

جرائم الحاسب الآلي دراسة تحليلية

دكتور
أسامة حسين محي الدين عبد العال

العدد الثاني- الجزء الثاني
السنة الخامسة والخمسون - يوليو ٢٠١٣

تقديم عام

يصف العديد من رجال الإقتصاد والإجتماع والقانون الثورة الحالية للمجتمعات الصناعية بأنها ثورة المجتمعات المعلوماتية، وهي ثورة صناعية ثانية مقارنة بالثورة الصناعية الأولى التي تحققت إبان القرنين التاسع عشر والعشرين الماضيين.

ويمكن القول بأنه إذا كان هدف الثورة الصناعية الأولى هو إحلال الآلة محل الجهد البدني للإنسان، فإن هدف الثورة الصناعية الثانية هو إحلال الآلة (الحاسب الآلي) محل النشاط الذهني للإنسان.

ومن الجدير بالذكر أن مجالات عديدة كالصناعة والتجارة والنقل والطب والتعليم والإتصالات والبحوث وغير ذلك الكثير والكثير ما كانت تتقدم وتتطور وتصل إلى هذه الكفاءة التي عليها الآن لولا عاملى السرعة والدقة اللذين توفرهما الحاسبات الآلية، بحيث أصبح من الصعوبة بمكان أن تقوم القطاعات المختلفة بأعمالها دون الإعتماد على الحاسبات الآلية....

ومع إزدياد الحاجة والعمل بالحاسب الآلي والنتائج الإيجابية المحققة نتطرق إلى الجانب السلبي لهذا الوضع وهو نشوء جرائم ناتجة عن ذلك الاستخدام، وهذه الجرائم إما أن تقع على الحاسب الآلي ذاته، وأما أن تقع بواسطته، بحيث يعد الحاسب الآلي أداة فى يد الجانى يستخدمه لتحقيق أغراضه الإجرامية.

ولما كانت جرائم الحاسبات الآلية أو كما يطلق عليها الفقه جرائم المعلوماتية لإرتباطها بالمعلومات المبرمجة آلياً هي ظاهرة حديثة النشأة لإرتباطها بتكنولوجيا حديثة هي تكنولوجيا الحاسبات الآلية، ولنا أن نتصور أن الكثيرين يروق لهم القول بأن الجريمة المعلوماتية هي أشبه بالخرافة، ولا تهديد حقيقى منبعه الحاسبات الآلية، وأن كافة أشكال السلوك غير المشروع التى قد ترتبط بالحاسبات الآلية هي فى حقيقتها جرائم عادية يمكن بشأنها تطبيق النصوص الجنائية القائمة دونما أن تتميز بأية سمات خاصة.

وقد أسفرت محاولات التطبيق للنصوص التقليدية على هذا النوع الجديد

من الإجماع عن كثير من المشكلات القانونية، واختلفت آراء الفقهاء في شأن تطبيق النصوص القائمة عليها وتضاربت أحكام القضاء في البلد الواحد، فصدرت أحكام تطبق النصوص القائمة على أى سلوك ينطوى على إعتداء على المعلومات المخزنة فى الحاسبات الآلية أو استعمالها غير المشروع، فى حين إعتبرته أحكام أخرى فعلاً مباحاً لم يرد بشأنه نص يجرمه ، بينما رأى البعض الآخر أن تلك النصوص ينحسر نطاق تطبيقها على الإحاطة بجرائم الحاسب الآلى لأن موضوعها يكمن فى المعلومات التى لا يمكن إعتبرها مالاً منقولاً لا تسحب إليه الحماية الجنائية بمقتضى تلك النصوص^(١).

أهمية دراسة جرائم الحاسب الآلى:

تتجلى أهمية دراسة جرائم الحاسب الآلى فيما يلى:

أولاً: منذ الحالة الأولى الموثقة عام ١٩٥٨م لجريمة أرتكبت بواسطة الحاسب الآلى^(٢) وحتى الآن كبر حجم هذه الجرائم وتنوع أساليبها وتعددت إتجاهاتها وزادت خسائرها وأخطارها، حتى صارت من مصادر التهديد البالغة للأمن القومى للدول خاصة تلك التى تركز مصالحها الحيوية على المعلوماتية، وتحولت هذه الجرائم من مجرد إنتهاكات فردية لأمن النظم والمعلومات إلى ظاهرة تقنية عامة يخرط فيها الكثير ممن تتوافر لديهم المهارة والمعرفة فى مجال الحاسبات ويرجع هذا التحول إلى عدة عوامل منها:

- ١- تزايد وعى المجرمين بإرتفاع عائد جريمة الحاسب الآلى وتدنى مخاطرها إذا ما قورنت بأية جريمة أو نشاط إجرامى آخر.
- ٢- إحباط وإستياء أفراد الطبقة المتوسطة فى المجتمع من الأوضاع والضغوط الإقتصادية المهينى لإستغلال مراكزهم الوظيفية فى إدارة وتشغيل الحاسب لإرتكاب الجرائم بإستخدامه.

١- أنظر: د/ نائلة محمد فريد - جرائم الحاسب الإقتصادية (دراسة نظرية وتطبيقية) دار النهضة العربية- القاهرة ، ٢٠٠٤ ، صفحة ١١.

٢- أنظر: د/ هشام محمد فريد رستم- قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة- أسيوط ١٩٩٤ هامش (١) صفحة ٩.

- ٣- إتساع دائرة إنتشار المعرفة بعلوم وتقنيات الحاسب والإقبال الهائل على تعلمها من قطاعات عدة فى المجتمع وحرص الكثير من الدول على تعليمها فى المدارس والجامعات.
- ٤- تركيز المعلومات المجسدة للأصول والأموال داخل الحاسبات .
- ٥- عدم كفاية رد فعل نظام العدالة الجنائية لمواجهة صور الإجرام المعلوماتى والذى يتجلى بشكل بالغ الدلالة فى إنخفاض فرصة تعرض مرتكبيها للإيداع فى المؤسسات العقابية بعد إدانتهم قضائياً.
- ٦- صعوبة إثبات هذه الجرائم نظراً لخبرة ومهارة ومعرفة الجناة العالية بثغرات القوانين الجنائية من ناحية، ولعدم كفاية النصوص الجنائية القائمة فى أغلب دول العالم على تحقيق أدوارها العقابية فى مكافحة هذا النوع من الإجرام المنظم، إما لقصور قاعدة التجريم عن تغطية معظم صور الإجرام المعلوماتى، أو لإعتمادها على وسائل الإثبات التقليدية التى تودى إلى إفلات كثير من الجناة فى تلك الجرائم عن العقوبات التى تقررها هذه القواعد الجنائية إضافة لذلك ارتكاب صور عديدة من الجرائم المعلوماتية على إقليم أكثر من دولة، بما يصعب جهود فرق البحث الجنائى من إكتشاف الجناة وتعقبهم وإنزال العقوبات الجنائية الملائمة عليهم إن وجدت.

ثانياً: أدى ظهور هذه الأنواع من الجرائم المعلوماتية إلى تبلور أنماط جديدة من الإعتداءات على الحقوق والمصالح التقليدية بتكنيك معلوماتى جديد، ولعل من أهم صور هذه الإعتداءات (غش الكمبيوتر) إختراق شبكة المعلومات، تزييف النقود بوسائل إلكترونية، تزوير المستندات الإلكترونية والإعتداء على الملكية المعلوماتية، إتلاف البرمجيات وتدميرها وسرقة المعلومات وغسيل الأموال عبر الإنترنت، وغير ذلك من صور الإجرام المعلوماتى التى يصعب حصرها، فضلاً عن إستخدام تقنية المعلومات الحديثة فى ارتكاب الجرائم التقليدية، كعمليات التجسس وسرقة الأموال التقليدية بتكنيك معلوماتى جديد، وعمليات الإغتيال والتفجير للأشخاص والأماكن باستخدام الكمبيوتر وتقنية الإتصال عن بعد، والسب والقذف وإنتهاك الآداب والأخلاق عبر شبكات

الإتصالات المتشعبة وشبكات الإنترنت^(٣).

ثالثاً: أصبحت الحياة الخاصة للأفراد التي تعتمد في الكثير من مظاهرها على تقنية المعلومات المستخدمة، مجالاً لصور متعددة للإنتهاك، كتجميع المعلومات الإسمية عن طريق بنوك المعلومات كما أصبحت حقوق الملكية الفكرية في مجال تقنية المعلومات مجالاً خصباً للسرقة والسلب.

رابعاً: أدى ظهور الإنترنت وسهولة استخدامه إلى تغير في شخصية ومواصفات من يرتكب جرائم الحاسب الآلي، وبصفة خاصة جرائم الإنترنت ، فإذا كانت جرائم الحاسب الآلي قد ارتكبت في الماضي من أشخاص على قدر كبير من الذكاء حيث كان لا يصل إلى جهاز الكمبيوتر سوى المبرمج أو المستخدم المؤهل، فإن تطور الحاسبات الآلية وظهور الكمبيوتر الشخصي وسهولة استخدامه والتعامل مع الإنترنت ، قد قام بتوسيع نطاق وحجم المتعاملين مع الحاسب الآلي وشبكة الإتصالات المعلوماتية المتشعبة، وترتب على أن أصبح من الصعوبة بمكان حصر من يرتكبون جرائم الإنترنت في طبقة أو فئة أو جنس معين، فمرتكب الجريمة المعلوماتية قد يكون من البالغين أو من الأحداث أو المتعلمين والمتقنين ومن الفقراء أو الأغنياء، كما لم يعد بالإمكان حصر جرائم الإنترنت في نوع معين من الجرائم، فقد تكون من الجرائم الماسة بأمن الدولة من جهة الداخل أو الخارج، وقد تكون من جرائم الإعتداء على الأشخاص أو الأموال.

ومما تقدم يتبين لنا بوضوح مدى أهمية دراسة جرائم الحاسب الآلي أو جرائم المعلوماتية، التي أصبحت ظاهرة تستحق التركيز عليها ووضعها داخل دائرة الضوء وبؤرة إهتمام الباحثين.

^٣ - انظر: د/ سعيد عبد اللطيف حسن - إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت - (الجرائم الواقعة في مجال تكنولوجيا المعلومات) - دار النهضة العربية- القاهرة- الطبعة الأولى - ١٩٩٩ صفحة (٧).

صعوبة الدراسة:

لاشك أن تطور الحاسب الآلي المذهل والسريع وظهور الإنترنت وإزدهار الحاسبات الآلية ، والإقبال الكبير على إقتنائها، أدى ذلك إلى إزدياد حجم المتعاملين في مجال الحاسب الآلي ، واستتبع أيضا أن أصبح من الصعوبة حصر من يرتكبون الجرائم المعلوماتية، وكذا حصر نوعيات هذه الجرائم.

هذا من ناحية ومن جانب آخر الأمر يتعلق بإثبات الجرائم المعلوماتية فمن الجدير بالذكر أن المشكلة الرئيسية في مجال إثبات جرائم الحاسب الآلي والإنترنت صعوبة إكتشافها وعند إكتشافها يصعب ملاحظتها لأسباب منها ذكاء ودهاء مرتكبيها والسرعة الفائقة في إرتكاب هذه النوعية من الجرائم والإجرام المنظم.

وقد ترتب على ذلك أن الأدلة التقليدية في الإثبات أصبحت غير مناسبة لإثبات الجرائم المعلوماتية، الأمر الذي يستلزم البحث عن أدلة جديدة من ذات الحاسب الآلي، ومن هنا تبدأ صعوبات البحث عن الدليل وتجميعه ومدى مصداقيته وقبوله في إثبات وقائع هذه الجرائم^(٤).

وأمام هذا الشكل الجديد من أشكال الإجرام، لا يبدو القانون الجنائي الحالي كافياً لكبح جماح هذا النوع الجديد من الإجرام المنظم، فنصوص التجريم التقليدية قد وضعت في ظل تفكير يقتصر إدراكية على الثورة الملموسة والمستندات ذات الطبيعة المادية، مما يتعذر معه تطبيقها لحماية القيم غير المادية المتولدة عن المعلوماتية^(٥).

إختيار موضوع الدراسة:

سبق القول أن مجالات عديدة كالصناعة والتجارة والإقتصاد والتعليم

٤- انظر: د/ سعيد عبد اللطيف حسن - إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت - (الجرائم الواقعة في مجال تكنولوجيا المعلومات) - دار النهضة العربية- القاهرة- الطبعة الأولى - ١٩٩٩ صفحة (٩).

٥- أنظر: د/ هشام محمد فريد رستم- قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة- أسبوط ١٩٩٤ - صفحة ١١، ١٢ .

والطب والهندسة، وغير ذلك ما كانت تتقدم بذات الكفاءة التي هي عليه الآن، ويعزى ذلك بعامل السرعة والدقة اللذين توفرهما الحاسبات الآلية، ويمكن القول بأنه من الصعب الآن أن يقوم قطاع معين بأعماله دون الاعتماد على الحاسبات الآلية.

وقد أدى ذلك إلى نشوء جرائم ناتجة عن ذلك الاستخدام، ولما كانت هذه الجرائم لم نعهد لها من قبل، فإن تطبيق النصوص الجنائية القائمة عليها يسفر عن كثير من المشكلات القانونية، خاصة وأن مجرمي هذا النوع يتميز بالذكاء والوعي الشديدين، إضافة إلى صعوبة إثبات هذه الجريمة.

وإنطلاقاً مما تقدم، وعلى الرغم من أن المراجع والمؤلفات والدراسات في هذا النوع من الإجرام لا تتطور ولا تتناسب مع إزدياد وتطور هذه الجرائم، وبالتالي يصبح البحث والتحري واستسقاء المعلومة المؤكدة من الصعوبة بمكان، ومع كل هذه الاعتبارات فقد رأينا البحث فيه محاولة منا لإلقاء بعض الضوء، كمحاولة جادة للتوصل إلى أوصاف دقيقة لمفهوم الجريمة المعلوماتية، والمجرم في هذه الجريمة، إنطلاقاً من البحث في مفهومه وقواعده، مع التعمق في البحث والتوثيق التاريخي لتشريعات الكمبيوتر.

منهج الدراسة:

حتى تؤتى هذه الدراسة ثمارها المرجوة، سنعمل بعون الله وتوفيقه على إتباع المنهج التحليلي والتاريخي لتشريعات الكمبيوتر.

أ- المنهج التاريخي:

يعطى هذا المنهج أهمية كبيرة لنشأة النظام القانوني وتطوره في السنوات السابقة، الأمر الذي يساعدنا على تشخيص الظاهرة، مما نأمل معه التوصل إلى حلول مناسبة تتناسب مع الفكر والظروف الحالية.

ب- المنهج التحليلي:

ويتم ذلك باستعمال التحليل المنطقي لتشريعات الكمبيوتر والجرائم المتعلقة به، بغية إستخلاص حكم المسائل التي يثور حولها الغموض والإختلاف.

خطة الدراسة:

إحفاقاً للحق، لا أدعى قط أن هذه الدراسة قد أملت بكل جوانب جرائم الحاسب الآلي، أو غطت جانباً متكاملاً له، فذلك عمل ليس باليسير ولا تتسع له صفحات الدراسة، إنما هو عمل موسوعي نظراً لتطور وتعدد مجالات الدراسة.

وفي الواقع حاولت أن أستنتج معالم جد موجزة عن هذه الجرائم، لذلك فالدراسة تقوم على ثلاثة فصول تحليلاً وتوضيحاً للصورة وقد مهدت للموضوع بمقدمة عامة تناولت فيها أهمية دراسة هذا النوع من الإجرام وصعوبة البحث فيه وأسباب إختيار هذه الدراسة ومنهجها.

وقد قسمت الدراسة على النحو التالي:

الفصل الأول: التأصيل التاريخي لتشريعات جرائم الكمبيوتر.

الفصل الثاني: مدلول الجريمة المعلوماتية.

الفصل الثالث: تقسيم الجرائم المعلوماتية.

الخاتمة والتوصيات.

الفصل الأول

التأصيل التاريخي لتشريعات جرائم الكمبيوتر

تمهيد:

إن ظاهرة جرائم الكمبيوتر والإنترنت أو جرائم التقنية العالية، أو الجريمة الإلكترونية، أو السبير كرايم (Cyber crime)، ظاهرة إجرامية حديثة نسبياً تفرع في جنباتها أجراس الخطر لتندثر مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة، باعتبارها تستهدف الإعتداء على المعطيات بدلالاتها التقنية الواسعة (بيانات ومعلومات وبرامج بأنواعها). وبالتالي فهي جريمة تقنية تنشأ في الخفاء يقارفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات وتطال إعتداءاتها معطيات الكمبيوتر المخزنة، والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت.

هذه المعطيات هي موضوع هذه الجريمة، وما تستهدفه إعتداءات الجناة تظهر مدى خطورة جرائم الكمبيوتر، فهي تنال الحق في المعلومات، وتمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري.

لذا فإن ادراك ماهية جرائم الكمبيوتر والإنترنت والطبيعة الموضوعية لهذه الجرائم، وإستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجم منها وسمات تركيبها ودوافعهم، يتخذ أهمية إستثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية. وإنتلاقاً من ذلك، فقد تزايدت خطط مكافحة هذه الجرائم، وانصبت الجهود على دراستها المتعمقة، وخلق آليات قانونية للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية، خاصة المنظمات والهيئات الإقليمية الأوروبية، وإدراكاً لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية، كان لا بد للعديد من الدول وضع قوانين وتشريعات خاصة لضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم⁽¹⁾.

¹- إن مواجهة هذه الجرائم تم في ثلاثة قطاعات مستقلة (حماية الكمبيوتر أو ما يعرف بجرائم

ويعد من أكثر مسائل ظاهرة جرائم الكمبيوتر والإنترنت إثارة للجدل والنقاش إلى جانب تعريفها وتحديد موضوعها أو مناط الحماية ومحلها مسألة تحديد قائمة جرائم الكمبيوتر وتحديد انماط السلوك الإجرامي والأفعال المكونة له وبيان التركيب القانوني لهذه الجرائم، وهذه المسائل اجتمعت الآراء فيها نحو عدم قابلية النصوص الجنائية التقليدية عن مواجهتها وعدم كفايتها للإلتحاق على هذه الانماط الجديدة من الجرائم نظراً للتطور السريع في هذه النوعية من الجرائم.

وهذا يستدعي دون أدنى شك تعديل قوانين العقوبات الوضعية وتبني قوانين جديدة، بحيث لا تبقى بعض أو كل جرائم الحاسب الآلي خارج نطاق النص التشريعي وبالتالي بمنأى عن العقوبة^(٧).

وانطلاقاً مما تقدم فإننا سنتناول هذا الفصل في مبحثين على النحو

التالي:

المبحث الأول : التأصيل التاريخي لتشريعات جرائم الحاسب الآلي

المبحث الثاني : مفهوم قانون الكمبيوتر

الكمبيوتر ذات المحتوى الاقتصادي، وحماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية) وحماية حق المؤلف على البرامج وقواعد البيانات (الملكية الفكرية للمصنفات الرقمية) -

انظر عبر الإنترنت Lawoffc@nol.com.jo

^٧ - في ذلك يقول الفقيه الألماني (Ulrich sieber) " لقد اظهر التحليل للقوانين المختلفة ان الحماية الجنائية للمعلومات في كل دولة بحاجة ماسة لوضع نظرية عامة لها ومرد ذلك انه في غالب الحالات تمت مناقشة الحماية الجنائية لكل من الحياة الخاصة والأموال والحقوق الذهنية إزاء إجرام تقنية المعلومات على حدة" ويعد هذا الفقيه الألماني أشهر القانونيين في ميدان دراسات جرائم الكمبيوتر، وله العديد من المؤلفات منذ منتصف السبعينات، وقد كلف عام ١٩٩٨ من قبل اللجنة الأوروبية ومجلس أوروبا لوضع دراسة تفصيلية تحليلية بخصوص الموقف القانوني والتشريعي لدول اتحاد أوروبا جميعاً مقارنة بأمريكا وكندا وأستراليا حول جرائم الكمبيوتر تعد الأوسع والأشمل في هذا المجال - انظر :

Ulrich sieber (legal aspects of computer – related crimes, eu comcrime, 1998).

المبحث الأول

التأصيل التاريخي لتشريعات جرائم الحاسب الآلي

إن كل اختراع أو فتح علمي يفرز واقعاً جديداً ويرتب آثاراً ما كانت قائمة قبل وجوده، فاختراع الطائرة مثلاً خلق آثاراً جديدة في مجال نقل الأفراد والبضائع، فالتائرة تجوب العديد من الدول أثناء ترحالها في الفضاء الجوي الذي يعطو هذه الدول، والطائرة قد تكون وراء ضرر يلحق بالركاب على متنها وقد يتعرض سطح الأرض وما عليه من أملاك وأشخاص للخطر.

والطائرة وسيلة نقل هامة تتطلب أموالاً هائلة للاستثمار وتتطلب ان تلحقها خدمات عديدة غير متصلة بالطائرة ذاتها وانما تتعلق بخدمات المسافرين والمطارات وخدمات الفضاء الجوي، وهذه الوسيلة بما تملكه من قدرات التنقل والاختراق قد تعرض امن الدولة للخطر، ولضمان سلامة الطيران ورعاية قواعده وتوحيدها نشأت الهيئات والمنظمات الدولية والإقليمية والمتخصصة في مجال الطيران.

هذه الآثار وغيرها أفرزها هذا الاختراع العلمي المميز، وتطلب التعامل معها حزمة من التشريعات الوطنية والاتفاقيات الدولية والإقليمية والثانية، عالجت وتعالج النظام القانوني للطائرة والمطارات وخدمات الركاب والشحن وما ينشأ في بينها من علاقات قانونية وتعالج المسؤولية عن الأضرار اللاحقة بالركاب وبالأشخاص والممتلكات على سطح الأرض وغيرها العديد من المسائل فيما أصبح يعرف بالقانون الجوي.

وبإيجاز فالطائرة خلقت فرعاً جديداً من فروع القانون تتكامل فيه النظريات والقواعد وتمتد من النطاق الوطني إلى النطاقين الإقليمي والدولي، وذات الامر يقال بشأن العديد من المخترعات والإكتشافات.

وبذات المنطق أفرزت تقنية المعلومات آثاراً شاملة على البناء الإداري والإقتصادي والسياسي والاجتماعي والثقافي والقانوني للدولة وقد أثرت على مختلف مناحي النشاط الانساني.

ومما هو ثابت أن القراءة التاريخية التحليلية لحركة التشريع فى مجال قانونى معين تقدم أساساً هاماً لتحقيق رؤية شاملة فى التعامل مع هذا المجال ، مسائلة وتحدياته وبدونها قد لا يتحقق الإنسجام والتناغم فى الحول والتدابير التشريعية التى تستهدف تنظيم هذا المجال ، وجدير بالذكر أن التعامل مع تشريعات تقنية المعلومات حتى فى أكثر الدول تقدماً جاءت قاصرة عن الاحاطة الشاملة بالمتطلبات التشريعية والقانونية لهذا المجال، ويلاحظ ان التعامل مع تقنية المعلومات تشريعياً تم خلال حقبة زمنية متباينة وتناول قطاعات وموضوعات دون غيرها.

ففى ميدان جرائم الكمبيوتر مثلاً، تم التعامل مع الحماية الجنائية للمعلومات ضمن ثلاث محاور منفصلة:

أولها: - حماية البيانات الشخصية المخزنة فى نظم المعلومات من مخاطر المعالجة الآلية، وهو ما يقع ضمن دراسات حقوق الإنسان باعتباره ينصب على حماية الحق فى الخصوصية Privacy، أو الحياة الخاصة.

وثانيها: حماية المعلومات ذات القيمة المالية أو التى تمثل اصولاً مالية من مخاطر الانماط الجرمية المستجدة التى تعتمد الكمبيوتر وسيلة للجريمة أو هدفاً أو بيئة لها، وهو ما عرف أيضاً بجرائم الكمبيوتر Computer crimes أو الجرائم المرتبطة بالكمبيوتر Computer- Related Crimes أو جرائم الكمبيوتر ذات الطبيعة الاقتصادية Economic Computer Crimes أو غير ذلك من اصطلاحات دالة عليها، ويقع ضمن نطاق دراسات القانون الجنائى الموضوعى وهو ما عبر عنه بالعموم بوصفه الحق فى المعلومات .

وثالثها: حماية برامج الحاسبات من مخاطر القرصنة المتمثلة بالنسخ غير المصرح به واعادة الانتاج والتقليد وهو ما يقع ضمن دراسات الملكية الفكرية وتحديد حق حماية حق المؤلف Copyright.

والحق أن محاولة تقصى التدابير التشريعية فى حقل تقنية المعلومات يعنى العودة إلى بداية السبعينات.

فالتطور التاريخى لتقنية المعلومات، يشير إلى ان السبعينات تحديدا شهدت إنتقالاً حقيقياً فى ميدان استخدام الحوسبة وتقاربها بانظمة الاتصالات، فالسبعينات شهدت التوجه نحو بناء الحواسيب الشخصية وشهدت إتساعاً تجارياً

حقيقياً في استخدام الحوسبة، وشهدت إنجازات في حقل تشبيك الحواسيب وربطها مهدت لولادة عصر الشبكات. وبالرغم من أن العديد من المسائل المتصلة باستخدام الكمبيوتر قد أثرت منذ الخمسينات والستينات إلا أن تلك المعالجات لم تؤد إلى اتخاذ تدابير تشريعية، لتكون ولادة القوانين الحقيقية ذات الصلة بالكمبيوتر قد تحققت مع مطلع السبعينات.

إن المرور بمنحنيات الزمان والمكان والموضوع، سيحملنا ضمن منحنيات متداخلة، إذ يتحقق التداخل بين الفترات الزمنية لكل طائفة من التشريعات، كما يتحقق التداخل بالنسبة للموضوعات محل التنظيم، ودون القفز إلى النتائج في هذا المقام، فإننا سنعمد إلى تقصى المسيرة التاريخية لتشريعات تقنية المعلومات، من خلال تتبع موجات التشريع وتحديد أطارها العام.

ويمكننا القول بأن الملامح الأولى لقانون الكمبيوتر بدأ مع شيوع استعمال الكمبيوتر، ولأنه أداة جمع ومعالجة للمعلومات فقد كانت أول تحدياته القانونية إساءة الاستخدام على نحو يضر بمصالح الأفراد والمؤسسات، ومعه نشأ الإرتباط بين القانون والكمبيوتر الذي إنطلق من التساؤل فيما إذا كانت أنشطة إساءة استخدام الكمبيوتر تقييم مسئولية قانونية أم أنها مجرد فعل غير مرغوب فيه أخلاقياً؟

وماذا إذا كان يتعين تنظيم استخدام الكمبيوتر أم لا؟

وهذا التساؤل أثر في مجالين : الأول : - المسئولية عن المساس بالأفراد والمؤسسات عند إساءة التعامل مع بياناتهم الشخصية المخزنة في نظم الكمبيوتر على نحو يمس أسرارهم حقهم في الخصوصية، والثاني: المسئولية عن الأفعال التي تمس أو تعتدى على أموال الأفراد ومصالحهم وعلى حقهم في المعلومات ذات القيمة الاقتصادية ، ولو دققنا في هذين المجالين لوجدنا أنفسنا أمام (الخصوصية) و (جرائم الكمبيوتر).

إذن ثمة حقيقة أولى أن بداية قانون الكمبيوتر إرتبط بالبحث في المسئولية عن أنشطة تتصل بالمعلومات ونظمها وتحديداً في المجال الجزائي.

والجدل الذي دار في ذلك الوقت (الستينات تحديداً وإمتد إلى مطلع السبعينات) أشبه بالجدل الدائر منذ نحو خمس سنوات بشأن الإنترنت: هل يتعين إخضاع التقنية الجديدة، توظيفها وإستخدامها- للتنظيم القانوني ام تترك للتنظيم

الذاتي، أو كما يعبر عنه الفكر الرأسمالي (تنظيم السوق نفسه) فلا نكون أمام قواعد قانونية تقر من الاطر الحاكمة بل أمام قواعد سلوكية وشروط عقدية.

في هذا الاطار فإن أول حالة موثقة لإساءة استخدام الكمبيوتر ترجع إلى عام ١٩٥٨ وفقاً لما نشرته معهد ستانفورد في الولايات المتحدة الأمريكية ، ليبقى الحديث من ذلك الوقت وحتى مطلع السبعينات في إطار البعد الأخلاقي وقواعد السلوك المتعين أن تحكم استخدام الكمبيوتر ولتتجه الجهود والمواقف نحو حسم الجدل باعتبار اساءة استخدام الكمبيوتر فعلاً موجباً للمسئولية القانونية، ولتنطق التشريعات الوطنية في مجال جرائم الكمبيوتر مع نهاية السبعينات (تحديداً في الولايات المتحدة ابتداء من ١٩٧٨). أما الجهد الدولي فقد تحقق ابتداء في مجال الخصوصية، ففي عام ١٩٦٨ ، شهد مؤتمر الأمم المتحدة لحقوق الإنسان طرح موضوع مخاطر التكنولوجيا على الحق في الخصوصية، إذ بالرغم من أن الحق في الخصوصية نشأ قبل هذا التاريخ حظى بجدل قانوني وقضائي وفكري منذ منات السنين، فإنه لم يكن ثمة إثارة لما يتصل بهذا الحق متعلقاً بالمعلومات الشخصية المعالجة آلياً بالقدر الذي أثير في المؤتمر المشار إليه، والذي استتبعه إصدار الامم المتحدة. قرارات في هذا المجال لتشهد بداية السبعينات (تحديد عام ١٩٧٣ في السويد) إنطلاق تشريعات قوانين حماية الخصوصية مع الإشارة إلى أنها نوقشت في نظم قانونية أجنبية كثيرة- كدول أوروبا الغربية مثلاً - ضمن مفهوم حماية البيانات **Data protection**.

وإنطلاقاً مما تقدم يمكننا القول بأن الخصوصية وحماية البيانات تمثل أول مجال من مجالات قانون الكمبيوتر من حيث الإهتمام التنظيمي الدولي ويعد ذلك بمثابة الحقيقية الثانية.

ولأن السبعينات بحق الإدراك العميق لأهمية برامج الكمبيوتر وباتت تشير إلى أنها ستكون القيمة الأكثر أهمية من بين عناصر تقنية المعلومات وستفوق عتاد الكمبيوتر المادى في أهميتها ، فإن مطلع السبعينات شهد جدلاً واسعاً حول موقع حماية برامج الكمبيوتر، أهى قوانين براءات الاختراع بوصف البرنامج من المصنفات القابلة للاستثمار في حقل صناعات الكمبيوتر؟ أم أنها تشريعات حق المؤلف باعتبار البرنامج في الأساس ترتيبت منطقياً لأوامر كتابية؟ هذا الجدل ربما لم يمنع من أن يتفق الجميع على وجوب الحماية، لكن

الخلافاً كان في موضعها، فإلى جانب هذين التوجيهين، كان ثمة آراء تجد في القواعد القانونية المدنية والشروط العقدية (تحديداً في حقل المنافسة والأسرار) موضعاً مناسباً لحماية حقوق المبرمجين. في هذه البيئة الجدلية بدأت تظهر التدابير التشريعية في حقل حماية البرمجيات اعتباراً من ١٩٧٣ (في الفلبين) مع أن موجة هذه التشريعات يتم إرجاعها للثمانينات لأن الأخيرة شهدت تدابير تشريعية وطنية واسعة في حقل حماية البرمجيات بسبب الأثر الذي تركته القواعد النموذجية لحماية برامج الكمبيوتر الموضوعية من خبراء المنظمة العالمية للملكية الفكرية (الوايبو) عام ١٩٧٨.

وصحيح أن تشريعات حماية البرامج تراكمت مع تشريعات الخصوصية وجرائم الكمبيوتر، لكنها كانت أسرع تنامياً وأوضح من حيث الرؤى للمحتوى ولمستقبل هذه التشريعات، ولهذا فإنها أوسع مدى من حيث عددها وإذا أردنا أن نعرف السر فإنه في الحقيقة يرجع إلى عاملين أساسيين، الأول: وجود المنظمة العالمية للملكية الفكرية (الوايبو)، التي ساهمت عبر ملتقياتها وأدلتها الإرشادية وقوانينها النموذجية في حسم الجدل بشأن موضع حماية البرمجيات ليكون قوانين حق المؤلف. والثاني: التوجه الإستراتيجي للأسواق الرأسمالية للاستثمار في حقل الملكية الفكرية ومصنفاتها كمقدمة لبناء الاقتصاد الرقمي الذي بدأت أول ملامحة في اتجاه الولايات المتحدة الأمريكية مدفوعه بتأثير الشركات متعددة الجنسيات لوضع الملكية الفكرية ضمن أجندة إتفاقيات تحرير التجارة والخدمات ومساومة الولايات المتحدة العالم كله على قبول إتفاقيات تحرير التجارة في البضائع مقابل إنجاز تقدم في مجالى تحرير الخدمات والملكية الفكرية^(٨).

^٨ - كانت الولايات المتحدة الأمريكية من بين الدول التي رفضت الانضمام لإتفاقيات الجات (١٩٤٧) المتعلقة بتحرير التجارة في البضائع. وظل موقفها هذا واضحاً في جولات المفاوضات التجارية السبعة حتى بدأت جولة الأورغواي (١٩٨٦-١٩٩٤) والتي شهدت تحولاً رئيسياً في التجارة الدولية عنوانه قبول أمريكا ضمن تحالف مصالح مع عدد من الدول الصناعية إتفاقيات عديدة في حقل تحرير تجارة البضائع مقابل دراج إتفاقيات تحرير الخدمات (جاتس) وإتفاقية الملكية الفكرية هذا التحول الذي أدى إلى ولادة منظمة التجارة اعتباراً من ١٩٩٥/١/١ بموجب اعلان مراكش انظر تفصيلاً (الكتاب الخامس من موسوعة القانونية وتقنية المعلومات) دليل التجارة الدولية والاستثمار (إتفاقيات

ولا يعنى هذا أن بقية موضوعات تقنية المعلومات لم تحظ بدعم وإهتمام هيئات دولية، لكن الفرق أن أيا منها حتى ذلك الوقت لم يكن موضع عمل منظمة متخصصة فيه كما هو حال منظمة الوايبو التى تتولى رعاية الملكية الفكرية وإدارة اتفاقياتها.

إذن الحقيقة الثالثة، أن أكثر تشريعات قانون الكمبيوتر نضجاً ووضوحاً فى أغراضها القوانين أو التدابير التشريعية المتعلقة بحماية الملكية الفكرية لبرامج الكمبيوتر (وفيما بعد قواعد البيانات والدوائر المتكاملة) ويتصور أن تحقق هذه التشريعات أيضاً حماية أوسع فى السنوات القادمة فى مجال أسماء مواقع الإنترنت والمحتوى الرقوى لمواقع الإنترنت.

وقبل أن نتواصل مع حقائق التاريخ، علينا أن نصل فى هذا المقام إلى استنتاج ، أن مطلع السبعينات شهد الإنطلاقة الحقيقية لحزمة تشريعات الخصوصية وأن السبعينات أيضاً (وعلى إمتداد الثمانينات والتسعينات) شهد إنطلاقة الحزمة الثانية المتمثلة بقوانين جرائم الكمبيوتر، فى حين شهدت الثمانينات (فعلياً) إنطلاقة حزمة ثالثة من التشريعات المتصلة بالكمبيوتر هى حزمة تشريعات حماية البرمجيات التى تمثل المصنف الأهم من بين المصنفات الرقمية ذات الاتصال بالكمبيوتر

ثلاثة حزم تشريعية: تشريعات الخصوصية (حماية) لحق فى البيانات الشخصية من مخاطر التكنولوجيا) ، قوانين جرائم الكمبيوتر (الإعتداء على نظم المعلومات والمعلومات ببعدها الاقتصادى) وتشريعات حماية برامج الكمبيوتر (الملكية الفكرية).

هذه مجالات ثلاثة فى ساحة قانون الكمبيوتر، وسنجد أن ثمة مجال رابع يكاد يكون الوعاء الذى يضمها جميعاً وهو مجال الأعمال الالكترونية، لكن يفصل بين مجال الأعمال الالكترونية والمجالات الثلاثة، فروع أخرى ربما لا تكون مستقلة بشكل كاف فى مبناها عن الفروع القانونية التى تتبعها لكنها بالتأكيد خلقت تغيرات جوهرية إستلزمتهما تقنية المعلومات. فأول الفروع التى برزت عقب الفروع الثلاثة المتقدمة، قواعد الإجراءات الجنائية للإستدلال والتحقيق والإثبات وإجراءات المحاكمة المتفقة مع طبيعة الإعتداءات فى الدعاوى التى

تتعلق بجرانم الكمبيوتر أو الإعتداء على الخصوصية وحتى في مجال قرصنة برمجيات الحاسوب المخزنة داخل النظم أو المحملة مع الأجهزة. وبالرغم من أن الدول الأوروبية وإستراليا كذلك قد تنبتهت لهذا الموضوع مبكراً مع مطلع السبعينات إلا أن الحزمة التشريعية المتصلة بهذه القواعد بدأت حقيقة وعلى نطاق واسع في منتصف الثمانينات (إبتداء من عام ١٩٨٤ في بريطانيا).

تبع هذا المجال تدابير تشريعية في ثلاثة مجالات أخرى كان للإنترنت وشبكات المعلومات ونماء استثمارات الخدمات التقنية الدور في توجيه الإهتمام الحقيقي بها، بل في ولادة مفهوم جديد لبداياتها التي ظهرت قبل شيوع الإنترنت، فمع تحول الإنترنت إلى الاستخدام التجارى الواسع ، ظهرت تحديات قانونية جديدة، بعضها ذو إتصال بتحديات سابقة أو قائمة، كتحديات حماية أمن المعلومات فى مجالى الخصوصية وجرانم الكمبيوتر وحماية البرامج فى بيئة الإنترنت ذاتها، لما أتاحتها من تسهيل إرتكاب الإعتداءات بعد أن وفرت مدخلاً سهلاً إلى نظم الكمبيوتر المرتبطة ضمنها، وتحديات أخرى أوجبته أنماط السلوك الجديدة التى ولدت بولادة الإنترنت، كالبيع والشراء على الشبكات وأداء الخدمة عبر الإنترنت، ومن هذه التحديات التنظيم القانونى للتجارة الإلكترونية.

هذه التحديات التى أوجدتها أو ضخمتها الإنترنت أو عدلت فى نطاقها ومخاطرها وجديتها، رافقتها حزم تشريعية بدأت فى مجال ما يعرف بتنظيم الأمن المعلوماتى، والمعايير التقنية وتحديداً ما يتصل بتشفير البيانات ، التى إنطلقت فى عام ١٩٩٠ من فرنسا تحديداً، ثم فى مجال مكافحة المحتوى غير القانونى للمعلوماتية، الذى إنطلق عام ١٩٩٦ فى أمريكا. وأخيراً المجال الأكثر إثارة للجدل وأوسعها تنظيمياً، مجال الأعمال الإلكترونية الذى أشرنا أعلاه إلى أنه المجال الرابع المركزى إلى جانب جرانم الكمبيوتر والخصوصية والملكية الفكرية. ومجال الأعمال الإلكترونية ليس لاحقاً للمجالات الأخيرة الثلاث ، إنما قد نجد تشريعات فى إطاره كالتشريعات المتعلقة بتقنيات الأعمال المصرفية، أو تلك المتعلقة بحجية الإثبات بالوسائل الإلكترونية، سابق بسنوات عديدة للمجالات المشار إليها، لكن قولنا بأنه المجال الأخير زمنياً يرجع إلى تبلور مفاهيم شمولية جديدة فى مجال الأعمال الإلكترونية عكسها تحديداً مفهوم التجارة الإلكترونية والبنوك الإلكترونية وهذا المفهوم الشامل نجد أنه إنطلق مع عام ١٩٩٦ الذى

شهد إقرار القانون النموذجي للتجارة الإلكترونية من قبل لجنة الأمم المتحدة لقانون التجارة (اليونسترال). وسنجد أن دولاً على المستوى التشريعي كانت قد بدأت الأهتمام بمسائل الأعمال الإلكترونية (كالاثبات بالوسائل الإلكترونية وحجية مستخرجات الحاسوب والتنظيم القانوني لبطاقات الائتمان وغيرها) من أواخر السبعينات وبداية الثمانينات ، لكنها لم تكن ضمن التصور الشامل للتجارة الإلكترونية التي إرتبطت واقعا بانشطة الاستثمار على الإنترنت .

أما من حيث الأطر الدولية العاملة في ميادين الموضوعات المتقدمة ، فإننا سنجد الجهد الاساسي والمميز موزع بين منظمة التعاون الاقتصادي والتنمية وهيئات أوروبا- (مجلس أوروبا والمفوضية الأوروبية واتحاد أوروبا والبرلمان الأوروبي) والأمم المتحدة، ومجموعة الدول الصناعية الثمانية والوايبيو ، والانتربول ، ومنظمة التجارة الدولية وغيرها من المنظمات .

وإنطلاقاً من ذلك يمكن القول بأن تشريعات قانون الكمبيوتر تنحصر في: الخصوصية، جرائم الكمبيوتر ، الملكية الفكرية للمصنفات الرقمية، الإجراءات الجنائية في البيئة الرقمية ، المعايير والمواصفات والأطر التنظيمية للتقنية وتأثيرها على النشاط الإداري والخدمي، المحتوى غير القانوني للمعلوماتية، الأعمال الإلكترونية وتحديداً التجارة الإلكترونية، وفي إطار كل منهما ثمة تشريعات ومجهودات دولية وإقليمية وسياسات وإستراتيجيات ومحتوى ومشكلات أيضاً.

المبحث الثاني

مفهوم قانون الكمبيوتر

وفق التوصيف المتقدم أن المجالات التشريعية سبعة ، أربعة منها تكاد تستقل تماماً فى أطرها التنظيمية والتشريعية ، إلا أن كل منها شهد تطوراً فترع فى إطارها أيضاً حقوق أخرى ، بعضها يرتبط بغيره وبعضها مستقل فى موضعه عنها، لكن حركة التطور- كما سيظهر من تحليل موضوعات هذه الحقول- يأخذها شيئاً فشيئاً نحو التكاملية والتوحد فى إطار واحد ، وهذا ما سيؤدى إلى تبلور قانون الكمبيوتر كفرع مستقل عن بقية الفروع القانونية، ولو أعدنا حصر كافة القطاعات المتقدمة وما تفرع عنه سنجد أنفسنا أمام المجالات التشريعية التالية فى نطاق قانون الكمبيوتر :

- ١- تشريعات الخصوصية أو قواعد حماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية.
- ٢- تشريعات جرائم الكمبيوتر ، ومن ثم تطورها لتشمل جرائم الإنترنت وشبكات الاتصال ضمن مفهوم اشمل (امن المعلومات).
- ٣- تشريعات الملكية الفكرية فى حقل حماية البرمجيات ومن ثم تطورها لتشمل بقية المصنفات الرقمية، إلى جانب تطورها على نحو يعكس الاتجاهات العالمية فى ادراج الملكية الفكرية ضمن تنظيمات التجارة الدولية للتوجه الحاصل نحو الاقتصاد الرقوى والاقتصاد المؤسسى على المعرفة ونحو راس المال الفكرى.
- ٤- تشريعات الأصول الاجرائية الجزائية، وتشريعات الاثبات المتفقة مع عصر الكمبيوتر والمعلومات والتي هى فى الحقيقة تطوير لقواعد الاجراءات والاثبات، لكنها أيضاً تتصل عضويًا بالحقوق الجديدة المعترف بها فى ميدان تقنية المعلومات.
- ٥- تشريعات المحتوى الضار (الحماية من محتوى المعلوماتية على الإنترنت)، ثمة اتجاهات متباينة بين توجه لدمجها مع تشريعات امن المعلومات كما فى أوروبا ، أو استقلالها عنها كما فى امريكا.
- ٦- تشريعات معايير الامن المعلوماتى وتطورها إلى تشريعات المواصفات القياسية لتبادل البيانات والتشفير، وثمة أيضاً اتجاهات لاعتبارها جزءاً من تشريعات التجارة الالكترونية فى حين هناك اتجاهات لتناول كل موضوع من

مواضيعها في تشريع مستقل.

٧- التشريعات المالية والمصرفية فيما يتصل بالمال الإلكتروني وتقنيات الخدمات المصرفية والمالية وفي مقدمتها البطاقات المالية ونظم التحويل الإلكتروني والتي تطورت لتشمل اطارا جديدة في مجال التوجه نحو الاتمته الكاملة للعمل المصرفي والمالي (البنوك الإلكترونية).

٨- تشريعات الاستثمار والتجارة والضرائب والجمارك والاتصالات والانظمة الحكومية المرتبطة بالمشروعات التقنية او المتأثرة بتقنية المعلومات.

٩- تشريعات التجارة الإلكترونية (التواقيع الإلكترونية، والتعاقد الإلكتروني، والتسوق الإلكتروني)، وسنجد أن هذه الطائفة تتضمن قواعد تتصل بكافة مجال تقنية المعلومات لأنها اثارت تحديات فيها جميعا، لهذا ثمة حقيقة أن التجارة الإلكترونية وحدها برغم أنها آخر حلقات تقنية المعلومات في الوقت الراهن الا أنها الاطار الاوسع المؤهل لتوحيد قواعد قانون الكمبيوتر.

١٠- تشريعات (اتفاقيات ومعاهدات) الاختصاص والقانون المطبق على المنازعات القضائية في بيئة الإنترنت (بشكل خاص منازعات الملكية الفكرية ومنازعات التجارة والاعمال والبنوك الإلكترونية).

أمام الموجات التشريعية المتقدم الاشارة اليها، وامام هذا التطور التاريخي والحصص المتقدم لمجالات الموضوعات المتصلة بتقنية المعلومات وعلاقتها بالقانون، يرد التساؤل: ما هو قانون الكمبيوتر Computer law ، أو قانون السيبر Cyber Law؟ وماذا عن الاصطلاحات الدالة عليه؟؟ ثم ، هل ثمة اساس لبناء نظرية عامة لقانون الكمبيوتر ، ام انه سيظل مجرد مبرر لتعديل قواعد قانونية قائمة في اكثر من فرع قانوني واكثر من تشريع في نطاق النظام القانوني الواحد.

القواعد العامة لقانون الكمبيوتر:

ابتداء تجدر الاشارة الى أن كلمة (سايبير لو – Cyber law) اصطلاح دال على قانون الكمبيوتر أو قانون تقنية المعلومات درج ضمن مجموعة اصطلاحات نحتت جميعها من تعبير (سيبر سبيس Cyberspace) وهذا التعبير الاخير يترجم بمعان كثيرة، ابرزها الفضاء التخيلي، أو الفضاء الإلكتروني، وهو مصطلح نحتته المؤلف وليام جيبسون William Gibson ليشير به إلى الحقيقة التخيلية لشبكات الكمبيوتر. ويشيع استخدام هذا المصطلح كمرادف لكلمة

"الإنترنت" أو البيئة الرقمية، بل انه يحل في الاستخدام الشائع مكان كافة التعبيرات المتصلة بتقنية المعلومات.

وقد تفرع عنه عدد كبير من الاصطلاحات فنجد تعبير (السيبر كاش - سايبركاش Cyber cash) ليدل على نظام دفع النقود بواسطة الشيكات الالكترونية أو بطاقات الائتمان وتعبير سيبر تايم Cyber time للدلالة على وقت الإنترنت من الوجهة التقنية وعلى عصر الإنترنت من الوجهة التوصيفية، وتعبير (سايبير كرايم - Cyber crime) للدلالة على الجرائم الالكترونية أو جرائم الكمبيوتر، وغيرها العشرات من التعبيرات التي تنطلق من فكرة البيئة التخيلية أو الافتراضية أو الرقمية لحقائق ومفاهيم واقعية، لهذا من المهم معرفة أن هذا الاستخدام استخدام عملي شائع، ولهذا فانه وان لم يكن بدقة الاصطلاحات الاكاديمية البديلة للتعبير عن ذات المعاني، فان استخدامها ليس فيه خطأ سيما وانه يساهم في تقريب الموضوع إلى اذهان المتقنين الذين تشيع بينهم اصطلاحات الإنترنت ، وتخلق في اوساطهم ثقافة خاصة بهم^(٩).

وبالعودة إلى قانون الكمبيوتر ، فثمة خلط واسع في تحديد المقصود بقانون الكمبيوتر وذلك تبعا للرؤية التي يعتمد عليها في تحديد اقسام هذا الموضوع والاطار العلمى محل المعالجة^(١٠)، وثمة ايضا تباين بشأن مشتملاته،

^٩ - وجدير بالذكر هنا ان كل موضوع من مواضيع العلم والفن ، جرى إختراقه بعدد من الاصطلاحات التي ترافقت مع شيوع تقنية المعلومات، ورغم وجود مدافعين عن اصول اللغة ورفضهم هذه الاختراقات التي عادة ما تكون نحتا لعدة كلمات للدلالة على استخدام معين أو مفهوم معين، فان حمى انتشار الاصطلاحات ادى إلى ان تهتم كثير من مواقع الانترنت بايراد الاصطلاحات الخاصة بالموضوع الذى تعرضه. فى هذا الحقل وفيما يتصل باثر تقنية المعلومات على الثقافة واللغة عموما واثرها من منظور عربى، انظر المؤلف القيم للدكتور نبيل على- الثقافة العربية وعصر المعلومات، منشورات دار المعرفة، العدد ٢٦٥ يناير ٢٠٠١.

^{١٠} - انظر التباين الحاصل فى مفهوم ونطاق قانون الكمبيوتر ضمن مجموعة المؤلفات التالية :

- Barry B. Sookman, Sookman computer Law: Acquiring protecting Information Technology, Carwell Legal Pubns, April 2000.

- David Bainbridge- Introduction to computer Law, 5th edition, Finical Times Management, 2000.

فنجده عند الغالبية يتصل بجرائم الكمبيوتر وامن المعلومات ونظمها فقط انطلاقا من أن هذا الفرع القانوني انما نشأ فى معرض الحماية القانونية للمعلومات وتحديد الحماية الجنائية. ونجده عند آخرين الفرع المتعلق بالإبداع وحماية الملكية الفكرية، لربطهم الوجود القانوني للمعلومات بنظم المعالجة ودورها فى انتاج المعرفة ولأن المعلومات من حيث طبيعتها (معنوية) ، ونجده عند آخرين موضوعات مستقلة عن بعضها البعض لا يربطها الا تعلق اى منها بالكمبيوتر أو برمجياته أو الإنترنت، حتى وصل هذا التشتت إلى درجة أن تتناول بعض مواقع الإنترنت قانون الكمبيوتر حتى لو كان عقود بيع الكمبيوتر كمنقولات مادية. وبرأينا أن هذا التشتت طبيعى فى ظل عدم الانطلاق من نظرية عامة توّطر هذا الفرع المستجد.

ولو عدنا إلى تاريخ نشأة القوانين، كل فرع على حده، لوجدناها قد نشأت ضمن تطور طبيعى تاريخى انطلق من حاجات التنظيم القانوني للعلاقات المستجدة، لتكون فى بدايتها تنظيمات جزئية ومن ثم تتطور إلى نظريات قانونية عامة فتعود القواعد الفرعية جزء من كل محكوم بالنظريات الشمولية والاكثر من هذه الفروع القانونية نشأ فى بيئة العرف القانوني وقواعد السلوك التي احتاجت فيما بعد للتقنين القانوني ووضع المدونات التشريعية أو احتاجت على الاقل إلى استقرار قضائي بشأنها، لكن تقنية المعلومات المتسارعة فى حركتها الداخلية وفيما تفرزه من تحديات وتفرضه من تغيرات فى انماط السلوك والعلاقات القانونية ، جعل الحاجة إلى التدخل التشريعي اقرب إلى الاستراتيجية المتلائمة معها من انتظار سيادة أعراف سلوكية تتحول إلى أعراف قانونية، لهذا كان نشوه هذا الفرع واقعا اسرع من غيره.

فالقانون الجوى على سبيل المثال، لم ينشأ بمجرد اختراع الطائرة، لكنه

- Emmanuel Michau, Computer Law in France, the computer law association, May 1998

- Ricardo Barretto & Ferreira da Silva, Computer Law in Latin America, The computer law Association, December, 1997.

- Vanessa Marsland, European Computer Law: An Introductory Guide, The computer law Association, December, 1996.

نشأ عند توفر الحاجات العملية إلى تنظيم استخدام الطائر وتنظيم المسئوليات القانونية المتصلة بهذا الاستخدام، وصحيح ان قواعده في حقل المسؤولية مثلاً قد تكون في غالبيتها تطبيق للقواعد القانونية العامة في هذا المجال ، لكن كثيراً منها ايضاً مثل خروجاً عن القواعد العامة.

لهذا كان لزاماً ان ينطلق بناء نظريات هذا القانون من خصوصية المحل الذي ينظمه، فالطائرة وهي في حقيقتها منقول مادي، لم تكن لتحتل قواعد المنقولات في كل الاحوال، لان ما يتصل باستخدامها مختلف عن العلاقات التي تتصل باستخدام الأموال المنقولة الأخرى.

وبفعل جهد دولي واقليمي ووطني وتضافر الآراء القانونية والفنية وآراء قطاعات الاقتصاد الخدمي في حقل الطيران، تبلور هذا الفرع وجمع في اطاره قواعد عديدة انتمت إلى اكثر من فرع عام، فنجده يضم قواعد ادارية تنظيمية وقواعد تتصل بالمسئوليات والحقوق المدنية واخرى تتعلق بالحماية الجزائية، ولوعدنا إلى فحصها قاعدة قاعدة نجدها في الغالب تمحورت حول الطبيعة الخاصة للطائرة قيمة ومهامها واستخدامها وما اتصل بها من خدمات فرعية وما تعلق بها جميعاً من علاقات قانونية وواجبات قانونية .

فالطائرة اساس فكرة القانون الجوي وفي نطاقها صيغت نظريات الاخطار الجوية والمسئوليات القانونية للناقل في حقل نقل الركاب والبضائع وغيرها، ومن الطبيعي ان تصاغ العديد من قواعده سندا لنظريات قائمة في فرع يتحقق فيه اتصال بالقانون الجوي وهو القانون البحري، لهذا لن نجد كثيراً من التباين في حقل التزامات الناقل الجوي والبحري بشأن البضائع الا في حدود تباين مميزات النقل ذاته، لكن كل هذا لا ينفى ان نظريات عامة قد صيغت لبناء هذا الفرع القانوني، والطائرة رأس الحربة في صياغتها وليست بذاتها بقدر ما هي واسطة النقل الجوي، فما هو رأس الحربة في صياغة قانون الكمبيوتر؟؟؟ .

ربما يكون التصور الأولي انه الكمبيوتر؟؟ لكنه قطعاً ليس التصور الصحيح إذا ما تعاملنا معه كجهاز، لأن التلفاز مثلاً لم ينتج فرعاً قانونياً مستقلاً، حتى بالنسبة للإعلام وقوانينه فانه لا يمثل اكثر من واسطة من وسائط الاعلام ذاته الذي يقوم أساسه نقل المعلومات للأخرين باشكالها المختلفة مرتبطاً بالثقافة

وبحرية الرأي والتعبير. لكننا لو عدنا لمفهوم الكمبيوتر الشامل كأداة لمعالجة البيانات، لوجدنا أن (وجوده الحيوي) يتعلق بالمعلومات بأشكالها العديدة وانماط السلوك التي اتصلت بالتعامل مع المعلومات واستثمارها.

فالكمبيوتر دون قيمة إن لم تتوفر المعطيات والبرامج، والبرامج عبارة عن أوامر تنظم لنتج برنامجا ذا هدف أما تشغيل الكمبيوتر أو إنفاذ مهمات تطبيقية فيه، إذن البرنامج معلومات. وقواعد البيانات المخزنة داخل نظم المعلومات قد تضم بيانات خام تعكس حقائق لا تتغير، كالبيانات الشخصية مثل الاسم وتاريخ الميلاد وغيرها، وقد تضم قواعد معرفية وحقائق ثابتة، كقواعد البيانات التي تتضمن حقائق علمية أو قرارات محاكم القضاء مثلاً، وقد تكون قواعد إنتاجية لمعلومات معتمدة على بيانات خام مدخلة داخل النظم، ومثالها قواعد البيانات المستخدمة في تنفيذ طلبات أو الإجابة عن تساؤلات معينة. ومواقع الإنترنت تحتوي ضرراً واصواتاً وكتابات نصية، وهي جميعاً معلومات، بعضها منتج كجهد إبداعي وبعضها الآخر حقائق إعلامية أو معرفية لا أكثر.

أذن ، مادة الكمبيوتر، بل هدف وجوده، يتمثل بالمعلومات (بمعناها الشامل للبيانات والمعلومات والمعطيات) لهذا صح القول أن محل نظريات قانون الكمبيوتر هي المعلومات وهي أساس بناء قواعده، وعندما نقول المعلومات فإننا نعنيها بذاتها وبنظم معالجتها وانماط استغلالها ، وطبائع السلوك والتصرفات المتصلة بها.

ومن الحق التساؤل ؟ لماذا إذن لا يكون القانون هذا قانون المعلومات؟

(١١)

^{١١} - ورد الإشارة إلى تعبير قانون المعلومات في العديد من المؤلفات ، وهي اما موقف للمؤلف ذاته أو مجادلة فيما يستخدمه الباحثون من اصطلاحات مع بحث حول نطاق حماية المعلومات واتجاهاته، انظر بالإضافة للمؤلفات المشار إليها في الهامش السابق مباشرة.

- Lawrence M Hertz, The computer and the law , Mathew Bender & Company, 1999 USA.

- Peter B. Maggs, Computer Law: Cases, comments, and Questions. wads West worth, 1996.

- Computer Law Forms Hand book, Clark Boardman Callaghan, 1995.

الحقيقة أن هذا الاستخدام وفي اطار استنتاجنا المتقدمة اكثر دقة في الدلالة على هذا الفرع، كما أن استخدام الاصطلاحين على نحو مترادف امر صحيح، لكن شيوع تعبير أو اصطلاح قانون الكمبيوتر انما نشأ عن الاهمية الاستثنائية للكمبيوتر كوسيلة لحفظ وخن ومعالجة ونقل المعلومات، إضافة إلى أن الاعتراف للمعلومات بالحق القانوني في الحماية والمحل القانوني للمصالح الناشئة ارتبط لدى القانونيين بوعاء المعلومة لا بذاتها فحماية حق المؤلف لم يمتد لحماية الافكار والخوارزميات انما للشكل النهائي الذي افرغ فيه الإبداع، فكانت حماية البرامج بوصفها اوامر مرتبة يتمثل الإبداع فيها في عملية الترتيب لا في الخوارزميات محلها، وحماية قواعد البيانات، لا يمتد للبيانات محل القاعدة بل لتصنيفها وتبويبها الإبداعى وهكذا.

ولأن اساس قانون الكمبيوتر ومبرر وجوده الحماية القانونية للمعلومات، فإن قصره على جرائم الكمبيوتر المتصلة بحماية استخدام الكمبيوتر ومخزونه المعلوماتي والحق في ملكية المعلومة ذات القيمة الاقتصادية اما بذاتها أو بما تمثلة، قد اغفل اوجه حماية اخرى وأنماطاً معلوماتية اخرى، فاغفل بذلك البيانات الشخصية مثلا، واغفل حماية انماط التعامل الالكتروني مع المعلومات،

- John Zeleznikow. Dan Hunter, Building Intelligent Legal Information systems, little Brown & company, 1994.
- Reba A. Best, D. Cheryn Picquet, Computer law and software protection., Mcfarland & company, 1993.
- G.P.V Vandenberghe, Advanced Topics, of law and Information technology, kluwer Law International. July 1989.
- A.W.Koers, Knowledge Based Systems in Law, Kluwer law International. July 1989.
- Richard L. Bernacchi, Aguide to the Legal and Management Aspects of Computer Thechnology, little Brown & Company, 1986, (2nd edition 1993).
- Colin Tapper, Computer Law, Longman 1982 (first edition 1978).
- Daniel Brooks, Computer Law, Parctising Law Inst. 1982.

واغفل العلاقات العقدية في بيئة المعلومات، وقصره ايضا على حماية الملكية الفكرية، يحقق الحماية فقط لأوعيه المعلومات واشكالها النهائية المنطوية على عنصر ابداعى، ويغفل حماية استخدام نظمها ويغفل حماية المعلومات ذات القيمة الاقتصادية.

ومثل هذا القول ينسحب على اى رأى يحصر قانون الكمبيوتر بأحد مجالاته ليكون عاجزا عن شمول مفردات حماية المعلومات.

وبالتالى المعلومات اساس الحماية ولن نجد جدلاً أكثر من الجدل فى تحديد مفهوم المعلومات وتعريفها وما يتصل بها من حقوق^(١٢) على مدى اصبح من الشائع ان نسمع عبارة (المعلومات عضية على التعريف) وتبعاً لهذا الموقف ايضا سمعنا ونسمع ان (جرائم الكمبيوتر تأبى التعريف) (والمعلوماتية تأبى الخضوع لفكرة التعريف) وهكذا.

والحقيقة أن كل هذا الجدل مصدره التباين فى العلم موضع البحث عند الاتجاه للتعريف، فعلم المعلومات ربطها دوماً بمادة المعرفة، وعلم الاعلام ربط المعلومة بوسائل توصيل المعلومة وبالالات ومهاراته، وعلم الحوسبة ربط المعلومة بانشطة المعالجة وسلوكيات استثمارها ، وعلم القانون تعامل مع المعلومة فى نطاق المصلحة محل الحماية والحق الذى الذى يحميه القانون، وثمة تركيز على تحديد ما يتعلق أو يتصل بها من مصالح أو حقوق وما يرد عليها من قيود، وتقييم الموقف من الاعتراف بهذه المصالح أو الاقرار بهذه الحقوق.

١٢- فى الوقوف على اتجاهات تعريف المعلومات وما يتصل بها من حقوق انظر، د/ احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلى، دار النهضة العربية، ٢٠٠٠، ص ٢٥ وما بعدها، وكذلك د. سعيد عبد اللطيف حسن، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت ، ط١ دار النهضة العربية، ١٩٩٩، القاهرة، ص ٣١ وما بعدها، د/ محمد شامى الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، ط٢ دار النهضة العربية، ١٩٩٨، وكذلك هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة، ١٩٩٢.

إذا انطلقنا من التحديد المتقدم والحقائق التاريخية لنشوء هذا الفرع، فإننا نصل إلى أن قانون الكمبيوتر هو ذلك الفرع الذى ظهر بسبب المسائل القانونية المستجدة والفريدة التى نشأت من استخدام الكمبيوتر والإنترنت، ويتميز عن غيره من الفروع بأنه متعدد الاثر والتاثير، فهو يطال فروعاً قانونية عديدة من الفروع المعروفة ضمن تقسيمات القانون، ويشمل فى نطاقه مسائل التعاقد، والاثبات، والضرر، والملكية الفكرية، والتوظيف، والدستورية، والبنوك والجزائى، والاجراءات والمدنية.. الخ.

ومن جهة اخرى وبرغم اتساع وتشعب مسائلة، فانه فرع ضيق يتعلق بمساحة ضيقة هى المسائل المرتبطة بالكمبيوتر (Computer- related topics)، على أن يكون مفهوماً أن الكمبيوتر ليس مجرد الحوسبة ومعالجة البيانات، بل المفهوم الشامل للكمبيوتر كنظام ادخال وخزن ومعالجة وتبادل ونقل للبيانات، اى يشمل وسائل الحوسبة والاتصالات بتفرعاتها العديدة، والمعبر عن دمجها فى هذه المرحلة بشبكات المعلومات وفى مقدمتها الإنترنت.

والاطار الضيق لقانون الكمبيوتر- من حيث يتعلق بالكمبيوتر واثره تمتد بالمقابل إلى مساحة رحبة من الاجابة عن تساؤلات عديدة، تغطى مسائل متنوعة، تتعلق بمسئوليات مختلفة المنشأ والمصدر: كيف احمى برنامج الكمبيوتر؟ هل يمكننى مقاضاه مزود خدمة الإنترنت على انقطاع الخدمة؟ هل يمكننى مراقبة اداء الموظفين عبر البريد الالكتروني ورسائلهم فى بيئة العمل؟ هل ابرام العقد على الإنترنت صحيح؟؟ كيف السبيل لانشاء موقع على الإنترنت وحماية محتواه من القرصنة؟ هل ارسال رسالة مازحة عبر البريد الالكتروني وتكرار ذلك بشكل ينقل نظام المتلقى ويزحمة يشكل مسؤلية قانونية؟ كيف يجازى من يطلع على اسرار مؤسسته التجارية عبر الدخول إلى نظام الكمبيوتر؟؟ هل تعتبر الرسائل الموقعة رقمياً رسائل صحيحة موقعة منى؟؟ هل انزال مقطوعة موسيقية عن الشبكة ووضعها على كمبيوتره الشخصى يخلق مسؤلية قانونية؟

إن الكمبيوتر اكثر من مجرد تقنية جديدة، انه وسيلة مؤثرة فى تغيير اتجاهات الثقافة والسلوك انه يمس كل ما نعمل ويخلق عدد من المسائل القانونية

خلال ذلك، حتى أن المفاهيم القانونية الرئيسية والبدئية قد تآثرت، فحتى وقت قريب ما كان احد يتصور أن الآلة ممثلة بالكمبيوتر ، قد تقوم بتصرفات أو تبرم عقوداً، لكن الآن ثمة العديد من نظم الكمبيوتر الذكية المرتبطة بشبكة الإنترنت تقوم بإبرام تصرفات وعقود دون تدخل بشري، الطلبات تجرى من كمبيوتر لكمبيوتر، البضائع تنقل والنقود تتداول.. ماذا يحصل عندما يحدث خطأ في الكمبيوتر أو في انفاذ اي كمبيوتر للصفقة على نحو خاطئ؟ هل يخل الكمبيوتر بالعقد؟

أن مبالغ ضخمة تستثمر في حقل التكنولوجيا ، انشاء وشراء الشبكات واطلاق مواقع الإنترنت (web sites)، الاستثمار في قواعد البيانات وعمليات المعالجة، البرمجة وتطوير البرمجيات، الخدمات التقنية بمختلف انواعها، ولو دققنا في هذا الانشطة لنتبين - مثلاً- الجهة التي تقوم بتنظيم عقودها ، لاكتشفنا حقيقة غريبة، وهي أن غالبية العقود- خاصة التي تعقد في البيئة العربية- يضعها اداريون وتقنيون وماليون ولكنهم قطعاً ليسوا من مجتمع القانون المختص بهذه الاعمال .. لماذا؟ لأن هذه عقود تتطلب لإعدادها فهماً وإدراكاً للجوانب التقنية، ادراكاً للجوانب العملية لتصرفات المستهلكين وجهات الانتاج والخدمة، والاطلاع على الجديد من القوانين، وليس في البيئة العربية فحسب، بل حتى في دول متقدمة، ثمة عقود ضعيفة البناء، فقيرة المحتوى ، مع أن جملة هذه الموضوعات تفرض عقود أكثر عمقا وتعميقا لانها ستمثل في الحقيقة القانون الذي يحكم النزاع وضعف العقود وثغراتها هو الذي يخلق منازعات متعددة في الواقع العملي.

والأصل أن المحامين اذ يتولون اعداد العقود فانهم يهدفون إلى منع النزاع- على الاقل في المسائل الرئيسية- وترك جانب قليل ليكون محل خصام ، ولا يعقل أن تكون التكنولوجيا عاجزة عن منع النزاع أو بشكل اسوء، أن تكون هذه العقود السبب في حصوله عند عدم دقتها وعند اتصافها بالعمومية بما تفتحه من فرصة لكل طرف للتشبث بما يخدم مصلحته ويبرر مسلكة

إن عقود الكمبيوتر (computer contracts) والخدمات التقنية الجيدة- كعقود توريد الاجهزة، ونقل المعرفة، وعقود البرمجيات ورخصها،

وعقود الخدمات التقنية في المؤسسات المالية أو عقود خدمات بناء المواقع وإدارتها ، والدعم والتطوير وعقود خدمات الاعلان الالكتروني .. إلخ - هي التي تجيب عن الاسئلة الرئيسية في المجال أو الموضوع الذي تعالجه: - ما الذي يؤديه النظام التقني؟ ما هي سرعة الاداء؟ كيف تؤدي الخدمة؟ ما هي خيارات المستخدم؟ ما هو الفحص أو المعاينة المقبولة لقبول الاجهزة أو البرمجيات الجديدة؟ ما هي كفالة الضمان وما هي شروطها ومدتها ونطاقها؟ ما هي حدود المسؤولية، اهي مطلقة ام مسنولية محددة، ووفقا لماذا هي محددة، وما مقدارها، والى اى مدى يتفق تحديد المسؤولية مع قواعد النظام القانوني؟ هل ثمة قيود على تحديد المسؤولية في بيئة الكمبيوتر؟ ماذا عن قواعد حماية المستهلك؟ من يملك حقوق الملكية الفكرية؟ لمن تؤول عند انتهاء الشركات خاصة شركات الاعمال غير المسجلة؟ ما هي معايير الخدمة التقنية، السرعة، مدة الانقطاع، المسؤولية عن الانقطاع؟ اين يتم حل النزاع، كيف يتم حله، اى قانون يطبق.

وقانون الكمبيوتر يختص ايضا بشئون الشركات العاملة في حقل صناعة الكمبيوتر والبرمجيات والاتصالات أو النقل، شركات تقنية المعلومات (It companies) ، كمزودي خدمات الإنترنت ("ISP" Internet service provider) ومنتجي الكمبيوتر والبرمجيات (Manufacturers) والموزعين (Distributors) ومطوري البرامج ومواقع الإنترنت (Software and web site developers) ومحلي النظم والشبكات واختصاصيي تكاملها (Network integrators) وغيرها في حقل صناعة الكمبيوتر والشبكات والبرمجيات وجميعها تتطلع إلى قانون الكمبيوتر لتحمي نفسها وتحقق اغراضها من خلال المشورة القانونية التي يقدمها قانون الكمبيوتر. انهم يحتاجون القانون من اجل عقد الصفقات، رخص الملكية الفكرية، حقوق التوزيع والاعلان، قانونية ما يقدمونه من مواد أو خدمات أو يحتاجونه لينظم لهم عملية اطلاق خدمات تجارية الكترونية مثلا أو خدمات الكترونية اخرى. قد تحتاج شركات تزويد خدمات الإنترنت لتعرف مسنوليتها تجاه المشتركين معها، كالمسئولية عن عدم وصول البريد الالكتروني، أو مسنوليتهم عند قيام احد مشتركهم بارسال رسالة تهديد أو رسالة مساس بسمعة الغير أو قيامه باى عمل غير قانوني عبر الشبكة من خلالهم ، وقد تحتاج هذه الشركة معرفة موقف القانون عندما تطلب منها جهة تحقيق ، كالشرطة الفدرالية الامريكية مثلا (FBI) المعلومات السرية عن المشتركين ومراسلاتهم. وقد

يحتاجون القانون عند إبرام صفقات البيع والشراء والاندماج والمشاركة المتصلة باعمالهم.

والاختصاص بنظر منازعات الإنترنت والقانون الواجب التطبيق ومشروعية امتداد التحقيق والتفتيش والضبط إلى خارج الحدود والاعتراف القانوني بوسائل التعاقد الالكترونية والمراسلات الالكترونية وحماية البيانات الشخصية من أنشطة الاعتداء، سواء من الغير ام من جهات معالجة هذه البيانات والانماط الجديدة فى الاستيلاء على المال عبر استخدام الكمبيوتر وأنشطة المساس بنظم الكمبيوتر والمعطيات المخزنة فيها وموقف المحاكم من منازعات الإنترنت، قبولاً واختصاصاً ومحتوى.. أنها جميعاً من مسائل قانون الكمبيوتر اذن .

فقانون الكمبيوتر هو كل شئ عن تألف الكمبيوتر والإنترنت والفضاء الافتراضى مع النظامين الاقتصادى والقانونى للدولة، انه مصدر خلق احكام واقرار نتائج قابلة للادراك والتنبؤ بها فى ظل التصرفات الافتراضية وفى اطار البيئة الافتراضية، وذلك من خلال قواعد عقدية وقانونية واضحة. ويعد قانون الكمبيوتر لذلك، الفرع القانونى الذى يعنى بالقواعد القانونية الناجمة عن استخدام الكمبيوتر بمفهومه الواسع (الدمج بين الحوسبة والاتصالات ومحتوى المواقع المعلوماتية) وتتصل بعمليات الكمبيوتر أو شبكات المعلومات (وتحديدا الإنترنت) وبأى تصرف أو سلوك فى هذا الاطار يتصل بالمعلومات ونظمها^(١٣).

^{١٣}- انظر: Mark Grossaman على الانترنت حيث يهتم بقانون الكمبيوتر منذ عام ١٩٩٦-
www.mgrossmanlaw.com وانظر ايضا موقع :

الفصل الثاني

مدلول الجريمة المعلوماتية

تمهيد:

يؤكد الخبراء أن الجرائم الالكترونية تزداد كلما توغل العالم في ازدياد استخدام الإنترنت، فالإنترنت بوابة بلا حراس بل هي ساحة إجرام تتحدى الاجهزة الامنية بما لديها من ثغرات قانونية ضخمة، مما أتاح لمافيا الجرائم الالكترونية التجول خلالها دون رقيب أو حسيب، وتكشف الخصوصية والسرية التي تنطوى عليها لغة الكمبيوتر، وكذلك يمكنها نقل المعلومات المحظورة بمجرد الضغط على زر بلوحة المفاتيح، دون أي مجهود ودون أي خوف من العقاب. مدلول الجريمة المعلوماتية:

الجريمة المعلوماتية لها مسميات كثيرة، فهي جريمة الكمبيوتر والإنترنت، والبعض الآخر يطلق عليها الجريمة الالكترونية، وهي جريمة إساءة استخدام تقنية المعلومات، وقد بذلت محاولات متعددة تسعى إلى ايجاد تعريف مناسب لهذه الجريمة وان كانت جميعها لا تخرج عن أحد اتجاهين:

الإتجاه الأول:

يرى انصار هذا الإتجاه أن الجريمة المعلوماتية هي " كل سلوك غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية، وملاحقته وتحقيقه من ناحية اخرى "

وبمعنى آخر هي " نشاط إجرامى تستخدم فيه تقنية الحاسب الآلى بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامى المقصود"^(١٤).

وطبقاً لهذا التعريف فانه يجب أن تتوافر معرفة التكنولوجيا الخاصة بالحاسبات الآلية بدرجة كبيرة، ليس فقط من أجل ارتكابها ولكن أيضاً من أجل التمكن من ملاحظتها والتحقيق فيها على نحو صحيح، أى أن يكون مرتكب الجريمة المعلوماتية والقائمون على ملاحظتها على درجة كبيرة من العلم بهذه التكنولوجيا.

ويرى مؤيدو هذا الإتجاه، أن الجرائم التى تفتقر إلى هذه الدرجة من

^{١٤} - انظر: د/ محمد الامين البشرى- التحقيق فى جرائم الحاسب الآلى - بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت-كلية الشريعة والقانون-جامعة الإمارات مايو ٢٠٠٥ صفحة ٦.

المعرفة تعد جرائم عادية تتكفل بها النصوص الجنائية العادية، ولا داع إطلاقاً لنصوص جديدة أخرى، وذلك خلافاً للجرائم التي تتوافر لها هذه المعرفة حيث تحتاج نصوصاً جديدة تتلاءم مع طبيعتها.

ويذهب البعض من مؤيدي هذا الاتجاه، إلى أن الجريمة المعلوماتية هي " كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومة المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقة".

ومع تقديرنا لهذا الرأي، وبقدر وجاهته إلا أننا نرى عدم تطلب القدر الكبير من المعرفة التقنية لارتكاب الجريمة المعلوماتية، فجريمة اتلاف البيانات المخزونة وسرقة المعلومات، لا تتطلب قدراً كبيراً من العلم بهذه التكنولوجيا، وكذلك هذا الاتجاه يخرج من نطاق الجريمة المعلوماتية كثير من الأفعال غير المشروعة جنائياً، والتي تستخدم الحاسب الآلي كأداة لارتكابها كالاختيال المعلوماتي وإشاعة الفواحش والأفعال المخلة بالأداب العامة عن طريق الحاسب الآلي^(١٥).

الاتجاه الثاني:

ذهب بعض أنصار هذا الاتجاه إلى القول بأن الجريمة المعلوماتية هي كل فعل غير مشروع يتم بمساعدة الحاسب الآلي، أو هي كل جريمة تتم في محيط الحاسبات الآلية.

وهذا الاتجاه يوسع كثيراً من مفهوم الجريمة المعلوماتية.

ويرى البعض الآخر من أنصار هذا الاتجاه أن الجريمة المعلوماتية هي " كل تلاعب بالحاسب الآلي ونظامه من أجل الحصول بطريقة غير مشروعة على مكسب للجاني أو الحاق خسارة بالمجنى عليه".

وانطلاقاً مما تقدم يمكن تعريف الجريمة المعلوماتية بأنها " كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دوراً لإتمامه على أن يكون هذا الدور على قدر من الأهمية"^(١٦).

^{١٥} - أنظر د/ نائلة عادل محمد فريد - جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية) دار النهضة العربية- القاهرة، ٢٠٠٤، صفحة ٢١- ٢٣.

^{١٦} - أنظر د/ نائلة عادل محمد فريد - المرجع السابق، صفحة ٢٥- ٢٦.

ولا يختلف الامر سواء كان الحاسب الآلي اداة لإتمام النشاط الاجرامى ام كان محلا له، ففي جريمة الاتلاف قد ينصب نشاط الفاعل على الحاسب الآلى ذاته أو على اى من مكوناته المادية وفي هذه الالة لا يعدو الحاسب الآلى أن يكون محلاً مادياً ينصب عليه سلوك الجانى الإجرامى دون أن يكون لوجوده اى دور فى الجريمة المعلوماتية، أما إذا انصبت فعل الإتلاف على المكونات المنطقية للحاسب الآلى (كالمعلومات أو البرامج أو أنظمة التشغيل) فان للحاسب ونظامه فى هذه الحالة دوراً مهماً لإتمام الجريمة المعلوماتية

مدلول الجريمة الالكترونية:

تعتبر الجريمة الالكترونية من أخطر الجرائم التي ترتكب عن طريق الإنترنت نظراً لتوسع استخدامها وتشعبها في شتى المجالات، وكذا إتساع نطاق مستخدمي شبكة الإنترنت بعد أن كانت قاصرة على البحث العلمي، واصبحت الشبكة مجالاً خصباً لنقل المعلومات الخطرة والهامة والحيوية سواء على المجالات المخبرائية أو الامنية أو الاقتصادية، والجريمة الالكترونية تعد نوع من انواع جرائم المعلوماتية.

والجريمة الالكترونية يمكن وصفها بانها: كل فعل يستهدف القضاء على استخدام التكنولوجيا الحديثة عبر الوسائط الالكترونية " ومع غزو الإنترنت دول العالم أصبح من الصعوبة بمكان ضبط وكشف هذه الجرائم نظراً لكونها عابرة للحدود ولا دين ولا وطن لها وتتم بسرعة فائقة دون رقيب أو حسيب ودون رقابة من اي دولة مما ادى إلى ارتكاب كافة صور النشاط الاجرامى المتعارف عليها عبر الإنترنت حتى القتل والسطو على برامج الحاسب بغرض سرقة البيانات وقاعدة المعطيات المعلوماتية حتى السرية منها واستخدامها فى التجسس أو تلك المتعلقة بالقرصنة والسطو على الاموال إلى جانب ظهور الارهاب الالكتروني وتهديد الامن القومى للدول ، وكذا جرائم الآداب العامة والمساس بالاخلاق من خلال الاباحية الالكترونية التى تجسدها المواقع الجنسية الاباحية^(١٧) ، خاصة الموجهة منها للاطفال والمقدرة باكثر من الف موقع يقدم مواد جنسية اباحية خاصة بالاطفال دون سن البلوغ يتم فيها استخدام دعارة الاطفال والنساء^(١٨) ، سواء بالغين أو قصر عن طريق تصويرهم مباشرة أو بالمحاكاة والتمثيل الرقمية للصورة باستعمال وسائل الترغيب والترهيب بالإغراء والتحذير أو التهديد.

١٧- انظر: د/ سعيد عبد اللطيف حسن - الجرائم الواقعة فى تكنولوجيا المعلومات - كلية الشريعة والقانون - القاهرة - ١٩٩٩ .

٢- انظر: د/ مدحت رمضان- جرائم الاعتداء على الاشخاص والانترنت - دار النهضة العربية - ٢٠٠٠ .

ويمكن القول بان الجريمة الالكترونية الخالصة تنطوي على ست خطوات اساسية^(١٩) يتم تنفيذها آلياً بواسطة برنامج أو عدة برامج، دون تدخل العنصر البشري وهذه الخطوات على النحو التالي:

١- البحث عن نظام الحاسب الآلي الذى يحتوى على المعلومات أو البرامج المطلوبة.

٢- الوصول إلى نقاط الضعف فى النظام الذى يحتوى على هذه المعلومات أو البرامج.

٣- الاستفادة من هذه النقاط للدخول إلى النظام ثم التحكم فيه.

٤- تنفيذ السلوك الإجرامى الذى تم التخطيط له وتحديده مسبقاً.

٥- تحويل هذا السلوك إلى ربح غير مشروع يحصل عليه الجانى أو إلى خسارة تلحق بالمجنى عليه.

٦- إخفاء جميع الأدلة تجنباً لكشف الفاعل وسلوكه الإجرامى.

وانطلاقاً مما تقدم ، فإننا نتناول هذا الفصل على مبحثين على النحو

التالى:

المبحث الأول: ماهية المعلومات

المبحث الثانى: خصائص الجريمة المعلوماتية.

١٩- أنظر د/ نانلة عادل محمد فريد - مرجع سابق، صفحة ٢٩، ٣٠ .

المبحث الأول ماهية المعلومات

المعلومات، هل هي ، مال، شئ ، شئ ذو قيمة، كيان، كيان معنوي. هل لأنها تتصل غالباً بوعاء تفرغ فيه ترتبط عضويًا بوعائها لذا فهي شئ مادي بالنظر للوعاء المفرغة فيه؟

أن المعلومات ذات طبيعة معنوية، تستقل تماما من حيث الاصل عن الوعاء المفرغة فيه وتعدو النظرة قاصرة إذ اتجهت نظريات قانون الكمبيوتر نحو حماية المعلومات وفق وعائها.

والمعلومات شائعة من حيث الاصل ، وحصيلة تراكم معرفي بشري ، ومن هنا ينشأ لكل فرد الحق في الوصول اليها ، ويتعين ان يكفل حق انسيابها وتدفعها ، وهذا هو جوهر واساس فكرة الحق في المعلومات.

لكن المعلومات فيما اتجهت اليه أنشطة تقنية المعلومات: -

اولا: أما أنها امست بذاتها ذات قيمة اقتصادية عالية تزداد يوما بعد يوم، لذا وصفت وتوصف بأنها المال، والمال من حيث الاصل يحظى بهذه الصفة لإتصاله بحق التملك، ملكية فرد أو شخص للمال، فمتى ما كانت المعلومات مال فانها قابلة للتملك وهو ما يفرز مفهوم الحق في ملكية المعلومات.

ثانيا: أو أنها - اي المعلومات - قد تتصل بشخص دون غيره عندما تتعلق ببياناته الاسمية أو الشخصية، لكنها تستخدم من الغير، وبالذات السلطات، لاغراض تتصل بالنشاط الاجتماعي والاقتصادي والسياسي في الدولة، من هنا تنشئ المعلومات حقا في السيطرة عليها، وحق في استخدامها ضمن قيود وضوابط، وهنا تبدأ وتنتهي حدود الحق في الخصوصية المعلوماتية، أو الحق في حماية البيانات الشخصية.

ثالثا: والمعلومات قد تكون الخلق الإبداعي للفكرة أو الابتكار فى تنظيم الحقائق والاورام، فنكون امام مصنفات وليده الاداء الإبداعي لعقول المؤلفين والمخترعين تمثل وعاء المعلومة، فتكون لذلك وبما انطوت عليه من عناصر تتطلبها نظام الملكية الفكرية، مادة حق الملكية الفكرية وموضعا للاستثمار المعنوى والاستغلال المادى، فتخلق بذلك الحق فى الملكية الفكرية للمصنفات المعلوماتية.

والقانون ليس بوسعه ان يكون وسيلة تنظيم إلا لحق يعترف به ويكفله القانون، وليس ثمة حماية الا حيث تتوفر المصلحة التى يحميها القانون، لهذا كان وجود قانون الكمبيوتر مرتببا بالاعتراف بالحق فى المعلومات، انسيابها وتدققها وقدرة الفرد على الوصول، لكن هذا الحق يثير اشكالية نطاق السيطرة على المعلومات عبر ما سيوفره الاعتراف بهذا الحق من مكناات وسلطات قانونية ، هذه السيطرة التى تتعارض جوهريا مع مفهوم الحق فى شيوع المعلومات وقدرة اى فرد فى الحصول عليها، وهذا إلى جانب ما تتصف به المعلومات من شمولية تمتد للأفكار والحقائق كان وراء دعوات عدم إخضاع الحق فيها لأية قيود. لكن الحقيقة ان ما ارتبط بهذا الحق من حقوق اخرى كالحق فى ملكية المعلومات والحق فيما يتصل بها من حقوق فكرية والحق فى الخصوصية انما هى ليست قيودا على الحق بالمعلومات بقدر ما هى تنظيم للمكناات والسلطات التى تقع فى نطاق الحق فى المعلومات وتنظيم للمصالح المعترف بها قانونا فى نطاق هذا الحق.

اذن، المعلومات كيان معنوى، يتعين الاعتراف بحمايتها بهذه الصفة وبما يتصل بها من سلوكيات واداء وانشطة استثمار، تماما كما تم الاعتراف بالمال المادى وخضع لقواعد ونظريات فى المجالين المدنى والجزائى، وأساس حماية المعلومات توفير الاطار القانونى المشابهة (من حيث شموليته ونطاقه وفعاليتيه) لذلك الذى وفرته التشريعات للمال المادى. والحق فى المعلومات يوجب اقرار مبادئ كفالة حرية الوصول للمعلومات واقرار قواعد بشأن ضوابط استخدامها والاطار القانونى لممارسة المكناات والسلطات المتصلة بها.

وفى اطار الحماية القانونية للمعلومات، ثمة مصلحة حقيقة يتعين ان يحميها القانون وهى حق الافراد فى المعلومات ، وحقهم فى سلامة ومشروعية

التعامل مع بياناته الشخصية، وحققهم في ثمرة ابداع عقولهم المتصلة بنطاق المعلومات والمفرغة ضمن مصنفات تحميها قواعد الملكية الفكرية، وحق مالكي المعلومات (باشكالها المختلفة) المصنفة او الخاصة بنشاطهم الاستثماري أو التجاري وادارتهم للمعلومات التي تمثل راس المال الفعلي لمشروعاتهم، وحق الفرد في سلامة ما يتعامل معه من معلومات سواء المرسله منه ام المستقبله ام المخزنة في نظامه التقني، واذا ما حولنا هذه الحقوق إلى مسميات فاننا نكون امام: الحق في المعلومات، الحق في ملكية المعلومات، الحق في الملكية الفكرية للمعلومات، الحق في الخصوصية المعلوماتية، الحق في ادارة المعلومات، الحق في امن التعامل المرتكز على المعلومات.

هذه هي المصالح المتعين حمايتها والحقوق المتعين الاعتراف بها، فاذا ما اردنا تحويلها لقواعد (عملية) تتصل بالمعلومات للانطلاق في رسم ملامح النظرية العامة للمعلومات فاننا نكون امام الاسس العامة التالية (المتعين اقرارها في النظام القانوني) :

١- ان الفرد من حيث الاصل له الحق في الحصول على المعلومات ، وتظل الحقائق والافكار العامة ملكا شائعا للبشرية لا ترد عليها مكناات قانونية تحد من الافادة منها ولا سلطات استثنائية الا متى ما اتصلت بجهد خلقي (ليس هو دائما المفهوم المقرر في نظام الملكية الفكرية فحسب) يبرر الاقرار بمصالح وحقوق ترتبط بصاحب الجهد الخلقى المتصل بها. فالافكار حول تصميم موقع الإنترنت تظل افكار شائعة لا يستأثر بملكيتها احد لكن متى ما تحولت إلى انماط خلقها مصمم موقع ما كانت ملكا في اطارها الإبداعى هذا للشخص الذى ابتكرها ، والخوارزميات المستخدمة فى البرمجيات لا يدعى ملكيتها احد، لكن ورودها ضمن تبويب معين ينتج برنامجا مبتكرا تخلق للشخص الذى قام بذلك مكنة الاعتراف بحقة فى نسبة هذا الإبداع له وفى حماية استغلاله المادى، وهكذا.

٢- ان البيانات الشخصية عنصر من عناصر حماية السرية الشخصية واحترام الحياة الخاصة يتعين ان تخضع من حيث نطاق الحماية لما خضعت له عناصر حماية الخصوصية المادية ، المسكن والمراسلات وغيرها.

٣- ان المعلومات ككيان معنوى لها ذات القيمة الاقتصادية للمال المادى، يتعين

ان تخضع لاحكامه وتعامل تماما كما يعامل ، فتحيطها حماية ذات الحقوق المقررة على المال المادى ويعترف لها بذات المصالح التى يعترف بها القانون للمال المادى.

٤- فى نطاق التصرفات المدنية والتجارية ، فان السلوكيات والتصرفات القائمة فى البيئة الرقمية (بيئة الكمبيوتر والإنترنت) يتعين ان تكون مقبولة ومعترف بها تعبيرا عن الارادة وعن الالتزام القانونى تماما كتلك التصرفات المعتمدة والمقبولة فى البيئة الحقيقية متى ما تحقق لها عنصر القدرة على التعبير بشكل صحيح منتج لاثره.

٥- وفى نطاق الحماية الجنائية يتعين الاقرار بصلاحيه المعلومات كمحل للحماية من أنشطة الاعتداء كافة، تماما كما المال المادى المحمى ضمن نصوص وقواعد حماية الاموال، ويتعين الاعتراف لمحيط المعلومات ووعائها التقنى بالصفة المقبولة لخضوعه للتصرفات التى ترتكب فى بيئة المحرر الكتابى والمستندات الخطية. ويتعين المساواة بين السلوكات المادية فى انتهاك السرية وبين السلوكيات المعنوية فى انتهاك الخصوصية.

٦- أن محل الجريمة المعنوى له ذات القيمة المعترف بها للمحل المادى للجريمة والسلوك المعنوى للجريمة تقوم به الجريمة تماما كما تقوم بالسلوك المادى فعلا وتركيا.

٧- ان قواعد الضبط والتفتيش فى البيئة الرقمية يتعين ان تتناسب مع مميزات هذه البيئة تماما كما تناسبت قواعد الضبط والتفتيش فى الوسط المادى مع مميزات وسلوكيات هذا الوسط.

٨- الادلة ذات الطبيعة الالكترونية يتعين مساواتها بالادلة ذات الطبيعة المادية – الادلة القائمة على الكتابة والورق – من حيث المقبولية والحجية.

٩- كلما كان التصرف المادى فى البيئة الواقعية محل اعتبار يتعين الاعتراف بما يقابله من تصرف معنوى فى البيئة الرقمية، فالتوقيع الالكترونى يقتضى مساواته بالتوقيع المادى. والتصديق الالكترونى يتعين مساواته بالتصديق المادى، وهكذا شريطة ان تحقق البيئة الرقمية من حيث المعايير والاجراءات المتصلة بالسلوكات المعنوية أو سلوكيات البيئة الافتراضية ما يوفر الثقة التى تحلت بها السلوكيات المادية.

١٠- ان البيئة الرقمية متى ما تحقق نمط ومعيار اجرائى يكفل لها الموثوقية والثقة بالسلوك فى بيئتها والاطمئنان للدليل المستخلص من وسائلها يتعين

ان تعامل كالبيئة الحقيقية، وفي نطاقها يكون الحق محل اعتراف وتكون المصلحة موضع تقدير وتكون القاعدة القانونية منطقية اذ لم تقبل تمييزاً بين بينتين توفر لهما ذات المعيار من حيث الثقة وذات العناصر من حيث الاطمئنان.

١١- ان المعلومات بذاتها وبما يتصل بها من سلوكيات متى ما تحقق الاعتراف القانوني بكيانها والاعتراف بما يتصل بها من تصرفات وما تنشئها التصرفات هذه من اثر ونتائج ومسئوليات، وما يتبع بها من حقوق ومصالح، حققت الاسس القانونية المقر بها ضمن قواعد كافة فروع التشريع الدستورية والمدنية والتجارية والمالية والادارية والجزائية وتشريعات حماية المستهلك، المتعلقة بالتصرفات المادية والمحل المادى والآثار الناتجة عن هذه السلوكيات والمراكز القانونية الناشئة عنها.

١٢- ان المعلومات مال، والتصرفات المعلوماتية ذات وجود واثر، فلا يتعين عندها ان تحرم من التنظيم التشريعي لانها لدى الكثيرين افتراض ووهم. وبنفس الوقت لا يتعين ان تشقى القواعد القائمة فى لى النصوص وتطويع النظريات القائمة لتستوعب المعلومات خاصة بعد ان تحقق اثرها كعماد للاقتصاد الرقى، ويتعين ان تصاغ النظريات بمرونة تستوعب القادم الجديد فى عصر المعلومات ووسائلها فتحظى بشمولية المعالجة لتحقيق سرعة الاستجابة فى مرحلة اصعب ما فيها ادراك سرعة التغير وولادة الانماط المستجدة. ولا يتعين ان يحتج بالمتغيرات للهروب من مسئوليات التنظيم التشريعي، لان الأسس للمتغيرات امست واضحة فكثير من المستجدات لا تؤثر فى صحة القواعد القائمة وغالباً ما قد يكفى معها تطوير الاطار الاجرائى وليس الموضوعى، واذا كان ثمة حاجة لمواكبة التشريع للتغيير فلن تكون أوسع أثراً أو نطاقاً مما شهدته التشريعات التقليدية ذاتها من تغييرات بسبب اثار العصر ومستجداته.

ومتى ما تم الاستناد إلى مثل هذه الأسس العامة جرى فض حالة التشتت والتناقض فى معالجة قانون عصر المعلومات (قانون الكمبيوتر) وكان الجواب لكل اطار فرعى قد توفر ضمن القواعد الكلية، وللتأكد من صحة النتائج فاننا نتساءل: هل تكفى هذه الاسس لمواجهة جرائم الكمبيوتر المتطورة من حيث نمطها واسلوبها يوماً بعد يوم؟؟

الإجابة طبعا بالإيجاب ، لان مانع حماية المعلومات من خلال النصوص القائمة فى قوانين العقوبات هو ان النصوص تعاملت على مدى الزمن الماضى مع المال المادى والمحرر المادى والسلوك المادى وهكذا، فان قبلت المعلومات محلا صالحا للجريمة، اما بالنص الخاص أو بالنص العام الذى يساويها بالمال المادى، واعتبرت السلوكيات المعنوية فى بيئة الإنترنت والكمبيوتر سلوكيات صالحة لارتكاب هذه الجرائم والجرائم التقليدية، وإذا ما قبل الدليل الالكترونى كدليل على إثبات الجرم ، وإذا ما تحققت قواعد تفتيش وضبط تراعى الطبيعة التقنية لبيئة جرائم الكمبيوتر، كانت جرائم الكمبيوتر محل تنظيم وتكون الحماية من مخاطرها قد تحققت.

المبحث الثاني

خصائص الجريمة المعلوماتية

سبق القول ان التطور الحاصل في تكنولوجيا الاعلام والاتصال وظهور الشبكة العالمية (الإنترنت) ، بكل ما حملته من تقدم وخدمات، لم يمر على العالم بسلام، لانه بقدر ما احدث آثار إيجابية وغير نمط حياة المجتمعات وساهم في التطور والرقى، بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول باسرها، كل هذا تجلى في تطويع الإنترنت والوسائل الالكترونية، لتكون عالماً جديداً لتظهر إلى الوجود الجرائم الالكترونية أو الجرائم المعلوماتية، وهذه الجرائم لها طابعاً قانونياً خاصاً يميزها عن غيرها من الجرائم التقليدية.

ويمكن القول بأن هناك العديد من السمات التي تتميز بها الجريمة المعلوماتية اهمها:

بداية نشر إلى أن جرائم الحاسوب من الجرائم العابرة للحدود السياسية Transnational، اذ بالامكان تصور ارتكاب هذه الجريمة في دولة ما وتحقق نتائجها في دولة أخرى، فتباعد مكان موقع الجريمة عن مكان نتائجها يثير مشاكل عديدة من حيث القانون الواجب التطبيق والإجراءات الجنائية وغير ذلك من المسائل القانونية.

وتتميز هذه الجريمة أيضا بسرعة تنفيذها حيث يمكن بضغطة واحدة على لوحة المفاتيح أن تنتقل ملايين الدولارات من مكان إلى آخر، كما أنها تتميز بأنها جرائم في الخفاء يصعب إثباتها لغياب الدليل المادي، وكذلك يطلق عليها الجرائم الناعمة حيث لا تتطلب استخدام العنف، فأتلاف بيانات في الحاسوب أو نقلها من مكان إلى آخر لا يتطلب اي كسر أو حرق مثلا.

ويمكن القول أيضا أن التأثيرات الإقتصادية لهذه الجرائم خطيرة جداً حيث يلحق خسائر فادحة بالمجتمع.

ونوجز بعض الخصائص في النقاط التالية:

أولاً: مقترفي جرائم الحاسوب:

قد يكون مقترف هذه الجريمة شخصاً عادياً يعمل لحسابه أو الآخرين، وقد يهدف إلى تحقيق مصلحة خاصة من وراء الجريمة التي يرتكبها ضد أحد نظم المعالجة الآلية للبيانات والمعلومات^(٢٠).

٢٠- أنظر: د/ احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية

ثانياً: الهدف والدافع من إقتراف جرائم الحاسوب:

الهدف الغالب على هذه الجرائم هو إدخال تعديل على عناصر الذمة المالية، ويكون الطمع الذي يشبعه الاستيلاء على المال دافعها، وبريق المكسب السريع محرك لمرتكبها، وقد ترتكب أحياناً لمجرد قهر نظام الحاسب الآلي وتخطفى حواجز الحماية المقامة حوله أو بدافع الإنتقام من رب العمل أو أحد زملاء أو الأصدقاء^(٢١).

ثالثاً: موضع جرائم المعلوماتية من مراحل تشغيل نظام المعالجة الآلية للبيانات:

على الرغم من إمكانية ارتكاب جرائم المعلوماتية أثناء اية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات فى الحاسب الآلى (الإدخال- المعالجة- الإخراج) ، فإن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن لطبيعتها إرتكابها إلا فى وقت محدد يعتبر بالنسبة لمراحل التشغيل - الأمثل لذلك، ففي مرحلة الإدخال : حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة، فانه يسهل إدخال معلومات غير صحيحة وعدم إدخال وثائق أساسية، وفى هذه المرحلة يرتكب الجانب الأكبر من جرائم المعلوماتية، وفى مرحلة المعالجة الآلية للبيانات: فانه يمكن إدخال أية تعديلات تحقق الهدف الإجرامى عن طريق التلاعب فى برامج الحاسب الآلى (مثل دس تعليمات غير مصرح بها فيها، أو تشغيل برامج جديدة تلغى- جزئياً أو كلياً - عمل البرامج الأصلية) ، والجرائم المرتكبة فى هذه المرحلة تتطلب توافر معرفة فنية عميقة لدى الجانى، واكتشافها صعب، وغالبا ما تقف المصادفة وراءه، وفى هذه المرحلة الأخيرة المتعلقة بالمخرجات يقع التلاعب فى النتائج التى يخرجها الحاسب بشأن بيانات صحيحة أدخلت فيه وعالجها بطريقة صحيحة^(٢٢).

رابعاً: التعاون والتواطؤ على الاضرار:

وهو أكثر تكراراً فى جرائم المعلوماتية عنه فى الانماط الأخرى لجرائم

للحاسب الآلى) - دراسة مقارنة- دار النهضة العربية، القاهرة، ٢٠٠٠، ص ١٦٧

٢١- أنظر: د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة، أسبوط، ١٩٩٢ صفحة ٣٨.

٢٢- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٣٩ .

الخاصة أو جرائم أصحاب الياقات البيضاء، وغالبا ما يكون متضامنا فيها متخصص في الحاسبات الآلية يقوم بالجانب الفني من المشروع الإجرامي ، وشخص آخر من المحيط أو من خارج المؤسسة المجنى عليها لتغطية عملية التلاعب وتحويل المكاسب اليه، كما أن من خصائص من يمارسون التلصص على الحاسبات تبادل المعلومات بصفة منتظمة حول أنشطتهم^(٢٣).

٢٣- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٤٠.

خامساً: دور المخالطة الفارقة:

تتجلى فى الجرائم المعلوماتية أعراض المخالطة الفارقة The differential association syndrome بشكل ملحوظ، نظراً لانتشار أنواع خاصة من الممارسات والعمليات غير المشروعة فى ميادين استخدام المعالجة الآلية للبيانات والمعلومات، واعتبار بعضها من قبيل الانحراف المقبول فى هذه الميادين، مما يتيح وييسر اقدام العاملين فيها على ارتكاب أفعال غير مشروعه قد تصل إلى حد الجرائم الخطيرة، أضف إلى ذلك أن الطبيعة التنافسية لعمل المتخصصين فى مجال الحاسبات الآلية ومراكزهم المرموقة – غالباً- يمكن أن تؤدى إلى نوع من الإثارة والتزاحم بينهم فى ارتكاب جرائم المعلوماتية^(٢٤).

سادساً: أعراض النخبة:

يعتقد بعض المتخصصين فى تقنية الحاسبات والمعلوماتية أن من مزايا مراكزهم الوظيفية ومهاراتهم الفنية استخدام الحاسبات الآلية وبرامجها وتقنياتها لأغراض شخصية، أو للتبارى الفكرى فيما بينهم، أو ممارسة بعض الهوايات الدائرة فى فلك هذه التقنية، وهو ما يعبر عنه بأعراض النخبة syndrome elitiste، وقد يدفع ذلك بعضهم إلى التمدادى فى استخدام نظم الحاسب الآلى بطريقة غير مشروعة قد تصل إلى حد ارتكاب الجرائم الخطرة^(٢٥).

سابعاً : اضرار جرائم المعلوماتية:

تقع جرائم المعلوماتية وترتكب فى اطار تقنية وتكنولوجيا متقدمة يتزايد استخدامها يوماً بعد يوم فى إدارة مختلف المعاملات الإقتصادية والمالية والخدمية – الوطنية والدولية على حد سواء – ويعتمد عليها فى تسيير معظم شئون الحياة اليومية للأفراد والشئون العامة لاكثر الحكومات بما فى ذلك الأمن والدفاع، ومن شأن ذلك أن يضىف أبعادا خطيرة غير مسبوقه على حجم الأضرار والخسائر التى تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات، ولا أدل على ذلك من أن حجم الخسائر المادية الناجمة عن هذه الجرائم قد بلغ وفقاً لتقديرات المركز الوطنى لجرائم الحاسب فى الولايات المتحدة الأمريكية

٢٤- أنظر: د/ هشام محمد فريد، المرجع السابق، ص ٤٠.

٢٥- أنظر: د/ هشام محمد فريد، المرجع السابق، ص ٤٠.

(NCCCD) حوالي ٥٠٠ مليون دولار امريكي سنويا، بينما قدرتها مصادر أخرى بما يتراوح بين ٣ و ٥ بليون دولار في السنة^(٢٦)، ولا شك أن هذه الخسائر قد فاقت بكثير تلك الأرقام في عرصنا الحالي.

^{٢٦}- أنظر: د/ هشام محمد فريد، المرجع السابق، ص ٤٠، ٤١ .

ثامناً: صعوبة اكتشاف جرائم المعلوماتية وإثباتها:

لا تحتاج جرائم المعلوماتية إلى أي عنف، أو سفك للدماء أو آثار اقتحام لسرقة الاموال، وإنما هي أرقام وبيانات تتغير أو تمحى تماماً من السجلات المخزونة في ذاكرة الحاسبات الآلية، ولأن هذه الجرائم في أغلب الأحيان لا تترك أي اثر خارجي مرئي لها، فإنها تكون صعبة في الإثبات. ومما يزيد من صعوبة إثبات هذه الجرائم أيضاً، ارتكابها عادة في الخفاء، وعدم وجود أي أثر كتابي لما يجرى خلال تنفيذها من عمليات أو أفعال إجرامية، حيث يتم بالنبضات الالكترونية نقل المعلومات، كما أن هذه الجرائم ترتكب غالباً وبصورة منظمة على صعيد أكثر من دولة باستخدام شبكات الإتصالات والمعلومات (الإنترنت)، ودون تحمل عناء الانتقال، اضافة إلى ذلك إجماع مجتمع الاعمال عن الإبلاغ عنها تجنباً للاساءة إلى السمعة وهز الثقة في كفاءة المنظمات والمؤسسات المجنى عليها، فضلاً عن امكانية تدمير المعلومات التي يمكن ان تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الزمنية^(٢٧).

وهناك صعوبات أخرى أيضاً في إثبات هذه الجرائم تكمن - كما سبق ان بينا- في الجناه مرتكبي تلك الجرائم الذين يتسمون بالذكاء والدهاء والخبرة التقنية أثناء ارتكابها، إضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي في إثباتها، ومن ثم يلزم البحث عن ادلة جديدة حديثة ناتجة من ذات الحاسب، ومن هنا تبدأ صعوبة البحث عن الدليل، وجمع هذا الدليل وتبدا مشكلات قبوله أن وجد، ومدى موثوقيته أو مصداقيته على إثبات وقائع الجريمة^(٢٨).

تاسعاً: السمات العامة للمتورطين في الانحراف المعلوماتي:

" تتوافر لدى الجناة مرتكبي جرائم المعلوماتية أو معظمهم مجموعة من السمات أو الخصائص التي تميزهم عن غيرهم من الجناة أو المتورطين في أشكال الانحراف والإجرام الأخرى، ولعل من أبرز هذه السمات ما يلي:"

أ- السن: تتراوح أعمار مقترفي جرائم المعلوماتية عادة بين ١٨ و ٤٦ سنة، والمتوسط العمري لهم ٢٥ سنة.

ب- التكوين والمعارف والعمل: ينتمي مرتكبو هذه الجرائم عادة إلى الطبقة المتعلمة، ومعظم يكونون من العاملين بنفس الجهة أو المؤسسة المجنى

٢٧- أنظر: د/ هشام محمد فريد، المرجع السابق، ص ٤١، ٤٢.

٢٨- أنظر: د/ هشام محمد فريد، المرجع السابق، ص ١١، ١٢.

عليها، وهم أشخاص محل ثقة، ولا تشوب سمعتهم أو نزاهتهم شائبة، والذي يغريهم على ارتكاب جرائمهم شعورهم بالأمن نتيجة جهل تلك الجهة أو المؤسسة وكبار مديريها بعلم وتكنولوجيا وتقنيات الحاسبات الآلية وعلوم وفنون البرمجة، فيتملكهم الشعور بإمكانية ارتكاب الجريمة دون أن يتم اكتشافها.

ج- تمثلهم صورة وخصائص روبن هود (أعراض روبن هود Robin Hood syndrome) : حيث يفرق معظم مرتبكي جرائم المعلوماتية – لا سيما الهواة منهم – تفرقة واضحة بين الأضرار بالأشخاص العاديين – الذي يعتبرونه غاية في اللا أخلاقية- والإضرار بمؤسسة أو جهة في استطاعتها اقتصادياً تحمل نتائج تلاعبهم ، وهو ما لا يجدون غضاضة في تقبله.

د- خشية الضبط وإفتضاح الأمر: لما يترتب على ذلك من ارتباك مالى وفقد للمركز والمكانة.

هـ - ارتفاع مستوى الذكاء^(٢٩) .

السمات المميزة لجرائم الكمبيوتر والإنترنت عن غيرها من الجرائم

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

* كما أنها تتسم بالخطورة البالغة نظرا لأغراضها المتعددة. ونظرا لحجم الخسائر الناجم عنها قياسا بالجرائم التقليدية. ونظرا لارتكابها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم امرا صعبا. ونظرا لانها بذاتها تنطوي على سلوكيات غير مألوفة، وبما اتاحته من تسهيل ارتكاب الجرائم الأخرى تمثل ايجاد وسائل تجعل ملاحقة الجرائم التقليدية امرا صعبا متى ما ارتكبت باستخدام الكمبيوتر .

* وتحقيق وتحري جرائم الكمبيوتر والإنترنت والمقاضاة في نطاقها تنطوي على

^{٢٩}- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٤٢، ٤٣.

مشكلات وتحديات ادارية وقانونية تتصل ابتداء بمعيقات ومتطلبات عمليات ملاحقة الجناة، فان تحققت مكنة الملاحقة اصبحت الإدانة صعبة لسهولة اتلاف الادلة من قبل الجناة أو لصعوبة الوصول إلى الادلة أو لغياب الاعتراف القانوني بطبيعة الادلة المتعلقة بهذه الجرائم. ونظرا لانها جرائم لا تحدها حدود وتعد من الجرائم العابرة للحدود. فتثير لذلك تحديات ومعيقات فى حقل الاختصاص القضائى والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

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

والحقيقة ان مسالة التباعد الجغرافى بين الفعل وتحقق النتيجة من أكثر المسائل التى تثير اشكالات فى مجال جرائم الحاسوب وبشكل خاص الاجراءات الجنائية والاختصاص والقانون الواجب التطبيق. وهذا بدوره عامل رئيسى فى نماء دعوات تظافر الجهود الدولية لمكافحة هذه الجرائم، ولعل هذه السمة تذكرنا بارهاصات جرائم المخدرات والاتجار بالرقيق وغيرها من الجرائم التى وقف تباين الدول واختلاف مستويات الحماية الجنائية فيها حائلا دون نجاح أساليب مكافحتها، فلم يكن من بد غير الدخول فى سلسلة اتفاقيات ومعاهدات دولية لمكافحة هذه الجرائم، وذات الامر يقال الان بشأن أنشطة غسل الأموال ، وهى فى ذات الوقت الاسباب ذاتها التى تجعل موضوع جرائم الارهاب والجرائم المنظمة والجرائم الاقتصادية المواضيع الرئيسية على أجندة اهتمام المجتمع الدولى.

ولمواجهة مثل هذه الجريمة (جريمة الحاسوب) العابرة للحدود مواجهة فعالة، يجب تجريم صورها في القانون الوطني للمعاقبة عليها، وان يكون هناك تعاون وتضامن دولي لمواجهة مشاكلها، من حيث مكان وقوعها واختصاص المحاكم بها وجمع المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد صورها وقواعد التسليم فيها وايجاد الحلول لمشكلاتها الأساسية وأبرزها:

١- غياب مفهوم عام متفق عليه بين الدول - حتى الآن- حول نماذج النشاط المكون للجريمة المتعلقة بالكمبيوتر والإنترنت.

٢- غياب الاتفاق حول التعريف القانوني للنشاط الاجرامى المتعلق بهذا النوع من الإجرام.

٣- نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء فى هذا المجال لتمحيص عناصر الجريمة أن وجدت وجمع المعلومات والأدلة عنها للدانة فيها.

٤- عدم كفاءة وملاءمة السلطات التى ينص عليها القانون بالنسبة للتحرى واختراق نظم الكمبيوتر، لأنها عادة متعلقة بالضبط والتحرى بالنسبة لوقائع مادية هى الجرائم التقليدية وغير متوائمة مع غير (الماديات) كاختراق المعلومات المبرمجة وتغييرها فى الكمبيوتر.

٥- عدم التناسب بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحرى فى الجرائم المتعلقة بالحاسوب.

٦- السمة الغالبة للكثير من جرائم الكمبيوتر هى أنها- كما أوضحنا اعلاه - من النوع العابر للحدود Transnational وبالتالي تثير من المشاكل ما تثيره امثال تلك الجرائم كجرائم الاتجار بالمخدرات والاتجار غير المشروع فى الاسلحة والإتجار فى الرقيق الأبيض والجرائم الإقتصادية والمالية وجرائم التلوث البيئى.

٧- عدم وجود معاهدات للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولى أو عدم كفايتها أن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر ودينامية التحريات فيها وكفالة السرعة بها". ويمثل مشروع الاتفاقيات الأوروبية لجرائم الكمبيوتر فى الوقت الحاضر المشروع الأكثر نضجا لمواجهة جرائم الكمبيوتر بل وواحدا من اهم ادوات التعاون الدولى فى هذا المجال.

الفصل الثالث

تقسيم جرائم المعلوماتية

نتناول هذا الفصل على مبحثين على النحو التالي:

- المبحث الأول : الجرائم التي تقع على الحاسب الآلي ومكوناته.
المبحث الثاني : الجرائم التي ترتكب بواسطة الحاسب الآلي ومكوناته.

المبحث الأول

الجرائم التي تقع على الحاسب الآلي ومكوناته

نتناول هذا المبحث من خلال ست مطالب على النحو التالي:

- المطلب الأول : سرقة البرامج والمعلومات المخزنة آلياً.
المطلب الثاني : سرقة منفعة الحاسب الآلي أو الاستعمال غير المصرح به لنظام الحاسب الآلي.
المطلب الثالث : بعض أفعال تزوير المعلومات والبيانات والبرامج المخزنة آلياً والتلاعب بها.
المطلب الرابع : إختراق الحاسب الآلي وإنتحال هوية المستخدم.
المطلب الخامس : التجسس المعلوماتي
المطلب السادس : الإتلاف المعلوماتي

المطلب الأول

سرقة البرامج والمعلومات المخزنة آلياً.

المقصود بسرقة البرامج والمعلومات المخزنة آلياً:

تعرف السرقة في مفهومها العام أو الواسع بانها: " الحصول على شئ من طرف آخر بدون علم منه، وفي الغالب فإنه سيترتب عليه اضرار بهذا الطرف الآخر، سواء كان هذا الضرر مادياً أو معنوياً أو أدبياً" ، ويمكن أن يشتق من هذا التعريف الموسع لمفهوم السرقة نوعان آخران من الأفعال غير المشروعة، وهما:

- أ- التجسس: وهو الحصول على معلومات بدون علم صاحب الشأن وذلك للاستفادة من هذه المعلومات بطريقة ما، أو لإلحاق ضرر بصاحب الشأن.
- ب- الاحتيال: وهو إعطاء الغير معلومات غير صحيحة بهدف التضلل، أو الحصول على معلومات أو أقوال بالادعاء بما هو غير صحيح^(٣٠).
- أما بالنسبة لتزيف الفقة للسرقة، فقد جرى تعريفها على انه: " اختلاس مال منقول مملوك للغير بغير تملكه"، كما يعرف السارق- حسب التعريف المقنن له - بأنه: " كل من اختلس منقولا مملوكا لغيره" (المادة ٣١١ من قانون العقوبات المصري)^(٣١).

والجدير بالذكر ، فإنه في فترة الخمسينات من القرن الماضي وحتى بداية الستينات، بدأ استخدام أجهزة الحاسب الآلي في الانتشار على المستوى الصناعي والتجاري في تطبيقات محدودة، وكان الهدف الاساسي من استخدامها هو إجراء العمليات الحسابية المعقدة، أو التي تتناول كما هائلاً من البيانات بسرعة وكفاءة عالية، ثم ما لبث أن صاحب هذه التكنولوجيا الحديثة اختلف في طريقة إجراء العمليات الحسابية وطرق تخزينها، وكذلك تقبل نوع وطبيعة الرقابة المطبقة، ومن خلال هذا الاختلاف ظهر نوع جديد من اللصوص اعتمد على تلك التكنولوجيا لتحقيق مكاسب مادية فائقة الربح، كما واكب انتشار استخدام الحاسبات الآلية على كافة المستويات وتنوع أنشطته تغيير في النمط العام

٣٠- أنظر: د/ عثمان حجازي - السرقات والكمبيوتر- ندوة الجرائم الاقتصادية المتسحدثة - من ٢٠ إلى ٢١ أبريل ١٩٩٣ - الجزء الأول - المركز القومي للبحوث الجنائية والاجتماعية - قسم بحوث الجريمة- القاهرة ١٩٩٤- ص ٣٦٤.

٣١- أنظر د/ هشام محمد فريد رستم- ندوة الجرائم الاقتصادية، صفحة ٤٣٦، ٤٣٧.

للتعامل واختلاف في طريقة تناول المعلومات، ومن ذلك أخذت المعلومات في حد ذاتها أهمية غير مسبوقة، وأصبحت المعلومة مستهدفة، وأصبح أيضا لها سوقها الخاص بها وثنمها المرتفع جدا، وترتب على ذلك في النهاية أن أصبحت تلك المعلومات هدفاً مشتركاً للسرقة في ابسط الحالات أو للتدمير أو التجسس في حالات اخرى، اصف إلى ذلك أن كمية الاموال المستثمرة في تطوير برامج ونظم الحاسبات الآلية قد تعدت مئات البلايين من الدولارات، ولنا أن نتصور مدى الجاذبية لمن تسول له نفسه سرقة هذه البرامج والنظم، والخطير في هذا الموضوع أن السرقة لم تقف عند حد الأشخاص، بل انضمت اليهم في ذلك مجموعة من الشركات المنظمة المنافسة، وحتى الحكومات، وذلك لسرقة المعلومات والبرامج، وترتب على ذلك كله تطور في اتجاه استحداث طرق جديد لحماية هذه البرامج والمعلومات^(٣٢)، كما أدى هذا التطور الهائل أيضا في تكنولوجيا صناعة برامج ونظم الحاسبات الآلية إلى تعرضها للعديد من أفعال التعدي الاخرى عليها - إلى جانب السرقة- كتقليدها وإفشاء سر صنعتها، وهي تمثل ظاهرة، وان كان لا يعرف بعد حجمه الحقيقي، إلا أنها ذات مجال واسع، ولاشك أنها تهدد - وعلى نحو مؤكد- العائد الاستثماري لمنتجى هذه البرامج^(٣٣).

وترجع البدايات الاولى لظاهرة سرقة المعلومات إلى فترة الستينات من القرن الماضي ايضا، عندما طرحت وسائل الاعلام على بساط البحث المعلومات الاولى التي تتناول ما يطلق عليه بصفة عامة " جريمة نظم المعلومات" حيث تعالج هذه المعلومات في غالبيتها التلاعب بالحاسب الآلي وتعطيلة وسرقة المعلومات المختزنة فيه، علاوة على التجسس عليه واستخدامه على النحو غير المشروع، ونظرا لأن هذه البيانات والمعلومات قد شيدت على تقارير الصحف، فكان من الصعب جدا معرفة ما إذا كانت هذه الظواهر من وحي الخيال أم هي من قبيل الحقيقة^(٣٤).

وهناك نماذج عديدة من الجرائم التي تقع على المعطيات المخزونة بالنظر إلى المصلحة المحمية قانونا، ومن تلك الجرائم ما يعد اعتداء على حقوق الملكية الفكرية عن طريق نسخ البرامج الاصلية وتسويقها أو استخدامها أو

٣٢- أنظر: د/ عثمان حجازي - المرجع السابق - صفحة ٣٦٥-٣٦٧.

٣٣- أنظر: د/ عبد الله حسين على محمود - سرقة المعلومات المخزنة في الحاسب الآلي - ط٢ - دار النهضة العربية - القاهرة - ٢٠٠٢ - صفحة ٢١٠.

٣٤- أنظر: المرجع السابق - صفحة ٤١، ٤٢.

اعادة نشر المعلومات المسجلة دون إذن مسبق، مما يعرض الشركات المنتجة لهذه البرامج للكثير من الخسائر المادية الفادحة، وقد كشف تقرير شامل حول قرصنة برامج الكمبيوتر عن تقدير الخسائر في هذا المجال والتي بلغت ١١.٢ مليار دولار امريكي في عام ١٩٩٦، وهي ثانياً دراسة مستقلة يتم نشرها من قبل اتحاد منتجي برامج الكمبيوتر التجارية وجمعية ناشري برامج الكمبيوتر، وهما الجمعيتان التجاريتان الرائدتان في مجال صناعة برامج الكمبيوتر، وقد اشارت أيضاً تلك الدراسة إلى أن من اصل ٥٢٣ مليون برنامج تطبيقي عملي جديد مستعمل عالمياً في عام ١٩٩٦ يوجد ٢٢٥ مليون برنامج غير شرعي، أي ما يوازي برنامجاً من اصل اثنين هو غير شرعي، مما يشكل زيادة نسبتها ٢٠% في عدد البرامج المقرصنة بالمقارنة مع تقديرات عام ١٩٩٥ والتي أفادت بوجود ١٨٧ مليون برنامج غير شرعي^(٣٥).

وهناك العديد من صور السرقات والانتهاكات التي تقع على البرامج والمعلومات المخزنة آلياً في الحاسب الآلي، ولعل من أهم تلك الاعتداءات غير المشروعة ما يلي:

أولاً: النسخ غير المشروع للبرامج والملفات (قرصنة البرامج Software piracy)^(٣٦)

^{٣٥}- أنظر : المرجع السابق - صفحة ٢١٠.

^{٣٦}- تعنى القرصنة Piracy في مفهومها العام" كل عمل عنف غير مرخص به يرتكب بقصد النهب من قبل سفينة خاصة ضد سفينة اخرى في أعالي البحار" وفي اللغة تطلق كلمة قرصنة على " السطو على سفن البحار" ومنذ اوائل القرن الثامن عشر صار هذا المصطلح يطلق وصفاً - من باب القياس والاستهجان - على نهب المصنفات المنشورة للغير بنسخها دون ترخيص لاغراض تجارية، وطبقاً لهذا المدلول شاع استخدام تعبير " قرصنة البرامج "Software piracy" وصف عملية النسخ غير المشروع لبرامج الغير، وان كان البعض يستخدم التعبير بمعنى واسع يشمل النسخ أو الاستخدام غير المرخص به للبرامج، فان آخرين يستخدمونه بمعنى نسخ البرامج المعلوماتية وتسويقها بصورة غير مشروعة، ويوسع فريق آخر من دلالة هذا التعبير بتبنيه تعريفاً لقرصنة البرامج مؤداه انصرافها إلى : كل أخذ غير مصرح به أو استيلاء أو اعادة انتاج أو استخدام لبرنامج معلوماتي في الوظيفة المعد لادائها طالما كان هذا البرنامج مقرا به، كمادة ذات قيمة، والقرصنة اذا وردت منعونة" بالمعلوماتية" كان مراداً بها نسخ البرامج بصورة غير شرعية أو الحصول على معلومات مخزنة في ذاكرة الحاسب الآلي دون وجه حق، وتتم هذه العملية الاخيرة اما بصورة مباشرة

هيأت حرية نسخ البرامج وتداولها بعيدا عن مصدرها الأصلي بيئة صالحة لدس البرامج الطفيلية بأشكالها المختلفة من قبل المتخصصين فى هذا المجال، كذلك فقد أدت هذه الممارسات إلى حرمان العديد من الشركات المنشأة للبرامج أو الملفات- وهى صاحبة الحق فى بيع تلك البرامج - من جنى أرباح عملها^(٣٧).

" ولأعمال القرصنة فى ميدان البرامج صور عديدة ومتنوعة، لعل أبرزها وأخطرها على صناعة البرامج المعلوماتية الصور الأربعة التالية:

١- تقليد البرامج Software contefeiting: ويقصد به محاكاة برنامج معين عن طريق صنع العديد من النسخ المماثلة له أو إنتاجها بحيث تبدو عند تسويقها كما لو كانت هى الأصل، والنسخ الجزئى للبرنامج كاف للقول بتقليده ما دامت المحاكاة تتعلق باجزائه الرئيسية، والتقليد- كصورة من صور القرصنة- يهدد برامج الألعاب الإلكترونية بصفة خاصة، فضلا عن كونه احد ابرز المشكلات التى تواجه منتجى البرامج العامة ، ونظرا لضخامة الأرباح التى تجنى من وراء هذا التقليد، وتدنى مخاطرة المحتملة، وصعوبة اثباته على الواقع العملى الملموس، فقد ادى ذلك إلى اعتباره- وبحق - من أبرز مجالات الانشطة غير المشروعة التى تجذب المتورطين فى الجريمة المنظمة.

٢- سرقة البرنامج المصدر Source program:، وازالة ما يميز هويته بادخال تغييرات على شكله وهيئته ، واعادة تجهيزه ليبدو كما لو كان منتجا جديداً لصانع آخر، واكثر المهددين بخطر هذا النمط من القرصنة هم منتجى حزم البرامج الجاهزة التى جرى تسويقها على نطاق واسع، ومن المتوقع

عن طريق الحصول على كلمة السر سواء بالحيلة أو باجراء تجارب مع الكلمات التى تستعمل لهذا الغرض عادة، واما بصورة غير مباشرة عن طريق النقاط الموجات الكهرومغناطيسية المنبعثة من الحاسب اثناء تشغيله وترجمتها ، ولا تختلط القرصنة وفقا لذلك بما يسمى " فيروس الحاسب " وان كان ممكنا الجمع بين الافتين، " كما لو عد قرصان الحاسب إلى زرع فيروس عندما يشعر انه على وشك ان يكشف امره).

د/ هشام محمد فريد رستم- قانون العقوبات ومخاطر تقنية المعلومات ، المرجع السابق، ص ١٠٤-١٠٧.

٣٧- أنظر: د/ هدى صلاح - الجريمة فى مجال نظم المعلومات - ندوة الجرائم الاقتصادية المستحدثة- المركز القومى للبحوث الجنائية والاجتماعية - القاهرة - ١٩٩٤، صفحة ٣٥٨.

تفاهم حدة هذا الخطر كلما تزايدت بين هؤلاء المنتجين حدة المنافسة.

٣- النسخ المباشر Straight forward copying للبرامج وبيعها دون دفع مقابل مالى للحصول على ترخيص بذلك من منتجها أو سداد انصبة فى العائدات الناتجة عن بيعها، وتعد أنظمة التشغيل المعقدة أو المتقدمة sophisticated operating systems للحسابات المتوسطة Mini computer اضافة إلى برامج الخدمات " المساعدة" وبرامج الترجمة Utility and Compilers programs، من أكثر المجالات التى يمارس فيها هذا النمط من القرصنة .

٤- النسخ غير المشروع للبرامج دخل المنظمات والشركات الكبيرة عند الحصول على منتجها على ترخيص نسخها مرة واحدة، فيتم نسخها بصورة غير قانونية مرات متتالية، وتشجيع ممارسة هذا النمط من القرصنة فى معظم الشركات والمؤسسات، وتزداد حدته بشكل خاص فى قطاع تسويق برامج الحاسب الشخصى Personnel computer^(٣٨).

أساليب ارتكاب افعال قرصنة البرامج والملفات:

تتنوع أيضا أساليب ارتكاب عمليات القرصنة التى يكون محلها برمجيات ونظم الحاسبات الالية، وتنقسم تلك الأساليب إلى أساليب تقليدية واخرى فنية:

١- الأساليب التقليدية:

ومن صور تلك الأساليب رشوة أو ابتزاز الموظفين العاملين فى شركات إنتاج برمجيات الحاسبات الالية، وتسلب الموظفين إلى الشركات المراد التجسس على برامجهم للعمل فيها فترة وجيزة تسمح لهم بالاطلاع على أسرار ودقائق برامجها، أو الإعلام عن وظائف وإجراء مقابلات مع المتقدمين لشغلها للحصول منهم على وصف لأعمالهم او عمليات الشركات التى ينتمون إليها، ويقدر البعض أن ٦٣% من عمليات سرقة البرامج ترتكب عن طريق الموظفين العاملين فى شركات انتاج البرامج الذين ينقلون البرامج الجديدة فى حقائب اوراقهم ويغادرون مكاتبهم رأسا إلى القراصنة^(٣٩).

٢- الأساليب الفنية:

" تفيد الخبرات المستمدة من بعض عمليات قرصنة برامج الحاسب

٣٨- أنظر : د/ هشام محمد فريد رستم، المرجع السابق ص ١١١، ١١٦.

٣٩- أنظر : د/ هشام محمد فريد رستم ، ص ١٢٦.

الآلى التى تم اكتشافها انه عندما تتوافر لدى أى شخص امكانية الإتصال المنطقى بالحاسب Logical access فان خطر الوصول إلى برامجه والحصول على نسخ منها يصبح قائما، ومن الحالات التى تشهد بتحقق هذا الخطر فعليا حالة لشاب يبلغ من العمر أربعة وعشرين عاما تمكن - باستخدام احدى خطوط الإتصال الهاتفى- من الدخول عن بعد إلى انظمة احدى مراكز الحاسبات وسرقة " نسخ " برنامج يخصه قيمته مليون دولار، وفى حالة اخرى تمكن مبرمج باحدى الشركات بمدينة بالو آلتو Palo Alto ، بولاية كاليفورنيا الأمريكية من الوصول عن بعد إلى ذاكرة الحاسب الالكترونى لشركة منافسة وطبع برامج معلوماتى معين يخص الشركة الاخيرة تبلغ قيمته ٣٠٠ الف دولار، وكانت مؤسسته قد لاحظت أن عدم استخدامه فى اعمالها الهندسية قد سبب انخفاضا فى مبيعاتها.

ويشير البعض إلى امكانية الحصول على نسخ من البرامج باستخدام شاشات التسجيل عن بعد وادوات المراقبة السمعية، ففى احدى حالات القرصنة كانت الوسيلة المستخدمة هى التقاط وتسجيل موجات البرامج المعلوماتية التى يجرى بثها عبر الأثير^(٤٠).

ومع أن منتجى البرامج يبذلون قصارى جهدهم لتزويدها بوسائل فنية تحميها من خطر النسخ غير المرخص به، الا أن جهدا مضادا لا يكف القرصنة

^{٤٠}- فى تلك الحالة تلقت شركة A & F لانتاج وبث البرامج المعلوماتية بانجلترا بلاغا من مجهول يفيد أن بعض مشغلى اجهزة الاستقبال والارسال اللاسلكية يتبادلون فيما بينهم بث برامج الشركة لتسجيلها دون دفع الرسوم المقررة للحصول من الشركة على ترخيص بذلك، وللتحقق من صحة تلك الواقعة، قامت الشركة المذكورة بشراء جهاز استقبال للموجات اللاسلكية واستخدامه فى مراقبة الموجات الحاملة للبرامج عبر الاثير، وسرعان ما اكتشفت أن ثلاثة من برامجها يجرى بثها بانتظام كى تسجل مجانا من قبل اخرين، وان واحدا ممن يقومون بذلك يبث بانتظام قائمة تحتوى على اكثر من ٤٠٠ برنامج، وكشفت اجهزة الرصد والمتابعة أن عمليات بث البرامج تغطى مساحات شاسعة من الولايات المتحدة، وقد قدرت الشركة حجم الخسائر الناجمة عن نقص مبيعات برامجها بسبب هذه القرصنة بمبلغ ٧٥ الف جنيه استرليني فى السنة، ومع ذلك فان تلك الشركة لم تتخذ اية اجراءات فعالة لملاحقة هؤلاء القرصنة قضانيا، واكتفت بالحصول من بعضهم - بعد التوصل اليهم - على تعهد بعدم تكرار ذلك مستقبلا تقديرا منها لعدم علمهم باحكام القانون التى تحظر هذا البث والتسجيل، واخذا فى الاعتبار أن ما قاموا به لم يتعد مجرد تبادل البرامج بين الاصدقاء.

د/ هشام محمد فريد رستم ، هامش (٣) ، ص ١٢٨ - ١٢٩

عن بذلة لفك رموز البرامج المسروقة، وزيادة قدرات برامج النسخ للتغلب على وسائل الحماية الفنية التي تزود بها البرامج المستنسخة ، ولا ادل على هذا الجهد من أن أي صبي صغير متمرس بالحاسب- كما يقول Michael Crichton- سيجيب إذا ما سئل عما إذا كان نسخ البرامج ممكنا، بان كل شئ يمكن نسخه ، والمعنى ذاته يؤكدده البعض بقوله أن الطرق الفنية لجعل نسخ البرامج مستعصيا هي الاسهل في الاستخدام لحمايتها من خطر القرصنة، والاسهل في ذات الوقت أيضا في امكانية تخطيها والتغلب عليها، ومن ثم نسخ وسرقة تلك البرامج ، ايه ذلك أن البرامج المخصصة لنسخ البرامج المحمية فنيا ضد خطر النسخ تنسخ هي الاخرى بدوها^(٤١)،^(٤٢).

ثانيا: النسخ غير المشروع البيانات المخزنة الكترونيا

وتعتبر هذه الصورة أيضا نوعا من انواع القرصنة المعلوماتية، حيث تخزن البيانات والمعلومات المعالجة الكترونيا على هيئة نبضات كهربائية في دوائر مجمعة أو على اشربة واسطوانات ممغنطة، وفي الحالتين يمكن نسخها على دعائم اخرى معينة^(٤٣)، ومن اشهر الامثلة على ذلك ما حدث لأكبر شركة امريكية متخصصة في توفير خدمات الانترنت في عام ٢٠٠١ - والتي تخدم أكثر من ٢٣ مليون مستخدم للإنترنت - عندما قام شاب يبلغ من العمر تسعة عشر عاما يدعى " جاى ساتيرو" باقناع مسنوليها بانه مفيد للشركة، فقاموا بتعيينه على الفور، وعنما اظهر مهارة في العمل، طوال سنتين متواصلتين يجمع معلومات سرية مهمة عن الشركة ، وفجأة قرر الاستقالة بحجة الحصول على وظيفة اخرى، لكنه في الحقيقة كان يجهز لاستخدام ما جمعه من بيانات في شن

^{٤١} - وتاكيدا لسهولة نسخ البرامج يقرر الدوريسيت - احد القراصنة في مجال سرقة البرمجيات الفرنسيين المهرة- ان اكثر من ٩٠% من البرامج لا تحتاج لاكثر من خمس دقائق لنسخها، وان كان بعض المعقد من تلك البرامج قد يتطلب عمل اسبوعين متواصلين لنسخة، والواقع ان الوسائل الفنية التي تزود بها البرامج لحمايتها من خطر النسخ غير المرخص، به ستعوق فحسب - كما قيل - المستخدمين الشرعيين الذين هم في حاجة لعمل نسخ احتياطية، اما القراصنة فسيمكنهم الاستمرار في نسخ البرامج نظرا لما يتمتعون به من مهارات تقنية تتيح لهم التغلب على ما تزود به البرامج من وسائل فنية.

د/ هشام محمد فريد رستم ، هامش (١) ، ص ١٢٩

^{٤٢} - د/ هشام محمد فريد رستم ، ص ١٢٧- ١٢٩

^{٤٣} - د/ هشام محمد فريد رستم ، ص ٢٣٥

هجمات شديدة القسوة على موقع الشركة ، وبعد فترة من استقالته لاحظ المسؤولين عن تامين موقع الشركة ان هناك شخصا يهاجم الموقع بإحتراف شديد، تنهار امامه جميع اجراءات التامين ويخترقها بسرعة، ثم يقوم باستبدال البرامج الخاصة بالموقع ببرامج اخرى من عنده تعطل العمل وتسبب مضايقات عديدة للعاملين فى الشركة، وبعد فترة طور هذا القرصان من عملياته وبدا يسرق الارصدة المدفوعة من اشتراكات الخدمات ، وقد كلفت هذه العمليات غير المشروعة الشركة ٥٠ ألف دولار خلال وقت قصير جدا^(٤٤).

ثالثا: الجرائم الالكترونية:

ذكرنا ان الجرائم الالكترونية هى نوع من انواع جرائم المعلوماتية، تتمثل فى استخدام برامج الحاسب الآلى ونظمه لالتقاط بيانات ومعلومات معالجة الكترونيا والتلاعب بانظمة الحاسبات التى تحتوى عليها، وذلك لاغراض غير مشروعة- تتمثل غالبا فى السرقة والاحتيال- وباستخدام هذه البرامج والتعرف على نقاط الضعف فى نظام الحاسب الآلى الخاص بالمجنى عليه، فان الجانى يستطيع أن يسيطر على نظام هذا الحاسب باكملة، ثم يقوم بنشاطه غير المشروع ، ويحول هذا النشاط فى النهاية إلى مكاسب غير مشروعه، وينتهى بمحو كل اثر يمكن أن يكشف عن افعاله الإجرامية.

ولعل خير مثال يمكن أن يوضح ميكانيزم الجريمة الالكترونية، ما قام به احد الجناة الالكترونيين فى الولايات المتحدة الأمريكية ويدعى " آلان كيدمان " فعلى الرغم من صغر سنة- الذى لم يتجاوز العشرين عاما- فانه قام بارتكاب العديد من الجرائم الالكترونية المحنكة فى الفترة من سنة ١٩٩٨ وحتى عام ٢٠٠٢، حيث تم التاكد من تورطه فى مجموعة هجمات الكترونية شنها على أجهزة كمبيوتر حساسة خاصة بوكالة الفضاء الأمريكية "ناسا" نتج عنها بعض الخلل فى أنشطة تلك الوكالة، وكان هذا الجانى يركز على الأجهزة المحملة ببرامج علمية مسنولة عن تطوير نظم اطلاق الاقمار الصناعية، وبالتالي اصبح بإمكانية تدمير البيانات المسجلة على قواعد أو تغييرها ببيانات اخرى تؤثر على دقة وسلامة انطلاق الاقمار الصناعية، مما كان سيؤدى إلى حدوث العديد من الكوارث الدولية، كما كان يقوم بكسر كلمات السر وحوجز المرور ودس العديد

^{٤٤} - مجلة الأهرام للكمبيوتر والإنترنت والاتصالات " لغة العصر " ، العدد التاسع عشر، يوليو

من البرامج غير الشرعية التي تستطيع اجبار أجهزة الكمبيوتر على تنفيذ الاوامر دون تمريرها على الانظمة الامنية الالكترونية، ولم يكتف هذا القرصان بجرائم الاختراق الالكتروني ومهاجمة أجهزة الكمبيوتر وقواعد البيانات الخاصة بالجامعات ووكالة الفضاء الأمريكية "ناسا" بل حاول توسيع نشاطه بعد أن اكتشف انه يمتلك موهبة إجرامية تمكنه من بدء رحلة المليون بسهولة وفي زمن قياسي بدلا من الاكتفاء بتدمير الأجهزة دون سبب واضح ودون مكاسب مالية، فبدأ في استخدام البرنامج الخاص بالتجسس على المواقع التجارية على الانترنت لتسجيل كلمات المرور واسماء المستخدمين الخاصة بكروت الائتمان التي يتم التعامل بها مع المواقع التجارية، وعن طريق استخدام كلمة المرور قام "كيدمان" بثلاث محاولات لتحويل الاموال الخاصة باصحاب كروت الائتمان لحسابه الخاص في البنك، وبعد محاولتين منهما فاشلتين نجح في الثالثة في سحب مبلغ كبير من المال عن طريق ارقام مسروقة لكارت ائتمان، لكنه لم يتمكن من تحويلها لحسابه الخاص نظرا لاكتشاف خطأ رقمي ارتكبه هذا القرصان لحدائته في هذا المجال، وهكذا تم ابلاغ الجهات الامنية في الولايات المتحدة الأمريكية لمراقبته وتعقبه واثبات العديد من الأفعال الجنائية التي قام بارتكابها^(٤٥).

رابعاً: السطو المسلح الالكتروني:

ادى التطور المستمر لاستخدام المعلوماتية إلى التزايد الحتمي للمعالجات والتخزينات ، ومن ثم زيادة تدفق المعلومات في شكل ممغنط أو الكتروني بدلا من الشكل الكتابي، كما ترتب على ظهور التقنيات المستحدثة – اي تقنيات بث المعلومات على شبكة اتصالات بعيدة Télématique والمعالجة عن بعد Télétraitement – نشوء مخاطر جديدة نتيجة للامكانيات المستحدثة للولوج والاستفسار عن بعد من المراكز المعلوماتية، وتشكل عمليات البث Transmission أيضا نقطة ضعف هامة في النظام المعلوماتي.

ويمكن أن نصادف المشاكل المرتبطة باستخدام انظمة المعالجات عن بعد وشبكات البث في مراحل عديدة ومختلفة لاستعمال الاساليب الالكترونية، وفي الواقع، فان المعلومات اثناء حركتها وبثها، تكون مهددة في كل لحظة بالانتقاط

^{٤٥} - مجلة الأهرام للكمبيوتر والإنترنت والاتصالات " لغة العصر " ، العدد الثامن ، اغسطس ٢٠٠١ ،

أو بالتسجيل غير المشروع.

١- التقاط المعلومات المتواجدة ما بين الحاسب الآلي والنهاية الطرفية:

ويتم هذا الالتقاط عن طريق توصيل خطوط تحويله، والتي ترسل اشارات الكترونية " ذبذبات الكترونية مكبرة" تمثل المعلومات المختلصة إلى النهاية الطرفية المتجسدة، أو عن طريق مرسل صغير يسمح بنقل المعلومات عن بعد، وعلى النقيض عندما تسلك المعلومات الطريق الجوى- كما فى حالة البث عن طريق القمر الصناعى - توضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية، والتي تسمح بالتقاط الاشعاعات واحتجاز مضمونها.

٢- التوصيل المباشر على خط الكترونى Wire Tape:

وتباشر هذه التقنية عن طريق وضع مركز تنصت يسهل تسجيل كل الإتصالات، كما يمكن أن تؤدي هذه الوظيفة أيضا ميكروفونات صغيرة.

٣- التقاط الاشعاعات الصادرة عن الجهاز المعلوماتى Electromagnetic pickup

ويمكن عن طريق هذه التقنية اعادة تكوين خصائص المعلومات التى تتحرك وتتنقل من خلال نظام معلوماتى، ويكفى لاتمام ذلك أن تسجل ثم تحل شفرة الاشعاعات الالكترومغناطيسية المنبثة بواسطة أجهزة الكترونية، وفى الواقع، تصدر بعض عناصر الانظمة القوية - وعلى وجه الخصوص الطابعات السريعة Les imprimantes rapides - اثناء تادية وظيفتها اشعاعات الالكترومغناطيسية، وقد ثبت انه بإمكان شاحنة صغيرة مجهزة تجهيزا خاصا وتقف بمحاذاة مبنى مكتظ بالحاسبات الآلية أن تلتقط وتسجل هذه الاشعاعات، ويمكن عن طريق جهاز لفك الرموز أن يطلب من طابعة متصلة بنظيرتها الموجودة فى المركز المستهدف النسخ الحرفى لنفس هذه المعلومات، ونذكر فى هذا الخصوص مثال شهير للسطو المسلح الالكترونى، وهو خاص باختلاس اموال عن طريق التقاط امر بالتحويل مرسل من بنك إلى آخر، وقد تمكن المختلس من تزيف الرسالة بالامر بدفع نفس المبلغ لحساب فتح باسمه.

٤- التدخل غير المشروع فى نظام بواسطة طرفيه بعيدة " الولوج غير المسموح

به فى نظم المعلومات " Phone Freak:

ادى ربط الحاسبات الآلية بعضها ببعض الاخر عن طريق شبكات المعلومات إلى سرعة انتقال المعلومات من جهة، والى سهولة التطفل عليه من

جهة اخرى، ويمكن عن طريق تقنية بث المعلومات على شبكات اتصالات بعيدية *télématique* التدخل أو الدخول في نظام معلوماتي من بعد، ثم يصبح بعد ذلك نسخ المعلومات أو التطفل عليها أو تدميرها شيئاً سهلاً، ويكفي لبلوغ ذلك استخدام جهاز المودم *Modem* والتزود بكلمة السر أو مفتاح الشفرة المناسب، حيث يسمح هذا الجهاز للمتطفلين من اية مسافة يتواجدون فيها بالولوج من الحاسبات الآلية المستهدفة، ودون اي مساس مادي بحق ملكية الغير، أو ترك اثر يدل على انتهاك المعلومات أو نسخها^(٤٦).

وقد أبانت صحيفة *Canard en Chainé* الفرنسية عن عملية تعدي من بعد على ذاكرات الحاسبات الآلية بالشركة الدولية للخدمات المعلوماتية *C.I.S.I* وهذه هي احدى الحالات النادرة التي كشف عنها في فرنسا^(٤٧).

خامساً : سرقة البرامج والمعلومات المخزنة آلياً عن طريق الهاكرز والكرارز^(٤٨):

^{٤٦}- أنظر : د/ محمد سامي الشوا، ص ٢٠٤.

^{٤٧}- أنظر : د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية، القاهرة، ١٩٩٤، صفحة ٦٨، ٧١.

^{٤٨}- في الستينات من القرن الماضي كانت كلمة هاكلز تطلق على المبرمجين الذين لهم خبرة واسعة ودراية كاملة بخبايا البرامج والنظم، وكانوا يقدمون يد العون لكل المؤسسات التي تدار بواسطة الكمبيوتر، وفي ذلك الوقت كانت لغات البرمجة السائدة هي الكوبول، والفورتان والبيزك التقليدي ، تلك اللغات التي لا يسمع عنها الان الا زوار متاحف الكمبيوتر، وحتى ذلك الوقت كانت كلمة هاكلز تطلق على المبرمجين الشرفاء ولعل اشهرهم في تلك الفترة هما: " دنيس ريتشى وكيفين تومسون" اللذان وضعوا حجر الاساس لنظام التشغيل *Unix* ومع بدايات ظهور نظام التشغيل *Windows* الذي كان يحتوى على العديد من الثغرات الامنية- ومازال ومع بداية ظهور الانترنت بدا بعض الهاكرز يأخذون منعطفاً اخر الا وهو الاختراق والتجسس على اجهزة الكمبيوتر وسرعان ما فقدت كلمة هاكلز معناها الحقيقي واصبحت تطلق على لصوص ومخترقي اجهزة الكمبيوتر بغرض سرقة المعلومات، ولعل اشهر لصوص الهاكرز على مر التاريخ والذي يطلق عليه " ملك الهاكرز " وهو " كيفين ميتيك " الذي حطم الكثير من الدفاعات الحصينة لاجهزة الكمبيوتر للعديد من المؤسسات والهيئات ووصل الى ادق ما تحتوى تلك الأجهزة من معلومات بدءاً من شركات الاتصالات الموجودة في محيط مدينته وصولاً إلى وزارة الدفاع الامريكية " البنجاجون"

الهاكرز والكراكز كلاهما لص معلوماتي، إلا أن هناك فارقا بينهما يتمثل في الغاية التي يسعى إليها كل منهما، فالغاية التي يسعى إليها الهاكرز هي اختراق أجهزة الحاسب الآلي للحصول على المعلومات، أما الكراكز فهم المحطمون لكلمات السر والكاسرون لحماية برامج الحاسب الآلي، وكل ما يشغلهم هو كيفية نسخ وتداول البرامج المحمية^(٤٩).

سادسا: بعض صور الاحتيال المعلوماتي التي تقع على البرامج والمعلومات المخزنة آليا:

ففي تلك الصور يقوم الجناة بالتلاعب في نظم معالجة المعلومات للحصول بغير حق على اموال أو أصول أو خدمات، كما يتم التلاعب أيضا في المعلومات والبيانات المعالجة آليا بنية تحقيق ربح مادي غير مشروع.

اما بالنسبة للكراكز فان كلمة كراكز Crachers في اللغة مأخوذة من الفعل Crack بمعنى كسر وتحطيم وبالفعل فان الكراكز هم المحطمون لكلمات السر والكاسرون لحماية البرامج، وكل ما يشغلهم هو كيفية نسخ وتداول البرامج المحمية.

مهندس احمد حسن خميس ، الهاكرز والكراكز ، دار البراء، الاسكندرية ، ٢٠٠٣ ، ص ٦- ٧.

^{٤٩}- أنظر : مهندس احمد حسن خميس، المرجع السابق ، ص ٦.

المطلب الثاني

سرقة منفعة الحاسب الآلي أو الاستعمال غير المصرح
به لنظام الحاسب الآلي

يقصد بسرقة منفعة الحاسب الآلي "استخدامه لأغراض شخصية أو تجارية بدون علم مالكة أو حائزة القانوني" أو استخدام نظام الحاسب الآلي وبرامجه بغير تصريح بذلك من مالكة أو حائزة" ويعد هذا الفعل غير المشروع من أكثر الجرائم المعلوماتية تعارفاً، وقد ترتكب تلك الجريمة إما بواسطة مستخدمى الشركات الخاصة أو المرافق العامة، وهناك العديد من الأمثلة التي تشير إلى حدوثها فى جميع انحاء العالم.

وتمارس سرقة منفعة الحاسب الآلي فى معظم حالاتها بغير غرض إجرامى، اى بدون تحقيق ربح أو استفادة ، حيث يلجأ إليها بعض الاشخاص – على سبيل المثال- لتحرير بطاقات مخصصة لأعمال الخير أو لنسخ ألعاب الفيديو أو برامج الحاسب الآلي لاستعمالهم الشخصى، الا انه فى بعض حالات سرقة منفعة الحاسب الآلي نجد أنفسنا ازاء مجموعة من المستخدمين تستغل الحاسب الآلي الخاص بالشركة أو الادارة التي تعمل بها كى تمارس فى الظلام أو الخفاء عملا على منوال عملها الاصلى، وهكذا اكتشف – على سبيل المثال- فى مدينة شيكاغو الأمريكية فريق مكون من خمسة اشخاص يعملون باحدى المراكز التعليمية بها، اقاموا بالفعل شركة حقيقية خاصة بهم لبرمجة اعمال عملائهم الخصوصيين على الحاسب الآلي التابع لمركز عملهم.

ويثير هذا الفرض من الناحية القانونية مسألتين : اولاهما: أن الجناة تمكنوا من الحصول على مزايا مالية غير مشروعة" كتوفير نفقات الاستعمال وتحقيق مكاسب مادية"، نظرا للاستعمال التجارى للحاسب الآلي التابع لمركز عملهم الاساسى، وثانيهما: الضرر الذى لحق بالمالك أو الحائز القانونى للحاسب الآلي لاسيما إذا ما كان هذا المالك أو الحائز مؤجراً للحاسب الآلي^(٥٠).

٥٠- انظر د/ محمد سامى الشوا - صفحات ٢٢٠ - ٢٢١ - مرجع سابق.

ويدخل أيضا في هذه الجريمة ما اصطلح على تسميته من قبل الفقة بسرقة وقت الآلة أو وقت الحاسب الآلى ، اى " استخدام وقت الآلة أو وقت الحاسب من اجل اغراض شخصية" ، فقد يحدث عملاً- وبدلا من الابقاء على استخدام الجهاز المعلوماتى والموجود بمكان العمل لاغراض مهنية بحتة ومسموح بها - أن يتم الاستيلاء على وقت هذا الجهاز بمعرفة بعض المستخدمين غير الامناء بغية انجاز اعمال خاصة بهم وبدون علم الحائز الشرعى للنظام المعلوماتى.

وجريمة سرقة وقت الحاسب الآلى أو الآلة من الجرائم الشائعة فى العديد من مراكز الابحاث فى مختلف دول العالم، ففى فرنسا- على سبيل المثال - من السهولة بمكان أن ينتقل باحث من اجل توفير نفقات معملة إلى مركز آخر، ويستعير كلمة السر أو شفرة الوصل للولوج (الدخول) فى بنك المعلومات الخاص بهذا المركز، ويعد هذا الوقت للحاسب الآلى من الامور المكلفة جدا، وقد يتسبب محاسب غير امين فى احداث خسائر لمنشأة بأكملها - نتيجة لاقترافة هذه الجريمة- تفوق باضعاف اجور المستخدمين بها.

ويمكن أن نذكر فى هذا الخصوص واقعة اثنين من مستخدمى شركات غاز بريطانية ، قاما عن طريق اعلانات صغيرة ببيع رسومات صممت بواسطة النظام المعلوماتى الخاص بهذه الشركة، وهناك أيضا المثال الخاص بـ ٢٠٠ مستخدم الذين قاموا باستخدام الحاسب الآلى الخاص بمركز تصنيع وحماية الصواريخ النووية من اجل تخزين العاب اليانصيب والخطابات الشخصية^(٥١).

المطلب الثالث

بعض أفعال تزوير المعلومات والبيانات والبرامج المخزنة آلياً والتلاعب بها.

قد ترتكب بعض افعال التزوير المعلوماتى، والتلاعب فى البرامج أو البيانات أو المعلومات المخزنة آلياً، وذلك لاغراض غير مشروعة تتمثل غالبا فى الاضرار بالمصالح العليا للدولة، والحياة الشخصية للأفراد.

^{٥١} - انظر د/ محمد سامى الشوا - صفحات ٨٥ ، ٨٦ - المرجع السابق..

والأمثلة على ذلك كثيرة ومتنوعة، نذكر منها، قيام أحد الأشخاص فى المانيا بالتلاعب فى نتيجة اختبار الدم الذى اجرى له لقياس نسبة المواد المخدرة به بعد أن تمكن من الوصول إلى نظام الحاسب الآلى الذى يحتوى على نتيجة هذه الاختبارات، وما قام به بعض الاشخاص أيضا فى المانيا من تلاعب فى سجلات الشرطة بهدف حذف اسماء بعض الأشخاص المطلوب القبض عليهم، وما حدث فى يناير عام ١٩٧٩ عندما تعرضت احدى الطائرات التى هبطت فى مطار كنىدى بولاية نيويورك الأمريكية وعلى متنها السفير الروسى للخطر نتيجة تلاعب احد المراقبين الجويين بنظام الحاسب الآلى، وما حدث فى الشركة الأمريكية "TRW Computer Credity data" عندما تمكن ستة من العاملين بها من التلاعب فى البيانات والمعلومات الخاصة بالمركز الائتمانى للأفراد الذين يرغب عملاء الشركة فى التعامل معهم، من خلال تعديل أو محو البيانات التى تظهر المركز الائتمانى السئ لصاحبها لتحل محلها بيانات جديدة تفيد تمتع صاحبها بمركز ائتمانى جيد، وذلك فى مقابل مبالغ مالية تم الاتفاق عليها، حيث قدر عدد السجلات التى تم التلاعب بها بحوالى مائة سجل، وبناء على تلك البيانات الإئتمانية التى تم ادخالها بالمحو أو بالاضافة أو بهما معا إلى نظام المعلومات الآلى الخاص بالشركة، قام العديد من عملائها بالدخول فى معاملات مالية وتجارية مع اشخاص ذوى سمعة ائتمانية سيئة.

المطلب الرابع

إختراق الحاسب الآلى وإنتحال هوية المستخدم.

من الممكن إختراق الحاسبات الآلية أو إنتحال هوية مستخدمى تلك الحاسبات أما مادياً أو الكترونياً، ويسمح الإختراق المادى بدخول الجانى إلى مناطق خاضعة للسيطرة عن طريق بوابات الكترونية أو آلية، واسلوب الإختراق الأكثر شيوعاً هو أن يقف شخص غير مسموح له بالدخول امام البوابات المغلقة حاملاً بين ذراعية متعلقات خاصة بالحاسبات الآلية- كالشرائط الممغنطة على سبيل المثال- أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب فيدخل معه فى نفس الوقت، ولذا فانه يمكن القول بان التواجد فى صالات الحاسب الآلية هو امر حتمى لارتكاب هذه الجرائم، وينطوى السلوك غير

المشروع فيها على اطلاع غير مسموح به على البيانات والمعلومات المخزنة في نظم المعلومات ، ولهذا السلوك صور عديدة ، منها:

١- سرقة القائمة: وهي عملية مادية بحتة يكتفى فيها السارق بسحب القائمة من الطابعة.

٢- الاطلاع على المعلومات : ويقصد به مطالعة ومشاهدة المعلومات التي تظهر على الحاسبات الآلية، ويتم ذلك لأغراض غير مشروعة تتمثل غالباً في السرقة والتجسس والاحتيال.

٣- التنصت المجرد على المعلومات: ويتم ذلك عن طريق استخدام مكبرات للصوت تلتقط المعلومات والبيانات.

اما عن انتحال هوية مستخدم الحاسب الآلي ، فيقصد به " سرقة شخصية مستخدم آخر" ويتطلب الوصول إلى الحاسب الآلي أو إلى الطرفيات لانتحال هوية مستخدمى الحاسبات الآلية معرفة دقيقة فى اغلب الاحيان لمستعملى تلك الأجهزة، ويرتكز فحص الهوية ثم انتحالها على مجموعة معلومات متوافقة يستخدمه المستعمل ككلمة السر، أو اية جملة خاصة بالمستعمل، أو اية خاصة فسيولوجية خاصة به (كالبصمة الرقمية، أو اية ملامح للوجه أو هندسة الكف أو الصوت) ، بالاضافة إلى اى شئ يمتلكه المستعمل- كالبطاقة الممغنطة أو المفتاح المعدنى، فلو تمكن اى انسان من الحصول على تلك المجموعة من المعلومات المتوافقة، فانه يصبح قادرا على انتحال شخصية اى مستعمل لجهاز الحاسب الآلي، والامثلة على ذلك عديدة فقد ادعى شاب انه صحفى فى احدى المجلات واتصل بشركات اتصالات هاتفية مدعيا انه بصدد نشر مقالة عن النظام المعلوماتى المستخدم فى تلك الشركة، فدعته الشركة لزيارة مقرها ، ثم قدم له موظفيها عرضاً كاملاً ومفصلاً عن الأجهزة المعلوماتية وتطبيقاتها فى الشركة، فكانت النتيجة انه سرق منهم معدات تزيد قيمتها على مليون دولار امريكى^(٥٢).

٥٢- انظر د/ عبد الله حسين على، مرجع سابق ، صفحات ٩٤- ٩٧.

المطلب الخامس التجسس المعلوماتي

الحاسبات الآلية أصبحت الآن ضرورة في كافة المجالات ، حيث تعهد مختلف الادارات والمؤسسات والمنظمات في كل من القطاع الحكومي والقطاع الخاصة بمعلوماتها الاكثر سرية إلى الحاسبات الالكترونية، مولية نظم تلك الحاسبات الامنية، ثقنتها شبة العمياء، وجاهلة أو متناسية ان هذا الجهاز كثيرا ما بدا - وفقا لوصف البعض - كخزانة بغير ابواب^(٥٣)، وقد ادى هذا الاستخدام المتزايد للحاسبات الآلية في مختلف المجالات إلى تمركز المعلومات بدرجة كبيرة في جميع الدول - المستخدمة لنظم المعلومات - في تلك الأجهزة ، كما ادى تخزين هذه البيانات و المعلومات على هذا النحو - إلى سهولة التجسس على الاسر الصناعية والتجارية والمهنية والعسكرية، ومن ثم اصبحت تلك البيانات والمعلومات المخزنة آليا في مجالات عديدة - كالأبحاث والتجارة والطاقة النووية.. وغيرها - تشكل الهدف المفضل لانشطة التجسس غير المشروع، وعلى سبل المثال، فان (الحسابات، والموازنات ، وعناوين العملاء) غالبا ما تجذب انتباه الجواسيس المعلوماتيين اليها"^(٥٤).

" ووفقا لرأى بعض الخبراء الأمنيين للحاسبات الالكترونية، فان سهولة اختراق انظمة تلك الحاسبات ، والوصول إلى ما تحوية من برامج وبيانات ومعلومات ، وترجع إلى عدة عوامل، أبرزها:

١- تسقط صناعة الحاسبات الآلية في اندفاعها للانتاج والتسويق مسألة الامن من حساباتها لصالح رفع القدرة الوظيفية وتحسين مستوى الاداء في الخدمة.

٢- توجه صناعة أجهزة الإتصال والحاسبات الآلية جل اهتمامها ، نحو

^{٥٣}- شبه البعض الحاسبات الآلية بانها خزائن بلا ابواب، وفي ذلك يقول Kenneth Weiss رئيس قسم الحاسبات الالية لدى شركة امريكية، انه " لو ادرك كبار المسؤولين الاداريين حقيقة المسئولية والمخاطر المحملة التي تهدد اصول الشركات وسمعتها ، لاغلقوا جميع شبكات ومراكز الحاسبات الالية.

د/ هشام محمد فريد رستم، هامش (١) ص ١٣٢، د/ محمد سامي الشوا، هامش (٢)، ص ٢١٢ ..

^{٥٤}- د/ هشام محمد فريد رستم، ص ١٣٢.

انتاج اسرع الوسائل للاتصال، دونما اهتمام موازن لحماية البرامج والمعلومات من الاعتراض غير المشروع والالتقاط، حتى لا تصطدم بارتفاع التكلفة وزيادة الاسعار.

٣- تزايد اعداد شبكات الحاسبات الآلية واتساع نطاقها بما قد يفوق القدرة على توفير الحماية لجميع اجزائها^(٥٥).

مجالات التجسس المعلوماتي:

تتعدد مجالات التجسس المعلوماتي بتعدد مجالات واوجه النشاط المختلفة، فعلى سبيل المثال، نجد انه في مجالات النشاط التجاري، تركز عمليات التجسس المعلوماتي، على كشف الأسرار التسويقية والتجارة (كحسابات التكلفة، وكشوف الميزانية، وحالة الأسواق، وعناوين العملاء.. وغيرها) وفي مجالات النشاط الصناعي والتقني، تسعى عمليات التجسس - بصورة كبيرة- إلى (كشف نتائج الابحاث والتطوير، والبيانات المتعلقة بعمليات الانتاج، وأسرار تصميمات المنتجات " لاسيما تصميمات الشرائح الصغيرة من أشباه الموصلات"، وفي المجالات الامنية والعسكرية والاستخباراتية والنووية، تكشف نشاطات التجسس جهودها نحو اختراق النظم الامنية والعسكرية والاستخباراتية والنووية للوصول إلى ادق تفاصيل أسرار البيانات والمعلومات المتعلقة بتلك الشئون، بما يكون له من بالغ الاثر على امن وبقاء الدول والحكومات.

وللتجسس المعلوماتي أيضا في مختلف المجالات ابعاد خطيرة غير مسبوقه، فالتكثيف المركز للمعلومات في ذاكرات الحاسبات الآلية يجعلها هدفا مغريا لأي متصلص يملك خبرة كافية وتجهيزات جيدة، سيما مع امكانية الاستعانة بالحاسبات الآلية في فرز المعلومات المخزنة وتصنيفها ونسخها بسهولة وسرعة فائقة، وبغير أن يتخلف عن ذلك اي اثر.

أساليب التجسس المعلوماتي:

" تتعد صور واشكال تخزين البيانات والمعلومات المعالجة الكترونيا، فقد تكون تلك البيانات و المعلومات مخزنة على هيئة نبضات كهربائية في دوائر الكترونية مجمعة، أو في وسائط وواعية معينة" كالبطاقات الورقية المثقبة، والاشرطة والاقراص المغناطيسية" ، كما انها قد تكون في حالة بث وانتقال من

٥٥- د/ محمد سامي الشوا، ص ٢١٢.

نهاية طرفية إلى أخرى، والتوصل غير المشروع إلى تلك البيانات والمعلومات له في كل حالة من حالتى تخزين وانتقال البيانات والمعلومات السابقتين اسالبيه.

١- أساليب التجسس والحصول على البيانات والمعلومات المخزنة:

وهذه الاساليب متعددة، ومتدرجة فى تعقيدها:

أ- فمن هذه الاساليب ماله طابع تقليدى، ومن قبيله: سرقة الاسطوانات التى تخزن فيها البيانات والمعلومات، ورشوة أو تهديد عاملين بالجهة المستهدفة. للكشف عن البيانات المخزنة داخل حاسباتها، والحاق موظفين بالجهة المستهدفة أيضا يتولون مهمة التجسس من خلال عملهم بها.

ب- ومن هذه الاساليب ماله طابع فنى، وذلك مثل: دس وحدات ناقلة للبيانات داخل أجهزة الحاسب الآلى، وتوصيله كهربائيا بشكل خفى بكابل خارجى، ومعالجة الشرائط والاسطوانات الممغنطة التى لم تكمل الجهة المالكة لها محوها أو اتلافها لاعادة اظهار محتوياتها، واستظهار المعلومات التى تستخدم اوراق الكربون عند تدوينها بمعالجة اوراق الكربون المهمة، واخفاء برنامج "حصان طرواده"^(٥٦)، فى البرامج التطبيقية بحيث يسمح بالوصول عن

^{٥٦}- برنامج حصان طرواده Torjans هو برنامج خادع يخفى وراءه غرضا غير مشروع ، حيث يظهر كبرنامج عادى يؤدي بعض المهام المفيدة والمالوفة لمستخدمة ، بينما الحقيقة على النقيض من ذلك تماما، حيث يخفى هذا البرنامج داخله بعض الاوامر والتعليمات التى تؤدي عند تشغيله مهام ضارة غير متوقعة تمثل اغراضه الحقيقية المضمرة، وهكذا فقد يبدو البرنامج كما لو كان معدا لتنظيم البيانات بالملفات أو تكثيفها، بينما الهدف الحقيقى من وراء تشغيله قد يكون محو هذه البيانات، من ذاكرة الحاسب الآلى أو التهديد بذلك لابتنزاز مستخدمة أو الاستيلاء على المال بتخريف البيانات المدخلة أو المخزنة، وعادة ما توجد برامج احصنة طرواده فى برامج الاعمال (كبرامج معالجة النصوص، وبرنامج ادارة قواعد البيانات) وغالبا ما تكون مختفية فى منتصف البرنامج أو فى مكان غير مستعمل منه ، والبرنامج الذى يتضمنها قد يعمل بطريقة صحيحة لعدة شهور قبل أن تظهر اعراض الاوامر غير المتوقعة وغير المشروعة، وقد تظهر هذه الاوامر وتنفذ مباشرة عند تشغيله ، وبرامج احصنة طرواده- وعلى خلاف ما يسمى بفيروسات الحاسبات الآلى- لا تتسخ نفسها ، واكتشافها بالغ الصعوبة، وكذلك ايضا محاولة اقتفاء اثر معدها، وقد تم نعت تلك البرامج بـ" برامج حصان طرواده" نظرا لخطورتها ، واثارها المدمرة، وقدرتها على الخداع، والمفاجأة والتضليل، مثلما فعل حصان طرواده الخشبى الكبير الذى ضم بداخله مجموعة من الجنود حينما احكم خداع جيش طرواده الذى كان يدافع عن ارضه حيال غزو اسبرطه لتلك المدينة، فعندما رآه اهل المدينة فرحوا به

بعد إلى قاعدة البيانات لقراءتها أو تعديلها بغير ان يشعر بذلك احد.
ج- كما يمكن أيضا باستخدام هوائيات متصلة بحاسب خاص التقاط وتسجيل ومعالجة الموجات الكهرومغناطيسية التي تنبعث من الحاسب الآلي اثناء تشغيله ، وترجمتها إلى بيانات واضحة، وذلك من مسافة تبعد عن الحاسب المستهدف بما يزيد على الاف الكيلومترات.

د- كما يمكن كذلك استغلال ما يعرف " بالابواب الخفية أو الخليفة Back doors" والمعروفة أيضا باسم " ابواب المصيدة Trap doors" في الوصول غير المشروع، وغير المحدود إلى برامج وملفات بيانات النظام، اذ من المعتاد عند اعداد البرامج ترك ثغرات أو نقاط دخول غير معلن عنها تتجنب اجراءات الامن العادية، وذلك بهدف السماح باضافة تعليمات إلى البرامج لتلأفي ما قد يظهر فيها من اخطاء ، ووجود هذه الثغرات قد لا يكون متعمدا دائما، حيث يمكن أن توجد عرضا في بعض الاحيان نتيجة اخطاء في التصميم الكلي للنظام أو نتيجة مواطن ضعف في مجموعة الدارات الالكترونية للحاسبات الآلية ، وعندما يكون تركها مقصودا ، فانها تلغى في الطبعة النهائية للبرنامج ، بيد أن هذا

وقاموا بادخاله داخل مدينة طروادة، وحينما استقر به الحال قام الغزاة بالخروج منه واستولوا على تلك المدينة، وفقا لما جاء بقصص الحرب التي رواها الشاعر الاغريقي القديم هوميروس في ملحمتي الاللياذة والأوديسة .

د/ هشام محمد فريد رستم- ص ٧٢- ٧٤، مهندس: احمد حسن خميس، المرجع السابق ، ص ٣٦ = ولمزيد من الايضاح ، فان برنامج حصان طراوده ما هو الا اسم لملف برنامج تجسس يتم ارساله وزرعة في جهاز الضحية ليكون هو حلقة الوصل بين جهاز المخترق وجهاز الضحية، ويطلق على هذا البرنامج اسماء عديدة، منها الملف اللاصق أو الصامت أو ملف الباتش Patch files وهو الاسم الأشهر في عالم الهاكرز، وهناك طرق عديدة لارسال هذا البرنامج وزرعاته لعل أشهرها على الاطلاق هو استخدام البريد الالكتروني، حيث يقوم المخترق بارسال رسالة إلى الضحية ويرفق بها ملف حصان طرواده، ونظر لسذاجة الضحية أو عدم الماماة بمضمون تلك الرسالة، فانه يقوم بفتحها وتحميل الملف المرفق بها اعتقادا منه أنه يمثل احد البرامج المفيدة، ثم يكتشف بعد ذلك أن هذا البرنامج لا يعمل فيظن أن به عطل ما فيهملة وكان شيئا لم يكن، وفي ذلك الوقت يكون حصان طرواده قدأخذ مكانه داخل نظام حاسب الضحية، وبدا في مهمة التجسس حتى وان قام الضحية بحذف البرنامج بعد ذلك فلا فائدة من ذلك فملف حصان طرواده يكتشف بعد ذلك فقط ليقيم بمهمة .

مهندس: احمد حسن خميس، المرجع نفسه ، ص ٣٦ .

الالغاء قد يتم في بعض الاحيان بصورة متعمدة اغفالة، وبذلك يكون متاحا- إذا ما وجدت عمداً أو عرضاً ثغرات أو نقاط دخول – الوصول إلى اجزاء من النظام غير مصرح بولوجها، والاطلاع على ملف البيانات المخزنة داخله.

٢- أساليب التجسس والحصول على البيانات والمعلومات المتنقلة:

إذا كانت البيانات والمعلومات في حالة انتقال فيما بين النهايات الطرفية، فإن اساليب التجسس عليها والتقاطها تختلف باختلاف الوسيلة الناقلة.

أ- فالبيانات التي يجرى نقلها عبر الاسلاك المعدنية أو خطوط الهاتف المخصصة لنظم الإتصالات الالكترونية لا يحتاج معترضها لاكثر من مجرد جهاز التقاط بسيط يمكن تركيبه من وحدات الكترونية تتوافر في الأسواق، وتثبيتته بطريقة خفية داخل صناديق التوزيع التي تنتهي إليها معظم وسائل الإتصال السلكية واللاسلكية، وقد يضاف جهاز حث إلى جهاز الالتقاط كي يعمل فحسب حال وجود بيانات أو اشارات في السلك أو الخط الذي تجرى مراقبته.

ب- أما المعترض لوصلات الموجة القصيرة المحتوية على حزمة من القنوات المحملة بالبيانات، فإنه يستفيد مما ينتج عن بث هذه الموجات من نتوءات اشعاعية، جانبية وخلفية، فيستخدم في مجال أحد هذه النتوءات أجهزة التقاط خاملة لا يصدر عنها أية اشارات لاسلكية، مما يجعل من الصعب اكتشافها.

ج- وبالكيفية السابقة يمكن اعتراض الإتصالات التي تبث من المحطات الأرضية في اتجاه الاقمار الصناعية، حيث يمكن أيضا استغلال ظاهرة النتوءات الجانبية والخلفية، أما الشعاع الذي يبثه القمر الصناعي إلى الأرض فإنه يغطي مساحة شاسعة منها تقدر بالآلاف الأميال المربعة، ومن أي موقع في نطاق هذه المساحة يمكن – باستخدام أجهزة خاصة- التقاط البيانات والمعلومات المرسلّة ، حتى أن البيانات التي يجرى عن طريق قمر صناعي- على سبيل المثال – إرسالها من كاليفورنيا (جنوب الولايات المتحدة الأمريكية) إلى نيويورك (بشرقيها) يمكن لمعارض في فلوريدا (بالجنوب) إلتقاطها^(٥٧).

٥٧- د/ هشام محمد فريد رستم- ص ١٤٠- ١٤٣.

المطلب السادس

الإتلاف المعلوماتي

يقصد بالاتلاف المعلوماتي أو التخريب المنطقي أو تدمير نظم المعلومات " مدى صلاحية البرامج و المعلومات المعالجة آليا لأن تكون محلا يرد عليه العدوان في جريمة الإتلاف، عندما لا يترتب على المساس بها أى إتلاف لأى من العناصر المادية التى يتكون نظام المعالجة الآلية للمعلومات".

وتتعدد الاساليب والوسائل التى يستخدمها الجناة فى جرائم المعلوماتية لإتلاف برامج الحاسب الآلى، والبيانات والمعلومات المعالجة والمخزنة آليا، والتلاعب بها، وتختلف تلك الأساليب أيضا باختلاف اغراض الجناة من حالة لأخرى.

والإتلاف المعلوماتي إما أن يكون عن عمد وقصد، وإما أن يكون بغير قصد، كما أن هذا الإتلاف قد يكون كلياً يتمثل فى محو البرامج والمعلومات المخزنة داخل جهاز الحاسب الآلى كلياً، وقد يكون جزئياً، ويطلق عليه فى هذه الحالة (تشويه أو تعيب) ويتمثل فى ادخال فيروس داخل الجهاز بحيث يعمل على التقليل من كفاءته أو يبطئ حركة الجهاز ذاته^(٥٨).

أساليب التخريب المنطقي للبرامج والمعلومات:

ينصب الإتلاف المعلوماتي أو التخريب المنطقي للحاسب الآلى ومكونات على الكيانات المنطقية له، والتى تتمثل - كما سبق أن ذكرنا- فى مجموعة من الاوامر والتعليمات اللازمة لتشغيل اجهزة الحاسب الآلى وإنجاز مهمة واكثر ما يتم التوسل به لتنفيذ التخريب المنطقي هو البرامج ذات الأثر التدميري التى تستهدف محو جزء أو كل برامج أو ملفات الحاسب أو البيانات و المعلومات المخزنة به، وكذلك أيضا سائر البرامج الخبيثة التى تصيب نظام الحاسب الالكتروني بالشلل والعطب، وهذه البرامج متعددة، ولكل برنامج منها تسمية شائعة تعبر عن وظائفه التخريبية والضرر الذى يمكن أن يلحقه بهذا الحاسب ومكوناته^(٥٩)، ولعل أبرز ما اثار منها مشكلات فنية، وتسبب فى خسائر مادية فادحة ما يلي:

^{٥٨}- انظر: محمد أمين الرومى- جرائم الكمبيوتر والانترنت -دار المطبوعات الجامعية الاسكندرية ٢٠٠٣ - صفحة ٥٦.

^{٥٩}- د. هشام محمد فريد رستم، ص ١٥٨.

أولاً: استخدام برامج القنابل المنطقية Logic Bomby:

القنبلة المنطقية عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة مضمون النظام بغية تسهيل تنفيذ عمل أو غرض غير مشروع^(٦٠).

وعلى سبيل المثال، فإنه يمكن إدراج تعليمات في برنامج نظام التشغيل وينصب البحث بعد ذلك على عمل معين يمكن أن يكون محلاً للاعتداء، كأن تسعى قنبلة منطقية إلى البحث عن حرف معين وليكن (أ) في أي سجل يتضمن أمراً بالدفع، وعندما تكتشفه، تحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل^(٦١).

أمثلة للتخريب المنطقي بواسطة استخدام برامج القنبلة المنطقية:

١- في الدانمارك، تمكن خبير في نظم المعلومات من وضع قنبلة منطقية في نظام إحدى الحاسبات، ترتب عليه محو أكثر من مائة برنامج، وقد تم أيضاً محو النسخ الاحتياطية لهذه البرامج عند تشغيلها نتيجة انتقال آثار القنبلة إليها، وتم ضبط الجاني، وقد عاقبة القضاء الدانمركي بالحبس لمدة سبعة أشهر^(٦٢).

٢- قام مبرمج نظم سابق بإحدى الشركات الكبرى في فورت ورت بولاية تكساس الأمريكية عام ١٩٨٥ بالدخول إلى نظام معلومات حاسب تلك الشركة، بعد عدة أيام من الاستغناء عنه، معتمداً على معرفته لكلمة السر التي لم تقم الشركة بتغييرها، ووضع فيه قنبلة منطقية من شأنها محو كل سجلات عمولة المبيعات مرة كل شهر، ولم يتم اكتشاف هذه القنبلة ووقف مفعولها إلا بعد أن محت أكثر من ١٦٨ ألف سجل من سجلات عمولة المبيعات الخاصة بتلك الشركة^(٦٣).

٣- ومن الحالات فائقة الخطر للقنابل المنطقية التي يذكرها بعض الخبراء

٦٠- أنظر : د/ محمد سامي الشواء، ص ١٩٤، أ. محمد أمين الرومي، ص ٥٦.

٦١- أنظر : د/ محمد سامي الشواء، ص ١٩٥.

٦٢- أنظر : د/ محمد سامي الشواء، ص ١٩٦، د. هشام رستم، ص ١٦٠.

٦٣- أنظر : د/ هشام محمد فريد رستم، ص ١٦٠.

والمختصين في مجال علوم الحاسبات الآلية، إخفاء قنابل منطقية، وبرامج أحصنة طرواده كذلك، في البرامج المعلوماتية التي تتبعها دولة لأخرى، مثلما كانت بعض الدول تقوم بإخفاء قنابل منطقية في البرامج التي كانت تتبعها للاتحاد السوفيتي (قبل تفككه)^(٦٤).

ثانيا: استخدام برنامج القنبلة الزمنية أو الموقوتة Time Bombs

القنبلة الزمنية أو الموقوتة على عكس القنبلة المنطقية تماما، هي برامج مصممة بحيث تبقى ساكنة وغير فعالة ، وغير مكتشفة بالتالي لمدد قد تصل إلى اشهر ، بل وحتى أعوام، وهذه المدة يحددها عادة مؤشر زمني يحتوية البرنامج – كتاريخ معين- بحيث ينشط برنامج القنبلة عند حلوله، ويؤدي مهمة التدميرية الهدامة^(٦٥) ، وتثير القنبلة الزمنية- على النحو السابق بيانه- حدثا في لحظة زمنية محددة بالساعة أو اليوم أو السنة، ومن ثم تنطلق أو تنفجر في زمن وتاريخ محدد من السنة، فهي مرتبطة دائما بعنصر الزمن، فيتم إدخالها في برنامج، وتنفذ في جزء من الملى ثانية أو في بضع ثوان أو دقائق وفقا للتحديد أو البرمجة اللازمة للانفجار، فعلى سبيل المثال يمكن ضبط القنبلة الزمنية أو الموقوتة لكي تنفجر بعد شهرين في يوم محدد وساعة محددة، لتحول مبلغا من النقود من حساب شخص معين في اللحظة التي يكون فيها مرتكب الجريمة متواجدا في بلدة اخرى غير بلدة المجنى عليه^(٦٦).

أمثلة لتدمير نظم المعلومات عن طريق استخدام برنامج القنبلة الزمنية:

١- في فرنسا، قام محاسب من الخبراء في نظم المعلومات – وبدافع الانتقام على أثر فصله من المنشأة التي يعمل بها- بوضع قنبلة زمنية في شبكة المعلومات الخاصة بتلك المنشأة، بحيث تنفجر تلك القنبلة بعد مضي ستة اشهر من رحيلة عن المنشأة، وترتب على ذلك أن حدث إتلاف لكل البيانات الخاصة بها^(٦٧).

^{٦٤}-أنظر : د/ هشام محمد فريد رستم ، ص ١٦٠.

^{٦٥}-أنظر : د/ هشام محمد فريد رستم ، ص ١٥٨.

^{٦٦}-أنظر : د/ محمد سامي الشواء، ص ١٩٥.

^{٦٧}-أنظر : د/ هشام رستم ، ص ١٥٩، د. محمد سامي الشواء، ص ١٩٦، أ. محمد أمين الرومي، ص

٢- في ألمانيا الديمقراطية (سابقاً) ، قام مبرمج بزرع البرنامج الذي يحول القنبلة الزمنية في النظام المعلوماتي الخاص بالشركة التي يعمل بها، وتم برمجة القنبلة- بالتالي- بحيث يتعين أن تنفجر بعد عامين من فصله من الشركة، وفي حوالى الساعة الثالثة مساءً، وكما سجل هذا الجاني في البرنامج الخاص بتلك القنبلة ، فإن الاستفهام الخاص بيوم وساعة وسنة التنفيذ ظل مستمراً وكان هذا الشخص متأكداً من أن لحظة التدمير ستراعى بكل دقة، وبسبب ظرف طارئ أدى إلى أنهيار النظام- "لحظة تفجير القنبلة الموقوتة" - فإن أكثر من ٣٠٠ طرفية ظلت لا تعمل لبضعة ايام، وكان من الصعب اكتشاف الفاعل نظراً للتفاوت في الزمن بين لحظة ارتكاب الفعل ولحظة النتيجة الاجرامية^(٦٨).

^{٦٨}-أنظر : د/ محمد سامى الشوا، ص ١٩٥-١٩٦، أ. محمد أمين الرومى، ص ٥٧.

ثالثا: استخدام برامج الدودة Worm Software:

تعرف برامج الدودة بأنها " تلك البرامج التي تستغل اية فجوات في نظم تشغيل الحاسب الآلي، لتنتقل من حاسب الى آخر مغطية شبكة باكملها، لتحديث فى النهاية أثارها التخريبية"، وقد تنتقل تلك البرامج من شبكة إلى أخرى عبر الوصلات Links التي ترتبط بينها، واثناء عملية انتقالها تتكاثر - كالبكتريا- بانتاج نسخ منها، ومن اهم اهداف تلك البرامج شغل اكبر مجال ممكن من سعة الشبكة، وبالتالي تقليل أو خفض كفاءتها، وقد تتعدى اهدافها ذلك لتبدأ بعد التكاثر والانتشار فى التخريب الفعلى للملفات والبرامج ونظم التشغيل وبروتوكولات الإتصال^(٦٩).

امثلة للاثلاف المعلوماتى عن طريق اسخدام برامج الدودة:

١- من أمثلة برامج الدودة التي ذاع صيتها بعد استخدامها ، برنامج اعده طالب بجامعة Clausthal- Zellerfeld بالمانيا الغربية (سابقا) لارسال تهنئة وتحية من خلال الحاسبات بمناسبة عيد الميلاد فى ديسمبر ١٩٨٧، وقد صمم هذا البرنامج بحيث يقرأ عناوين البريد الالكترونى المخزنة فى ذاكرة كل حاسب يصل اليه، ويرسل بعد ذلك تهنئة إلى اصحاب تلك العناوين، ثم ينتج نسخة من نفسه ويرسلها إلى كل الحاسبات المتصلة بالحاسب المضيف.. وهكذا دواليك، وكانت النتيجة أن استمر هذا البرنامج - بعد دخوله شبكة VNET التابعة لشركة IBM والتي تربط بين حاسبات فى ٤٥ دولة- فى التكاثر التسلسلى، إلى أن غطى فى غضون ساعتين اكثر من نصف مليون حاسب، مما ادى إلى انهيار قدرة الشبكة على تحمل تدفق الخدمات المرسله، وتعطلها لمدة يومين تقريبا تم خلالها استتصال البرنامج من النظام^(٧٠).

٢- من امثلة برامج الدودة أيضا ما يعرف بـ "Internet Worm" والذي عن طريقة تمكن طالب امريكى يدعى " روبرت موريس " - وكان طالب دراسات عليا فى جامعة كورنيل بولاية نيويورك- من تدمير ١٦ الف شبكة حاسب آلى منتشرة فى ارجاء الولايات المتحدة الامريكية ، وترتب على ذلك الهجوم أن حدثت خسائر فادحة، تمثلت فى تأخير الابحاث لآلاف الساعات، وفى اعادة البرمجة بتكاليف

^{٦٩}-أنظر : د/ هشام محمد فريد رستم ، ص ١٦١ .

^{٧٠}-أنظر : د/ هشام محمد فريد رستم ، ص ١٦١ .

بلغت عدة ملايين من الدولارات^(٧١).

٣- تم اكتشاف حالة من برامج الدودة اطلق عليها مصطلح " البرامج الدودية ضد القتلة مستخدمى الذرة" ويرمز اليها برمز "WANK" حيث غزت تلك البرامج مرتين خلال عام ١٩٨٩ شبكة علوم الارض والفضاء بالولايات المتحدة الامريكية، كنوع من أنواع الاحتجاج على اطلاق مكوك فضاء يحمل مجسما فضائياً مغطى ببودرة نووية^(٧٢)

رابعاً: استخدام فيروسات الحاسب الآلى *Programms virus* التعريف بفيروسات الحاسب الآلى

تعددت تعريفات الفيروسات التى تصيب الحاسبات الآلية ومكوناتها المنطقية وتؤدى إلى اتلافها وتدميرها لدى المتخصصين فى جرائم المعلوماتية^(٧٣)، فمنهم من عرفها بانها " مجموعة من التعليمات المرمزة"

^{٧١}- اطلق البعض على هذا البرنامج اسم "Inter net" (نسبة إلى الشبكة التى اصابها بالعطب) واسماء اخرون " دودة موريس Morist Worm" (نسبة إلى معد روبرت ت. موريس الذى كان يبلغ من العمر ٢٣ عاماً) وقد ادخل هذا البرنامج إلى شبكة انترنت مساء يوم ٣ نوفمبر ١٩٨٨، من خلال احدى وسائل التدقيق *adebug feature* فى حزمة البرامج الخاصة بالبريد الالكترونى، حيث بحث دخوله عن طريق "= باب خفى" من خلال كلمة سر بسيطة ليصل النظم الاخرى المرتبطة بالشبكة، وفى مدة لا تتجاوز الاربع والعشرين ساعة كان هذا البرنامج قد انتشر عبر تلك الشبكة وغطى اطارها كليا، وقد تآثرت به ثلاث شبكات كبرى مرتبطة، شبكة انترنت، وهى (شبكات اربانت ARPA NET، وشبكة هيئة مشروعات الابحاث المتقدمة الولايات المتحدة الامريكية وتعرف باحرفها الاولى، وترتبط تلك الشبكة حاسبات مدنية، باخرى عسكرية، وميلنت MIL Net وهى الشبكة العسكرية Military Network، وهى تتبع وزارة الدفاع الامريكية، وتستخدم فى الاتصالات العسكرية التى لا تنسم بدرجة عالية من السرية، وتعرف وفقا لاحرفها الاولى " وشبكة أن. أس إف نت NSF Net وهى شبكة مؤسسة العلوم القومية الامريكية وترتبط بين الجامعات ومعاهد الابحاث ومصادر علمية كثيرة، وتعرف ايضا بأحرفها الأولى، كما تآثر به اكثر من ستة الاف حاسب آلى فى ارجاء الولايات المتحدة الامريكية المختلفة، قام هذا البرنامج بملء ذاكراتها حتى لم يعد بمقدورها القيام باى عمل.

د. هشام محمد فريد رستم، ص ١٦٣، د. محمد سامى الشوا، ص ١٩٤، أ. محمد أمين الرومى، ص ٥٨.

^{٧٢}- د. محمد سامى الشوا، ص ١٩٤، أ. محمد أمين الرومى، ص ٥٨.

^{٧٣}- يرجع الفضل فى وضع اول تصور لفيروس معلوماتى إلى الدكتور "فريد كوهن" فى الحلقة

(المكودة) ، تنتج لنفسها نسخا مطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات ومكونات النظام المنفذ لتقوم فى مرحلة معينة بالتحكم فى اداء النظام الذى اصابته^(٧٤)، ومنهم من عرفها بانها " مجموعة من التعليمات التى تتكاثر بمعدل سريع جدا لدرجة تصيب النظام المعلوماتى بالشلل التام" أو هى " خلايا كهرومغناطيسية نائمة ومبرمجة بحيث تنشط فى وقت محدد لتخريب البرنامج الاصلى، وتنتشر فى الاجهزة الاخرى التى تضمها الشبكة بحيث تفسد ما تحوية من معلومات"^(٧٥)، ومنهم من عرف الفيروس أيضا بانه " برنامج حاسب مثل اى برنامج تطبيقي آخر، ولكن يتم تصميمه بواسطة احد المخربين بهدف محدد، وهو احداث اكبر ضرر ممكن بنظام الحاسب ، ولتنفيذ ذلك يتم اعطاؤه القدرة على ربط نفسه بالبرامج الاخرى، وكذلك اعادة انشاء نفسه حتى يبدو وكأنه يتكاثر ويتوالد ذاتيا، وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة ، وكذلك بين مواقع مختلفة فى الذاكرة حتى يحقق اهدافه التدميرية"^(٧٦) ، كما عرفه المركز القومى للحاسب الآلى بالولايات المتحدة الامريكية فى تقرير أعده حول الإعتبارات الامنية فى الحاسبات الشخصية بانه " برامج مهاجمة تصيب أنظمة الحاسبات بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التى تصيب الانسان، وهو فى العادة برنامج صغير مكتوب بلغة متدنية المستوى مثل "لغة التجميع" مما يزيد من صعوبة اكتشافه، ويقوم بالتجول فى الحاسب الآلى باحثا عن برنامج غير مصاب، وعندما يجد واحداً ينتج نسخة من نفسه لتدخل فيه، وتتم عملية الادخال هذه فى جزء من الثانية، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ اوامر الفيروس^(٧٧).

الدراسية الاسبوعية التى القاها بجامعة جنوب كاليفورنيا بالولايات المتحدة الامريكية عن امنية الحاسب الآلى - وذلك فى نوفمبر ١٩٨٣ ، حيث قام دكتور كوهن بتعريف الفيروس على أنه "برنامج يصيب البرامج الاخرى حيث يعدل فيها عن طريق ادخال نسخة منه فيها يقوم بانتاجها ، ولديه القدرة على تطوير نفسه خلال عملية اعادة انتاج نفسه، ويمكنه الانتشار فى النظام أو الشبكة ليسبب فى البرنامج والبيانات تغييرات تحكيمية".

د. هشام محمد فريد رستم ، ص ١٦٤، هامش (١).

^{٧٤}- أنظر : د/ هشام محمد فريد رستم ، ص ١٦٣.

^{٧٥}- أنظر : د/ محمد سامى الشواء، ص ١٨٩.

^{٧٦}- أنظر : أ/ محمد أمين الرومى، ص ٢٦.

^{٧٧}- الفيروس - سواء كان حيويًا أم إلكترونيًا- يمثل بشكل أساسي- كما يقول " فيليب المردي وت" -

خللا فى المعلومات، فالفيروس الحيوى عبارة عن نبذ صغير جدا من الشفرة الوراثية التى تستطيع ان تسيطر على آليه الخلية الحية وان تخدعها بحيث تقوم تلك الخلية نفسها بصنع آلاف النسخ المماثلة من الفيروس الأسمى، وعلى نفس النحو، يحمل فيروس الحاسب ضمن تعليماته الوصفة اللازمة لصنع نماذج مطابقة له، وعندما يصاب حاسب ما بفيروس نمطى، فان هذا الاخير يسيطر على نظام تشغيل القرص، وبعدئذ، ومع كل اتصال للحاسب المصاب مع جزء غير مصاب من البرنامج، فان نسخة جديدة من الفيروس تنتقل إلى هذا البرنامج الجديد، وبهذا الشكل تنتشر العدوى من حاسب إلى اخر بواسطة مستخدمى الحاسبات أنفسهم الذين يتبادلون الاقراص فيما بينهم، أو الذين يرسلون البرامج إلى بعضهم البعض عبر خطوط التليفون من خلال الشبكة العالمية للإتصالات والمعلومات (انترنت) .

د. هشام محمد فريد رستم ، هامش (١) ص ١٦٤ .

خصائص فيروسات الحاسب الآلي

تتمتع فيروسات الحاسب الآلي بقدرة عالية جدا على مهاجمة أجهزة الحاسبات الآلية والشبكة العامة والخاصة، وتسفر تلك المهاجمة عن تدمير للبرامج والبيانات والمعلومات المخزنة آليا، وتعويق للاتصالات، وتشوية للبيانات والمعلومات، بل وفي احيان كثيرة فانها تضلل المستخدم ببيانات خاطئة، وتتسلل تلك الفيروسات إلى الحاسبات الآلية التي ضمت عند اتصالها باحدى الشبكات الملوثة بها، أو عند نقل برنامج مصاب لذاكرة الحاسب الآلي، حيث لا تلبث أن تتكاثر خفية ودون دراية من المستخدم أو من نظام تشغيل الحاسب، وتقوم بعملها بسرعة وحذر في أول الأمر، وما تلبث أن تتمكن من حاسب الضحية حتى تحدث آثارها التدميرية وتصيبه بالشلل التام^(٧٨).

ولعل أهم ما يميز فيروسات الحاسب الآلي عن غيرها من البرامج التخريبية الاخرى هو انتاجها نسخا من نفسها، وقدرتها اثناء عملية الانتاج الذاتى على التغير والتطور والتكيف مع البرامج المتنوعة (وإن كان بإمكانها أن تحدث طفرة) وتمتعها إلى حد ما بقدر من الذاتية، وامكانية تسببها فى احداث كافة انواع الآثار الضارة لنظام الحاسب الآلي " بدءا من مجرد عرض عبارات أو رسوم على الشاشة، مروراً بتغيير البيانات والمعلومات أو محوها، وانتهاء بتدمير النظام بأكمله" والخطر الاساسى للفيروس المعلوماتى يكمن فى امكانية استجماعه سائر مقومات التخريب الموزعة على ما عداه من برامج مخربة، اضافة إلى ذلك سرعة انتشاره، وتغير شكل ومضمون النسخ التى ينتجها من نفسه حتى تتكيف مع المحيط الذى تستقر فيه، وامكانية استخدامه فى احداث تغيير لوغارتمى للبيانات أو محوها أو تدمير نظام الحاسب بأكمله كما سبق منذ قليل^(٧٩).

وعموما ، فانه يمكن اجمال خصائص فيروسات الحاسب الآلي فيما يلى:

١- القدرة الفائقة على الاختفاء : فالفيروس ما هو الا برنامج له القدرة على اخفاء نفسه عن الضحية مستخدم جهاز الحاسب الآلي ، ويستخدم فى اخفاء نفسه وسائل متعددة، منها - على سبيل المثال- ارتباطه بالبرامج شائعة الاستخدام، حيث أن كل مستخدم للحاسب الآلي يهتم بتوفير اكبر قدر ممكن من

^{٧٨}- أنظر : د / محمد سامى الشوا، ص ١٨٩- ص ١٩٠.

^{٧٩}- أنظر : د / هشام محمد فريد رستم ، ص ١٦٥.

البرامج التي تمكنه من الاستفادة بخصائص حاسبة الشخصي، واغلب المستخدمين يقومون بنسخ هذه البرامج دون السؤال عن مصدرها أو كنهها، وعند تشغيلها ينتقل الفيروس إلى القرص الصلب ويقوم بإداء أعماله التخريبية، بل أن هناك من الفيروسات ما يدخل إلى الحاسب الآلي كملفات متخفية، بحيث لا يستطيع المستخدم في اغلب الاحيان ملاحظة وجودها على شاشات الحاسبات الآلية عن طريق فهرس الملفات، وبعض الفيروسات تقوم بالاستقرار في اماكن معينة يصعب على المستخدم ملاحظتها " مثل الذاكرة" وتنتظر في هذا المكان حتى تشير الساعة إلى تاريخ معين فتقوم بتشغيل نفسها وتنفيذ اعمالها التدميرية، كما أن بعض الفيروسات تقوم باخفاء اي اثر يدل على وجودها، حيث تظل البرامج المحتوية عليها تعمل بكفاءة دون اخطاء ولمدد طويلة، وفي ذات الوقت يقوم الفيروس بالانتقال من برنامج إلى اخر بخفة وروية.

٢- الانتشار: لفيروس الحاسب الآلي قدرة فائقة على الانتشار- كما سبق القول- تفوق قدرة الفيروس الحيوى أو البيولوجي، فعلى سبيل المثال، فإنه يمكن لفيروس حاسب آلي أن ينتقل إلى الملايين من اجهزة الحاسبات الآلية الخاصة بالمتسخدمين الضحايا في نفس الوقت، كما يمكن في ثوان معدودة أن ينتقل من قارة إلى اخرى.

٣- القدرة على الاختراق: تتمتع فيروسات الحاسبات الآلية أيضا بقدرة فائقة على اختراق نظام البيانات والمعلومات بالحاسب الآلي وكذلك الموانع التي يقيمها المستخدم.

٤- القدرة على التدمير: عندما يدخل فيروس الحاسب الآلي إلى جهاز الحاسب الخاص بالضحية، فإنه يظل ساكنا حتى تبدأ لحظة الصفر التي يبدأ عندها في النشاط والحركة، وساعة الصفر هذه اما أن تكون كلمة معينة يكتبها مستخدم الحاسب الآلي أو الجاني المعلوماتي، أو اشارة معينة أو عند تاريخ معين في السنة، ويعمل الفيروس غالبا على مسح البيانات والمعلومات المخزنة في ذاكرة الحاسب الآلي أو على تدمير نظام الحاسب بأكمله^(٨٠).

الاضرار الناشئة عن استخدام فيروسات الحاسب الآلي:

لفيروسات الحاسبات الآلية اثار وخيمة يصعب حصرها والاحاطة بها وإدراكها، وسوف نورد فيما يلي بعض الاضرار التي تصيب الحاسبات الآلية

^{٨٠}- أنظر: أ/ محمد أمين الرومي، ص ٢٨-٢٩ .

ومكوناتها المنطقية نتيجة استهدافها عن طريق الفيروسات المعلوماتية:

- ١- فقد الملفات المعلوماتية من الذاكرة : حيث يقوم الفيروس المعلوماتي بمسح أجزاء من الملفات المخزنة" فى حالة الاتلاف الجزئى للبرامج والبيانات المخزنة آليا" أو يقوم بمسح الملفات المخزنة فى الحاسب الآلى بأكملها " وذلك فى حالة الاتلاف الكلى لذاكرة الحاسب الآلى ونظامه.
- ٢- ملء ذاكرة الحاسب الآلى بالنفايات.
- ٣- كتابة رسالة على الشاشة وذلك فى غالبية الفيروسات الحميدة.
- ٤- ابطاء تشغيل الجهاز، بحيث يستغرق وقتاً أطول من المعتاد لتجميع البيانات ومعالجتها.
- ٥- تغيير وظائف المفاتيح من على لوحة المفاتيح، مما يؤدي إلى صعوبة استخدام الجهاز .
- ٦- إتلاف البرامج والمعلومات وتدميرها جزئياً.
- ٧- نسخ البرامج و المعلومات من مستخدم إلى مستخدم مما يشكل خطورة بالغة، حيث أن هذه البرامج و المعلومات غالباً ما تحتوى على اسرار ومعلومات ذات قيمة مالية كبيرة"^(٨١).

انواع فيروسات الحاسب الآلى:

- تتعدد انواع الفيروسات المعلوماتية التى تستخدم فى التخريب المنطقى لبرامج وبيانات الحاسب المخزنة آليا، ويقسم الفقة تلك الفيروسات من حيث تكوينها واهدافها إلى ما يلى:
- أ- فيروس عام العدوى: وهو ذلك الفيروس الذى ينتقل إلى اى برنامج و ملف معلوماتى.
 - ب- فيروس محدد العدوى: وهو ذلك الفيروس الذى يستهدف نوعاً محدداً من النظم لينتقل إليه ويهاجمه، ويتميز هذا النوع عن النوع السابق بأنه أبطأ فى الانتشار واصعب فى الاكتشاف.
 - ج- فيروس عام الهدف : وتندرج تحت هذا النوع من الفيروسات الغالبية العظمى التى تم اكتشافها حتى الآن، ويرجع ذلك إلى سهولة اعداد تلك الفيروسات،

^{٨١}-أنظر : / محمد أمين الرومى، ص ٢٩ - ٣٠.

واتساع مدى تخريبها.

د- فيروس محدد الهدف : ويحتاج إعداده إلى درجة عالية من الكفاءة والمهارة، والى دراية تامة بالتطبيق أو الهدف أو الغرض الذى يستهدفه، وقد يجرى هذا الفيروس تلاعبا ماليا أو يدخل تعديلات فى تطبيق عسكرى، وبعضه قد ينهى وجوده بعد تنفيذ هدفه، وتكمن خطورة بعض الفيروسات من هذا النوع فى انها لا تؤدي إلى تعطيل عمل البرنامج، بل تبدل فحسب من هدفها^{٨٢}.

^{٨٢}-أنظر : د/ هشام محمد فريد رستم ، ص ١٦٦، د. محمد سامى الشوا، ص ١٩١.

المبحث الثاني

الجرائم التي ترتكب بواسطة الحاسب الآلي ومكوناته

نتناول هذا المبحث من خلال تسعة مطالب على النحو التالي:

المطلب الأول: الاحتيال المعلوماتي

المطلب الثاني: التزوير المعلوماتي

المطلب الثالث: النصب المعلوماتي

المطلب الرابع: جرائم الاعتداء على حرية الحياة الخاصة

المطلب الخامس: جرائم الاعتداء على حقوق الملكية الفكرية والادبية.

المطلب السادس: جرائم إفشاء الاسرار فى اطار المعلوماتية

المطلب السابع: جرائم السب والقذف عبر الإنترنت.

المطلب الثامن: الجرائم المخلة بالآداب العامة فى اطار المعلوماتية

المطلب التاسع: غسيل الأموال عبر الإنترنت

المطلب الأول

الاحتيال المعلوماتي

ينصرف اصطلاح الاحتيال بوجه عام إلى الغش والخداع الذى يعمد إليه أى شخص للحصول من الغير بدون وجه حق على فائدة أو منفعة أو ميزة ما، ويقصد بالاحتيال المعلوماتي إساءة استخدام الحاسبات الآلية والتلاعب فى نظم المعالجة الإلكترونية للبيانات والمعلومات للحصول بغير حق على اموال أو اصول أو خدمات.

ويتميز الاحتيال المعلوماتي عن غيره من انماط الاحتيال التقليدى أو العادى بالتعقيد الناجم عن استخدام المفاتيح والشفرات والدلائل الإلكترونية فى ارتكابه، ونظرة الكثيرين إليه باعتباره نوعا من التحدى الذهنى الذى يثير الرغبة فى اتيانه، وامكانية اقترافه عن بعد، وعدم تركه آثار مادية تدل على وقوعه بالاضافة إلى فداحة خسائره وسهولة طمسه واخفائه.

ولعل الهدف الرئيسى للتلاعب الذى يتحقق به الاحتيال المعلوماتي فى

قطاع المعلومات هو البيانات التي تمثل في نظم معلومات الحاسبات الإلكترونية أموالاً أو أصولاً وموجودات، وأكثر البيانات استهدافاً لهذا التلاعب هو المتعلق منها بالمستحقات المالية والإيداعات المصرفية وتقديرات الائتمان وحسابات ونتائج الميزانيات، وأكثر ما يرد عليه هذا التلاعب - وفقاً لما تم الكشف عنه من حالات الاحتيال والغش المعلوماتي- هو حسابات المرتبات والمعاشات وأوامر الدفع وحسابات التكلفة والنفقات، بالإضافة إلى قوائم المبيعات وكشوف الإعانات الاجتماعية، والحسابات المعدة بواسطة الحاسبات الآلية لميزانيات البنوك والشركات وقطاعات الأعمال.. وغيرها، أما أكثر صور الاحتيال المعلوماتي اضراً وخطراً على الأنشطة الاقتصادية والاقتصاد القومي ككل، فتتمثل فيما يقع منه على أنظمة التحويل الإلكتروني للأموال والودائع المصرفية أو ما يسمى " بالأموال الإلكترونية أو الافتراضية" نظراً لضخامة حجم ما يتم تداوله عبر هذه الأنظمة من أموال، واختزالها- أي تلك الأنظمة- كذلك المسافات بما يتيح تنفيذ الاحتيال عبر الحدود الإقليمية للعديد من الدول، واختزالها أيضاً الزمن اللازم لاتمام التعاملات والتحويلات المالية، وكذا الزمن اللازم لسلب الأموال بالاحتيال والغش إلى ثوان معدودة، وهو ما انعكس من جهة في صيروره الأموال المتداولة عبر هذه الأنظمة هدفاً من أهداف الجريمة المنظمة والقوى الخارجية المعادية، وفي فداحة الخسائر الناجمة عن عمليات الاحتيال الواقعة في محيط هذه الأنظمة من جهة أخرى.

ومن المتوقع تفاقم خطر هذه الصور من الاحتيال المعلوماتي في المستقبل أكثر مما هي عليه الآن، نظراً لاطراد الاعتماد على الأنظمة الإلكترونية في تحويل ونقل الاعتمادات والأموال والودائع، وتسارع وتيرة تحول المجتمع إلى مجتمع لا يتداول النقود ولا الشيكات^(٨٣).

وتتعدد الأساليب التي ترتكب بها أفعال الاحتيال والغش المعلوماتي، ويجمعها كلها رباط يتمثل في التعدي على البرامج والمعلومات المخزنة آلياً، والتلاعب فيها للحصول بغير حق على أموال أو أصول أو خدمات، وتحقيق العديد من الأغراض الإجرامية الأخرى، وتفصيل ذلك فيما يلي:

التعدي على المعلومات والبرامج بغية تحقيق أغراض غير مشروعة:

تتحقق تلك الجرائم بواسطة العديد من الأفعال الإجرامية، التي تمثل

^{٨٣}- أنظر: د/ هشام محمد فريد رستم، ص ٤٥ - ٤٩.

السمة العالية لأفعال تعدى المحتالين والتي تتجسد في صورة المعالجة غير المشروعة- سواء للمعلومات والبيانات المخزنة آليا أو للبرامج ذاتها - بغرض تحقيق العديد من الاهداف الاجرامية غير المشروعة.

اولا: التعدى على المعلومات والبيانات المخزنة آليا:

يعد التلاعب فى المعلومات والبيانات المعالجة إلكترونيا - وفقا لاراء الخبراء والمتخصصين فى مجال الحاسبات الآلية- من اكثر افعال الغش ارتكاباً فى دول العالم المختلفة، وعلى وجه الخصوص فى اوروبا والولايات المتحدة الامريكية، ويتم ذلك التلاعب اما عن طريق ادخال معلومات مصطنعة أو اتلاف المعلومات الموجودة بالفعل فى الحاسب الآلى.

١- ادخال معلومات مصطنعة:

وترتكب تلك الجرائم المعلوماتية فى اغلب صورها عن طريق المسئول عن القسم المعلوماتى، والذي يسند إليه على وجه الخصوص وظيفة المحاسبة والمعاملات المالية، حيث يعتبر فى افضل وضع يؤهله لارتكاب هذا النمط من التلاعب غير المشروع، ويبدو أن الغش فى الدفع هو الاكثر تكراراً والاكثر سهولة أيضا فى تنفيذ تلك الجرائم، لاسيما فى وسط منشأة تملك قدراً كبيراً من النقود، وتحقق تلك الصورة من جرائم المعلوماتية عن طريق عدة اشكال تجلت فى الواقع العملى الملموس، نذكر منها:

أ- ضم مستخدمين غير موجودين فى الواقع:

وينطبق ذلك على وجه الخصوص بالنسبة لمنشأة تضم العديد من الفروع، والتي يتغير عدد مستخدميها وفقا للظروف الاقتصادية وقائمة الطلبات، حيث يقدم مدير احد هذه الفروع معلومات وهمية إلى الادارة المركزية تتعلق باستئجار مستخدمين مؤقتين، وكفى بالنسبة له- وفى نهاية كل تعد - أن يستلم الشيكات النقدية الخاصة بالمستخدمين المؤقتين: المزعومين، وقد وقعت شركة ASSE- DIC على سبيل المثال- ضحية لمثل هذا النمط من الافعال الاجرامية غير المشروعة.

ب- الابقاء على مستخدمين تركوا الوظيفة بالفعل:

ويتلخص هذا النمط من افعال الغش المعلوماتى، فى أن المبرمج المسئول عن الادارة المعلوماتية بدالمن أن يحفظ ملفات الاشخاص الذين تركوا العمل بالمنشأة، فانه يبقى هذه الملفات على قيد الحياة، ويجعلها تدر دخلا لصالحه مع نهاية كل شهر.

ج- اختلاس النقود:

يرى الخبراء أن بإمكان أي شخص يشغل مركزا على قدر من الأهمية في إحدى المنشآت أو الإدارات أو المؤسسات أو البنوك، ولديه الكفاءة والخبرة الفنية اللازمة لاستخدام الحاسب الآلي، أن يعترف من هذا الأخير ما يشاء من معلومات يرغب فيها، بغية اختلاس العديد من المبالغ المالية والحاسبات الضخمة في النهاية، منتهزا ضعف مراقبة الحاسب الآلي لمدى مشروعية هذا العمل وعدم قدرته على ذلك في أغلب الأحيان:

ومن الأمثلة على ذلك نذكر:

١- قيام شرطه مرسيليا الفرنسية بالقبض على مستخدم يعمل لدى فرع مصرف تابع لبنك Indo-Suez، تمكن من عمل تحويلات لنقود وهمية مستخدما في ذلك الحاسب الآلي الخاص بذلك البنك، وتلك المبالغ - ولو انها لم ترد في الخزينة الخاصة بالبنك - الا انها قد سجلت في ذاكرة الحاسب الآلي قبل أن تنتقل بواسطة محررات مصطنعة إلى حساب فتح باسمه في سويسرا، وقد وجهت الأجهزة الامنية لهذا الشخص تهمة اختلاس سبعة ملايين فرنك فرنسي.

٢- في فبراير من عام ١٩٨١ تم كشف قضية شهيرة جدا في اسرائيل، تتلخص وقائعها في أن شخصا يدعى Vladimir Loriblitt وهو مهاجر روسي عمل مبرجما في وزارة المالية، وكان مولعا باصطناع الشركات الوهمية، قام بادخال فواتير وهمية لا حصر لها في الحاسب الآلي، وقد سمح له ذلك أن يحول إلى تلك الشركات الوهمية العديد من الشيكات والمبالغ النقدية المسددة من T.V.A.

٢- اتلاف المعلومات الموجودة بالفعل في الحاسب الآلي :

يمكن للمسئولين عن تخزين المعلومات وحفظها- وبمنتهى السهولة أن يغيروا ويتلفوا المعلومات المكلفين بحفظها داخل جهاز الحاسب الآلي، ومن الأمور السهلة في الواقع والتي تجسد تلك الأفعال الإجرامية استبدال رقم حساب بأخر، أو احلال بطاقة محل أخرى، وهذا النوع من الجرائم على قدر كبير من الخطورة، لانه في حالة نجاح التزوير، فانه يمكن لهذه الجرائم أن تستمر لفترة من الزمن حتى يتم كشف الفعل غير المشروع.

ومن الأمثلة على ذلك نذكر:-

أ- استطاعت مجموعة من المستخدمين الإداريين خلال سنوات عديدة أن يضاعفوا من روايتهم عن طريق استخدام الحاسبات الآلية، حتى لحظة الكشف عن تلك الأفعال الإجرامية بمحض الصدفة.

ب- قام بعض المستخدمين الإداريين أيضا بتقاضى ساعات إضافية لم يتم تنفيذها على الإطلاق عن طريق استبدال قوائم الحاسبات بساعات عمل.

ج- امكن تقديم احد مرتكبي جرائم التزوير فى المعلومات للمحاكمة فى المانيا الشرقية (سابقا) ، حيث قام مستخدم بمكتب القوى العاملة- كان مكلفا بتوزيع الاعانات العائلية – بتحويل مبلغ وقدره ٥٠٠ الف مارك المانى لحسابه الخاص فى شكل مرتبات، وقد نفذ ذلك عن طريق ازالة الرقم الاول لتلك المبالغ المحولة من المنفذ الخاص بمراقبة الحاسب الآلى ، وقد حكم عليه بالسجن لمدة ثلاث سنوات.

ج- لجأ بعض مرتكبي افعال الغش المعلوماتى الاكثر مهارة واحترافا الى الهجوم المباشر على المعلومات المحمولة بواسطة شبكات الإتصالات البعيدة، وهم شديدي الولع بالتقاط اذونات التحويل عن طريق وسائل الكترونية مصطنعة وتزويدها بالامر بدفع نفس المبلغ ولكن لحساب آخر.

ويتم اتلاف المعلومات أو تعديلها فى افعال الغش والتزوير المعلوماتى

بوسائل متعددة ، نذكر منها:

أ- ممارسة Bluff : وتتجسد تلك الممارسة فى استخدام الحاسبات الإلكترونية من اجل طبع فواتير مصطنعة أو فواتير ذات قيمة كبيرة، ويقوم العملاء بتسديدها منخدعين فى الثقة التامة التى يتوسمونها فى تلك الحاسبات، والقليل من هؤلاء العملاء الذين يبدون اعتراضهم يتلقون خطابا تفسيريا مذيلا بصيغة صارت تقليدية ومألوفة وهى: (تقبلوا عذرا، فقد اخطا حاسبنا الالى) وهكذا يستخدم الحاسب الآلى المتهم بسوء الادارة ككبش فداء ووسيلة سهلة لارتكاب تلك الأعمال غير المشروعة.

ب- التلاعب فى الاشرطة الممغنطة: اخفقت عملية نصب قدرت بحوالى ٢١ مليون فرنك فرنسى بسبب خطأ لمعلوماتى مبتدئ وتتلخص وقائع تلك القضية فى انه بتاريخ ٢٩ فبراير ١٩٨١ وصل إلى أحد فروع الشركة العامة شريط ممغنط قادم من شركة Isover st gobain ، وقد احتوى هذا الشريط على ١٣٩ اذنا بالدفع، وعند معالجته بالقسم المعلوماتى للبنك تم رفضه بواسطة الحاسب الآلى نظرا لوجود عيب جسيم يتعلق بطول تسجيل هذا الشريط، وقد القى القبض على مرتكب هذه المحاولة الاحتيالية، وكان بالامكان – وفقا لراى الخبراء – أن يكتب لتلك المحاولة النجاح فى حالة المعرفة التقنية اللازمة فى المجال المعلوماتى لدى هذا المزيف .

ج- محو المعلومات: تمكن شخصان من اختلاس ٦١ الف دولار، وهي عبارة عن مبالغ مدفوعة مرسله من شركات التأمين إلى احد المراكز الجامعية، ولكي يؤدي كل من هذين المحتالين عملهما الآثم على خير وجه، فقد قاما بمحو كل الحسابات القائمة في تسجيلات الحاسب الآلي الخاص بذلك المركز الجامعي وجعلها غير قابلة للتحويل.

وبالامكان أيضا أن تكون البيانات والمعلومات المعالجة آليا ليست فقط محلا للمحو الانتقائي، وإنما أيضا للالغاء بلا قيد أو شرط، وهكذا ، فقد تم الكشف في مدينة دالاس الامريكية عن اربعة من مستخدمي بلديتها، كانوا قد استبعدوا ٢٧١ مخالفة من سجلات المدينة مقابل تقاضي نسبة مئوية محددة بلغ مجموعها حوالي ١٦٣٠٠ دولار امريكي.

د- التلاعب في المعلومات من بعد: يمكن أن تنفذ تلك الجرائم، في حين يوجد مرتكبها على بعد عدة كيلومترات من مكان الاقتراف النهائي لها وتحقق نتيجتها الاجرامية، ويستطيع مرتكب فعل الغش المعلوماتي، هذا اذا ما تزود - على سبيل المثال- بكلمة السر أو مفتاح الشفرة أن يغير من ايه مسافة محتوى ومضمون ذكريات الحاسبات الآلية وما يوجد عليها من بيانات أو معلومات، أو أن يستبدل ارقام حسابات غيرها، ومن الامثلة على ذلك، أن طالبا امريكي تدخل تدخلًا غير مشروع في احد النظم المعلوماتية ، واصبح مالكا له لفترة من الزمن، بعد أن قام بتغيير مفتاح الشفرة الخاص به، وترتب على ذلك أن رفض هذا النظام امداد اصحابه ومستخدميه الشرعيين بالخدمات المعلوماتية لبضعة ساعات^(٨٤).

ثانيا: التعدي على برامج التطبيق ونظم التشغيل:

يستلزم هذا النمط من الجرائم- وهو من جرائم المتخصصين والمحترفين - معرفة فنية دقيقة وعميقة في مجال برمجة الحاسبات الآلية، وتنفيذه - وان كان من الصعوبة بمكان - الا انه يمكن أن يتحقق في مراحل مختلفة من صنع برامج التشغيل أو التطبيق أو في لحظة صيانتها أو تحديثها .

١- تعديل نظم أو برامج التطبيق:

يمثل هذا النوع من التعديل نسبة لا يستهان بها من افعال الغش والاحتيال المعلوماتي، واختلاس النقود في معظم هذه الافعال كان هو الهدف والغرض المبتغى.

^{٨٤}-أنظر : د/ محمد سامي الشوا ، ص٧١-٧٧.

ومن الامثلة على هذا التعديل والتي توضح مدى خطورة هذا النمط من الاجرام المعلوماتي نذكر:

أ- قيام مبرمج كان يعمل باحد البنوك بتعديل برنامج إدارة الحسابات في هذا البنك، بحيث يضيف بموجب هذا التعديل ١٠ سنوات لمصاريف إدارة الحسابات على كل عشرة دولارات، ودولار واحد على الحسابات التي تتعدى عشرة دولارات، وقد تم قيد المصاريف الزائدة في حساب خاص فتحة باسم مستعار، وهكذا فقد حصل هذا الجاني المختلس على عدة مئات من الدولارات كل شهر، وكان بالامكان أن يستمر هذا العمل الاجرامي لولا أن البنك الذي كان يعمل به اراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول واخر عميل له وفقا للترتيب الابددي، وحينئذ اكتشف البنك عدم وجود هذا الاسم المستعار.

ب- اعد أحد المختلسين ويدعى Royce برنامجا لادارة المعلوماتية، بحيث يسمح هذا البرنامج بادارة صحيحة لحسابات المنشأة، والتي تتضخم في فترات زمنية ببعض النفقات ثم يقوم باستقطاع مبلغ زهيد من الايرادات كل شهر، وقد استطاع Royce أن يحقق فائدة على قدر كبير من الاهمية من خلال هذه الكسور المحسوبة بدقة والتي بلغ مقدارها حداً كبيراً، وتمكن في خلال ست سنوات من اختلاس مبلغ وقدره مليون دولار.

٢- تعديل نظم التشغيل:

يسمح نظام أو برنامج التشغيل - كما سبق القول - بتنظيم وضبط وتزامن توالى التعليمات والوظائف الخاصة بالحاسب الآلي، وهناك اشكال متعددة لتعديل برامج التشغيل من اجل الحصول على مزايا غير مشروعه وتحقيق العديد من الاهداف الاجرامية، لعل اهمها:

أ- التعديل عن طريق المداخل المميزة:

يمكن أن يحتوى اى برنامج للتشغيل فى نسخته الاولى على اخطاء وعيوب منطقية، وقد لا يكتشف البعض منها الا عند استخدامه، ويمكن للمبرمجين عن طريق المداخل المميزة لتلك البرامج - والتي هى فى حقيقتها عبارة عن ممرات خالية متروكة فى البرنامج - احداث تعديلات فى شفرة هذا البرنامج والمنافذ الوسطية، وتستبعد بالطبع هذه المنافذ عند التصحيح النهائى لبرنامج التشغيل، وقد يصل الامر ببعض المبرمجين من ذوى النوايا السيئة والاعراض غير المشروعه- والذين لهم دراية باهمية السلاح التقنى الموجود بين

أيديهم- أن يتغاضوا عن استبعاد هذه المداخل المميزة ولا يبنهوا إليها أي شخص، ونظرا لكونهم هم المؤتمنين فقط على هذا السر، فانه يمكنهم في لحظة معينة أن يستخدموا تقنية معلوماتية تتخذ من برامج التشغيل هدفا لها ويطلق عليها اصطلاح "Trappe" أي المصيدة ووفقا لهواهم، ويستمررون تبعا لذلك في استغلال برنامج التشغيل المعيب من الناحية الفنية، وبالامكان أيضا عن طريق هذه المداخل المميزة الولوج في كل المعلومات التي تحتويها ذاكرات الحاسبات الآلية، ومن ثم التوصل إلى الشفرات والتعليمات المستهدفة.

وإجمالاً، فانه يمكن عن طريق هذه الوسيلة أن يصبح مرتكب فعل الغش هو سيد النظام المعلوماتي، مع ما يترتب على ذلك من نتائج ايجابية بالنسبة له، ونتائج سلبية مع مزيد من الخسائر الفادحة بالنسبة لصاحب أو المستخدم الاصلى للحاسب الآلي المسلوب.

ب- اصطناع برنامج:

يقصد الخبراء المعلوماتيون بلفظي " تصنيع وتشكيل " استخدام الحاسب الآلي من اجل التخطيط للجريمة ومراقبتها وتنفيذها , أي اصطناع برنامج كامل ومخصص فقط لارتكاب فعل الغش المعلوماتي، والمثال الذي يساق عادة- بمناسبة هذا النمط من الغش المعلوماتي - من قبل بعض المتخصصين، هو ذلك الخاص بشركة تأمين بولاية لوس انجلوس الامريكية، والتي اختلقت بفضل حاسبها الآلي ومعاونة مبرمجها عددا وهمياً من المؤمن عليهم بلغ حوالي ٦٤ الف وثيقة تأمين وقد تقاضت تلك الشركة من اتحاد شركات التأمين بالولايات المتحدة الامريكية عمولة نظير اجمالي تلك الوثائق (٦٤ الف وثيقة) واقتصر دورها فقط على إدارة الحسابات ، وامعانا في التضييل، وبغرض اعطاء العقود لاهمية مظهراً مشابها لتلك الحقيقية، فقد قامت الشركة المذكورة بتنشيط الملفات المختلفة عن طريق تغيير الموطن والوظيفة وبعض الاقرارات الاخرى.

المطلب الثاني

التزوير المعلوماتي

يقصد بالتزوير- وفقاً للراجح من أقوال الفقه- " كل تغيير للحقيقة مقترن

بقصد الغش يقع في محرر باحدى الطرق التى نص عليها القانون ويكون من شأنه أن يسبب ضرراً للغير^(٨٥).

وبالنظر إلى المحررات فى نطاق المعلوماتية، فإننا نلاحظ أن الاعتماد على مستخرجات الحاسب الآلى من مستندات معلوماتية تخرج من الطابعة على هيئة اوراق أو شرائط ممغنطة مسجل عليها المعلومات قد بات ضرورة ملحة فى عصرنا الحالى، فجميع الإدارات والهيئات الحكومية والمدنية والتجارية أصبحت تعتمد - كما سبق أن بينا- على تلك الآلة الالكترونية فى تسيير شئونها المختلفة، وكذلك ايضا فى المحلات التجارية والفواتير المحاسبية فى جميع المجالات^(٨٦).

ومن تحليل عناصر جريمة التزوير المادية، " فإننا نجد أن تغير الحقيقة الذى يقوم به التزوير هو فحسب الذى يقع فى محرر، لذلك لايعد تزويراً تغيير الحقيقة الذى يقع دون كتابة- بقول أو فعل- " كإدلاء شخص بأقوال كاذبة امام المحكمة، أو العبث فى العدادات الحاسبة(كعداد السيارة الاجرة وعدادات الكهرباء والغاز والمياه)، وإن جاز أن تقوم بتلك الافعال جريمة اخرى كشهادة الزور أو النصب أو الغش فى المعاملات، والمحرر فى جوهره كتابة مركبة من حروف أو علامات تعبر عن معنى أو فكرة معينة، وإمكانية القراءة البصرية للمدون به هو ما تفترضه نصوص التزوير التقليدية فى اغلب دول العالم، ويترتب على ذلك أنه لا ينطوى تحت هذه النصوص البيانات المخزنة إلكترونياً، فهذه البيانات- سواء كانت مخزنة فى ذاكرة الحاسب الآلى، ام متضمنة فى برامجة أو فى اشرطة الادخال أو الاخراج الممغنطة- ليست مقروءة ولا يمكن للمعنى الذى حمله أن ينتقل عن طريق عين الأدمى، إذ تسجل تلك البيانات على هيئة جزئيات دقيقة ومثبتة الكترومغناطيسيا على دعامة تركيبية بشكل يسمح للحاسب فقط بقراءتها ، الامر الذى يتعذر معه اعتبارها محرراً، وهذا هو ما ذهب اليه عدد غير قليل من الفقة، وتطبيقاً لذلك، لم تقر احدى محاكم الاستئناف بالولايات المتحدة (فى قضية U.Sv. Jones) حكما اصدرته محكمة المقاطعة بادانة شخص عن جريمة تزوير لقيامه بتحريف بيانات حسابات المدفوعات وادخالها فى نظام معلومات الحاسب الآلى الذى عالجها واصدر فى مخرجاته

^{٨٥}- تعريف الاستاذ جارسون السائد فى الفقة الفرنسى لجريمة تزوير المحررات والذى درج الفقة فى كل من فرنسا ومصر على استعماله والأخذ به ، د. أحمد حسام طه تمام، ص ٣٨٦- ص ٣٨٧ ، د. هشام محمد رستم، ص ٣٢٣.

^{٨٦}-أنظر : د/ أحمد حسام طه تمام، ص ٣٨٧- مرجع سابق .

خمس شيكات بمبلغ ١٣٠ ألف دولار قابلة للدفع في حساب وهمي، وفي تسببها للحكم السابق، قررت تلك المحكمة " أن ثمة فارقا بين محرر مزور ومحرر دون به ما يخالف الحقيقة دون أن يتعرض مضمونه لتحريف (محرر صحيح في تنفيذه واخراجه)، وان افعال المتهم لا تشكل اصطناعا أو عملاً لمحرر مزور، وانه إذا كان من رأى محكمة المقاطعة أن الواقعة لا يستفاد منها أن الشيكات - بما سطر عليها من بيانات تغير الحقيقة- قد صدرت من الشركة المجنى عليها إلى الحساب الوهمي، فان المحكمة الاستئنافية لا تقرها في ذلك، لأن الشيكات - بما أثبت فيها من قابلية المبلغ المعين بها للدفع لامر الشخص الوهمي- تتضمن وجود التزام على عاتق المجنى عليه لصالح المستفيد، ومع أن هذا الالتزام لم يكن له بالقطع وجود، إلا أن ما وقع من غش قد أفضى إلى اعتقاد المجنى عليه بأن على عاتقه التزام حقيقي تجاه هذا الشخص الوهمي، وهو ما تم بناء عليه إصدار صك أو مستند حقيقي أو أصلي متضمنا ما يغير الحقيقة كما لو كان قد صدر لدائن فعلى".

على أن رأيا آخر، يدافع عنه جانب من الفقه البلجيكي والمصري، يذهب إلى أن التغيير الذي يقع في برامج الحاسب الآلي أو في البيانات والمعلومات المخزنة إلكترونيا يمكن أن يتحقق به في بعض الحالات جريمة التزوير في المحررات، ويشير انصار هذا الرأي إلى أن الفقه الحديث يقبل ذلك بالنسبة للاوراق المقواة المثقبة، وان ثمة تطورا حدث بالفعل بشأن المعلومات المسجلة على الاسطوانات والاشرطة الممغنطة ينحو إلى تطبيق نص التزوير في المحررات على تحريفها، ويرى أحد الفقهاء المصريين أن البرنامج متى دون على اسطوانة أو شريط ممغنط يعتبر محرراً، وتغيير الحقيقة فيه يعد بالتالي تزويرا، ويعيب هذا الرأي- عدم اتساقه مع المفهوم المستقر عليه فقها وقضاء لمدلول المحرر، إذ يفترض هذا المفهوم أن المعنى الذي تعبر عنه الرموز أو العلامات المدونة بالمحرر ينتقل إلى الشخص بالنظر، وهو ما لا يتحقق في البرامج المعلوماتية أو البيانات المخزنة إلكترونيا، لأنها تسجل كهرومغناطيسيا على الاسطوانات أو الاشرطة الممغنطة، فلا يمكن مشاهدتها في ذاتها والتعرف عليها عن طريق النظر، كما أن من عناصر المحرر أن يدل بذاته على من ينسب اليه، هو ما لا يتحقق كذلك في برامج الحاسب الآلي.

من أجل ذلك حاول رأى ثالث التوفيق بين هذين الاتجاهين، معتبرا أن نصوص التزوير التقليدية في المحررات من الممكن أن تنطبق في حالة ظهور المعلومات والبيانات المزورة في المخرجات الورقية للحاسب الآلي، وقد تبني

هذا الاتجاه بعض الفقه في كل من بوليفيا وفرنسا ومصر، ففي فرنسا من المستقر فقها وقضاء أن الشرط الأول لقيام جريمة التزوير في المحررات هو أن تكون هناك كتابة .. ومن ثم فإن تغيير الحقيقة الذي يقع في الاشرطة الممغنطة لا تقوم به جريمة التزوير في المحررات المنصوص عليها في المادة ١٤٥ من قانون العقوبات الفرنسي وما بعدها، وذلك لانقفاء الكتابة، غير أن هذه الجريمة يمكن أن تقع في حالة إخراج الحاسب الآلي أوراقا لها قوة أو قيمة في الاثبات، كما هو الحال بالنسبة للمستند المحاسبي المزور أو الفاتورة المزورة) وفي مصر، يرى البعض من الفقه أنه (يجب أن تكون الكتابة في المحرر مركبة من حروف، وإن لم تكن من نوع الحروف المعروفة، مثل الكتابة المختزلة والشفرة السرية، وهذا ما ينطبق على البيانات الموجودة في الحاسبات الآلية على الذاكرة والمعالجة آليا، فهي عبارة عن لغة خاصة بالحاسب الآلي وموجات هرتزية، فإذا وقع اعتداء عليها بتغيير الحقيقة فإنه يكون اعتداء على البيانات وليس تزويرا، إلا إذا خرج في صورة محرر مكتوب بعد المعالجة الآلية للمعطيات الموجودة بالداخل والتي تم الاعتداء عليها^(٨٧).

وإزاء هذا الخلاف في الفقه والقضاء حول مدى جواز تطبيق النصوص التقليدية على الأفعال التي تشكل تغييرا للحقيقة في البيانات المخزنة إلكترونيا في الحاسب الآلية والى يتحقق بها الركن المادي لجريمة التزوير المعلوماتي، وإزاء ضيق نطاق تلك النصوص وعجزها- حسب الراجح في الفقه والقضاء - عن مواجهة التزوير الذي يقع في مجال المعالجة الإلكترونية للبيانات، وحماية للثقة الواجب توافرها في المستندات المعالجة إلكترونيا- سيما بعد تعاظم الاعتماد عليها في تسيير شؤون المجتمع الحديث- فقد عمد المقتن في العديد من الدول إلى ادخال هذه النوعية المستحدثة من التزوير في دائرة التجريم والعقاب بمقتضى نصوص خاصة سنها لهذا الغرض، أو بتعديلات أدخلها على بعض النصوص التقليدية للتزوير^(٨٨).

^{٨٧}-أنظر : د/ هشام رستم، ص ٣٢٦-٣٣٠. د. أحمد حسام طه تمام، ص ٣٩١.

^{٨٨}-أنظر : د/ هشام رستم، ص ٣٣١، ٣٣٢.

المطلب الثالث النصب المعلوماتي

يقصد بالنصب "الاستيلاء على حيازة مال الغير الكاملة بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال"، ويتميز النصب عن السرقة - رغم تماثلهما في الموضوع والغاية- في أن الاستيلاء على الحيازة الكاملة للمال يتم في السرقة بغير رضا حر من مالك أو حائز هذا المال ، بينما يحصل في النصب بتسليم مشوب بالاحتيال^(٨٩) عن طريق استعمال الجاني لإحدى الطرق الاحتيالية التي ينص عليها نص التجريم عادة في جريمة النصب، كما عرفة بعض الفقة بأنه "الاستيلاء بطريق الإحتيال على شئ مملوك للغير بنية تملكه" ، أو هو "الاستيلاء على منقول مملوك للغير بخداع المجنى عليه وحمله على تسليمه"^(٩٠). ومن الممكن أن يكون الحاسب الآلي احد وسائل الجاني في ارتكاب جريمة النصب، ويطلق على جريمة النصب في هذه الحالة اصطلاح " النصب المعلوماتي"، ولعل خير مثال للطرق الاحتيالية المستخدمة في النصب المعلوماتي هو التلاعب المعلوماتي، والذي يقصد به "التلاعب بالبرامج والبيانات للتغيير فيها بما يترتب عليه ايهام المجنى عليه بصحتها بما يجعله يسلم بها"^(٩١)، فجريمة النصب المعلوماتي تبدو من الواضح بمكان في الحالات التي يتوصل فيها شخص عن طريق التلاعب في منظومات المعالجة الإلكترونية للبيانات إلى الاستيلاء على مال الغير، كأن يتلاعب في البيانات المدخلة أو المخزنة داخل الحاسب أو في برامج لاستخراج شيكات تدفع له، أو لتحويل كل أو بعض ارصدة الغير أو الفوائد المستحقة لهم إلى حسابه، أو التلاعب في الاشارات الإلكترونية المرتدة من الحاسب المركزي إلى جهاز الصرف الآلي للنقود لاختلاس أموال من ارصدة العملاء أو من رصيد جهاز الصرف نفسه دون

^{٨٩}- أنظر : د/ حسن صادق المرصفاوي، قانون العقوبات الخاص، منشأة المعارف، الاسكندرية،

١٩٩١، ص ٣٩٤، د. هشام محمد فريد رستم، ص ٢٦٨

^{٩٠}- أنظر : د/ هشام محمد فريد رستم، هامش (١) ، ص ٢٦٨

^{٩١}- أنظر : د/ هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢، ص ١٣٢.

التأثير في بيانات الحاسب المركزي وفي حسابات العملاء^(٩٢)، كما يمكن أيضا استخدام الحاسب الآلي بهدف التزييف أو التزوير، وحالة الفواتير المزورة هي المثال الواضح على ذلك، وفي الواقع فإنه يوجد في هذه الحالة مستندات من مستخرجات ناتجة عن استخدام الحاسب الآلي تكون ذات طبيعة من شأنها الإيهام بوجود أموال وهيمة، وذلك بسبب اعدادها بطريقة الكترونية وحسابية من شأنها الإيحاء بوجود قوة واموال، وذلك في الحالة التي تكون عليها الوثيقة مستخرجة من الحاسب الآلي، ويرجع ذلك للثقة التي يعطيها الاشخاص للوثائق المستخرجة من الحاسبات الالية^(٩٣).

كما يمكن كذلك استخدام الحاسب الآلي في ارتكاب جرائم النصب المعلوماتي عن طريق احدى الوسائل التديسية" كاستخدام صفة غير صحيحة أو اسم كاذب" والدليل الواضح على ذلك هو استعمال الكارت الائتماني أو البطاقة البنكية الممغنطة باسم كاذب أو بصفة كاذبة^(٩٤)، " وتعتبر الجرائم المتعلقة باساءة استخدام البطاقات البنكية الممغنطة أو الكروت الائتمانية الممغنطة من الجرائم المقلقة خصوصا في المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور والحدثة، وتمنح فيها البطاقات الائتمانية وتستخدم كذلك باقل قدر ممكن من الاجراءات، ففي وقتنا الحاضر اصبح فتح الحساب البنكي أو الائتماني في اغلب دول العالم من الحقوق التي اعترف بها القضاء للناس كافة، بل أن فتح حساب بنكي اصبح من الامور الواجبة، كما في حالة لو كان الموظف أو العامل يحصل على مرتبة أو اجرة من خلال احد البنوك، وقد نتج عن ذلك أن اصبح الحصول على احدى البطاقات البنكية من الامور المرتبطة بأحقية الفرد في فتح حساب بنكي، ومنح البطاقة الائتمانية يتم من قبل البنك باسم الشخص وان صغرت قيمة وداعة، وكما أن دفاتر الشيكات يتم الحصول عليها بسهولة، فكذا الحال بالنسبة للبطاقات الائتمانية أو البنكية، فهي تستخدم كذلك بنفس السهولة في تسوية المدفوعات التي يقوم الفرد بها نظير الشراء والحصول على الخدمات المختلفة من التجار وغيرهم، ومهما كانت قيمة هذه المدفوعات سواء قلت ام كثرت، وتتعدد صور اساءة استخدام البطاقات البنكية، ولعل من اشهر تلك الصور (جريمة استخدام البطاقات المسروقة أو منتهية الصلاحية، وجريمة تزوير

^{٩٢}-أنظر : د/ هشام محمد فريد رستم، ص ٢٦٩- ٢٧٠.

^{٩٣}-أنظر : د/ احمد حسام طه تمام، ص ٢٠٩- ٢١٠.

^{٩٤}-أنظر : د/ هدى حامد قشقوش، المرجع نفسه، ص ١٣٢- ١٣٣.

البطاقات الحقيقية، وصورة قيام صاحب البطاقة ذاته بسحب مبالغ نقدية أكبر من المبالغ المسموح له بسحبها من آلة التوزيع الآلي للنقود مستغلاً بذلك بعض الثغرات التي ما زالت هذه الآلات تعاني منها حتى الآن)، وتتنوع كذلك طرق تنفيذ جريمة سحب مبالغ نقدية أكبر من المبالغ المسموح بسحبها من آلة التوزيع الآلي للنقود، فبعض حاملي البطاقات البنكية يكتفون باستخدام تلك البطاقة في سحب مبالغ أكثر مما ينبغي لهم سحبة، والبعض الآخر وهم الأكثر خطورة يقومون بإبلاغ البنك بضياع بطاقتهم الائتمانية- دون أن يكون ذلك صحيحاً- ثم يقومون على الفور، وقبل أن يقوم البنك بالتحفظ على أموالهم وحمايتهم، باستخدام البطاقة المبلغ عن ضياعها في سحب مبالغ معينة من حساباتهم البنكية، بحيث يعطوا انطباعاً بان سارق البطاقة أو من وجدها هو الذي قام بسحب تلك المبالغ النقدية^(٩٥).

المطلب الرابع

جرائم الاعتداء على حرمة الحياة الخاصة

أهمية البيانات والمعلومات المتعلقة بالحياة الخاصة والمخزنة إلكترونياً، لحياة الأفراد خصوصيتها بما تحويه من أسرار وخصوصيات، والمحافظة عليها من أكثر الأمور التي تحظى بحماية دستورية وقانونية في كافة دساتير العالم المتمدين وقوانينها^(٩٦).

" ولئن كان صحيحاً ما لاحظته بعض علماء الاجتماع من أن ثمة ارتباطاً وثيقاً بين التقدم التقني واتساع نطاق الرقابة الاجتماعية على الأفراد، فإن هذه الرقابة قد بلغت منتهاها مع تسارع وتيرة تقدم تقنية الحاسبات الآلية وأطراد الاعتماد عليها في تسيير شؤون المجتمعات، إذ تتيح تلك الآلات الإلكترونية إمكانات فائقة لتخزين ومعالجة واسترجاع ونقل كم هائل من البيانات والمعلومات التي تقوم الدول الحديثة بجمعها عن الأفراد، وهو ما يجعلها - حسب وصف بعض الفقه- أداة للرقابة غير مسبوقه في يد السلطات، اصف إلى ذلك أن كثيراً

^{٩٥}-أنظر : د/أحمد حسام طه تمام، ص ٢١٠- ٢١١

^{٩٦}-أنظر : د/ أحمد حسام طه تمام، ص ٣١٥

من المؤسسات الكبرى والشركات الحكومية والخاصة تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل.. الخ.

وتستخدم الحاسبات الآلية وشبكات الاتصال والمعلومات في خزن تلك البيانات الخصوصية ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مصرح أو ماذون به أو بطريق التحايل أكثر من ذي قبل، ويفتح مجالاً أوسع لاساءة استخدامها أو توجيهها توجيهاً منحرفاً أو خاطئاً أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكماً خفياً من واقع سجلات البيانات الشخصية المخزنة، الأمر الذي حدا بكثيرين إلى وصف استخدام الحاسبات الآلية كبنوك للبيانات والمعلومات بأنه تهديد غير مقبول للخصوصية والحريات المدنية.

وفي ثناياها، تحمل تلك الحاسبات نفس المخاطر المهددة للخصوصية التي عرفتتها البشرية في مجال النظم اليدوية لتسجيل وحفظ واسترجاع البيانات الشخصية، غير انها تضيف إليها ابعادا جديدة وخطيرة نابعة من طبيعة تلك الآلات التقنية المتقدمة في مجالات تخزين البيانات والمعلومات ومعالجتها ونقلها.

ففي مجالات التخزين، نجد أن التقدم العلمي لا يصادف اية عقبات فنية، ولذلك فإن سعة ذاكرات الحاسبات الآلية غير محدودة علمياً، ووسائط أو اوعية المعلومات يتزايد على الدوام حجم تخزينها للبيانات والمعلومات مع صغر وتضاؤل شكلها الخارجي، ومن شان ذلك انشاء بنوك أو مراكز وطنية للمعلومات تخزن فيها الدولة ملفات تحتوي معلومات شاملة ومفصلة عن الافراد، وهو ما حدث بالفعل في دول العالم المتمدين، وتكمن في هذه المراكز والبنوك أكثر التهديدات جسامة لحرمة الحياة الخاصة للأفراد، ففي هذه البنوك يمكن تخزين اكبر قدر ممكن من المعلومات عن ملايين الأشخاص، والاحتفاظ بها إلى الابد، واستخراج بيانات كافية عن اي انسان من المسجلين بها، وتعرية حياته بكشف تفاصيل سابقة على وقت استخراج تلك البيانات بزمان طويل، مما قد يسبب له اضراراً بليغة يتعذر أو يستحيل اصلاحها وتداركها، فضلاً عن أن هذه المعلومات

الشخصية تصبح فى هذه البنوك مجمعة، متوافرة، سهلة المنال ومتاح استخدامها فى اغراض الرقابة على الافراد والاشخاص الطبيعية والمعنوية على حد سواء.

وفى مجالات معالجة البيانات تتجلى المخاطر التى تهدد حرمة الحياة الخاصة للأفراد عند ربط الحاسبات بعضها ببعض أو ربطه بحاسب مركزى أو بشبكات عامة للاتصالات و المعلومات ، حيث يتسنى بذلك تبادل المعلومات فيما بين المراكز المعلوماتية المتباعدة مكانيا والمختلفة من حيث اغراض تخزين البيانات بها، وربط هذه المعلومات بعضها البعض واستكمالها وتحليلها ومعالجتها على نحو يتيح التوصل إلى معلومات جديدة عن شخص أو مجموعة اشخاص.

واخيرا ، وفى مجالات نقل البيانات و المعلومات: يلاحظ أن المخاطر المهددة للخصوصية تظهر بشكل واضح وجلى فى عدم قدرة شبكات الاتصال على توفير امان مطلق أو كامل لسرية ما ينقل عبرها من بيانات ومعلومات، وامكانية استخدام هذه الشبكات فى الحصول بصورة غير مشروعة من بعد على المعلومات^(٩٧).

صورة الانتهاكات المعلوماتية الواقعة على حرمة الحياة الخصوصية لعل من اخطر الجرائم التى يمكن أن تقع عن طريق الحاسبات الآلية وشبكات الاتصالات و المعلومات الخاصة بها (الإنترنت) هى جرائم الاعتداء على حرمة الحياة الخاصة، نظرا لعدم وجود الحماية التقنية الفاعلة والفعالة فى نفس الوقت لما يتم تداوله من بيانات ومعلومات واسرار ومراسلات بطريقة الحاسبات الآلية والإنترنت^(٩٨)، وللانتهاكات المعلوماتية لحرمة الحياة الخاصة صور واشكال تمارس من خلالها العديد من الاعتداء على الاسرار المعلوماتية المتعلقة بالافراد والاشخاص وخصوصية حياتهم، ولعل من ابرز تلك الصور ما يلى:

^{٩٧}-أنظر : د/ هشام محمد فريد رستم ، ص ١٧٨ - ١٨٤

^{٩٨}- أنظر : د/ مدحت رمضان، جرائم الاعتداء على الاشخاص والإنترنت، دار النهضة العربية- القاهرة- ٢٠٠٠ - صفحة ١٠١.

أولاً: استخدام بيانات شخصية غير صحيحة:

ويتحقق ذلك في احد شكلين، هما:

١- التلاعب في البيانات الشخصية أو محوها من قبل اشخاص غير مصرح لهم بذلك.

٢- جمع أو معالجة أو نشر بيانات شخصية غير صحيحة من قبل الاشخاص المرخص لهم بذلك قانوناً :

١- التلاعب في البيانات الشخصية أو محوها من قبل اشخاص غير مصرح لهم بذلك.

ويقترن هذا التلاعب أو المحو عادة بتحقيق مصالح مالية للجناة، إلى جانب انتهاك السرية وحرمة الحياة الخاصة للأفراد، ويمكن الإشارة في هذا الخصوص إلى حالة واقعية حدثت في شركة TRW company credit الأمريكية، وتخلص وقائع هذه القضية في أن هذه الشركة كانت تزود عملاءها (وكان أكثرهم من البنوك والمتاجر الكبرى وشركات تسهيلات الائتمان وشركات تاجير السيارات والمعدات الثقيلة) من خلال حاسباتها وانظمتها المعلوماتية بمعلومات تتعلق بالمركز الائتماني للأشخاص الذين يرغب هؤلاء العملاء في التعامل معهم، وذلك تجنباً للمخاطر التي قد تترتب على التعامل مع اشخاص لا يتمتعون بمركز ائتماني جيد، وكانت الشركة تقدم هذه الخدمة نظير اشتراك يدفعه العملاء، وذلك من واقع بيانات عن اشخاص (بلغ عددهم سنه ١٩٧٦ حوالى ٥٠ مليون شخص) كانت الشركة تقوم بجمعها وحفظها في الملفات المخزنة بحاسباتها الآلية، وقد اغرى هذا النشاط ستة من العاملين بتلك الشركة- من بينهم كاتب بقسم علاقات المستثمرين - على الاتجار في هذا النشاء والتلاعب في هذه البيانات عن طريق تعديل أو محو البيانات التي تظهر المركز الائتماني السيئ لأصحابها لتحل محلها بيانات جديدة تفيد تمتع صاحبها بمركز ائتماني جيد، وذلك في مقابل مبالغ مالية تم الاتفاق عليها، وبناء على هذه البيانات الائتمانية الزائفة التي تم إدخالها بالمحو أو الاضافة أو بهما معا إلى نظام معلومات حاسب شركة TRW، فقد تورط العديد من عملائها في معاملات مالية وتجارية مع اشخاص ذوى سمعة ائتمانية سيئة، وقد قدر البعض عدد السجلات التي تم التلاعب في بياناته بأكثر من مائة سجل، رغم أن الادعاء العام قام بتسجيل ست عشرة حالة تزوير فقط، وكشأن اكثر الجرائم المعلوماتية، فإن امر الجناة في تلك القضية لم يكتشف الا عرضاً، إذ اتصلوا بأحد الاشخاص

عارضين عليه تعديل البيانات الانتمانية الخاصة به مقابل ٦٠٠ دولار يدفعها، فاستشاط غضبا وقام بإبلاغ مكتب التحقيقات الفدرالية FBI، وفي التحقيقات اعترف كاتب قسم علاقات المستهلكين تفصيلا وشهد على ما قام به شركاؤه.

٢- جمع أو معالجة أو نشر بيانات شخصية غير صحيحة من قبل الأشخاص المرخص لهم بذلك قانونا :

وهذه هي الطريقة الثانية التي يتم من خلالها استخدام بيانات شخصية غير صحيحة، حيث تنصب أفعال الجمع أو المعالجة أو النشر التي يأتيها المصحح لهم بذلك من قبل القانون على بيانات ومعلومات مزورة أو غير صحيحة، وقد يتم ذلك كله بصورة عمدية، حينما يكون ارتكاب هذه الأفعال والانتهاكات مصحوبا بالعلم بمخالفة البيانات الشخصية للحقيقة وكونها غير صحيحة مع إرادة جمعها أو معالجتها أو نشرها، إلا أن كثيرا من حالات جمع أو معالجة أو نشر البيانات و المعلومات الشخصية غير الصحيحة إنما يتم عن طريق الإهمال وبوجه خاص في نطاق نظم تقارير الائتمان.

ثانيا: جمع أو تخزين بيانات شخصية صحيحة ولكن على نحو غير مشروع جنائيا:

لا يتم انتهاك الخصوصية وحقوق الأفراد الشخصية في مجال المعلوماتية- فقط - عن طريق استخدام بيانات ومعلومات شخصية غير صحيحة، وإنما قد يتم ذلك أيضا عن طريق جمع أو تخزين بيانات شخصية صحيحة في ذاتها ولكن على نحو غير مشروع جنائيا، وصفة عدم المشروعية الجنائية التي تلحق أفعال الجمع أو التخزين في هذه الحالة قد يكون مصدرها الأساليب غير المشروعة المستخدمة للحصول على هذه البيانات و المعلومات، وقد يكون مصدرها أيضا مضمون هذه البيانات ذاته.

١- عدم مشروعية أساليب وطرق جمع أو تخزين البيانات والمعلومات:

يعتمد في الحصول على البيانات والمعلومات على عدد من الأساليب التي يمكن استخدامها، والتي تشكل انتهاكا واضحا للخصوصية، ومن بين تلك الأساليب التقاط الارتجاجات التي تحدثها الأصوات في الجدران الاسمنتية للحجرات وترجمتها ومعالجتها بحاسب آلي مزود ببرنامج خاص لترجمتها إلى كلمات وعبارات، أو مراقبة واعتراض والتقاط وتفريغ الرسائل المتبادلة عن طريق البريد الإلكتروني، أو توصيل أسلاك بطريقة خفية إلى الحاسب الآلي الذي تخزن داخله البيانات المطلوب الاستيلاء عليها، أو التوصل بطريق غير مشروع

إلى ملفات بيانات تخص الآخرين، ومما لا شك فيه أن الزيادة المستمرة في استخدام الحاسبات الشخصية والبريد الإلكتروني وشبكات الاتصالات ونقل البيانات والمعلومات عن بعد سوف تؤدي حتما إلى زيادة استعمال هذه الأساليب غير المشروعة، وإلى تفاقم الأضرار والخسائر الناتجة عنها.

وقد أشار الاستاذ Sieber إلى حالة واقعية استخدمت فيها طريقة ماسة بجرمة الحياة الخاصة للحصول على بيانات شخصية، وتتلخص هذه الحالة في قيام مراهق من ألمانيا الاتحادية (سابقا) - لا يتجاوز عمره ستة عشر عاما- بنصب (مصادر بيانات) لالتقاط وجمع بيانات ذات طبيعة شخصية خاصة بمستخدمي أنظمة الفيديو تيكس Video Tex ، إضافة إلى قيامه بعمليات تلاعب واتلاف لبيانات بعض المستخدمين وتغيير كلمات السر التي يستخدمها بعضهم للتعامل مع النظام، مما أدى إلى حرمانهم من استخدامه^(٩٩).

٢- عدم مشروعية مضمون البيانات التي يتم جمعها أو تخزينها:

البيانات والمعلومات ذات الطبيعة الشخصية متعددة ومتنوعة، ومن بينها زمرة أو مجموعة لا يفترض - نظرا لطبيعة مضمونها- أن يتم جمعها أو تخزينها، وتحديد نوعية البيانات التي تتألف منها هذه الزمرة هو أحد أبرز الصعوبات التي تواجه حماية الحق في الخصوصية، لأن بالإمكان استخدام الحاسبات الآلية في معالجة بيانات شخصية جزئية (كالبيانات الصحية والتعليمية، والبيانات المتعلقة بمستوى وكيفية أداء الخدمة العسكرية، والعمليات البنكية، والمعاملات الضريبية، والتعامل ببطاقات الائتمان، وطلبات الإعانة التي تقدم لجهات حكومية، والتبرعات التي تقدم لجهات معينة، والاشتراك في صحف معينة ونوعية الكتب التي يتم استعارتها من المكتبات العامة.. الخ) على نحو يتيح مراقبة الأفراد وتحليل تصرفاتهم للتعرف على أبرز السمات المميزة لسلوكهم واستنتاج صورة تقريبية لشخصياتهم ، وهو ما يجعل حياتهم أشبه بكتاب مفتوح بمقدور أي شخص لديه إمكانية التوصل إلى ملفات الحاسب الآلي قراءته، فعدم وجود ضوابط قانونية في هذا المجال يؤدي إلى إمكانية جمع وتخزين ونقل كم هائل من المعلومات قد تتعلق بأدق الأمور الخاصة بالأفراد، وهو ما قد يسمح بخلق صورة تفصيلية لشخصياتهم بمجرد الاطلاع على الملف الذي يحتوى على هذه المعلومات داخل نظام الحاسب الآلي.

^{٩٩}-أنظر : د/ هشام محمد فريد رستم ، هامش (١) ص ١٩١

والواقع أن تحديد من له الحق في جمع وتخزين البيانات من ناحية، ونوعية هذه البيانات من ناحية أخرى، هي واحدة من أهم الصعوبات التي تواجه حماية الحياة الخاصة في مجال المعلوماتية أيضاً.

ثالثاً: الإفشاء غير المشروع للبيانات الشخصية وإساءة استخدامها:

تنقسم البيانات الشخصية التي تخزن في ذاكرات الحاسبات الآلية وبنوك المعلومات من حيث الحماية التي يكفلها لها قانون العقوبات- وفقاً لراى الاستاذ Sieber- إلى نوعين: " نوع يضم البيانات الشخصية السرية المشمولة بالحماية الجنائية التقليدية للاسرار، ونوع يضم ما عدا ذلك من بيانات شخصية غير سرية".

١- البيانات الشخصية السرية المشمولة بالحماية الجنائية التقليدية للاسرار:

تلحق صفة عدم مشروعية افشاء البيانات الشخصية فى الأحوال التى تسرى فيها على هذه البيانات النصوص الجنائية التقليدية المتعلقة بحماية الاسرار، ويبدو ذلك بوضوح فى مجالات عديدة، وعلى وجه الخصوص فى مجالات الطب والمحاماة والاعمال المصرفية، ومن قبيل ذلك الكشف عن شخصية صاحب الحساب أو الوديعة المرقمة، أو افشاء معلومات خاصة باحد الموكلين فى مكتب للمحاماة مخزنة على الحاسب الآلى الخاص بهذا المكتب والافصاح بها لمن ليس له حق الاطلاع عليها ومعرفتها، وتبدو سمة عدم المشروعية واضحة أيضاً فى حالة اساءة استخدام هذه البيانات والمعلومات باستخدامها فى غير الغرض الذى جمعت وخزنت من اجلة.

ولعل اكثر البيانات الشخصية السرية تعرضاً لخطر الافشاء غير المشروع هو المخزن منها فى ذاكرات الحاسبات الآلية للبنوك.

كما يتجلى أيضاً هذا الافشاء للبيانات والمعلومات السرية فى القطاع الامنى والشرطى، حيث يتزايد الاعتماد على الأنظمة الإلكترونية فى تخزين ومعالجة ونقل البيانات المتعلقة بملايين الاشخاص، ومن الامثلة على ذلك، ما ذكره الاستاذ Sieber، من قيام احد ضباط شرطة العاصمة النمساوية فيينا بتزويد مخبر خاص - خلال الفترة من عام ١٩٦١ حتى عام ١٩٧٨ - ببيانات السجلات الجنائية وملفات معلومات البحث الجنائى وملفات الشرطة الجنائية الدولية (الانتربول) المخزنة فى حاسب الشرطة عن بعض الاشخاص.

٢- البيانات الشخصية غير السرية:

من البيانات الشخصية ما يصعب- فى بعض الاحيان- اعتبار افشائه

محققا لضرر أو خطر على المجتمع يستوجب وصفه بأنه " غير مشروع جنائيا" أو " إجرامى " ، ويبدو ذلك بشكل واضح فى حالة المقارنة بواسطة الحاسب الآلى بين البيانات الشخصية المسجلة إلكترونيا لدى مختلف الاجهزة الحكومية بهدف ضبط الأداء وضمان حسن الادارة، وكشف الاحتيال الذى قد يمارسه البعض للاستفادة من المساعدات التى تقدمها هذه الاجهزة.

ويرى بعض الفقه أن برامج المقارنة الإلكترونية للبيانات تسهم فى ضبط الاداء بالنسبة للاجهزة الحكومية، وتحسين مستوى هذا الاداء، وضمان حسن تطبيق القانون، اضافة إلى انخفاض تكلفتها مقارنة بفاعليتها فى كشف الغش والاحتيال للحصول على المساعدات الحكومية بعيدا عن التعرض لخصوصيات المستفيدين، الا أن رايًا آخر يعارض ذلك متخوفاً، من امكانية استغلال هذه المقارنة لتحقيق اغراض لا تتعلق بكشف الغش والاحتيال ، أو أن يؤدي التماضى فى السعى لكشف ذلك إلى التغاضى عن التأثيرات السلبية لهذه المقارنة على السرية الشخصية والخصوصية ، ويقرر هذا الراى ايضا انه لئن كان ممكنا تبرير هذه المقارنة فى حالات فردية، الا أن التماضى فيها يظل قائما ومهددا بكشف الستار عن الاسرار والحياة الخاصة.

رابعا: مخالفة القواعد الشكلية المنظمة لجمع ومعالجة ونشر البيانات ذات الطبيعة الشخصية التى تدخل فى نطاق الحماية التشريعية لخصوصية المعلومات:

أن ضرورة حماية خصوصية المعلومات حتى فى الحالات التى اجيز فيها جمعها ومعالجتها ونشرها، قد دفع غالبية النظم القانونية الى وضع مجموعة من القواعد الشكلية لتنظيم جمع ومعالجة ونشر البيانات الشخصية، مثل ضرورة الحصول على ترخيص بذلك ، وفى كثير الدول يعد خرق هذه القواعد الشكلية جريمة يعاقب عليها القانون.

المطلب الخامس

جرائم الاعتداء على حقوق الملكية الفكرية والادبية

من الجرائم التى انتشرت ايضا – وبصورة خطيرة – فى الاونة الاخيرة،

جرائم الاعتداء على حقوق الملكية الادبية والفكرية بواسطة استخدام الحاسبات الآلية وشبكة الانترنت"، والاعتداء على الحقوق الادبية والفكرية أو ما اصطلح على تسميته "بحقوق المؤلف" لا ينبغي الخلط بينه وبين الاعتداء على الملكية الادبية والفكرية التي تنصب على البرامج والمعلومات في مجال المعلوماتية وتكنولوجيا المعلومات ، فهذه الاخيرة- الملكية الادبية والفكرية- تنصب على البرامج و المعلومات، اما الاعتداء على الحقوق الفكرية والادبية فهو يقع دائماً على العناصر غير المادية لنظام المعلوماتية، "والمثال الواضح على استخدام الحاسب الآلي في الاعتداء على الحقوق الفكرية والادبية هو استخدام ما يمنحه الحاسب من وسائل لخرق قواعد القانون المتعلقة بحقوق المؤلف . كما لو استخدم الحاسب الآلي في السطو على بنوك المعلومات التي تتضمنها برامج حاسب آخر ، أو كما في حالة تخزين هذه المعلومات على حاسب معين ثم يقوم المسئول عن هذا التخزين باستخدام هذه المعلومات أو التفريط فيها بدون إذن صاحبها".

والواقع أن استخدام معلومة معينة بدون إذن صاحبها يتضمن انتهاكاً مزدوجاً لحقوق هذا الشخص ، فهو من ناحية اعتداء على القيمة المالية التي قد تمثلها المعلومة، وهو من ناحية اخرى اعتداء على حق من الحقوق المعنوية على اعتبار أن للمعلومة قيمة ادبية علاوة على قيمتها المادية^(١٠٠).

المطلب السادس

جرائم إفشاء الأسرار في اطار المعلوماتية

قد تستخدم الحاسبات الآلية وشبكات الاتصال والمعلومات الخاصة بها في ارتكاب العديد من الجرائم المتعلقة بإفشاء الاسرار، والحاسب الآلي يعتبر بالفعل وسيلة فعالة في هذا النوع من الجرائم نظراً لكونه آلة مستعدة تماماً لفتح ابوابها لمن يحسن إستخدامها.

والواقع أنه يمكن استخدام الحاسب الآلي في ارتكاب انواع عديدة من هذه الجرائم أهمها:

١ - إفشاء سرية المعلومات:

^{١٠٠}- أنظر : د/ هشام رستم، ص ١٨٧- ص ٢٠١، د. نائلة عادل محمد فريد ، ص ٢٤٢- ص ٢٤٦.

قد تتخذ المعلومات صور المعاملات اليومية (كالخطابات والمحادثات الهاتفية) وتشكل هذه المعلومات قدراً كبيراً من المعلومات التي تحظى بأهمية خاصة في مجال تكنولوجيا المعلومات، وهو ما يتطلب حمايتها من الوصول اليها والتلاعب بها، ومما لا شك فيه أن افشاء سرية الاتصالات بما تشمله من خطابات ومحادثات هاتفية باعتباره صورة من صور المعلومة، قد يقضى إلى تدمير العديد من المؤسسات والمصالح بل وتعريض الدول ايضاً واقتصادياتها لاضرار بالغة، نتيجة لاعتماد قطاعات مختلفة في الدولة - في تسيير شئونها - الحيوية - على سرية تلك الاتصالات والخطابات.

ولعل في العبث في شبكات الاتصالات والمعلومات الخاصة بالحاسب الآلي، وانتهاك العديد من مواقع البريد الإلكتروني على شبكة الانترنت، ما ينبئ عن تفشي تلك الجرائم في الحاضر والمستقبل القريب والبعيد على حد سواء.

٢- إفشاء اسرار الدفاع الوطني والامن القومي:

قد تمس الجرائم المعلوماتية المصالح العليا للدولة، عن طريق افشاء العديد من الاسرار والمعلومات التي تتعلق بالامن القومي للدولة" كما لو كانت تتعلق بالمخابرات العامة أو بالدفاع الوطني" ولاشك في أهمية هذه البيانات والمعلومات المخزنة آلياً وتأثيرها البالغ على مستقبل الدول والشعوب على حد سواء.

٣- إفشاء الاسرار المهنية:

يتوقف نجاح العديد من اصحاب المهن الحرة والمؤسسات والنشاطات على التكتم والاحتفاظ بالعديد من الاسرار المهنية واسرار العملاء في حاسباتهم الآلية وعدم اطلاق الغير عليها، كما يقوم العديد من اصحاب المهن الحرة ايضاً بتخزين بيانات ومعلومات تتعلق بآدق تفاصيل واسرار حياة العملاء وتعاملاتهم في حاسباتهم الآلية مع تعهدهم بالاحتفاظ بها وعدم اطلاق الغير عليها، ولاشك أن في افشاء تلك الاسرار والمعلومات ما يعرض حياة العديد من الاشخاص ومصالحهم لآخطار واضرار بالغة.

٤- إفشاء الاسرار الصناعية:

وهناك اخيراً من المعلومات ما اطلق عليه " سر المهنة أو سر الصناعة"

فكثير من المشروعات المالية والاقتصادية والخدمية يتوقف نجاحها على مثل هذا السر الذي يميزها عن غيرها من جودة الانتاج أونى الإستثنائية ، كما أن من المعلومات ما يتعلق بخطوات ومراحل الانتاج الصناعى المختلفة ، فالسلعة أو الخدمة تمر بعدة مراحل متفاوتة حتى تصل إلى شكلها النهائى الذى نراها عليه، وتعد هذه المراحل من المعلومات المهمة التى يحرص اصحاب الاعمال والمشروعات على الاحتفاظ بها وحمايتها من الاطلاع عليها من قبل الغير، ولا يخفى على احد حجم الاضرار الناجمة والمترتبة على الافشاء بأى من هذه المعلومات ذات الاهمية القصوى.

المطلب السابع

جرائم السب والقذف عبر الإنترنت

يقصد بالسب " كل تعبير يחדش الشرف والاعتبار " وقد عرفته محكمة النقض المصرية بانه " فى اصل اللغة الشتم سواء باطلاق اللفظ الصريح الدال عليه أو باستعمال المعارىض التى تومئ اليه ، وهو المعنى الملحوظ فى اصطلاح القانون الذى اعتبر السب كل الصاق لعيب أو تعبير يحط من قدر الشخص نفسه أو يחדش من سمعته لدى غيره " (١٠١)، (١٠٢).

اما القذف فيعرف بانه " الإسناد العلنى لواقعة محددة تستوجب عقاب أو احتقار من اسندت إليه " ، ويقصد بالاسناد " نسبة امر أو واقعة إلى شخص معين بأية وسيلة من وسائل التعبير عن المعنى " (١٠٣).

ويتميز السب عن القذف فى أن القذف لا يتحقق الا باسناد واقعة معينة يكون من شأنها لو كانت صحيحة عقاب من اسندت اليه أو احتقاره بين اهل وطنه، اما السب فلا يستلزم أن يكون موضوع الاسناد واقعة معينة، بل يتحقق بالصاق أية صفة أو عيب أو معنى شأنن إلى المجنى عليه (١٠٤).

١٠١- نقص ٢٨ يناير ١٩٨٥ ، مجموعة احكام النقض، س ٣٦ ، رقم ٢٥ ، ص ١٧٧ .

١٠٢- د. على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى ، شرح قانون العقوبات " القسم الخاص " ، دار المطبوعات الجامعية، الاسكندرية، ١٩٩٩ ، الكتاب الثانى " جرائم الاعتداء على الانسان والمال ، ص ٢١٥ .

١٠٣- د. على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى، المرجع السابق، ص ١٧٦ .

١٠٤- د. على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى، المرجع نفسه ، ص ٢١٥ .

والسب والقذف كلاهما من جرائم الاعتداء على الشرف والاعتبار، ويقصد بالشرف والاعتبار " المكانة الاجتماعية التي تحيلها الانسان فى مجتمعة والتي تتكون من مجموعة من الصفات الموروثة والمكتسبة، ومن علاقاته بغيره من ابناء المجتمع، والتي يتحدد على اساسها مركزه الاجتماعى وما يستحق من احترام وتقدير بين مخالطيه" وحق الانسان فى شرفه واعتباره من الحقوق اللصيقة بالشخصية القانونية والمتفرعة عنها ايا كانت المكانة الاجتماعية التي يحتلها فى المجتمع، وبالتالي لا يوجد شخص معدوم الشرف والاعتبار كلية منذ أن اعترفت القوانين الحديثة لكل فرد بشخصيته القانونية، والارتباط بين الشرف والاعتبار والشخصية القانونية- على هذا النحو - يسمح بالقول أن الاشخاص المعنوية- وليس فقط الشخص الطبيعي- لها الحق فى الشرف والاعتبار وتستحق ذات الحماية ما دام يعترف لها بالشخصية القانونية.

وهكذا فان شرف الانسان واعتباره يعتبر " قيمة اجتماعية" لا تقل اهمية عن تلك التي تتعلق بحق الانسان فى الحياة وفى سلامة بدنة، ومن ثم كانت جديرة باسباغ الحماية الجنائية عليها^(١٠٥).

وفى إطار جرائم المعلوماتية ، فإننا نجد العديد من افعال السب والقذف ترتكب على شبكة الانترنت، وبصفة خاصة على مواقع البريد الالكتروني والشبكة العالمية العنكبوتية (ويب) مع تزايد المنافسة غير المشروعة بين مختلف النشاطات فى اطار من حرية التجارة والحركة التي لا تحدها اية حدود، كما يزداد ارتكاب تلك الجرائم، ايضا بواسطة استخدام هذه الشبكات بغية التشهير والانتقام من العديد من الاشخاص والمؤسسات باقل السبل والتكلفة الممكنة، كما تكمن خطورة هذه الجرائم عند اختلاف وجهات النظر بين الدول والحكومات بصدد قضية أو مسألة معينة، فتعمد تلك الدول والحكومات إلى التشهير بغيرها من الدول الاخرى، والشعوب من خلال السيطرة على مؤسسات اعلامية تقوم ببث العديد من افعال السب والقذف والتشهير والتنكيل على مواقعها عبر شبكة الانترنت، بغية تضليل الراى العام بصدد تلك القضايا، أو التشهير والانتقام من الاطراف المعتدى عليها، والتي تراها تلك الدول والمؤسسات المسيطرة عليها عدوا لها من وجهة نظرها السياسية أو العنصرية، والمثال الواضح على ذلك ما

^{١٠٥}- د.على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى، ص ١٧٣

تقوم به بعض وسائل الاعلام التي تسيطر عليها الكيانات الصهيونية فى الدول الغربية من بث الروح المعادية للإسلام على شبكة الانترنت، وتضليل الراى العام فى تلك الدول وفى غيرها حول حقيقة الصراع العربى الإسرائيلى وماهى القضية الفلسطينية.

المطلب الثامن

الجرائم المخلة بالآداب العامة فى اطار المعلوماتية

دفعت وسائل التكنولوجيا الحديثة بعض الجناة إلى محاولة استغلال التقدم العلمى فى نشر العديد من الصور الجنسية الفاضحة والافعال الفاحشة المخلة بالآداب العامة على شبكة الانترنت، والتي غالباً ما يكون محلاً لها الاطفال الصغار سواء كان ذلك عن طريق تصويرهم فى اوضاع جنسية مخلة، أو استخدام التقنية الرقمية الحديثة (DIGITAL) فى تركيب صور اطفال ابرياء على اجساد عارية أو اوضاع جنسية بصورة تتعارض مع الاحترام الواجب لطفولتهم، كما اتخذ الاعتداء على الحق فى الصورة شكل الاعتداء على ملكية الشخص لصورته والاستغلال المالى لها.

أولاً: جرائم اشاعة الصور والافعال الفاحشة المخلة بالآداب العامة على شبكة الانترنت

الاشاعة فى اللغة تعنى " أن الخبر ينتشر غير مثبت منه" وهى مشتقة من الفعل (اشاع) أى " أظهر ونشر"^(١٠٦).

وتتحقق تلك الجرائم من خلال العديد من الافعال المادية التى تتجسد فى عرض أو نشر أو توزيع اية صور أو اقوال أو افعال فاحشة وفاضحة ومخلة بالآداب العامة على شبكة الانترنت ، كما تتحقق ايضا من خلال انشاء العديد من المواقع الجنسية على شبكة الانترنت والترويج لها أو استقطاب الزائرين اليها ، أو تبادل رسائل البريد الالكترونى التى تحوى العديد من الصور والاشارات والاقوال والافعال الفاحشة بين المستخدمين لشبكة الانترنت ، أو ارسال الرسائل

^{١٠٦} - المعجم الوجيز ، مجمع اللغة العربية، الهيئة العامة لشئون المطابع الاميرية ، ١٩٩٠، ص ٣٥٧.

الجنسية عبر خدمة الرسائل في البريد الالكتروني على شبكة الانترنت من مواقع جنسية مجهولة المصدر أو الهوية إلى العديد من المواقع على تلك الشبكة.

وقد يكون الغرض من تلك الجرائم ارتكاب العديد من أفعال النصب والاحتيال المعلوماتي وقد يكون الغرض منها أيضا - وكما سبق أن بينا - اتلاف العديد من المكونات المنطقية للحاسب الآلي عن طريق استخدام الفيروسات الجنسية التي تقوم بعمليات التدمير لتلك المكونات.

ثانيا: جرائم الاستغلال الجنسي للأطفال عبر شبكة الانترنت:

" نتيجة للتقدم التكنولوجي الهائل في مجال استخدام الحاسب الآلي الإنترنت ، فقد ظهرت على الإنترنت بعض المواقع التي تتناول بالعرض والتوزيع صور خارجة للأطفال، مما دفع المجتمع الدولي إلى محاولة التدخل لوقف مثل تلك النشاطات والاعتداءات الاجرامية التي تمس الكرامة الانسانية والحياء العام، ولذا فقد لقي هذا الموضوع من قبل خبراء اليونسكو بباريس في الفترة من ١٨ - ١٩ يناير ١٩٩٩ ، فقد عقد المؤتمر الدولي لمكافحة استغلال الاطفال في الجنس على الإنترنت في الفترة من ٢٩ سبتمبر إلى الاول من اكتوبر ١٩٩٩ بقيينا بالنمسا بمبادرة من وزير خارجية النمسا ووزيرة خارجية الولايات المتحدة الامريكية في تلك الفترة، وقد اكد المؤتمر على تدعيم التعاون الدولي في مجال مكافحة هذا النوع من النشاط، وتشجيع وضع قواعد ذاتية للسلوك من قبل موردي خدمة الإنترنت، وتشجيع انشاء خطوط ساخنة للاتصال تسمح للمواطنين بالابلاغ عن المواقع الاباحية للأطفال على الإنترنت ، وقد كان الهدف الرئيسي لذلك المؤتمر هو توعية الجمهور لمواجهة الاستغلال الجنسي للأطفال على الإنترنت، وخصوصا أن الإنترنت اصبح بالفعل جزءا من حياتنا اليومية سواء تعلق الامر بالاتصالات أو العمل أو التجارة، ومع الاخذ في الاعتبار حق كل منا في الاتصال بطريق الإنترنت ، وقد اكد هذا المؤتمر على انه في اطار الحماية الخاصة للطفل بمقتضى الاتفاقية الدولية المتعلقة بحقوقه، فانه يقع التزام على عاتق الدول المختلفة بمحاربة الاستغلال التجاري للأطفال عن طريق الجنس، وقد اعترف المؤتمر بتزايد مشكلة الاستغلال الجنسي للأطفال على الإنترنت، كما اكد المؤتمر على وجوب عدم التسامح مع مثل هذا الامر، وضرورة تدخل المشرع الوطني لتجريم التجارة الجنسية على الإنترنت التي تنطوي على استغلال للطفولة، وتدعيم التعاون الدولي في مجال مكافحة هذه الجرائم، وانشاء وحدات

خاصة لمكافحة هذه الجرائم، واعداد برنامج تدريب خاص للتأهيل فى هذا المجال، واكد المؤتمر كذلك على أنه يتعين على الدول المختلفة أن تضع قواعد دنيا يتم بمقتضاها وضع تعريف متقارب لهذه الجريمة واعتبار أن الحياة العمدية وانتاج وتوزيع واستيراد وتصدير ونقل والاعلان عن صور الاطفال الاباحية بطريق الكمبيوتر أو وسائل التخزين الالكترونى من الجرائم المعاقب عليها، وانه يتعين من الناحية الاجرائية اتخاذ الإجراءات الكفيلة للمحافظة على البيانات المتحفظ عليها بما فيها تلك البيانات الموجودة تحت يد مورد خدمة الإنترنت ولو كان فى بلد آخر مع الاخذ فى الاعتبار المشكلات الخاصة بالتخزين وحجمه والوامر القضائية ومقتضيات حماية البيانات والتي يمكن أن تكون محلا للمطالبة بتعاون متبادل بشأن كل تفتيش أو قبض أو افشاء لمحتوى هذه البيانات، واوصى المؤتمر بضرورة اتخاذ اجراءات مشتركة تسمح بتجاوز الحدود لتفتيش وضبط اجهزة الكمبيوتر بما يسرع بالاجراءات الجنائية، علاوة على انه يتعين اقامة وسائل الاتصال الدائم لتحقيق التعاون الدولى فى هذا المجال.

المطلب التاسع

غسيل الأموال عبر الإنترنت

اولا: المقصود بغسيل الأموال:

يعنى مصطلح غسيل الأموال أن هذه الأموال "القدرّة إذا بقيت في أيدي حائزها فإن ذلك يؤدي إلى اكتشاف نشاطهم الإجرامي وبالتالي فإن غسيل الأموال هي محاولة من هؤلاء الأشخاص المجرمين بكافة الطرق لإخفاء الأصل غير الشرعى لهذه الأموال لكي يوجه إلى الإستثمار فى أعمال اقتصادية كل البعد عن الأعمال غير الشرعية التي حصلت منها هذه الأموال^(١٠٧).

وبعبارة اخرى اكثر تفصيلا، فإن غسيل الأموال غير المشروعة أو الأموال القدرّة هو جريمة من الجرائم الاقتصادية، تحكمها فى اغلب الاحوال قواعد القانون الجنائى الدولى، تتضمن عملية أو سلسلة من العمليات الاقتصادية والمالية المركبة، يبغى مرتكبها اضعاف الصفة الشرعية على اموال متحصلة من أنشطة اجرامية ومصادر غير شرعية عن طريق اخفاء المصدر الاجرامى لهذه

^{١٠٧}-أنظر : د/ عبد الرحمن صبرى ، غسيل الاموال فى اسواق المال الناشئة، مقالة منشورة بجريدة الاهرام، السنة ١٢٤، العدد رقم ٤١٢٥٨ بتاريخ ١١/٢٢/١٩٩٩ صفحة قضايا وارهاء.

الأموال، بما يمكن الجناة في نهاية الامر من الانتفاع بتلك الأموال- في طمأنينة ويسر- وادخالها في دائرة التعامل الاقتصادي والمالي القانوني^(١٠٨).

وجريمة غسيل الأموال- وكاية ظاهرة اجرامية- يلتزم لحققها وقيامها قانونا توافر اركان وعناصر معينة حيث لا تقوم تلك الجريمة بغير تحقق هذه الاركان وعناصرها مجتمعة ومكتملة، وياتلف الركن المادي لتلك الجريمة من ثلاثة عناصر هي: وجود جريمة اولية أو اصلة سابقة تعتبر مصدرا للمال القدر غير المشروع، وان يتمخض عن تلك الجريمة مال غير نظيف، وان يقوم الجاني بارتكاب نشاط اجرامي يتحقق به غسل هذا المال عبر التنظيف، ويتمثل هذا النشاط في اجراء عملية أو سلسلة من العمليات الاقتصادية والمالية – البسيطة أو المركبة- بغية لتطهير تلك الأموال القذرة وادخالها إلى حيز الوجود المالي والاقتصادي والقانوني لتبدو في النهاية كأنها مشروعة من مصدر مشروع).

اما الركن المعنوي لجريمة غسيل الأموال فيحوى عنصرين هما: عنصر العلم (علم الجاني بعناصر الركن المادي لتلك الجريمة)، وعنصر الارادة (ارادة تحقيق النتيجة الاجرامية، التي تتمثل في تلك الجريمة في ارادة تطهير تلك الأموال واخفاء مصدرها الاجرامي غير المشروع).

ثانياً: اساليب غسيل الأموال عبر شبكة الإنترنت:

لاشك أن التقدم العلمي الهائل في مجال تكنولوجيا المعلومات ووسائل الاتصالات خاصة مع بداية النصف الثاني من القرن العشرين- كما سبق أن بينا- وشيوع استخدام تلك التكنولوجيا في اجراء المعاملات المالية والانتمانية، قد امد الجناة في جرائم غسيل الأموال ببدال وخيارات جسمية ومبتكرة وحديثة لارتكاب جرائمهم القذرة ومحو آثارها الاجرامية في سهولة ويسر، ووضع في ذات الوقت العديد من العراقيل والصعوبات والتحديات امام السلطات المختصة- من اجهزة ضبط ومكافحة وتحقيق وقضاء- بتعقب تلك الجرائم وملاحقة مرتكبيها وتقديمهم للعدالة وتنفيذ الجزاءات الجنائية عليهم.

ومن ثمرات هذا التقدم، والتي لاقت اهمية بالغة ودراسة تفصيلية في

^{١٠٨}-أنظر : د/ اشرف توفيق شمس الدين – دراسة نقدية القانون مكافحة غسل الأموال الجديد- دار النهضة العربية ٢٠٠٣ ص ٣.

الأونة الاخير لدى المتخصصين فى مجال الجريمة، وعلى وجه الخصوص " الجريمة المنظمة" ، استخدام مرتبكي جرائم غسل الأموال لشبكة الاتصالات الدولية عبر اجهزة الحاسب الآلى والمعروفة باسم (الإنترنت) للتحويل الالكترونى للاموال غير النظيفة من شخص لآخر- عن طريق اجهزة الحاسب الآلى الشخصية- عبر الدول، ودون حاجة إلى اللجوء لاساليب تحويل النقود والأموال التقليدية من خلال البنوك وغيرها من المؤسسات المصرفية .

وقد لوحظ أن الإنترنت يعد وسيلة مثالية لمرتبكي جرائم غسل الأموال غير المشروعة، وخاصة وان بعض المجرمين يقوم بإنشاء صندوق بريدية الكترونية باسماء وهمية، بل ويقوم البعض بتأسيس العديد من المراكز المالية- والمعروفة باسم " لاوفشور" – عن طريق شبكة الإنترنت ، وبالتالي فان كافة العمليات المالية التى يجرونها تكون- غالبا- باسماء وهمية أو خيالية، وبالإضافة إلى ذلك. فان هناك بنوكا عبر الإنترنت- مثل : (بنك الاتحاد الاوربى) " وهو اول بنك يتم تاسيسه على الإنترنت عام ١٩٩٤" - تمارس انشطتها عادة فى الدول أو الجزر التى تتبنى مبدا " سرية الحسابات البنكية" بصفة مطلقة، وتوفر تسهيلات كبيرة لجذب رؤوس الأموال إليها، ويمكن لعملاء هذه البنوك تحويل اموالهم بسهولة وسرعة فى سرية تامة، فيستطيع الشخص من منزلة- على سبيل المثال- عن طريق الكمبيوتر الشخصى المربوط بشبكة الإنترنت أن يجرى العديد من العمليات المالية التى يريدونها وهو يتمتع بدرجة عالية من السرية والحماية ، وتعرض بنوك الإنترنت هذه خدمات متعددة على الجمهور، منها: (فتح حساب مباشرة- سواء بالنسبة للأفراد أو الشركات – مع امكان فتح حسابات بنكية رقيمة أو مشفرة ، وتحويل الأموال إلكترونيا فى اى مكان فى العالم وبجميع العملات، وارسال الشيكات لاي مستفيد فى اى بلد،والدفع المباشر عبر الإنترنت، وشراء وبيع جميع العملات إلى غير ذلك من الخدمات الانتمائية والبنكية الاخرى التى تقدمها تلك البنوك للعديد من عملائها والمستفيدين من خدماتها المتعددة)، ولاشك فى اهمية هذه البنوك بالنسبة للعديد من الجناة مرتبكي جرائم غسل الأموال ، وتسهيلها الدائم للعديد من عمليات غسل الأموال المنظمة التى تتم على اقليم اكثر من دولة، وقد أشارت بعض التقديرات إلى أن حوالى ٢٨.٥ مليار دولار امريكى يتم غسلها سنويا عبر الإنترنت لتخترق حدود ٦٧ دولة.

ومن أجل رصد عمليات وحجم واساليب غسيل الأموال فقد قامت الدول الصناعية السبع الكبرى اثناء قمه L'Arche التى عقدت فى باريس فى يوليو سنة ١٩٨٩ ، بانشاء مجموعة عمل مالى دولية اطلق عليها " فريق عمل المهام المالية FATF أو GAFI " لدراسة الوسائل اللازمة لمنع استخدام الانظمة البنكية الدولية فى غسل الأموال، ودراسة ومناقشة وسائل واتجاهات واساليب غسيل الأموال سنويا، وقد انضمت إلى تلك المجموعة المالية العديد من دول العالم، وقامت تلك الدول بارسال العديد من الخبراء الاقتصاديين والماليين لحضور اجتماعات تلك المجموعة التى تتعقد بصفة دورية كل سنة لمناقشة ودراسة المسائل السابق بيانها، بالاضافة إلى دراسة الاساليب الفعالة لمكافحة غسيل الأموال.

وقد قام فريق عمل المهام الدولية (FATF) برصد اهم اساليب غسيل الأموال عبر الإنترنت فى تقريرين متتاليين عن سنتين متتاليتين (التقرير الحادى عشر فى ٣ فبراير ٢٠٠٠ عن الفترة من (١٩٩٩ - ٢٠٠٠)) (التقرير الثانى عشر فى ١ فبراير ٢٠٠١ عن الفترة من (٢٠٠٠ - ٢٠٠١)) " وسنعرض فيما يلى لاهم ما جاء فى هذين التقريرين من اساليب لغسل الأموال عبر شبكة الإنترنت:

١- العمليات المصرفية عبر الإنترنت:

تقدم الاعداد المتزايدة من المؤسسات المالية فى الوقت الراهن خدمات مصرفية جزئية عبر الإنترنت، وفى الوقت ذاته، فان جهات اخرى تستخدم الإنترنت لتقديم خدمات غسل الأموال ، وفى بعض الاحيان يطلق على هذه الخدمات اسم " خدمات مالية مقدمة عن بعد " أو " فرص استثمارية" لاضفاء صبغة قانونية عليها، وفى ظل انتشار كل انواع النشاط التجارى عبر الإنترنت والامكانيات المرتقبة لاختراق هذه الوسيلة، قام خبراء FATF بدراسة هذا الموضوع بصورة دقيقة فى محاولة للقاء المزيد من الاهتمام على الاحتمالات المرتقبة لاستخدام هذه الوسيلة (الإنترنت) فى عمليات غسيل الأموال ، ويأتى هذا الموضوع فى اطار جهودات FATF الرامية إلى تحديد التضمينات الرئيسية لغسل الأموال الناتجة عن تقديم وسائل التكنولوجيا الحديثة.

وتختلف خدمات المعاملات التجارية من مؤسسات إلى أخرى عبر الإنترنت، ولكنها تتضمن العديد من الأنشطة مثل: (فتح الحسابات الجديدة " كالتشيكات والادخار.. وغيرها) ودفع الفواتير، والكروت الدائنة والمدينة، وكروت السحب من ماكينات الصرف الآلي، والإقراض عبر الإنترنت، ومنح الودائع في بعض الاحيان وعلى الرغم من تقديم بعض الخدمات عبر الإنترنت عن طريق بنوك تقتصر خدماتها على تلك المقدمة عبر الإنترنت، فإن المؤسسات التي تقدم خدمات المعاملات التجارية قائمة بالفعل، بالإضافة إلى المؤسسات التقليدية والتي تحولت إلى أنظمة مصرفية عبر الإنترنت لتقديم خدمات إضافية لعملائها.

ويرتكز الاهتمام الرئيسي فيما يتعلق بالمعاملات المصرفية عن طريق الإنترنت في الخفض الواضح للاتصالات المباشرة بين العميل والمؤسسة المالية، حيث يستطيع العميل الدخول إلى الحساب الخاص به عن طريق الكمبيوتر الشخصي باستخدام برامج استعراض الإنترنت، والدخول إلى الإنترنت على المستوى العالمي من خلال شركات توفير خدمات الإنترنت، ويتم الدخول فور قيام العميل بتقديم الكود الشخصي الخاص به إلى شبكة الإنترنت الخاصة بالبنك، ونظرا لان هذا الدخول غير مباشر، فإن المؤسسة المالية لا يوجد لديها أي وسيلة للتأكد من هوية العميل الذي قام بالفعل بالدخول إلى الحاسب الآلي والوصول إلى الحساب المقصود، وبالإضافة إلى ذلك، فإنه في ظل السرعة المتزايدة للدخول على الإنترنت، فإن العميل يتمتع بإمكانية الدخول إلى الحساب الخاص به من أي مكان في العالم، ولا تتمكن المؤسسة من اثبات الموقع الذي تم منه الدخول إلى الحساب، ويرجع ذلك إلى أن الدخول يتم عبر شركات توفير خدمات الإنترنت، ومن ثم يتمكن أي فرد يرغب في إخفاء هويته الحقيقية- من القائمين بعمليات غسيل الأموال أو أية أنشطة إجرامية أخرى- من الحصول على حساب مصرفي على الإنترنت غير خاضع لأي ضوابط، كما يمكنه السيطرة على هذا الحساب من أي مكان في العالم.

٢- أنظمة التحويلات البديلة:

على الرغم من عدم وجود تعريف اصطلاحى متفق عليه على نطاق واسع فيما يتعلق بـ " أنظمة التحويلات البديلة "، فإن هناك اتفاق جزئي حول الخصائص الشائعة لهذه المنظمة، وبادئ ذي بدء فإنه ينبغي التنويه إلى أن نظام التحويلات البديلة يتم استخدامه للإشارة إلى ما يطلق عليه حاليا في بعض

الاحيان اسم " انظمة سرية" أو " انظمة مصرفية موازية "وقد تطورت هذه الانظمة بوجه عام . اعتمادا على عوامل اخلاقية أو ثقافية أو تاريخية خاصة وفي بعض الحالات، شكلت هذه الانظمة الوسائل التقليدية لنقل الأموال وذلك قبل انتشار الانظمة المصرفية الغربية فى القرن التاسع عشر والقرن العشرين، ويتمثل العامل الرئيسى فى هذه الانظمة- والذى تشترك فيه مع النظام المصرفى الرسمى أو " البنك المراسل" فى نقل القيمة من مكان إلى آخر بدون الانتقال المادى للعملة، وتعمل انظمة التحويلات البديلة فى اغلب الاحيان- خارج الانظمة التشريعية المالية القومية، وهناك انظمة توظف عوامل من الاقتصاد القانونى أو حتى الخدمات المالية المنتظمة، الامر الذى يؤدى بدوره إلى صعوبة الكشف عن هذه الحالات من قبل سلطات تنفيذ القانون.

ويتمثل العامل الاساسى فى كل نظام من انظمة التحويلات البديلة فى أن كل هذه الانظمة تعتمد بصورة أو باخرى على اجراء "صافى القيمة" أو " التحويل الدفترى أو الاسمى" لنقل القيمة، وفى واقع الامر ، يتم استخدام هذه الانظمة فى اغلب الاحيان لتقديم خدمة مالية اساسية لبعض الجاليات المهاجرة، وتعد هذه الانظمة مضمونة إلى حد كبير، فضلا عن انها اقل تكلفة مقارنة بالبنوك التقليدية، اصف إلى ذلك انه يتم استخدامها فى بعض الاحيان للتهرب من صرف العملة الصارمة، وتقدم هذه الانظمة ايضا درجة من عدم المعرفة باسم المستخدم ، وهذه الخاصية الاخيرة – تقديم درجة من عدم المعرفة باسم المستخدم- دفعت البعض إلى استغلال هذه الانظمة فى اعمال غير مشروعة مدنيا وجنائيا.

وقد تناول الخبراء بالمناقشة – فى تقرير فريق عمل المهام المالية حول غسيل الأموال الصادر فى ٣ فبراير ٢٠٠٠ – نماذج رئيسية ثلاثة من انظمة التحويلات البديلة قد تستخدم فى غسل الأموال التى يكون الإنترنت احد وسائلها ، وهذه النماذج هى : (السوق السوداء لصرف عملة البيزو "BMPE" ، ونظام الحوالات المصرفية، والانظمة الصينية/ الشرق اوسطية"^(١٠٩)).

٣- استخدام الجهاز المصرفى (اون لاين) فى غسل الأموال:

تزايدت اعداد المؤسسات المالية التى تقدم الخدمات المصرفية أون لاين عبر شبكة الإنترنت فى الوقت الحاضر بصورة مذهلة، واثاء إجراء التدريبات

^{١٠٩}- ملخص تقرير فريق عمل المهام المالية حول غسل الأموال (FATF) الحادى عشر (١٩٩٩-

٢٠٠٠) ٣ فبراير ٢٠٠٠.

الرمزية للتقرير الثاني عشر لفريق عمل المهام المالية لغسيل الأموال (FATF) والصادر في ١ فبراير ٢٠٠١، كثرت المناقشات حول العمليات المصرفية أون لاين، مما قد اثار العديد من الاهتمامات التي تداولت اثناء التدريب فى عام ٢٠٠٠، وعلى ذلك، فقد قيل أن الصفقات المالية التي تتم من خلال الإنترنت لا تشكل اى خطر على عملية غسل الأموال، ومع ذلك، فإن هناك ثلاث سمات خاصة للإنترنت قد تساهم من جانبها فى اثارة عدد من المخاطر التقليدية لغسل الأموال، منها:

- أ- تسهيل الاتصال من خلال الإنترنت
- ب- تبدد صفة التواصل بين العميل والمؤسسة
- ج- الاسراع فى اجراء الصفقة الإلكترونية.

وبعيدا عن الخلافات والمناقشات التي دارت فى الاجتماع الحادى عشر والثانى عشر لمجموعة العمل المالى الدولية (FATF) حول مدى توافر أو عدم توافر عميات غسل الأموال عن طريق استخدام الخدمات المصرفية اون لاين عبر شبكة الإنترنت، فقد استطاعت بعض الهيئات التشريعية - اثناء الاجتماع الثانى عشر لفريق عمل المهام المالية لغسل الأموال (FATF) - عرض عدد من القضايا التي من خلالها اصبح غسل الأموال مطبقا اعتمادا على نفس الوسائل المستخدمة فى قضايا الاحتيال الاخرى، ويستفيد مرتكبي تلك القضايا من نوعية التواصل من خلال الإنترنت، ولعل من اهم الطرق المستخدمة فى غسل الأموال عن طريق شبكة الإنترنت انشاء شركة للدفع عبر هذه الشبكة، وعلى ذلك فان القائم بعمليات غسل الأموال يعتمد على تلك الخدمات، ويقوم بالسداد عن طريق استخدام كروت الائتمان أو الاقتراض بضمان الحسابات وخاصة فى مناطق الجريمة المتصلة، وتقوم الشركة التابعة للقائم بعمليات غسل الأموال باعداد فاتورة لشركات كروت الائتمان والتي من جانبها تقوم بسداد قيمة الخدمات التي حصلت عليها، والشركة من ناحية اخرى تجد مبررا تلك المدفوعات، ومن خلال هذا النموذج يتضح أن القائم بغسل الأموال يتحكم فى الأموال المدفوعة والشركة التي تقدم الخدمة عبر الإنترنت، اما عن شركات كروت الائتمان وشركات الإنترنت وسداد الفواتير، والبنك الذى يبدأ فى تنفيذ الاجراءات اللاشريعة، فان كلا منهم يعد مسنولا عن جزء من تلك العملية (عملية غسل الأموال غير المشروع) وفى واقع الامر، فان تلك العملية تتشابه مع عمليات الاحتيال مع

وجود بعض الاختلافات، حيث انه فى عملية الاحتيال نجد أن حسابات البنوك تنتمى لطرف ثالث برئ بدلا عن منفذ العملية.

ولعل من اهم المشاكل التى قد تواجه المحقق عند التطرق لتلك العملية هى صعوبة ادراك التواصل بين افراد العملية، حيث أن القائم بغسل الأموال يقوم من جانب بالاعتماد على بعض المتطابقات الخرافية أو الخيالية وذلك لتسجيل وجودة على الشبكة، وعند التأكد من الاستفادة القصوى التى تعود عليه من الاتصال السهل والمباشر بشبكات الإنترنت فى مناطق جغرافية عدة،- ومن ثم التأكد من ابتعاده التام عن نشاطاته الاجرامية التى يقوم بها- سيكون على دراية وعلم بتفاوت التشابه فى اهم تسجيلات التواصل عبر شبكات الإنترنت التى يوفرها مقدمو الخدمة، وهذا بدوره سيجعل تسمية المحقق للعملية صعب للغاية، هذا بالاضافة إلى أن مكونات العملية ستكون مجزأة مما سيجعل الامر صعبا لتحديد ما إذا كان النشاط غير المشروع ذو اساس فعلى ام لا بغض النظر عن الادراك الكلى للعملية.

خلاصة القول، فإن المجرم الذى يعتمد على شبكة الإنترنت يستفيد من بعض عناصر هذا النظام، مما يؤكد غموض الامر امام المحققين.

٤- المقامرة عبر شبكة الإنترنت :

تعد المقامرة عبر شبكة الإنترنت بمثابة خدمة جيدة للتستر على عمليات غسل الأموال التى تتم عبر هذه الشبكة، وهناك ادلة ضمن تشريعات فريق عمل المهام المالية لغسيل الأموال (FATF) يتضح من خلالها أن المجرمين يعتمدون كليا على المقامرة عبر الإنترنت من اجل ارتكاب جرائم اخرى وغسل الأموال الناجمة عن ارتكاب تلك الجرائم.

وبالرغم من المحاولات المتعددة للتعامل مع جرائم المقامرة عبر شبكة الإنترنت- سواء عن طريق التحكم أو منح التراخيص أو الحظر الكلى- فقد تزايد ارتكاب تلك الجرائم بصورة كبيرة، فعلى سبيل المثال ، يتم اجراء الصفقات من خلال كروت الائتمان من ناحية، فى حين أن استبدال بعض مواقع المقامرة يجعل عمليات التشغيل والمتابعة للاطراف الاخرى وفريق عمل المهام المالية لغسيل الأموال (FATF) نحو تتبع تلك الجرائم اكثر صعوبة أن لم يكن مستحيلا، علاوة على ذلك فإنه يتم رصد صفقات المقامرة لاهميتها وادارتها من خلال الإنترنت- حيث انها تعتمد اساس على البرمجة- ولكن هذا الأمر قد يواجه صعوبات فى جمع المعلومات والادلة

الخاتمة

كانت الغاية من هذه الدراسة، " جرائم الحاسب الآلي - دراسة تحليلية " إلقاء الضوء على هذا النوع من الجرائم . وقد رأينا من خلال هذه الدراسة، كيف أصبحت الجريمة المعلوماتية بمختلف أبعادها وأشكالها جريمة العصر، حيث تعاضمت قوتها وخطورتها، لمواكبتها حركة التطور في شتى المجالات العلمية والتكنولوجية، واستطاعتها الاستفادة التامة من الثورة التكنولوجية في مجال الاتصالات والمواصلات. لذا فهي أمر واقع فرض وجوده على رجال الفقه والقانون، لما يميزها من خصائص عن غيرها من الجرائم موضوع القوانين الجنائي والقوانين الأخرى، وأصبحت من الموضوعات الساخنة المتداولة في المحافل الدولية والمؤتمرات الإقليمية، للبحث عن الصيغة المثلى والأسلوب الفعال تجاه مواجهة هذا النوع من الجرائم، بالنظر لجسامة الأضرار والأخطار المترتبة عن تزايد حجم نشاطها وتغلغلها في كافة أرجاء المعمورة. والواقع أن هذه الدراسة ليست من السهولة بمكان، حيث يمكن القول

بأن

ثورة الإتصالات والمعلومات أفرزت وسائل جديدة للبشرية تجعل الحياة أفضل من ذي قبل، إنما فتحت الباب على مصراعيه لظهور صور من السلوك المنحرف إجتماعيا لم يكن من الممكن وقوعها في الماضي وتخرج عن دائرة التجريم والعقاب القائمة ولأن المشرع لم يتصور حدوثها أصلا .

فمن جهة أولى أتاحت نظم الكمبيوتر ظهور صور جديدة من الجرائم لم تكن موجودة في الماضي، وذلك مثل سرقة المعلومات والأسرار المودعة في قواعد المعلومات، ومن جهة ثانية أتاحت هذه النظم الفرصة لإرتكاب الجرائم التقليدية بطرق غير تقليدية كما في جرائم الغش واتلاف وفساد المعلومات المخزنة في قواعد المعلومات .

ويمكن القول أن ظاهرة الجريمة المعلوماتية اليوم، أصبحت محور اهتمام الكافة من دول ومنظمات بأنواعها، بل هي حديث الناس في المنازل والأماكن العامة، والجميع يرى الظاهرة من وجهة نظر مختلفة، وأزعم أنني من خلال هذه الدراسة قد حاولت إلقاء الضوء على هذه الظاهرة، كمحاولة جادة للتعرف على الجوانب العديدة والمتشعبة لهذا النوع من الجرائم، واحسب أنني حاولت من خلال استخدام المنهج التحليلي لهذه الجريمة التوصل إلى أمور قد

تساعدنا على إستجلاء الموقف بطريقة مناسبة تقود إلى الإدراك والإلمام بالجوانب المرتبطة بهذه الجريمة ،

نظرا لأن هذه الجريمة تتميز بعدة خصائص لعل أبرزها ما يلي :-

- لا يتم فى الغالب الأعم الإبلاغ عن جرائم الإنترنت إما لعدم إكتشاف الضحية لها وإما خشيته من التشهير , لذا نجد أن معظم جرائم الإنترنت تم اكتشافها بالمصادفة ، بل وبعد وقت طويل من ارتكابها علاوة على أن الجرائم المكتشفة هى أقل بكثير من تلك التى لم تكتشف بعد ، فالفجوة بين عدد هذه الجرائم الحقيقى وما تم اكتشافه فجوة كبيرة .
- من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقنى كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبها .
- هذا النوع من الإجرام لا يترك أثرا له بعد ارتكابها علاوة على صعوبة الإحتفاظ الفنى بآثارها إن وجدت , فهذه الجرائم لا تترك أثرا فليست هناك اموال أو مجوهرات مفقودة إنماهى أرقام تتغير فى السجلات ولذا فإنة معظم جرائم الإنترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها
- تعتمد هذه الجرائم على قمة الذكاء فى ارتكابها ويصعب على المحقق التقليدى التعامل مع هذه الجرائم إذ يصعب عليه متابعة جرائم الإنترنت والكشف عنها وإقامة الدليل عليها فهى جرائم تتسم بالغموض وإثباتها من الصعوبة بمكان والتحقيق فيها يختلف عن التحقيق فى الجرائم التقليدية
- الوصول إلى الحقيقة بشأنها يستوجب الإستعانة بخبرة فنية عالية المستوى
- عولمة هذه الجرائم يودى إلى تشتيت جهود التحرى والتنسيق الدولى لتعقب مثل هذه الجرائم فهذه الجرائم هى صورة صادقة من صور العولمة فمن حيث المكان يمكن إرتكاب هذه الجرائم عن بعد , وقد يتعدد هذا المكان بين أكثر من دولة , ومن الناحية الزمنية تختلف المواقيت بين الدول , الأمر الذى يثير التساؤل حول تحديد القانون الواجب التطبيق على هذه الجريمة فئات الجناة فى هذا المجال تشمل فئات متباينة هى :-
 - أ- مستخدمو الحاسب بالمنازل
 - ب- الموظفون الساخطون على منظماتهم
 - ت- المتسللون ومنهم الهواة والعاثين بقصد التسلية

ث- المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته , وتقع أغلب جرائم الإنترنت حاليا تحت هذه الفئة

ج- العاملون في الجريمة المنظمة .

ومن الجدير بالذكر ان هذه الدراسة تمت على الوجه التالي :-

قامت الدراسة على ثلاثة فصول , وقد مهدت لها بتقديم عام حيث تضمن : أهمية دراسة جرائم الحاسب الآلي _ صعوبة الدراسة _ إختيار موضوع الدراسة _ منهج الدراسة _ خطة الدراسة .

وقد تناول الفصل الأول التأسيس التاريخي لتشريعات جرائم الكمبيوتر, وذلك من خلال تمهيد ومبحثين , حيث خصصت المبحث الأول للتأسيس التاريخي لتشريعات جرائم الحاسب الآلي ثم خصصت المبحث الثاني لمفهوم قانون الكمبيوتر , و من خلال المبحث الاول يتبين لنا ان محاولة تقصي التدابير التشريعية في مجال تقنية المعلومات يعني العودة الي السبعينات,فالتطور التاريخي لتقنية المعلومات يشير الي ان السبعينات تحديدا شهدت انتقالا حقيقيا في ميدان الحوسبة ,وتقاربها بانظمة الاتصالات .

و من خلال هذا المبحث ايضا توصلت الي ثلاث حقائق الاولي ان بداية قانون الكمبيوتر ارتبط بالبحث في المسؤولية عن أنشطة تتصل بالمعلومات ونظمها وتحديد في المجال الجزائي.

و الثانية ان الخصوصية و حماية البيانات تمثل اول مجال من مجالات قانون الكمبيوتر من حيث الاهتمام الدولي .

و الحقيقة الثالثة ان اكثر تشريعات قانون الكمبيوتر نضجا ووضوحا في اغراضها القوانين او التدابير التشريعية المتعلقة بحماية الملكية الفكرية لبرامج الكمبيوتر و يتصور ان تحقق هذه التشريعات حماية اوسع في السنوات القادمة في مجال اسماء مواقع الانترنت والمحتوى الرقمي لمواقع الانترنت.

و من خلال المبحث الثاني(مفهوم قانون الكمبيوتر)راينا ان المجالات التشريعية في هذا المجال تؤدي إلى تبلور قانون الكمبيوتر كإفرض مستقلة عن بقية الفروع القانونية وقد تطرقنا من خلال هذا المبحث الي ان اساس قانون الكمبيوتر و مبرر وجوده الحماية القانونية للمعلومات فان قصره علي جرائم الكمبيوتر المتصلة بحماية استخدام الكمبيوتر و مخزونه المعلوماتي و الحق في ملكية المعلومة ذات القيمة الاقتصادية اما بذاتها او بما تمثلة قد اغفل حماية اخري و انماط معلوماتية اخري فاغفل بذلك البيانات الشخصية مثلا واغفل

حماية انماط التعامل الالكتروني مع المعلومات و اغفل العلاقات العقدية في بيئة المعلومات و قصره ايضا علي حماية الملكية الفكرية يحقق الحماية فقط لاولوية المعلومات و اشكالها النهائية المنطوية علي عنصر ابداعي و يغفل حماية استخدام نظمها و يغفل حماية المعلومات ذات القيمة الاقتصادية و مثل هذا القول ينسحب علي اي رأي يحصر قانون الكمبيوتر بأحد مجالاته ليكون عاجزا عن شمول مفردات حماية المعلومات .

وبالفصل الثاني مدلول الجريمة المعلوماتية حيث ذهبنا إلى أن تعريف الجريمة المعلوماتية هو كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية .

وقد تناولنا هذا الفصل من خلال مبحثين خصصنا الأول لماهية المعلومات والثاني خصائص الجريمة المعلوماتية .

والفصل الثالث تقسيم جرائم المعلوماتية , حيث تناولت هذا الفصل من خلال مبحثين , خصصت الأول للجرائم التي تقع على الحاسب الآلي ومكوناته وخصصت الثاني للجرائم التي ترتكب بواسطة الحاسب الآلي ومكوناته .

وقد تناولت المبحث الأول من خلال ست مطالب على النحو التالي:

المطلب الأول: سرقة البرامج والمعلومات المخزنة آلياً.
المطلب الثاني: سرقة منفعة الحاسب الآلي أو الاستعمال غير المصرح به لنظام الحاسب الآلي.
المطلب الثالث: بعض أفعال تزوير المعلومات والبيانات والبرامج المخزنة آلياً والتلاعب بها.

المطلب الرابع: اختراق الحاسب الآلي وإنتحال هوية المستخدم.

المطلب الخامس: التجسس المعلوماتي

المطلب السادس: الإلتلاف المعلوماتي

أما المبحث الثاني فقد تناولته من خلال تسع مطالب على النحو التالي:-

المطلب الأول : الاحتيال المعلوماتي

المطلب الثاني : التزوير المعلوماتي

المطلب الثالث : النصب المعلوماتي

المطلب الرابع : جرائم الاعتداء على حرية الحياة الخاصة

- المطلب الخامس : جرائم الاعتداء على حقوق الملكية الفكرية والادبية.
 المطلب السادس : جرائم إفشاء الاسرار فى اطار المعلوماتية
 المطلب السابع : جرائم السب والقذف عبر الإنترنت.
 المطلب الثامن : الجرائم المخلة بالآداب العامة فى اطار المعلوماتية
 المطلب التاسع : غسيل الأموال عبر الإنترنت

وبما تقدم أكون قد فرغت من دراستى هذه وأحسب أننى لا أدعى بأن هذه الرسالة قد تناولت الموضوع من كل جوانبه نظرا لأن ذلك ليس بالعمل اليسير ولكن كل ما أتمناه أن أكون قد أضفت بهذه الدراسة ولو نقطة واحدة تظل مضيئة على مر التاريخ ومن خلال هذا البحث أزعم أن هناك بعض النتائج قد وضحت لنا ومنها حددنا بعض التوصيات ربما الأخذ بها قد يساهم فى سد نقص أو علاج ثغرة :

اولا : النتائج :-

- ١- مبدأ الشرعية الجنائية يفرض عدم جواز التجريم و العقاب عند إنتفاء النص , الأمر الذى يمنع مجازاة مرتكبى السلوك الضار أو الخطر على المجتمع بواسطة الكمبيوتر طالما أن المشرع الجنائى لم يقيم بسن التشريعات اللازمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب وبالتالي على المشرعين مواكبة التطورات وسن التشريعات اللازمة للتصدى لظاهرة الإجرام المعلوماتى .
- ٢- انعدام وجود تصور واضح المعالم للقانون والقضاء تجاه جرائم الإنترنت لكونها من الجرائم الحديثة , وتلك مشكلة أكثر من كونها ظاهرة ولانعدام وجود تقاليد بشأنها كما هو الشأن فى الجرائم الأخرى ويساعد ذلك انعدام وجود مركزية وملكية عبر الإنترنت .
- ٣- رغم صدور عدد من التشريعات العربية بشأن حماية الملكية الفكرية والصناعية التى تضمنت النص على برامج الحاسب واعتبرتها من ضمن المصنفات المحمية فى القانون إلا أنه مكافحة الجرائم المعلوماتية فى الدول العربية مازالت بلا غطاء تشريعى يحددها ويجرم كافة صورها , وإذا كان التشريعات العربية بصفة عامة قاصرة فى مجال ملاحقة صور السلوك الضار والخطر المتعلقة باستخدام الحاسوب (الكمبيوتر)

والإنترنت , فإن هذا القصور إنعكس مردوده على الجانب الإجرائي المتعلق بمكافحة الإجرام المعلوماتي , فلم تصدر تشريعات جنائية إجرائية كافية لتعقب مقترفي هذا الإجرام .

٤- تتعدد مظاهر القصور التشريعي التي يتعين أن تواجه كافة مظاهر السلوك السلبي المتعلقة بتقنية المعلومات , فالتشريعات مازالت ناقصة وقاصرة في مجالات عدة منها على سبيل المثال :

- التشريعات الخاصة بالملكية الفكرية فيما يتعلق بأسماء مواقع الإنترنت وعناصرها ومحتواها والنشر الإلكتروني , وفي حقل التنظيم الصحفي للنشر الإلكتروني
- تنظيم التجارة الإلكترونية والتشريعات الضريبية التي تغطي الميادين الخاصة بالضريبة في ميدان صناعة البرمجيات والأعمال على الإنترنت والتجارة الإلكترونية
- مقاييس إطلاق التقنية .
- القواعد التشريعية لنقل التكنولوجيا .
- التراخيص والإستثمار والضرائب المتعلقة بتكنولوجيا المعلومات .
- تنظيم حجية ومقبولية مستخرجات الحاسب .
- وسائل الإثبات التقنية والإثبات المدني .
- تنظيم الصور الإجرامية في ميدان الحاسب والإنترنت .
- أنظمة الدفع النقدي الإلكتروني .
- تنظيم عمل مقاهي الإنترنت .
- البرمجيات الصناعية .
- ٥- التفتيش على أجهزة الحاسوب : يجب أن تخضع لقواعد مختلفة عن القواعد العادية للتفتيش للبحث عن أداة الجريمة العادية , ورغم ذلك نجد أن التشريعات العربية في مجملها لم تحدد قواعد خاصة للتفتيش على الحاسبات الآلية وكيفية وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء إنتقالها , كما أن الإجراءات الجنائية للجهات القائمة على التفتيش غير حاسمة بشأن مسألة ضبط برامج الحاسب والمعلومات الموجودة بالأجهزة وفقا للشروط الخاصة بالإجراءات العادية للتفتيش .

- ٦- إذا كان المحقق مهمته البحث عن الحقيقة وإذا كان القاضي مهمته الفصل فيما يعرض عليه من منازعات , فعمل كلاهما يحتاج إلى بيئة قانونية تساعد على أداء الوظيفة , وهذه البيئة القانونية مازالت غامضة أو قاصرة ومواطن القصور والغموض متعددة منها :
- هل إعتداءات الأشخاص على الأموال فى البيئة الحقيقية يمكن تطبيق مفهومها على اعتداءات المجرم المعلوماتى ؟
 - هل المعلومات بذاتها لها قيمة مالية ؟ ام هى تكون كذلك عندما تمثل أصولا أو حقوقا ؟
 - كيف يمكن حماية السر التجارى أو الأسرار الشخصية وبيانات الحياة الخاصة من إعتداءات المجرم المعلوماتى أو المتطفل دون تصريح وإذن هل هناك معايير تحكم مقدمى خدمات الإنترنت بأنواعها ؟
 - ما مدى المسئولية القانونية فى حالة تحميل الملفات الموسيقية من الإنترنت بغير موافقة صاحب الموقع ؟
 - هل يعتبر النشر الإلكتروني من قبيل النشر الصحفى المنظم فى تشريعات الصحافة والمطبوعات ؟
 - هل إبرام العقد بالإنترنت تتوافر فيه سلامة وصحة التعبير عن الإرادة بالقدر الذى يوفره التعاقد الكتابى او الشفهى فى مجلس العقد العادى ؟
 - هل توقيع العقود والمراسلات إلكترونيا يتساوى مع توقيعها ورقيا ؟
 - هل ما يعتد به من دفع وإحتجاجات بشأن التزامات أطراف التعاقد أو علاقات الدفع التقليدية متاح بذاته أو أقل منه أو أكثر فى البيئة الرقمية؟
 - هل لرسائل البريد الإلكتروني حجية فى الإثبات؟ وهل لها ذات قيمة المراسلات الورقية ؟
 - هل الإنتخاب الإلكتروني هو تصويت صحيح ومقبول لمن إختارناه ممثلا لنا فى عالم المكان والجغرافيا ؟
 - هل العلامة التجارية محمية من أن تكون إسم بطلق لطرف آخر ؟
 - ماذا عن تصميم الموقع .. هل ثمة قدرة على منع الآخرين من سرقة واستخدامه ؟
 - ماذا إن تم ربط موقعك على الإنترنت مع موقع لا ترغب فيه ان يكون بينهما رابط ؟

- ماذا عن فرض المحتوى على المستخدم .. هل يظل المستخدم عاجزا لاحول له ولا قوة أمام تدفق مواد لايرغبها أو لا يطلبها على صندوق بريده او خلال تصفحه المواقع التي يريدتها ؟
- هل إغلاق المواقع ذات المحتوى غير المشروع فى بعض النظم والمشرع فى غيرها تجاوز على ديمقراطية العالم النخيلى ؟
- متى نشأ النزاع أيا كان وصفه أو مصدره فمن هو القاضى الرقمى ؟
- ما هو القانون الذى يحكم النزاع ؟ وما المحكمة ؟ وما المحكم ؟
- ما هى أخلاق المجتمع الرقمى وقواعد السلوك فيه .. هل ذاتها أخلاق العالم الحقيقى أم ثمة تباين فى المفهوم والقيود ؟
- هل ثمة قدرة للمستخدم أن يطالب بحقوق فى مواجهة الطرف الوسيط فى كل تعامل أو إستخدام نتج عنه مساسا بحق من حقوقه ؟
- من هو حاكم الإنترنت .. وما الدستور الذى يحكمه ومن الشرطى الذى يهرع له المستخدم إذا تعرض لإعتداء سافر على حقوقه أو بياناته أو محتوى موقعه أو رسائله أو خصوصيته ؟
- كيفية حماية برامج الحاسب ؟
- كيفية مقاضاة مزورى خدمة الإنترنت على إنقطاع الخدمة ؟
- مراقبة أداء الموظفين عبر البريد الإلكتروني ورسائلهم فى بيئة العمل
- هل إرسال رسالة مزاحة عبر البريد الإلكتروني يمكن أن تشكل جريمة جنائية وهل يمكن أن ترتب مسئولية مدنية ؟
- كل ما سبق يعد من قبيل الفراغ التشريع فى مجال مكافحة الجرائم المعلوماتية ومما لاشك فيه أن هناك أسبابا تستوجب سد هذا الفراغ منها:-
- ١- سهولة إخفاء الجريمة : فالجريمة المعلوماتية غالبا مستترة وخفية
- ٢- نقص خبرة الشرطة وجهات الإدعاء والقضاء
- ٣- صعوبة الوصول إلى مرتكبى أغلب الجرائم المعلوماتية
- ٤- صعوبة الإثبات وذلك يرجع إلى الطبيعة الخاصة للدليل فى الجرائم المعلوماتية وصعوبة الوصول إليه وسهولة محوه وكذا أدلة الإدانة ذات نوعية مختلفة فهى مغنوية الطبيعة
- ٥- إحجام الجهات والأشخاص المجنى عليهم عن الإبلاغ عن الجرائم المعلوماتية

٦- وجود العديد من الصعوبات الشديدة في ضبط وتوصيف الجرائم المعلوماتية .

ثانيا التوصيات :-

بعد ان عرضنا النتائج المستخلصة من الدراسة فإننا نرى لزاما أن نعرض الحلول المقترحة على النحو التالي :-

١- ضرورة تقنين قواعد جديدة لمكافحة الجرائم المعلوماتية تؤخذ بعين الاعتبار للطبيعة الخاصة بهذه الجرائم ولا سيما فيما يتعلق بالإثبات فى الدعاوى الناشئة عن هذه الجرائم سواء فى ذلك الدعاوى الجنائية والمدنية والتأديبية , كما ينبغى تعديل قواعد الإجراءات الجنائية لتلائم مع هذه الجرائم

٢- ضرورة التنسيق والتعاون الدولى قضائيا واجرائيا فى مجال مكافحة الجرائم المعلوماتية

٣- ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية , وذلك من رجال الشرطة المدربين مع أجهزة الحاسوب والإنترنت

٤- يتعين تدريب رجال النيابة العامة والقضاء بشأن التعامل مع اجهزة الحاسوب والإنترنت

٥- ينبغى أن تنص التشريعات العربية على أن الإنترنت من وسائل العلانية فى قانون العقوبات والقوانين ذات الصلة بالجرائم المعلوماتية مع الأخذ فى الاعتبار أن الإنترنت اوسع إنتشارا من وسائل نشر أخرى

٦- يجب تعديل قانون إجراءات الجنائية لبيان مايجب إتباعه من أحكام حال التفتيش على الحاسبات وعند ضبط المعلومات التى تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته

٧- ينبغى أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكتروني واية تقنية أخرى قد تفيد فى إثبات الجريمة والحصول على دليل والكشف عن الحقيقة

٨- ضرورة النص صراحة فى القوانين المنظمة للإثبات الجنائى والمدنى بما يسمح للقاضى بأن يستند إلى الأدلة المستخرجة من الحاسب الآلى والإنترنت , طالما أن ضبط هذه الأدلة جاء وليدة إجراءات مشروعة وتتم مناقشة هذه الأدلة بالمحكمة وبحضور خبير

٩- يجب إعتبار نشر وطباعة الصور الجنسية عن طريق الإنترنت مما يدخل ضمن زمرة جرائم الآداب

- ١٠- ضرورة تجريم استخدام الأطفال في تصوير أفلام تمثلهم في
أوضاع مخلة بالآداب العامة وعرضها على شبكة الإنترنت
- ١١- ضرورة تجريم الدخول غير المصرح به على البريد الإلكتروني
لإتلاف محتوياته
- ١٢- ضرورة نشر الوعي بين صفوف المواطنين وخاصة الشباب
بخطرات التعامل مع المواقع السيئة على شبكة الإنترنت
- ١٣- ضرورة إدخال مادة أخلاقيات استخدام الإنترنت ضمن المناهج
الدراسية في التعليم قبل الجامعي
- ١٤- ضرورة إنشاء قسم بكليات الحقوق للجرائم المعلوماتية وتشجيع
طلاب الدراسات العليا على الدراسة والبحث فيه
- وبذا أكون قد فرغت من هذه الدراسة (جرائم الحاسب الآلي -دراسة تحليلية)
ومنتهى املى وهدفى أن تكون قد حققت ما هو مستهدف منها وتكون إضافة
حقيقية يمكن الإستفادة منها فى هذا المضمار

والله ولى التوفيق ...

المراجع

- ١- د/ احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، ٢٠٠٠
- ٢- د/ اشرف توفيق شمس الدين - دراسة نقدية القانون مكافحة غسل الأموال الجديد- دار النهضة العربية ٢٠٠٣
- ٣- د/ سعيد عبد اللطيف حسن - إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت - (الجرائم الواقعة في مجال تكنولوجيا المعلومات) - دار النهضة العربية- القاهرة- الطبعة الأولى - ١٩٩٩
- ٤- د / حسن صادق المرصفاوى، قانون العقوبات الخاص، منشأة المعارف، الاسكندرية، ١٩٩١
- ٥- د/ على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى ، شرح قانون العقوبات " القسم الخاص " ، دار المطبوعات الجامعية، الاسكندرية، ١٩٩٩، الكتاب الثانى " جرائم الاعتداء على الانسان والمال
- ٦- عبد الرحمن صبرى ، غسيل الاموال فى اسواق المال الناشئة، مقالة منشورة بجريدة الاهرام، السنة ١٢٤، العدد رقم ٤١٢٥٨ بتاريخ ١١/٢٢/١٩٩٩ صفحة قضايا واراء.
- ٧- محمد أمين الرومى- جرائم الكمبيوتر والانترنت -دار المطبوعات الجامعية الاسكندرية ٢٠٠٣
- ٨- د/ محمد شامى الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، ط٢ دار النهضة العربية، ١٩٩٨
- ٩- د/ محمد الامين البشرى- التحقيق فى جرائم الحاسب الآلى - بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت-كلية الشريعة والقانون-جامعة الإمارات مايو ٢٠٠٥
- ١٠- د /مدحت رمضان- جرائم الاعتداء على الاشخاص والانترنت - دار النهضة العربية - ٢٠٠٠
- ١١- د/ نائلة محمد فريد - جرائم الحاسب الإقتصادية (دراسة نظرية وتطبيقية) دار النهضة العربية- القاهرة ، ٢٠٠٤
- ١٢- د / نبيل على- الثقافة العربية وعصر المعلومات، منشورات دار المعرفة، العدد ٢٦٥ يناير ٢٠٠١
- ١٣- د/ هشام محمد فريد رستم- قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة- أسبوط ١٩٩٤

١٤ - د/ هدى حامد قشقوش ، جرائم الحاسب الالكترونى فى التشريع
المقارن، دار النهضة العربية، القاهرة، ١٩٩٢

المراجع عبر الإنترنت :-

Mark Grossaman

على الانترنت حيث يهتم بقانون الكمبيوتر منذ عام ١٩٩٦-

www.mgrossmanlaw.com

The cyberlaw encyclopedia. <http://gahtan.com/techlaw>

Lawoffc@nol.com.jo

Ulrich sieber (legal aspects of computer – related crimes, eu comcrime, 1998). الكتاب الخامس من موسوعة القانونية وتقنية (المعلومات) دليل التجارة الدولية والاستثمار (اتفاقيات منظمة التجارة الدولية) عبر شبكة الانترنت www.law-d7.com

المراجع الأجنبية :-

- Barry B. Sookman, Sookman computer Law: Acquiring protecting Information Technology, Carwell Legal Pubns, April 2000.
- David Bainbridge- Introduction to computer Law, 5th edition, Finical Times Management, 2000.
- Emmanuel Michau, Computer Law in France, the computer law association, May 1998
- Ricardo Barretto & Ferreira da Silva, Computer Law in Latin America, The computer law Association, December, 1997.
- Vanessa Marsland, European Computer Law: An Introductory Guide, The computer law Association, December, 1996.
- Lawrence M Hertz, The computer and the law , Mathew

Bender & Company, 1999 USA.

- **Peter B. Maggs, Computer Law: Cases, comments, and Questions. West wads worth, 1996.**

- **Computer Law Forms Hand book, Clark Boardman Callaghan, 1995.**

- **John Zeleznikow. Dan Hunter, Building Intelligent Legal Information systems, little Brown & company, 1994.**

- **Reba A. Best, D. Cheryn Picquet, Computer law and software protection., Mcfarland & company, 1993.**

- **G.P.V Vandenberghe, Advanced Topics, of law and Information technology, kluwer Law International. July 1989.**

- **A.W.Koers, Knowledge Based Systems in Law, Kluwer law International. July 1989.**

- **Richard L. Bernacchi, Aguide to the Legal and Management Aspects of Computer Thechnology, little Brown & Company, 1986, (2nd edition 1993).**

- **Colin Tapper, Computer Law, Longman 1982 (first edition 1978).**

- **Daniel Brooks, Computer Law, Parctising Law Inst. 1982.**