وزارة التعليم العالي والبحث العلمي
جامعة عبد الحميد ابن باديس
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة نيل شهادة الماستر في الحقوق

تخصص: علم الإجرام والعلوم الجنائية

تحت عنوان

الجريمة المعلوماتية

من إعداد الطالبة:
*جزار منصورية

تحت إشراف الأستاذة:
*سالمي نضل

أعضاء اللجنة المناقشة:

1-الأستاذة: غالي كحلة (رئيس)
2- الأستاذة: بوخدمي فادية (مناقش)
3- الأستاذة: سالمي نضل (مؤطرة)

السنة الجامعية: 2017/2016

شكر وعرفان

يسرني أن أتقدم بجزيل الشكر والعرفان إلى اللجنة

الموقرة التي قبلت مناقشة هذا البحث المتواضع.

كما يسرني أن أتقدم بالشكر الجزيل إلى التي

شجعتني ووقفت وراء هذا العمل المتواضع

بمجهوداتها ونصائحها القيّمة

استاذتي المشرفة: سالمي نضال.

إهـــــــــداء

إلى التي أهدتني نور الحياة وسقتني من دفقات حبها و رعايتها إلى التي قدمت لي آيات الحب والحنان، إلى أعذب كلمة رددها لساني إلى من وضعت الجنة تحت قدميها، إلى أمي الحبيبة أطال الله في عمرها.

إلى الذي استلهمت منه معاني الثبات وزرع في قلبي حب العلم ووضع بين جنابتي القوة والعزيمة، إلى الذي وهبني كل رعايته واهتمامه، إلى أبي العزيز أدامه الله لي.

إلى زوجي وجميع أفراد أسرته.

إلى من أشد بهم أزري أخواتي

إلى فلذة كبدي فريال

إلى جميع الأصدقاء

عرفت الجريمة منذ فجر البشرية ولقد ناهضها الإنسان منذ اللحظة الأولى التي استشعر فيها بخطر يهدد كيانه وتقدمه، فالجريمة وليدة ما تمر به المجتمعات من ظروف وأسباب، و مرجع ذلك ما يحويه السلوك الإنساني في علاقاته المتشابكة بين الخير والشر.

ومن الثابت أن الجريمة والنشاط المعادي للمجتمع اقتحمه نوع جديد من المجرمين إلى جانب المجرم التقليدي الذي عهدناه في الماضي والذي كانت تقتصر جرائمه على أبعادها الفردية والاجتماعية، وذلك نتاج نمط حياة الإنسان ولقد بلغ هذا التطور أوجه بظهور الدولة بمفهومها المعاصر.

و لقد عرفت العديد من الدول تطورا هاما في مختلف الميادين ومن نتائجه ظهور ما يعرف بالمعلوماتية، هذه الأخيرة التي تعتبر سمة العصر والمقياس الذي يحدد مدى تقدم الشعوب وكذا مساهمتها في تسريع انجاز الأعمال فكان لزاما على الدول من أجل ضمان نهضتها وتماشيا مع عصر المعلوماتية أن تعمل على مواكبة التطور التكنولوجي الذي نجم عنه تحول العديد من الدول إلى مجتمعات الكترونية تعتمد على الرقمية في أداء عملها.

ولقد نجم عن هذه الثورة أثار سلبية اثرت على حقوق الأفراد وحرياتهم، نتيجة استغلال الأفراد والجهات للتقنية المعلوماتية في غير الغرض الذي خلقت من أجله وأضحى هذا النظام محلا للاعتداء وإساءة استخدامه، فقد ترتب على ذلك إحاطة هذه الظواهر بكثير من الغموض حتى دعا ذلك الكثيرين إلى القول أن الجريمة المعلوماتية هي أشبه بالخرافة وانه لا يوجد تهديد حقيقي بالحسابات الآلية فهي في حقيقتها جرائم يمكن بشأنها تطبيق النصوص التقليدية القائمة دون أن تتميز بأي سمات خاصة.

كما اختلفت آراء الفقه في شأن تطبيق النصوص عليها، وتضاربت أحكام القضاء في البلد الواحد بصفة عامة واتخذت بعض المحاولات طابعا إقليميا والبعض الآخر طابعا دوليا.

تدخل الجريمة الالكترونية في نطاق دراسات القانون الجنائي الوطني، والتي تقع في صميم القسم الخاص لقانون العقوبات، وباعتبارها أفعال تخطى حدود الدولة فتعد أيضا من اهتمامات رجال القانون الجنائي الدولي، كما تدخل في عداد الجريمة المنظمة التي تقوم على أساس تنظيم هيكلي وتدرجي له الاستمرارية لتحقيق مكاسب طائلة.

وتكمن أهمية دراسة هذا الموضوع فيما يكتسبه من جدة وغموض، وأمام انتشار ظاهرة الجريمة المعلوماتية، أو جرائم الانترنت، مقابل الفراغ القانوني خاصة في التشريع الوطني موازاة بما تعرفه مقاهي الانترنت من إقبال واسع، وإدمان شبابنا على شاشات الكمبيوتر، وربط أغلب بيوتنا وإداراتنا بالشبكة العنكبوتية، مما يدفعنا للبحث عن الأسلوب الأمثل للتعامل مع هذه الظاهرة بسبب ما خلفته من حيرة لدى رجال القانون لعدم إمكانية تطبيق النصوص القانونية السارية لعدم تناسبها مع طبيعة الجريمة المعلوماتية التي تغزو مجتمعنا بمختلف فئاته، و رغم أن ملفات المتابعة القضائية لها تعد شبه معدومة، مما يتطلب سن نصوص تشريعية لمكافحة هذه الجريمة التي خرقت كل المبادئ والأسس القانونية كما تكمن أهميته في اتساع مجاله وكلما تناولنا فكرة منه بقي الكثير منه يحتاج لتوضيح لأنه موضوع جديد من جهة ويحتاج لإيجاد إجراءات جديدة لمتابعته من جهة ومن أجل ذلك يجب الوقوف عند هذه الظاهرة الجديدة لتفكيك معانيها وإعطائها تعريفا دقيقا، وهنا تكمن صعوبة هذا الموضوع، فيحتاج بذلك لتوضيح سبل ارتكاب الجريمة المعلوماتية لتحديد أنواعها وطرق قمعها، أمام النقص الرهيب في المعلومات المتعلقة بالموضوع خاصة عند القانون وطلبته وهي صعوبة أخرى، تنبثق منها وسابقتها مجموعة المشكلات القانونية التي يطرحها الموضوع هي: ماهية الجريمة المعلوماتية؟ وما مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية، وردع مرتكبيها؟ ماهي الإجراءات الواجب اتخاذها لتفادي الثغرات القانونية التقليدية والحيلولة دون إفلات المجرمين من العقاب؟ الأمر الذي يتطلب بحث واسع وعميق.

وبما أن دراستي للموضوع مقيدة بعدد محدد من الصفحات فتناوله سيكون بشكل ضيق مع محاولة الإلمام بأكبر قدر من المعلومات، لتقريب الفكرة لذهن كل من يقرأ هذه المذكرة

وإزالة اللبس بالإجابة عن الإشكالات المطروحة، من خلال التطرق إلى تعريف وخصائص الجريمة المعلوماتية، أركانها، أنواعها، والعوائق في الفصل الأول ليصل بنا الحديث في الفصل الثاني عن الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري والتشريعات الأخرى من خلال نصوص الملكية الفكرية والصناعية والنصوص المستحدثة لتكون مذكرتنا هذه تطبيقية أكثر منها نظرية .

الفصل الأول: ماهية الجريمة المعلوماتية

عرفت البشرية في نهاية القرن الماضي اتساعا وتزايدا مطردا لنطاق استخدام تقنية المعلوماتية في المجتمع ونظرا للتطور السريع لهذه التقنية فقد مكنت من استعمالات متعددة وفي جميع المجالات، مما أدى إلى ظهور نوع جديد من الجرائم أطلق عليها تسمية الجرائم المعلوماتية.

وقد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة ونظرا لجسامة أخطارها وفداحة خسائرها وسرعة انتشارها أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفنيين والمهتمين بأمن الصرح المعلوماتي، لتحديد مفهومها،خصائصها،التمييز بينها وبين ما يقترب منها من ظواهر ومعرفة العوامل المختلفة التي تدخل في هذا التحديد.

المبحث الأول: مفهوم الجريمة المعلوماتية

سوف نتطرق في هذا المبحث إلى مفهوم الجريمة المعلوماتية، ونحاول من خلاله الوصول إلى تعريف يليق بها، ويتلاءم مع طبيعتها لننتقل بعد ذلك إلى خصائص هذه الجريمة.

المطلب الأول: تعريف الجريمة المعلوماتية وخصائصها

تعددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقا واتساعا وقد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، وما يستتبع ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها.

الفرع الأول : تعريف الجريمة المعلوماتية

تعرف الجريمة عموما في نطاق القانون العام بأنها سلوك الفرد عملا كان أو امتناعا يواجهه المجتمع بتطبيق عقوبة جزائية، وذلك بسبب الاضطرابات التي يحدثه في النظام الاجتماعي[1] وهو التعريف الذي يستند على عناصر الجريمة إلى جانب بيانه لأثرها (السلوك والسلوك غير المشروع وفق القانون ،الإرادة الجنائية وأثرها العقوبة أو التدبير الذي يفرضه القانون)، وهي الأوصاف التي تميز بين الجريمة عموما وبين الأفعال المستهجنة في نطاق الأخلاق والجرائم المدنية أو التأدبية.

أما مصطلح المعلوماتية فهو مشتق من كلمة المعلومات (Information)، وهي الكلمة التي شاع استعمالها منذ خمسينات القرن الماضي في مجالات مختلفة وسياقات شتى مما جعل لها في الاستعمال الدارج مفاهيم متنوعة.[2]

---

[1]–أحسن بوسقيعة، الوجيز في القانون الجزائي العام،الجزائر ،دار هومة، 2007،الطبعة الثالثة،ص3.

[2] –عزة أحمد خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي، القاهرة،دار النهضة العربية،1994،الطبعة الأولى، ص18 .

فالمعلومة لغة مشتقة من كلمة "علم"، ودلالتها فيها ،وتدور بوجه عام حول المعرفة التي يمكن نقلها أو اكتسابها[1]، وقريب من ذلك إشارتها في اللغة الفرنسية إلى فحوى عمليات الاتصال التي تستهدف نقل وتوصيل إشارة أو رسالة أو الإعلام عنها واتخاذ وظيفتها في نقل المعارف (Transfert de connaissances).

والمعلومات في اللغة الانجليزية والألمانية والروسية تعني كلمة Information اللاتينية الدالة بحسب الأصل على شيء للإبلاغ والتوضيح، أو على عملية « Process » الإبلاغ ، النقل أو التوصيل وهو نفس ما يعنيه لفظ « Xinxi » المقابل لها في اللغة الصينية[2].

أمّا اصطلاحا فهناك المئات من التعريفات التي أدلى بها باحثون من تخصصات وثقافات مختلفة لفهم وإدراك المعنى المراد بمصطلح "المعلومات".

ولا يوجد إلى يومنا هذا نص قانوني يعطي تعريفا جامعا مانعا للمعلومة، غير أن القانون الفرنسي الصادر في 29 يوليو 1982 الخاص بالاتصالات السمعية و البصرية أشار إلى تعريف عام للمعلومة حيث ينظر إليها بوصفها "صوت ، صورة ، وثائق – بيانات أو رسائل من أي نوع".

« Sons, images, documents, données ou messages de toute nature »

ويعرف الأستاذ Catala المعلومة بأنها "رسالة ما معبر عنها بشكل يجعلها قابلة للنقل أو الإبلاغ للغير"[3]،ويعرفها البعض الآخر بأنها "رمز أو مجموعة رموز تنطوي على إمكانية الإفضاء إلى معنى"[4].

---

[1]– المعجم الوسيط ، مجع اللغة العربية،القاهرة، دار الدعوة،1998،الطبعة الثالثة

[2]–أحمد خليفة الملط،الجرائم المعلوماتية،الاسكندرية، دار الفكر الجامعي، 2006، الطبعة الثانية ،ص72.

[3] –Pierre CATALA »La propriété de l'information » Cité par f.Toubal ; le logiciel–analyse juridique Fudul L.G.D.J 1986 P126–127.

[4]– هشام فريد رستم،جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة،بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين،مجلة الأمن العام العدد151،ص24.

ويستخلص مما ذكر أعلاه من تعريفات أن المعلومة هي "مجموعة رموز يستخلص منها معنى معين في مجال محدد، وتتمتع بالتحديد والابتكار والسرية والاستئثار". وبالنظر إلى المعلومة باعتبارها نتاج نشاط إنساني فإنه يجب أن يتوفر فيها عنصران أساسيان أولهما التحديد والابتكار وثانيهما السرية والاستئثار، إذ أن المعلومة المحددة هي التي يمكن فقط حصرها في دائرة خاصة بها، وأن الاعتداء على القيم يفترض دائما أن يقع على شيء محدد يكون محلا لحق محدد، ويجب أن تكون المعلومة مبتكرة وسرية كون السرية صفة لازمة تحصر حركة الرسالة وتحمل المعلومة في دائرة محددة من الأشخاص، فلا يمكن تصور الجرائم الخاصة بالسرقة والنصب وخيانة الأمانة إذا انعدم هذا الحصر لأن المعلومة غير السرية تقبل التداول، ومن ثم تكون بمنأى من أي حيازة، أما الاستئثار فهو أمر ضروري لأنه في جميع الجرائم التي تنطوي على اعتداء قانوني على القيم يستأثر الفاعل سلطة تخص الغير وعلى نحو مطلق[1].

وتماشيا مع ماذكر أعلاه فإن المعلوماتية "هي علم المعالجة العقلية للمعلومات باستخدام آلات تعمل ذاتيا" "La science du traitement rationnel par des machines automatique d'information notament"[2]،

وإن هذا التعريف هو الراجح لدى الفقه لتضمنه جميع المعلومات التي يتم تجميعها بمعرفة الإنسان والتي تتمتع بالتحديد ،الابتكار ،السرية ،الاستئثار والمجمعة عن طريق شبكات المعلومات والمعالجة آليا وفقا لأنظمة المعلومات.

ففي أول السبعينات ازدهرت صناعة جديدة أطلق عليها صناعة المعلومات، وأصبحت مصدرا للثروة وتتصف بعظمة التعقيد التقني وضخامة ما يستثمر فيها من أموال، وأصبحت مقياسا لتقدم الأمم[(3)]، ومصدرا للقوة الاقتصادية والسياسة والعسكرية، وموارد لا تقل ولا تنضب، تتزايد دوما ولا تتناقص بالاستخدام، ولا تستهلك وترتبط بالزمان والمكان وتتفاعل مع التطور وهي في الحقبة المعاصرة مفتاح للموارد الأخرى وسلعة

[(1)]–أحمد خليفة الملط،المرجع السابق، ص76.

[(2)]– أحمد خليفة الملط،المرجع السابق، ص81.

[(3)] –هشام فريد رستم، المرجع السابق، ص23 .

وخدمة تباع وتشترى ومصدر قوة اقتصادية وسياسية لمن يحسن جمعها وتنسيقها واستخدامها لارتباطها بمختلف مجالات النشاط الإنساني وتداخلها في كل جوانب الحياة المعاصرة، وأصبح توفيرها وحسن استغلالها من الأسس الضرورية لدفع عجلة التقدم في الأمم والمجتمعات وصار توفيرها وانسيابها بمثابة النبض والعصب لجهود التنمية والتحديث والرقي المعرفي والحضاري وبات الوعي بأهميتها مظهرا ومقياسا لتقدم الدول[1] ومن ثم بات من الضروري حماية هاته المعلومات من أي مساس بها ولكن نظرا لتنوعها وتنوع طرق المساس بها اختلف الفقه حول تعريف هذه الظاهرة.

وإن المشكلة الأولى والأساسية التي تعترض ظاهرة الجريمة المعلوماتية هي عدم وجود تعريف مجمع عليه لهذه الجريمة، وذلك لغياب تعريف قانوني للجرائم المعلوماتية عند جل التشريعات، إلا أنه قد بذل الفقه من أجل ذلك عدة محاولات لتعريف هذه الجريمة اتجهت بعضها إلى التضييق من مفهوم هذه الجريمة بتقليل الحالات التي يمكن أن يتصف النشاط الإجرامي بها، والبعض الآخر ذهب إلى التوسيع من مفهوم الجريمة المعلوماتية حتى أنه يمكن القول أنه يدخل في عدادها في كثير من الأحيان أفعال لايمكن أن تعد من قبيل جرائم الحاسب الآلي.

أولا: الاتجاه المضيق من مفهوم الجريمة المعلوماتية

يعرف أنصار هذا الاتجاه الجريمة المعلوماتية بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى"[2]. ومن خلال هذا التعريف يتبين لنا أنه لايكفي فقط أن تتوافر معرفة تكنولوجيا الحاسبات الآلية بدرجة كبيرة من أجل ارتكاب الجريمة المعلوماتية ولكن أيضا من أجل ملاحقتها ومتابعتها والتحقيق فيها بمعنى لابد أن يتوافر قدر كبير من العلم بهذه

---

[1]– هشام فريد رستم، المرجع السابق، ص33.

[2] –Parker (Donn B), Nycum(s) and Aura(s), Computer Abus : Stanford Research Institut, 1973 ; Taber(J.K) On Computer Crime, C.L.J, 1973, Vol 1, P517.

التكنولوجيا لدى الجناة والقائمون على معاينة وملاحقة مرتكبيها[1]، وقد أخذت وزارة العدل الأمريكية بهذا التعريف في تقرير صادر عنها عام 1989 المتعلق بجرائم المعلوماتية[2].

وقد انتقد هذا التعريف لكونه يحصر الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، إذ أنه في كثير من الحالات يرتكب الفعل دون الحاجة إلى هذا القدر من المعرفة ورغم ذلك لا يمكنا إنكار أن هذه الأفعال تدخل في عداد الجرائم المعلوماتية كإتلاف البيانات المخزنة داخل النظام المعلوماتي، كما أن هذا الفعل مجرم قانونا عند معظم التشريعات بما فيها التشريع الجزائري كما سنرى لاحقا.

ويستند أنصار هذا الاتجاه إلى أن الجرائم التي تفتقر إلى هذا القدر من المعرفة تعد جرائم عادية تخضع للنصوص التقليدية للقوانين الجنائية،ومن ثم فلا حاجة إلى نصوص جديدة لتجريمها[3].

كما تجدر الملاحظة أن جانب من هذا الاتجاه يرى أن الجرائم المعلوماتية ليس هي التي يكون الحاسب الآلي أداة لارتكابها، بل هي التي تقع على الحاسب الآلي أو على نظامه المعلوماتي فقط، فيعرفون هذه الجريمة بأنها "نشاط غير مشروع موجه لنسخ تغيير أو حذف أو الوصول غلى المعلومات المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه"[4] وما يعاب على هذا التعريف أنه يخرج من نطاق الجريمة عدد كبير من الأفعال غير المشروعة والتي يستخدم فيها الحاسب الآلي كأداة لارتكابها كالاحتيال المعلوماتي والذي سنتناوله فيما بعد.

---

[1]–نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية،بيروت، منشورات الحلبي الحقوقية، 2005، الطبعة الأولى، ص29 .

[2] –Benson (Carl), jablon (Andrew), Kaplan (Paul) & Resenthal (Mara), Computer Crimes, Americain C.L.Review, vol34, N°21,997, p410.

[3] – نائلة عادل محمد فريد قورة، نفس المرجع، ص29 .

[4] – هشام محمد فريد رستم، المرجع السابق، ص31.

ثانيا: الاتجاه الموسع لمفهوم الجريمة المعلوماتية

على عكس الاتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة وتختلف مواقفهم حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية.

فيعرف فريق من الفقهاء الجريمة المعلوماتية بأنها: "كل سلوك إجرامي يتم بمساعدة الحاسب الآلي" أو هي: "كل جريمة تتم في محيط الحاسبات الآلية"[1]. ويعرفها الأستاذ Tièdement بأنها: "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"[2].

من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة المعلوماتية، حيث أن مجرد مشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة المعلوماتية ومن تم يتضح لنا صعوبة قبول هذا التوجه، فجهاز الحاسب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته أو الأقراص أو الأسطوانات الممغنطة أو اللواحق على سبيل المثال، ومن ثم لا يمكن إعطاء وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة[3].

كما تجدر الملاحظة إلى أن هناك تعريفات أخرى في إطار الاتجاه الموسع كانت أكثر تحديدا في تعريف الجريمة المعلوماتية، ومن ذلك تعريفها بأنها: "كل تلاعب بالحاسب الآلي ونظامه من جل الحصول بطريقة غير مشروعة على مكسب أو إلحاق خسارة بالمجني عليه"[4].

ويلاحظ من خلال التعريفات السابقة أنها قد أغلقت جانبا على قدر كبير من الأهمية في تعريف الجريمة المعلوماتية ألا وهو الدور الكبير الذي يقوم به الحاسب الآلي

---

(1) –Roden (adrian), computer crime and the law, C.L.J ..,1991,vol.15,p.399

(2) –هشام محمد فريد رستم، المرجع السابق، ص29.

(3) – نائلة عادل محمد فريد قورة، المرجع السابق،ص ص 30–31.

(4) –Law commission, working paper n°110, computer misuse, London : HMSO, 1988 para.2.2

في هذه الجريمة، فإن كان من المتفق عليه أن الجريمة المعلوماتية قد تتخذ أحد المظهرين، يتمثل الأول في استخدام الحاسب الآلي كوسيلة لارتكاب الجريمة، والثاني في الاعتداء على الحاسب الآلي ذاته، ولهذا فإنه يثور أمامنا التساؤل الآتي: هل تعد الجريمة المعلوماتية في كل الحالات التي يستخدم فيها نظام الحاسب الآلي من أجل ارتكاب الجريمة، وفي كل الحالات التي يقع فيها اعتداء على الحاسب الآلي ونظامه؟

لاشك أن الإجابة على ها التساؤل تكون بالنفي[1]، إذ قد ترتكب الجريمة ويستعمل الحاسب الآلي ولا تكون أمام جريمة معلوماتية كمن يقوم بالاتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السرقة أو السطو على بنك أو لارتكاب أي جريمة اخرى، كما أنه قد لا نكون بالضرورة أمام جريمة معلوماتية إلا إذا ما تم الاعتداء على الحاسب الآلي ونظامه كمن يقوم بتخريب الوحدة المركزية لجهاز الحاسب الآلي أو أحد مكوناته المادية.

وباستقرائنا لمختلف التعريفات نجد أن تعريف التعاون الاقتصادي والتنمية (OECD) الخاص باستبيان الغش المعلوماتي عام 1982 والذي أوردته بلجيكا في تقريرها على أن الجرائم المعلوماتية هي: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[2]

و يتسم بالوضوح وذلك للأسباب التالية:

- تحديده لماهية السلوك الإجرامي للجريمة التي قد تقع به، إذ شمل كل من الفعل الإيجابي و السلوك السلبي المتمثل في الامتناع.
- تعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة الجرائم التقنية وذلك لربطه بين الجريمة وأي تدخل للتقنية المعلوماتية بصفة مباشرة أو غير مباشرة.
- يعبر عن الطابع التقني المميز الذي تنطوي تحته أبرز صور الجريمة المعلوماتية.
- يتيح إمكانية التعامل مع التطورات المستقبلية التقنية.

---

[1]–نائلة عادل محمد فريد قورة، المرجع السابق، ص31.

[2]–أحمد خليفة الملط، المرجع السابق، ص87 .

ونستخلص مما سبق أن اختلاف الفقه في وضع تعريف للجريمة المعلوماتية مرده الاختلاف في المعيار المعتمد عليه والزاوية التي ينظر إليها كل اتجاه لهاته الجريمة.

وقد اصطلح المشرع الجزائري على تسمية الجرائم المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها بموجب أحكام المادة 02 من قانون 09-04 [1] على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

ويمكن استخلاص من خلال استقراء التعريف المعتمد من طرف المشرع الجزائري الملاحظات الآتية:

- أن المشرع الجزائري اصطلح على الجرائم المعلوماتية بتسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة الواقعة على النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر 07 وترك المجال واسعا لأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.
- أن المشرع الجزائري لم يقم بتحديد درجة دور المنظومة المعلوماتية أو نظام الاتصالات الإلكترونية في ارتكاب هذه الجرائم إذ حسب التعريف فإنه يكفي بمجرد أن ترتكب الجريمة أو يسهل ارتكابها المنظومة المعلوماتية أو نظام الاتصالات الالكترونية، مما يجعل التعريف يشمل عدد كبير من الجرائم حتى تلك الجرائم التي يكون فيها للتقنية المعلوماتية دور ثانوي.
- كما أن المشرع الجزائري لم يحدد صور السلوك المجرم الذي يرتكب أو يسهل ارتكابه منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

[1] – ج.ر، العدد 47 ،ص05.

- أن هذا التعريف تضمن تكرار كون أن مفهوم نظام الاتصالات الإلكترونية يندرج تحت مصطلح المنظومة المعلوماتية ذلك أن المشرع الجزائري عرف هذه الأخيرة بموجب أحكام المادة 02 على أنها "نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين".

وحسب رأينا فإن تعريف الجريمة المعلوماتية الأقرب إلى الصواب هو كل اعتداء على النظام المعلوماتي أو كل اعتداء يتم باستخدام النظام المعلوماتي وكان له دور رئيسي في السلوك المجرم.[1]

الفرع الثاني: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي، وقد كان لظهور شبكة المعلومات وتطورها إلى الصورة التي أصبحت عليها الان فيما يعرف بالانترنت أثره في إعطاء شكل جدي للجريمة المعلوماتية.

ولعل أهم ما أضفته شبكة المعلومات على الجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود للجريمة، وسوف نحاول فيما يلي التطرق إلى بعض السمات الخاصة بالجريمة المعلوماتية .

أولا: السمات الخاصة بالجريمة المعلوماتية

تميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية من عدة جوانب، سواء كان هذا التمييز في السمات العامة أو كان في الباعث على تنفيذها أو في طريقة التنفيذ

[1]- نائلة عادل محمد فريد قورة، المرجع السابق، ص49.

ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تخطى آثار هذه الجريمة حدود الدولة الواحدة.

أ- السمات العامة للجريمة المعلوماتية

تتميز الجريمة المعلوماتية بمجموعة من الخصائص المميزة لها نوجزها فيما يلي:

- قلة عدد الحالات التي تم اكتشافها بالفعل مقارنة بما يتم اكتشافه من الجرائم التقليدية فعلى سبيل المثال أحصت وزارة الداخلية في فرنسا عام 1986 حوالي 1200 جريمة معلوماتية في حين كان هناك حوالي 53600 جريمة ضد الأشخاص و 18900 جريمة تندرج تحت وصف جرائم الآداب و3 مليون جريمة ضد الأموال[1].
- ارتفاع الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم التقليدية إذ حسب تقرير المركز الوطني للبيانات (NCCD) في بحث منشور عبر شبكات الأنترنت[2] في 21 جوان 1999 للباحث pernard D standlar أن إجمالي الخسائر الناجمة في الشهر بلغت حوالي 810000 دولار أي ما يساوي 800 مليون دولار سنويا، وتوصل مكتب التحقيقات الفيدرالي FBI إلى أن متوسط الخسارة التي تخلفها الجريمة المعلوماتية يبلغ حوالي 500000 دولار في حين لا تزيد الخسارة التي تخلفها جرائم السرقة العادية 3500 دولار[3].
- عدم اتسام الجريمة المعلوماتية بالعنف الذي تتميز به غيرها من الجرائم التقليدية، حتى أنه يقال أنه لا يوجد شعور حقيقي بعدم الأمان في مواجهة الجريمة المعلوماتية كالذي يوجد بصورة دائمة في مواجهة غيرها من الجرائم[4].

فالصورة التقليدية للمجرم تكاد تختفي في هاته الجرائم بل وعلى العكس من ذلك فالمجرم المعلوماتي عادة ما يكون ينتمي إلى مستوى اجتماعي مرتفع عن غيره من

---

[1] - نائلة عادل محمد فريد قورة، المرجع السابق، ص50 .

[2]- الباحث Pernard D standlar تحت عنوان Computer crime lawعام 1999 .

[3] -Rose (Philipe), la criminalité informatique à l'horizon 2005-analyse prospective, l'harmattan 1992 p49.

[4] -نائلة عادل محمد فريد قورة، المرجع السابق ، ص50.

المجرمين، ونادرا ما يكون محترفا للإجرام و عائد إليه كمجرم بالمعنى المتعارف لهذه الكلمة[1]، و ذلك لكون الأسباب والعوامل التي تقف وراء ارتكاب الجريمة المعلوماتية تختلف بالمقارنة بالجريمة التقليدية.

- اختلاف الجريمة المعلوماتية من حيث رد فعل المجني عليه اتجاهها واتجاه مرتكبها فمن ناحية فإن المجني عليه نادرا ما يقوم بالإبلاغ عنها وذلك لأسباب تتعلق بسمعة المؤسسة التي يمثلها ومخافة على زعزعة الثقة فيها[2].

كما أن للمجني عليه في الجرائم المعلوماتية دورا مثيرا للريبة في بعض الأحيان، فهو قد يشارك بطريق مباشر أو غير مباشر في ارتكاب الفعل وذلك بسبب وجوده في ظروف تجعل من قابليته للتعرض للجريمة مرتفع بشكل كبير ومرد ذلك إلى القصور الذي يكتنف أنظمة الحاسبات الآلية والذي يساعد في ارتكاب الفعل الإجرامي[3].

- غياب الشعور العام بعدم أخلاقية الفعل أو المساس بمصالح وقيم يحرص المجتمع على حمايتها بل إن الكثير من العاملين في مجال المعلوماتية لا يجدون حرجا في استعمال الشفرات والدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة أو نسخ البرامج بدلا من شرائها، وهذا لا ينفي وصف الجريمة على هاته الأفعال من حيث اعتدائها على مصالح لها أهميتها في المجتمع ومن تستحق الحماية القانونية ومعاقبة من يمس بها.

- وسيلة تنفي الجريمة المعلوماتية و تتميز في أغلب الحالات بالطابع التقني، مما يجعل أدلة الإدانة فيها غير كافية ويرجع ذلك إلى عدم وجود أي أثر كتابي، إذ يتم نقل المعلومات بالنبضات الإلكترونية بالإضافة إلى إمكانية الجاني تدمير دليل الإدانة في أقل من ثانية[4].

---

(1) –Wasik (martin), crime and the computer, oxford university press, 1991.p19

(2) –هشام فريد رستم، المرجع السابق، ص41.

(3) –Rose(philipe), op.cit.P53.

(4) –هشام فريد رستم، المرجع السابق، ص41.

ب- الطبيعة المتعدية الحدود الدولية للجريمة المعلوماتية

يمكن القول أن من اهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود، فيعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة.

فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، ولقد تميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة[1].

ومن القضايا التي لفتت النظر إلى البعد الدولي لجرائم الحاسبات الآلية، قضية عرفت باسم مرض نقص المناعة المكتسبة (الإيدز)، وتتلخص وقائعها عام 1989 في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)[2]، وكان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة ،يقوم الفاعل من خلالها بطلب مبلغ مالي حتى يتمكن المجني عليه من الحصول على مضاد الفيروس وفي الثالث من فبراير عام 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب تسليمه لمحاكمته أمام القضاء الإنجليزي حيث إن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة وبالفعل وافق القضاء الأمريكي على تسليم المتهم وتم توجيه له إحدى

---

(1) -E Recommendation No.R89-9 on computer crime and final Report of the European committee on Crime problems, Srasbourg 1++0,P83.

(2)- أحمد خليفة الملط، المرجع السابق، ص543.

عشرة تهمة ابتزاز وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية.

وأيا ما كان الأمر فإن لهذه القضية أهميتها من ناحيتين، الأولى: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية، والثانية: أنها المرة الأولى أيضا التي يتقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث (فيروس)[1].

ولقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي،

أم تلك التي يوجد بها المعلومات محل الجريمة أم تلك التي تضررت مصالحها نتيجة لهذا التلاعب.

كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة[2]،ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية وهو ما يقتضي أيضا تبادل المعلومات بين مختلف الدول وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية".

وتعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية وتجنب خلق ما يسمى "بجنة جرائم المعلوماتية " « Havens Computer Crime » إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي بطبيعة الحال إلى التنسيق بين قوانين الدول المختلفة لضمان تحقق "مبدأ ازدواجية

---

(1) –Clough (bryan) & mango (paul) approaching zero : data crime and the criminal underworld, 1992, pp.136-146.

(2)– نائلة عادل محمد فريد قورة، المرجع السابق، ص54.

التجريم"، إذ نجد أن هذا المبدأ يقف عقبة رئيسية طالما أن الكثير من القوانين لم يتم تعديلها حتى تتلاءم مع هذه الجرائم.

وتجدر الإشارة ان المشرع الجزائري قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون رقم 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات والذي استحدث بموجبه أحكاما خاصة بالجرائم الماسة بالأنظمة المعلوماتية من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، إضافة إلى قانون رقم 04/09 المؤرخ في 209.08.05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إذ تضمنت بعض القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال هذه الجرائم كما أنشأت هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته وسن أحكام خاصة بالتعاون والمساعدة القضائية الدولية[1].

ونستخلص مما سبق إلى أنه وفي سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المتخلفة في محورين:

الأول داخلي يتمثل في تلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.

الثاني دولي يتحقق عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرموا المعلوماتية عن عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى.

ثانيا: السمات الخاصة بالمجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، و إنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين.

---

[1]– وقد علق المشرع الجزائري التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على شرط احترام الاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل، ومن ثمة نستخلص أنه لا غنى عن الاتفاقات الدولية في مجال مكافحة هذه الجريمة.

و لقد اختلف الباحثون في تحديد هذه السمات[1]، و يعد الأستاذ **Parker** واحدا من أهم الباحثين الذين عالجوا الجريمة المعلوماتية بالدراسة بصفة عامة و بالمجرم المعلوماتي بصفة خاصة، و مع ذلك يعد المجرم المعلوماتي مجرما لارتكابه فعل إجرامي يتطلب توقيع العقاب عليه، و كل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء، و إن كانت في رأيه لا تتطابق معها.

فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه يكون على درجة من العلم و المعرفة[2].

و يتفق مجرمو المعلوماتية مع ذوي الياقات البيضاء في كون أن الفاعل في الحالتين يبرر جريمته كونه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.

و يتميز المجرم المعلوماتي بالإضافة إلى ذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و يرمز إليها الأستاذ **Parker** بكلمة**S.K.R.A.M** وهي تعني المهارة **Skills**، المعرفة **Knowledge**، الوسيلة **Resources**، السلطة **Anthority**، و أخيرا الباعث **Motives** [3].

و تعد **المهارة:** المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي،و التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين.

إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، بل إن الواقع العلمي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم

---

(1)– نائلة عادل فريد قورة، المرجع السابق، ص54.

(2)- ليس من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو الحال في جرائم ذوي الياقات البيضاء أنظر Suthreland (Eduin H) « Whithe collar criminality » Gers (Gilbert) in chite collar criminal The offender in business the professions atherton press 1968.

(3) –Parker (DonnB) Figding computer crime A new Framework for protecting information 1988/P 114.

يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما **المعرفة**: فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها بكامل ملابستها و مدى إمكانية نجاحها أو فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون له تصورا كاملا لجريمته ،كون أن مسرح الجريمة المعلوماتية هو النظام المعلوماتي[1]، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها و ذلك قبل تنفيذ جريمته.

أما **الوسيلة**: فيراد بها الإمكانيات التي يتزود بها الفاعل لارتكاب جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية في أغلب الحالات تتميز نسبيا بالبساطة و بسهولة الحصول عليها، كما أنه نظرا لمهارته و قدرته يستطيع حتى ابتكارها، إذ ان الواقع أثبت أنه كلما كان النظام المعلوماتي غير مألوف و يتميز بالخصوصية كانت الوسائل المتطلبة لارتكاب الجريمة أكثر صعوبة.

أما **السلطة**: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي و التي تمكنه من ارتكاب جريمته،و هذه السلطة إما تكون مباشرة كالشفرة الخاصة بالدخول إلى النظام المعلوماتي و التي تعطي للفاعل مزايا متعددة مثل فتح الملفات و محو ،تعديل محتوياتها ، مجرد قراءتها أو كتابتها.

و قد تتمثل هذه السلطة في حق استعمال الحاسب الآلي نفسه أو الدخول إلى مكان تواجده كما هو الحال في الشبكات الداخلية لبعض الإدارات مثلا.

و قد تكون هذه السلطة غير مباشرة كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

و أخيرا يأتي **الباعث** لارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق

[1] –نائلة عادل محمد فريد قورة، المرجع السابق، ص57.

غير مشروع يظل الباعث و بعد عرضنا لدوافع ارتكاب الجريمة المعلوماتية نتطرق في المطلب الموالي حتى نضبط مفهومها أكثر.

المطلب الثاني: أنواع الجرائم المعلوماتية

تعددت محاولات الفقه لتحديد أنواع الجرائم المعلوماتية و ذلك لصعوبة حصر هذه الأنواع بصفة دقيقة بالنظر لحداثة ظهور هذه الجريمة و كذا عدم و جود تعريف عام متفق عليه للجريمة المعلوماتية و تحديد مجالها و كذا بالنظر للتطور التكنولوجي في كل صوره للارتباط الوثيق بينهما.

و نظرا لذلك تعددت تقسيمات الجرائم المعلوماتية إلى طوائف مختلفة تتميز كل منها بسمات خاصة بها بالنظر إلى اختلاف المعيار المعتمد في التقسيم.

فهناك من قسم الجرائم المعلوماتية إلى ثلاث طوائف تتمثل في جرائم الحاسب الآلي الاقتصادية و جرائم الحاسب الآلي التي تنطوي على الاعتداء على حرمة الحياة الخاصة و أخيرا جرائم الحاسب الآلي التي تهدد المصالح القومية أو السلامة الشخصية للأفراد[1].

و قسمها آخرون بالاعتماد على معيار أنماط السلوك المختلفة التي تمثل الجريمة المعلوماتية و مدى اتفاقها أو اختلافها مع القواعد التي تحكم القانون الجنائي إلى ثلاث طوائف رئيسية تمثلت الأولى في الدخول و الاستعمال غير المصرح بهما لنظام الحاسب الآلي و الثانية تتمثل في طائفة الاحتيال المعلوماتي و سرقة المعلومات و الطائفة الأخيرة تتمثل في الجرائم التي يساعد الحاسب الآلي على ارتكابها و الأفعال التي تساعد على ارتكاب جرائم الحاسبات الآلية[2].

---

(1) –Sieber (Ulrich), Criminal liabijlity for the transfer of data in international computer network, New problems for German law, European journal of Crime, law and criminil justice, Vol. 34, 1997, bp 3-27.

(2) –Wasik (Martin),op, cit .p41.

و من الملاحظ أن هذه التقسيمات أو بعضها لم تراع بعض أو كل خصائص هذه الجرائم و موضوعها و الحق المعتدى عليه لاعتمادها على معيار واحد للتقسيم متناسية معايير أخرى.

و يرى البعض من الفقهاء أنه يجب مراعاة في كل محاولة لتقسيم الجرائم المعلوماتية اعتباران هما:

- التطور المستمر الذي يطرأ على الجريمة المعلوماتية بصفة عامة.
- معيار الجريمة المعلوماتية أي ما يدخل في إطار هذه الجرائم و ما يخرج منه[1].

و مراعاة للاعتبارين السابقين ذهب الفقه الراجح إلى تقسيم الجرائم المعلوماتية إلى طائفتين رئيسيتين بالاعتماد على محل الجرائم المعلوماتية التي تنصب على معطيات الحاسوب و تطال الحق المعلومات بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة إذ يستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسب الآلي.

و تتمثل الطائفة الأولى في الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي أما الطائفة الثانية تتمثل في الجرائم المعلوماتية الواقعة على النظام المعلوماتي، و هذا ما سنتطرق له بشكل من التفصيل من خلال الفرعين المواليين.

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

يشتمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، و يعد الحاسب الآلي في هذه الطائفة وسيلة لتسهيل النتيجة الإجرامية و مضاعفا لجسامتها.

و يهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعه[2]، إذ تهدف هذه الجرائم الاعتداء على أموال العير، فيستخدم المجرم المعلوماتي

---

[1] –نائلة عادل محمد فريد قورة، المرجع السابق، ص 256.

[2] – نائلة عادل محمد فريد قورة، المرجع السابق، ص 265.

ذاته أو برامجه أو نظمه كوسيلة لتنفيذ الجريمة، و منه لا يكون النظام المعلوماتي هو محل الحماية الجنائية.

تتعدد صور الجرائم المعلوماتية المرتكبة باستخدام النظام المعلوماتي بعضها ذكرها المشرع الجزائري، في حين أن البعض الآخر رأى الفقه إمكانية تطبيق القواعد القانونية القائمة في قانون العقوبات عليها، ونتعرض لهذا بالتفصيل:

أ- الجرائم المعلوماتية الواقعة على الأشخاص الطبيعية

تقع هذه الجرائم على الأشخاص و تنقسم بدورها إلى طائفتين بحسب نوع الحقوق المعتدى عليها و دور النظام المعلوماتي في اقترافها.

تتمثل الطائفة الأولى في الجرائم الواقعة على حقوق الملكية الفكرية و الأدبية، أما الطائفة الثانية تكمن في الجرائم الواقعة على حرمة الحياة الخاصة وسنتناولها فيما يلي:

أولا: طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية و الأدبية

يمكن أن يكون النظام المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية و الأدبية و مثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج نظام معلوماتي آخر، أو حالة تخزين و استخدام هذه المعلومات أو التفريط فيها دون إذن صاحبها، ذلك أن استخدام معلومة معينة دون إذن صاحبها يتضمن اعتداء على حق من الحقوق المعنوية إضافة إلى كونه اعتداء على قيمتها المالية كون أنه للمعلومة قيمة أدبية بجانب قيمتها المادية و يندرج ضمن الحقوق الفكرية كذلك براءات الاختراع، إذ تتمثل فكرة للمخترع تحتوي على حق معنوي و آخر مالي [1].

و قد نص المشرع الجزائري على حقوق الملكية الفكرية و براءات الاختراع في عدة نصوص قانونية نذكر من بينها:

- المادة: **38** من الدستور الجزائري التي تنص على أن " حرية الابتكار الفكري و الفني و العلمي مضمونة للمواطن".

[1] -أحمد خليفة الملط، المرجع السابق، ص 184.

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ و الإعلام إلا بمقتضى أمر قضائي ".

- الأمر **05/03** المؤرخ في **2003.07.19** المتعلق بحقوق المؤلف و الحقوق المجاورة. و الأمر **07/03** المؤرخ في **2003.07.19** المتعلق ببراءات الاختراع.

ثانيا: طائفة الجرائم المعلوماتية الواقعة على الحياة الخاصة

لقد كفلت جل الدول الحياة الخاصة لمواطنيها بالحماية و قد حذا الدستور الجزائري حذو الدساتير الدولية بحرصه على حماية الحياة الخاصة للمواطنين بموجب المادة: **39** من الدستور الجزائري و التي تنص على أنه " لا يجوز انتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، و يحميهما القانون ،سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة."

و لا شك أن الحاسبات الآلية بما لها قدرة فائقة على تخزين أكبر كم ممكن من المعلومات، أصبحت مخزنا لأهم المعلومات و أكثرها حساسية.

و لأهمية المعلومات التي تحتويها أنظمة الحسابات الآلية أصبح لهذه الحسابات دورا هاما في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة[1].

و عليه يمكن أن يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد، كأن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه، أو أن يجمع المعلومات بعلم الشخص المعني و لكن يقوم المكلف بحفظها بإطلاع الغير عليها بدون إذن صاحبها، أو أن يقوم شخص باختراق معلومات تتمثل في أسرار مكتوبة و سير ذاتية و مذكرات حياة شخصية لشخص آخر[2].

---

[1]- نائلة عادل محمد فريد قورة، المرجع السابق، ص275.

[2]- أحمد خليفة الملط، المرجع السابق، ص187.

كما أن مختلف التشريعات حمت الأسرار المهنية ذلك أن المعلومات التي توجد داخل النظام المعلوماتي تكون ذات طبيعة سرية، و منه يفترض توافر الثقة فيمن أوكلت إليه، فجل التشريعات ألزمت الطبيب و المحامي بالمحافظة على الأسرار التي يقرها لهما المريض أو الموكل في الدعاوى[1].

الفرع الثاني: الجرائم المعلوماتية الواقعة على النظام المعلوماتي

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية بالاعتماد على التصنيف الذي يقوم على محل الجريمة المعلوماتية يتمثل في الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي.

و هذا ما سنتطرق له بشيء من التفصيل من خلال الفروع الثلاثة الموالية:

أولا: جرائم الاعتداء على المكونات المادية للنظام المعلوماتي

يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة و المعدات الملحقة به و التي تستخدم في ارتكاب جرائم عادية و تقليدية[2]، كأن تكون محلا للسرقة ، خيانة الأمانة الإتلاف العمدي كإحراقها ، ضرب الآلات بشيء ثقيل أو حاد ،العبث بمفاتيح التشغيل أو خربشة الشريط و إفساد أسطوانات التشغيل مغناطيسيا بتعريضها إلى أي مجال مغناطيس متلف، و يترتب على هذا الإتلاف خسائر كبيرة[3].

---

[1] – أحمد خليفة الملط، المرجع السابق، ص200.

[2]– أحمد خليفة الملط، المرجع السابق، ص176.

[3]– ذكي أمين حسونة، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، في الفترة من 25 إلى 28 أكتوبر 1993 تقرير مصر، ص471 .

و من أمثلة ذلك ما حدث في فرنسا حيث أدى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة و توثيق المعلومات الحسابية إلى خسائر مالية معتبرة قدرت بـ **5** ملايين فرنك فرنسي[1].

و يرى البعض من الفقهاء أنه يندرج ضمن هذه الطائفة من الجرائم المعلوماتية سرقة وقت آلة، فقد يلجأ العاملين بالنظام المعلوماتي إلى استخدامه في أعمال خاصة بهم، و عليه تكون واقعة السرقة منصبة على وقت الجهاز الذي يكن تقويمه ماليا و ليس على الأشياء المادية بمعنى الكلمة[2].

و تجدر الإشارة أن خطورة واقعة السرقة لا تكمن في الشيء المسروق لضآلة قيمته، بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسارتها بأموال طائلة.

ب: الجرائم المعلوماتية الواقعة على البرامج التطبيقية

يقوم الجاني في هذه الصورة بتحديد البرنامج أولا ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية.

أولا: تعديل البرنامج: الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود و تكثير هذه الجرائم في مجال الحسابات[3].

و من أمثلة ذلك قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات و قام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم **Zzwick** و حصل على إثر ذلك على مئات الدولارات كل شهر و كان من الممكن أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول و آخر عميل له ليكتشف عدم وجود ما يدعى**Zzwick** [1].

---

(1) –Rose (philippe), OP–cit, p58,59.

(2) – André Lucas, le droit de l'informatique, paris, PUF 1987, P519,521.

(3) –أحمد خليفة الملط، المرجع السابق، ص173.

و هناك نظام آخر يسمى سلامي **Salami** و يتم الاختلاس بموجب هذا النظام باستقطاع مبالغ زهيدة و على فترات زمنية طويلة و متباينة من خلال صفقات عديدة يترتب عليها تحقيق فائدة كبيرة و قد حقق بموجب هذا البرنامج أحد المستخدمين الأمريكيين بإحدى المنشآت التجارية الكبرى يدعى **E.Royce** في خلال **6** سنوات ما يقرب من **2** مليون دولار[2].

ثانيا: التلاعب في البرنامج: يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة[3] أو عن طريق قيام أحد المبرمجين بزرع برنامج فرعي غير مسموح في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي، و يصعب اكتشاف هذا البرنامج لصغره و دقته[4].

ج: الجرائم المعلوماتية الواقعة على برنامج التشغيل

تعد برامج التشغيل تلك البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم و ضبط ترتيب التعليمات الخاصة بالنظام.

و تقوم الجريمة المعلوماتية في هذه الصورة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها باسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[5].

و يتحقق هذا النوع من الجرائم المعلوماتية في شكلين:

أولا: المصيدة: تتمثل هذه الصورة في إعداد المبرمج برنامج به أخطاء و عيوب عمدا، لا يكتشف بعضها إلا عند استخدام البرنامج، إذ يترك المبرمج ممرات خيالية و فواصل و فرغات في البرنامج يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرعات إضافية

---

(1) –Duleroy ® et rocco (A.M), l'inforamatique nouvelle, avril 1976, les escrocs a l'informatique, le nouvel Economsiste, les octobre, 1979, n202.

(2)– أحمد خليفة الملط، المرجع السابق، ص174.

(3) – أحمد خليفة الملط، المرجع السابق، ص545.

(4)–le rapport du conseil de l'Europe, 15, 18 novembre 1976.

(5)– أحمد خليفة الملط، المرجع السابق، ص175.

أو إحداث مخارج وسيطة للولوج داخل النظام المعلوماتي و الوصول إلى كل المعلومات التي تحويها الذاكرة.

و بهذه التقنية يمكن للمبرمج استخدام البرنامج في أي وقت وفق أهوائه، و بذلك يصبح هو المهيمن على النظام و على صاحب العمل المعتدى عليه[1].

ثانيا: تصميم برنامج وهمي

و تقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه مخصص خصيصا لارتكاب الجريمة و مراقبة تنفيذها، و من أمثلة ذلك قيام إحدى شركات التأمين الأمريكية في مدينة لوس أنجلوس بواسطة مبرمجيها تصميم برنامج وهمي يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم **46.000** بهدف تقاضي هذه الشركة من إتحاد شركات التأمين عمولات من نظيراتها[2].

ثالثا: جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي

للمعلومة المعالجة آليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي و لما لها من قيمة اقتصادية، و بهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها أو عن طريق إتلافها و هذا ما سنتناوله فيما يأتي:

أ- التلاعب بالمعلومات

يتم التلاعب في المعلومات الموجودة داخل النظام المعلوماتي بطريق مباشر أو غير مباشر.

فأما التلاعب المباشر يتم عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، و يأخذ هذا التلاعب عدة صور كضم مستخدمين غير موجودين بالعمل لاسيما في المنشآت التي تضم عددا كبيرا من العاملين المؤقتين و دائمي التغيير بهدف

---

[1]- محمد سامي الشوا، ثورة المعلومات وانعكساتها على قانون العقوبات،القاهرة،دار النهضة العربية،1994،الطبعة الثانية،ص82.

[2] -equity fuding life insurence, l(informatique nouvelle, mai 1976.

الحصول على مرتباتهم، أو بالإبقاء على ملفات مستخدمين تركوا العمل للحصول على مبالغ مالية شهرية أو عن طريق عمل تحويلات لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك و تسجيلها و إعادة ترحيلها و إرسالها لحساب آخر في بنك آخر بهدف اختلاس تلك النقود[1].

في حين التلاعب غير المباشر يتم عن طريق التدخل غير المباشر لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين أو بواسطة التخزين أو بواسطة التلاعب عن بعد باستخدام أدوات معينة و معرفة أرقام و شفرات الحسابات[2]،و يتخذ ذلك عدة صور من بينها التلاعب في الشرائط الممغنطة و قد قام في هذا الصدد أحد الموظفين بأحد فروع الشركة الفرنسية **Isoverst gobain** بإرسال شريط ممغنط يحتوي على **139** إذن دفع و عند معالجته بالبنك بالقسم المعلوماتي تم رفض نسخه لعيب في طول الشريط، و قد قال الخبراء أنه لو نجحت هذه العملية لتم النصب على البنك بحوالي **21** مليون فرنك فرنسي[3].

كما قد يتحقق التلاعب غير المباشر في المعلومات عن طريق التلاعب عن بعد باستخدام الجاني كلمة السر أو مفتاح الشفرة أو أداة ربط بالمركز المعلوماتي لأي جهة،

و تكمن خطورة هذه الصورة في إمكانية تسلل الجاني إلى المعلومات المخزنة بالنظام المعلوماتي والحصول على المنفعة المالية التي يريدها من مسافات بعيدة.

ب- إتلاف المعلومات.

قد يهدف الجاني من خلال ارتكابه الجريمة المعلوماتية إتلاف المعلومات المخزنة بالنظام المعلوماتي.

---

(1) –و قد تم ضبط مستخدم يعمل لدى فرع مصرفي تابع لبنك Indo–suej بفرنسا كونه حول مبالغ تقدر بسبعة ملايين فرنك فرنسي، لأكثر من التفاصيل أنظر .l'informatique nouvelle, mai 1976 n°73

(2)-أحمد خليفة الملط، المرجع السابق، ص179.

(3)– Trib de paris, 12 ème ch, corr, jugement du 13 janv 1982, DALLOZ S 1982, p502.

و يتخذ الإتلاف عدة صور فقد يتم عن طريق طرق الإتلاف العادية كالحرق أو الضرب أو السرقة أو عن طريق استبدال أو محو المعلومات، و يشكل استبدال المعلومات نوع من الجرائم الغش أو التزوير المعلوماتي و هو على درجة كبيرة من الخطورة لأنه بآخر أو إحلال رقم مكان آخر[1]، فمثلا هناك مجموعة من المستخدمين الإداريين استطاعوا خلال سنوات قليلة مضاعفة رواتبهم عن طريق النظام المعلوماتي[2].

الفرع الثالث: الجرائم المعلوماتية الواقعة على النظم المعلوماتية الأخرى

هذا النوع من الجرائم لا يستلزم تدخلا لإتلاف الوظائف الطبيعية للنظام المعلوماتي و لا تعديلا على المعلومات المعالجة، بل يقتصر في غالب الأحيان على الولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات و التصنت عليها لدى النظم المعلوماتية الأخرى بالإضافة إلى إساءة استخدام البطاقات الائتمانية و سوف نبين هاتين الصورتين كالآتي:

أولا: الولوج غير المشروع للمعلومات المعالجة آليا

تقوم هذه الصورة بوجود المجرم المعلوماتي داخل أحد المراكز المعلوماتية بهدف الولوج إلى المعلومات التي تمت معالجتها آليا و الإطلاع عليها من دون تصريح و قد يكون هذا الولوج إما مباشرا أو غير مباشر.

فأما الولوج المباشر فيعد من أكثر الأفعال المرتكبة و أسهلها تنفيذا و يتخذ عدة صور إذ يستطيع الجاني الاستيلاء على المعلومات المخزنة لدى الأنظمة المعلوماتية بعدة طرق باستخدام آلة الطباعة أو استخدام شاشة النظام أو الإطلاع على المعلومة بالقراءة على ما هو مكتوب عليها أو استخدام مكبر الصوت[3].

---

[1]- أحمد خليفة الملط،مرجع سابق، ص182.

[2]- محمد سامي الشوا، مرجع سابق، ص75.

[3] – أحمد خليفة الملط، مرجع سابق، ص190.

و من أمثلة الولوج المباشر قيام موظف سابق بأحد البنوك الفدرالية الأمريكية الذي كان يعمل في النظام المعلوماتي الخاص بالبنك نقل المعلومات المالية المخزنة في النظام و نقلها لرئيسه الجديد بعد حصوله على كلمة السر من زميل سابق له[1].

و أما الولوج غير المباشر ظهر بظهور تقنيات مستحدثة، لها صلة بالنظام المعلوماتي كالمعالجة عن بعد إذ أن هذه التقنيات أدت إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للولوج و الاستفسار عن بعد من المراكز المعلوماتية، إذ أنه أثناء حركتها و بثها تكون مهددة للالتقاط و التسجيل غير المشروعين في كل لحظة كتوصيل خطوط تحويلية لالتقاط المعلومات المتواجدة ما بين النظام المعلوماتي و النهاية الطرفية و إرسال المعلومات المختلسة إلى النهاية الطرفية عن طريق إشارات إلكترونية أو الولوج غير المشروع عن طريق نهاية طرفية بعيدة عن طريق نظام معلوماتي و معرفة كلمة السر أو مفتاح الشفرة المناسب[2].

ثانيا: إساءة استخدام البطاقات الائتمانية

أدى إدخال النظام المعلوماتي في مجالات عمليات البنوك إلى ظهور هذا النوع الجديد من الجرائم المعلوماتية.

و تعد من أخطر الجرائم المعلوماتية لاسيما في المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور و الحداثة، و يتخذ هذا النوع من الجرائم المعلوماتية صورتين.

تتمثل الأولى في إساءة استخدام العميل البطاقات الائتمانية و ذلك عن طريق عدم احترام العميل المصدر إليه البطاقات الائتمانية شروط العقد المبرم بينه و بين البنك كأن يستعمل بطاقة ائتمانية انتهت مدة صلاحيتها أو بطاقة تم إلغاؤها أو الشراء بأكثر من قيمتها....إلخ.

---

[1]- محمد سامي الشوا، مرجع سابق، ص67.

[2] – أحمد خليفة الملط، المرجع السابق، ص192.

و أما الصورة الثانية تتمثل في إساءة استخدام الغير البطاقات الائتمانية كأن يقوم سارق استعمال البطاقة الائتمانية للحصول على السلع و الخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة[1].

المطلب الثالث: أركان الجريمة المعلوماتية

مثل الجريمة العادية للجريمة الإلكترونية أركان تتمثل في:

الفرع الأول: الركن المادي

يتكون الركن المادي للجريمة الالكترونية من السلوك الإجرامي و النتيجة و العلاقة السببية مع العلم أنه يمكن تحقق الركن المادي دون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقق نتيجتها ، مثل إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة فرغم عدم تحقق النتيجة إلا أنه لا مناص من معاقبة الشخص و يتخذ الركن المادي عدة صور بحسب كل جريمة .

- **جريمة الغش المعلوماتي** : الركن المادي فيها هو تغيير الحقيقة في مستند رسمي أو محرر رسمي ، ولكن المستند هنا ليس مستند عادي يدخل ضمن أدلة الإثبات ، بل هي عبارة عن تسجيلات الكترونية أو محررات الكترونية .
- **جريمة الإرهاب الالكتروني و المواقع الإباحية و مواقع القمار**_: الركن المادي في هذه الجرائم هو إطلاق المواقع التي تحث إما على الانضمام إلى الجماعات الإرهابية ، كما تورد كيفية صنع القنابل اليدوية.

– أما المواقع الإباحية فتزود مواقعها بالصور و أفكار الشذوذ الجنسي و هناك مواقع تنشر فكرة الانتحار أو تشويه صورة الإسلام .[2]

---

[1]– أحمد خليفة الملط، المرجع السابق،ص196.

[2]– محمد أمين الرومي، جرائم الكمبيوتر و الانترنيت،الاسكندرية، دار المطبوعات الجامعية، 2003،طبعة الأولى، ص 182.

– أما مواقع القمار فهي لغسيل الأموال فالركن المادي هنا سلوك المجرم المعلوماتي في تزويد المواقع بالمعلومات اللازمة للانحراف أو القتل و هذا المجرم أقل من المخترق أو المتسلل ، هذا فيما يخص السلوك الإجرامي أما النتيجة فهي الأثر المادي المتمثل في انحراف المجتمع و تدمير الأخلاق و المعتقدات وظهور عادات غريبة على المجتمع زيادة إلى تفشي العنف فتصميم الموقع من طرف المجرم مرتبطة بالتأثيرات الخطيرة التي يتحمل عبؤها المجتمع من انحراف و هذا ما يعرف بالعلاقة السببية .

الفرع الثاني : الركن المعنوي

يعرف بأنه العلم بعناصر الجريمة و إرادة ارتكابها[1]و بالتالي يتكون هذا الركن من عنصرين هما العلم و الارداة .

– فالعلم :هو إدراك الأمور على نحو مطابق للواقع ، يسبق الإرادة .

– أما الارداة : فهي اتجاه لتحقيق السلوك الإجرامي .

ويتخذ القصد الجنائي عدة صور منها القصد العام و القصد الخاص .

القصد الجنائي العام : هو الهدف الفوري و المباشر للسلوك الإجرامي و ينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها .

القصد الجنائي الخاص : هو ما يتطلب توافره في بعض الجرائم فلا يكفي بمجرد تحقيق الغرض من الجريمة بل هو ابعد من ذلك أي انه يبحث في نوايا المجرم بطرحنا السؤال: ما هو الهدف الذي يريد الجاني تحقيقه من الجريمة ؟

فأي قصد يجب توافره في الجريمة الالكترونية ؟

إن المجرم الالكتروني يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بأركان الجريمة و بالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليون و أنهم قد تسللوا صدفة ، فلا انتفاء العلم كركن للقصد الجنائي ، كان يجب عليهم أن يتراجعوا بمجرد دخولهم و لا يستمروا في الاطلاع على أسرار الأفراد

[1] – عبد الله سليمان، شرح قانون العقوبات قسم عام الجزء الأول للجريمة،الجزائر، دار الهدى،2006،الطبعة الخامسة،ص43 .

و المؤسسات لأن جميع المجرمين و الأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية و معرفية كبيرة تصل في كثير من الأحيان الى حد العبقرية .

فالقصد الجنائي متوافر في جميع الجرائم الالكترونية دون أي استثناء و لكن هذا لا يمنع أن هناك بعض الجرائم الالكترونية تتطلب ان تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الانترنيت .

أما جرائم نشر الفيروسات عبر الشبكة فهي تتوفر على القصد الجنائي الخاص فالمجرم يهدف إلى تعطيل عمل الشبكة و في جميع الحالات المشرع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص.

الفرع الثالث: المجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره في تمييز المجرم المعلوماتى عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الاجرامى النمطي. وهذا ماسو ف نعرض له موضحين أهم سمات المجرم المعلوماتى ثم خصائصة المميزة وأخيرا لأنماط هذا المجرم وذلك على النحو التالي.

أولا: سمات المجرم المعلوماتي

يمكن أن نستخلص مجموعة من السمات التي يتميز بها المجرم المعلوماتي، والتي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين، ويعد الأستاذ parker واحد من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامه والمجرم المعلوماتي بصفة خاصة، ويرى parker أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة إلا انه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب علية.

وفيما يلي عرضا لبعض السمات العديدة للمجرم المعلوماتي والتي في الغالب تميزه عن غيره من المجرمين العاديين:

1- المجرم المعلوماتي مجرم متخصص

تبين في عديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يعكس أن المجرم الذي يرتكب الإجرام المعلوماتي هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

2- المجرم المعلوماتي مجرم عائد إلى الإجرام

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وأدت إلى تقديمهم إلى المحاكمة في المرة السابقة، ويودى ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة.

3- المجرم المعلوماتي مجرم محترف

يتمتع المجرم المعلوماتي باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر يقتضى الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.

4- المجرم المعلوماتي مجرم غير عنيف

المجرم المعلوماتي من المجرمين الذين لا يلجئون إلى العنف بتاتا في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام – الحيلة – فهو لا يلجا إلى العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدرا من العناء للقيام به.

فضلا عما تقدم ، فالمجرم المعلوماتي مجرم ذكى, ويتمتع بالتكيف الاجتماعي، أي لا يناصب أحد العداء وأيضا يتمتع بالمهارة والمعرفة وأحيانا كثيرة على درجة عالية من الثقافة.[1]

---

[1]- قراصنة أنظمة الكمبيوتر إعداد : دورثي إي. دينغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة : آمنة علي يوسف، ديسمبر 1998، ص 88.

ثانيا: خصائص المجرم المعلوماتي

يتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيرة من المجرمين، وهى:

1- المهارة

يتطلب تنفيذ الجريمة المعلوماتية قدرا من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال التكنولوجي، أو بمجرد التفاعل الاجتماعي مع الآخرين، وهذه ليست قاعدة في أن يكون المجرم المعلوماتي على هذا القدر من العلم ,وهذا ما اثبتة الواقع العملي أن جانب من انجح مجرمي المعلوماتية، لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام.

2- المعرفة

تميز المعرفة مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يكون تصورا كاملا لجريمته، ويرجع ذلك إلى أن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة.[1]

3- الوسيلة

ويراد بها الإمكانيات التي يحتاجها المجرم المعلوماتي لإتمام جريمته.

وهذه الوسائل قد تكون في غالب الأحيان، وسائل بسيطة وسهلة الحصول عليها خصوصا إذا كان النظام الذي يعمل به الكمبيوتر من الأنظمة الشائعة أما إذا كان النظام من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلى قدر من الصعوبة.

4- السلطة

يقصد بالسلطة، الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في

---

(1)- آمنة علي يوسف، نفس المرجع، ص90.

مواجهة المعلومات محل الجريمة.

وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الالى وإجراء المعاملات، كما أن السلطة قد تكون شرعية من الممكن أن تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

5- الباعث

وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويضل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية, ويرى البعض أيضا ما يخالف ذلك في أن الربح المادي لا يعد هو الباعث في أغلب الأحيان على ارتكاب جرائم المعلوماتية وإنما هناك أمور عديدة أخرى في الغالب تكون هي الباعث مثل الانتقام من رب العمل، وأيضا مجرد الرغبة قهر نظام الحاسب واختزا ق حاجزة الامنى[1].

- الأنماط المختلفة للمجرم المعلوماتي

يقسم مجرمي المعلوماتية (cybr criminals) إلي مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال إلي وجود عدد من الأنماط المختلفة لمجرمي المعلومات، نرصدها فيما يلى:

الطائفة الأولي(pranksters):

وهم الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم. ومن أمثلة هذه الطائفة صغار مجرمي المعلوماتية.

الطائفة الثانية(hackers):

وتضم الأشخاص الذين يستهدفوا من الدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول إليها كسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف اكتساب الخبرة وبدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

---

[1]- آمنة علي يوسف، نفس المرجع، ص92.

الطائفة الثالثة(malicious hackers):

وهؤلاء الأشخاص هدفهم إلحاق خسائر بالمجني عليهم، دون أن يكون الحصول على مكاسب مالية ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

الطائفة الرابعة(personal problem solvers):

وهم الطائفة الأكثر شيوعا من مجرمي المعلوماتية فهم يقومون بارتكاب جرائم المعلوماتية بحيث يترتب عليها في كثير من الأحيان خسائر كبيرة تلحق بالمجني عليه، ويكون الباعث في هذه الجريمة إيجاد حلول لمشاكل مادية تواجه الجاني لا يستطيع حلها بالطرق العادية.

الطائفة الخامسة(career criminals):

وهم مجرمي المعلوماتية الذين يهدفون من وراء نشاطهم الاجرامى تحقيق ربح مادي بطريق غير مشروع، ويقترب المجرم المعلوماتي من هذه الطائفة في سماته إلى المجرم التقليدي.

ومن جانب آخر، أكدت بعض الدراسات والأبحاث العلمية على أن فئات المجرمين(أو الجناة) تتحدر من:

- مستخدمو الحاسب بالمنازل.
- الموظفون الساخطون على منظماتهم.
- المتسللون ومنهم الهواة أو العابثون بقصد التسلية.
- المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته وتقع أغلب جرائم الانترنت حاليا تحت هذه الفئة بتقسيمها .
- العاملون في الجريمة المنظمة .

ويتمتع هؤلاء الجناة بصفات أخرى غير متوفرة فى الجناة العاديين نذكر منها:

- أعمارهم تتراوح عادة بين 18 إلى 46 سنة والمتوسط العمري لهم 25 عاما .
- المعرفة والقدرة الفنية الهائلة .

- الحرص الشديد وخشية الضبط وافتضاح الأمر .
- ارتفاع مستوى الذكاء ومحاولة التخفي .

ومن الجدير بالذكر فى هذا الصدد أن هناك اتفاق بين الخبراء والمتخصصين على أن جرائم الانترنت تمثل تحديا جديدا في عالم الجريمة، وذلك للأسباب التالية:

– صعوبة التعرف على هوية الجاني، فهو لا يترك أثرا لجريمته، وان وجد فقد لا تدل عليه.

– وجود بعض العقبات في محاكمة الجاني حال اكتشاف هويته إذا كان من بلد لا يعتبر ما قام به جرما.

– اتساع شريحة الجناة لتشمل صغار مستخدمي الانترنت، بسبب توفر الوسائل والبرامج المستخدمة في التخريب لصغار مستخدمي الانترنت، مما يجعل جرائم الانترنت لا تتطلب خبرة عالية.

– نقص الوعي بسلبية الاستخدام السيئ للانترنت، مما يجعل البعض ينظر للأعمال التخريبية على الانترنت – كاختراق المواقع – عمل بطولى.

المبحث الثاني: عوائق الاستدلال في الجريمة الإلكترونية

إن إثبات الجريمة من العقبات التي يعمل الخبراء على كسرها من أجل إيجاد وسائل لإثباتها و بالتالي فهي تتطلب خبرة فنية عالية و اعتماد أسلوب واضح لتحقيق و لكن قبل هذا يجب أن نبين نوعية الدليل في هذه الجرائم[1].

المطلب الأول: العوائق المتعلقة بالأدلة

لا يترك المجرم المعلوماتي أو الإلكتروني في الكثير من الأحيان آثار تقودنا إليه من أجل معاقبته، و هذا راجع لكون أن الجريمة مسرحها الشبكة العنكبوتية التي توصف بأنها عالم افتراضي، فكيف لعالم افتراضي أن يبقى على الأثر لحين اكتشافه [1] .

[1] – محمد أمين الرومي،المرجع السابق، ص 141 .

الفرع الأول: عدم ظهور الدليل المادي

كما وضحنا سابقا أن الجريمة المعلوماتية تتم ببيئة لا علاقة لها بالورق أو المحررات فعن طريق "كليك" (clique) بسيط يمكن تغيير الكثير من المعلومات في وقت قصير، فيصعب استخلاص الدليل المادي لهذه الجريمة، لأنه في عالم غير واقعي.

فهناك الكثير من المواقع التي تحث على الإرهاب و الانتحار و لا يعرف حتى مالكها الحقيقي، لذا فإنه لابد من وضع أجهزة مراقبة و برامج من أجل تفادي الاختراق والقرصنة، و تهيأ المحققين لتعامل مع المجرمين الذين يتمتعون بمؤهلات عالية.

و من مبررات عدم ظهور الدليل المادي هو أننا نتعامل مع معلومة–هذه المعلومة–هي الوسيلة لاقتراف الجريمة [2]المعلومة التي كانت في أصل فكرة، جسدت في قالب فني و قد أكدت إحصائيات أمريكية أن الموظفين العاملين بالمؤسسات التي تعتمد على نظام المعلوماتية هم الذين يقومون باختراق أجهزة المؤسسات و الإختلاص لدرايتهم بالثغرات الأمنية الموجودة و التعامل معها و بالتالي عدم إمكانية ظهور الدليل المادي و يعمل المجرم المعلوماتي على التخطيط الجيد من أجل عدم ترك الدليل المادي، حتى و إن تركه فإنه بإمكانه العودة و محوه قبل وصول أيدي العدالة إليه.

الفرع الثاني: انعدام الأدلة

لكل جريمة طريقة لاقترافها وكيفية معينة يستخلص منها الدليل لإدانة المجرم .فمثلا انتحال الشخصية في بطاقة الائتمان تتم عن طريق معرفة كلمة السر ، وتدمير معلومات أو العبث فيه يتم عن طريق الخرق الآلي .

فكل هذه الأفعال غير المشروعة ، الدليل فيها غير مرئي فقط لأن هؤلاء المجرمين يستخدمون أساليب و تقنيات عالية ، فقد تحولت أساليب النقل المعلوماتي من

---

[1] – محمد عادل ريان،جرائم الحاسب الآلي وأمن البيانات،الكويت،مجلة العربي ،1995،العدد440،ص 82.

[2] – عبد الفتاح بيومي حجازي ،الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، مصر،دار الكتب القانونية،2005، ص34 .

التمثيلي إلى الرقمي و أصبحت المعلومة عبارة عن نبضات الكترونية غير مرئية تجوب شبكات مشفرة.[1]

وقد وصلت ببعض العصابات الإيطالية من محترفي خرق الشبكة إلى تصميم برنامج للمحو التلقائي لأي أثر ناتج عن اختراقهم مما يؤدي بالضرورة إلى استحالة رؤية الدليل .

ومما يزيد من صعوبة عدم رؤية الدليل التالي :

- عندما تراجع الشركات التجارية معاملاتها فهي لا تهتم كثيرا باختراقات البسيطة لأنظمتها الموجودة على الشبكة .
- في بعض الأحيان النادرة قد يرى الدليل و لكن لا تقوم معظم الشركات التجارية بالتبليغ و هذا خوفا على سمعتها التجارية.
- ذكاء المجرم و تنوع أساليب الاحتيال و عدم الاهتمام بالوسائل الوقائية الأمنية ، يجعل من الصعب رؤية الدليل من أجل إدانة المجرم وسط هذا الكم المعلوماتي .

المطلب الثاني: مشاكل الاستدلال

كما ذكرنا سابقا فإن مشاكل إثبات الجرائم الالكترونية أنها تترك أثرا كما أنه يصعب الاحتفاظ بالآثار ، بحيث تعتمد على التقنيات العالية حيث يصعب الاستدلال فيها و مع صعوبة إثباتها ، إلا أن ما يزيد الوضع سوءا هو الإحجام على الإبلاغ و نقص الخبرة و هو ما سنحاول تبيانه في هذا الفرع .

الفرع الأول: عدم الإبلاغ

إن عدم الإبلاغ من طرف الأشخاص الذين شاهدوا المجرم عند قيامه بالجريمة هو ما زاد في عدم اكتشاف الجريمة ومن أسبابه نجد :

- عدم إبلاغ الشركات وخصوصا التجارية منها بعمليات الخرق التي يقوم بها المجرم المعلوماتي و هذا خوفا على سمعتها التجارية ، وهروب الزبائن من التعامل معها .[2]

---

(1) – لا يستطيع الإنسان قراءتها بل الآلة هي التي تقوم بذلك

(2)- أسامة أبو الحجاج ،دليلك الشخصي الى الأنترنت،القاهرة، دار نهضة ،1998،ص20.

- إن هذا الإبلاغ يتسرب إلى المجرم المعلوماتي و بالتالي تكشف الثغرات الأمنية في النظام المعلوماتي.
- نقص الغطاء تشريعي لهذه السلوكيات .

وقد يحدث أن يبلغ عن سلوكيات مشبوهة للمجرمين المعلوماتيين و لكن في الكثير من الأحيان إذ لا يمكن اكتشاف الشخص الذي قام بالسلوك الإجرامي، فمثلا جريمة نشر فيروس في الكثير من الأحيان لا يمكن اكتشاف الشخص الذي قام بنشره ومما يزيد من مشكل عدم الإبلاغ ما يلي :

- المعرفة المتأخرة من أن الجهاز أصيب بفيروس عن طريق الشبكة
- ضخامة الأضرار حيث أن الفيروس ليس مقيد برقعة جغرافية معينة
- تحويل الشبكة لساحة من المعارك بين الدول مما أصبحت المعاملات التجارية غنيمة سهلة للاختراق.

و على ضوء هذه الصعوبات عرضت بعض الاقتراحات على لجنة خبراء مجلس أوربا و لكن قوبل هذا الاقتراح بالرفض لأن الشركة التي تم التسلل لموقعها تصبح هي الجانية و ليست المجني عليها.

و من الصعوبات التي تواجه الإبلاغ أيضا هو عدم وجود شبكة دولية فعلية للتبادل المعلوماتي.

الفرع الثاني: نقص الخبرة

إن صعوبة اكتشاف الجريمة بالدرجة الأولي مرده نقص خبرة المحققين مما يضعنا أمام معادلة غير متكافئة طرفها أجهزة التحقيق بنقص خبرتها في مجال الكمبيوتر و الانترنت و الطرف الآخر قراصنة محتلون و منحلون أخلاقيا يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية .[1]

[1]- أسامة أبو الحجاج ،نفس المرجع،ص21.

و قد وصل بعض المجرمين المعلوماتيين الإطلاق على أنفسهم اسم النخبة أما رجال الشرطة فقد أطلقوا عليهم اسم الضعفاء و نلاحظ أن عملية سن التشريعات أبطأ من عملية الإجرام و هذا في العالم كله دون استثناء و من العوامل المساعدة في نقص الخبرة في الجرائم المعلوماتية هي :

- عدم تخصيص أموال من أجل التأهيل الجيد للمحققين.
- حداثة الجريمة و خصوصيتها التي لم يعتد عليها رجال الشرطة. مما جعلهم قاصرين في مواجهتها.
- ضخامة المعلومات الموجودة على الشبكة و انتشار أجهزة الكمبيوتر مما يصعب عملية التحقيق .
- الانترنت بيئة خصبة للسلوك الإجرامي .
- التطور السريع للتقنية الحديثة .
- عدم وجود هيئات قضائية مختصة .
- وجود مواقع على الشبكة تسهل عملية إرسال البريد الالكتروني دون الحاجة الى ذكر البيانات اللازمة مثل معرفة المرسل .

و يميل الفقه الجنائي إلى القول بضرورة تنمية الخبرة و المهارات للأشخاص المتخصصين لوضع مناهج مدروسة للتدريب على التحقيق إثباتها مراعين في ذلك خصوصية التطور التقني السريع دون إهمال التعاون الدولي في مثل هذه الحالات.

الفصل الثاني: الحماية الجزائية من الجريمة المعلوماتية وسبل مكافحتها

لابد من الاعتراف أن الإسهام في اقتراح حلول للإشكالات التي يطرحها موضوع الحماية الجزائية للمعلوماتية مهمة تعترضها صعوبة منهجية كبرى مصدرها اتساع وتشعب الجوانب التي تتعلق بالمعلوماتية، لذلك ارتأينا أن تكون نقطة الانطلاق من عنوان هذا الفصل، فنتعرض في المبحث الأول إلى الجوانب الموضوعية في نصوص الجريمة المعلوماتية، ونتعرض في مبحث ثاني للجوانب الإجرائية في نصوص الجريمة المعلوماتية.

المبحث الأول: الجوانب الموضوعية في نصوص الجريمة المعلوماتية

سنتناول في هذا المبحث الحماية الجزائية للجريمة المعلوماتية في ظل قانون العقوبات في المطلب الأول وإلى الحماية الجزائية من الجريمة المعلوماتية التي تطرق إليها نصوص الملكية الفكرية في المطلب الثاني[1].

المطلب الأول: الحماية الجزائية في ظل قانون العقوبات

لقد نص المشرع الجزائري في قانون العقوبات على المساس بأنظمة المعالجة الآلية أو ما يعرف بالغش المعلوماتي بموجب التعديل الذي تم بالنسبة لقانون العقوبات رقم 06/23 المؤرخ في 2006/12/20 المتضمن قانون العقوبات الجزائري في قسمه السابع مكرر، والذي شمل المواد من 394 مكرر إلى 394 مكرر7، متبعا في ذلك خطى التشريعات الغربية التي اتجهت في وقت متقدم إلى إصدار تلك النصوص المتعلقة بالجريمة المعلوماتية و من أهم تلك التشريعات نجد التشريع الفرنسي ولا ننسى أول اتفاقية حول الإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي و سنتطرق في الفرع الأول إلى جريمة المساس بأنظمة المعالجة الآلية للمعطيات أما الفرع الثاني خصصناه للتزوير المعلوماتي.[2]

الفرع الأول:جريمة المساس بأنظمة المعالجة الآلية للمعطيات

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي، وهو الفعل المنصوص والمعاقب عليه في المواد 394 مكرر إلى المادة 394 مكرر 7 ومن خلال دراسة نصوص هذه المواد لاحظنا أنّ المشرع الجزائري لم يعرف لنا نظام المعالجة الآلية للمعطيات وحسنا فعل لأنّها ليست من مهمة التشريع وإنما هي من مهمة الفقه ولذلك

---

[1]–عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري التحري والتحقيق،الجزائر، دار هومه ، 2012،الطبعة 3 ص175.

[2]–ج.ر ، العدد 84، القانون رقم 06/23 المؤرخ في 2006/12/24

اتجهنا للفقه الفرنسي والذي عرفه كما يلي كل مركب يتكون من وحدة أو مجموعة وحدات المعالجة والتي تتكون منها الذاكرة ،البرامج ،المعطيات و أجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية.[1]

وبالعودة إلى قانون العقوبات الجزائري، نجد أن الغش المعلوماتي يأخذ صورتين أساسيتان وهما:

*المساس بمنظومة المعلوماتية.

Information Introduction Dans Système

*صور أخرى من الغش المعلوماتي

Atteintes Au Système Informatique

أولا: الدخول في المنظومة المعلوماتية

ويشمل فعلين هما: الدخول والبقاء.

1-جريمة الدخول غير المشروع

تنص المادة 394 مكرر من قانون العقوبات الجزائري والتي تقابلها المادة 323/1 قانون عقوبات فرنسي على معاقبة كل من يدخل عن طريق الغش في اي جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذ ترتب على الدخول أو البقاء أو حذف أو تغيير معطيات المنظومة أو تخريب النظام.

أ-الركن المادي:

يتكون الركن المادي لهذه الجريمة من نشاط إجرامي يتمثل في فعل الدخول المرخص به إلى نظام المعالجة الآلية للمعطيات أو جزء منه.

ولم يحدد لا المشرع الجزائري ولا المشرع الفرنسي المقصود بالدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات ويمكن تعريفه بأنه كل فنيات الدخول الاحتيالي في

[1]-أمال قارة،الحماية الجزائية للمعلوماتية في التشريع الجزائري،الجزائر،دار هومة،2007،الطبعة الثانية،ص ص102.101.

منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لا حق له في ذلك مفتاح الدخول في منظومة.[1]

وقد أشار المؤتمر 15 للجمعية الدولية لقانون العقوبات المنعقد في البرازيل سنة 1994 بشأن جرائم الكمبيوتر إلى هذا المعنى أشار أن الدخول غير المرخص به التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن، كما انه لم يحدد كل منها وسيلة أو طريقة الدخول، لذا فإن الجريمة تقع بأي وسيلة كانت، فقد يلجأ الجاني إلى إدخال فيروس أو يدخل عن طريق استخدام كلمة السر mot de passe لشخص آخر أو عن طريق تجاوز نظام الحماية إذا كان ضعيفا، ويستوي أن يتم الدخول مباشرة أو بطريقة غير مباشرة كما هو الحال في الدخول عن طريق شبكات الاتصال التلفونية.

ولا عبرة لهذه الجريمة بصفة مرتكب الفعل الإجرامي، فقد يكون الفاعل يعمل في مجال الأنظمة المعلوماتية أو لا ،سواء كان يفهم أو لا يفهم أسلوب تشغيل النظام، فيكفي أن يكون الجاني ممن ليس لهم الحق في الدخول إلى النظام المعلوماتي حتى تتوفر جريمة الدخول غير المشروع[2]

وبالتالي فإن الركن المادي لجريمة الدخول غير المرخص به يتحقق بمجرد شروع أي شخص في الدخول أو الدخول الفعلي إلى نظام المعالجة الآلية للمعطيات بأي طريقة وتقع جريمة الدخول سواء تم الدخول إلى النظام كله أو جزء منه فقط، أي يكفي لتوافر الجريمة أن يتم الدخول على بعض عناصر النظام، كأن يتم الدخول إلى طرفيه الحاسب أو البرامج فقط، كما تقع الجريمة بمجرد الدخول دون اشتراط تحقيق النتيجة، فلا تشترط لقيامها مثلا التقاط متدخل المعلومات أو البرامج التي يحتويها النظام، بل إن

---

[1]–أحسن.بوسقيعة،الوجيز في القانون الجزائي العام،الجزائر،دار هومة، 2007،الطبعة الثالثة، ص445.

[2]– علي عبد القادر القهوجي، شرح قانون العقوبات، مصر، دار المطبوعات الجامعية، 2003، الطبعة الأولى، ص131.

الجريمة تقع حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام فجريمة الدخول غير المشروع من جرائم السلوك المحض.[1]

ب-الركن المعنوي:

يتمثل الركن المعنوي لجريمة الدخول في القصد الجنائي بعنصريه العلم والإرادة، فإن اتجهت إرادة الجاني إلى فعل الدخول أي أن دخول الجاني إلى نظام المعالجة الآلية للمعطيات كان بإرادته وليس بمحض الصدفة البحتة وكان يعلم بأنه يدخل إلى نظام المعالجة الآلية للمعطيات الخاصة بالغير دون أن يكون له الحق بذلك، ومن ثمة فإنه لايتوافر القصد الجنائي إذا كان دخول الجاني داخل النظام المسموح أي مشروع أو إذا وقع خطأ أو كان يجهل وجود حظر للدخول.

وبالتالي فإنه لقيام جريمة الدخول غير المرخص به يجب أن يتوافر بجانب الركن المادي نية الغش، ويقصد بالغش أن يباشر الفاعل سلوكه عن طريق الخديعة وسوء النية وبغرض خداع الغير، ولا يشترط توافر قصد جنائي خاص كما لا يشترط أن يترتب على دخول الجاني إلى نظام المعلومات تحقق نتيجة معينة ويمكن للقاضي الجزائي أن يستدل على توافر القصد الجنائي لدى الجاني إذا كان النظام المعلوماتي محاط بنظام أمني وقت اختراقه، فنظام الأمن لا يعدو إلا أن يكون وسيلة إثبات سوء نية من قام بانتهاك النظام ودخل بطريقة غير مشروعة.[1].

ثانيا: جريمة البقاء غير المشروع

نص المشرع الجزائري على هذه الجريمة في المادة 394 مكرر من ق.ع.الجزائري المقابلة لنص المادة 323/1 من ق.ع.الفرنسي ويقصد بالبقاء الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم اداء إتاوة.

وتقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل بعد، كما يجرم البقاء حتى ولو تم بصفة عرضية وجريمة البقاء غير المشروع كأي جريمة لابد من ان تتوفر على ركنين المادي و المعنوي .[2]

---

[1]- محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، الإسكندرية، الدار الجامعية للطباعة والنشر، 2004،ص101.

[2]-أحسن.بوسقيعة، مرجع سابق، ص445.

أ-الركن المادي:

يتخذ النشاط الإجرامي المكون للركن المادي صورة البقاء غير المشروع ويقصد به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول إلى النظام وذلك حين يكون الدخول إلى النظام مشروعا.

كما إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، يجب في هذه الحالة على المتدخلان أن يقطع وجوده وينسحب فورا وإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توفر ركنها المعنوي.

ويعتبر البقاء أيضا جريمة في الحالة التي يستمر فيها الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله أو في الحالة التي يطبع فيها نسخة المعلومات في الوقت الذي كان مسموحا له فيها الرؤية والاطلاع فقط.[1]

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الحالة التي لايكون فيها للجاني الحق في الدخول إلى النظام المعلوماتي ويدخل إليه فعلا ضد إرادة من له الحق في السيطرة عليه ثم يبقى داخل النظام بعد ذلك، وإذا كانت جريمة الدخول غير المشروع تتحقق منذ اللحظة التي يتم فيها الدخول فعلا للنظام المعلوماتي فإن جريمة البقاء تبدأ منذ اللحظة التي يبدأ الجاني في التجول داخل النظام المعلوماتي أو يستمر في التجول بعد انتهاء المدة المحددة له، فإذا دخل الجاني دخول غير مشروع وظل ساكنا فالفعل المجرم هنا دخول غير مشروع، أما إذا بدأ التجول فإن الفعل يصبح مكون لجريمة البقاء غير المشروع في نظام يعلم مسبقا أن مبدأ دخوله واستمرار البقاء فيه غير مشروع.

وقد نص المشرع الجزائري في المادة 394مكرر2 المقابلة للمادة 323/1 من قانون العقوبات الفرنسي على مضاعفة العقوبة إذا نتج عن البقاء إما محو أو تعديل معطيات النظام وإما عدم صلاحية النظام لأداء وظائفه.

---

[1]-علي عبد القادر القهوجي، مرجع سابق، ص133.

ويكفي لتوافر هذه الظروف وجود علاقة سببية بين البقاء غير المشروع وتلك النتيجة الضارة سواء محو أو تعديل معطيات النظام أو عدم قدرته على تنفيذ المعالجة الآلية للمعطيات، ويلاحظ أن القانون الفرنسي لا يشترط أن تكون النتيجة الضارة مقصودة لأنه نص على تجريم الاعتداء القصدي على النظام عن طريق جعله غير صالح للقيام بوظائفه في المادة323/3 باعتباره جريمة مستقلة[1].

1-الركن المعنوي:

هذه الجريمة مثل سابقتها جريمة عمدية لابد فيها من توافر قصد جنائي،ويكفي فيها توافر القصد العام فيجب أن يعلم الجاني بأنه يتجول في نظام المعالجة الآلية للمعطيات دون أن يكون له الحق في ذلك وأن تتجه إرادته إلى البقاء في نظام المعالجة الآلية للمعطيات، ولا عبرة بالباعث الذي يجعل الجاني يبقى على اتصال بنظام المعالجة الآلية للمعطيات غير المسموح له البقاء فيه، فقد يكون باعثه هو الفضول أو المزاح أو الحصول على المعلومات أو غير ذلك.[2]

وبالتالي إذا توفر الركن المادي الذي يتخذ صورة البقاء داخل النظام المعلوماتي والركن المعنوي المتمثل في القصد الجنائي العام بعنصريه العلم والإرادة قامت جريمة البقاء غير المشروع.[3]

ثالثا: المساس بمنظومة المعلوماتية

تتحدث المادة 394 مكرر 1 من قانون العقوبات الجزائري والتي تقابلها في النص الفرنسي المادة 323/3 من قانون العقوبات "كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية، أزال أو عدل بطريق الغش المعطيات التي يتضمنها....." وحتى تقع هذه الجريمة لابد من توافر الركن المادي والركن المعنوي.

---

[1]-سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، الاسكندرية ،دار الفكر الجامعي، 2007، ص93.

[2]-علي عبد القادر القهوجي، مرجع سابق،ص117.

[3]-مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية ماهيتها...مكافحتها، مصر ،دار الكتب القانونية، 2005 ،ص201.

1-الركن المادي:

يتمثل النشاط الإجرامي لهذه الجريمة كما هو واضح من نص المادة السابق في الإدخال، التعديل أو المحو وتنطوي هذه الأفعال على التلاعب في المعطيات والمعلومات التي يحتويها نظام المعالجة الآلية للمعطيات .

سواء بإضافة معطيات جديدة غير صحيحة ،محو أو تعديل معطيات موجودة من قبل ذلك ، فإن النشاط الإجرامي في هذه الجريمة يرد على محل و موضوع محدد وهو المعلومات والمعطيات التي تمت معالجتها آليا والتي أصبحت مجرد إشارات ورموز تمثل تلك المعلومات وليست المعلومات في حد ذاتها باعتبارها أحد عناصر المعرفة.

كما أن محل هذا النشاط الإجرامي يقتصر في تلك الجرائم عن المعلومات الموجودة داخل النظام والتي تشكل جزء منه.[1]

وبالتالي فالركن المادي لهذه الجريمة يتحقق إذا وقع اعتداء قصدي بالإدخال المحو أو التعديل على المعطيات الموجودة داخل النظام، ويكفي توافر أحد أفعال الاعتداء هذه ولا يشترط اجتماعها، وسنتعرض لهذه الأفعال على النحو التالي:

فعل الإدخال:

ويقصد بالإدخال إضافة معطيات جديدة على الدعامة سواء كانت خيالية أم كان يوجد بها معطيات من قبل، وقد يتم إدخال هذه المعطيات بقصد التشويش على صحة المعطيات القائمة ولعل اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولاسيما في المنشآت ذات الأموال، حيث يعد المسؤول عن النظام المعلوماتي في أفضل وضع يؤهله لارتكاب هذا النمط غير المشروع من التلاعب والذي يكون بضم مستخدمين تركوا العمل، وبالفعل قام أحد المسؤولين عن القسم المعلوماتي بإحدى الشركات الفرنسية بإعادة ملفات مستخدمين سابقين لهم حقوق مالية وقام بتحويلها إلى حسابه وحسابات أخرى قد تم فتحها خصيصا لهذا الغرض ليتم بعد ذلك اختلاس أكثر من مليوني فرنك فرنسي.[2]

---

[1]-علي عبد القادر القهوجي،مرجع سابق،142.

[2]-محمد أمين شوابكة،جرائم الحاسوب والأنترنت،عمان،دار الثقافة للنشر والتوزيع،2006،الطبعة الأولى،ص232.

وفي حادثة أخرى قامت شركة أمريكية بلوس أنجلس باصطناع برنامج وهمي مخصص لارتكاب فعل الغش المعلوماتي، فبفضل حاسبها الآلي ومعاونة مبرمجيها اصطنعت وثائق وهمية لعدد من الأموات (64000) اقتصر دورها على إدارة الحسابات وقامت بتغييرعنوانهم و وثائقهم لتبيعها بعد ذلك لأشخاص وحصلت مقابل ذلك على عمولات من شركات التأمين التي تعمل لحسابها كما قام الجناة بوضع شفرة خاصة في البرنامج لا تظهر في الطباعة إلا الوثائق السليمة تماما ليتمكنوا بعد ذلك من الاستيلاء على مبلغ قدره 200 مليون دولار من هذه العملية الوهمية.[1]

فعل المحو أو الإزالة:

يقصد بالمحو أو ازالة كل أو جزء من المعطيات الموجودة داخل النظام أو نقل وتخزين المعطيات إلى المنطقة الخاصة بالذاكرة، ويعتبر المحو جريمة إتلاف طالما وقع ثمة إتلاف أو تخريب لشيء موضوع الجريمة وتعطيله أيا كانت الوسيلة المستخدمة،فقد اعتبر المؤتمر الخامس عشر (15) للجمعية الدولية لقانون العقوبات المنعقد في البرازيل بتاريخ تشرين الأول 1994 بشأن جرائم الكمبيوتر في مقرراته وتوصيات أن الإدخال أو التعديل أو المحو يشكل جريمة تزوير، كما اعتبر المحو للبرامج أو المعلومات جريمة اتلاف.

فعل التعديل:

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، وقد يطال التعديل البرامج سواء برامج التشغيل أو التطبيق ويتم تعديل برامج التشغيل إما عن طريق المصيدة أو المداخل المميزة والتي هي عبارة عن ممرات خالية متروكة في برنامج ما يمكن من خلالها الدخول إلى التعليمات المخزنة في الكمبيوتر ومن ثمة التوصل إلى الشفرات والتعليمات أو عن طريق اصطناع برنامج وهمي أو ناقص من الناحية الفنية بإحداث فجوات في البرنامج حتى يمكن من استغلالها في ممارسة أفعال الغش.

[1]–كامل عفيفي، جرائم الكمبيوتر، لبنان، منشورات الحلبي الحقوقية، 2003، الطبعة الأولى،ص ص54،55 .

كما قد يتم تعديل البرامج التطبيقية لاختلاس الأموال ومثال ذلك أن مبرمج كان يعمل في أحد البنوك وقام بوسيلته الخاصة بتعديل برنامج إدارة الحسابات بإضافة 10 سنت لمصاريف إدارة الحسابات الداخلية عن كل 10 دولارات، دولار واحد على الحسابات التي تتعدى 10دولارات وتم قيد المصاريف الزائدة في حساب خاص وكان باسم مستعار، و هكذا حصل المبرمج على عدة مئات من الدولارات كل شهر و كان بالإمكان أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعامة إن يكافئ أول وأخر عميل له وفق الترتيب الأبجدي، وعند ئد اكتشف عدم وجود ذلك الاسم المستعار.

إن التعديل أو التغيير الذي يقع على المعطيات أو البرامج من شأنه أن يشكل جريمة التزوير والتي تقوم على تغيير الحقيقة بقصد الغش تغييرا يترتب عليه إلحاق الضرر بالغير، وهذا ما سنتكلم عليه لاحقا.[1]

2-الركن المعنوي:

يتمثل الركن المعنوي لجريمة الاعتداء القصدي على المعطيات في القصد الجنائي العام، ولا يشترط توافر القصد الجنائي الخاص إذ يكفي أن تتجه إرادة الجاني إلى الاعتداء على البرامج أو المعلومات بالإدخال أو التعديل أو المحو وأن يعلم بأن نشاطه ذلك يترتب عليه التلاعب في البرامج أو المعلومات.

وبالتالي فإنه إذا توفر القصد الجنائي العام بعنصريه العلم والإرادة إلى جانب الركن المادي تقع جريمة الاعتداء القصدي على المعطيات ويستحق مرتكب تلك الجرائم العقوبة المقررة لتلك الجريمة.

ويلاحظ أن المشرع الفرنسي وخلاف المشرع الجزائري نص على جريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات .

---

[1]-عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مصر ،دار الكتب القانونية، 2005، ص116.

وذلك في المادة 323/2 قانون عقوبات فرنسي، وإذا كانت الجريمة مثلها مثل جريمة الاعتداء القصدي على المعطيات تهدف إلى محاربة أفعال التخريب والقرصنة.

ومن التطبيقات القضائية لهذه الجريمة، قضي في فرنسا بأنه يقع تحت طائلة نص المادة 323/3 قانون العقوبات الفرنسي والتي تقابلها في القانون الجزائري المادة 394 مكرر 1.

تعمد إدخال فيروس المعلوماتية في برنامج الغير، وكذا الامتناع عن إخبار هذا الأخير بإدخال مثل هذا الفيروس، ولو حصل ذلك بصفة عرضية.[1]

كما يقع تحت طائلة النص المذكور، تعمد تعديل أو إزالة التي يتضمنها نظام المعالجة الآلية.[2]

رابعا: صور أخرى للغش المعلوماتي

تضمن نص المادة 394 مكرر 2 من قانون العقوبات الجزائري بتجريم الأعمال التالية:

تصميم أو بحث ، تجميع ، توفير ، الاتجار في معطيات مخزنة ، معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السالفة الذكر.

*حيازة ، إفشاء ، نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم الغش المعلوماتي.

كما نصت المادة 6 من اتفاقية بودابست على جريمة الاستخدام غير المشروع للمعطيات على معاقبة كل من يقوم عمدا بإنتاج أو استعمال أو استيراد أو توزيع برنامج حاسوب بغرض ارتكاب ، كلمة سر ، رمز وصول أو بيانات مماثلة بغرض ارتكاب الجرائم المنصوص عليها في المواد 2 إلى5 ولايشترط اجتماع تلك الجرائم بل يكفي توافر إحدى تلك الجرائم، إلا أنه يجب لقيام تلك الجريمة توافر ركنين مادي ومعنوي.

---

(1) –أحسن بوسقيعة، مرجع سابق، ص446.

(2)– أحسن بوسقيعة، مرجع سابق، ص446.

1- الركن المادي:

يتكون الركن المادي من نشاط إجرامي يتمثل في تصميم أو بحث أو تجميع أو توفير ، نشر ، الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم، كما يتخذ النشاط الإجرامي في جريمة الاستخدام غير المشروع للمعطيات صورة حيازة ، إفشاء ، نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

ويزداد الأمر خطورة إذا تعلق الأمر بالمعطيات المتعلقة بالحياة الخاصة كتلك المتعلقة بالحالة الصحية للشخص ، المتعلقة بوضعه المالي ، معلومات ذات صلة بانتماءاته السياسية أو الحزبية، فمن شأن حيازة هذه المعلومات ، إفشائها ، نشرها او استعمالها في أي غرض بعد الحصول عليها عن طريق الدخول غير المصرح به أن يشكل خرق للحياة الخاصة.[1]

2- الركن المعنوي:

إن جريمة الاستخدام غير المشروع للمعطيات جريمة عمدية يتخذ فيها الركن المعنوي صور القصد الجنائي العام بعنصريه العلم والإرادة، فيجب إرادة الجاني إلى ارتكاب الأفعال المشكلة لجريمة الاستخدام غير المشروع للمعطيات، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه استخدام غير المشروع للمعطيات.

ولا يشترط لتوافر الركن المعنوي قصد جنائي خاص، بل أن الجريمة تقوم بمجرد القيام بأحد الأفعال المكونة للنشاط الإجرامي مع علمه واتجاه إرادته إلى ذلك.[2]

- العقوبات المقررة لجرائم الاعتداء على نظم المعالجة الآلية للمعطيات

قرر كل من المشرع الجزائري في المواد 394 مكرر إلى المادة 394 مكرر7 والمشرع الفرنسي في المواد 323/1 إلى المادة323/7 من قانون العقوبات الفرنسي

---

[1] –أمال قارة، مرجع سابق، ص128.

[2]– أمال قارة، مرجع سابق، ص131.

عقوبات مقابلة لجرائم الاعتداء على نظم المعالجة الآلية للمعطيات، وهناك عقوبات أصلية وعقوبات تكميلية.

اولا: العقوبات الأصلية

باستقرائنا لنصوص مواد قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر7 اعتمدنا على جدول توضيحي بسيط لمختلف العقوبات المقررة للجرائم التي تناولتها في الفرع الأول:

الجريمة	العقوبة المقررة له	المادة المعاقبة
• الدخول في منظومة معلوماتية أو البقاء فيها. • تخريب نظام اشتغال المنظومة المعلوماتية	الحبس3: أشهر.....سنة الغرامة50.000:إلى 200.000دج الحبس6: أشهر.....سننتين الغرامة50.00 إلى 300.000دج	394 مرر 394 مكرر
• المساس بالمنظومة معلوماتية	الحبس: شهرين.....3 سنوات الغرامة500.000: إلى 4.000.000دج	394 مكرر1
• صور أخرى للغش المعلوماتي: –تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن إن ترتكب بها إحدى جرائم الغش المعلوماتي السالفة الذكر. – حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المحصلة من إحدى جرائم الغش المعلوماتي	الحبس: شهرين.....3سنوات الغرامة: 1.000.000 إلى10.000.000دج	394 مكرر2

ثانيا: العقوبات التكميلية

نص المشرع الجزائري في المادة 394 مكرر 6 من قانون العقوبات الجزائري على بعض العقوبات التكميلية يحكم بها القاضي إلى جانب العقوبات الأصلية لكل جريمة وتمثلت تلك العقوبات في[1]:

-المصادرة.

-إغلاق المواقع.

-غلق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

-مصادرة الأشياء التي استخدمت أو كان من شأنها أن تستخدم في ارتكاب الجريمة أو الأشياء الناتجة عن الجريمة.

-غلق المؤسسة أو المؤسسات التي ساهمت في ارتكاب الجريمة مدة لا تتجاوز خمس سنوات.

-الاستبعاد من التعامل في الأسواق العامة مدة لاتتجاوز خمس سنوات.

-الحرمان من إصدار الشيكات مدة لاتتجاوز خمس سنوات.

-نشر الحكم أو لصقه طبقا للشروط المنصوص عليها في المادة 131/35[2].

الفرع الثاني: جريمة التزوير الالكتروني

إن التعديل أو التغيير الذي يقع على المعطيات أو البرامج من شأنه أن يشكل جريمة تزوير والتي تقوم على تغيير الحقيقة بقصد الغش تغييرا يترتب عليه إلحاق الضرر بالغير ويلاحظ أن المشرع الفرنسي بعد تعديل قانون العقوبات لسنة 1988 وصدور قانون العقوبات لسنة 1994 عدل المادة 441/1 لكي تستوعب بجانب التزوير العادي جريمة التزوير الالكتروني حيث نصت بعد تعديلها على:

---

[1] -أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري،الجزائر ،دار هومة، 2007،الطبعة الأولى، ص98.

[2]- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، بيروت ،دار البداية البيضاء ،2007،الطبعة الأولى،ص55.

"إن كل تغيير للحقيقة بطريق الغش....في محرر مكتوب أو في أي دعامة أخرى تحتوي تعبير عن الفكر" فالمشرع فصل بذلك بين التزوير في البيانات المسجلة في ذاكرة الكمبيوتر وبين التزوير في محررات نظام المعالجة الآلية للمعلومات حيث أفرد نص خاص، للصورة الأولى بينما احتوت الصورة الثانية في النص العام لجريمة التزوير. [1]

ونجد المشرع الجزائري لم يتكلم عن التزوير المعلوماتي لذلك سنتطرق إلى تحديد جريمة التزوير المعلوماتي (الفقرة الأولى) وموقف المشرع الجزائري من التزوير المعلوماتي (الفقرة الثانية).

أولا: تحديد جريمة التزوير الإلكتروني

إن موضوع التزوير هو المحرر الذي لابد من توافر شروط فيه تتمثل في الكتابة من قبل شخص وأن ينتج أثاره القانونية هذه من الناحية التقليدية لجريمة التزوير لكن في مجال المعلوماتية فالأمر يختلف فجريمة التزوير الالكتروني تقع على المستندات الالكترونية، وقد أدرج المشرع الفرنسي في نص المادة 441 الخاص بالتزوير كل صور التزوير الحديثة التي تنشأ عن استخدام الحاسوب كما أن الغاية من تجريم أفعال التزوير هو حماية الثقة العامة التي تنشأ من تعامل الأفراد بالمحررات بمفهومها التقليدي ووضع نص خاص بالتزوير الالكتروني يحقق الحماية للنظام الالكتروني فقط دون الحفاظ على الثقة العامة وبذلك فإن المحررات المعلوماتية تخرج من المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها، لذلك إلغاء النص يخضع المحررات المعلوماتية إلى النصوص التقليدية الخاصة بالتزوير بالمفهوم الجديد للمحررات.

ثانيا: موقف المشرع الجزائري من جريمة التزوير الالكتروني

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير الالكتروني الذي يعتبر من أخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسوب الآن، ونجد أن المشرع الجزائري تكلم عن التزوير الخاص بالمحررات في الأقسام الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من

[1]–عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت،القاهرة، دار النهضة العربية،2009، ص104.

قانون العقوبات في المواد 214 إلى 229 التي تشترط المحرر لتطبيق جريمة التزوير ولم يتخذ أي موقف لتوسيع مفهوم المحرر من أجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير، وكان من الأفضل لو أضاف المشرع الجزائري نصا خاصا بالتزوير الالكتروني مثلما قام به المشرع الفرنسي.[1]

المطلب الثاني: الحماية الجزائية من الجريمة المعلوماتية في ظل نصوص الملكية الفكرية والملكية الصناعية

إن نسبة الحماية الجزائية من الجريمة المعلوماتية من خلال قانون العقوبات وذلك نتيجة للطبيعة المميزة للمال الالكتروني، ولما كانت الحاجة ملحة وضرورية لحماية برامج الحاسوب الآلي التي تعد من المال الالكتروني، كان لابد من التشريعات من خلق آليات قانونية للتصدي للظواهر الإجرامية المتنوعة ضد برامج الكمبيوتر ووضعت جزاءات تعاقب على مختلف الجرائم الماسة بها، وشملت هذه الحماية نصوص الملكية الفكرية وخاصة قانون حقوق المؤلف وقانون الملكية الصناعية وبالأخص قانون الاختراع المطبق في بعض الدول كالولايات المتحدة الأمريكية واليابان على عكس المشرع الجزائري الذي لا يعتبر البرامج من قبيل الاختراعات مما يجعلها غير قابلة للحماية.[2]

وعليه سنتناول في هذا المبحث إلى الحماية الجزائية برامج الكمبيوتر من خلال نصوص الملكية الفكرية من خلال الفرع الأول، ونتطرق في الفرع الثاني إلى الحماية الجزائية لبرامج الكمبيوتر من خلال نصوص الملكية الصناعية.

الفرع الأول: الحماية الجزائية لبرامج الحاسوب من خلال نصوص الملكية الفكرية

يعتبر حق المؤلف من أبرز صور الملكية الفكرية وأهمها، لذلك قامت العديد من الدول سواء عبر تشريعات داخلية أو اتفاقيات دولية بإقرار حماية قانونية لحق المؤلف

---

[1]– جعفر حسن جاسم الطائي، مرجع سابق،ص188.

[2]– محمد حسنين في الملكية الفكرية،الجزائر، المؤسسة الوطنية للكتاب،1985 ، ص132.

وسايرها المشرع الجزائري في ذلك والذي أصدر عدة قوانين لحماية حق المؤلف أحدثها الأمر رقم 03/05 الموافق لـ 19 يوليو 2003.

فنجد أن المشرع الجزائري من خلال نص المادة الرابعة من الأمر رقم 03/05 قد نص صراحة على اعتبار برامج الكمبيوتر كمصنفات أدبية محمية وكذلك القانون الفرنسي الصادر في 3 يوليو 1985.

ونظرا لما تتعرض له برامج الكمبيوتر، من جرائم متعددة ومتنوعة فإن أغلب التشريعات المعاصرة الخاصة بحماية حقوق المؤلف لم تخلو من الحماية الجزائية لكون الحماية المدنية لا تردع هذه الاعتداءات الخطيرة فالحماية الجزائية لما تشتمل عليه من قوة وردع زاجرة تكفل حماية أكثر فعالية لحق المؤلف حيث نص المشرع الجزائري في المواد 151 إلى 159 من قانون رقم 03/05 على جرائم وعقوبات الاعتداء على حقوق المؤلف، وهذا ما أورده كذلك المشرع الفرنسي من جرائم وعقوبات بموجب المادة 335/2 من الأمر رقم 01/657 الصادر في 14 سبتمبر 2001.

لذلك ستقتصر دراستنا في هذا المطلب على الاعتداءات الواردة على برامج الكمبيوتر (الفقرة الأولى) وفي (الفقرة الثانية) نخصصه للجزاءات المقررة لتلك الجرائم.[1]

أولا: الاعتداءات الواردة على برامج الكمبيوتر

ومن تلك التشريعات التشريع الجزائري الذي جرم الاعتداء على حقوق المؤلف بما فيها حقوق مؤلفي البرامج، وذلك في المواد 151،154،155، من الأمر 03/05 المتعلق بحقوق المؤلف والحقوق المجاورة، أما المشرع الفرنسي فنص عليها في المادة 335/02 من الأمر 01/657 المتعلق بحقوق المؤلف والحقوق المجاورة، أما المشرع المصري فنص عليها في نص المادة 47 من القانون 92/38.

وما يلاحظ أن المشرع أدخل جميع جرائم الاعتداء على حقوق المؤلف بما فيهم مؤلفي البرامج تحت وصف جنحة التقليد وإن كان لا يطبق عليها جميعها ذلك الوصف.

[1]–محمد حسنين ، نفس المرجع ، ص125.

1- جريمة التقليد

لم يضع المشرع في مختلف الدول تعريفا لجريمة التقليد، وكل ما فعله هو أنه بين فقط الأفعال التي تشكل جريمة التقليد، أما الفقه فقد تباين في تعريفها، ومن بينها اعتداء مباشر أو غير مباشر على حقوق المؤلف الأدبية أو المالية المحمية لقانون حق المؤلف ولقد نص المشرع الجزائري في المادة 151 من الأمر 03/05 على أنه يعد مرتكب لجنحة التقليد كل من يقوم بالكشف غير المشروع للمصنف أو يمس بسلامته، أو يقوم باستنساخ مصنف ، يقوم باستيراد ، تصدير نسخ مقلدة منه ، يقوم بتأجير أو وضع رهن التداول لنسخ مقلدة أما المادة 154 منه فقد نصت على أنه يعد مرتكب لجنحة التقليد كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف، ونصت المادة 155 منه على أنه يعد مرتكب لجنحة التقليد كل من يرفض عمدا دفع المكافئة المستحقة للمؤلف.

والحقيقة أن كل الأفعال السابقة لا يصدق عليها وصف جنحة التقليد بل هي جرائم ملحقة بجريمة التقليد.

- تتكون جريمة التقليد من ركن مادي وركن معنوي.

أ-الركن المادي:

يتمثل محل النشاط الإجرامي لجريمة التقليد بصفة عامة في المصنف المحمي ولذا أضاف المشرع الجزائري برامج الكمبيوتر كمصنفات محمية قانونا وذلك من خلال حقوق المؤلف والحقوق المجاورة من خلال الأمر 03/05 والذي نص عليها في المادة الرابعة منه صراحة كمصنفات أدبية مكتوبة محمية.[1]

وتماشيا مع ذلك تطلب المشرع الجزائري معيار الابتكار أو الإبداع لحماية المصنف، وذلك في المادة 3 من الأمر 03/05 المتعلق بحقوق المؤلف والحقوق المجاورة، والمشرع الفرنسي في المادة 111/1 من قانون الملكية الفكرية إلى معيار الابتكار والإبداع، ونصت على مايلي:

[1]- عبيد الكعبي، مرجع سابق، ص155.

« **L'auteur d'une de l'esprit, du seul fait de sa création** »

ويعتبر عنصرا أساسيا لحماية الملكية الفكرية في الاتفاقيات الدولية، إلا أن تطبيق الطابع الشخصي للابتكار على برامج الكمبيوتر تعترضه عدة صعوبات أهمها أن برامج

الكمبيوتر أشياء مخصصة لإيجاد حلول لمسائل تقنية في مجال معين أو تطوير البرامج السابقة، وليست الغاية منها التعبير عن أفكار المؤلف وإظهار شخصيته من خلال مصنفه.

أما النشاط الإجرامي لجريمة التقليد فلقد نص المشرع الجزائري في المادة 151/1 على أنه يعد مرتكب لجنحة التقليد كل من يقوم بالكشف غير المشروع عن مصنف أو يمس بسلامته، أما الفقرة الثانية فنصت على أنه يعد مرتكب لجريمة التقليد كل من يقوم باستنساخ مصنف بأي أسلوب من الأساليب في شكل نسخ مقلدة من خلال استقراء نص المادة نجد أن النشاط الإجرامي لجريمة التقليد يتمثل في الاعتداء على حق من حقوق المؤلف والمتمثل فيما يلي[1]:

*الكشف غير المشروع للمصنف: للمؤلف وحده الحق في تقرير نشر مصنفه من عدمه،واختيار الوقت والطريقة التي بها إذاعة أو نشر برنامجه، ومن ثمة فإن أي إضافة ترد على البرنامج من شخص دون إذن المؤلف يعتبر اعتداء على سلامة البرنامج وهذا يشكل جريمة التقليد[2].

ب- الركن المعنوي:

جريمة التقليد جريمة عمديه يجب لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة وعلى ذلك فإن الركن المعنوي لجريمة تقليد البرامج يتحقق بتوافر القصد الجنائي العام دون الحاجة إلى توافر سوء النية، فيكفي أن يعلم الجاني بأن نشاطه الإجرامي يرد

---

[1] -عبيد الكعبي، مرجع سابق، ص157.

[2] - محمد حسام لطفي، النظام القانوني لحماية الحقوق الذهنية ، عمان، دار الثقافة للطباعة والنشر،1987، ص83.

على برنامج منسوب لشخص آخر وإن ما ينسخه من البرامج بدون وجه حق وأن تتجه إرادته إلى النشر أو الاستعمال أو النسخ حتى يتوافر القصد الجنائي.[1]

2- الجرائم الملحقة بجرائم التقليد

ولقد نصت على هذه الجرائم في التشريع الجزائري لحقوق المؤلف والحقوق المجاورة في المادة 151 في الفقرات 3،4،5، أما في التشريع الفرنسي فإنه نص عليها في المادة 335/2 من قانون العقوبات وبالرجوع إلى التشريع الجزائري والفرنسي لحقوق المؤلف المجاورة.

3 -جريمة التعامل في البرامج المقلدة

نصت المادة 151 ف3،4،5، من قانون حقوق المؤلف والحقوق المجاورة ولابد من قيام هذه الجريمة توافر الركن المادي والركن المعنوي.

أ- الركن المادي:

يشمل الركن المادي في هذه الجريمة في التعامل في البرامج المقلدة، سواء تم التقليد للبرامج في الداخل أو في الخارج، ويكون البرنامج مقلدا إذا كان مشابها للبرنامج الأصلي الذي يحميه القانون وبمعنى آخر يقوم التقليد على محاكاة للبرامج تتم فيه المشابهة بين البرنامج الأصلي والنسخة المقلدة، فالعبرة بأوجه الشبه لا بأوجه الاختلاف بحيث يكون من شأنه أن ينخدع به الجمهور، ويتخذ كل صور الاعتداء على كل حق من حقوق المؤلف السابقة الذكر.

ولقد نص كل من المشرع الجزائري والفرنسي والمصري على صور التعامل المجرمة التالية:

استيراد أو تصدير برامج مقلدة، ونص عليه المشرع الجزائري في الفقرة الثالثة من المادة 151 من الأمر رقم 03/05 المتعلق بحقوق المؤلف والحقوق المجاورة، ولم يكتفي المشرع بتجريم فقط أفعال التعامل ببرامج المقلدة داخل الإقليم الوطني وإنما ذهب إلى تجريم أفعال إدخال مصنفات إلى خارج الإقليم الوطني أي استيرادها وكذا تصديرها من

[3]-محمد العقاد، جريمة التزوير في المحررات الحاسب الآلي، القاهرة ، دار النهضة العربية، 1995،ص36.

التراب الوطني وبالتالي فإنه متى كانت الأفعال المتابع بشأنها تعد أعمال استيراد أو تصدير لبرامج مقلدة اعتبر ذلك جريمة تقليد يعاقب عليها القانون كما يعتبر تقليد عرض المصنفات المقلدة المستوردة أو إعدادها بغرض تصديرها سواء تعلق الأمر بمصنفات وطنية أو أجنبية على نشر ، استعمال و ترجمة للبرنامج، و لا يشترط أن تكرر عمليات البيع لتوافر الجريمة، بل يكفي لقيامها عملية بيع واحدة أما عن العرض من أجل بيع البرامج المقلدة فلقد جرمها المشرع الجزائري كذلك و أراد من تجريم ذلك تفادي حصول البيع و لم يشترط المشرع أن يتم هذا العرض في مكان خاص لذلك متى وجد الشخص يقوم بعرض برامج مقلدة في أي مكان فالجريمة قائمة في حقه، و يقوم مقام هذا العرض القيام بالدعاية له في قائمة معروضات أو نشرات تجارية[1].

و لم يشترط المشرع أن يتم هذا العرض في مكان خاص لذلك متى وجد الشخص الذي يقوم بعرض برامج مقلدة في أي مكان فالجريمة قائمة في حقه و يقوم مقام هذا العرض القيام بالدعاية له في قائمة معروضات أو نشرات تجارية.

التداول أو التأجير للبرامج المقلدة و بالنسبة للتداول فانه سلوك مجرم كذلك في التشريع الجزائري، و يعني قيام شخص بالتصرف في البرامج المقلدة بمقابل أو بغير مقابل، و سواء كان التصرف ناقل للملكية ، ناقل لحق الاستغلال ، حق الانتفاع أو الاستعمال و كذا التأجير للبرامج المقلدة فإنه سلوك مجرم و يعني قيام شخص ما بتمكين مستأجر من البرامج المقلدة من استعماله مدة معينة مقابل أجرة معينة و يكفي لتوافر الجريمة عملية استئجار واحدة.

ب- الركن المعنوي

يتمثل الركن المعنوي لجريمة التعامل بالبرامج المقلدة بالبيع ، العرض للبيع التداول التأجير ، الاستيراد او التصدير في القصد الجنائي العام، و الذي يقتضي أن يكون

[1]- جميل عبد الباقي صغير، جرائم التكنولوجيا الحديثة،القاهرة، دار النهضة العربية،2002، ص114.

الجاني عالما بأن ما يبيعه أو يتداوله ، يؤجره ، يعرضه للبيع ، يستورده أو يصدره برامج مقلدة مع اتجاه إرادته إلى ذلك،و القصد الجنائي في هذه الجريمة هو قصد مفترض [1].

ثانيا : الجزاءات المقررة لجرائم الاعتداء على برامج الكمبيوتر

نظرا لخطورة و جسامة الجرائم المرتكبة على حق المؤلف و بالأخص حقوق مؤلفي برامج الكمبيوتر، ظهرت الحاجة لوضع جزاءات رادعة، لهذا سنتطرق إلى العقوبات الأصلية و العقوبات التكميلية المخصصة لهذا النوع من الجرائم.

1-العقوبات الأصلية

حدد المشرع الجزائري في المادة 153 من الأمر 03/05 عقوبة تتمثل في الحبس من 3 أشهر إلى 3 سنوات و غرامة من 500.000 دج إلى 1.000.000 دج سواء كان النشر قد حصل في الجزائر أو خارجها.

و يلاحظ أن قيمة الغرامة التي جاءت في التشريع الجزائري غير رادعة مثل ما هو الحال في التشريع الفرنسي، الذي قد تصل قيمة الغرامة إلى مليون فرنك فرنسي فضلا عن تعويض للطرف المتضرر من عملية القرصنة، فالمكاسب التي يحققها سارقي حقوق الملكية الفكرية من جراء الاعتداء على حقوق مؤلفي البرامج كبيرة جدا، لذلك يجب أن تكون الغرامة على قدر حجم الجريمة، و في هذا الصدد قال عصام الكردي الخبير القانوني في مجال حماية الملكية الفكرية إن القانون لا يجب أن يتضمن الحد الأقصى و أن يتم تحديد حد أدنى للغرامة و يترك للقاضي تحديد الحد الأقصى للغرامة، كما يرى أنه على القانون جعل الحبس جوازا مع مضاعفة الغرامة و ذلك في المرة الأولى و جعله و جوبي مع مضاعفة الغرامة في حالة العود.[2]

و نص المشرع الجزائري على تشديد العقوبة في حالة العود بموجب المادة 156 من الأمر 03/05، فالجاني يكفي أن يرتكب مرة ثانية جريمة من الجرائم المنصوص عليها في المواد 151، 154، 155 من الأمر 03/05.

---

[1] – أحمد ضياء الدين خليل، الظاهرة الإجرامية بين الفهم و التحليل، القاهرة،دار الطويعي للطباعة، الطبعة الأولى،1992، ص201.

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص،الجزائر،دار هومة،2007،الطبعة الثالثة ، ص38 .

2- العقوبات التكميلية و تدابير الأمن

تتمثل العقوبات التكميلية في التشريع الجزائري في المصادرة و نشر الحكم حيث تم النص على المصادرة في المادة 157 من الأمر 03/05 التي تضمنت على أنه تقرر الجهة القضائية المختصة مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي للمصنف و مصادرة العتاد المخصص لمباشرة النشاط أو المشرع و النسخ.

و يلاحظ ان المشرع الجزائري أوجب على الجهة القضائية المختصة في المادة 159 من الأمر 03/05 أن تأمر في جميع الحالات المنصوص عليها في المواد 151،152 بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك كله الإيرادات موضوع المصادرة للمؤلف أو لأي مالك حقوق أخر أو ذي حقوقهما لتكون عند الحاجة بمثابة تعويض عن الضرر اللاحق بهم، و لقد جعل المشرع الجزائري المصادرة جوازية فالجهة القضائية أن تقرر الحكم بمصادرة النسخ المقلدة و الأدوات المستخدمة في التقليد، و المصادرة وجوبية و يتعين على القاضي إن يحكم بها و إن لم يفعل كان حكمه معيبا مستوجبا نقضه للخطأ في تطبيق القانون[1].

أما عن عقوبة نشر الحكم فنص عليها المشرع الجزائري في المادة 158 من الأمر رقم 03/05 و التي تقضي انه يمكن للجهة القاضية المختصة بطلب من الطرف المدني، أن تأمر بنشر أحكام الإدانة كاملة أو مجزئة في الصحف التي تعنيها و تعليق هذه الأحكام عليه و كل مؤسسة أو قاعة حفلات يملكها على أن يكون ذلك على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها.

و يقصد بهذه العقوبة التشهير بالمحكوم عليه و التأثير على شخصيته الأدبية و المالية، و هي بذلك عقوبة ماسة بشرف الاعتبار.

أما عن تدابير الأمن فقد نص المشرع الجزائري بموجب المادة 156/2 عن عقوبة الغلق، حيث نصت أنه يمكن للجهة القضائية المختصة أن تقرر الغلق النهائي المؤقت

[1] -علي عبد القادر القهوجي، مرجع سابق، ص46.

مدة لا تتعدى 6 أشهر التي يستغلها المقلد، أو شريكه أو أن تقرر الغلق النهائي عند الاقتضاء و يستفاد من هذا النص أن عقوبة الغلق جوازية يجوز للقاضي أن يحكم بها [1].

الفرع الثاني: الحماية الجزائية للبرامج الحاسوب في ظل نصوص الملكية الصناعية

إن قانون الملكية الفكرية يشمل عدة مجالات منها: العلامات التجارية براءة الاختراع، الرسوم و النماذج تسمية المنشأ، و ما يهمنا بصدد حماية برامج الكمبيوتر هو حمايتها من خلال براءة الاختراع.

أولا: الشروط الواجب توفرها في براءة الاختراع

بصدور الأمر 03/07 المؤرخ في 19/07/2003: المتضمن براءة الاختراع و بالعودة إلى نصوصه نجد المادة الثانية منه عرفت الاختراع بأنه: " فكرة المخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية "، و بشأن الشروط الواجب توفرها في الاختراع كي تطبق عليه أحكام المادة الثالثة من ذات الأمر التي تنص على ما يلي: " يمكن إن تقع تحت براءة الاختراع الجديدة الناتجة عن نشاط الاختراعي و القابلة للتطبيق صناعيا ".[2]

و من خلال نصوص الملكية الفكرية نجد أنه يضفي حماية جنائية عن طريق براءة الاختراع، حيث لابد من توافر شروط معينة في الاختراع تتمثل فيما يلي:

* الابتكار.
* الجدة.
* القابلية للتطبيق الصناعي.
* المشروعية.

[1]-أحسن بوسقيعة، نفس المرجع، ص 38.

[2]- علي عبد القادر القهوجي،مرجع سابق، ص48.

إن الفقه التجاري الذي يتناول موضوع براءة الاختراع كموضوع من موضوعاته على كون الاختراع ذو صفة مادية، و ذلك يتضح من الشروط الواجب توفرها في الاختراع حتى يتمتع بالحماية القانونية التي تقررها النصوص قانون براءة الاختراع التي لا تطبق إلا على أشياء المادية الملموسة سواء كان منتجا أو وسيلة خاصة إذ لاحظنا أن كل ذلك في إطار شرط القابلية للاستغلال الصناعي، ليتبين لنا أنه يحتوي على بعد مادي، و هذا ما يفرق على أساسه الفقه التجاري بين الابتكار الصناعي و المصنفات الأدبية،وعلى هذا نستطيع أن نقول بأن الفقه التجاري و غن كان قد اختلف في ترتيب شروط الاختراع التي تؤهله للحصول على البراءة، فإنه متفق على الطابع المادي لهذا الاختراع أو الابتكار الجديد القابل للاستغلال الصناعي[1].

و بناءا على ذلك فإن أحكام قانون براءة الاختراع يمكن أن تطبق على المكونات المادية للكمبيوتر متى توافرت فيها الشروط التي يتطلبها هذا القانون أما مكونات الكمبيوتر غير مادية فلا يمكن أن نطبق النصوص الخاصة بقانون براءة الاختراع و ذلك لانتفاء الطابع المادي لها.

ثانيا: مدى تطبيق نصوص براءة الاختراع على برامج الكمبيوتر

يرى الدكتور محمد حسنين أن الحماية لقوانين براءة الاختراع تتمثل في برامج الكمبيوتر و لأنها تستعمل للتعامل مع آلات الكمبيوتر، و إدارتها فهي بذلك تصبح جزءا منها، و لما كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الكمبيوتر فهي من هذه الزاوية تصبح قابلة للبراءة[2] .

أما المنتقدون فيقولون على الرغم من مزايا الحماية التي توفرها قوانين براءة الاختراع إلا أنه توجد عدة أسباب تحول دون امتداد نصوص براءة الاختراع إلى المكونات غير المادية للكمبيوتر:

---

[1]- أمال قارة، مرجع سابق ،ص65.

[2]– محمد حسنين ، مرجع سابق، ص125.

حسبما يراه المختصون في الميدان فإنه من الصعب توفير حماية ناجعة للبرمجيات بالرجوع إلى قانون الملكية الصناعية، و يتعلق الأمر خاصة بشرطين لابد من توفرهما في العمل الإبداعي لكي يظفر صاحبه بالبراءة:

* الجدة.

* القابلية لاستغلال الصناعي.

هذان الشرطان تتفق حولهما التشريعات المقارنة مع التشريع الجزائري فيما يضيف هذا الأخير شرطا أخر هو إن يكون الاختراع نشاطا خلاقا (Une activité inventive)[1].

1- شرط الجدة.

طبقا للمادة 09 من الأمر: 03/07 " يعتبر الاختراع ناتجا عن نشاط اختراعي لم يكن ناجما بداهة عن الحالة التقنية ".

و يرى الفقهاء أن هذا لا يمكن تحققه في البرمجيات، و لا من الهين إثباته، إذ يجب للتقرير بتوافر هذا الشرط أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لكي تقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا، الأمر الذي يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة و التمييز في المجال الذي تتولى بحثه.

و تقرير جدة الاختراع في معظم الأحيان يكون أمرا جزافيا، لما تتميز به من طابع ذهني بحت،و قد يكون صعبا على المبرمجين ذاتهم، فكيف يكون الوضع بالنسبة للقاضي عند عرض هذه المسألة عليه.

إن صعوبة تقييم طابع الجدة بالنسبة للكيانات غير المادية ليس مرده لاعتبارات قانونية، بل مرجع ذلك عدم توافر الكفاءات اللازمة التي يمكنها بحث و فحص الكيان المعنوي، و النظر في مدى توافر شرط الجدة بالنسبة له من عدمه.

---

(1)- كامل عفيفي ، مرجع سابق، ص45.

2- صعوبة الاستغلال الصناعي بالنسبة للكيان المعنوي.

يجب أن يكون الاختراع قابلا للاستغلال الصناعي لكي يتمتع بنصوص الحماية الخاصة ببراءة الاختراع، هذا الشرط يفترض أن يكون الاختراع ذا صفة مادية و يجب أن يؤدي استغلاله إلى منتج صناعي، أو يمكن الوصول إلى نتيجة صناعية و كل هذه الأمور تتناقض مع الكيان المعنوي.

و يقول البعض أنه مع تقديرنا للحجج التي قالت بعدم انطباق صفة الوسائل الصناعية على البرامج لانعدام طبيعتها المادية، إلا أن ذلك يعد تفسيرا فقهيا للتشريعات المعاصرة التي لم تتطلب صراحة مادية الاختراع أو وسائله[1].

فالنظريات العلمية هي مجرد أفكار لكن إذا تم استخدامها في غرض صناعي معين اكتسبت براءة الاختراع، كذلك الحال بالنسبة للبرامج أو الكيان المعنوي إذا ما تم استثمارها، و عليه هناك إمكانية تطبيق الوسائل المستحدثة على البرامج و بالتالي يمكن أن تحظى بالحماية القانونية المقررة للاختراعات.

التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءة الاختراع و ذلك راجع لأحد السببين التاليين:

- تجرد برامج المعلوماتية من أي طابع صناعي، و هذا ما أثبتته الإحصائية التي أجرتها المنظمة العالمية للملكية الفكرية عام 1978 التي جاء فيها أن 1% فقط من البرامج يستوفي شرط قابلية الاستغلال الصناعي.
- صعوبة البحث في مدى جدية البرامج لتقدير مدى استحقاقها لبراءة الاختراع و يمكن استثناءا الحصول على براءة الاختراع بخصوص برامج الإعلام الآلي في حالتين هما:
- أن يكون البرنامج جزءا من ذاكرة الكمبيوتر.
- أن يكون طلب براءة الاختراع ينصب على وسيلة صناعية جديدة يستخدم البرنامج في تحقيق إحدى مراحلها.

[1]- أمال قارة، مرجع سابق، ص67.

و تجدر الإشارة إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءة الاختراع و ذلك طبقا للمادة 07 من الأمر 03/07 المتضمن براءة الاختراع " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب ".[1]

فنظرا لاستبعاد نظام براءة الاختراع في حماية البرامج الكمبيوتر، و نظرا لصعوبة استحداث تشريع خاص بالبرمجيات، تبنى المشرع الجزائري نظام الحماية وفقا لحقوق المؤلف و الحقوق المجاورة و هو ما سارت عليه غالبية التشريعات و الاتفاقيات الدولية.

المطلب الثالث: الجوانب الإجرائية في نصوص الجريمة المعلوماتية

إن الطبيعة الخاصة للجرائم المعلوماتية لابد أن تنعكس على قانون الإجراءات الجزائية، فليستلزم على المجتمع المعلوماتي في مجال قانون الإجراءات الجزائية أن ينشأ قواعد إجرائية حديثة غلى جانب القواعد الموضوعية، فلما كانت هذه الجرائم المعلوماتية تتميز بصعوبة اكتشافها و إثباتها و تحتاج إلى خبرة فنية عالية للتعامل معها، فإن ذلك أثار العديد من المشكلات العملية و الإجرائية التي جعلت القواعد الإجرائية التقليدية قاصرة عن مواجهة تلك المشاكل، و لهذا اتجهت بعض التشريعات كالتشريع الانجليزي و الأمريكي و الجزائري إلى تعديل بعض قواعدها الإجرائية لجعلها قادرة على مواجهة تلك المشاكل الإجرائية كتلك المتعلقة بالاختصاص المحلي، و إجراءات التحقيق الابتدائي خاصة التي تهدف إلى جمع الأدلة.

و سوف نتناول في هذا الفرع قواعد الاختصاص المحلي ، وقواعد التحقيق الابتدائي في الفرع الثاني.

[1]- أمال قارة، نفس المرجع، ص69.

الفرع الأول: قواعد الاختصاص المحلي

عالج المشرع الاختصاص المحلي للجهات القضائية و ذلك بتحديد لكل جهة قضائية[1] مجالها الجغرافي الذي لا يجوز الخروج عنه، و قد اعتمد على عناصر معينة تربط بين اختصاص الجهات القضائية بالنظر في الخصومة الجزائية، و هذا المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه، لكن لما كانت الجريمة المعلوماتية جرائم عابرة للإقليم، إذ غالبا ما يكون الجاني في بلد و المجني عليه في بلد آخر .

أولا: الاختصاص المحلي للنيابة العامة

يتحدد الاختصاص المحلي للنيابة العامة وفقا للمادة 37 من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة و محل إقامة احد الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي دائرته القبض على هؤلاء الأشخاص حتى و لو تم القبض لسبب أخر[2].

و بالتالي فإن اختصاص وكيل الجمهورية يجب أن لا يتعدى مكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو بمكان القبض على هؤلاء الأشخاص حتى و لو تم لسبب أخر لكن لما كانت الجريمة المعلوماتية جريمة قد ترتكب في مكان معين و تكون أثارها في مكان أخر فإن المشرع الجزائري بموجب المادة 37 فقرة 2 من قانون الإجراءات الجزائية أجاز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص المحاكم الأخرى إلا أنه ترك كيفية تطبيق ذلك عن طريق التنظيم الذي سيحدد المحاكم التي يمتد إليها الاختصاص.

---

[1]– عبد الله أوهايبيه، شرح قانون الإجراءات الجزئية الجزائري التحري و التحقيق، الجزائر،دار هومه، 2012، الطبعة الثالثة،ص132.

[2]– أحسن بوسقيعة، قانون الإجراءات الجزائية في ضوء الممارسة القضائية، الجزائر،منشورات برتي، 2010، ص21.

و يتعين على ضابط الشرطة القضائية طبقا للمادة 40 مكرر 1 من قانون الإجراءات الجزائية الجزائري أن يخبروا وكيل الجمهورية وكيل الجمهورية لدى محكمة الكائن بها الجريمة و يبلغونه بأصل و نسختين من إجراءات البحث و يرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى مجلس القضائي التابعة له المحكمة المختصة، و الذي يطالب طبقا لنص للمادة 40 مكرر2 من هذا القانون بالإجراءات فورا إذ اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة 40 مكرر من هذا المحكمة التي وقعت بها الجريمة، و هذه الإجراءات تتعلق بتحريك الدعوى العمومية أو مباشرتها أو رفعها بمجرد أن يتبين للنائب العام لدى مجلس القضائي التابعة له المحكمة المختصة و هذا ما نصت عليه المادة 40 مكرر 3.

ثانيا: الاختصاص المحلي لقاضي التحقيق و محاكم الجنح

1- الاختصاص المحلي لقاضي التحقيق

يقصد بالاختصاص المحلي لقاضي التحقيق المجال الذي يباشر فيه قاضي التحقيق و يتحدد الاختصاص المحلي لقاضي التحقيق طبقا لنص للمادة 40 من قانون الإجراءات الجزائية لمكان وقوع الجريمة أو محل إقامة أحد هؤلاء الأشخاص المشتبه في مساهمتهم في اقترافها أو محل القبض على أحد هؤلاء الأشخاص حتى و لو كان هذا القبض قد حصل لسبب أخر[1].

إلا أن المشرع ألغى في التعديل الجديد الفقرة 2 و 3 من المادة 40، و أصبحت تنص الفقرة 2 على أنه يجوز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و بالتالي فإن المشرع أجاز إمكانية تمديد الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم لكنه ترك تحديد كيفية تطبيق تلك الإجراءات لتنظيم الذي سيصدر لاحقا.

(1)-عبد الله أوهايبيه، مرجع سابق، ص347.

2- الاختصاص المحلي لمحاكم الجنح

يتحدد الاختصاص المحلي لمحاكم الجنح طبقا للمادة 329 من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة، أو بمحل إقامة أحد الأشخاص المهتمين، أو شركائهم، أو بمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى و لو تم القبض لسبب أخر، غير أن المشرع في التعديل الصادر بموجب القانون 04/14 أضاف فقرة أخرى أجاز فيها أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يمدد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم.

لكن على المستوى الدولي فإن الأمر بحاجة إلى اتفاقيات دولية ثنائية أو جماعية، و لقد شرعت بعض الدول في عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الحاسوب الآلي، إلا أن ذلك لم يحقق تقدما في معالجة الاختصاص القضائي، فلذلك فالحاجة الماسة إلى قوانين جنائية أكثر مرونة حتى تواكب سرعة تقدم الحاسب الآلي في جميع المجالات.

الفرع الثاني: قواعد التحقيق الابتدائي

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشأن واقعة جنائية معروضة عليها و ذلك بالبحث عن الأدلة المثبتة لذلك، و التحقيق مرحلة لاحقة لإجراءات جمع الاستدلال و تسبق مرحلة المحاكمة التي تقوم بها جهة الحكم، و عليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة [1].

و يهدف التحقيق الابتدائي إلى كشف الحقيقة و للوصول إلى هذا الغرض يلجأ المحقق إلى مجموعة من الإجراءات بعضها يهدف للحصول على الدليل، و تسمى إجراءات جمع الدليل كالتفتيش ، الضبط ، المعاينة ، الشهادة و الخبرة، و بعضها الأخر

[1]-عبد الله أوهايبيه،نفس المرجع،ص348.

يمهد للدليل و يؤدي إليه و تعرف بالإجراءات الاحتياطية ضد المتهم كالقبض و الحبس المؤقت[1].

و سوف تقتصر دراستنا على إجراءات جمع الأدلة المادية التي يكوّن منها القاضي الجزائي اقتناعه تلقائيا بحكم العقل و المنطق، فهي أقوى مفعولا في الاقتناع من الأدلة فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جمع الإجراءات الضرورية للكشف عن الحقيقة[2].

أولا: التفتيش في مجال الجريمة المعلوماتية

لقد تعددت التعريفات التي أضافها الفقه على التفتيش، إلى أنها تجتمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل و ذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات القانونية المقررة، و قد أحاط القانون التفتيش بضمانات عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة، و إذا كان التفتيش للأشياء المادية بما فيها المكونات المادية للحاسوب لا يثير إشكالية، فما مدى خضوع البرامج و المعلومات كمكونات معنوية للحاسوب للتفتيش؟ و ما هي ضوابط تفتيش نظم الحاسوب؟

1- مدى قابلية نظم الحاسوب للتفتيش

أشرنا سابقا إلى أن الحاسوب يتكون من مكونات مادية و مكونات معنوية، و لا تثار أدنى صعوبة، إذ أنّ الصعوبة إذا كان محل جرائم الحاسوب الآلي مكونات مادية حيث ينطبق بصددها و يجوز فيها تفتيش الأشخاص بنفس الضمانات و القيود المنصوص عليها في هذا الصدد[3].

---

[1]-عبد الله أوهايبيه، نفس المرجع،ص345.

[2] -عبد الله أوهايبيه، محاضرات في قانون الإجراءات الجزائية، ألقيت على طلبة سنة ثانية حقوق، جامعة الجزائر، الموسم الجامعي 2001/2002.

[3]-عبد الله هلالي، تفتيش نظام الحاسب الآلي و ضمانات متهم المعلومات، القاهرة، دار النهضة العربية،1997،الطبعة الأولى،ص.74.

أما إذا كان محل جرائم الحاسوب الآلي مكونات غير مادية أي معنوية، كبرامج لحاسوب أو بياناته، فقد ثار خلاف كبير في الفقه بين مؤيد و معارض، حيث يذهب رأي بأن الغاية من التفتيش هو جمع الأدلة المادية التي تفيد في كشف الحقيقة ،فإن هذا المفهوم يمتد ليشمل البرامج و البيانات، و قد لجأ الفقه في العديد من الدول استنادا إلى عمومية نصوص التفتيش و التوسع في تفسيرها و ذلك بمد حكمها إلى البرامج والبيانات المخزنة في أنظمة المعالجة الآلية للمعطيات و أبرز مثال على ذلك الفقه الكندي عندما وسع من تفسير المادة 487 من قانون العقوبات الكندي التي تنص على إمكانية إصدار أمر قضائي لتفتيش أي شيء تتوفر بشأنه أسس أو مبررات معقولة تدعو للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة أو أنه سيتيح دليلا على ارتكاب الجريمة و هكذا فإن هذا النص يفسر على أنه يسمح بضبط و بتفتيش البيانات و برامج الحاسب الآلي[1].

و في هذا المعنى نجد المادة 251 من قانون الإجراءات الجزائية اليوناني تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع و حماية الدليل، و يفسر الفقه اليوناني أن عبارة أي شيء تشمل تفتيش البرامج و البيانات المعالجة الالكترونية.

و على النقيض يرى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد كشف الحقيقة ،فإن هذا المفهوم المادي لا ينطبق على برامج وبيانات الحاسب الآلي غير محسوسة و يقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (مواد معالجة الكترونية)، و لذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة أو أية مادة معالجة بواسطة الحاسب الآلي.

و الحقيقة أن الحاجة ماسة لتدخل تشريعي لتقرير الضوابط القانونية الكفيلة لتغلب على الصعوبات الإجرائية التي تثار عند تفتيش الأنظمة الالكترونية، ففي الولايات

[1]–كامل عفيفي، جرائم الكمبيوتر، لبنان، منشورات الحلبي، الحقوقية، 2003، ص.366.

المتحدة الأمريكية تم تعديل المادة 34 من قانون الإجراءات الجنائية الفيدرالية عام 1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر و الكشف عن الوسائط الالكترونية[1].

2- ضوابط تفتيش نظم الحاسب الآلي

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات بيد أن تحقيق تلك الغاية لا يكون بأي ثمن، ففي كل الحالات فإن الغاية لا تبرر الوسيلة، فالبحث عن الحقيقة القضائية لا ينبغي أن يكون طليقا من كل قيد، بل إن ذلك يخضع لضوابط معينة و من هذا المنطق يجب أن يخضع التفتيش لضوابط يمكن تقسيمها إلى ضوابط موضوعية و ضوابط شكلية.

أ: الضوابط الموضوعية

تنحصر هذه الضوابط فيما يلي:

- وقوع جريمة المعلوماتية: الجريمة المعلوماتية هي كما سبق كل فعل غير مشروع يكون الحاسوب الآلي وسيلته أو محله و ذلك لتحقيق أغراض غير مشروعة و هناك العديد التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لفرنسا والتي أصدرت قانون رقم 88/19 في 5 يناير 1988 و المتعلق بالغش المعلوماتي الذي تم تعديله مع صدور القانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من أول مارس 1994.
- اتهام شخص أو أشخاص معنيين بارتكاب الجريمة المعلوماتية أو المشاركة فيها فينبغي أن يتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية سواء بصفته فاعلا أو شريكا، بحيث أنه إذا لم تتوافر هذه الدلائل كان على قاضي التحقيق أن يصدر أمر بأن لا وجه للمتابعة،و هذا ما تؤكده المادة 163 من قانون الإجراءات الجزائية الجزائري و المادة 177 من قانون الإجراءات الجزائية الفرنسي.

[1]- أحمد السمدان – النظام القانوني لحماية برامج الكمبيوتر، مجلة الحقوق، الكويت، العدد4، سنة 1987.

و في مجال المعلوماتية يمكن القول إن تعبير الدلائل الكافية يقصد به مجموعة المظاهر و الدلائل التي تقوم على المضمون العقلي و المنطقي لملابسات الواقعة و كذلك على خبرة القائم بالتفتيش و التي تنسب الجريمة المعلوماتية إلى شخص معين سواء بصفته فاعلا أو شريكا.

- توافر قرائن على وجود أشياء لدى المتهم المعلوماتي أو غيره تفيد في كشف الحقيقة فلا يكفي مجرد وقوع جناية أو جنحة بل يجب أن تتوافر قرائن قوية على وجود أشياء تفيد كشف الحقيقة، و يستو أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله[1].

و هكذا فإن التفتيش لا يجري إلا إذا توافرت لذا المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء المتحصلة منها أو أية أشياء أخرى أو مستندات الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره.

- إجراء التفتيش لنظم الحاسوب الآلي من قبل سلطة مختصة بالتحقيق: يجب أن يقوم بتفتيش نظم الحاسوب الآلي سلطة مختصة بالتحقيق، و قد جعل المشرع المصري الاختصاص بالتفتيش كإجراء التحقيق في الجرائم التقليدية للنيابة العامة بصفة أصلية و لقاضي التحقيق في حالات خاصة و ذلك على خلاف التشريع الفرنسي و الجزائري الذين أناطا الاختصاص الأصيل بقاضي التحقيق أما النيابة العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس، أما انجلترا فإن معظم الإجراءات الجنائية منوطة بالشرطة القضائية ما عدا بعض الجرائم التي تناط بالمدعي العام.

[1]– أحمد السمدان، النظام القانوني لحماية البرامج،الكويت،ب.د.ن،1987،ص70.

ب: الضوابط الشكلية

بالإضافة إلى الضمانات الموضوعية لتفتيش نظام الحاسب الآلي توجد ضمانات شكلية يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريات الفردية من التعسف أو الانحراف من استخدام السلطة و هي كالتالي[1]:

- الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش الخاص بنظم الحاسوب الآلي و الهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء و صحة الضبط، و قد استوجب المشرع الجزائري في المادة 45/1 أن يتم التفتيش في حضور صاحب المسكن الذي يجري فيه التفتيش و كذلك المشرع الفرنسي استوجب في الفقرة الأولى من المادة 57 من قانون الإجراءات الجزائية حضور صاحب المسكن الذي يجري فيه التفتيش و عدم حضوره يترتب عليه بطلان إجراءات التفتيش.

ويجب أن يتضمن محضر التفتيش تاريخ تحريره ، توقيع محرره و كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها[2].

- تحديد أوقات لإجراء تفتيش نظام الحاسوب الآلي فحرصا على عدم التضييق من نطاق الاعتداء على الحرية الفردية و حرمة المسكن حرصت التشريعات الإجرائية على حضر القيام بتفتيش المنازل و ما في حكمها في وقت معين، فالقانون الفرنسي ينص في المادة 59 من قانون الإجراءات الجزائية على أن التفتيش لا يمكن أن يبدأ قبل الساعة السادسة صباحا و بعد التاسعة مساءا، و لقد أخذت بعض التشريعات العربية بمبدأ عدم جواز تفتيش المنازل ليلا كقانون

---

[1]– أحمد السمدان، نفس المرجع ،ص71.

[2]–عبد الله الهلالي، تفتيش نظام الحاسب الآلي و ضمانات متهم المعلومات، القاهرة، دار النهضة العربية1997،ص80.

التونسي و الجزائري، أما بالنسبة لتشريعات الدول الانجلسكسونية كالقانون الانجليزي و الأمريكي فإنها لا تقيد التفتيش بوقت معين.

لكن المشرع الجزائري بموجب المادة 47 من قانون الإجراءات الجزائية الجزائري قرر إجراء التفتيش و المعاينة و الحجز في كل ساعة من ساعات الليل و النهار أو الليل و في كل محل سكني غير سكني، بناء على إذن مسبق من وكيل الجمهورية المختص إلا أنه أوجب الحفاظ على السر المهني.

- أن يتم التفتيش بناءا على إذن مكتوب ولقد نصت المادة 44 من قانون الإجراءات الجزائية الجزائري على ضرورة أن يكون التفتيش بناءا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا إذن قبل الدخول إلى المكان و الشروع في تفتيش نظم الحاسوب الآلي.

إن التفتيش لنظم الحاسوب الآلي يتطلب مذكرة قضائية تجيز تفتيش أنظمة الكمبيوتر، فإجراء التفتيش دون تلك المذكرة مسألة تثير الكثير من المعارضة خاصة في ظل ما يتقرر من قواعد تحمي الخصوصية و تحمي حقوق الأفراد. و يجب أن تكون المذكرة واضحة في تحديد النظام محل التفتيش[1].

3-الضبط في مجال الجريمة المعلوماتية

منح المشرع في المادة 63 صلاحية القيام بالتحقيقات الابتدائية لأعوان الضبطية القضائية بشرط أن تكون تحت رقابة ضباط الشرطة القضائية.

أ: فيما يخص التوقيف للنظر

إن التحقيق الابتدائي في الجرائم الخطيرة المذكورة في المادة 16 من قانون الإجراءات الجزائية أصبح عسيرا و صعبا خاصة و أن مرتكبي هذه الجرائم أصبحوا يستعملون أساليب متعددة ، حديثة و معقدة.

[1] -أحسن بوسقيعة، قانون الإجراءات الجزائية في ضوء الممارسة القضائية،الجزائر، منشورات برتي، 2010، ص25.

و أصبحت مدة الوضع تحت النظر لا تتماشى و متطلبات التحقيق الأولي، مما جعل المشرع الجزائري يعدلها بالمادة 51 و بالتالي نصت على أنه:

" يمكن تمديد أجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات "

و نلاحظ أن المشرع ربط تجديد مدة التوقيف للنظر بطبيعة الجريمة موضوع التحري و اشترط أن يكون تمديد المدة بإذن مكتوب من وكيل الجمهورية و أثناء التحقيق الابتدائي كثيرا ما يقوم ضباط الشرطة القضائية باستدعاء أشخاص لإجراء التحقيق، إلا أنهم لا يمتثلون للاستدعاءات الواردة إليهم مما يقلص من فعالية و سرعة التحقيق لذا استوجب ترخيص رجال الضبطية القضائية استعمال القوة لإحضارهم[1].

ب: استعمال القوة لإحضار الأشخاص

لقد نصت المادة 65 الفقرة 1 أنه يجوز لضباط الشرطة القضائية بعد الحصول على إذن مسبق من وكيل الجمهورية المختص أن يستخدم القوة العمومية لإحضار الأشخاص الذين لم يستجيبوا لاستدعائين.

هذه المادة تتيح استعمال القوة لإحضار الأشخاص أمام الضبطية القضائية لأخذ أقوالهم بشرط أن يكون إحضارهم بترخيص من وكيل الجمهورية المختص، و لا يمكن إبقاؤهم في حالة التوقيف إلا للمدة اللازمة لأخذ أقوالهم بشرط أن يكون قد تم استدعائهم مرتين على الأقل و لم يمتثلوا[2].

و حتى يحقق التفتيش غايته في جمع الأدلة الإجرامية لا بد من وسيلة التقاط تلك الأدلة، و هذه الوسيلة هي الضبط، و الضبط في معظم الأحيان يكون هو غرض التفتيش و إن لم يكن هو السبب الأوحد له يأتي الضبط لأسباب أخرى غير التفتيش مثل المعاينة.

و يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت و يفيد في كشف الحقيقة عنها و عن مرتكبها و هو من حيث الطبيعة القانونية من إجراءات الاستدلال أو

---

[1]–أحسن بوسقيعة، نفس المرجع، ص29.

[2]– أحسن بوسقيعة، نفس المرجع، ص34.

التحقيق، و تحدد طبيعته بحسب الطريقة التي تم فيها وضع اليد على الشيء المضبوط، فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة استدلال.[1]

و إذا كانت الجرائم الواقعة على المكونات المادية للحاسوب الآلي لا تثير صعوبة للتقرير بصلاحية هذه الجرائم لضبط أدلتها،ومع ذلك أن الضبط لا يرد بحسب الأصل إلا على أشياء مادية، إلا أن الأمر بالنسبة للجرائم الواقعة على المكونات المعنوية للحاسوب الآلي تثير مشاكل بالنسبة لضبط أدلتها.

و قد اختلف الفقهاء بين مؤيد و معارض، و نجد المشرع الجزائري قد أجاز بموجب المادة 47 والتي تضمنت الضبط أو الحجز في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في محل سكني أو غير سكني، و في ساعة من ساعات النهار أو الليل بإذن مسبق من وكيل الجمهورية.

و من اجل ضبط أدلة الجريمة فإن المشرع الجزائري بموجب المواد 65 مكرر 10 ق.ا.ج أجاز اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و إذا اقتضت ذلك ضرورة التحقيق الابتدائي بإذن من قاضي التحقيق لمدة أربعة أشهر قابلة للتجديد، و تنفذ العمليات المأذون بها تحت المراقبة مباشرة لقاضي التحقيق، و تتم العمليات المحددة دون المساس بالسر المهني المنصوص عليه في المادة 45 من ق.ا.ج.

و يبقى أن نتساءل عما يجوز إذ يجوز لضباط الشرطة القضائية الاطلاع على محتويات الحاسوب الآلي التي يتم ضبطها[2].

ولقد أجاب القسم 110 من قانون الإجراءات الألماني على هذا التساؤل إن سلطة الإطلاع على مطبوعات الحاسوب الآلي وحاملات البيانات الأخرى تقتصر على المدعي العام فقط و لايخول القانون لضباط الشرطة القضائية الحق في الإطلاع عليها دون إذن

---

[1]– أحسن بوسقيعة، نفس المرجع، ص34.

[2]–عبد الله أوهايبيه، مرجع سابق، ص212.

الشخص في حيز مادي ويتم ذلك بإخراجها على الورق أو بأخذ تسجيل منها أو جمعها على أقراص مرنة أو ممغنطة.

إلا أنه هناك سؤال آخر يطرح نفسه بشدة، إلا أي حد يمكن اعتبار هذه المستخرجات بصورها المختلفة مستندات تصلح أن تكون أدلة إثبات مقبولة أمام القضاء. مع العلم أن القاعدة في الدعاوي الجزائية هي جواز الإثبات بكافة طرق الإثبات القانونية و القيد على هذه القاعدة أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، و بالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الالكترونية خاصة مع احتمال ظهور أنشطة إجرامية عديدة.

إذ اعترف الفقه و القضاء الجنائيين في فرنسا بمستخرجات الحاسوب الآلي سواء كانت مخرجات ورقية أو الكترونية كالأشرطة المغنطيسية و غيرها من الأشكال الالكترونية الأخرى بأن لها قيمة دلائل الإثبات و بالتالي تصلح كأدلة إثبات أمام القضاء الجنائي، لاسيما و أن التعديل المدخل على قانون العقوبات الفرنسي بمقتضى القانون 08 يناير 1988 لم يتضمن ما يخالف وجهة النظر هذه[1].

المبحث الثاني: الحلول التشريعية وتطبيقات عن أساليب مكافحة الجريمة المعلوماتية

تمثل هذه الحلول التشريعية في تدابير وقائية تتخذها الدولة و قوانين تسنها من أجل مكافحة هذه الجريمة و حماية المجتمع[2].

و لكن لصعوبة التعامل مع هذه الجرائم الجديدة في الوقت الراهن يتطلب الأمر بداية اللجوء إلى حلول قصيرة المدى ثم حلول طويلة المدى و هو إعادة النظر في معظم التشريعات لأن معظم الانترنت أصبح ظاهرة تمس جميع مجالات الحياة.

---

[1]–حجازي عبد الفتاح بيومي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، مصر،دار المجلة الكبرى، دار الكتب القانونية،2004،ص164.

[2]– سامر محمد سعيد، الأنترنت(المنافع والمخاطر)، بيروت،دار سعاد الصباح المطابع التعاونية الصحافية،1998، ص199.

الفرع الأول: الحلول التشريعية القصيرة المدى

إن هذه الحلول تتمثل في إصدار السلطة المختصة بعض المراسيم التنظيمية لمقاهي الانترنت دون احتكار المعلومة فيمكن في إجراءات إستعجالية فرض بعض الأمور على أصحاب مقاهي الانترنت :[1]

- وضع البرامج اللازمة لمنع الدخول إلى المواقع المخلة بالحياء ، و هذا من أهم الظواهر التي برزت في مجتمعنا في ظل غياب التربية السليمة مما يؤدي للانحلال الخلقي لشبابنا و حتى المراهقين الذي أصبح من السهل عليهم دخول أي موقع يشاءون بالإضافة إلى المواقع الإباحية هناك المواقع الإرهابية و مواقع للعنف كتعليم القتل ، فلا بد من تدبير عاجل .
- وضع برامج للحماية من الفيروسات [2] و هذا كله بمراسيم تنظيمية و يمكن للدولة أن تدعم هذه العملية بتخفيض أسعار هذه البرامج.
- التوعية القانونية و التعريف بمدى خطورة الجرائم الإلكترونية.
- إصدار مراسيم من أجل تنظيم تكوين محققين و رجال شرطة و قضاة على التقنية المعلوماتية و المعرفة الكافية لجرائم الانترنت[3].
- تعريض أشخاص أو مقاهي الانترنت لغرامة مالية أو حتى إغلاق المقهى إذ تثبت أنه يسمح للمراهقين أو حتى الشباب بالدخول للمواقع السابقة ففي المواد الجنائية لا يمكننا ذكر أكثر من هذا احتراما لمبدأ لاعقوبة إلا بنص قانوني.

أما من ناحية المواد المدنية و التجارية فإنه:

- يمكن للمحاماة لعب دور مهم لتكييف بعض السلوكيات و المعلومات، مع محاولة القضاة تكييف بعض المنازعات التجارية الإلكترونية قياسا على التجارة العادية لحين صدور التشريع المنظم للتجارة الإلكترونية.

---

[1]– سامر محمد سعيد ،نفس المرجع، ص201.

[2]– محمد عادل الريان ، جرائم الحاسب الآلي وأمن البيانات،الكويت،مجلة العربي ،1995،العدد440،ص123.

[3]–محمد أمين الرومي، جرائم الكمبيوتر و الانترنيت،الاسكندرية، دار المطبوعات الجامعية، 2003،طبعة الأولى ص201.

- اعتماد حرية الإثبات في المجال التجاري.

يجب على المشرع أن يوقع بعض المعاهدات لمكافحة الجريمة الإلكترونية.

- يجب على المشرع أن يوقع بعض الاتفاقيات التي تتبنى تعريف التوقيع الإلكتروني و العقد الإلكتروني و مسايرتها بسن قوانينها التنظيمية.

الفرع الثاني: الحلول التشريعية البعيدة المدى

إن الطابع اللامادي و الإفتراضي لشبكة الانترنت يستلزم تعديل العديد من التشريعات الحالية بالإضافة إلى استحداث أخرى ، و هذا لا يضطرنا بالضرورة إلى خلق شيء جديد بل يمكننا الاستفادة من الدول الأخرى التي سبقتنا في مجال التشريع لتجريم هذه السلوكيات ما دامت هذه التشريعات لا تخالف النظام العام و الآداب العام و بما أنه لا يمكن معاقبة شخص من دون نص قانوني – الركن الشرعي – إذن لابد من سن نصوص قانونية تتناسب و التطور الحالي. و لكن الملاحظ أنه رغم زيادة انتشار الجرائم الإلكترونية و فعاليتها إلا أن المشرع لم يضع لحد الآن الإطار القانوني لأي من هذه الظواهر[1].

لذا على المشرع أن يعدل أو يصدر قوانين جديدة ، ففي نطاق الحماية الجنائية يتعين الإقرار بصلاحية المعلومات كمحل للحماية من أنشطة الاعتداء كافة[2] فبدأ بالتشريعة العامة وهي القانون المدني ، فعلى المشرع أن يعدل فيه بسن تشريع جديد يتضمن المحررات الإلكترونية و من بينها العقد الإلكتروني والتوقيع الإلكتروني و غيرها من المفاهيم في العالم الافتراضي الجديد.

---

(1) –www.arabcia.net.

(2)– محمد أمين الرومي، نفس المرجع، ص 128.

- **القانون التجاري :** لقد ظهر في عالمنا اليوم مفهوم جديد هو التجارة الإلكترونية والتسويق الإلكتروني، و الدفع عن طريق بطاقة الائتمان و هي مجالات خصبة للاحتيال فلا بد على المشرع أن ينظمها.
- **الإثبات:** و هذا في اعتقادنا من أهم الخطوات التي يجب أن يقوم بها المشرع و هذا بتبني الخبرة و المعاينة كأساليب للتحقيق و إثبات الجريمة الإلكترونية.
- تعديل قانون الإجراءات الجزائية و تعديل قانون حقوق المؤلف و الحقوق المجاورة
- تعديل قانون الإجراءات المدنية و تحديد الاختصاص النوعي و المحلي لهذه الجرائم و المعاملات.
- تحديد مسؤولية مزودي الانترنت.
- تكليف النظام القضائي لمعالجة هذه الجرائم و تأهيل القضاة ، و أهم قانون يجب تعديله هو قانون العقوبات الجزائري الذي يعتبر أهم حل في الحلول التشريعية طويلة المدى .

المطلب الثاني: تطبيقات عن أساليب مكافحة الجريمة المعلوماتية

في هذا المطلب نحاول الاطلاع على مدى ملائمة التشريعات و مدى نجاعتها لمكافحة الجريمة الالكترونية، فبين غافل و مواكب للتطور هو حال دول العالم.

فقبل ظهور هذه السلوكيات المجرمة في معظم الدول المتقدمة، كانت هناك قوانين تنظم جرائم الحاسب الآلي، فلم يتم سوى تعديل بعض العقوبات أو الغرامات المالية و كان أوّل ظهور لمصطلح الجرائم الالكترونية سنة 1998 في مؤتمر باستراليا و بتاريخ2001/11/27 عقد المؤتمر الأوروبي لمكافحة الجريمة عبر الانترنت و قد عقد مؤتمر الأمن العربي حول الجريمة الالكترونية للدولة العربية سنة 2002.

الفرع الأول: الأساليب الدولية

و من الدول التي ساهمت في التطور الواضح في مجال المعلوماتية الولايات المتحدة الأمريكية و الدول الأوروبية 2001 تضع سياسة عامة من أجل تجريم هذه الأفعال و من بين بنود هذه الاتفاقية بند ينص على أن السلطات القضائية في أيّ دولة يمكنها الحصول على معلومات مخزّنة في كمبيوتر أي دولة أخرى في إطار التحقيق في جريمة تمّ ارتكابها عبر الإنترنت.[1]

و قد شارك في إعداد هذه الاتفاقية عدة دول متقدمة أحسّت بمدى خطورة هذه الجرائم كاليابان و جنوب إفريقيا و كانت الولايات المتحدة الأمريكية أول دولة صادقت على الاتفاقية الأوروبية لمكافحة الجريمة الالكترونية من خارج الاتّحاد.

و من بين الدول التي صادقت على تعديل القوانين هي فرنسا حيث غيّرت الغرامات المالية و حددت مدة السجن و يتضح من هذا التغيير أنّ التكييف الجنائي لهذه السلوكيات المجرمة قد كيّفه المشرع الفرنسي بجنحة أو جناية.

ففي المادة 226-16 من قانون العقوبات الفرنسي أصبحت الغرامة تقدر بـ 45000 اورو و مدة السجن 03 سنوات حيث نصت: " كل فعل عن قصد أو عن غير قصد الذي يرمي إلى المعالجة الآلية للمعلومات الاسمية بدون احترام الشكليات الأولية المقررة يعاقب عليها بـ 45000 اورو و السجن 03 سنوات"[2].

---

[1] -محمد أمين الرومي ، نفس المرجع ، ص 129.

[2] -Le traitement judiciaire de la cybercriminalité guide méthodologique ministère de la justice française p. 07.

الفرع الثاني: الأساليب المحلية

لقد ادخل استغلال شبكة الانترنت في نظام الخوصصة بعد أن كانت محتكرة من طرف مركز البحث في الإعلام العلمي و التقني (cerist) بموجب المرسوم التنفيذي رقم 98-257 المؤرخ في 25أوت 1998.

فالجزائر قد فتحت مجالا واسعا للانترنت و أدخلت عدة تقنيات حديثة، تجدر الإشارة هنا إلى أن بعض مصالح البلديات تسعى حاليا إلى فتح بريد الكتروني لاستخراج الوثائق.

و قد أورد هذا المرسوم في :

المادة الأولى: يضبط هذا المرسوم شروط و كيفيات إقامة خدمات "انترنت" استغلالها.

المادة الثانية: تعرف خدمات انترنت كما يلي: خدمات "واب" الواسعة النطاق (w.w.w.web) world vide web: خدمات تفاعلية للاطلاع أو احتواء صفحات متعددة الوسائط Multimédia(نصوص، رسوم بيانية، صوت أو صورة) موصولة بينها عن طريق صلات تسمى نصوص متعددة *Hy pertexte*

- البريد الالكتروني Email: خدمات تبادل رسائل الكترونية بين المستعملين.
- تلنات*Telnalt*: خدمات النفاذ إلى حواسب متباعدة بصيغة المحاكاة الطرفية.
- بروتوكول نقل الملفات (FTB*file Transferprotocole) : خدمات تعبئة الملفات عن بعد بصيغة نقطة إلى نقطة.
- منبر التحاور NEWGROUPS**: خدمات تسمح بتبادل المعلومات بين مجموعة من المستعملين ذوي اهتمام مشترك حول موضوع معيّن.

كما أورد إجراءا وقائيا في المادة 8/14 من هذا المرسوم.[1]

نص المادة 14 يلتزم مقدم خدمات *[2] انترنت خلال ممارسة نشاطاته بما يلي:

- تسهيل النفاذ إلى خدمات انترنت حسب الإمكانيات المتوفرة إلى كلّ الراغبين في ذلك باستعمال أنجع الوسائل التقنية.
- المحافظة على سرية كل المعلومات المتعلقة بحيات مشتركيها الخاصة و عدم الإدلاء بها إلاّ في الحالات المنصوص عليها في القانون.
- إعطاء مشتركيه معلومات واضحة و دقيقة حول موضوع النفاذ إلى خدمات انترنت و صيغة مساعدتهم كلما طلبوا ذلك.
- عرض أيّ مشروع خاص باستعمال منظومات الترميز على اللّجنة.
- احترام قواعد حسن السير بالامتناع خاصة عن استعمال أية طريقة غير مشروعة سوا اتجاه المستعملين أو اتجاه مقدمي خدمات * انترنت * الآخرين.
- تحمل مسؤولية محتوى الصفحات و موزعات المعطيات التي يستخرجها و يأويها، طبقا للأحكام التشريعية المعمول بها.
- إعلام مشتركيه بالمسؤولية المترتبة عليهم فيما يتعلق بمحتوى الصفحات التي يستخرجونها، وفقا للأحكام التشريعية المعمول بها.
- اتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة فهو النص الوحيد الذي نظم استخدام الانترنت.[2]

---

(1)-Le traitement judiciaire de la cybercriminalité guide méthodologique ministère de la justice française p. 08.

(2) –www.arabcia.net.

المطلب الثالث: الجهود الدولية في محاربة الجريمة المعلوماتية وأهم العراقيل التي تواجهها

إن محاربة الجريمة المعلوماتية على المستوى الدولي أو الوطني لا تستقيم إلا بإيجاد أساس تشريعي موحد وتصور شامل لمفهوم هذه الجريمة من أجل تحديد الأفعال التي تشكل جريمة معلوماتية إضافة إلى عقد اتفاقيات سواء ثنائية او جماعية يكون هدفها التنسيق وتوحيد الجهود قصد محاربة الجريمة وتشكيل لجان متخصصة في البحث والتحقيق والتحري يكون أعضاؤها ذوي كفاءات عالية في المجال المعلوماتي والتعامل مع المعلومة الالكترونية هذا التنسيق والانسجام لا يمكن له أن يقوم إلا بملائمة التشريعات الوطنية للاتفاقيات الدولية مجال مكافحة الجريمة المعلوماتية في إطار التعاون الدولي الجاد والمثمر.

الفرع الأول: الجهود الدولية في محاربة الجريمة المعلوماتية

أن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين، كان لا بد من إيجاد آلية معينه للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها، ولكي يتم ذلك ويكون هناك تعاون دولي ناجح في مجال تحقيق العدالة كان لازما تنظيم هذا النوع من التعاون الدولي تشريعيا وقضائيا وتنفيذيا.

وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل، فقد تكون هناك حاجة إلى مساعدة من السلطات في البلد الذي كان منشأ الجريمة، أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرَّم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة، وهناك عنصران أساسيان للتعاون، المساعدة غير الرسمية من محقق لآخر، والمساعدة الرسمية المتبادلة[1].

[1]- جميل عبد الباقي الصغير ، جرائم التكنولوجيا الحديثة، القاهرة،دار النهضة العربية،2002،ص 75.

وقد تكون المساعدة غير الرسمية أسرع إنجازاً، وهي الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أي أوامر تفتيش أو طلب تسليم المجرم).

وهي تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتولد نتيجة الاتصالات التي جرت مع الوقت في مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

ومن ناحية أخرى فإن المساعدة الرسمية المتبادلة هي عملية أكثر إرهاقاً يتم اللجوء إليها عادة عملاً بترتيبات معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية.

وهي تشترط في الغالب الأعم أن تكون الجريمة المعنية على درجة معينة من القسوة وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب. ويشار إلى هذا الأمر الأخير باعتباره "تجريماً مزدوجاً."

وسوف نبحث فيما يلي التعاون القضائي والتعاون الدولي:

أولا:التعـاون القضائـــي

إن فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالإنترنت غالبا ما تقتضي تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالإنترنت ، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة ولتحديد مصدر الجريمة و غالبا ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها ، وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه ، وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى بمعنى الحاجة إلى ما يسمي التعاون القضائي.

ثانيا:التعاون الأمني على المستوى الدولي

1- ضرورة التعاون الأمني الدولي:

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدرٍ من الأمن والنظام وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم وتشغل بال الحكومات والمختصين والأفراد على حد السواء.

ومع تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها[1] .

2- جهود المنظمة الدولية للشرطة الجنائية "الأنتربول":

أسس الأنتربول الذي هو أكبر منظمة شرطية في العالم عام 1923 ومهمته تتمثل في تقديم المساعدة إلى أجهزة إنقاذ القانون في بلدانه الأعضاء الـ 186 لمكافحة جميع أشكال الإجرام على مستوى التراب الوطني، للأنتربول بنية تحتية متطورة للإسناد الفني والميداني و تمكين قوى الشرطة في سائر أنحاء العالم من مواجهة التحديات الإجرامية المتنامية في القرن الحادي والعشرين، كما تركز المنظمة اهتماما على ستة مجالات إجرامية أعطتها الأولوية هي الفساد، المخدرات، الإجرام المنظم، الإجرام المالي والمرتبط بالتكنولوجيا المتقدمة، المجرمون الفارون، تهديد السلامة العامة والإرهاب، والاتجار في البشر.

تقع الأمانة العامة للأنتربول في ليون بفرنسا، وهي تعمل على مدار الساعة وطوال أيام السنة، للأنتربول ستة مكاتب إقليمية في مختلف أرجاء العالم، ومكتب لتمثيله في مقر الأمم المتحدة في نيويورك ولكل بلد عضو في الأنتربول مكتب مركزي وطني يعمل فيه موظفو شرطة وطنيون مؤهلون أفضل تأهيل.

---

[1]- جميل عبد الباقي الصغير ، نفس المرجع ،ص 78.

تهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعّال في مكافحة الجريمة من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها[1]وتتبادلها فيما بينها ، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف[2]، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت .

ويقوم الأنتربول بعملية ملاحقة مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة، عن طريق تعقب الأدلة الرقمية وضبطها, والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية.

الفرع الثاني: العراقيل التي تواجه مكافحة الجريمة المعلوماتية

رغم التطور التشريعي الهام الذي عرفته السياسات الجنائية فإنه على المستوى الوطني او الدولي وما صاحب ذلك من تغيير للمفاهيم القانونية في سبيل محاربة الجريمة المعلوماتية التي لا تعترف بالإقليم فلا زالت هناك مجموعة من الإشكالات والصعوبات التي تعرقل وتقلص المجهودات الرامية إلى وضع حد لهذه الجرائم ويمكن تلخيص هذه المعوقات في العناصر التالية:

---

(1)- Malcom Anderson : " Policing the world : Interpol the Politics of International Police Co- Operation " , Clarendon press.Oxford,1989,p 168-185.

(1)- هذا يؤكد أن هذه المنظمة ليست سلطة دولية عليا فوق الدول الأعضاء فالتعاون الشرطي في إطار هذه المنظمة يحكمه مبدأ احترام السيادة الوطنية للدول الأعضاء.

أولا: عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي ذلك، أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب إتباعها [1].

ثانيا: مسألة الطبيعية القانونية للمال المعلوماتي ومدى اعتباره مالا ماديا أو معنويا ومنقولا باعتبارها هذا الأخير محلا لمعظم جرائم الأموال [2].

ثالثا: عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة بخصوص الجريمة المعلوماتية بين الدول المختلفة خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق[3].

رابعا: عدم وجود معاهدات ثنائية أو جماعية بين الدول نحو يسمح بالتعاون المثمر في هذا المجال وحتى في حال وجودها فإنها لا تستطيع مواكبة التطور السريع لنظم وبرامج الحاسب وشبكة الانترنت[4].

خامسا: ضخامة كم البيانات المعلوماتية التي تقف عائقا أمام إجراءات التحقيق الجنائي والبحث عن دليل الإدانة والأكثر من ذلك تتجلى الصعوبة عندما يقوم الجاني بتشتيت المعلومات والمستندات رغبة منه في عدم الابقاء على أي دليل إثبات إضافة إلى أن طباعة كل ما هو موجود على الدعامة الممغنطة لحاسب متوسط العمر، يتطلب مئات ألاف الصفحات في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئا مفيدا للتحقيق.

---

[1]– عبدالفتاح بيومي حجازي ،مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنيت ،مصر، دار الفكر الجامعي، 2006، الطبعة الأولى ،ص ص 142-143 .

[2]–لحسن بيهي، الجريمة الإلكترونية مقاربة قانونية وقضائية، مجلة الواحة القانوينة، العدد 2 السنة الرابعة، ص 376

[3]–عبد الفتاح بيومي حجازي، مرجع سابق، ص 144.

[4]– عبد الفتاح بيومي حجازي ، مرجع سابق، ص 145 .

من خلال دراستنا لموضوع الجريمة المعلوماتية عرفنا أنها جريمة مستحدثة، يكون الحاسب الآلي فيها أداة لارتكاب الجريمة، و ترتكب من مجرم ذو خبرة فائقة في مجال الحاسب الآلي بحيث تعتمد على قمة الذكاء في ارتكابها، و كما نعلم أنها جريمة لا حدود جغرافية لها فهي تتخطى حدود الدولة التي ارتكبت فيها لتتعدى البلدان على مستوى العالم.

و عرفنا كذلك أن أكثر تلك الجرائم يكون ضمن أهدافها الأساسية هو الحصول على المعلومات الالكترونية التي تكون أما محفوظة على أجهزة الحاسبات الآلية و إما منقولة عبر شبكة الانترنت و أخرى هدفها إما الاستيلاء على الأموال و إما تستهدف الأفراد و الجهات الأخرى هدفها الاعتداء على حقوق المؤلف.....الخ.

و نظرا لخصوصية الجريمة المعلوماتية فإن اكتشاف وقوعها و إثباتها يعتبر من الصعوبة بمكان لأنها لا تترك أثرا بعد ارتكابها و من الصعب الاحتفاظ الفني بآثارها إن وجدت، إضافة إلى أنها تحتاج إلى خبرة فنية و يصعب على المحقق التقليدي التعامل معها.

و يلعب البعد الزمني و المكاني و القانوني، دورا هاما في تشتيت جهود التحري و التنسيق الدولي لتعاقب مثل هذه الجرائم.

و هي جرائم تتسم بالغموض حيث يصعب إثباتها و التحقيق فيها ليس كما هو الحال في الجرائم التقليدية و كثير من الجرائم المعلوماتية لا يتم الإبلاغ عنها أما لعدم اكتشاف الضحية لها و إما خشيته من التشهير.

و رأينا أن التشريع حاول التصدي لهذه الجريمة سواء من خلال النصوص التقليدية في قانون العقوبات أو من خلال النصوص خاصة بها، فبعض الجرائم المعلوماتية كيفت على أنه يمكن إخضاعها للنصوص الجنائية التقليدية في حال غياب نص خاص بها مثل جريمة سرقة البرامج و البيانات المعالجة آليا و جريمة التحويل الالكتروني الغير مشروع للأموال و جريمة تزوير المحررات التجارية الالكترونية و غيرها تخضع كلها لنصوص جرائم الأموال في قانون العقوبات و جرائم أخرى كيفت على أساس

إخضاعها لنصوص خاصة بها كجريمة الاعتداء على الخصوصية السرية، فيجرمها القانون الأمريكي الخاص بالمعلوماتية و الحريات، الاعتداء على البيانات الاسمية و الشخصية، و ينص القانون الفرنسي الخاص بالحريات و المعلوماتية وجوب الإيفاء بإجراءات مسبقة قبل إنشاء قواعد البيانات و يخضع ذلك إلى رقابة اللجنة القومية للمعلوماتية و الحريات.

أما بالنسبة للتعديل الذي قام به المشرع الجزائري في قانون رقم 04/15 ما هو إلا نقل حرفي عن قانون العقوبات الفرنسي، و كذلك فإن التعديل لم يتضمن سوى ثلاث أنواع من الجرائم فكان جليا بالمشرع الجزائري و على غرار المشرع الفرنسي أن يجرم بعض الأفعال الأخرى باعتبارها جرائم الكترونية و منها جرائم الاعتداء على البيانات الاسمية و الشخصية و جريمة انتهاك سرية البريد الالكتروني و غيرها.

أما من الناحية الإجرائية الجزائية، فإن قواعد الإجراءات الجزائية للعديد من الدول جاءت قاصرة و لا تتلاءم مع الطبيعة الخاصة للجريمة المعلوماتية بما فيها برامج الحاسوب الآلي، فمن حيث الاختصاص المكاني الحاجة الماسة لمراجعة قواعد في ضوء المستجدات الواقعة و تنظيمها بشكل كافي، و اتخاذ التدابير اللازمة لحل مشكل الاختصاص القانوني و القضائي في إطار اتفاقيات ثنائية أو جماعية.

أما من حيث إجراءات التحقيق فيلاحظ غياب نصوص إجرائية تتكفل بوضع ضوابط لتفتيش و ضبط المعلومات، و فرض ضمانات قانونية للمتهم المعلوماتي أثناء التفتيش.

أما نطاق استنباط الأدلة و إثبات الجريمة المعلوماتية فإن العديد من الدول لم تتبنى مخرجات الحاسوب الآلي كدليل أمام القضاء، لذلك فإن تطوير أدلة الإثبات بما يتلاءم مع هذا الشكل من الجرائم بات أمر ضروري.

و في ظل قصور الحماية الجزائية للجرائم المعلوماتية و برامج الحاسوب الآلي من خلال نصوص الجريمة المعلوماتية و الذي يرجع إلى حداثة هذا النوع من الإجرام، أصبحت هناك ضرورة لتكاثف الجهود الدولية وتوافق السياسات الجنائية في مواجهة هذه

الجرائم المعلوماتية بوضع اتفاقية دولية تستمد منها التشريعات الجنائية الداخلية ضوابط نصوصها لتحقيق تنظيم جنائي موضوعي و إجرامي شامل.

و لمواجهة الصعوبات المثارة في مجال الجريمة المعلوماتية لا يسع الباحث في نهاية هذا البحث سوى التوصية كالأتي:

- و جوب التوسع في إسباغ الحماية الجنائية لبرامج الحاسوب.
- وجوب تجريم الوقائع الإجرامية ذات الصبغة الدولية أو عبر الوطنية كتهريب متحصلات جرائم المخدرات باستعمال الحاسوب الآلي و غسيل الأموال و تمويل الجماعات الإرهابية عبر الانترنت.
- إيجاد العقوبات الملائمة على نحو يحقق أهدافها في مجال الردع العام و الخاص.
- اتخاذ التدابير اللازمة لحل مشكلات الاختصاص القانوني و القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود في إطار تنسيق دولي متكامل، بالإضافة إلى مراجعة قواعد الاختصاص المكاني و تنظيم قواعدها بشكل كافي في ضوء المستجدات الحاصلة.
- مراجعة قواعد إجراءات التحقيق الابتدائي كتلك المتعلقة بالتفتيش و الضبط و تحديثها بما يتلاءم مع الطبيعة الخاصة للجرائم المعلوماتية، و تحديث نظرية الإثبات الجنائي للتوصل إلى إثبات الجرائم المعلوماتية التي يصعب إثباتها.
- ضرورة إحالة هذا النوع من الجرائم غلى قضاء متخصص في الجرائم المعلوماتية نظرا لتعقد القضايا المتعلقة بها وحاجتها إلى معلومات خاصة قد لا تتوفر للقضاء العادي.
- القيام بدورات تدريبية لجهاز الشرطة القضائية تكفل له معرفة تقنيات المعلومات و كيفية استخدامها بما يكفل حسن تطبيقها للقانون بصدد الجرائم المعلوماتية.
- تبادل المعلومات بين الأجهزة المنوط بها تنفيذ القانون و هي الشرطة و النيابة و القضاء من جهة و بين خبراء نظم المعلومات من جهة أخرى بهدف التعرف على أساليب ارتكاب الجريمة المعلوماتية و منع ارتكابها و ملاحقة مرتكبيها.

قائمة المصادر والمراجع

1/ الأوامر:

01-الأمر رقم 03/05 الموافق لـ 2003/07/19 المتضمن حقوق المؤلف والحقوق المجاورة.

02-الأمر 03/07 المؤرخ في: 2003/07/19 المضمن براءة الاختراع.

2/ القوانين:

01- الجريدة الرسمية العدد 47 الصادرة بـ 2009/08/16 والمتضمنة القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها.

02-القانون رقم 06/22 المؤرخ في 2006/12/20 المتضمن قانون الإجراءات الجزائية الجزائري.

03-القانون رقم 06/23 المؤرخ في 2006/12/20 المتضمن قانون العقوبات الجزائري.

04-القانون الفرنسي المؤرخ في 1994/03/01، المعدل لقانون رقم 88/19 المؤرخ في 1988/01/05 المتضمن قانون الغش المعلوماتي.

05-قانون العقوبات الفرنسي الجديد- دار لوز طبعة 2000.

3-المراجع:

المؤلفات العامة:

01-أحسن بوسيقعة، الوجيز في القانون الجزائي الخاص الجرائم ضد الأموال، الجزء الأول، الطبعة السادسة، دار هومة، الجزائر ،2007.

02-أحسن بوسقيعة، قانون الإجراءات الجزائية في ضوء الممارسة القضائية، طبعة 2009-2010 منشورات برتي.

03- أحمد ضياء الدين خليل، الظاهرة الإجرامية بين الفهم و التحليل، القاهرة،دار الطويعي للطباعة، الطبعة الأولى،1992، ص201.

04- أسامة أبو الحجاج ،دليلك الشخصي الى الأنترنت،القاهرة، دار نهضة ،1998،ص20.

05- سامر محمد سعيد، الأنترنت(المنافع والمخاطر)، بيروت،دار سعاد الصباح المطابع التعاونية الصحافية،1998، ص199.

06- عبد الله أوهايبيه، شرح قانون الإجراءات الجزائية الجزائري التحري والتحقيق، دار هومة الطبعة الثالثة 2012.

07- عبد الله سليمان، شرح قانون العقوبات قسم عام الجزء الأول للجريمة،الجزائر، دار الهدى،2006،الطبعة الخامسة،ص43 .

08- لحسن بيهي، الجريمة الإلكترونية مقاربة قانونية وقضائية، مجلة الواحة القانوينة، العدد 2 السنة الرابعة، ص 376

09- محمد حسنين، الوجيز في الملكية الفكرية، المؤسسة الوطنية للكتاب، الجزائر 1985.

المؤلفات الخاصة:

01-أسامة أحمد المناعسة، جلال محمد الزغبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، الأردن، 2004.

02-أمال قارة، الحماية الجزائية للمعلوماتية في تشريع الجزائري، الطبعة الثانية، دار هومة2007.

03-أحمد السمدان – النظام القانوني لحماية برامج الكمبيوتر، مجلة الحقوق، الكويت، العدد4، سنة 1987.

04-أحمد خليفة الملط،الجرائم المعلوماتية،الاسكندرية، دار الفكر الجامعي، 2006، الطبعة الثانية ،ص72.

05- أحمد ضياء الدين خليل، الظاهرة الإجرامية بين الفهم و التحليل، دار الطويعي للطباعة، ط 1/1992، ص201.

06-جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، الطبعة الأولى، دار البلدية، البيضاء2007.

جميل عبد الباقي الصغير،جرائم التكنولوجيا الحديثة، دار النهضة العربية.

07-ذكي أمين حسونة، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، في الفترة من 25 إلى 28 أكتوبر 1993 تقرير مصر، ص471 .

08-زينات طلعت شحادة، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، مطبعة صادر،2006.

قائمة المصادر والمراجع

09-سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية 2007.

10-عزة أحمد خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي، القاهرة،دار النهضة العربية،1994،الطبعة الأولى، ص18

11-عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دراسة مقارنة، بدون طبعة، دار النهضة العربية، القاهرة.

12-عبد الله الهلالي، تفتيش نظام الحاسب الآلي وضمانات متهم المعلومات، دراسة مقارنة، الطبعة الأولى، القاهرة، دار النهضة العربية.

13-عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر 2005.

14-عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، بدون طبعة الاسكندرية2007.

15- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية 1999.

16-كامل عفيفي، جرائم الكمبيوتر، لبنان، منشورات الحلبي، الحقوقية2003.

17-محمد أمين الرومي، جرائم الكمبيوتر والانترنت، بدون طبعة، دار المطبوعات الجامعية، الإسكندرية2003.

18-محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2006.

19-محمد العقاد، جريمة التزوير في المحررات الحاسب الآلي، القاهرة ، دار النهضة العربية، 1995،ص36

20-محمد حسام لطفي، النظام القانوني لحماية الحقوق الذهنية ، عمان، دار الثقافة للطباعة والنشر،1987، ص83

21-محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994.

22-محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، اسيوط 1995.

23-محمد علي ريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية2004.
24-محمد مهرج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، الأردن، دار الثقافة للنشر والتوزيع، الطبعة الأولى، سنة2004.
25-مصطفى محمد موسى،أساليب إجرامية بالتقنية الرقمية ماهيتها...مكافحتها، دراسة مقارنة بدون طبعة، دار الكتب القانونية، مصر 2005.
26- محمد عادل ريان،جرائم الحاسب الآلي وأمن البيانات،الكويت،مجلة العربي، 1995،العدد440، ص 82
27-نائلة عادل محمد فريد قورة،جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، مصر 2005.
28-هشام فريد رستم،جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة،بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين،مجلة الأمن العام العدد151،ص24.
29-هدى قشوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992
30-André Lucas, le droit de l'informatique, paris, PUF 1987, P519,521.
31-Benson (Carl), jablon (Andrew), Kaplan (Paul) & Resenthal (Mara), Computer Crimes, Americain C.L.Review, vol34, N°21,997, p410.
32-E Recommendation No.R89-9 on computer crime and final Report of the European committee on Crime problems, Srasbourg 1++0,P83.
33-Clough (bryan) & mango (paul) approaching zero : data crime and the criminal underworld, 1992, pp.136-146.
34-Duleroy ® et rocco (A.M), l'inforamatique nouvelle, avril 1976, les escrocs a l'informatique, le nouvel Economsiste, les octobre, 1979, n202.
35-equity fuding life insurence, l(informatique nouvelle, mai 1976.
36-Le traitement judiciaire de la cybercriminalité guide méthodologique ministère de la justice française p. 07

37-le rapport du conseil de l'Europe, 15, 18 novembre 1976.

38-Law commission, working paper n°110, computer misuse, London : HMSO, 1988 para.2.2

39-Parker (Donn B), Nycum(s) and Aura(s), Computer Abus : Stanford Research Institut, 1973 ; Taber(J.K) On Computer Crime, C.L.J, 1973, Vol 1, P517.

40-Trib de paris, 12 ème ch, corr, jugement du 13 janv 1982, DALLOZ S 1982, p502.

41-Roden (adrian), computer crime and the law, C.L.J ..,1991,vol.15,p.399

42-Rose (Philipe), la criminalité informatique à l'horizon 2005-analyse prospective, l'harmattan 1992 p49.

43-Sieber (Ulrich), Criminal liabijlity for the transfer of data in international computer network, New problems for German law, European journal of Crime, law and criminil justice, Vol. 34, 1997, bp 3-27.

45-Wasik (martin), crime and the computer, oxford university press, 1991.p19

4-المقالات والمحاضرات:

01-عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمن العربي2002.

02-عبد الله أوهابية،محاضرات في قانون الإجراءات الجزائية، ألقيت على طلبة سنة ثانية حقوق،جامعة الجزائر،الموسم الجامعي 2002/2001.

5- المواقع الالكترونية:

01-www.afric.com

02-www.arabcia.net

03-www.club-internet.com

04-www.avocato.com

05-www.aljazeera.net

06-www.iris.sgdg.org/documents/rapport-ce

6- الأحكام والقرارات القضائية:

01-قرار محكمة النقض بفرنسا في قضية log bax بتاريخ 1979.

02-قرار محكمة الاستئناف بأمريكا في قضية شركة ويلان ضد شركة غاسلو بتاريخ 1986/08/04.

03-القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة سجناء هافانا 1990 قرار بشأن الجرائم ذات صلة بالكمبيوتر.

04-قرار محكمة النقض بفرنسا في قضية Bourquin.

05-قرار محكمة النقض بفرنسا في قضية Maillot.

الفهرس