



مجلة العلوم القانونية والسياسية

اسم المقال: مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها

اسم الكاتب: م.م. مشتاق طالب وهيب

رابط ثابت: <https://political-encyclopedia.org/index.php/library/1018>

تاريخ الاسترداد: 2025/05/17 09:41 +03

الموسوعة السياسية هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.

لمزيد من المعلومات حول الموسوعة السياسية – Encyclopedia Political – يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسية – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام

<https://political-encyclopedia.org/terms-of-use>

تم الحصول على هذا المقال من موقع مجلة العلوم القانونية والسياسية جامعة ديالي ورفده في مكتبة الموسوعة السياسية
مستوفياً شروط حقوق الملكية الفكرية ومتطلبات رخصة المنشاع الإبداعي التي يتضمن المقال تحتها.



مفهوم الجريمة المعلوماتية

ودور الحاسوب بارتكابها

Concept of IT Crime (Cybercrime)
and Computer Role for its being Committed

الكلمة المفتاحية : الجريمة المعلوماتية

م.م. مشتاق طالب وهيب

كلية القانون والعلوم السياسية – جامعة ديالى

Assistant. Lecturer. Mushtaaq Taleb Wehaeeb
College of Law and Political Sciences-University of Diyala
E-mail: mwahaib@yahoo.com

ملخص البحث

تعد الجريمة المعلوماتية من المواقف الأكثر انتشاراً على المستوى الدولي والإقليمي والمحلي. فلقد أخذت هذه الجريمة، باعتبارها نتاج الاستخدام السلبي للتكنولوجيا وما يتصل بها من تقنيات، حيزاً كبيراً من الاهتمام بهذا الجانب وذلك لجسامه الآثار الناشئة عن هذه الظاهرة الحديثة نوعاً ما وفي جميع مجالات الحياة. في الوقت الذي وجدت هذه الجرائم صدى لدى المعنيين بمواجهتها، لم تجد هناك اتفاق أو شبه اتفاق لديهم على مصطلح معين أو تعريف ما أو تصنيف محدد بحيث تشير إلى الأنشطة غير القانونية وغير الاجتماعية التي يمكن أن تدرج تحت مسمى هذه الجريمة. لذلك فإن تحديد النقاط السابقة مع ما يتصل بها من قضايا مهمة قد تثار في ظل هذا المصطلح، كتحديد الدور الذي يلعبه الحاسوب والأنظمة التقنية وعلاقتها بالعامل البشري، يكون من أساسيات إنشاء استراتيجية قانونية في سبيل مكافحة هذه الجريمة.

المقدمة

يحيط بكل ظاهرة الكثير من الأسئلة تتعلق في بيان ماهيتها بعد أن تصبح واقعاً في حياتنا وبصورة خاصة ما يتصل بالتطور التكنولوجي في مجال الاتصال والذي بات قلق القانونين، وجميع المهتمين بهذا المجال في محاولة تقليل مستوى الانشطة الاجرامية في المجتمع^(١)، منها أمر محظوظ وليس لهم فقط بل حتى الناس العاديين وفي جميع المجالات. كيف لا وأنها غزت جميع ميادين الحياة، وبالشكل الذي لا يقتصر على النطاق المحلي أو الإقليمي بل امتد إلى العالم ككل. فهذه التقنيات ورغم أنها جعلت الحلم حقيقة مادية بعد أن كان خيال يدور في الذهن وجعلت كل شيء في متناول اليد مقدمة للمجتمع الإنساني فوائد لا يمكن عدها، لكن نجدها في ذات الوقت قلق يتزايد وهاجس أمني يهدد كيان المجتمع وذلك نتيجة لما أفرزته من سلبيات تخالف الأسس الصحيحة للبناء الاجتماعي متبلورة في جرائم تخرج عن نطاق السيطرة وتحاجم المصالح العامة والخاصة على حد سواء. لقد خلقت هذه التقنيات أعمال تحمل في العديد من جوانبها الصفة الإجرامية. خصوصاً، أن العلاقة بين معدل الجريمة وظهور هذه التقنيات هي علاقة طردية، حيث أن هذه التقنيات تقلل من صعوبات ارتكاب الجريمة وبالشكل الذي يزيد من معدلات ارتكابها^(٢). وللارتباط الوثيق بين هذه التقنيات المتمثلة بالحاسوب والمعلومات وهذه الأفعال ظهر ما يعرف بالجريمة المعلوماتية. وهذه الجرائم تجذب مستوى من الاهتمام مما جعلها فريدة انتجت ثروة من الدراسات الفقهية والتقارير الحكومية ومجموعة من التشريعات الجديدة^(٣). واظهرت الاحصائيات أن هذه الجريمة قد أصبحت ظاهرة نامية^(٤). في الحقيقة، هذه الظاهرة تضع الكثير من علامات الاستفهام. ولأجل إزالة الغموض المحيط بها يتطلب الأمر تحديد مفهوم هذه الظاهرة ورسم الإطار الواضح لمدلولها، وكذلك بيان علاقة دور الحاسوب في تنفيذ هذه الجريمة. لذا سيتم تقسيم هذا الموضوع إلى مبحثين، خصصنا الأول لتحديد مفهوم الجريمة المعلوماتية، وكرسنا الثاني لبحث تصنيف الجريمة المعلوماتية وأهمية الحاسوب في ارتكابها.

المبحث الأول

مفهوم الجريمة المعلوماتية

لتسلیط الضوء على معنى محمد للجريمة المعلوماتية، فقد ناقشنا هذا في أمرين تمثلا في:-
 الأول إيضاح تعريف الجريمة المعلوماتية والثاني استعراض أهم الخصائص التي تمتاز بها هذه الجريمة، التي يمكن القول بأنها جريمة العصر كونها ظاهرة حديثة في اغلب الجوانب، سعياً منا في تحديد إطار عميق لمفهوم الجريمة المعلوماتية .

المطلب الأول : تعريف الجريمة المعلوماتية

من وجهة النظر الواسعة، تحديد التعريف والمصطلح يكون نقطة بداية مهمة. حيث أنها تقدم قاعدة لتطوير القانون المتعامل مع المشاكل المصاحبة لسوء استخدام هذه الأجهزة والتكنولوجيات. علاوة على ذلك، أن فهم نطاق المصطلح يسهل المواءمة الدولية للقوانين^(٥). ولكي تكون أمام تعريف دقيق للجريمة المعلوماتية يحيط بكل جوانبها كونها ظاهرة هي عبارة عن خليط من أمور فنية وقانونية. فقد قسمنا هذا المطلب إلى ما يأتي :-
 أولاً : - المصطلح الأنسب :-

يلاحظ على الأبحاث والدراسات التي أجريت بقصد هذا الموضوع، عدم الاتفاق على مصطلح معين يكون أكثر دقة للدلالة على مفهوم هذه الظاهرة الإجرامية المستحدثة. إذ أن هناك العديد من المصطلحات التي شاع استخدامها على مستوى الفقه أو التشريعات كل حسب نظرته لهذا الموضوع.

ففي بدايات هذا النوع من الجرائم أطلق عليها مصطلح احتيال الحاسوب (computer fraud) على اعتبار أن هذه الجريمة هي الأكثر شيوعاً عند ظهور هذه الجرائم^(٦). والحقيقة أن هذا المصطلح أصبح لا يلائم ما أصبحت عليه هذه الجرائم، ذلك أن الاحتيال هو الآن أحد أنواع هذه الجرائم وليس مصطلح يطلق على الظاهرة ككل.

وهناك أيضاً مصطلح جرائم التكنولوجيا العالية (high-tech)، كون أن استخدام هذا المصطلح يكون استقراء للتطورات التكنولوجيا في العقود الأخيرة^(٧). في الواقع، أن هذا المصطلح يتجاوز تكنولوجيا شبكات المعلومات ليشمل التطورات التكنولوجية الأخرى مثل التكنولوجيا النانوية والهندسة الحيوية^(٨). كما هذه التسمية واسعة ومطلقة بحيث تشمل الكثير من الأجهزة التي لا ترتبط مع الهدف المقصود من التسمية. زيادة على ذلك، هناك الكثير من الأجهزة التقنية يمكن أن تستخدم لارتكاب الجريمة، وبالتالي الخلط بين مفهوم الظاهرة التي نحن بصددتها وبين هذه الجرائم كاجرائم التي ترتكب بواسطة الأجهزة التقنية في مجال الطب وغيرها.

ويستخدم أيضاً مصطلح جرائم الكمبيوتر (Computer Crimes) للتعبير عن هذه الظاهرة^(٩). والذي يشير لتعريف أية انشطة اجرامية ترتكب ضد الحاسب أو جهاز مشابه، أو البرنامج أو البيانات في داخله، أي أن الحاسب يكون فيها الهدف للنشاط الاجرامي^(١٠). والحقيقة أنه مصطلح غير دقيق، كونه يركز على عنصر أساسي في ارتكاب الجريمة وهو الحاسب مهملاً بذلك الجوانب الأخرى التي تستند عليها هذه الجريمة. ومن جانب ثانٍ، أنه يستبعد الجرائم التي يكون فيها الحاسب وسيلة لتنفيذ العمل الاجرامي كالاحتيال المرتبط بالحاسوب. لذلك نجد قسم آخر من الفقه يفضل مصطلح سوء استخدام الحاسوب (Computer Misuse) على هذا المصطلح، على اعتبار أنه يتيح لتشكيله أوسع من القضايا المتعلقة بالحواسيب^(١١).

ودرج البعض على استخدام مصطلح جرائم إساءة استعمال الحاسوب (Computer Abuse Crimes)^(١٢)، باعتبار أن هذه الجرائم لا تتحقق إلا باستخدامه واستخدامه سيء. وهذا أيضاً معيب كونه يركز على الحاسوب في ارتكاب الجريمة ويهمل باقي صور الاستعمال، حيث أن الكثير من الأفعال تتم باستخدام الحاسوب بصورة مشروعه ولكن يقوم بنفس الوقت بارتكاب عمل جرمي كمن يستخدم الحاسوب وهو أساساً مخول باستخدامه في تغيير بعض المعلومات والتي هي أصلاً من اختصاصه إدراج تلك المعلومات. وأيضاً شاع استخدام مصطلح الإجرام الكوني (Cybercrime)^(١٣)، والذي يستخدم للإشارة إلى الأنشطة الاجرامية التي تكون فيها الحاسوب أداة تسهيلية لتنفيذ الجرائم التقليدية^(١٤). وهذا باعتقادنا غير

دقيق، لأنه ينافي المدلول الحقيقى لهذا المصطلح الذى يتمثل في اعمال اجرامية تتم ضد الحاسوب والأنظمة المعلوماتية على حد سواء، وليس فقط الاستخدام المجرد للحاسوب أو جهاز آخر كأدلة لارتكاب الجريمة. وهناك من يستخدم مصطلح جريمة تكنولوجيا المعلومات والاتصالات (ICT Crime) للإشارة إلى جميع الافعال التي تشملها المصطلحات السابقة^(١٥).

أما على صعيد الفقه الفرنسي فقد درج الغالبية استعمال مصطلح الجريمة المعلوماتية **Le delit informatique** أي مجموعة الجرائم المتصلة بالمعلوماتية^(١٦). وبه قد تأثر الفقه المصري الذي استقر على استخدام مصطلح الجريمة المعلوماتية على اعتبار أنها تمثل صور السلوك التي تشكل جرائم يعاقب عليها القانون دون سواها^(١٧).

الحقيقة، هذه المصطلحات ينبغي أن لا تعامل حرفياً، ولكن إلى حد ما مصطلحات وصفية على نحو واسع تشدد على دور التكنولوجيا في ارتكاب الجريمة^(١٨). على الرغم من أنه لا يوجد مصطلح واحد متفق عليه، فأنا نعتقد أن المصطلح الأكثر دقة هو جريمة المعلومات باعتبار أن هذه الجرائم لا تتم إلا باستخدام جهاز الحاسوب والذي يتراكم عمله على البرامج المعلوماتية. أي أنه لا فائدة من الحاسوب بدون هذه البرامج سواء كانت تشغيلية أو تطبيقية ولا يستطيع الحاسوب إنجاز أي عمل دون هذه البرامج وبعد إدخال المعلومات التي تعالج ألياً وفق برامج معينة تقوم المعلومات المدخلة إليها بدور كبير جداً في ارتكاب العمل الجرمي عن طريق تلك البرامج الموجود في الحاسوب. لذا فإن هذه الجرائم المقترنة بالتقنيات الحديثة في غالبية صورها (إذا ما كانت جميعها) تتعامل مع عنصر المعلومات، التي يندرج في إطارها كل البيانات أو النصوص أو الصور أو الأشكال أو الأصوات أو الرموز أو قواعد البيانات وبرامج الحاسوب، مع ما يرتبط بها من أنظمة تقنية أخرى مخصصة لأجل الاتصال بالشبكة، التي تكون عبارة عن مجموعة من أجهزة الحاسوب أو أنظمة معالجة مرتبطة بعضها وتترکز أساساً على مفهوم المعلومات، أو أنظمة معالجة تستخدم لإنشاء أو إرسال أو معالجة أو تخزين المعلومات.

ومن جانب ثانٍ اتجاه بعض القوانين^(١٩) وجانب من الفقه إلى استخدام هذا المصطلح الذي يعد حسب تقديرنا الأكثر شيوعاً وملاءمة لهذه الظاهرة، وأنه يدل بحد ذاته على مفهوم

دقيق ومدلول واضح لها إذ ينصرف إلى كل سلوك يتعلق بالمعلومات المعالجة ألياً. زيادة على ذلك، أنه لا يركز على الحاسب في تكيف أو تسمية الفعل لأن هذه التسمية هي خليط من اندماج المعلومات والأنظمة التقنية المتمثلة بدرجة كبيرة بالحاسوب. كما وأنه مصطلح شامل لجميع المصطلحات التي يستخدمها المعنيين بهذا المجال للدلالة على الأفعال الجنائية التي تتم بواسطه هذه العوامل أو ضدها. حيث أنه يشمل الحاسوب وكذلك أي تكنولوجيا متصلة بعمليات الاتصال أو أنظمة معالجة البيانات والمعلومات. عليه فسوف نستخدم مصطلح جريمة المعلومات للدلالة على هذه الظاهرة .

ثانياً : تعريف الجريمة المعلوماتية :-

بالرغم من أن هذا المصطلح قد دخل في الاستعمال الشائع، فإن كثيرين سوف يجدون أنه من الصعوبة تعريف هذا المصطلح بصورة دقيقة^(٢٠). لذلك فقد صاغ الفقه وكثير من المؤسسات المتخصصة مجموعة من التعريفات التي كانت متباعدة فيما بينها ضيقاً واتساعاً تبعاً للمعيار الذي اعتمد في تعريف هذه الجريمة والدور الذي يمكن أن يلعبه الحاسوب والنظام المعلوماتي في ارتكاب الجريمة المعلوماتية.

وعليه سوف نعرض في هذا المجال مجموعة من التعريفات وفق ترتيب يقوم على أساس المعيار المعتمد في التعريف وكالآتي :-

الاتجاه الأول : - التعريف القائم على أساس وسيلة ارتكاب الجريمة :-

لقد اعتمد هذا الاتجاه في تعريف الجريمة المعلوماتية على الوسيلة المستخدمة في ارتكاب الجريمة. لذلك فقد عرفت بأنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسوب^(٢١). وهي أيضاً رد فعل إجرامي يستخدم الحاسوب في ارتكابه كأدلة رئيسية^(٢٢). وكذلك قيل بأنها نشاط إجرامي تستخدم فيه تقنية الحاسوب بطريقة مباشرة أو غير مباشرة أو هدف لتنفيذ العمل الإجرامي المقصود^(٢٣). وقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دوراً رئيسياً في ارتكابها^(٢٤). وعرفها آخرون بأنها أي نوع من أنواع الجرائم التي ترتكب باستخدام

الحاسوب^(٢٥)، أو تسهل باستخدام الحاسب أو شبكة أو جهاز^(٢٦). أو هي أي جريمة التي بطريقة أو بأخرى تنطوي على استعمال تكنولوجيا المعلومات^(٢٧). أو الاستفادة من تكنولوجيا شبكة الانترنت^(٢٨). كما توصف بأنها سلوك غير مشروع أو غير اخلاقي متعلقة باستخدام الحاسبات أو البرامج أو البيانات من أجل النظر في المدى الذي به هذه الانشطة ينبغي أن تكون بصورة صحيحة الموضوع للقانون الجنائي^(٢٩). وهي أيضاً الجرائم التي فيها الحاسب يلعب دوراً نشطاً بدلاً من دور سلبي^(٣٠).

الاتجاه الثاني :- تعريف الجريمة المعلوماتية باعتبار موضوعها :-

إن فكرة التعريفات في ظل هذا الاتجاه تتركز في الجريمة التي تقع ضد الحاسب أو النظام وليس باعتبارهما الحاسب الوسيلة في ارتكابها. لذلك عرفت بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو للوصول إلى المعلومات المخزونة داخل الحاسب أو التي تحول عن طريقه^(٣١). وأيضاً هي كل سلوك غير شرعي أو غير مسموح به يتعلق بالمعالجة الإلية للبيانات أو نقلها^(٣٢). وذهب رأي يؤيد ذلك بأنها الجرائم المرتكبة ضد المال المرتبط بالمعالجة الآلية للبيانات^(٣٣).

الاتجاه الثالث :- تعريف الجريمة المعلوماتية على أساس المعرفة بـ تقنية المعلومات :-

إن الجريمة المعلوماتية هنا هي الجريمة التي يكون مطلوب لتنفيذها توافر المعرفة التقنية لدى الفاعل^(٣٤). وعلى هذا النسق، هي نسخة من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطاً بـ تقنية المعلومات^(٣٥). وهي أيضاً الجرائم التي تتضمن أي فعل غير قانوني تكون المعرفة بتكنولوجيا الحاسوب أساسية لارتكابها^(٣٦). وعرفت بأنها الجريمة التي يتم ارتكابها إذا قام الشخص باستخدام معرفته بالحاسوب لإنجاز عمل غير قانوني^(٣٧). أو هي الجريمة التي تنجز من خلال معرفة خاصة بتكنولوجيا الحاسب^(٣٨).

الاتجاه الرابع :- تعريف الجريمة المعلوماتية وفق معايير متعددة :-

هناك الكثير من التعريفات التي حاولت إيجاد صيغة معينة قابلة لاحتواء الجريمة المعلوماتية بين قوسين من خلال اعتماد معايير متعددة. لذلك، نجد جانب من الفقه يعرف الجريمة

المعلوماتية بأنها أي حادثة تتضمن فعلاً مقصوداً يتعرض بموجبه الجني عليه أو يمكن أن يتعرض فيه أي شخص آخر لخسارة، فيما يتحقق مرتكبها أو يمكن أن يحقق مكتباً بمساعدة الحواسيب^(٣٩).

وهناك التعريف الذي تضمنته توصيات منظمة التنمية والتعاون الاقتصادي لسنة ١٩٨٦ ورد فيه، أنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها^(٤٠).

ويبدو هذا التعريف أنه يوسع من نطاق هذه الجريمة، ذلك أن التسوية بين السلوك غير المشروع قانوناً، والسلوك الذي يستحق اللوم أخلاقياً واستهجان الكافة، يعارض حقيقة هي أنه ليس بالضرورة أن يكون الانحراف عن الأخلاق والسلوك المؤثم يكون معاقب عليه من قبل القانون^(٤١).

وعرفت أيضاً بأنها أي سلوك غير مشروع يرتكب بواسطة نظام حاسوبي أو شبكة حاسوبية بما في ذلك جرائم من قبيل حيازة المعلومات أو عرضها أو توزيعها بصورة غير مشروعة^(٤٢). وهي كذلك الجريمة الجنائية التي تنطوي على الحاسوب كموضوع للجريمة أو أداة مستخدمة لارتكاب العنصر المادي للجريمة^(٤٣). أو هي اعمال اجرامية مرتكبة باستخدام شبكات الاتصالات الالكترونية وانظمة المعلومات أو ضد هذه الانظمة والشبكات^(٤٤).

تحليل تعريفات الجرائم المعلوماتية :-

بعد هذا العرض الموجز لبعض التعريفات التي حاولت تحديد هذه الظاهرة، لابد لنا من وقفة نبين من خلالها ما هو التعريف المناسب باعتماد المعيار الملائم لذلك. وعليه يمكن القول، أنه ما من شك في أن الاتجاه الذي اعتمد موضوع الجريمة كمعيار لتعريف الجريمة المعلوماتية بأنه جيد نوعاً ما. فهو أن يصلح لبعض جرائم قانون العقوبات القسم الخاص إلا أنه لا يناسب بقية أنواع الجرائم المعلوماتية، خاصة وأن هذه الجرائم هي بحد ذاتها محل خلاف وجدل.

أما الاتجاه الذي اعتمد على وسيلة ارتكاب الجريمة فهو غير دقيق، ذلك لأن تعريف الجريمة المعلوماتية يقوم في الأساس على العمل الرئيسي المكون لها وليس فقط الوسيلة

المستخدمة في التنفيذ. إذ لا يمكن أن يطلق على جريمة ما أنها جرائم الحاسب بمجرد أن الأخير قد استخدم في التنفيذ، حيث يجب الرجوع إلى الفعل الأساس المكون للجريمة ومحل الاعتداء وليس فقط للوسيلة المستخدمة لارتكابها.

أما الاتجاه نحو اعتماد المبدأ الشخصي، الدراية والمعرفة في الأمور الفنية للحاسوب في ارتكاب الجريمة، فهو في اعتقادنا غير ناجح في تعريف الجريمة المعلوماتية. لأنه ربط مفهوم هذه الجريمة بمعيار شخصي يصعب تحديده بشكل دقيق وواضح. وأنه شرط شخصي متصل بالفاعل فإنه من الصعب معرفة وجوده في حالة لو كان أحد المشتركين في هذه الجريمة يفتقر إلى صفة المعرفة التقنية. لذا لا يمكن القول بشمولية هذا التعريف، وانه كان غير صائب في هذه المحاولة.

أما بخصوص الاتجاه الرابع الذي اعتمد أكثر من معيار. نعتقد أنه كان موفقاً بعض الشيء في مجال شمولية التعريف، لكنه لم يكن في ذات الدرجة في الترتيب والتحديد والتكييف. ولكنه كان أفضل من سابقيه في هذا المجال، لأنه أراد من خلال اللجوء إلى عدة معايير التغلب على معوقات كثيرة لتحديد هذه الظاهرة، التي يكون التعريف فيها عاجز في حالة اعتماده مبدأ منفرد معين لتحديدها، خاصة أنها ظاهرة متعددة أو لديها سرعة التجدد والاستجابة للمتغيرات التكنولوجية إزاء البطء في الاستجابة لدى التشريعات.

وأخيراً بناء على ما تقدم، أن التعريف الذي يمكن أن ينسجم مع طبيعة هذه الجريمة هو أنه (كل سلوك غير مشروع يتضمن القيام بعمل أو الامتناع عن عمل، يكون فيه الحاسوب والنظام المعلوماتي (وما يرتبط بهم) عنصر في ارتكاب الاعتداء، يتطلب عليه تحقيق مصلحة غير مشروعة للفاعل أو الحق ضرر بالغير). ويمكن تبرير هذا التعريف كالتالي :-

أولاً:- هذا التعريف يكون شامل لجميع أنواع الأفعال الإجرامية سواء كانت متعمدة أو غير متعمدة. لأنه أحياناً بعض الأعمال تسبب أضراراً بالغة بالغير حتى وإن لم تكن عمديه، كما في حالة دخول المتطفلين، أي أنه يشمل جميع أوجه الفعل سواء كان ايجابياً أو سلبياً.

ثانياً:- إنه تعريف يستوعب حالة الفعل الإجرامي التي يكون فيه الحاسوب والنظام المعلوماتي الوسيلة أو الهدف في ارتكاب العمل الجرمي، مع التأكيد على أهمية النظام المعلوماتي

كأحد المكونات الرئيسية الالازمة لتشغيل الحاسب. إذ لا يمكن تصور أن يكون للحاسوب أي دور في الجريمة دون أن يكون هناك برامج التشغيل، فالحاسوب يعتمد بالدرجة الأساس في عمله على البرامج التشغيلية والتطبيقية وهي الأساس في الانظمة المعلوماتية.

ثالثاً:- إن هذا التعريف لا يقتصر على الحاسوب أو النظام المعلوماتي بل يتضمن كل كيان أو برنامج أو مكون للحاسوب أو النظام المعلوماتي من خلال ذكر عبارة (وما يرتبط بهم) التي تكون شاملة لجميع معطيات التكنولوجيا من معلومات، بيانات لم تعالج بعد، مخزونة، مخرجة، برامج تشغيلية أو تطبيقية أو أية معطيات أخرى كالنصوص والرسوم والصور... الخ . بل وحتى جميع الخدمات التي تقدم بواسطتهما، وأقصد ما ينتج عن الشبكة الدولية للمعلومات.

رابعاً:- احتوى التعريف أيضاً أمر جوهري وهو النتيجة الإجرامية التي تتولد عن هذا السلوك غير المشروع. والرغبة في التركيز على خطورة الظاهرة، وإظهار حجم الخسائر التي يتکبدها العالم بسبب انتشارها على المستوى الدولي، فقد استوعب جميع النتائج السلبية والاباحية. فهو يشمل الفعل الذي يعود على الجاني بمصلحة دون أن يلحق ضرراً بالغير كإعلان الصور الإباحية مقابل مبلغ من المال على موقع معين. أو أنه يلحق ضرر بالغير دون أن يحقق فائدة للفاعل كما في الدخول على أنظمة بعض المؤسسات بقصد الإضرار لا أكثر أو للهو أو الهواية، أو الاثنين معاً كالتهديد بتعطيل معلومات نظام معين ما لم يتم تحقيق مطالبه.

خامساً:- أخيراً أن التعريف جامع لكل أركان وشروط الجريمة المعلوماتية بالمعنى القانوني. فهو يحدد الركن المادي وهو السلوك غير المشروع سواء كان القيام بعمل أو الامتناع عن عمل كان ملزماً القيام به. ويحدد الوسيلة والهدف في ارتكاب الفعل الجرمي وهو الكمبيوتر والنظام المعلوماتي وباختلاف الدور الذي يحتله كل عنصر. وكذلك يبين موضوع الجريمة الذي يكون فيها الاعتداء على حقوق الآخرين. وأيضاً النتيجة الإجرامية من خلال توضيح العلاقة السببية بين فعل الجاني والنتيجة التي ستظهر بسبب هذا الفعل وهي تحقيق فائدة للجاني أو الحق ضرر بالغير.

المطلب الثاني : خصائص الجريمة المعلوماتية وال مجرم المعلوماتي

تمثل الجريمة المعلوماتية طبيعة خاصة تميزها عن بقية الجرائم التقليدية. وذلك لارتباطها بالحاسوب وانظمة المعلومات وما تتمتع به من تقنية وأمور فنية في اغلب الجوانب. هذه الحقيقة اضفت على هذه الجرائم عدة خصائص والتي انعكست بدورها على مرتكب الجريمة، الذي يعرف بال مجرم المعلوماتي لتمييزه عن المجرم التقليدي. ونتيجة لذلك اكتسبت هذه الجرائم شكل جديد. وسنحاول هنا التعرف على أهم سمات الجريمة المعلوماتية، ومن ثم بيان ابرز صفات المجرم المعلوماتي.

أولاًً : - خصائص الجريمة المعلوماتية :-

إن هذه الجرائم تميز بسميات تتصل بصفة عامة بتحقيقها ومستلزمات ارتكابها وصعوبة التحقيق فيها وفي الباعث على تنفيذها وكذلك خطورتها التي أكدت الإحصائيات بالأرقام الخسائر الناتجة عنها بعد أن هدمت الحدود السياسية والطبيعية لتصبح جريمة عبر الحدود. حتى أن خطورة هذه الظاهرة دفع بالبعض إلى القول أنها فرع مهم للجريمة المنظمة^(٤٥).

الخاصية الأولى : - الحاسوب عنصر في ارتكاب الجريمة :-

يعد الحاسوب أداة وحده الإنسان قادر على استخدامه بصورة ايجابية أو سلبية. لذا فقد يستخدم الإنسان هذه الأداة في الغرض غير الطبيعي المخصص لاستخدامها. إن وجود هذه الآلة يشتمل على وجه العموم المكونات المادية لأجهزة الحاسوب وملحقاتها وكذلك المكونات المعنوية والتي تشمل جميع الكيانات وبرامج التشغيل والتطبيق. وهذه الجريمة ذات طبيعة تقنية والسلوك الإجرامي فيها أيضاً ذا مضمون تقني. فالحاسوب هو دائماً عنصر مهم في الاعتداء مع ما يمكن أن يتعامل معه ضمن مجال معطياته^(٤٦). وهي خاصية تنفرد بها عن بقية الجرائم، ذلك أن الحاسوب العنصر المهم الذي يمكن الشخص من تنفيذ الجريمة أيًّا كان نوعها^(٤٧). إن الحاسوب وما يرتبط به من تقنيات تلعب أدواراً عديدة في هذه الجرائم، فهو إما أن يكون موضوعاً للجريمة أو هدفاً للجريمة، أو أداة تساعد في تحطيم وتطوير تنفيذ الجريمة، أو قد تكون مثالاً أو نموذجاً للجريمة^(٤٨). وتبعاً لهذا الدور تبرز أهمية هذه التقنية في هذه الجرائم.

الخاصية الثانية : - صعوبة اكتشاف الجريمة المعلوماتية والتحقيق فيها وإثباتها : - تتميز الجريمة المعلوماتية بقلة عدد الحالات المكتشفة فعلياً إذا ما قورن ذلك مع الجرائم التقليدية. ويرى البعض أن الأسباب راجعة إلى اتسامها بالطابع التقني الذي يضفي عليها الكثير من التعقيد. بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجنى عليهم من فقدان ثقة عملائهم^(٤٩). فضلاً عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قليلة جداً^(٥٠). وقد تكون أحياناً فقدان الثقة والإيمان في قدرة هيئات تطبيق القانون في حل هذه الجرائم^(٥١).

هذه الجرائم غالباً ما تكون فيها الأدلة نادرة وقد لا تكون مادية تشير إلى الفاعل، وإنما كيانات منطقية تكون ضمن فضاء الحاسوب الآلي يمكن بسهولة إخفائها والتخلص منها. وانعدام الأثر الخارجي المرئي يعود إلى أن تنفيذ الجريمة يتم أصلاً بالبنية التحتية الكهربائية، حيث تتغير وتتحدى الأرقام والدلائل والمعلومات من ذاكرة الحاسوب^(٥٢).

ومن جانب آخر فإن الجاني ينفذ هذه الجريمة عن بعد، وهو لا يكون متواجداً في مسرح الجريمة خاصة إذا تم ذلك عن طريق شبكة الانترنت. فالمفهوم الجغرافي لمكان ارتكاب الجريمة يكون منعدماً وبشكل يزيد من صعوبة ملاحقة مرتكبي هذه الجرائم^(٥٣).

كما أن الكثير من البيانات المطلوب تدقيقها تفوق القدرات البشرية عند مراجعتها، فذاكرة الحاسوب تحوي الكثير من المعطيات بمحنة أنواعها، وقد تلجأ سلطات التحقيق في اغلب الأحيان إما لحجز هذه المعطيات لتدقيقها ومراجعتها في سبيل الوصول إلى دليل، وهو أمر فيه الكثير من الصعوبة، أو التغاضي عن هذه المعطيات كلياً على أمل الحصول على اعتراف من المتهم أو الاستعانة بالخبرات الفنية على أبعد حد^(٥٤).

إن نقص الخبرات الفنية لدى سلطات التحقيق أيضاً من الأسباب المهمة لهذه الطبيعة، إذ يتطلب التحقيق في هذه الجرائم قدرًا كبيراً من المهارات والمعلومات التقنية، ولعل قلة خبرات سلطات التحقيق هو أحد أسباب الإخفاق في اكتشاف هذه الجرائم^(٥٥)، بل والأكثر من هذا أحياناً الحق ينافي الدليل عن خطأ لقلة الدراسة في كيفية التعامل مع هذه التقنية^(٥٦).

إن فقدان الأدلة والخبرة بهذه التقنيات يعيق قدرة المحقق على إجراء تفتيش ناجح، بل وحتى اعتبار أن الحاسوب ربما يكون مصدراً للدليل في الجريمة^(٥٧). لذا فإن انشاء وحدات تحقيق بهذه الجرائم وتزويدها بالأنواع الأكثر شيوعاً لتقنيات الحاسوب لتكون قادرة على إجراء تفتيش على نحو متخصص يكون أمراً ضرورياً^(٥٨).

ويمكن معالجة هذا النوع من الإشكاليات عن طريق الاستعانة بالخبرات الفنية إضافة إلى إتباع إجراءات أمنية مناسبة ومنح الجهات المعنية سلطات كافية. وبالفعل فقد انشئت بعض الدول وحدات متخصصة في مجال التحقيق في هذه الجرائم. وعلى سبيل المثال، السويد التي كانت من أوائل البلدان التي قد استحدثت دوريات مراقبة الانترنت للكشف عن بعض الجرائم كالقرصنة ونشر المواد الإباحية المتعلقة بالأطفال والوصول إلى مرتكبها^(٥٩).

أخيراً، فإن عدم كفاية النصوص الجرائية الموضوعية والإجرائية في اغلب دول العالم لمواجهة الجريمة المعلوماتية يكون أيضاً سبباً مهماً. فقد يتم اكتشاف الجريمة والإبلاغ عنها والقبض على مرتكبها ولكن السلطات غير قادرة على مواصلة التحقيق لقلة أو انعدام النصوص القانونية التي تعالج هذه القضايا، فضلاً عن أنها تكون غير قادرة على إحالة المتهم للقضاء لعدم وجود النصوص أو عدم كفيتها لشمول تلك الواقعة^(٦٠).

الخاصية الثالثة : - الطبيعة الدولية للجريمة المعلوماتية :-

تقليدياً، الجريمة والعقوبة تكونان إلى حد كبير محلية، إقليمية أو وطنية. اليوم، اختلافات كثيرة تواجهنا مصاحبة للخاصية العابرة للحدود لهذه الجريمة^(٦١). إن التقنيات الحديثة وما صاحبها من تقدم في مجال الاتصال ألغى الحدود الجغرافية بين الدول بحيث أن الجريمة المعلوماتية تخطت حدود الدولة التي ترتكب فيها لتتعدى أثارها إلى كافة البلدان على مستوى العالم^(٦٢). فالتقنيات المتصلة عالمياً قد جعلت هذه الجريمة مشكلة عابرة للحدود^(٦٣). فالطبيعة العالمية للجريمة تمكّن الجاني من ارتكاب الجرائم في دولة ما والتي ستؤثر على المجنى عليه في دولة أخرى^(٦٤). بل والأكثر من ذلك أن الضرر الناتج عن الجريمة لم يلحق المجنى عليه داخل إقليم دولة الجاني.

خاصة أن المواد المعروضة تتعارض مع الثقافات المتلقية لهذه التقنية في الدين والعرف الاجتماعي والنظام السياسي للدولة^(٦٥).

إن من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية قضية عرفت باسم مرض نقص المناعة المكتسبة (الايدز). وتتلخص وقائعها في عام ١٩٨٩، عندما قام أحد الأشخاص بتوزيع عدد كبير من نسخ برنامج يهدف إلى إعطاء بعض النصائح حول المرض. إلا أن حقيقة هذا البرنامج يحتوي فيروس (حصان طروادة) الذي بمجرد تشغيله يتقطع جهاز الحاسوب عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان، حتى يتمكن الجني عليه من الحصول على مضاد الفيروس. وفي ٣/٢/١٩٩٠ تم إلقاء القبض على المتهم جوزيف بوب في أوهايو في USA وتقدمت UK بطلب تسليميه لحاكمته أمام القضاء الانكليزي، حيث أن إرسال هذا البرنامج قد تم في UK، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، ومن ثم توجيه إحدى عشر تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات المحاكمة للمتهم لم تستمر بسبب حالته الصحية العقلية. وآياً كان الأمر فإن هذه القضية أهميتها من ناحيتين: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية، والثانية أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج الفيروس^(٦٦).

إن الخاصية المميزة، والأكثر تعقيداً، في الميدان الدولي هو ارتكاب الجريمة عبر الحدود الإقليمية لبلدان ذات سيادة، غالباً بمجرد نقر فوق زر. فالتحول من الجريمة المحلية إلى الجريمة العالمية يثير مشاكل اختصاصية عديدة ويمكن أن يخلق عوائق للتحقيق الجنائي وتطبيق القانون^(٦٧).

لقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلاً مهماً يتعلق بتحديد الدولة التي يختص قضاها بمحالقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي أم تلك الدولة التي توجد بها المعلومات محل الجريمة أم تلك التي تضررت مصالحها نتيجة التلاعب^(٦٨). كما وأشارت هذه الطبيعة الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة

المعلوماتية، وبصفة خاصة جمع وقبول الأدلة، حيث تتبادر مواقف الدول بقبول الأدلة الناتجة من أنظمة الحاسوب الآلية^(٦٩).

لقد أشارت هذه الصفة أيضاً إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تناولتها. فيجب أن يشمل التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن التعاون يجب أن يمتد لمكافحة الجريمة المعلوماتية وهذا يقتضي أيضاً تبادل المعلومات بين الدول في هذا المجال^(٧٠).

والوسيلة المثلثى للتعاون الدولي هنا تكون عن طريق عقد الاتفاقيات الدولية^(٧١). ولكن الوصول إلى هذه الاتفاقيات يقتضى بطبيعة الحال التنسيق بين قوانين الدول لضمان مبدأ ازدواجية التحريم، سواء في مجال القواعد الموضوعية أو الإجرائية. وهذا يتم من خلال تبادل المعلومات والخبرات بشأن هذه الجريمة خصوصاً في إطار تسليم وملاحقة المجرمين، إذ تشتراك أكثر من دولة في أثار الجريمة المعلوماتية الواحدة.

وفي سبيل مكافحة الجريمة المعلوماتية، يجب على الدول التحرك في محورين: الأول داخلي بحيث تتواءم تشريعاتها الداخلية مع هذا النمط من الجرائم. والثاني دولي عن طريق عقد الاتفاقيات الدولية، حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية غياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى^(٧٢).

الخاصية الرابعة : - أضرار الجريمة المعلوماتية باللغة :-

إن العقود الأخيرة شهدت تطويراً سريعاً في المعلومات وطبيعتها وقيمتها الإنسانية والحضارية والاقتصادية والتجارية. وبعد أن أصبحت المعلومات عاملاً أساسياً ثالثاً بجوار الطاقة والمادة وصيروها إلى طاقة كامنة للمخاطر، جعلت هذه المعطيات للجرائم المعلوماتية موضوعاً وميداناً لها والتي أفرزت أثراً خطيراً على المؤسسات وأمن الدول وحقوق الأفراد الخاصة. إذ يمكن القول تقريباً أنه لا توجد مؤسسة مستثناء من هذه الجرائم^(٧٣). وبالفعل فقد تكبدت العديد من الدول والأفراد كما هائلاً من الخسائر المادية والمعنوية، ولقد كانت قطاعات التجارة،

الصناعة والمؤسسات المالية الأكثر عرضة للخسائر الناجمة عن هذه الجرائم. وهناك عوامل عديدة يعزّز إليها هذا النمو الغريب نوعاً ما في الجرائم المرتبطة بتكنولوجيا الاتصالات والمعلومات وهي: النمو التكنولوجي السريع، التوافر السهل لأدوات الجريمة وتقنيات البرمجة، سرعة الاتصالات، الدرجة العالية للإنترنت وزيادة الاعتماد على تكنولوجيا الحواسيب^(٧٤).

فمثلاً في تسعينيات القرن الماضي، أظهرت الدراسة التي قام بها معهد أمن الكمبيوتر (C.S.I) ومؤسسة أبحاث الولايات المتحدة (U.S.A research Inc.) أن عدد الاقتحامات والاختراقات لأنظمة الكمبيوتر قد سجلت زيادة بـ ١٠٠٪ عن عام ١٩٨٩، وزيادة تقدر بنحو ٤٢٪ عن جرائم أخرى غير الاختراق^(٧٥).

كما اظهر مسح اجري من قبل معهد أمن الكمبيوتر (C.S.I) في عام ١٩٩٩ أن خسائر شركة أمريكية من جرائم هذه التقنية بلغت أكثر من \$١٢٣,٠٠٠,٠٠٠ (٦٣٪). في حين اظهر مسح اجري في عام ٢٠٠٠ أن أكثر من ٩٠٪ من عينة التقرير قد اكتشفوا هجمات الكترونية. حيث وصل عدد الشركات الأمريكية المتضررة من تلك الجرائم إلى (٢٧٣) شركة بلغ مجموع خسائرها أكثر من ٢٦٦ مليون دولار^(٧٧). والجدير بالذكر أن جرائم التقنيات الحديثة تسبّب لاقتصاد الولايات المتحدة الأمريكية خسائر تقدر بـ ١١٧,٥ بليون سنوياً^(٧٨).

وبينت إحصائيات الجمعية الأمريكية للأمن الصناعي أن الخسائر التي تسبّبها هذه الجرائم للصناعات الأمريكية قد تصل (\$٦٣,٠٠٠,٠٠٠,٠٠٠)، وأن (٢٥٪) من الشركات الأمريكية تتضرّر منها، وقد أصيب (٦٣٪) من الشركات الأمريكية والكندية بفيروسات حاسوبية ووصل فقد السنوي بسبب سوء استخدام الكمبيوتر الآلي إلى (\$٥٥٥,٠٠٠,٠٠٠)^(٧٩).

أما في بريطانيا، فقد قدر اتحاد الصناعات الانكليزي الخسائر الناجمة عام ١٩٧٦ بمبلغ يتراوح ما بين ٢٥ إلى ٣٠ مليون جنيه إسترليني. وأكّد وزير التكنولوجيا البريطاني (Lord Reag) عام ١٩٩٢ بأنّ الجرائم التي تتعرّض لها أنظمة الحواسيب تضرّ بإعمال أكثر

من نصف الشركات الصناعية والتجارية في بريطانيا بتكلفة سنوية تقدر بحوالي بليون جنيه إسترليني^(٨٠). من جهة أخرى بين مركز الحاسوب الوطني البريطاني أن أكثر من ٨٠٪ من المنظمات (المؤسسات) البريطانية تعاني من اختراق أمني في السنتين الأخيرتين ما قبل عام ١٩٩٥^(٨١).

ولم تسلم بقية الدول من هذا الخطر الإجرامي، بل أن اغلب الدول التي اعتمدت في حياتها هذه التقنية هي معرضة لخسائر الناجمة عنها ومنها الدول العربية التي لم تكن بعيدة عن ذلك. فقد بينت إحصائية نشرت عام ١٩٩٧ أن خسائر الدول العربية كانت في البحرين مثلاً ٥ ملايين \$ وفي مصر ١٠ \$ مليون وفي الأردن نحو ٣ \$ مليون وفي السعودية قدرت بنحو ٣ مليون وفي الإمارات ٣ \$ مليون^(٨٢).

حالياً، في بعض البلدان التي لا تملك أي مشتكى حول هذه الجرائم ولا توجد تقارير رسمية حول معدل الجريمة، لا يعني أن مستخدمي التقنيات الحديثة فيها لا يكونون ضحايا أو فاعلين لهذه الجرائم^(٨٣). من جانب آخر، أن تقدير جسامته المشكّلة تتّنوع بشكل كبير، جزئياً بسبب التعريف المتنوعة لهذه الجريمة، التقييدات في تخمين الضرر المسبّب والصعوبات في الكشف والابلاغ. لكن بعض الدراسات تؤكد أن الخسائر تصل إلى البلايين من الدولارات سنوياً^(٨٤).

وقد حدد البعض أسباب انعدام المعلومات حول التهديدات الالكترونية إلى أسباب عديدة: (١) جميع الدول تقريباً لا تملك آليات ابلاغ مطلوبة ومتاحة في هيئات القطاع العام أو الخاص. (٢) الاهتمام القليل في الابلاغ عن التهديدات الالكترونية لأسباب تتعلق بعمليات السوق والمنافسة، بل واحياناً لا يكون هناك تنفيذ كافي لأليات الابلاغ القائمة. (٣) كثير من الدول لا تملك هيئات مدربة لمكافحة هذه التهديدات^(٨٥).

لذلك، تبرز الحاجة إلى ايجاد نموذج جيد يمكن من تقدير تكاليف الهجمات الالكترونية، والذي بدوره يكون معاقاً بعدة عوامل ابرزها: (١) الصعوبة في معرفة العدد الحقيقي للهجمات. (٢) عدم وجود دراسات شاملة تؤسس شكل صحيح الذي يمكن على الاقل أن يعطينا فكرة عن ماهية الشيء الذي نتعامل معه. (٣) عدم وجود تعاون بين مراكز الابلاغ عن جرائم

الحاسب عالمياً. (٤) عدم وجود إداريين نظام مدربين بشكل كافي قادرين على التعامل مع القضايا الناجمة عن هذه التهديدات. (٥) تكنولوجيا المراقبة البدائية^(٨٦).

أخيراً، لا يكون هناك انكار أن جرائم تكنولوجيا الاتصالات والمعلومات ستستمر في أن تكون صناعة البليارات من الدولارات مالم يتم اتخاذ التدابير اللازمة وبسرعة^(٨٧).

ثانياً :- سمات المجرم المعلوماتي :-

كان لارتباط الجريمة المعلوماتية بالحاسب الآلي والنظام المعلوماتي أثر على تمييز الجرم المعلوماتي عن بقية المجرمين.

الجرائم المعلوماتية فكرة جديدة على الفقه الجنائي نوعاً ما. ففي هذا النوع من الجرائم نحن لسنا بصدده سارق أو محتال أو مزور عادي ولكن مجرم ذو مهارة تقنية في اغلب الأحيان ودراءة بالتقنيك المستخدم في الحاسب والنظام المعلوماتي وقدر على استخدام ذلك لاختراق الكود السري لتغيير المعلومات أو لتقليل البرامج أو التحويل من الحاسيبات عن طريق استخدام هذه التقنية، فشخصية الجرم وميكانيكيه ارتكابه للجريمة له سماته الخاصة^(٨٨). وسنبحث هذا في جانبين كالتالي :-

الجانب الأول :- خصائص المجرم المعلوماتي :-

لقد حملت الجرائم المعلوماتية في طياتها طائفة جديدة من المجرمين يمتلكون سمات خاصة إضافة إلى الصفات العامة الأخرى التي توجد في الجرم العادي^(٨٩). ويترکز الاختلاف بين الجرم المعلوماتي عن بقية المجرمين في الدوافع والطوابع والسمات. وعليه يمكن أن نجمل سمات المجرم المعلوماتي في نطاق الجريمة بالآتي :-

الخاصية الأولى :- الذكاء :-

للمجرم المعلوماتي ذكاء من نوع معين ودراءة بأحدث ما وصلت إليه التقنية الرقمية في اغلب الأوقات، ولديه القدرة على التفكير وفهم العلاقات بين العناصر المكونة ل موقف ما والتكييف معه من أجل تحقيق أهدافه^(٩٠). وقد اظهرت الإحصائيات التي أجراها العديد من

الباحثين في أوروبا وأمريكا إلى أن مستوى الذكاء يرتبط بنوع الجريمة، فارتفاع مستوى الذكاء قد يدفع بعض الناس الأذكياء وخصوصاً الجرميين منهم إلى أنواع معينة من الجرائم^(٩١).

الجرم في هذا المجال يمتلك القدرة على التفكير بطرق جديدة بمعنى يكون مبدعاً، وهذا يتضمن الطلاقة والمرونة والأصالة^(٩٢) الالكترونية الرقمية، وأيضاً يمتلك القدرة على معرفة ذاته وإرضائها والقدرة على التعامل مع الأرقام واستخدامها بما يحقق أهدافه الالكترونية الإجرامية، ولديه الإمكانيّة على رؤية علاقة الأشكال أو الأشياء مع بعضها البعض في الفضاء الالكتروني^(٩٣).

الخاصية الثانية : - المهارة والمعرفة والتخصص :-

تعد المهارة المطلوبة لتنفيذ النشاط الإجرامي أبرز خصائص الجرم المعلوماتي. الكثير من مجرمي الحاسوب يكونوا بدرجة عالية ماهرين وواسعي الاطلاع وهم يصرفون الكثير من الوقت في البحث والاعداد لارتكاب جرائمهم^(٩٤). حيث يتطلب تنفيذ الجريمة بصفة عامة قدرأً من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة التخصصية أو عن طرق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين. إلا أن ذلك لا يعني ضرورة أن يكون الجرم المعلوماتي على قدر كبير من العلم أو أن تكون لديه خبرة كبيرة، بل أن الواقع العملي قد ثبت أن بعض النجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمه لارتكاب الجريمة المعلوماتية عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال^(٩٥).

وتجدر الإشارة إلى أن الجرم المعلوماتي في اغلب الأحيان يكون متخصصاً. فقد ثبت في العديد من القضايا أن عدداً من الجرميين لا يرتكبون سوى جرائم الحاسوب أي إنهم متخصصون في هذا النوع من الجرائم^(٩٦). لذا يمكن القول أنه لا يسهل على الشخص المبتدئ سوى في حالات قليلة ونادرة أن يرتكب جرائمه بطريق هذه التقنية، فالامر يبدو أنه يحتاج إلى الدقة والتخصص في هذا المجال للتغلب على القضايا التي أوجدها المتخصصون لحماية أنظمة الحاسوب كما في البنوك مثلاً^(٩٧).

الخاصية الثالثة : - الدافع والتكييف الاجتماعي :-

قد يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى انطلاقاً من الرغبة في سد التغرات التي أدت إلى التعرف عليهم وتقديعهم للمحاكمة في المرة السابقة، وقد ينتهي به الأمر مع ذلك في المرة الثانية إلى تقديمهم إلى المحاكمة^(٩٨). ومن جانب آخر، فإن الجرم المعلوماتي لا يرتكب الجريمة المعلوماتية بداعف العنف لذلك قيل أنه جرم غير عنيف وأنه ينتمي إلى إجرام الحيلة، فهو لا يستخدم العنف في ارتكاب جرائمه، وهذا النوع أصلاً من الجرائم لا يتطلب العنف للقيام به^(٩٩).

يدرك أن الجرم المعلوماتي عندما ينفذ جريمته يقصد من ورائها الحصول على بعض المكاسب المادية كمالاً أو القبول أو التحدي^(١٠٠). في المقابل، أن العديد من الجرميين يرتكبون هذه الجرائم بداعف اللهو ومحرث إظهار تفوقهم على الآلة أو البرامج المخصصة لأمن النظم المعلوماتية ويكتفوا بالتفاخر بأنفسهم وأن يظهروا لضحاياهم ضعف أنظمتهم^(١٠١). إذ أنه من الواضح أن مجرمي الحاسوب مندفعين بموجب دوافع واضحة في اغلب الاحيان والتي تمثل في الجشع، الشهوة، الانتقام والمغامرة^(١٠٢). ناهيك عن الدوافع العديدة الأخرى التي تكون وراء المخالفات التي ترتكب في هذه البيئة كالكسب المالي، الإرهاب، الابتزاز، الإضرار الخبيث^(١٠٣). وكذلك النشاط السياسي، التجسس العسكري أو السياسي أو الاقتصادي أو الصناعي، الكراهية^(١٠٤).

وأحياناً، فإن الجرم المعلوماتي يحاول من خلال ارتكاب هذه الجريمة حل مشكلة شخصية شديدة. إذ أنه في هذه الاحوال نشير إلى أن حاجة قوية تدفعهم لارتكاب الجريمة. وليس الجشع كما تصوره بعض هيئات تطبيق القانون^(١٠٥).

وعلى صعيد آخر، فإن الجرم المعلوماتي لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به^(١٠٦)، بل أنه إنسان متكيف معه ومرتفع الذكاء مما يساعده على عملية التكييف مع المجتمع، وهنا ترتكز خطورته الإجرامية التي تزيد كلما زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه^(١٠٧).

وأخيراً، يجب أن لا نستخلص من ذلك انعدام خطر الإجرام المعلوماتي بحججة عدم توافر النوايا الإجرامية. ولكن أيضاً السلوك غير الوعي يمكن أن يسبب أضراراً جسيمة حتى ولو لم يكتشف أي عداء للمجتمع. والدليل على ذلك حصول نماذج إجرامية عديدة نتيجة الجريمة المعلوماتية التي وقعت من كبار وأحداث صغار كان لها آثار خطيرة. والشخص يستطيع ارتكاب الجريمة المعلوماتية بمفرده أو من خلال تجنيده ضمن عصابات الجريمة المنظمة عن طريق شبكة الانترنت^(١٠٨). وهذه أيضاً بحد ذاتها مشكلة أخرى تستلزم الدراسة وامتناعها.

الجانب الثاني : - أنماط الجرم المعلوماتي :-

بعد أن بيننا أهم خصائص الجرم المعلوماتي CYBER CRIMINAL، نبين أهم الطوائف التي يمكن أن ترتكب هذه الجريمة. لقد اظهرت الدراسات المختلفة في هذا المجال عن وجود أنماط من مجرمي المعلوماتية، ولكن هذا لا يعني بطبيعة الحال أن كل مجرم يندرج تحت طائفة محددة فقط بل يمكن أن يكون الجرم المعلوماتي الواحد مزيجاً من أكثر من طائفة^(١٠٩). وتمثل هذه الطوائف في الآتي :-

الطائفة الأولى:- Pranksters: - وهم الأشخاص الذين يرتكبون جرائم المعلوماتية بالحيلة ضد الآخرين بدون قصد إحداث ضرر معين^(١١٠). ويندرج تحت هذه المجموعة صغار مجرمي المعلوماتية، ويقصد بهم الشباب المفتون بالمعلوماتية والحاسب، وكثيراً ما لفتوا النظر في الآونة الأخيرة عقب أفعال انتهاك غير مسمومة في العديد من ذاكرات الحاسوب الآلي. وتترافق هذه المجموعة أفعالهم عن طريق استخدام حاسبات ميكروية خاصة بهم أو بمدارسهم، وليس لهم حدود جغرافية لأفعالهم التي قد تصل إلى أنظمة ومراكز بعيدة عن أماكن تواجدهم^(١١١).

الطائفة الثانية:- Hackers: - فهي تضم الأشخاص التي تهدف الدخول إلى أنظمة الحاسوب الآلي غير المصرح لهم الدخول إليه وكسر الحواجز الأمنية الموضوعة لهذا الغرض، بهدف اكتساب الخبرة أو بداع الفضول أو مجرد إثبات القدرة على اختراق هذه الأنظمة، غالباً ما يعودون لاختراقها بعد تطوير الحماية فيها مما يبعث فيهم روح التحدي للاختراق^(١١٢).

الطائفة الثالثة: - **Malicious hackers**: أشخاص هدفهم إلحاق خسائر بالجني عليهم دون أن يكون الحصول على المكاسب المادية من ضمن أهدافهم. ويندرج تحت هذه الطائفة الكثير من صانعي الفيروسات الذين يقومون بها^(١١٣). وفي استطاعتهم اختراق الأنظمة والقيام بعمليات حسابية لا تنتهي فيقوم الحاسب بالتنفيذ والحساب حتى تنفذ مصادره من ذاكرة رئيسية وثانوية مما يؤدي إلى انهاي النظام المعلوماتي^(١١٤).

الطائفة الرابعة: - **Software crackers**: وهذه الطائفة متخصصة بفك شفرات البرامج وليس تخريب الشبكة، إذ يقومون بخرق مقاييس الحماية التي تمنع من استنساخ البرامج أو ما يعرف بكسر رقم التسلسل **serial number** . وينضوي تحت هذه الفئة الأشخاص الذين يقومون بهذه العملية بقصد تحقيق الربح المادي^(١١٥).

الطائفة الخامسة: - **Career criminals**: مجموعة من المجرمين يقصدون من وراء نشاطهم الإجرامي الحصول على الربح المادي بطريقة غير مشروعة، وفي الغالب تعمل هذه الطائفة ضمن عصابات منظمة هدفها تحقيق الربح المادي مثل عصابات سرقة السيارات. ويمكن القول أن نسبة هذا النمط قليلة مقارنة ببقية الفئات كون أن العمل الإجرامي في هذا المجال يتطلب نوعاً من المهارة الفنية وهو لا يتوافر عادة في اغلب هذه العصابات^(١١٦).

الطائفة السادسة: - **Extreme Advocates**: وهي مجموعة تقوم بتوظيف المعارف التي اكتسبوها في مجال المعلوماتية لتمرير طروحات تخدم توجههم سياسياً أو ايديولوجياً، وهذا يقودهم إلى اختراق الواقع الفردية أو الجماعية لتغيير المعلومات التي تحتوي عليها. ومن الأمثلة على ذلك قيام أحد الجماعات الإرهابية في أوروبا باسم **The Red Brigades** بتدمير ما يزيد عن ٦٠ مركزاً للحسابات الآلية خلال الثمانينيات لفت الأنظار إلى أفكارهم ومعتقداتهم^(١١٧).

الطائفة السابعة : - **Mercenaries** : وهم أولئك الذين يستخدمون من قبل أفراد ومؤسسات أو حكومات لاقتحام برامج ونظم حاسوبية معينة لتدمیرها أو سرقة ما فيها أو تشويهها مقابل مبلغ من النقود^(١١٨).

وأخيراً، فإنه أي كانت درجة الدقة في رسم حدود كل طائفة من الطوائف التي ينتمي إليها الجرم المعلوماتي فأنها لا تخرج عن ثلات بواتر وراء تنفيذ الجرم المعلوماتي الجريمة المعلوماتية^(١١٩). فهو أما باعث تشتراك فيه مع غيرها من جرائم الأموال وهو تحقيق الربح المادي، أو باعث تتميز به عن غيرها من الجرائم ويتمثل بالرغبة في الدخول إلى أنظمة الحاسوب ليس لغرض سوى التسلية أو إثبات الخبرة والقدرة التي يتمتع بها الجاني، أو باعث يتمثل في الرغبة بالإضرار بهذه الأنظمة سواء كان بداع الإضرار بمؤسسة التي ينتمي إليها الجاني أو الأنظمة أو بداع المنافسة. كما أنه ينبغي الاشارة هنا، إلى أن هذه الطوائف غير مستقرة ولن يستوي الوحيدة في بيئه التكنولوجيا، إذ بالإمكان القول أن هذه الأصناف قابلة للتتجدد بقدر أي تطور يتم في مجال التقنيات الحديثة وهذا بالتأكيد ناتج عن الصلة بين مجرمي هذا النمط والتكنولوجيا الحديثة التي أن صح القول البيئة التي ينشأ فيها هؤلاء.

المبحث الثاني

تصنيف الجريمة المعلوماتية وأهمية الحاسوب إليها

بدايةً أن واقع الجريمة المعلوماتية قد افرز الكثير من الصور سواء كانت تقليدية ترتكب بأسلوب جديد أو جرائم حديثة مبتكرة والتي كانت نتاج انتشار هذه التقنية والامكانيات التي توفرها^(١٢٠). وفي مقابل تعدد الجريمة المعلوماتية كان للحاسوب أهمية كبيرة جداً في تنفيذها وهي ناشئة عن علاقة هذا الجهاز - مع ما يتصل به - بطبيعة هذه الجرائم كونه أحد الركائز الأساسية لارتكابها، لذلك فقد ارتبط وجود هذه الجريمة بوجود هذه التقنية وما يتصل بها من مفاهيم وأنظمة المعلومات وشبكات الاتصال. لذا سنبين أهم صور هذه الظاهرة التي تعد جريمة القرن الحالي. ثم سنوضح أهمية تقنية الحاسوب في ارتكاب الجريمة.

المطلب الأول : تصنيف الجريمة المعلوماتية

هناك حقيقة لا يمكن لأي شخص أن ينكرها وهي أنه رغم المحاولات التي بُرِزت في إطار هذا المشروع إلا أنها نوعاً ما عجزت عن احتواء تصنيف واضح وصريح ومحدد للجريمة المعلوماتية بسبب الطبيعة المستعصية لها والتي على برهنت أنها لا يمكن وضعها بين قوسين، كونها ظاهرة لها القابلية على التجدد وفقاً لمتغيرات التكنولوجيا المستمرة، فكلما ظهرت تقنية ظهرت موازاتها نمط إجرامي. والتي تفرض في ذات الوقت على القانون مواجهتها من خلال التحليل وإيجاد التكيف المناسب ووضع الحلول الملائمة. لذا فإن فهم أنواع هذه الجرائم إلى حد ما سيساعد تطبيق القانون وفي تقديم رؤية للاستراتيجيات الحقيقية^(١٢١). وعليه سنحاول باختصار عرض أهم المحاولات لتصنيف أنواع هذه الظاهرة وفي محورين :-

المحور الأول : - المحاولات الفقهية :-

كثيرة هي المحاولات الفقهية الجادة في مجال إيجاد تصنیف دقيق لأنواع هذه الظاهرة من خلال اعتماد المعيار الملائم لذلك والذي يكون الأساس للتقسيم.

فقد قسم رأي فقهي^(١٢٢) الجرائم الناشئة عن هذه التقنية إلى ثلاث طوائف رئيسة تتعلق الأولى بجرائم الحاسوب الاقتصادية وتشمل الاحتيال المعلوماتي الذي يقوم على التلاعيب في نظم المعاجلة للحصول بغير حق على أموال وأصول أو خدمات، والتجسس المعلوماتي في نطاق قطاع الأعمال الذي يقوم على اختراق نظام الحاسوب بهدف توظيف واستغلال ما يتم التوصل إليه من معلومات، وقرصنة برامج الحاسوب. والإتلاف المعلوماتي سواء تعلق بالمكونات المادية أو المعنوية. والدخول غير المصرح به إلى نظام الحاسوب. وسرقة الخدمات أو الاستعمال غير المصرح به لنظام الحاسوب. والجرائم التقليدية في نطاق قطاع الأعمال.

أما الطائفة الثانية فتشمل الجرائم المتعلقة بانتهاك الحياة الخاصة وتشمل استخدام بيانات شخصية غير صحيحة بهدف تغييرها أو محوها من أناس غير مرخص لهم أو جمع أو معاجلة أو نشر بيانات غير صحيحة من قبل أفراد مرخص لهم. كذلك جمع وتخزين بيانات صحيحة على نحو غير مشروع. والإفشاء غير المشروع للبيانات الشخصية السورية وإساءة استخدامها أو غير السورية إذا ترتب عليها ضرر^(١٢٣).

بينما الطائفة الثالثة فهي تلك الجرائم التي تهدد المصالح القومية أو السلامة الشخصية للأفراد، وتشمل الجرائم الماسة بالمصالح العليا للدولة كالوصول إلى معلومات حساسة تتعلق بالأمن القومي كالمخابرات والدفاع، أو تمس دولة أخرى. وتشمل أيضاً جرائم المعلومات الماسة بالسلامة الشخصية للأفراد كالالتلاعيب بأنظمة حركة الطيران أو حياتهم كاستخدام الحاسوب في المستشفيات مثلاً^(١٢٤).

في حين أن هذه الجرائم وفقاً لرأي آخر في الفقه تقسم إلى نوعين:- جرائم سایر مرتکبة بواسطة مجرمين عنيفين أي جرائم عنيفة مثل (cyber terrorism). وجرائم اللا عنيفة أو محتملة العنف كالتعدي على ممتلكات الغير (cyber trespass)^(١٢٥).

وقسم جانب من الفقه هذه الجرائم إلى ثلاث طوائف رئيسية أدرج تحت كل منها مجموعة من الأفعال غير المشروعة، مراعياً في هذا التقسيم وصف الجوانب المتنوعة للجريمة المعلوماتية

وفي تعريف قضايا القانون الجنائي الموضوعي الذي يكون مأخوذاً بعين الاعتبار في الفئات التالية^(١٢٦):

أولاًً - الدخول والاستعمال غير المصرح بهم لنظام الحاسوب وتشمل الدخول غير المصرح به لنظام الحاسوب بنية ارتكاب جريمة معلوماتية أخرى والاعتراض غير المشروع لنظام الحاسب، والأفعال غير المشروعة المتصلة بالمعلومات الشخصية المعالجة ألياً، والاستعمال غير المصرح به لنظام الحاسب الآلي.

ثانياً - الاحتيال المعلوماتي وسرقة المعلومات وتشمل التلاعب في المعلومات المعالجة ألياً بنية تحقيق ربح مادي غير مشروع، والحصول غير المشروع على المعلومات المعالجة ألياً بنية استخدامها في أغراض غير مشروعية، والحصول غير المشروع على المعلومات المعالجة ألياً، وقرصنة الحاسيب الآلية.

ثالثاً - الجرائم التي يساعد الحاسوب على ارتكابها وتشمل التخريب والإتلاف للمكونات المادية أو المعنوية للحاسوب، والاستعمال غير المشروع للحاسبات لإعاقة المستخدمين الشرعيين لنظام الحاسب عن الوصول إلى المعلومات التي يحتوي عليها، واستخدام أنظمة الحاسب للاعتداء على سلامة وأمن الأفراد، والتهديد بتدمير مكونات الحاسب لابتزاز المجنى عليهم، والإفشاء غير المشروع للمعلومات المؤمن إليها بمقتضى وظيفة، وصناعة وبيع المعدات والأدوات التي تساعده على ارتكاب جرائم الحاسب مثل إعداد البرامج الخبيثة (الفيروسات).

وجزء آخر من الفقه حاول تقسيم الجرائم المعلوماتية الاقتصاديةأخذاً بنظر الاعتبار التطور المستمر الذي يطرأ على الجريمة المعلوماتية بصفة عامة وما يدخل في إطار هذه الجرائم وما يخرج عنها، باعتماد الدور الذي يقوم به الحاسوب كأساس لتقسيم الجرائم المعلوماتية. فباختلاف هذا الدور وتتنوعه تتعدد طوائف الجريمة المعلوماتية وبالتالي فإن طوائف الجريمة تقسم إلى الجرائم التي تعتمد في تنفيذها على الحاسوب. والجرائم التي يكون فيها الحاسوب محل للعمل الإجرامي. وطائفة الجرائم التي يرتبط وجودها بوجود الحاسب^(١٢٧).

وفي هذا السياق، قسم آخرون هذه الجرائم إلى ثلاث طوائف فرعية هي:- الجرائم التي يكون الحاسب فيها هدف النشاط الاجرامي مثل (Hacking) و(Malicious Software). والجرائم الموجودة حالياً هي التي يكون فيها الحاسب أداة مستخدمة لارتكاب الجريمة مثل الاختيال المعلوماتي (Fraud) وانتهاك حقوق الملكية الفكرية (Copyright Infringement). والجرائم التي فيها يكون استخدام الحاسب جانب عرضي لارتكاب الجريمة لكن قد يحمل دليل الجريمة مثل الرسالة في تحقيقات جريمة قتل^(١٢٨).

ونجد قسماً آخر يقسم هذه الجرائم إلى فئتين رئيسيتين هما:- الجرائم التي تكون على الأكثر تكنولوجية في الطبيعة مثل جرائم الفايروسات. والجرائم التي تملك عنصر بشري بصورة واضحة أكثر مثل جرائم الإرهاب^(١٢٩).

في حين صنف آخرون هذه الجرائم إلى اربع فئات هي:- جرائم ضد الاشخاص مثل (Cyber Stalking). جرائم ضد أموال الاشخاص كإتلاف الحاسب. جرائم ضد المنظمات سواء كانت حكومية أو خاصة أو شركات أو مجتمع الافراد كالإرهاب. وجرائم ضد المجتمع مثل المواد الاباحية للأطفال (Child Pornography)^(١٣٠).

والجدير بالذكر أن المحاولات العديدة من جانب الفقه في وضع تصنيف لهذه الجرائم بالخصوص يكون أحد العناصر المهمة لمكافحة هذه الجرائم وخطوة مهمة في هذا الاتجاه^(١٣١). المحور الثاني :- المحاولات الدولية لتصنيف الجرائم المعلوماتية:-

تفرض الجرائم المعلوماتية بطبيعتها الحاجة إلى تعاون دولي من أجل مكافحة هذه الظاهرة، وهذا راجع بصفة أساسية إلى الطبيعة الدولية التي سبق الإشارة إليها^(١٣٢). فوجود هذه التقنيات مع ما قدمته من خدمات في مجال الاتصال كشبكات الانترنت التي ربطت العالم في كافة المجالات كالجامعات والبنوك وشركات الطيران وغيرها من مؤسسات البنية التحتية، أصبح التعاون الدولي من أجل حل المشكلات الجديدة الناجمة عن التطور التكنولوجي أمر ضروري. والحقيقة يمكن إجمال المشكلات التي تفرض التعاون الدولي في مكافحة الجريمة المعلوماتية في عدم وجود تعريف عام متفق عليه للجريمة المعلوماتية، وعدم وجود اتفاق عام حول أشكال السلوك التي

تدرج تحت وصف الجريمة المعلوماتية، والنقص الكبير في خبرات السلطات التي تتعامل مع هذه الجريمة، وندرة الاتفاقيات الدولية التي تشجع التعاون الدولي في هذا المجال، وعجز الاتفاقيات الموجودة بالفعل عن مراعاة الطبيعة والمتطلبات الخاصة بها^(١٣٣).

وبناء على ما تقدم، يبرز الشعور بضرورةبذل الجهود لإزالة الصعوبات التي تعترض مكافحة الجريمة المعلوماتية من خلال إيجاد تعريف متافق عليه للجريمة المعلوماتية وتذليل الإشكالات المختلفة لهذه الجريمة من خلال محاولة تقسيمها^(١٣٤).

فلقد بدأ اهتمام منظمة التعاون الاقتصادي والتنمية OECD بالحاسب الآلي والمشكلات التي يثيرها خاصة بعد التهديد المعلوماتي للخصوصية منذ عام ١٩٧٧، واستمرت جهود المنظمة فيتناول ظاهرة الجريمة المعلوماتية، وفي سبتمبر عام ١٩٨٥ شكلت لجنة لدراسة الجريمة المعلوماتية، التي قامت بإجراء مسح لهذه الجريمة في الدول الأعضاء، ومن خلال إعداد دراسة مقارنة لقوانين هذه الدول، وقد أسفر عمل اللجنة عن صدور تقرير نشر عام ١٩٨٧ تحت عنوان جرائم الحاسوب الآلي (تحليل لأنظمة القانونية المختلفة)، ولقد خلصت اللجنة في تقريرها إلى تصنيف مجموعة من الأفعال يمكن أن تشكل جرائم معلوماتية، وتعد قاسم مشترك بين الاتجاهات المختلفة للدول ويمكن إيجازها فيما يلي :-

- ١ - إدخال معلومات إلى نظام الحاسوب، أو تعديل أو حشو معلومات موجودة بالفعل على نحو غير مشروع، وذلك بنية تحويل الأموال أو الممتلكات التي تشملها هذه المعلومات.
- ٢ - إدخال معلومات إلى نظام الحاسوب، أو تعديل أو حشو معلومات موجودة بالفعل، أو اعتراض نظام الحاسوب الآلي، وذلك بنية إعاقةه عن أداء وظيفته.
- ٣ - استغلال برامج الحاسوب تجاريًّا وطرحها في الأسواق، وذلك انتهاكًا لحقوق مالك هذه البرامج (قرصنة البرامج) والحصول غير المشروع على المعلومات.
- ٤ - الدخول أو الاعتراض غير المصرح بهم لنظام الحاسوب التي تتم عمداً، سواء كان هذا الدخول أو الاعتراض بنية ارتكاب جريمة لاحقة عليه أم لا.
- ٥ - الاستعمال غير المصرح به لنظام الحاسوب^(١٣٥).

أما على مستوى أوروبا فنجد تقسيم الجرائم المعلوماتية متجسدًا في الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت لعام ٢٠٠١^(١٣٦)، التي كانت نتيجة العمل من أجل وضع إطار عام لتصنيف هذه الجرائم أو على الأقل وضع قائمة الحد الأدنى محل التعاون الدولي في حقل مكافحة الجريمة المعلوماتية، وهو جهد تقوده دول أوروبا ولكن بنفس الوقت بمساهمة من قبل بعض الدول الأخرى^(١٣٧)، والجرائم المعلوماتية وفق هذه الاتفاقية تصنف إلى الآتي :-

- ١- الجرائم التي تستهدف عناصر (السرية والسلامة والمwoffورية) المعطيات والنظم وتضم الدخول غير القانوني وتدمير المعطيات واعتراض النظم وإساءة استخدام الأجهزة^(١٣٨).
- ٢- الجرائم المرتبطة بالحاسوب وتضم التزوير والاحتياج المرتبط بالحاسوب^(١٣٩).
- ٣- الجرائم المرتبطة بالمحظوظ وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللا أخلاقية^(١٤٠).
- ٤- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة، وقرصنة البرمجيات^(١٤١).

بينما نجد لجنة المجتمعات الأوروبية (المفوضية الأوروبية) في أحدى الرسائل الصادرة عنها بخصوص التوجه نحو سياسة عامة بشأن مكافحة الجريمة (المعلوماتية) السiberانية قد أوضحت أن هذه الجرائم تتمثل في ثلاثة فئات من الأنشطة الجنائية وهي:- جرائم تقليدية ترتكب باستخدام الشبكات الالكترونية كالاحتياج المعلوماتي (Fraud). وجرائم المحظوظ اللا قانوني التي تتمثل في النشر غير الأخلاقي والقانوني للمواد على الوسط الالكتروني مثل جرائم سوء استخدام المواد الجنسية للأطفال (Child sexual abuse material) وجرائم العنصرية (Racism) وغيرها. أما الفئة الثالثة تشمل جرائم فريدة بالنسبة للشبكات الالكترونية كالمجتمعات ضد انظمة المعلومات أو المنظمات أو الافراد^(١٤٢).

وقد حددت لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (الاسكوا) هذه الجرائم من خلال الإرشاد الخامس الخاص بالجرائم السiberانية^(١٤٣)، بالآتي:- (١) جرائم التعدي على المعلوماتية كجريدة اعتراض البيانات. (٢) جرائم التعدي على الانظمة المعلوماتية كالولوج غير المشروع لنظام المعلوماتي. (٣) جرائم اساءة استعمال الاجهزه او البرامج المعلوماتية.

(٤) جرائم التعدي على الاموال والمعاملات كالتزوير والاحتيال المعلوماتي أو السرقة والاختلاس بوسائل معلوماتية. (٥) جرائم الاستغلال الجنسي كجريمة عرض مواد اباحية لقاصرین بواسطة نظام معلوماتي. (٦) جرائم التعدي على الملكية الفكرية للأعمال الرقمية كجريمة تقليل امضاء المؤلف أو ختمه. (٧) جرائم البطاقات المصرفية والنقود الالكترونية كجريمة تقليل بطاقة مصرفية. (٨) الجرائم التي تمس المعلومات الشخصية كجريمة افشاء معلومات ذات طابع سري. (٩) جرائم العنصرية ضد الانسانية بوسائل معلوماتية كجريمة نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية. (١٠) جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية كجريمة ترويج الكحول لقاصرین على الانترنت. (١١) الجرائم المعلوماتية ضد الدولة والسلامة العامة كجريمة تعطيل الاعمال الحكومية بوسائل معلوماتية^(٤٤).

التقسيم المقترن للجرائم المعلوماتية :-

عرضنا سابقاً ابرز المحاولات الفقهية والدولية لتصنيف الجرائم المعلوماتية التي أرادت أن تضع بالقدر المستطاع إطار نستطيع من خلاله تصنيف نتاجات هذه الظاهرة في الوقت الراهن حسب تقديرنا لذلك.

ولابد من الإشارة هنا، أن الاعتداء على المكونات المادية للحاسب لا يثير تلك الصعوبة لأنه بالإمكان تدارك المسائلة من خلال تطبيق النصوص التقليدية في قانون العقوبات العراقي وقانون حماية حق المؤلف بصورةه الحالية، كون أن الاعتداء يرد على أشياء مادية ملموسة يمكن أن تشملها النصوص القائمة وعلى سبيل المثال السرقة أو التخريب أو الإتلاف. وبالتالي لا تكون هناك مشكلة لأنه ينطبق والمفاهيم التي تقوم عليها هذه النصوص وهي النظرة المادية التي سبق الإشارة إليها وإيضاحها في إطار تعريف هذه الجريمة، إذ لا تثير أي جدل في تطبيق هذه النصوص وإخضاع العمل الجرمي لها.

ومن جانب آخر، أن محاولة وضع تصنیف دقيق للجرائم المعلوماتية تأتي ضمن سياق الجهود الرامية إلى مكافحتها من خلال وضع تصور شامل ومحدد لها، وكذلك يدخل في سياق

القانون الجنائي الخاص، لأنه يركز على تحديد الجريمة ووضع المفهوم الملائم لها والذي يتناسب مع ميزات هذه الجريمة التي أثبتت صعوبة احتوائها في إطار معين نتيجة لذلك.

والقول بخلاف ذلك لا يحمل أي نوع من الصحة، وأن وضع الجريمة المعلوماتية وما ينشأ عنها في قانون أو قسم تحت تسمية القانون المعلوماتي كلام مبالغ فيه نوعاً ما حالياً لأنه بالنتيجة أي عمل يهدد أي مصلحة يحميها القانون تعد جريمة تنطوي تحت مظلة القانون الجنائي الخاص ولكن ليس بصورةه الحالية، وإنما وفق شكل وصيغة القانون الجنائي المرن والقابل للاستجابة للتطورات الحية المستمرة وألا فلا أهمية لكلامنا هذا ونكتفي بالشروع في البحث لإيجاد تسمية وقسم جديد يكون قادراً على أداء هذه المهمة.

إن وضع تصنيف للجريمة المعلوماتية يساعد على تقديم الاقتراح متكملاً نسبياً للمشرع العراقي عند توافر الإرادة لديه في الاستجابة لمتغيرات العصر التكنولوجي. ومن بعد، صياغة النص الشامل والمرن لاستيعاب كل جديد في إطار الجريمة المعلوماتية، ذلك أن عدم وجود النص أو جموده يؤدي إلى هروب الجاني من يد العدالة وبالتالي الإفلات من العقاب. كما أن خطورة الفعل الجريمي المرتكب وأضراره السلبية والكبيرة على النواحي الاجتماعية والاقتصادية والصناعية والتجارية، يهدد كيان وجود الدولة والمجتمع العراقي وبالشكل الذي يضعف ثقة المواطن العراقي بالتقدم التقني، يدعو إلى ذلك.

وبقصد ذلك نأخذ بعين الاعتبار ما يأتي :-

١- إن الجرائم المعلوماتية هي ظواهر حديثة نسبياً ظهرت على الساحة الدولية نتيجة التعامل اليومي باستخدام التقنيات الحديثة في كافة مجالات الحياة.

٢- إن الجريمة المعلوماتية ومن خلال ارتباطها مع التقنيات الحديثة أكسبتها طابع التغيير المستمر، فلديها القدرة على الظهور بأساليب جديدة كلما كان هناك ظهور لأي تطبيق حديث في هذا المجال إذ هي الانعكاس السلبي لهذه التقنيات.

٣- إن الجريمة المعلوماتية خرقت كافة القواعد التي تحكم مكانية الجرائم التقليدية. إذ أنها ظاهرة لا تعترف ولا تتقيد بالحدود الجغرافية المحددة للفعل الاجرامي. وبالتالي فإن اثارها

تتعدي إلى دول أخرى، والتي لا تنحصر في مكان تنفيذ الجريمة. وهو ما يفرض مبدأ عالمية القانون الجنائي.

وعليه، ارتأينا تقسيم الجرائم المعلوماتية وفقاً مبدأ من و قادر على استيعاب أي مستجد في إطار هذه الجريمة وفي ذات الوقت تكون قد غطينا ما موجود حالياً من أعمال تعد من صور الجريمة المعلوماتية. وبشكل عام يمكن القول بوجود أربع طوائف رئيسية للجرائم المعلوماتية وهي:-

الطاقة الأولى : - الجرائم الواقعة على الأشخاص.

الطاقة الثانية : - جرائم ضد الثقة والمصلحة العامة للمجتمع.

الطاقة الثالثة : - الجرائم الواقعة على الأموال.

الطاقة الرابعة : - الجرائم الماسة بأمن الدولة والمنظمات والهيئات.

إن هذا التقسيم وأن كان يبدو للوهلة الأولى أنه تقليدي لكنه التقسيم الذي نستطيع من خلاله أن نشمل جميع صور الجريمة المعلوماتية الحالية أو التي يمكن أن تولد في المستقبل.

أما المعيار المعتمد في هذا التقسيم فهو معيار غير حديث أيضاً وإنما هو معيار معروف، استطاع حسب رأينا أن يلم جميع الجرائم المعلوماتية، وهو معيار المصلحة محل حماية القانون. ذلك أن مفهوم المخل القانوني للجريمة المعلوماتية يتمثل بالمصلحة القانونية التي سعى المشرع إلى حمايتها من الاعتداء، وحسب هذه النظرة - وفي تقديرنا - على سبيل المثال، فإن المخل الفعلي يختلف عن المخل القانوني لجريمة التزوير. فالمخل الفعلي لهذه الجريمة هنا يكون الحاسوب والنظام المعلوماتي وما يحتويه من معلومات وسندات الكترونية، بينما المخل القانوني لجريمة التزوير هنا هو الاعتداء على المصلحة القانونية التي منحها المشرع الحماية وهي الثقة العامة بهذه الأنظمة والمستخرجات.

وعليه يمكن القول، أن هناك تمييزاً بين المخل المباشر لجريمة التزوير وبين المصلحة الخمية التي تكون الغاية والحكمة من تحريم الفعل. بالمعنى الأدق نحن نعتمد على المصلحة المقصودة من سبب التجريم للفعل، وهي المصلحة التي يحميها القانون من عبث المجرمين وتمثل بالثقة العامة.

إن السبب الذي دفع إلى اعتماد هذا المعيار يتركز في الآتي :-

- ١- التداخل الموجود بين الأفعال الإجرامية في ظل الظاهرة المعلوماتية. حيث أن الجرائم المعلوماتية دائمًا تتركز في كونها أفعال تستخدم الحاسوب والنظام المعلوماتي، وهي في هذا المجال تشير الكثير من التداخل فيما بينها بحيث نجد أن الفعل الواحد يمكن أن يوصف بأكثر من صورة. إن جرائم المعلوماتية تنطوي في أغلب الظروف، ومهما اختلفت في تصنيفها، على أفعال مشتركة تدخل في تكوين كل منها. بمعنى آخر، أنه في حالة إذا ما كانت الجريمة منظوية على أفعال مشتركة فإن هذه الأفعال تشكل كل واحدة بصورة منفصلة جريمة معاقب عليها. وهي تخضع لسلطة المحكمة التقديرية في ذلك.
- ٢- إن هذا التصنيف يبتعد عن اعتماد الوسيلة في تحديد الجريمة. أي بمعنى آخر، إننا لا نعتمد على الوسيلة في تصنيف الفعل المعلوماتي الجرمي، إذ أن الوسيلة لا يمكن أن تدخل في هذا المجال. ولكن هذا لا يعني أن الوسيلة لا تكون لها علاقة في بيان خطورة الفعل المرتكب. على العكس من ذلك، إذ أن في ظروف معينة تكون الوسيلة المرتکبة ظرفاً مشدداً للعقوبة التي يستحقها الجاني ولكنها ليست المعيار في تكيف فعل الجاني. فمن البديهي أن تكون هناك أدلة لارتكاب الجريمة المعلوماتية فلا يمكن تصور وجود الجريمة المعلوماتية بدون الحاسوب والنظام المعلوماتي، وطبعاً أن يختلف دور هذه الأدوات وأهميتها بالنسبة للفعل من حيث كونها فعالة أو لا وهو ما سنوضحه لاحقاً.
- ٣- إن هذا التقسيم يبتعد عن استخدام الباعث لارتكاب الجريمة في تقسيم الجرائم المعلوماتية. بمعنى أدق لا يهمنا في هذا الأمر فيما إذا كان قصد الجاني هو الحصول على المكتب المادي أو مجرد الإضرار بالغير أو مجرد التسلية أو إثبات القدرة أو المهارة، فما دام فعله ينطوي على تحديد لأحد المصالح الأساسية لوجود المجتمع فإن هذا الفعل يعد جريمة معاقب عليها قانوناً بغض النظر عن السبب الذي دفع الجاني إلى ارتكاب هذا الفعل. بمعنى لا يكون له تأثير كبير في تصنيف الجرائم. لكن لا ننكر أهمية هذا الباعث في تشديد أو تخفيف العقوبة دون أن يكون ذلك في تصنيف الجرائم.

٤- إن نتيجة الاعتداء بطبيعة الحال أمر مهم جداً. ذلك أن عدم تحديد هذه النتيجة يجعل هناك صعوبة في وصف الفعل أو الطائفة التي ينتمي إليها، وبالتالي إهدار العلاج الأنسب لمكافحة هذا النوع من الجرائم. كالسرقة مثلاً التي تصنف ضمن طائفة الجرائم الواقعة على الأموال كونها ترد على مال ملوك للغير، فتصنيف هذه السرقة راجع إلى كونها تهدد ملكية الفرد للمال بالزوال، حتى وإن كان هذا المال معنوي وفق ما نتبناه من توسيع مفهوم المال ليشمل المعلومة وما تحمل في جوانبها من بيانات وبرامج لها قيمة اقتصادية ووفق الاتجاه الفقهي الذي ينادي بهذا.

النتيجة التي يمكن الوصول إليها، من خلال هذا التقسيم باعتماد هذا المعيار، تتلخص في أن الجريمة المعلوماتية مكونة من (سلوك غير مشروع يقوم به شخص معين مستخدماً الحاسب والنظام المعلوماتي كمحل مباشر وفعلي للاعتداء يهدد أحد المصالح الأساسية التي سعى المشرع لحمايتها والتي تمثل أحد المركبات لوجود المجتمع الإنساني).

وعليه، تبرز لنا أهمية تقسيم الجريمة المعلوماتية في ضوء المعيار والمبررات السابقة للفصل بين ما يقع ضمن الجريمة المعلوماتية أم لا. وكذلك كمحاولة لوضع تصنيف دقيق ومن قادر على استيعاب أي نوع مستجد في هذا الإطار. خاصة وأن للحاسوب أهمية متباعدة في ارتكاب هذه الجريمة، وهذا نابع من الدور الذي يلعبه هذا الجهاز والنظام المعلوماتي في تنفيذ الجريمة المعلوماتية. وهذا ما سنبينه في المطلب التالي.

المطلب الثاني : أهمية تقنية الحاسب للجريمة المعلوماتية^(١٤٥)

كثيراً ما يرتبط الحاسوب ونظام المعلومات بارتكاب الجريمة المعلوماتية^(١٤٦). خاصة وأن الجرم المعلوماتي لا يمكن له أن ينفذ فعله المصنف ضمن هذه الجرائم إلا بعد الاستعانة بهذه التقنية التي تحمل أهمية كبيرة في هذا المجال.

إن أهمية الحاسب وانظمه المعلوماتات في تنفيذ الجريمة المعلوماتية يبرز من خلال الدور الذي يمكن أن يلعبه في تنفيذ الجريمة، وكذلك من خلال الإمكانيات التي يمكن أن يقدمها الحاسوب للمجرم المعلوماتي للوصول إلى هدفه الإجرامي^(١٤٧).

لذا سنبحث هذا الموضوع في شقين هما :-

الشق الأول :- دور الحاسوب في الجريمة المعلوماتية :-

يكون للحاسوب ونظام المعلومات أهمية في تنفيذ الجريمة المعلوماتية. وتبين هذه من خلال الدور الذي يتمتع به الحاسوب في تنفيذ الجريمة وبطبيعة الحال مع ما يتصل به من أنظمة وتقنيات. لكن في نفس الوقت فإن هذا الدور متذبذب في تنفيذ الجريمة وحسب ما يأتي :-

١ - دور الحاسوب كواسطة في تنفيذ الجريمة :-

هنا لا يمكن تصور وجود الجريمة المعلوماتية إلا بعد وجود الحاسوب وتكنولوجيا المعلومات، كونها كأداة رئيسية في تنفيذ العمل الإجرامي المكون للجريمة المعلوماتية، نظراً لما يحتويه من معلومات وأصول تكون هي المادة الأولية لصنع الجريمة. فالحاسوب ليس مجرد وسيلة لتسهيل النتيجة الإجرامية أو مضاعفة جسامتها، بل يمكن القول أن المعلومات والبيانات التي ينطوي عليها تشكل المركب الأساس لارتكاب الجريمة المعلوماتية^(١٤٨).

والاعتقاد بأن هذه الجريمة تتسم بقدر كبير من التعقيد وإنها تتطلب جانبي لديه مهارات تقنية بالغة التعقيد هو اعتقاد خاطئ. ف الصحيح أن الجريمة المعلوماتية بصفة عامة لها طابع تقني وأن الجرم المعلوماتي لديه نوع من المهارات التقنية، إلا أن ذلك لا يعني درجة معقدة من هذه التقنية، فالحواسيب آلات بسيطة قادرة على القيام بعمليات معقدة ولا يستلزم تشغيلها بطريقة مشروعة أو غير مشروعة سوى قدر معقول من الخبرة الفنية في هذا المجال^(١٤٩).

والرأي لدينا هو العكس، بدليل أن هذه الجرائم تنطوي على درجة من التعقيد في أحياناً معينة، وعلى أمور تقنية صعبة نوعاً ما لا يمكن للشخص العادي استخدامها^(١٥٠)، وإنما كان بالإمكان السيطرة على هذه الظواهر من لحظة نشوئها. الواقع يظهر خلاف ذلك حيث قلة عدد الجرائم المكتشفة منها يؤكد صحة كلامنا. ومن جانب ثانٍ الكبير من الدراسات أكدت على أن هذه الظاهرة هي ظاهرة تقنية بحد ذاتها لها سلبيات على المستوى القانوني ولا يمكن للشخص العادي أن يتحقق في هذه الجرائم أو أن يتوصلا إلى النتيجة التي يرغب الوصول إليها ما لم تكن لديه خلفية بالجوانب الفنية لهذه الظاهرة، وذلك بسبب طبيعتها المعقدة التي تحتاج إلى

معرفة تقنية في إطار ذلك . في نفس الوقت، لا نقول أن هذه القاعدة مطلقة ولكن إلى جانب الجرائم المعلوماتية المقدمة تقنياً هناك أيضاً جرائم بسيطة يمكن للشخص أن يقوم بها بمجرد إحاطته بقدر معقول من الأمور التي تمكنه من استعمال هذه التقنية وعلى سبيل المثال ارسال الرسائل غير المرغوب فيها. خلاصة قولنا أن الجرائم المعلوماتية عموما هي ظواهر تقنية لها انعكاسات سلبية على الجانب القانوني وهذه الظواهر هي عموماً فنية ودرجة التعقيد هي صفة لها ولكن ليست مطلقة فهي على الأكثرب تحتاج إلى دراية ومهارة فنية في التعامل معها.

ويكون للحاسوب هذا الدور في تنفيذ جريمة الاحتيال المعلوماتي وسرقة المعلومات والتزوير المعلوماتي وكذلك التجسس المعلوماتي. فالحاسوب يلعب دوراً رئيسياً لارتكاب العمل الإجرامي بما يتضمنه من معلومات باللغة الأهمية كتلك الخاصة بالجيش والمعلومات الصناعية وكذلك الإفشاء غير المشروع للمعلومات المبرمج آلياً عن طريق العاملين، لما تتسم به هذه المعلومات من أهمية وسرية بالغة في كثير من الأحيان^(١٥١).

بالرغم أن هذه لا تكون جرائم جديدة، فقد يكون من الصعوبة محاكمة هذا النوع من الأنشطة تحت القوانين القائمة . فعلى سبيل المثال القانون المختص بالسرقة، ربما لا يشمل سرقة الأموال غير المادية عندما الفعل الملام يتكون من نسخ الأموال بدلاً من سرقتها بالكامل. لذلك، فإن السلطات المختصة تجد من المستحسن أما تبني تشريع جديد يعالج الجرائم في هذه الفئة أو تعديل التشريع القائم لضمان الكفاية لهذا الغرض^(١٥٢).

٢- الدور العرضي للحاسوب في ارتكاب الجريمة :-

تتكون هذه الفئة من جرائم فيها استخدام الحاسوب أو نظام الحاسوب يكون عرضياً لارتكاب الجريمة، فهنا الحاسوب يلعب دوراً ثانوياً في الجريمة^(١٥٣). أي أن دور الحاسوب في هذه الجرائم يكون غير أساسي في تنفيذ الفعل^(١٥٤)، فالحاسوب هنا يستعمل من أجل ارتكاب الجريمة كونه أكثر سرعة ودقة في الوصول إلى نتيجة إجرامية مؤكدة و يجعل الجريمة أكثر صعوبة في التعرف والتتبع^(١٥٥). ومع أن هذا الدور قد لا يكون واضح بصورة كافية في إتمام العمل الجرمي فإن ذلك لا يمنع من أنه دور غير أساس، ولا يمنع أيضاً من تجريم الفعل من كونه جريمة معاقب

عليها قانوناً. وحيث أن الأساس في كل حالة هنا بوضوح تام مغطاة بالجرائم السابقة بالكامل^(١٥٦)، فالقانون الجنائي الموضوعي متخصص في هذه الحالة يكون غير ضروري. لكن قانون اجرائي جديد يتعامل مع هذه الجرائم التي تقع ضمن هذه الطائفة يكون أمراً مطلوباً^(١٥٧). بالخصوص، أن أحد جوانب الجريمة يكون الحاسب مع ما يرتبط به من أنظمة تتطلب بطبيعة الحال قواعد خاصة تتفق وطبيعة هذه الجرائم وما اجراءات استرجاع المعلومات، في هذه الحالة، إلا دليل واضح على هذه الحاجة. وبالتحديد إذا نظرنا إلى الحاسب في هذه الفئة كدليل على الجريمة أكثر من اعتبار آخر. إذ ربما بشكل ملحوظ، أنه كان اشراك الحاسب الذي قاد إلى القاء القبض على الجناة^(١٥٨).

ويتمثل هذا الدور في جريمة الابتزاز وهي جريمة تقوم على التهديد للحصول على مبلغ معين من المال أو أي شيء آخر مقابل عدم افشاء الجاني إسراً تتعلق بالمجني عليه أو عدم المساس بأشياء أو أشخاص لهم أهمية خاصة لديه. والحقيقة أن الحاسب هنا يسهل تنفيذ هذه الجريمة بما يحتويه من قدرات، خاصة من خلال الاستعانة بهذه الوسيلة في كتابة خطابات التهديد للمجني عليهم أو نشر معلومات شخصية، فالدور هنا ليس مؤثراً في ارتكاب الجريمة. وامثلة هذا النوع عديدة، كغسيل الاموال والعمليات البنكية غير القانونية وتسجيلات الجريمة المنظمة. بمعنى آخر أن هذه الجرائم يمكن أن تحدث بدون الحاسب، فالأنظمة هنا ببساطة تسهل الجرائم^(١٦٠).

٣- دور الحاسب الآلي باعتباره هدف لجريمة المعلوماتية :-

لقد رأينا سابقاً أن دور الحاسب قد يكون عنصراً أساسياً لتنفيذ الفعل الجرمي وقد يكون دور غير أساسي في الجريمة. بينما في حالات كثيرة أظهرها الواقع أن الحاسب وما يرتبط من أنظمة يكون بحد ذاته هدف للأعمال الإجرامية. وبغض النظر عن هدف الجاني من ارتكاب هذا الفعل سواء كان القصد الحصول على المكاسب المادي أو مجرد الإضرار بالضحية أو قد يكون مجرد إظهار مهارة الجاني في مجال تكنولوجيا المعلومات.

والحقيقة هنا لابد من توضيحيها هي أن الحاسوب محل الاعتداء لا يشمل مكوناته المادية. لأن الاعتداء ضد مكونات الحاسب المادية لا يندرج ضمن نطاق مشكلة الجريمة المعلوماتية وتخرج عنها، كونها أعمال إجرامية خاضعة للنصوص التقليدية القائمة^(١٦١). باعتبار أن الاعتداء في هذه الصورة وارد على شيء مادي يمكن لصيغة النصوص الحالية أن تتکفل بحمايتها كتخريب أو إتلاف أي مال مادي عائد للغير.

فالذى يعنينا هنا هو إذا حدث الاعتداء ضد أحد مكونات أو عناصر الحاسب المعنوية التي يتكون منها كالمعلومات أو البرامج. إذ تثير هذه المسألة صعوبة تمثيل في عجز النصوص القائمة عن معالجتها كجريمة الإنلاف في القوانين المختلفة، نظراً للطبيعة المادية التي تتطلبها هذه النصوص في المال الذي يقع ضده الإنلاف. في حين أن المعلومات المترجمة ألياً هي بمثابة نبضات كهربائية تفتقر إلى الطبيعة المادية إلا في الحالات التي يؤدي فيها إنلاف المكون المعنوي إلى إنلاف مكون من المكونات المادية للحاسوب. وكذلك الحال بالنسبة إلى الأفعال التي تسبب عرقلة النظام للحاسوب وتنعه من أداء مهمته، وهو ما يطلق عليه إعاقة أنظمة الحاسوبات^(١٦٢).

إذ من الواضح في هذا المجال أن المظاهر لاعتبار الحاسوب هدفاً في حقل التصرفات غير القانونية، عندما تكون سرية وسلامة وتوافر في أنظمة المعلومات هي موضوع الاعتداء^(١٦٣). بمعنى أن توجه الهجمات للحاسوب عن طريق معلومات الحاسوب وخدماته بقصد المساس بالسلامة والتكامل والقدرة والكفاءة لأنظمة للقيام بعملها، وهدف هذا النمط بشكل خاص المعلومات المخزنة داخله بهدف السيطرة على عمل النظام دون تخويل ودون أن يكون مقابل للاستخدام وسرقة خدمات أو وقت الحاسوب أو المساس بسلامة المعلومات وتعطيل خدمات الحاسوب وغالبية هذه الأفعال تتضمن ابتداء الدخول غير المصرح إلى النظام المهدى.

إن الجرائم التي تقع في هذه الفئة تعالج بشكل صحيح أكثر كجرائم جديدة والتي لا يمكن أن تحاكم بسهولة في ظل القوانين القائمة ولذلك تتطلب تبني قوانين تستهدف هذه الانشطة بصورة معينة^(١٦٤). ذلك أنها جرائم (معلوماتية) ساير حقيقة (صحيحة) لم تكون موجودة قبل ظهور التكنولوجيا^(١٦٥).

الشق الثاني : - أهمية تقنية الحاسوب في الجريمة المعلوماتية : -

تبرز العلاقة بين الحاسوب والأنظمة المعلوماتية من جهة والجريمة المعلوماتية من جهة ثانية، في كون أن الحاسوب عبارة عن أداة تعمل وفق أنظمة تنفذ وتعالج البيانات والمعلومات التي يتم إدخالها إلى الحاسوب لتقوم بعد ذلك بمعالجتها آليةً وفق ما هو مطلوب وبناء على إيعازات توجه إليه لتحقيق غايات معينة وفق استخدامات محددة يرغب في تفيذها الشخص مصدر الأوامر.

عليه، سنبحث هذه المسالة لبيان مدى العلاقة بين الجريمة المعلوماتية وهذه التقنية وكلاسي : -

أولاًً : - أهمية الحاسوب في صياغة بيانات ارتكاب الجريمة المعلوماتية : -

كان لا يستطيع الحاسوب فيما مضى من الوقت التمييز بين خطوط البشر المختلفة^(٦٦). أما الآن فقد أصبح للحاسب استخدامات نتيجة للمزايا التي قدمها هذا الجهاز تمكنه من القيام بهذه الوظيفة. ولكن يجب أن لا ننسى في ذات الوقت، أن هذا الجهاز إنما هو يقوم بتنفيذ جملة من الأوامر عن طريق البيانات المدخلة إليه ووفقاً لأنظمة تشغيلية وتطبيقية تتعلق بعملية إدخال ومعالجة واستخراج البيانات.

فالحاسب يكون من مجموعة من أجهزة متكاملة مع بعضها البعض لغرض تشغيل ومعالجة البيانات المدخلة وفقاً لبرنامج موضوع مسبقاً للحصول على النتائج المطلوبة^(٦٧). وهو في نفس الوقت يمثل في المراحل التي تكون فيها جهاز الإدخال الذي يترجم البيانات إلى إشارات مفهومة من قبل الحاسب^(٦٨). وهناك تقنيات خاصة بصياغة البيانات والمعلومات المستخدمة في الجريمة ومن هذه التقنيات آلات تشغيل البطاقات^(٦٩)، وآلات تشغيل الأشرطة^(٧٠). وتوجد أيضاً طريقة لوحة المفاتيح وهي منتشرة على نطاق واسع جداً وهي لوحة متصلة بالحاسب تؤدي إلى إدخال البيانات والمعلومات أو البرامج إلى الحاسوب لتنفيذها ومعالجتها آليةً. وأيضاً توصل العلم الحديث إلى طرق جديدة لإدخال المعلومات والبيانات وهي برنامج الكتابة اليدوية الرقمية^(٧١). وكذلك هناك تقنية الصوت، حيث يستطيع الحاسوب بالتعرف على بصمة المتكلم، وهي بدائل عن استخدام الرقم السري حيث يستطيع صاحب الحاسوب جعل صوته الوحيدة القادر على التعامل معه^(٧٢). وهناك أيضاً الكثير من التقنيات في هذا المجال مثل القلم

الالكتروني إذ يمكن من خلاله الكتابة بصورة مباشرة على شاشة الحاسب وغيرها من التقنيات والتي تظهر بفعل الجهد المتواصلة التي تبذلها الشركات في هذا المجال.

ومن جانب آخر، هناك انظمة وتقنيات تتولى معالجة البيانات المدخلة وفق الاوامر والاياعات المحددة لأداء وظيفة معينة من اجل الوصول إلى النتائج التي من اجلها ادخلت البيانات. واجدير بالذكر في هذا السياق، أن هذه البرامج تختلف تبعاً للوظيفة التي يمكن أن تؤديها فمنها ما يكون تشغيلي يتصل بعمل الحاسب واخرى تتصل بمعالجة وتنفيذ البيانات وهناك برامج تتصل بعمليات انتاج المخرجات وفق صيغ متعددة. وهناك برامج صممت خصيصاً لأغراض الاتصال ونقل وتبادل البيانات والمعلومات.

ثانياً : - داعي استخدام الحاسب في ارتكاب الجريمة المعلوماتية :-

للحاسِب داعي استخدام عديدة جعلت منه أداة للتوسيع وفتح مجال جديد للإجرام وضع القوانين أمام ضرورة إيجاد حلول تشريعية لذلك . إن داعي استخدام الحاسِب هي الطاقة التخزينية والتي تعد من أهم أسباب استخدامه في تنفيذ الجريمة، إذ لو لا هذه الطاقة لما كان هناك جريمة اعتداء على هذه المعلومات بالسرقة والإتلاف على أقل تقدير، والتي اثارت المشاكل القانونية المترتبة على إمكانية تزوير المستندات^(١٧٣).

فالحاسِب أصبح لديه القدرة على تخزين المعلومات كما في ذاكرة الإنسان، فهو يستوعب تلك المعلومات سواء كان ذلك في وحدة التخزين الداخلية أو وحدات التخزين الخارجية. يضاف إلى ذلك، السرعة الفائقة سواء في استرجاع المعلومات أو معالجتها في جميع الحالات والتي أصبح استخدام الحاسِب من مقومات أي عمل فيها. وأيضاً عامل الدقة لديه، إذ يسترجع ويختزن ويعالج ما يملئ عليه مع الإمكانيات والمو Rosenberg في التعديل وكيف يشاء مالك الحاسِب. وغيرها من المزايا التي لم يقدمها أي جهاز آخر فهو حقاً أحدث ثورة في جميع الحالات.

ثالثاً : - حاجة تقنية الحاسب للعامل البشري :-

للحاسوب صلة وثيقة بال مجرم المعلوماتي، والتي تظهر في أن تشغيل الحاسوب لا يتم من تلقاء نفسه إذ لابد وأن يتم ذلك من قبل شخص له ال دراية والخبرة والمعرفة في مكونات الحاسوب المادية والمعنوية^(١٧٤).

إن الحاسوب ورغم الدقة والذكاء والسرعة في معالجة البيانات، إلا أنه آلة عميماء حسب التعبير الدقيق الذي اخترناه، إذ أنه لا يمكن لها أن تقوم بأي عمل أو مهمة ما لم تتلق الأوامر والبيانات والمعلومات الالازمة لتنفيذ أي وظيفة معينة. وهذا بطبيعة الحال يفترض وجود العامل البشري الذي يتطلب وجوده بمقتضى تلك الحاجة التي يعاني الحاسوب من عدم توافرها. خصوصاً، وأن البدء بتنفيذ أي عمل اجرامي يتطلب منذ البدء تدخل العامل البشري في إنشاء التهديدات الالكترونية التي تكون في اغلبها برامج معينة تصمم خصيصاً لهاجمة المعلومات المقصودة والمخزنة ضمن النطاق الالكتروني.

ولقد اشرنا سابقاً، أن الشخص الذي يتعامل مع هذه الآلة لا نقول أنه يتمتع بذكاء مطلق ولكن على الأقل له القدرة والمعرفة الكافية بجوانب عمل الجهاز والأنظمة المتصلة به والمفردات التي يتعامل معها. فال مجرم المعلوماتي لا يستطيع على سبيل المثال اختراق أي نظام معلوماتي مصرفي أو مالي إلا بعد استخدام جهاز الحاسوب، كون أن هذا الجهاز هو الأداة التي يمكن من خلاله الدخول إلى النظام المقصود، وينفس الوقت جميع ما يستلزم تشغيل هذه الآلة من برامج وأنظمة. فالحاسوب الطريق المضيء للمجرم المعلوماتي الذي يحيط علما بجوانب إدارته بصورة معقولة على أقل تقدير . خصوصاً، وأن كتابة البيانات التي يتم الاعتداء عليها لا تكتب بلغة حية^(١٧٥)، بل تكتب عن طريق لغة تكون عبارة عن مجموعة من القواعد والمعطيات المتعارف عليها والتي تشكل في نهاية الأمر لغة الحاسوب والنظام المعلوماتي. فإذاً هي علاقة تبادلية بين تكنيات وانظمة الحاسوب والعامل البشري إذ لا يمكن تصور وجود احدهما دون الآخر في نطاق الاجرام الالكتروني.

الخاتمة

إن تحديد مفهوم ومحفوظ هذه الظاهرة يعد من أساسيات السياسة الجنائية التي تهدف إلى مكافحة الجريمة المعلوماتية المتزايدة، كذلك فإن هذا الأمر يسهل من عملية المواءمة بين القوانين المختصة بهذا الشأن كونه يوحد الأسس التي عليها هذه الاستراتيجية تقوم سواء على المستوى الوطني أو الإقليمي أو الدولي.

إن هذه الظاهرة جل ما يميزها أنها تتميّز بالحداثة والمرنة والقابلية على التطور تبعاً لتطور التكنولوجيا. فلم نجد هناك اتفاق بين المهتمين بما على مصطلح واحد لها، فكل جانب يستخدم المصطلح الذي يراه مناسب وفق أسباب معينة تعكس وجهة نظر ذلك الجانب الفقهى أو التشريعى. وعلى العموم أننا نجد، وفقاً للمتغيرات التي ترتبط بهذه الجريمة، أن مصطلح جرائم المعلومات أو تكنولوجيا المعلومات هو الأفضل من بين المصطلحات التي شاع استخدامها على كافة الأصعدة حاليًا، فهي تتمثل في السلوكيات التي تتعلق بالمعلومات المعالجة أليًا. وتبعاً لما تقدم، نجد أيضًا هناك خلاف كبير بشأن تحديد المضمون الذي يتمثل في تحديد مفهوم ذلك المصطلح. وبالتالي، كان هناك وجهات نظر متعددة حول التعريف الدقيق لمدلولات هذا المصطلح ضيقاً واسعاً وفق المعيار المعتمد في ذلك التعريف. مع ذلك فقد وجدنا أن أفضل ما يمكن أن يعرف به مصطلح الجريمة المعلوماتية بأنها كل سلوك غير مشروع يتضمن القيام بعمل أو الامتناع عن عمل، يكون فيه الحاسوب والنظام المعلوماتي (وما يرتبط بهم) عنصر في ارتكاب الاعتداء، يتربّ عليه تحقيق مصلحة غير مشروعة للفاعل (الجاني) أو الحق ضرر بالغير.

وحيث أن الجريمة المعلوماتية تميّز عن بقية الجرائم التقليدية المعروفة، إن صح القول، فإن هذا الأمر بطبيعة الحال راجع إلى الخصائص التي تتمتّع بها هذه الجريمة. وهذه الخصائص تتمثل في أن الحاسوب والأنظمة التقنية عنصر في تنفيذها، لذلك فإن كشف الجريمة المعلوماتية والتحقيق فيها واثباتها يكون أمراً صعباً إلى حد معين. وما يزيد أمر ذلك صعوبة أنها ظاهرة كسرت الحواجز الجغرافية وتغلبت على جميع القواعد التي تحكم مفهوم المكانية للجريمة، ولذلك فهي جريمة لا تعترف بالحدود. فقد نجد كل عنصر من عناصر الجريمة متحقق في مكان ما أو إقليم

دولة معينة، وبالتالي كانت الأضرار والخسائر التي تسببها هذه الجريمة عالية جداً ومتزايدة بصورة مستمرة إذا ما قورنت بالجرائم التقليدية.

ونتيجة لما تقدم، فإن الشخص الذي يرتكب هذه الجرائم يكون نوعاً ما متميزاً عن مجرمي الجرائم التقليدية. فنحن ليس أمام سارق أو محظوظ أو مزور عادي وإنما أمام ما يدعى بال مجرم المعلوماتي الذي إضافة إلى خصائص الجرم العادي نجده يتمثل في نوعاً من الذكاء ودرأة بأحدث ما وصلت إليه التقنية الرقمية، التي تكون البيئة لممارسة نشاطه الاجرامي. ناهيك عن، أن لديه المهارة المطلوبة لتنفيذ النشاط الاجرامي الذي يكون نابعاً من امتلاكه قدرأً من المعرفة والمهارة التي قد يكتسبها جراء دراسته أو خبرته العملية بهذا المجال. وفي اغلب الأحيان، نجد أنه يتميز بدوافع متنوعة ما بين الانتقام أو المكسب المالي أو الفضول أو التحدى أو الإرهاب أو الابتزاز أو الانشطة السياسية ... الخ. وبالتالي فإن هؤلاء مجرمين نجدهم يوصفون بسميات خاصة ومحددة ترتب عليه وجود طوائف عديدة لهم تختص كل فئة بممارسة انشطة معينة كالقراصنة أو صانعي الفايروسات أو مقلدي برامج وغيرهم.

من جانب ثالث، أن الواقع لهذه الجرائم قد افرز جرائم مبتكرة جديدة لم تكن معروفة من قبل أو جرائم تقليدية ترتكب بأسلوب جديد. وقد بذلت في هذا الإطار جهود كبيرة من أجل تصنيف الجرائم المعلوماتية سواء على مستوى المجهود الفردي للفقهاء أو على مستوى المنظمات الدولية أو الإقليمية. وحيث أن الجرائم المعلوماتية قد أثبتت أنها جرائم لا يمكن حصرها بين قوسيين ونتيجة الخصائص المشار إليها سابقاً، فإنها تصنف إلى أربع طوائف هي:- جرائم ضد الأشخاص، وجرائم ضد الثقة والمصلحة العامة، وجرائم ضد الأموال وجرائم ضد امن الدولة والمنظمات والمؤسسات. وبطبيعة الحال، ينطوي تحت كل طائفة مسميات عديدة تتمثل انشطة جرامية تخالف البناء الصحيح للمجتمع وتحدد وجوده. وهذا التقسيم نابع من مبدأ المصلحة التي سعى المشرع إلى حمايتها. لذلك، فإننا حاولنا وضع تصنيف قادر على استيعاب أي مستجدات في هذا الإطار ومتفهم لوضعية هذه الجرائم، خصوصاً وأنها ترتبط بالحاسوب وتكنولوجيا المعلومات الذين تكون لهم أدواراً متباعدة في تنفيذ الجريمة. أن دور الحاسوب مع ما

يرتبط به يتزدّد ما بين دور اساسي، عليه يعتمد تنفيذ الجريمة باعتباره أداة فعالة في هذا المجال، إلى دور هامشي أو عرضي يسهل من ارتكاب الجريمة ليس إلا، حيث أنها تتم حتى بدونه. وقد يكون هذا الدور كهدف للنشاط الاجرامي لما تحتويه هذه التقنية من مواد تكون هي الموضوع لتنفيذ الجريمة. وأن انتشار هذه الانماط بطبيعة الامر تتطلب وجود قانون اجرائي جديد قادر على التعامل مع القضايا الاجرامية التي تثار في ظل هذه الجرائم التي يكون أحد جوانبها الحاسب. ولكن في نفس الوقت فإن قانون موضوعي يكون أمراً مطلوباً في ظل الفئة الاولى والثالثة فقط.

إن الامكانيات التي يتتيحها الحاسب والأنظمة المرتبطة به جعلت منه أهمية كبيرة في الجريمة سواء من خلال صياغة البيانات التي تكون الاساس في تنفيذها، وهذا بطبيعة الحال يستلزم وجود العنصر البشري الذي يعتبر العامل القادر على الاستخدام والتحكم في هذه التقنية سلباً أو ايجاباً.

الهواش

– (١) ينظر:

H. Jahankhani and Ameer Al-Nemrat, "Examination of Cyber-criminal Behaviour", International Journal of Information Science and Management, Special Issue January / June, 2010, Available at <http://188.136.184.17/ojs/index.php/ijism/article/view/135/121> (07/02/13) .P.42.

– (٢) انظر بنفس المعنى :

Deng-Yiv Chiu, Tien-Tsun Chung and Chen-Shu Wang, "Attacking and defending perspective of e-Crime behavior and psychology: A systemic dynamic simulation approach", 2009 Fourth International Conference on Innovative Computing, Information and Control, P.1036. Available at: <http://ieeexplore.ieee.org/Xplore/guesthome.jsp> (12/12/12).

– (٣) انظر :

W. Cole Durham, Jr. and Russell C. Skousen, "The Law of Computer-Related Crime in the United States", the American Journal of Comparative Law, Year: 1990 Volume: 38. Available at: <http://www.jstor.org/stable/840559>. (12/10/12).P.557.

– (٤) انظر :

Raluca Georgiana, "Borderless Crime - Computer Fraud", Database Systems Journal, Year: 2012 Volume: III Issue: 1 P.49. Available at: <http://www.dbjournal.ro> .

– (٥) انظر

Robert W.K Davis and Scott C. Hutchison, "Computer Crime in Canada: An Introduction to Technological Crime and Related Legal Issues", Thomson Canada Limited, 1997, Canada, P.2.

– (٦) نائلة عادل محمد فريد – جرائم الحاسوب الآلي الاقتصادية – مطابع الحلبي الحقوقية –

ص ٢٧.

انظر :

Pieter Kleve, Richard De Mulder and Kees van Noortwijk, "The definition of ICT Crime, Computer Law and Security Review", The International Journal of Technology and Practice, Year: 2011 Volume: 27 Issue: 2. P.164. Available at: www.sciencedirect.com , (٢٢/١٢/ 2012).

- (٧) انظر:

Jonathan Clough, “Principles of Cybercrime”, 1st Ed, Cambridge University Press, UK, 2010, P.9.

- (٨) انظر :

Na Jin – Cheon, Wu Hao, Ji Yong and Tay Mia Hao, " Analysis of computer crime in Singapore using Local English Newspapers", Raman than Mani Kandan, Nanyang Technological University, online available at: <http://www.las.org.sgsjlim>. (11/11/2011). And look at Ronald B. Standler, “computer crime”, online available at: <http://www.rbsz.com/ccrime.htm>. (11/11/2011). And see: Joseph Migga Kizza and others, “Ethical and Social Issues in the Information Age”, 3rd Edition, Springer-Verlag London Limited, 2007, P.240.

- (٩) انظر :

Warren B. Chik, “Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore”, P.4. Available at: www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc . (20/01/13).

- (١٠) انظر :

Martin Wasik, “Crime and the computer”, Oxford University press, USA, 1991, P.3.

(١١) احمد كيلان عبد الله صقر - الجرائم الناشئة عن إساءة استخدام الحاسوب - ماجستير - جامعة بغداد - كلية القانون - ٢٠٠٢ - ص ٢٩ - ٣٠ .

- (١٢) انظر :

Paul Hunton, “The growing phenomenon of crime and the internet : A cybercrime execution and analysis model”, Computer Law & Security Review: The International Journal of Technology and Practice, Volume 25, Issue 6, November 2009, P. 529, available at www.sciencedirect.com. (22/12/2012). And see: The Convention on cybercrime, December 21, 2001. <http://www.coe.int> . Also see: Sarah Gordon and Richard Ford, “On the definition and classification of cybercrime”, Journal in Computer Virology, Year: 2006 Volume: 2 Issue: 1, P.13. Available at: <http://link.springer.com>. (12/12/12).

(١٣) انظر :-

Warren B. Chik, op. cit. P.5.

(١٤) انظر :-

Pieter Kleve and others, op. cit. P.162.

(١٥) محمد سامي الشوا - ثورة المعلومات وانعكاساتها على قانون العقوبات - مصر - ٢٠٠٣

F.Guerin,Maitiser l informatique , aspects juridiques,fiscaux ,Soiciaux , ed Delmas P.A.1.

(١٦) ينظر :- سليمان احمد فضل - الموجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت) - دار النهضة العربية - ٢٠٠٧ - القاهرة - ص ١٧ ; مصطفى محمد موسى - أساليب إجرامية بالتقنية الرقمية - الطبعة الأولى - مصر - ٢٠٠٣ - ص ٥٦ .

(١٧) انظر :-

Jonathan Clough, Op. cit. P.9.

(١٨) لاحظ على سبيل المثال قانون دولة الامارت العربية المتحدة ومشروع القانون الجرائم المعلوماتية العراقي لسنة ٢٠١٠ .

(١٩) انظر :-

Sarah Gordon and Richard Ford, op. cit. P.13.

(٢٠) هشام محمد فريد رستم - قانون العقوبات ومخاطر تقنية المعلومات - مكتب الآلات الحديثة - ١٩٩٢ - ص ٢٩ وهو يشير إلى الفقيه الالماني Tiedemann .

(٢١) انظر :-

Leslie D .Ball, computer crime in "The information technology revolution", Cambridge, 1985, PP. 543-544.

(٢٢) محمد الأمين البشري - بحث (التحقيق في جرائم الحاسوب الآلي) - مقدم إلى مؤتمر القانون والكمبيوتر والانترنت - مايو ٢٠٠٠ - كلية الشريعة والقانون - دولة الإمارات - ص ٦ .

(٢٣) مشار إليه لدى هشام فريد رستم - مرجع سابق - ص ٣٠ .

- (٢٤) عبد الرحمن عبد العزيز الشنيفي – امن المعلومات وجرائم الحاسوب الآلي – طبعة أولى –
الرياض – ١٩٩٥ – ص ٢٨ .
- (٢٥) انظر :-

Sarah Gordon and Richard Ford, Op. Cit. P.14.

– (٢٦) انظر :-

COMMISSION OF THE EUROPEAN COMMUNITIES: “Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime”, Brussels, 26.1.2001, COM (2000) 890 final, P. 12. Available at: <http://europa.eu/>. (23/07/12).

– (٢٧) انظر :-

Nicholas Thomas, “Cyber Security in East Asia: Governing Anarchy”, Asian Security, vol. 5, no. 1, 2009, P.7 .Available at <http://www.tandfonline.com/>.(03/02/13).

– (٢٨) انظر :-

Martin Wasik, op. cit. P.3.

– (٢٩) انظر :-

Richard Totty & Anthony Hardcastle, “Computer-related crime”, Chris Edwards, Nigel Savage and Ian Walden, “Information Technology and the law”, 2nd Ed, Macmillan publishers, UK, 1990, P.142.

(٣٠) عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت –
دار الكتب الوطنية – مصر – ٢٠٠٥ – ص ٥ وهو يشير إلى

Michael Alexander , “Computer Crime” ,Ugly secret for business, Computer world ,Vol. XXIV, No. 11, 1990, pp. 1, 4; p.104.

(٣١) هدى حامد قشقوش – جرائم الحاسوب الالكتروني في التشريع المقارن – القاهرة –
١٩٩٢ – ص ١٥ .

(٣٢) محمد محي الدين عوض – جرائم نظم المعلومات (الكمبيوتر) – الرياض – ١٩٩٣ –
ص ٢٧ .

(٣٣) عبد الفتاح بيومي حجازي - مرجع سابق - ص ٦ وهو يشير إلى David Thompson, "Current trend in computer control crime", Computer quarterly, Vol.9, No.1- 1991, p.2.

(٣٤) المصدر اعلاه وهو يشير إلى Artur Solaz, "Computer related embezzlement", Computers security, Vol .6, No.1, 1987, p. 52.

- (٣٥) انظر :

JUDGE STEIN SCHJØLBERG & AMANDA M. HUBBARD, "HARMONIZING NATIONAL LEGAL APPROACHES ON CYBERCRIME", The Paper Was Prepared for the ITU WSIS Thematic Meeting on Cybersecurity, June 2005, P.4. Available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf. (30/06/12). And they are referring to Stein Schjolberg, "Computers and Penal Legislation – A Study of the Legal Politics of a new Technology", CompLex 3/86, Universitetsforlaget, Norway (1983).

(٣٦) عبدالله يوسف - التقنية والجرائم المستحدثة - بحث مقدم في الندوة العلمية (الظواهر المستحدثة وسبل مواجهتها) المنعقدة في تونس ١٩٩٩/٦/٣٠ - ٢٨ - ص ٢٦ .

- (٣٧) انظر :

Mansoor Al-A`ali, "Computer Crime and the Law from an Islamic Point of View", Journal of Applied Sciences, Year: 2007 Volume: 7 Issue: 12; P.1559; Available at: <http://docsdrive.com/pdfs/ansinet/jas/2007/1558-1565.pdf> . (31/05/12).

(٣٨) هشام رستم - مرجع سابق - ص ٣٣ وهو يشير إلى التعريف الذي صاغه الفقيه (Sheldon Hecht)

And also in the same meaning see: Donn B. Parker, "The Dark Side of Computing: SRI International and the Study of Computer Crime", IEEE Annals of the History of Computing, Year: 2007 Volume: 29 Issue: 1, P.5. Available at: [\(17/01/13\)](http://ieeexplore.ieee.org.tiger.semperTool.dk/Xplore/home.jsp).

- (٣٩) انظر :

JUDGE STEIN SCHJØLBERG & AMANDA M. HUBBARD, op. cit. P.4.

(٤٠) عبد الحميد عبد المطلب - جرائم استخدام شبكة المعلومات الدولية- الجريمة عبر الانترنيت - بحث مقدم مؤتمر القانون والكمبيوتر والانترنيت - كلية الشريعة والقانون - دولة الإمارات - عام ٢٠٠٠ - ص ٣ .

(٤١) ورقة العمل الأساسية مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة الجرميين - البند الخامس - الطبعة العربية - فيينا - ١٠ - ٢٠٠٧/٤/١٧ - ص ١٠ (Alcon f. 187).

(٤٢) انظر :-

Melanie Kowalski, "Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics", Catalogue no. 85-558-XIE, December 2002, Canadian Centre for Justice Statistics, P.6. Available at: <http://publications.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf>. (25/01/13).

(٤٣) انظر :-

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMITTEE OF THE REGIONS: "Towards a general policy on the fight against cybercrime", COMMISSION OF THE EUROPEAN COMMUNITIES, Brussels, 22.5.2007, COM (2007) 267 final, P.2. Available at: http://europa.eu/rapid/press-release_MEMO-07-199_en.htm?locale=en. (20/01/13).

(٤٤) انظر في نفس المعنى :-

Raluca Georgiana, op. cit. P.50.

(٤٥) احمد كيلان صقر - مرجع سابق - ص ٣٤ .

(٤٦) منير ومدوح الجنبي - جرائم الانترنت والحاسب الالي ووسائل مكافحتها - الاسكندرية - ٢٠٠٦ - ١٤ .

(٤٧) انظر :-

Donn B. Parker, Op. Cit. P.5.

(٤٨) انظر :-

David Icove, Karl Seger and William VonStorch, "Computer Crime: A CrimeFighter's Handbook", O'Reilly & Associates Inc, 1st ED, 1995, P.1.

(٤٩) راشد صالح الغيلاني - الجريمة المعلوماتية - بحث منشور في مجلة العين الساهمة - ع ٨٣ - إدارة عن شرطة عمان السلطانية - مسقط - ١٩٩٨ - ص ٤٣ ; عبد الستار الكبيسي - المسؤولية الناشئة عن استعمال الحاسوب - بحث مقدم إلى الندوة القانون والحاوسوب - بيت الحكمة - بغداد - أب ١٩٩٩ - ص ١٢٨ .

(٥٠) انظر :-

David Thompson, “1997 computer crime and security survey”, Information Management & Computer Security, Year: 1998 Volume: 6 Issue: 2; P.93. Available at :

[\(23/12/12\).](http://www.emeraldinsight.com.tiger.sempertool.dk/journals.htm?articleid=862712&show=html)

(٥١) عمر حسن عدس - جرائم الحاسوب الآلي - إشكالها وأساليب مواجهتها - بحث مقدم إلى المؤتمر ١٩ لقادة الشرطة والأمن العرب - تونس ١٩٩٥/١٠/١٨-١٦ - ص ١٠٧ ، عبدالله يوسف - مرجع سابق ص ٢١٨ .

(٥٢) وليد عبد الحي - إشكالية الفضاء الإلكتروني في حقوق الملكية الفكرية - بحث مقدم إلى المؤتمر العلمي الأول حول الملكية الفكرية - كلية القانون - جامعة اليرموك - الأردن - توز - ٢٠٠٠ - ص ٢ .

(٥٣) راشد الغيلاني - مرجع سابق - ص ٤٣ .

(٥٤) والجدير بالذكر في هذا المجال إلى أن هناك زيادة ملحوظة في عدد الجرائم المبلغ عنها رسميًا. فنجد على سبيل المثال ، في الولايات المتحدة الأمريكية أن عدد الحوادث المبلغ عنها لمركز حوادث امن المعلومات الفدرالي (US-CERT) قد زاد على مدار السنوات الماضية. فقد كان عدد هذه الجرائم ٥,٥٠٣ في عام ٢٠٠٦ ، بينما وصل إلى ١٦,٨٤٣ في عام ٢٠٠٨ أي بنسبة ٢٠٦%. بينما كان عدد الحوادث المبلغ عنها ٣٠,٠٠٠ في عام ٢٠٠٩ أي بنسبة أكثر من ٤٠%. وفي عام ٢٠١١ كان عدد الحوادث المبلغ عنها ٤٢,٨٨٧ أي زيادة بنسبة ٦٨٠% تقريبا. لاحظ بشان هذا الدراسات التي صدرت عن مكتب المحاسبة الحكومي الأمريكي . انظر في هذا :-

United States Government Accountability Office, “INFORMATION SECURITY: Cyber Threats and Vulnerabilities Place Federal Systems at Risk”, May 5, 2009, P.7. Available at: <http://www.gao.gov/products/GAO-09-661T>. (03/02/13). Also see: CYBERSECURITY: “Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats”, June 16/ 2010, P.3. Available at: <http://www.gao.gov/assets/130/124835.pdf>. (03/02/13). And see: CYBERSECURITY: “Threats Impacting the Nation”, April 24/ 2012, P.9. Available at: <http://www.gao.gov/assets/600/590367.pdf>. (03/02/13).

(٥٥) راشد الغيلاني – مرجع سابق – ص ٤٣ .

(٥٦) انظر :-

Gerald L. Kovacich & Andy Jones, “High-Technology Crime Investigator’s Handbook: Establishing and Managing a High-Technology Crime Prevention Program”, 2nd ED, Elsevier Inc, USA, 2006, P.100.

(٥٧) انظر :-

Ibid, P.99.

(٥٨) ورقة العمل الأساسية لمؤتمر الأمم المتحدة العاشر – مرجع سابق – ص ٩ (A/Conf 187/10) وبالفعل نجد حاليا على سبيل المثال اغلب الدول التي اهتمت في مكافحة هذه الجرائم إلى إنشاء وحدات متخصصة في الاستجابة والتعامل مع البلاغات التي تتعلق بهذه الجرائم كالولايات المتحدة الأمريكية واستراليا واليابان وكندا وعدد من الدول الآسيوية والعربية وغالبية الدول الأوروبية . حيث بإمكان أي شخص أن يجد موقع هذه الوحدات منتشرة على شبكة الانترنت.

(٥٩) جليل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة – الكتاب الأول – الجرائم الناشئة عن استخدام الحاسوب – القاهرة – ١٩٩٢ – ص ١٨ .

(٦٠) انظر :-

Xingan Li, “International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene”, Webology, Volume 4, Number 3, September, 2007, P.1. Available at: <http://www.webology.org/2007/v4n3/a45.html>. (12/12/13).

(٦١) منير ومدوح الجنبيهى – مرجع سابق – ص ١٥ .

– (٦٢) انظر :

Xingan Li, Op. Cit. P.2.

– (٦٣) انظر :

Peter Grabosky, “Computer Crime: A Criminological Overview”, Prepared for Presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 15 April 2000. P.١٦. Available at <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.4660>. (30/12/2012).

(٦٤) ذياب موسى البدائنة – جرائم الحاسوب والانترنت – بحث مقدم إلى الندوة العلمية المعقودة في تونس ١٩٩٩/٦/٣٠-٢٨ – أكاديمية نايف العربية للعلوم الأمنية – الظواهر الإجرامية المستحدثة وسبل مواجهتها – الرياض – ١٩٩٩ – ص ١١١.

(٦٥) نائلة عادل محمد فريد – مرجع سابق – ص ٥٣ وهي تشير إلى :

Clough (Bryan) and Mango (Paul), “Approaching zero: Data crime and criminal Underworld”, 1992, pp.136-146.

– (٦٦) انظر :

Miriam F. Miquelon Weismann, “International Cybercrime: Recent Development in The Law”, in “Cybercrime: The investigation, Prosecution and Defense of A Computer-related crime”, By Ralph D. Clifford, 2nd ED, Carolina Academic Press, USA, 2006, P.244.

– (٦٧) نائلة محمد فريد – مرجع سابق – ص ٥٤ وهي تشير إلى

Deborah Fisch Nigri, “National and international aspects of computer crime : THE EMERGING NEED FOR STATUTORY CONTROL”, Thesis, University of London, Center for Criminal Law studies, Queen Mary and Westfield college, January 1993. p315.

– (٦٨) انظر :

Ulrich Sieber, “The international Handbook on Computer Crime ”Computer related Economic crime and infringements of privacy”, John Wiley & Sons, 1986, p.110.

– (٦٩) انظر :

Ibid, p. 114.

(٧٠) ينظر اتفاقية بودابست للجرائم الكونية لعام ٢٠٠١

(٧١) نائلة محمد فريد - مرجع سابق - ص ٥٥.

(٧٢) انظر :-

David Icove (Eds), op. Cit. P.5.

(٧٣) انظر :-

Joseph Migga Kizza (Eds), op. Cit. PP.252-254.

(٧٤) احمد كيلان صكر - مرجع سابق - ص ٨٣ وهو يشير إلى

Wade Roush, "Hackers: Taking a bite out of computer crime", technology review-USA- April 1995. Home page <http://www.mit.edu/techreview>.

(٧٥) عبد الرحمن جلهم حمزة - جرائم الانترنت من منظور شرعى وقانوني - بدون سنة طبع أو مكان طبع - ص ٢٢ وهو يشير إلى

Rapalus P. (2000, may), "Ninity Percent of Survey Repondents detect Cyber Attacks", Computer Security Institute, Available at: <http://www.gocsi.com/prelen ooo321/htm>.

(٧٦) انظر :-

Lori Enos, "Study: Cybercrime Continues to Boom", E-Commerce Times, 22/03/2000. Available at: <http://www.ecommercetimes.com/story/2795.html>. (11/02/2013).

(٧٧) انظر :-

John P. Mello Jr, "Cybercrime Costs US Economy at Least \$117B Each Year", TechNewsWorld, 07/26/2007. Available at: <http://www.technewsworld.com/story/58517.html>. (03/03/2013).

(٧٩) عبد الرحمن جلهم حمزة - مرجع سابق - ص ٢٢ وهو يشير إلى

Jonathan Reuvid, "The Regulation and Prevention of Economic Crime", 1998, London, Kogan, P.14.

(٨٠) احمد كيلان صكر - مرجع سابق - ص ٣٨ . وهو يشير إلى :-

Dr. Peter Porting, "Information technology and criminality: appearance and defense measures", Betrie bswirt schafti – Wiesbaden- 1992-p. 48.

(٨١) انظر :-

David Icove (Eds), op. cit. P.4.

(٨٢) ذياب البداية - مرجع سابق - ص ٩٧ وهو يشير إلى PC Magazine, 1997 . pp.24-26.

- (٨٣) انظر :

Florence Tushabe and Venansius Baryamureeba, "Cyber Crime in Uganda: Myth or Reality?" PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY VOLUME: 8 OCTOBER 2005, P.66. Available at:
[\(31/05/2012\).](http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.102.8447)

- (٨٤) انظر :

W. COLE DURHAM, JR. and RUSSELL C. SKOUSEN, "The Law of Computer-Related Crime in the United States", the American Journal of Comparative Law, Year: 1990 Volume: 38, P.560. Available at:
[\(07/02/2013\).](http://www.jstor.org.tiger.sempertool.dk/stable/pdfplus/840559.pdf)

- (٨٥) انظر :

Joseph Migga Kizza (eds), op. Cit. PP.251-252.

- (٨٦) انظر :

Ibid, PP.254-255.

- (٨٧) انظر :

Madison Ngafeeson, "Cybercrime Classification: A Motivational Model", P.3. Available at:
[\(29/01/2013\).](http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf)

(٨٨) هدى حامد قشقوش - مرجع سابق - ص ٢٧ وهي تشير إلى

Deveze J. le vol de "biens informatiques la smaine juridique 59, e annee - No44 30 oct- 1985.

. (٨٩) هدى حامد قشقوش - مرجع سابق - ص ٢٧ .

(٩٠) عبد الهادي القهوجي وفتوح عبد الله الشاذلي - علم الإجرام والعقاب - المطبوعات الجامعية - ص ١٥٣-١٦١ .

. (٩١) مصطفى محمد موسى - مرجع سابق - ص ٢١ .

- (٩٢) إبراهيم وجيه محمود - القدرات العقلية - مصر - ط - ١٩٧٩ - ص ٢١٠ .
- (٩٣) مصطفى محمد موسى - مرجع سابق - ص ٢٣ .
- (٩٤) انظر : -

David Icove (Eds), op. cit. P.66.

- (٩٥) نائلة محمد فريد - مرجع سابق - ص ٥٧ .
- (٩٦) عبد الفتاح بيومي حجازي - التزوير في جرائم الكمبيوتر والانترنت - مصر - ٢٠٠٨ - ص ١٠٧ .
- (٩٧) عبد الفتاح بيومي حجازي - مرجع اعلاه - ص ١٠٧ .
- (٩٨) سليمان احمد فضل - مرجع سابق - ص ٢٢ .
- (٩٩) عبد الفتاح بيومي حجازي - التزوير - مرجع سابق - ص ١٠٧ .
- (١٠٠) انظر : -

Gerald L. Kovacich and Andy Jones, op. cit. P.29.

- (١٠١) ولعل ما يبرر ذلك القضية التي عرضت أمام القضاء الألماني بخصوص الجرم الذي لم يتجاوز عمره ١٧ عام والذي بين في اعترافاته أنه كان القصد من دخوله إلى نظام الفيديو تكس الخاص *Buna post* والمعروف بمصطلح *BTX video text* في كشف عيوب هذا النظام ، وأشار إلى هذه القضية محمد سامي الشوا - مرجع سابق - ص ٥١ .
- (١٠٢) انظر : -

Peter Grabosky, op. cit. P.3.

- (١٠٣) انظر : -

David Thompson, op. cit. p.93.

- (١٠٤) انظر : -

Joseph Migga Kizza (Eds), op. cit. PP.249-250.

- (١٠٥) انظر : -

Donn B. Parker, “Fighting computer crime – A new framework for protection information”, john Wiley & Sons Inc, USA, 1998, P.142.

(١٠٦) كما وأن الأدوات المتاحة على موقع الانترنت والتي تمكن الشخص أو هذا الجرم من أن يصبح شخصاً مؤمناً (موثوقاً). كما أنه هذه الامكانيات تجعل أكثر سهولة من يقوم بتسلیب بنك باستخدام الاسلحة. فهو الان بإمكانه بمجرد استخدام الحاسوب أن يقوم بأعماله غير النظيفة . لاحظ في هذا المعنى :-

Carolyn Nisbet, “New Directions in Cyber-crime”, 2002, QinetiQ Ltd, P.2. Available at:

http://apps.qinetiq.com/perspectives/pdf/EP_White_Paper3_Cyber%20Crime.pdf. (27/01/2013).

(١٠٧) سليمان احمد فضل - مرجع سابق - ص ٢٢ .

(١٠٨) عبد الفتاح بيومي حجازي - التزوير - مرجع سابق - ص ١١٣ .

(١٠٩) انظر :-

Donn B. Parker, “Fighting computer crime”, op. cit. PP.144-146

(١١٠) انظر :-

Ibid, P.144.

(١١١) محمد سامي الشوا - مرجع سابق - ص ٥٣ .

(١١٢) مصطفى محمد موسى - مرجع سابق - ص ٢٦ . وكذلك في نفس المعنى :-

Donn B. Parker, “Fighting computer crime”, op. cit. P.144.

(١١٣) انظر :-

Donn B. Parker, Ibid, P.144.

(١٤) نائلة محمد فريد - مرجع سابق - ص ٦٢ .

(١٥) مصطفى محمد موسى - مرجع سابق - ص ٢٦ .

(١٦) نائلة محمد فريد - مرجع سابق - ص ٦٢ ، عبد الرحمن جلهم - مرجع سابق - ص ٢٧ .

(١٧) نائلة محمد فريد - مرجع سابق - ص ٦٣ .

(١٨) مصطفى محمد موسى - مرجع سابق - ص ٢٩ .

(١٩) نائلة محمد فريد - مرجع سابق - ص ٦٣ وهي تشير إلى

Rose (philipe), “La criminalité informatique à l horizon 2005 – Analyse prospective”, L harmattan, 1992 .p.6.

(١٢٠) انظر في هذا المعنى :-

Ralph D. Clifford, op. cit. P.5.

وهناك من يقسم الجرائم المرتبطة بالإنترنت إلى جرائم جديدة ناتجة من انتشار استخدام الانترنت ويمكن أن ترتكب مباشراً. وجرائم ذات شكل قديم موجودة سابقاً وتستخدم التكنولوجيا وشبكة الانترنت لغرض تنفيذ هذه الجرائم . لاحظ في هذا السياق :

H. Jahankhani, and Ameer Al-Nemrat, op. cit. P.44.

(١٢١) انظر :-

David L. Carter, “Computer Crime Categories, How Techno-Criminals Operate”, The FBI Magazine, July 1995. Available at: <http://www.lectlaw.com/files/cri14.htm>. (22/02/2013).

(١٢٢) انظر :-

Ulrich Sieber, op. cit. PP.3-27.

(١٢٣) انظر :-

Ulrich Sieber, op. cit. PP.21-26.

(١٢٤) انظر :-

Ibid. P.26, 27.

(١٢٥) لمزيد من التفصيل حول هذا انظر :-

Mohamed Chawki, “Cybercrime in France: An Overview”, 07 December 2005, Computer Crime Research Center. Available at: <http://www.crime-research.org/articles/cybercrime-in-france-overview> . (08/01/2013).

(١٢٦) انظر :-

Martin Wasik, op. cit. P.42.

(١٢٧) نائلة محمد فريد - مرجع سابق - ص ٢٥٥-٢٥٩ .

(١٢٨) انظر :-

Jonathan Clough, “The Council of Europe Convention on Cybercrime: Defining ‘Crime’ in a Digital World”, Criminal Law Forum; December 2012, Volume 23, Issue 4, P.372. Available at: <http://link.springer.com.tiger.sempertool.dk/article/10.1007%2Fs10609-012-9183-3>. (30/11/2012).

(١٢٩) لمزيد من التفصيل حول هذا انظر :-

Sarah Gordon and Richard Ford, op. cit. PP.14-15.

(١٣٠) انظر :-

Taraq Hussain Sheakh, “Cyber Law: Provisions and Anticipation”, International Journal of Computer Applications; Volume 53– No.7, September 2012. P.11. Available at:

<http://research.ijcaonline.org/volume53/number7/pxc3882204.pdf>.

(01/01/2013).

(١٣١) في هذا المعنى انظر :-

Madison Ngafeeson, op. cit. P.2.

(١٣٢) وایماناً من هذا بعد الدولي لهذه الجرائم نجد عديداً من القوانين النموذجية والاتفاقيات التي اعدت بشأن معالجة اهم المشاكل الناجمة عن الاستخدام غير القانوني لهذه التقنيات والتي تمثل انشطة اجرامية تحدد جميع مستخدمي هذه التقنيات وعلى جميع المستويات . فنجد مثلاً قانون الامارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها .

Available at:

http://arabic.mjustice.dz/liguearabe/loi_emir_ar_crim_tech_info.pdf.
(17/02/2013).

وكذلك مسودة معايدة للاقتحاد الافريقي بشأن الثقة والامن في الفضاء الالكتروني

Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa. Available at:

<http://www.au.int/en/cyberlegislation>. (17/02/2013) ;

وكذلك مشروع القانون النموذجي الخاص بالحاسوب والجريمة المرتبطة بالحاسوب الذي قدم في عام ٢٠٠٢ لدول الكومنولث .

Model Law on Computer and Computer Related Crime of Commonwealth.

Available at:

http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.
(17/02/2013).

(١٣٣) انظر :-

International Review of Criminal policy – United Nations, Manual on the Prevention and Control of Computer related crime. Nos. 43 & 44. P. 3, 4.

(١٣٤) سنحاول هنا الاشارة إلى اهم المحاولات البارزة في تصنيف هذه الجرائم على المستوى الدولي دون انكار بقية المحاولات لهذه المسالة . اذ اننا نجد اغلب المنظمات الدولية التي اهتمت بهذا الامر من خلال صياغة الاتفاقيات أو القرارات أو التوصيات أو القوانين الاسترشادية كمجلس أوربا والاتحاد الأوروبي والجامعة العربية والامم المتحدة والاتحاد الافريقي ومجموعة الشمان والاسيان ومنظمة دول امريكا الجنوبيه وغيرها .

(١٣٥) وقد انصرف اهتمام المنظمة بعد ذلك إلى حماية أنظمة الحاسوب وشبكات المعلومات باعتبار ذلك الخطوة الأولى لمكافحة الجريمة المعلوماتية . وفي هذا الإطار أصدرت المنظمة في ٢٦ نوفمبر ١٩٩٢ توصية إلى الدول الأعضاء تتعلق بالتدابير والإجراءات الأمنية التي ينبغي الأخذ بها لحماية أنظمة المعلومات والتي حلّت محلها التوصية الصادرة في ٢٥ يوليو ٢٠٠٢ والتي تضمنت تسعة مبادئ ينبغي مراعاتها عند الأخذ بالتدابير والإجراءات الأمنية اللازمة لحماية أنظمة الحاسوب وهي كالتالي :

1- Accountability principle. 2- Awareness principle. 3- Ethics principle.
4-Multidisciplinary principle. 5- Proportionality principle. 6- Integration principle. 7- Timeliness principle. 8- Reassessment principle. 9- Democracy principle.

Looking: Recommendation of the Council Concerning Guidelines for the Security of information systems, 1992, Recommendation of the Council Concerning Guidelines for the Security of information systems and Networks: Towards a Culture of Security, 25 July 2002.

(١٣٦) وهذا التصنيف لا يبدو متسقا تماما، لأنه لا يستند إلى معيار محدد في تصنيف هذه الجرائم . حيث نجد في الفئة الاولى والثالثة والرابعة يعتمد معيار موضوع الحماية القانونية. بينما نجد في الفئة الثانية يركز على معيار الاسلوب المستخدم في ذلك . وبؤدي هذا عدم الاتساق إلى بعض التداخل بين الفئات . لاحظ بشان هذا :-

International Telecommunication Union, “UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES”, This Report was commissioned by the ITU Development Sector’s ICT

Applications and Cybersecurity Division and was prepared by Dr. Marco Gercke, Draft April 2009, P.17. Available at: www.itu.int/ITU-D/cyb/cybersecurity/ledislation.html. (17/02/2013).

(١٣٧) مثل امريكا وكندا واستراليا واليابان وجنوب افريقيا ودول اخرى انضمت لاحقاً لهذه الاتفاقية في مسعى خلق اجماع دولي حول المشاكل التي تثار بواسطة الاستخدام غير المشروع لهذه التقنيات .

(١٣٨) انظر المواد من ٢ إلى ٦ من الاتفاقية الاوربية .

(١٣٩) انظر المادة ٦ و ٧ من الاتفاقية .

(١٤٠) انظر المادة ٩ من الاتفاقية .

(١٤١) انظر المادة ١٠ من الاتفاقية .

(١٤٢) انظر :-

Commission of The European Communities, “Towards a general policy on the fight against cybercrime”, op. cit. P.3.

(١٤٣) وهو أحد المخاور الستة لمشروع جنة الامم المتحدة الاقتصادية والاجتماعية لغرب اسيا والذي يضمن:- (الاتصالات الإلكترونية وحرية التعبير، والمعاملات الإلكترونية والتوفيق الإلكتروني، والتجارة الإلكترونية وحماية المستهلك، ومعالجة البيانات ذات الطابع الشخصي، والجرائم السيبرانية، والملكية الفكرية في المجال المعلوماتي والسيبراني) . لاحظ في هذا الشأن: ارشادات الاسكوا للتشرعيات السيبرانية: مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية . بيروت، ٢٠١٢ . ص أ.

Available at:

<http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf>. (13/09/2012).

(١٤٤) لاحظ الارشاد الخامس الخاص بالجرائم السيبرانية للجنة الامم المتحدة الاقتصادية والاجتماعية لغرب اسيا .

Available at:

<http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Dir-5-Cybercrimes.pdf>. (11/01/2012).

(١٤٥) نود الاشارة هنا إلى أمر مهم جداً وهو أن مفهوم الحاسب هنا لا يقصد به الحاسب كمكون مادي يتمثل فقط بالاجزاء المادية (hardware) وإنما يتمثل في الاجزاء المعنوية (Software) وما يرتبط بها من انظمة اتصالات وبرامج المعلومات . بمعنى أكثر دقة، إننا نقصد هنا بمفهوم الحاسب أي جهاز يؤدي نفس هذه الوظائف من معالجة ونقل وخزن وتحويل البيانات، كذلك مع ما يرتبط بهذا الجهاز من تقنيات أخرى أو شبكات اتصال بين تلك الأجهزة . لذا فإن مفهوم الحاسب والأنظمة يكون بأوسع ما يمكن تصوره في اداء هذه الوظائف وأهمام .

(١٤٦) ما دام ارتكاب الجريمة يتم عن طريق هذه التقنية وتبعاً للدور الذي يمكن أن يتخرذن الحاسب في تنفيذها . في المقابل، فإن الحاسب يستخدم على نطاق واسع في التحقيق الاستدلالي لكشف كافة الجرائم . ناهيك عن أن جهات تنفيذ القانون في دول عديدة تعتمد على النظم التقنية في أداء المهام من خلال اتباع قواعد البيانات ضمن جهاز إدارة العدالة والتطبيق القانوني . ومع تزايد نطاق الجرائم المعلوماتية واعتماد الجناء على وسائل التقنية المتعددة والمتطرفة، فإنه أصبح لزاماً استخدام نفس الوسائل المتطرفة للكشف عنها . ومن هنا جاء الحاسب ليلعب دوراً مهماً في كشف الجرائم المعلوماتية وتتبع فاعليها، بل وإبطال اثر الهجمات التدميرية لمحترقي النظم وتحديداً هجمات الفيروسات وإنكار الخدمة وقرصنة البرمجيات . لاحظ: جميل عبد الباقي الصغير - أدلة الإثبات الجنائي والتكنولوجيا الحديثة - النهضة العربية - مصر - ص ٩٠-١٠٠ . من جانب ثانٍ، أن اغلب الدول المعينة من المؤكدة الان تسعى وستبقى تسعى في ايجاد التقنيات الحديثة في مجال التحقيق والكشف والمراقبة . فإن واقع الحال يبين أن الاستمرار في استعمال تقنيات بدائية في المراقبة والكشف عن هذه الجرائم يكون من بين الاسباب الرئيسية في عدم ايجاد نموذج جيد قادر على تقدير مخاطر هذه التقنيات . انظر هذه الاسباب لدى :-

Joseph Migga Kizza(Eds), op. cit. P.255.

(١٤٧) كما أن هذه الامكانيات لا تقتصر على توفير الفرص للنشاط الاجرامي . اذ أن هذا الجهاز له من الامكانيات ما تمكنه من أن يكون أحد الادوات الفاعلة في كشف الجريمة وتحديد هوية الجاني . ولعل في جهاز تحديد المجرمين من أقوى الأدلة على ذلك، والذي هو عبارة عن آلة صغيرة بحجم بطاقة الائتمان يقوم بتحليل DNA للآثار التي يتم العثور عليها، حيث أن عملية التحليل تكون في نفس مسرح الجريمة بواسطة هذا الجهاز المتصل بالحاسوب الآلي الذي يحمل قاعدة بيانات بأسماء المجرمين المسجلين وصفاتهم الوراثية ويقارن بينها ليحدد المجرم قبل أن يكرر أفعاله الإجرامية . د. مصطفى محمد موسى - مرجع سابق - ص ٧٤ . ناهيك عن أنه حتى في بعض الاحيان يكون ما يحتويه الحاسوب من وثائق ومعلومات مفيدة في كشف الجريمة اذا استغلت بصورة صحيحة . وأن اغلب الناس يجهل امكانية استرجاع ما تم حذفه سابقا وبالتالي يكون دليل في هذه الجريمة . لاحظ في هذا المعنى :-

Gerald L. Kovacich and Andy Jones, op. cit. P.100.

(١٤٨) نائلة محمد فريد - مرجع سابق - ص ٢٦٥ وهي تشير إلى Deborah Fisch Nigri, p.130 . نائلة محمد فريد - مرجع سابق - ص ٢٦٥ .

(١٤٩) وهناك من يرى بان معظم الجرائم المرتبطة بالحاسوب في الواقع تكون بعيدة كل البعد عن التكنولوجيا العالية، بل هي جريمة الرجل العادي . لاحظ :-

Jack Molnar, "Putting Computer-Related Crime in Perspective", Journal of Policy Analysis and Management, Vol: 6, No: 4, Privatization: Theory and Practice (Summer, 1987), P.714. Available at:
[http://www.jstor.org.tiger.sempertool.dk/stable/pdfplus/3323530.pdf?acceptTC=true. \(01/07/2012\).](http://www.jstor.org.tiger.sempertool.dk/stable/pdfplus/3323530.pdf?acceptTC=true. (01/07/2012).)

(١٥٠) نائلة محمد فريد - مرجع سابق - ص ٢٦٦ وهي تشير إلى Deborah Fisch Nigri, p. 131.

(١٥١) انظر :-

Susan W. Benner, "Defining Cybercrime: A Review of State and Federal Law", at Ralph D. Clifford, op. cit. P.18.

(١٥٢) انظر :-

Ibid, P.19.

(١٥٣) انظر :-

Richard Totty & Anthony Hardcastle, op. cit. P.142.

(١٥٤) انظر :-

David L. Carter, op. cit. P.3.

(١٥٥) انظر :-

Martin Wasik, op. cit. P.2.

(١٥٦) انظر عكس هذا لدى :-

Susan W. Benner, op. cit. P.19.

(١٥٧) انظر :-

Richard Totty & Anthony Hardcastle, op. cit. P.143.

(١٥٨) فيما يذهب رأي خلاف ذلك إلى تسهيل الحاسوب الآلي بما يحتويه من معلومات وبيانات والتي يمكن أن تكون مخالفة جريمة الابتزاز، باعتبار أن المعلومات أصبحت لها قيمة مادية كبيرة وأصبح الحاسوب مخزناً لكثير من الأسرار . نائلة محمد فريد - مرجع سابق - ص ٢٦٣ .

وهي تشير إلى صاحب هذا الرأي **Deborah Fisch Nigri, P.128**

(١٥٩) انظر :-

David L. Carter, op. cit. P.3.

(١٦٠) انظر في نفس المعنى :-

Jonathan Clough, "Principles of Cybercrime", op. cit. p.27.

(١٦١) نائلة محمد فريد - مرجع سابق - ص ٢٧٨ وهي تشير إلى

Vergutch (Pascal), "La repression des delits informatiques dans une perspective internationale", These, Universite de Montpellier 1, 1996. P.282.

(١٦٢) انظر :-

**Marc D. Goodman and Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace", P.10. Available at:
<http://law.scu.edu/international/File/goodmanbrenner.pdf>. (18/07/2012).**

(١٦٣) انظر :-

Susan W. Bernner, "Defining Cybercrime", op. cit. p.17.

(١٦٤) انظر :-

Jonathan Clough, “The Council of Europe Convention on Cybercrime”, op. cit. P.372.

(١٦٥) د. هدى حامد قشقوش - مرجع سابق - ص ٢٣ .

(١٦٦) معجم الحاسيبات - الإدارة العامة للمعجمات - مجمع اللغة العربية ، القاهرة - مصر، ١٩٨٧ - ص ١٣ .

(١٦٧) انظر :-

Martin Wasik, op. cit. P.5.

(١٦٨) وهي تشبه الآلة الكاتبة لتنقية الكروت بدل طبعها ثم بعد ذلك تراجع بحالة المراجعة ثم تنقل هذه الكروت إلى آلة القراءة البطاقات وهي من ضمن وسائل الإدخال وتقوم هذه الآلة بقراءة هذه الثقوب وتحويلها إلى نبضات إلى الحاسوب الالكتروني لتخزينها . لاحظ: هدى حامد قشقوش - مرجع سابق - ص ٢٣ .

(١٦٩) وهي تقوم بصياغة البيانات والمعلومات عن طريق تنقية شرائط ورقية وهي تشبه الشرائط المستخدمة في التلكس وتقرأ هذه البيانات والمعلومات عن طريق وحدة القراءة وهي متصلة بالحاسوب الالكتروني . انظر: المرجع اعلاه - ص ٤ .

(١٧٠) ويقصد به تحويل النص المكتوب بواسطة لوحة المفاتيح إلى الخط اليدوي الخاص بصاحب الحاسوب الآلي الشخصي، ولكن يعبأ عليها إلى إمكانية استغلالها من قبل غير أشخاص فيما لو قاموا باستخدام الجهاز . ولقد نجحت شركة MEDIATIC في ابتكار هذا البرنامج وهو يحمل اسمها ، الذي يتم تركيبه في الحاسوب بواسطة خبراء الشركة . مصطفى محمد موسى - مرجع سابق - ص ٦ .

(١٧١) ويعرف هذا بتقنية Voiceprint وتقوم شركة IBM بجهود كبيرة في مجال بحوث الحاسوب يتم من خلالها الحسب من التعرف على الصوت . انظر: مرجع اعلاه - ص ٤٧ .

(١٧٢) عمر الفاروق الحسيني - تأملات في بعض صور الحماية القانونية للحاسوب الآلي - بحث مقدم مؤتمر الحاسوب الالكتروني - القاهرة - مايو ١٩٩١ - ص ٢٠ .

. ٢٨) هدى حامد قشقوش - مرجع سابق - ص ٢٨ (

(١٧٤) فالبيانات المخزونة في الحاسوب تكتب بلغة الصفر والواحد أو لغة ثنائية . مزيد من التفصيل انظر :-

Debra Littlejohn Shinder, "Scene of the Cybercrime: Computer Forensics Handbook", Syngress Publishing Inc, USA, 2002, PP.166-169.

(١٧٥) ينظر : طاهر الشيخ - مقدمة الحاسوب الالكترونية - مركز الحاسوب بجامعة عين الشمس - سبتمبر ١٩٩١ - مصر - ص ٢٧ ; هدى حامد قشقوش - مرجع سابق - ص ٢٩ .

المصادر

أولاً:- المصادر باللغة العربية :-

- ١- ارشادات الاسكوا للتشريعات السيبرانية - مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية . بيروت - ٢٠١٢ .
- ٢- إبراهيم وجيه محمود - القدرات العقلية - مصر - ط - ٢٥ - ١٩٧٩ .
- ٣- أحمد كيلان عبد الله صكر - الجرائم الناشئة عن إساءة استخدام الحاسوب - اطروحة ماجستير - جامعة بغداد - كلية القانون - ٢٠٠٢ .
- ٤- الارشاد الخامس الخاص بالجرائم السيبرانية للجنة الامم المتحدة الاقتصادية والاجتماعية لغرب اسيا .
- ٥- جمیل عبد الباقی الصغیر - أدلة الإثبات الجنائي والتکنولوجيا الحديثة - النهضة العربية - مصر - بدون سنة طبع .
- ٦- جمیل عبد الباقی الصغیر - القانون الجنائي والتکنولوجيا الحديثة - الكتاب الأول - الجرائم الناشئة عن استخدام الحاسوب - القاهرة - ١٩٩٢ .
- ٧- ذياب موسى البداینة - جرائم الحاسوب والانترنت - بحث مقدم إلى الندوة العلمية المعقودة في تونس ٢٨-١٩٩٩/٣٠ - أكاديمية نايف العربية للعلوم الأمنية - الظواهر الإجرامية المستحدثة وسبل مواجهتها -الرياض - ١٩٩٩ .
- ٨- راشد صالح الغيلاني - الجريمة المعلوماتية - بحث منشور في مجلة العين الساهرة - ع ٨٣ - إدارة عن شرطة عمان السلطانية - مسقط - ١٩٩٨ .
- ٩- سليمان احمد فضل - الموجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت) - دار النهضة العربية - ٢٠٠٧ - القاهرة .
- ١٠- طاهر الشيخ - مقدمة الحاسوبات الالكترونية - مركز الحاسوب بجامعة عين الشمس - سبتمبر ١٩٩١ - مصر .

- ١١- عبد الحميد عبد المطلب - جرائم استخدام شبكة المعلومات الدولية- الجريمة عبر الانترنت - بحث مقدم مؤتمر القانون والكمبيوتر والانترنت - كلية الشريعة والقانون - دولة الإمارات العربية المتحدة - عام ٢٠٠٠ .
- ١٢- عبد الرحمن جلهم حمزة - جرائم الانترنت من منظور شرعى وقانوى - بدون سنة طبع أو مكان طبع .
- ١٣- عبد الرحمن عبد العزيز الشنيفي - امن المعلومات وجرائم الحاسب الآلي - طبعة أولى - الرياض - ١٩٩٥ .
- ١٤- عبد الستار الكبيسي - المسؤولية الناشئة عن استعمال الحاسوب - بحث مقدم إلى الندوة القانون والحواسيب - بيت الحكمة - بغداد - أب ١٩٩٩ .
- ١٥- عبد الفتاح بيومي حجازي - التزوير في جرائم الكمبيوتر والانترنت - مصر - ٢٠٠٨ .
- ١٦- عبد الفتاح بيومي حجازي - الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت - دار الكتب الوطنية - مصر - ٢٠٠٥ .
- ١٧- عبد الهادي القهوجي وفتح عبد الله الشاذلي - علم الإجرام والعقاب - المطبوعات الجامعية - بدون سنة طبع .
- ١٨- عبد الله يوسف - التقنية والجرائم المستحدثة - بحث مقدم في الندوة العلمية (الظواهر المستحدثة وسبل مواجهتها) المنعقدة في تونس ٢٨/٣٠/٦ . ١٩٩٩ .
- ١٩- عمر الفاروق الحسيني - تأملات في بعض صور الحماية القانونية للحاسوب الآلي - بحث مقدم مؤتمر الحاسوب الالكتروني - القاهرة - مايو ١٩٩١ .
- ٢٠- عمر حسن عدس - جرائم الحاسوب الآلي - أشكالها وأساليب مواجهتها - بحث مقدم إلى المؤتمر ١٩ لقادة الشرطة والأمن العرب - تونس ١٦/١٨/١٠ . ١٩٩٥ .
- ٢١- قانون الامارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها .

- ٢٢- محمد الأمين البشري - بحث (التحقيق في جرائم الحاسب الآلي) - مقدم إلى مؤتمر القانون والكمبيوتر والانترنت - مايو ٢٠٠٠ - كلية الشريعة والقانون - دولة الإمارات العربية المتحدة .
- ٢٣- محمد سامي الشوا - ثورة المعلومات وانعكاساتها على قانون العقوبات - مصر - . ٢٠٠٣
- ٢٤- محمد محى الدين عوض - جرائم نظم المعلومات (الكمبيوتر) - الرياض - ١٩٩٣ .
- ٢٥- مصطفى محمد موسى - أساليب إجرامية بالتقنية الرقمية - الطبعة الأولى - مصر - . ٢٠٠٣
- ٢٦- معجم الحاسوبات - الإدارية العامة للمعجمات - مجمع اللغة العربية - القاهرة - . ١٩٨٧
- ٢٧- منير ومدوح الجنبي - جرائم الانترنت والحاسب الآلي ووسائل مكافحتها - الاسكندرية - ٢٠٠٦ .
- ٢٨- نائلة عادل محمد فريد - جرائم الحاسب الآلي الاقتصادية - مطابع الحلبي الحقوقية - بدون سنة طبع .
- ٢٩- هدى حامد قشقوش - جرائم الحاسب الالكتروني في التشريع المقارن - القاهرة - . ١٩٩٢
- ٣٠- هشام محمد فريد رستم - قانون العقوبات ومخاطر تقنية المعلومات - مكتب الآلات الحديثة - ١٩٩٢ .
- ٣١- ورقة العمل الأساسية لمؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة الجرميين - البند الخامس - الطبعة العربية - فيينا - ١٠ - ١٧/٤/٢٠٠٧ .
- ٣٢- وليد عبد الحي - إشكالية الفضاء الالكتروني في حقوق الملكية الفكرية - بحث مقدم إلى المؤتمر العلمي الأول حول الملكية الفكرية - كلية القانون - جامعة اليرموك - الأردن - توز - ٢٠٠٠ .

ثانياً:- المصادر باللغة الانكليزية :-

- 1- Carolyn Nisbet, “New Directions in Cyber-crime”, 2002, QinetiQ Ltd. Available at:
http://apps.qinetiq.com/perspectives/pdf/EP_White_Paper3_Cyber%20Crime.pdf.
- 2- COMMISSION OF THE EUROPEAN COMMUNITIES: “Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime”, Brussels, 26.1.2001, COM (2000) 890 final. Available at: <http://europa.eu/>.
- 3- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMITTEE OF THE REGIONS: “Towards a general policy on the fight against cybercrime”, COMMISSION OF THE EUROPEAN COMMUNITIES, Brussels, 22.5.2007, COM (2007) 267 final. Available at: http://europa.eu/rapid/press-release_MEMO-07-199_en.htm?locale=en.
- 4- David Icove, Karl Seger and William VonStorch, “Computer Crime: A CrimeFighter’s Handbook”, O’Reilly & Associates Inc, 1st ED, 1995.
- 5- David L. Carter, “Computer Crime Categories, How Techno-Criminals Operate”, The FBI Magazine, July 1995. Available at: <http://www.lectlaw.com/files/cri14.htm>.
- 6- David Thompson, “1997 computer crime and security survey”, Information Management & Computer Security, Year: 1998 Volume: 6 Issue: 2. Available at: <http://www.emeraldinsight.com.tiger.sempertool.dk/journals.htm?articleid=862712&show=html>.
- 7- Debra Littlejohn Shinder, “Scene of the Cybercrime: Computer Forensics Handbook”, Syngress Publishing Inc, USA, 2002.
- 8- Deng-Yiv Chiu, Tien-Tsun Chung and Chen-Shu Wang, “Attacking and defending perspective of e-Crime behavior and psychology: A systemic dynamic simulation approach”, 2009 Fourth International Conference on Innovative Computing, Information and Control. Available at: <http://ieeexplore.ieee.org/Xplore/guesthome.jsp>.
- 9- Donn B. Parker, “Fighting computer crime – A new framework for protection information”, John Wiley & Sons Inc, USA, 1998.
- 10- Donn B. Parker, “The Dark Side of Computing: SRI International and the Study of Computer Crime”, IEEE Annals of the History of Computing, Year: 2007 Volume: 29 Issue: 1. Available at: <http://ieeexplore.ieee.org.tiger.sempertool.dk/Xplore/home.jsp>.

- 11- Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa. Available at: <http://www.au.int/en/cyberlegislation>.
- 12- Florence Tushabe, and Venansius Baryamureeba, "Cyber Crime in Uganda: Myth or Reality?" PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY VOLUME: 8 OCTOBER 2005. Available at: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.102.8447>.
- 13- Gerald L. Kovacich & Andy Jones, "HIGH-TECHNOLOGY CRIME INVESTIGATOR'S HANDBOOK: Establishing and Managing a High-Technology Crime Prevention Program", 2nd ED, Elsevier Inc, USA, 2006.
- 14- Gideon Emcee Christian, "A New Approach to Data Security Breaches", Canadian Journal of Law and Technology, Vol. 7, No. 1. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1704922.
- 15- H. Jahankhani and Ameer Al-Nemrat, "Examination of Cyber-criminal Behaviour", International Journal of Information Science and Management, Special Issue January / June, 2010, Available at <http://188.136.184.17/ojs/index.php/ijism/article/view/135/121>.
- 16- International Review of Criminal policy – United Nations, Manual on the Prevention and Control of Computer related crime. Nos. 43 & 44.
- 17- International Telecommunication Union, "UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES", This Report was commissioned by the ITU Development Sector's ICT Applications and Cybersecurity Division and was prepared by Dr. Marco Gercke, Draft April 2009. Available at: www.itu.int/ITU-D/cyb/cybersecurity/ledislation.html.
- 18- Jack Molnar, "Putting Computer-Related Crime in Perspective", Journal of Policy Analysis and Management, Vol: 6, No: 4, Privatization: Theory and Practice (Summer, 1987). Available at: <http://www.jstor.org.tiger.sempertool.dk/stable/pdfplus/3323530.pdf?acceptTC=true>.
- 19- John P. Mello Jr, "Cybercrime Costs US Economy at Least \$117B Each Year", TechNewsWorld, 07/26/2007. Available at: <http://www.technewsworld.com/story/58517.html>.
- 20- Jonathan Clough, "Principles of Cybercrime", 1st Ed, Cambridge University Press, UK, 2010.
- 21- Jonathan Clough, "The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World", Criminal Law

- Forum; December 2012, Volume 23, Issue 4. Available at:
<http://link.springer.com.tiger.sempertool.dk/article/10.1007%2Fs10609-012-9183-3>.
- 22- Joseph Migga Kizza and others, "Ethical and Social Issues in the Information Age", 3rd Edition, Springer-Verlag London Limited, 2007.
- 23- JUDGE STEIN SCHJØLBERG & AMANDA M. HUBBARD, "HARMONIZING NATIONAL LEGAL APPROACHES ON CYBERCRIME", The Paper Was Prepared for the ITU WSIS Thematic Meeting on Cybersecurity, June 2005. Available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.
- 24- Leslie D .Ball, computer crime in "The information technology revolution", Cambridge, 1985.
- 25- Lori Enos, "Study: Cybercrime Continues to Boom", E-Commerce Times, 22/03/2000. Available at: <http://www.ecommercetimes.com/story/2795.html>.
- 26- Madison Ngafeso, "Cybercrime Classification: A Motivational Model". Available at: http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf.
- 27- Mansoor Al-A`ali, "Computer Crime and the Law from an Islamic Point of View", Journal of Applied Sciences, Year: 2007 Volume: 7 Issue: 12. Available at: <http://docsdrive.com/pdfs/ansinet/jas/2007/1558-1565.pdf>.
- 28- Marc D. Goodman and Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace". Available at: <http://law.scu.edu/international/File/goodmanbrenner.pdf>.
- 29- Martin Wasik, "Crime and the computer", Oxford University press, USA, 1991.
- 30- Melanie Kowalski, "Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics", Catalogue no. 85-558-XIE, December 2002, Canadian Centre for Justice Statistics. Available at: <http://publications.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf>.
- 31- Model Law on Computer and Computer Related Crime of Commonwealth. Available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

- 32- Mohamed Chawki, "Cybercrime in France: An Overview", 07 December 2005, Computer Crime Research Center. Available at: <http://www.crime-research.org/articles/cybercrime-in-france-overview>.
- 33- Na Jin – Cheon, Wu Hao, Ji Yong and Tay Mia Hao, " Analysis of computer crime in Singapore using Local English Newspapers", Raman than Mani Kandan, Nanyang Technological University, online available at: <http://www.las.org.sgsjlim>.
- 34- Nicholas Thomas, "Cyber Security in East Asia: Governing Anarchy", Asian Security, vol. 5, no. 1, 2009. Available at <http://www.tandfonline.com/>.
- 35- Paul Hunton, "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model", Computer Law & Security Review: The International Journal of Technology and Practice, Volume 25, Issue 6, November 2009. Available at www.sciencedirect.com.
- 36- Peter Grabosky, "Computer Crime: A Criminological Overview", Prepared for Presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 15 April 2000. Available at: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.4660>.
- 37- Pieter Kleve, Richard De Mulder and Kees van Noortwijk, "The definition of ICT Crime, Computer Law and Security Review", The International Journal of Technology and Practice, Year: 2011 Volume: 27 Issue: 2. Available at: www.sciencedirect.com.
- 38- Ralph D. Clifford, "Cybercrime: The investigation, Prosecution and Defense of A Computer-related crime", 2nd ED, Carolina Academic Press, USA, 2006.
- 39- Raluca Georgiana, "Borderless Crime - Computer Fraud", Database Systems Journal, Year: 2012 Volume: III Issue: 1. Available at: <http://www.dbjournal.ro> .
- 40- Recommendation of the Council Concerning Guidelines for the Security of information systems, 1992.
- 41- Recommendation of the Council Concerning Guidelines for the Security of information systems and Networks: Towards a Culture of Security, 25 July 2002.
- 42- Richard Totty & Anthony Hardcastle, "Computer-related crime", Chris Edwards, Nigel Savage and Ian Walden, "Information Technology and the law", 2nd Ed, Macmillan publishers, UK, 1990.

- 43- Robert W.K Davis and Scott C. Hutchison, "Computer Crime in Canada: An Introduction to Technological Crime and Related Legal Issues", Thomson Canada Limited, 1997, Canada.
- 44- Ronald B. Standler, "computer crime", online available at: <http://www.rbsz.com/ccrime.htm>.
- 45- Sarah Gordon and Richard Ford, "On the definition and classification of cybercrime", Journal in Computer Virology, Year: 2006 Volume: 2 Issue: 1. Available at: <http://link.springer.com>.
- 46- Taraq Hussain Sheakh, "Cyber Law: Provisions and Anticipation", International Journal of Computer Applications; Volume 53– No.7, September 2012. Available at: <http://research.ijcaonline.org/volume53/number7/pxc3882204.pdf>.
- 47- The Convention on cybercrime, December 21, 2001. <http://www.coe.int>.
- 48- Ulrich Sieber, "The international Handbook on Computer Crime "Computer related Economic crime and infringements of privacy", John Wiley & Sons, 1986.
- 49- United States Government Accountability Office, "INFORMATION SECURITY: Cyber Threats and Vulnerabilities Place Federal Systems at Risk", May 5, 2009. Available at: <http://www.gao.gov/products/GAO-09-661T>.
- 50- United States Government Accountability Office, CYBERSECURITY: "Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats", June 16/ 2010. Available at: <http://www.gao.gov/assets/130/124835.pdf>.
- 51- United States Government Accountability Office, CYBERSECURITY: "Threats Impacting the Nation", April 24/ 2012, P.9. Available at: <http://www.gao.gov/assets/600/590367.pdf>.
- 52- W. Cole Durham, Jr. and Russell C. Skousen, "The Law of Computer-Related Crime in the United States", the American Journal of Comparative Law, Year: 1990 Volume: 38. Available at: <http://www.jstor.org/stable/840559>.
- 53- W. COLE DURHAM, JR. and RUSSELL C. SKOUSEN, "The Law of Computer-Related Crime in the United States", the American Journal of Comparative Law, Year: 1990 Volume: 38. Available at: <http://www.jstor.org.tiger.sempertool.dk/stable/pdfplus/840559.pdf>.
- 54- Warren B. Chik, "Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United

States, the United Kingdom and Singapore”. Available at: www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc.

- 55- Xingan Li, “International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene”, Webology, Volume 4, Number 3, September, 2007. Available at: <http://www.webology.org/2007/v4n3/a45.html>.

Abstract

Concept of IT Crime (Cybercrime) and Computer Role for its being Committed

The information crimes are considered of more prevalent topics on the international, regional and local levels currently. This crime has taken, as result of the negative using of technology and technics related, significant space of interesting in that side, because the magnitude of effects resulting from this modern phenomenon in all areas of life to some extent.

In the time that these crimes found resonance with people who are interested in fighting them, we haven't found that they have agreement or semi-agreement on specific term or definition or classification determined to refer to the non-social and illegal actives which could fall under the title of this crime.

So, determining points mentioned above and issues related which can be arisen in the light of that term, such as determining the role played by a computer and technic systems and their relationship to the human factor, represents the fundamentals of the establishment of a legal strategy for combatting these crimes.

In this study we have examined concept of the information crime which contains: defining of the information crime, determining characteristics of the information crime and clarifying types and features of cybercriminal.

While the second part of this study has contained: determining accurate and clear classification of the information crime, displaying the relationship and the role of the information technologies and a computer in committing the crime. And a need of that technique to the human factor in fulfilling these illegal behaviors.