جامعة العقيد الحاج لخضر – باتنة
كلية الحقوق و العلوم السياسية
قسم الحقوق

الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن

مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية

تخصص : قانون جنائي و علوم جنائية

إعداد الطالب :
معتوق عبداللطيف

إشراف الأستاذ الدكتور :
زرقين رمضان

أعضاء لجنة المناقشة

الاسم و اللقب	الدرجة العلمية	الجامعة الأصلية	الصفة
أ.د نواصر العايش	استاذ التعليم العالي	جامعة باتنة	رئيسا
أ.د زرقين رمضان	استاذ التعليم العالي	جامعة باتنة	مشرفا ومقررا
أ.د طاشور عبد الحفيظ	استاذ التعليم العالي	جامعة قسنطينة	عضوا مناقشا
د. بوهنتالة عبد القادر	استاذ محاضر	جامعة باتنة	عضوا مناقشا

السنة الجامعية 2011- 2012

شكر وتقدير

وأنا انهي كتابة هذه المذكرة، لايسعني إلا أن أتقدم بالشكر الجزيل إلى كل أساتذة قسم الدراسات العليا بجامعة باتنة اللذين رافقونا طيلة المشوار الدراسي فكانوا نعم الأساتذة وهم :

الأستاذة الفاضلة د. رحاب شادية و الأساتذة الأفاضل : د.بنيني احمد، د. سعادنة العيد، د. زرارة لخضر، و الأستاذ فاضل رابح ، وأخص بالشكر الوافر أستاذنا، الذي كان مرجعا لنا في القانون الجنائي الخاص ، والمشرف على إعداد المذكرة الأستاذ الدكتور زرقين رمضان، على ما قدمه لنا من توجيهات خلال ملتقى القانون الجنائي للأعمال ، و لا يفوتني أن اذكر استاذنا الدكتور بارش سليمان – رحمه الله– وأشكره على ما قدمه لنا من نصائح قيمة وحرصه و حثه لنا على مواصلة البحث في مجال القانون الجنائي والعلوم الجنائية .

كما أتقدم بالشكر إلى السيد رئيس لجنة المناقشة والأساتذة الافاضل أعضاء لجنة المناقشة على قبولهم مناقشة المذكرة و على ما بذلوه من جهد و وقت في سبيل تقويم هذه الدراسة.

فجزاهم الله عنا خير جزاء

اهداء

إلى والدي العزيز أطال الله في عمره ، عرفانا بفضله ووفاء لعهده

إلى والدتي العزيزة أطال الله في عمرها ،عرفانا بفضلها وتقديرا لها

إلى كل من يسعى لمكافحة الجريمة

أهدي هذا العمل

مقدمة

تميزالعصر الحالي بظهور الحاسبات الآلية ، التي تعد أهم اختراع عرفته البشرية على مر عصورها، حسب اعتقاد العديد من الباحثين ، وبالأخص علماء الاجتماع ، فقد كان لصناعة الحاسبات الآلية الفضل الأساسي في التطور الرهيب الذي حدث في العديد من مجالات البحث العلمي، وهذا راجع لما توفره هذه الأجهزة من سرعة و دقة في التحليل ، فضلا عن معالجة المعلومات وتخزينها وإعادة استرجاعها في وقت وجيز. [1]

ومما زاد من أهمية الحاسب الآلي في الحياة العصرية ظهور الشبكة الدولية للمعلومات المعروفة باسم الانترنت، بما تتيحه من إمكانية الاتصال الخارجي و تبادل المعلومات بشكل فعال مما أسفرعن تدفق للمعلومات في مختلف المجالات الحيوية كان نتيجتها نقل المجتمع البشري إلى عصر المعلومات فصار يطلق عليه عند علماء الاجتماع بمجتمع المعلومات. [2]

و مع التقدم السريع الذي عرفته صناعة الحاسبات الآلية و سهولة الولوج إلى شبكة الأنترنت ، ازداد الاعتماد عليها في مختلف المعاملات و الخدمات الالكترونية وتبادل المعلومات والمعارف ، حيث برز إلى الوجود مجال جديد للاتصال واسع الأرجاء يتمثل في الفضاء الافتراضي الذي يحتوي على كم هائل يتجاوز الملايير من الصفحات من المعلومات و الوثائق العلمية و الأدبية و السياسية و التاريخية و التجارية و المواقع الخدماتية بمختلف أشكالها ، يلتقي فيه كل من يرغب في ذلك، سواء على مستوى الأشخاص أو الشركات و المؤسسات، فيتسنى من خلال هذا الفضاء الافتراضي تبادل الأفكار و المعلومات و الآراء بكل حرية ، كما يمكن أن تتم عبره التحويلات المالية من سحب وإيداع عبر البنوك الالكترونية ، وكذلك عقد اكبر الصفقات التجارية التي تتم دونما الحاجة إلى إجراء تنقلات أو لقاءات، بل كل ما تتطلبه هو بضع نقرات على لوحة المفاتيح للحاسب الآلي.
و تشير بعض التقديرات الصادرة عن منظمة التعاون الاقتصادي و التنمية (OCDE) إلى أن قيمة المبادلات التجارية في العالم ، و التي تتم عبر شبكة الانترنت أو ما يعرف بالتجارة الالكترونية ، قد تجاوزت 400 مليار دولار عام 2000 وهو ما يعادل عشرة أضعاف ما تم تداوله مقارنة بعام 1998 وتقفز هذه القيمة لتبلغ 8500 مليار دولار عام 2005 . [3]

وبالمقابل فقد كان لانتشار استعمال الحاسب الآلي بين الأشخاص وتوسع فئات مستخدميه ، مع ما تتيحه تقنية الانترنت المذهلة من تيسير تبادل المعلومات والاستفادة من توظيفها في ميادين مختلفة، أن أدى إلى ظهور أنماط جديدة من الجرائم اتخذت من الفضاء الافتراضي ساحة لها وفرضت تحديات جديدة على المنظومة القانونية . ومما ساهم في تطور صور الإجرام المعلوماتي عدم مواكبة التشريعات في كثير من دول العالم لهذا الشكل من الإجرام مما أحدث فراغا تشريعا وثغرات قانونية مكنت مرتكبي هذه الجرائم من الإفلات من المتابعة و العقاب في كثير من الأحيان .

---

[1] Zanella (Paolo), Architecture et technologie des ordinateurs, Bordas, Paris, 1989, p.15.

[2] Masuada (Yoneji), The Information Technology Revolution, Oxford Blackwell, Oxford ,1985, p. 620.

[3] دراسة منشورة بتاريخ 06/06/ 2001 في الموقع : http://www.oecd.org تحت عنوان :

Garreau(Alain), Les effets du Commerce Eléctronique sur les transports, Paris ,p. 6 .

وباعتبار أن عدم مواكبة التشريعات في كثير من دول العالم لهذا التطور السريع لأشكال الجريمة ،أن أدى إلى حدوث فراغ تشريعي و ثغرات قانونية مكنت مرتكبي هذه الجرائم من الافلات من المتابعة و العقاب في كثير من الأحيان ، وساهم ذلك في تنامي صور الاجرام المعلوماتي ، حيث صارت الدول التي لم تضع قوانين خاصة لمكافحة الجريمة المعلوماتية قواعدا تنطلق منها الهجمات الالكترونية لتهدد أمن و سلامة الأفراد وتعتدي على شرفهم و تمس خصوصياتهم ، بل و تتجاوز ذلك لتضع استقرار اقتصاد الدول و أمنها القومي امام تحديات بالغة لارتباطها مع كافة اشكال الجريمة و امتيازها بخصوصيات تجعل من امر متابعتها في غاية التعقيد.

أهمية ودواعي اختيار البحث :

تتجلى أهمية البحث المستمر في جرائم المعلوماتية في أن هذا النوع المستجد من الإجرام مرتبط بالتقنية الحديثة المتمثلة في الحاسب الآلي و شبكة ألانترنت ، و التي هي في تطور دائم مما يفرض على المشرع الجنائي مواكبة هذه الظاهرة مع إيجاد الحلول التشريعية لمكافحتها، وعدم الاكتفاء بالنصوص التقليدية التي أضحت عاجزة سواء من الناحية الموضوعية، باعتبار أن الإجرام المعلوماتي يطال حقوقا غير مادية (المعلومات، البيانات، المعطيات الشخصية ، التجارة الالكترونية....،الخ) أو من الناحية الإجرائية وما تثيره من صعوبات تتمحور حول إثبات الجريمة أو القانون الواجب التطبيق أو المحكمة المختصة في نظر هذه الجرائم وكذا حتمية التعاون الدولي في هذا المجال.

و قد انضمت الجزائر مؤخرا إلى ركب الدول التي وضعت تشريعات بهذا الخصوص، فقد تم مواجهة هذا النوع من الإجرام من خلال صدور القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات و الذي نص على حماية جزائية للأنظمة المعلوماتية والذي تم تعزيزه بالقانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها ، وعلى الرغم من أهمية صدور هذه القوانين الأخيرة ، إلا أنه لا يمكننا القول باكتمال البنية التشريعية في الجزائر في مجال مكافحة جرائم المعلوماتية .

وانطلاقا من أهمية دراسة هذا النوع المستجد من الجرائم ارتأينا أن نعالج موضوع جرائم المعلوماتية من خلال التطرق إلى أهم صورها وكذا القوانين المقارنة التي تصدت للإجرام المعلوماتي لنتبين النقائص التي يجب على المشرع الجزائري تداركها ليكتمل الاطار القانوني لمكافحة هذه الجرائم.
كما يتسنى لنا من خلال هذه الدراسة معرفة بعض الثغرات القانونية التي تحول دون مكافحة هذه الجرائم بالشكل المناسب ، و باتباع الوسائل الأمنية الحديثة و الاجراءات الوقائية الفعالة دون المساس بحقوق و حريات الأفراد في نقل و تبادل المعلومات عبر شبكة الأنترنت .

ومن خلال البحث في دور التشريعات الجنائية الحالية الوطنية منها و الدولية في الحد من انتشار الجريمة المعلوماتية باعتبارها جريمة ذات بعد دولي و مرتبطة بالتطور التكنولوجي المستمر للحاسب الآلي وشبكة الانترنت ، يتضح لنا مدى الصعوبات التي تعترض رجال القانون و تضع الجهود المبذولة لمكافحتها في مواجهة تحديات مستمرة.

ومن المؤكد أن البحث في مجال جرائم المعلوماتية لا يخلو من صعوبات تعترض الباحث خلال الدراسة و جمع المعلومات و تحليلها ، ولعل أبرز هذه الصعوبات تكمن في الطابع التقني لهذه الجرائم ، من هنا تتبين لنا ضرورة الإلمام بالمصطلحات التقنية الخاصة بـأجهزة الحاسب الألي من مكونات مادية و معنوية وبرامج

تشغيل و برامج تطبيقية ، وكذا مراحل القيام بهذه الجرائم وكيفية تأثير الفيروسات بمختلف أنواعها على جهاز الحاسب الألي من خلال تخريب النظم المعلوماتية ، بالإضافة إلى خطوات متابعة واثبات هذه الجرائم ، كل هذه التعقيدات تحتم على الباحث أن يختار بعناية فائقة مصادر المعلومات سواء التقنية أو القانونية .

ولعل عزائي كان في تعدد هذه المصادر خاصة الأجنبية منها نظرا لما حظيت به جرائم المعلوماتية من اهتمام بسبب انتشارها في هذه البلدان المتطورة التي تعتمد على الوسائط الإلكترونية في مختلف ميادين الحياة بخلاف الدول النامية التي لا زالت لم تصل الى هذا المستوى من استخدام تكنولوجيات الاعلام و الاتصال.

أما في الجانب القضائي فإن قلة الأحكام الجزائية الخاصة بجرائم المعلوماتية الصادرة عن محاكم جزائرية ، وصعوبة الحصول عليها إن وجدت ، جعلنا نعتمد في معظم الحالات على ما تصدره الأجهزة القضائية الأجنبية وبالأخص الفرنسية منها .

إشكالية البحث:

تكمن الإشكالية التي نحن بصدد معالجتها في هذا البحث في مدى كفاية ونجاعة القوانين الحالية في مكافحة جرائم المعلوماتية والانترنت في ظل اختلاف وعدم انسجام التشريعات على الصعيد الدولي، حيث مازالت بعض الدول تعتمد على النصوص السارية على الجرائم التقليدية كالسرقة ، النصب و الاحتيال والتزوير وغيرها من الجرائم على الرغم من الاختلاف بين النوعين ، وكذلك عدم إمكانية تطبيق النصوص الموضوعية أو الإجرائية التقليدية على جرائم المعلوماتية ، فعدم وجود إستراتيجية تجريم ومتابعة دولية موحدة لتعزيز التعاون الدولي، يقلل من فرص تطويق ظاهرة الإجرام المعلوماتي ويحد من فاعلية النصوص التشريعية الوطنية للوقاية والتصدي لهذه الظاهرة.

المنهج المتبع في الدراسة :

خلال دراستنا لهذا النوع من الإجرام ارتأينا ان نعالج الإشكالية المطروحة وفق منهج تحليلي مقارن حيث من خلال هذا المنهج يتسنى لنا إجراء دراسة مقارنة لأهم الأنظمة القانونية للدول التي أصدرت تشريعات في هذا المجال وتقييم مدى اكتمال البنية التشريعية لهذه الدول بشأن مواجهة جرائم المعلوماتية.

خطة الدراسة :

رأينا أن نستهل دراستنا بمبحث تمهيدي نخصصه لدراسة مفهوم الجريمة المعلوماتية ، ثم نعرض في الفصل الأول الأحكام العامة للجريمة المعلوماتية من خلال دراسة آليتها ووسائلها وأركانها ، في حين نخصص الفصل الثاني لصور جرائم المعلوماتية مع شرح عناصرها ومناقشة أهم ما صدر في التشريع و القضاء المقارن من قوانين و أحكام بغرض التصدي لهذه الجرائم ، على أن نتناول في الفصل الثالث التطور التشريعي لمكافحة جرائم المعلوماتية في الجزائر من خلال دراسة القوانين الاجرائية و الموضوعية الصادرة بهذا الخصوص .

وبناءا عليه ارتأينا أن تكون الخطة المتبعة على النحو التالي :

مبحث تمهيدي: مفهوم الجريمة المعلوماتية

المطلب الأول: تعريف الجريمة المعلوماتية

المطلب الثاني: خصائص الجريمة المعلوماتية و سمات الجاني و المجني عليه

الفصل الأول: القواعد العامة للجريمة المعلوماتية

المبحث الأول: آلية الجريمة المعلوماتية، محلها و وسائلها

المبحث الثاني: أركان الجريمة المعلوماتية

المبحث الثالث: أحكام الشروع، المساهمة والمسؤولية الجنائية في الجريمة المعلوماتية

الفصل الثاني: صور الجريمة المعلوماتية ومكافحتها في القوانين المقارنة

المبحث الأول: صور جرائم الحاسب الآلي

المبحث الثاني: صور جرائم الانترنت

المبحث الثالث: مكافحة الجريمة المعلوماتية في القوانين المقارنة

الفصل الثالث: مكافحة الجريمة المعلوماتية في التشريع الجزائري و الحلول المقترحة لمواجهة تحديات الإجرام المعلوماتي

المبحث الأول: القواعد الإجرائية في متابعة و إثبات الجريمة المعلوماتية حسب القانون الجزائري

المبحث الثاني: التطور التشريعي لمكافحة الجريمة المعلوماتية في الجزائر

المبحث الثالث: الحلول المقترحة لمواجهة تحديات انتشار الإجرام المعلوماتي

مبحث تمهيدي
مفهوم الجريمة المعلوماتية

أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية للجريمة المعلوماتية، ويرجع السبب في ذلك إلى تعدد وجهات النظر بخصوص مفهوم هذا النوع المستجد من الجرائم ، حيث ظهرت عدة اتجاهات فقهية في محاولة فهم المقصود بالجريمة المعلوماتية و تحديد تعريف لها مع تبيين طبيعتها القانونية ، كما أن تعريف الجريمة المعلوماتية يستوجب الإلمام بالجانب الموضوعي و الإجرائي لها ، مع دراسة العوامل المختلفة التي تتداخل في تكوين الجريمة والإحاطة بالأمور الفنية لها.

وعليه سنحاول من خلال المبحث التمهيدي أن نتطرق إلى مفهوم الجريمة المعلوماتية ، حيث نعرض في المطلب الأول مختلف التعريفات التي استخدمت لوصف وضبط خصائص هذا النوع من الإجرام ، مع تبيين المعايير التي استند عليها الفقهاء في تعريفهم للجريمة المعلوماتية ، وكذا الغرض الذي توخاه المشرع من تجريم هذا النمط من السلوك ، ومن خلال إعطاء صورة عن حجم الجريمة وانتشارها في العالم وكذا دوافع ارتكابها يتضح لنا سبب الاهتمام المتزايد لمكافحة هذه الجرائم.
ولا يكتمل البحث في مفهوم الجريمة المعلوماتية دون البحث في خصائصها ، و تحديد سمات الجاني أو ما يعرف بالمجرم المعلوماتي ، و تصنيف فقهاء القانون الجنائي لفئاته المختلفة ، وهو ما سنتطرق إليه في المطلب الثاني.

المطلب الأول
تعريف الجريمة المعلوماتية

إن البحث في إيجاد التعريف المناسب للجريمة المعلوماتية تكتنفه العديد من الصعوبات ، ويرجع السبب في ذلك إلى عدم توصل الفقهاء إلى وضع مفهوم شامل يحدد ماهية الجرائم المعلوماتية ويحصر نطاقها، ليس هذا فحسب ، بل أن تعدد مسمياتها عقد من محاولة فهم هذه الظاهرة الحديثة نسبيا واختيار التعريف المناسب لها ، فقد تنوعت التعبيرات الدالة على الجريمة المعلوماتية ، مما أدى ببعض المهتمين بها إلى القول أن هذه الجريمة مستعصية على التعريف مستدلين في ذلك بتعدد المحاولات التي بذلت من دون التوصل إلى تعريف موحد وكذا إلى استخدام "ملايين الكلمات من اجل ذلك" [1] ، أو كما قيل بشأنها أنها جريمة تقاوم التعريف . [2]
و مرد ذلك الى التطور السريع و المستمر الذي يشهده عالم المعلوماتية ، وكذا ما يرتبط به من تكنولوجيات الإعلام و الاتصال، فضلا عن اختلاف وجهات النظر حول العنصر الذي يستند عليه الفقهاء عند محاولة تعريف الجريمة المعلوماتية ، فبينما يتجه البعض إلى تضييق مفهومها و حصر نطاقها في الجرائم التي تتم على جهاز الحاسب الآلي أو داخل نظامه فقط ، أو تلك التي تتطلب معرفة عالية بتقنية المعلوماتية ، فإن البعض الآخر يوسع من مجال الجرائم المعلوماتية لتشمل كل سلوك إجرامي بمساعدة الحسب الآلي .
وهذا ما سنقوم بعرضه فيما يلي كما نتطرق الى تقدير حجم الخسائر التي تسببهاالجرائم المعلوماتية في العالم .

---

[1] هشام محمد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، أسيوط ، 1995، ص 29 .

[2] محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، القاهرة، 1994، ص 5 .

الفرع الأول
محاولات تعريف الجريمة المعلوماتية والغاية من تجريمها

قبل أن نتناول مختلف التعريفات التي استعملت لتحديد مفهوم الجرائم المعلوماتية لابد من الإشارة إلى تعدد تسمياتها والتي قد تبدو للوهلة الأولى أنها تختلف من حيث دلالتها ، إلا أن معظمها يشير إلى نفس الظاهرة ، فبينما استعمل البعض اسم " الجرائم الإلكترونية "، فقد أطلق البعض الأخر اسم "جرائم الحاسب الآلي و الانترنت " أو "الجرائم المتصلة بالكمبيوتر" ، و"جرائم تكنولوجيا المعلومات" ، في حين هناك من فضل تسمية " جرائم المعلوماتية " وهناك من وجد في تسمية "جرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات " أكثر دلالة و مواكبة للتطور الذي يشهده عالم الإعلام والاتصال، وهذا المسمى استخدم في مشروع القانون العربي النموذجي الموحد الصادر عن جامعة الدول العربية سنة 2004 ، والذي اعتمده مجلس وزراء العدل العرب في الدورة التاسعة عشر بالقرار رقم 495-19 بتاريخ 2003/10/8 . [1]

كما انتشر اصطلاح " السيبر كرايم " أو" الجرائم السيبيرية" في المجال الأوروبي، ويقصد به جرائم العالم الافتراضي [2] ، للتمييز بين الجريمة المعلوماتية التي لاتحتاج الى وجود شبكة أنترنت عن الجريمة السيبيرية أو الجريمة الالكترونية ، التي تتطلب أكثر من جهاز حاسب الي متصلين عبر شبكة الانترنت .

أما عن سبب اختيارنا لتسمية " جرائم المعلوماتية " في هذا البحث فإنه راجع إلى كون الاصطلاح يجمع بين تقنية الحاسب الآلي أو المعلوماتية - Informatique- بما تشمله هذه التقنية من جهاز الحاسب وكافة ما يرتبط به من تقنيات و ابتكارات سواء في الوقت الحالي أو في المستقبل وكذا إمكانية الاتصال عبر شبكة الانترنت ، كما أن مصطلح المعلوماتية يدل على" تقنية التعامل مع المعلومات" [3] ، وبالتالي فان الاعتداء الذي يطال هذه المعلومات ، بما لها من طبيعة قانونية يشكل أهم عنصر في جرائم المعلوماتية .

وقد تبدو الحدود الفاصلة بين جرائم الحاسب الآلي وجرائم الانترنت واهية ، إذ لا تختلف الجريمتان إلا بوجود شبكة الإنترنت مع تداخل بين عناصر الجريمتين في غالب الأحيان ، إلا أننا صنفنا الجرائم المعلوماتية في الفصل الثاني الى جرائم الحاسب الآلي و جرائم الأنترنت من باب توضيح دور شبكة الأنترنت وكذا مساهمتها في تفاقم جرائم الحاسب الالي وظهور أنماط اكثر تطورا من الاجرام المعلوماتي .

سنقوم في هذا الفرع بعرض مختلف المحاولات التي بذلت لتعريف الجريمة المعلوماتية مع تقديم التعريف الذي نراه انسب ، كما نبين هدف المشرع من تجريم الاعتداء على الحاسب الآلي و شبكة الأنترنت أو الاعتداء الذي تستعمل فيه هذه الوسائل التكنولوجية.

---

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي،دار الكتب القانونية، القاهرة،2007 ، ص 35.

[2] خالد ممدوح إبراهيم ، أمن الجريمة الالكترونية، الدار الجامعية ، الإسكندرية ، 2008 ، ص 54.

[3] هشام محمد رستم ، المرجع السابق ، ص35 .

أولا- محاولات تعريف الجريمة المعلوماتية :

أ) الاتجاه الأول - تعريف الجرائم المعلوماتية بالاستناد إلى محل الجريمة :

يعتقد أنصار هذا الاتجاه أن الجريمة تعتبر جريمة معلوماتية عندما يكون جهاز الحاسب الآلي هو محل الجريمة ، أي أن يتم الاعتداء على الحاسب الآلي أو على نظامه ، حيث يضيق أنصار هذا الاتجاه من نطاق الجرائم المعلوماتية ويحصرونها في الحالات التي تكون فيه مكونات الحاسب غير المادية مثل البرامج و البيانات و المعطيات المخزنة في ذاكرة الحاسب محلا للجريمة ، كأن يتم سرقة أو تقليد أو إتلاف أو تعطيل برنامج الحاسب أو إفشاء محتوياته او حذف او تغيير او تزوير او نسخ المعلومات المعالجة .

لذلك فقد عرف "روزنبلات Rosenblatt " الجرائم المعلوماتية بأنها « نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه » [1].
كما عرفها البعض الاخر بأنها « غش معلوماتي ينصرف الى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها » [2] .
اما الفقيه الالماني "زيبر Sieber Ulrich" فقد اعتبر انه يدخل ضمن نطاق الجرائم المعلوماتية « كل تصرف غير مشروع يتعلق بالمعالجة الالية للمعطيات او نقلها» [3] .
في حين اشارت الدكتورة هدى قشقوش الى ان جرائم الحاسب الالي «هي مجموع الجرائم التي تتصل بالمعلوماتية » [4] ، حيث حصرت هذه الجرائم في الاعتداء على الاموال المعلوماتية التي هي عبارة عن الادوات المكونة للحاسب الالي وبرامجه ومعداته، حيث أننا نكون بصدد جرائم معلوماتية حينما تكون المكونات غير المادية للنظام من بيانات وبرامج مخزنة في ذاكرة الحاسب او المنقولة عبر شبكة الاتصال قد تعرضت لاعتداء بالسرقة او التزوير او ادعاء ملكيتها او تقليدها او اتلافها او تعطيلها.

ب) الاتجاه الثاني- تعريف الجرائم المعلوماتية بالاستناد إلى التحكم في تكنولوجيا المعلوماتية :

عرفت الجريمة المعلوماتية عند انصار هذا الاتجاه بانها « كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الالية بقدر كبير لازما لارتكابه من ناحية ، ولملاحقته وتحقيقه من ناحية اخرى» [5] .
اذ يرى انصار هذا الاتجاه ان الالمام بتكنولوجيا المعلومات و استخدام الحاسب الالي ضروري لادراج الجريمة المرتكبة ضمن الجرائم المعلوماتية ومن بينهم " ديفيد تومبسون David. Tompson " الذي عرف هذا النوع من الجرائم بقوله انها « اية جريمة يكون متطلبا لاقترافها ان تتوافر لدى فاعلها معرفة بتقنية الحاسب » [6] . كما قدم الفقيه"ستين سكيولبيرج Stein. Schiolberg " تعريفه لجرائم الحاسب بقوله « أي فعل غير مشروع تكون المعرفة بتقنية المعلومات اساسية لمرتكبه و التحقيق فيه وملاحقته قضائيا » . [7]

---

[1] Alexander (Michael) , Computer crime , Computer World , Vol XXIV, N°11,1990, p.104.

[2] علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب ، دار الجامعة الجديدة للنشر، الاسكندرية ، 1997 ، ص 2 .

[3] Lucas (André) et Deveze (Jean) , Le droit de l'informatique et de l'internet ,P . U, Paris, 2001, p.496.

[4] هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ،دار النهضة العربية ،القاهرة ، 1992، ص 5.

[5] Parker (Donn B.), Combattre la criminalité informatique, OROS ,Paris, 1985, p. 18.

[6] Thompson (David), Current trends, in Computer control crime, Computer Quarterly, vol 9N°1,1991, p.2.

[7] محمود احمد عبابنة ،جرائم الحاسوب و ابعادها الدولية ، دار الثقافة للنشر و التوزيع ،عمان ، 2005 ، ص 16 .

ج) الاتجاه الثالث - تعريف الجرائم المعلوماتية بالاستناد الى وسيلة ارتكاب الجريمة:

بخلاف الاتجاهين السابقين اللذين اعتمدا على محل الجريمة و ضرورة الإلمام بتكنولوجيا الحاسب الالي حتى يتم تصنيف الجريمة على أنها جريمة معلوماتية ، فان البعض الأخر قد وسع من نطاق هذه الجرائم و استند على وسيلة ارتكاب الجريمة ، حيث نجد أن الفقيه الألماني " تايديمان Tiedemann " قد عرفها بأنها « كل أشكال السلوك غير المشروع أو الضار بالمجتمعوالذي يرتكب باستخدام الحاسب الآلي».[1]

في حين عرفها البعض الاخر بانها « تلك الجرائم التي يكون فيها دور الحاسب ايجابيا اكثر منه سلبيا ».[2]
وقد ميز بعض الفقهاء بين مظهرين للسلوك الاجرامي في جرائم المعلوماتية حيث يكون استخدام الحاسب الالي إما من أجل ارتكاب جريمة أخرى بغرض الحصول على مكسب مادي ، أو أن يكون الغرض من الاعتداء هو إلحاق الضرر بالمجني عليه [3].
كما جاء في تعريف آخر« أنها فعل اجرامي يتم باستخدام الحاسب كاداة رئيسية » [4] .
وفي اطار التعريفات التي وسعت من نطاق جرائم المعلوماتية نذكر تعريف مجموعة من خبراء منظمة التعاون الاقتصادي (OCDE) التي اقترحت في اجتماع لها بباريس سنة 1983 ، تعريفا للجريمة المعلوماتية جاء فيه أنها «كل سلوك غير مشروع او غير اخلاقي او غير مصرح به يتعلق بالمعالجة الالية للبيانات او بنقلها» [5].
أما الاستاذ الامريكي " دافيد وال David Wall" فقد عرف الجريمة المعلوماتية بقوله « هي كل فعل غير مشروع يتعلق بشكل او باخر بالحاسب الالي» [6].

وبخلاف الاتجاهات السابقة التي تبنت معايير مختلفة لتعريف الجريمة المعلوماتية ، فقد برزت تعريفات لم تستند إلى معيار معين حيث نذكر تعريف الفقيه الفرنسي "ماسى Massé " الذي عرفها بقوله « الاعتداءات القانونية التي يمكن ان ترتكب بواسطة المعلوماتية بغرض تحقيق الربح » [7].

وعلى نفس المنوال جاء تعريف الخبير الامريكي " باركرParker"حيث قال بانها « فعل اجرامي ،ايا كانت صلته بتقنية المعلومات ،فيه يتكبد المجني عليه نتيجة له خسارة ويحقق الفاعل ربحا بصفة عمدية » [8].

---

(1) Tiedemann (Klaus), fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, Rev.Dr.Pén.Crim n°7,Bruxelles, 1984, p 61.

(2) Totty (Richard) &Hardcastle (Antony) ,Computer -Related Crime in information technology and the law, Macmilla Publishers, U.K.1986, p 26.

(3) Wasik (Martin) ,Crime and The Computer ,Oxford University Press,1991 ,p 2.

(4) Ball (Leslie D),computer crime,in'' The information technology revolution'',Cambridge ,1985p 543.

(5) Alterman(H.) et Bloch(A.) : La Fraude Informatique (Paris, Gaz. Palais), [3 sep. 1988] p. 530.

(6) WALL (David), Crime and the Internet, Routledge, N.Y, 2001, p. 3.

(7) Massé (Michel), Infractions contre l'ordre financier, Rev .sc .crim, Janvier 1985 N°1, p 107 .

(8) Parker (Donn B.), Figting Computer Crime "A new Framework for Protecting Information", Joh Wiley and sons, 1998, p 112.

د) - نقد التعريفات السابقة واختيار التعريف الانسب للوضع الراهن للجريمة المعلوماتية

يبدو من خلال استعراض مختلف التعريفات عدم وجود معيار متفق عليه لتحديد نطاق الجرائم المعلوماتية ، فانصار الاتجاه الذي يرى ضرورة أن يتم الاعتداء على الحاسب الآلي من خلال العبث بمكوناته غير المادية من أنظمة وبيانات قد ضيقوا إلى حد كبير من نطاق الجرائم المعلوماتية ، مما يجعل قسما كبيرا من السلوكيات غير المشروعة التي تستخدم الحاسب الالي تخرج عن نطاق الجرائم المعلوماتية مثل جريمة الاحتيال المعلوماتي وغيرها .

أما القائلون بضرورة إلمام الجاني بتكنولوجيا الحاسب الآلي لتكييف الاعتداء بأنه جريمة معلوماتية فيمكن اعتبار هذا الرأي نسبيا في اعتقادنا، إذ أن بعض الاعتداءات تستوجب بالفعل تحكما كبيرا في تكنولوجيا الحاسب الآلي وملحقاته ، لكن على الرغم من ذلك فان أفعالا غير مشروعة كثيرة لا تتطلب مهارة و قدر من العلم كعملية إتلاف البيانات المخزنة مثلا .

كما يمكن توجيه النقد إلى أنصار الاتجاه الذي يستند على اتخاذ الحاسب كوسيلة في ارتكاب الجريمة من عدمه ، فيمكن القول بأنه لا ينبغي تجريم السلوك بناءا على الوسيلة ، فقد اعتمد هؤلاء معيارا فيه توسع كبير لنطاق جرائم المعلوماتية ، فمجرد استعمال الحاسب في الجريمة يجعل منها جريمة معلوماتية ، وهذا الأمر قد يدخل الالتباس من حيث تصبح جرائم عادية أو تقليدية استعمل فيها الحاسب الآلي جرائم معلوماتية ، وهذا غير منطقي فجرائم مثل سرقة الحاسب الآلي أو احد مكوناته المادية تبقى جرائم تقليدية ، أو الجرائم التي يستعمل فيها الحاسب لطباعة مستند ما أو تزوير محرر تبقى جرائم تقليدية ولا تدخل ضمن نطاق الجرائم المعلوماتية .

كما أن الذين رأوا أن الغرض من ارتكاب الجرائم المعلوماتية هو دوما تحقيق الربح المادي فقد اهملوا دوافع كثيرة تحفز الجناة على هذا السلوك الاجرامي باعتبار أن العائد المادي ليس بالضرورة هو الدافع للقيام بالاعتداء وسوف نرى ذلك من خلال تطرقنا لدوافع ارتكاب الجرائم المعلوماتية لاحقا.

ووفقا لهذه الاسباب ، نعتقد أن التعريف الانسب لجرائم المعلوماتية والأصلح لوصف الجرائم المعلوماتية في الوضع الراهن يجب أن يأخذ بعين الاعتبار عدة معايير، فالسلوك المكون للواقعة الاجرامية، والذي يجب أن يكون بصورة فعل ينهي عنه القانون أو امتناع عن فعل يأمر به القانون ، كما يجب أن يقع هذا السلوك اعتداءا على مصلحة محمية جنائيا ،حيث يتنوع السلوك في الجريمة المعلوماتية من اعتداء على أموال معنوية ، أو على حرمة الحياة الخاصة و يصل حتى إلى القتل و هذا ما سنوضحه في الفصل الثاني عند دراستنا لصور الجريمة المعلوماتية ، مع ضرورة ابراز علاقة السلوك الاجرامي بالحاسب الآلي وملحقاته و ما يتعلق بهما من تكنولوجيا الاعلام و الاتصال ، مع عدم ربط النص التشريعي الجنائي بالتكنولوجيا التي تشهد تطورا متلاحقا بل يجب أن يستوعب صورا جديدة للجريمة المعلوماتية قد تظهر مستقبلا ، و يتاتى ذلك من خلال التركيز على الغاية أو الغرض من هذه التكنولوجيا و الاهداف المرجوة منها.

ثانيا- الغاية من تجريم الافعال التي تشكل جرائم معلوماتية :

طرحت الغاية من تجريم الاعتداء على النظم المعلوماتية إشكالا يتعلق بالمصلحة المحمية جنائيا من هذا الاعتداء ، وقد ظهرت اتجاهات تشريعية مختلفة في محاولة تحديد هذه المصلحة [1] ، نذكر منها :

أ) - الاتجاه الاول : يرى اصحاب هذا الرأي أن حق الملكية الخاصة هو المعني بالحماية ، باعتبار أن المعلومات المخزنة في الحاسب الالي و البرامج الخاصة به هي أموال يتحصل المعتدي عليها على ربح مادي جراء ذلك ، وأيد هذا الرأي بعض المشرعين في بعض الولايات في الولايات المتحدة الامريكية .

ب) - الاتجاه الثاني : وهو الذي تبنته المملكة المتحدة والذي يعتد بسلامة المعلومات و البيانات المحتواة في الحاسب الآلي حيث لا تثير طريقة التلاعب بهذه المعلومات اشكالية اذ يدرجها المشرع ضمن أشكال التزوير.

ج) - الاتجاه الثالث: يهتم اصحاب هذا الاتجاه بكون المعلومات في حد ذاتها مصلحة جديرة بالحماية سواء تعلقت بالحياة الخاصة للأفراد ، أو كانت معلومات اقتصادية أو ذات طبيعة حكومية ، فتتجه هذه التشريعات إلى تجريم مجرد الاطلاع عليها عن طريق الدخول غير المصرح به إلى نظام الحاسب الالي . وقد تبنت هذا الاتجاه الولايات المتحدة الامريكية كقانون فدرالي وكذا الدول الاسكندينافية.

د) - الاتجاه الرابع : يستند البعض الاخر الى شكل الفعل الاجرامي ،فهو الذي يبين المصلحة المحمية جنائيا ، فإذا كان السلوك الاجرامي يهدد الملكية فان نصوص حماية الملكية كفيلة بردعه ، اما اذا كان السلوك الاجرامي يهدد سرية المعلومات فان نصوصا خاصة تحمي هذه المصلحة .

و لكن إذا نظرنا إلى أن جرائم المعلوماتية تقع سواء كان الحاسب الآلي متصل بشبكة انترنت أم لا، ومنها الاختراق و التلاعب في بيانات وبرامج الحاسب الآلي، و الاحتيال والتزوير المعلوماتي وسرقة الهوية و إساءة استعمال البريد الالكتروني، و الاحتيال في استعمال البطاقات المصرفية، و إساءة استخدامها و انتهاك حرمة الحياة الخاصة و غيرها من الجرائم التي سنتطرق لها في الفصل الثاني ، فإن من شأن هذه الجرائم أن تشيع عدم الثقة في استعمال الوسائل التكنولوجية في المجتمع ، ومما لا شك فيه أن فقدان الثقة في التكنولوجيا ينتج عنه تخلف الدول و المجتمعات دون الأخذ بعين الاعتبار الخسائر الجسيمة الاقتصادية و العلمية التي يسفر عنها ابتعاد المجتمع عن استعمال الوسائل الحديثة ، فالراجح ، حسب ما نرى ، أن الغاية من تجريم تلك الاعتداءات هو حماية الثقة العامة في استعمال التكنولوجيا الحديثة في كافة المجالات .

---

[1] نائلة عادل قورة، جرائم الحاسب الالي الاقتصادية ، الطبعة الاولى، منشورات الحلبي الحقوقية ، بيروت ، 2005، ص 309.

الفرع الثاني
حجم الجرائم المعلوماتية و دوافع ارتكابها

ان تقدير حجم الجرائم المعلوماتية تكتنفه الكثير من الصعوبات ، فمن جهة هناك من يبالغ في تقدير حجمها و حجم الخسائر الناتجة عنها بسبب عدم ادراك أبعاد الجريمة من الناحية التقنية حيث يلعب الاعلام دورا في اثارة الغموض وتهويل المخاطر بشكل يجعل تقييمه لحجم الظاهرة غير دقيق ، ومن هنا كان اللجوء إلى المراكز القانونية المهتمة باجراء الدراسات أو التحقيقات و الاحصائيات الجنائية في الجرائم المعلوماتية ، أمرا لابد منه على الرغم من انها تقدم احصائيات لا تعكس بالضرورة حجم الاجرام الحقيقي كما هو موجود في الواقع ، ولكنها تعطي صورة عما يسمى بالاجرام الظاهري فقط وهو الوارد في سجلات الشرطة ، اي عدد الجرائم المبلغ عنها ، كما تقدم احصائيات عن عدد الجرائم التي صدر بشأنها احكام قضائية.

ومما لاشك فيه ان الحجم الحقيقي لهذه الجرائم اكبر بكثيرمما يبدو،نظرا لما توفره الجرائم المعلوماتية من سهولة في ارتكابها و امكانية فقدان اثر الجريمة .
سنحاول أن نقدم ابرز الاحصائيات بهذا الخصوص كما نتطرق الى دوافع ارتكاب الجرائم المعلوماتية .

أولا- حجم الجرائم المعلوماتية :

في أحدث تقرير صادر في الولايات المتحدة الامريكية عن مركز الشكاوي من جرائم الانترنت عبر العالم Internet Crime Complaint Center (IC3) ، الذي يجمع في تقريره تحقيقـات المركزالوطني لجرائم الياقات البيضاء NW3C بالتنسيق مع مكتب التحقيقات الفدرالي FBI ، والذي يضم تقريرا مفصلا عن الجرائم المبلـغ عنها من 01 جانفي سنة 2009 الى 31 من ديسمبر من نفس السنة ، حيث ورد فيه أن حجم جرائم الاحتيال المعلوماتي ارتفع الى 560 مليون دولار امريكي سنة 2009 بعد ان كان حجمها 265 مليون دولار امريكي سنة 2008 .
وجاءت في صدارة الجرائم المرتكبة المبلغ عنها جريمة الاحتيال المعلوماتي واهمها الاحتيال في استعمال البطاقات المصرفية وكذلك سرقة الهوية ، كما ان مقارنة الجرائم المبلغ عنها سنة 2001 مع سنة 2009 توضح ارتفاعا بنسبة % 667,8. [1]
وقدرت شركة Symantec ، وحسب تحقيق اجرته سنة 2010 ، فان الجرائم المعلوماتية تسبب خسائر مالية تقدر ب (114) مليار دولار سنويا على المستوى الدولي وهي في تزايد مطرد .[2]
أما الشركة الامريكية المتخصصة في الأمن المعلوماتي "McAfee " ، في دراسة لها قدمت بمناسبة المؤتمر الاقتصادي العالمي في دافوس بسويسرا تعود لسنة 2008 ، ان الجرائم المعلوماتية تسببت في أضرارمباشرة وغير مباشرة للشركات قدرت ب ألف (1000) ملياردولارامريكي ، وتغلب على هذه الجرائم سرقة المعطيات المعلوماتية .[3]

---

(1) انظر في الملحق رقم 2: Internet Crime Report of Internet Crime Complaint Center, IC3, 2009

(2) (3) احصائيات مسجلة بتاريخ 15 أكتوبر 2010 ، أنظر في الموقع :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-445352-cybercriminalite-coute-114- dollars_- 2010.html

أما عن سرعة وتيرة ارتكاب الجرائم المعلوماتية فقد كشفت دراسة قدمت في المؤتمر الدولي الأول حول حماية امن المعلومات المنعقد بالقاهرة سنة 2008 ، أن جريمة تحدث كل ثلاث دقائق على الإنترنت التي تضم 500 مليون موقع وأكثر من 15 بليون صفحة وملايين قواعد المعلومات وغيرها من الصور والتسجيلات .[1]

ثانيا- دوافع ارتكاب الجرائم المعلوماتية

عند النظر في دوافع ارتكاب الجرائم المعلوماتية ،يجب أن نربط ذلك بالخدمات التي تقدمها شبكة الانترنت ، حيث صارت امكانية الاتصال متاحة مع أي شخص في كل أنحاء العالم بفضل خدمة البريد الالكتروني ، الذي يمكننا من ارسال و استقبال و نقل الملفات و بصورة سريعة جدا ، كما أن خدمة المحادثة صوتا وصورة وكتابة متوفرة كذلك ، ضف إلى ذلك خدمة نقل وتحويل الملفات من حاسب آلي إلى آخر ، مع امكانية الاحتفاظ بها سواء في ذاكرة الجهاز أو في خدمة الأرشيف الالكتروني ، وقد اتاحت شبكة الانترنت ايضا امكانية الدخول إلى حاسب آلي عن بعد باستعمال برامج وتطبيقات تسمح بذلك ، دون أن ننسى مجمل الخدمات العلمية والاعلامية من مشاهدة الاحداث العالمية فور وقوعها ، وقراءة الصحف اليومية و نشر وتلقي المعلومات المختلفة في كافة المجالات ومتابعة أسواق المال و الأسهم والسندات ، وامكانية التعاقد على شراء السلع أو اجراء عمليات تجارية عبر شبكة الانترنت أو مايسمى بالتجارة الالكترونية ،...الخ.

ومن خلال النظر في الخدمات التي توفرها الانظمة المعلوماتية وشبكة الانترنت ، يتضح لنا ماهي دوافع المجرمين لارتكاب هذا النوع من الاجرام ، وإن كان السعي إلى تحقيق الربح يأتي في المرتبة الأولى ، حيث بينت دراسة أشار اليها الأستاذ باركر Parker بان 43 % من حالات الاحتيال المعلوماتي المعلن عنها ، كان سببها الأول هو الحصول على المال [2] .

وكنا قد قدمنا ، حسب تقرير مركز الشكاوي من جرئم الانترنت عبر العالم ، أن الجرائم التي يكون الغرض منها تحقيق الربح كالاحتيال المعلوماتي قد تفاقمت بشكل كبير، ويرجع السبب في كون الاحتيال المعلوماتي في طليعة الجرائم المعلوماتية إلى أن البنوك تعتمد بشكل كبير على أنظمة التمويل الالكتروني ، فلا يتطلب تحويل الاموال سوى معرفة رموز و أرقام سرية تمكن من اجراء هذا التحويل ، فبمجرد تمكن المجرم المعلوماتي من الحصول على هذه الرموز فانه يقوم بتحويل ملايين الدولارات إلى رصيده دون أن يترك اي دليل يدينه [3] .

وقد لا تتطلب العملية الا استعمال برامج تطبيقية صممت لاختراق نظام الحاسب والحصول على المعلومات المخزنة به ، حيث حدث ان قام ثلاثة شبان من هولندا سنة 2005 باستعمال برنامج من هذا النوع يسمى "Botnet " أو يسمى كذلك" Spybot " [4] ، باختراق مئة الف 100.000 حاسب آلي والتحكم فيها بعد ذلك عن بعد و استغلالها سواء في الحصول على أموال أو لشن هجمات على مواقع الكترونية معينة .[5]

---

[1] راشد بن حمد البلوشي ،ورقه عمل مقدمه الي المؤتمر الدولي الاول حول حماية امن المعلومات و الخصوصيه في قانون الانترنت ، القاهرة ، 2008 .

[2] محمد سامي الشوا ، المرجع السابق، ص 50 .

[3] محمود أحمد عبابنة ، المرجع السابق ، ص 24.

[4] انظر في الملحق رقم 1 – المصطلحات الواردة في الدراسة-.

[5] Abbas Jaber, Les infractions commises sur Internet, L'Harmattan ,paris, 2009, p. 30.

وتظهر الدوافع التجارية لعمليات قرصنة المواقع الحكومية والشركات التجارية إذا ما تصفحنا ما تعرضه مواقع القرصنة من خدمات للحصول على هذه المعلومات .

غير أن البحث عن تحقيق الربح السريع ليس دائما الدافع لارتكاب الجرائم الالكترونية ، إذ أن جرائم كثيرة ترتكب لا يهدف منها مرتكبوها سوى ابراز قدراتهم في التحكم في التكنولوجيا، ومنها اختراق المواقع الالكترونية وتعطيلها ، حيث قام أحد الهواة الاوروبيين باختراق موقع البنتاغون و تمكن من العبث في بيانات احد مراكز المعلومات به. [1]

وتعتبر الدوافع السياسية كذلك من أهم المحفزات على ارتكاب الجرائم المعلوماتية ، إذ تم تسخير شبكة الانترنت في العديد من الصراعا ، فشبكة الانترنت تستعمل بشكل شبه دائم لاختراق مواقع حكومية أو تعطيلها او الترويج لاعمال ارهابية او لافكار متطرفة او محظورة.

وقد صارت الجريمة المعلوماتية بمثابة السلاح تستعمل في الصراعات بين الدول ، وكان مؤلف كتاب "مهن الذكاء الاقتصادي" قد استشرف ظهور نوع جديد من الهيمنة بعد انهيار الاتحاد السوفياتي ، إذ اعتبر أن التحكم في تكنولوجيا المعلومات هو السلاح الحديث الذي يعوض السلاح التقليدي. [2]

وقد تعددت التقنيات المستعملة نظرا لرواج الطلب على برامج القرصنة مثل برامج" Sniffer " التي تمكنك من الحصول على كلمة السر لأي حاسب آلي أو موقع أو بطاقة مصرفية ، وذلك في ثواني معدودة [3].
و كانت أولى هذه العمليات في بداية الثمانينات عندما تمكن شباب ألمان من اختراق عدة حاسبات الية لأمريكيين وتم بيع المعلومات المتحصل عليها الى جهاز المخابرات السوفياتي KGB . [4]

المطلب االثاني

خصائص الجريمة المعلوماتية و سمات الجاني و المجني عليه

ان ضبط خصائص الجريمة المعلوماتية و حصر ما يميزهذا النمط المستحدث نسبيا من الاجرام عن غيره من الاجرام التقليدي . يسهل عمل المشرع ويمكنه من صياغة النصوص التشريعية الملائمة لمكافحة هذه الجرائم ، ومما لاشك فيه أن خطورة الجرائم المعلوماتية يجعل منها من مصاف الجرائم المنظمة و الجرائم الارهابية و الاتجار بالمخدرات ،هذا ان لم تكن اخطر منها كما قال " كولن روز Colin ROSE " وهو خبير في نظم المعلوماتية وامن الشبكات في إحدى الشركات الاسكتلندية ان جرائم المعلوماتية هي اكبر ثالث تهديد للدول العظمى بعد الاسلحة الكيميائية و البكتريولوجية و النووية [5].

---

[1] جميل عبد الباقي الصغير، القانون الجنائي و التكنولوجيا الحديثة ،الطبعة الاولى،دار النهضة العربية القاهرة،1992، ص 17.

[2] Lacoste (P) , Les métiers de l'intelligence économique, Défense nationale,Paris,2006,P.144.

[3] [4] Abbas (Jaber.), Op cit, pp. 26 - 27.

[5] Chawki (M), Essai sur la notion de Cybercriminalité, IEHE, Lyon, 2006, p .2.

ولأن الجريمة المعلوماتية تتميز عن غيرها من الجرائم التقليدية بارتباطها بجهاز الحاسب الآلي و التقنيات الحديثة في مجال تكنولوجيا المعلومات ، فقد أضفى عليها هذا طابعا خاصا سوف نتبينه من خلال تطرقنا في الفرع الأول لخصائص الجريمة المعلوماتية ، وفي الفرع الثاني نتناول أهم سمات الجاني أو ما يعرف بالمجرم المعلوماتي ، ثم نتعرف على المجني عليه أو ضحية الاعتداء في هذا النوع من الإجرام.

الفرع الأول
خصائص الجريمة المعلوماتية

للجريمة المعلوماتية مجموعة من الخصائص تميزها عن غيرها من الجرائم التقليدية ، وبسبب هذه المميزات فرضت الجريمة المعلوماتية نفسها على فقهاء القانون بشكل جعل من اللازم القيام بمراجعة المبادئ والاسس التي بني عليها القانون الجنائي من خلال نصوصه التقليدية.

ومن أبرز خصائص الجريمة المعلوماتية يمكن ذكر:

أ ـ الجرائم المعلوماتية من الجرائم العابرة للحدود :

بعد ظهور شبكة الأنترنت أتيحت امكانية الاتصال بين عدة حاسبات آلية مهما كانت المسافة الفاصلة بينهما حيث لم يعد هناك ما يحول دون تبادل المعلومات ونقلها بكميات مذهلة و بسرعة هائلة ، وقد أدى ذلك إلى نتيجة مفادها أن عدة اماكن متفرقة في دول مختلفة قد تتاثر بالجريمة المعلوماتية الواحدة وفي آن واحد ، حيث أنه لم يعد للمسافة التي تفصل بين الجاني ومكان ارتكابه للجريمة دور كبير ، وهذا ما ميز الجريمة المعلوماتية عن الجرائم التقليدية بشكل كبير [1].

ب ـ صعوبة اكتشاف و اثبات الجرائم المعلوماتية :

تمتاز الجرائم المعلوماتية بصعوبة اكتشافها و اثباتها نظرا لعدم ترك الجاني آثارا مرئية أو ملموسة في أغلب الأحيان ، فتغيير بيانات الحاسب الآلي أو الاحتيال المعلوماتي و غيرها من الجرائم يتم بواسطة ادخال رموز و أرقام ، وهي امور تقنية تتسم بتعقيدها وصعوبة اكتشافها أو اثباتها. وعادة ما يتم اكتشاف الجريمة بمحض الصدفة [2] .

كما أن عدم تبليغ المجنى عليهم عن الجريمة لأسبابهم الخاصة أو حماية لثقة المتعاملين في المؤسسات أو الشركات المعتدى عليها ، يعيق من مهمة التحقيق .

وقد أشار توم فوريستر في كتابه "مجتمع التقنية العالية " إلى أنه حسب اعتقاد الخبراء فإن 15 % فقط من جرائم اللاحتيال المعلوماتي هي التي يعلن عنها من قبل الشركات ، و أن العديد من الجرائم تمر بدون الكشف عنها ونادرا ما تتم محاكمة الحالات التي يتم الكشف عنها نظرا لصعوبة اثباتها. [3]

---

[1] Sieber (Ulrich), The international Handbook on Computer Crime ''Computer related Economic Crime and the infringements of privacy, John Wiley and Sons, 1986, p. 83.

[2] جميل عبد الباقي الصغير، المرجع السابق، ص 17.

[3] توم فوريستر، مجتمع التقنية العالية ، الطبعة الاولى، ترجمة ونشر مركز الكتب الاردني ، عمان، 1989، ص400 .

ج ـ تتطلب وسائل خاصة تتمثل في الحاسب الالي و شبكة الانترنت و المعرفة التقنية :

تتطلب الجريمة المعلوماتية توفر الحاسب الآلي وكذلك شبكة الانترنت في حالة جرائم الأنترنت نظرا لأنهما وسيلتا ارتكاب الجريمة و أدواتها الرئيسية ، أما عن المعرفة التقنية فهي ضرورية بحسب درجة خطورة الجريمة المعلوماتية .

د ـ تتطلب خبرة و تحكما في تكنولوجيا المعلوماتية عند متابعتها:

بسبب الطبيعة التقنية للجرائم المعلوماتية ، فإن رجال الضبطية القضائية لا يتعاملون باحترافية ومهارة اثناء البحث و التحري ، لذلك فان المحقق في الجرائم المعلوماتية يجب ان يكون متخصصا حتى لا يتسبب في اتلاف الدليل الالكتروني خطأ .

الفرع الثاني
سمات الجاني و المجني عليه في الجريمة المعلوماتية

انعكست خصائص الجريمة المعلوماتية على طرفي الجريمة وهما الجاني او ما يعرف بالمجرم المعلوماتي و المجني عليه وهو ضحية سلوك المجرم المعلوماتي ، وذلك بسبب الطبيعة الخاصة لها من حيث انها ترتبط بتكنولوجيا معقدة و تختلف عن الجرائم التقليدية .

وسوف نتطرق لاهم سمات المجرم المعلوماتي ونحدد فئاته ثم نتطرق لتحديد المجني عليهم في الجرائم المعلوماتية .

أولا ـ سمات الجاني او المجرم المعلوماتي :

اختلف الفقهاء في ادراج المجرم المعلوماتي ضمن طائفة المجرمين ذوي الياقات البيضاء ، وكان الاستاذ الأمريكي "سيذرلاند Sutherland " أول من أطلق هذه التسمية في مؤلفه " اجرام ذوي الياقات البضاء" سنة 1939، وقد قصد بها الطبقة العليا من المجرمين والتي ترتبط بمكانتها الاجتماعية و المهنية .[1]

ويرجع السبب في كون أن هذه الطائفة الاخيرة ترتكب جرائمها من خلال المهنة التي تنتمي اليها بخلاف المجرم المعلوماتي الذي له سمات خاصة تميزه عن هؤلاء ، ولو أنه يتميز في اغلب الحالات بامتلاكه لقدر من العلم و المعرفة التكنولوجية تساعده على ارتكاب جرائمه ، كما ان جرائم اصحاب الياقات البيضاء اقتصادية في مجملها بخلاف الجرائم المعلوماتية . وقد اعتبر بعض الفقهاء ان جرائم المعلوماتية تتشابه مع جرائم ذوي الياقات البيضاء بل انها تدخل في نطاقها. [2]

---

[1] Geis (G.), White-Collar Crime, Offences in Business, Politics and The professions, N.Y, The Free Press, 1995, p. 23.

[2] Glineur(P.), Droit et Ethique de l'Informatique, Story Scientia, Bruxelles, 1991, p 180.

وقد أشار الأستاذ "باركر Parker " إلى أنه رغم تشابه المجرم المعلوماتي مع المجرمين ذوي الياقات البيضاء في العديد من الصفات كعدم اعتباره لسلوكه كنوع من الاجرام ، إلا أن له خصائص تميزه تشمل المهارة و المعرفة و التحكم في الوسيلة و السلطة و الباعث. [1]

فالمهارة المطلوبة تكون بقدر الخبرة المكتسبة في هذا المجال ، أما المعرفة فقد قصد بها الاحاطة بظروف الجريمة وفهم كيفية التوصل الى تحقيق النتيجة دون فشل، و بامتلاكه للوسيلة المتمثلة في جهاز الحاسب الالي المراد اختراقه ، أما السلطة فهي الامتياز الذي يسمح للمجرم المعلوماتي الولوج الى جهاز الحاسب الالي في حالة كونه شخص موظف أو يملك الحق في استعمال الحاسب الآلي المستهدف .

و بالإضافة لما ذكرنا فمن سمات المجرم المعلوماتي أنه يتخصص في نوع معين من الإجرام كما أنه يعود في كل مرة إلى ارتكاب جرائمه كنوع من اشكال التحدي و تطوير المهارات في حالة ما اذا تم القبض عليه.

ونظرا لطبيعة الجريمة المعلوماتية فإن المجرم المعلوماتي لا يتسم بالعنف كما تشير الدراسات أن اغلب مرتكبي الجرائم المعلوماتية من الأذكياء ، فالشخص الذي يستعمل الحاسب الآلي ويتغلب على التشفير، ويتمكن من سرقة أو تحويل أموال من بنك، يجب أن يكون على قدر من الذكاء، فهو يمارس النصب أوالسرقة باستخدام وسائل التقنية الحديثة. [2]

ولكن مهما قيل عن المجرم المعلوماتي من أنه متكيف اجتماعيا أوانه ليس مجرما بطبعه ،أو انه لم يكشف عن أي عداء للمجتمع ، و يمتاز بصفات خاصة ، فهو يبقى مجرما يتطلب توقيع العقاب عليه ، فتعدد الجرائم المعلوماتية و تنوعها وتدرج خطورتها تقتضي عدم التهاون في مكافحة الإجرام المعلوماتي . [3]

وقد تم تصنيف مرتكبي الاجرام المعلوماتي إلى فئتين تضم الأولى شبابا وطلبة من هواة ارتكاب الجرائم المعلوماتية ويطلق عليهم تسمية " الهاكر Hacker ". [4]

«وهوالشخص الذي يتسلى باستخدام تفصيلي لنظام مبرمج والذي يبحث عن تنمية معارفه في هذا المجال »

«*Le hacker peut être considéré comme une personne qui prend du plaisir à explorer en détail un système programmable et qui cherche sans cesse à étendre ses connaissances dans ce domaine* ». [5]

وقد اصطلح على تسميتهم بصغار نوابغ المعلوماتية [6] ، و الأمثلة كثيرة على الجرائم المرتكبة من قبلهم و التي تتنوع بين اختراق انظمة الحاسبات الالية و العبث بمحتوياتها .

---

[1] Parker (Donn B.), Op cit, p 136.

[2] غنام محمد غنام ،عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر،بحث مقدم الى مؤتمر القانون و الانترنت، جامعة الامارات، ماي 2000، ص5 .

[3] محمد سامي الشوا ، المرجع السابق ،ص37 .

[4] أنظر في الملحق رقم 1-المصطلحات الواردة في الدراسة.

[5] Martin (D) et Martin (F.P) ,Cybercrime , Paris, Press Universitaires, 2001, p. 75.

[6] محمد سامي الشوا ، المرجع نفسه، ص 39.

أما الفئة الثانية فتضم المحترفين ويطلق عليهم تسمية " الكركر Crackers "، وهم أكثر احترافية و تخصصا في مجال الحاسب الآلي وتكنولوجيا المعلوماتية و على جانب كبير من الخطورة الاجرامية بحكم مهارتهم وخبرتهم في هذا المجال. [1]

ثانيا - تحديد المجني عليه في الجريمة المعلوماتية :

قد يكون ضحايا الاجرام المعلوماتي إما مؤسسات حكومية أو شركات تجارية أو افراد عاديين ، فاختراق النظام المعلوماتي قد يرتكب على أي من هؤلاء ، ويرجع السبب في ذلك إلى انتشار استعمال الحاسب الآلي و شبكة الانترنت مما يوسع من فئات ضحايا الاجرام المعلوماتي .

وغالبا ما تكون سلبية تعامل المجنى عليهم مع مرتكبي هذه الجرائم عاملا أساسيا في تفاقم ظاهرة الإجرام المعلوماتي ، فبسبب احجام المجنى عليهم عن التبليغ عن الاعتداء المرتكب في حقهم، سواء كان اختراق للنظام المعلوماتي أو الاحتيال و الاستيلاء على البطاقة المصرفية أو انتهاك حرمة الحياة الخاصة الى غيرها من الجرائم ، يصعب على رجال الشرطة تحديد مرتكبي هذه الجرائم مما يحد من فعالية الجهود المبذولة لمكافحة الاجرام المعلوماتي.

ولكن ليس كل ضحايا هذه الجرائم يدركون انهم وقعوا ضحية احتيال معلوماتي أو انتحال للهوية ، فالطبيعة التقنية و غير المادية للجريمة المعلوماتية و التي تقع اعتداءا على بيانات أو معلومات مخزنة ضمن أنظمة المعالجة الالية للمعطيات أو ضد معلومات تتسم بالسرية ترتبط بالحياة الخاصة للافراد ، مع ما تمتاز به هذه الاعتداءات من خصائص تضمن لمرتكبيها سرعة في الأداء و سهولة في الافلات من المتابعة ، تجعل من ضحايا هذه الجرائم يعلمون في ظرف متأخر وقوعهم ضحية لها ، و قد لا يعلمون ذلك اطلاقا .

أما المؤسسات المصرفية و الشركات الكبرى و التي غالبا ما تتعرض لأعمال النصب و الاحتيال المعلوماتي أو القرصنة ، فان سبب احجامها عن التبليغ عن هذه الجرائم مردُه الى حرصها على عدم المساس بسمعتها لدى زبائنها و شركائها ، لما في ذلك من خطورة على وضعها المالي و خشية من عزوف الزبائن عن التعامل معها لعجزها عن توفير الحماية اللازمة لشبكاتها الداخية و الخارجية .

---

[1] انظر في الملحق رقم 1- المصطلحات الواردة في الدراسة.

الفصل الاول
القواعد العامة للجريمة المعلوماتية

سبق وان اشرنا في المبحث التمهيدي الى خصوصية الجريمة المعلوماتية وتميزها عن باقي الجرائم ، ونتيجة لهذا التميز فقد استلزم أن تكون لها أحكامها الخاصة بها.

و لتحديد الطبيعة القانونية للجريمة المعلوماتية يتعين أن نتعرف على العوامل المختلفة التي تتداخل في تكوين الجريمة ، وعليه فقد ارتأينا أن ندرس في هذا الفصل آلية ارتكاب الجريمة المعلوماتية والوسائل المستعملة في ذلك و كذا العناصر المكونة للجريمة .

ولأن أهم ما يميز الجرائم المعلوماتية عن غيرها من الجرائم التقليدية هو محل الجريمة المتمثل في المعلومات فإننا سنتناوله من خلال تحديد مفهوم المعلومات وعرض خصائصها وتبيين قيمتها القانونية ، كما نتطرق لدراسة أحكام المساهمة والشروع و المسؤولية الجنائية عن الجريمة .

وعليه سوف نخصص المبحث الاول لدراسة آلية الجريمة المعلوماتية و محلها ووسائلها ، في حين نتناول في المبحث الثاني أركان الجريمة ،على أن يكون المبحث الثالث مخصصا لدراسة احكام المساهمة و الشروع و المسؤولية الجزائية في الجرائم المعلوماتية .

المبحث الأول
آلية الجريمة المعلوماتية ، محلها و وسائلها

تقتضي الجرائم المعلوماتية كما رأينا في المعايير المستند عليها عند تعريفها أن يكون المجرم على دراية بتكنولوجيا الحاسب الآلي ، فطبيعة هذه الجرائم تقتضي أن يكون مرتكبها يمتلك حدا ادنى من تكنولوجيا المعلوماتية ، وتختلف أساليب ارتكابها باختلاف القصد الجنائي لدى الجاني ، فجريمة السرقة أو التقليد أو الاحتيال المعلوماتي أو غيرها من الجرائم تتطلب من الجاني القيام بآليات معينة يكتمل معها سلوكه الإجرامي .

و باختلاف الوسائل المستخدمة في ارتكاب الجريمة ، يختلف تكييفها وتتغير طبيعتها من جريمة تقليدية إلى جريمة معلوماتية ، كما يختلف تكييف الجريمة بحسب المحل الذي وقع عليه الاعتداء، سنحاول أن نتطرق إلى آلية ارتكاب الجريمة المعلوماتية في المطلب الأول، وفي المطلب الثاني نتناول محل الاعتداء، أما في المطلب الثالث فسوف نخصصه لتحديد وسائل ارتكاب هذه الجرائم.

المطلب الأول
آلية الجريمة المعلوماتية

تتم معالجة المعطيات في الحاسب الآلي عبر ثلاثة مراحل هي الإدخال و المعالجة ثم الإخراج، ويمكن للمجرم المعلوماتي أن يرتكب جريمة في أي من هذه المراحل ، فمثلا بامكانه ادخال معلومات غير صحيحة أثناء مرحلة الادخال وتتم اثناء هذه المرحلة معظم الجرائم المعلوماتية ، أما في مرحلة المعالجة الالية للمعطيات فإنه يمكن وضع برامج جديدة تقوم بحذف البرامج الأصلية ، وتتميز هذه المرحلة بضرورة تحكم المجرم في تقنيات الحاسب الالي و عملياته ، أما في المرحلة الأخيرة وهي الاخراج فإن التلاعب يقع على البيانات المخرجة التي لا تكون مطابقة للبيانات المدخلة .[1]

أما اذا كان الحاسب الآلي موصول بشبكة الأنترنت فإن الدخول غير المصرح به إلى أنظمة البيانات المخزنة أو المنقولة عبر الأنظمة المعلوماتية قد يكون بهدف تدمير المعطيات ، أو الاستيلاء على البيانات المخزنة ، ثم يتم اخفاء هذا الاعتداء عبر اعادة انتاج وطرح البيانات عبر الشبكة و بالتالي الاحتيال على المتعاملين الذين يطلبون خدمة الدفع عبر الانترنت. [2]

وعليه يمكن تحديد خطوات الية تنفيذ الجريمة المعلوماتية كما يلي :

أ ـ البحث عن نظام الحاسب الالي الذي يحتوي على المعلومات او البرامج المطلوبة.

ب ـ الوصول الى نقاط ضعف النظام و الاستفادة منها .

ج ـ الدخول الى النظام ثم التحكم فيه و القيام بتعديل البيانات اوحذف جزء منها او اتلافها.

د ـ الاستفادة من السلوك الاجرامي سواء ببيع المعلومات او من خلال الحاق الخسارة بالمجني عليه .

ه ـ اخفاء جميع الادلة و محو اثار الاعتداء .

المطلب الثاني
محل الجريمة المعلوماتية

قد تستهدف الجرائم المعلوماتية إما المعلومات المخزنة في جهاز الحاسب الالي من خلال سرقتها ، أو تغييرها أو حذفها ، كما قد ترتكب اضرارا بجهاز الحاسب الالي وبمكوناته المادية وغير المادية عن طريق نشر الفيروسات التي تدمر أنظمة الكمبيوتر وتعرقل كل الأنشطة المرتبطة به ، كما افرز انتشار استعمال الأنترنت استهداف الاشخاص او المؤسسات ، مع ظهور اشكال متنوعة من الجرائم المعلوماتية مثل التهديد و التحريض على ممارسة الفاحشة ، و السب و القذف والترويج للارهاب والمخدرات ، وذلك من خلال ارسال بريد إلكتروني يحتوي على مواد منافية للآداب العامة أو مروجة لاستهلاك المخدرات.

و تعرف المعلومات بانها "مجموعة من الرموز او الحقائق او المفاهيم او التعليمات التي تصلح لان تكون محلا للتبادل و الاتصال او للتفسير و التأويل او للمعالجة سواء بواسطة الافراد او الانظمة الالكترونية ،وهي تتميز بالمرونة بحيث يمكن تغييرها ، وتجزئتها ، وجمعها او نقلها بوسائل مختلفة ". [3]

---

(1) احمد محمد الرفاعي ، الحماية المدينة للمستهلك ، دار النهضة العربية ، القاهرة، 1994 ، ص 71.

(2) عبد الله عبد الكريم عبدالله ، جرائم المعلوماتية و الانترنت،منشورات الحلبي الحقوقية ، بيروت ، 2007 ، ص20 .

(3) Parker (Donn) ,Op.cit, p 27.

وتختلف البيانات عن المعلومات في كون أن البيانات كما عرفتها منظمة التعاون الاقتصادي و التنمية (OCDE) بانها « عبارة عن مجموعة من الحقائق أو المفاهيم أو التعليمات التي تتخذ شكلا محددا يجعلها قابلة للتبادل و التفسير بواسطة الأفراد أو بوسائل إلكترونية ، أما المعلومات فهي المعنى المستخلص من هذه البيانات ، ولكن القانون لم يفرق بينهما في الحماية اذ ان كلتاهما جدير بالحماية ذاتها ». [1]

كما تختلف المعلومات من حيث نوعها أو الدور الذي تقوم به داخل المنظومة المعلوماتية ، فهناك معلومات تكون بشكل برامج تشغيل للحاسب الالي ، وهناك معلومات تتعلق بقطاع المال و الأعمال و التي تخص حجم المعاملات و أسرار التعاملات المصرفية، أوأن تكون معلومات ذات قيمة صناعية أو مهنية تخص طريقة الانتاج تحتاج إلى السرية و الحماية كما توجد معلومات بشكل أعمال أدبية أوفنية ، فكل مجال يتعلق بنوع معين من المعلومات .

وقد أثارت المعلومات إشكالية باعتبارها محلا يقع الاعتداء عليه تتمثل في كونها ذات طبيعة غير مادية، حيث اختلف الفقهاء حول طبيعتها القانونية ، فبينما يرفض جانب من الفقه اعتبار المعلومات كقيمة مالية إلا ما كان منها متعلقا بحقوق الملكية الأدبية أو الفنية أو الصناعية [2] ، يرى جانب من الفقه الفرنسي بان استبعاد المعلومات من طائفة الاموال لا يمنع عنها الحماية القانونية ، فطبيعتها الخاصة تجعل منها تدخل ضمن طائفة المنافع والخدمات وتخضع للحماية وفق قواعد المسؤولية التقصيرية [3] ، وذلك استنادا الى نص المادة 1382 من القانون المدني الفرنسي.

أما الإتجاه الأخر فقد ذهب إلى امكانية اعتبار المعلومات كقيمة مالية ، وقد علل الاستاذ الفرنسي "بيار كاتالا Pierre Catala" ذلك بكون المعلومة اشبه بالسلعة ، وأنها نتاج لعمل بشري وتنتمي إلى من يحوز العناصر المكونة لها بطريقة مشروعة ، و تكون في شكل يجعل منها صالحة للاطلاع عليها و تبليغها بشكل مفهوم . وبالتالي فبتوفر القيمة الاقتصادية لها المتمثلة في سعر السوق ، بالاضافة الى تبعيتها لمالكها تصبح المعلومات في ذاتها قيمة مالية بغض النظر عن الوسيط المادي الحامل لها. [4]

أما بعض اساتذة القانون فقد استنتج من أحكام محكمة النقض الفرنسية صلاحية المعلومات لأن تكون محلا ينصب عليه النشاط الاجرامي [5]، وذلك عندما ايدت محكمة النقض الفرنسية حكما في 8 ديسمبر 1971 حكم محكمة الاستئناف الذي يقضي بانطباق وصف خيانة الامانة على سلوك المتهم الذي قام بتسليم اقراص ممغنطة كان مؤتمنا عليها الى الغير بغرض اعادة نسخها قبل اعادتها فالمعلومات هي التي أعطت للأقراص قيمتها وحصول الغير عليها أفقدها قيمتها على الرغم من اعادتها لمالكها الأصلي. [6]

---

(1) Recommendation of the Council Concerning Guidlines for the security of Information System,26 November 1992.

(2) Goutal (Jean-Louis) ,Informatique et droit privé, in Bensoussan Alain, Linant de Bellefonds (Xavier),Maisel (Herbert) ,in Emerg ence du droit de l'informatique, Edition des parques,1983,p 92.

(3) Lucas de Leyssac (Marie-Paule),Une Information Seule est-elle Susceptible de Vol d'une autre atteinte juridique aux biens,Dalloz Siery,1985, p 43.

(4) Lucas de Leyssac (Marie-Paule), Ibid, p 46.

(5) Delmas-Marty (Mireille), Droit Pénal des Affaires, Presse Universitaire de France, 1990, p.46.

(6) Cass.crim.,8 Décembre 1971,Bull.crim.,N°341, p.856.

المطلب الثالث

وسائل الجريمة المعلوماتية

يقصد بالوسيلة الإمكانيات التي تتيح للمجرم المعلوماتي القيام بسلوكه الاجرامي . وتتميز وسائل الجريمة المعلوماتية في أغلب الحالات بكونها سهلة الحصول ، نظرا لتوافرها في العصر الحالي و بأسعار معقولة. ويمكن أن نذكر منها :

أ- الحاسب الالي : يقابله في اللغة الانجليزية مصطلح Computer أي حاسب و في اللغة الفرنسية Ordinateur بمعنى ناظمة الية ، ومن التعريفات التي اعطيت له انه « مجموعة متداخلة من الاجزاء لديها هدف مشترك من خلال اداء التعليمات المخزنة وهو الة حاسبة الكترونية ذات سرعة عالية ودقة كبيرة يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على النتائج المطلوبة ».[1]

كما عرف بأنه « جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية في الثانية الواحدة و بدرجة عالية الدقة و لديه القدرة على التعامل مع كم هائل من البيانات وتخزينها واسترجاعها عند الحاجة اليها » .[2]

وورد في الموسوعة الشاملة لمصطلحات الحاسب الآلي بأنه « جهاز إلكتروني يستطيع ترجمة اوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات ادخال بيانات Data input ، أو اخراج معلومات Information output، واجراء عمليات حسابية أو منطقية ،وهو بالكتابة على اجهزة الاخراج أو التخزين ، و البيانات يتم ادخالها بواسطة مشغل الحاسب عن طريق وحدات الادخال مثل لوحة المفاتيح واسترجاعهامن خلال وحدة المعالجة المركزية التي تقوم باجراء العمليات الحسابية ، وكذلك العمليات المنطقية ، وبعد معالجة البيانات تتم كتابتها على اجهزة الاخراج مثل الطابعات أو وسائط التخزين المختلفة ».[3]

ويتكون الحاسب الالي من المكونات المادية التالية [4] :

أولا- وحدات الادخال :

وهي الوحدات التي من خلالها يتم ادخال البيانات او الاوامر والتي يستعملها المجرم المعلوماتي خلال ارتكاب جريمته و تشمل هذه الوحدات كل من " الفأرة Mouse "، و " لوحة المفاتيح Keyboard " ، " مشغل الاسطوانات Disk Drive " .

ثانيا- وحدة المعالجة المركزية Central Processing Unit :

وتشمل "وحدة الذاكرة الرئيسية Main Memory "، التي تقوم بحفظ البيانات و النتائج بشكل مؤقت ، و "وحدة الحساب و المنطق Arthimatic Logic Unit "، و "وحدة التحكم Control Unit ".

---

(1) هلالي عبد الله احمد، تفتيش نظم الحاسب الالي و ضمانات المتهم المعلوماتي،الطبعة الاولى ،دار النهضة العربية ، القاهرة، 1997،ص16.

(2) عزة محمود احمد خليل ، مشكلات المسؤولية المدنية في مواجهة الحاسب الالي ،رسالة دكتوراه حقوق ، القاهرة، 1994،ص18.

(3) محمد فهمي ،الموسوعة الشاملة لمصطلحات الحاسب الالكتروني ، المكتب المصري الحديث، القاهرة،1991،ص 108.

(4) احمد خليفة الملط ،الجرائم المعلوماتية ،دار الفكر الجامعي،الاسكندرية ، 2005، ص 29 وما بعدها .

ثالثا ـ وحدات الاخراج [1]:

وهي الوسائط المستخدمة لاظهار نتائج التشغيل ومعالجة البيانات ، ومن اهمها "الشاشة Monitor "، و "الطابعة Printer"، "الراسمات Plotters "، " وحدات تركيب الاصوات Voice synthesizers".

رابعا ـ وحدات التخزين Storage divices**:**

تعتبر هذه الوحدات من اهم الوسائل التي تقع عليها الجرائم المعلوماتية لانه من خلالها يتمكن مستخدم الجهاز من تخزين ملفاته ، وتشمل" الاقراص الصلبة Hard disk "، و "الاقراص المرنة Flopy disk "، و"اقراص الليزرCD rom" .

خامسا ـ المودم Modem **:**

وهو الجهاز الذي يمكن الحاسب الالي من الاتصال الخارجي عبر شبكة الانترنت.

ب ـ الشبكات Networks**:**

تشمل مختلف الشبكات مثل الانترنت و الشبكات الداخلية او الانترانت ، وهذه الشبكات و خاصة شبكة الانترنت اعطت بعدا لجرائم الحاسب الالي وجعلت منها جرائم عابرة للحدود بفضل الامكانيات التي تتيحها للمجرم المعلوماتي من سرعة و عدم ترك الدليل المادي .

المبحث الثاني
أركان الجريمة المعلوماتية

سبق وأن أشرنا في معرض حديثنا عن مفهوم الجريمة المعلوماتية إلى الجدل الواقع في تسميتها، وكذلك في تمييز جرائم الحاسب الآلي عن جرائم الأنترنت أو اعتبارهما جريمة واحدة من حيث أنهما يختلفان في البعد العالمي الذي تتيحه شبكة الانترنت ، وعلى الرغم من تعدد صور الجريمة المعلوماتية وتنوعها باختلاف الوسائل التقنية المستعملة في ارتكابها وكذا الهدف من ارتكابها ، فقد يكون جهاز الحاسب الالي هدفا للجريمة كما في حالة الدخول أو الاستعمال غير المصرح به الى نظامه للحصول على المعلومات المحتواة في داخله ، أو قصد التلاعب بها او اتلافها ، او قد يكون جهاز الحاسب الالي اداة لارتكاب الجريمة في حالات التزوير و التقليد او الاستيلاء على الاموال عن طريق الاحتيال .

فلكل جريمة عناصرها الخاصة بها ، كما أن هناك جرائم تتطلب وقوع النتيجة وهي جرائم مادية، وجرائم اخرى شكلية تسمى جرائم السلوك المحض تقوم بمجرد ارتكاب الفعل الاجرامي ولا تتطلب ترتُب نتيجة عن ذلك. [2]

سنتناول أركان الجريمة المعلوماتية بصفة عامة من خلال الاشارة الى ما يجمع بين هذه الجرائم على ان نتناول دراسة أركان الجرائم المعلوماتية باختلاف صورها في الفصل الثاني .

---

[1] احمد خليفة الملط ،المرجع السابق، ص 29 وما بعدها .

[2] محمد نجيب حسني ،شرح قانون العقوبات،القسم العام،دار النهضة العربية ،القاهرة ،1982، ص 283 .

المطلب الا ول
الركن المادي للجريمة المعلوماتية

في القواعد العامة يعرف الركن المادي في الجريمة التقليدية بأنه سلوك اجرامي معين يتطلبه القانون كمناط للعقاب على هذه الجريمة ، على أن تتحقق نتيجة ضارة لهذا السلوك الاجرامي، كشرط بذاته يتعين قيامه حتى يعاقب على الجريمة كما يجب أن يرتبط النشاط أو السلوك الاجرامي و النتيجة الضارة بعلاقة سببية ، أو مايعرف بالاسناد المادي. [1]
ويتضح من خلال هذا التعريف انه حتى يعاقب المجرم على سلوكه الاجرامي لابد ان يتطابق هذا السلوك الاجرامي مع النموذج الاجرامي المنصوص عليه في قانون العقوبات .

ومن القواعد العامة للركن المادي في الجريمة أن يحدد المشرع السلوك الاجرامي في كل جريمة ضيقا و اتساعا على نحو يمكن القاضي من تكييف السلوك الاجرامي أو فعل الجريمة ورده الى القاعدة القانونية او النص التجريمي الذي يحكمه ، فجريمة النصب تتطلب القيام باعمال احتيالية للاستيلاء على مال الغير، وجريمة التزوير تتطلب طرقا حددها القانون ، في حين انه في جريمة القتل لم يحدد القانون طرق ازهاق الروح. [2]
و في جرائم المعلوماتية يتطلب القيام بالسلوك الاجرامي وجود حاسب آلي وأحيانا تتطلب الجريمة أن يكون متصلا بشبكة الأنترنت كما يتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته.
فمثلا قد يقوم مرتكب الجريمة بتجهيز الحاسب الآلي لكي يحقق له حدوث الجريمة، فيقوم بتحميله ببرامج اختراق، أو يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلي تهيئة صفحات تحمل مواد مخلة بالآداب العامة وتحميلها علي الجهاز ، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.

ولا تستوجب كل جريمة معلوماتية وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم المعلوماتية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية ، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشئ، فشراء برامج اختراق أجهزة الحاسب الالي أو الموقع أو العنوان الالكتروني، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للاطفال تعد جرائم في حد ذاتها.
والسلوك الاجرامي في الجرائم المعلوماتية يختلف حسب نوع الجريمة ، فاحيانا يكون نشاطا واحدا في الجرائم البسيطة كفعل الدخول غير المصرح به الى نظام المعالجة الالية للمعطيات الذي يتحقق بفعل الدخول غير المشروع ، اذ أن عدم مشروعية الفعل تقترن بكون الدخول غير مصرح به، بينما يكون السلوك الاجرامي في جريمة السرقة المعلوماتية و الاتلاف العمدي للمعلومات و البرامج ، أو جريمة القرصنة أو الاحتيال المعلوماتي سلوكا اجراميا متعددا ينطلق من الدخول الى نظام الحاسب الآلي أوإلى موقع ما على شبكة الانترنت بوجه غير شرعي ثم القيام بالتلاعب بمحتوياته ، هذا التلاعب الذي ينطوي على عدة انشطة اجرامية من ادخال لبيانات غير صحيحة أو محو او تدمير لمحتويات هذا النظام ، أو نشر لمواد مخلة بالنظام و الآداب العامين.

---

[1] رؤوف عبيد، مبادئ القسم العام من التشريع العقابي، الطبعة الثالثة ، دار الفكر العربي، القاهرة ، ص188 وما يليها .

[2] رمسيس بهنام ، النظرية العامة للقانون الجنائي ، الطبعة الثالثة ، منشأة المعارف بالاسكندرية ، ص 497.

كما أن السلوك الاجرامي في الجرائم المعلوماتية قد يكون وقتيا أي يبدأ ويتنهي بمجرد تمامه، مثل جريمة السرقة المعلوماتية أوالاعتداء على معطيات الحاسب الآلي باتلافها، وقد يكون مستمرا مثل حيازة صور وافلام مخلة بالحياء وعرضها على شبكة الأنترنت، أوانشاء مواقع لتحريض القصر على الفسق و الدعارة أو مواقع معادية بغرض الترويج للارهاب .

و تطرح مسألة النتيجة الإجرامية في جرائم المعلوماتية مشاكل عدة ، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية ، فلو قام احد المجرمين في أمريكا باختراق جهاز حاسب آلي رئيسي وهو مايعرف باسم " الخادم Server " في احد البنوك في فرنسا ، وهذا الجهاز الخادم موجود في الصين فمعرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين وهذا ما يثير أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن، فمن خلال تناولنا لصور جرائم المعلوماتية في الفصل الثاني سنتبين بعض هذه المسائل التي يطرحها الركن المادي للجريمة المعلوماتية ، وذلك بصدد كل جريمة على حدا.

المطلب الثاني
الركن المعنوي للجريمة المعلوماتية

جرائم المعلوماتية هي في أغلبها جرائم عمدية ، حيث يستوجب المشرع فيها توفر القصد الجنائي بركنيه العلم و الإرادة ، إذ يجب أن تتجه ارادة المجرم إلى إرتكاب سلوك يحظره القانون، كالإعتداء على نظام المعالجة الآلية للمعطيات ، بما يشمله من صور كفعل الإدخال لبيانات أوالمحو أو التعديل ، أوإلى نسخ البرامج بوجه غير شرعي من موقع على شبكة الانترنت أين يقوم القراصنة او الهاكرز بفك شيفرة الموقع أو تخريبه للحصول على البرمجيات إما للمنفعة المادية أو لايقاع الضرر بالشركة المعتدى على منتجها .
ويختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى ، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة ، أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي بما يتضمنه من معلومات وبرامج ، وعلى هذا النحو فدخوله الى نظام الحاسب الالي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غبير الشرعي.

وفي جريمة الاحتيال المعلوماتي التي هي بدورها جريمة عمدية ، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني .
والقصد الجنائي المشترط في جريمة الاحتيال المعلوماتي هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص اخر من ممتلكاته على نحو غير مشروع .

أما في جريمة اتلاف المعلومات فان المشرع اشترط توفر القصد الجنائي العام فقط حيث يكفي علم الجاني بانه يقوم باعمال من شانها ان تؤدي الى اتلاف المعلومات او محوها ، وقد تباينت التشريعات المختلفة في اشتراط القصد الجنائي الخاص ، وهذا ما سوف نتطرق اليه بصدد دراسة كل جريمة على حدا في الفصل الثاني .

المطلب الثالث
الركن الشرعي للجريمة المعلوماتية

تستمد الجرائم المعلوماتية شرعيتها من متخلف التشريعات الوطنية الصادرة بهذا الخصوص، فقذ بذلت هيئة الأمم المتحدة بالإضافة إلى المجلس الاوروبي جهودا مضنية لاقناع الدول بضرورة وضع التشريعات الملائمة لمواجهة جرائم المعلوماتية وتعزيز التعاون الدولي في هذا المجال .

وكمثال عى ذلك التوصية رقم R(89)9 المتعلقة بالجرائم المرتبطة بالحاسب الآلي التي أصدرها المجلس الاوروبي والاتفاقية التي تخص الاجرام المعلوماتي اوالسيبيري الموقعة في نوفمبر سنة 2001 ببودابست [1] ، و دخلت حيز التنفيذ في جويلية سنة 2004، وصادقت عليها بعض اعضاء النمجلس الاوروبي بالاضافة الى كندا و اليابان والولايات المتحدة الأمريكية و جنوب افريقيا حيث جعل منها وثيقة دولية ملزمة بالنسبة للدول الاطراف فيها .

وتواجه المشرع عند تنظيمه لمجال الحماية الجنائية من مخاطر جرائم المعلوماتية جملة من العراقيل ، تتمثل أولاها في مدى امكانية ملاءمة النصوص التقليدية مع هذا الطابع المستجد من الجرائم حيث أن الاخلال بمبدا الشرعية والوقوع في التفاسير الموسعة يخل بمبادئ القانون الجنائي ، وقد ظهرت اختلافات في تقدير المشرعين بين من يرى ضرورة وضع نصوص جديدة خاصة بجرائم المعلوماتية أو تكييف النصوص القديمة مع هذه الجرائم ، ومن يرى أن النصوص التقليدية تفي بالغرض ولا حاجة لتضييع الوقت بالتشريع لجرائم عادية ترتكب بوسائل تقنية متطورة.

فبينما يرى البعض أن ادراج النصوص المجرمة للأفعال التي تقع بواسطة جهاز الحاسب الالي او الانترنت أو تقع اعتداءا عليهما ضمن النصوص القديمة يخل بالبنيان القانوني للجريمة من حيث ان المشرع يتطلب في الجرائم التقليدية سلوكا محددا يتحقق به الركن المادي للجريمة ، فضلا عن الطابع المادي للنتيجة الاجرامية مما لا يتوافق وطبيعة المحل غير الملموس في الجرائم المعلوماتية ، في حين أن البعض الاخر يذهب الى اعتبار أن الجرائم المعلوماتية و المرتبطة بالتكنولوجيات الحديثة ما هي الا جرائم عادية استعمل فيها الحاسب الآلي كوسيلة لارتكاب الجريمة ، و أن المطلوب من المشرع هو العقاب عليها بواسطة النصوص التقليدية .

ولأن مراحل ارتكاب هذه الجرائم تتسم بتعقيدها فالمطلوب من المشرع إلماما كبيرا بالمصطلحات التقنية ومعرفة دقيقة للأفعال التي من شأنها أن تشكل جريمة معلوماتية ، حتى لا يتم المساس بحرية تلقي و تبادل المعارف و الحفاظ على الحق في احترام الحياة الخاصة .

---

[1] للاطلاع على النص الكامل لاتفاقية الإجرام المعلوماتي او السيبيري راجع الموقع الالكتروني الخاص بالمجلس الأوروبي :

http: //www.conventions.coe.int/treaty/EN/treaties/html/185.htm

المبحث الثالث
أحكام الشروع ، المساهمة والمسؤولية الجنائية في الجريمة المعلوماتية

نظمت اغلب التشريعات الصادرة بخصوص الجرائم المعلوماتية أحكام الشروع في الجريمة المعلوماتية و المساهمة الجنائية وكذا اسباب قيام المسؤولية الجنائية فيها.

وتنظيم المشرع لهذه الأحكام اكتنفه الكثير من الاشكاليات ، ومثال على ذلك الشروع في حيازة برامج خبيثة أو الشروع في الدخول الى نظام معالجة الية للمعطيات ، بما ان حيازة برامج تهدف الى اتلاف البيانات، أو حيازة صور اباحية، أو الدخول الى نظام المعالجة الالية للمعطيات و غيرها من الامثلة هي في حد ذاتها تعد من الجرائم المعلوماتية ، فأين تنتهي الاعمال التحضيرية فيها وأين يبدأ التنفيذ؟.

كما أن المساهمة الجنائية في الجريمة المعلوماتية تثير اشكالية العقاب على الاعمال التحضيرية التي تتم في اطار اتفاق جنائي ، وهذا ما سنتطرق إليه خلال دراستنا لكيفة تنظيم المشرع للمساهمة الجنائية عندما يتعلق الأمر بجريمة معلوماتية .

أما فيما يتعلق بالمسؤولية الجنائية في الجرائم المعلوماتية، فقد برز الخلاف حول مسؤولية مقدم الخدمة أو مزود خدمة الانترنت عن الأعمال الإجرامية التي ترتكب من قبل مستخدمي الشبكة .

في هذا المبحث سوف نتناول دراسة الإشكاليات التي أثارها كل من الشروع و المساهمة الجنائية في الجريمة المعلوماتية ، وكذا كيفية معالجة المشرع لفكرة المسؤولية الجنائية ، خاصة وأن الجرائم المعلوماتية ذات طبيعة خاصة ، باعتبار الطابع التقني لها وكونها ترتب في غالب الأحيان نتائج غير مادية مما يصعب من تطبيق القواعد العامة للقانون الجنائي عليها.

المطلب الاول
الشروع في الجرائم المعلوماتية

يعود اول تشريع نص على فكرة الشروع في الجرائم التقليدية الى عهد الملك " شارلكان" في " تشريع كارولين " ،والذي كان يتضمن نصا مقتضاه أنه إذا تجرأ انسان على أن يشرع في ارتكاب جريمة بأفعال ظاهرة تؤدي إلى اتمامها ، ولكنه منع عنها رغم ارادته ، أي باسباب خارجية عنها، فان الارادة الاجرامية التي نجمت عنها هذه الأفعال ينبغي عقابها [1] . فالجريمة قد تقع كاملة من حيث ركنها المادي فنكون بصدد جريمة تامة كما قد يقع السلوك الاجرامي ناقصا فتقف عند حد الشروع فيها الذي لاعقاب عليه الااذا نص القانون على ذلك صراحة [2].

ونصت المادة 30 من قانون العقوبات الجزائري على أن « كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة الى ارتكابها تعتبر كالجناية نفسها إذا لم توقف، أو يخب أثرها إلا نتيجة لظروف مستقلة عن ارادة مرتكبها، حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها ».

---

[1] رؤوف عبيد ، المرجع السابق، ص 368.

[2] احمد فتحي سرور، الوسيط في القانون العام ، الطبعة الرابعة، دار النهضة العربية ، القاهرة، ص338.

فالشروع جريمة وقعت و لكنها لم تكتمل ، فهي إما ناقصة أو أوقف تنفيذها قبل إتمامها أو خاب أثرها، لسبب خارج عن إرادة مرتكبها .
و قد عرفت المادة 45 من قانون العقوبات المصري الشروع بانه «البدء في تنفيذ فعل بقصد ارتكاب جناية أو جنحة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الفاعل فيها، ولا يعتبر شروعا مجرد العزم على إرتكابها ولا الأعمال التحضيرية لذلك» .
وقد عاقبت أغلب التشريعات على الشروع في الجريمة المعلوماتية بمختلف صورها ، فالمشرع الجزائري على غرار المشرع الفرنسي نص بذلك صراحة في المادة 394 مكرر 7 من قانون العقوبات في القسم السابع المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات التي نصت على أنه « يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها » ، في حين نص المشرع الفرنسي على تجريم ومعاقبة الشروع في جريمة الاعتداء على نظم المعالجة الآلية للمعطيات في المادة 323-7 من قانون العقوبات الفرنسي ، أما اتفاقية بودابست الصادرة ب 23 نوفمبر سنة 2001 فقد نصت في المادة 11 على ضرورة أن تقوم الأطراف المصادقة على الإتفاقية بالتشريع لمعاقبة الشروع في جرائم الاعتراض غير القانوني المتعمد ، و الاعتداء المتعمد على المعطيات و على الأنظمة المعلوماتية ، جرائم التزوير المعلوماتي و الاحتيال المعلوماتي و كذا الشروع في الجرائم المرتبطة بدعارة الأطفال و التي خصتها دون غيرها من جرائم المحتوى الضار[1].

و للشروع ركنان هما، الركن المادي ، و الركن المعنوي أوالقصد الجنائي .

والركن المادي بدوره يقوم على دعامتين هما البدء في تنفيذ السلوك الاجرامي ، الذي يفصل مرحلة الاعمال التحضيرية ،غير المعاقب عليها قانونا ، عن مرحلة الشروع المعاقب عليه [2].

وغالبا ما يطرح التمييز بين المرحلة التحضيرية و مرحلة البدء في التنفيذ اشكالا في الفصل بينهما، خاصة في الجرائم المعلوماتية ، ففي جريمة الاحتيال المعلوماتي يرى الفقهاء ان الاعمال التحضيرية تتمثل في كل نشاط ياتيه الجاني قبل استعماله لوسائل الاحتيال، أي أن العمل التحضيري ينتهي بمجرد سعي الجاني للاتصال بالحاسب الآلي لتنفيذ وسيلة الاحتيال، وهذا ما يتفق مع جريمة النصب التقليدية ، أين يعد كل نشاط يقوم به الجاني قبل اتصاله بالمجني عليه للنصب عليه باستعمال الطرق الاحتيالية، عملا تحضيريا و سعيه للاتصال به يعد بدءا في التنفيذ [3] .
والعبرة هنا تكون بالقصد الجنائي فالمتهم قد لا يسأل عن شروع في جريمة الاحتيال الا اذا اتجهت ارادته الى ارتكاب هذه الجريمة ، بل قد يسأل عن دخول أو استعمال غير مصرح به لنظام الحاسب الالي أو حتى لشروع في جريمة الاتلاف ، إذ أن التفرقة بين هذه الجرائم لا يمكن التحقق منه إلا باثبات وجهة ارادة المجرم المعلوماتي.
و الشروع نوعان : شروع تام وفيه يحقق الجاني النشاط الاجرامي كاملا ولكن على الرغم من ذلك لا تتحقق النتيجة الاجرامية لاسباب لادخل لارادته فيها وهو ما يعرف بالجريمة الخائبة أما النوع الثاني فهو الشروع الناقص حيث لا يكتمل النشاط الاجرامي لسبب يخرج عن ارادة الفاعل وهو ما يعرف بالجريمة الموقوفة [4].

---

[1] انظر في الموقع : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm

[2] مامون محمد سلامة، قانون العقوبات، القسم العام،دار النهضة العربية ،القاهرة، 1990، ص 389.

[3] محمد عبد الحميد مكي، الاحتيال في قانون العقوبات - دراسة مقارنة- رسالة دكتوراه، جامعة القاهرة ،1988.، ص 700.

[4] محمود نجيب، حسني المرجع السابق، ص 345.

ونحن بصدد دراسة الشروع في الجرائم المعلوماتية ، فاننا نتصور حدوث الشروع بنوعيه التام و الناقص ، وعلى هذا النحو فاننا يمكن ان نتصور حدوث الشروع في جريمة الاحتيال المعلوماتي بنوعيه التام و الناقص ، فلو قام الجاني بادخال بطاقة إلكترونية إلى جهاز الحاسب الآلي و أدخل الشفرة الخاصة بالجهاز، إلا أن عملية تحويل الاموال لم تتم لعطل أصاب الجهاز ، ففي هذه الحالة يكون الشروع تاما إلا أن النتيجة الاجرامية لم تتحقق لأسباب خارجة عن إرادة الجاني، وهو ما يعرف بالجريمة الخائبة ، أما إذا بدأ الجاني في التلاعب في البيانات وانقطع التيار الكهربائي ولم يستطع الجاني أن يغير من بيانات الحاسب و الوصول الى هدفه ، فالشروع يكون ناقصا و تكون الجريمة موقوفة.

المطلب الثاني
المساهمة في الجرائم المعلوماتية

تناول المشرع الفرنسي في المادة 323-4 تجريم الاشتراك أوالإتفاق ضمن جماعة للتحضيرلارتكاب أي من جرائم الاعتداء على نظام المعالجة الالية للمعطيات التي وردت في المواد 323-1 الى 323- 3-1 من قانون العقوبات الفرنسي ، في حين أن المشرع الجزائري الإشتراك في الإعداد لجريمة بغرض ارتكاب أي من الجرائم التي نظمها في قسم المساس بأنظمة المعالجة الآلية للمعطيات وذلك في المادة 394 مكرر5 من قانون العقوبات و التي نصت على أن « كل من شارك في مجموعة او في اتفاق تألف بغرض الإعداد لجريمة أو اكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها ».

وعلى الرغم من أن تجريم الأعمال التحضيرية لإرتكاب جريمة يعد خروجا عن القواعد العامة للقانون الجنائي، اذ الأصل أنه غير معاقب عليها ، ما لم تشكل جريمة مستقلة كالدخول غير المصرح به لنظام معلوماتي ، أو حيازة معطيات منظومة معلوماتية متحصل عليها من عمليات الاختراق لأي غرض كان ، أو حيازة صور مخلة بالحياء ، إلا أن رغبة المشرع الفرنسي و الجزائري في مكافحة الإجرام المعلوماتي دفعت بهما إلى تجريم الإشتراك في التحضير لإرتكاب هذه الجرائم [1] .

و يعتبر الحكم الصادر عن محكمة جنح باريس بتاريخ 12 اكتوبر1988 [2]، اول حكم قضائي تطرق الى وصف جريمة المساهمة في التامر بهدف الاستعداد لارتكاب جرائم احتيال معلوماتي، وفق المادة 265 من قانون العقوبات الفرنسي الصادر في 5 يناير 1988 [3] ، و الخاصة بجريمة الاتفاق على سرقة تكنولوجيا بطريق الاشتراك في تجمع اجرامي . وتنص على انه « كل من ساهم في اتفاق او تامر اقيم بغرض الاعداد وتجسد في واقعة واحدة او عدة وقائع مادية لجريمة او لعدة جرائم منصوص عليها في المواد 462-2 الى 462-6 من قانون العقوبات الفرنسي المتعلقة بالغش المعلوماتي يعاقب بالعقوبات المنصوص عليها لذات الجريمة أو من أجل جريم ات عقوبة أشد ».

و تتلخص وقائع القضية في قيام السيد " Hivart "وشركاؤه بالاستيلاء على أكثر من عشرة ملايين فرنك فرنسي من شركة توظيف الاموال الفرنسية " Tuffier Ravier " التي كان يعما بها كمراجع للحسابات ، وذلك بتحويله للاموال من حساب الى اخر لاشخاص شركاء معه في الجريمة ، وهذا بعد أن تحصل على شفرة

---

[1] محمود نجيب، حسني، القسم العام، المرجع السابق، ص 352.

[2] محمد سامي الشوا، المرجع السابق ، ص 6.

[1] La Loi N°88-19 du 5 Janvier 1988 relative à la Fraude Informatique, J.O.R.F N° 4 du 6 Janvier 1988.

الدخول الى ادارة تحويل الاموال وقد تمت ادانته بعد القاء القبض عليه هو وشركاؤه بعدة جرائم تتمثل في جريمة خيانة الامانة و التزوير و استعمال محررات مزورة و كذا جريمة المساهمة في التامر بهدف الاستعداد لارتكاب جرائم احتيال معلوماتي .

المطلب الثالث
المسؤولية الجنائية في الجريمة المعلوماتية

اتجه جانب من الفقه إلى اعتبار المسؤولية في مجال المعلوماتية هي مسؤولية تقصيرية حيث تقوم على أساس الخطأ المفترض من واقع حيازة المعلومات و حراستها ويحكمها القانون المدني ، إذ تدخل في نطاق المسؤولية التقصيرية ضمن نص المادة 1382 من القانون المدني الفرنسي ، وعليه يكون حارس المعلومات وغالبا ما يكون مورد الخدمة هو المسؤول عن الأضرار التي يسببها بث المعلومة عبر شبكة الانترنت ولا يعفى من المسؤولية إلا باثبات السبب الأجنبي، إذ يتعين على مقدم الخدمة منع نشر محتوى صفحات الشبكة المتعارضة مع القوانين والنظم واللوائح او المصلحة العامة.

ومن الممكن أن تتعلق المسؤولية عن الضررالناتج بمسؤولية المتبوع عن التابع حيث يعد كل متدخل على الشبكة في أي مرحلة تابعا لمورد الخدمة أو الشركة التي تتولى عملية بث المعلومات عبر الانترنت، في حين يرى اتجاه آخر عدم مسؤوليته باعتبار أن عمله فني ، إذ ليس بمقدور مقدم الخدمة أن يراقب تصرفات كل مستعمل للانترنت [1] .

وفي هذا الاطار فقد نصت اتفاقية بودابست لمكافحة جرائم المعلوماتية او جرائم الفضاء المعلوماتي لسنة 2001 في المادة 12، على قيام المسؤولية الجنائية للاشخاص المعنوية في حالة ارتكابهم للجرائم المنصوص عليها في الاتفاقية [2] وجاء فيها :

« ا ـ سوف يتبنى كل طرف تدابير تشريعية، وأي تدابير أخري لضمان قيام مسؤولية الأشخاص المعنوية عن أي جريمة موصوفة في هذه المعاهدة إذا ما ارتكبت لصالح الشخص المعنوي بواسطة شخص طبيعي اقترفها بشكل منفرد أو بوصفه جزء من عضو في الشخص المعنوي علي أساس من :

- تفويض من الشخص المعنوي
- سلطة اتخاذ قرارات لصالح الشخص المعنوي
- سلطة لممارسة رقابة أو سيطرة داخل الشخص المعنوي

ب ـ إلي جانب الحالات الواردة في البند 1 سوف يتخذ كل طرف التدابير اللازمة لضمان قيام مسؤولية الشخص المعنوي إذا ما أدي نقص الإشراف أو السيطرة من قبل الشخص الطبيعي المشار إليه في الفقرة 1 إلي إمكانية ارتكاب جريمة قائمة طبقا لهذه المعاهدة لصالح الشخص المعنوي بواسطة شخص طبيعي اقترفها تحت سيطرته.

---

[1] محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الانترنت، بدون طبعة، دار النهضة العربية ، القاهرة، 2002 ، ص 116.

[2] Convention sur la cybercriminalité, Budapest, 2001 ,à l'adresse :

http: //www.conventions.coe.int/treaty/EN/treaties/html/185.htm

ج - هذه المسؤولية لن تؤثر علي قيام المسؤولية الجنائية للأشخاص الطبيعيين الذين اقترفوا الجريمة » .

حيث اشارت المادة إلى قيام المسؤولية الجنائية لكل من الشخص الطبيعي أو المعنوي الموردين لخدمة الأنترنت في حالة تقصيرهم في منع وقوع الجريمة المعلوماتية ، مع عدم تاثير ذلك على قيام المسؤولية الجنائية للاشخاص الطبيعيين مرتكبي الجريمة .

أما في الجزائر و على نفس المنوال الذي قررت فيه اتفاقية بودابست مسؤولية مقدموا خدمة الانترنت ، جاءت المادة 11 من القانون رقم 09/ 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها ، حيث نصت المادة على قيام المسؤولية الجزائية للاشخاص الطبيعية و المعنوية، اذا أخل مقدموا الخدمات بالتزاماتهم التي تفرضها عليهم المادة 10 و المادة 11 ، المتعلقة بحفظ المعطيات المتعلقة بمساعدة السلطات المكلفة بالتحريات القضائية اثناء متابعة الجريمة ، والتي تسمح بالتعرف على مستعملي الخدمة و المتعلقة بالتجهيزات المطرفية المستعملة للاتصال وكذا مدة وزمن الاتصال، بالاضافة الى المعطيات التي تسمح بمعرفة المرسل و المرسل اليه وكذا عناوين المواقع المطلع عليها.

كما ألزمت المادة 12 مقدمي خدمة الانترنت بضرورة التدخل الفوري لسحب المحتويات المخالفة للقانون بمجرد علمهم بها و ضرورة وضع الترتيبات اللازمة لمنع امكانية الدخول إلى الموزعات التي تحتوي على معلومات مخالفة للنظام العام أو للاداب العامة [1] .

[1] قانون رقم 09-04 مؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها ، ج ر عدد47 ، المواد 10- 11 - 12 ، ص 7- 8 .

الفصل الثاني

صور الجريمة المعلوماتية و مكافحتها في القوانين المقارنة

كان من بين نتائج التطور المذهل والمتسارع والمتلاحق لتكنولوجيا المعلوماتية وشبكات المعلومات أن ظهرت أنماط متعددة من الجرائم وفرت لها الوسائل التقنية الحديثة البيئة المناسبة للنشاط الإجرامي حيث ساهمت شبكات الاتصال المتعددة في عولمة الجريمة ، إذ لم تعد جرائم الحاسب الالي تقتصر على أشكالها المعروفة بل تنوعت الانشطة الاجرامية بصورة مطردة حيث استغل المجرمون الفراغ التشريعي في بعض الدول في هذا المجال من ناحية ،وكذا صعوبة متابعة واثبات هذه الجرائم من ناحية اخرى .

وتشمل الجرائم المعلوماتية جرائم الحاسب الالي و جرائم الأنترنت ، وعلى الرغم من أن الحدود الفاصلة بين الجريمتين تبدو واهية ، إلا أننا إرتأينا تقسيمها بهذا الشكل حتى يتسنى لنا معرفة الدور الذي تلعبه شبكة الأنترنت في إعطاء البعد العالمي لجرائم الحاسب الآلي.

فجرائم الحاسب الآلي ويقابلها في اللغة الفرنسية مصطلح "La criminalité Informatique" كما سبق أن أشرنا إلى ذلك عند تقديمنا لأهم التعريفات للجريمة المعلوماتية ، تتمثل في كل فعل غير مشروع يرتكب بواسطة عمليات إلكترونية ضد نظام المعلوماتية أو البيانات التي يحتويها ، مهما كان الهدف المنشود .

أما جرائم الانترنت فهي جرائم الفضاء المعلوماتي ، ويقابلها في اللغة الفرنسية مصطلح " La Cybercriminalité " التي قد تشمل جرائم الحاسب الالي من دخول غير مصرح به و البقاء في منظومة معلوماتية أو تغيير أو تعديل أو اتلاف البيانات، إذا كان الولوج لجهاز الحاسب الالي عبر شبكة الأنترنت ، كما تضم ايضا الجرائم المرتكبة اعتداءا على الأشخاص و الأموال بواسطة شبكة الأنترنت وسوف نعرض صورها في المبحث الثاني.

سنتناول في هذا الفصل دراسة أصناف الجريمة المعلوماتية ضمن مبحثين ، نخصص المبحث الأول لصور جرائم الحاسب الآلي، و المبحث الثاني لجرائم الأنترنت ، ونظرا للارتباط الوثيق بين صنفي الجريمتين فسوف نستند في تقسيمنا إلى الدور الذي يلعبه كل من جهاز الحاسب الالي أو شبكة الانترنت في ارتكاب الجريمة ، أما في المبحث الثالث فسوف نتناول جهود مكافحة الجريمة المعلوماتية في القوانين المقارنة.

المبحث الاول

صور جرائم الحاسب الالي

بدأ اهتمام فقهاء القانون الجنائي بدراسة جرائم الحاسب الالي في مطلع السبعينات ،إلا أن حداثتها وارتباطها بالحاسب الالي أظهرت اتجاهات مختلفة في محاولة تقسيم هذه الجرائم وادراج الأفعال التي تدخل ضمن نطاقها. ومن أهم هذه المحاولات نجد تقسيم الأستاذ الالماني" زيبر Sieber " الذي قسم جرائم الحاسب الالي الى ثلاثة طوائف [1]:

أ ـ طائفة جرائم الحاسب الالي الاقتصادية

ويندرج ضمن هذه الطائفة الجرائم التالية :

1- الاحتيال المعلوماتي La Fraude informatique : ويقوم على التلاعب في نظم معالجة المعلومات للحصول بغير حق على أموال أو أصول أو خدمات.

2 ـ التجسس المعلوماتي Espionnage assisté par ordinateur : يتم باختراق نظام الحاسب الالي بهدف توظيف و استغلال ما يتم الوصول عليه من معلومات في القطاع الاقتصادي.

3 ـ قرصنة برامج الحاسب الالي Piratage de logiciel : يتم ذلك من خلال نسخ البرامج أو البيانات بصورة غير شرعية.

4 ـ الاتلاف المعلوماتي Sabotage Informatique : يقوم الاتلاف على محو او تدمير البرامج او البيانات .

5 ـ الدخول غير المصرح به الى نظام الحاسب الالي l'accès non autorisé dans un system informatique : و تتمثل في اختراق نظام الحاسب الالي دون وجه حق.

6 ـ سرقة الخدمات او الاستعمال غير المصرح به لنظام الحاسب الالي Vol de temps de l'ordinateur : ويقوم على استعمال الشخص للوظيفة التي يؤديها الحاسب أو الخدمات التي يقدمها خلال فترة زمنية دون التصريح له بذلك.

7 ـ الجرائم التقليدية في القطاع الاقتصادي التي تساعد الحاسبات على ارتكابها

---

[1] Sieber (Ulrich), Op.cit, pp. 3-27.

ب ـ طائفة الجرائم المتصلة بانتهاك حرمة الحياة الخاصة

ويندرج ضم نهذه الطائفة الجرائم التالية:

1 ـ استخدام بيانات شخصية غير صحيحة : إما بتغيير البيانات الشخصية أو محوها عن طريق اشخاص غير مصرح لهم بذلك أو جمع ا ونشر بيانات شخصية غير صحيحة .

2 ـ جمع وتخزين بيانات صحيحة على نحو غير مشروع : وذلك من خلال التوصل الى بيانات أشخاص اخرين بطريق غير مشروع ثم القيام بجمعها و تخزينها.

3 ـ الإفشاء غير المشروع للبيانات الشخصية و إساءة استخدامها : ويتعلق الأمر إما بالبيانات السرية الخاصة بالمجال المهني أو البيانات الشخصية غير السرية المتعلقة بالحياة الخاصة للأفراد.

ج ـ طائفة الجرائم المعلوماتية التي تهدد المصالح القومية او السلامة الشخصية للافراد :

ويتعلق الأمر بالتلاعب في انظمة الحاسبات الالية المرتبطة بمجال الطيران أو المجال العسكري أو المرافق العامة.

كما حدد الاستاذ " فاسيك مارتن Wasik Martin " جرائم الحاسب الالي حسب وجهة نظره وقسمها الى ثلاثة أقسام [1] :

أولا ـ جرائم الدخول و الاستعمال غير المصرح بهما لنظام الحاسب الالي :

وتضم مجموعة الجرائم التالية :

1 ـ الدخول غير المصرح به الى نظام الحاسب الالي.

2 ـ الدخول غير المصرح به إلى نظام الحاسب الالي بنية ارتكاب جريمة اخرى

3 ـ الاعتراض غير المشروع لنظام الحاسب الالي

4 ـ الأفعال غير المشروعة المتصلة بالمعلومات الشخصية المعالجة اليا

5 ـ الاستعمال غير المصرح به لنظام الحاسب الالي

ثانيا ـ الاحتيال المعلوماتي وسرقة المعلومات :

تضم هذه الطائفة الجرائم التالية :

1 ـ التلاعب في المعلومات المعالجة اليا بنية تحقيق ربح مادي غير مشروع

2 ـ تزوير المعلومات المعالجة اليا بنية استخدامها في أغراض غير مشروعة

3 ـ الحصول غير المشروع على المعلومات المبرمجة اليا

4 ـ قرصنة برامج الحاسبات الالية

---

[1] Wasik (Martin), Op.cit, p.4.

ثالثا ـ الجرائم التي يساعد الحاسب الالي على ارتكابها

ويدخل في نطاق هذه الطائفة الجرائم التالية :

1 ـ التخريب و الاتلاف سواء انصب على المكونات المادية أو المعنوية للحاسبات الالية.

2 ـ الاستعمال غير المشروع للحاسبات الالية لاعاقة المستخدمين الشرعيين لنظام الحاسب الالي عن الوصول إلى المعلومات التي يحتوي عليها .

3 ـ استخدام أنظمة الحاسبات الالية للاعتداء على أمن و سلامة الافراد.

4 ـ التهديد بتدمير مكونات الحاسب الالي لابتزاز المجني عليهم .

5 ـ الافشاء غير المشروع للمعلومات المؤتمن عليها بمقتضى الوظيفة .

6 ـ صناعة و بيع المعدات المساعدة لارتكاب جرائم الحاسب الالي كبرامج الفيروسات .

وقد اخترنا أن نتناول في هذا المبحث جرائم الحاسب الالي من خلال ثلاثة مطالب نتناول في المطلب الاول جرائم سرقة المعلومات و النصب والاحتيال المعلوماتي و جريمة التزوير المعلوماتي وفي المطلب الثاني جرائم الدخول والبقاء و الاستعمال غير المصرح به لنظام الحاسب الالي في حين نتناول في المطلب الثالث جرائم إتلاف المعلومات وتخريبها .

المطلب الأول
جرائم سرقة المعلومات، النصب و الاحتيال و التزوير المعلوماتي

تتعرض المعلومات باعتبارها ذات قيمة مالية ، كما أوضحنا ذلك في دراسة الطبيعة القانونية للمعلومات، إلى جريمة السرقة من خلال اختلاسها ، كما تكون عرضة للنصب بالاستيلاء عليها باستعمال طرق احتيالية أو لفعل التلاعب بها بتغييرها أو محوها أو تعديلها ، و هو ما يعرف بالاحتيال المعلوماتي.

سنتناول في هذا المطلب شرح هذه الافعال الاجرامية وتوضيح ما اثارته تطبيقاتها من اشكاليات قانونية فيما يتعلق بتكييفها القانوني .

الفرع الأول
جريمة سرقة المعلومات و البرامج

تعرف السرقة في الجرائم التقليدية بأنها اختلاس لشيء مملوك للغير ، وقد نصت المادة 350 من قانون العقوبات الجزائري على أنه « كل من اختلس شيئا غير مملوك له يعد سارقا» ، وتقابلها المادة 379 من قانون العقوبات الفرنسي .
ووفقا لهذا التعريف فإن أركان جريمة السرقة حسب القواعد العامة تتمثل في الركن المادي وهو فعل الاختلاس وكذلك محل الاختلاس و هو المال المنقول المملوك للغير بالاضافة الى الركن المعنوي المتمثل في القصد الجنائي.

وفعل الاختلاس حسب رأي الفقهاء يعني سلب حيازة الشيء من مالكه أوحائزه بغير رضاه [1] . ويقصد بسلب الحيازة كل فعل مادي ياتيه الجاني ويترتب عليه اخراج الشيء من حيازة صاحبها وحائزه ، وادخاله في حيازته هو، مهما كانت الوسيلة المستعملة في سلب الحيازة، وسواء احتفظ الجاني لنفسه بحيازة الشيء المسلوب أو تنازل عنها لغيره . ولا يكفي انتقال الحيازة من المجني عليه إلى الجاني لاعتبار الفعل اختلاسا، بل يجب ان يكون هذا الانتقال بغير رضا مالك الشيء اوحائزه [2].

من ناحية اخرى فان فعل الاختلاس ينتفي بالتسليم الارادي الصادر من الحائز نفسه والذي يكون القصد منه هو نقل الحيازة الى الجاني [3].

اما فيما يتعلق بجريمة السرقة المعلوماتية فقد اختلفت اراء الفقهاء بخصوص وقوعها من عدمه، ويرجع الاختلاف إلى أمرين هما فعل الاختلاس و محل الاختلاس ، فالرأي المؤيد لفكرة السرقة المعلوماتية يرى ان الركن المادي للسرقة المعلوماتية وهو فعل الاختلاس يتكون من عنصرين هما العنصر الموضوعي وهو النشاط او السلوك الارادي المؤدي إلى نتيجة مع وجود علاقة سببية بينهما ، أما العنصر الاخر الشخصي فهو نية الجاني في تملك الشيء وحيازته [4] . حيث عند تشغيل الحاسب الالي والحصول على المعلومات أو البيانات يكون قد اختلسها و استحوذ عليها بطريق غير مشروع .

ولا تتطلب هذه السرقة نشاطا ماديا كالذي يوجد في جريمة السرقة التقليدية ولكن الاختلاس المعلوماتي يتحقق بوسائل اخرى كاستعمال كلمة السر و الحصول على البيانات بغير رضا صاحبها ، فيرى أصحاب هذا الرأي امكانية وقوع السرقة المعلوماتية مع عدم امكانية تطبيق النص التقليدي لجريمة السرقة عليها [5].

أما الرأي الاخر فقد رأى عدم وجود امكانية وقوع جريمة السرقة المعلوماتية لارتباط فعل الاختلاس بالمحل المادي للاختلاس في السرقة [6] ، اذ ان اختلاس نسخة من برنامج أو معلومة من جهاز حاسب آلي لا يحرم صاحبها منها ولا ينقل اليه حيازتها [7].

أما بالنسبة لمحل جريمة السرقة المعلوماتية وهو المعلومات فقد اثارت هي الاخرى عدة اراء و اتجاهات بخصوص صلاحية المعلومة لأن تكون محلا للاعتداء عليها بصفة عامة و في جريمة السرقة بصفة خاصة.

حيث يرى بعض الفقهاء أنه يلزم في محل جريمة السرقة أن يكون مالا ذا طبيعة مادية ، فالمال المادي المنقول المملوك للغير هو الذي يصلح أن يكون محلا للتملك أما الاموال المعنوية فلا تصلح أن تكون محلا لجريمة السرقة [8] .

---

[1] عمر السعيد رمضان، مبادىء قانون العقوبات،القسم الخاص،دار النهضة العربية ، القاهرة، ص 416.

[2] عمر السعيد رمضان، المرجع نفسه، ص 417.

[3] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي ، المرجع السابق، ص409.

[4] عبد الفتاح بيومي حجازي، التجارة الالكترونية - الحماية الجنائية للتجارة الالكترونية، دار الفكر الجامعي، الاسكندرية،2004، ص193.

[5] غنام محمد غنام، المرجع السابق ، ص16.

[6] Devèze (Team), Le Vol de biens informatiques, J.C.P.1985, 1.3210., M.1.

[7] مدحت عبد الحليم رمضان،الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة ، 2000 ، ص 148

[8] عمر السعيد رمضان ،المرجع نفسه، ص 407.

كما أن تجريم سرقة المعلومات حسب البعض تواجهه حقيقة أن المعلومة تبقى مجرد فكرة وأن طبيعتها مجهولة وفضلا عن ذلك فالمعلومة تعد شيئا معنويا مما يجعل التعدي عليها له أوصاف اخرى غير السرقة [1].

وقد طرحت مسألة إمكانية وقوع المعلومات محلا للإعتداء عليها بغض النظر عن الوسيط الذي يحملها. حيث رأى جانب من الفقه أن المعلومة المجردة من الدعامة أو الوسيط الحامل لها تبقى غير قابلة للسرقة بما أن المحل المادي شرط مطلوب في الاعتداءات ذات الوصف القانوني و التي تقع على الاموال في صورة النصب و خيانة الامانة و اخفاء الاشياء المسروقة [2] ، إلا أن التطبيقات القضائية سارت في غير هذا الاتجاه ، حيث تعرضت محكمة النقض الفرنسية لموضوع سرقة المعلومات ، وتعتبرالاحكام الصادرة في قضايا مثل قضية Logabax ، و قضية و قضية Bourquin، من أشهر التطبيقات في تناول موضوع سرقة المعلومات .

وتتلخص وقائع قضية شركة Logabax ، في قيام موظف يعمل لدى هذه الشركة بنسخ مستندات سرية و استعملها كأدلة ضد الشركة في قضية اخرى، الا ان الشركة اتهمته بالسرقة، فقدم للمحاكمة التي برأته من تهمة السرقة و تم تأييد الحكم على مستوى محكمة استئناف Versailles بتاريخ 29 سبتمبر 1977 ، إلا أن محكمة النقض الفرنسية و في حكمها الصادر بتاريخ 8 جانفي 1979 نقضت الحكم و اعتبرت أن سلوك المتهم تنطبق عليه المادة 379 من قانون العقوبات الفرنسي المجرمة للسرقة وعللت ذلك بكون أن المتهم لم تكن له سوى اليد العارضة على الشيء وهو ما يختلف عن الحيازة ، و بالتالي فإن تصوير المستندات يعد اختلاسا لها اثناء مدة تصويرها دون رضا مالكها [3].
وقد تعرض هذا الحكم الى العديد من الانتقادات ،من بينها أن العقاب على اعادة انتاج المنتج هو خروج عن الشرعية ومن جهة اخرى أن فعل الاختلاس انصب على المحتوى الفكري للمستندات وعليه لا يمكن القول بحدوث اختلاس في هذه الحالة [4] ، فقد رأت الاستاذة Lucas de Leyssac " ان الاختلاس وقع من خلال اخذ المعلومات وليس من خلال تصوير المستندات [5] ، أما الجانب الآخر من الفقه فقد رأى أن الحكم السابق يدخل في اطار سرقة المنفعة Vol d'usage [6] ، حيث أن اختلاس المستندات كان لغرض استعمالها فقط ، وهذا ما أوجد تطبيقا مستحدثا في جريمة السرقة وذلك عن طريق التصوير Vol par photocopiage.

أما التطبيق الحقيقي لفعل سرقة المعلومات ، والذي يعد في نظر الفقهاء ثورة حقيقية في مجال سرقة المعلومات ، فهو الحكم الصادر في قضية "Bourquin" [7]، أين تمت إدانة عاملين في مطبعة " Bourquin "

---

[1] Sargos.P et Masse.M ,Le droit penal special de l'informatique et droi penal ,Cujas, 1983, p.25 .

[2] عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الالي، الطبعة الثانية، دار النهضة العربية القاهرة ،2002 ،ص151.

[3] Cass.crim.8 Janvier 1979, Gaz . Pal., 1979, 1, Note, p.502.

[4] نائلة عادل قورة، المرجع السابق ، ص125 .

« qu'en prenant des photocopies des documents en cause, à des fins personnelles à l'insu et contre le gré du propriétaire de ces documents, le prévenu qui n'en avait que la simple détention matérielle, les avait appréhendés frauduleusement pendant le temps nécessaire à leur reproduction »

[5] Lucas de Leyssac (Marie-Paule), Op.cit ,N° 27-31.

[6] Gattegno (Patrice), Droit Pénal Spécial, 1999 ,p202 ; Veron (Michel) ,Droit Pénal des affaires , 1992 ,p 26 ; Bernardini (Roger), Droit Pénal Spécial,2000,p158.

[7] Lucas de Leyssac (Marie-Paule), L'arret Bourquin,Une double Révolution :Un Vol d'Information Seul, une Soustraction Permettant d'appréhender des reproductions qui ne constitueraient pas des Contrefaçons , Rev .Sc.Crim , 3 Juillet-Septembre 1990 , p 507 .

سنة 1989 ، لقيامهما بسرقة سبعين قرصا ممغنطا و المحتوى المعلوماتي لسبعة و أربعين قرصا ، وأيدت محكمة النقض الفرنسية ما ذهبت إليه محكمة الإستئناف [1] ، إلا أن بعض الفقهاء يرون بأنه لا يمكن القول بأن الحكم السابق قد أدان المتهمين لسرقة المعلومات منفصلة عن اطارها المادي أو الوسيط الحامل لها ، فالسرقة لم ترد على المعلومات في حد ذاتها [2].

وحسب رأي الأستاذة "Lucas de Leyssac " فإن الحكم لا يعد بالفعل ثورة حقيقية في تجريم الإعتداء على الأموال ، و تعتبر أن المعلومات يمكن ان تكون محلا لجريمة السرقة اذ لا يتعارض ذلك مع مبادئ القانون الجنائي إذ ليس من اللازم أن يكون المحل في جريمة السرقة ماديا ، لأنه حسب نص المادة 379 من قانون العقوبات الفرنسي المجرمة لفعل السرقة ، فإن كلمة " شئ " تتيح ادراج أشياء غير مادية كمحل لجريمة السرقة ، كما أن فعل الاختلاس بالنسبة للمعلومات، قد يتحقق بمجرد قراءتها إلا أن هذا الفعل لا يمكن العقاب عليه إلا اذا ارتبط بوسيط مادي وهذا ما يحفظ لفعل الاختلاس ماديته التي تستوجبها قواعد الشرعية الجنائية [3] .

أما في المملكة المتحدة فقد أثار تطبيق نص السرقة على سرقة المعلومات اشكالية في القضاء البريطاني ليس بسبب المعلومات التي اختلف موقف القضاء بين اعتبارها أموالا أو استبعادها من نطاق الاموال ، بل حتى بسبب اشتراط الاستيلاء على هذه الأموال بشكل نهائي ، فعلى الرغم من أن المادة الرابعة من قانون السرقة البريطاني الصادر سنة 1968 قد عرفت الأموال بأنها تشمل النقود و الحقوق العينية و سائر الاموال غير المحسوسة و المعلومات السرية التي تدخل في نطاق الاموال غير المحسوسة ، إلا أن الحكم الصادر في قضية Oxford v.Moss ، قد عبر عن موقف القضاء الإنجليزي في استبعاد المعلومات من نص السرقة و عدم اعتبارها أموالا بالمفهوم القانوني، وعليه فقد حكم ببراءة الطلبة المتهمين بسرقة معلومات من ورقة أسئلة الإمتحانات بجامعة أكسفورد باعتبار أن هذه المعلومات لا ترقى إلى درجة الأموال التي يحميها القانون المتعلق بالسرقة . [4]

وقد أيد بعض الفقهاء الإنجليز هذا الموقف غير المجرم لسرقة المعلومات على هذا النحو و لكنهم رأوا أن صعوبة تطبيق نص السرقة في هذه القضية لا يكمن في استبعاد المعلومات من نطاق الأموال و إنما في عدم توفر نية الإستيلاء على المعلومات بشكل دائم ، حيث أن الطالبين قد أعادا ورقة الامتحان بشكلها الأصلي ، و لكن بمقابل ذلك فان الاطلاع على على هذه المعلومات السرية يفقدها قيمتها العملية مما أثار عدة اشكاليات في تطبيق نص السرقة على سرقة المعلومات [5] .

---

[1] Cass .crim ,12 Janvier 1989, Bull.crim ,N°14 ,p.38 :

« *Attendu qu'il appert de l'arret attaqué que Guenu et Boyer ont été déclarés coupable d'une part , du vol de 70 disquettes et d'autre part , de celui du* ***contenu informationel*** *de 47 de ces disquettes durant le temps necessaire à la reproduction des informations, le tout au prejudice de la S A Bourquin qui en était propritaire ;*

Attendu que sous couvert d'un prétendu defaut de base légale ,le moyen se borne à tenter de remmettre en cause l'appréciationsouvraine des juges du fond , qui ont relevé sans insuffisance, à l'encontre des prevenus ,l'ensemble des éléments constitutifs des délits dont ils ont été reconnus coupables » .

[2] Veron (Michel) , Droit Pénal des affaires,Dalloz, 1999., p.197.

[3] Lucas de Leyssac (Marie-Paule),Ibid ,p.509.

[4] كامل سعيد ، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنولوجيا ، (Oxford v.Moss (1978) 68 Cr .App R 183)، بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، 25 أكتوبر 1993، ص 349 .

[5] Bainbridge (David) , Introduction to Computer Law, Fourth Edition, Longman, 2000, p .316.

وفي معرض حديثنا عن معالجة بعض التشريعات لفعل سرقة المعلومات نجد في هذا السياق الأحكام الصادرة عن القضاء الامريكي ومنها ما أيد ان تكون المعلومات محلا لجريمة السرقة و منها ما عارض ذلك.

ومن الأحكام المؤيدة نجد الحكم الصادر في قضية Hancock v .State سنة 1966 ، التي تعتبر أول قضية تناولت موضوع اساءة استخدام الحاسبات الالية بشكل عام ، وتتلخص وقائع القضية في قيام مبرمج للحاسبات الآلية في احدى الشركات بطبع المعلومات المحتواة ضمن 59 برنامج ملك للشركة ، ومن ثم اتفاقه مع شخص اخر يعمل في شركة اخرى على بيعه اياها بمبلغ خمسة ملايين دولار، غير انه تم القاء القبض على المتهم الذي قدم للمحاكمة بتهمة السرقة [1].

واثارت القضية في حينها اشكالا بالنسبة لتكييف الدعوى إذ يميز القانون الامريكي بين السرقة بوصفها جناية و يحدد لها عقوبة بالسجن مدة لا تتجاوز العشر سنوات وبين كونها جنحة ، حيث وضع المشرع الامريكي في ولاية تكساس قيمة المال محل السرقة معيارا للتمييز بين الوصفين ، وفي قضية الحال اثار دفاع المتهم قيمة المال محل السرقة و هو الاوراق التي طبعت عليها المعلومات والتي لا تتجاوز قيمتها 34 دولارا ، إلا أن المحكمة استندت على نص المادة 1418 من قانون العقوبات الخاص بولاية تكساس التي عرفت الأموال التي تصلح أن تكون محلا لجريمة السرقة والتي تضمنت كل كتابة من أي نوع بشرط أن يتم التحقق من قيمتها المالية بحسب المعلومات التي تحتوي عليها و التي قدرت في الجريمة السابقة ب 2,5 مليون دولار[2] .

وعلى الرغم من تباين القوانين الخاصة بجرائم الكمبيوتر في الولايات المتحدة الأمريكية من ولاية الى أخرى ، وكذا بينها و بين القانون الفدرالي الذي جرم سنة 1984 الوصول غير المرخص به إلى المعلومات وقانون حماية البنية التحتية للمعلومات الصادر سنة 1996 [3] ، إلا أن مصطلح سرقة المعلومات لم يرد في هذه القوانين بل تم تجريم الفعل تحت مسميات أخرى كالوصول غير المشروع للمعلومات ، أو اختراقها أو تقليدها إلى غير ذلك .

أما موقف المشرع الجزائري فيمكننا القول أنه لم يشرع نصوصا تجرم السرقة المعلوماتية من خلال النص صراحة على سرقة المعلومات إلا أنه أضفى حماية للمعلومات من خلال قوانين متعددة كالقانون رقم 15/04 المتضمن لجرائم المساس بأنظمة المعالجة الآلية للمعطيات [4] و القانون رقم 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها [5] والذي وضع إجراءات لمراقبة الاتصالات الإلكترونية وتفتيش أي منظومة معلوماتية في حالة أي اعتداء يطال منظومة معلوماتية تابعة لمؤسسات الدولة أو النظام العام . كما أكد المشرع الجزائري حماته لبرامج الحاسب الآلي من خلال تجريمه للإعتداء على حقوق المؤلف و الحقوق المجاورة في الأمر 97 /10 ومن بعده الأمر 05/03 الصادر بتاريخ 2003/07/19، في المواد 151 و 152 التي جرمت استنساخ أو تقليد أي مصنف وبأي منظومة معالجة معلوماتية [6].

---

(1) نائلة عادل قورة ،المرجع السابق، ص 147.

(2) جاء في نص المادة 1418 من قاون العقوبات لولاية تكساس مايلي :

"All writing of every description,provided such proprety possesses any ascertainable value"

(3) محمود أحمد عبابنة ، المرجع السابق،ص99.

(4) القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر66 -156 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات ، ج.ر عدد 71، ص 8.

(5) القانون رقم 09-04 مؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها، ج .ر عدد 47، ص 5.

(6) الأمر03-05 الصادربتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر 7-14، ج ر عدد 44.

ومما تقدم نستخلص أن جانبا من الفقه اعترض على اعتبار وقوع السرقة على المعلومات على أساس أن فعل السرقة يقع اعتداءا على أموال مادية منقولة وهو ما لا يصلح قوله على الأفكار و المعلومات [1] ، بالإضافة الى أنه يصعب القول بحيازة المعلومة لأن الحيازة لا ترد سوى على الاشياء المادية [2] ، أما الجانب المقابل فقد رأى أن تطور أهمية المعلومات و اعتبارها من القيم المالية و الاقتصادية الحديثة جعل من فكرة وقوعها محلا لجريمة السرقة ممكنة ، حيث أنه يوجد من المعلومات ما لها قيمة مالية تقدر بثروات طائلة و يمكن اختلاسها و الاستيلاء عليها من مالكها أو حائزها الشرعي، أما الاشياء المادية فتنتفي عنها صفة المال اذا انعدمت قيمتها فلا تصلح أن تكون محلا لجريمة السرقة [3].

ولأن الثورة المعلوماتية أدت الى ظهور أنماط جديدة من الجريمة فقد انتهى جانب من الفقه إلى أنه يمكن استخدام الوسائل الإلكترونية كالحاسب الآلي في التعدي على الأموال من خلال ادخال بيانات غير صحيحة أو تعديل للبيانات المخزنة أو محوها من أجل اختلاس الأموال المادية أو زيادة الذمة المالة للجاني [4] .

وخلاصة لما تطرقنا إليه فإنه يعد مختلسا الشخص الذي يستخدم بيانات غير صحيحة عبر منظومة معلوماتية ليستولي على الأموال التي تمثلها هذه البيانات أو المعلومات، على الرغم من اعتبارها من قبيل الاموال المعنوية ، فحيازة المعلومة تترتب عليها حيازة السلع أو الخدمات المقدرة بالمال ، وهو ما يعد سرقة في صورتها المعلوماتية.

الفرع الثاني
جريمة النصب وجريمة الاحتيال المعلوماتي

أولا- جريمة النصب و الاحتيال في صورتها التقليدية :

تعرف جريمة النصب (L'Escroquecrie) بانها الاستيلاء على حيازة مال الغير الكاملة بوسيلة يشوبها الخداع ، تسفر عن تسليم ذلك المال ، أو بأنها « استعمال الجاني وسيلة من وسائل التدليس المحددة على سبيل الحصر ، وحمل المجني عليه بذلك على تسليم الجاني مالا منقولا مملوكا للغير » [5].

وهوبالتالي يختلف عن السرقة في كون الاستيلاء على الحيازة الكاملة للمال في جريمة السرقة تتم بدون رابط بين الجاني و مالك او حائز هذا المال ، اما في جريمة النصب فان الاستيلاء على المال يكون بتسليم يشوبه الاحتيال لاستعمال الجاني لطرق احتيالية نص عليها المشرع على سبيل الحصر[6].

وقد بين المشرع الجزائري الافعال المشكلة لجريمة النصب في صورتها التقليدية في نص المادة 372 من قانون العقوبات التي نصت على أنه « كل من توصل الى استلام أو تلقى اموال اومنقولات او سندات أو تصرفات ، أو اوراق مالية أو وعود أومخالصات او ابراء من التزامات أوإلى الحصول على أي منها او شرع

---

[1] هشام محمد رستم ، المرجع السابق ، ص 51.

[2] غنام محمد غنام ، المرجع السابق ، ص 10.

[3] أحمد حسام طه تمام ،الجرائم الناشئة عن استخدام الحاسب الالي وشبكة الانترنت، دار النهضة العربية، القاهرة 2000، ص 544 .

[4] Raymond Gassin, le droit pénal de l'informatique -D, 1986, Chron, p.36.

[5] فوزية عبد الستار ، شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية ، القاهرة ، 1990، ص 817 .

[6] محمد عبدالله ابوبكر سلامة ،جرائم الكمبيوتر و الانترنت، منشأة المعارف ، الاسكندرية،2006، ص 181 .

في ذلك ، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال اسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو باحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة اخرى وهمية او الخشية من وقوع اي شيء منها ...» [1].

أما قانون العقوبات الفرنسي الجديد لسنة 1992 فقد حدد في المادة 313 -1 أركان جريمة النصب و الاحتيال ، حيث نصت على أن« النصب هو الفعل الذي يتم باتخاذ اسم كاذب او صفة غير صحيحة ، أو بالاستعمال غير المشروع لصفة صحيحة ،أو باستعمال الطرق الاحتيالية ، وذلك لخداع شخص طبيعي أو معنوي وحمله بناءا على ذلك على تسليم نقود أو قيم أو أي مال ، أو تقديم منفعة أوقبول تصرف ينطوي على التزام أو مخالصة ، وذلك اضرارا بالمجني عليه أو بالغير » [2]. و يبدو أن المشرع الفرنسي قد وسع من مجال محل جريمة النصب عند استعماله لفظ " أي مال " حتى يمكن ادخال الأموال المعنوية ضمن طائفة الأموال التي تصلح محلا لجرية النصب ، إلا أن بعض أساتذة الفقه رأوا غير ذلك كما سنرى لاحقا عند دراستنا للنتيجة الاجرامية في الاحتيال المعلوماتي .

أما المشرع المصري فقد جرم النصب ، بنصه في المادة 336 من قانون العقوبات على أنه « يعاقب بالحبس كل من توصل الى الإستيلاء على نقود أو عروض أوسندات دين أو سندات مخالصة أو أي متاع منقول ، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها إما باستعمال طرق احتيالية من شأنها ايهام الناس بوجود مشروع كاذب أو واقعة مزورة أو احداث الأمل بحصول ربح وهمي أو تسديد المبلغ الذي اخذ بطريق الاحتيال أو ايهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور ، وإما بالتصرف في مال ثابت أو منقول ليس ملكا له ولا له حق التصرف فيه ، وإما باتخاذ اسم كاذب أو صفة غير صحيحة ...» [3].

وبخلاف المشرع الفرنسي فإن المشرع المصري حصر محل جريمة النصب في أشياء مادية منقولة لا تحتمل تفسيرا آخرا مما لا يمكن معه ادخال الأموال المعنوية ضمن الأموال التي تقع عليها جريمة النصب.

والركن المادي لجريمة النصب و الإحتيال في صورتها التقليدية يتكون من ثلاثة عناصر هي :

أ- السلوك الاجرامي المتمثل في استخدام طرق احتيالية نص عليها القانون على سبيل الحصر كاتخاذ اسم كاذب أو صفة كاذبة أو استعمال سلطة خيالية أو التحصل على اعتماد مالي أو احداث أمل بالفوز بأي شيء.

ب- النتيجة الاجرامية المتمثلة في قيام المجني عليه بتسليم ماله إلى الجاني .

ج- العلاقة السببية بين السلوك الاجرامي و النتيجة الاجرامية، حيث يشترط المشرع أن يكون تسليم المجني عليه لماله بسبب الغلط الذي أوقعه فيه الجاني من خلال استعماله للطرق الاحتيالية.

ولكن ما مدى امكانية وقوع المعلومات محلا في جريمة النصب و الاحتيال أي مدى انطباق وصف النصب على الحصول على المعلومات بطرق احتيالية ، هذا ما سنتطرق إليه فيما يلي.

---

(1) الامر 66-156 المؤرخ في 18صفر1386 الموافق لـ 8 يونيو1966 المتضمن قانون العقوبات،المادة 372 ، ج.ر عدد 49 ، ص 741.

(2) Ordonnance n° 2000-916 du 19/09/2000,art 3,J.O.R.F du 22/09/2000 en vigueur le 01/01/2002.

(3) عبد الفتاح بيومي حجازي،المرجع السابق،ص461.

ثانيا – جريمة الاحتيال المعلوماتي :

مع انتشار الاحتيال في مجال المعلوماتية ظهر الاهتمام بتعريفه كنوع مستقل عن النصب والاحتيال في الصورة التقليدية حيث صار يطلق عليه مصطلح الاحتيال المعلوماتي (La Fraude Informatique) .
ولو أن جوهرالنصب واحد في الجريمتين أين يستعمل الجاني وسائل احتيالية للاستيلاء على مال الغير إذ يعتبر الاحتيال عنصرا من عناصر الركن المادي لجريمة النصب ، و يكمن الفرق بين النصب و الاحتيال في صورته التقليدية والاحتيال المعلوماتي في محل السلوك الاجرامي المتمثل في المعلومات ونوع الوسائل الاحتيالية التي يلجأ إليها الجاني ، و التي تتمثل غالبا في التلاعب في معطيات و معلومات الحاسب الالي المخزنة ، كما أن الوسائل الاحتيالية في جريمة النصب في الافعال التي ذكرها المشرع على سبيل الحصر من استعمال لاسماء او صفات كاذبة او سلطة خيالية الى غير ذلك ، فان وسائل الاحتيال في جريمة الاحتيال المعلوماتي يمكن ان تتخذ عدة صور مختلفة.

وقد أوردت التوصية رقم 89/R9 للمجلس الاوروبي تعريفا للاحتيال المعلوماتي أقرته هيئة الامم المتحدة ، وبينت من خلاله السلوك الاجرامي لفعل الاحتيال المعلوماتي، و جاء فيها بأنه الادخال أو المحو أو التعديل أو كبت البيانات أو برامج الحاسوب أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية لشخص آخر، بقصد الحصول على منفعة اقتصادية غير مشروعة له [1] .

فالاحتيال المعلوماتي هو التلاعب العمدي بمعلومات وبيانات تمثل قيمة مادية يختزنها نظام الحاسب الالي ، أو الادخال غير المصرح به لمعلومات وبيانات صحيحة ، أو التلاعب في الأوامر و التعليمات التي تحكم عملية البررمجة أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي حتى يقوم بعملياته بناءا على هذه البيانات أو الأوامر حتى يتمكن من الحصول على ربح غير مشروع و إلحاق الضرر بالغير [2]. وحتى يتضح الفرق بين الاحتيال المعلوماتي و الاحتيال في صورته التقليدية نوضح أركان جريمة الاحتيال المعلوماتي .

أ) - الركن المادي في الاحتيال المعلوماتي:

أ- 1) السلوك الاجرامي : يمكن اجمال صور السلوك الاجرامي في الاحتيال المعلوماتي فيما يلي :

- التلاعب في البيانات المدخلة :

وتتمثل هذه الوسيلة في ادخال المعلومات والبيانات المراد معالجتها اليا ،ومن ثم التلاعب بها اما عن طريق الجاني او عن طريق شخص اخر حسن النية [3].
ومن اهم وسائل التلاعب في مرحلة ادخال البيانات تغيير المعلومات اما بشكل كلي اوجزئيا من خلال اضافة اجزاء اليها او استبدالها بمعلومات اخرى، وقد اعتبر القضاء الفرنسي ان ادخال معلومة بعد اجراء تعديل عليها او ادخال معلومة غير صحيحة الى نظام الحاسب الالي بنية الحصول على ربح غير مشروع للجاني يعد من قبيل الطرق الاحتيالية مما تقوم به جريمة النصب [4].

---

[1] La Recommandation N ° R (89) 9 sur la criminalité informatique et le rapport final du Comite d'Europe sur le problème de la criminalité, Strasbourg, 1990.

[2] نائلة عادل قورة، المرجع السابق ،ص 425.

[3] Bainbridge (David), Op.cit, p 292.

[4] CA de Paris ,28Novembre1990,Juris-Data,N° 025569 .
« Doit être condamnée la prévenue coupable d'escroquerie et d'introduction abusive dans un système de traitement automatisé ».

ومن الأمثلة على هذا الأسلوب قيام مستخدم في بنك "Indo-Swez" باختلاس مبلغ سبعة ملايين فرنك فرنسي ، وبعد أن قام بتحويلات لنقود وهمية خزنت على ذاكرة الحاسب وقام بنقلها إلى محررات مصنعة ثم قام بفتح حساب باسمه في بنك سويسري [1] ، كما يتم التلاعب في البيانات المدخلة من خلال حذف جزء منها أو حذفها كلها، ومن وسائل التلاعب بالبيانات إخفاءها أو إعاقة الوصول إليها.

- التلاعب في البرامج :

يرى البعض ان التلاعب في البرامج هو الاحتيال المعلوماتي بحق [2] ، و يتم ذلك عن طريق وسيلتين [3] **:**

- تتمثل الوسيلة الاولى في تغيير البرامج المطبقة داخل الحاسب الالي لدى المؤسسة ، و اجراء تعديلات عليه تتيح للجاني القيام بجريمته ، و يكون الجاني في اغلب الاحيان من التقنيين من ذوي الخبرة ، ومن الأمثلة على هذا الاسلوب قيام شخص يدعى" رويس E .Royce "، يعمل في مؤسسة تجارية ، بتعديل برنامج بشكل صار يقوم باقتطاعات لمبالغ زهيدة على فترات مختلفة من خلال الصفقات التي ابرمتها المؤسسة مع المنتجين الموزعين [4].

- أما الوسيلة الثانية فتتمثل في تطبيق برامج اضافية تهدف الى تعديل المعلومات المخزنة في الحاسب الالي [5]، ومن الامثلة على ذلك قيام مبرمجين في بريطانيا سنة 1988 بتصميم برنامج محاسباتي يمكن مستخدميه من خلال استعمال شفرة خاصة أن يتلاعب في البيانات المتعلقة بقيمة الضريبة المضافة ، ثم قاما بتوزيعه على 120 محل تجاري ، وتم بيع الشفرة إلى 12 محل من بين 120 مقابل مبالغ ضخمة تجاوزت 100.000 جنيه استرليني، وبعد تقديمهما للمحاكمة ادينا بتهمة التلاعب في البرامج ، و حكم عليهما بالحبس مدة تسعة اشهر و بغرامة قدرها 34.000 جنيه استرليني [6] .

- التلاعب في المعطيات :

يتم التلاعب في المعطيات من قبل شخص ليس مدخلا للبيانات ولا مبرمجا، حيث يقوم بفك رموز الشفرة الخاصة بنظام التحويل الالكتروني للاموال داخل البنوك ومن ثم يقوم بتحويل مبالغ مالية لحسابه الخاص ولعل اشهرالحالات بهذا الخصوص هي حالة الخبير في الكمبيوتر" ستانلي ريفكين Stanly Rifkin " سنة 1978 في بنك بلوس انجلس هو '' The Security Pcific Banc''، حيث بعد ملاحظته لكيفية اجراء عمليات التحويل الالكتروني وكذا الشفرة المستخدمة لذلك بفضل تمتعه بحرية الحركة داخل البنك باعتباره خبيرا به ، وعن طريق هاتف خارج البنك استطاع ان يتصل بشبكة المعلومات الخاصة بالبنك و تحويله لمبلغ عشرة ملايين دولار امريكي الى بنك في نيويورك ثم الى بنك اخر في سويسرا ، وعمل في تجارة الالماس ، ولم يلق عليه القبض الا بعد ان كشف عن ذلك علانية ، حيث قدم للمحاكمة في مارس 1979 بمحكمة لوس انجلس التي ادانته بعدة تهم منها التلاعب في نظام التحويل الالكتروني بغرض تحقيق ربح غير مشروع ، وحكمت عليه بالسجن لمدة ثماني سنوات [7] .

---

[1] محمد سامي الشوا،مرجع سابق ، ص73.

[2] Lioyd (Ian), Information Technology Law,Butterworths Press: London,Dublin,Edinburgh, 1997,p .128

[3] Siber (Ulrich), Op.cit,p .7

[4] محمود احمد عبابنة،المرجع السابق، ص57 .

[5] Parker (Donn B .), Op.Cit,p.7 .

[6] Bainbridge (David) , Op.Cit.,p.294.

[7] Norman (Adrian R .D), Computer Crime and the Law, Criminal Law Journal,Vol.15,1991.

أ- 2) : النتيجة الإجرامية في الإحتيال المعلوماتي :

حتى تقوم جريمة النصب يجب أن تؤدي وسائل الإحتيال التي حددها المشرع إلى تغليط المجني عليه، بحيث يقوم بتسليم المال إلى الجاني ، وهذا التسليم المادي هو النتيجة الاجرامية في جريمة النصب و الإحتيال التقليدية، ويشترط في هذا التسليم أن يكون تحت تاثير الوسائل الاحتيالية .

وقد اثيرت عدة مسائل بهذا الخصوص ، ففكرة تسليم المال في جريمة النصب في صورتها المعلوماتية أثارت اشكالية التسليم المادي للمال ،فعلى الرغم من أنه في بعض الحالات نجد أن الحاسب الالي يقوم بفعل التسليم المادي للمال عند الاستعمال غير المشروع لبطاقات الإئتمان ، إلا أن الحالات الأخرى كحالات تحويل المال من حساب المجني عليه إلى حساب الجاني، فقد استفيد من اجتهادات القضاء أن التسليم الذي يحدث في جريمة الاحتيال المعلوماتي يستوي مع التسليم المادي في جريمة النصب التقليدية، اذ أن العبرة بقيام الحاسب بوضع المال محل السلوك الاجرامي تحت تصرف الجاني[1] .
و استند بعض الفقهاء الفرنسيين في هذا الموضوع على المبدأ الذي أقرته محكمة النقض الفرنسية وهو ما يعرف "بالتسليم المتساوي Remise par équivalent "، اذ قررت المحكمة أن التسليم الذي يتم عن طريق العملة الكتابية يعادل التسليم الذي يتم عن طريق النقود[2] .

أما الاشكالية الاخرى التي اثيرت فتتعلق بموضوع التسليم أو محل الجريمة ، ففي جريمة النصب في صورتها التقليدية تطلب المشرع أن يكون محل الجريمة مالا منقولا مملوكا للغير ، وكونه منقولا اشارة ضمنية على طبيعته المادية [3] .في حين أنه في جريمة النصب في مجال المعلوماتية وبالنظر الى طبيعة المعلومات غير المادية ، فيرى جانب من الفقه أن النتيجة الاجرامية التي قوامها تسليم المال لا تتحقق في هذه الحالة [4] .
حيث رأى الاستاذ " فيرون Veron " أن عبارة " أو أي مال Bien quelconque " لا تعني توسع المادة الجديدة 313 -1 ، التي عوضت المادة 405 من قانون العقوبات الفرنسي القديم ، لتشمل المعلومات بل تخص قيمة المال موضوع التسليم ولا تفسر بأنها تعنى طبيعة المال محل الجريمة ، في حين أن المعلومات ولو أننا افترضنا تمتعها بقيمة مادية الا ان طبيعتها المعنوية تتعارض مع فكرة التسليم المفترض في جرائم النصب و السرقة التي تتطلب شيئا ذا طبيعة مادية [5] .

و رأى فقهاء اخرون أن الحصول على المعلومات يمكن أن ينظر إليه من زاوية الإحتيال من أجل الحصول على منفعة ، مثلما نصت المادة 313-1 من قانون العقوبات الفرنسي على فكرة المنفعة التي تصلح لأن تكون محلا لجريمة النصب، وهذه المنفعة تتمثل في تبادل المعلومات و بالتالي فإن النشاط الاجرامي لا ينصب على المعلومات في حد ذاتها بل على نقل وتبادل المعلومات ، فالنشاط الاجرامي في جريمة النصب المعلوماتية لا يتعلق بالمعلومات في حد ذاتها بل يتمثل في الحصول على المنفعة الناتجة عن نقل المعلومات [6] .

---

[1] جميل عبد الباقي، المرجع السابق، ص94 .

[2] Cass.crim., 17Octobre1967, Bull.crim.,N°252,p594 ; Cass.crim.,13Octobre 1971 , Bull.crim. N°261, p.643.

[3] محمود محمود مصطفى ،شرح قانون العقوبات، القسم الخاص ،مطبعة جامعة القاهرة ،1984 ، ص 561.

[4] أمال عبد الرحيم عثمان ، شرح قانون العقوبات ، القسم الخاص ،دار النهضة العربية ، القاهرة ،2001، ص 533 .

[5] Véron (Michel), Op.cit, p 222 .

[6] Vergutch (Pascal), La repression des délits informatiques dans une péerspective internationale, Thèse, Université de Montpellier 1 ,1996, p. 118.

غير أن جانبا من الفقه الفرنسي رأى أن المعلومات تصلح لأن تكون محلا لجريمة النصب على الرغم من طبيعتها غير المادية ، معللين ذلك بقولهم أن الذي يحصل على المعلومات بمجرد الاطلاع عليها يساوي الحصول على المستند المادي الحامل للمعلومات [1]. كما رأى جانب آخر من فقهاء القانون الجنائي أن تخلي المشرع الفرنسي في المادة الجديدة 313 -1 من قانون العقوبات عن لفظ الاشياء حتى لا تنصرف إلى الأموال المادية المنقولة فقط ، واستعمل لفظي "نقود Fond "و" اموال Bien " حتى يمكن ادخال الأموال المعنوية ضمن الأموال التي تكون محلا لجريمة النصب [2] .

ونخلص من ذلك الى أن النتيجة الاجرامية في النصب و الاحتيال في صورته التقليدية لا تختلف عنها في الاحتيال المعلوماتي اذ أن العبرة بقيام الحاسب الآلي بوضع المال المعلوماتي محل النشاط الاجرامي تحت تصرف الجاني وذلك تحت تأثير الوسائل الاحتيالية التي تطرقنا اليها في صور السلوك الاجرامي للاحتيال المعلوماتي.

ب)- الركن المعنوي لجريمة الاحتيال المعلوماتي:

جريمة الاحتيال المعلوماتي من الجرائم العمدية ، حيث لا يختلف الأمر بين جريمة النصب و جريمة الاحتيال المعلوماتي من حيث أن كلتاهما جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي الذي يجب أن يتوفر لدى الجاني حتى تقوم مسؤوليته الجنائية و يعاقب على هذه الجريمة .
والقصد الجنائي المتطلب في جريمة الاحتيال المعلوماتي هو القصد الجنائي بنوعيه العام و الخاص .

فالقصد الجنائي العام يتطلب علم الجاني بأن ما يقوم به من ادخال وتغيير للبيانات و المعلومات في نظام الحاسب الآلي يعتبر تلاعبا بها ، كما يجب أن يعلم الجاني عند قيامه بالتلاعب بالمعلومات أن المال الذي هو بصدد الاستيلاء عليه مملوك لغيره ، كما يجب أن تتجه ارادة الجاني إلى ارتكاب هذا السلوك الاجرامي المكون لجريمة الاحتيال المعلوماتي.

أما القصد الجنائي الخاص المشترط في جريمة الاحتيال المعلوماتي فيتمثل في نية التملك، فاذا كان غرض الجاني هو الاستيلاء على مال المجني عليه [3] ، فقد تحقق القصد الجنائي الخاص وهذا ما عبرت عنه الكثير من التشريعات التي جرمت الاحتيال المعلوماتي ، ونذكر المادة (1030 – A4) من القانون الفدرالي لجرائم الحاسبات الآلية في الولايات المتحدة الامريكية التي تطلبت نية الحصول على شيء ذي قيمة لقيام جريمة الإحتيال المعلوماتي [4].
وعلى الرغم مما قيل عن مدى امكانية تطبيق النصوص القانونية التقليدية الخاصة بالنصب و الاحتيال على الاحتيال المعلوماتي ، إلا أننا نرى أن مبدأ الشرعية وتفاديا للتفسير الموسع للنصوص القانونية الجنائية ، أدى بالمشرع الفرنسي إلى وضع القانون رقم 19-88 الصادر سنة 1988 الخاص بجرائم الاعتداء على نظم المعالجة الآلية للمعطيات [5].

---

(1) Linant De Bellefonds (Xavier) et Hollande (Alain) ,Droit de l'informatique et de la télématique, Dellmas, Edition Dalloz, 1990, p.113.

(2) مدحت عبد الحليم رمضان ، المرجع السابق ، ص 144.

(3) عمر السعيد رمضان، المرجع السابق، ص595.

(4) Olivenbaum (Josef M.),Rethinking Fedral Computer Crime Legislation,Setton Hall Law revieuw , vol.27,1997,p586.

(5) La Loi N°88-19 du 5 Janvier 1988 relative à la Fraude Informatique, J.O.R .F,,N° 4 du 6 Janvier 1988 .

كما قام المشرع الأمريكي بسن قوانين فدرالية متعلقة بتجريم الاحتيال على الحاسب الآلي سنة 1984 المعدل سنة 1996 [1]، وهذا ما سنتطرق إليه في المبحث الثالث ، أما المشرع الجزائري فقد جرم الاحتيال المعلوماتي من خلال سنه للقانون رقم 04-15 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات [2] مما يبين مدى الصعوبة التي واجهت المشرع في تطبيق نص جريمة النصب و الاحتيال التقليدية على الاحتيال المعلوماتي ، وتفاديا للاخلال بالمبادىءالعامة للقانون الجنائي .

لكن المشرع الجزائري لم يتطرق لأشكال من النصب و الإحتيال المعلوماتي يتصور وقوعها كالحصول على خدمة أو منفعة عبر شبكة الأنترنت واستعمل فيها الجاني طرقا احتيالية للحصول عليها ، فالملاحظ أن نص المادة 372 من قانون العقوبات الجزائري لا يمكن تطبيقه عى هذا الفعل ، بخلاف المشرع الفرنسي الذي نص على تقديم المنفعة كمحل في جريمة النصب في المادة 313-1 مما يتيح استيعاب الاحتيال المعلوماتي الذي يقع للحصول على منفعة او خدمة عبر شبكة الأنترنت .

الفرع الثالث
جريمة التزوير المعلوماتي

يعرف التزوير بانه تغيير الحقيقة في محرر بالطرق التي حددها القانون تغييرا من شأنه أن يرتب ضررا للغير ، وبنية استعمال هذا المحرر فيما اعد له [3] .

وجرم التزوير رغبة من المشرع في حماية الثقة في المحررات الرسمية والعرفية ، كونها وسيلة السلطة العامة في مباشرة اختصاصاتها، ووسيلة الأفراد لاثبات علاقاتهم و حقوقهم المتنازع عليها [4] .

ومما لاشك فيه أن ظهورطابعات الليزر و الماسحات المتطورة قد سهلت من عملية التزوير بشكل كبير ، ومع ازدياد الاعتماد على الحاسبات الالية في معالجة و تخزين المعلومات المتعلقة بجوازات السفرالبيومترية ووثائق الميلاد و الوفاة و رخص قيادة السيارات و إلى غير ذلك من المعاملات القانونية ، صار من اللازم حماية هذه المعلومات من التلاعب فيها وتزويرها ، فالتزوير في المجال المعلوماتي يتم عن طريق تغيير الحقيقة على المستندات المخرجة من الحاسب الالي نتيجة لتغيير البيانات الموجودة داخل الجهاز.

ولتبيين كيفية قيام جريمة التزوير المعلوماتي ، نتطرق لدراسة اركان هذه الجريمة ووسائلها.

---

(1) 18 USC § 1030 - Fraud and related activity in connection with computers ,in : Computer Crime & Intellectual Property Section United States Department of Justice : http://www.cybercrime.gov/1030analysis.html. or http://www.cybercrime.gov/ccmanual/ccmanual.pdf

(2) القانون رقم 04/ 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر66 /156 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات ، ج.ر عدد 71، ص 8.

(3) فوزية عبد الستار، المرجع السابق، ص 244.

(4) محمود نجيب حسني، شرح قانون العقوبات- القسم الخاص- الجرائم المضرة بالمصلحة العامة، القاهرة، 1972، ص 279.

أ- الركن المادي لجريمة التزوير المعلوماتي:

الركن المادي لجريمة التزوير التقليدية يتمثل في تغيير الحقيقة في المحرر بإحدى الطرق التي نص عليها المشرع اضرارا بالغير، أما في جريمة التزوير المعلوماتي فإن تغيير الحقيقة يتخذ صورتين تتمثل الأولى في التلاعب في المعلومات المخزنة في الحاسب الآلي و الصورة الثانية تتمثل في ادخال معلومات غير صحيحة ينتج عنها مستند غير صحيح .

وقد واجه تطبيق النص التقليدي لجريمة التزوير على جريمة التزوير المعلوماتي صعوبات عدة أهمها الشرط الذي يقتضي أن ينصب تغيير الحقيقة على محرر و هو شرط أساسي في الركن المادي لهذه الجريمة وعلى هذا الاساس قام المشرع الفرنسي باصدار القانون الخاص بجرائم المعلوماتية رقم 88- 19 في جـانفي 1988 و الذي جرم بموجبه تغيير الحقيقة في البيانات و المعلومات المعالجة اليا بمقتضى المادة 462- 5 و المادة 462-6 التي جرمت استعمال هذه المستندات المزورة اليا [1] .

إلا ان هاتين المادتين لاقتا اعتراضا من مجلس الشيوخ الفرنسي لمساواتهما بين المعلومات المعالجة آليا و المحررات ، حيث صدر قانون العقوبات الفرنسي الجديد اثر تعديل سنة 1992 الذي ضم في الفصل الثالث من الباب الثالث المواد 323-1 الى 323-7 ، التي جاء بها القانون رقم 88-19 ، و الذي تضمن جرائم الاعتداء على انظمة المعالجة الالية للمعطيات ، و لم يتم الأخذ بالمادتين 462-5 و 462-6 ، فقد حلت المادة 441-1 محل المادة 155 من القانون القديم حيث توسعت في مفهوم المحرر الذي يقع عليه التزوير و أصبحت تشمل كل سند للتعبير عن فكرة ، بحيث صار يشمل الاقراص الممغنطة و الاسطوانات المدمجة و غيرها ، فتم اخراج جريمة تزوير المستندات المعلوماتية من بين جرائم الاعتداء على نظام المعالجة الالية للمعطيات ، وصارت تخضع للمادة 441-1 من قانون العقوبات الفرنسي.

و افترض المشرع الفرنسي أن تغيير الحقيقة يتم بأي وسيلة كانت ، فعبارة "كل سند للتعبير عن فكرة" تشمل مخرجات الحاسب الآلي المطبوعة على مستند أو دعامة ممغنطة أو مسجلة أو مطبوعة على الورق، اذ صارت العديد من الوثائق الرسمية يعتمد في اصدارها على الحاسب الآلي فهي وثائق معلوماتية تستوجب الحماية نظرا للثقة التي تقتضيها محتوياتها. وسوف نتناول فيما يلي المسائل التي اثارتها فكرة المستند المعلوماتي وكذا الطرق التي يتم بها التزوير المعلوماتي .

أ- 1- المحرر و المستند المعلوماتي :

اشترط المشرع في جريمة التزوير التقليدية أن يقع فعل تغيير الحقيقة على محرر من المحررات العمومية أو الرسمية أو في المحررات العرفية أو التجارية أو المصرفية أو في بعض الوثائق الادارية و الشهادات ، كما اشترط في المحرر أن يكون في شكل " كتابة "أو عبارات خطية ، في حين انه في جريمة التزوير المعلوماتي فان المستند المعلوماتي هو الدعامة المادية التي تم تحويل المعطيات المعالجة عليها ، فيكون إما قرص مضغوط أو شريط ممغنط [2].

فالمستند المعلوماتي الذي يقع عليه فعل التزوير هو كل جسم منفصل أو يمكن فصله عن نظام المعالجة الالية للمعطيات التي نظمها المشرع الفرنسي في الباب الثالث من القسم الثاني من الكتاب الثاني من قانون العقوبات الفرنسي في المواد من 323-1الى 323-7، والتي سوف نتناولها في المطلب اللاحق.

---

[1] La Loi N°88-19 du 5 Janvier 1988 relative à la Fraude Informatique, J.O.R.F,N° 4 du 6 Janvier 1988 .

[2] محمد عقاد ، جريمة التزوير في محررات الحاسب الآلي- دراسة مقارنة - بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون ، دار النهضة العربية ، القاهرة، 1995، ص 36.

وتجريم المشرع الفرنسي لتزوير الوثائق المعلوماتية جاء بسبب ارتباط هذه الوثائق أو المستندات المعلوماتية بقانون الاثبات ، لذلك جاءت المادة 441-1 من قانون العقوبات الفرنسي لتجرم التزوير الذي من شأنه أن يسبب ضررا والذي يتم بأي وسيلة كانت و في محرر أو أي سند للتعبير عن الرأي ، ويشمل ذلك الأقراص الممغنطة و الأسطوانات المدمجة ، وأي بطاقة مغناطيسية أو وسيط يصلح لممارسة حق أو تصرف ، أي أن المشرع الفرنسي اشترط ان يكون للمستند المعلوماتي قيمة في الاثبات لأي حق من الحقوق .

أما بالنسبة للمشريع الجزائري فقد أدرج النصوص الخاصة بتزوير المحررات في المواد من 214 إلى 229 من قانون العقوبات التي تشترط المحرر لتطبيق جريمة التزوير، و عليه فانه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير وهذا ما يستدعي تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدية على غرار المشرع الفرنسي عند اضافته لعبارة " أي سند للتعبير عن الرأي" لتعوض فكرة المحررالتقليدية، أو بإدراج نص خاص بالتزوير المعلوماتي يخرج عن نطاق جرائم المساس بنظم المعالجة الالية للمعطيات التي تناولها في القسم السابع مكرر ضمن المواد من 394 مكررالى 394 مكرر7 والتي تهدف لتحقيق الحماية الجنائية للنظم المعلوماتية [1] .

أ- 2- طرق التزوير التقليدية ومدى استعمالها في التزوير المعلوماتي :

لم يتناول المشرع الفرنسي طرقا محددة يقع بها التزوير في المادة 441-1 المعدلة من قانون العقوبات ، فقد ذكر عبارة " بأي طريقة كانت" بخلاف بعض القوانين الاخرى التي أوردت طرقا معينة للتزويرفي صورته التقليدية كالقانون المصري في المواد 296، 298، 221،712،112 من قانون العقوبات و المواد من 214 إلى 229 من قانون العقوبات الجزائري، وهذه الطرق ذكرت على سبيل الحصر في جريمة التزوير التقليدية ، بخلاف جريمة التزوير المعلوماتي التي أدت الى ظهور أنماط لا تطالها نصوص قوانين العقوبات الحالية ، وتتمثل طرق التزوير فيمايلي :

ب - طرق التزوير المادي:

- **وضع امضاءات او اختام او بصمات مزورة :**

ويتم ذلك عن طريق "الماسح الضوئي Scanner " بادخال صورة لتوقيع او ختم او بصمة و من ثم اضافتها الى ورقة تحتوي على المعلومات المزورة ، وبالتالي تكتسب الوثيقة صفتها الرسمية بعد ان يتم تدوين بيانات غير صحيحة عليها.

- **تغيير المحررات او الاختام او الامضاءات او زيادة كلمات :**

من أساليب التزوير المادي التي يقوم بها الجاني أن يتم تغيير المحررات او الاختام أو الامضاءات أو حذف أو زيادة كلمات إلى المحرر ، أما فيما يخص المستند المعلوماتي فإن الجاني ومن خلال استعماله لجهاز الحاسب الالي يقوم بمعالجة بيانات النص وتغيير بعض محتواه بالاضافة أو الحذف أو التعديل ثم اخراج النص في شكل محرر. وتتشابه هذه الصورة من التزوير مع صور الاعتداء على نظام المعالجة الالية للمعطيات ، ويعاقب المشرع الفرنسي على هذا الفعل ضمن جرائم الاعتداء على نظام المعالجة الالية للمعطيات التي سنتطرق اليها في المطلب اللاحق.

---

[1] القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر66 -156 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات، ج.ر عدد 71، ص 11 .

- **اصطناع محرر:**

يتم اصطناع المحرر بأكمله ويتم امهاره بتوقيع مزور أووضع ختم مزور أو توقيع وختم سليمين ولكن تم الحصول عليهما بطريق غير مشروع، أما في المستند المعلوماتي فإن الجاني يقوم بصياغة المحرر المزور حسب رغبته و من ثم ادخال عناصر المحرر المراد تزويره من ختم و توقيع باستعمال جهاز الماسح الضوئي ، ثم طباعة المحرر المزور فيبدو كانه محرر سليم .

ج - طرق التزوير المعنوي :

- **اصطناع واقعة خيالية:**

تتمثل هذه الصورة من صور التزوير المعنوي في قيام الجاني بجعل واقعة غير حقيقية تبدو وكانها واقعة حقيقية ويقع هذا النوع من التزوير في محرر رسمي في أغلب الاحيان من قبل الموظف العام أو الضابط العمومي المختص بتدوين المحرر، وبما أن جهاز الحاسب الالي عوض الورق و القلم في اعداد الكثير من المحاضر و المحررات الرسمية و العرفية فإن وقوع التزويرالمعلوماتي بهذه الطريقة هو أمر وارد .

- **انتحال شخصية الغير:**

يقصد بانتحال شخصية الغير قيام الجاني بالتعامل متخذا لنفسه هوية غير هويته سواء كانت حقيقية أم وهمية ، وتقع هذه الصورة من التزوير عند قيام الجاني بانتحال شخصية مالك لعقار و من ثم التصرف باسمه أو انتحال شخصية دائن و املاء مخالصة دين إلى غير ذلك من الصور و التي يتصور وقوعها بالطريق المعلوماتي خاصة في مجال البطاقات الائتمانية عندالاستيلاء عليها.

د - عنصر الضرر في التزويرالمعلوماتي:

الضرر عنصر اساسي في جريمة التزوير سواء في صورتها العادية او المعلوماتية ، وقد انقسم الفقه في تحديد مفهوم الضرر في التزوير المعلوماتي بين فريق يضيق من فكرة الضرر ويرى عدم قيامه في التزوير المعلوماتي ، إلا اذا انصب التزوير على وثيقة معلوماتية لها بعد قانوني ، أي معدة لاثبات االحقوق أو نقلها أو تعديلها أو انقضائها ، مستندين على اراء الفقيه " جارو" الذي يرى ان عنصر الضرر يدخل ضمن عناصر الركن المادي للتزوير وقد اخذ المشرع الفرنسي بهذا الرأي، فالمادة 441-1 من قانون العقوبات تشترط حصول ضرر حتى يمكن العقاب على التزوير المعلوماتي، أما الفريق الاخرفقد ربط بين فكرة الضرر في التزوير المعلوماتي و الخسارة الناتجة عن التزوير ، فكلما كانت هناك خسارة فالضرر قائم ، ولا يهم أن تكون الوثيقة معدة للاثبات ام لا [1] .

---

[1] احمد حسام طه تمام ، المرجع السابق ، ص 408.

ثانيا- الركن المعنوي لجريمة التزوير المعلوماتي :

جريمة التزوير المعلوماتي مثل جريمة التزوير في المحررات من الجرائم العمدية التي يلزم لقيامها توافر القصد الجنائي العام بعنصريه العلم و الإرادة ، أي اتجاه إرادة الجاني إلى تغيير الحقيقة مع علمه بأن هذا التزوير أو التغيير في الحقيقة يتم في وثيقة رسمية أو عرفية وأن هذا التغيير من شانه أن يرتب ضررا فعليا أو محتملا ، بالاضافة إلى القصد الجنائي الخاص المتمثل في اتجاه نية المزور إلى استعمال الوثيقة المعلوماتية المزورة ، مع الاشارة إلى أن استعمال الوثيقة المزورة معلوماتيا يشكل جريمة مستقلة عن تزويرها .

أما إذا كان الجاني جاهلاً بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق لديه القصد الجرمي، وكذلك الحال إذا انتفى علم الجاني بأي ركن من أركان الجريمة، فلا يترتب عليه توافر القصد الجنائي لأنه يفترض بالفاعل ان يكون عالماً بكافة أركان جريمته ، كما قد لا يتحقق القصد الجنائي إذا كان الفعل الذي يقوم به الجاني غير واضح بصورة صريحة كما هو الحال بالنسبة لإنتحال صفة الغير أو الاتصاف بصفة غير صحيحة فقد يقوم مبرمج بيانات بتغيير الحقيقة في المحررات ولكنه غير عالماً بهذا التغيير .

و ينتفي القصد الجنائي إذا أهمل المبرمج القائم بتحرير المحرر تغيير بيانات معينة دون قصد فالإهمال وعدم الاحتياط لايحقق العلم في القصد الجرمي هذا من ناحية ، ومن ناحية اخرى يستوجب قيام القصد الجنائي في التزوير المعلوماتي أن تكون ارادة الجاني متجهة إلى احداث النتيجة الجرمية التي وقعت ، أو أية نتيجة جرمية أخرى وهي الاضرار بالأخرين حتى وإن كان هذا الإضرار محتمل الوقوع ، وعليه فإن الركن المعنوي يتحقق في جريمة التزوير المعلوماتي بعلم القائم بفعل التزوير بأن الادخال أو الإتلاف أو المحو أو التحوير للبيانات والبرامجيات المعالجة آلياً يؤدي إلى التأثير على المجرى الطبيعي لتلك البيانات أو المعلومات ، وأنه قد وقع فعله بإرادته التي تتجه الى تحقيق هذا التغيير في الحقيقة لأجل استعمالها أو للتسبب في الأضرار للغير.

وتعقيبا على ما تطرقنا إليه في ما يخص التزوير المعلوماتي ، فإننا نؤكد على ضرورة تدخل المشرع الجزائري لتجريم التزوير الملعلوماتي الذي يقع على مستند معلوماتي كالبطاقات الالكترونية ، وذلك إما بتعديله للنصوص المجرمة للتزوير في المحررات من المواد 214 الى 229 من قانون العقوبات ، مثلما فعل المشرع الفرنسي باضافته لعبارة " اي سند للتعبير عن فكرة " في المادة 441-1 من قانون العقوبات الفرنسي ، مما أمكن معه متابعة أعمال التزوير التي تقع على بطاقات الإئتمان و غيرها من البطاقات المغناطيسية ، لأن هناك فراغ تشريعي في القانون الجزائري في هذا المجال و لا يمكن تطبيق نصوص الجرائم الماسة بأنظمة المعالجة الألية للمعطيات ، بالنظر إلى أن المستند المعلوماتي المتمثل في مخرجات الحاسب الألي كبيانات أو معلومات مسجلة على بطاقات إلكترونية أو أقراص مضغوطة هو جسم منفصل عن نظام المعالجة الألية للمعطيات ولم تنص المواد 394 مكرر و مايليها عن حالة تغيير أو حذف معطيات منفصلة عن نظام المعالجة الآلية.

المطلب الثاني
جرائم الدخول و البقاء والاستعمال غير المصرح به لنظام الحاسب الالي

مع تزايد التعامل بالحاسبات الالية في العديد من المجالات ، ظهرت الحاجة الى اظفاء نوع من الحماية الجنائية لنظام الحاسب الالي و برامج تشغيله ، وهذا بالنظر الى ما تحتويه من معلومات و بيانات مخزنة في هذه الانظمة و ارتباطها بمصالح حيوية للأفراد و المؤسسات .

ولأن للمجرم المعلوماتي اهداف و أغراض مختلفة من اعتداءه على الحاسب الآلي فقد ظهرت اشكال من الجرائم لم يكن لها وجود من قبل كجرائم اختراق نظام المعالجة الالية للمعطيات أو ما تعرف كذلك جرائم الدخول و البقاء و الاستعمال غير المصرح به الى نظام الحاسب الالي.

فهذه الجرائم تفترض وجود نظام للمعالجة الالية للمعطيات الذي عرفه مجلس الشيوخ الفرنسي بأنه « كل مركب يتكون من وحدة أو مجموعة وحدات معالجة ، و التي تتكون كل منها من الذاكرة و البرامج و المعطيات واجهزة الادخال و الاخراج و اجهزة الربط ، والتي يربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام المعالجة الفنية » [1] .

في هذا المطلب سنتناول صورا من صور الاعتداء على نظام المعالجة الالية للمعطيات وهي جرائم الدخول و البقاء و الاستعمال غير المصرح به الى نظام الحاسب الالي ، على ان نتناول صور اخرى كاتلاف و تدمير بيانات الحاسب الالي في المطلب الثالث.

الفرع الاول
جريمة الدخول غير المصرح به لنظام الحاسب الالي

كل الجرائم المعلوماتية تتطلب ابتداءا اتصال الجاني بجهاز الحاسب الالي ، ولأن العديد من الاعتداءات على الانظمة المعلوماتية تستهل باختراق الحاسب الالي ، فإن المشرع أراد حماية المنظومة المعلوماتية أو المعلومات التي تحتوي عليها من الوصول اليها، أو العبث بها من طرف من ليس لهم الحق في الدخول إلى نظام الحاسب الالي . وهناك عدة احتمالات قد تنتج عن الدخول غير المصرح به ، فقد يقوم الجاني بمجرد قراءة المعلومات أو قد يقوم بنسخها مع انها قد تكون سرية كما قد يقوم بمحوها أو تعديلها ، بالاضافة إلى الدخول لإرتكاب جريمة أخرى كالسرقة أو الاحتيال أو الاتلاف أو غيرها من الجرائم ، وفي غالب الأحيان يترتب عن الدخول غير المصرح به خسارة معتبرة تلحق سواء بجهاز الحاسب الالي أو بالمعلومات المحتواة فيه ، إلى غير ذلك من الأضرار ، و لهذه الاسباب اتجهت غالبية التشريعات إلى تجريم الدخول غير المصرح به ، ففي فرنسا يجرم الدخول أو البقاء داخل نظام للمعالجة الآلية للمعطيات بموجب الفقرة الأولى من المادة 323-1 من قانون العقوبات التي تنص على أنه « يعاقب على الدخول أو البقاء في كل أو جزء من منظومة للمعالجة الالية للمعطيات بالحبس سنتين وغرامة مالية تقدر بـ 30.000 اورو » [2] .

---

[1] علي عبد القادر القهوجي، المرجع السابق ص 43.

[2] La Loi N°88-19 du 5 Janvier 1988 relative à la fraude informatique,, J.O. N° 4 du 6 Janvier 1988, article 323-1.

أما في الولايات المتحدةالأمريكية فتجرم المادة (1030 A- -1) من القانون الفدرالي لسنة 1996 الحصول على معلومات عن طريق الدخول غير المصرح به إلى الحاسب الالي ، في حين تجرم المادة (1030- A -3) مجرد الدخول غير المصرح إلى الحاسبات الالية الحكومية فقط [1] .
كما تجرم المادة (1030-A -4) الدخول غير المصرح به إلى نظام الحاسب الآلي متى كان بنية الحصول على أي شيء له قيمة تتجاوز الخمسة الالف دولار امريكي [2].

وقد ورد في نص المادة (1030-A -1) على أنه « يعاقب كل من يتصل عن علم وبصورة غير مرخصة أو اتصل بصورة مرخصة و استغل هذا للحصول على معلومات سرية تابعة للحكومة الامريكية تتعلق بالأمن القومي بهدف الاضرار بالولايات المتحدة الأمريكية أو الحصول على معلومات تتبع مؤسسات مالية بعقوبات تصل إلى الحبس مدة لا تزيد عن عشرين عاما » ، فالقانون الفدرالي الأمريكي لم يجرم الدخول غير المصرح به كسلوك اجرامي بحت مثلما فعل المشرع الفرنسي في المادة 323-1 لكن اشترط سوء النية و الغرض المحدد لهذا الدخول أي أنه اشترط قصدا جنائيا خاصا يتمثل في الحصول على معلومات سرية تتعلق بالحكومة الامريكية .

أما المشرع الجزائري فقد نص في القانون رقم رقم 04-15 المتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات [3] ، وضمن المواد من 394 مكرر إلى 394 مكرر 7 على تجريم ومعاقبة الاعتداءات التي تمس أنظمة المعالجة الالية لمعطيات ، فقد نصت المادة 394 مكرر على أنه « يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج ، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات أو يحاول ذلك » فالمادة اشترطت أن يكون فعل الدخول عن طريق الغش ، و بأي طريقة كانت ،و لم تهتم بكون المنظومة المعلوماتية المخترقة محمية بشيفرة أم لا.

أولا - الركن المادي لجريمة الدخول غير المصرح به لنظام الحاسب الالي :

تقوم جريمة الدخول غير المصرح به إلى نظام الحاسب الالي بفعل الدخول الذي ينطوي على سلوك ايجابي يبدأ بمجرد قيام الفاعل بتشغيل الحاسب الالي فهذه الجريمة تعد من جرائم السلوك المحض حيث أن الاعتداء على الحق الذي يحميه القانون يكون احتماليا فلا يهم ان يتحقق الضرر أم لا ، طالما أن فعل الدخول مجرم بصفة مجردة [4] .
والدخول المجرم يشمل كافة أشكال الولوج إلى نظام الحاسب الالي ، ومن أمثلة ذلك انتهاك كلمة السر أو شفرة الدخول مع عدم التصريح للجاني باستخدامها فهو ولوج بغير ارادة صاحب النظام المعلوماتي أو من له حق السيطرة عليه ، مثل الانظمة التي تتعلق بأسرار الدولة أو تتعلق بحرمة الحياة الخاصة [5] .

---

[1] Olivenbaum (Josef M.), Op.cit, p.586.

[2] Conley (John M .) and Bryan (Robert M.) A Survey of Computer Crime Legislation in the United State , Information and Communication Technology Law, Vol 8, 1999, p.38.

[3] القانون رقم 04- 15 ،مرجع سبق ذكره، المادة 394 مكرر، ص 11 .

[4] Wasik (Martin), The Computer Misuse Act 1990, Crim.L.J. 1990, p.769.

[5] علي عبد القادر القهوجي، المرجع السابق، ص 50.

كما يتحقق الدخول غير المصرح به إذا كان صاحب النظام قد وضع قيودا على الدخول أو كان الدخول يتطلب تسديد مبلغ من المال ولم يقم الجاني بتسديده وتحايل ودخل إلى النظام بصفة غير مشروعة ، حيث يفهم من نصوص المواد المجرمة للدخول غير المصرح به أنها جريمة وقتية أي تتم بمجرد الدخول إلى النظام ، فيكفي أن يكون الجاني من الاشخاص الذين لايحق لهم الدخول إلى هذا النظام حتى يتحقق الركن المادي للجريمة. كما لا يشترط أن يتم فعل الدخول باختراق النظم الامنية ، وهذا ما أكدته محكمة استئناف باريس في حكم صادر لها سنة 1994 [1] .

ومن تطبيقات تجريم الدخول غير المشروع أو غير المصرح به إلى نظام الحاسب الآلي الحكم الذي أصدرته محكمة استئناف جنح AIX-EN PROVENCE في اكتوبر من سنة 1996 عندما ادانت احد مندوبي شركة France télécom عن جريمة الدخول غير مصرح به إلى نظام المعالجة الالية للمعطيات لقيامه بتوصيل جهاز المينيتل Minitel بخط يقدم ألعاب التليماتيك التي تقدم جوائز عن كل اتصال بالبرنامج، فسبب خسائر قدرت بنحو 750.000 فرنك فرنسي، وبعد احالته على المحكمة بتهمة السرقة ، لم تاخذ المحكمة بهذا التكييف و أدين بجريمة الدخول غير المصرح به الى نظام المعالجة الالية للمعطيات حسب المادة 323-1 من قانون العقوبات الفرنسي [2].

كما أيدت محكمة النقض الفرنسية ، القرار الذي اصدرته محكمة استئناف "مونبولييه MONTPELLIER " بتاريخ 12 مارس 2009 ، القاضي بادانة الشخص بغرامة 1000 أورو تطبيقا لنصوص المواد 323- 1 الى 323-3 من قانون العقوبات الفرنسي وذلك لاعتدائه على نظام المعالجة الالية للمعطيات عن طريق نشره لبرامج تتيح امكانية اختراق أنظمة المعالجة الالية للمعطيات [3] .

ثانيا- الركن المعنوي لجريمة الدخول غير المصرح به لنظام الحاسب الالي :

جريمة الدخول غير المشروع أو غير المصرح به إلى نظام الحاسب الآلي من الجرائم العمدية ، وقد اشترطت العديد من النصوص التشريعية كالتشريع الفرنسي الذي نص على الدخول عن طريق الغش شرط القصد العام المتطلب لقيام الجريمة ، حيث يجب أن يعلم الجاني بأنه بدخوله إلى نظام الحاسب الآلي فإنه يعتدي على حق محمي جنائيا وأن محل هذا الحق هو نظام الحاسب الآلي بما يحتويه من معلومات و برامج ، وأنه لا يحق له الدخول إلى النظام فلا تتحقق الجريمة إذا دخل الشخص سهوا أو صدفة ، وعليه في هذه الحالة أن ينسحب فور علمه بعدم مشروعية دخوله .

أما القصد الجنائي الخاص فقد اشترطته بعض التشريعات دون غيرها ، ففي المملكة المتحدة يتطلب قانون إساءة استخدام الحاسب الالي لسنة 1990 في المادة الثانية منه تجريم الدخول غير المصرح به متى توافر لدى الجاني قصد خاص يتمثل في نية ارتكاب جريمة أخرى لاحقة لفعل الدخول [4] .

---

[1] CA de paris, 5 Avril 1994,D.,1994.,I.R.,p130.

[2] جميل عبد الباقي الصغير، الانترنت و القانون الجنائي، دار الفكر العربي القاهرة، 2001، ص 61.

[3] انظر منطوق القرار في الملحق رقم 4.

[4] Bainbridge (David), Hacking -The Unauthorised Access of Computer System, the Legal Implications, M.L.Rev.,March 1989,vol 52, p.211.

الفرع الثاني
جريمة البقاء غير المصرح به في نظام الحاسب الالي

يعرف البقاء غير المصرح به داخل نظام الحاسب الآلي أو نظام المعالجة الالية للمعطيات بأنه « التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام » [1] ، وقد كان غرض المشرع من تجريم فعل البقاء داخل نظام المعالجة الالية للمعطيات هو تجريم هذا الفعل بالنسبة لمن كان دخوله إلى نظام الحاسب الآلي بمحض الصدفة ، و انتفى لديه القصد الجنائي لفعل الدخول غير المصرح به ، وبالتالي إذا كان دخوله صدفة و بقي داخل نظام الحاسب و انصرفت ارادته إلى ذلك فإنه يعاقب عن فعل البقاء غير المصرح به دون فعل الدخول غير المصرح به [2] .

وفعل البقاء غير المصرح به داخل نظام الحاسب مجرم في أغلب التشريعات التي تناولته ، حيث نصت المادة 323- 1 من قانون العقوبات الفرنسي و المادة 394 مكرر من قانون العقوبات الجزائري عن فعل البقاء غير المشروع عن طريق الغش داخل كل أو جزء من منظومة معلوماتية ، أما المشرع الأمريكي فقد جرم فعل البقاء غير المشروع عن طريق تجريمه لتجاوز الدخول المصرح به أو تجاوزالحدود الممنوحة للدخول المصرح به حسب نص المادة (1030 - A -6) من القانون الفدرالي لجرائم الحاسب الآلي [3].

اولا - الركن المادي لفعل البقاء غير المصرح به داخل نظام الحاسب الالي :

تقوم جريمة البقاء غير المصرح به داخل نظام الحاسب الالي بسلوك اجرامي سلبي يتمثل في رفض خروج الجاني الذي دخل صدفة الى نظام الحاسب الالي مع علمه بأن دخوله و بقاءه غير مصرح بهما ، فبامتناعه عن الخروج يتحقق الركن المادي للجريمة .

ثانيا - الركن المعنوي لفعل البقاء غير المصرح به:

جريمة البقاء غير المصرح به من الجرائم العمدية ، ويتطلب لقيامها توافر القصد الجنائي العام بعنصريه العلم و الارادة ، اذ يجب ان يعلم الجاني ان بقاءه هو سلوك مجرم وانه ضد رغبة من له حق السيطرة على نظام الحاسب الالي ، ومع ذلك فان ارادة الجاني تتجه الى البقاء داخل النظام ، وعليه فان القصد الجنائي لا يقوم اذا كان فعل البقاء سهوا او خطأ، اما في غير ذلك من الحالات فمتى توافر القصد الجنائي فانه لا مجال للاعتداد بالباعث ولو كان ذلك لمجرد الفضول [4] .

---

[1] علي عبد القادر القهوجي، المرجع السابق، ص 52.

[2] احمد حسام طه تمام، المرجع السابق،ص 399 .

[3] 18 USC § 1030 – 6 in : http://www.cybercrime.gov/ccmanual/ccmanual.pdf , Op.cit, p49.

[4] علي عبد القادر القهوجي، المرجع نفسه ،ص 54.

الفرع الثالث
جريمة الاستعمال غير المصرح به لنظام الحاسب الآلي

من بين التحفظات الواردة في القواعد العامة لجريمة السرقة التقليدية، أن السرقة لا تقع على المنفعة [1].
اذ أن فعل الاختلاس لا يتصور إلا في الاشياء المادية ، كما سبق وأن وضحنا ذلك من خلال اراء الفقهاء ، ونفس الشيء يمكن قوله في جريمة الاستعمال غير المصرح به لنظام الحاسب الآلي ، التي تعرف تسميات متعددة تصب كلها في نفس المفهوم ، ومنها جريمة اساءة استخدام وقت الحاسب الالي، أو سرقة وقت الحاسب الالي ، واخيرا جريمة سرقة الخدمة و سرقة منفعة الحاسب الالي .

و من أمثلتها اكتشاف استخدام الحاسب الآلي في أكبر معامل انتاج الصواريخ النووية في الولايات المتحدة الامريكية من قبل مائتي مستخدم، وذلك لأغراضهم الشخصية [2] ، وقد لاقى تكييف هذا الفعل صعوبات كثيرة ، فهناك من اعتبره سرقة للتيار الكهربائي [3] ، وغيره كيفه على أنه احتيال ، والبعض وصف الفعل بأنه اساءة ائتمان ، والبعض الاخر اعتبره استعمالا لأشياء الغير بدون وجه حق [4] .

ومما لاشك فيه أن اثار هذه السلوك الاجرامي تظهر في الجانب الاقتصادي لكبريات الشركات المطالبة بتسديد قيمة الوقت الفعلي لاستخدام الحاسبات الآلية أو عندما يتسبب هذا الاستعمال غير المصرح به في فقدان الشركة لخدماتها أو لزبائنها كنتيجة لذلك .
فيما لم يتضمن القانون الفرنسي نصا صريحا لتجريم سرقة وقت الحاسب الآلي أو الاستعمال غير مصرح به لنظام الحاسب الالي ، عندما تناول في فصل المعالجة الالية للمعطيات ضمن المادة 323 من قانون العقوبات الفرنسي ، تجريم الدخول و البقاء غير مصرح بهما داخل نظام الحاسب الالي ، حيث انقسم الفقه الفرنسي حول تجريم الاستعمال غير المصرح به بين فريق يرى أن الاستعمال غير المصرح به لنظام الحاسب الالي يدخل ضمن مفهوم الدخول والبقاء غير المصرح بهما داخل نظام الحاسب الالي باعتبار فعل الدخول والبقاء سابق على فعل الاستعمال [6] ، من جهة مقابلة رأى فقهاء اخرون أن نص جريمة الدخول أو البقاء غير المصرح بهما داخل نظام الحاسب الآلي لا يمكن تطبيقه على الاستعمال غير المصرح للحاسب الالي ، باعتبار أن جريمة الدخول غير المصرح به هي جريمة وقتية تتم بمجرد الدخول إلى نظام الحاسب الالي بخلاف جريمة الاستعمال غير المصرح به و التي تعتبر جريمة مستمرة أي تتطلب فترة زمنية لقيامها [7] .

كما أنه في جريمة الاستعمال غير المصرح به لنظام الحاسب الالي استخدام لوظائف الجهاز في حين أن الدخول أو البقاء لا يتعدى كونهما تواجدا من غير استخدام لوظائف الحاسب الالي و علل انصار عدم ملاءمة تطبيق نص المادة 323 من قانون العقوبات الفرنسي بالنظر في الغاية من تجريم فعلي الدخول والبقاء وهي حماية المعلومات ، أما في الاستعمال غير المصرح به فإن الغاية تكمن في حماية النظام بكامله بالاضافة إلى أن جريمة الاستعمال غير المصرح به قد تحدث على الرغم من أن الدخول أو البقاء كانا مصرحا بهما.

---

(1) محمد زكي أبو عامر، قانون العقوبات، القسم الخاص، دار المطبعات الجامعية ، الاسكندرية ، 1989 ،ص 910 .
(2) هدى حامد قشقوش ، المرجع السابق ،ص 82 .
(3) محمد حسام لطفي ، الحماية القانونية لبرامج الحاسب الالي ، دار الثقافة للطباعة و النشر ،ص 160 .
(4) محمود أحمد عبابنة ، المرجع السابق ، ص 89.
(6) Vivant (M) et Le Stanc (Ch), Lamy droit de l'Informatique,1989,N°2479,p.1504.
(7) Champy (Guillaume), Fraude informatique, Thèse, Université Aix-Marseille III, 1990, p.508.

وقد حاول الفقه الفرنسي ايجاد مفهوم مشترك أو حل موحد لتكييف جريمة الاستعمال غير المصرح به، لكنه لم يوفق في ذلك فبين من رأى امكانية تطبيق نصوص السرقة ، استنادا على فكرة سرقة الكهرباء، التي لا تتطلب الانتقال المادي في فعل الاختلاس بل يكفي مجرد الاعتداء على حيازة الشيء اثناء فترة الاستخدام [1] ، والذين وجدوا في نص جريمة النصب حلا يتوافق مع فعل الاستخدام غير المصرح به للحاسب الآلي لما في ذلك من استعمال لطرق احتيالية عند الدخول لنظام الحاسب الالي لاستغلاله [2].

و هناك من رأى عدم امكانية تطبيق أي من هذه النصوص على السلوك محل الخلاف ، حيث أن فعل الاختلاس في جريمة السرقة يعني الاستئثار بالسيطرة على المال محل الجريمة وهو ما لا يتوافق في حالة الحاسب الالي خاصة عندما يكون نظام الحاسب يقدم عدة خدمات لمستعملين اخرين وهذا عند استعمال أنظمة مشتركة أو عند التعامل عن بعد في حالة توفر شبكة اتصال [3].

و انتقد أصحاب هذا الرأي فكرة القياس على سرقة الكهرباء باعتبار أن محل التجريم في هذه الحالة هو الكهرباء أو الطاقة المستعملة من قبل الحاسب و ليست الخدمة التي يقدمها .

كما وجهوا النقد الى من قال بامكانية تطبيق نصوص جريمة النصب نظرا لأن الاشياء المتحصلة في جريمة النصب هي قيم مادية و أموال، أما المزايا المتحصل عليها من خلال استخدام الحاسب لا تمثل قيمة مالية محددة ، غير أن جانبا اخرا من الفقه الفرنسي رأى بخلاف كل ذلك أن الصياغة الجديدة للمادة 313 - 1 من قانون العقوبات الفرنسي جاءت اكثر مرونة من المادة السابقة 405 التي حصرت المحل الذي تقع عليه جريمة النصب و هي « " اموال Fonds "،" المنقولات Meubles"،" التزامات Obligations "،" تصرفات Disposition"، "سندات Biellets "، " وعود Promesses ، "مخالصات Quittances " ، "ابراء من اعباء Décharges" » [4].

أما المادة 313 - 1 فقد حددت محل جريمة النصب المتمثل في" أموال Fonds" ، " قيم مادية Valeurs " ، " أي منفعة كانت Bien quelconque " ، "تقديم خدمة ما Fournir un service "، "الموافقة على تصرف ينشأ عنه التزامات أو اعباء Consentir un acte operant obligations ou décharges "، خاصة مع اضافة عبارة " أي منفعة كانت Bien quelconque " التي أزالت الطابع الحصري للمادة السابقة وجعلت النص أكثر مرونة ، إذ من الممكن تطبيق هذا النص على الحالات الناشئة في مجال تكنولوجيا المعلومات .

أما الرأي القائل بإمكانية تطبيق نص خيانة الأمانة على الاستعمال غير المصرح به ، فقد انتقد لكون أن جريمة خيانة الامانة تقتضي وجود عقد عمل ينص على تسليم الحاسب الآلي للعامل لأداء عمل محدد [5] ، بالاضافة إلى أن أشخاصا اخرين من غير العمال قد يستعملون الحاسب الالي وبالتالي لا ينطبق عليهم الامر في هذه الحالة [6] .

---

(1) Linant de Bellfonds (Xavier) et Hollande (Alain), pratique du Droit de l'Informatique, Op.cit, p 257.

(2) Gassin (Raymond), Le droit pénal de l'informatique, D.1986, Chr.V, p 35.

(3) Devèze (Jean), Op.cit, pp.185-213.

(4) Lamy droit de l'informatique, 1997 ,N° 2451, p. 1437.

(5) Aupècle Guicheney (Nadine), Les infractions pénales favorisées par l'Informatique ,Thèse,Université de Monpellier, 1984, N° 229.

(6) Chamoux (Françoise), La Loi sur la Fraude Informatique : de nouvelles incriminations, J .C.P., 1988, Doctrine 3321. N°8.

من خلال ما استعرضنا يمكن القول أن الفقه الفرنسي لم يتناول صراحة جريمة الاستعمال غير المصرح به للحاسب الآلي ، و ترك حرية تكييف الفعل للسلطة التقديرية للقضاة .

ويرجع عدم تجريم أغلب التشريعات لفعل الإستعمال غير المصرح به لنظام الحاسب الآلي إلى ضآلة قيمة الخسائر الناتجة عن هذا الإستعمال والتي لا تتعدى في أغلب الحالات قيمة استهلاك التيار الكهربائي ، مما لم يستوجب تدخل المشرع الجنائي لتجريم الفعل .

وعلى غرار المشرع الفرنسي ، فإن المشرع الإنجليزي رأى أن تجريم الاستعمال غير المصرح به للحاسب الآلي هو أمر غير سوي ، وأن هناك نصوصا يمكن تطبيقها على هذا الفعل ، حيث أشار بعض الفقهاء إلى تطبيق نص السرقة على الاستعمال غير المصرح به لنظام الحاسب الآلي ، إلا أن هذا الرأي انتقد لعدم وجود نية التملك لدى الفاعل الذي لا ينوي حيازة الخدمات التي يقدمها الحاسب الآلي ، وأمام صعوبة تطبيق نص السرقة رأى بعض الفقهاء إمكانية تطبيق نص جريمة الحصول على الخدمات أو المنافع عن طريق الاحتيال على فعل الاستعمال غير المصرح به للحاسب الآلي [1]، والذي ينص على أنه « ...يعاقب كل من يحصل بطريق الاحتيال على خدمات أو منافع يقدمها الغير ...بأن يجعل هذا الأخير يعتقد أن هذه المنفعة قد تم تسديد ثمنها ... »[*].

إلا أن تطبيقات هذا النص أثبتت أن أغلب مستعملي الحاسب الآلي من موظفي الشركات يمتلكون شيفرات الدخول مما ينفي فكرة الاحتيال التي وردت في النص ، وأمام صعوبة تكييف الفعل رأى بعض الفقهاء أن سكوت المشرع عن تجريم الفعل لا يمنع الشركات من مواجهة الاستعمال غير المصرح به للحاسب الآلي بجزاءات داخلية.

غير انه يوجد بعض التشريعات الاخرى التي تطرقت لهذا الفعل ومنها الولايات المتحدة الامريكية ، حيث جرم قانون ولاية فرجينيا الصادر سنة 1986 الاستعمال غير المصرح به للحاسب الالي او سرقة الخدمات التي يقدمها الحاسب الالي ، حيث جاء في نص المادة " كل من يستخدم عمدا و بسوء نية حاسبا اليا او شبكة للحاسبات الالية بغرض الحصول عل الخدمات التي يقدمها الحاسب او الشبكة دون ان يكون مصرحا له بذلك يعد مرتكبا لجريمة سرقة خدمات الحاسب الالي" [3].

أما المشرع الجزائري الذي لم يجرم الاستعمال غير المصرح به لنظام الحاسب الآلي في قسم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فكان من الافضل أن يتجه إلى تجريم الفعل أسوة بالمشرع الأمريكي على أن يرتبط التجريم بسوء نية الفاعل ، وهذا بالنظر الى الزيادة الكبيرة في استعمال الحاسبات الآلية في الشركات و المؤسسات العمومية و الخاصة ، وللأعباء الاقتصادية التي تنتج عن اساءة استعمال الحاسب الآلي ، لكن يجب على المشرع أن يحدد الحالات التي تنطوي على استعمال غير مصرح به وأن لا يتم تجريم مجرد القيام بعمليات بسيطة التي يقوم بها الموظفون و التي لا تنطوي على خسائر كبيرة كالألعاب الترفيهية أو ماشابهها .

---

[1] Taper (Colin) , Computer low ,3rd edition,Longman,London, 1983,P.290.

[*] المادة 1 من النص الخاص بجرائم السرقة في القانون الانجليزي لسنة 1978.

[2] Kurtz (Robin K.), Computer Crime in virginia :A Critical Examination of the Criminal Offenses in the virgivinia Computer Crime Act,W.M.L.Rev, 1986, Vol 27, p.783.

المطلب الثالث

جريمة إتلاف المعلومات و تخريبها باستعمال الفيروسات

لا يثيرموضوع اتلاف المكونات المادية للحاسب الآلي أي اشكال، باعتبارتجريم المشرع للاتلاف العمدي لملك الغير في أغلب النصوص التقليدية لجريمة الإتلاف ، فقد جرمه المشرع الجزائري في المادة 412 من قانون العقوبات ، والمشرع الفرنسي في المادة 443 و المشرع المصري في المادة 361 .
اما اتلاف المكونات غير المادية للحاسب الالي و المتمثلة في المعلومات و البرامج فقد تدخل المشرع في العديد من الدول لتجريمه بصفة مستقلة عن اتلاف الدعامة الحاملة للمعلومات كما سنوضح ذلك في هذا المطلب من خلال تناولنا لإتلاف المعلومات إما بمحوها أو حذفها أو تدميرها أو باستعمال البرامج المختلفة كالفيروسات.

الفرع الاول
جريمة إتلاف المعلومات

استخدمت العديد من التشريعات التي جرمت الاتلاف المعلوماتي تعبير اخفاء المعلومات أو محوها للتعبير عن تدميرها ، و قد تضمنت المادة المادة 462-4 من قانون العقوبات الفرنسي لسنة 1988 الخاص بجرائم المعلوماتية و التي حلت محلها في تعديل سنة 1994 المادة 323 -3 تجريما لفعل اتلاف المعلومات ، و لم يضع المشرع الفرنسي شروطا تتعلق بطبيعة المعلومات بل ترك النص عاما ويتسع ليشمل كافة المعلومات [1].

وفي المملكة المتحدة تم تجريم الاتلاف العمدي للمعلومات بموجب المادة الثالثة من قانون اساءة استخدام الحاسب الالي لسنة 1990 ، والتي نصت على أنه يعد مرتكبا لجريمة الاتلاف المعلوماتي " كل من يقوم بعمل من شأنه احداث تغييرات غير مصرح بها في محتوى أي حاسب آلي،متى توافر لديه العلم و الارادة وقت قيامه بهذا الفعل" [2].

أما في الولايات المتحدة الأمريكية فقد نصت المادة (1030- A-5) من القانون الفدرالي الخاص بجرائم الحاسب على جريمة الاتلاف المعلوماتي، إلا أنها اشترطت أن يكون الحاسب الآلي تابع لحكومة الولايات المتحدةالأمريكية أو يستخدم لصالحها ، كما أضافت حالة أخرى إذا كان الإتلاف يتعلق بمعلومات طبية و ترتب عن هذا الاتلاف خسارة مادية تقدر بألف دولار [3].
ولم يغفل المشرع الجزائري عن تجريم فعل إتلاف المعلومات ، فقد نص عليه ضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أين ذكر عدة صور من جريمة إتلاف المعلومات، وتتمثل هذه الصور فيما يلي :

---

(1) Bibent (Michel), Le Droit du traitement de lnformation, Nathan, Paris 2000, p.121.

(2) Wasik (Martin), Op.cit, p767.

(3) Griffith (Doddss), The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem, V .L.Rev, vol. 43, p.453.

- إتلاف المعلومات كظرف مشدد لجريمة الدخول غير المصرح به لنظام الحاسب الآلي، حيث نصت المادة 394 مكرر من قانون العقوبات على أنه « ...تضاعف العقوبة اذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ».

- تجريم تخريب نظام اشتغال المنظومة المعلوماتية في المادة نفسها «... وإذا ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر الى سنتين و الغرامة من 50.000 دج الى 150.000 دج...» .

- تجريم ازالة أو تعطيل بطريق الغش المعطيات التي يتظمنها الحاسب الآلي ، من خلال نص المادة 394 مكرر 1.

ولتوضيح البنيان القانوني لجريمة اتلاف المعلومات نتطرق لأركان الجريمة فيما يلي :

أولا- الركن المادي لجريمة اتلاف المعلومات :

يتمثل الركن المادي في جريمة اتلاف المعلومات إما في اجراء تعديلات جزئية أو كلية لها بصورة غير مشروعة Modification ، كما قد يتخذ صورة " تدمير هذه المعلومات Destruction " أو " ادخال معلومات بشكل غير مشروع إلى نظام الحاسب الالي Introduction " ، حيث نصت الكثير من قوانين العقوبات على الادخال غير المشروع للمعلومات كصورة من صور التدمير .

و التعديل هو كل تغيير غير مشروع للمعلومات و البرامج ويتم عن طريق استخدام إحدى وظائف الحاسب الآلي، أما تدمير المعلومات ، حسبما ورد في توصية المجلس الاوروبي بخصوص الجرائم المعلوماتية ، فهو محوها بصورة كلية أو اخفاءها بحيث لا يمكن الوصول اليها .[1]

في حين أن فعل الاتلاف بالادخال غير المشروع للمعلومات يترتب عنه تعديل للمعلومات أو تدميرها ، وفي احدى تطبيقات القضاء الفرنسي لجريمة اتلاف المعلومات بفعل ادخال غير مشروع للمعلومات ، أدانت محكمة استئناف باريس سنة 1990 أحد الاشخاص بتهمة اتلاف المعلومات لقيامه بادخال معلومات غير صحيحة إلى نظام الحاسب الآلي [2] ، كما ايدت محكمة النقض الفرنسية سنة 1994 حكما قضى بادانة احد الاشخاص بتهمة اتلاف المعلومات لقيامه بتدوين بيانات غير صحيحة تتعلق بالنسب الخاصة بضريبة المبيعات [3] .

---

[1] La Recommandation N ° R (89) 9 sur la criminalité informatique et le rapport final du Comite d'Europe sur le problème de la criminalité, Strasbourg, 1990.

[2] CA de Paris, 28 Novembre 1990, Juris-Data, N°25569.

[3] Cass.Crim.5Janvier 1994, J .C.P.EditionGénéral, 1994, N°856.

ثانيا - الركن المعنوي لجريمة الاتلاف :

جريمة اتلاف المعلومات هي جريمة عمدية ، حيث تتطلب أغلب التشريعات لقيامها القصد العام ، أي علم الجاني بأن ما يقوم بفعله من شأنه أن يؤدي إلى اتلاف المعلومات أو تعديلها مع اتجاه ارادته الى ارتكاب هذا الفعل ، أما التشريعات التي تطلبت قصدا خاصا يتمثل في نية تحقيق الربح او الاضرار بالغير، كالتشريع البرتغالي و التركي فقد تعرضت لانتقاد بعض الفقهاء ، اذ أنه بتطبيق القصد الجنائي الخاص فإنه يؤدي إلى استبعاد العديد من أفعال الاتلاف وعدم تجريمها عندما لا تتجه نية الجاني إلى تحقيق ربح مادي أو اضراره بالغير على الرغم من قيمة المعلومات المتلفة ، كما أن تقدير الخسائر يجب الا يقتصر على الاضرار المادية فقط التي تلحق بالمجني عليه [1]، وبسبب هذا النقد تراجع المشرع الفرنسي عن اشتراط القصد الخاص عند تعديله لقانون العقوبات سنة 1992.

الفرع الثاني
تخريب المعلومات باستعمال الفيروسات

شهد العالم انتشارا في استخدام الفيروسات او البرامج الخبيثة للاعتداء على أجهزة الحاسب الالي وازدادت وتيرة الاعتداءت مع انتشار استخدام الأنترنت و استعمال البريد الالكتروني الذي يساعد في انتقالها و رغم أن غالبية التشريعات لم تتناول الاشارة الى استخدام الفيروسات كسلوك مستقل عن جريمة الاتلاف أو التعديل غير المصرح به إلا أنه من الشائع القيام باتلاف المعلومات و البرامج باستعمال الفيروسات التي تختلف في اساليبها في اتلاف المعلومات ، وهذا ما جعل المشرع الامريكي يقوم سنة 1989 باصدار قانون فدرالي لمكافحة فيروسات الحاسبات الالية حيث يجرم فيه اعداد و توزيع البرامج الخبيثة . إلا أن هذا القانون تعرض للنقد كونه لم يفصل بين اعداد البرنامج الخبيث و توزيعه فصدر سنة 1994 قانون يجرم نقل الفيروس أو البرنامج الخبيث كسلوك مستقل عن اعداده .[2]

ومن أشهر الفيروسات و البرامج الخبيثة نذكر فيروس "حصان طروادة Trojan horses " الذي يتمتع بقدرة كبيرة على الاختفاء داخل البرنامج الأصلي ثم القيام بتعديله أو تغييره أو تدمير محتواه .
وتستعمل كذلك في اتلاف المعلومات ، البرامج الخبيثة كبرنامج الدودة Worm Software" ، الذي يرجع ظهوره إلى سنة 1988 حيث كانت جريمة الاعتداء باستخدام فيروس مايعرف بدودة موريس، حيث قام الطالب" روبرت موريس Morris Robert " ، وهو باحث في الدكتوراه بجامعة كورنيل في الولايات المتحدة الأمريكية بإعاقة أكثر من ستة آلاف جهاز حاسب آلي خاص بوكالة الفضاء الأمريكية ناسا NASA ، مستخدما برنامج الدودة على شبكة الانترنت وقد ترتب عن ذلك خسائر قدرت باثني عشر مليون دولار، وعند تقديمه للمحاكمة ظهر الفراغ التشريعي فيما يتعلق باستخدام البرامج الخبيثة في تعطيل أجهزة الحاسب الالي فالمادة (A- 1030) من القانون الفدرالي الخاص بجرائم الحاسب والمتعلقة بمعاقبة الدخول العمدي غير المصرح به لا تتفق مع حالة الطالب موريس الذي لم تتجه نيته إلى اعاقة الانظة المعلوماتية وإنما كان استعماله لبرنامج الدودة بهدف اجراء دراسة على الجوانب الأمنية لأنظمة الحاسبات الالي على شبكة الانترنت [3] .

---

(1) Vergutch (Pascal), Op.cit.p233.
(2) Vergutch (Pascal), Ibid, p.286.
(2) Marion (Camille Cardoni), Computer Viruses and the Law , D,L,Rev.1989 ,vol. 93,p.92 .

أما في فرنسا فإن جريمة اتلاف المعلومات باستخدام الفيروسات يسري عليها النص المتعلق باتلاف المعلومات بصفة عامة الوارد ضمن المادتين 323-2 و 323-3-1 من قانون العقوبات ، فقد نصت المادة 323-3-1 على تجريم حيازة بدون وجه شرعي أو وضع تحت تصرف أو تقديم برنامج أو معطيات يمكن ارتكاب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، وعليه فقد ذهبت محكمة النقض الفرنسية في حكم لها صادر سنة 1996 إلى أن ادخال البرامج الخبيثة إلى نظام الحاسب الآلي هو سلوك معاقب عليه تطبيقا للفقرة الثانية من المادة 323 من قانون العقوبات الفرنسي [1] ، أما محكمة جنح ليموج فقد ادانت سنة 1994 شخصا بتهمة اتلاف المعلومات داخل نظام الحاسب الآلي باستعمال برنامج خبيث هو" حصان طروادة " [2]،

وبخلاف المشرع االفرنسي فإن المشرع الجزائري جرم اتلاف المعلومات دون الإشارة إلى استخدام الفيروسات أو البرامج الخبيثة ، فنصوص المواد 394 مكرر الى 394 مكرر 1 و 394 مكرر 2 جرمت اتلاف المعلومات أو المعطيات المعلوماتية عن طريق حذفها أوتغييرها أو تعديلها أو تجميعها بشكل غير مشروع ، وجاء هذا التجريم ضمن نصوص عامة تتسع لتشمل كافة أنواع المعلومات وكل أشكال الاتلاف مهما كانت الطريقة المتبعة في ذلك، كما أن نص المادة 394 مكرر 2 الذي جرم « ...تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم... » فعند ذكر المشرع لعبارة " يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم " مما يمكن القضاة من ادخال اتلاف المعطيات المخزنة بأي وسيلة كانت ومن ضمنها الفيروسات.

وتتعدد أنواع الفيروسات و البرامج الخبيثة المستخدمة في اتلاف المعلومات كما تختلف في خصائصها كما سنبين ذلك فيما يلي:

أولا- أنواع الفيروسات المستخدمة في اتلاف المعلومات :

عرف أحد الخبراء وهو "Fred Cohen " الفيروسات بأنها نوع من البرامج التي تؤثر في البرامج الأخرى بحيث تعدل في تلك البرامج لتصبح نسخة منها، وهذا يعنى ببساطة أن الفيروس ينسخ نفسه من حاسب آلي إلى حاسب آلي اخر بحيث يتكاثر بأعداد كبيرة [3] .

وفيروسات الحاسب الآلي هي عبارة عن أنواع من البرامج إلا أن الأوامر المكتوبة في هذه البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالة البريدية المرسل معها الفيروس تحدث اصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به.

ويمكن تقسيم الفيروسات إلى خمسة انواع :

1- الفيروسات المصاحبة للبرامج التشغيلية " exe": وهي فيروسات ترافق الملفات المسؤولة عن تشغيل البرامج الموجودة على الحاسب مثل نظام الدوز أو الوندوز وبالتالي فإن إصابة هذه الملفات يؤدي إلى تعطيل البرنامج بالكامل .

---

(1) Cass.Crim.12 Décembre 1996, Bull.crim.N° 465.

(2) Corr.de Limoge, 14 Mars 1994, E.S.I,Juin 1994, p 238.

(3) انظر في الموقع: Highley, Reid. (1999). Viruses: The Internet's Illness.[Online]

http://www.chemistry.vt.edu/chem- dept/dessy/honors%20/papers99/highleh.html

2- برامج الدودة Worm software: وهي عبارة عن برامج تقوم باستغلال أية فجوة في أنظمة التشغيل لكي تنتقل من حاسب لآخر، وهي لا تقوم بحذف أو تغيير الملفات بل تقوم بالقضاء على موارد الجهاز و استخدام الذاكرة بشكل كبير مما يؤدي إلى بطء ملحوظ جداً في الجهاز، وتتكاثر هذه البرامج أثناء عملية انتقالها بإنتاج نسخ منها.

3- فيروس حصان طرواده Trojan horses: ينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي فلا يمكن ملاحظته بواسطة مضادات الفيروسات إلا أن اثره التدميري خطير حيث لا يمكن الشعور به أثناء قيامه باداء مهمته التخريبية او التجسسية وبالتالي فإن فرص القضاء عليه تكون شبه معدومة . كما تعمل هذه الفيروسات على اخفاء نفسها عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيير أشكالها و تكمن خطورة فيروس حصان طروادة كذلك في أنه يتيح للدخيل الحصول على " كلمات المرور passwords" وبالتالي الهيمنه على الحاسب الآلي بالكامل. كما أن المتسلل لن يتم معرفته أو ملاحظته كونه يستخدم الطرق المشروعة التي يستخدمها مالك الجهاز. [1]

4- **القنبلة الزمنية Time bombe :** تكون بشكل فيروس ينشط في تاريخ معين محدد بالذات، فهو يثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة والوقت اللازم [2].

5- **القنبلة المنطقية Logic bombe:** هذا النوع ينشط بمجرد حدوث واقعة معينة مثل بدأ تشغيل الجهاز أو عند إنجاز أمر معين في الحاسب الآلي أو عند بدأ تشغيل برنامج معين[3].

ثانيا- خصائص الفيروسات [4] :

تمتاز الفيروسات بمجموعة من الخصائص تمكنها من القيام بدورها التخريبي ، ومنها :

أ) القدرة على التخفي: للفيروسات قدرة كبيرة على التخفي والخداع عن طريق الارتباط ببرامج أخرى للتمويه كالدخول إلى ملفات مخفية أو الخاصة بالذاكرة وبعد فترة معينة أو مباشرة يشغل نفسه ويبدأ بنشاطه التدميري.

ب) القدرة على العدوى: للفيروسات القدرة على التكاثر وزيادة أعدادها ، حيث يزرع الفيروس على الاسطوانات الخاصة بالحاسب، وبمجرد تحميله ينتقل وينسخ نفسه من جهاز لآخر بسرعة كبيرة.

ج) الاختراق: يتمتع الفيروس بقدرة فائقة على الدخول للنظام والتسلل إليه واختراق كل سبل الحماية.

د) التدمير: الهدف الأساسي للفيروسات هو تخريب وتعطيل البرامج، وأهم مظاهرها إبطاء جهاز التشغيل ، ومن اشهر تقنيات تدمير المعلومات ما يعرف بـ" crashing" وتعتمد على بث برامج تقوم باتلاف كافة البرامج المخزنة في ذاكرة الحاسب الالي [5].

---

[1] انظر في الملحق رقم 1- المصطلحات الواردة في الدراسة.

[2] محمد امين الرومي،جرائم الكمبيوتر والانترنت،دار المطبعة الجامعية، الاسكندرية،2004، ص 56.

[3] محمد امين الرومي،المرجع نفسه،ص57.

[4] محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة للنشر الإسكندرية، طبعة 2003، ص 294.

[5] Gomez (Urbina A)., Rivero(A). et Lopez (N)., Hacking Interdit, 1ère édition, Paris, 2006.p5.

المبحث الثاني

صور جرائم الأنترنت

تمثل جرائم الأنترنت البعد العالمي لجرائم الحاسب الالي ، والأنترنت شبكة تتالف من عدد كبير من الحاسبات الآلية و التي ترتبط فيما بينها إما عن طريق الخطوط الهاتفية أو عن طريق الاقمار الصناعية ، أما خدمة الأنترنت فيتحصل عليها الشخص باشتراكه ودفع مقابل هذه الخدمة أو عن طريق استفادة مشروعة منها فيتمكن من ربط الاتصال مع عدد كبير من الحاسبات الآلية عبر العالم ، و بسبب التطور الهائل لتكنولوجيا المعلومات ، وبالنظر للعدد الهائل من الأفراد و المؤسسات الذين يرتادون هذه الشبكة ومن خلال الإمكانيات التي تتيحها كتبادل المعلومات وربط الإتصال مع أي جهاز مزود بخدمة الانترنت ، ونتيجة للإستغلال السيء لهذه الخدمة ، أصبحت مسرحا لكثير من الجرائم التي يطلق عليها جرائم الأنترنت ، أو الجرائم الإلكترونية ، أو كما تسمى حاليا عند الاوربيين الجرائم السيبرانية أو جرائم الفضاء الإفتراضي .

و تفترض هذه الجرائم وجود جهاز حاسب آلي وهو الكيان المادي للنظام الالي لمعالجة المعلومات ، ويشمل كل المكونات المادية من الأجهزة و الآلات والمعدات...الخ [1] ، بالإضافة إلى وجود كيان معنوي يتمثل في البرامج و المعلومات التي يتم تحميلها على جهاز الحاسب الآلي ليكون قادرا على آداء وظائفه.[2] بالاضافة إلى ذلك يشترط وجود خدمة الانترنت التي اطلق عليها اسم الشبكة المتكاملة من المعلومات و الاتصالات التي تقوم على استخدام اجهزة الكمبيوتر المرتبطة ببعضها وطنيا أو اقليميا أو عالميا . [3]

أما عن نوع الجرائم التي ترتكب بحق مرتادي شبكة الأنترنت سواءا كانوا أفرادا أو مؤسسات فقد تنوعت ولم تعد تقتصر على اختراق الشبكة وتخريبها أو سرقة المعلومات ، فقد ظهرت أيضا الجرائم الأخلاقية كممارسة الدعارة عبر الأنترنت ، و انشاء المواقع الاباحية ، و الاستغلال الجنسي للاطفال ، بالاضافة الى الجرائم الماسة باعتبار الأشخاص كالتهديد و السب و القذف و الاعتداء على حرمة الحياة الخاصة ، هذا فضلا عن الجرائم المالية و الجرائم المنظمة و جرائم الارهاب المعلوماتي وكل شكل من أشكال الجرائم التقليدية التي سهلت شبكة الانترنت من ارتكابها .

سوف نتناول في هذا المبحث أهم الجرائم التي ترتكب بواسطة شبكة الانترنت وكيفية تصدي المشرع لها في القانون الجزائري و القانون المقارن .

---

[1] عمر الفاروق الحسيني،المشكلات الهامة فى الجرائم المتصلة بالحاسوب الالي وابعادها الدولية ، ط 2، بدون ناشر، 1995، ص 1.

[2] عمر الفاروق الحسيني ، المرجع نفسه ، ص 15.

[3] محمد السعيد رشدى ، الانترنت والجوانب القانونية لنظم المعلومات ، بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق ،جامعة حلوان بعنوان الاعلام والقانون بتاريخ 14-15/ مارس 1999م ص 3 وما يليها .

المطلب الأول

الجرائم المخلة بالآداب ، الجرائم ضد شرف واعتبار الاشخاص و الإعتداء على حرمة الحياة الخاصة عبر الأنترنت

إلى جانب الصورة الايجابية و المشرقة للأنترنت في حياة الافراد ، إلا أن آثارها السلبية في نشر الافكارالضارة و غير الاخلاقية ، باتت تغزو المجتمعات وتهدد كياناتها من خلال افساد الاخلاق ونشر الثقافة الاباحية ، حيث تتوفر شبكة الانترنت عل اكثر الوسائل فعالية و جاذبية من عرض لملايين الصور و تسجيلات الفيديو و الحوارات المفتوحة المليئة بما هو مخالف للعادات و التقاليد و القيم و الكرامة الانسانية .

وتعمل الدول الغربية على وضع قيود للمارسة الدعارة عبر الانترنت ، منها عدم استغلال الاطفال جنسيا وكذا جعل هذه الممارسات تقتصر على أشخاص مصرح بهم وليسوا نتيجة لاتجار بالبشر. و تطالب العديد من الدول بالحد من الاباحية التي توفرها الشبكة لمستخدميها لما نتج عن ذلك من آثار سلبية على استقرار المجتمع.

وفي هذا السياق فقد تباينت مواقف مختلف التشريعات في تجريم ممارسة الدعارة عبر الأنترنت ، وهذا ما سنتطرق إليه في هذا المطلب ، مبرزين أهم الجرائم الأخلاقية التي ترتكب بواسطة شبكة الانترنت من ممارسة للدعارة و إنشاء المواقع الإباحية وكذا الاستغلال الجنسي للأطفال بالإضافة الى الجرائم ضد شرف و اعتبار الأشخاص كالسب و القذف و التهديد وكذا الاعتداء على حرمة الحياة الخاصة للأفراد.

الفرع الأول

الجرائم المخلة بالاداب عبر الأنترنت

تختلف الجرائم المخلة بالاداب التي ترتكب على شبكة الانترنت بين ممارسة الدعارة وانشاء المواقع الاباحية و لعل جريمة الاستغلال الجنسي للاطفال أكثر هذه الجرائم التي حظيت بعناية خاصة من قبل المشرعين نظرا للخطورة الاجرامية التي تميز مرتكبيها واثر ذلك على شريحة هشة تحتاج الى رعاية وحماية المشرع الجنائي.

أولا - جريمة ممارسة الدعارة عبر الانترنت:

اتخذت ممارسة الدعارة اشكالا متعددة نتيجة مسايرتها لتكنولوجيا الاتصالات ، فقد اصبحت ممارسة الجنس عن بعد ضمن هذه الاشكال المتعددة ، ويتم ذلك باستعمال فتيات مدربات في الغالب هن نتيجة للاتجار بالبشر حيث تحت وطاة التهديد و مقابل مبالغ مالية يجبرن على ممارسة الدعارة كما توجد شبكات و منظمات اجرامية تقوم بنقل حفلات و عروض اباحية مباشرة او مسجلة للترويج للدعارة وتكون موجهة في اغلب الاحيان الى شريحة الشباب و مقابل عمولات مالية مما جعل من هذه الصورة من الدعارة تتطور و تتحول الى دعارة الكترونية .

وقد جرم المشرع الفرنسي ضمن المادة 225 -10-1 من قانون العقوبات التحريض على ممارسة الدعارة بأي وسيلة كانت ، غير أن تطبيقات القضاء الفرنسي كانت أكثر تحديدا وتضييقا اذ اعتبرت أن ممارسة الدعارة عبر الأنترنت لا تتوفر فيه الأفعال الملوسة كالأقوال و الحركات التي يمكن أن تمثل تحريضا على الدعارة [*] ، كما أن الدعارة في فرنسا ليست مجرمة الا اذا كانت علنية وتتضمن أفعالا جنسية مع علم الجاني بأنه يخل بأنه يقوم بسلوك يخل بالآداب العامة حسب المادة 222-32 من قانون العقوبات الفرنسي .

أما المشرع الأمريكي فقد صادق على قانون " العفة في الاتصالات Communications Decency Act (47 U.S.C. 201 et sec) " سنة 1996 ، والذي يعد أول محاولة من الكونغرس الأمريكي لتنظيم المواد الاباحية على شبكة الأنترنت، إلا أنه في سنة 1997 أقرت المحكمة العليا بعدم دستورية القانون ، وأضاف الكونغرس الأمريكي القسم 230 للقانون المتعلق بالعفة على الأنترنت والذي يعفي مقدمي خدمة الأنترنت من المسؤولية و المتابعة عن المحتوى غير القانوني أو المخل بالآداب ، كما صادق الكونغرس سنة 1998 على قانون اخر لحماية القصر "Child Online Protection " ، كرد فعل على وصف المحكمة العليا بعدم دستورية القانون السابق ، ويمنع هذا القانون اتاحة محتوى مخل بالاداب في متناول القصر ، كما ألزم هذا القانون مقدمي خدمة الأنترنت بالحرص على عدم اتاحة المحتوى المخل بالآداب للقصر ، وتعرض لمواجهة المحاكم الفدرالية لعدم دستوريته لمعارضته لحرية التعبير الا أن المحكمة الدستورية أقرت بعدم تعارضه مع حرية التعبير [1]، وفي سنة 2003 تم إلغاء قانون العفة في الإتصالات و ذلك بعد أن تفوق معارضي حظر انتشار الاباحية على شبكة الانترنت ودعاة حرية البالغين في تبادل هذه المواد.

في حين أن المشرع الجزائري قد جرم ممارسة الدعارة ولم يحدد إذا ما كانت عبر شبكة الأنترنت أم لا ، حيث نصت المادة 1/343 من قانون العقوبات على أنه « يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة من 500 الى 20.000 دج وما لم يكن الفعل المقترف جريمة أشد كل من اقترف عمدا أحد الأفعال الاتية :

- ساعد أو عاون أوحمى دعارة الغير أو أغرى الغير على الدعارة بأي طريقة كانت ... »[2] ، فحسب نص المادة يدخل الترويج لأعمال الدعارة عبر الأنترنت و نشر المواد الاباحية تحت طائلة النص الذي لم يحدد طريقة معينة لذلك .

إلا أن الاشكال الذي غالبا ما يقع في التطبيقات القضائية للمادة السابقة ان الركن المادي في جريمة مساعدة و معاونة او اغراء الغير على الدعارة يقتضي فعلا ماديا كقيام الجاني بفعل مساعدة او حماية او اغراء الغير لممارسة الدعارة و أن يكون هناك عملا جنسيا قد تم بالفعل كدليل على ثبوت الجريمة فالقضاء الجزائري كثيرا ما واجهته صعوبات في توضيح مفهوم ممارسة الدعارة بالمعنى القانوني ، مما يستوجب تدخل المشرع لوضع نص قانوني صريح يجرم الافعال الباحية عبر شبكة الانترنت تفاديا للاشكالات التي قد يطرحها تفسير وتطبيق نص المادة 342 من قانون العقوبات الجزائري .

---

[*] Art 225 – 10 / 1 : « Le fait par tout moyen , y compris par une attitude meme passive de procéder publiquement au racolage d'autrui en vue de l'inciter à des relations sexuelles en échange d'une rémunération ou d'une promesse de rémunération est puni de deux moix d'emprisonnement et de 3750 euros d'amende »

[1] Duque (Nina)، La pornographie sur internet : Une analyse du débat senatorial sur le Communications Decency Act of 1996 aux Etats Unis , Université du Québec à Montreal , 1999, P.5.

[2] المادة 343 من الامر 66-156 المؤرخ 8 يونيو1966 المتضمن قانون العقوبات، ج.ر عدد 49 ، ص 737 ، معدلة بالأمر 75-47 المؤرخ في 17 جوان 1975، ج. ر عدد 53، ص 757.

ثانيا - جريمة انشاء المواقع الاباحية :

تتيح شبكة الانترنت امكانية صناعة و نشر الإباحة الجنسية لتوفرها على أكثر الوسائل فعالية وجاذبية، حيث ظهرت ملايين المواقع التي تعرض صورا و فيديوهات اباحية و حوارات جنسية مسجلة او مباشرة ، والتي تهدف في غالب الاحيان الى تحقيق مكاسب مادية كبيرة عن طريق زيادة عدد المتصفحين ، اذ تقوم في بادئ الامر بالترويج و الإشهار و تتيح امكانية الولوج المجاني ثم تشترط مبالغ مالية للحصول على خدماتها كتحميل الافلام الاباحية. [1]

وتسعى الدول لمحاربة هذه المواقع أو على الأقل ضمان عدم وصول الأحداث اليها ، ولكن تواجهها صعوبة عدم امكانية مراقبة هذه المواقع بصفة شاملة حيث أنها تلجا الى تغيير عناوينها بصفة مستمرة ، فالقانون الفرنسي بما أنه يجرم بموجب نصوص المواد 225-5 الى 225-12 الوساطة و تسهيل ممارسة الدعارة فيمكن القول أن انشاء المواقع الاباحية التي تحرض على ممارسة الدعارة يدخل ضمن الأفعال المجرمة بنصوص هذه المواد ، وقد أدانت محكمة Bobigny في حكمها الصادر بتاريخ 8 مارس 2007 صاحب موقع أنترنت بتهمة التحريض على الدعارة بموجب المادة 225-5 وحكمت عليه بالحبس أربع أشهرموقوفة النفاذ [2].

ثالثا - جريمة الاستغلال الجنسي للأطفال عبر الانترنت :

مع ازدياد حالات الاستغلال الجنسي للاطفال و تنامي صناعة الاعمال الاباحية و صور الأطفال الفاضحة عبر الأنترنت ، باتت الحاجة ملحة لحمايتهم سواء من الإستغلال الجنسي الذي يقع عليهم ، أو من افسادهم من خلال تمكينهم من الاطلاع على مواقع جنسية تنظم دعارة الأطفال عبر شبكة الانترنت.

وتقع جريمة الاستغلال الجنسي للاطفال او القصر بتوافر الأركان التالية :

- وجود طفل او قاصر لم يتعد سنه التاسعة عشر (حسب القانون الجزائري و يختلف ذلك حسب تشريع كل بلد) ، حيث يكون محل عرض مرئي او مسموع يتضمن عرضا للاعضاء الجنسية للطفل ، او طفل يقوم بارتكاب سلوك جنسي.

- تتضمن الأفعال المجرمة انتاج مواد اباحية و فاضحة للطفل بهدف توزيعها عبر الأنترنت و تسهيل عرضها على الآخرين أو بيعها أو حيازتها أو تخزينها في جهاز الحاسب الالي .

وهناك عدة تشريعات دولية بخصوص مكافحة الاستغلال الجنسي للاطفال ، نذكر منها :

- إتفاقية منظمة العمل الدولية بشأن منع أسوء أشكال عمالة الأطفال لعام 1999.
- البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الاباحية 2000.
- إتفاقية المجلس الأوروبي بشأن الإجرام المعلوماتي بودابست 2001.
- قرار مجلس الاتحاد الأوروبي رقم 68 لسنة 2004 بشأن مكافحة تعرض الأطفال للفساد الجنسي وإباحية الأطفال .

وقد جرمت العديد من الدول الاستغلال الجنسي للاطفال حماية لهذه الشريحة الهشة من المجتمع و التزاما منها بالاتفاقيات الدولية التي صادقت عليها .

---

[1] محمد عبد الله ابو بكر سلامة ، المرجع السابق ،ص 190.

[2] أنظر في الموقع : http://www.legalis.net/?page=jurisprudence-decision&id_article=2163

ولأن تعريض القصرلمشاهدة الأعمال الاباحية أو جعلهم مادة لها بات يهدد استقرار مجتمعات بأكملها ، حيث بينت دراسة أجراها " المرصد القومي الفرنسي للعمل الاجتماعي ODAS "سنة 1994 عن وجود ما يقرب عن اربعين الف طفل كانوا ضحية اعتداء جنسي [1] ، مما دفع بالمشرع الفرنسي و تطبيقا للمعاهدات الدولية إلى القيام بتجريم انتاج وتوزيع أو حيازة صورجنسية مخلة بالآداب لقصر باستعمال شبكات الاتصال وهذا في المادة 13 من القانون رقم 98- 468 الصادر سنة 1998 المتعلق بوقاية القصر من الجرائم الجنسية وكذا المادة 225-7 من قانون العقوبات الفرنسي [2] ، كما تجرم المواد 227-22 ،227-23 ، 227-24 صنع أو نقل أو عرض بأي وسيلة كانت رسالة تتسم بالعنف أو لها طبيعة جنسية إذا كان من الممكن أن يطلع عليها طفل أو تكون بحضور طفل.

وفي تطبيق لجريمة حيازة صور اباحية لقصر فقد ادانت محكمة استئناف Aix-en-Provence بفرنسا بتاريخ 23 افريل 2008 الجاني G. Anthony ، وذلك لحيازته صورا لقصر بغرض توزيعهاعبر شبكة الانترنت، وحكم عليه بسنة حبس غير نافذ و غرامة مالية بقيمة 5000 اورو. [3]

أما المشرع الأمريكي فقد جرم الاستغلال الجنسي للاطفال عبر حزمة من القوانين الفيدرالية ، حيث أصدر سنة 1944 قانون حماية الطفل (Child Protection Act) الذي يجرم فعل القيام عمدا بنقل أو تلقي أو توزيع أو بيع مواد اباحية تتعلق بالأطفال أو حيازتها بنية بيعها وذلك بأية وسيلة كانت بما فيها الحاسبات الآلية ، وفي سنة 1996 أصدرالقانون الخاص بحماية الطفل من الأعمال الاباحية Child Pornographie Protection الذي وسع من مفهوم الاعمال الاباحية المتعلقة بالطفل والتي تتم عبر شبكة الأنترنت لتشمل المواد المتعلقة بالأطفال ولو كانت خيالية أي لا ترتبط بأفعال حقيقية .[4]

وفي سنة 1998 صادق الكونغرس على قانون اخر لحماية القصر "Child Online Protection " أو ما يعرف بالقانون رقم Act 47 USA / 231 ، كرد فعل على وصف المحكمة العليا بعدم دستورية قانون العفة في الاتصالات، ويمنع هذا القانون اتاحة محتوى مخل بالآداب في متناول القصر وجعل له عقوبة الحبس 16 شهرا وغرامة بـ 50.000 دولار ، كما ألزم القانون مقدمي خدمة الأنترنت بالحرص على عدم اتاحة المحتوى المخل بالآداب للقصر، وفرض على المكتبات المدرسية و غيرها من المحلات العمومية و الخاصة أن تمنع ولوج القصر الى المواقع الاباحية ، ودخل هذا القانون حيز التنفيذ سنة 2000.

ويعد القانون الفدرالي رقم 18 C.S.U / 2256 اهم قانون لحماية القصر حيث قدم تعريفا شاملا للجريمة وكافة صورها والأنشطة المؤثمة بموجب القانون، و شمل التجريم في هذا القانون أفعال التحريض ، و المساعدة أو الاشتراك ، الانتاج والتوزيع كما أورد عقوبات رادعة على من يرتكب أي من هذه الأفعال.

---

(1) Gassin (Raymand), Droit de l'enfant et de l'adolescence, litec , 1995, p 2143 .

(2) Article 13 de la Loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, J.O. n°139, 18 juin 1998, p.9255., spécialement quant à la diffusion de messages pédophiles et quant à la mise en contact de mineurs avec l'auteur des faits grâce à l'utilisation d'un réseau de télécommunications (v. notamment les articles 225-7 et 227-22 code pénal).

(3) انظر منطوق الحكم في الموقع : http://www.Legalise.net

(4) مدحت رمضان ، جرائم الاعتداء على الأشخاص و الأنترنت ،دار النهضة العربية ،2000 ، ص129.

أما المشرع البريطاني فقد أضاف مادة لقانون حماية الطفل الصادر سنة 1978 والذي يجرم في المادة الأولى منه قيام أي شخص بالتقاط أو السماح بالتقاط أو انتاج أي صور ضوئية حقيقية أو غير حقيقية لطفل أو قام بتوزيعها أو عرضها سواء أنتجت بواسطة الرسم بالكمبيوتر أو تبدو على أنها كذلك حيث أضيفت سنة 1994 مادة لتجريم تخزين البيانات على أسطوانة كمبيوتر أو على أية وسيلة الكترونية أخرى بحيث يمكن تحويلها الى صورة ضوئية. [1]

أما في الجزائرفقد كشفت دراسة استطلاعية قامت بها الهيئة الوطنية للترقية الصحة و البحث العلمي أن نسبة الاطفال الذين تعرضوا لصدمة نفسية جراء مشاهدتهم لمواد اباحية بلغت 55,33%. [2]

ولم يحدد المشرع الجزائري وسيلة معينة لتحريض القصر على الدعارة ، فنص المادة 342 من قانون العقوبات الجزائري المتعلق بتحريض القصر على الفسق و الدعارة يمكن تطبيقه على الأفعال التي تتم باستعمال شبكة الانترنت و التي يكون موضوعها التحريض على فساد الاخلاق .

كما تجرم المادة رقم 333 مكرر من قانون العقوبات الجزائري صناعة أو حيازة أو عرض او توزيع صور أو اعلانات أو مطبوعات إلى غير ذلك من الأشياء المخلة بالحياء ، ويمكن أن تنطبق المادة على استعمال الأنترنت في ذلك لأنها تدخل ضمن الأشياء التي يمكن عرضها على الجمهور والتي يمكن بواسطتها نشر وتوزيع أو حيازة مواد مخلة بالآداب ، وعلى الرغم من هذه التشريعات في الجزائرإلا أننا نرى أنه من الأولى ايلاء هذا النوع من الجرائم أهمية خاصة و وضع نص خاص بتجريم نشرهذه المواد الخاصة بالقصروالمخلة بالآداب عبر شبكة الانترنت اقتداءا بالدول التي سبق وأن شرعت في هذا المجال و كذا حماية للأطفال من هذه الجرائم الخطيرة التي تهدد كيان الاسرة و المجتمع.

الفرع الثاني
الجرائم ضد شرف واعتبار الاشخاص عبر الأنترنت

أولا : جريمة التهديد عبر الانترنت :

التهديد عبر الانترنت من الجرائم التي انتشرت مؤخرا ، حيث يستخدم الجاني شبكة الانترنت لزرع الخوف في نفس المجني عليه وابتزازه وذلك بالضغط على ارادته و تخويفه من أن ضررا ما سيلحقه أو سيلحق ممتلكاته أو اشخاصا له بهم صلة . ومن ابرز الطرق التي يستخدمها الجاني ارسال الرسائل الالكترونية "E-mails" ، أو يكون التهديد مباشرا باستعمال غرف الحوار و الدردشة ، كما قد تلجأ بعض التنظيمات الاجرامية إلى انشاء مواقع تتضمن في محتوياتها تهديدا بالقتل أو بوضع متفجرات أو نشر فيروسات لإلحاق الدمار بشبكة الانترنت ، كما تتضمن صور التهديد الاخرى ابتزاز المجني عليه للحصول على مقابل مادي وتهديده بنشر صور أو أسرار خاصة.

وقد جرمت أغلب التشريعات التهديد حماية للسلامة النفسية و الجسدية للأشخاص ، حيث جرم المشرع الفرنسي التهديد بارتكاب جريمة في المادة 222-17 و المادة 222-18 من قانون العقوبات الفرنسي وجعل له عقوبة الحبس 6 أشهر و غرامة 7500 أورو ، و اشترط أن تكون الجريمة المهدد بارتكابها معاقب على الشروع فيها ، و أن يكون التهديد مجسدا بأفعال مادية تتمثل في محرر مكتوب أو صورة أو أية وسيلة أخرى ،

---

[1] مدحت رمضان ، المرجع السابق ، ص 131.

[2] Khiati (Mostapha), Cybercriminalité et enfance en Algerie, Edition FOREM, 2007, p.58

أما اذا كان التهديد بارتكاب جريمة قتل فتكون العقوبة بالسجن ثلاث سنوات والغرامة المالية المقدرة بـ 45000 أورو(*).

وعلى غرار المشرع الفرنسي فقد جرم المشرع الجزائري التهديد بموجب المواد 284 الى 287 من قانون العقوبات، واشترط أن يكون التهديد بالقتل مكتوبا في محرر موقع أو غير موقع أو بصورة أو برموز أو شعارات ، فقد حصر المشرع الجزائري الطرق التي يتم بها التهديد مما ضيق من حدود الجريمة خاصة إذا كان التهديد مرسلا عبر البريد الإلكتروني، وهذا بخلاف المشرع الفرنسي الذي وضع عبارة "أي شيء" في تعداده للوسائل التي يتم بها التهديد مما يعطي للقاضي الجزائي مجالا أوسع ويمكنه من وضع التهديد الذي يتم عبر الأنترنت تحت طائلة نص المادة.

ثانيا: السب و القذف عبر الانترنت

يعرف السب بانه كل تعبير يخدش و يجرح الشرف و الاعتبار ، أما القذف فهو اسناد علني لواقعة محددة تستوجب العقاب أو احتقار من اسندت إليه [1] . ويتفق السب و القذف في أن كلاهما هو اعتداء على شرف و اعتبار المجني عليه .

ويتكون الركن المادي لجريمة القذف من ثلاثة عناصر هي : فعل الاسناد و موضوع الاسناد والمسند اليه أو المجني عليه ، و الاسناد هو نسبة الأمرالشائن إلى المجني عليه على سبيل التاكيد، وتكون وسائل التعبير إما قولا أو كتابة أو اشارة، أما موضوع الاسناد فيشترط أن يكون أمرا معينا و محددا بحيث لو أنه كان محققا لأوجب العقاب على من اسندت إليه.

والركن الثاني في جريمة القذف يتمثل في العلانية أي اعلان و احاطة الكثير من الناس بالواقعة المنسوبة إلى المجني عليه ، فقد رأى المشرع أن خطورة جريمة القذف تكمن في إعلانها للناس لذا كانت العلانية ركنا من أركان الجريمة.

وجريمة القذف هي جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي العام، بحيث يتحقق القصد متى كانت الواقعة المسندة إلى المجني عليه شائنة في حد ذاتها.

وقد جرم المشرع الفرنسي القذف في المادة 29 وما يليها من القانون المتعلق بجرائم الصحافة لسنة 1881 ، مع التفرقة بين القذف العلني و غير العلني و القذف الموجه الى الأفراد أو إلى الهيئات العمومية ، وفي حالة النشر فقد جعل المسؤولية تقع على عاتق مدير نشر الجريدة [2]، أما الأمر الصادر بتاريخ 17 جانفي 2003 فقد حدد مسؤولية مقدمي خدمة الانترنت و المضيف أو صاحب الموقع الذي نشر فيه القذف ، كما ألزم قانون الثقة في الاقتصاد الرقمي رقم 2004-575 الصادر بتاريخ 21 جوان 2004 صاحب موقع الأنترنت بأن يقدم هويته لمقدم الخدمة كما يمكن لمضيف النشر أو صاحب الموقع أن يكون مسؤولا عما ينشر في موقعه اذا لم يقم بإزالة المحتوى على الرغم من اعلامه بذلك ، وذلك تحت طائلة العقوبات [3].

(*) Art.222-17 « La menace de commetre un crime ou un délit contre les personnes dont la tentative est punissable est punie de six moix d'emprisonnement et de 7500 euros d'amende lorsqu'elle est soit matérialisée par un écrit , une image ou tout autre objet »

(1) محمد عبدالله ابوبكر سلامة ، المرجع السابق ،ص 196.

(2) أنظر في الموقع : http://www.diffamations.com/laloi.html

(3) La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ,J.O, n°143 du 22juin 2004.

ولأن متابعة جريمة القذف عبر الأنترنت قد تثير عدة اشكاليات تتعلق باستمرارية الجريمة ، فقد قضت محكمة Court of Claims بنيويورك أن المادة التي ورد فيها قذف و الموزعة عبر الأنترنت لايمكن متابعة مرتكبها بعد سنة من تاريخ النشر على الأنترنت [1].

أما المشرع الجزائري فقد جرم المساس بشرف واعتبارالاشخاص أوالهيئات من خلال نص المادة 296 من قانون العقوبات التي عرفت فعل القذف بانه ادعاء بواقعة من شانها المساس بشرف و اعتبار الاشخاص أو الهيئة المدعى عليها بها او اسنادها مباشرة اليهم وحددت لها المادة 298 عقوبة تتراوح بين الحبس مدة شهرين الى ستة اشهر و غرامة من 25000 دج الى 50000 دج او باحدى العقوبتين ، وذكر المشرع وسيلة الادعاء كأن تكون شفاهة أو كتابة أو بالنشر أو بلكتابة على اللافتات ، كما جرم قذف الأفراد بسبب إنتمائهم الديني أو المذهبي أو العرقي بغرض إحداث الكراهية بين المواطنين وحدد لذلك عقوبة الحبس من شهر إلى سنة والغرامة من 10.000 دج إلى 10.000 دج أو بإحدى العقوبتين. [2]

كما جرم المشرع الجزائري سب الاشخاص في المادة 297 وعرفه بانه كل تعبير مشين او عبارة تتضمن تحقيرا او قدحا لا ينطوي على اسناد اية واقعة ، وقرر له في المادة 299 عقوبة الحبس من شهر الى ثلاثة اشهر و غرامة من 10000 الى 25000 دج ، أما اذا كان السب موجه إلى أفراد بسبب إنتمائهم الديني أو المذهبي أو العرقي بالحبس من خمسة أيام إلى ستة أشهر و بالغرامة من 5000دج إلى 50.000 دج أو بإحدى العقوبتين [3].

وبناءا على ما قدمنا فانه يمكن القول انه مع الوسائل التي تتيحها شبكة الانترنت و بتوفر باقي الاركان فإن جرائم السب والقذف تجد في الشبكة المعلوماتية مجالا خصب لارتكابها باقل الطرق تكلفة واسهلها ودون ترك أي أثر أو دليل واضح يسمح بمتابعة الجاني ، و في غالب الأحيان يكون العديد من الشخصيات السياسية و الدينية عرضة للسب و القذف بغرض تشويه السمعة للنيل من مصداقيتها كما قد يكون القذف نتيجة للابتزاز او التهديد باسناد امور خادشة للشرف الذي يكون غرضه دفع مقابل مادي او حمل الشخص على القيام بعمل او الامتناع عنه ، إلا أنه بالنظر إلى المواد السابقة فيمكن القول أن القذف و السب عبر الانترنت يدخل تحت طائلة العقوبة بما أن الأنترنت سارت أهم وسيلة لتوفير العلانية ومخاطبة جمهور عريض.

ثالثا: إهانة رئيس الجمهورية والهيئات العمومية

من بين الجنح التي يرتكبها الأفراد ضد النظام العمومي جنحة إهانة الموظف، والسبب الذي جعلنا نتطرق إلى إهانة رئيس الجمهورية أو أي هيئة عمومية أخرى كونها يتم العقاب عليها اذا كانت علنية ، فإهانة الموظف العادي لا تتطلب فيها العلنية حسب المادة 144 من قانون العقوبات، أما اذا كانت الاهانة علنية و بالوسائل التي حددتها المادة 144 مكرر و 144 مكرر1 وموجهة ضد البرلمان أو المجالس القضائية أو المحاكم أو الجيش أو أية هيئة عمومية أخرى فان العقوبة حسب المادة 146 تكون نفسها المطبقة في نص المادة 144 مكرر و 144 مكرر1 ، وقد نصت المادة 144 مكرر المعدلة بالقانون رقم 01-09 على معاقبة كل من أساء الى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو اعلامية أخرى ، حيث نصت المادة على عقوبة الحبس من ثلاثة أشهر الى اثني عشر شهرا والغرامة من 50.000 الى 250.000 دج [4].

---

[1] FERAL-SCHUHL (Christiane), Cyber Droit, (Le droit à l'épreuve de l'internet), 2eme 2dition, édition Dalloz, Paris, 2000, P.90.

[2] [3] المواد 298 ،298 مكرر،299 معدلة بالقانون رقم 06-23 الصادر بتاريخ 20 ديسمبر 2006،ج.ر عدد 84، ص 22 .

[4] القانون رقم 01-09 المؤرخ في 26 جوان 2001 المعدل والمتمم للأمر رقم 66-156 المتعلق بقانون العقوبات، ج.ر عدد 34 ، ص 17.

الفرع الثالث
جريمة الإعتداء على حرمة الحياة الخاصة عبر الانترنت

تكفل غالبية الدساتير حق الشخص في حماية حياته الخاصة ، حيث نصت مختلف التشريعات على حق الافراد في الخصوصية التي هي أحد الحقوق اللصيقة التي تثبت للإنسان [1]. إلا أن هذا الحق قد يتم انتهاكه من خلال نشر معلومات أو صور تتصل بحرمة الحياة الخاصة للأفراد، حيث أتاحت الانترنت امكانية الوصول إلى البيانات الشخصية و المعلومات السرية الخاصة للأفراد أو لعائلاتهم .

ففي فرنسا صدر القانون رقم 17-78 بتاريخ 6 جانفي 1978 الخاص بالمعالجة الآلية للبيانات و الحريات [2]، الذي نظم عملية المعالجة الآلية للبيانات ووضع قيودا لحماية الأفراد من التعدي على خصوصياتهم وحرياتهم ، والذي أحال في تجريمه للإعتداء على الحياة الخاصة للأفراد في المادة 50 الى المواد 226-14 و 226-16 من قانون العقوبات الفرنسي ، حيث نص على عقوبة 5 سنوات سجن و غرامة 300.000 أورو على القيام بإجراء معالجة آلية للبيانات من دون احترام شروط المعالجة الآلية للبيانات لخصوصيات الأفراد وحرماتهم الشخصية ، وتطبيقا لأحكام هذا القانون فقد قضت محكمة نانت Nantes بتاريخ 16 ديسمبر1985 بإدانة شخص قام بإجراء معالجة آلية للبيانات الشخصية دون أن يخطر اللجنة الوطنية للمعالجة الآلية للبيانات و الحريات المكلفة بإجراء هذه المعالجة والحرص على احترام حقوق المواطنين خلال جمع وتخزين ومعالجة المعلومات الشخصية [3]، وقد عززت حماية المشرع للحياة الخاصة بالقانون رقم 321-2000 الصادر بتاريخ 12 أفريل 2000 والذي عدل المادة 226-20 من قانون العقوبات الفرنسي وجرم الاحتفاظ بمعلومات أو بيانات أكثر من المدة المصرح بها للشخص القائم بالمعالجة الآلية للمعطيات وحدد لها عقوبة السجن 3 سنوات و غرامة مالية 45.000 أورو[4].

أما في الولايات المتحدة الامريكية فالقوانين متعددة لحماية البيانات الشخصية أو حماية الحياة الخاصة ،حيث صدر أول قانون سنة 1970 لحماية البيانات ، كما صدر قانون الخصوصية Privacy Act سنة 1974 الذي جاء في المادة A-552 منه على أنه " لايجوز لأية جهة أن تنشء أي معلومات يتضمنها نظام المعلومات بأي وسيلة من وسائل الاتصال لأي شخص أو لأي جهة ما لم يكن ذلك بناءا على طلب كتابي و بموافقة صاحب الشأن الذي تتعلق به المعلومات ، أو إذا كان ذلك تحقيقا للمصلحة العامة أو اجابة لأمر المحكمة ". [5]

وفي المملكة المتحدة فإن الاعتداء على حرمة الحياة الخاصة لا يواجه بنصوص صارمة تجرم هذا الفعل ، حيث لازالت المملكة ترفض أن تعترف باستقلالية الحق في الحياة الخاصة ، و ليس أدل على ذلك قضية كوريللي ضد وول ، أين رفضت المحكمة ادانة المدعى عليه الذي قام بنشر و بيع صور المدعية دون اذنها .

---

(1) محمد امين الشوابكة،جرائم الحاسوب و الانترنت ، طبعة اولى ، دار الثقافة ، عمان ،2004 ، ص 58.

(2) La loi n° 17 -78 du 6Janvier 1978 relatif aux fichiers et aux libertés, J.O du 7 Janvier 1978.

(3) WEILL (Pierre Alain), Etat de la législation et tendances de la jurisprudance relatives à la protection des données personnelles en Droit pénal Français , Rapport publié sur Reveue Internationale du Droit Comparé,1987, p.670.

(4) Loi 2000-321 du 12 -04-2000 relative aux droits des citoyens dans leurs relations avec les administrations,J.O,n°88 du 13-04-2000 , p.5646.

(5) ZOLLER (Elizabeth), Le Droit au respect de la vie privée aux Etats Unis, Droit et Justice N° 63, Université ParisII, 2005, p.35.

وذلك على أساس أنه ليس هناك نص يجرم هذا الفعل، [1] ، وحتى نصوص التشهير و القذف في قانون العقوبات الانجليزي فانها تقف عاجزة عن الاحاطة بكل جوانب هذه الجرائم اذ لا نجد سوابق قضائية بهذا الخصوص في القضاء الانجليزي مما جعل البعض يطالب بضرورة ايجاد قوانين اكثر تحديدا ودقة لحماية الحياة الخاصة.

أما المشرع الجزائري فقد جرم المساس بالحياة الخاصة للأفراد بأية تقنية كانت من خلال المادة 303 مكرر من قانون العقوبات [2]، التي نصت على أنه يعاقب بالحبس من ستة اشهر الى ثلاثة سنوات و بغرامة من 50.000 دج إلى 300.000 دج ، وذلك إذا قام بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية أو نقل صورة لشخص في مكان خاص ، بغير إذن صاحبها أو رضاه ، لكن لم يتطرق المشرع الجزائري إلى الحالات التي يتم فيها تخزين بيانات ومعلومات خاصة بالأفراد من قبل الهيئات العمومية ثم استعمالها لأغراض أخرى غير قانونية أو لمساومة أصحابها مما يستوجب الإسراع بسن تشريعات تنظم كيفية التعامل مع المعلومات الناتجة عن المعالجة الآلية للبيانات خاصة في ظل تعميم جواز السفر البومتري و غيره من وثائق الهوية أو القضائية.

وتتخذ جريمة الاعتداء على حرمة الحياة الخاصة للأفراد أشكالا متعددة ، من أبرزها :

أولا- جمع وتخزين بيانات شخصية صحيحة على نحو غير مشروع :

يعتمد الجاني في هذه الصورة على استخدام طرق و أساليب غير مشروعة لجمع وتخزين بيانات ومعلومات عن الافراد مثل البيانات المتعلقة بالعمليات البنكية ، المعاملات الضريبية، بيانات خاصة بمرحلة أداء الخدمة العسكرية، الاشتراك في الصحف و الدوريات ، حيث أن الحصول على هذه البيانات الخاصة يتيح امكانية استغلالها في غير الأهداف المرسومة من أجلها، وهذا ما يفسح المجال لايقاع الضرر و المخاطر بالأفراد ، فالمعلومات المتعلقة بالاحصاء السكاني لا يجوز استعمالها لغير هذا الهدف و لو كان مشروعا مثل استعمالها في الأغراض الضريبية نظرا لاستعمالها في غير الاطار المحدد لها أو الذي جمعت من أجله ، وقد أوصى المجلس الاوروبي في اتفاقيته الخاصة بحماية المعلومات على وضع قيود وضمانات لحماية الأفراد من الاعتداء على حقوقهم وحرياتهم و بالخصوص الحياة الخاصة بهم ، ووجوب استخدام المعلومات في الغرض المحدد لها. فأوجب تدخل المشرع حتى يمنع أي جهاز سواء كان خاصا أو عموميا من اعطاء معلومات إلى جهاز آخر، مختلف عنه في الغاية المرجوة من جراء تخزين المعلومات. [3]

ومن الامثلة الشهيرة بهذا الخصوص قيام " كلود غيبلرClaude Gubler " وهوالطبيب الخاص للرئيس الفرنسي السابق" فرنسوا ميتران François Metterant " بنشر سر مرض الرئيس في كتاب على شبكة الانترنت سنة 1996 ، حيث أثارت القضية ضجة كبيرة انتهت بعزل الطبيب من جدول الأطباء و اصدار رئيس محكمة باريس أمرا بوقف نشر الكتاب بتاريخ 18 جانفي سنة 1996 [4].

---

[1] ممدوح بحر ، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة ، مكتبة دار الثقافة، عمان،بدون طبعة، 1996، ص 96.

[2] المادة 303 مكررمن قانون العقوبات،أضيفت بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 ،ج.ر عدد 84 ، ص 23.

[3] نعيم مغبغب ، مخاطر المعلوماتية و الانترنت على الحياة الخاصة وحمايتها، الطبعة الثانية ، منشورات الحلبي الحقوقية ،بيروت ،2008، ص192.

[4] انظر في الموقع : http://www.denistouret.net/Constit/Gulber.html

ثانيا - استخدام بيانات شخصية غير صحيحة :

تتمثل هذه الصورة من صور انتهاك الحياة الخاصة في استخدام بيانات الأفراد غير الصحيحة على نحو غير مشروع ، حيث يتم التلاعب بهذه الببيانات من قبل أشخاص موظفين في الغالب لدى شركات التأمين وذلك مقابل الحصول على ربح مادي ، ومثل هذه الحالات وقع في الولايات المتحدة الأمريكية ، أين قام موظفون لدى شركة أمريكية "Trw Company Credit "متخصصة في تزويد البنوك والشركات الكبرى بمعلومات عن المركز الائتماني للافراد ووضعيتهم المالية ، مقابل اشتراك يدفعه العملاء ، وكانت الشركة تحتفظ بمعلومات في أجهزة الكمبيوتر لديها عن أكثر من 50 مليون شخص ، فقام موظفون لدى هذه الشركة بتعديل المعلومات التي تظهر مركزا سيئا للشخص والتلاعب بها مقابل مبلغ مالي مما يتيح لصاحب المعلومات أن يظهر في وضعية مالية مريحة ، مما تسبب في تورط البنوك والشركات الكبرى في التعامل مع قرابة مئة شخص من الافراد السيئ الوضع المالي ، ولم تكتشف الجريمة إلا عرضا [1] .

ثالثا- جرائم البريد الالكتروني المتعلقة باتهاك حرمة الحياة الخاصة:

يتعرض الكثير من مستخدمي البريد الالكتروني " E-Mail " إلى انتهاك حرمة حياتهم الخاصة ، والتوصل إلى المعلومات السرية و الشخصية بسهولة من طرف قراصنة الحاسب الآلي أوما يعرفون "بالهاكرز Hackers"، والسبب في ذلك راجع إلى تطور التقنيات المستخدمة في اختراق أجهزة الحاسب الالي ، وينتج عن عملية الاختراق تسريب البيانات الرئيسية والمعلومات الخاصة بمستخدم البريد الالكتروني.

ومن بين هذه التقنيات المستخدمة لانتهاك الخصوصية ما تتطلب تحكما في مجال المعلوماتية، ومنها أن يتم الحصول على الرقم الخاص لجهاز الحاسب الآلي المتصل بالأنترنت، فعندما يقوم أي شخص بزيارة موقع ما يقوم ذلك الموقع بمعرفة العنوان الخاص بالحاسب الالي حيث أن كل حاسب آلي متصل بالإنترنت له عنوان خاص به يسمى" Addresses IP " [2] وكل عنوان مكون من جزئين، الأول يشمل أرقام الشبكة والثاني يشمل أرقام مقدم الخدمة ويتم معرفة المعلومات الخاصة بجهاز الحاسب الالي من خلال برامج تتمثل في نصوص صغيرة ترسلها العديد من مواقع الانترنت ، ويتم تخزينها في جهاز من يزور تلك المواقع لعدة أسباب غالبا ما تكون بغرض الدعاية و الإعلان ، دون أن يشعر صاحب الجهاز بذلك ، وفورا يتم اصدار رقم خاص ليميز ذلك الزائر عن غيره من الزوار ويمكن لهذه المواقع أن تقوم بجمع المعلومات المخزنة في الحاسب الالي وارسالها إلى مصدرها أو احدى شركات الجمع والتحليل للمعلومات ، وكلما قام ذلك الشخص بزيارة الموقع يتم ارسال المعلومات وتجديد النسخة الموجودة لديهم ، ويقوم المتصفح بعمل المهمة المطلوبة منه مالم يقم صاحب الجهاز بتعديل وضع جهازه ، وقد تستغل بعض المواقع المشبوهة تلك المعلومات وتستعملها لأغراض غير مشروعة. كما قد يحصل أصحاب المواقع على معلومات شخصية لصاحب الجهاز مما يشكل انتهاكا لخصوصيته. [3]

---

[1] محمد بن عبدالله ابوبكر سلامة ، المرجع السابق ،ص 187.

[2] انظر في الملحق رقم 1- المصطلحات الواردة في الدراسة.

[3] حسن طاهرداود، ، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية ، الرياض،1420 هـ ، ص 50.

و قد يتم اختراق جهاز الحاسب الآلي من خلال رسائل البريد الاكتروني فهذه الرسائل هي أسرع وأسهل الطرق لنشر الفيروسات كفيروس" حصان طروادة " وبرامج التجسس عبر الأنترنت ، حيث يتم إرسال رسائل بعناوين مثيرة لإقناع المتلقي بفتح تلك الرسالة وبالتالي يتم زرع الفيروس أو ملف التجسس في الجهاز .

ويمكن أن يتعرض البريد الإلكتروني" للاغراق Spam " [1] ، عندما يتم ارسال كميات كبيرة من الرسائل الإلكترونية الى الشخص المستهدف مما يؤدي الى تدمير هذا البريد سواء كان العنوان البريدي لشخص أو شركة ، ويعتبر البريد الالكتروني من أقوى وسائل الجناة ، إذ يقومون بتهديد ضحاياهم أو ابتزازهم بعد حصولهم على معلوماتهم الخاصة .

كما يعد البريد الإلكتروني وسيلة لإرتكاب الجرائم المالية ، حيث يقوم المجرمون بإرسال البريد للمجني عليه باسم بنك استمثاري، ثم يتم اقناع المجني عليه بتحويل مبالغ مالية للجاني للمشاركة في مشاريع استثمارية ناجحة اويقوم الجاني بارسال بريد إلكتروني منتحلا صفة البنك الذي يدير حساب المجني عليه ويطلب منه القيام بتعديل بياناته الشخصية وتأكيد حسابه البنكي وتغيير كلمة المرور، وبمجرد قيامه بذلك يكون قد ارسل بياناته الشخصية إلى الجاني الذي يستعملها في انتحال شخصية المجني عليه و الإحتيال بإسمه. وانتشرت هذه الجرائم بشكل كبير وأغلب مرتكبيها هم أشخاص يقيمون في دول افريقية وأغلبهم من دولة نيجيريا.

---

[1] انظر في الملحق رقم 1 – المصطلحات الواردة في الدراسة.

المطلب الثاني
الجرائم المالية و الجرائم المنظمة عبر الانترنت و الإرهاب المعلوماتي

الجرائم المنظمة والجرائم المالية وجريمة الإرهاب ليست وليدة للتقدم العلمي الحاصل في مجال تكنولوجيات الإعلام و الإتصال إلا أنها استفادت كثيرا منه ، ووفرت لها الإمكانيات المتاحة على شبكة الأنترنت سبل نمو وانتشار هذه الجرائم ، حيث صارت الجماعات الإجرامية تعتمد شيئا فشيئا في أعمالها على شبكة الانترنت ، مما ضاعف من خطورتها وجعل أجهزة الأمن عبر مختلف الدول تسعى جاهدة لتطوير قدراتها في مجال المعلوماتية و شبكات الاتصال لغرض مسايرة التطورات الحاصلة في وسائل و اليات ارتكاب الجرائم.
سنتناول في هذا المطلب جملة من أشكال الجرائم المالية و الجرائم المنظمة و كذا جريمة الإرهاب المعلوماتي ، مبينين السلوك الاجرامي لكل صورة وكيفية استغلال شبكة الانترنت في ارتكابها.

الفرع الأول
الجرائم المالية

مكنت شبكة الأنترنت المجرمين من طرق جديدة لإرتكاب جرائم مالية قديمة كالإحتيال و مختلف أشكال السرقات ، ومع ارتباط العمليات التجارية بشبكة الأنترنت في كثير من الدول وهو ما يعرف بالتجارة الإلكترونية ازدادت حالات السطو على البطاقات الإلكترونية لغرض استعمالها في الإستيلاء على مال الغير من خلال إجراء تحويلات بها من حساب الى آخر، كما صارت عصابات تبييض الأموال تعتمد على التحويلات البنكية من حساب إلى اخر عبر البنوك الالكترونية التي تضمن سرعة و سرية هذه التحويلات.

- **أولا : جرائم الاستيلاء على البطاقات الالكترونية**

البطاقات الالكترونية هي عبارة عن بطاقة بلاستيكية صادرة عن مؤسسة ما تمنح لأحد عملائها، وتسمح له بإجراء معاملات مالية كدفع قيمة الخدمات أو المشتريات التي يحصل عليها، وكذلك سحب مبالغ نقدية من حسابه، ويمكننا أن نصنف هذه البطاقات إلى أربعة أنواع هي [1]:

بطاقات سحب النقود Cash Card**:** جميع البطاقات الإلكترونية تؤمن سحب النقود ، أما هذا النوع من البطاقات فدورها الرئيسي هو سحب النقود فقط من خلال أجهزة السحب النقدي الالي عن طريق ادخال الرقم السري ويمكن سحب النقود من من منافذ التوزيع سواء داخل البلد أو خارجه.

بطاقات الوفاء Delit Card**:** هي اداة وفاء بثمن السلع و الخدمات، بحيث لا يتم دفع الثمن نقدا،بل يتم خصم المبلغ من الرصيد البنكي للعميل و تحويله الى حساب المستفيد .

بطاقات الائتمان Credit Card **:** تسمح لحاملها بتسديد ثمن مشترياته على دفعات، فهي تفترض أن حاملها مدين بحيث يحصل على مايريده من سلع وخدمات ثم يقوم البنك خلال أجل متفق عليه بتسديد ثمن ذلك للتاجر و استرداد المبلغ من حامل البطاقة في حدود الاتفاق بينه و بين البنك ، ومن أمثلتها بطاقة " فيزا كارد Visa Card"، "ماستر كارد Master Card" و" الاكسس Access".

---

[1] نائلة عادل قورة،المرجع السابق ، ص 509.

بطاقات ضمان الشيكات Cheque Guarantee Card **:** تعتبر وسيلة يضمن بها صاحب الخدمة او التاجر حصوله على مقابل الشيك من البنك المصدر للبطاقة ،حيث تحتوي هذه البطاقة على اسم العميل و توقيعه ورقم حسابه والحد الاقصى الذي يتعهد البنك بوفائه، حيث يبرز العميل البطاقة ثم يقوم بالتوقيع على الشيك أمام المستفيد.

البطاقات الذكية Smart Card**:** تحتوي هذه البطاقات على معالج دقيق وذاكرة ومزودة بنظام أمان لحمايتها، ويمكنها اختزان ملايين الدولارات ، ومن ميزاتها أيضا أنها تجمع كل البطاقات السابقة فهي تصلح لجميع المعاملات المالية.

تتعدد صور السلوك المجرم في مجال البطاقات الالكترونية فلا تقع كلها من طرف المستولي على البطاقة بل منها ما يقع من قبل الحامل الشرعي للبطاقة وتتمثل هذه الصور فيما يلي :

أ) جرائم تقع من قبل الحامل الشرعي للبطاقة:

الجرائم التي تقع من الحامل الشرعي للبطاقة قد تكون بالشكل التالي[1] :

أ-1- استخدام بطاقة منتهية الصلاحية أو ملغاة : كأن يستمر حامل البطاقة في استعمالها رغم أنها منتهية الصلاحية أو ملغاة لسبب ما ، فيمتنع حامل البطاقة عن ارجاعها ومن ثم يستعملها بصفة غير مشروعة.

أ-2- اساءة استخدام البطاقات الالكترونية : يتمثل السلوك الإجرامي في هذه الحالة في قيام الجاني إما بتجاوزحد الإئتمان المقرر في البطاقة أثناء السحب أو تجاوزالرصيد الذي يضمنه البنك .

ب) جرائم تقع من قبل المستولي على البطاقة:

يقوم الجاني في هذه الحالة بالإستيلاء على البطاقة الإلكترونية بسرقتها أو تزويرها ومن المعلوم أن سرقة البطاقة لايمكن الجاني من استعمالها إذ أن الجاني في أغلب الأحيان يلجأ إلى الإحتيال للحصول على الرقم السري الذي يمكنه من استعمال البطاقة الإلكترونية حيث يتمثل السلوك المجرم في الوصول بشكل غير مشروع إلى بيانات البطاقات الإلكترونية باستخدام الأنترنت أو أية تقنية للمعلومات بغرض الحصول على أموال الغير، بما أن الحصول على هذه البيانات يكفي لتسديد ثمن المشتريات أو الخدمات المتحصل عليها .

ثانيا- جريمة لعب القمار في الكازينوهات الافتراضية:

تجرم كل الدول العربية لعب القمار سواء بالطريقة التقليدية أو عبر الأنترنت ، أما التشريعات الغربية فإنها تختلف في تجريمها للعب القمار عبر الأنترنت ، ففي فرنسا وبعد أن كان هناك فراغ تشريعي في هذا المجال صدر القانون رقم 476- 2010 بتاريخ 12 ماي 2010 المتعلق بتنظيم ألعاب القمار عبر الأنترنت ، ولكن المشرع لم يجرم انشاء مواقع ألعاب القمار عبر الأنترنت ولكنه نظم أحكامها وجعلها خاضعة لإشراف الدولة، وقرر في المادة 56 من القانون السابق أحكاما جزائية لمخالفي القانون تتراوح بين السجن من 3 سنوات و الغرامة 90.000 اورو في حالة عدم الحصول على الاعتماد .[2]

---

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت ، المرجع السابق ، ص570 ومابعدها.

[2] Artcile de Thibault Verbiest, Les casinos virtuels : une nouvelle cybercriminalité ?, à l'adresse : http://www.legalis.net/legalnet/articles/casinos_virtuels_notes.htm

أما في الولايات المتحدة الأمريكية فلعب القمار عبر الأنترنت غير مصرح به إلا في بعض الدول السياحية لهذا يلجأ اغلب أصحاب نوادي القمار إلى إدارة نواديهم أو كازينوهاتهم الافتراضية من هذه الدول فمعظم هذه النوادي تقول أنها موجودة في حوض الكاريبي، وتابعت شرطة المباحث الفيدرالية الامريكية F.B.I بعض مواقع الانترنت التي تقوم بالمقامرة ، وتبين لها أن هذه المواقع موجودة في أغلبها في حوض الكاريبي وجزر الأنتيل ، وجزيرة انتيجوا، وجمهورية الدومينيكان [1].

ثالثا- جريمة تبييض الاموال عبر الانترنت :

وفرت شبكة الانترنت لمجرمي تبييض الاموال كل ما يحتاجونه من سرعة تحويل الاموال و سرية التعامل و عدم ترك الاثر، وبفضل توفر البنوك الالكترونية التي تتبنى مبدأ سرية الحسابات البنكية وبالتالي فان عملية اخفاء المصدر غير المشروع للاموال واستثمارها في مشاريع اقتصادية مشروعة يتسترون خلفها. وبسبب تزايد عدد عمليات تبييض الاموال عبر الانترنت قررت هيئة F.A.T.F التي تعنى بالمكافحة المالية الدولية لجرائم تبييض الاموال ان مواجهة هذه الجرائم التي تطورت بسبب نظم الدفع الالكتروني ، تقع ضمن التحديات المستقبلية للهيئة [2].

ويتمثل الركن المادي لهذه الجريمة في القيام بتحويل أو نقل الأموال غير المشروعة أي اجراء عمليات مصرفية لتحويل الأموال وتكون عبر وسائل إلكترونية كالتحويل من حساب إلى آخرعن طريق شبكة الانترنت أو تمويه مصدرها غير المشروع أو اخفائه ، أو القيام بحيازة هذه الاموال مع العلم أنها عائدات اجرامية و ذلك لإضفاء الصفة المشروعة على تلك الاموال ، وحتى تتم عملية تبييض الأموال بطريقة تضمن اخفاء المصدر غير المشروع للأموال ، فانها تمر بمراحل مختلفة كمرحلة الايداع " Placement " أين يتم توظيف الاموال داخل البنوك أو شراء العقارات أو فتح حسابات في مصارف وهمية ، ثم تأتي مرحلة التجميع "Empilage" وذلك من خلال القيام بعمليات معقدة لفصل الأموال المشبوهة عن مصدرها الأصلي أين يتم استعمال التحويل الألكتروني عبر الانترنت ليتم دمج الأموال "Intégration " في الدورة الاقتصادية معتمدين في ذلك على الخدمات المصرفية الالكترونية بالاستعانة بشبكة الانترنت ولا يتطلب ذلك سوى التسجيل في البنك و ادخال شفرة سرية لتحويل أموال ضخمة [3] ، أو استخدام بطاقة الائتمان لشراء المجوهرات،او الأشياء الثمينة، كما شاع استخدام البطاقة الذكية smart card عن طريق ما يعرف بتقنية " موندكس الشهيرة " ذات القيمة المخزنة ، اين يقوم الجناة بتشفير عمليات التحويل بحيث لا يمكن تتبع العملية من طرف اجهزة الامن [4].

وجريمة تبييض الاموال عبر الأنترنت هي جريمة عمدية ، حيث تقوم على القصد الجنائي العام بعنصريه العلم و الإرادة ، أي علم الجاني بأنه يمارس نشاطا غير مشروع يتمثل في اخفاء المصدر غير المشروع للأموال ، و انصراف ارادته إلى ارتكاب هذا السلوك الإجرامي ، أما القصد الجنائي الخاص فيتمثل في نية اخفاء المصدر غير المشروع لهذه الاموال. [5]

---

[1] ممدوح عبد الحميد عبد المطلب ، جرائم استخدام شبكة المعلومات العالمية ، بحث مقدم إلى مؤتمر القانون و الكمبيوترالانترنت، كلية الشريعة و القانون بجامعة الإمارات سنة 2000، ص 70.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت ، المرجع السابق، ص 133.

[3] صلاح الدين السيسي، غسيل الأموال – الجريمة التي تهدد استقرار الاقتصاد الدولي، دار الفكر العربي، القاهرة، 2004، ص 11.

[4] ممدوح عبد الحميد عبد المطلب، ،المرجع نفسه ، ص 71.

[5] عبد الفتاح بيومي حجازي،المرجع نفسه، ص 172.

وتبييض الأموال مجرم في أغلب القوانين التزاما منها بالاتفاقيات الدولية ، فالمشرع الفرنسي نص على ذلك في القانون 87-1157 الصادر سنة 1987 و الذي عزز بالقانون رقم 90-614 المؤرخ في 12 جويلية 1990 المتعلق بمساهمة المؤسسات المالية في مكافحة تبييض الأموال المتأتية من المتاجرة بالمخدرات والذي ألزم البنوك بضرورة الاحتفاظ ببيانات المرسل و المرسل إليه ، وفي تعديل 1996/05/13 عاقب على جريمة تبييض الأموال بخمسة سنوات حبس و بغرامة 375000 أورو في المادة 324 فقرة 1 إلى 6 ، واعتبر أن التبييض هو عملية تسهيل بكل الوسائل التبرير الكاذب لمصدر الأموال أو الدخول ، لمرتكب جناية ، أوجنحة عادت عليه بفائدة مباشرة أو غير مباشرة.[1]

كما جرم المشرع الأمريكي تبييض الاموال من خلال قانون سرية الحسابات لسنة 1970 و الذي يلزم المؤسسات المالية بالابلاغ عن المعاملات المالية التي تزيد عن عشرة الاف دولار ، بالاضافة الى جملة من القوانين الاخرى كقانون الرقابة والسيطرة على غسيل الاموال سنة 1986 وقانون مكافحة غسيل الاموال سنة 1992 وقانون قمع غسيل الاموال سنة 1994 [2] ، كما تجرم العديد من التشريعات القيام بإنشاء مواقع على شبكة الأنترنت لتسهيل عمليات تبييض الأموال [3].

أما المشرع الجزائري فلم يتخلف عن مواكبة للتشريع الدولي و إلتزاما منه بالاتفاقيات الدولية في المجال مكافحة تبييض الاموال ، حيث جاء القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 الذي نص على تجريم صور تبييض الاموال المختلفة ضمن المواد من 389 مكرر الى 389 مكرر 7 من قانون العقوبات وحددت له عقوبة الحبس من خمس سنوات الى عشر سنوات مع الغرامة المالية التي تصل الى 3000,000 دج.[4]

الفرع الثاني
الجرائم المنظمة عبر شبكة الانترنت

استغلت عصابات الجريمة المنظمة شبكة الأنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بسهولة ، حيث ساعدتها كثيرا في تطوير وسائلها ، فالسرية تشكل عادة جزءا رئيسيا من استراتيجية الجريمة المنظمة، وشبكة الإنترنت توفر فرصا ممتازة للمحافظة على هذه السرية ، مع امكانية إلغاء الحواجز المكانية و الزمانية مستغلة الفراغ التشريعي في بعض الدول التي مازالت لم تواكب التطور الحاصل في الجريمة المعلوماتية ، حيث يوفر لها هذا الفراغ قدرا كبيرا من الحماية و الحرية في ممارسة عملياتها العابرة للأوطان.

وقد تم الاهتمام بمكافحة الجريمة المنظمة من خلال عقد المؤتمرات الدولية التي كان أولها مؤتمر الأمم المتحدة السابع سنة 1985 لمنع الجريمة الذي اعتمد خطة عمل ميلانو كما تلته عدة مؤتمرات كالمؤتمر الثامن لمنع الجريمة بفنزويلا سنة 1990 و المؤتمر الوزاري العالمي الخاص بالجريمة المنظمة عبر الوطنية المنعقد في نابولي بايطاليا سنة 1990 ، وعبرت جميع هذه المؤتمرات عن اهمية التعاون الدولي واعطاء الاولوية في مكافحة الجريمة المنظمة .

---

(1) لعشب علي ، الاطار القانوني لمكافحة غسيل الاموال ، OPU ،الجزائر ، 2007،ص 62.

(2) لعشب علي، المرجع نفسه ، ص 61.

(3) عبد الفتاح بيومي حجازي، جريمة غسل الاموال بين الوسائط الالكترونية ونصوص التشريع، دارالفكرالجامعي ،الطبعة الاولى ، الاسكندرية، 2005. ص151.

(4) القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 ،ج.ر عدد 71 ، ص 11، المادة 389 مكرر-1 معدلة بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، ج.ر عدد 84،ص26 .

و عرفت الأمم المتحدة الجريمة المنظمة في المادة 02 من اتفاقية باليرمو لمكافحة الجريمة عبر الوطنية سنة 2000 بانها « جماعة ذات هيكل تنظيمي ، مؤلفة من ثلاثة أشخاص أو أكثر ، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو اكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية ، من أجل الحصول بشكل مباشر أو غير مباشر على منفعة مالية أو منفعة مادية اخرى » .[1]

ومن أهم النشاطات الاجرامية التي تقوم بها المنظمات الإجرامية الاتجار بالمخدرات و الاتجار بالبشر و غسيل الاموال ، حيث صارت تقوم بتوظيف اختصاصيين ماليين وخبراء في الانترنت لإدارة شؤون غسيل الأموال.
سنتناول أهم الجرائم التي ترتكبها المنظمات الاجرامية عبر الانترنت و المتمثلة في الاتجار بالمخدرات عبر الانترنت و الاتجار بالبشر .

أولا - الاتجار بالمخدرات عبر الانترنت :

الاتجار بالمخدرات مجرم في أغلب التشريعات الوطنية و الدولية منها الاتفاقية الموحدة المتعلقة بالمخدرات لسنة 1961 و المتممة باتفاقية المؤثرات العقلية لسنة 1971 واتفاقية الامم المتحدة المتعلقة بمكافحة الاتجار غير المشروع بالمخدرات و المؤثرات العقلية بفيينا سنة 1988.

و في الجزائر ، وبعد المصادقة على كافة الاتفاقيات السابقة فقد تم اصدار القانون رقم 04-18 المؤرخ في 2004/12/25 المتعلق بالوقاية من المخدرات و المؤثرات العقلية وقمع الاستعمال و الاتجار غير المشروعين بها [2] ، حيث تجرم المادة 13 من هذا القانون ترويج المخدرات او عرضها على الغير بهدف استهلاكها ، و تعاقب على ذلك بالسجن لمدة تتراوح بين السنتين و 10 سنوات والغرامة المالية بين 100,000 دج الى 500,000 دج اما اذا كان المجني عليه قاصرا فيمكن ان تصل العقوبة الى 20 سنة سجنا.

أما المتاجرة بالمخدرات فقد حددت لها المادة 17 من نفس القانون عقوبة تتراوح بين 10 سنوات الى 20 سنة سجنا وغرامة مالية بين 5 000.000 دج لتصل الى 50,000,000 دج ، أما اذا كان من يقوم بالمتاجرة منظمة اجرامية فإن العقوبة تصل إلى السجن المؤبد ، ولم تحدد المادة طريقة معينة لتجارة المخدرات إذ نصت على تجريم عرض المخدرات للتجارة بأي شكل كان مما يدخل الترويج للمخدرات عبر الأنترنت تحت طائلة المادة.

و يتطلب الركن المادي لجريمة الاتجار بالمخدرات عبر الانترنت انشاء موقع او نشر معلومات على شبكة الانترنت بقصد الترويج للمخدرات أو المؤثرات العقلية و مافي حكمها أو تسهيل التعامل فيها.

ونظرا إلى امكانية الترويج لتجارة المخدرات عبر شبكة الانترنت فقد ازدادت مهارة عصابات تجارة المخدرات ، ومن الأمثلة على ذلك قيام المنظمات الكولومبية لتجارة المخدرات باتباع الممارسات التي تقوم بها الشركات العادية لتنويع الأسواق والمنتجات، واستغلت أسواقاً جديدة في أوروبا الغربية ودول الاتحاد السوفياتي السابق [3].

---

[1] راجع : اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر2000، على الموقع التالي :
http://www1.Umn.edu/humanrts/arab/CorgCRIME.html

[2] قانون رقم 04-18 مؤرخ في 25 ديسمبر سنة 2004، يتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها، ج.ر عدد 83 ، ص 3.

[3] منير محمد الجنبيهي وممدوح محمد الجنبيهي، بروتوكولات وقوانين الانترنت، دار الفكر الجامعي،الاسكندرية، 2005، ص 74 .

ثانيا - الاتجار بالبشر عبر الانترنت :

تحظرأغلب الدساتير الإتجار في البشر ، وفقا لنص المادة 04 من الإعلان العالمي لحقوق الانسان التي تحظر استرقاق أو استعباد أو الاتجار في البشر بأي شكل من الأشكال.
ويعرف الإتجار بالبشر بأنه شكل من أشكال التحكم غير الطوعي في الانسان ، حيث يلجأ الجناة الذين ينتظمون في منظمات إجرامية إلى الاستيلاء على جوازات سفر المجنى عليهم من النساء و الرجال، وإلى اختطاف القصر، ومن ثم استغلالهم في تحقيق مكاسب مادية غير مشروعة ، من خلال اجبارهم على العمل في تجارة الجنس أو في السوق السوداء وخصوصا في تهريب العملة و المخدرات وهو ما يعرف بالعبودية القسرية.

وقد تصدى المشرع الفرنسي للإتجار بالبشر بموجب المادة 225-4 من قانون العقوبات وحدد له عقوبة السجن 7 سنوات وغرامة مالية ب 150.000 اورو ، كما جرم في الجزائر في تعديل قانون العقوبات بموجب القانون رقم 09-01 المؤرخ في 25 فبراير 2009 ، حيث نصت المادة 303 مكرر 4 من قانون العقوبات على عقوبة الحبس لمدة تتراوح بين ثلاث سنوات و عشر سنوات و الغرامة المالية التي تصل الى 1.000,000 دج. [1]

وتتيح شبكة الأنترنت سرية التواصل بين الجناة ، مما ساهم في تفاقم الظاهرة حيث يتمثل السلوك الاجرامي لهذه الجريمة في انشاء موقع أو نشر معلومات على شبكة الانترنت بقصد الإتجار في الأشخاص أو تسهيل التعامل في هذا المجال ، وهذا مايستدعي تدخل المشرع لتجريم انشاء هذا النوع من المواقع والتحري عن تلك التي تختبىء تحت غطاء توفير العمالة في بلدان أوروبية خصوصا للنساء ثم يتم استغلالهن في أعمال الدعارة.

الفرع الثالث
الإرهاب المعلوماتي

يتمثل السلوك الإجرامي في الأرهاب المعلوماتي في انشاء موقع أو نشر معلومات على شبكة الانترنت يخص جماعة ارهابية ، وتحت مسميات تمويهية لتسهيل اتصال اعضاء هذه الجماعة الارهابية ، أو الترويج لأفكارها وتجنيد إرهابيين جدد ، أو لتمويلها اولإبراز قوة التنظيم الإرهابي، ولإعطاء التعليمات وللتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية ، فقد أنشئت على شبكة الانترنت مواقع إرهابية تبين كيفية صناعة القنابل والمتفجرات، والأسلحة الكيماوية الفتاكة، كما تبين طرق اختراق البريد الإلكتروني، وكيفية اختراق وتدمير المواقع الإلكترونية، والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات الى غير ذلك من الاعمال التخريبية .

ويتميز الإرهاب المعلوماتي عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية ، والوسائل الإلكترونية التي اوجدتها حضارة التقنية في عصر المعلومات ، لذا فإن الانظمة الالكترونية و البنية التحتية هي هدف الارهابيين .

---

[1] القانون رقم 09-01 المؤرخ في 25 فبراير 2009 المتعلق بالاتجار بالاشخاص، ج ر عدد 15، ص 3 .

وقد أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى، وبسبب ترابط الشبكات المعلوماتية فان إمكانية انهيار البنى التحتية للأنظمة ، والشبكات المعلوماتية ليس في الدول المستهدفة او في كبرى الشركات فقط بل في العالم كله وهو أمر غير مستبعد ، وتكمن خطورة الارهاب المعلوماتي في سهولة استخدام هذا السلاح الرقمي ، حيث يقوم الارهابي المعلوماتي من منزله أو مكتبه ، وفي سرية تامة بعيدا عن أنظار السلطات والمجتمع، بالضغط على لوحة المفاتيح ومن ثم تدمير البنية المعلوماتية من خلال استهداف المواقع الحيوية و اغلاقها اوإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال ، تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها, أو التحكم في خطوط الملاحة الجوية والبرية والبحرية, أو شل محطات إمداد الطاقة والماء ، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية فيتسبب ذلك في خسائر كبيرة تفوق تلك التي تسببها المتفجرات و الاعمال الارهابية التقليدية .

ويتم استخدام البريد الإلكتروني في التواصل بين الإرهابيين فيما بينهم مما يضمن سرية الاتصالات وتبادل المعلومات ، كما تقوم الجماعات الارهابية باستغلال شبكة الانترنت في انشاء مواقع لنشر بياناتها و الترويج لهذه الجماعات و تكوين قاعدة فكرية بين اوساط مستخدمي الشبكة لاستقدام عناصر جديدة وتجنيدها مما يضمن استمرارية العمل الارهابي .

و الموقع عبارة عن معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل Hyper text mark up language أو (HTML) ولأجل رؤية هذه الصفحات يتم طلب استعراض " شبكة المعلومات العالمية WWW Browser " ويقوم بحل رموز (HTML) وإصدار التعليمات لإظهار الصفحات المكتوبة. وإنشاء مواقع خاصة بالجماعات الارهابية على شبكة الأنترنت لخدمة أهدافهم وترويج أفكارهم الضالة أصبح سهلاً وممكناً، ولذا فإن معظم التنظيمات الإرهابية لها مواقع إلكترونية ، وهي بمثابة المقر الافتراضي لها.[1]

وقد سنت العديد من الدول تشريعات أرادت بها الاحتراز من استعمال شبكة الأنترنت كوسيلة لتنظيم وتسهيل الأعمال الإرهابية ، فالمشرع الفرنسي أصدر القانون رقم 64-2000 في 23 جانفي 2006 المتعلق بمكافحة الإرهاب [2] ، والذي اعتبر مثيرا للجدل نظرا للأحكام التي جاء بها خاصة المادة 6 التي تنص على إلزامية أن تقوم شركات الإتصالات ومزودي خدمة الانترنت و أصحاب مقاهي الأنترنت بالاحتفاظ ببيانات وسجلات الاتصالات لمدة سنة واحدة ، كما عدل القانون في المادة 13 منه المادة 30 من قانون الاعلام الالي و الحريات وذلك بالحد من حجم المعلومات التي يجب تبليغها للجنة الوطنية للإعلام الآلي و الحريات، و التي تتعلق بأمن الدولة و الدفاع و الأمن العام ، كما أضاف القانون مادة جديدة الى قانون البريد و الاتصالات الالكترونية بحيث لم يعد الحصول على اذن مسبق من الجهات القضائية شرطا لازما لمصالح الشرطة للوصول الى التسجيلات و البيانات المعلوماتية أثناء التحري عن الجرائم اذ يكفي الاذن من قبل مسؤول سامي في جهاز الشرطة للحصول على هذه التسجيلات .

---

(1) Création d'un site Web à l'adresse : http://ar.html.net/

(2) Loi n° 2006-64 du 23/01/2006 parue au J.O n° 20 du 24/01/2006 à l'adresse : http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124

أما المشرع الامريكي فقد اتخذ خطوات متقدمة في مجال مكافحة الارهاب الالكتروني والترويج للعمليات الإرهابية عبر شبكة الانترنت ، ومن المفارقات أن العديد من المواقع المروجة للإرهاب تتخذ الولايات المتحدة الامريكية مضيفا لها ، مستفيدة من الدستور الأمريكي الذي يمنع المساس بحق حرية التعبير ، كما أن الولايات المتحدة الامريكية لم توقع على البروتوكول الإضافي لمعاهدة بودابست لذات الغرض ، مما دفع بالسلطات الامريكية الى اللجوء الى الوسائل التكنولوجية لمنع محركات البحث من الولوج الى المواقع المعادية أو الارهابية ، ولكن بعد أحداث 11 سبتمبر 2001 صادق الكونغرس بأغلبية ساحقة على قانون ضد الأرهاب هو " USA Patriot Act " في 25 أوكتوبر 2001 . [1]

ويجرم هذا القانون بالإضافة الى انشاء مواقع تروج للإرهاب تقديم المساعدة أو النصيحة لإرهابيين بواسطة موقع أنترنت، كما أعطى لجهاز المكتب الفدرالي للتحقيقات FBI الحق في التجسس على كل جهاز اتصالات يخص شخص له علاقة أو شبهة مباشرة أو غير مباشرة مع جماعة ارهابية ، كما اعتبر القانون أن الدخول غير المصرح به الى نظام معالجة آلية للمعطيات قد يشكل عملا ارهابيا ، ووسع القانون من قائمة المعلومات التي يمكن للمحققين الحصول عليها والاحتفاظ بها دون شرط الحصول على إذن قضائي.

وتعد قضية "بابار أحمد BABAR Ahmed " من الأمثلة المهمة في هذا المجال ، وهو شخص بريطاني مقيم في بريطانيا قام بإنشاء موقعين على شبكة الانترنت لدعم الأعمال الجهادية في الشيشان ، وكان مضيف الموقعين في الولايات المتحدة الأمريكية ، فسلمته الحكومة البريطانية إلى نظيرتها الأمريكية أين حوكم بموجب قانون "USA Patriot Act " وأدين بتهمة استعمال الانترنت لتمويل والترويج للإرهاب. [3]

وفي المملكة المتحدة فقد كانت هجمات لندن 2005 السبب الرئيسي الذي دفع الحكومة البريطانية لسن قانون ضد الأرهاب وهو " Terrorism Act 2006 " و الذي يجرم في القسم الثالث من الفصل الاول إنشاء موقع انترنت يروج للأعمال الأرهابية بعد أن اتخذت العديد من الجماعات الأرهابية المملكة المتحدة مكانا مناسبا لدعم الارهاب ، الى ان صادق البرلمان البريطاني على القانون السابق بعد أن ألغى البند المتعلق بالوقف للنظر لمدة 90 يوما ولكن أثبتت التطبيقات عجز القانون في منع الجماعات الارهابية من انشاء مواقع انطلاقا من المملكة المتحدة.[3]

أما في الجزائر فإن القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها ، والذي سنتطرق إليه بالتفصيل في الفصل الثالث ، قد حدد الحالات التي تسمح باللجوء إلى مراقبة الإتصالات الإلكترونية ومن بينها الوقاية من الافعال الموصوفة بجرائم الإرهاب و التخريب و الماسة بأمن الدولة ، إلا أنه بخلاف القانون الفرنسي و الأمريكي في هذا المجال فان المشرع الجزائري حسب المادة 04 ألزم ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الاجرام المتصل بتكنولوجيات الاعلام و الاتصال بالحصول على إذن قضائي من طرف النائب العام لدى مجلس قضاء الجزائر صالح لمدة 6 أشهر قابلة للتجديد لإجراء عملية المراقبة ، مع تشديد المشرع على عدم المساس بالحياة الخاصة للغير.[4]

---

[1] USA Patriot Act à l'adresse :http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[2] « British Man Arrested on several Terrorisme related Charges » communiqué de presse,United States Attorney Office District of Connecticut,6 Aout 2004 à l'adresse : http://www.US.doj.gov/usao/ct/presse2004/20040806.html

[3] Terrorism Act 2006 à l'adresse : http://www.northants.police.uk/files/documents/Terrorism/te98%5ETerrorism%20Act%202006.pdf

[4] القانون رقم 09- 04 مؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها، ج .ر عدد 47 ، ص 5.

المطلب الثالث
جرائم التجسس المعلوماتي وانتهاك الملكية الأدبية و جرائم اتلاف المواقع وتخريب شبكة المعلومات

في عصر المعلومات برزت صور من الجرائم وسيلتها واحدة تتمثل في الإمكانيات التي تتيحها التكنولوجيا الحديثة ، لكن أغراضها تختلف من جريمة إلى اخرى ، فبينما يهدف الجناة في جريمة التجسس المعلوماتي إلى الحصول على المعلومات ذات القيمة الاستراتيجية ، فإن غرضهم من اختراق أجهزة الحاسب الآلي أو المواقع الإلكترونية قد يكون إما لانتهاك حقوق الملكية الأدبية من خلال قرصنة البرامج أو تدفعهم الرغبة في العبث و اتلاف المواقع الالكترونية و تخريب شبكة الاتصالات ، وهذا ما سوف نتناوله في هذا المطلب ، حيث نتطرق لكل جريمة من الجرائم السابقة ونبين السلوك الاجرامي فيها.

الفرع الأول
التجسس المعلوماتي

التجسس المعلوماتي هو الحصول على معلومات سرية قد تخص الأفراد ، أو تتعلق بالمؤسسات الحكومية و العسكرية أو على المؤسسات المالية و التجارية و الاقتصادية للدولة .
ويكمن الخطر في عملية التجسس في استغلال الجناة لهذه المعلومات السرية فيما يضر مصلحة ووحدة الدولة ، فبعد اختراق الجاني للشبكات و المواقع الالكترونية من خلال برامج وفيروسات مخصصة للتجسس ، مثل فيروس "حصان طروادة Trojan Horse " [1] وبعد أن يجمع المعلومات السرية المتحصل عليها من اجهزة الحاسب الالي الخاصة بالمؤسسات الاقتصادية و العسكرية المتصلة بشبكة الانترنت أو من خلال المواقع الإلكترونية و البريد الالكتروني لهذه المؤسسات يقوم بتهريبها إلى الدولة المعادية أوالى المنظمات الاجرامية أو الجماعات الارهابية .
ومن بين الطرق الحديثة في عمليات التجسس هناك برنامج " الكي لوجر keylogger " [2] ، وهو جهازيستعمل للتجسس حيث يقوم بتسجيل الدقات على لوح المفاتيح ويسجلها في ذاكرته وبذلك يتمكن الجاني من الحصول على الكلمات السرية وشيفرات الدخول الى غير ذلك من المعلومات ، كما بوجد برنامج التجسس " spyware " [3] الذي يقوم بجمع المعلومات من جهاز الحاسب المسجل عليه ومن ثم يقوم بارسال المعلومات الى الشركة صاحبة البرنامج ، بالاضافة الى برامج مثل " Sniffer " [4] المختصة في الحصول على كلمات السر.
فالسلوك الاجرامي في التجسس المعلوماتي يتمثل في الدخول غير المشروع عن طريق شبكة الانترنت او احدى وسائل تقنية المعلومات إلى موقع محمي بغرض الحصول على معلومات سرية للدولة و إفشاء هذه الأسرار ، لذا تشدد كل التشريعات في عقوباتها على جرائم التجسس وتعتبرها خيانة على غرار المشرع الجزائري الذي جرم في المادة 63 من قانون العقوبات فعل تسليم معلومات تضر بالمصالح العسكرية أو الاقتصادية " باية وسيلة كانت " ، مما ينطبق على جرائم التجسس التي تتم عن طريق شبكة الانترنت وحدد لها عقوبة الاعدام.

---

(1) (2) (3) (4) انظر في الملحق رقم 1- المصطلحات الواردة في الدراسة.

الفرع الثاني
جرائم القرصنة المعلوماتية و انتهاك الملكية الادبية

إن التطور السريع الذي شهدته تكنولوجيات الاعلام و الاتصال جعلت من عمليات انتهاك الملكية الادبية مشكلة تطرح بقوة ، حيث اتاحت شبكة الانترنت لمرتكبي جرائم القرصنة الالكترونية او المعلوماتية امكانية الولوج الى اغلب اجهزة الحاسب الالي المرتبطة عبر هذه الشبكة ، ومن خلال عمليات الاختراق و التسلل يمكن للجاني ان يقوم باعمال القرصنة و انتهاك الملكية الادبية لصاحب الجهاز او الموقع الاللكتروني ، ، حيث يستطيع القراصنة القيام بعملية " نسخ البرامج و الملفات Piratage de logiciel " بوجه غير شرعي أو بث الأعمال الادبية و الافلام السينمائية ، مما يتيح لكل متصفح للشبكة ان يتحصل على نسخة مقلدة من هذا المنتج، وهو ما يعد جنحة تقليد وتعدي على على حقوق المؤلف الشرعي وانتهاكا للقوانين التي تحمي الملكية الفكرية.
كما تشمل الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسب الآلي و نظمه وهو ما يعرف بقرصنة البرمجيات كنسخ و تقليد البرامج و اعادة انتاجها دون ترخيص مما يشكل اعتداءا على العلامة التجارية وبراءة الاختراع.
وأهم المعاهدات التي تحمي الملكية الفكرية تلك التي وقعتها المنظمة العالمية للملكية الفكرية التابعة للأمم المتحدة " وايبو WIPO " و ذلك في استوكهولم في 14 يوليو سنة 1967 وتم تعديلها في 28 سبتمبر 1979 والتي تنص على امتداد حقوق المبدعين الى خمسين سنة بعد وفاة المبدع [1] .
كما وضعت سنة 1978 قواعد دولية لحماية برامج الحاسب الآلي ضد كل أشكال القرصنة و التعدي من خلال "هيئة المؤلفين الدوليين لبرامج الحاسوب" التي تقوم بالتنسيق مع الشركة الدولية "مايكروسوفت" بمراقبة حواسيب الشركات والإدارات، والبحث في مدى حرصها على احترام بنود عقود الترخيص بالاستعمال.
وبالنظر إلى مختلف صور الاعتداء التي تطال المعلومات نجد أنها تتنوع بين اعتداء على معطيات الحاسب الآلي لقيمتها المادية أوالمعنوية ، و الاعتداء على حقوق الملكية الفكرية لبرامج الحاسب الآلي الذي يشكل اعتداء على الحقوق المالية و الأدبية لصاحب البرنامج ، لذا نجد أن أشكال الحماية القانونية تنوعت بين حماية حقوق الملكية الأدبية للبرامج أو حماية البيانات الشخصية المتعلقة بالحياة الخاصة، وحماية المعطيات و المعلومات السرية من خلال تجريم المساس بأنظمة المعالجة الآلية للمعطيات.

وقد نصت أغلب التشريعات على جنحة التقليد ضمن أحكام القوانين الخاصة بالملكية الفكرية ، ففي فرنسا تجرم المادة L335 - 2 من قانون حماية الملكية الفكرية تقليد مصنف أدبي مكتوب أو موسيقي أو رسوم الى غير ذلك من الاعمال الفنية التي ذكرتها المادة وجعلت لها عقوبة الحبس من ثلاثة أشهر الى سنتين وغرامة من 6000 الى 20.000 فرنك فرنسي ، كما جرمت المادة L335- 3 اعادة انتاج أو توزيع و بأي طريقة كانت مصنف محمي بموجب قانون حماية الملكية الفكرية ، ونص المشرع الفرنسي في المادة (L.112 -1) على حماية البرامج المعلوماتية من التقليد ، و أقر حماية تمتد لمدة 25 سنة من تاريخ اختراعها حسب نص المادة (L.123- 5) [2] ، في حين أن القانون رقم 98-536 الصادر في 1 جويلية 1998 [3] فقد نص في المادة (L.431) على حماية جنائية ضد الاعتداء على حقوق منتجي قواعد البيانات [4] .

---

[1] غسان رباح، الوجيز في قضايا حماية الملكية الفكرية و الفنية ،منشورات الحلبي الحقوقية،الطبعة الاولى،2008،ص75.

[2] la loi n° 92-597 du 1er juillet 1992 relative au code de la propriété intellectuelle, J.ORF n°153 du 3 /7/ 1992, p. 8801

[3] la loi n° 98-536 du 1er juillet1998 à l'adresse : http://www.wipo.int/wipolex/fr/details.jsp?id=5589

[4] انظر في الملحق رقم 1- المصطلحات الواردة في الدراسة.

وتثير متابعة جنحة التقليد عبر الانترنت اشكالية الاختصاص، ففي حكم صادر عن محكمة النقض الفرنسية بتاريخ 29 نوفمبر 2011 تم نقض قرار محكمة استئناف باريس الصادر في 5 نوفمبر 2009 الذي ادان بجنحة التقليد عبر شبكة الانترنت " F. Giuliano" و ذلك لقيامه باعادة انتاج مقال لكاتب ايطالي"T.Antonio " حرره لفائدة يومية "Le Monde الفرنسية" غير انه في اليوم الذي يسبق صدور المقال على الجريدة الفرنسية نشر على جريدة ايطالية "Il Foglio " بدون رضا صاحب المقال ، وعلى هذا الأساس فقد أدانت محكمة استئناف باريس الجريدة الايطالية وحكمت عليها بغرامة 10.000 اورو عن جنحة تقليد عن طريق نشر او اعادة انتاج مصنف محمي بحقوق المؤلف، إلا أن محكمة النقض استندت على المادة 113 من قانون العقوبات الفرنسي و التي تنص على أن قانون العقوبات يطبق على الجرائم المرتكبة فوق تراب الجمهورية و يعتبر كذلك متى كانت احدى عناصر الجريمة مرتكبة فوق تراب الجمهورية الفرنسية ، وكون الجريدة الايطالية مدونة باللغة الايطالية و موجهة الى الجمهور الايطالي و أنها غير موزعة بصورتها الورقية على التراب الفرنسي بالإضافة إلى أن ادارة الموقع كانت في ايطاليا، فاعتبرت أن أحكام جنحة التقليد لا تنطبق عليها و نقضت الحكم . [1]

أما في الجزائر فإن المشرع الجزائري قد أكد حمايته لبرامج الحاسب الآلي من خلال النص على تجريم الاعتداء على حقوق المؤلف و الحقوق المجاورة ، وجاء في المادة 4 من الامر 97-10 المتعلق بحقوق المؤلف و الحقوق المجاورة أن مصنفات وقواعد البيانات تعتبر كمصنفات ادبية ، و لو أن مصطلح قواعد البيانات (Bases des données) أريد به برامج الحاسب الالي و مصطلح مصنفات البيانات من خلال مايقابله في النص الفرنسي يشير إلى برمجيات الحاسب الالي (Les logiciels) ، فان عدم الدقة في وضع المصطلح المناسب من شانه أن يؤدي الى الابتعاد عن المغزى الاساسي من وضع النص ، حيث أن البرمجيات أوسع بكثير من مصنفات البيانات و مصطلح قواعد البيانات يختلف عن برامج الحاسب الالي.
وبعد صدور الامر رقم 03-05 الذي الغى الامر رقم 97-10 بموجب المادة 163 ونص صراحة في المادة (04 فقرة أ) على اعتبار برامج الحاسب الالي من بين المصنفات الادبية المحمية ومن خلال نص المادة 151 من الامر رقم 03-05 المتعلق بحماية حقوق المؤلف و الحقوق المجاورة [2] ، ذكر المشرع الجزائري الأفعال التي تشكل جريمة التقليد ونص على أنه : " يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية :

- الكشف غير المشروع للمصنف او المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف.
- استنساخ مصنف او اداء باي اسلوب من الاساليب في شكل نسخ مقلدة .
-استيراد او تصدير نسخ مقلدة من مصنف او اداء.
- بيع نسخ مقلدة لمصنف او اداء.
- تاجيراو وضع رهن التداول لنسخ مقلدة لمصنف او اداء.

كما نصت المادة 152 من نفس الامر على ان « يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الامر فيبلغ المصنف او الاداء عن طريق التمثيل او الاداء العلني او البث الاذاعي السمعي او السمعي البصري او التوزيع بواسطة الكابل او باية وسيلة نقل اخرى لاشارات تحمل اصواتا او صورا او باي منظومة معالجة معلوماتية » وعاقب على جنحة التقليد في المادة 153 بالحبس من ستة اشهر الى ثلاث سنوات وبغرامة من 500.000 دينار الى 1.000.000 دينار.

---

[1] انظر منطوق القرار في الملحق رقم 4 .

[2] الأمر 05/03 الصادر بتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر 14/73، ج.ر عدد 44 بتاريخ 2003/07/23.

الفرع الثالث
جرائم اختراق المواقع وإتلافها وتخريب شبكة المعلومات

تضم هذه الطائفة من الجرائم أفعال الاختراق والعمليات التخريبية التي تطال أجهزة الحاسب الآلي و المواقع الإلكترونية و شبكة الأنترت ، حيث تشمل هذه الجرائم مايلي :

أولا - جرائم الاختراق :

تعد مواجهة جرائم الاختراق من أهم التحديات في هذه الفترة ، فتزايد عدد المتسللين وتعدد الطرق المتطورة باستمرار و التي تستخدم في عمليات الاختراق تستوجب البحث عن أنجع السبل لتحقيق حماية أجهزة الحاسب الآلي من عمليات الاختراق .

ولكي تتم عملية الاختراق على شبكة الانترنت لا بد من برنامج يتم تصميمه لكي يتيح للمخترق إختراق جهاز الحاسب الالي للمجني عليه، أو بريده الالكتروني أو اختراق موقع إلكتروني ما على الشبكة ، ولهذا الغرض فقد تم تصميم عدة برامج تتيح عملية الاختراق .

وبسبب الثغرات الموجودة في نظام الحماية الخاص بجهاز الحاسب الالي أو الموقع الإلكتروني تسهل عملية الإختراق، وفي غالب الأحيان يلجأ المخترق أو الهاكر Hacker [1] إلى طرق متعددة نذكر منها :

1- الاغراق بالرسائل أو Spam [2]:

حيث يتم إرسال كم هائل من الرسائل عبر البريد الإلكتروني لأجهزة الكمبيوتر المراد العمل على تعطيلها. وتكون هذه الرسائل محملة بملفات كبيرة وترسل بأعداد كبيرة لا تتناسب مع المساحة المحددة للبريد الإلكتروني و تصل لجهاز الكمبيوتر مرة واحدة وفي نفس الوقت مما يؤدي الى امتلاء منافذ الإتصال وبالتالي توقف تلك الأجهزة عن العمل.

2- الفيروسات:

يتم اختراق جهاز الحاسب الالي للمجني عليه بارسال الفيروس وهو عبارة عن برنامج مثل أي برنامج موجود داخل جهاز الكمبيوتر تم تصميمه للتأثير على كافة أنواع البرامج الأُخرى الموجودة على الجهاز سواء بعمل نسخة منها أو تعطيلها عن العمل.وتبدأ الفيروسات عملها بمجرد قيام المجني عليه بفتح الرسالة . واشهر هذه الفيروسات احصنة طروادة Trojans وهي برامج تجسسية ، الديدان Worms و القنبلة المعلوماتية Information Bomp وهي برامج تخريبية تستعمل لتعطيل جهاز الحاسب الالي المخترق .

وتتعدد دوافع المخترق بحسب طبيعته فقد يكون من الهواة أو الهاكر يهدف إلى العبث بمواقع الآخرين و ببريدهم الإلكتروني أو يكون من فئة المحترفين أو الكراكر[3] الذي تكون له دوافع مالية كالحصول على ارقام البطاقات الالكترونية أو الحصول على المعلومات لاغراض تجسسية.

---

(1) (2) (3) انظر في الملحق رقم 1-المصطلحات الواردة في الدراسة.

ثانيا – جريمة اتلاف المواقع :

تعد جريمة اتلاف المواقع من اكثر الجرائم الشائعة التي تستهوي فئة المخترقين أوالهاكرز، حيث يقومون بتغيير تصاميم المواقع أومايسمى بتغيير وجه المواقع أوعرقلة الوصول إليها و تدميرها أحيانا .

ويعد أهم أسباب هذا السلوك هو سرعة انتشار الخبر حول اختراق الموقع لما في ذلك من ابراز لقدرات المخترق.

و من الوسائل المستخدمة لتدمير المواقع ارسال مئات الآلاف من الرسائل الإلكترونية (E-mails) من جهاز الحاسوب الخاص بالمدمر إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع ، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي، أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه.

ثالثا - جريمة تخريب شبكة المعلومات :

يتمثل السلوك الاجرامي في هذه الجريمة في إدخال عن طريق شبكة المعلومات (الأنترنت) ما من شأنه ايقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو اتلاف أو تعديل البرامج أو المعطيات أو المعلومات فيها.

و يلجأ المخترقون إلى عدة وسائل لهذا الغرض كنشر الفيروسات أو ارسال مئات الرسائل الى البريد الالكتروني لشخص ما ، مما يؤدي الى تعطل الشبكة و عدم امكانية استقبال أي رسائل فضلا عن امكانية انقطاع الخدمة إو انكار الخدمة " Le déni de service " إذا كانت الجهة المتضررة هي مقدمة خدمة الانترنت ، حيث يتم ملء منافذ الاتصال و قوائم الانتظار مما ينتج عنه انقطاع الخدمة ، و بالتالي التسبب في خسائر مادية و معنوية كبيرة لمستخدمي الشبكة.

وقد حدث في شهر فبراير سنة 2000 أن كان موقع " ياهوو Yahoo " وهو محرك بحث شهير عرضة لهجوم الكتروني تخريبي تسبب في تعطله و رفض تقديم الخدمة لمرتادي الموقع مما سبب عطلا في شبكة المعلومات. [1]

---

[1] Henri Manzanaré et philipe Nectoux, L'informatique au service de juriste,Litec, Paris,1987.p .417.

المبحث الثالث

مكافحة الجريمة المعلوماتية في القوانين المقارنة

يرى بعض المتخصصين في دراسة الإجرام المعلوماتي أن زيادة نمو وكثافة تكنولوجيا المعلومات و الاتصالات و جني فوائد مجتمع المعلومات يؤدي أيضا إلى زيادة الجرائم المتصلة بالحاسب الالي ، و بالتالي فإنه من مصلحة الأمن الاقتصادي و الأمن العام سن تشريعات محلية لمكافحة الجرائم المتصلة بالحاسب الآلي للحد من إنتشارها. [1]

وهذا ما جعل العديد من الدول تسارع لتطوير بنيتها التشريعية لتنظيم مجال تكنولوجيا المعلومات و الاتصالات. إلا أن سبل هذه المكافحة اختلفت بين دولة و أخرى ، فبينما كان اصدار تشريعات جديدة تحدد السلوكات المجرمة وتلائم طبيعة الجريمة المعلوماتية هو المنهج الذي اتخذته دول كالولايات المتحدة الأمريكية فقد قامت دول أخرى مثل فرنسا بتعديل قانون العقوبات عدة مرات لتواكب التطور الحاصل في الجرائم المعلوماتية، في حين نجد دولا أخرى مازالت تعتمد على النصوص التقليدية القائمة لمواجهة هذه الجرائم مع مايثيره ذلك من اشكالات تتعلق بالاخلال بمبدأ الشرعية الجنائية ، وأحيانا يفلت الجاني من العقاب بسبب عدم تكييف هذه الدول لقوانينها العقابية مع هذا الاجرام المستجد.

سنتناول في هذا المبحث الاطار القانوني لمكافحة الجريمة المعلوماتية في بعض التشريعات الغربية كما سنتطرق لأهم التجارب العربية بهذا الخصوص ، وفي الاخير سنتناول مكافحة الجريمة المعلوماتية على المستوى الدولي من خلال دراسة بدايات التشريع الدولي في هذا المجال .

المطلب الاول

الإطار القانوني لمكافحة الجرائم المعلوماتية في الدول الغربية

أسفرت دراسة اجريت سنة 1987 تتعلق بالوسائل التي اتجه اليها المشرع في تعامله مع الجريمة المعلوماتية عن اختلاف بين الدول في تقرير الحماية الجنائية لنظم المعلوماتية ، فالولايات المتحدة الامريكية وعلى المستوى الفدرالي مثلا تهتم بحماية المعلومات في حد ذاتها ، و خاصة المتعلقة منها بالحياة الخاصة للأفراد و التي تكون لها قيمة اقتصادية ، أو المعلومات ذات التي تصنف في نطاق أسرار الدولة. و قد اخذت العديد من الدول الاسكندنافية بهذا الإتجاه حيث أن أغلب هذه التشريعات تجرم الدخول غير المصرح به لنظام الحاسب الآلي ، بينما اتخذت تشريعات أخرى من مبدأ حماية المعلومات باعتبارها ملكية خاصة أسلوبا في صياغة النصوص لحماية الأنظمة المعلوماتية من الاعتداء ومن أمثلة التشريعات التي سارت في هذا الاتجاه نجد تشريعات مختلف الولايات في الولايات المتحدة الامريكية بالاضافة الى النمسا وسويسرا. [2]

---

[1] Hon Russel Fox, Justice in The Twenty First Century, Cavendish Publishing, London, 2000, p .22.

[2] Kaspersen (Henric W.K) , Stands for computer crime legislation- comparative analysis, Kuler law & taxation publishers, 1989, p .52.

أما الاتجاه الذي اتخذته المملكة المتحدة فهو يركز على سلامة المعلومات و البيانات التي يحتوي عليها الحاسب الآلي مع صرف النظر عن طبيعة الاعتداء الاجرامي الذي يطالها مثلما فعلت من خلال المادة الثامنة من القانون الخاص بجرائم التزوير و التزييف لسنة 1981 بعد أن تم اضافة المعلومات كمحل في جريمة التزوير .

في حين أنه في فرنسا فقد تم تعديل قانون العقوبات عدة مرات حيث وضعت نصوصا تتعامل مع الأوجه المختلفة لجرائم المعلوماتية .
وحاليا نجد دولا أخرى اعتمدت موقفا تشريعيا يجمع بين مختلف الاتجاهات السابقة كهولندا و السويد وهو الاتجاه السائد حاليا وبدأت العديد من الدول بالأخذ بهذا الاسلوب لإلمامه بمختلف أوجه الحماية الجنائية للمعلومات .
سنحاول تبيين كيف تعاملت التشريعات الغربية مع الجريمة المعلوماتية وأخذنا كمثال على ذلك كل من فرنسا و المملكة المتحدة و الولايات المتحدة الأمريكية من خلال ابراز اهم ما أصدرته هذه الدول من قوانين لمكافحة الاجرام المعلوماتي.

الفرع الاول
مكافحة الجرائم المعلوماتية في فرنسا

يعتبر القانون الخاص بالمعلوماتية وملفات البيانات و الحريات رقم 78- 17 الصادر بفرنسا و المؤرخ في 6 جانفي سنة 1978 ، أول قانون ينظم الجوانب القانونية المتصلة بالمعلوماتية و اثرها على الخصوصية ، حيث نص على انشاء اللجنة الوطنية للمعلوماتية و الحريات، مهمتها مراقبة حسن تطبيق هذا القانون ، وقد نص هذا القانون في المادة 14 منه على حماية البيانات الخاصة سواء كانت ملك للدولة أو للأشخاص [1] .

و كانت فرنسا من الدول التي اهتمت بتطوير منظومتها القانونية لتتلاءم مع مستجدات الاجرام المعلوماتي ، حيث تضمن قانون العقوبات الفرنسي من خلال التعديلات المتلاحقة عليه نصوصا خاصة بالمعالجة الالية للبيانات ، فقد أصدرت سنة 1988 القانون رقم 19- 88 الذي يعد أول تشريع فرنسي لتجريم بعض صور جرائم الحاسب الآلي وهو ما عرف بقانون "Godfrain ". [2]

حيث نص في المادة 462 منه على تجريم القيام بالدخول أو البقاء بطريقة كلية أو جزئية داخل منظومة لمعالجة المعلومات ، و عاقبت على ذلك بالحبس لمدة شهرين إلى سنة وغرامة مالية بقيمة ثلاثة آلاف إلى خمسين ألف فرنك فرنسي ، أما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل أو اتلاف للمعطيات المخزنة فإن العقوبة ستكون بالحبس من شهرين إلى سنتين و بالغرامة المالية التي تتراوح بين عشرة آلاف فرنك إلى مئة ألف فرنك ، وبصدور القانون الجديد سنة 1994 تم تعديل المادة السابقة بالمادة 323 حيث تم النص على تجريم المساس بنظام المعالجة الالية للمعطيات بمختلف أشكال الاعتداء التي ذكرتها المواد 323 -1، 323 -2، و323-3 .

---

[1] Ber-Gabal , le control de l'administration par la commission national de l'informatique et des libertés, R.D.P, 1980 p.1034.

[2] La loi N°88-19 du 5 Janvier 1988 relative à la Fraude Informatique, J.O.,N° 4 ,6 Janvier 1988.

فقد ورد في المادة 323 -1 تجريم فعل الدخول أو البقاء بطريقة احتيالية في كل أو جزء من نظام المعالجة الالية للمعطيات وعاقبت على ذلك بالحبس مدة سنتين و غرامة مالية بقيمة 30.000 أورو ، أما اذا نتج عن ذلك حذف او تعديل للمعطيات الموجودة في النظام او تحريف لمجريات النظام فتكون العقوبة الحبس لمدة ثلاث سنوات و الغرامة بقيمة 45.000 أورو [1].

وجرمت المادة 323-2 فعل اعاقة أو تعطيل تشغيل نظام المعالجة الالية للمعطيات بخمس سنوات حبس وغرامة بـ 75.000 أورو.
أما المادة 323-3 فقد جرمت ادخال بطريقة احتيالية معطيات الى نظام المعالجة الالية ، او حذف او تعديل المعطيات ، فيعاقب بالحبس مدة بخمس سنوات حبس وغرامة بـ 75.000 أورو.
وعاقبا المادة 323-3-1 على جلب أو حيازة أو اعطاء أو وضع تحت تصرف أداة أو برنامج معلوماتي أو أية معطيات يمكن أن ترتكب بها أي جريمة من الجرائم المذكورة في المواد 323-1 إلى 323-3 ، ويعاقب على ذلك بنفس العقوبة المقررة للجريمة نفسها أو بالعقوبة الأشد .
في حين نصت المادة 323-4 على معاقبة الاشتراك و المساهمة في تنفيذ الجرائم المنصوص عليها في الفقرات 323-1 الى 323-3 وجعلت عقوبة الشريك و المساهم بنفس عقوبة الفاعل الأصلي .

أما المادة 323-5 فقد أشارت إلى معاقبة الأشخاص الطبيعيين مقترفي الافعال المجرمة السابقة بعقوبات تكميلية الى جانب العقوبات الاصلية تتمثل في المنع من الحصول على الحقوق المدنية و العائلية حسب اجراءات المادة 131- 26 من قانون العقوبات الفرنسي ، و المنع من ممارسة الوظائف العامة ، ومصادرة المواد التي استخدمت في ارتكاب الجريمة او المعدة لذلك ، واذا كان الفعل مرتكبا من طرف احدى المؤسسات فيكون العقاب بالاغلاق و الطرد من الصفقات العامة ونشر الحكم حسب شروط المادة 131-35 من قانون العقوبات الفرنسي.

وأشارت المادة 323-6 الى مسؤولية الاشخاص المعنوية جزائيا وفقا للشروط المنصوص عليها في المادة 121-2 من قانون العقوبات الفرنسي ويعاقب بالغرامة المنصوص عليهافي المادة 131-38 من قانون العقوبات الفرنسي و العقوبات المذكورة في المادة 131-39 ، و المنع المنصوص عليه في البند الثاني من المادة 131-39 .

وأخيرا في تم النص على معاقبة الشروع في ارتكاب اي من الجرائم المنصوص عليها سابقا بنفس عقوبة الجريمة التامة كما ورد في المادة 323- 7.
وقد تم تعديل المواد السابقة بالقانون رقم 575- 2004 المتعلق بالثقة في الاقتصاد الرقمي بتاريخ 21 جوان 2004 الذي شدد من العقوبات السابقة في المواد 45 و46 حماية للتعاملات الاقتصادية من خطر فقدان الثقة بين المتعاملين ، كما وضع أحكاما جزائية لتنظيم عملية تشفير الوثائق المعلوماتية في المادة 35 بحيث سمح بالقيام بعملية التشفير لكن بعد طلب الرخصة من السلطات المختصة بذلك وحدد عقوبات تتراوح بالحبس سنتين مع الغرامة بقيمة 30.000 أورو لكل مخالف لهذه الاحكام ، أما المادة 37 من قانون الثقة في الاقتصاد الرقمي فقد خصصها لتشديد العقوبة على كل من يستعمل الوسائل المادية المعدة لغرض التشفير في ارتكاب أو تسهيل ارتكاب جرائم . [2]

---

(1) Code pénal français, DALLOZ, Paris, ed. 2006, p.58.

(2) LOI n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O.R.F n°143 du 22 juin 2004 p. 11168

الفرع الثاني
مكافحة الجرائم المعلوماتية في المملكة المتحدة

قامت المملكة المتحدة بتبني عدة تشريعات حماية للأنظمة المعلوماتية لديها وذلك بعد أن أظهرت التجارب القضائية ضرورة وجود نصوص خاصة بذلك ، حيث صدر قانون إساءة استخدام الحاسب الالي لسنة 1990 الذي نظم جرائم الحاسب الآلي ضمن ثلاثة حالات تتعلق الأولى بالدخول غير المصرح به إلى معطيات الحاسب الآلي وبرامجه المخزنة ، حيث نص القانون على أن الشخص يكون مذنبا بالدخول غير المصرح به إذا ارتكب احدى الافعال التالية [1]:

- تسبب بقيام الكمبيوتر بأية وظيفة بنية التوصل غير المصرح به الى برنامج ما أو أية معطيات داخل جهاز الكمبيوتر.
- كان الدخول غير مصرح به.
- تم تعديل التوقيت لجعل الكمبيوتر يقوم بالمهمة المذكورة .

و جرمت المادة الاولى من هذا القانون فعل الدخول غير المصرح به إلى نظام الحاسب الالي. ومما جاء في نص هذه المادة :

- « يعاقب على الدخول غير المصرح به إلى نظام الحاسب الالي بالحبس بحد اقصى ستة اشهر او بغرامة قدرها الفا جنيه استرليني او كليهما معا ».

أما الحالة الثانية فقد تناولت تجريم الدخول غير المصرح به مع وجود بنية ارتكاب او تسهيل ارتكاب جرائم اخرى ، فقد نصت المادة الثانية على أنه «يعاقب على الدخول غير المصرح به الى نظام الحاسب الالي و ذلك بنية ارتكاب او تسهيل ارتكاب جريمة اخرى بالسجن لمدة خمس سنوات او بغرامة مالية يقدرها القاضي او بكليهما معا ».

حيث أريد من هذا التجريم معالجة الحالات التي يتم فيها الولوج الى نظام الحاسب الالي بنية ارتكاب جريمة اخرى كاسرقة او التهديد او النصب مع اشتراط ان تتوافر نية الدخول الى نظام الحاسب الالي لارتكاب جريمة اخرى [2].

أما الحالة الثالثة فتتعلق بتجريم الإتلاف المعلوماتي ، من خلال نص المادة الثالثة التي جاء فيها « كل من يقوم بعمل من شأنه احداث تغييرات غير مصرح بها في محتوى أى حاسب آلي، متى توافر لديه العلم و الإرادة وقت قيامه بهذا الفعل» [3].

و جاء في المادة السابعة عشر من القانون سالف الذكر تعريفا للمقصود بإحداث تغييرات في محتوى الحاسب الآلي ، حيث ذكرت المادة بأنه كل تعديل أو محو للبرامج أو اضافة معلومات إلى الحاسب الآلي وقد أدرجت المادة الثالثة من قانون اساءة استخدام الحاسب الالي اعاقة نظام الحاسب الالي ضمن المفهوم الواسع لفعل الاتلاف .

---

[1] غسان رباح،الوجيز في حماية الملكية الفكرية و الفنية،منشورات الحلبي الحقوقية، الطبعة الاولى،بيروت،2008، ص153.

[2] Bainbridge (David), Op.cit. p.314.

[3] نائلةعادل قورة، المرجع السابق، ص 211.

و في تطبيقات القضاء الانجليزي بهذا الخصوص نجد مثالا عن ذلك قضية "Goulden " أين قام المتهم بادخال برنامج الى نظام الحاسب الآلي لشركة كان يعمل بها من شأن هذا البرنامج أن يحول دون الدخول إلى نظام الحاسب الآلي مستخدما شفرة لا يعلمها إلا المتهم ، وقد نتج عن اعاقة النظام خسائر كبيرة للشركة ، مما جعل المحكمة تنتهي الى ادانته بتهمة الاتلاف حسب المادة الثالثة من قانون اساءة استخدام الحاسب الالي الصادر سنة 1990. [1]

ويجرم التزوير بمقتضى قانون التزوير و التزييف الصادر سنة 1981، حيث تعاقب المادة الأولى منه كل من يقوم بنية تحقيق ربح له او للغير او الحاق خسارة بالغير بتدمير أو محو او اخفاء أو تزوير بيانات حسابية ، وكذلك كل من يقوم باستخدام مثل هذه البيانات أو المستندات أو التسجيلات المزورة ، و يشمل مصطلح التسجيلات المزورة المعلومات التي يتم تسجيلها الكترونيا ، وقد نصت المادة الثانية على أنه يعد مرتكبا لجريمة التزوير كل من يقوم بخلق أداة مزورة بنية اقناع شخص اخر بقبولها بوصفها أداة سليمة و يقصد بالأداة حسب المادة الثامنة بأنها كل اسطوانة او شريط ممغنط أو شريط صوتي أو أي جهاز آخر سجل فيه أو عليه معلومات ، أو حفظت بوسائل ميكانيكية أو الكترونية أو بوسائل أخرى . ويفهم من هذه المادة ضرورة وجود وسيط مادي تسجل عليه المعلومات .

وتطبيقا لذلك فقد رفض القضاء البريطاني تطبيق هذه المادة في قضية " R. V .Gold "، أين رات المحكمة أن استعمال شفرات غير سليمة للدخول إلى نظام الحاسب الآلي لا يمكن اعتبارها أداة مادية لأنها مجرد اشارات إلكترونية [2].

ونظرا لفشل النيابة في الإتهام أو الحصول على إدانة في العديد من القضايا المشابهة فقد صدر قانون اساءة استخدام الحاسب الآلي سنة 1990 الذي سبق ذكره.

أما بخصوص جريمة الاحتيال المعلوماتي فقد اظهرت دراسة اجريت في المملكة المتحدة من سنة 1983 عرفت باسم صاحبها "Ken Wong" ، بينت أن 63% جرائم المعلوماتية تتعلق بالاحتيال المعلوماتي و أغلبها تلك المتعلقة بالتحويلات الالكترونية للاموال. [3]

و تم تجريم الاحتيال المعلوماتي في التحويل الالكتروني غير المشروع للأموال بموجب تعديل سنة 1996 الذي طرأ على الفقرة الأولى من المادة الخامسة عشر من القانون الخاص بالسرقة لسنة 1968 ، وذلك بعد أن تم رفض تطبيق النص الخاص بجريمة السرقة على فعل الحصول على ممتلكات الغير عن طريق الاحتيال من خلال التحويل الالكتروني غير المشروع للاموال من رصيد لاخر في قضية " R .v.Preddy" سنة 1996 بعد أن رفض مجلس اللوردات البريطاني تطبيق المادة الخاصة بالسرقة على التحويل الاكتروني غير المشروع للاموال ، حيث تم اضافة الفقرة أ إلى نص المادة الخامسة عشر و التي تعاقب على فعل الحصول عن طريق الإحتيال على تحويل الكتروني للأموال من رصيد لآخر له أو للغير ولا يهم الطريقة التي تم بها التلاعب في البيانات من اجل اجراء عملية التحويل [4].

---

[1] Dumbill (Eric), Computer misuse act 1990 - recent development , C.L.P., vol 8, N° 4, p 106 .

[2] Wasik (Martin), Op.cit,1991., p .113.

[3] Cornwall (Hugo), Datatheft , Computer Fraud Industrial Espionage and Information Crime , Heinemann, London , 1987 p .57.

[4] Bainbridge (David), Op.cit, 2000.p.297.

الفرع الثالث
مكافحة الجرائم المعلوماتية في الولايات المتحدة الأمريكية

يعد القانون الفدرالي لجرائم الحاسب الآلي "Federal Computer Fraude and Abuse Acte " أول مواجهة على المستوى الفدرالي لجرائم الحاسب الالي ، وقد صدر هذا القانون في سنة 1984 وخضع لتعديلات اساسية سنة 1986 ثم 1994 و 1996 ، وتضمن سبعة نصوص جوهرية تمثلت في تجريم الدخول غير المصرح به الى الحاسب الالي ونظامه ، و التي وردت ضمن نصوص المواد (A1-1030) إلى(A4- 1030)، كما تم تجريم اتلاف الحاسب الالي ونظامه ومايحتوي عليه من معلومات في المادة (A5- 1030) .

أما الحصول غير المشروع على الشفرات الخاصة بالدخول الى نظام الحاسب الآلي فقد جرمت ضمن المادة (A6- 1030) ، ونصت المادة (A7- 1030) على تجريم الابتزاز المعلوماتي ، حيث تم تحديد العقوبة بناءا على عدة اعتبارات تتعلق بوجود نية عند المتهم بتحقيق الربح المادي وكذا بمدى جسامة الضرر اللاحق بالضحية وكذا وجود ظرف العود عند المتهم من عدمه [1].

وتعد قضية الولايات المتحدة الأمريكية ضد الطالب الامريكي "موريس Morris " التي اشرنا إليها في معرض حديثنا عن جريمة الاتلاف المعلوماتي مثالا على حرص المشرع الامريكي على اكتمال بنيته التشريعية لمكافحة الجريمة المعلوماتية [2].

فقد ظهر الفراغ التشريعي فيما يتعلق باستخدام البرامج الخبيثة في تعطيل اجهزة الحاسب الالي ، وعدم تطابق السلوك الاجرامي للطالب موريس مع نص المادة (A- 1030) المتعلقة بمعاقبة الدخول العمدي غير المصرح به ، كما أن نيته لم تتجه إلى اعاقة الأنظة المعلوماتية ، لذلك عند تعديل المادة السابقة بصدور " قانون حماية بنية المعلومات القومية " The NII Protection Act" لسنة 1996 ، فقد صارت تنص على تجريم تعديل المعلومات و البرامج و الشفرات و الاوامر داخل نظام الحاسب الالي ، مما يترتب عليه اضرار تلحق بالحاسب الآلي متى كان احداث الضرر عمدا ، كما جرمت المادة الدخول العمدي وغير المصرح به إلى حاسب آلي يتمتع بالحماية متى ترتب على ذلك اضرار، على الرغم من توقع الجاني وكيفت الفعل على أنه جناية في الحالتين، أما في حالة وقوع الاتلاف نتيجة للاهمال والخطأ فيكون الفعل جنحة .

وفيما يتعلق بالاحتيال الذي يتم بناءا على الدخول المصرح به و بالخصوص في حالات استعمال البطاقات الممغنطة فان المشرع الامريكي قد تناول ذلك من خلال المادة (A– 1029) من القانون الفدرالي لسنة 1984 التي جرمت استعمال بطاقات مسروقة أو منتهية الصلاحية أو المزورة مع العلم بذلك و أضيف إليها في تعديل سنة 1994 حيازة الأجهزة المساعدة على تزوير البطاقات الائتمانية.[3]

وقد تم تجريم الاحتيال المعلوماتي من خلال المادة (A4- 1030) التي تعاقب على الدخول غير المصرح به عمدا إلى حاسب مشمول بالحماية إذا كان الحصول على منفعة مادية هو الغرض من هذا الدخول ، و اعتبر وقت الحاسب الآلي و الذي يقدر بأكثر من خمسة آلاف دولار أمريكي من قبيل المنفعة المالية .

---

(1) Conley (John M) & Bryan (Robert M) , Op.cit., p. 38.

(2) Marion (Camille Cardoni), Computer viruses and the law , Dckinson low review, vol.93,1989. p.92.

(3) Vergutch (pascal) , Op.cit.,p 103,104,159.

كما أقرت الفقرة الخامسة من المادة السابقة أن الأشخاص المسموح لهم بالدخول إلى النظام لا تتقرر مسؤوليتهم عن أعمال الاتلاف إلا إذا كانت عمدا ، في حين يكون الأشخاص غير المصرح لهم بالدخول مسؤولين عن أعمال الاتلاف في جميع الحالات. [1]

وقد أقرت وزارة العدل الأمريكية سنة 2000 تصنيفا جديدا لجرائم الكمبيوتر، يشمل الأفعال التالية [2]:

- السطو على بيانات الكمبيوتر
- الاتجار بكلمة السر
- حقوق الطبع (البرامج و الأفلام و التسجيلات الصوتية) وعمليات الهاكرز أو القرصنة
- سرقة الأسرار التجارية باستخدام الكمبيوتر
- تزوير الماركات التجارية باستخدام الكمبيوتر
- تزوير العملة باستخدام الكمبيوتر
- الصور الجنسية الفاضحة و استغلال الأطفال
- الاحتيال بواسطة شبكة الانترنت
- تهديدات القنابل بواسطة شبكة الانترنت
- الاتجار بالأسلحة النارية و المتفجرات والمخدرات و غسيل الأموال عبر شبكة الانترنت

وفي سنة 1986 اصدرالمشرع الأمريكي قانونا عاما لمواجهة جرائم الكمبيوتر تحت رقم (474-99-100) ورقمه التشريعي 1213/ 1986 ، حيث أورد فيه جميع المصطلحات الضرورية لاستيفاء الشروط التي يفرضها الدستور الأمريكي لتطبيق القانون على الجرائم المعلوماتية ، وصدر استنادا عليه قوانين ولايتي تكساس و الينوى الخاصة بجرائم الكمبيوتر[3] .

---

[1] Senate Report N° 104-357 th Congress, 2nd Session, Detailled Discussion of The NII Protection Act, 1996.

[2] ممدوح عبد الحميد عبد المطلب، المرجع السابق ، ص 5.

[3] ممدوح عبد الحميد عبد المطلب ، المرجع نفسه ، ص 6.

المطلب الثاني

الإطار القانوني لمكافحة الجرائم المعلوماتية في الدول العربية

على غرار الدول الغربية التي نصت تشريعاتها على مكافحة الجريمة المعلوماتية ، قامت بعض الدول العربية بتطوير ببنيتها التشريعية لمواكبة قوانين الدول السباقة في هذا المجال، وإلتزاما منها بالمعاهدات الدولية التي انظمت إليها ، وعلى هذا الأساس ظهرت بعض التجارب القليلة في الدول العربية مما يبين التباين الحاصل بينها فيما يتعلق بنظرتها إلى خطورة الإجرام المعلوماتي ، وربما يرجع السبب إلى اختلاف الدول العربية في اعتمادها على استخدام الحاسب الآلي و الأنترنت وغيرها من تكنولوجيات المعلومات و الاتصالات ، ففي حين نجد دولا مثل الامارات العربية المتحدة و العربية السعودية من الدول الرائدة في التشريع لمكافحة هذا النوع المستجد من الجرائم ، توجد دول عربية اخرى لاتزال تبذل جهودا لتكييف قوانينها التقليدية مع الجرائم المعلوماتية ، على الرغم من صدور "القانون العربي الموحد للانترنت" الذي يمكن أخذه كمرجع للتشريعات العربية التي مازالت لم تطور من بنيتها القانونية لردع الجرائم المعلوماتية .

لكن من جهة أخرى وبسبب مساهمة ثورة المعلومات والاتصالات في انتشار التجارة الإلكترونية وظهور العقود الإلكترونية كوسيلة قانونية جديدة حيث انتشرت منذ سنة 1992 استخدام الأنترنت في ابرام الصفقات وعرض المنتجات مما أدى ببعض الدول إلى الاسراع في الاعتراف بهذا الشكل الجديد من التجارة .

ففي الجزائر مثلا أصبح للكتابة في الشكل الإلكتروني والتوقيع الالكتروني مكانا ضمن قواعد الإثبات في القانون المدني الجزائري من خلال نصي المادتين 323 مكررا و 327 فقرة 2 من القانون المدني الجزائري .

كما أن المشرع التونسي في القانون رقم 83- 2000 الخاص بتنظيم التجارة الالكترونية والتوقيع الالكتروني سوى بين المحررات الالكترونية والمحررات الورقية ولكنه قيد ذلك بشروط لتفادي الاستغلال غير المشروع للتوقيع الالكتروني، وأكد على ذلك في الفصل 5 من هذا القانون، وفي الفصل 6 منه.

وعلى الرغم من أن التجارة الالكترونية والتعاقد والتوقيع الالكتروني من بين الأمورالقانونية التي عمد المشرع العربي إلى الاهتمام بها بشكل معقول، إلا أن الجانب الأكثر أهمية الذي أولاه هذا الأخير عناية زائدة هو ما يتصل بمكافحة الجريمة المعلوماتية ، حيث ظهرت في بعض الدول العربية التي واكبت التطور الحاصل في هذا الاجرام قوانين لردع مرتكبي هذه الجرائم ، ومن هذه التشريعات ما يتعلق بمكافحة تهديد أمن الدولة من خلال منع ومحاربة تمويل الإرهاب و الترويج له عبر مواقع الانترنت ، ومنها ما يتعلق بحماية أمن وسلامة النظم المعلوماتية من أخطار التجسس وسرقة المعلومات ، وأخيرا ما يتعلق بالنظام و الآداب العامة وشرف واعتبار الأشخاص.

في هذا المطلب سنتطرق لتجارب كل من الأمارات العربية المتحدة و مصر وتونس في مجال التشريع بخصوص الجرائم المعلوماتية.

الفرع الاول
تجربة الامارات العربية المتحدة في مكافحة الجرائم المعلوماتية

تعد دولة الامارات العربية المتحدة من الدول العربية القليلة و الرائدة في مجال التشريع الخاص بحماية النظم المعلوماتية ، ويعتبر القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم المعلوماتية مثالا على ذلك [1] .

فقد أورد المشرع الاماراتي في هذا القانون جملة من المصطلحات ذات الدلالة القانونية نذكر منها :

- **المعلومات الالكترونية :** وهي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وتشمل الكتابة والصور والصوت والارقام والحروف والرموز و الاشارات وغيرها.

- **البرنامج المعلوماتي :** هو مجموعة من البيانات و التعليمات و الأوامر ، قابلة للتنفيذ بوسائل تقنية المعلومات ومعدة لانجاز مهمة ما.

- **نظام المعلومات الإلكتروني :** هو مجموعة برامج وادوات معدة لمعالجة و ادارة البيانات أو المعلومات أو الرسائل الالكترونية أو غيرذلك.

- **الشبكة المعلوماتية :**

- هو ارتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات وتبادلها.

- **المستند الالكتروني:**

عبارة عن سجل او مستند يتم انشاؤه أو تخزينه أو استخراجه أو نسخه أو ارساله أو ابلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط الكتروني اخر و يكون قابلا للاسترجاع بشكل يمكن فهمه.

- **الموقع:**

- هو مكان اتاحة المعلومات على الشبكة المعلوماتية.

- **وسيلة تقنية المعلومات:**

- أية أداة الكترونية مغناطيسية ، بصرية ،كهروكيميائية، او اية اداة اخرى تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية و يشمل أية قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الاداة.

- **البيانات الحكومية:**

- يشمل ذلك بيانات الحكومة الاتحادية و الحكومات المحلية و الهيئات العامة و المؤسسات العامة الاتحادية و المحلية.

---

[1] عبدالله عبد الكريم عبد الله،المرجع السابق، ص 63 .

وتناول القانون السابق مجموعة من الجرائم المعلوماتية كجريمة اختراق المواقع و الانظمة الإلكترونية أين تم التمييز بين اختراق الأنظمة المعلوماتية دون ترتب نتيجة عن ذلك، و بين الاختراق مع ترتب نتيجة متعلقة بإلغاء أو حذف أو تدمير معلومات ، إذ جعل العقوبة في الحالة الثانية أشد و تقدر بالحبس مدة لاتقل عن ستة اشهر مع الغرامة المالية و في حالة اختراق النظم المعلوماتية و ترتب عن ذلك انتهاك لمعلومات شخصية تكون العقوبة هي الحبس مدة لاتقل عن سنة و الغرامة المالية المقدرة بعشرة الاف درهم .

كما شدد في عقوبة الجرائم السابقة إذا كان مرتكب الجريمة قد قام بالفعل بسبب تاديته لعمله او سهل للغير القيام بذلك.

وعاقبت المادة الرابعة من القانون السابق على تزوير مستندات معترف بها معلوماتيا وكذا على استعمال المستند المزور مع العلم بذلك.

ومن الجرائم التي نص عليها القانون كذلك جريمة تعطيل الوصول إلى البرامج أو الخدمة أو الدخول إلى الأجهزة و كذا العبث بالشبكة المعلوماتية عن طريق ايقافها عن العمل أو تدمير أو مسح أو اتلاف بيانات أو معلومات فيها .

وجرم القانون كذلك العبث بالفحوص الطبية باستخدام الانترنت وكذا القيام بالتنصت أو اعتراض مرسل عن طريق الشبكة المعلوماتية و استخدام الانترنت في الابتزاز أو التهديد حيث حدد عقوبة السجن مدة عشر سنوات إذا كان التهديد بارتكاب جناية أو اسناد أمور خادشة للشرف و الاعتبار.

كما نص القانون على تجريم السرقة و الاحتيال و الاستيلاء على سندات و كذا الحصول دون وجه حق على بيانات البطاقات الإلكترونية ، بالإضافة إلى بعض الأفعال الماسة باعتبار الأشخاص و الآداب العامة و كذا التحريض على الدعارة و المساس بالاديان وهذا ما تؤكده المادة 15 ، و انتهاك الحياة الخاصة التي أكدت عليها المادة 16 بنصها على أنه « كل من اعتدى على أي من المبادئ أو القيم الأسرية أو نشر أخبارا أو وصورا تتصل بحرمة الحياة الخاصة أو العقلية للأفراد، ولو كانت صحيحة عن طريق شبكة المعلومات أو إحدى وسائل تقنية المعلومات يعاقب بالحبس مدة لا تقل عن سنة، وبالغرامة التي لا تقل عن خمسين ألف درهم، أو بإحدى هاتين العقوبتين » .

كما لم يغفل القانون الإتحادي كذلك عن تجريم الاتجار بالبشر و بالمخدرات عبر الانترنت و كذا غسل الاموال و الترويج للأعمال الارهابية و كذا التجسس على المؤسسات الحكومية ، و نصت المادة 20 على تجريم انشاء مواقع أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة يعاقب بالحبس مدة لا تزيد على خمس سنوات.

وقد تعرض القانون السابق لجملة من الانتقادات اثناء حلقة نقاشية نظمها معهد التدريب و الدراسات القضائية بالامارات العربية المتحدة إذ رأى المشاركون اغفال المشرع لبعض الجرائم كالقمار ، و كذا وقوع نصوصه العقابية في تناقضات مختلفة كعدم معاقبة من يحصل على أموال أكبر مما هو موجود في رصيد بطاقته الإلكترونية في حين تم تجريم الوصول إلى بيانات البطاقات الالكترونية باستخدام الانترنت [1] .

---

[1] عبد الله عبد الكريم عبدالله ، المرجع السابق ، هامش الصفحة 79.

الفرع الثاني
تجربة مصر في مكافحة الجرائم المعلوماتية

بعد انعقاد المؤتمر التاسيسي الاول لجمعيات قانون الانترنت بالقاهرة في سبتمبر سنة 2004 و المؤتمر الدولي الأول لقانون الانترنت بمدينة الغردقة في أوت 2005 ، بدأ الاهتمام في مصر بمكافحة الجرائم المعلوماتية وتأسست الجمعية المصرية لمكافحة جرائم المعلوماتية سنة 2005 و هي منظمة غير حكومية تعنى بنشر الوعي و اعداد الدراسات والمؤتمرات حول جرائم المعلوماتية .

وتعتبر حركة التشريع في مجال مكافحة الجرائم المعلوماتية في مصر ضعيفة مقارنة بدولة الامارات العربية المتحدة ولا يزال الاعتماد على النصوص التقليدية بخصوص بعض الجرائم كالتزوير أو الاحتيال أو السرقة أو المساس باعتبار الاشخاص يطبق على بعض الجرائم المعلوماتية .

و يعتبر قانون التوقيع الالكتروني الصادر سنة 2004 [1] أول قانون يصدر بشأن تجريم بعض الأفعال المتعلقة بالنظم المعلوماتية حيث جرم أفعالا تتعلق بالحصول على توقيع أو وسيط أو محرر إلكتروني بدون وجه حق، أو اعتراضه أو تعطيله عن اداء وظيفته ، وقد عرف الوسيط الإلكتروني بأنه " أداة أو أدوات أو أنظمة انشاء التوقيع الإلكتروني" فهو نظام معلوماتي يساعد على انشاء التوقيع الإلكتروني و اصدار المحررات الاليكترونية.

الفرع الثالث
تجربة تونس في مكافحة الجرائم المعلوماتية

يعد القانون التونسي المتعلق بالتجارة الاليكترونية رقم 83 لسنة 2000 الخاص بالمبادلات الالكترونية والمؤرخ في 9 أوت 2000، و الذي بين احكاما خاصة بالمبادلات التجارية الاليكترونية أول تشريع يتعرض للجرائم المعلوماتية .

ومما جاء فيه ما نصت عليه المادة 48 بخصوص افشاء أسرار تتعلق بالشفرة الخاصة بالتوقيع الإلكتروني و يتم ذلك عن طريق اختراق منظومة معلوماتية و فك رموز الشفرة أو كلمة السر و نشرها أو استعمالها بدون وجه حق ، حيث عاقبت المادة 48 على هذا الفعل بالحبس مدة تتروح بين ستة اشهر الى سنتين وغرامة مالية بين الف و عشرة الالف دينار تونسي .

أما المادة 50 فقد جرمت وعاقبت استغلال ضعف أو جهل شخص أو باستعمال الحيل في اطار عمليات البيع الإلكتروني بدفعه لابرم إلتزام أو تعهدات .

كما عاقبت المادة 52 من نفس القانون ، مزودي خدمات المصادقة الإلكترونية عندما يقومون بافشاء المعلومات التي عهدت اليهم في اطار نشاطهم مع استثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الاعلام بها [2] .

---

[1] عبد الفتاح بيومي حجازي ،التوقيع الاليكتروني في النظم القانونية المقارنة ، دار الفكر الجامعي، الاسكندرية، 2005، ص 556.

[2] عبد الله عبد الكريم عبدالله ، المرجع السابق، ص 85.

وتعتمد السلطات التونسية تشريعات متشددة فيما يخص استعمال شبكة الانترنت ، اذ تجبر كل مستعمل للشبكة أن يقوم بالتعريف عن هويته الحقيقية معتمدة في ذلك على برامج تمكنها من مراقبة كل مستعمل و معرفة المواقع التي يزورها ، ومن أهم القوانين التي أصدرها المشرع التونسي قانون عدد 38-98 بتاريخ 2 جوان 1998 الذي ينص على مراقبة البريد الالكتروني وامكانية مصادرة أي رسالة من شأنها المساس بالنظام و الامن العموميين. كما أصدر بتاريخ 10 ديسمبر 2003 القانون رقم 75-2003 المتعلق بمكافحة الارهاب ومنع تبييض الاموال. [1]

المطلب الثالث

الاطار القانوني لمكافحة الجرائم المعلوماتية على المستوى الدولي

اكتسبت جرائم المعلوماتية طابعا دوليا باعتبارها من الجرائم العابرة للحدود ، غير أنه لا يمكن اعتبارها من صنف الجرائم الدولية التي تدخل في اطار اختصاصات المحكمة الجنائية الدولية التي أسس نظامها في روما سنة 1998 ، فجرائم المعلوماتية يعاقب عليها من خلال التشريعات الوطنية فالسلوك الاجرامي فيها يتم على المستوى الداخلي غير أن التطور المذهل في وسائل الاتصال أعطى لهذه الجرائم بعدا دوليا ، فهي جرائم داخلية قد ترتكب على مستوى عالمي. [2]

وقد تم بذل العديد من الجهود الدولية سواء على مستوى الامم المتحدة او المنظمات الاقليمية لمكافحة الجرائم المعلوماتية نذكر منها :

- تقرير منظمة التعاون الاقتصادي و التنمية لسنة (1986)
- توصية مجلس اوروبا بشان الجرائم المتعلقة بالكمبيوتر (سبتمبر 1989)
- مؤتمر الامم المتحدة الثامن لمنع الجريمة و معاملة السجناء (هافانا- 1990)
- المؤتمر السادس للجمعية المصرية للقانون الجنائي حول جرائم الكمبيوتر (القاهرة- 1993)
- المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات (ريودي جانيرو- 1994)
- اتفاقية بودابست لمكافحة الجرائم المعلوماتية (بودابست - 2001)

سوف نتطرق في هذا المطلب لأبرز الجهود الدولية المبذولة لمكافحة الجرائم المعلوماتية من خلال التعرض لاهم القرارات الدولية الصادرة بهذا الخصوص.

---

(1) Loi n° 2003-75 du 10 Décembre 2003 relative au soutien des efforts internationaux de lutte contre le terrorisme et a la répression du blanchiment d'argent , La législation du secteur de la sécurité en Tunisie à l'adresse : http://www.legislation-securite.tn/ar/node/29195.

(2) عمر الفاروق الحسيني ، المرجع السابق ، ص 138.

الفرع الأول

القرار الصادر عن الامم المتحدة بشأن جرائم الكمبيوتر(هافانا 1990)

بعد انعقاد مؤتمر الامم المتحدة السابع لمنع الجريمة و معاملة المجرمين في مدينة ميلانو الايطالية سنة 1985 و الذي كان قد اشار الى مشكلة الجريمة المعلوماتية و مكافحتها و متابعة مرتكبيها ، انبثقت عنه مجموعة من التوجيهات منها تكليف لجنة الخبراء العشرين لدى منظمة الامم المتحدة بدراسة موضوع حماية نظم المعلومات و الاعتداء على الحاسب الالي ، و التي أقرت جملة من المقترحات و التوصيات ، وبعد انعقاد المؤتمر الثامن لمكافحة الجريمة و معاملة المجرمين في شهر اوت سنة 1990 بهافانا العاصمة الكوبية ، تبنى مقترحات و توصيات و مبادىء أجازها مؤتمر هافانا [1] .

وتتلخص توصيات مؤتمر هافانا 1990 فيما يلي [2]:

1- التاكيد على أن وضع اطار قانوني دولي يتطلب بذل جميع الدول الاعضاء جهدا جماعيا.

2- الطلب من الدول الاعضاء أن تكثف من جهودها في سبيل مكافحة عمليات اساءة استخدام الكمبيوتر وإذا دعت الضرورة اتخاذ جملة من التدابير التالية :

أ- تحديث القوانين و أغراضها الجنائية بما في ذلك التدابير المؤسسية ، من أجل :

1- ضمان أن تطبق الجزاءات والقوانين الراهنة، بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم وإدخال تغييرات مناسبة إذا دعت الضرورة إلى ذلك.

2- وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة..للتصدي إلى هذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي.

3- مصادرة أو رد الأصول بصورة غير مشروعة والناجمة عن ارتكاب جرائم ذات صلة بالحاسوب

ب- تحسين تدابير امن الحاسب الالي مع مراعاة حماية الخصوصية و احترام حقوق الانسان و حرياته الاساسية.

ج اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة تنفيذ القوانين بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحاسب الآلي.

د- اعتماد تدابير مناسبة لتدريب القضاة و المسؤولين عن منع الجريمة الاقتصادية و الجرائم المتعلقة بالحاسب الالي و التحري و الادعاء فيها .

ه- الاهتمام بوضع قواعد للاداب المتبعة في استخدام جهاز الحاسب الالي.

و- اعتماد سياسات تعالج المشكلات المتعلقة بضحايا جرائم الحاسب الالي.

---

[1] محمد الامين البشري و محسن عبد الحميد احمد ، معايير الامم المتحدة في مجال العدال الجنائية و منع الجريمة ، الطبعة الاولى ، اكاديمية نايف للعلوم الامنية ، الرياض ، 1998 ، ص 19 .

[2] يونس عرب، جرائم الكمبيوتر و الانترنت، الطبعة الاولى ، منشورات اتحاد المصارف العربية ، بيروت ، 2002 ، ص 314.

الفرع الثاني

القرارات الصادرة عن المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر (ريودي جانيرو 1994)

أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات ، الذي انعقد في ريودي جانيرو بالبرازيل في 4 اكتوبر من سنة 1994 ، و الذي تمت خلاله مناقشة جرائم الحاسب الالي، بأن تتضمن قائمة الحد الادنى من الأفعال المشكلة لجرائم الحاسب الالي و المتعين تجريمها، و التي يمكن ذكرها على النحو التالي [1] :

1- الاحتيال أو الغش المرتبط بالكمبيوتر :- ويشمل الإدخال والإتلاف والمحو لمعطيات الكمبيوتر أو برامجه ، أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى إلحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير .

2- تزوير الكمبيوتر أو التزوير المعلوماتي :- ويشمل إدخال أو إتلاف أو محو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد فيما لو ارتكبت بغير هذه الطرق ، من قبيل أفعال التزوير المنصوص عليها في القانون الوطني .

3- الأضرار بالبيانات والبرامج (الإتلاف) :- وتشمل المحو والإتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه.

4- تخريب وإتلاف الكمبيوتر:- وتشمل الإدخال أو المحو أو الإتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات (الشبكات).

5- الدخول غير المصرح به :- وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن .

6- الاعتراض غير المصرح به:- وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات.

وقد وضع القرار الصادر عن المؤتمر بعض القواعد الاجرائية لمكافحة هذه الجرائم كوجوب تحديد السلطات المؤهلة بتفتيش و ضبط الادلة في بيئة معلوماتية و السماح لها باعتراض المراسلات وكذا ضرورة ان يكون هناك قدر من التعاون بين الضحايا و الشهود و مستخدمي هذه التكنولوجيا لاتاحة استخدام المعلومات في المتابعة القضائية .

كما اكد القرار على ضرورة وضع بعين الاعتبار كل المسائل المتعلقة بانتهاك حرمة الحياة الخاصة و التجسس و المخاطر الخسائر الاقتصادية اثناء عمليات التفتيش و ضبط الادلة .كما اشار القرار الى تكييف التشريع و الاجراءات القضائية مع طبيعة الادلة الالكترونية .

---

[1] محمد الالفي ، المسؤولية الجنائية عن الجرائم الاخلاقية عبر الانترنت، الكتب المصري الحديث للنشر ، القاهرة ، 2005، ص 176 .

الفرع الثالث
اتفاقية بودابست لمكافحة جرائم المعلوماتية و الأنترنت (بودابست 2001)

لعب المجلس الأوروبي دورا مهما في مكافحة الجرائم المعلوماتية ، وصدر عنه العديد من التوصيات لحماية تدفق المعلومات ، ففي سنة 1981 وقع المجلس الاوروبي اتفاقية تتعلق بحماية الاشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية ، و في افريل من سنة 2000 تقدمت اللجنة الاوروبية لمشكلات الحاسب الالي (CDPC) بمشروع اتفاقية جرائم المعلوماتية و التي تم المصادقة عليها في بودابست بالمجر سنة 2001. [1]

وتتكون الاتفاقية من مقدمة و أربعة فصول ، حيث تم استعراض أهداف الاتفاقية و مرجعياتها السابقة و بعض التدابير التشريعية الإقليمية و الدولية المتعلقة بجرائم المعلوماتية ، كما ثمنت المقدمة التعاون الدولي في هذا المجال ، و أكدت مقدمة الاتفاقية على أهمية ما اتم انجازه من قبل الأمم المتحدة و منظمة التعاون الاقتصادي و التنمية و الاتحاد الاوروبي و مجموعة الدول الصناعية (مجموعة الثمانية).

وجاء الفصل الاول للاتفاقية لتعريف المصطلحات التي تضمنتها الاتفاقية من خلال نص المادة الأولى التي عرفت المنظومة المعلوماتية بأنها « أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين » ، و عرفت المعطيات المعلوماتية بأنها « أي عمليات عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها ».

وفي الفصل الثاني الذي جاء تحت عنوان الاجراءات المتعين اتخاذها على المستوى الوطني تضمن ثلاثة اقسام ، يضم القسم الأول منها المواد من المادة 2 الى المادة 13 و يعالج النصوص الموضوعية للجرائم المعلوماتية و التي جاءت في خمسة طوائف على النحو التالي :

طائفة الجرائم التي تستهدف أمن المعلومات و سريتها و سلامتها وتوفرمعطيات المنظومة المعلوماتية وتشمل:

- جريمة الدخول غير القانوني(Accès illégal)
- جريمة الاعتراض غير القانوني (Interception illégale)
- جريمة التدخل في المعطيات (Atteinte à l'intégrité des données)
- جريمة التدخل على منظومة الحاسب (Atteinte à l'intégrité du système)
- جريمة اساءة استخدام الاجهزة (Abus de dispositifs)

---

(1) Convention sur la cybercriminalité, Budapest, 2001 à l'adresse : http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

و ضمت الطائفة الثانية الجرائم المرتبطة بالحاسب الالي (Infractions informatiques) و تشمل :

التزوير المعلوماتي (Falsification informatique) الذي نصت عليه المادة السابعة و يكون بادخال أو تعديل أو حذف أو إخفاء لمعطيات معلوماتية مما ينتج عنه ظهور معطيات غير شرعية لتكون معتبرة قانونا وكأنها معطيات شرعية وبغض النظر عما إذا كانت هذه المعطيات مقروءة أو غير مقروءة ويحق اشتراط نية أو قصد الغش لقيام المسؤولية الجنائية .

- الاحتيال المعلوماتي (Fraude informatique) نصت عليه المادة الثامنة وهو القيام بادخال أو حذف أو تعديل أو التعدي على عمليات المنظومة المعلوماتية بنية الحصول على منفعة اقتصادية لنفسه أو لغيره .

وجاء في الطائفة الثالثة الجرائم المرتبطة بالمحتوى ، وخصت بالذكر جرائم دعارة الاطفال دون غيرها من جرائم المحتوى، حيث أوجبت على الدول الموقعة على الاتفاقية تجريم عرض أو توزيع أو نقل أو اتاحة مواد اباحية للأطفال من خلال نظام الكمبيوتر.

وضمن الطائفة الرابعة تم النص على الجرائم المرتبطة بحقوق المؤلف و الملكية الفكرية لمحاربة القرصنة المعلوماتية ، حيث ألزمت على الدول وجوب اتخاذ تدابير تشريعية تجرم الاعتداء على حق المؤلف وفقا للقوانين الوطنية للدول الموقعة على الاتفاقية و اتفاقية الويبو لحق المؤلف و اتفاقية تربس و اتفاقية بيرن لحماية المصنفات الأدبية و الفنية بخصوص اعمال القرصنة التي ترتكب باستخدام نظام الكمبيوتر .

و نصت الطائفة الخامسة على أحكام المساهمة و الشروع والمسؤولية الجزائية للأشخاص المعنوية ، حيث أوجبت المعاقبة على الشروع في هذه الجرائم المعلوماتية وكذلك معاقبة المساهم في ارتكابها ، كما أوجبت معاقبة الاشخاص المعنوية الذين ترتكب الجريمة لمصلحتهم من طرف الشخص الطبيعي الذي يتصرف لمصلحته استنادا إلى تمثيل قانوني أو باعتباره مناطا به اتخاذ القرار عن الشخص القانوني أ أو لأنه خاضع لسلطته ، كما نصت علىمسؤولية الأشخاص الطبيعية و المعنوية عن غياب أو تخلف الرقابة و الإشراف و التحكم بتصرفات الأشخاص الطبيعيين .

ونصت المادة 13 على معايير اتخاذ العقوبة حيث أوجبت الإتفاقية على الدول الأعضاء فيها إقرار عقوبات سالبة للحرية بالنسبة للأشخاص الطبيعيين و غرامات مالية بالنسبة للأشخاص المعنوية .

أما المواد من 14 الى 21 فقد عرضت القواعد الاجرائية حيث نظمت أحكام التفتيش و مصادرة معلومات الحاسب الالي المخزنة و التي تفيد التحقيق في حين نصت المادة 22 على أحكام الاختصاص المحلي.

وجاء ضمن الفصل الثالث من الاتفاقية و ضمن المواد من 23 الى المادة 35 المبادئ العامة و النصوص الخاصة للتعاون الدولي في مجال التحقيق و تبادل المعلومات و تقديم المساعدة و تسليم المتهمين و وجوب التعاون لاتخاذ الاجراءات و التشريعات اللازمة لتحقيق التعاون ما بين الدول الموقعة عليها.

واخيرا تضمنت الاتفاقية أحكاما ختامية ضمن الفصل الرابع تشمل المواد من 36 الى المادة 48 والتي نصت على كيفية دخول المعاهدة حيز التنفيذ و كذا امكانية الانضمام للمعاهدة بالنسبة للدول غير الأعضاء في المجلس الاوروبي والذين لم يشاركوا في اعدادها.

ويلاحظ ان الاتفاقية قد سعت الى تحقيق وحدة التدابير التشريعية بين الدول الاوروبية و الدول المصادقة عليها من غير الدول الاوروبية .

الفصل الثالث

مكافحة الجريمة المعلوماتية في التشريع الجزائري و الحلول المقترحة لمواجهة تحديات الإجرام المعلوماتي

عرفت الجزائر تطورات وتغيرات في العديد من المجالات الحياتية على غرار دول العالم نتيجة لما افرزته ثورة المعلومات ، حيث صارت تكنولوجيات الاعلام و الاتصال تفرض نفسها على عادات و سلوكيات الأفراد، مما حتم على المشرع الجزائري القيام باعادة النظر في المنظومة التشريعية لمواجهة الانماط الجديدة من الإجرام ، وعلى الرغم من أن المشرع الجزائري قد استحدث نصوصا تهيأ لما ستفرضه البيئة الإلكترونية من تحديات تتعلق أساسا بمدى قدرة السلطات على مسايرة هذه التطورات المتلاحقة ، إلا أننا نعيب على المشرع الجزائري عدم طرحه لهذه النصوص بصفة منتظمة ومتوازنة ، فقد أصدر القانون رقم 04- 15 الخاص بجرائم المساس بأنظمة المعالجة الآلية للمعطيات في 10 نوفمبر 2004 [1] لينتظر حتى سنة 2009 ليصدر القانون رقم 09- 04 الذي نص على القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها [2] ، على الرغم من تناول هذا القانون الأخير لشرح مصطلحات وردت في القانون السابق استدراكا لذلك ، كما أنه أصدر القانون رقم 10-05 المتعلق بالاثبات بالكتابة الالكترونية [3] المعدل للقانون المدني في المادتين 323 مكرر323 مكرر 1 و المادة 327 الصادر بتاريخ 20 جوان 2005 إلا انه لم ينظم التجارة الإلكترونية على غرار المشرع التونسي كما انه لم يضع أحكاما توضح كيفية اثبات هوية الموقع إلكترونيا مما يحتم على المشرع الجزائري تدارك هذا الفراغ التشريعي.

ولو ان المشرع الجزائري قد استدرك جوانبا من التشريع في مجال الجريمة المعلوماتية وأغفل أخرى ، إلا أن هذا لا يمنعنا من القول أن التشريع الجزائري قد خطى خطوات عملاقة لمواكبة التشريعات الدولية بهذا الصدد.

سنحاول في هذا الفصل تناول أهم ما جاء به المشرع الجزائري من قواعد اجرائية و موضوعية لغرض التصدي للجريمة المعلوماتية ، حيث نتناول في المبحث الأول القواعد الاجرائية الخاصة لمتابعة الجريمة المعلوماتية و كذا مراحل اثباتها مع تبيين أهم الصعوبات التي تواجه المحققين خلال مراحل البحث عن الأدلة الجنائية في هذا النوع من الجرائم ، على أن نتطرق في المبحث الثاني لدراسة التطور التشريعي في الجزائر لمكافحة الاجرام المعلوماتي حيث نستعرض أهم ما نص عليه القانون المتعلق بالمساس بنظام المعالجة الالية للمعطيات وكذا القانون المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الاعلام و الاتصال ، أما المبحث الثالث فسوف نخصصه لاستعراض الحلول الكفيلة بمواجهة التحديات التي تفرضها الجريمة المعلوماتية.

---

[1] القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر66 /156 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات،ج.ر عدد 71 ، ص 11-12.

[2] القانون رقم 09-04 مؤرخ في 5 أوت 2009 المتضمن اللقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها، ج .ر عدد 47 ، ص 5.

[3] المواد 44- 46 من القانون رقم 05-10 مؤرخ في 20 جوان 2005 المعدل و المتمم للأمر75-58 المؤرخ في 26 سبتمبر 1997 المتضمن القانون المدني،ج.ر عدد 44، ص 17.

المبحث الاول

القواعد الإجرائية في متابعة و إثبات الجريمة المعلوماتية حسب القانون الجزائري

تعد متابعة الجريمة المعلوماتية من أهم التحديات التي تواجه رجال الضبطية القضائية بالنظر إلى طبيعة الجرائم المعلوماتية الخاصة من حيث أنها تتعلق بمحل غير مادي بالإضافة إلى صعوبة دور الشرطة و مختلف الاجهزة الامنية في مراقبتها ومنع حدوثها وكذا التحري عن مرتكبيها.

ولأن متابعة الجريمة المعلوماتية تفرض على المحقق أن يتمتع بمهارات تخص التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود ، والأهم من ذلك هو معرفة المحقق لأساسيات عمل الحاسب الآلي و مبادئ عمل شبكة الأنترنت ، فإن دراسة كل هذه الجوانب يمكننا من ايجاد الحلول المناسبة لتجاوز المعيقات التي تقف في وجه رجال الشرطة أثناء مراحل جمع الادلة واثبات الجريمة المعلوماتية .

سنتطرق في هذا المبحث لاهم القواعد الاجرائية التي جاء بها المشرع الجزائري لمواجهة هذه الانماط المستجدة من الجرائم ، حيث نخصص المطلب الأول لقواعد الاختصاص النوعي و المحلي اما في المطلب الثاني فسوف نتطرق فيه لبعض الاجراءات الخاصة بمتابعة الجريمة المعلوماتية على ان نتناول مراحل اثباتها و الصعوبات التي تعترض مراحل البحث عن الادلة في المطلب الثالث.

المطلب الاول

قواعد الاختصاص النوعي و المحلي في الجريمة المعلوماتية حسب القانون الجزائري

إدراكا من المشرع الجزائري لخصوصية الجريمة المعلوماتية وطبيعتها المعقدة ، ولغرض التحكم أكثر في معالجة الأنواع المستحدثة من الإجرام ، ورغبة منه في ضمان فعالية وسرعة الفصل في القضايا ذات الطبيعة الخاصة مثل الجريمة المنظمة العابرة للحدود الوطنية ، وجريمة الارهاب وتبييض الاموال والجرائم الماسة بانظمة المعالجة الالية للمعطيات ، و الجرائم المتعلقة بالتشريع الخاص بالصرف ، والتي تتطلب تخصصا و تكوينا خاصا لمختلف الجهات القضائية من نيابة وقضاة تحقيق وقضاة حكم لمتابعة هذه الجرائم ، فقد تم انشاء جهات قضائية موسعة الاختصاص أو ما يعرف بالاقطاب القضائية المتخصصة .
بالإضافة إلى ذلك فقد نظم المشرع الجزائري جانب التعاون الدولي و المساعدة القضائية التي تلعب دورا كبيرا في جمع الادلة في الجريمة المعلوماتية فهاته الجرائم غالبا ما ترتكب من قبل شخص أجنبي وفي إقليم أجنبي مما يؤكد حتمية التعاون الدولي حتى تتسنى متابعة هذه الجرائم بفعالية أكبر .
سنتناول فيما يلي أحكام الإختصاص النوعي و المحلي التي جاء بها القانون رقم رقم 04- 14 ونوضح كيف يمتد إختصاص وكيل الجمهورية وقاضي التحقيق إلى دائرة إختصاص محكام أخرى

الفرع الاول
الاختصاص النوعي في الجريمة المعلوماتية

يتحدد الاختصاص النوعي للمحكمة للفصل في القضية المعروضة عليها تبعا لنوع الجريمة التي تنظر فيها ، حيث تختص محكمة الجنايات في الفصل في الجنايات و الجرائم الموصوفة بأفعال ارهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري ، كما تختص المحاكم في النظر في الجنح و المخالفات فيما عدا الاستثناءات المنصوص عليه في قوانين خاصة حسب المادة 328 من قانون الاجراءات الجزائية الجزائري .

ولأن الطبيعة التقنية المعقدة للجرائم المعلوماتية تفرض على رجال القضاء أن يخضعوا لتكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع الجزائري مع بعض انواع الجرائم المتعلقة بالمتاجرة بالمخدرات و الجريمة المنظمة عبر الحدود الوطنية و جرائم تبييض الاموال و الارهاب ، و الجرائم المتعلقة بالتشريع الخاص بالصرف باجراءات خاصة اذ جعل الاختصاص ينعقد الى دائرة اختصاص محاكم اخرى وهذا ما نصت عليه المواد 37 ، 40، و المادة 329 من قانون الاجراءات الجزائية الجزائري اثر التعديل الذي جاء به القانون رقم 04- 14 المؤرخ في 10 نوفمبر 2004 و الذي حددت احكامه في المرسوم التنفيذي رقم 06- 348 والمتعلق بالتنظيم القضائي حيث نص على انشاء اقطاب قضائية متخصصة ذات إختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة، قسنطينة، وهران، وورقلة. [1]

الفرع الثاني
الاختصاص المحلي في الجريمة المعلوماتية

من المتعارف عليه أن الاختصاص المحلي يتحدد طبقا لضوابط ثلاث هي مكان وقوع الجريمة أو مكان إقامة المتهم أو مكان ضبطه حسب نص المادة 37 من قانون الاجراءات الجزائية الجزائري و التي عدلت بموجب القانون رقم 04/ 14 .

كما نصت أحكام المرسوم التنفيذي رقم 06- 348 المؤرخ في 5 اكتوبر سنة 2006 على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق إلى دائرة اختصاص محاكم أخرى ، ويتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة وكذا محكمة قسنطينة ومحكمة و ورقلة ومحكمة وهران . [2]

وفي نطاق الجرائم المعلوماتية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان اخر ، فان الاختصاص ينعقد لمكان السلوك أو مكان تحقق النتيجة، و تعد الجريمة المعلوماتية اذا تمت عن طريق شبكة الانترنت جريمة مستمرة حيث تعتبر انها ارتكبت في جميع الاماكن التي امتدت الجريمة فيها . [3]

---

[1] القانون رقم 04- 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر66 /155 المتضمن قانون الاجراءات الجزائية، ج. رعدد71، ص 4.

[2] المرسوم التنفيذي رقم 06 -348 المؤرخ في 5 اكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق، ج رعدد 63، ص 29 .

[3] جميل عبد الباقي الصغير ، المرجع السابق ، ص 63 .

و متى كانت الجريمة المعلوماتية ،أيا كان نوعها ، فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيات الاعلام و الاتصال اذا ارتكبت خارج الاقليم الوطني ، أواذا كان مرتكبها اجنبيا وتستهدف مؤسسات الدولة الجزائرية او الدفاع الوطني او المصالح الاقتصادية الاستراتيجية للدولة وذلك في إطار التعاون الدولي [1].

المطلب الثاني
قواعد المتابعة الخاصة حسب القانون الجزائري

كان لتطور اساليب ارتكاب الجريمة المعلوماتية واخذها منحى تصاعديا بين الجرائم المرتكبة في الجزائر أن فرض على المشرع الجزائري الاعتماد على قواعد اجرائية خاصة في سبيل مكافحة الجريمة المعلوماتية ، وهو ما جاء به القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم للامر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن لقانون الاجراءات الجزائية [2] ، حيث نص على اجراءات خاصة تهدف إلى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و بعض الجرائم الأخرى ، وتتمثل هذه الاجراءات في اعتراض المراسلات وتسجيل الاصوات والتقاط الصور و التسرب ، التي نتطرق لها تباعا في الفرع الاول و الثاني.

الفرع الاول
اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

أتاح المشرع الجزائري حسب نص المادة 65 مكرر 5 من قانون الاجراءات الجزائية الجزائري لضابط الشرطة القضائية القيام ببعض الأعمال إذا ما دعت إلى ذلك مقتضيات البحث والتحري والتحقيق الابتدائي في الجرائم المتلبس بها وكذاجرائم المخدرات او الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الجرائم الموصوفة بأفعال الإرهاب أو التخريب أو الجرائم المتعلقة بالتشريع الخاص بالصرف أو جرائم الفساد ، حيث أجاز لوكيل الجمهورية أن يأمر ضابط الشرطة القضائية باعتراض المراسلات التي تجري عن طريق وسائل الاتصال السلكية واللاسلكية، ووضع الترتيبات التقنية اللازمة لالتقاط الصور وتسجيل المكالمات السرية وبدون موافقة المعني وذلك في الأماكن العامة والخاصة ، كما يسمح الإذن المسلم من قبل وكيل المهورية بالدخول إلى المحلات السكنية أو غيرها و لو خارج المواعيد المحددة في المادة 47 من قانون الاجراءات الجزائية ، ويكون تنفيذ هذه العمليات تحت إشراف ورقابة وكيل الجمهورية في مرحلة البحث والتحري ، أما في مرحلة التحقيق الابتدائي فتكون تحت إشراف قاضي التحقيق الذي أمر بها.

---

[1] قانون رقم 09-04 مؤرخ في 5 وات 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها، ج ر عدد 47 ، المادة 15.

[2] القانون رقم 06-22 ، مرجع سبق ذكره ، المادة 65 مكرر 5 إلى 65 مكرر 18.

الفرع الثاني

التسرب

المقصود بالتسرب حسب نص المادة 65 مكرر 12 من قانون الاجراءات الجزائية الجزائري هو قيام ضابط أو عون الشرطة القضائية بمراقبة الأشخاص المشتبه في أنهم ارتكبوا الجريمة بإيهامهم أنه مساهم معهم أو شريك بحيث يستعمل الضابط أو العون هوية مستعارة و ذلك اذا ما اقتضى البحث و التحري في واحدة من الجرائم التالية :
جرائم المخدرات او الجريمة المنظمة عبر الحدود الوطنية او الجرائم الماسة بأنظمة المعالجة الالية للمعطيات او جرائم تبييض الأموال او الجرائم الموصوفة بأفعال الإرهاب أو التخريب او الجرائم المتعلقة بالتشريع الخاص بالصرف او جرائم الفساد .

وقد نظم المشرع الجزائري احكام التسرب في الفصل الخامس من قانون الاجراءات الجزائية من المادة 65 مكرر 11 الى المادة 65 مكرر 18 حيث بين فيها كيفية القيام بعملية التسرب وكذا شروط الاذن بالقيام بهذا الاجراء و كذلك الاحكام الجزائية لمن تسبب في كشف هوية الضابط او العون المتسرب حيث نص على عقوبة الحبس من سنتين الى خمس سنوات و غرامة من 50.000 دج الى 200.000 دج وتشدد العقوبة في حالة ما أدى الكشف عن هوية الضابط المتسرب إلى أضرار بالضابط المتسرب أو احد اقاربه المباشرين. ويتم الاستماع الى الضابط المتسرب بوصفه شاهدا عن الجرائم المرتكبة بعد انتهاء المهلة المحددة في رخصة التسرب.

المطلب الثالث

مراحل اثبات الجريمة المعلوماتية والصعوبات التي تواجهها

يعتبر موضوع إثبات الجريمة المعلوماتية من الموضوعات النادرة من حيث التطبيق القضائي ، وذلك بسبب صعوبة جمع الأدلة فيها كما أن هذه النوعية من الجرائم توجد في بيئة تعتمد التعاملات فيها على نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب وهذه البيانات التي يمكن استخدامها كأدلة ضد المجرم المعلوماتي ، يمكن في أقل من الثانية العبث بها أو محوها بالكامل لذلك فإن الصدفة تلعب دورا في اكتشاف الجرائم المعلوماتية أكثر من الدور الذى تلعبه أساليب المراقبة والمتابعة.

و الإجراءات التي تهدف إلى جمع الأدلة في جرائم المعلوماتية كثيرة، منها الانتقال ومعاينة مسرح الجريمة و التفتيش و ضبط الادلة و سماع الشهود و الاستجواب و المواجهة و الخبرة ، وليس على المحقق الإلتزام بإتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم اساسا لمباشرتها جميعا وانما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقضي به المصلحة وما تسمح به هذه الظروف . [1]

---

[1] عمر السعيد رمضان، مبادئ قانون الاجراءات الجنائية، الجزء الاول، دار النهضة العربية ، القاهرة ، ص 3.

ويعد ايجاد الدليل الذي تثبت به الجريمة المعلوماتية من أهم التحديات لمواجهة الجريمة المعلوماتية حيث تبدو قواعد الإجراءات الجزائية التقليدية عاجزة عن مواجهة العديد من الأفعال التي تهدد المصالح الاجتماعية والاقتصادية و التي ارتبطت بظهور وانتشار جهاز الحاسب الآلى وشبكة الانترنت [1].

في هذا المطلب سنتطرق للاجراءات المتبعة لاثبات الجريمة المعلوماتية ثم نبين الصعوبات التي تعترض رجال الضبطية القضائية و القضاة أثناء مراحل البحث عن الادلة ، على أن نتناول اخيرا مفهوم الدليل الرقمي وحجيته .

الفرع الاول
مراحل اثبات الجريمة المعلوماتية

أولا) الانتقال ومعاينة مسرح الجريمة المعلوماتية :

تعرف المعاينة عند فقهاء القانون الجنائي بأنها « رؤية بالعين لمكان أو شخص او شيء لاثبات حالة وضبط كل ما يلزم لكشف الحقيقة ».[2]
وتعرف كذلك بانها « اثبات لحالة الأماكن و الأشخاص و كل ما يفيد في كشف الحقيقة » [3].

و يتطلب هذا الإجراء انتقال ضابط الشرطة القضائية إلى مكان ارتكاب الجريمة وذلك لاثبات حالة مكان ارتكاب الجريمة و حالة الاشياء و الموجودة التي قد تساعد في كشف الحقيقة وذلك قبل أن تمحى آثار ارتكاب الجريمة.

و قد نصت المادة 42 من قانون الاجراءات الجزائية الجزائري على وجوبية انتقال ضابط الشرطة القضائية فورا إلى مكان وقوع الجناية للقيام بالمعاينات ، وجاء في نص المادة أنه « يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس ان يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل الى مكان الجناية ويتخذ جميع التحريات اللازمة. كما نصت المادة نفسها على ضرورة سهر ضابط الشرطة القضائية على المحافظة على الاثار التي يخشى ان تختفي ، وكذا على ضرورة ضبطه لكل ما يمكن ان يؤدي الى اظهار الحقيقة ».[4]

كما نصت المادة 64 الفقرة 3 على جواز قيام ضابط الشرطة القضائية القيام بالمعاينة في أي وقت واي مكان إذا تعلق الامر بواحدة من الجرائم المذكورة في المادة 47 ومنها جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

---

[1] غنام محمد غنام ، المرجع السابق ، ص 10.

[2] محمد زكي ابو عامر ، الاجراءات الجنائية،دار منشاة المعارف،الاسكندرية،الطبعة الثانية ،(د.ت)، ص 222.

[3] ابراهيم حامد طنطاوي ، سلطات مأمور الضبط القضائي، مطبعة دار التأليف ، القاهرة ، 1991 ،ص288.

[4] الامر رقم 66-156 الصادر بتاريخ 8 يونيو 1966 المتضمن لقانون الاجراءات الجزائية الجزائري، ج.رعدد48 ، المادة 42 ، ص 622.

ونظرا إلى خصوصية الجرائم المعلوماتية من جهة الصعوبة التي تتعلق بطبيعة الدليل ، كما سنوضح ذلك لاحقا ، فإن المعاينة في هذا النوع من الجرائم تقتضي القيام ببعض القواعد و الارشادات الفنية التي يمكن أن نذكر منها مايلي [1] :

أ) - القيام بتصوير الحاسب الالي و ملحقاته و مختلف التوصيلات المرتبطة به.

ب) - ملاحظة طريقة اعداد نظام الحاسب الالي و برامج تشغيله و نوع نظام المعالجة الالية للمعلومات وما إذا كان الحاسب الالي معزول أو متصل بشبكة الانترنت.

ج)- المحافظة على البيانات المخزنة وذلك حتى لا تتعرض للاتلاف اثر وجود مجال مغناطيسي او نتيجة لعدم معرفة كيفية التعامل مع مثل هذه المواد المعلوماتية .

د) - حفظ المستندات الخاصة بالادخال و كذا بالمخرجات مع الاخذ بعين الاعتبار آثار البصمات التي قد توجد على الأدلة المادية المرتبطة بها ، ومن بينها الاقراص الممغنطة و أقراص الليزر وحتى المطبوعة على اوراق بطبيعة الحال.

ه)- ضرورة توفر قدر من الخبرة الفنية في مجال الحاسب الالي على ضباط و أعوان الشرطة القضائية القائمون بعملية المعاينة .

ثانيا) التفتيش في الجريمة المعلوماتية :

يعرف التفتيش بأنه " اجراء من اجراءات التحقيق يقوم به موظف مختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم". [2]

وقد اجاز القانون الجزائري لضابط الشرطة القضائية تفتيش مساكن المشتبه فيهم بشروط تحت طائلة البطلان ، نصت عليها المادة 44 من قانون الاجراءات الجزائية الجزائري ، تتمثل في الحصول على إذن من وكيل الجمهورية أو قاضي التحقيق مع استظهار هذا الاذن قبل الشروع في عملية التفتيش ولا يختلف الامر بالنسبة للتفتيش في احد الجرائم التي نصت عليها المادة 37 من نفس القانون ومن بينها الجرائم الماسة بانظمة المعالجة الالية للمعطيات ، وقد اعفى المشرع الضابط القائم بعملية التفتيش من ضرورة حضوره مع صاحب المسكن أو مع ممثل له وهذا إذا تعلق الامر بجريمة المساس بانظمة المعالجة الالية للمعطيات حسب ما ورد في نص المادة 45 من قانون الاجراءات الجزائية الجزائري .

أما عن ميقات التفتيش فقد أعطى المشرع الجزائري، وفق المادة 47 من نفس القانون، كامل الصلاحية لضابط الشرطة القضائية في اجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني و في كل ساعة من ساعات الليل او النهار وذلك بناءا على اذن مسبق من وكيل الجمهورية ، وذلك عندما يتعلق الامر بجريمة المساس بانظمة المعالجة الالية للمعطيات .

---

[1] عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر و الانترنت،دار الفكر الجامعي ، الاسكندرية 2006، ص 183.

[2] ابراهيم حامد طنطاوي ، المرجع السابق، ص 743.

والتفتيش في مجال الجريمة المعلوماتية يخضع لمعيارمدى قابلية مكونات الحاسب الآلي " المادية Hard Ware " ومكوناته غير المادية أو "المنطقية Soft Ware" ، بالإضافة إلى شبكات الإتصالات التي يكون مرتبطا بها في غالب الأحيان إلى التفتيش [1].

فأما التفتيش المنصب على المكونات المادية المتثملة في جهاز الحاسب الآلي وملحقاته بالاضافة إلى المطبوعات و المذكرات و المراسلات فإنه لا يثير أية إشكال نظرا للطبيعة المادية لهذه المكونات.
في حين أن امتداد التفتيش إلى المكونات غير المادية كالبيانات فإن جانبا من الفقه رأى أن عملية التفتيش يجب أن تمتد إلى البيانات المخزنة في ذاكرة الحاسب الآلي بما أن الغاية من عملية التفتيش هي ضبط الادلة .

واستند هؤلاء في رايهم إلى بعض النصوص الاجرائية كقانون الاجراءات الجزائية اليوناني الذي اشار في المادة 251 منه إلى سلطة جهات التحقيق في القيام بـ"أي شيء" يتيح جمع الادلة ، مما يفسر بامتداد التفتيش إلى المكونات غير المادية للحاسب الالي. [2]

أما الجانب المقابل من الفقه فقد رأى بعدم امكانية امتداد التفتيش الذي غايته هي ضبط الأدلة المادية إلى ضبط الأدلة غير المادية، حيث يقترح أصحاب هذا الرأي ضرورة تعديل النصوص الإجرائية بإضافة امكانية البحث و ضبط بيانات الحاسب الآلي وأية مادة معالجة بواسطته [3].

وفي هذا الاتجاه سارالمشرع الامريكي حيث تم تعديل المادة 34 من قانون الاجراءات الجنائية سنة 1970 بحيث صار بالامكان تفتيش اجهزة الحاسب الالي و الكشف عن الوسائط الالكترونية بما في ذلك البريد الالكتروني و البريد الصوتي والبريد المنقول بجهاز الفاكس [4].

أما المشرع الجزائري فقد نص في القانون رقم 09/ 04 المؤرخ في 5 أوت 2009 و المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها وفي المادة 05 منه على جوازقيام السلطات القضائية المختصة وكذا ضباط الشرطة القضائية بالدخول بغرض التفتيش إلى منظومة معلوماتية أو منظومة تخزين معلوماتية و إلى كافة المعطيات المخزنة فيها ،كما يمكن القيام بذلك عن طريق التفتيش في مكان ارتكاب الجريمة او عن بعد ، وهذا ماسنتناوله في المطالب اللاحقة.

و تخضع شبكات الإتصال للتفتيش وذلك حسب الاحتمالات التي افترضها الفقهاء و المتمثلة في كون الحاسب الآلي متصل بنهاية طرفية مع جهاز آخر داخل نفس الدولة ، و بالتالي يمكن أن يمتد التفتيش إلى البيانات التي توجد في الحاسب الآخر، وقد سبق النص على ذلك في التشريع الألماني حسب القسم 103 من قانون الاجراءات الجزائية الالماني [5] ، و تسمح بعض التشريعات اللجوء الى التصنت ومراقبة و اعتراض الاتصالات فالقانون الفرنسي الصادر في 10 يوليو سنة 1991 اجاز " إعتراض الإتصالات البعدية Telematique " بما في ذلك شبكات تبادل المعلومات [6].

---

[1] عبد الله حسين محمود،سرقة المعلومات المخزنة في الحاسب الالي ، دار النهضة العربية، القاهرة ، ص372 .

[2] هلالي عبد الله، تفتيش نظام الحاسب الالي وضمانات المتهم المعلوماتي، دار النهضة العربية،القاهرة، 1997، ص 82.

[3] هلالي عبد الله ،المرجع نفسه، ص 84.

[4] عبد الله حسين محمود ، المرجع السابق، ص373.

[5] عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتروالانترنت، المرجع السابق، ص 381.

[6] عبد الله حسين محمود، المرجع نفسه ، ص376.

و أجاز المشرع الجزائري لضابط الشرطة القضائية و تحت اشراف وكيل الجمهورية القيام باعتراض المراسلات التي تجري عن طريق وسائل الاتصال السلكية واللاسلكية وهذا حسب ماورد في نص المادة 65 مكرر 5 من قانون الاجراءات الجزائية الجزائري . وقد يمتد التفتيش إلى حاسب الي موجود في دولة اخرى حسب الاتفاقيات المبرمة بين الدول وفق مبدا التعاون و المساعدة القضائية الدولية حسبما نصت عليه اتفاقية المجلس الاوروبي بخصوص الجرائم المعلوماتية .

كما أجاز المشرع الجزائري قبول طلبات المساعدة القضائية مع وضعه لقيود لعدم المساس بالسيادة الوطنية وكذا الحفاظ على سرية المعلومات المبلغة وهذا وفقا لماورد في المواد من 15 الى 18 من القانون رقم 09- 04 والتي نصت على القواعد المتعلقة بالتعاون الدولي و الاختصاص القضائي وكذا تنظيم المساعدة القضائية الدولية و تبادل المعلومات وهذا ما سنتطرق اليه خلال دراستنا لمضمون القانون رقم 09- 04 في المبحث الثاني .

ثالثا) ضبط الأدلة في الجريمة المعلوماتية :

ان الغرض من القيام بعملية التفتيش هو ضبط الاشياء التي يحتمل انها استعملت في ارتكاب الجريمة ، وهو من اعمال الضبطية القضائية حسب نص المادة 12 من قانون الاجراءات الجزائية الجزائري، وعلى ضابط الشرطة القضائية ان يحرر محضرا بالشياء المضبوطة ويرسله الى وكيل الجمهورية ، واذا كانت الجريمة متلبس بها فان ضابط الشرطة القضائية ملزم بالمحافظة على اثار الجريمة التي يخشى ان تختفي ، ويقوم بوضعها في كيس و يختم عليه بختمه ، كما يقوم بعرض الاشياء المضبوطة على الاشخاص المشتبه فيهم للتعرف عليها ، مثلما نصت على ذلك المواد 42، 45،و المادة 47 مكرر من قانون الاجراءات الجزائية الجزائري.

وقد يكون الدليل المادي عبارة عن مستند او محرر مكتوب اومطبوع او منسوخ او مصور او مسجل بحيث يكون مناسبا لاثبات الواقعة [1] .

وكانت عملية ضبط الادلة في الجريمة المعلوماتية تثير عدة اشكالات فيما يخص البيانات و المعلومات المجردة من الطابع المادي لها كالدعامة اوالوسيط الحامل لها، وسبق ان تطرقنا لوجهات نظر الفقهاء بهذا الخصوص عند حديثنا عن عملية تفتيش المنظومة المعلوماتية .
فبعض الفقهاء رأوا عدم صلاحية البيانات والمعلومات لان تكون ادلة مادية يمكن ضبطها مجردة من دعامتها المادية ، الا ان اتجاه اخرارى ان البيانات و المعلومات رغم كونها مجردة من الدعامة المادية فانه لا يوجد ما يمنع من صلاحيتها لان تكون محلا للضبط [2].

وللتوفيق بين وجهتي النظر السابقتين ظهر اتجاه ثالث راى بعدم جدوى تطويع النصوص التقليدية و تطبيقها على البيانات و المعلومات المخزنة اليا و اقترح تدخل المشرع لتوسيع نطاق الاشياء الممكن ضبطها مع ضرورة اعداد ضباط الشرطة القضائية وتكوينهم في كيفية التعامل مع ادلة من هذا النوع.

---

[1] رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة، دار النهضة العربية، القاهرة، 1997، ص 10.

[2] عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتروالانترنت، المرجع السابق ، ص218..

ويقترح أصحاب هذا الاتجاه بعض الحلول بهذا الصدد [1] :

- ضرورة انشاء اقسام متخصصة بمدارس الشرطة للتدريب على كيفية التعامل مع هذا النوع من الادلة لتفادي اتلافها.
- تشجيع المجني عليهم في جرائم المعلوماتية على الابلاغ عن هذه الجرائم.
- منح سلطة التحقيق الصلاحية القانونية لاختراق نظام الحاسب و ضبط ما يحتويه من بيانات مخزنة .

- ضرورة اتباع الطرق الفنية في ضبط الدعامة المادية التي تحوي البيانات مع ضرورة نسخها للمحافظة على المعلومات ، كما يوصى بحمايتها من درجة الحرارة المرتفعة و من الرطوبة و من المجال المغناطيسي إلى غير ذلك من الارشادات التقنية في التعامل مع هذه الادلة.

وتتعدد الأدلة المادية التي لها قيمتها الخاصة في اثبات الجريمة المعلوماتية و التي يجوز ضبطها ونسبتها إلى المجرم المعلوماتي ، ومن أهم هذه الادلة :

1) جهاز الحاسب الآلي وملحقاته:

كما سبق وأن وضحنا عند التطرق لتعريف الجريمةالمعلوماتية ، فإن وجود الحاسب الآلي مهم وأساسي لإرتكاب الجريمة ، ولكل جهاز خصائص معينة من سرعة و قدرة على التخزين .

ويتكون الحاسب الالي من " وحدة المعالجة المركزية Unité Centrale " ، " لوحة المفاتيح Clavier " و " الشاشة Ecran " . وتظهر اضافات جديدة للحاسب الالي بصفة متسارعة حيث ظهر المودم والماوس والسماعات والسيرفر او الخادم ، اما الاجهزة الكبيرة فانها تتغير بإستمرار خاصة من حيث الحجم والهيكل ومن المفيد في مرحلة التحقيق ان يكون المشرف على التحقيق مطلعا على مختلف أشكال اجهزة الحاسب الآلي فور ظهورها.

ومن ملحقات الحاسب الالي ايضا التي يمكن اعتبارها ادلة اثبات نذكر منها [2] :

- **المودم** Modem :

المودم demodulator/ Modulator وهو الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال مع بعضها البعض عبر خطوط الهاتف وقد تطورت المودم إلى أجهزة إرسال الفاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.

- **الطابعات** Printers :

تقوم الطابعات باخراج المعلومات و البيانات مطبوعة على اوراق ، وتختلف في دقتها ومواصفتها من طابعة الى اخرى كما تعتبر بطاقات الإئتمان والمواد البلاستيكية المستعملة في إعداد تلك البطاقات قرائن للاثبات في جرائم الحاسب الآلي.

---

[1] عفيفي كامل عفيفي،جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة و القانون ، منشورات الحلبي الحقوقية، 2003 ، ص359.

[2] عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتروالانترنت ، المرجع السابق ،ص396.

2) الأوراق :

على الرغم من قلة استخدام الأوراق في الجرائم المعلوماتية ، إلا أننا نجد أن العديد من الجناة يقومون بطباعة المعلومات على الورق لذلك تعتبر الأوراق من الأدلة التي ينبغي الإهتمام بها كدليل على الجريمة المعلوماتية.

وهنا نجد أن هذه الأوراق قد تكون عبارة عن [1] :

- أ) أوراق تحضيرية يتم اعدادها يدويا كمسودة لتصوير العملية التي يتم برمجتها.
- ب) أوراق تالفة تطبع للتأكد ثم ترمى في سلة المهملات.
- ج) أوراق اصلية يتم الاحتفاظ بها لاغراض الجريمة.
- د) أوراق اساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات بحيث تكون لها علاقة بالجريمة وغالبا ما تكون تحمل بيانات تم تزويرها أو التلاعب بها بواسطة الحاسب الآلي.

رابعا) سماع الشهود في الجريمة المعلوماتية :

الشهادة كدليل في الدعوى الجزائية لها اهميتها البالغة ، اذ تمكن من كشف العمل غير المشروع الذي يجتهد المجرم المعلوماتي في اخفائه ، فسماع الشهود من الأمور المألوفة في الجرائم التقليدية ، إذ يمكن لرجال الضبطية القضائية سماع أقوال الأشخاص الحاضرين وقت ارتكاب الجريمة، حيث أن المشتبه فيه أو من تواجد في مكان ارتكاب الجريمة يكون مدفوعا إلى الإدلاء بأقواله أمام ضابط الشرطة القضائية لما لهذا الاخير من سلطة تخول له احتجاز الأشخاص الذين يرى فيهم ضرورة التحقيق معهم.

وقد أجاز المشرع الجزائري لضابط الشرطة القضائية منع أي شخص من مبارحة مكان الجريمة ريثما ينتهي من تحرياته حسب نص المادة 50 من قانون الاجراءات الجزائية الجزائري.

و اثارت مسألة التزام الشاهد المعلوماتي بتقديم ما يعلمه من معلومات جوهرية عدة اراء، اذ يرى البعض ضرورة ان يلتزم الشاهد بالإفصاح عن ما يعرفه من كلمات المرور السرية ، أو شفرات البرامج ، ويمثل هذا الاتجاه جزء من فقهاء القانون الفرنسيين، وذلك اعمالا بالمواد 62، 109، 138 من قانون الاجراءات الجزائية الفرنسي ، مع أن عدم الافصاح عن هذه المعلومات لا يضع الشاهد تحت طائلة العقاب الا في مرحلة التحقيق و المحاكمة [2] .

أما الإتجاه الاخر ويمثله جزء من فقهاء القانون في ألمانيا فيرى أنه لا يدخل ضمن إلتزامات الشاهد الإفصاح عن الشفرات و كلمات المرور المختلفة وفقا لما تمليه التزامات الشهادة في الجرائم التقليدية .

ويختلف مفهوم الشاهد في الجريمة المعلوماتية عنه في الجرائم التقليدية ، وذلك للإعتبارات التقنية المميزة للجريمة المعلوماتية ، فالشاهد هو صاحب الخبرة و التخصص في تقنية الحاسب الالي بحيث تكون لديه معلومات اساسية عن الدخول الى الحاسب المراد البحث فيه عن ادلة للجريمة ، ولهذا يطلق عليه مصطلح

---

[1] محمد الامين البشري،المرجع السابق ،ص17.

[1] عبد الله حسن محمود،المرجع السابق،ص 390 .

الشاهد المعلوماتي ، ويشمل عدة فئات أهمها [1]:

أ- القائم على تشغيل الحاسب الآلي Computer Operator:
وهو الشخص المسؤول عن تشغيل جهاز الحاسب الالي وملحقاته ، وتكون لديه خبرة في تشغيل الجهاز وإستخدام لوحة المفاتيح في ادخال البيانات كما يجب أن تكون لديه معلومات المحدودة عن قواعد كتابة البرامج.

ب - المبرمجون Programmers :
وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تصنيفهم إلى فئتين [2] **:**

الفئة الأولى: مخططو برامج التطبيقات Application programers :
يقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقومون بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات.

الفئة الثانية : مخططو برامج النظم System programmers :
يقومون بإختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية أي أنهم يقومون بالوظائف الخاصة بتجهيز الحاسب بالبرامج والاجزاء الداخلية التي تتحكم في وحدات الادخال والاخراج ووسائط التخزين بالاضافة إلى ادخال اي تعديلات أو اضافات لهذه البرامج.

ج- المحللون Analyst :
المحلل وهو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة ومن ثم استنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات.

د- مهندسو الصيانة والإتصالات:
وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

ه- مديرو النظم :
وهم الذين يوكل لهم أعمال الأدراة في النظم المعلوماتية [3].

خامسا) الخبرة في الجريمة المعلوماتية:

تكتسي عملية ندب الخبير خلال التحقيق في جرائم المعلوماتية أهمية بالغة ، وذلك للطبيعة الفنية والتقنية الدقيقة الذي تتميز به ادوات ارتكاب الجريمة المعلوماتية وكذلك لتنوع الاجهزة في هذا المجال وسرعة تطورها ، وندب الخبير من سلطات المحقق وليس هناك في القانون ما يلزم المحقق بذلك ، ويحدد المحقق للخبير المهمة التي كلف بها و ميعاد تسليمه لتقريره ، كما يجب عليه ان يؤدي اليمين القانونية بهذا الخصوص.

---

[1] عبد الله حسن محمود،المرجع السابق ، ص 386.

[2] عبد الله حسن محمود،المرجع نفسه ، ص 389.

[3] هلالي عبد الله، المرجع السابق ، ص 25.

والمستندات المتحصل عليه خلال عملية التفتيش لا يحتاج المحقق فيها لمساعدة من قبل الخبراء وهذه المستندات تتمثل في : سجلات إدارة الكمبيوتر، وثائق البرامج، السجلات، البيانات المطبوعة ، ويتم التخطيط على هذه المستندات ويمكن تحديد ما إذا كانت كاملة، أصلية، أو صورا من خلال استجواب القائمين على حفظها.

أما الأدلة الأخرى فيكون فحصها أكثر تعقيدا مثل :

الأشرطة الممغنطة الأسطوانات، البرامج وتتطلب استعانة المحقق باحد الخبراء حتى يتمكن من الالمام بمحتوياتها.
وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي [1] :

أ)- تركيب الحاسب الالي وصناعته ونوعه ونوع نظام نشغيله وأهم الأنظمة الفرعية التي يستخدمها بالأضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير.... الخ.

ب)- طبيعة بيئة الحاسب أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الإتصالات وتردد موجات البث وأمكنة اختزانها.

ج)- الموضع المحتمل لأدلة الأثبات والشكل أو الهيئة التي تكون عليها.

د)- أثر التحقيق من الوجهة الإقتصادية والمالية على المشاركين في إستخدام النظام.

ه)- كيف يمكن عند الإقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو الحاق ضرر بالأجهزة.

و)- كيف يمكن عند الإقتضاء نقل أدلة الإثباتات إلى أوعية ملائمة بغير ان يلحقها تلف.

ي)- كيفية تجسيد الأدلة في صورة مادية بنقلها إذا امكن إلى اوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع اثبات ان المسطور على الورق مطابق للمسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة.

---

[1] هشام محمد فريد رستم،المرجع السابق، ص 41.

الفرع الثاني
الصعوبات المواجهة لاثبات الجريمة المعلوماتية

تعترض المحققين في جرائم المعلوماتية من رجال الضبطية القضائية و رجال القضاء جملة من الصعوبات أثناء قيامهم بالبحث و التحري وجمع أدلة إثبات الجريمة المعلوماتية ، وتختلف أسباب هذه الصعوبات فمنها ما يرجع إلى طبيعة الدليل غير المادية في الجرائم المعلوماتية ،ومنها مايرجع إلى صعوبة المتابعة بالنظر إلى خصوصية الجريمة المعلوماتية وما تثيره من اشكالات سوف نتطرق اليها فيما يلي :

أولا) صعوبات تتعلق بطبيعة الدليل في الجريمة المعلوماتية

الدليل الجنائي في الجرائم المعلوماتية له طبيعة خاصة ، فهو ذو طابع فني في غاية الدقة، فضلا عن ذلك فيتميز بصعوبة استخلاصه اذ يتطلب مهارة في التحكم بالتقنية العالية للحاسب الالي . ويمكننا أن نذكر أهم الصعوبات المتعلقة بطبيعة الدليل والتي تعترض المحقق اثناء تحريه عن الجريمة المعلوماتية ، وذلك على النحو التالي :

أ - الطبيعة الخاصة للدليل في الجرائم المعلوماتية :

فهو ليس بدليل مرئي يمكن فهمه بمجرد القراءة، ويتمثل – حسب ما تتيحه النظم المعلوماتية من أدلة على الجرائم التي تقع عليها أو بواسطتها - في بيانات غير مرئية لا تفصح عن شخصية معينة عادة.

وتظهر هذه المشكلة بصفة خاصة بالنسبة لجرائم الانترنت مثل:

الجرائم التي ترتكز على البريد الإلكتروني في ارتكابها ، حيث يكون من الصعب على جهات التحري تحديد مصدر المرسل ، ويسهل ارتكاب جرائم الاعتداء على النظم المعلوماتية بسبب هذه الطبيعة غير المرئية لدليل الجريمة ، و الأمثلة كثيرة بهذا الخصوص، ومنها قيام أحد المبرمجين بمركز حاسبات إحدى الشركات الألمانية باعداد برنامج في حاسب الشركة يتيح له ادخال بيانات مرتبات أشخاص وهميين إلى ذاكرة الحاسب وتحويل هذه المرتبات الى حساب خاص له ، وحتى لا تتم طباعة هذه البيانات على الأوراق ، فقد أجرى الجاني تعديلا على البرنامج يمنع امكانية طباعة هذه البيانات الوهمية في كشف الرواتب عند مراجعتها، كما نجح في اقتطاع الاموال التي تحصل عليها من حساب اجمالي الضرائب بحيث لا تظهر هذه الأموال في حسابات الشركة و لا يمكن ادراك وجود عجز في ميزانيتها ، وبعد اكتشاف أمره صدفة بعد استيلائه على مبلغ 193.000 مارك، حكم عليه بالحبس سنتين بتهمة الاحتيال واساءة الائتمان. [1]

ب- صعوبة الوصول إلى الدليل:

حيث تقوم الشركات الكبرى و المواقع العالمية المعروفة على الانترنت بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية لمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها أو نسخها، و يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه وذلك من خلال استخدامه كلمات مرور بعد تخريب الموقع مثلا ، أو استخدامه تقنيات التشفير.

---

[1] هشام محمد فريد رستم، المرجع السابق، هامش ص26.

ج- سهولة محو الدليل:

فالجاني يستطيع أن يتوجه إلى أي "مقهى الانترنت " عام او خاص والدخول على أحد المواقع وإرسال رسالة على البريد الإلكتروني لآخر تحوي عبارات سب وقذف او تحرض على العنف او غيرها ، ثم يقوم بمحو الدليل وإعادة كل شيء كما كان عليه وبالتالي فقدان كل اثر ممكن لتتبع الجاني.

د- أدلة الإدانة ذات نوعية مختلفة فهي معنوية الطبيعة :

تتنوع الأدلة المعلوماتية من حيث طبيعتها مثل سجلات الحاسب الالي ومعلومات الدخول والاشتراك والنفاذ والبرمجيات ، ولذا فهذه الأدلة تثير أمام القضاء مشكلات عديدة ؛ ولاسيما فيما يتصل بمدى قبولها وحجيتها والمعايير اللازمة لذلك.

ه- الضخامة البالغة لكم البيانات المتعين فحصها:

تحتوي الانظمة المعلوماتية على كم هائل من البيانات و المعلومات ، بحيث أن طباعة هذه المعلومات على الورق يتطلب مئات الالاف من الصفحات، اما حجز البيانات الالكترونية فلا يقلل من صعوبة البحث عن الدليل الرقمي ، فضخامة حجم هذه البيانات يجعل من مهمة الاطلاع عليها بصفة كلية امرا مستحيلا مما يجعل من الاستعانة بالخبرة الفنية لتحديد ما يجب ضبطه امر لا مناص منه ، اذ لا بد من الاستعانة بما تتيحه التكنولوجيا الحديثة في نظم المعالجة الالية للمعطيات في مجال فحص و التدقيق في هذه المعطيات التي تحتوي على دليل الجريمة او كما يعرف بالدليل الرقمي .

ثانيا) صعوبات تتعلق بمتابعة الجريمة المعلوماتية [1] :

فضلا عن الصعوبات التي تواجه المحققين بسبب طبيعة الدليل الجنائي في الجريمة المعلوماتية ، فهناك صعوبات تتعلق بمتابعة الجريمة في حد ذاتها، ومن بين هذه الصعوبات :

أ- إحجام الجهات أوالأشخاص المجني عليهم عن الإبلاغ عن الجرائم المعلوماتية [2] :

حيث تظل الجريمة مجهولة اذا لم يتم الابلاغ عنها فلا تصل الى علم السلطات المختصة ، ويحدث ذلك غالبا بالنسبة للجهات المالية كالمصارف والبنوك ومؤسسات السمسرة ؛ إذ أن مجالس إداراتها – في الغالب الأعم – تفضل كتمان هذه الجرائم تفاديا للآثار السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية تجاهها ؛ إذ قد يؤدي ذلك إلى تضاؤل الثقة فيها من جانب المتعاملين معها.

ب- نقص خبرة سلطات الاستدلال و التحقيق في ضبط ووصف الجريمة المعلوماتية :

اذ يصادف رجال الضبطية القضائية والمحققين والقضاة صعوبات جمة فيما يتعلق بإجراءات ضبط الجرائم المعلوماتية ؛ وإضفاء الوصف القانوني المناسب على الوقائع المتعلقة بهذه الجرائم.

ويرجع ذلك إلى الطبيعة الخاصة لهذه الجرائم . فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

---

[1] عبد الفتاح بيومي حجازي،مبادئ الاجراءات الجنائية في جرائم الكمبيوتر و الانترنت، المرجع السابق،ص 108.

[2] عبد الفتاح بيومي حجازي ، المرجع انفسه ،ص 109.

ج- تصادم التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية :

وذلك لأن هذا لتفتيش يتم – غالباً - على نظم الحاسب الالي وقواعد البيانات وشبكات المعلومات، الأمر الذي قد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة ؛ بسبب االارتباط بين الحواسيب وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول.
ولاشك في أن امتداد التفتيش إلى نظم غير النظام محل الاشتباه قد يمس – في الصميم - حقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

د- فكرة الاختصاص والطبيعة الدولية للجرائم المعلوماتية :

غالبا ما تتم الجرائم المعلوماتية بأفعال ترتكب من قبل أشخاص من خارج الحدود ، كما أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود ، مما يثير التساؤل حول الإختصاص القضائي بهذه الجرائم ؛ علاوة على أن امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود ؛ أمر يحتاج إلى تعاون دولي شامل يستهدف تحقيق مكافحة هذه الجرائم ؛ مع احترام السيادة الوطنية للدول المعنية .

الفرع الثالث
مفهوم الدليل الرقمي ومدى حجيته في القانون الجنائي

يثير الدليل الرقمي اشكاليات تتعلق في طبيعته الخاصة وكيفية الحصول عليه خصوصا و أنه يتطلب خبرة وإلماما كبيرين بتكنولوجيا الحاسب الالي و شبكات الاتصال ، فما هو الدليل الرقمي و ماهي حجته القانونية ومدى اعتماد القضاة عليه خلال مراحل ومتابعة واثبات الجريمة المعلوماتية ؟

أولا مفهوم الدليل الرقمي [1]:

الدليل الرقمي" Digital Evidence " هو الدليل المأخوذ من جهاز الحاسب الالي ، ويكون في شكل نبضات مغناطيسية أو كهربائية ويمكن تجميعها وتحليلها باستخدام برامج خاصة، فهي مكون رقمي يمكنه ان يقدم المعلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، بحيث يصلح لان يكون دليلا يعتمد عليه امام الجهات القضائية.

وسمي بالدليل الرقمي بسبب أن البيانات داخل نظام الحاسب الالي او في الوسط الافتراضي سواء كتابات او صوراً او رسومات أو نصوص او تسجيلات صوتية او مرئية فانها تأخذ شكل أرقام على هيأة الرقمين (1 أو 0) ثم يتم تحويل هذه الأرقام ومعالجتها لتظهرعند عرضها في شكل صورة أو مستند أو تسجيل [2].

---

[1] عبد الناصر محمد فرغلي ومحمد عبيد المسماري، الاثبات الجنائي بالادلة الرقمية، ، بحث مقدم للمؤتمرالعربي الاول للأدلة الجنائية، اكاديمية نايق للعلوم الامنية ، الرياض ، 2007، ص 11.

[2] طارق محمد الجملي ،الدليل الرقمي في مجال الاثبات الجنائي ، ورقة عمل مقدمة للمؤتمر المغاربي الاول حول المعلوماتية والقانون نظته اكاديمية الدراسات العليا بتاريخ 28 اكتوبر 2009 بطرابلس ، ليبيا ،ص 4.

ويمكن الحصول على هذا الدليل الرقمي في مخرجات الطابعة على الورق مثل التقارير والرسوم وفي أجهزة الكمبيوتر وملحقاتها ، وفي الأقراص المرنة والصلبة وأشرطة تخزين المعلومات وفي أجهزة الاتصال كالمودم والبرامج وأجهزة التصوير مثل الة التصوير الرقمية والمواقع الالكترونية وكذا البريد الإلكتروني.
وتستخدم عدة طرق علمية و تكنولوجية تساهم في جمع الأدلة الرقمية، حيث تعتمد هذه الطرق على برامج تسمح بنسخ الملفات أو إعادة استرجاعها كما تقوم بالتفتيش عن المعلومات و البيانات المراد ضبطها في أي جزء من الحاسب الالي، او تمكن القائم بمهمة البحث و التحري من تشغيل جهاز الحاسب الالي اذا كان محميا بشفرة الدخول.
كما توجد برامج اتصالات تسمح للمحقق بإختراق جهاز الحاسب الالي للجاني ونقل محتوياته المعلوماتية إلى جهازه ، حيث أن كل جهاز حاسب آلي متصل بشبكة الانترنت له رقم خاص أو عنوان يميزه عن باقي الاجهزة المتصلة وهو ما يعرف بـ" بروتوكول IP " وكذلك "بروتوكول TCP " المسؤول عن نقل المعلومات ، وباعتماد الخبرة العلمية يتمكن المحقق من معرفة كل المواقع التي اتصل بها الجاني بالاضافة الى حصوله على كل المعلومات المخزنة في جهاز الحاسب الالي للجاني .[1]

ثانيا - حجية الدليل الرقمي:

حتى يتحقق الدليل اللازم للاثبات فانه لابد من ان تتوفر فيه شروط تجعل له حجية وقيمة يثبت بها الحق اد يجب ان يكون معترفا به و قابلا للمناقشة امام القضاء ، وكما اسلفنا فالدليل الرقمي له من المميزات ما تعطيه الحجية والقدرة على اقناع الخصوم اثناء مناقشة محتوياته ومن خلاله يمكن ترجيح براءة او ادانهة المتهم .

فالدليل الرقمي له اهمية تماثل الدليل المادي وربما تفوقه لما له من مميزات ينفرد بها عن الدليل المادي العادي.
و على الرغم من الصعوبات التي تكلمنا عنها عند تطرقنا لاثبات الجريمة المعلوماتية فانه باعتماد الطرق التكنولوجية الحديثة يمكن الحصول بسهولة على ادلة لاثبات الجريمة .
فمن مميزات هذا الدليل الرقمي انه يمكن نسخه و الحصول على صورة او نسخة مطابقة للديل الاصلي، كما يمكن اعادة استرجاعه اذا ما تم محوه وذلك باعتماد برامج وتكنولوجيا خاصة ، واذا ما تم استرجاعه فانه يمكن معرفة تاريخ محوه من قبل الجاني وبذلك الحصول على دليل اضافي لادانة الجاني . كما يستطيع المحققون ان يتبادلوا فيما بينهم هذه المعلومات و الادلة بشكل سريع وعبر دول العالم ، حيث انه بالامكان نقل كم كبير من المعلومات الت تشكل دليلا جنائيا في دعامة صغيرة الحجم ولكن سعتها التخزينية عالية.

وقد جعلت خصائص الدليل الرقمي التي تكلمنا سابقا من المشرع في بعض الدول وخاصة التي تعتمد نظام الأدلة القانونية أن يعترف بمشروعية الدليل الرقمي في الاثبات الجنائي ،أما الدول التي تعتمد نظام الاثبات الحر فان الاشكال لا يطرح بما ان القاضي يتمتع بحرية مطلقة و وفق اقتناعة الشخصي بالوقائع المعروضة امامه ، وكمثال على اتجاه التشريعات الى النص على مشروعية الدليل الرقمي المشرع البلجيكي الذي عدل من قانون الاجراءات الجنائية بموجب قانون صادر بتاريخ 28 نوفمبر 2000 [2] وذلك باضافة المادة 39 مكرر التي تسمح بضبط الادلة الرقمية ، وعلى غرار المشرع البلجيكي فالمشرع الجزائري جعل من البيانات و المعلومات المحتواة في نظام المعالجة الالية للمعطيات من الادلة التي يجوز حجزها وضبطها مما يثبت حجية الدليل الرقمي في التحقيق الجنائي .

---

[1] انظر في الملحق رقم1: المصطلحات الواردة في هذه الدراسة.

[2] عمرمحمد بن يونس ، مذكرات في الاثبات الجنائي عبر الانترنت- ندوة الدليل الرقمي- القاهرة ، 8 مارس 2006، ص 5.

المبحث الثاني

التطور التشريعي لمكافحة الجريمة المعلوماتية في الجزائر

إن الحديث عن موقع الجزائر من التطورات التشريعية لمواجهة الإجرام المعلوماتي يقودنا إلى ذكر أولى بدايات استعمال الأنترنت في الجزائر التي تعود إلى سنة 1993 عن طريق مركز الابحاث CERIST ، و بعد أن تم تحرير القطاع سنة 1998 ازداد عدد مقدمي خدمة الانترنت و مستعمليها بشكل نسبي مقارنة بدول العالم المتقدم ، إلا أن الوضع الحالي الخاص باستعمال شبكة الانترنت في الجزائر مازال ضعيفا مقارنة بدول الجوار، ففي دراسة احصائية اجرتها احدى المؤسسات المتخصصة ورد فيها أن عدد مستخدمي الانترنت في الجزائر بلغ 1,9 مليون شخص خلال سنة 2005 وأن الجزائر تحتل المرتبة العاشرة افريقيا في هذا المجال وأن نسبة السكان المتصلين بشبكة الانترنت لم يتجاوز 2,4 % حتى نهاية 2005 ، لكن هذه النسب لم تلبث أن شهدت طفرة حيث أظهر التقرير الذي أعدته وكالة الانباء الجزائرية في اكتوبر سنة 2006 أن عدد مستخدمي الأنترنت فاق الثلاثة ملايين شخص ، أما نتائج التقرير العالمي لتكنولوجيا المعلومات لسنة 2010 ، والذي يصدر عن المنتدى الاقتصادي العالمي في دافوس بسويسرا ، ومن خلال مؤشر استخدام التكنولوجيا أو NRI (Networked Readiness Index) ، فقد صنف الجزائر في المراتب الاخيرة من بين 133 دولة من حيث مؤشرات استخدام تكنولوجيا المعلومات في المؤسسات الحكومية و الأسواق والمعاملات التجارية والبنى التحتية ، أو ما يعرف بمصطلح البيئة الإلكترونية ، وكذا جاهزية الدولة والمؤسسات الاقتصادية واستعدادها لاستخدام تكنولوجيا المعلومات ، وجاء تصنيف الجزائر في المراتب الاخيرة كما هو مبين في الجدول التالي :

ترتتيب الجزائر ضمن نتائج التقرير العالمي لتكنولوجيا المعلومات لسنة 2009/ 2010 [1]

الدول	السويد	أمريكا	فرنسا	الامارات العربية المتحدة	تونس	مصر	المغرب	الجزائر	التشاد
مؤشر (NRI)	1	5	18	23	39	70	88	113	133
1.مؤشر البيئة التكنولوجية	1	10	19	24	47	70	75	120	133
2.مؤشر الجاهزية التكنولوجية	4	7	26	5	16	65	106	93	130
3.مؤشر الاستخدام التكنولوجي	3	2	15	30	49	70	87	125	131

[1] التقرير العالمي لتكنولوجيا المعلومات لسنة 2010/2009 - الصادر عن المنتدى الاقتصادي العالمي - دافوس- سويسرا .

غير أن تأخر الجزائر في استخدام تكنولوجيا المعلومات و الأنترنت لم يقف حائلا دون أن تصدر تشريعات تكفل الحماية الجنائية للأنظمة المعلوماتية ، و تحفظ حقوق الأفراد من مخاطر الاستخدام السيئ لتكنولوجيا المعلومات ، حيث أدرك المشرع الجزائري ضرورة عدم الاكتفاء بالنصوص التقليدية كجريمة السرقة ، و النصب وخيانة الأمانة ، وفعل التحطيم العمدي لملك الغير، وكذا تجريم الاعتداء على حقوق المؤلف و الحقوق المجاورة و تجريم التقليد ، وكذا تجريم بعض الأفعال حتى قبل أن تستغل شبكة الانترنت في ارتكابها واستفحالها كانتحال الألقاب و الأسماء و إساءة استعمالها ، و كذا الاعتداء على شرف و اعتبار الأشخاص ، و على حياتهم الخاصة و إفشاء الأسرار، و وانتهاك الآداب و تحريض القصر على الفسق و الدعارة وغيرها من الجرائم المالية كتبييض الأموال و الجريمة المنظمة و الجرائم الماسة بأمن الدولة و الأفعال الموصوفة بجرائم الإرهاب و التخريب .

وبالإضافة الى ذلك فقد ضمن المشرع الجزائري الحماية الجزائية لنظم المعلوماتية من خلال القانون رقم 04/ 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر156/66 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات ، و الذي تم تعزيزه بالقانون القانون رقم 09/ 04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها .

سنحاول في هذا المبحث مناقشة التطور التشريعي لمواجهة الاجرام المعلوماتي في الجزائر، من خلال النصوص التقليدية و كذا نصي القانونين السابقين ، مع تبيين صور الجرائم التي جاء بها كل نص ومدى فاعلية هذه التشريعات في مواجهة الاجرام المعلوماتي في الجزائر .

المطلب الاول

القانون رقم 04 - 15 المتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات

تدارك المشرع الجزائري الفراغ الذي كان موجودا بخصوص تجريم بعض الاعتداءات على النظم المعلوماتية حيث أصدر القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر رقم 156/66 المتضمن لقانون العقوبات [1]، حيث ورد ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث من الامر السابق و ضمن القسم السابع مكرر وتحت عنوان المساس بانظمة المعالجة الالية للمعطيات ، ويشمل المواد من 394 مكرر الى غاية المادة 394 مكرر 7 ، وكان ذلك رغبة من المشرع الجزائري في مواكبة التشريع الدولي بخصوص مكافحة الجريمة المعلوماتية و بالأخص الاتفاقية الأوروبية حول الإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي وتم وضعها للتوقيع بتاريخ 2001/11/23 وتعرف باتفاقية بودابست ، حيث يهدف تجريم المساس بالنظم المعلوماتية إلى حماية المعطيات أو المعلومات وبالتالي تعزيز ثقة المواطن في النظم المعلوماتية وذلك لحماية وتشجيع استعمال الحاسب الالي بما أنه صار معيارا للتقدم الحضاري و النمو الاقتصادي .

الفرع الاول

مفهوم جريمة المساس بانظمة المعالجة الالية للمعطيات وصورها في القانون الجزائري

سوف نتناول مفهوم جريمة المساس بانظمة المعالجة الالية للمعطيات والصور التي جاء بها المشرع الجزائري حسب القانون رقم 04-15 :

أولا - مفهوم جريمة المساس بانظمة المعالجة الالية للمعطيات :

لم يتناول المشرع الجزائري تحديد مفهوم أنظمة المعالجة الآلية للمعطيات إلا أنه ورد ضمن نص المادة 394 مكرر من قانون العقوبات الأفعال التي تشكل مساسا بهذه الانظمة حيث نصت المادة على أنه :« يعاقب بالحبس من ثلاثة اشهر الى سنة وبغرامة من 50000 دينار الى 100000 دينار جزائري كل من يدخل او يبقى عن طريق الغش في كل او جزء من منظومة للمعالجة الالية للمعطيات او يحاول ذلك ».
وتضاعف العقوبة اذا ترتب على ذلك حذف او تغيير لمعطيات المنظومة .
واذا ترتب عن الافعال المذكورة اعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة اشهر الى سنتين و الغرامة من 50000 دينار جزائري الى 150000 دينار جزائري» .

---

[1] القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر66 /156 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات ، ج.ر عدد 71 ، ص 11-12.

ويقابل هذه المواد في قانون العقوبات الفرنسي المواد 323-1 الى 323- 7 التي تناولت جرائم المساس بمنظومة المعالجة الالية للمعطيات ، إلا أن تعريف أنظمة المعالجة الآلية للمعطيات في التشريع الجزائري جاء متأخرا عن نص القانون المتضمن المساس بانظمة المعالجة الالية للمعطيات ، حيث تدارك المشرع ذلك من خلال القانون الذي صدر لاحقا والذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها أين تم تعريف كل من المنظومة المعلوماتية وكذا المعطيات المعلوماتية في المادة الثانية بنفس التعريف الذي ورد في المادة الاولى من اتفاقية بودابست لمكافحة الاجرام المعلوماتي او الاجرام السيبيري كما يسميه البعض ، وذلك بالقول بان المقصود بالمنظومة المعلوماتية هو « اي نظام منفصل أو مجموعة من الانظمة المتصلة ببعضها البعض او المرتبطة ، يقوم واحد منها او اكثر بمعالجة الية للمعطيات تنفيذا لبرنامج معين » .

أما المعطيات المعلوماتية فقد عرفت بانها « عمليات عرض للوقائع او للمعلومات او المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شانها جعل منظومة معلوماتية تؤدي وظيفتها » (*) .

ثانيا - صور و أركان جريمة المساس بانظمة المعالجة الالية للمعطيات :

من خلال نص المادة 394 مكرر والى المادة 394 مكرر 2 يمكننا القول ان جريمة المساس بانظمة المعالجة الالية للمعطيات تأخذ الصور التالية :

الصورة الاولى - الدخول او البقاء في منظومة للمعالجة الالية للمعطيات عن طريق الغش:

(Accès ou le maintien frauduleux dans un système de traitement automatisé des données)

نصت المادة 394 مكرر على هذه الصورة من الاعتداء حيث يتمثل الركن المادي لهذه الصورة في فعلي الدخول او البقاء داخل المنظومة المعلوماتية وان يكون ذلك عن طريق الغش .

أ- فعل الدخول في نظام المعالجة الالية للمعطيات :

تقع الجريمة بمجرد الدخول الاحتيالي في منظومة معلوماتية ويكون ذلك من خلال استعمال شفرة الدخول او مفتاح الدخول لمنظومة معلوماتية بغير وجه حق وبما ان المشرع الجزائري لم يحدد طريقة الدخول فانه يمكننا القول ان الجريمة تقع سواء كانت المنظومة المعلوماتية محمية بشفرة الدخول او غير محمية اذ يكفي ان يكون الدخول عن طريق الغش أي بطريقة احتيالية .

(*) ورد في المادة الاولى من اتفاقية بودابست :

Article 1 – Définitions
Aux fins de la présente Convention,
a - l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;

b - l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;

ب - فعل البقاء في نظام المعالجة الالية للمعطيات :

يكون فعل البقاء المجرم من خلال التواجد داخل المنظومة المعلوماتية بغير وجه حق ، وسواء كان الدخول شرعيا أم لا فإنه يشمل البقاء داخل منظومة معلوماتية اكثر من الوقت المحدد أو المصرح به ، كما يجرم فعل البقاء حتى ولو حصل الدخول بصفة عرضية وكان يتوجب على مرتكب هذا السلوك أن ينسحب بمجرد تجاوزه المدة الشرعية لبقاءه ، فبقاؤه داخل المنظومة المعلوماتية مع علمه بعدم مشروعية ذلك يؤكد النية الاجرامية للفاعل .
ونفس الأمر ينطبق في حالة كون الدخول إلى المنظومة المعلوماتية كان شرعيا ثم تجاوز المدة المشروعة لبقاءه أما إذا كان الدخول غير شرعي فإننا نكون أمام جريمتين مجتمعتين جريمة الدخول وجريمة البقاء في منظومة معالجة آلية للمعطيات أو ما يسمى بالتعدد المادي للجرائم .

وتعد جريمتي الدخول و البقاء في منظومة معالجة آلية للمعطيات من جرائم السلوك البحت ، فالجريمتين تقعان بمجرد ارتكاب فعلي الدخول أو البقاء دون أن يتطلب المشرع نتيجة اجرامية لهذا السلوك [1].

ومن أمثلة هذه الجرائم قيام الشخص بنسخ معلومات أو طباعتها على الرغم من أنه كان يحق له الاطلاع عليها فقط فتتحقق جريمة البقاء في منظومة معلوماتية متى توفرت النية الاجرامية المتمثلة في الحصول على المعلومات بصفة احتيالية .

فهذا التجريم يهدف الى حماية المنظومة المعلوماتية بصفة مباشرة ، و حماية المعطيات أو المعلومات بصفة غير مباشرة، وكذا ينطبق القول على الموظف الذي يبقى في منظومة معلوماتية لمدة تتجاوز المدة المسموح له بها ، وهو ما يعرف في بعض التشريعات بسرقة الخدمات أو الاستعمال غير المصرح به لنظام الحاسب الالي [2].

و نص المشرع الجزائري في المادة 394 مكرر فقرة 2 و 3 على صورة مشددة من جريمتي الدخول و البقاء في المنظومة المعلوماتية حيث ضاعف من العقوبة المقررة لها وذلك إذا ترتب عن السلوك الاجرامي حذف أو تغيير لمعطيات المنظومة وكذا في حالة تخريب نظام اشتغال المنظومة المعلوماتية .

الصورة الثانية - المساس بمنظومة المعالجة الالية للمعطيات :

(Atteintes au système informatique)

نصت المادة 394 مكرر 1 على انه « يعاقب بالحبس من ستة اشهر الى ثلاث سنوات وبغرامة من 500.000 دينار جزائري الى 2.000.000 دينار جزائري كل من أدخل بطريق الغش معطيات في نظام المعالجة الالية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها » ، فمن خلال نص المادة يتبين لنا أن الصورة الثانية من جرائم الاعتداء على منظومةالمعالجة الالية للمعطيات تشمل الفعلين التاليين :

---

[1] جميل عبد الباقي صغير، المرجع السابق، ص 28.

[2] Kurtz (Robin K.), Op.Cit, p.27.

أ- ادخال معطيات في نظام معالجة آلية للمعطيات :

يتمثل الركن المادي في هذا السلوك المجرم في اضافة معطيات غريبة عن نظام المعالجة الآلية ، ويستوي الأمر فيما إذا كانت المنظومة المعلوماتية أو الدعامة الحاملة للمعطيات خالية أم تحتوي على معطيات. [1]

حيث يهدف المشرع من هذا التجريم حماية المعطيات الموجودة في المنضومة المعلوماتية .

ب - ازالة أو تعديل المعطيات التي يتضمنها نظام المعالجة الالية للمعطيات :

يقصد بازالة المعطيات محو جزء منها أو كلها ، وتنتشر هذه الجريمة في وسط الموظفين المصرح لهم باستعمال جهاز الحاسب الآلي الخاص بالشركة التي كلفتهم بحفظ المعطيات في نظام الحاسب الآلي، كما قد يتم التلاعب بهذه المعطيات من خلال تعديلها وذلك بتغييرها و استبدالها بمعطيات أخرى.

وقد تتم إزالة المعطيات من خلال التلاعب ببرنامج المعالجة عند اعطاءه معلومات مغايرة للمعلومات الاصلية بحيث ينتج عن ذلك معالجته لها وبالتالي اعطاءه لنتائج مختلفة عن تلك التي صمم لاجلها ، وغالبا ما يستعمل الجاني برامج فيروسات تعمل على محو المعطيات و اتلافها أو تعديلها .

ويهدف المشرع من خلال تجريم فعلي الازالة أو التعديل إلى حماية المعطيات الموجودة داخل المنظومة المعلوماتية ولم تنفصل عنها بعد.

الصورة الثالثة - تجريم المساس بالمعطيات سواء خارج منظومة المعالجة الالية او ضمنها:

كما ضمن المشرع حماية المعطيات الموجودة في نظام المعالجة الآلية ولم تنفصل عنها بعد ، فإنه تناول بالحماية المعطيات الموجودة خارج منظومة المعالجة ، إذ تناولت المادة 394 مكرر 2 تجريم السلوكات التالية :

أ - تصميم او بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية .

ولم تشترط المادة السابقة أن تكون المعطيات داخل منظومة المعالجة الآلية او خارجها بحيث محل الجريمة يتمثل في المعطيات ذاتها سواء كانت مخزنة في أقراص أوفي ذاكرة الحاسب الالي أو كانت معالجة آليا أو مرسلة عن طريق المنظومة المعلوماتية وذلك اذا استعملت في ارتكاب احدى الجرائم المنصوص عليها في قسم المساس بأنظمة المعالجة الالية للمعطيات .

ب- حيازة أو افشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في قسم المساس بانظمة المعالجة الالية للمعطيات .

وبذلك يهدف المشرع فضلا عن حماية المعطيات عدم استعمالها في الجرائم التقليدية المنصوص عليها في قانون العقوبات . لكن ينبغي أن نتساءل عن التغيير أو الحذف أو التعديل الذي يطرأ على معطيات منفصلة عن نظام المعالجة الآلية كالبطاقات الإلكترونية حيث لم يشر المشرع إلى ذلك واكتفى بذكر التصميم والبحث و التجميع و التوفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية

---

[1] علي عبد القادر القهوجي ، المرجع السابق ،ص 59.

الفرع الثاني

المساهمة و الشروع في جريمة المساس بأنظمة المعالجة الالية للمعطيات

جرم المشرع الجزائري المساهمة و الشروع في ارتكاب جنحة المساس بأنظمة المعالجة الآلية للمعطيات في المادة 394 مكرر 5 والمادة 394 مكرر 7، وجعل العقوبة المقررة لكل منهما تماثل العقوبة المقررة للجريمة ذاتها. وجاء تجريم المشرع الجزائري للمساهمة و الشروع في هذه الجريمة تبنيا منه للمادة 11 من اتفاقية بودابست لمكافحة الاجرام المعلوماتي .

أولا - المساهمة في جريمة المساس بانظمة المعالجة الالية للمعطيات :

نصت المادة 394 مكرر 5 من قانون العقوبات الجزائري والتي تقابلها المادة 323 فقرة 4 من قانون العقوبات الفرنسي على أن « كل من شارك في مجموعة أو في اتفاق تالف بغرض الاعداد لجريمة أو اكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها » .

وقد ارتأى المشرع الجزائري أن يوسع من نطاق التجريم ليشمل الأعمال التحضيرية التي تجسدت بأفعال مادية وتمت في اطار اتفاق جنائي .

ويفهم من نص المادة ان العقاب على الأعمال التحضيرية تشترط وجود اتفاق جنائي أي ان العمل التحضيري المرتكب من قبل شخص واحد غير معاقب عليه ، ومن المتعارف عليه ان الأعمال التحضيرية غير معاقب عليها ما لم تكن تشكل جريمة مستقلة كحيازة برامج تسهل المساس بمنظومة المعالجة الآلية أو حيازة صور مخلة بالآداب العامة ، والسبب في تجريم المشرع للأعمال التحضيرية التي تتم في إطار إتفاق جنائي هو رغبته في مكافحة الجريمة المعلوماتية وعدم السماح بتشكيل جماعات إجرامية تحترف الإجرام المعلوماتي ، كما أنه اشترط ان يتجسد العمل التحضيري في افعال مادية كتجريب عدة كلمات سر أو محاولة الدخول الى منظومة معلوماتية بطريقة احتيالية .

بالإضافة إلى ذلك إشترط المشرع الجزائري أن يكون الاتفاق بغرض التحضيرلارتكاب احدى جرائم المساس بمنظومة المعالجة الآلية ،أي أن يكون كل فرد على علم بانه عضو في مجموعة اجرامية وان تتجه ارادة كل فرد إلى ارتكاب النشاط الاجرامي .

ثانيا- الشروع في ارتكاب جريمة المساس بانظمة المعالجة الالية للمعطيات :

عاقب المشرع الجزائري على الشروع في ارتكاب جريمة المساس بمنظومة المعالجة الالية للمعطيات بنفس العقوبة المقررة للجريمة ذاتها من خلال نص المادة 394 مكرر 7 ، ومن خلال ترتيب المواد يتبين لنا ان المشرع الجزائري قد عاقب على الشروع في التحضير لارتكاب جريمة في اطار الاتفاق الجنائي بخلاف المشرع الفرنسي الذي استبعد الشروع في الاتفاق الجنائي لارتكاب الاعمال التحضيرية للجرائم الماسة بنظام المعالجة الالية للمعطيات اذ ان المشرع الفرنسي اعتبران ذاك يدخل في اطار الشروع في الشروع .

الفرع الثالث
الجزاءات المقررة لمرتكب جريمة المساس بأنظمة المعالجة الآلية للمعطيات

قرر المشرع الجزائري لردع ارتكاب إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات عقوبات تنوعت بين السالبة للحرية و الغرامة المالية كما نص على عقوبات تطبق على الشخص الطبيعي وأخرى على الشخص المعنوي :

أولا - العقوبات الاصلية :

1 - العقوبات المطبقة على الشخص الطبيعي :

تدرجت العقوبات المطبقة على الشخص الطبيعي وفقا لطبيعة الجريمة و خطورتها حيث يتبين لنا من خلال استقراء النص هذا التدرج :

أ - جريمة الدخول أو البقاء بطريق الغش في منظومة معلوماتية :

قرر لها المشرع الجزائري في صورتها البسيطة في المادة 394 مكرر عقوبة الحبس من ثلاثة اشهر الى سنة ، و الغرامة المالية من 50.000 دج الى 100.000 دج ، أما في صورتها المشددة ضاعف المشرع من العقوبة المقررة لها حسب نص المادة 394 مكرر فقرة 2 و3.

ب- جريمة ادخال معطيات أو ازالة معطيات من نظام المعالجة الالية :

قرر لها المشرع في المادة 394 مكرر 1 عقوبة الحبس من ستة اشهر الى ثلاث سنوات والغرامة المالية من 500.000 دج الى 2000.000 دج.

ج - جريمة تصميم أو بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او مرسلة او حيازتها أو افشاء ها او استعمالها :

قرر لها المشرع في المادة 394 مكرر 2 عقوبة الحبس من شهرين الى ثلاث سنوات والغرامة المالية من 1000.000 دج الى 5000.000 دج .

كما ضاعف المشرع الجزائري من عقوبة كل الجرائم المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام حسب نص المادة 394 مكرر 3 .

2 - العقوبات المطبقة على الشخص المعنوي :

تماشيا مع نص المادة 18 مكرر من قانون العقوبات التي اخضع فيها المشرع الجزائري الشخص المعنوي الى عقوبات تتوافق وطبيعته ، فانه في المادة 394 مكرر 4 قد قرر معاقبة الشخص المعنوي الذي يرتكب احدى جرائم المساس بنظام المعالجة التالية للمعطيات الى غرامة مالية تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي .

ثانيا- العقوبات التكميلية :

نص المشرع على عقوبات تكميلية في المادة 394 مكرر 6 تتمثل فيمايلي :

- المصادرة الأجهزة و البرامج و الوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية.
- إغلاق المواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها .

المطلب الثاني

القانون رقم 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها

مع تزايد المخاوف من انتشار الاجرام المعلوماتي بمختلف أشكاله في الجزائر و التنامي المستمر في الاعتماد على تكنولوجيات الإعلام و الإتصال ، و بالأخص على شبكة الأنترنت ، كان لازما على المشرع الجزائري أن يتدخل ويكيف النصوص القانونية مع هذا التطور المتلاحق للجريمة المعلوماتية أو الجريمة الافتراضية ، وعلى الرغم من أن عدد القضايا التي طرحت على العدالة الجزائرية منذ سنة 2005 لا يوحي باستفحال الظاهرة حسب احصائيات مركز البحوث القانونية و القضائية بوزارة العدل في الجزائر، حيث انه لم يتجاوز 38 قضية توبع من اجلها 88 متهم ، لكن المخاوف من تزايد عدد مستخدمي الانترنت في الجزائر الذي بلغ 4,5 مليون شخص الى غاية بداية سنة 2010 ، و بسبب الاعتماد على البطاقات المصرفية في المستقبل القريب و امكانية استخدام الأنترنت ذي التدفق العالي يؤكد ضرورة الاستعداد لهذه الظروف و تطوير الكفاءات القضائية و الأمنية لمواجهة هذه الجرائم .[1]

وتتنوع الجرائم المعلوماتية في الجزائر بين هجمات على المواقع الالكترونية الجزائرية العمومية او الخاصة و تدميرها وكذا اعمال الدعاية الارهابية و سرقة المعطيات و عرض الصور الخليعة على الانترنت حيث جاءت الاحصائيات المقدمة بالشكل التالي :

- الدخول غير المشروع و اتلاف المعطيات او تعديلها : 13 قضية .
- الدخول غير المشروع : 11 قضية .
- ادخال معلومات عن طريق الغش : 8 قضايا.
- حيازة معطيات من دخول غير مشروع : 3 قضايا .
- نشر صور للاستغلال الجنسي للاطفال : قضية واحدة .

ويهدف المشرع من خلال وضعه القانون رقم 09/ 04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحته [2]، والذي جاءت نصوصه مطابقة في اغلبها لنصوص اتفاقية بودابست لمكافحة الاجرام المعلوماتي او الافتراضي وخاصة النصوص الاجرائية منها ،إلى وضع إطار قانوني يتلاءم مع خصوصية وخطورة الجريمة المعلوماتية ،فقد جاء القانون جامعا بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدر الاعتداءات والتعرف على مرتكبها في سبيل تحقيق حماية جنائية للمعطيات الإلكترونية من الجرائم المعلوماتية.

---

[1] وردت هذه االاحصائيات في مداخلة لمدير مركز البحوث القانونية و القضائية بوزارة العدل في الجزائر اثناء الملتقى الدولي حول محاربة الجريمة المعلوماتية المنعقد بالجزائر بتاريخ 5 ماي 2010.

[2] القانون رقم 09- 04 مؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها، ج .ر عدد 47 ، ص 5.

وقد قامت الجزائرباتخاذ عدة خطوات لتكييف جهازها الأمني و القضائي بطريقة تمكنها من التحكم في محاكمة هذا النوع من الجرائم فقد تم على مستوى أمن كل الدوائر عبر الوطن إنشاء فرقة متخصصة من الشرطة القضائية مهمتها التحقيق في الجرائم المعلوماتية وكذا مركز وطني لمكافحة هذه الجرائم مهمته تطوير أساليب وتقنيات التعامل مع هذا النوع من الجرائم.

في هذا المطلب سنتعرض لدراسة القانون رقم 09/ 04 المؤرخ في 5 أوت 2009 و المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها ، الذي تضمن تسعة عشر مادة موزعة على ستة فصول ، حيث نتطرق لأهم ما جاء فيه من قواعد اجرائية واحكام جديدة بخصوص التصدي للجريمة المعلوماتية أو الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال كما ورد ذكرها في نص القانون .

الفرع الاول

المصطلحات الواردة في القانون رقم 09- 04

قدم نص القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال جملة من المصطلحات الواردة في النص ، وذلك على النحو التالي :

الأحكام العامة :

بين من خلالها المشرع أهداف القانون المتمثلة في وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و كذا مجال تطبيقه وشرح المصطلحات التقنية الواردة فيه .

تشمل الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات التي وردت في نص المادة 394 مكرر من قانون العقوبات ، وكذلك كل جريمة ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية .

فقد أدخل المشرع في مفهوم الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال بالإضافة الى جرائم المساس بأنظمة المعالجة الالية للمعطيات ، جرائم الحاسب الالي و جرائم الانترنت ، التي تطرقنا اليها في الفصل الثاني وكذلك الجرائم الجديدة التي ترتكب بواسطة الهاتف الخلوي، وكل نظام آخر للاتصالات ، بحيث أراد المشرع أن لا يرتبط النص بالتكنولوجيا المتسارعة التطور بل بالاهداف المرجوة من تكنولوجيا الاعلام و الاتصال وبالتالي امكانية تطبيق النص على أي تكنولوجيا قد تظهر في المستقبل في مجال الاعلام و الاتصال .

و جاء في نص القانون عدة مصطلحات تقنية توجب على المشرع شرحها في المادة الثانية من نص القانون وتقابلها المادة الاولى من اتفاقية مكافحة الاجرام المعلوماتي ببودابست ،حتى لا يفقد النص قيمته القانونية ولا يعطى المجال لتعدد التفسيرات ، و تتمثل هذه المصطلحات فيما يلي :

- المنظومة المعلوماتية :

« أي نظام منفصل او مجموعة من الانظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو اكثر بمعالجة الية للمعطيات تنفيذا لبرنامج معين ».

- المعطيات المعلوماتية :

«أي عمليات عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها ».

يتبين لنا أن المعطيات المعلوماتية أو معطيات الحاسب الآلي تشمل الحقائق و المعلومات و المفاهيم بأي شكل مناسب للمعالجة في نظام الحاسب الالي ويشمل التعريف كذلك البرامج التطبيقية بمختلف أنواعها و برامج التشغيل .

- مقدمو الخدمة :

«أي كيان عام أو خاص يقدم لمستعملي خدماته ،القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات ، واي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها ».

من خلال الشرح يتبين لنا أن مصطلح مقدمي الخدمة يشمل كل شخص عام أو خاص يزود المستخدمين بالخدمات التي تمكن اجهزة الحاسب الآلي من الاتصال ببعضها وكذا كل شخص يعالج المعطيات المخزنة بهدف تمكين مستعملي اجهزة الحاسب الالي من الاتصال .

- المعطيات المتعلقة بحركة السير:

«أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الاخيرة باعتبارها جزءا في حلقة اتصالات ، توضح مصدر الاتصال و الوجهة المرسلة اليها ، والطريق الذي تسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة » .

- الاتصالات الالكترونية :

« أي تراسل أو ارسال أو استقبال علامات أو اشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة اي وسيلة إلكترونية ».

الفرع الثاني

اجراءات المتابعة الخاصة التي جاء بها القانون رقم 09- 04

جاء القانون بمكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال بإجراءات خاصة منها ما يتعلق بمراقبة الاتصالات الالكترونية وما يتعلق باجراءات التفتيش و الحجز ، كما ألزم القانون المتعاملين في مجال تكنولوجيا الاعلام و الاتصال بتقديم يد المساعدة بهدف الوقاية من الجرائم المنصوص عليها في هذا القانون .

وتشمل هذه الاجراءات التي نص عليها المشرع على قواعد خاصة بالتفتيش و الحجز في مجال الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال مع عدم الاخلال بالقواعد العامة لقانون الاجراءات الجزائية الجزائري ، وتتمثل هذه القواعد الاجرائية فيما يلي :

أولا - مراقبة الاتصالات الإلكترونية :

بين المشرع في هذا الفصل ومن خلال المادة الرابعة الحالات التي يسمح فيها باللجوء الى المراقبة الالكترونية حيث يضمن القانون حماية الحريات الفردية سيما منها الخصوصية.

وقد أورد بوضوح في المادة الرابعة الأحكام الخاصة بالمراقبة الإلكترونية التي لا يجوز إجراؤها إلا بإذن السلطات القضائية المختصة ، كما تم تحديد الحالات التي يجوز فيها اللجوء إلى المراقبة الإلكترونية وهي الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب، والجرائم التي تمسّ بأمن الدولة أو حالة توفر معلومات عن اعتداء محتمل بهدّد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام.

وتتمثل الحالات التي تسمح فيها باللجوء الى المراقبة الالكترونية فيما يلي :

ا- الوقاية من الافعال الموصوفة بجرائم الارهاب و التخريب و الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني او النظام العام .

ج- لمقتضيات التحريات و التحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الإلكترونية.

د- في اطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

فالمشرع من خلال حصره للحالات التي يتم اللجوء فيها إلى مراقبة الإتصالات أراد أن يوازن إلى حد ما بين حرية الافراد في سرية الاتصالات و احترام خصوصياتهم ، وبين مكافحة الجرائم الماسة بالنظام و الأمن العموميين ، حتى لا يتم تقييد حرية الأفراد و لا يتم الإخلال بالأحكام القانونية التي تضمن سرية المراسلات و الإتصالات في حالة ما إذا ترك الحرية لرجال الضبطية في مراقبة الإتصالات الإلكترونية، وجعل إجراء عملية مراقبة الإتصالات الإلكترونية تحت إشراف السلطات القضائية ، و في حالة الجرائم الموصوفة بجرائم

الإرهاب والتخريب والماسة بأمن الدولة يتم منح الإذن لضابط الشرطة القضائية إجراء عملية المراقبة من قبل النائب العام لدى مجلس قضاء الجزائر ،يكون صالحا لمدة ستة أشهر قابلة للتجديد.
كما شدد المشرع من ان المعطيات المجمعة جراء عملية المراقبة تكون موجهة حصريا للوقاية من الأعتداءات الإرهابية و الماسة بأمن الدولة ، وذلك تحت طائلة العقوبات في حالة المساس بالحياة الخاصة للغير.

ثانيا - تفتيش المنظومة المعلوماتية:

أجاز المشرع الجزائري في المادة الخامسة من هذا القانون للسلطات القضائية المختصة وكذا لضباط الشرطة القضائية ، الدخول بغرض التفتيش إلى منظومة معلوماتية ، منظومة تخزين معلوماتية و إلى كافة المعطيات المخزنة فيها ، ويمكن القيام بذلك عن طريق التفتيش في مكان ارتكاب الجريمة او عن بعد .

كما اجاز القانون تمديد التفتيش في كل منظومة معلوماتية اخرى قد تكون على علاقة بالمنظومة المعلوماتية الاولى .

أما اذا كانت المنظومة المعلوماتية موجودة في بلد اجنبي فقد بين القانون ان عملية التفتيش تخضع للاتفاقيات الدولية المبرمة وفق مبدأ المعاملة بالمثل.

ثالثا - حجز المعطيات المعلوماتية:

نص المشرع في المادة السادسة على حجز المعطيات المخزنة داخل المنظومة المعلوماتية إذا كانت مفيدة للكشف عن الجرائم أو مرتكبيها، كما أتاح للمحققين إمكانية نسخ هذه المعطيات على دعامة تخزين إلكترونية تكون قابلة للحجز وفق القواعد المقررة في قانون الاجراءات الجزائية .

رابعا - حفظ المعطيات المحجوزة:

بين المشرع في المادة السابعة كيفية حفظ المعطيات التي لا يمكن حجزها وذلك من خلال منع الوصول اليها ووضعها تحت تصرف الاشخاص المرخص لهم باستعمالها.

خامسا - التزامات مقدمي الخدمات و خدمة الانترنت :

ألزم المشرع المتعاملين في مجال الإتصالات الإلكترونية من مقدمي الخدمات و خدمة الانترنت بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية للكشف عن الجرائم و مرتكبيها ، حيث تمّ تحديد الالتزامات التي تقع على عاتق المتعاملين في مجال الاتصالات الالكترونية خاصة إلزامية حفظ المعطيات المتعلقة بحركة السير التي من شأنها المساعدة في الكشف عن الجرائم ومرتكبيها، وهدف المشرع من ذلك الى إعطاء مقدمي الخدمات دورا إيجابيا في مساعدة السلطات العمومية في مواجهة الجرائم وكشف مرتكبيها.

سادسا- انشاء الهيئة الوطنية للوقاية من الاجرام المتصل بتكنولوجيات الاعلام و الاتصال و مكافحته:

نص المشرع في المادة 13 على ضرورة انشاء هيئة ذات وظيفة تنسيقية تعمل على اتخاذ الاجراءات اللازمة للوقاية من هذه الجرائم و تتولى تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية وكذا مصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم واحال على التنظيم كيفية تشكيلتها وسيرها .

الفرع الثالث

التعاون الدولي لمواجهة جرائم تكنولوجيا الاعلام و الاتصال

تناول المشرع في هذا الفصل ضمن المواد من 15 إلى المادة 18 بعض القواعد المتعلقة بالتعاون الدولي و الاختصاص القضائي وكذا تنظيم المساعدة القضائية الدولية و تبادل المعلومات ، وذلك على النحو التالي :

- الاختصاص القضائئ:

بالإضافة إلى القواعد العامة بخصوص الاختصاص والمنصوص عليها في قانون الاجراءات الجزائية ، فقد جعل المشرع الجزائري من اختصاص المحاكم الجزائرية النظر في الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال التي يرتكبها شخص أجنبي و في إقليم أجنبي ، وذلك إذا كانت تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الاستراتيجية للوطن.

- المساعدة القضائية:

نضم المشرع الجزائري كيفية قبول طلبات المساعدة القضائية بين الدول فيما يخص جمع الادلة في الجريمة المعلوماتية ، بحيث جعل من البريد الالكتروني و جهاز الفاكس وسائل مقبولة لطلب المساعدة القضائية ، كما وضع قيودا على طلبات المساعدة القضائية تتعلق بعدم المساس بالسيادة الوطنية ، وكذا الحفاظ على سرية المعلومات المبلغة ، واشترط أن لا يتم استخدام المعلومات المقدمة في اطار المساعدة القضائية في غير الغرض الذي قدمت من اجله.

المبحث الثالث

الحلول و التوصيات المقترحة لمواجهة تحديات انتشار الإجرام المعلوماتي

أظهر الانتشار الكبير للحاسبات الآلية و الأنترنت في الحياة العملية ضرورة وضع الحلول العملية والقانونية لمواجهة التحديات التي تعرقل جهود مكافحة الجرائم المعلوماتية ، وعلى الرغم من أن العديد من التشريعات الوطنية قد تداركت هذا الوضع من خلال سن قوانين تجرم وتعاقب على بعض السلوكات التي تعد جرائم مرتبطة بتكنولوجيات الاعلام و الاتصال ، إلا أنه لا ينبغي أن تتوقف هذه الجهود المبذولة عند هذا الحد ، بل إن حتمية مواكبة التطورات المتلاحقة لهذه التكنولوجيات تفرض على المشرع أن يضع القواعد الرئيسية التي تمكنه من الاستعانة بها عند سن أي تشريع جديد يخص تنظيم استخدام الانترنت و سبل اثبات الجرائم المعلوماتية بمختلف صورها مع مراعاة الأحكام التي تضمن عدم المساس بحقوق الافراد في الخصوصية.

وفي هذا المبحث سنستعرض بعض الحلول و التوصيات المقترحة لمواجهة انتشار الجرائم المعلوماتية على المستوى الوطني و الدولي.

المطلب الأول

الحلول المقترحة على المستوى الوطني

بعد أن تناولنا في المباحث السابقة كيفية تصدي المشرع الجزائري للجرائم المعلوماتية من خلال تجريمه لصور المساس بنظام المعالجة الالية للمعطيات وكذا الجرائم التي ترتكب عن طريق منظومة معلوماتية أو أي نظام لإتصالات الإلكترونية، نتناول في هذا المطلب الحلول التي نقترحها لمكافحة جرائم المعلوماتية على المستوى الوطني وكذا سبل تحقيق الوقاية منها، مبينين العناصر والمواضيع الواجب توافرها في التشريعات الوطنية والتي يجب أن تكون شاملة ومحددة ورادعة وقابلة للتطوير للتصدي لهذه الجرائم .

وتتمثل هذه المقترحات فيما يلي:

أولا) مقترحات تخص الجانب الموضوعي للتشريعات :

أ- ضرورة سن التشريعات لمكافحة جرائم المعلوماتية، بحيث تكون هذه النصوص واضحة وذلك بإدخال كافة صور السلوك الضار والخطر على المجتمع التي يستخدم فيها الأنترنت ، على أن يراعى خلال سن هذه التشريعات المقترحات التالية :

1- حماية واحترام الحياة الخاصة للأفراد ضد أي انتهاك.

2- تحقيق التوازن بين حماية التكنولوجيا وحماية حقوق الافراد .

3- تعداد صور الجرائم المعلوماتية التي تتم بواسطة أو ضد الحاسب الالي أو شبكة الأنترنت مع جعل النص مرنا ومواكبا للتطورات المتلاحقة لتكنولوجيا المعلومات بحيث يستوعب الجرائم التي قد تحدث مستقبلا نتيجة للتطور المستمر لتكنولوجيا المعلومات و الاتصالات .

4- الحرص على تعزيز التعاون الإقليمي و الدولي لمكافحة هذه الجرائم نظرا للطبيعة العابرة للحدود لها.

ب- ضرورة تشديد العقوبة ووضع نص خاص بتجريم استخدام الأطفال في تصوير أفلام تمثلهم في أوضاع مخلة بالآداب العامة وعرضها على شبكة الانترنت وباستخدام البريد الإلكتروني وعدم الاكتفاء بالنصوص التقليدية فيما يخص تجريم تحريض القصر عى الفسق و الدعارة.

ج- اعداد قانون يشرع استخدام الوثائق الالكترونية والتوقيع الالكتروني واعتماد جهات مصدرة لشهادات التوثيق الرقمي لتأكيد الهوية نظرا لاهميتها في التعاملات المصرفية ولاعمال التجارة الالكترونية والخدمات الحكومية الالكترونية .

د- السعي لتعديل قانون التجارة ليأخذ بعين الاعتبار مواضيع التجارة الالكترونية والوثائق الالكترونية وتنظيم جباية الضرائب والرسوم المترتبة على إتمام الصفقة في المعملات الالكترونية وحماية خصوصية البائع والمشتري، ومنع المتاجرة عبر الانترنت في السلع والخدمات المحرمة مثل المواد الفاضحة غير الأخلاقية، والأسلحة.

ثانيا) مقترحات تخص الجانب الاجرائي للتشريعات:

أ- تعديل قواعد الإجراءات الجنائية لتتلاءم مع طبيعة الجرائم المعلوماتية بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها في حال تفتيش الحاسب الالي وعند ضبط المعلومات التي تحتويها حتى يستمد الدليل مشروعيته كما ينبغي أن يسمح لسلطات الضبط والتحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل الجريمة .

ب- تقنين قواعد جديدة لمكافحة الجرائم المعلوماتية بحيث تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولاسيما فيما يتعلق بالإثبات الجنائي والمدني ، مع ضرورة النص صراحة في القوانين المنظمة للإثبات – الجنائي والمدني – بالشكل الذي يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والانترنت في الإثبات ، طالما أن ضبط هذه الأدلة جاء وليد إجراءات مشروعة ، على أن تتم مناقشة هذه الادلة بالمحكمة والاستناد إلى تقرير الخبراء .

ج- تطوير قدرات المؤسسات الامنية الجزائرية للتحكم في التكنولوجيا الرقمية و خاصة تقنية تفتيش أجهزة الكمبيوتر عن بعد ، وذلك لمكافحة جرائم الانترنت مع وضع ضوابط لضمان احترام قوانين حماية المعلومات أثناء جمعها وتبادلها، كما يلزم أن تمتد إجراءات التفتيش إلى أية نظم حاسب ألي أخرى يمكن ان تكون ذات صلة بالحاسب الالي محل التفتيش .

د- منح سلطة توجيه الأوامر لمن تكون لديه معلومات خاصة للدخول وإعطاء كلمة السر للتمكن من معرفة ما يحويه الحاسب الآلي والانترنت وذلك لتمكين السلطات القائمة بالضبط والتفتيش للحصول على المعلومات المخزنة .

ه- تعزيز قدرات الموارد البشرية في عمليات التحقيق والإدعاء والمحاكمة في الجرائم المتصلة بالكمبيوترمن خلال العمل على زيادة معرفة القضاة والمدعين العامين بهذه النوعية الجديدة من الجرائم الخطيرة وآليات مكافحتها، وكيفية التحقيق فيها وجمع المعلومات والأدلة.

و- ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية ، وذلك من خلال تدريب رجال الشرطة على كيفية التعامل مع أجهزة الحاسب الآلي والإنترنت ، على أن يتم إنتقاء هم من ذوي التخصص في المعلوماتية.

ز- إنشاء وكالة خاصة لأمن أنظمة الإعلام الآلي، من أجل تأمين جميع المواقع الحكومية والخاصة وحماية المعطيات المتداولة على الشبكة المعلوماتية وتأمين المعطيات الحكومية المختلفة .

ح- تشجيع تبادل المعلومات بين قوات شرطة الاجرام المعلوماتي والشركات الخاصة حول طرق التحقيق والتكنولوجيات المستخدمة لملاحقة ومقاضاة المجرمين.

ط- تطوير نظام تشغيل كمبيوتر وطني خاص بالدولة كنظام " لينكس" المفتوح من أجل ضمان حماية البيانات والمعطيات المتداولة وطنيا بين مختلف الهيئات والمنظمات والدوائر الحكومية من خطر الجوسسة الاقتصادية و العسكرية و الامنية على غرار كثير الدول مثل روسيا ، وبذلك تتجنب أنظمة التشغيل التقليدية التي تسمح

للقراصنة بالحصول على المعطيات السياسية والاقتصادية والأمنية بسهولة ويسر، مما يسبب خسائر كبيرة للأفراد والمؤسسات.

ي - اتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم المعلوماتية ؛ وذلك من خلال إيجاد خط مفتوح يختص بتلقي البلاغات المتعلقة بهذه الجرائم، ولاسيما الجرائم الأخلاقية كحالات الإعلان عن البغاء وممارسة الفجور أو الاستغلال الجنسي للأطفال عبر الانترنت مع تشجيع وتدريب المجني عليهم على القيام بالتبليغ عن اية جريمة معلوماتية تقع عليهم.

ك- نشر الوعي بين صفوف المواطنين – ولاسيما الشباب – بمخاطر التعامل مع المواقع السيئة علي شبكة الإنترنت مع إدخال مادة " أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم ما قبل الجامعي مع إنشاء قسم جديد بكليات الحقوق بالجامعات العربية لدراسة الحماية القانونية للمعلوماتية أو تحت مسمى آخر قانون المعلوماتية والانترنت أو قانون الحاسب الآلي والانترنت .

ل- تفعيل دور المجتمع المدني ولاسيما الجمعيات الأهلية للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقيا عبر شبكة الانترنت.

م- تأهيل الخبراء على بحث تكنولوجيا المعلومات للوصول الى معايير امنية مشتركة تحد من جرائم المعلوماتية.

المطلب الثاني

الحلول المقترحة على المستوى الدولي

إن التعاون الدولي هو اللبنة الأولى والركيزة الأساسية في مواجهة هذا النوع من الجرائم نظرا لأنها غالبا ما تتم من أماكن مختلفة في العالم وباستخدام تقنيات حديثة ، و هو ما أكدت عليه إتفاقية مجلس أوروبا بشأن الإجرام" السيبيري "عندما نصت على" ضرورة إلتزام الدول الأعضاء بتسليم المجرمين والمساعدة المتبادلة في التحقيق وجمع الأدلة وإتخاذ التدابيرالتشريعية التي تمكنها من الوفاء بهذه الإلتزامات."

وقد قامت عدة دول أوروبية إلتزاما منها بالمعاهدات التي وقعتها في توحيد جهودها لأجل محاربة جرائم الأنترنت من خلال تبادل الخبرات في مجال الامن المعلوماتي ومتابعة الجريمة في مكان ارتكابها وحتى منعها من الوقوع باعتماد معايير خاصة.

ونظرا لأهمية التعاون الدولي في هذا المجال نورد بعض الحلول التي تعزز التعاون بين الدول لمكافحة الاجرام المعلوملتي، ومنها :

أ) ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية.

ب) بحث التعاون مع الدول الاخرى في مجال الخبرة و المعلومات في شأن تشريعات الحاسب الالي والانترنت.

ج)- توثيق الروابط مع مختلف مراكز الدراسات و البحوث الأمنية و التقنية عبر مختلف الدول لغرض نشر و تبادل نتائج الدراسات و البحوث الخاصة بأمن المعلومات.

د)- تنظيم مؤتمرات دولية بمشاركة المنظمات الدولية ذات الصلة بالبحث في جرائم المعلوماتية و أمن المعلومات من أجل وضع تشريعات نموذجية دولية لمساعدة الدول المتاخرة في هذا المجال للإعداد لتشريع وطني لمكافحة جرائم المعلوماتية.

ه)- الاستفادة من تجارب الدول المتقدمة التي حققت نجاحا في مواجهة هذه الجرائم من أجل تعميم الفائدة بما أن هذه الجرائم ذات طبيعة عابرة للحدود .

و)- حث الدول إلى الإسراع والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية.

ز)- تطوير القوانين والإجراءات الوطنية الجنائية الكفيلة بمنع الإرهابيين من استغلال قوانين اللجوء والهجرة للحصول على ملاذ آمن أو استخدام أراضي الدول كقواعد للتجنيد أو التدريب أو التخطيط أو التحريض أو الانطلاق منها لشن الهجمات الإرهابية المعلوماتية ضد الدول الأخرى.

خاتمة

لقد أصبح من الواضح في عالم اليوم أن هناك ارتباط وثيق بين النتائج التي تقدمها باستمرار صناعة تكنولوجيا المعلومات و الاتصالات ، و طرق ارتكاب الجرائم المعلوماتية التي لا زالت مخاطرها في ازدياد مطرد مع ما تقدمه لها هذه التكنولوجيات الحديثة ،حيث تتوسع دائرتها لتشمل كافة مرافق الحياة العامة ، وتكمن هذه المخاطر في سيطرة الوسائل التكنولوجية على معظم أوجه حياتنا اليومية ، حيث مكنت طرق المعالجة الآلية للمعلومات المجتمعات من تجاوز حدود التفكير العادية نظرا للإمكانيات المتاحة أمامها ، فلا يخلو مجال من مظاهر التأثر بالمعلوماتية ؛ فالحياة السياسية لم تعد تقتصر على الاجتماعات في القاعات المغلقة بل وجدت في منتديات الدردشة فضاء خصبا لنشر الأفكار، أما في المجال الاقتصادي فالتأثر كان أكثر وضوحا وليس أدل على ذلك من انتشار الشركات والمصارف في الفضاء الإفتراضي ، وازدهار التجارة الإلكترونية التي بلغت أرقام أعمالها حدودا قياسية ، هذا بالإضافة إلى مناحي الحياة الاخرى فالإعلام ازدهر لما وفرته المعلوماتية من سرعة وصول الخبر وبشكل وسائط متعددة ، كما أستعملت في مناهج التعليم لسهولة تخزين ومعالجة كم هائل من المعلومات مما ساعد على تنمية الموارد البشرية للدول ووفر الظروف الملائمة لحرية الابداع في المجال الصناعي و الأدبي والفني .

لكن ليس خافيا أن الإنحراف في إستخدام الوسائل التكنولوجية و إساءة استعمال الحاسب الآلي و شبكة الانترنت نتج عنه أضرار لا يمكن تداركها بسهولة و لأنها تهدد سلامة البيانات المخزنة في أجهزة الحاسب الآلي وتقيد حرية تنقل المعلومات التي ننتجها أو نتداولها جميعا كأفراد ومؤسسات والتي تعد ثروة حقيقية لا تقدر بثمن ويستوجب حمايتها من السطو عليها أو العبث بها . وأكثر من ذلك فقد أدى تنامي الجرائم المعلوماتية إلى تعطيل وتيرة انتاج البرمجيات و غيرها من الأعمال التي تحميها قوانين الملكية الفكرية نتيجة لأعمال القرصنة مما أثر على حركة الابداع الفكري ، و كنتيجة لاستفحال طرق الجرائم المعلوماتية فإنها بدأت تهدد الإقتصاد العالمي بسب الخسائر الكبيرة التي تنجم عنها .

ومن خلال دراستنا لصور الجريمة المعلوماتية تبين لنا كيف يمكن لوسائل التكنولوجيا التي من المفروض أن تساهم في رفاهية المجتمع أن تصبح هاجسا يقلق الأفراد بمختلف فئاته وتجعله يعكف عن استخدامها على الرغم من مخاطر تراجع الأفراد في استعمال وسائل الاتصالات الحديثة على عجلة التنمية ، فلا يجب أن يقابل التطور السريع للتقنيات الحديثة عزوف فئات المجتمع و المؤسسات عن استخدام الوسائل التكنولوجية الحديثة في مقابل تطور الأساليب الجرمية المتجددة قبل المجرمين المعلوماتيين .

و أخطر ما في الأمر أن أغلب مرتكبي هذه الجرائم يتمكنون من البقاء مجهولي الهوية وهذا الأمر يتيح لهم الاستمرار والتفنن بطرق التلاعب بموارد الآخرين عن طريق السيطرة على أنظمتهم الإلكترونية ، فقد تمكن قراصنة الأنترنت من التسلل إلى كافة الشبكات من شبكات الكهرباء و الماء إلى شبكات الاتصالات المختلفة ، ولا يوجد ما يمنعهم من التسلل و التحكم في شبكات الملاحة الجوية و وزارات الدفاع عبر العديد من الدول .
و على الرغم من أن العالم لم يشهد بعد جرائم معلوماتية كبيرة أو إرهابا معلوماتيا من نو ع مشابه للإرهاب التقليدي ، إلا أن هشاشة البنية التحتية للشبكة العالمية للمعلومات ، وعدم فعالية البرامج الأمنية سواء على مستوى أنظمة المعالجة الآلية أو على شبكة الأنترنت ، كل هذه المعطيات تحذر من احتمالات وقوع لهجمات إرهابية معلوماتية ربما تؤدي إلى نتائج كارثية على المجتمعات والاقتصاد العالمي.

وانطلاقا من حتمية التصدي لهذا الإجرام برزت الحاجة إلى تنظيم مجال المعلوماتية وسن تشريعات بهذا الخصوص تحقيقاً لمبدأ الردع العام والخاص في هذا المجال وللمساعدة في زرع الثقة بين أوساط المجتمع في الإستفادة من إيجابيات هذه الثورة المعلوماتية ، وهذا بدوره يشجع على زيادة استخدام الوسائل التي توفرها تقنية المعلومات بدون هضم للحقوق، وبدون خشية العواقب السلبية، لأن بناء أي مجتمع رقمي يتطلب وجود نوعا من التفاعل الآمن والفوري بين خدمات الالكترونية عالية المستوى والفاعلية و التي تقدم من قبل مؤسسات حكومية أو خاصة وبين أفراد من المجتمع يستفيدوا من تلك الخدمات ، كما يمكننا تنظيم مجال المعلوماتية من رفع كفاءة العمل الإداري، والارتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع إيقاع العصر وهو ما بات يعرف بمصطلح الحكومة الإلكترونية ، أين يصبح للمحررات الإلكترونية التي تصدرها صفة المحررات الرسمية ، وهذا لن يتأتى إلا بشعور الأفراد بالأمن والثقة خصوصا مع تطور التعاملات الالكترونية حيث صار من الضروري وضع القواعد العامة التي تحكم إستخدام التقنية في التعاملات التجارية ، وتطوير النصوص التشريعية فيما يخص خدمات التصديق الإلكتروني لمنع الاحتيال و سرقة الهوية ، مما يثري قطاع الأعمال على الصعيدين المحلي والدولي، ويساعد على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

ومن مزايا سن تشريعات لمكافحة جرائم المعلوماتية أيضا تحقيق التوازن الضروري بين مصلحة المجتمع في الاستعانة بالتقنية الحديثة في الحياة اليومية ومصلحة الفرد في حماية خصوصيته والحفاظ على سرية الاتصالات و المراسلات التي تكفلها أغلب الدساتير و اتفاقيات دولية كالإعلان العالمي لحقوق الإنسان الصادر من الجمعية العامة للأمم المتحدة بموجب قررها رقم 217 المؤرخ في 1948/12/10 و المؤتمر الدولي لحقوق الإنسان المنعقد سنة 1968 في مونتريال بكندا و الذي وجه الأنظار إلى الأخطار الجديدة الناتجة عن التطورات التقنية والعلمية على هذا الحق مثل التجسس الإلكتروني [1] ،

وما يدعوا للقلق أن الكثير من البلدان التي لا تعتمد كثيرا على تكنولوجيا الإعلام و الاتصال في تعاملاتها الادارية أو الاقتصادية لا تتملك لحد الآن تشريعاً صريحاً يخص الجرائم المعلوماتية ، وربما يعود السبب في ذلك إلى قلة أو انعدام الدعاوي القضائية على مستوى محاكمها بخصوص الجرائم المعلوماتية ، ونتيجة للفراغ التشريعي في مجال مكافحة الإجرام المعلوماتي ، و لأن الطابع العابر للحدود لهذه الجرائم لا يمنع مجرمي المعلوماتية من استغلال هذه الظروف لارتكاب جرائمهم انطلاقا من هاته الدول، وجعلها قاعدة للهجمات الالكترونية أو للاحتيال المعلوماتي ، كما يجعلها مقصدا لإنشاء مواقع أنترنت غير مشروعة ، بالإضافة إلى أن الآثار السلبية للجرائم المعلوماتية على الأمن والاقتصاد الوطنيين بالغة التعقيد و مترابطة فيما بينها خاصة أن هذه الجرائم تتسم بالعالمية وتأخذ أبعادا دولية مما يقتضي وجوب التعاون الدولي وتوحيد الجهود لمواجهتها عبر إبرام الاتفاقيات بين الدول وعدم البقاء على الحياد لمحاولة الحد منها.

لقد حاولنا في دراستنا للجريمة المعلوماتية تبيين الاحكام العامة لها موضحين في الفصل التمهيدي اهم المحاولات لتعريف الجريمة المعلوماتية واختلاف المعايير المستند عليها في ذلك والهدف المتوخى من التجريم.

كما قدمنا في هذا البحث بعض التقديرات لحجم الجرائم المعلوماتية و خصائصها ودوافع ارتكابها بالاضافة الى ذكر سمات المجرم المعلوماتي وتحديد فئاته المختلفة.

---

[1] ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي ، مكتبة دار الثقافة للنشر والتوزيع ، الأردن ،1996 ، ص 80.

و في الفصل الاول تناولنا البنيان القانوني للجريمة المعلوماتية ، حيث استهلت الدراسة بتقديم آلية ارتكاب الجريمة والوسائل المستعملة في ذلك ، كما تناولنا طبيعة المحل مبرزين اهم الاراء التي ظهرت في تحديد الطبيعة القانونية للمعلومات ، ثم تطرقنا لدراسة عناصر الجريمة المعلوماتية وتعرضنا لشرح أحكام الشروع و المساهمة وقواعد المسؤولية الجنائية .

أما الفصل الثاني فقد خصصناه لدراسة صور الجريمة المعلوماتية ، حيث عرضنا أنواع جرائم الحاسب الالي وجرائم الانترنت مبرزين بعض النصوص في القوانين المقارنة التي تناولتها ، وأوضحنا كيف اختلف الفقهاء في مدى اعتبار الجريمة المعلوماتية من قبيل الجرائم التي تتطلب تشريعا خاصا بها ، أو امكانية تطبيق النصوص التقليدية عليها ، ورأينا كيف أن الجرائم المعلوماتية أظهرت إلى الوجود مبادىء جديدة إلى القانون الجنائي حيث لم تعد الطبيعة المادية للمحل أو للسلوك الإجرامي عنصرا أساسيا في هذا النوع من الجرائم خاصة فعل الاختلاس في جرائم السرقة المعلوماتية و الاحتيال المعلوماتي وكذا تسليم الشيء المختلس ، كما قدمنا بعض النماذج التطبيقية و القضايا العملية في مجال جرائم المعلوماتية .

بعد ذلك تناولنا جهود مكافحة الجريمة المعلوماتية في بعض الدول الغربية و الدول العربية وأخذنا كمثال عن التشريع الغربي كل من فرنسا والولايات المتحدة الأمريكية و المملكة المتحدة ، أما في التشريع العربي فقد أخذنا التشريع الاماراتي و المصري و التونسي ، كما تحدثنا عن جهود المكافحة الدولية من خلال التطرق لأهم القرارات الصادرة عن الامم المتحدة ، حيث عرضنا أهم ما جاء به كل من مؤتمر هافانا لسنة 1990 بشأن جرائم الكمبيوتر و مؤتمر ريودي جانيرو سنة 1994 وكذا أهم اتفاقية صادرة عن الاتحاد الاوروبي بخصوص جرائم المعلوماتية وهي اتفاقية بودابست لسنة 2001.

في حين خصصنا الفصل الثالث لدراسة التطور التشريعي لمكافحة الجريمة المعلوماتية في الجزائر أين تناولنا القواعد الاجرائية الخاصة بمتابعة هذا النوع من الجرائم حسب قانون الاجراءات الجزائية الجزائري و القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها ، موضحين أهم الصعوبات التي تعترض المحققين أثناء عملية البحث و التحري لإثبات الجريمة المعلوماتية ، ثم عرجنا على الحديث عن القوانين التي جاء بها المشرع الجزائري بهذا الخصوص ، و هما القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات و القانون رقم 09-04 مؤرخ في 5 وات 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها .

كما بينا ضرورة أن يتجه المشرع الجزائري إلى سن تشريعات صريحة بخصوص تجريم بعض السلوكات المرتكبة على شبكة الانترنت كاختراق المواقع و البريد الالكتروني وعدم الاكتفاء بالنصوص التقليدية في بعض الجرائم كجريمة التزوير في مستند منفصل عن نظام المعالجة الآلية للمعطيات وضرورة اضافة المحرر الإلكتروني إلى جريمة التزوير التقليدية على غرار المشرع الفرنسي الذي أضاف عبارة "كل سند للتعبير عن فكرة" الى نص جريمة التزوير التقليدية .

وأخيرا اوردنا بعض المقترحات لمكافحة الجرائم المعلوماتية على المستويين الوطني و الدولي وسبل تحقيق الوقاية منها والتصدي لمختلف صور الاجرام المعلوماتي وابرزنا الدور الذي يلعبه التعاون الدولي في هذا المجال نظرا لارتباط شبكات الاتصالات ببعضها عبر دول العالم.

ومن اهم الاستنتاجات التي توصلنا اليها من خلال هذه الدراسة :

- ضرورة الاهتمام بسن تشريعات صارمة تحدد بوضوح عناصر الجريمة المعلوماتية ، على ان تكون رادعة بما ان الوصول الى المجرم المعلوماتي هو عملية صعبة في غالب الاحيان وذلك للحد من تنامي اشكال الاجرام المعلوماتي.

- حتمية البحث بصفة مستمرة عن الأساليب والأدوات المستخدمة من قبل المجرمين المعلوماتيين وحصرها ،وكذا الاهتمام بالتعرف على التسهيلات التي يمكن أن تقدمها أيّ خدمة إلكترونية جديدة وأدوات ضبط هذه الجرائم والتحقيق فيها.

- التعجيل بوضع دراسة مستقبلية لما قد يحصل جراء تطور هذه الجرائم خصوصاً في هذه المرحلة التي تستعد فيها الجزائرالى تنفيذ مشروع الحكومة الالكترونية وتنظيم التجارة الالكترونية مع الاسراع باصدار قوانين صارمة تردع أي شخص يحاول العبث بالوثائق الرسمية .

- نشرثقافة استخدام الحسب الالي وشبكة الانترنت في الامور الايجابية في اوساط الشباب و الاحداث مع تنبيههم للسلوكات المجرمة قانونا اذ ان معظم المجرمين المعلوماتيين هم من فئة الشباب و المراهقين من مستخدمي الانترنت و الذين قد لا يدركون ان ما يقومون به من افعال القرصنة و السب و القذف او انتهاك الخصوصية او اعمال الاتلاف المعلوماتي الى غير ذلك تعد سلوكا اجراميا معاقب عيه قانونا ، ويكون ذلك من خلال تعبئة وسائل الاعلام ودور الشباب والمدارس والكليات.

- عقد مؤتمرات دولية بين اجهزة الشرطة و القضاء وسن اتفاقيات بخصوص تسليم المجرمين المعلوماتيين امر لابد منه حتى لا يتم خرق هذه الاتفاقيات فيتم التعامل بالمثل ومن ثم يفلت العديد من مجرمي الانترنت من العقاب.

- تعزيز التعاون الدولي وحث الدول التي لا تكافح قوانينها الجرائم المعلوماتية على الانضمام الى الاتفاقيات الدولية مع ضرورة بذل الجهود لتوحيد المصطلحات القانونية المستعملة في هذا المجال.

ونخلص اخيرا ، بعد استعراضنا لمجمل جوانب الجرائم المعلوماتية وتبيين مدى خطورتها على الحياة العلمية و العملية و الاجتماعية و المالية ، ان توحيد الجهود وتبادل الخبرات بين الدول ونقل التكنولوجيا في مجال الامن المعلوماتي يسهل على الدول غير المتطورة من مهمة حماية انظمتها المعلوماتية ، ويمكن الدول المتطورة من ضمان عدم استغلال المجرمين المعلوماتيين ضعف بعض الدول في المجال المعلوماتي تكنولوجيا وقانونا واستخدامها كقاعدة لاعمالهم الاجرامية ، مما يفرض عدم اقتصار عملية المكافحة على الجهود الفردية بسبب طبيعة هذه الجرائم العابرة للحدود.

ملاحـق

ملحق رقم -01
المصطلحات الواردة في الدراسة

البرمجيات الخبيثة (بالإنجليزية: Malware) [1] : هي اختصار لكلمتين هما "software malicious": وتعني البرمجية الماكرة أو الخبيثة، وهي برنامج مخصص للتسلل إلى نظام الحاسب أو تدميره بدون رضا المالك. وما إن تم تثبيت البرمجية الخبيثة فإنه من الصعب جداً إزالتها. وبحسب درجة البرمجية من الممكن أن يتراوح أذاها من إزعاج بسيط (بعض النوافذ الإعلانية الغير مرغوب بها خلال عمل المستخدم على الحاسب متصلاً أم غير متصلا بالشبكة) إلى أذىً غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال. من الأمثلة على البرمجيات الخبيثة هي الفيروسات، وأحصنة طروادة.

برامج التجسس (بالإنجليزية: spyware) [2]: هي برامج حاسوبية تثبت خلسة على أجهزة الحاسب الالي للتجسس على المستخدمين أو لغرض السيطرة الجزئية على الكمبيوتر، وهذا من دون علم المستخدم، وفي حين أن الاسم (برامج التجسس) يشير إلى البرامج السرية التي تراقب سلوك المستخدمين، إلا أن مهامها تتجاوز بكثير مجرد الرصد،فبرامج التجسس يمكنها جمع مختلف المعلومات الشخصية ، مثل تصفح الإنترنت، ورصد المواقع التي تمت زيارتها ، ويمكن لهذه البرامج أيضا أن تسيطر على الكمبيوتر المصاب بها، وتتحكم به وتقوم بعدة مهام، مثل: تركيب برامج إضافية ، تحويل عائدات دعائية لطرف ثالث ، تغيير الصفحة الرئيسية لمستعرض الويب، إعادة توجيه مستعرض الويب، توجيه لمواقع ويب ضارة ومفخخة والتي من شأنها ان تتسبب في المزيد من الفيروسات، كما يمكن أيضا لبرامج التجسس أن تغير إعدادات الكمبيوتر، مما قد يؤدي إلى بطئه والتأثير على الاتصال بشبكة الانترنت.ومثال عن هذه البرامج برنامج **سباي بوت** Spybot.

البوتنت Botnet [3]**:** تقنية خبيثة في مجال تكنولوجيا المعلومات تمكن من التحكم في مجموعة من أجهزة الكمبيوتر المتصلة بشبكة الإنترنت، ، و يتم استخدامها لأغراض خبيثة .
وتستخدم شبكات Botnets الخبيثة في المقام الأول لعدة اغراض :

- ارسال الرسائل غير المرغوب فيها للترويج لتجارة غير مشروعة أو التلاعب بالمعلومات .
- إجراء عمليات الاحتيال بمختلف صورها .
- التعرف على الأجهزة الأخرى عن طريق نشر الفيروسات والبرمجيات الخبيثة (البرامج الخطيرة) .
- توليد نقرات غير صحيحة على صلة الإعلان في صفحة الويب لارغام المتصفح على مشاهدة الاعلان.
- التقاط المعلومات على أجهزة الكمبيوتر من اجل سرقتها او بيعها او استعمالها في ابتزاز الضحية.
- إرسال عدد كبير من الفيروسات لتوقيف الخادم عن العمل .

- **برامج التشمم** (بالإنجليزية Sniffer) [4] : برامج تستخدم لقرصنة البريد الألكتروني والحصول على كلمة السر وكل المعطيات المتداولة ، كما تسجل كل صفحات الويب التي زارها الضحية .

---

[1] انظر في الموقع : http://en.wikipedia.org/wiki/Malware

[2] انظر في الموقع : http://en.wikipedia.org/wiki/spyware

[3] انظر في الموقع : http://en.wikipedia.org/wiki/Botnet

[4] انظر في الموقع : http://erictechnicien.com/spywares.html

- برامج كيلوغر (بالإنجليزية Keylogger) [1] : هو برنامج لتسجيل النقرات على لوحة المفاتيح وحفظها، دون علم المستخدم ، او كما يسمى **راصد لوحة مفاتيح** فهو أحد برامج التجسس وهو مخفي يرسل عبر البريد الالكتروني اويتم تحميله من أحد المواقع غير الموثوقة أو يكون ضمن البرامج المجانية ، حيث يقوم برنامج التجسس بنقل كافة ما يكتب بلوحة المفاتيح إلى جهات بعيدة عادة إلى صاحب التجسس أو مرسل البرنامج ، فهو أخطر هذه البرامج ويستخدم لمراقبة أجهزة معينة ومعرفة ما يكتب عليها، مثل ارقام السر وكلمات الدخول ارقام بطاقات الائتمان، ويمكنه تسجيل عناوين المواقع التي تمت زيارتها ، أو الوصول إلى رسائل البريد الإلكتروني المرسلة، فتح الملفات أو حتى إنشاء شريط فيديو يصور كل نشاط على الكمبيوتر.

- **البريد المزعج** (بالإنجليزية: E-mail Spam) [2] : هوإرسال كم كبير من البريد الإلكتروني غير المرغوب فيها الى المتلقين دون طلب منهم ، ويكون ذلك لغرض الدعاية في معظم الاوقات.

- **التشفير** (بالإنجليزية: encryption) [3]: هي عملية تحويل المعلومات التي تكون بشكل نص بسيط عند التخزين على وسائط التخزين المختلفة أو عند نقلها على الشبكات بحيث تصبح غير مقروءة لأحد باستثناء من يملك معرفة خاصة أو مفتاح خاص لإعادة تحويل النص المشفر إلى نص مقروء و عملية الفك هذه تتم عن طريق ما يدعى المفتاح ، ونتيجة عملية التشفير تصبح المعلومات مشفرة وغير متاحة لأي أحد مشفرة وغير متاحة لأي أحد و يستعمل التشفير لأغراض سرية عسكرية أو سياسية أو أمنية و تعاكس هذه العملية عملية فك التشفير (decryption) وهي عملية استخدام المفتاح لإعادة النص المشفر إلى نص مقروء. [3]

- حصان طروادة (بالإنجليزية Trojan Horse)[4] **:** عبارة عن شفرة صغيرة يتم تحميلها لبرنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية ، غالبا ما تتركز على إضعاف قوى الدفاع لدى جهاز الضحية ليسهل اختراقه وسرقة بياناته.
و حتى تتمكن أحصنة طروادة من تنفيذ مهمتها يجب أن يكون بمقدورها أن تعمل بدون أن يتم إغلاقها من المستخدم أو مدير النظام التي تعمل عليه، فالاختفاء هو الطريقة التي تساعد حصان طروادة على بدء العمل في النظام، فعندما يظن المستخدم أن هذا البرنامج بريء أو مرغوب به، قد يتحفز المستخدم لتنصيب البرنامج دون أن يعلم ما الذي يقوم بعمله هذا البرنامج. وهذه هي التقنية التي يستخدمها حصان طروادة.

وعلى العموم، فحصان طروادة هو أي برنامج يدعو المستخدم لتشغيله لكنه يخفي في الحقيقة أذى أو نتائج سيئة كأن يتم حذف جميع ملفات المستخدم، أو يقوم بتنصيب برنامج مؤذي في نظام المستخدم لتخدم أهداف الجاني على المدى البعيد.
اما سبب التسمية فيرجع لتشابه عمله مع أسطورة حصان طروادة الخشبي الذي اختبأ به عدد من الجنود اليونانيون وكانوا سببا في فتح مدينة طروادة.

---

[1] انظر في الموقع : http://www.commentcamarche.net/contents/virus/keylogger.php3

[2] انظر في الموقع :http://fr.wikipedia.org/wiki/Spam

[3] انظر في الموقع : http://www.larousse.fr/encyclopedie/nom-commun-nom/cryptographie/38869

[4] انظر في الموقع :http://en.wikipedia.org/wiki/Trojan Horse

- رسائل التصيد (بالإنجليزية Phishing) [1] : هي رسائل تصل عير البريد الالكتروني تحمل برامج خبيثة هدفها التجسس لحساب مرسلها ، ويتم استخدام برامج خاصة لتغيير اسم مرسل الرسائل اذ غالبا ما يستعمل اسم بنك معين أو موقع مشهور ويتم استدعاء الضحية للتسجيل في الموقع أو ربما اعطائه برنامج جديد للتجربة اوالقيام باجراء عملية تنظيف لجهازه فيقع ضحية لهم من خلال سرقة معلوماته الخاصة او كلمات المرور الخاصة به.

- عنوان بروتوكول الإنترنت (بالإنجليزية IP Adresse) [2] **:** هو المعرف الرقمي او رقم التعريف لأي جهاز (حاسوب ، هاتف محمول، آلة طابعة،...إلخ) مرتبط بشبكة معلوماتية تعمل بحزمة بروتوكولات الإنترنت، سواء أكانت شبكة محلية أو شبكة خارجية .

-**البروتوكول TCP** [3]**:** هو بروتوكول يقوم بنقل المعلومات فهو المسؤول عن تدقيق صحة نقل المعلومات من الحاسب الى الخادم حيث يتعرف على الاخطاء ويقوم باعادة الارسال بشكل صحيح .

وقد تم تطوير البروتوكول TCP /IP من قبل هيئة البحوث التابعة لوزارة الدفاع الامريكية لوصل عدد من الشبكات المختلفة من الانظمة ضمن شبكة واحدة ، فكان نتية هذا الوصل نشأة شبكة الانترنت ، و يؤمن البروتوكول TCP /IP عملية نقل المعلومات من الحاسب الالي الى الشبكة الرئيسية ثم الى الشبكات الاقليمية و أخيراالى شبكة الانترنت ، وله القدرة على العمل أوتوماتيكيا فالانترنت ليس لها مركز يتحكم في ادارتها .

- **قواعد البيانات** (بالإنجليزية Database) [4] : مجموعة الملفات التي تحتوي الكثير من المعلومات المخزنة في جهاز الكمبيوتر حيث يتم استخدام قاعدة البيانات للتمكن من معالجة بسهولة المحتوى وتخزين بكفاءة كميات كبيرة جدا من المعلومات ويتم تنظيم قاعدة بيانات في نموذج بيانات محددة سلفا وفقا لنوع المعلومات التي سيتم تخزينها. الهيكل المادي من الملفات يحتوي على فهارس لتسريع عمليات البحث والفرز

- الكراكر (بالإنجليزية cracker)[5] : هو نوع من قراصنة الاعلام الالي ، متخصص في كسر حواجزالامن المصممة لحماية البرمجيات التي تتطلب كلمات مرور.

- الهاكر (بالإنجليزية Hacker) [6] : هاكر كلمة إنجليزية تعني" بارع"، تستخدم في مجال الاعلام الالي لوصف الشخص الذي يتمتع بالذكاء والمهارة من مبرمجي الكمبيوتر ، والذي من خلال معرفته الفنية يتمكن من تعديل برنامج بشكل يختلف عن ما كان مخططا له أصلا.

---

[1] انظر في الموقع : http://fr.wikipedia.org/wiki/Phishing

[2] انظر في الموقع : http://fr.wikipedia.org/wiki/Adresse_IP

[3] انظر في الموقع :http://ecommercetechnologiy.org/data/25.htm

[4] انظر في الموقع :http://fr.wikipedia.org/wiki/Base_de_donn%C3%A9es

[5] انظر في الموقع : http://fr.wikipedia.org/wiki/Cracker

[6] انظر في الموقع : http://fr.wikipedia.org/wiki/Hacke

ملحق رقم 02

تقرير مركز الشكاوي عن جرائم الانترنت لسنة 2009

Internet Crime Complaint Center

2009 Internet Crime Report

INTERNET CRIME COMPLAINT CENTER

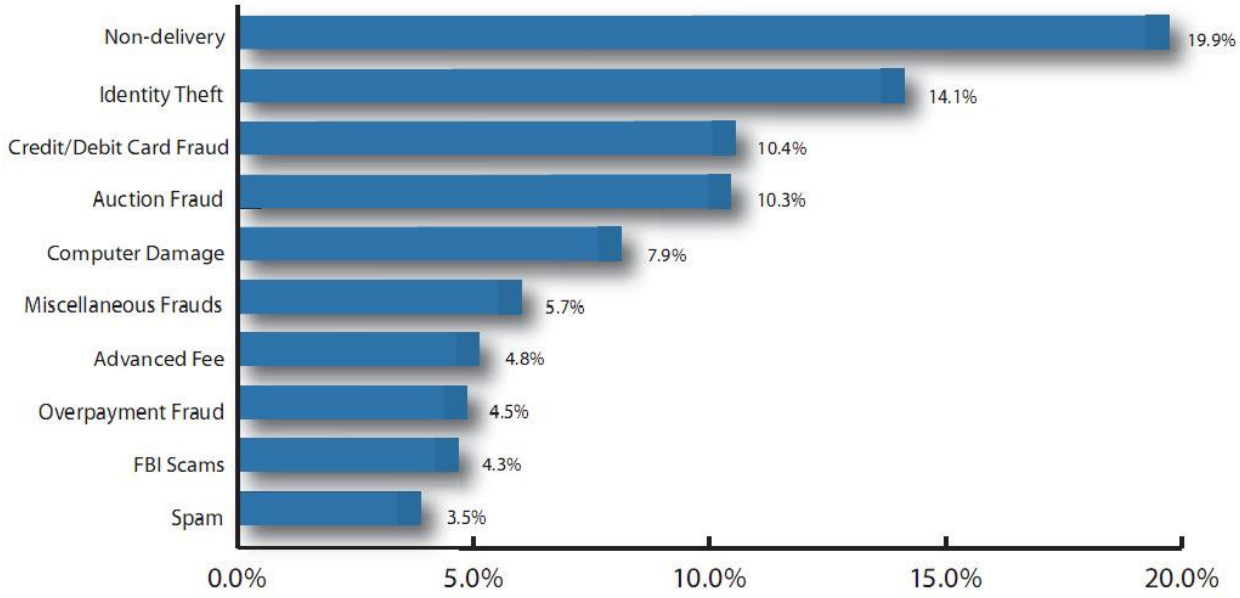
Executive Summary

From January 1, 2009 through December 31, 2009, the Internet Crime Complaint Center (IC3) Web site received 336,655 complaint submissions. This was a 22.3% increase as compared to 2008 when 275,284 complaints were received. Of the 336,655 complaints submitted to IC3, 146,663 were referred to local, state, and federal law enforcement agencies around the country for further consideration. The vast majority of referred cases contained elements of fraud and involved a financial loss by the complainant. The total dollar loss from all referred cases was $559.7 million with a median dollar loss of $575. This is up from $264.6 million in total reported losses in 2008. Unreferred submissions generally involved complaints in which there was no documented harm or loss (e.g., a complainant received a fraudulent solicitation email but did not act upon it) or complaints where neither the complainant nor perpetrator resided within the United States (i.e., there was not an appropriate domestic law enforcement agency for direct referral).

Figure 1 : Yearly Dollar Loss (in millions) of Referred Complaints

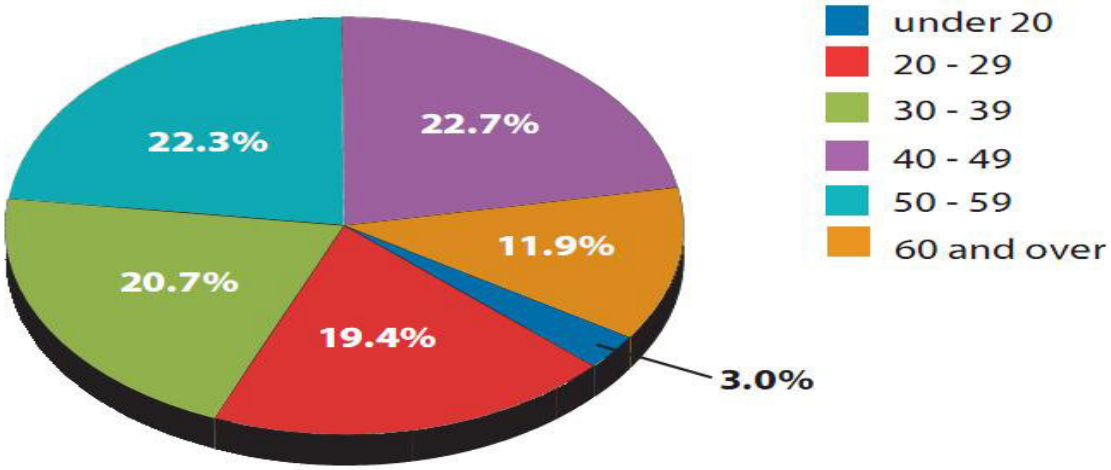
يبين تقريرمركزالشكاوي عن جرائم الانترنت في العالم حجم الخسائر المالية نتيجة لجرائم الانترنت، واغلبها للاحتيال المعلوماتي سنة 2009 ، والتي بلغت 559,7 مليون دولار امريكي مقابل 264,6 مليون دولار امريكي سنة 2008 ، غير ان اكثر من90 % من المبلغين هم من مواطني الولايات المتحدة الأمريكية رغم ان المركز عالمي و يتلقى البلاغات من كل دول العالم.

Figure2 : 2009 Top 10 Most Referred IC3 Complaint Categories (Percent of Total Complaints Referred)



يبين تقريرمركزالشكاوي عن جرائم الانترنت لسنة 2009 ترتيب نسب الجرائم المعلوماتية المبلغ عنها، حيث كانت جريمة عدم تسليم السلعة في صدارة الترتيب، تليها سرقة الهوية ثم الاحتيال في البطاقات الائتمانية ثم الاحتيال في المزادات العلنية، تليه جريمة الاتلاف المعلوماتي ثم انواع اخرى من الاحتيال المعلوماتي واخيرا جريمة اغراق البريد الالكتروني بالرسائل .

Figure 3 : Age of Complainant



يبين التقرير ان اكبر فئة عمرية للمبلغين عن الجرائم تبلغ اعمارهم بين 40 سنة و 49 سنة واقل نسبة للمبلغين عن الجرائم هي فئة الشباب اقل من 20 سنة.

ملحق رقم 03

مشروع القرار الخامس حول مكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية في مؤتمر منظمة الامم المتحدة المنعقد بتاريخ 16 نوفمبر 2000 حول منع الجريمة و العدالة الجنائية

الأمم المتحدة
A/55/593
الجمعية العامة
Distr.: General
16 November 2000
Arabic
Original: English

الدورة الخامسة و الخمسون
البند ١٠٥ من جدول الأعمال

منع الجريمة و العدالة الجنائية

مشروع القرار الخامس

مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية

إن الجمعية العامة،

إذ تشير إلى إعلان الألفية للأمم المتحدة [٢٥] الذي تعتزم فيه الدول الأعضاء كفالة إتاحة منافع التكنولوجيا الجديدة، وبخاصة تكنولوجيا المعلومات و الاتصالات للجميع ، بما يتفق و التوصيات الواردة في الإعلان الوزاري الصادر عن الجزء الرفيع المستوى من دورة المجلس الاقتصادي و الاجتماعي [٢٦] ،

واذ تشير ايضا الى قرارها ٥٤ / ١٢١ المؤرخ في ١٤ كانون الاول / ديسمبر ١٩٩٠ ،الذي ايدت فيه توصيات نؤتمر الامم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين [٢٧] ، واذ تشير بصورة خاصة الى القرار المتعلق بالجرائم ذات الصلة بالحواسيب [٢٨] ، الذي دعا فيه المؤتمر الثامن الدول الى تكثيف جهودها لمكافحة اساءة استعمال الحواسيب بفعالية اكبر،

واذ تشدد على المساهمات التي يمكن ان تقدمها الامم المتحدة ، لاسيما لجنة الامم المتحدة لمنع الجريمة و العدالة الجنائية ،في الترويج لمزيد من الفعالية و الكفاءة في انفاذ القوانين وفي اقامة العدل، و لاعلى مستويات النزاهة و الكرامة الانسانية،

واذ تسلم بان حرية تدفق المعلومات يمكن ان تعزز التنمية الاقتصادية و الاجتماعية و التعليم و الحكم الديمقاطي ،

واذ تشير الى اوجه التقدم الكبير في استحداث تكنولوجيا المعلومات و وسائل الاتصالات السلكية و اللاسلكية و تطبيقها ،

---

[٢٥] القرار ٥٥/٢

[٢٦] الوثائق الرسمية للجمعية العامة ،الدورة الخامسة و الخمسون، الملحق رقم ٣ (A/55/3/Rev.1)،الفصل الثالث.

[٢٧] مؤتمر الامم المتحدة الثامن لمنع الجريمة و معاملة المجرمين،هافانا ،٢٧ اب/اغسطس-٧ايلول/سبتمبر ١٩٩٠.
(منشورات الامم المتحدة،رقم المبيع A.91.IV.2)، الفصل الاول.

[٢٨] المرجع نفسه، الفصل الاول، الفرع جيم، القرار ٩٠.

واذ تعرب عن القلق ازاء الامكانيات الجديدة التي يتيحها التقدم التكنولوجي للنشاط الاجرامي ، لاسيما اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية،

واذ تلاحظ ان الاعتماد على تكنولوجيا المعلومات، على الرغم من احتمال اختلافه من دولة الى اخرى، قد حقق زيادة كبرى في التعاون و التنسيق على المستوى العالمي،مما قد يؤدي في حالة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية الى التاثير على نحو خطير على جميع الدول،

واذ تسلم بان الثغرات في مجال حصول الدول على تكنولوجيا المعلومات واستخدامها يمكن ان يضعف فعالية التعاون الدولي في مكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية ، واذ تلاحظ الحاجة الى تيسير نقل تكنولوجيا المعلومات بخاصة في البلدان النامية،

واذ تلاحظ ضرورة منع اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية ،

واذ تسلم بالحاجة الى تعاون الدول مع القطاع الخاص لمكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية ،

واذ تشدد على الحاجة الى تعزيز التنسيق و التعاون بين الدول لمكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية ، مؤكدة في هذا السياق على الدور الذي يمكن ان تقوم به الامم المتحدة و المنظمات الاقليمية،

واذ ترحب باعمال مؤتمر الامم المتحدة العاشر لمنع الجريمة و معاملة المجرمين الذي عقد في فينا من ١٠الى ١٧ نيسان/افريل ٢٠٠٠ [٢٩]،

واذ تحيط علما بعمل لجنة الخبراء المعنية بالجرائم و الفضاء الحاسوبي التابعة لمجلس اوروبا بشان مشروع اتفاقية تتعلق بجرائم الفضاء الحاسوبي ، والى المبادئ التي اتفق عليها وزراء داخلية مجموعة الثمانية في واشنطن، العاصمة في ١٠كانون الاول / ديسمبر ١٩٩٧ والتي ايدها رؤساء دول مجموعة الثمانية في برمنغهام، المملكة المتحدة لبريطانيا العظمى و ايرلندا الشمالية ، في ايا ر/مايو ١٩٩٨، واعمال مؤتمر مجموعة الثماني الذي عقد في باريس من ١٥ الى ١٧ ايار/مايو ٢٠٠٠ بشأن اقامة حوار بين الحكومات والقطاع الصناعي بشأن السلامة والثقة في الفضاء الحاسوبي والتوصيات التي اقرها في ٢ اذار/ مارس ٢٠٠٠ الاجتماع الثالث لوزراء العدل او الوزراء او المدعين العامين في الامريكيتين ، الذي عقد في كوستاريكا من ١الى ٣ اذار /مارس ٢٠٠٠ في اطار منظمة الدول الامريكية،

-١- تلاحظ مع التقدير الجهود التي تبذلها الهيئات المذكورة اعلاه من اجل منع اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية، كما تلاحظ قيمة امور منها التدابير التالية الرامية الى مكافحة هذا النوع من اساءة الاستعمال لتكنولوجيا المعلومات :

(أ) ينبغي ان تكفل الدول عدم توفير قوانينها وممارساتها ملاذا امنا للذين يسيئون استعمال تكنولوجيا المعلومات لاغراض اجرامية،

(ب) ينبغي ان تنسق جميع الدول المعنية التعاون في مجال انفاذ القانون لدى التحقيق والمقاضاة في القضايا الدولية المتعلقة باساءة استخدام تكنولوجيا المعلومات لاغراض اجرامية،

(ج) ينبغي ان تتبادل الدول المعلومات المتعلقة بالمشاكل التي تواجهها في مكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية،

(د) يتعين تدريب العاملين على انفاذ القوانين وتجهيزهم بما يمكنهم من مكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية،

(هـ) ينبغي ان تحمي النظم القانونية سرية البيانات ونظم الحواسيب وسلامتها وتوفرها، من أي عرقلة غير مأذون بها، وان تضمن معاقبة من يقوم باساءة استعمالها لاغراض اجرامية،

(و) ينبغي ان تيسر النظم القانونية حفظ البيانات الالكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الحصول عليها،

---

[٢٩] انظر A / CONF.187/15.

(ز) ينبغي ان تضمن نظم المساعدة المتبادلة التحقيق في الوقت المناسب في اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية وجمع الادلة في مثل هذه الحالات وتبادلها في الوقت المناسب،

(ح) ينبغي توعية عامة الناس بضرورة منع اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية ومكافحتها،

(ط) ينبغي قدر الامكان تصميم تكنولوجيا المعلومات بطريقة تساعد على منع اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية و الكشف عنها وترقب المجرمين وجمع الادلة،

(ي) تقتضي مكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية وضع حلول تاخذ في عين الاعتبار حماية حريات الافراد وحياتهم الخاصة والمحافظة على قدرة الحكومات على مكافحة هذا النوع من اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية،

٢- تدعو الدول الى اذ هذه التدابيرالمذكورة اعلاه في الاعتبار في جهودها الرامية الى مكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية،

٣ - تقرر ابقاء مسألة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية على جدول اعمال دورتها السادسة و الخمسين ضمن البند المعنون " منع الجريمة و العدالة الجنائية "

ملحق رقم 04

قرارات قضائية صادرة عن محكمة النقض الفرنسية

1 - قرار قضائي صادر عن الغرفة الجنائية بمحكمة النقض الفرنسية بتاريخ 27 اكتوبر سنة 2009 ، يرفض الطعن المقدم من طرف السيد (س) ضد قرار غرفة الجنح بمحكمة استئناف مونبولييه الصادر بـ 12 مارس 2009 والتي أدانته بتهمة المساس بنظام المعالجة الالية للمعطيات وفق المواد 323-1 ، 323-2 و323-3 من قانون العقوبات الفرنسي و حكمت عليه بغرامة 1000 اورو، وذلك لقيامه بشكل غير مشروع بتوزيع برنامج على موقعه الالكتروني يسهل القيام باختراق و قرصنة انظمة المعالجة الالية للمعطيات.

وقد اسس الجاني طعنه على خرق محكمة الاستئناف للمادة 8 من الاعلان العالمي لحقوق الانسان، والمادة 6 و 7 من الاتفاقية الاوروبية لحقوق الانسان، وكذا المادة 6 من الاتفاقية الاوروبية للجرائم المعلوماتية ، والمواد 34 و37 من الدستور و المواد 323-1 ،323-2و 323-3 و111-3 و 121-3 من قانون العقوبات ، و المواد 591 و593 من قانون الاجراءات الجزائية لانعدام الاساس القانوني للجريمة مبرزا حسن نيته و عدم وجود القصد الجنائي لارتكاب هذه الجريمة ، إلا أن الغرفة الجنائية بمحكمة النقض قد رفضت هذا الطعن وأيدت قرارالغرفة الجزائية بمحكمة الاستئناف التي اعتبرت أن معرفة الجاني وخبرته في مجال المعلوماتية تمكنه من ادراك أن ما يقوم بتوزيعه ونشره هو برنامج خطير لاختراق أنظمة المعالجة الالية للمعطيات وان هناك الكثير من الاشخاص يهمهم الحصول على هذا النوع من البرامج وبالتالي أن محكمة الإستئناف طبقت القانون تطبيقا صحيحا ، وهذا نص قرار رفض الطعن:

Cour de cassation
chambre criminelle
Audience publique du 27 octobre 2009
N° de pourvoi: 0982346
Publié au bulletin
REPUBLIQUE FRANCAISE
AU NOM DU PEUPLE FRANCAIS

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par : X...,contre l'arrêt de la cour d'appel de MONTPELLIER, chambre correctionnelle, en date du 12 mars 2009,

qui, pour mise à disposition, sans motif légitime, de moyens conçus ou spécialementadaptés pour commettre **une atteinte à un système de traitement automatisé de données**,l'a condamné à 1000 euros d'amende ;

Vu le mémoire produit ;

Sur le moyen unique de cassation, pris de la violation des articles 8 de la Déclaration des droits de l'homme, 6 et 7 de la Convention européenne des droits de l'homme, [*l'article*] 6 de la Convention européenne sur la cybercriminalité du 23 novembre 2001, 34 et 37 de la Constitution, 323-1,323-2,323-3et [l'article] 323-3-1du code pénal, 111-3 et 121-3du code pénal, 591 et 593 du code de procédure pénale, défaut de motifs et manque de base légale ;

"en ce que l'arrêt infirmatif [de la cour d'appel de Montpellier] attaqué a déclaré X...coupable de mise à disposition sans motif légitime de programmes ou données conçus ou adaptés pour une

atteinte au fonctionnement d'un système de traitement automatisé de données, et, en répression, l'a condamné à une peine d'amende de 1000 euros ;
"aux motifs que le tribunal [de première instance] a relaxé X... au motif qu'il est établi que le site « www… » n'incitait en aucune façon à l'utilisation de ces codes à des fins malveillantes ou de piratage informatique ; que la seule intention qui ait animé X... est un souci d'information des menaces existantes non corrigées à destination des utilisateurs de programmes informatiques ; qu'il justifie d'ailleurs en avoir été remercié par Microsoft ; qu'aucune intention n'est établie ;
que [toutefois] l'article 323-3-1 du code pénal [créé par la LCEN article 46] réprime le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre des atteintes aux systèmes de traitement automatisé des données, sans que le texte n'exige que soit caractérisée une incitation à l'utilisation d'un tel système ;que, s'agissant du motif légitime exonératoire, la cour estime que X... ne peut valablement arguer d'un motif légitime tiré de la volonté d'information dès lors que, par la mise en place d'un système de veille destiné à des abonnés et par la communication d'informations d'alerte directement à Microsoft à son adresse email, X... a fait la preuve de ce qu'il connaissait les dispositifs permettant de concilier le souci d'information avec la nécessaire confidentialité de ce type d'informations, étant précisé que X..., selon ses propres déclarations, n'a pas été remercié par Microsoft pour avoir publié sur le site web les exploits le concernant mais pour l'avoir avisé directement à son adresse mail des failles existantes ;que, s'agissant de l'élément intentionnel de l'infraction, X... ne peut arguer de sa bonne foi ; alors que la fréquentation de son site par un public tout venant lui procurait des revenus publicitaires adossés au nombre de visiteurs ; qu'en conséquence, il est établi qu'il avait un intérêt économique à la diffusion d'informations dont il ne pouvait ignorer, du fait de son expertise en cette matière et ses antécédents judiciaires, qu'elles présentaient un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance ; qu'il y a lieu, en conséquence, d'infirmer le jugement déféré et de déclarer X...coupable de l'infraction poursuivie ;que, sur la peine, la cour constate que X... a développé son activité de conseil en matière de sécurité informatique ; qu'eu égard à sa personnalité et à sa progression professionnelle, il y a lieu d'être modéré dans la répression et de le condamner à une peine d'amende de 1 000 euros ;
"1°) alors qu'il n'y a point de délit sans intention de le commettre ;que toute infraction doit être définie en des termes clairs et précis pour exclure l'arbitraire et permettre au prévenu de connaître exactement la nature et la cause de l'accusation portée contre lui, que la Convention européenne sur la cybercriminalité réprime en son article 6, d'une part, la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, soit d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci dessus, soit d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5, et, d'autre part, la possession d'un élément visé aux paragraphes ci dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 ; qu'elle ajoute que cet article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie

conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique ;
qu'en s'en référant, pour retenir la culpabilité de X..., à l'article 323-3-1 du code pénal dont les termes généraux établissent une responsabilité pénale en l'absence de toute intention frauduleuse, la cour d'appel n'a pas légalement justifié la condamnation prononcée ;
"2°) alors qu'il n'y a point de délit sans intention de le commettre ; qu'en ne caractérisant pas de la part de X... une intention spécifique de diffuser les informations litigieuses dans le but précis de permettre la commission de l'une ou l'autre des infractions visées aux articles 323-1 à 323-3 du code pénal, la cour d'appel a privé sa décision de base légale au regard des textes susvisés ;
"3°) alors que, en se bornant, pour caractériser l'élément intentionnel de l'infraction reprochée à X..., à s'en référer à son intérêt économique et à considérer que les informations diffusées sur son site présentaient un risque d'utilisation à des fins de piratage, sans rechercher, ne seraitce que pour écarter cette éventualité, si,nonobstant la conscience qu'il avait de l'existence d'un tel risque, X... n'avait pas été seulement animé de l'intention de remédier à une insécurité informatique, la cour d'appel a privé sa décision de base légale au regard des textes susvisés ;
"4°) alors que, de surcroît, en s'en référant, pour caractériser l'élément intentionnel de l'infraction, aux antécédents judiciaires de X..., sans mieux s'expliquer sur ce point au regard des circonstances de l'espèce, la cour d'appel, qui a statué par des motifs abstraits et généraux, a privé sa décision de base légale au regard des textes susvisés" ;
Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que X... a diffusé sur le portail internet de la société XX Consulting, spécialisé dans le conseil en sécurité informatique, dont il est le gérant, des écrits directement visibles sur le site et accessibles à tous permettant d'exploiter des failles de sécurité informatique ; que, renvoyé devant le tribunal correctionnel pour mise à disposition, sans motif légitime, de moyens conçus ou spécialement adaptés pour commettre une atteinte à un système de traitement automatisé de données, il a été relaxé ;
Attendu que, pour infirmer, sur appel du ministère public, le jugement et condamner le prévenu, l'arrêt énonce qu'il ne peut valablement arguer d'un motif légitime tiré de la volonté d'information, dès lors que, du fait de son expertise en la matière, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance ;
Attendu qu'en l'état de ces énonciations, abstraction faite du motif surabondant relatif aux antécédents judiciaires du prévenu, et dès lors que la constatation de la violation, sans motif légitime et en connaissance de cause, de l'une des interdictions prévues par l'article 323-3-1 du code pénal implique de la part de son auteur l'intention coupable exigée par l'article 121-3 du même code,
la cour d'appel a justifié sa décision ;
D'où il suit que le moyen doit être écarté ;
Et attendu que l'arrêt est régulier en la forme ;
REJETTE le pourvoi ;
Ainsi jugé et prononcé par la Cour de cassation, chambre criminelle, en son audience publique, les jour, mois et an que dessus ;**La Cour** : Mme Anzani (président), M. Guérin (conseiller rapporteur), Mme Palisse (conseiller de la chambre) ;
Avocat : SCP Nicolay, De Lanouvelle et Hannotin.

2 - قرار قضائي صادر عن الغرفة الجنائية بمحكمة النقض الفرنسية بتاريخ 29 نوفمبر2011 تم فيه نقض قرارصادر عن محكمة استئناف باريس بتاريخ 5 نوفمبر 2009 و الذي أدان بجنحة التقليد عبر شبكة الانترنت "F. Giuliano" و ذلك لقيامه باعادة انتاج مقال لكاتب ايطالي"T.Antonio " حرره لفائدة اليومية الفرنسية "Le Monde " غير انه في اليوم الذي يسبق صدور المقال على الجريدة الفرنسية نشر على جريدة ايطالية "Il Foglio " بدون رضا صاحب المقال ، وعلى هذا الاساس أدانت محكمة استئناف باريس الجريدة الايطالية وحكمت عليها بغرامة 10.000 اورو عن جنحة تقليد عن طريق نشر أو اعادة انتاج مصنف محمي بحقوق المؤلف وفق المادة L. 335-2 وما يليها من قانون الملكية الفكرية ، إلا أن محكمة النقض استندت على المادة 113 من قانون العقوبات الفرنسي و التي تنص على أن قانون العقوبات يطبق على الجرائم المرتكبة فوق تراب الجمهورية و يعتبر كذلك متى كانت احدى عناصر الجريمة مرتكبة فوق تراب الجمهورية الفرنسية ولأن الجريدة الايطالية مدونة باللغة الايطالية و موجهة إلى الجمهور الايطالي و أنها غير موزعة بصورتها الورقية على التراب الفرنسي و أن ادارة الموقع كانت في ايطاليا، فاعتبرت أن احكام جنحة التقليد لا تنطبق عليها لأنها مرتكبة خارج التراب الفرنسي و نقضت القرار. وفيما يلي نص القرار:

Cour de cassation
Chambre criminelle
Date de la décision: mardi 29 novembre 2011
N°: 09-88250
Publié au bulletin
Solution: Cassation sans renvoi

Président: M. Louvel
Rapporteur: Mme Harel-Dutirou
Avocat général: M. Cordier
Avocats en présence: Me Copper-Royer, SCP Hémery et Thomas-Raquin

REPUBLIQUE FRANCAISE
AU NOM DU PEUPLE FRANCAIS

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :
Statuant sur le pourvoi formé par : M. Giuliano X..., contre l'arrêt de la cour d'appel de PARIS, chambre 5-13, en date du 5 novembre 2009, qui, pour **contrefaçon par édition ou reproduction** d'une oeuvre de l'esprit au mépris des droits de l'auteur et contrefaçon par diffusion ou représentation d'une oeuvre de l'esprit au mépris des droits de l'auteur, l'a condamné à 10 000 euros d'amende, et aProno ncé sur les intérêts civils ;
La COUR, statuant après débats en l'audience publique du 15 novembre 2011 où étaient présents :
M. Louvel président, Mme Harel-Dutirou conseiller rapporteur, MM. Arnould, Le Corroller, Nunez, Mme Radenne, M. Fossier, Mme Mirguet conseillers de la chambre, M. Roth conseiller référendaire
Avocat général : M. Cordier ; Greffier de chambre : Mme Leprey ;
Sur le rapport de Mme le conseiller référendaire HAREL-DUTIROU, les observations de la société civile professionnelle HÉMERY et THOMAS-RAQUIN, de Me COPPER-ROYER, avocats en la Cour, et les conclusions de M. l'avocat général CORDIER ;
Vu les mémoires produits en demande et en défense ;
Sur le moyen unique de cassation, pris de la violation des articles L. 121, L. 121-8, L. 122-4, L. 335-2, L. 335-3 du code de la propriété intellectuelle, 5, alinéa 2, de la Convention d'union

de Berne, 111-2, 111-3, 113-2 et 113-7 du code pénal, 593 et 689 du code de procédure pénale, défaut de motifs et manque de base légale ;
" en ce que l'arrêt attaqué a rejeté l'exception d'incompétence des juridictions françaises soulevée par M. X..., l'a déclaré coupable des faits de contrefaçon qui lui était reprochés et a confirmé le jugement déféré sur la peine et en toutes ses dispositions civiles ;
" aux motifs qu'en ce qui concerne le critère de compétence lié à la commission de l'infraction, qu'il ressort de la procédure et des éléments fournis par le conseil de M. X...que la publication critiquée de l'article de M. Y... a eu lieu en Italie ; que le journal IL Foglio n'était pas diffusé en France au moment des faits ; que le site internet accessible à partir de l'adresse www. illfoglio. it était exclusivement rédigé en langue italienne et vise le public italien ; que le site internet ne permettait pas de commander le journal IL Foglio à partir du territoire français ; que la seule accessibilité au site internet et la lecture d'articles du journal dans sa langue d'origine ne permettent pas d'établir un lien suffisant, substantiel ou significatif avec le pays dont la loi de protection est revendiquée ; qu'il n'existe pas de critère de rattachement suffisamment étroit avec le territoire national français ; qu'il convient de retenir que les faits n'ont pas été commis en France mais en Italie ; qu'il ressort de l'article 113-7 du code pénal que lorsque la victime est française au moment de l'infraction, la loi française est également applicable à tout délit commis hors du territoire de la République ; qu'en l'espèce, le délit a été commis sur le territoire italien mais l'une des victimes, la société éditrice du Monde, est une personne morale de nationalité française ; qu'il est de jurisprudence constante que le désistement de la partie civile est sans conséquence sur la mise en oeuvre de l'action publique ; que, par ailleurs, le journal Le Monde n'a pas perdu sa qualité de victime par l'effet de son désistement de partie civile, ces deux notions étant juridiquement distinctes, le journal Le Monde ayant toujours subi un préjudice certain, direct et personnel ; qu'enfin, l'article 113-8 du code pénal dispose que, dans l'hypothèse où la compétence française est retenue en raison de la nationalité française de la victime, la poursuite appartient au seul ministère public ; que la plainte avec constitution de partie civile n'a pas été déclarée irrecevable, l'action publique ayant été mise en mouvement par un réquisitoire introductif en date du 2 mars 2004 ; qu'enfin le ministère public a requis le renvoi de M. X...devant le tribunal correctionnel ; qu'en conséquence, qu'en application de l'article 137 (sic lire 113-7) du code pénal, la compétence de la juridiction française doit être retenue en raison de la nationalité française de la personne morale, la société éditrice du Monde, alors que les faits ont été commis en Italie ;
1) alors que l'article 113-7 du code pénal constitue une loi de compétence internationale et non une loi d'incrimination ; que son application nécessite donc que la loi pénale française sanctionne les faits incriminés et poursuivis, le juge pénal français qui ne peut appliquer la loi étrangère n'étant compétent que si la loi française est applicable ; que l'étendue de la protection ainsi que les moyens de recours garantis à l'auteur pour sauvegarder ses droits se règlent d'après la loi du pays où se sont produits les agissements incriminés ; que la loi française n'incrimine ainsi que les faits de contrefaçon d'une oeuvre de l'esprit commis sur le territoire français ; qu'en l'espèce, la cour d'appel a constaté que les faits de contrefaçon « n'ont pas été commis en France mais en Italie » ; qu'en retenant néanmoins la compétence des juridictions françaises pour en connaître, au motif que la loi française serait applicable à tout délit commis hors du territoire de la République lorsque la victime est française au moment de l'infraction et que tel serait le cas de la société éditrice du Monde, bien que le délit de contrefaçon de droit d'auteur ne soit incriminable par la loi française que si les faits ont été commis sur le territoire français, la cour d'appel a violé les textes susvisés ;
2) alors que nul ne peut être puni pour un délit dont les éléments ne sont pas définis par la loi ; que la loi française n'incrimine que les faits de contrefaçon d'une oeuvre de l'esprit commis sur le territoire français ; qu'en déclarant en l'espèce M. X...coupable du délit de contrefaçon de droit d'auteur, tout en constatant que les faits incriminés n'ont pas été commis en France mais en Italie, la cour d'appel a violé les textes susvisés " ;

Vu l'article 5 § 2 de la Convention pour la protection des oeuvres littéraires et artistiques du 9 septembre 1886 et les articles L. 335-2 et suivants du code de la propriété intellectuelle ;
Attendu qu'il résulte de ces textes que, d'une part, la protection dûe à tout auteur d'un pays unioniste est exclusivement dévolue à la législation du pays où elle est réclamée, cette dernière désignant la loi de l'Etat sur le territoire duquel se sont produits les agissements délictueux et non celle du pays où le dommage a été subi ; que, d'autre part, la perprétation de la contrefaçon sur le territoire de la République est un élément constitutif de l'infraction ;
Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que M. X..., de nationalité italienne, a été renvoyé devant le tribunal correctionnel pour avoir, sur le territoire italien et sur le territoire français, sans l'accord de l'auteur, M. Y... , de même nationalité, et sans l'accord du journal français Le Monde, éditeur exclusif, d'une part, reproduit, dans la parution des éditions papier et électronique du quotidien italien Il Foglio, un texte destiné à l'exclusivité du journal Le Monde intitulé Fatwa à l'italienne, d'autre part, diffusé cet article en tous points de distribution des éditions papier et électronique du même quotidien ; que le tribunal, qui a rejeté l'exception d'incompétence des juridictions françaises opposée par le prévenu, a déclaré celui-ci coupable des faits reprochés et a prononcé sur les intérêts civils ; que, sur appel de M. X..., la cour d'appel a confirmé cette décision que, par arrêt du 9 septembre 2008, la Cour de cassation a cassé cet arrêt au motif que la juridiction du second degré n'avait pas vérifié si les faits avaient été commis en France ; que, par arrêt du 5 novembre 2009, la cour d'appel a confirmé le jugement entrepris ;
Attendu que pour déclarer la loi française applicable, l'arrêt retient que l'une des victimes, le journal Le Monde, est de nationalité française et qu'en conséquence, les juridictions françaises sont compétentes en application de l'article 113-7 du code pénal ; que les juges ajoutent que l'article de M. Y... est une oeuvre de l'esprit pour laquelle son auteur bénéficie d'une protection juridique en vertu des dispositions du code de la propriété intellectuelle et qu'ainsi, en reproduisant et diffusant cet article dans le quotidien qu'il dirige, sans solliciter l'autorisation de son auteur et du journal auquel il était destiné, le prévenu, a sciemment violé le droit moral de l'auteur et commis le délit de contrefaçon ; ;
Mais attendu qu'en se déterminant ainsi, alors que l'atteinte portée aux droits d'auteur a eu lieu hors du territoire national, la cour d'appel a méconnu les textes susvisés et le principe ci-dessus énoncé ;
D'où il suit que la cassation est encourue ; que, n'impliquant pas qu'il soit à nouveau statué sur le fond, elle aura lieu sans renvoi, ainsi que le permet l'article L. 411-3 du code de l'organisation judiciaire
; Par ces motifs :

CASSE et ANNULE, en toutes ses dispositions, l'arrêt susvisé de la cour d'appel de Paris, en date du 5 novembre 2009 ;

DIT n'y avoir lieu à RENVOI ;
DIT n'y avoir lieu à application, au profit de M. Y..., de l'article 618-1 du code de procédure pénale
ORDONNE l'impression du présent arrêt, sa transcription sur les registres du greffe de la cour d'appel de Paris et sa mention en marge ou à la suite de l'arrêt annulé ;
Ainsi fait et jugé par la Cour de cassation, chambre criminelle, et prononcé par le président le vingt-neuf novembre deux mille onze ;
En foi de quoi le présent arrêt a été signé par le président, le rapporteur et le greffier de chambre.

ملخص المذكرة

عرف العالم خلال السنوات الاخيرة تقدما غير مسبوق في مجالات الاعلام والاتصال التي أصبحت تعتمد أكثر فأكثر على الابتكارات الجديدة في مجالي الالكترونيك و المعلوماتية (الانترنت ، الرقمنة، انظمة الوسائط المتعددة...) ، فقد اصبح من الواضح اليوم أن هناك ارتباط وثيق بين النتائج التي تقدمها باستمرار صناعة تكنولوجيا المعلومات و الاتصالات و طرق ارتكاب الجرائم المعلوماتية التي لا زالت مخاطرها في ازدياد مطرد مع ما تقدمه لها هذه التكنولوجيات الحديثة.

حيث بدأت هذه الجرائم تهدد الإقتصاد العالمي نتيجة الخسائر الكبيرة الناتجة عنها ، و لعل أخطر ما في الأمر أن أغلب مرتكبي هذه الجرائم يبقون مجهولي الهوية وهذا الأمر يتيح لهم الاستمرار والتفنن بطرق التلاعب بموارد الآخرين عن طريق السيطرة على أنظمتهم الالكترونية ، فقد تفنن قراصنة الانترنت في التسلل الى كافة الشبكات من شبكات الكهرباء و الماء إلى شبكات الاتصالات المختلفة ولا يوجد ما يمنعهم من التسلل و التحكم في شبكات الملاحة الجوية و وزارات الدفاع عبر العديد من الدول .

ومن الناحية القانونية ، فقد قامت العديد من الدول بمواكبة التطور التكنولوجي بوضع النصوص الملائمة لمختلف استعمالات الاعلام الالي (التجارة الافتراضية، التوقيع الالكتروني، حماية المعطيات الشخصية...) كما تم وضع قوانين خاصة لمواجهة ما يسمى بالاجرام المعلوماتي ، إلا أن ما يدعو للقلق أن الكثير من البلدان وهي من البلدان التي لا تعتمد كثيرا على تكنولوجيا المعلومات و الاتصالات في تعاملاتها لذا فهي لا تتملك لحد الان تشريعاً صريحاً يخص الجرائم المعلوماتية وربما يعود السبب كذلك الى قلة او انعدام الدعاوي القضائية على مستوى محاكمها بهذا الخصوص ، الا ان الطابع العابر للحدود لا يمنع مجرمي المعلوماتية من استغلال هذا الظرف لا رتكاب جرائمهم انطلاقا من هاته الدول و جعلها قاعدة لذلك.

ولأن تنظيم مجال المعلوماتية وسن تشريعات بهذا الخصوص يساهم في زرع الثقة في ثقافة المجتمع العامة ، وهذا بدوره يشجع على زيادة استخدام وسائل تقنية المعلومات بدون هضم للحقوق، وبدون خوف من العواقب السلبية، و خصوصا مع تطور التعاملات الالكترونية صار من الضروري وضع القواعد العامة لاستخدام التقنية في التعاملات والتوقيعات الالكترونية، ولتعزيز الثقة بها وتسهيل استخدامها على الصعيدين المحلي والدولي ، كما ان مكافحة جرائم المعلوماتية تسعى الى تحقيق التوازن الضروري بين مصلحة المجتمع في الاستعانة بالتقنية الحديثة ومصلحة الإنسان في حماية حياته الخاصة والحفاظ على أسراره، والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

لقد حاولنا في دراستنا للجريمة المعلوماتية تبيين الاحكام العامة لها موضحين أهم المحاولات لتعريف الجريمة المعلوماتية واختلاف المعايير المستند عليها في ذلك والهدف المتوخى من التجريم.

ثم تناولنا البنيان القانوني للجريمة المعلوماتية في الفصل الأول ، حيث استهلت الدراسة بتقديم آلية ارتكاب الجريمة المعلوماتية والوسائل المستعملة في ذلك ، كما تناولنا طبيعة المحل مبرزين اهم الاراء التي ظهرت في تحديد الطبيعة القانونية للمعلومات .

ثم تطرقنا لدراسة عناصر الجريمة المعلوماتية بصفة عامة وتعرضنا لشرح احكام الشروع و المساهمة وقواعد المسؤولية الجنائية .

أما الفصل الثاني فقد خصصناه لدراسة صور الجريمة المعلوماتية حيث عرضنا انواع جرائم الحاسب الالي وجرائم الانترنت وكيف اختلف الفقهاء في اعتبار الجريمة المعلوماتية من قبيل الجرائم ومدى امكانية تطبيق النصوص التقليدية عليها كما قدمنا بعض النماذج التطبيقية و القضايا العملية في مجال جرائم المعلوماتية من خلال مقارنة تشريعات الدول بصدد كل جريمة معلوماتية .

بعد ذلك تناولنا جهود مكافحة الجريمة المعلوماتية في بعض الدول الغربية و الدول العربية كما تحدثنا عن جهود المكافحة الدولية من خلال دراسة اهم القرارات الصادرة عن الامم المتحدة ، حيث عرضنا اهم ما جاء به كل من مؤتمر هافانا لسنة 1990 بشان جرائم الكمبيوتر و مؤتمر ريودي جانيرو سنة 1994 وكذا اهم اتفاقية صادرة عن الاتحاد الاوروبي وهي اتفاقية بودابست لسنة 2001 بخصوص جرائم المعلوماتية.

في حين خصصنا الفصل الثالث لدراسة التطور التشريعي لمكافحة الجريمة المعلوماتية في الجزائر حيث تناولنا اهم اشكال يواجه المحققين و المتمثل في اثبات الجريمة المعلوماتية ، كما تطرقنا لعرض القانونين رقم 04/ 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر66 /156 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات و القانون رقم 09-04 مؤرخ في 5 وات 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها.

واخيرا اوردنا بعض المقترحات لمكافحة الجرائم المعلوماتية على المستووين الوطني و الدولي .

Résumé

Le monde a connu au cours des dernières années un progrès sans précédent dans les domaines de l'informations et de la communication qui s'appuient de plus en plus sur les performences de l'éléctronique et les innovations de l'informatique (Internet, numérisation , multimédia…) , de ce fait il est devenu évident qu'il ya une étroite corrélation entre l'industrie de la technologie de l'information et de la communication et les formes de commettre des crimes informatiques, qui présentent des risques sans cesse évolutives avec ces nouvelles technologies en menaçant l'économie mondiale par des pertes financières importantes, et peut-être la chose la plus dangereuse c'est que la plupart des auteurs de ces crimes restent anonymes, ce qui leur permet de continuer à commetres leurs actes illicites, en manipulant les ressources des autres à travers le contrôle de leurs systèmes électroniques.

Ces cybercriminels ont prouvé une aptitude de s'infiltrer dans tous les différents réseaux de communication, d'électricité et d'eau ; de plus il n'y a rien pour les empêcher de s'infiltrer dans les systèmes de contrôle de navigation aérienne ou même les ministères de la défense de nombreux pays.

Au plan juridique, beaucoup de pays ont accompagné cette évolution technologique par la mise en place de dispositifs appropriés aux différentes utilisations de l'outil informatique (cybercommerce, signature électronique, protection des données à caractère personnel…). Dans le même sillage , des lois spécifiques ont été adoptées pour faire face à la délinquance informatique et aux nouvelle formes de criminalité évoluant dans le cyberespace , mais le plus inquiétant c'est que de nombreux pays sous développés n'utilisent pas la technologie de l'information et de communication dans la gestion, ce qui explique l'absence d'une législation expressément pour les délits informatiques et peut-être aussi à défaut de contentieux auprès des tribunaux, mais la nature transfrontalière de ces cybercrimes n'empêche pas les criminels d'exploiter ces circonstances pour commettre ses actes en faisant de ces pays une base pour leurs attaques informatiques.

Toutefois l'organisation du domaine de l'informatique et la promulgation des lois à cet égard contribue à encourager la société pour l'utilisation des technologies de l'information en toute confiance et sans crainte des conséquences négatives , notamment avec le développement du commerce électronique , il est devenu nécessaire d'élaborer des règles générales pour l'utilisation de ces technologies

d'information et de la communication dans les transactions et les signatures électroniques, à l'échelle local et international.

Aussi la lutte contre la criminalité informatique, a pour objectif de faire l'équilibre nécessaire entre l'intérêt de la société pour l'utilisation des technologies modernes et l'intérêt des individus pour protéger leurs vies privées.

On a essayé dans notre étude d'exposer les dispositions générales de la cybercriminalité en expliquant les différentes tentatives pour définir cette forme de criminalité.

Dans le premier chapitre, on a exposé la structure juridique du crime informatique, en expliquant le mécanisme du crime et les moyens utilisés dans ce domaine, ensuite on a étudié les éléments de la cybercriminalité en général, ainsi que les dispositions de la tentative et de la responsabilité pénale.
Dans Le deuxième chapitre on a étudié les différentes formes de la cybercriminalité, en analysant l'applicabilité des textes traditionnels sur ces nouveaux crimes.

Ensuite on a traité les différents efforts pour lutter contre la cybercriminalité dans certains pays occidentaux et arabes ainsi qu'à l'échelle internationale, et ce à travers l'étude des décisions les plus importantes émises par les Nations Unies, tel que la Congrès de La Havane de 1990 sur les délits informatiques et la Congrès de Rio de Janeiro 1994, ainsi que la Convention de Budapest 2001 émise par l'Union européenne.

Le troisième chapitre était consacré pour l'étude du progrès législatif en Algérie pour lutter contre la cybercriminalité, d'où on a traité le problématique des enquêteurs avec les procédures et la preuve de la cybercriminalité et on a exposé également les lois N° 04-15 du 10 novembre 2004 , modifiant et complétant le code pénal , qui a incriminé les actions malveillantes dirigées contre les systèmes de traitement automatisé de données (accès illicite au système informatiques) et la lois N° 04-09 du 05 Aout 2009 , portant les règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.

Et enfin on a cité quelques propositions pour faire face à la délinquance informatiques et aux nouvelles formes de cybercriminalité a l'échelle nationale et internationale.

قائمة المراجع

اولا - المراجع باللغة العربية:

المؤلفات العامة:

ابراهيم حامد طنطاوي ، سلطات مامور الضبط القضائي ، مطبعة دار التأليف ، القاهرة ، 1991

احمد فتحي سرور، الوسيط في القانون ا لعام، دار النهضة العربية ، القاهرة،1991.

أمال عبد الرحيم عثمان ،شرح قانون العقوبات ، القسم الخاص ،دار النهضة العربية القاهرة ،2001.

رؤوف عبيد، مبادئ القسم العام من التشريع العقابي، الطبعة الثالثة، دار الفكر العربي ،1979 .

رمسيس بهنام ، النظرية العامة للقانون الجنائي ، الطبعة الثالثة ، منشأة المعارف بالاسكندرية ، (د.ت).

رمزي رياض عوض،مشروعية الدليل الجنائي في مرحلة المحاكمة ، دار النهضة العربية ، القاهرة، 1997

عمر السعيد رمضان،مبادىء قانون العقوبات،القسم الخاص،دار النهضة العربية ،القاهرة ، 1986.

عمر السعيد رمضان،مبادئ قانون الاجراءات الجنائية، الجزء الاول، دار النهضة العربية،القاهرة ،(د. ت).

فوزية عبد الستار ، شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية ، القاهرة ، 1990.

محمد زكي أبو عامر، قانون العقوبات، القسم الخاص، دار المطبعات الجامعية ، الاسكندرية ، 1989.

محمد زكي ابو عامر ، الاجراءات الجنائية،دار منشاة المعارف، الطبعة الثانية ،الاسكندرية ،(د.ت).

مامون محمد سلامة، قانون العقوبات، القسم العام، دار النهضة العربية ،القاهرة، 1990.

محمود محمود مصطفى ،شرح قانون العقوبات، القسم الخاص ،مطبعة جامعة القاهرة ،1984.

محمد نجيب حسني ،شرح قانون العقوبات،القسم العام،دار النهضة العربية ، القاهرة،1982 .

محمود نجيب حسني،شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1988.

المؤلفات الخاصة:

أحمد حسام طه تمام ،الجرائم الناشئة عن استخدام الحاسب الالي وشبكة الانترنت، دار النهضة العربية ، القاهرة ،2000.

احمد محمد الرفاعي ، الحماية المدنية للمستهلك ، دار النهضة العربية ، القاهرة، 1994.

احمد خليفة الملط ،الجرائم المعلوماتية ،دار الفكر الجامعي ،الاسكندرية ، 2005.

اسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة و بنوك المعلومات، دار النهضة العربية ، القاهرة، 1994.

توم فوريستر ،مجتمع التقنية العالية ، قصة ثورة تقنية المعلومات، الطبعة الاولى، مركز الكتب الاردني ،عمان، 1989.

جميل عبد الباقي الصغير، القانون الجنائي و التكنولوجيا الحديثة ،الطبعة الاولى،دار النهضة العربية ، القاهرة،1992.

خالد ممدوح إبراهيم ، امن الجريمة الالكترونية، الدار الجامعية ،الإسكندرية ، 2008.

حسن طاهرداود،جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية ، الرياض،1420 ه.

صلاح الدين السيسي، غسيل الأموال – الجريمة التي تهدد استقرار الاقتصاد الدولي، دار الفكر العربي، القاهرة، 2004.

عبد الله عبد الكريم عبدالله ، جرائم المعلوماتية و الانترنت، منشورات الحلبي الحقوقية ،بيروت ، 2007.

عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الالي، الطبعة الثانية ، دار النهضة العربية ،القاهرة ،2002.

عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي،دار الكتب القانونية،القاهرة ،2007.

عبد الفتاح بيومي حجازي،التجارة الالكترونية -الحماية الجنائية للتجارة الالكترونية،دارالفكر الجامعي،الاسكندرية ،2004.

عبد الفتاح بيومي حجازي، جريمة غسل الاموال بين الوسائط الالكترونية ونصوص التشريع، الطبعة الاولى ، دارالفكرالجامعي، الاسكندرية، 2005.

عبد الفتاح بيومي حجازي،التوقيع الاليكتروني في النظم القانونية المقارنة، الطبعة الاولى، دارالفكر الجامعي،الاسكندرية،2005.

عبد الفتاح بيومي حجازي،مبادئ الاجراءات الجنائية في جرائم الكمبيوتروالانترنت،دار الفكر الجامعي الطبعة الاولى، الاسكندرية،2006 .

عفيفي كامل عفيفي،جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة و القانون ، منشورات الحلبي الحقوقية 2003

عمر الفاروق الحسيني،المشكلات الهامة فى الجرائم المتصلة بالحاسوب الالي وابعادها الدولية ، ط 2، (بدون ناشر).

علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب ، دار الجامعة الجديدة للنشر، الاسكندرية ، 1997.

غسان رباح، الوجيز في قضايا حماية الملكية الفكرية و الفنية ،منشورات الحلبي الحقوقية، الطبعة الاولى،2008 .

لعشب علي ، الاطار القانوني لمكافحة غسيل الاموال ، OPU ،الجزائر ، 2007.

محمد الالفي ، المسؤولية الجنائية عن الجرائم الاخلاقية عبر الانترنت، الكتب المصري الحديث للنشر ، القاهرة ، 2005

محمد الامين البشري،التحقيق في جرائم الحاسب الالي، بحث مقدم الى مؤتمر القانون و الكمبيوتر و الانترنت- مايو 2000، كلية الشريعة والقانون، جامعة الامارات،2000.

محمد الامين البشري و **محسن عبد الحميد احمد** ، معايير الامم المتحدة في مجال العدال الجنائية و منع الجريمة ، الطبعة الاولى، اكاديمية نايف للعلوم الامنية ، الرياض ، 1998.

محمد امين الرومي،جرائم الكمبيوتر والانترنت،دار المطبعة الجامعية، الاسكندرية ،2004.

محمد امين الشوابكة ، جرائم الحاسوب و الانترنت، طبعة اولى ،دار الثقافة ، عمان ،2004.

محمد حسام لطفي ، الحماية القانونية لبرامج الحاسب الالي ، دار الثقافة للطباعة و النشر،(د.ت).

محمد حسين منصور، المسئولية الالكترونية، دار الجامعة الجديدة للنشر الإسكندرية، 2003.

محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، 1994.

محمد عبدالله ابوبكر سلامة ،جرائم الكمبيوتر و الانترنت، منشأة المعارف ، الاسكندرية ،2006.

محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الانترنت، دار النهضة العربية،2000 .

محمد فهمي ، الموسوعة الشاملة لمصطلحات الحاسب الالكتروني ، المكتب المصري الحديث، القاهرة ،1991.

محمود احمد عبابنة ،جرائم الحاسوب و ابعادها الدولية ، دار الثقافة للنشر و التوزيع ، 2005.

مدحت عبد الحليم رمضان،الحماية الجنائية للتجارة الاليكترونية، دار النهضة العربية، القاهرة ، 2000 .

مدحت عبد الحليم رمضان ، جرائم الاعتداء على الأشخاص و الأنترنت ،دار النهضة العربية ،2000.

ممدوح خليل بحر ، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة ، مكتبة دار الثقافة، عمان، 1996.

منير محمد الجنبيهي و **ممدوح محمد الجنبيهي**،بروتوكولات وقوانين الانترنت،دار الفكر الجامعي، الاسكندرية، 2005.

نائلة عادل قورة، جرائم الحاسب الالي الاقتصادية ، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت ،2005.

نعيم مغبغب،مخاطر المعلوماتية و الانترنت على الحياة الخاصة وحمايتها،الطبعة الثانية، منشوراتالحلبي الحقوقية،بيروت ،2008.

هشام محمد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة ، أسيوط ، 1995.

هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ،دار النهضة العربية ، 1992.

هلالي عبد الله احمد، تفتيش نظم الحاسب الالي و ضمانات المتهم المعلوماتي،الطبعة الاولى، دار النهضة العربية، القاهرة، .1997

هلالي عبد الله احمد ،التزام الشاهد بالاعلام في الجرائم المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة .

يونس عرب، جرائم الكمبيوتر و الانترنت، منشورات اتحاد المصارف العربية ، بيروت ، الطبعة الاولى ،2002.

الرسائل العلمية:

عزة محمود احمد خليل ، مشكلات المسؤولية المدنية في مواجهة الحاسب الالي ،رسالة دكتوراه ، القاهرة، 1994.

محمد عبد الحميد مكي، الاحتيال في قانون العقوبات ، دراسة مقارنة، رسالة دكتوراه، جامعة القاهرة ،1988.

المقالات والبحوث والتقارير:

التقرير العالمي لتكنولوجيا المعلومات لسنة 2010/2009 - الصادر عن المنتدى الاقتصادي العالمي - دافوس- سويسرا.

راشد بن حمد البلوشي ،ورقه عمل مقدمه الي المؤتمر الدولي الاول حول حماية امن المعلومات و الخصوصيه في قانون الانترنت، القاهرة ، 2008 .

طارق محمد الجملي ،الدليل الرقمي في مجال الاثبات الجنائي ، ورقة عمل مقدمة للمؤتمر المغاربي الاول حول المعلوماتية والقانون نظته اكاديمية الدراسات العليا بتاريخ 28 اكتوبر 2009 بطرابلس ، ليبيا

عبد الناصر محمد فرغلي ومحمد عبيد المسماري، الاثبات الجنائي بالادلة الرقمية، ، بحث مقدم للمؤتمرالعربي الاول للأدلة الجنائية، اكاديمية نايق للعلوم الامنية ، الرياض ، 2007.

عمرمحمد بن يونس ، مذكرات في الاثبات الجنائي عبر الانترنت- ندوة الدليل الرقمي- القاهرة ، 8 مارس 2006.

غنام محمد غنام،عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر،بحث مقدم الى مؤتمر القانون والكمبيوترو النترنت، جامعةالامارات ، 2000.

محمد السعيد رشدى ، الانترنت والجوانب القانونية لنظم المعلومات ، بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق ، جامعة حلوان بعنوان الاعلام والقانون بتاريخ 14-15/ مارس 1999.

محمد عقاد –جريمة التزوير في محررات الحاسب الآلي- دراسة مقارنة ،بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، دار النهضة العربية، القاهرة، 1995.

كامل سعيد ، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنولوجيا ، (Oxford v.Moss (1978) 68 Cr .App R 183)، بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، 25 أكتوبر 1993، ص 349 .

ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية، بحث مقدم إلى مؤتمر القانون و الكمبيوترالانترنت، كلية الشريعة و القانون بجامعة الإمارات سنة 2000.

هشام محمد فريد رستم، اصول التحقيق الجنائي و الفني بانشاء الية عربية موحدة للتدريب التخصصي، بحث مقدم

لمؤتمر القانون و الكمبيوتر، جامعة الامارات العربية المتحدة ، 2000 .

النصوص القانونية المعتمد عليها :

- القانون رقم 09-04 مؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها، ج .ر عدد 47.

- القانون رقم 09-01 المؤرخ في 25 فبراير 2009 المتعلق بالاتجار بالاشخاص المعدل والمتمم للأمر رقم 66-156 المتعلق بقانون العقوبات ،ج ر عدد 15.

- القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر66 /156 المتضمن لجرائم المساس بانظمة المعالجة الالية للمعطيات ج.ر عدد 71.

- قانون رقم 04-18 مؤرخ في 25 ديسمبر سنة 2004، يتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها، ج.ر عدد 83.

- القانون رقم 04- 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر66 /155 المتضمن قانون الاجراءات الجزائية، ج.ر عدد71.

-القانون رقم 01-09 المؤرخ في 26 جوان 2001 المعدل والمتمم للأمر رقم 66-156 المتعلق بقانون العقوبات، ج.ر عدد 34.

- المواد 44- 46 من القانون رقم 05-10 مؤرخ في 20 جوان 2005 المعدل و المتمم للأمر75-58 المؤرخ في 26 سبتمبر 1997 المتضمن القانون المدني،ج.ر عدد 44.

- الامر 66-156 المؤرخ في 18صفر1386 الموافق لـ 8 يونيو1966 المتضمن قانون العقوبات، ج.ر عدد 49 .

- الأمر03-05 الصادربتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر73-14، ج رعدد44 .

- المرسوم التنفيذي رقم 06-348 المؤرخ في 5 اكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق، ج.ر عدد 63.

ثانيا - المراجع باللغة الفرنسية:

1-Ouvrage Généraux :

Bernardini (Roger.), Droit Pénal Spécial,Gualino Editeur,2000.

Delmas-Marty (Mireille.), Droit Pénal des Affaires, Presse Universitaire de France, 1990 .

Gattegno (Patrice.), Droit Pénal Spécial,Dalloz, 1999.

Veron (Michel.), Droit Pénal des affaires,Dalloz, 1999.

2-Ouvrage Spéciaux :

Abbas(Jaber.), Les infractions commise sur Internet,L'Harmattan,paris,2009.

Bibent (Michel.), Le Droit du traitement de lniformation,Nathan,2000

Chawki (M.), Essai sur la notion de Cybercriminalité,IEHE,Lyon ,2006.

Feral-schuhl (Christiane), Cyber Droit, (Le droit à l'épreuve de l'internet), 2eme 2dition, édition Dalloz, Paris, 2000

Gassin (Raymond.), Droit de l'enfant et de l'adolescence, litec , 1995

Glineur (P.), Droit et Ethique de l'Informatique, Story Scientia, Bruxelles, 1991, p 180.

Gomez Urbina(A.), Rivero(A.) , et Lopez(N.), Hacking Interdit, 1ère édition, Paris, 2006 .

Manzanaré (Henri) et **Nectoux (philipe)**, L'informatique au service de juriste,Litec, Paris,1987

Khiati(Mostapha),Cybercriminalité et enfance en Algerie,Edition FOREM,2007

Linant De Bellefonds (Xavier.) et **Hollande (Alain.)** ,Droit de l'informatique et de la télématique, Dellmas, Edition Dalloz, 1990.

Lucas (André)et Deveze(Jean), Le droit de l'informatique et de l'internet ,Presse universiaire de Paris, 2001.

Manzanaré (Henri.) et **Nectoux (philipe.)** , L'informatique au service de juriste,Litec, Paris,1987.

Parker (Donn B .) , Combattre la criminalité informatique , OROS ,Paris, 1985

Sargos(P.) et Massé (M.), Le droit pénal special de l'informatique et droi pénal, Cujas 1983

Zanella (Paolo), Architecture et technologie des ordinateurs, Bordas,Paris,1989.

3-Thèses :

Aupècle Guicheney (Nadine.) ,Les infractions pénales favorisées par l'Informatique, Thèse,Université de Monpellier, 1984.

Champy (Guillaume.) ,Fraude informatique,Thèse, Université Aix-Marseille III ,1990

Vergutch (Pascal.), La repression des délits informatiques dans une péerspective internationale, Thèse, Université de Monpellier 1, 1996.

Weill (Pierre Alain), Etat de la législation et tendances de la jurisprudance relatives à la protection des données personnelles en Droit pénal Français , Rapport publié sur Reveue Internationale du Droit Comparé,1987.

Zoller (Elizabeth), Le Droit au respect de la vie privée aux Etats Unis, Droit et Justice N° 63, Université ParisII, 2005.

4- Articles et Notes :

Alterman (H.) et Bloch(A.) , La Fraude Informatique (Paris, Gaz. Palais), [3 sep. 1988].

Ber-Gabal, Le control de l'administration par la commission national de l'informatique et des libertés, R.D.P 1980.

Chamoux (Françoise.), La Loi sur la Fraude Informatique :de nouvelles incriminations , J .C.P., 1988, Doctrine 3321. N° 8.

Deveze (Team.), Le Vol de biens informatiques, J.C.P.1985, I.3210.

Duque (Nina)، La pornographie sur internet : Une analyse du débat senatorial sur le Communications Decency Act of 1996 aux Etats Unis , Université du Québec à Montreal , 1999.

Gassin(Raymond.),Le droit pénal de l'informatique, D.Chr.V 1986.

Goutal (Jean-Louis.) ,Informatique et droit privé, in **Bensoussan Alain**, **Linant de Bellefonds (Xavier)**, **Maisel (Herbert)** ,in Emergence du droit de l'informatique, Edition des parques,1983.

Lamy droit de l'informatique, 1997 ,N° 2451.

Lacoste (P), Les métiers de l'intelligence économique, Défense nationale,Paris, 2006.

Lucas de Leyssac (Marie-Paule), Une Information Seule est-elle Susceptible de Vol d'une autre atteinte juridique aux biens,Dalloz Siery,1985

Lucas de Leyssac (Marie-Paule), L'arret Bourquin,Une double Révolution :Un Vol d'Information Seul, une Soustraction Permettant d'appréhender des reprductions qui ne constitueraient pas des Contrefaçons , Rev .Sc.Crim , 3 Juillet-Septembre 1990.

Massé (Michel.), Infractions contre l'ordre financier, Rev .sc .crim, Janvier 1985 N°1.

Tiedemann (Klaus.), Fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, Rev.Dr.Pén. Crim n°7, Bruxelles ,1984.

Vivant (M.) et **Le Stanc (Ch.),** Lamy droit de l'Informatique, 1989, N°2479.

5- Jurisprudence et textes juridiques :

-Cass.Crim.12 Décembre 1996, Bull.crim.N° 465.

-Corr.de Limoge, 14 Mars 1994, E.S.I, Juin 1994, p 238.

-Cass.Crim.5Janvier 1994, J .C.P. , Edition Général,1994,N°856.

- CA de paris, 5 Avril 1994,D.,1994.,I.R.,p130.

-CA de Paris ,28Novembre1990, Juris-Data, N° 025569 .

-Cass .crim ,12 Janvier 1989, Bull. crim , N°14 ,p.38

-Cass.crim.8 Janvier 1979, Gaz . Pal., 1979, 1, Note p.502.

-Cass.crim.,13Octobre 1971 , Bull.crim. N°261, p643.

-Cass.crim.,8 Décembre 1971,Bull.crim.,N°341,p.856.

-Cass.crim., 17Octobre1967, Bull.crim.,N°252,p594.

-Code pénal français, DALLOZ, Paris, ed. 2009.

-La Loi N°88-19 du 5 Janvier 1988 relative à la fraude informatique, J.O.R .F,N°4 du 6 Janvier 1988 (France) modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004.

- La Loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, J.O. R.F n°139, 18 juin 1998 (France) .

-La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ,J.O.R.F n°143 du 22juin 2004.

-La loi n° 92-597 du 1er juillet 1992 relative au code de la propriété intellectuelle, J.O.R.F n°153 du 3 /7/ 1992.

-La loi n° 98-536 du 1er juillet1998 à l'adresse :
http://www.wipo.int/wipolex/fr/details.jsp?id=5589

- Ordonnance n° 2000-916 du 19/09/2000,art 3,J.O.R.F du 22/09/2000 en vigueur le 01/01/2002.

- La Recommandation N ° R (89) 9 sur la criminalité informatique et le rapport final du Comite d'Europe sur le problème de la criminalité, Strasbourg, 1990.

-La loi n° 17 -78 du 6Janvier 1978 relatif aux fichiers et aux libertés, J.O.R.F du 7 Janvier 1978.

- Loi 2000-321 du 12 -04-2000 relative aux droits des citoyens dans leurs relations avec les administrations,J.O.R.F n°88 du 13-04-2000.

- Loi n° 2006-64 du 23/01/2006 parue au J.O.R.F n° 20 du 24/01/2006 relative à la lutte contre le terrorisme à l'adresse : http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124

ثالثا- المراجع باللغة الانجليزية:

1-Books :

Bainbridge (David.) , Introduction to Computer Law, Fourth Edition, Longman, 2000.

Ball (Leslie D.),computer crime,in'' The information technology revolution'',Cambridge ,1985.

Cornwall (Hugo.), Datatheft , Computer Fraud Industrial Espionage and Information Crime , Heinemann , London , 1987.

Geis (G.) , White-Collar Crime,Offences In Business, Politics And The professions ,N.Y, The Free Press.

Lioyd (Ian.), Information Technology Law,Butterworths Press: London,Dublin,Edinburgh, 1997.

Masuada (Yoneji.), The Information Technology Revolution, Oxford Blackwell, 1985.

Martin (D.) et **Martin (F.P)** ,Cybercrime , Paris, Press Universitaires, 2001.

Norman (Adrian R .D), Computer Crime and the Law, Criminal Law Journal,Vol.15,1991.

Parker (Donn B.), Figting Computer Crime '' A new Framework for Protecting Information'',John Wiley and sons ,1998.

Russel(Hon Fox), Justice in The Twenty First Century, Cavendish Publishing, London, 2000.

Sieber (Ulrich) ,The international Handbook on Computer Crime ''Computer related Economic Crime and the infringements of privacy,John Wiley and Sons,1986.

Taper (Colin) , Computer low , 3rd edition,Longman,London, 1983.

Wall (David.), Crime and the Internet , Routledge, N.Y, 2001.

Wasik (Martin) ,Crime and The Computer ,Oxford University Press,1991.

2-Articles :

Conley (John M.) and **Bryan (Robert M.)** , A Survey of Computer Crime Legislation in the United State , Information and Communication Technology Law, Vol 8, 1999.

Olivenbaum (Josef M.), Rethinking Fedral Computer Crime Legislation,S.H.L.Rev.,1997, vol.27.

Kaspersen (Henric W.K), Stands for computer crime legislation- comparative analysis, Kuler law & taxation publishers, 1989

Totty (Richard) &**Hardcastle (Antony)** ,Computer -Related Crime in information technology and the law, Macmillan Publishers , U.K.1986.

Wasik (Martin), The Computer Misuse Act 1990, Crim.L.J. 1990.

3-Reports :

Alexander (Michael.), Computer Crime, Computer World, Vol XXIV,N°11,1990.

Bainbridge (David), Hacking -The Unauthorised Access of Computer System, the Legal Implications, M.L.Rev.,March 1989,vol 52, p.211.

Dumbill (Eric.), Computer misuse act 1990 - recent development , C.L.P., vol 8, N° 4

Thompson(David.), Current trends, in computer control crime, computer quarterly, vol 9N°1,1991.

Griffith (Doddss.),The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem,V .L.Rev, vol.43.

Internet Crime Report , Internet Crime Complaint Center, IC3, 2009.

Recommendation of the Council of Europe Concerning Guidlines for the security of Information System,26 November 1992.

Kurtz (Robin K.), Computer Crime in virginia :A Critical Examination of the Criminal Offenses in the virgivinia Computer Crime Act,W.M.L.Rev, 1986, Vol 27

Marion (Camille Cardoni), Computer Viruses and the Law , D,L,Rev.1989 ,vol. 93.

Senate Report N° 104-357 th Congress, 2nd Session ,Detailled Discussion of The NII Protection Act , 1996.

المواقع الالكترونية:

- احصائيات مسجلة بتاريخ 15 أكتوبر 2010 ، أنظر في الموقع :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-445352-cybercriminalite-coute-114- dollars-2010.html

- للاطلاع على النص الكامل لاتفاقية الإجرام المعلوماتي او السيبيري راجع الموقع الالكتروني الخاص بالمجلس الأوروبي :

http: //www.conventions.coe.int/treaty/EN/treaties/html/185.htm

- راجع : اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر2000، على الموقع التالي :
http://www1.Umn.edu/humanrts/arab/CorgCRIME.html

- أنظر في الموقع : Highley, Reid. (1999). Viruses: The Internet's Illness.[Online]
http://www.chemistry.vt.edu/chem- dept/dessy/honors%20/papers99/highleh.htm

- انظر في الموقع : http://www.larousse.fr/encyclopedie/nom-commun-nom/cryptographie/38869

-أنظر في الموقع : http://www.legalis.net/?page=jurisprudence-decision&id_article=2163

- انظر في الموقع :http://www.commentcamarche.net/contents/virus/keylogger.php3

- انظر في الموقع :http://fr.wikipedia.org/wiki/Base_de_donn%C3%A9es

- أنظر في الموقع : http://www.diffamations.com/laloi.html

- Loi n° 2003-75 du 10 Décembre 2003 relative au soutien des efforts internationaux de lutte contre le terrorisme et a la répression du blanchiment d'argent , La législation du secteur de la sécurité en Tunisie à l'adresse : http://www.legislation-securite.tn/ar/node/29195.

- Garreau(Alain), Les effets du Commerce Eléctronique sur les transports, Paris ,p. 6 , en date du 06 /06/2001 à l'adresse : http://www.oecd.org

- Artcile de Thibault Verbiest, Les casinos virtuels : une nouvelle cybercriminalité ?, à l'adresse : http://www.legalis.net/legalnet/articles/casinos_virtuels_notes.htm

- Création d'un site Web à l'adresse : http://ar.html.net/

-18 USC § 1030 - Fraud and related activity in connection with computers ,in : Computer Crime & Intellectual Property Section United States Department of Justice :

http://www.cybercrime.gov/1030analysis.html. Or
http://www.cybercrime.gov/ccmanual/ccmanual.pdf

- USA Patriot Act à l'adresse :
http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

- « British Man Arrested on several Terrorisme related Charges » communiqué de presse,United States Attorney Office District of Connecticut,6 Aout 2004 à l'adresse :
http://www.US.doj.gov/usao/ct/presse2004/20040806.html

- Terrorism Act 2006 à l'adresse :
http://www.northants.police.uk/files/documents/Terrorism/te98%5ETerrorism%20Act%202006.pdf

الفهرس

الموضوع الصفحة