاني المقيم : هناك صعوبة في حالة ما إذا تم ارتكاب الجريمة بواسطة شخص أجنبي مقيم في الخارج ووقت الجريمة أمريكا أو مصر ، فهنا لا بد من تدخل الأنتربول الدولي للقبض على الجاني وإخضاعه للعقاب .

٧- تنازع القوانين الجنائية من حيث المكان : هناك مبادئ تحكم تطبيق القانون الجنائي ، منها إقليمية القانون الجنائي وعينية القانون الجنائي ، وعالمية القانون الجنائي . وتثور المشكلة في حالة ارتكاب الفعل المؤثم في الخارج ، فأى من القوانين الجنائية سوف يخضع لها الجاني ؟

٨- صعوبة تحديد المسؤول جنائياً عن الفعل الإجرامي : يظهر ذلك في حالة وقوع جريمة على شبكة الإنترنت ، كأن يدخل المستخدم للشبكة على موقع فيجد به أفعال إباحية ، فهل يسأل عن هذه الجريمة عامل الاتصال أم مورد المعلومات أو غير ذلك من العاملين في مجال الإنترنت ؟ .

٩- القصور في القوانين الجنائية : أدى ذلك القصور ومحاوله الفقه والقضاء إلى إخضاع جرائم الإنترنت إلى نصوص قانون العقوبات .

١٠- افتراض العلم بقانون جميع دول العالم : فالشخص الذي ينوي ارتكاب جريمة من جرائم الإنترنت فيقوم بالنشاط الإجرامي في دولته ، وتتحقق النتيجة في دولة أخرى يخضع للقانون الجنائي لتلك الدولة التي تحقق فيها النتيجة الإجرامية ، وهنا يجد الشخص نفسه خاضعاً لقانون دولة لا يعرف عنه أي شيء على أساس أن جميع دول العالم تفترض العلم بقانونها ، إذ يسود مبدأ عدم جواز الاعتذار بالجهل بالقانون ، فيمكن تصور الفعل الذي أتاه الشخص في دولته فعل مباح ولكنه يشكل جريمة في الدولة التي تحقق فيها نتيجة فعله . ويعد ذلك الأمر غير مقبول .

١١- صعوبة السيطرة على أدلة ثبوت الجريمة : حينما يتحدد مكان ارتكاب الجريمة التي تمت بواسطة استعمال شبكة الإنترنت أفراد الضبطية القضائية للقبض على الجاني وتحرير أدلة الجريمة ومنها جهاز الكمبيوتر المستعمل في الاتصال بالشبكة وما يحويه من برامج ومعلومات . تثار مشكلة معرفة الرقم السري الذي بدونه لا يعمل جهاز الكمبيوتر ، وفي هذه الحالة لا يجوز لأجهزة

التفتيش إجبار المتهم على الإفشاء عن الرقم السري ، إذ يعد ذلك إجراء غير قانوني . كذلك قد يتمكن الجاني من تدمير البيانات المخزنة داخل الكمبيوتر والتي تعد دليل إدانته في ثوان معدودة أثناء إجراء التفتيش ، ففي مثل هذه الحالات المختلفة يكون هناك صعوبة في جمع الأدلة المادية التي تثبت ارتكاب إحدى جرائم الإنترنت .

١٢- صعوبة المطالبة بالتعويض المدني : هناك صعوبة بالنسبة للمطالبة بالتعويض المدني عن ارتكاب أحد جرائم الإنترنت ، إذ يرجع في ذلك لأحكام القانون الدولي الخاص وما يثيره من صعوبات واتجاهات فقهية وتشريعية معارضة . (محمد - ٢٠٠٤ ص ١٤٠ - ١٤٣)

١٣- جهل الناس بثقافة الإنترنت : إذ إن الأغلبية من البشرية لا يعرف الكثير عن الإنترنت ، وحتى أولئك الذين يستعملونها ، مما يقعون في عدة أحيان في مطبات أو أخطاء لا يفطنون بها ، إلا أنها من الناحية القانونية تعد جريمة ويحاسب عليها القانون .

١٤- جهل المؤسسات أو مقاهي الإنترنت كذلك بجرائم تكنولوجيا المعلومات : هناك العديد من الناس الذين يعيشون أو يكتسبون لقمة عيشهم من وراء عملهم في منتديات أو مقاهي الإنترنت ، وكذلك المسؤولين عن إدارة هذه المقاهي ، هؤلاء أغلبهم لا يعرفون شيئاً عن جرائم تكنولوجيا المعلومات ، ولو كانوا يعرفون لوضعوا لافتات تحذير للزبائن لماهية جرائم تكنولوجيا المعلومات .

حادي عشر : استنتاجات البحث :

١ - إن جرائم تكنولوجيا المعلومات عابرة للحدود ويمكن ارتكابها من داخل وخارج حدود البلد .

٢ - هناك العديد من التسميات لهذا النوع من الجرائم إلا أن التسمية الأعم والأشمل و الأنسب هي جرائم تكنولوجيا المعلومات .

٣ - إن الحاسب وشبكة الانترنت هما مكان ارتكاب جرائم تكنولوجيا المعلومات .

٤ - يواجه المحققون صعوبة في التحقيق و التحري و المقاضاة في هذا النوع من الجرائم وذلك لعدم وجود شاهد او دليل على وقوع الجريمة .

٥ - مرتكبوا جرائم تكنولوجيا المعلومات هم اشخاص ذو خبرة فائقة في مجال الحاسب الالي و الانترنت .

٦ - هناك عدة دوافع وراء ارتكاب جرائم تكنولوجيا المعلومات منها المكاسب المادية و الانتقام من رب العمل و غيرها من الدوافع الاخرى .

٧ - تنوع جرائم تكنولوجيا المعلومات وفقاً لحاجة و دوافع مرتكبيها .

٨ - تقف وراء مكافحة جرائم تكنولوجيا المعلومات عدة مشكلات منها صعوبة التوصل إلى الجاني وصعوبة إلحاق العقوبة بالجاني المقيم خارج الحدود الوطنية .

ثاني عشر : التوصيات : آليات الحد من جرائم تكنولوجيا المعلومات :

رغم كل المشاكل والصعوبات السابقة الذكر ، التي واجهت وتواجه المجتمع ، لاسيما المعنيون بمكافحة جرائم تكنولوجيا المعلومات ، لم تهبط إرادة أصحاب عقول المعرفة والتقنية والتكنولوجية ، ورجال القانون والأمن في إيجاد أو ابتكار قوانين وطرق وتكنولوجيا معلومات جديدة قادرة على استكشاف المجرمين وإمكانية ملاحقتهم لإنزال العقوبة القانونية التي تتواءم وفعلهم الإجرامي . وفيما يلي أهم الطرق والأساليب التي يمكن أن تنجح في مجال مكافحة جرائم تكنولوجيا المعلومات :

١- يجب الاهتمام بموضوع التربية الأسرية والمدرسية وذلك من أجل إعداد وبناء جيلاً قادراً على التعايش الفعال والإيجابي في ظل العصر الرقمي ، ولذلك فإن مكافحة جرائم تكنولوجيا المعلومات تعتمد أولاً وقبل كل شيء على مبدأ التربية وإعداد الفرد إعداداً اجتماعياً سليماً . وكما قال الشاعر :

وإنما الأمم الأخلاق ما بقيت
فإن همو ذهبت أخلاقهم ذهبوا

٢- الانضمام إلى المعاهدات الدولية لمكافحة جرائم الإنترنت ، مثل معاهدة بودابست عام (٢٠٠١) والمعاهدة الأوروبية لمكافحة جرائم الإنترنت والتي تعمل على زيادة التعاون والتنسيق بين الجهود الدولية .

٣- إدخال تلك المعاهدات الدولية إلى حيز التنفيذ قوياً وفعالاً من دون تأخير .

٤- العمل على إصدار قوانين جديدة تجرم جرائم تكنولوجيا المعلومات في كافة أنحاء العالم بحيث يكون هناك قدر كبير من التناسق ، مثلما فعلت السويد وصدرت أول قانون خاص بها (the special law) وسمي بقانون (البيانات) الذي صدر عام ١٩٧٣ ، وكذلك فعلت بريطانيا عام ١٩٨١ ، وكذلك فعلت الولايات المتحدة الأمريكية عام ١٩٨٥ .

٥- يجب التركيز على مبدأ التعاون الدولي ، فهو من أهم سبل مكافحة جرائم تكنولوجيا المعلومات وملاحقة مرتكبيها وتسليمهم المطلوبين منهم أمنياً إلى الدول التي تطالب بهم .

٦- سن القوانين وعقد الاتفاقيات الخاصة بحماية حق الملكية الفكرية في عصر تكنولوجيا المعلومات والدخول في تلك الاتفاقيات مثل معاهدة برن لحماية المصنفات الأدبية ومعاهدة تريبس في ذات المجال .

٧- العمل على تأمين الشبكات على نحو يمنع اختراقها قدر الإمكان .

- ٨- يجب التركيز على دور المجتمع في مكافحة جرائم تكنولوجيا المعلومات وذلك من خلال :
- أ- تكريس دور الأسرة معلوماتياً ،بمعنى أن يسارع الأب والأم إلى الإلمام بتقنية الإنترنت والتعامل معها على نحو يمكن من مراقبة الطفل أو الحدث حال تجواله على الشبكة ولا تترك له الحرية كاملة في هذا المجال .
- ب- اهتمام المدرسة في المراحل التعليمية بتسخير تقنية الإنترنت لأغراض تعليمية ،وتدريس ثقافتها للطفل على نحو يعي معه أخطارها قبل المزايا المستمدة منها .
- ج- محاولة السيطرة على جماعات الأصدقاء والشللية التي تدفع الطفل أو الحدث إلى الانحراف الإنترنتي سواء من خلال اللقاء على مقاهي الإنترنت أو من خلال اللقاء في غرف الدردشة وتسريب الخبرات الضارة فيما بينهم .
- ٩- العمل على نشر ثقافة الإنترنت في المجتمع وإظهار كل من منافعها والتركيز عليها ، وكذلك سلبياتها والعمل على تجاوزها .
- ١٠- العمل على تأهيل رجال الأمن ورجال الضبط والتحقيق الجنائي وإدخالهم دورات تدريبية في الداخل والخارج في أرقى وأفضل المعاهد والمؤسسات التي تهتم بشؤون جرائم تكنولوجيا المعلومات . ومن أجل تفعيل دور رجال القانون والأمن يتطلب أن يتناول منهج دوراتهم التدريبية الآتي :
- ١- أنواع المخاطر والتهديدات التي يمكن أن تتعرض لها شبكة الإنترنت .
- ٢- مفاهيم الحاسب الآلي والإنترنت ، من برامج وتطبيقات وأسماء الأجهزة .
- ٣- أنواع جرائم تكنولوجيا المعلومات وسبل مكافحتها .
- ٤- منهج التحقيق ، أي الإجراءات المتبعة في تحقيق هذه الجرائم ، ويشمل ذلك:
- أ- إجراءات التحقيق .
- ب- تخطيط التحقيق .
- ج- تجميع المعلومات وتحليلها .
- د- المواجهة والاستجواب .
- ح- مراجعة النظم الفنية للبيانات .
- و- أساليب العمل الجنائي .
- ٥- أمن الحاسوب وشبكات المعلومات .
- ٦- القانون ونظرية الإثبات .
- ٧- استعمال الحاسب والإنترنت كوسيلة للحصول على أدلة الاتهام .
- ٨- الملاحقة الدولية والتعاون المشترك في مجال جرائم المعلوماتية

مصادر البحث :

- ١- ابن منظور لسان العرب ،مادة جرم .
- ٢- جعفر حسن جاسم . تكنولوجيا المعلومات ودورها في الحد من الكوارث الطبيعية في المنطقة العربية . مجلة الجامعي ،ع ١٦ ، ٢٠٠٨ .
- ٣- جعفر حسن جاسم الطائي . جرائم تكنولوجيا المعلومات : رؤية جديدة للجريمة الحديثة .- عمان : دار البداية ، ٢٠٠٧ .
- ٤ - سرحان سليمان سرحان ، محمود عبد المنعم المشهداني . أمن الحاسوب والمعلومات .- عمان : دار وائل ، ٢٠٠١ .
- ٥ - الشبكة القانونية العربية – فرع القانون . جرائم الكمبيوتر والإنترنت . متاح في : . arab@wnwt-law subjects – تاريخ الزيارة ، ٢٠٠٤ / ١١ / ١٢ .
- ٦ - صالح بن محمد المسند ، عبد الرحمن بن راشد المهيني . جرائم الحاسوب الآلي : الخطر الحقيقي في عصر المعلومات . المجلة العربية للدراسات الأمنية والتدريب ، م ١٥ ، ع ٢٩ ، ٢٠٠٠ .
- ٧- محمد أمين الرومي . جرائم الكمبيوتر والإنترنت .- الإسكندرية : دار المطبوعات الجامعية ، ٢٠٠٤ .
- ٨ - محمد شحاته ربيع ، جمعة سيد يوسف ، معتز عبد الله . علم النفس الجنائي .- القاهرة : دار غريب ، ١٩٩٤ .
- ٩ - منير محمد الجنيهي ، ممدوح محمد الجنيهي . جرائم الإنترنت والحاسب ووسائل مكافحتها .- الإسكندرية : دار الفكر الجامعي ، ٢٠٠٤ .
- ١٠- نانسي سترن ، روبرت سترن . الحاسبات في عصر المعلومات ؛ تعريب سرور علي إبراهيم ، هندي عبد الله العلي .- الرياض : دار المريخ ، ١٩٩٨ .