الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة أبو بكر بلقايد تلمسان
كلية الحقوق و العلوم السياسية

جـرائم المعلومـاتية

مذكـرة لنيـل شهـادة المـاجستيـر فـي العلوم الجنائية وعلم الإجرام

من إعداد الطالب : **تحت إشراف الأستاذ :**
سوير سفيان **بن عمار محمد**

أعضاء لجنة المناقشة

▪ **كحلولة محمد**	**أستاذ جامعة تلمسان**	**رئيسا**
▪ **بن عمار محمد**	**أستاذ جامعة تلمسان**	**مشرفا**
▪ **بن مرزوق عبد القادر**	**أستاذ محاضر أ جامعة تلمسان**	**عضوا**

السنة الجامعية

2011-2010

بسم الله الرحمن الرحيم

"ربّ اشرح لي صدري ويسّر لي أمري واحلل عقدة من لساني يفقهوا قولي"

صدق الله العظيم

"سورة طه الآية25-28 "

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.

و قد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة و نظرا لجسامة أخطارها و فداحة خسائرها و سرعة انتشارها أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفنيين و المهتمين بأمن الصرح المعلوماتي ,لتحديد مفهومها، و خصائصها و التمييز بينها و بين ما يقترب منها من ظواهر ، و معرفة العوامل المختلفة التي تتدخل في هذا التحديد.

و سوف نحاول من خلال هذا الفصل تحديد ماهية الجريمة المعلوماتية وذلك بإلقاء الضوء على تعريف الجريمة المعلوماتية و تبيان خصائصها في المبحث الأول لنتطرق فيما بعد في المبحث الثاني إلى تحديد دوافع ارتكابها لنصل أخيرا إلى أنواع الجرائم المعلوماتية و هو الأمر الذي سنتناوله بالدراسة في المبحث الثالث.

المبحث الأول : تعريف الجريمة المعلوماتية و خصائصها

تعدّدت تعريفات الجريمة المعلوماتية و تباينت فيما بينها ضيقا و اتساعا و قد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، و ما يستتبع ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها. و سوف نحاول من خلال هذا المبحث الوصول إلى تعريف يتلاءم مع طبيعة الجريمة المعلوماتية (المطلب الأول)، لننتقل بعد ذلك إلى خصائص هذه الجريمة (المطلب الثاني) .

المطلب الأول : تعريف الجريمة المعلوماتية

تُعرَّف **الجريمة** عموما في نطاق القانون الجنائي العام بأنها سلوك الفرد عملا كان أو امتناعا يواجهه المجتمع بتطبيق عقوبة جزائية ،و ذلك بسبب الاضطرابات التي يحدثه في النظام الاجتماعي [1]؛و هو التعريف الذي يستند على عناصر الجريمة إلى جانب بيانه لأثرها (السلوك، و السلوك غير المشروع وفق القانون الإرادة الجنائية و أثرها العقوبة أو التدبير الذي يفرضه القانون) ؛و هي الأوصاف التي تميز بين الجريمة عموما ،و بين الأفعال المستهجنة في نطاق الأخلاق أو الجرائم المدنية أو التأديبية.

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

فالمعلومة لغةً مشتقة من كلمة "**علم**" ، ودلالتها فيها و تدور بوجه عام حول المعرفة التي يمكن نقلها أو اكتسابها [1]، وقريب من ذلك إشارتها في اللغة الفرنسية إلى فحوى عمليات الاتصال

[1] – د / أحسن بوسقيعة – الوجيز في القانون الجزائي العام ، الطبعة الثالثة 2006 ، دار هومه ص 3 عن
g .stéfani ;g.levasseur ;b.bouloc : droit général DALLOZ ;17éme édition P.5 .

[2] – د / عزة محمود أحمد خليل –مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي، دراسة مقارنة في القانون المدني و الشريعة الاسلامية ، رسالة دكتورا، مقدمة لكلية الحقوق 1994 ص18 .

التي تستهدف نقل و توصيل إشارة أو رسالة أو الإعلام عنها و اتخاذ وظيفتها في نقل المعارف **(Transfert de connaissances)**

والمعلومات في اللغة الانجليزية و الألمانية و الروسية تعني كلمة **Information** اللاتينية الدالة بحسب الأصل على شيء للإبلاغ و التوضيح ،أو على عملية " **Process** " الإبلاغ أو النقل أو التوصيل و هو نفس ما يعنيه لفظ " **Xinxi** " المقابل لها في اللغة الصينية[2].

أما اصطلاحا فهناك المئات من التعريفات التي أدلى بها باحثون من تخصصات و ثقافات مختلفة لفهم و إدراك 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 أو صور أو وثائق أو بيانات أو رسائل من أي نوع " ,Sons images, documents, données ou messages de toute nature**"، و يعرف الأستاذ **Catala** المعلومة بأنها "رسالة ما معبر عنها بشكل يجعلها قابلة للنقل أو الإبلاغ للغير"[3]، و يعرفها البعض الأخر بأنها "رمز أو مجموعة رموز تنطوي على إمكانية الإفضاء إلى معنى"[4].

ويستخلص مما ذكر أعلاه من تعريفات أن المعلومة هي "مجموعة رموز يستخلص منها معنى معين في مجال محدد ،و تتمتع بالتحديد ،و الابتكار ،و السرية ،و الاستئثار". و بالنظر إلى المعلومة باعتبارها نتاج نشاط إنساني فإنه يجب أن يتوفر فيها عنصران أساسيان **أولهما** التحديد و الابتكار و **ثانيهما** السرية و الاستئثار، إذ أن المعلومة المحددة هي التي يمكن فقط حصرها في دائرة خاصة بها؛ و

---

[1] – المعجم الوسيط "أعلم فلان بالخبر :أخبره به.....و أعلم فلانا الأمر؛جعله يعلمه ،و في لسان العرب العلم نفيض الجهل و علمت الشيء أعلمه علما عرفته وفي مختار الصحاح علم الشيء عرفه.....(استعمله) الخبر (أعلمه) إياه .

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

[3] - Pierre CATALA « la propriété de l'information » Cité par f.Toubal ;le logiciel- analyse juridique FUDUL .L.G.D.J.1986 P 126-127 .

[4] – د.هشام فريد رستم ،جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة و معاملة المجرمين ، مجلة الأمن العام العدد 151، سنة1995 ، ص24 .

أن الاعتداء على القيم يفترض دائما أن يقع على شيء محدد يكون محلا لحق محدد، و يجب أن تكون المعلومة مبتكرة و سرية كون السرية صفة لازمة تحصر حركة الرسالة و تحمل المعلومة في دائرة محددة من الأشخاص ، فلا يمكن تصور الجرائم الخاصة بالسرقة و النصب و خيانة الأمانة إذا انعدم هذا الحصر لأن المعلومة غير السرية تقبل التداول، و من 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 و على نحو مطلق[1].

و تماشيا مع ما ذكر 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 والابتكار والسرية والاستئثار والمجمعة عن طريق شبكات المعلومات والمعالجة آليا وفقا لأنظمة المعلومات.

ففي أول السبعينات ازدهرت صناعة جديدة أطلق عليها **صناعة المعلومات**، وأصبحت مصدرا للثروة و تتصف بعظمة التعقيد التقني و ضخامة ما يستثمر فيها من أموال، و أصبحت مقياسا لتقدم الأمم[3]، و مصدرا للقوة الاقتصادية و السياسية و العسكرية ،و موردا لا يقل و لا ينضب ،تتزايد دوما و لا تتناقص بالاستخدام، و لا تستهلك ،و ترتبط بالزمان و المكان ،و تتفاعل مع التطور ،و هي في الحقبة المعاصرة مفتاح للموارد الأخرى و سلعة و خدمة تباع و تشترى ،و مصدر قوة اقتصادية و سياسية لمن يحسن جمعها و تنسيقها و استخدامها لارتباطها بمختلف مجالات النشاط الإنساني و تداخلها في كل جوانب الحياة المعاصرة، و أصبح توفيرها و حسن استغلالها من الأسس الضرورية لدفع عجلة التقدم في الأمم و المجتمعات ،و صار تدفقها و انسيابها بمثابة النبض و العصب لجهود التنمية و التحديث و الرقي المعرفي و الحضاري و بات الوعي بأهميتها مظهرا و مقياسا لتقدم

[1]– د.حمد خليفة الملط ،المرجع السابق ،ص76 .

[2] - د. أحمد خليفة الملط ، المرجع السابق ،ص81.

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

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 و الأساسية 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، و البعض الآخر ذهب إلى التوسيع من مفهوم الجريمة المعلوماتية حتى أنه يمكن القول أنه يدخل في عدادها في كثير من الأحيان أفعال لا يمكن أن تعد من قبيل جرائم الحاسب الآلي .

الفرع الأول : 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 لا يكفي فقط أن تتوافر معرفة تكنولوجيا الحاسبات الآلية بدرجة كبيرة من أجل ارتكاب الجريمة المعلوماتية ولكن أيضا من أجل ملاحقتها ومتابعتها والتحقيق فيها بمعنى لا بد أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة والقائمون على معاينة وملاحقة مرتكبيها[3]، وقد أخذت وزارة العدل الأمريكية بهذا التعريف في تقرير صادر عنها عام **1989** المتعلق بجرائم المعلوماتية[4].

---

[1] – أنظر د.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 , P 517.

[3]– د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية، منشورات الحاتي الحقوقية، الطبعة الأولى 2005، ص 29 .

[4]- Benson (Carl), Jablon (Andrew), Kaplan (Paul) & Resenthal (Mara), Computer Crimes, Americain C.L.Review, vol.34, N°21,997, p.410.

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 يمكننا 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[1].

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 أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه**"[2] ، وما يعاب على هذا التعريف أنه يخرج من نطاق الجريمة المعلوماتية عدد كبير من الأفعال غير المشروعة والتي يستخدم فيها الحاسب الآلي كأداة لارتكابها كالاحتيال المعلوماتي والذي سنتناوله فيما بعد.

الفرع الثاني: الاتجاه الموسع من مفهوم الجريمة المعلوماتية

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

[1] - د.نائلة عادل محمد فريد قورة ، المرجع السابق، ص 29 .

[2] - د. هشام محمد فريد رستم ، المرجع السابق، ص31.

فيعرف فريق من الفقهاء الجريمة المعلوماتية بأنها:" **كل سلوك إجرامي يتم بمساعدة الحاسب الآلي** "، أو هي:" **كل جريمة تتم في محيط الحاسبات الآلية** "[1]. و يعرفها 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 و من 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، و من ذلك تعريفها بأنها:" **كل تلاعب بالحاسب الآلي و نظامه من أجل الحصول بطريقة غير مشروعة على مكسب أو إلحاق خسارة بالمجني عليه** "[4].

ويلاحظ من خلال التعريفات السابقة أنها قد أغفلت جانبا على قدر كبير من الأهمية في تعريف الجريمة المعلوماتية ألا و هو الدور الكبير الذي يقوم به الحاسب الآلي في هذه الجريمة، فإن كان من المتفق عليه أن الجريمة المعلوماتية قد تتخذ أحد المظهرين، يتمثل الأول في استخدام الحاسب الآلي كوسيلة لارتكاب الجريمة، و الثاني في الاعتداء على الحاسب الآلي ذاته، فإنه يثور أمامنا التساؤل الآتي: هل تعد الجريمة معلوماتية في كل الحالات التي يستخدم فيها نظام الحاسب الآلي من أجل ارتكاب الجريمة، و في كل الحالات التي يقع فيها اعتداء على الحاسب الآلي و نظامه؟

[1] - roden (adrian), computer crime and the law, C.L.J.., 1991, vol .15, p.399 .

[2] - د, هشام محمد فريد رستم، المرجع السابق، ص 29.

[3] - د.نائلة عادل محمد فريد قورة ، المرجع السابق. ص 30، 31.

[4] - law commission, working paper N° 110, computer misuse, London: HMSO, 1988 para.2.2.

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

و باستقرائنا لمختلف التعريفات نجد أن **تعريف منظمة التعاون الاقتصادي و التنمية (OECD)الخاص باستبيان الغش المعلوماتي** عام **1982** و الذي أوردته بلجيكا في تقريرها بأن الجرائم المعلوماتية هي: "***كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية***"[2] يتسم بالوضوح و ذلك 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 و ذلك لربطه بين الجريمة و أي 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 إذ بنصه على " تدخل التقنية المعلوماتية " يفتح المجال لكامل صور هذه التقنية القديمة و الجديدة و المستقبلية.

و نستخلص مما سبق أن اختلاف الفقه في وضع تعريف للجريمة المعلوماتية مرده الاختلاف في المعيار المعتمد عليه و الزاوية التي ينظر إليها كل اتجاه إلى هاته الجريمة .

[1] – د.نائلة عادل محمد فريد قورة ، المرجع السابق، ص 31.

[2] – د.أحمد خليفة الملط، المرجع السابق، ص 87.

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

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

- أن المشرع الجزائري اصطلح على الجرائم المعلوماتية بتسمية الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.
- أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة فسمى الجرائم الواقعة على النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في قانون العقوبات من المادة **394** مكرر إلى **394** مكرر **07** و ترك المجال واسع لأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية .
- أن المشرع الجزائري لم يقم بتحديد درجة دور المنظومة المعلوماتية أو نظام الاتصالات الإلكترونية في ارتكاب هذه الجرائم إذ حسب التعريف فإنه يكفي مجرد أن ترتكب الجريمة أو يسهل ارتكابها المنظومة المعلوماتية أو نظام الاتصالات الإلكترونية ، مما يجعل هذا 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.
- 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

1 - قانون 09-04المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها،الجريدة الرسمية العدد 47 لسنة 2009.

02 على أنها "نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر بمعالجة آلية 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.

المطلب الثاني : خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية ، و ذلك نتيجة ارتباطها بتقنية المعلومات و الحاسب الآلي مع ما يتمتع به من تقنية عالية ،و قد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات و الحقائق ، و التي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف **بالمجرم المعلوماتي** لتميزه أيضا عن المجرم التقليدي ،و قد كان لظهور شبكة المعلومات و تطورها إلى الصورة التي أصبحت عليها الآن فيما يعرف بالانترنت أثره في إعطاء شكل جديد للجريمة المعلوماتية.

و لعل أهم ما أضفته شبكة المعلومات على الجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود للجريمة ، و سوف نحاول فيما يلي التطرق إلى بعض السمات الخاصة بالجريمة المعلوماتية من خلال الفرع الأول ثم سنتناول بالدراسة أهم السمات التي تميز المجرم المعلوماتي في الفرع الثاني.

الفرع الأول : السمات الخاصة بالجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية من عدة جوانب ، سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة.

أولا : 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 و **3** مليون جريمة ضد الأموال[1].
- ارتفاع الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم التقليدية إذ حسب تقرير المركز الوطني للبيانات **(NCCCD)** 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** بليون 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 و على العكس من ذلك فالمجرم المعلوماتي عادة ما يكون ينتمي إلى مستوى اجتماعي مرتفع عن غيره من المجرمين ، و نادرا ما

---

1 – د. نائلة عادل محمد فريد قورة، المرجع السابق, ص 50.

2 –بحث منشور على شبكة الأنترنت www.google.com للباحث pernard D standlar تحت عنوان computer crime law عام 1999.

3- Rose (Philipe), la criminalité informatique à l'horizon 2005 – analyse prospective, l'harmattan, 1992.p 49.

4 - د. نائلة عادل محمد فريد قورة، المرجع السابق، ص 50.

يكون محترفا للإجرام أو عائد كما أنه لا ينظر إليه كمجرم بالمعنى المتعارف لهذه الكلمة[1] ، و ذلك لكون الأسباب و العوامل 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 و ذلك لأسباب تتعلق بسمعة المؤسسة التي يمثلها ومخافة 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 و ذلك بسبب وجوده في ظروف تجعل من قابليته للتعرض للجريمة مرتفع بشكل كبير و مرد ذلك إلى القصور الذي يكتنف أنظمة الحاسبات الآلية و الذي يساعد في ارتكاب الفعل الإجرامي[3].

- غياب الشعور العام بعدم أخلاقية الفعل أو بمساس بمصالح و قيم يحرص المجتمع على حمايتها بل إن الكثير من العاملين في مجال المعلوماتية لا يجدون حرجا في استعمال الشفرات و الدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة أو نسخ البرامج بدلا من شرائها ، و هذا لا ينفي وصف الجريمة عل هاته الأفعال من حيث اعتدائها على مصالح لها أهميتها في المجتمع ومن تم تستحق الحماية القانونية و معاقبة من يمس بها.
- وسيلة تنفيذ الجريمة المعلوماتية تتميز في أغلب الحالات بالطابع التقني، مما يجعل أدلة الإدانة فيها غير كافية و يرجع 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].

ثانيا : الطبيعة المتعدية الحدود(الدولية) للجريمة المعلوماتية

1 -Wasik (martin), crime and the computers, oxford university press ,1991.p 19.

2 – د. هشام فريد رستم ، المرجع السابق ، ص 41.

3 -Rose(philipe), op.cit.P 53.

4 – د.هشام فريد رستم ,لمرجع السابق, ص 41.

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

فالقدرة التي تتمتع بها الحاسبات الآلية في نقل و تبادل 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 و حجم المعلومات و الأموال المستهدفة و المسافة التي قد تفصل الجاني عن هذه المعلومات و الأموال، قد ميزت 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) ، و تتلخص 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]، و كان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل خلالها بطلب مبلغ مالي يرسل على عنوان حتى يتمكن المجني عليه من الحصول على مضاد للفيروس ، و في الثالث من فبراير عام **1990** تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية، و تقدمت المملكة المتحدة بطلب تسليمه لمحاكمته أمام القضاء الإنجليزي حيث إن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة

[1]- The Recommendation No . R89 – 9 on computer Related crime and final Report of the European committee on Crime problems ,Srasbourg 1990, P83.

2 برنامج له قدرة كبيرة على الإختفاء بالبرنامج الأصلي, وعند تشغيل البرنامج يبدأ نشاطه التدميري الذي يؤدي إلى تعديل ومحو بعض البيانات وقد يصل به الحد إلى تدمير النظام كله,نقلا عن أحمد خليفة الملط, المرجع السابق,ص543.

، و بالفعل وافق القضاء الأمريكي على تسليم المتهم و تم توجيه له إحدى عشرة تهمة ابتزاز وقعت معظمها في دول مختلفة ، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية .

و أيا ما كان الأمر فإن لهذه القضية أهميتها من ناحيتين، الأولى: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية، و الثانية، 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 توجد بها المعلومات محل الجريمة ، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب[2] .

كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية و بصفة خاصة فيما يتعلق بجمع و قبول الأدلة[3] ، و لذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية و العمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم ، فيجب أن يشمل هذا التعاون تبادل المعلومات ، تسليم المجرمين ،و ضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى ،كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية ،و هو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، و تعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "**إبرام الاتفاقيات الدولية**".

و تعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية و تجنب خلق ما يسمى "**بجنة جرائم المعلوماتية Computer Crime Havens**" ، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي بطبيعة الحال التنسيق بين قوانين

---

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

[2] – إن المشرع الجزائري قد عقد الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني ، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني وهذا ما نصت عليه المادة 15من قانون 04/09

[3] – د. نائلة عادل محمد فريد قورة ، المرجع السابق، ص54.

الدول المختلفة لضمان تحقق "مبدأ ازدواجية التجريم"، إذ نجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها حتى تتلاءم مع هذه الجرائم.

و تجدر الإشارة أن المشرع الجزائري قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون رقم **15/04** المعدل و المتمم للأمر **156/66** المتضمن قانون العقوبات ،و الذي 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 2009.08.05** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها إذ تضمن بعض القواعد الإجرائية الخاصة بالتفتيش و الحجز في مجال هذه الجرائم ، كما أنشأ هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام و الاتصال و مكافحته و سن أحكام خاصة بالتعاون و المساعدة القضائية الدولية [1].

ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المختلفة في محورين :

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

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

الفرع الثاني : السمات الخاصة بالمجرم المعلوماتي

[1] - و قد علق المشرع الجزائري التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال على شرط احترام الاتفاقيات الدولية ذات الصلة و الاتفاقات الدولية الثنائية و مبدأ المعاملة بالمثل ، و من ثمة نستخلص أنه لا غنى عن الاتفاقات الدولية في مجال مكافحة هذه الجريمة .

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.

و لقد اختلف الباحثون في تحديد هذه السمات[1]، و يعد الأستاذ **Parker** واحدا من أهم الباحثين الذين عنوا الجريمة المعلوماتية بالدراسة بصفة عامة و بالمجرم المعلوماتي بصفة خاصة ، ومع ذلك يعد المجرم المعلوماتي مجرما لارتكابه فعل إجرامي يتطلب توقيع العقاب عليه، وكل 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.

ويتميز 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]

وتعد **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.

---

[1] – د.نائلة عادل فريد قورة ،المرجع السابق، ص 54.

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) "White collar criminality " Gers (Gilbert) in white collar criminal The offender in business the professions atherton press 1968.

[3] -Parker (Donn B) Figding computer crime A new Framework for protecting information 1998/P 114

إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال, بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم 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 ملابساتها و مدى إمكانية نجاحها أو فشلها ، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته كون 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 أن 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 التي تعطي للفاعل مزايا متعددة مثل فتح الملفات و محو أو تعديل محتوياتها أو 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 غير مشروع يظل الباعث

1 – د. نائلة عادل محمد فريد قورة ، المرجع السابق ، ص 57.

الأول وراء ارتكاب الجريمة المعلوماتية[1] ، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب و تخطي حواجز الحماية المضروبة حوله، و أخيرا الانتقام من رب العمل أو أحد الزملاء .

و يفرق مرتكبي هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية لاأخلاقية ، و بين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم، و هو ما يطلق عليه أعراض روبن هود **The Roben Hood Syndrome** [2]. وهذا ما سنتناوله في المبحث الموالي.

المبحث الثاني : دوافع ارتكاب الجريمة المعلوماتية

الدافع ، الباعث ، الغرض أو الغاية تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي تتصل بما يعرف بالقصد الخاص في الجريمة.

وللجريمة المعلوماتية عدة دوافع لارتكابها فبعضها يرجع إلى دوافع شخصية و البعض الآخر يرجع إلى دوافع خارجية ، و كل هذه الدوافع يكون مصدرها الرغبة الإجرامية و هذا ما سنتعرض له من خلال المطلبين التاليين.

المطلب الأول : الدوافع الشخصية

يقصد بالدوافع الشخصية تلك العوامل اللصيقة بشخصية المجرم المعلوماتي و التي تدفعه لارتكاب الجريمة المعلوماتية .

ويمكن رد الدوافع الشخصية لدى مرتكب الجرائم المعلوماتية إلى دوافع مالية و هذا ما سنتناوله في الفرع الأول و أخرى ذهنية أو نمطية نتناولها في الفرع الثاني.

---

[1] –و يرى البعض أن أغلب مجرمي المعلوماتية ليس لديهم أطماع مادية بقدر ما يحاولون حل مشكلات مادية تواجههم لا يستطيعون حلها باللجوء إلى الجرائم الأخرى أنظر Parker (DonnB),OP-cit, p142 .

2– أنظر الدكتور هشام محمد فريد رستم، المرجع السابق، ص38.

الفرع الأول : الدوافع المادية

يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل ، و هو من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم المعلوماتية ، ذلك أن خصائص هذه الجرائم ، و حجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع بما يحققه من ثراء فاحش .

و من أمثلة ذلك ذلك ما حدث في فرنسا سنة **1986** حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو **70000** فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على **670.000** فرنك فرنسي[1].

ومنذ بداية الظاهرة فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر و فيما بعد احتيال الإنترنت هو تحقيق الكسب المالي، ففي دراسة الفقيه **Parker** الصادرة في إحدى مجلات المتخصصة بخصوص موضوع الأمن المعلوماتي تبين أن[2] :

- 34% من جرائم الغش المعلوماتي ترتكب من أجل اختلاس الأموال.
- 23% ترتكب من أجل سرقة المعلومات.
- 19% ترتكب من أجل الإتلاف.
- 15% ترتكب من أجل سرقة وقت الحاسوب لأغراض شخصية .

وإذا انتقلنا للدراسات الحديثة كالدراسات المسحية و الدراسات الإحصائية و التقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية **N.F.I.C**.[3] نجد أن هذا الدافع يسود على غيره من الدوافع ، الشيء الذي يعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية.

1 - Rose philippe la criminalité informatique que sais je ? 1er édition, PUF, 1988, P 490.

2 – نبيل صقر، موسوعة الفكر القانوني ، جرائم الكمبيوتر و الأنترنت في التشريع الجزائري ، دار الهلال للخدمات الإعلامية، طبعة 2005، ص 118.

3 – للمزيد من التفاصيل أنظر. نبيل صقر، المرجع السابق، ص62-63.

وهناك فئة من مرتكبي الجرائم المعلوماتية يرجع ارتكابهم لها إلى الديون الناتجة من المشاكل العائلية و الخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، فقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه الحالات، فالغاية تبرر الوسيلة[1].

الفرع الثاني : الدوافع الذهنية أو النمطية

تعتبر الدوافع الذهنية أو الدوافع النمطية تلك العوامل النفسية اللصيقة بالمجرم المعلوماتي تدفعه إلى ارتكاب الجريمة المعلوماتية بهدف الرغبة في إثبات الذات و تحقيق انتصار على تقنية الأنظمة المعلوماتية و الرغبة في قهر النظام و التفوق على تعقيد و سائل التقنية دون أن يكون له نوايا آثمة .

و يرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم، و عليه فإنه يرى البعض"أن الدافع إلى ارتكاب الجرائم المعلوماتية يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح"[2].

في حين أن الدراسات لا تظهر هذه الحقيقة على إطلاقها إذ يظهر السعي إلى تحقيق الربح دافعا أكثر تحريكا لجرائم المعلوماتية من الرغبة في قهر النظام إلا أن الدافع الأخير يتجسد في نسبة مرتفعة من جرائم المعلوماتية خاصة ما يعرف بأنشطة "**HACKERS**" المتطفلين الداخليين [3] على النظام و المتجسدة في جرائم التواصل مع أنظمة الحاسب تحديدا عن بعد.

و يميل مرتكبوا الجرائم المعلوماتية إلى إظهار تفوقهم ومستوى ارتقاء براعتهم ، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجاد و غالبا ما يجدون الوسيلة للتفوق عليها، و يتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم المعلوماتية

1 – أنظر د. أحمد خليفة ملط ، المرجع السابق ، ص 89.

2 – أنظر د. أحمد خليفة الملط ، المرجع السابق ، ص 90.

3 – حسب ترجمة غرفة التجارة العربية البريطانية،و الخارق المأجور حسب ترجمة الأستاذ كامل سعد .

الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة كسر حواجز الأمن لأنظمة الحواسيب و شبكات المعلومات لإظهار تفوقهم على وسائل التقنية .

و إن هذا الدافع هو أكثر الدوافع التي يجري استغلاله من قبل المنظمات الإجرامية لأجل استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة[1].

بالإضافة لهذه الدوافع الشخصية اللصيقة بشخص المجرم المعلوماتي هناك دوافع أخرى خارجية خارجة عن نطاق المجرم المعلوماتي تدفعه لارتكاب الجريمة نتطرق لها في المطلب الموالي.

المطلب الثاني : الدوافع الخارجية

في بعض المواقف يتأثر الإنسان و يستسلم للمؤثرات و الدوافع الخارجية بارتكابه بعض الجرائم المعلوماتية، نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات .

و تتعدد المؤثرات التي تدفع المجرم المعلوماتي إلى اقتراف مثل هذا السلوك من بينها دافع الانتقام و التواطؤ على الإضرار برب العمل و دافع المنشأة نوردها في الفرعين المواليين .

الفرع الأول : دافع الانتقام و إلحاق الضرر برب العمل

قد يكون الانتقام مؤثرا في ارتكاب الجرائم المعلوماتية ، إذ قد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل و المشكلات المالية و من طبيعة علاقات العمل المنفردة في حالات معنية، و هذه العوامل قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة مثلت قوة محركة لبعض العاملين لارتكاب جرائم المعلوماتية ،باعثها الانتقام من المنشأة أو رب العمل.

[1] - نبيل صقر، المرجع السابق، ص 119.

و من أمثلة ذلك قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشآت بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات و ديون المنشأة[1] .

و تجدر الملاحظة أن مرتكبو الجرائم المعلوماتية و التي يكون دافعهم لارتكابها هو الانتقام و إلحاق الضرر برب العمل عادة ما يلجئون إلى استخدام أنشطة زرع الفيروسات في نظم المعلوماتية .

الفرع الثاني : الدوافع الخاصة بالمنشأة

يقصد بالدوافع الخاصة بالمنشأة أو المؤسسة تلك العوامل الخارجية التي تسهل للجاني ارتكاب الجريمة داخل المنشأة باستعماله التقنية المعلوماتية الخاصة بالمؤسسة إذ تكون وسائل ارتكاب الجريمة المعلوماتية في متناوله .

إذ يعتقد بعض المتخصصين في تقنية الأنظمة المعلوماتية,أن العاملين في منشأة معينة أن من مزايا مراكزهم الوظيفية و مهاراتهم الفنية استخدام الأنظمة المعلوماتية و برامجها لأغراض شخصية أو ممارسة بعض الهوايات الدائرة في مجال التقنية ، و من شأن ذلك أن يؤدي إلى تمادي بعضهم إلى استخدام الأنظمة بصفة غير مشروعة تصل إلى ارتكاب جرائم خطيرة بالمنشأة لمصلحته الخاصة [2].

و من أمثلة ذلك قيام مستشار لدى أحد البنوك الكبرى يسمى **Stanley Rifkin** تحويل مبلغ **10** مليون دولار إلى حساب بنكي مفتوح باسمه في سويسرا كونه كان يتمتع بثقة مطلقة من البنك و كون أن اختصاصاته سمحت له بالولوج إلى مفتاحين إلكترونيين من ثلاثة أساسية للتحكم في التحويلات الإلكترونية للنقود من بنك لآخر ، و قد تمكن بفضل معالجته الآلية للمعلومات و تألفه الشديد مع النظام المعلوماتي من الوصول إلى المفتاح الثالث [3].

و في الأخير نخلص إلى القول أن الفعل الواحد قد يعكس دوافع متعددة و خاصة، فمحرك أنشطة الإرهاب الالكتروني و حروب المعلومات دوافعه سياسية و إيديولوجية ،في حين أن أنشطة

[1] - comment se protéger contre le crime informatique. temps réels P264-1984.
[2] : د . أحمد خليفة الملط ، المرجع السابق ، ص 91 .
[3] - Voir, L'informatique nouvelle ,Sep.1980.P20,Temps réels no1,9-21981.

الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، و قد تتداخل و تشترك هذه الدوافع في الفعل الواحد فتتمازج دون إمكانية التفرقة بينها.

و بناءا على ما تقدم يمكن أن نقسم مجرمي المعلوماتية **Cyber criminals** إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية و يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة و تتمثل هذه الطوائف فيما يأتي[1] :

-**تضم الطائفة الأولى**: **Pranksters** الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية و المزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث).

-أما الطائفة الثانية "Hackers" فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها و كسر الحواجز الأمنية الموضوعة لهدا الغرض، و ذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

-وتتضمن الطائفة الثالثة "Malicious Hackers" أشخاص هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، و يندرج تحت هذه الطائفة الكثيرون من مخترعي فيروسات الحاسبات الآلية و موزعيها.

-أما الطائفة الرابعة "Personnel Problem Solvers" فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ويكون الهدف من ورائها إيجاد حلول لمشكلات مادية تواجههم، و لا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية وغالبا ما يكون المجني عليه مؤسسة مالية.

-وتشمل الطائفة الخامسة "Career Criminals" مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على أفعالهم وصف الجريمة المنظمة ،أو على الأقل يشترك

[1]- د نائلة عادل محمد فريد قورة ، المرجع السابق ، ص 58 .

في تنفيذ النشاط الإجرامي أكثر من فاعل ، و يقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي[1] .

-أما الطائفة السادسة "Extreme Advocates" فتدخل في عدادها الجماعات الإرهابية أو المتطرفة ،و التي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات و أفكار اجتماعية أو سياسية أو دينية و يرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، و يركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص و الممتلكات من أجل لفت الأنظار إلى ما يدعون إليه ، و إن اعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالها و الأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات.

و من الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوربا باسم "**The Red Brigades**" بتدمير ما يزيد عن 60 مركزا للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها و معتقداتها[2].

-و أخيرا تأتي الطائفة السابعة "The Criminally Negligent" و التي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا و هي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية في أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح ، ففي نيوزلندا على سبيل المثال قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات و لم يتمكنوا من إبلاغ قائد الطائرة لهذا التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال و قتل 60 راكبا على متنها، و لقد تمت محاكمة المتهمين بتهمة القتل الخطأ[2].

[1] -Parker (DonnB) ,op_cit,P144-146.

2 - د . نائلة عادل محمد فريد قورة ، المرجع السابق ، ص63 .

[2] - د. نائلة فريد محمد قورة ،المرجع السابق ، ص 63 .

و بعد عرضنا لدوافع ارتكاب الجريمة المعلوماتية نتطرق في المبحث الموالي لأنواعها حتى نضبط مفهومها أكثر.

المبحث الثالث : أنواع الجرائم المعلوماتيـة

تعددت محاولات الفقه لتحديد أنواع الجرائم المعلوماتية و ذلك لصعوبة حصر هذه الأنواع بصفة دقيقة بالنظر لحداثة ظهور هذه الجريمة و كذا عدم وجود 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 التقسيـم.

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].

وقسمها 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 تتمثل 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] .

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.

[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 criminal justice, Vol. 34, 1997, b p 3-27.
[2]- Wasik (Martin),op, cit .p41.

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 في المعلومات بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة إذ يستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسب الآلـي.

وتتمثل 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 المطلبين المواليين.

المطلب الأول : الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

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

و يهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة [2]،إذ تهدف هذه الجرائم الاعتداء على أموال الغير ،فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته أو برامجه أو نظمه كوسيلة لتنفيذ الجريمة ، و منه لا يكون النظام المعلوماتي هو محل الحماية الجنائيـة.

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 ، نتعرض لهذه الأفكار بشكل من التفصيل من خلال الفروع الثلاثة الموالية كالآتـي.

1 - د. نائلة عادل محمد فريد قورة ، المرجع السابق، ص 256 .

2 - د نائلة عادل محمد فريد قورة ، المرجع السابق ، ص 265 .

الفرع الأول: 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، و أما الطائفة الثانية تكمن في الجرائم الواقعة على حرمة الحياة الخاصة نتناولها فيما يأتي:

أولا : طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية والأدبية

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 أن للمعلومة قيمة أدبية بجانب قيمتها المادية و يندرج ضمن الحقوق الفكرية كذلك براءات الاختراع إذ تمثل فكرة للمخترع تحتوي على حق معنوي و آخر مالي للمخترع [1].

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

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

حقوق المؤلف يحميها القانون .

1 - د 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 وقد حذا الدستور الجزائري حذو الدساتير الدولية بحرصه على حماية الحياة الخاصة للمواطنين[1] بموجب المادة: **39** من الدستور الجزائري والتي تنص على أنه"لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون.

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة."

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

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 [2].

وعليه 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 ولكن يقوم المكلف بحفظها بإطلاع الغير عليها بدون إذن صاحبها، أو أن يقوم شخص اختراق معلومات تتمثل في أسرار مكتوبة و سيرٍ ذاتية و مذكرات حياة شخصية لشخص آخر[3].

1 تنص المادة 45 من الدستور المغربي"الحياة المواطنين الخاصة حرمة يحميها القانون و المراسلات والبرقيات والمحادثات التيلفونية وغيرها من وسائل الاتصال لها حرمتها وسريتها مكفولة ولا تجوز مصادرتها أو الإطلاع عليها أو رقابتها إلا بأمر قضائي مسبب و لمدة محدودة وفقا لأحكام القانون".

2 - د .نائلة عادل محمد فريد قورة ، المرجع السابق ، ص 275 .

3 - د. أحمد خليفة الملط ، المرجع السابق، ص187.

الفرع الثاني : 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 المعلومات بالقراءة على ما هو مكتوب عليها أو باستخدام مكبر الصوت[1] .

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 [2].

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

1 - د أحمد خليفة الملط ، المرجع السابق ، ص 190 .
2- د محمد سامى الشوا ، ثورة المعلومات و انعاكساتها على قانون العقوبات ، دار النهضة العربية ،1994 ، ص 67 .

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 [1].

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.

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[2].

1 - د أحمدخليفة الملط ، المرجع السابق ،ص 192.
2 - د أحمد خليفة الملط ، المرجع السابق ، ص 196 .

الفرع الثالث : الجرائم المعلوماتية الواقعة على الأسرار

تقع هذه الجرائم باستعمال النظام المعلوماتي لإفشاء الأسرار سواء كانت الأسرار عامة تخص مصالح الدولة و نظام الدفاع عنها أو أسرار خاصة تتعلق بالأفراد أو المصالح الاقتصادية للمؤسسات المختلفة أو ما يطلق عليها الأسرار المهنية ، و يتخذ هذا النوع من الجرائم صورتين الأولى تتعلق بالجرائم الواقعة على أسرار الدولة و الثانية تتعلق بالجرائم الواقعة على الأسرار المهنية .

و تقع هذه الجريمة لسرقة معلومات قصد التشهير بشخص أو جماعة معينة أو بيعها لتحقيق مصالح مختلفة كالحصول على عائد مادي ممن يهمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الامتناع عن القيام بعمل.

و هذه الجرائم تسبب أضرار لأصحابها أدبية و مادية معتبرة ، لذا حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات و الجنح ضد الشيء العمومي من المادة **61** إلى **96** مكرر من قانون العقوبات [1] بالإضافة للمادة **394** مكرر **03** من قانون العقوبات التي نصت " تضاعف العقوبات المنصوص عليها في هذا القسم [2]إذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام ، دون إخلال بتطبيق عقوبات أشد " ، و حذا بذلك حذو مختلف تشريعات الدول على غرار المشرع المصري الذي نص على ذلك في قانون العقوبات في الكتاب الثاني المتعلق بالجنايات و الجنح المضرة بأمن الحكومة لاسيما عندما يكون إفشاء هذه الأسرار متعلقا بأسرار الدفاع الوطني[3] .

كما أن القانون الفيدرالي للولايات المتحدة الأمريكية لجرائم الحاسبات الآلية الصادر سنة **1984** عاقب بموجب أحكام المادة **01،03/1040** كل من يقوم بالدخول غير المصرح له إلى نظام الحاسب

1 - الأمر 156/66 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات المعدل و المتمم .
2 - القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات .
3 - د أحمد فتحي سرور ، الوسيط في قانون العقوبات ، الطبعة الرابعة ، سنة1991 ، ص 47 .

الآلي بإفشاء معلومات توجد داخل هذا الحاسب الآلي متى كان هذا الحاسب يستعمل بواسطة حكومة الولايات المتحدة الأمريكية أو لمصلحتها و ترتب عن ذلك الإضرار بهذا الاستعمال[1] .

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 الدعـاوى [2].

المطلب 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:

الفرع الأول: جرائم الاعتداء على المكونات المادية للنظام المعلوماتي

1 - د نائلة محمد فريد قورة ، المرجع السابق ، ص 276 .

2 - د أحمد خليفة الملط ، المرجع السابق ، ص 200 ، كما أن المشرع الجزائري نص من خلال المادة 301 من قانون العقوبات على معاقبة الأطباء و الجراحون و الصيادلة و القابلات و جميع الأشخاص المؤتمنون بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليهم و أفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاءها و يصرح لهم بذلك ، كما أن المادة 302 من قانون العقوبات تعاقب كل من يعمل بأية صفة كانت في مؤسسة و أدلى أو شرع في الإدلاء إلى أجانب أو إلى جزائريين يقيمون في بلاد أجنبية بأسرار المؤسسة التي يعمل فيها دون أن يكون مخولا له بذلك .

يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة و المعدات الملحقة به و التي تستخدم في تشغيله كالأسطوانات و الشرائط و الكابلات...إلخ، ونتيجة للطبيعة المادية لهذه المكونات فالاعتداء عليها يكون عن طريق جرائم عادية و تقليدية[1]، كأن تكون محلا للسرقة أو خيانة الأمانة أو الإتلاف العمدي كإحراقها أو ضرب الآلات بشيء ثقيل أو حاد أو العبث بمفاتيح التشغيل أو خربشة الشريط و إفساد أسطوانات التشغيل مغناطيسيا بتعريضها إلى أي مجال مغناطيس متلف، و يترتب على هذا الإتلاف خسائر كبيرة[2].

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 ب **5** ملايين فرنك فرنسي[3].

و يرى البعض من الفقهاء أنه يندرج ضمن هذه الطائفة من الجرائم المعلوماتية سرقة وقت الآلة، فقد يلجأ العاملين بالنظام المعلوماتي إلى استخدامه في أعمال خاصة بهم، و عليه تكون واقعة السرقة منصبة على وقت الجهاز الذي يمكن تقويمه ماليا و ليس على الأشياء المادية بمعنى الكلمة[4].

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.

الفرع الثاني: جرائم الاعتداء على المكونات المنطقية (البرامج) للنظام المعلوماتي

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة ، و قد تقع هذه الجرائم إما على البرامج التطبيقية و إما على برامج التشغيل و سنتطرق لهاتين الصورتين فيما يأتي:

1 - د أحمد خليفة الملط ، المرجع السابق ، ص 176.
2 - د. ذكي ذكي أمين حسونة، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 1993 في الفترة من 25 إلى 28 أكتوبر 1993 تقرير مصر، ص 471.
3- Rose (philippe), OP-cit, p58,59.
4- André Lucas, le droit de l'informatique, paris, PUF 1987, P519,521.

أولا: الجرائم المعلوماتية الواقعة على البرامج التطبيقية

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

أ- تعديل البرنامج: الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود و تكثر هذه الجرائم في مجال الحسابات[1] .

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** [2].

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[3].

ب – التلاعب في البرنامج: يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية[4] أو عن طريق قيام أحد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي

1 - د. أحمد خليفة الملط ،المرجع السابق، ص173.

2- Duleroy ® et rocco (A.M), l'informatique nouvelle, avril 1976, les escrocs a l'informatique, le nouvel Economsiste, les octobre, 1979, n 202.

3 - د. أحمد خليفة الملط ، المرجع السابق ، ص 174.

4 هي عبارة عن برنلمج أو جزء من برنامج ينفد في لحظة محددة أو كل فترة زمنية منتظمة ويتم وضعه في شبكة معلوماتية بهدف أو حالة فحوى النظام بغرض تسهيل تنفيد عمل غير مشروع.نقلا عن أحمد خليفة الملط, المرجع السابق,ص545.

يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي، و يصعب اكتشاف هذا البرنامج لصغره و دقته[1].

ثانيا: الجرائم المعلوماتية الواقعة على برامج 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 بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[2].

و يتحقق هذا النوع من الجرائم المعلوماتية في شكلين:

أ- **المصيدة:** تتمثل هذه الصورة في إعداد المبرمج برنامج به أخطاء و عيوب عمدا، لا يكتشف بعضها عند استخدام البرنامج، إذ يترك المبرمج ممرات خيالية و فواصل و تفرعات في البرنامج حتى يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرعات إضافية 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[3].

ب – 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

1 - و قد قام مبرمج بأحد البنوك زرع برنامج فرعي بمنشأة بالكيانات المنطقية بإدارة الحسابات يتجاهل كل عمليات السحب التي تتم من قبله عن طريق بطاقات أو شيكات حسابية إذ يتحمل البنك نتيجة لذلك هذه الحسابات في باب ميزانية الإدارة ، لأكثر من التفاصيل راجع le rapport du conseil de l'Europe, 15,18 novembre 1976.
2 - د. أحمد خليفة الملط ، المرجع السابق ، ص 175.
3 - د. محمد سامي الشوا ، المرجع السابق ، ص 82.

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[1].

الفرع الثالث: 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:

أولا: التلاعب في المعلومات

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 الحصول على مرتباتهم[2] ، 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[3].

في حين التلاعب غير المباشر يتم عن طريق التدخل غير المباشر لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين أو بواسطة التلاعب عن بعد باستخدام أدوات معينة و

1- Equity fuding life insurence, l'informatique nouvelle, mai 1976.

2 - قام أحد المسؤولين عن القسم المالي بإحدى الشركات الفرنسية اختلاس أكثر من مليون فرنك فرنسي و وضعه في حسابه الخاص و حساب شركائه باستعمال هذه الطريقة ، لأكثر من التفاصيل أنظر Escroquerie aux Assedic de paris, jugement du 2 fev 1982 TGI de paris 13 ème ch expertise n°39, avril 1982

3 - 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 1976n°73

معرفة أرقام وشفرات الحسابات[1]، 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[2].

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 و الحصول على المنفعة المالية التي يريدها من مسافات بعيدة.

ثانيا: إتلاف المعلومات .

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

ويتخذ الإتلاف عدة صور فقد يتم عن طريق طرق الإتلاف العادية كالحريق أو الضرب أو السرقة أو عن طريق استبدال أو محو المعلومات.

ويشكل استبدال المعلومات نوع من جرائم الغش أو التزوير المعلوماتي و هو على درجة كبيرة من الخطورة لأنه في حالة نجاحه يستمر لوقت طويل قبل اكتشافه و يتولد عنه مكاسب كبيرة بمجرد استبدال رقم بآخر أو إحلال رقم مكان آخر[3] ، فمثلا هناك مجموعة من المستخدمين الإداريين استطاعوا خلال سنوات قليلة مضاعفة رواتبهم عن طريق النظام المعلوماتي[4].

1 - د. أحمد خليفة الملط ، المرجع السابق ، ص179.
2 - Trib de paris, 12 ème ch, corr, jugement du 13 janv 1982, DALLOZ S 1982,p 502.
3 - د. أحمد خليفة الملط, المرجع السابق, ص182.
4 - د. محمد سامي الشوا ,المرجع السابق, ص 75.

وقد استعمل شخص يدعى **vladimir loriblitt** بإسرائيل طريقة تدعى ب **bluff** إذ كان يعمل بوزارة المالية و قام بإدخال فواتير وهمية لا حصر لها و تحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي اصطنعها.

وأما محو المعلومات فهو من أسهل طرق الإتلاف كون أنه من خصائص الجرائم المعلوماتية قدرة الجاني على محو آثار جريمته في فترة وجيزة جدا لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو البرنامج عن طريق الفأرة، فمثلا قام شخصان باختلاس مبلغ يقدر ب **61.000** دولار مرسلة من شركات التأمين إلى إحدى المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز و جعلها غير قابلة للتحصيل[1].

وفي الأخير بعد تناولنا في هذا الفصل الجرائم المعلوماتية بصفة عامة ، أين بينا مختلف الآراء الفقهية في تعريف الجريمة المعلوماتية انتهينا إلى كونها كل اعتداء على النظام المعلوماتي أو يتم باستخدام النظام المعلوماتي و كان له دور رئيسي في السلوك المجرم ، و هي بهذا المفهوم تتميز بعدة خصائص تميزها عن باقي الجرائم الأخرى إذ من أهم هذه السمات طبيعتها المتعدية الحدود و طابعها التقني الذي يعقد من مسألة إثباتها الشيء الذي يميز مرتكبيها و يجعل دوافع ارتكابهم للجرائم المعلوماتية بمختلف أنواعها تختلف عن المجرمين العاديين .

كما أن للنظام المعلوماتي أهمية كبيرة باعتباره تقنية حديثة في عالم تكنولوجيا المعلومات ، إلا أنه غالبا ما يكون مصدر خصب للجرائم التي تقع عليه و بواسطته، و بذلك تعد الجرائم المعلوماتية جرائم خطيرة و سريعة و متطورة و في تزايد مستمر تبعا لازدياد استخدام تلك التقنية ، و لذا سنحاول من خلال الفصل الموالي إبراز صور الحماية الجزائية للمعلوماتية في التشريع الجزائري لما لها من قيمة مالية و اقتصادية كبيرة.

1 -Le monde informatique, 21 fev 1983, sous le titre « la délinquance en cal belanc se parte lien ».

الفصل الثاني : الحماية الجزائية للمعلوماتية في التشريع الجزائري

إن مهمة تقريرالحماية الجزائية للمعلوماتية مهمة صعبة تعترضها صعوبة منهجية مصدرها تشعب الجوانب التي تتعلق بالمعلوماتية[1]، وكذا حداثة الموضوع واتسامه بطبيعة علمية بحتة تخرج من مجال تكوين رجال القانون[2].

ونتيجة لذلك اختلفت وجهات نظر الفقهاء والمشرعين والقضاة فيما يخص أمر الحماية الجزائية المقررة للمعلوماتية، وهذا ما سنتطرق له من خلال هذا الفصل وذلك بالتعرض في المبحث الأول للفرضية القائلة بالحماية الجزائية للمعلوماتية في إطار نصوص جرائم الأموال و ذلك بالتفصيل في مدى إمكانية خضوع أفعال الاعتداء على المعلوماتية للنصوص التقليدية لجرائم الأموال باعتبار الإعلام الآلي قيمة اقتصادية جديدة، و لنتعرض في مبحث ثاني للفرضية القائلة بالحماية من خلال نصوص الملكية الفكرية باعتبار المعلوماتية نتاج فكر و إبداع، لنتعرض أخيرا في مبحث ثالث للاتجاه الحديث في حماية المعلوماتية من خلال نصوص مستحدثة واكبت صدور القانون **15/04** المعدل و المتمم للأمر **156/66** المتضمن قانون العقوبات، و الذي استحدث نصوصا خاصة بالجرائم المعلوماتية الماسة بالأنظمة المعلوماتية و الذي نأمل من خلال إدماج أحكام خاصة بالإجرام المعلوماتي سيساهم في مسايرة التشريع للتطورات التكنولوجية[3].

[1] - أمال قارة، ، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة الطبعة الأولى سنة 2006 , ص 09.

[2] - أمال قارة، المرجع السابق، ص 08.

[3] - د .محمود محمود مصطفى ، شرح قانون العقوبات القيم الخاصة، الطبعة 8، سنة 1984 مطبعة جامعة القاهرة ، ص 304.

المبحث الأول : الحماية الجزائية للمعلوماتية من خلال نصوص جرائم الأموال

إن ظهور المعلوماتية و تطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة ، و من أهمها ما يسمى أزمة القانون الجنائي في مواجهة واقع المعلوماتية مما أدى إلى البحث في الأوضاع القانونية القائمة و مدى ملاءمتها لمواجهة هذه المشاكل .

ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية **بمبدأ شرعية الجرائم** فإنه لا يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى و لو كانت أفعالا مستهجنة، و على مستوى عال من الخطورة الإجرامية.

ومن ثم سنحاول تحديد مدى إمكانية استعانة القاضي الجزائي بقانون العقوبات التقليدي لتوفير الحماية لهذه القيمة الاقتصادية الجديدة ألا و هي المعلوماتية في ظل النصوص التقليدية ، والذي تحكمه مبادئ القانون الجنائي وفي مقدمتها "**مبدأ الشرعية**" والذي يتفرع عنه مبدأين أساسيين أولهما التفسير الضيق للنص الجنائي , وثانيهما حضر القياس في مجال التجريم ,بالإضافة إلى كون أن ظاهرة المعلوماتية لم تكن مطروحة على الساحة التشريعية وقت سن النصوص التقليدية ، و هنا تكمن خطورة المحاولة.

و عليه سنقوم بدراسة جرائم الاعتداء على الأموال في هذا المبحث و المتمثلة في جريمة السرقة و النصب و خيانة الأمانة و كذا تحطيم ملك الغير، كونها تشترك في المصلحة المحمية ألا و هي الأموال ، كما أنها تتحد في الموضوع و القصد ، كون محل الجريمة يتمثل في مال منقول مملوك للغير قصد الجاني فيها ضم المال إلى ملكه[1]، في حين أنها تختلف فيما بينها من ناحية الوسيلة التي يلجأ إليها الجاني في الحصول على مال الغير ففي السرقة ينتزع الجاني حيازة المال بغير رضاء صاحبه[2]، و في النصب لا يحصل الجاني على المال من صاحبه باختياره و إنما تحت تأثير طرق

1- أنظر في هذا المعنى د/أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول ،الجرائم ضد الأشخاص و الجرائم ضد الأموال، الطبعة الخامسة منقحة و متممة في ضوء النصوص الجديدة ،دار هومه ، 2006 ، ص249،248 .

2-د/أحسن بوسقيعة ، المرجع السابق، ص255 .

احتيالية[1] ، و أما في خيانة الأمانة يغير الجاني نيته في حيازة الشيء من حيازة وقتية أو ناقصة إلى حيازة كاملة بقصد التملك[2] .

ولكن قبل ذلك يتوجب علينا أولا تحديد مدى اعتبار المعلوماتية موضوعا لجرائم الأموال وهذا ما سنناوله في المطلب الأول , ثم نتطرق في المطلب الثاني إلى مدى خضوع المعلوماتية للنشاط الإجرامي لجرائم الأموال .

المطلب الأول : مدى اعتبار المعلوماتية موضوعا لجرائم الأموال

لتحديد مدى إمكانية إخضاع الاعتداءات الواردة على أموال الإعلام الآلي للنصوص التقليدية لجرائم الأموال ، وجب أولا البحث في مدى إمكانية انطباق وصف المال على المعلوماتية ، و ثانيا البحث في مدى اعتبار المعلوماتية مالا يصلح أن يكون موضوعا لجرائم الأموال ، هذا ما سنتطرق له من خلال الفرعين المواليين.

الفرع الأول : مدى انطباق وصف المال على المعلوماتية

يعتبر **المال** كل ما يصلح أن يكون محلا للحق ذو القيمة المالية ، و الشيء هو محل الحق، و تنقسم الأشياء إلى أشياء مادية و أخرى غير مادية أي معنوية.

و يقصد بالمال المعلوماتي الحاسوب بكل مكوناته و هو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات و معالجتها و تخزينها و استرجاعها عند الطلب، و يتكون من كيانين: كيان مادي، و آخر معنوي.

1- أنظر في هذا المعنى ، د/أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول,المرجع السابق ، ص 305 .

2- أنظر في هذا المعنى ، د/أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول, المرجع السابق ، ص 347 .

يضم **الكيان المادي Hardware** الأجهزة المادية المختلفة و هي جهاز الإدخال جهاز الإخراج و وحدات التشغيل المركزية التي يتم من خلالها معالجة المعلومات و تخزينها و إخراجها وجميع الأجهزة الملحقة بها.

أما **الكيان المعنوي Software** فيشمل البرامج المختلفة التي يتحقق من خلالها قيام الحاسب الآلي بوظائفه المختلفة بالإضافة إلى المعلومات المطلوب معالجتها[1] .

وإذا كانت جرائم الأموال من وجهة النظر التقليدية لا ترد إلا على أشياء مادية[2] ، فإن الأجهزة المادية للحسابات لا تحتاج إلى نصوص خاصة لحمايتها جزائيا إذ تشملها نصوص الجرائم التقليدية كونها أموال مادية بطبيعتها ،إلا أن الأمر يختلف بالنسبة للكيان المعنوي كون أن جرائم الاعتداء على الأموال تشترط أن يكون موضوعها شيئا ماديا، في حين أن طبيعة الكيان المعنوي ليست كذلك[3].

و لكن مع التطور ازدادت الأشياء المعنوية عددا و تفوق بعضها من حيث قيمته على الأشياء المادية، مما استدعى البحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الحق المالي حتى يمكن إسباغ صفة المال على الشيء المعنوي.

و من هذه الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسب الآلي، و التي تكون عادة مثبتة على دعامة أو حامل **Support** مثل الأقراص أو الشرائط الممغنطة من البلاستيك أو الورق المقوى أو أي مادة أخرى ، إلا أن البرنامج مستقل عن دعامته لا جدال في أنه شيء معنوي و بالتالي لا يصدق عليه وصف المال طبقا للتحديد التقليدي للأموال الذي يشترط أن يكون محله شيئا ماديا.

---

[1] - د . محمد فتحي عبد الهادي ، مقدمة في علم المعلومات ، مكتبة غريب القاهرة، سنة 1984، ص 217.

[2] - و لهذا كان تعريف المال بصدد جرائم الأموال بأنه " كل شيء مادي يصلح لأن يكون محلا لحق من الحقوق المالية " أنظر د . أحمد عبد الرزاق السنهوري، الوسيط في شرح القانون المدني حق الملكية ، الجزء الثامن دار إحياء التراث العربي بيروت، 1952 ص 09.

[3] - أمال قارة ، المرجع السابق ، ص 15 .

و عليه إذا سجل البرنامج أو نقش على دعامة فإن تلك الدعامة بما عليها من برامج تصلح لأن تكون محلا لجرائم الأموال على الرغم من أن الدعامة منفصلة عن البرنامج تعتبر ضئيلة القيمة إذا ما قيست بقيمة البرنامج، كما أن الاعتداء عليها ليس غاية في ذاته و إنما الباعث على ذلك هو البرنامج نفسه لا دعامته ، و مع ذلك لا تأثير لهذه البواعث في القانون الجنائي[1]، و من ثمة يعتبر الاعتداء على الدعامة في هذه الحالة قد وقع على شيء مادي، مما يصلح تكييفه حسب النشاط الإجرامي بإحدى جرائم الأموال التي يتطابق نموذجها مع هذا النشاط.

أما إذا وقع الاعتداء على البرنامج مستقلا عن دعامته فإن الأمر يختلف إذ يعتبر أنه وقع على شيء معنوي، هذا الشيء المعنوي لابد و أن تثبت له صفة المال أولا حتى يمكن البحث بعد ذلك في مدى إمكانية وقوع جرائم الأموال عليه.

و قد ثار جدل فقهي حول ما إذا كانت المعلومات صالحة لأن تكون محلا لجرائم الأموال أم لا ، و انقسم الفقه في هذا الشأن إلى اتجاهين .

إذ ذهب أصحاب الاتجاه الأول إلى اعتبار المعلومات صالحة لأن تكون محلا للاعتداء عليها طالما كانت هذه المعلومات تعكس الرأي الشخصي لصاحبها و لا تتوقف عند نطاق المعلومات العامة كون أن هذا النوع من المعلومات يعتبر معلومات مرتبطة بشخصية صاحبها ، فهو الذي فكر فيها، كما أنه من خصائصها القابلية للانتقال ، و هذا يعني أن هناك طرفا آخر يستقبل هذه المعلومات[2] ، و من هنا تنشأ علاقات فيما بينها و بين من يملكها فيكون له نقلها و إيداعها و حفظها و تأجيرها و بيعها.

و من أمثلة هذه المعلومات برامج الحاسب الآلي، إذ أن هذه البرامج ترتب حقوقا لصاحبها و تخول له إبرام عقود متعلقة بها مثل الإيجار و البيع و الحفظ، أو أي صورة أخرى من صور الاستغلال كون أنه من خصائصها القابلية للانتقال بالإضافة لقيمتها الاقتصادية، إذ تطرح في

1- د .علي عبد القادر القهوجي ,الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة و النشر بيروت ، سنة 1999، ص 7.

2 - Catala (Pierre) : Ebauche d'une théorie juridique de l'information 1984,p 87.

السوق للتداول مثلها في ذلك مثل أي سلعة، و لها سوق تجاري خاص بها يخضع لقوانين السوق الاقتصادية.

و لهذا السبب اعتبر الفقه الحديث أن المعيار المعتمد لاعتبار الشيء مالا يقوم على القيمة الاقتصادية للشيء بدلا من كيانه المادي ، و بالتالي حسب هذا الرأي فإن القانون الذي يرفض إسباغ صفة المال على شيء له قيمة اقتصادية هو بلا جدال قانون ينفصل تماما عن الواقع[1].

فما دامت البرامج في جوهرها معلومات معالجة بطريقة ما و لها قيمة اقتصادية فإنه يجب معاملتها على أنها مال[2] .

وما يؤكد هذا المعنى أن المشرع الحديث يعترف لصاحب هذه المعلومات بما يطلق عليه الحق في الملكية الفكرية، و لولا أن المعلومات مالا ما كان المشرع ينص على هذا الحق.

و إن كانت طبيعة هذه الملكية محل جدل فقهي[3]، فإنها على كل حال نوع من الملكية و لصاحبها الحق في احتكار استغلال هذا المال غير المادي أي المعلومات و التي تشمل برامج الحاسب الآلي.

في حين يفرق البعض الآخر من الفقهاء بين المعلومات و البيانات التي تمت معالجتها الكترونيا فيرون أن الأولى باعتبار أن عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها لها طبيعة غير مادية ، و من ثم لا سبيل إلى اختلاسها ، أما البيانات التي تمت معالجتها الكترونيا، فتتحدد في كيان مادي يتمثل في نبضات أو إشارات الكترونية ممغنطة يمكن تخزينها على وسائط معينة و نقلها و استغلالها و إعادة إنتاجها، فضلا عن إمكانية تقديرها كميا و قياسها فهي بذلك ليست شيئا معنويا في الحقوق و الآراء و الأفكار بل شيئا له وجود مادي في العالم الخارجي المحسوس.

---

[1] - عكس الفقه التقليدي استبعد المعلومات من طائفة الأموال على أساس أنها غير مادية ، أي أن عدم مادية المعلومات هو الذي أدى إلى عدم الاعتراف لها بصفة المال ، راجع Carbonnier : droit civil, P U E Paris 1973 T 3 les biens N 17 p 54

[2] - Carbonnier (M) droit civil P U E Paris 1973 T 3 les biens N° 17 -18 P Vivant à propos de bien informationnel J C P 1984 I doct 3132 . 54 et 55.

[3] - د . عبد الرشيد مأمون شديد ، الحق الأدبي للمؤلف النظرية العامة و تطبيقاتها ، دار النهضة القاهرة سنة 1978 ، ص 22.

و عليه فإنه وفقا لهذا الرأي فإن المعلومات إذا لم تعالج آليا في صورة نبضات إلكترونية عن طريق الحاسب لا تعتبر من قبيل الأموال الخاضعة للحماية الجنائية.

الشيء الذي يؤدي إلى القول أن **عملية المعالجة** هي التي تحول المعلومات من أموال معنوية إلى أموال مادية ، الأمر الذي يخضعها للنصوص التقليدية لجرائم الأموال ، و يأخذ نفس حكمها البيانات المخزونة سواء في برامج الحاسب أو في ذاكرته و بالتالي تأخذ برامج و بيانات الحاسب حكم الأموال عليه و بالتالي تتمتع بالحماية الجزائية المقررة لها، وهذا ما أكدته محكمة النقض الفرنسية في قضية **Antanioli**[1].

و في الأخير نخلص إلى القول أن اعتبار المعلومات مالا قابلا للتملك أو الاستغلال كما سبق أن وضحناه يزيل عقبة كبيرة تسمح بإضافة هذا النوع من الأموال إلى مجموعة الأموال التي يحميها القانون الجنائي .

و منه يمكن أن يكون هذا المال موضوع جرائم الاعتداء على الأموال و بالتالي يمكن إسباغ حماية النصوص التقليدية عليه، كون أن هذه النصوص جاءت عامة و لم تشترط أن تقع جرائم الأموال على منقول مادي.

و عليه يكون من المتصور أن تقع هذه الجرائم على مجال غير مادي طالما اعترف له بصفة المال و قابليته للتملك، و قد سايرت هذا الاتجاه محكمة النقض الفرنسية في العديد من أحكامها[2].

[1] – تتلخص وقائعها في قيام المدعو Antanioli و هو يعمل محاسب بإحدى المؤسسات- بإعادة جداول ورسوم نيابية توضح عمل المؤسسة، و ذلك من خلال بعض المستندات المحاسبة التي يحورها بمقتضى وظيفته، ثم قام بتسليمها إلى شخص آخر يقوم دراسات لإنشاء مؤسسة منافسة، وقد قضت محكمة الاستئناف بإدانته بجريمة السرقة لقيامه باغتصاب حيازة هذه المستندات، و قيامه باختلاس المعطيات التي تحتوى عليها هذه المستندات و التي تعد أموالا معنوية محكومة لرب العمل، و تسليمها إلى الغير، و لقد أبدت محكمة النقض ما ذهبت إليه محكمة الاستئناف، و رفضت الطعن الذي تقوم به المتهم، و الذي أسس على عدم اعتداء الحكم في استظهار للركن المادي لجريمة السرقة ، إلا بواقعة توصيل المعلومات التي وصفها الحكم بأنها أموال معنوية، دون استظهار الاختلاس المقتضي إلى تغيير حيازة شيء مادي، و هو ما لا تقوم جريمة السرقة بدونه، حيث قررت محكمة النقض أن الحكم المطعون فيه، قد بين جميع العناصر المكونة لجريمة السرقة المادية منها و المعنوية، للمزيد من التفاصيل أنظر د. نائلة محمد فريد قورة، المـــرجع السابق، ص 132-133.

[2] – من أحكامها في هذا الصدد حكمها القاضي بسرية المحتوى المعلوماتي للشرائط خلال المدة اللازمة لنسخ و إعادة إنتاج المعلومات إضرارا بالمطبعة المالكة لها ، أنظر د. علي عبد القادر القهوجي ، المرجع السابق ، ص 23 .

الفرع الثاني : مدى اعتبار المعلوماتية مالا بصدد جرائم الأموال

بعد أن خلصنا في الفرع السابق إلى اعتبار الفقه الراجح برامج الحاسب مالا ، كون أن المعلومات تعتبر شيئا منقولا مملوكا للغير بالرغم من كونها شيء غير مادي ,طرح إشكال مفاده مدى اعتبار البرامج استنادا إلى هذه الصفة تدخل تحت مفهوم الشيء الذي يصلح محلا لجرائم الأموال ، نتطرق للإجابة عن هذه الإشكالية فيما يلي :

أولا : مدى اعتبار البرنامج مالا بصدد جريمة السرقة

سنركز من خلال دراستنا لجريمة السرقة على الإشكالات المتعلقة بالسرقة في مجال المعلوماتية ، مما يستلزم الرجوع إلى أحكام جريمة السرقة التقليدية ومقارنتها بالاعتداءات في مجال المعلوماتية.

ففيما يخص المفهوم المادي لمحل السرقة ، ذهب جانب من الفقه إلى أن الأخذ بهذا المفهوم يؤدي لا محالةلإبعاد المعلومات من مجال تطبيق جريمة السرقة ، و اعتمد في تحليله على كون الأموال غير المادية هي أموال غير مجسدة ، و من ثم فإن المعلومة وحدها تكون غير قابلة للسرقة إذا كانت منفصلة عن سندها المادي(كتاب،ورق،قرص) .

غير أن القضاء الفرنسي تطور و أصبح يقر بسرقة المعلومات ، من خلال القرارين اللذين أصدرتهما محكمة النقض الفرنسية حال فصلها في قضيتي "بوركان **bourquin** " ولوقاباكس[1] **logabax** " اللذان أيدت فيهما محكمة النقض قرارها الصادر في

[1] – تتلخص وقائع القضية الأولى في قيام اثنين من العاملين بمطبقة Bourquin ، و من أجل إنشاء مؤسسة منافسة، ينسخ سبعة و أربعين قرصا ممغنطا تحتوى على معلومات بالغة الأهمية خاصة بعملاء المطبعة و ذلك داخل مؤسسة Bourquin و الاستعانة بمعداتها، كما قاموا بالاستلاء على سبعين قرصا ممغنطا من ناحية، و من جهة أخرى بسرقة المحتوى المعلوماتي لسبعة و أربعين قرصا، خلال الفترة اللازمة لإعادة إنتاجها و ذلك إضرارا بالمؤسسة المالكة لجميع هذه الأقراص، و لقد أيدت محكمة النقض ما ذهبت إليه محكمة الاستئناف من إدانة المهتمين من سرقة سبعين قرصا، و المحتوى المعلوماتي لسبعة و أربعين قرصا من جهة أخرى، كما رفضت الطعن المقدم من المهتمين مقررة أن قضاة الموضوع قد أثبتوا توفر كافة العناصر المكونة للجريمة، و يعد هذا الحكم على جانب كبير من الأهمية، من جهة يأتي هذا الحكم أكثر وضوحا من حيث تحديد المجال الذي تنصب عليه جريمة السرقة، ألآ و هو المعلومات في حد ذاتها، و من جهة أخرى فهو يتعرض لنسخ المعلومات المسجلة على الأقراص الممغنطة بصفة خاصة.

وتتلخص وقائع القضية الثانية في قيام مهندس يعمل بمؤسسة Logabax بنسخ مشدين على درجة كبيرة من السرية، يتعلقان بعمل المؤسسة، ثم قام بتقديم هذه الصور، فيما بعد، في دعوى ضد المؤسسة، و قدم المتهم للمحاكمة بتهمة السرقة، إلا أن محكمة أول درجة برأته من السرقة، ثم استئناف الحكم أمام محكمة الاستئناف Versailles و التي أبدت في حكمها بتاريخ 29 سبتمبر 1988 حكم محكمة أول درجة، حكم

1989/01/12 الذي قضى بإدانة شخصين من أجل سرقة أقراص ممغنطة وسرقة محتواها خلال الفترة الضرورية لنقل المعلومات إلى سند آخر[1].

وبهذا القرار يكون القضاء الفرنسي قد خلص إلى أن المعطيات المعلوماتية صالحة لأن تكون محل سرقة، تتحقق هذه السرقة بتحويل ما يحتويه قرص من معلومات إلى سند آخر و لو كان الاختلاس مؤقتا و لم يدم إلا الوقت اللازم لنقل ما يحتويه القرص إلى ذلك السند[2]، و يمكن التمييز في هذا الإطار بين :

أ- الاعتداءات الماسة بأشياء مادية[3] :يقصد بالأشياء المادية كل ما هو ملموس أو مجسد أو تابع أو حتى من أصل المنهاج المعلوماتي، و تتمثل هذه الأشياء أساسا في الأجهزة و المعدات و التوابع و الحوامل و الكوابل و الأسلاك بل حتى الجهاز الرئيسي ذاته.

فكلما طالت الاعتداءات كل أو بعض هذه الأشياء المادية التابعة للمناهج فلا إشكال ، لأن الجريمة تكون قائمة حسبما ما تقتضيه نصوص السرقة التي تنص على وجوب توفر الركن المادي المتمثل في اختلاس الشيء الذي يكون بداهة في ملك صاحبه ، لاسيما أن السرقة في هذا المستوى تكون منصبة على أشياء مادية ملموسة و مجسدة[4].

ب-**الاعتداءات الماسة بأشياء غير مادية[5]** : يوصف النموذج كما حددته قاعدة التجريم ، المحل المادي لسلوك الاختلاس و أنه منقول مملوك للغير .

محكمة أول درجة، و أسست حكمها على عدم تحقق أركان جريمة السرقة، و لقد رأت أن المتهم لم يختلس المستندات التي تحتوى على هذه المعلومات، بل أنها ظلت في حيازة المؤسسة و هو ما يجعل العناصر المكونة للسرقة غير متحققة، إلا أن محكمة النقض الفرنسية، كان لها رأي آخر، حيث رأت المحكمة أن المادة 389 من قانون العقوبات تنطبق على سلوك المتهم، باعتبار أن تصوير المستندات، لأغراض شخصية بغير علم المؤسسة المالكة لهذه المستندات، و ضد رغبتها، يشكل جريمة السرقة، فالجاني في رأي محكمة النقض الفرنسية، لم تكن له على هذه المستندات سوى اليد العارضة، فيكون بذلك قد استولى عليها أثناء المدة اللازمة لإعادة إنتاجها، لمزيد من التفاصيل أنظر د. نائلة محمد فريد قورة، المرجع السابق، ص 121-132.

[1]- د. أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول, المرجع السابق، ص259 .

[2]- د. أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول, المرجع السابق ، ص260 .

[3] - Fidemann (K) fraudes et delits d'affaire commis à l'aide d'ordinateurs électronique, Rev drpen et crim 1984 P 618.

4- أمال قارة ، المرجع السابق، ص 21.

5 - Rollant Reflexions sur le vol d'usage J C P 1 doctorat p 92.

و مقتضى قابلية محل الاختلاس للنقل من مكان إلى آخر هو أن يكون ذا طبيعة مادية ، و عليه لا يصلح محلا للاعتداء في جريمة السرقة كل ما لا يتمثل أو يتجسد على صورة أو كيان مادي ، و تطبيقا لذلك لا تصلح الأموال المعنوية كالأفكار و الآراء و الابتكارات و الحقوق الشخصية أو العينية أو المنافع أن تكون محلا للسرقة[1].

في حين أن الحقوق التي اتخذت مظهرا ماديا يتمثل في وثيقة أو محرر ، فإن هذه الأخيرة تكون عندئذ منقولات مادية يصح أن يرد عليها الاختلاس .

و على ضوء ذلك يمكن القول بأن الاستيلاء على البيانات المخزنة الكترونيا باختلاس أوعيتها و وسائطها المادية كالبطاقات المثقبة و الأشرطة و الأسطوانات و الأقراص الممغنطة لا يثير شبهة حول وقوعه تحت طائلة العقاب عن جريمة السرقة لأن لهذه الأوعية و الوسائط فضلا عن قيمتها الذاتية [2] لها كيان مادي ملموس و لهذا ذهب البغض إلى القول بأنه من الجائز أن تنصب السرقة على الاستعمال **vol d'usage** و من هذا القبيل استعمال المعلومات الموجودة في أسطوانة ممغنطة .

إلا أنه يثار التساؤل عما إذا كانت البيانات المعالجة الكترونيا غير المقترن اختلاسها باختلاس وسائطها أو أوعيتها المادية قابلة لأن تكون موضوعا لحق الملكية ، و في هذا الصدد من المتصور

---

1 – أنظر في هذا المعنى د. أحسن بوسقيعة ، **الوجيز في القانون الجزائي الخاص ،الجزء الأول**, المرجع السابق، ص256 ،257 ،263 .

2– إن قيمة هذه الأوعية في ذاتها تبدو ضئيلة إذا ما قورنت بقيمة المعلومات التي قد تحتويها و من الأمثلة القضائية التي تبدي ذلك جليا قضية Hancock U State بالولايات المتحدة الأمريكية، تتلخص وقائعها في قيام مبرمج بشركة تكساس للمعدات بنسخ 59 برنامج مملوك للشركة و تقدم بيعها لشركة منافسة مقابل 5 ملايين دولار ، و في دفاعه تمسك المتهم بأن قيمة البرامج التي نسخها لا تتعدى 35 دولار و هي قيمة الأوراق المستخدم لنسخها و كان هدفه من ذلك الاستفادة من التدحرج الذي يقيمه قانون عقوبات ولاية كاليفورنيا التي تعاقب تبعا لقيمة الشيء المسروق ، غير أن المحكمة استندت إلى تقرير الخبير الذي أكد أن هذه البرامج طبقا لما تنتجه من إمكانات لمستخدمها تساوي بتحفظ 2.5 مليون دولار و عليه رفضت دفاع المتهم و قررت أن قيمة الأشياء المسروقة هي قيمة البرامج في حد ذاتها و ليست قيمة الأوراق المستخدمة في نسخها و أدانت المتهم بجريمة السرقة ، لأكثر من التفاصيل أنظر د . سهير لطفي ، تقرير حول ندوة الجرائم الاقتصادية المستخدمة المنعقدة في 20- 01/04/21 بالقاهرة.

في بيئة المعالجة الالكترونية للبيانات الاستيلاء على المعلومات ذاتها دون أوعيتها المادية في ثلاث صور:

تتمثل الصورة الأولى في الالتقاط الذهني للبيانات ، ويتحقق هذا الالتقاط بالاختزان أو الحفظ الواعي أو العرضي للمعلومات في ذاكرة الإنسان إثر مطالعتها بالبصر إن كانت قد ظهرت على شاشة الحاسب في شكل مرئي، أو عن طريق سماعها بالأذن إن تمثلت في صورة صوتية صادرة من الأجهزة .

و في ضوء الراجح في الفقه المقارن ، فإنه و إن كان يمكن القول بأن الموجات أو الإشعاعات المنبعثة من الأجهزة المعلوماتية حال تشغيلها تصلح أن تكون محلا للسرقة بسبب تجسيدها في صورة مادية كهرومغناطيسية، فإن التقاطها لا يتحقق به معنى النزع أو سلب الحيازة ، فبالتالي لا تقع جريمة السرقة لانتفاء أحد عناصر ركنها المادي، و الأمر كذلك أيضا بالنسبة لالتقاط البيانات المعالجة الكترونيا أثناء تنقلها إرسالا و استقبالا فيما بين الأجهزة المعلوماتية[1] .

أما الصورة الثانية تتمثل في النسخ غير المشروع للبيانات المخزنة الكترونيا، إذ تخزن البيانات المعالجة الكترونيا على شكل نبضات كهربائية في دوائر الكترونية مجمعة أو على أشرطة و أسطوانات ممغنطة، و في كلتا الحالتين يمكن نسخها على دعامات أخرى وبسط أحكام السرقة على عملية الاستنساخ هذه.

وقد قضت محكمة النقض الفرنسية في هذا الصدد بإدانة متهم بالسرقة ليس لقيامه بالتصوير و إنما لاستيلائه على المستند الأصلي أثناء المدة اللازمة لاستنساخه و بذلك حافظت على شرط توافر الصفة المادية في محل السرقة[2] .

في حين أن الصورة الثالثة تتمثل في الالتقاط الهوائي للبيانات المعالجة أو المنقولة الكترونيا، فكما هو معروف فإن الحاسبات الآلية و كوابلها و دائرتها الكهربائية و ما يتصل بها

1- د .علي راشد ، القانون الجنائي أصول النظرية العامة ، القاهرة مكتبة سيد عبد الله وهبة سنة 1970 ، ص 307.

2 - أنظرقضيتي Bourquin وLogabax ,ص56من المذكرة .

من توابع تصدر أثناء تشغيلها إشعاعات كهرومغناطيسية يمكن التقاطها و ترجمتها إلى بيانات مرئية على شاشة تلفزيونية ، و من ثمة هناك إمكانية لاعتراض و التقاط البيانات أثناء نقلها بالموجات القصيرة من نهاية طرفية إلى نهاية أخرى.

و قد استقر الفقه و القضاء في تفسير نص المادة **350 من قانون العقوبات الجزائري** الذي ينص أن "كل من اختلس شيئا غير مملوك له يعد سارقا"، على أن فعل الاختلاس يجب أن يرد على شيء مادي ملموس ، في حين أن المشرع ذكر كلمة شيء دون قيد و دون أن يصفه بالمادي أو المجسم.

و بالتالي فإن عدم تحديد طبيعة الشيء محل السرقة ، هو الذي دفعب البعض إلى القول بإمكانية اختلاس التيار الكهربائي على الرغم من أنه ليست له طبيعة مادية ، و مبدأ تجريم الاستيلاء على الطاقة يطبق على كل قوة أو طاقة يمكن إخضاعها لسيطرة الإنسان و يكون بوسعه أن يوجهها على النحو الذي يحقق منفعته[1] .

و نفس الشيء يدفعنا للتساؤل حول مدى اعتبار الأفكار و المعلومات و بالتالي برامج الحاسب الآلي طاقة ذهنية ، كونها أشياء تقبل التملك و الحيازة من خلال الدعامة التي توجد عليها ، و لا تنقل إلا بموافقة حائزها عن طريق كلمة السر و هي على هذا النحو و على الرغم من أنها شيء غير مادي تصلح لأن تكون محلا لجريمة السرقة و لا يمثل الأخذ بهذا الاتجاه خروجا عن مبدأ الشرعية ، كون أن نص جريمة السرقة يقبل هذا التفسير لأنه:

- لا تحدد طبيعة الشيء محل الجريمة مادي أم معنوي.
- أن الأشياء المعنوية يصدق عليها وصف المال لقيمته الاقتصادية .

و عليه يمكن للقاضي الجزائي تطبيق أحكام السرقة على أموال الإعلام الآلي ، و إن كان من الأفضل أن ينص التشريع الجزائري صراحة على غرار بعض التشريعات المقارنة على اعتبار المعلومات و المعطيات أحد عناصر الذمة المالية ، و يجرم الاعتداء الذي يقع عليها ، كما اتجهت

1 ـو نحن نرى أن سبب تجريم سرقة الطاقة و الكهرباء هو المشرع نفسه من خلال نص المادة 350 الفقرة التانية من قانون العقوبات.

تشريعات أخرى إلى إعطاء مفهوم موسع للمال، حيث يضم المعلومات المعالجة و عرفته " كل شيء له قيمة مالية ، و يدخل فيه تبعا لذلك الأشياء المعنوية و المعلومات و المعطيات التي تمت معالجتها آليا" ، و أقرت بذلك صلاحيتها لأن تكون محلا لجريمة السرقة[1] .

ثانيا : مدى اعتبار المعلوماتية مالا بصدد جرائم النصب و خيانة الأمانة و تحطيم ملك الغير.

أ- **مدى اعتبار المعلوماتية مالا بصدد جرائم النصب** : اختلف الفقه وانقسم إلى اتجاهين حول مسألة مدى صلاحية اعتبار البرامج والبيانات إذا كانت مستقلة عن الدعامة المادية محلا لجريمة النصب .

فذهب أنصار الاتجاه الأول إلى عدم صلاحية البرامج لأن تكون محلا لجريمة النصب وذلك لعدم وجود نشاط مادي يتم به التسليم والاستلام ، و أنه حتى لو حصل فإنه لايترتب عنه حرمان المجني عليه من حيازة هذه البرامج وهو مالا يتفق وطبيعة النشاط الإجرامي لجريمة النصب[2] .

أما أنصار الاتجاه الثاني ذهبوا إلى اعتبار البرامج والبيانات صالحة لأن تكون موضوعا لجريمة النصب وذلك لكون النص القانوني لجريمة النصب يعطي أمثلة للأشياء التي تصلح محلا لجريمة النصب[3].

فمن خلال استقراء نص المادة **372 من قانون العقوبات** التي تنص على أنه " كل من توصل إلى استلام أوتلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبرام التزامات أو الحصول على أي منها أو شرع في ذلك و كان ذلك بالاحتيال

1 – أمال قارة ، المرجع السابق ، ص 30.

2– د.علي عبد القادر القهوجي, المرجع السابق, ص31.

3– أمال قارة ، المرجع السابق ، ص31

...." ، نستخلص أنه لا يوجد ما يحول دون وقوع البرامج و البيانات تحت طائلة النصب باعتبارها أموالا أو منقولات.

و لذلك أصبح من المتصور أن يقوم أحد الأشخاص بالتلاعب في هذه البيانات و يحولها كلها أو بعضها لصالحه باستخدام طرق احتيالية أو اتخاذ اسم أو صفة غير صحيحة .

ب- **مدى اعتبار المعلوماتية مالا بصدد جريمة خيانة الأمانة :** إن الطبيعة غير المادية للقيم في محل الجريمة المعلوماتية تثير بعض المشاكل القانونية لكون خيانة الأمانة ترد على منقول مادي ذا قيمة مالية [1] ، و مع ذلك فإن بعض هذه القيم مثل المعلومات أو المعطيات أو البرامج تصلح أن تكون محلا لخيانة الأمانة بصفتها بضائع، إذ تنص المادة: **376 من قانون العقوبات** " كل من اختلس أو بدد بسوء نية أوراق تجارية أو نقودا أو **بضائع** أو أوراق مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو إبراء...." ؛ و منه المعلومات أو المعطيات أو البرامج تصلح لأن تكون موضوعا لخيانة الأمانة بصفتها بضائع ، كون أن لها قيمة ذاتية يمكن تقدير قيمتها فيمكن تطبيق مفهوم البضاعة عليها، و هو ما أخذ به القضاء الفرنسي[2].

ج- مدى اعتبار المعلوماتية مالا بصدد جريمة التحطيم العمدي لملك الغير: تعتبر البرامج و البيانات وفقا للرأي الراجح من قبيل الأموال التي يجب أن تكون مشمولة بالحماية الجزائية، و من المتصور أن تكون هذه البرامج و البيانات محل جريمة الإتلاف ، مما ينتج عنه خسائر فادحة لا يستهان بها على الإطلاق ، فمن المتصور كذلك أن يتم محو أو إتلاف هذه البرامج و البيانات إما بصورة كلية أو جزئية باستخدام وسائل فنية تتفق و طبيعتها.

وبالرجوع إلى التشريع الجزائري نجد أن الاعتداء على الكيان غير المادي للحاسوب يمكن إخضاعه إلى نص المادة: **412 قانون العقوبات الجزائري** و التي حددت الأشياء الخاضعة

[1] – أنظر في هذا المعنى د.أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول, المرجع السابق ، ص 347 .

[2]– د . عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية , دار الثقافة للطباعة والنشر ، ص 179.

للإتلاف إذ جاء فيها أنه " كل من أتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة و ذلك بواسطة مواد من شأنها الإتلاف أو بأية وسيلة أخرى ..." ، و بالتالي فإن المكونات المادية للحاسوب يمكن أن تخضع لهذا النص التجريمي.

و يستخلص مما سبق أن صلاحية البرامج لأن تكون محلا لجرائم الأموال أمر يمكن استخلاصه من النصوص استنتاجا من عموميتها و من إمكانية إسباغ صفة المال على المعلومات ، إلا أن جانبا من الفقه ما يزال يرى عدم صلاحية البرامج كمحل لهذه الجرائم ، و في رأينا لن يحسم هذا الخلاف إلا بتدخل المشرع للنص صراحة على طبيعة الأشياء التي تكون محلا لهذه الجرائم سواء كانت مادية أو معنوية ، أو بإعطاء مفهوم موسع للمال حيث يضم المعلومات كأن يعرفه بأنه كل شيء له قيمة مالية ، و يدخل فيه تبعا لذلك الأشياء المعنوية و بذلك تقر صلاحيتها لأن تكون محلا لجرائم الأموال.

المطلب الثاني : مدى خضوع المعلوماتية للنشاط الإجرامي لجرائم الأموال

إذا كان الكيان المادي للمعلوماتية يخضع للنشاط الإجرامي لجرائم الأموال دون أي إشكال فإن خضوع برامج الحاسب للنشاط الإجرامي المكون للركن المادي لجرائم الأموال يطرح إشكال ، لذا سنحاول دراسة مدى إمكانية خضوع برامج الحاسب للنشاط الإجرامي المكون للركن المادي لجرائم الأموال من خلال الفرعين المواليين:

الفرع الأول : مدى خضوع المعلوماتية للنشاط الإجرامي في جريمة السرقة

فعل الاختلاس في جريمة السرقة هو الاستيلاء على حيازة الشيء دون رضا مالكه أو حائزه[1] السابق ، و يتحقق هذا الاستيلاء إما بنزع الشيء من مكانه و إما بالاستيلاء عليه بعد سبق التسليم بناءا على اليد العارضة. و يفترض الاستيلاء بهذا المعنى أن المالك أو الحائز الشرعي للشيء يفقد حيازته و سيطرته على هذا الشيء ، أي أن الاستيلاء ينتج عنه خروج الشيء المستولى عليه من ذمة و دخوله في ذمة أخرى[2] ، و بمعنى آخر يعد الاختلاس إفراغ ذمة و إشغال ذمة أخرى بحيث لا يوجد مجال للتزاحم بين ذمتين في الاستيلاء على الشيء[3].

و بإسقاط هذا المعنى للاختلاس على برامج الحاسب الآلي أو المعلومات المعالجة بصفة عامة نجد أنه يصطدم بعدة عقبات [4] ، أدت إلى انقسام الفقه إلى رأيين فمنهم من قال بصلاحية وقوع الاختلاس على المعلومات مباشرة، و منهم من رفض ذلك معتبرا أن هذا الفعل وقع على الأصل الذي تم تصويره أو على الآلة التي قامت بالتصوير[5].

و بالمقابل فإن المشرع الجزائري لم يجرم سرقة الاستعمال ، و عليه فإن المخرج الوحيد لتجريم نسخ صور للبرامج أو المعلومات لا يكون إلا بالتدخل الصريح من المشرع ، و الجريمة التي تقع في هذه الحالة ترتبط بوظيفة الحاسب الآلي فهذا يؤدي خدمة، و من هنا الأفضل النص على تجريم الاعتداء على هذه الخدمة و بهذا نتجنب الجدل حول سرقة المعلومات حيث أنه بالنص على

1 – د.أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول, المرجع السابق ، ص 247 .

2 – أنظر في هذا المعنى ، د.أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول, المرجع السابق ، ص 248 .

3 – د . علي عبد القادر القهوجي ، المرجع السابق ، ص 95.

4 – و يمكن حصر ذلك في ثلاث عقبات وهي :

أ– عدم خروج البرامج والمعطيات من سيطرة حائزها رغم دخولها في حيازة مختلسها .

ب– إمكانية وقوع الاختلاس على البرامج والمعطيات في حالة تجسدها في شكل سمعي أو مرئي أو عن طريق الالتقاط الذهني لها .

ج– إذا كانت المعلومات التي تحويها البرامج من طبيعة غير المادية فكيف يمكن تصور ورود فعل الاختلاس الذي هو من طبيعة مادية على شيء معنوي .

5 – لأكثر من التفاصيل أنظر أمال قارة, المرجع السابق,ص36-45.

سرقة الخدمة **vol de service** [1] أو سرقة استعمال الأصل نحقق حماية مباشرة للبرامج و المعلومات.

الفرع الثاني : مدى خضوع المعلوماتية للنشاط الإجرامي في جرائم النصب و خيانة الأمانة و تحطيم ملك الغير

إذا كان خضوع الكيان المادي للمعلوماتية للنشاط الإجرامي لجرائم النصب و خيانة الأمانة و تحطم ملك الغير لا يثير أي إشكال فإن السؤال يطرح بالنسبة للكيان المنطقي (البرامج) ، هذا ما سنحاول التطرق له فيما يأتي .

أولا : مدى خضوع البرامج للنشاط الإجرامي في جريمة النصب ، يتمثل النشاط الإجرامي في جريمة النصب في الاستيلاء على الحيازة الكاملة لمال مملوك للغير عن طريق إحدى وسائل الاحتيال المحددة قانونا على سبيل الحصر.

فإذا لجأ الجاني إلى إحدى الطرق الاحتيالية، و حمل المجني عليه على تسليم دعامة مادية مثبتا عليها أحد البرامج التي تخصه ثم استولى الجاني عليها يتحقق بذلك النشاط الإجرامي في جريمة النصب و تقع الجريمة.

إلا أن الإشكال الذي يطرح نفسه في هذا الصدد هو هل من المتصور أن تقع هذه الجريمة على المعلومات التي يتكون منها البرنامج فقط؟ و هل يتصور أن يتحقق النشاط الإجرامي لجريمة النصب من خلال الطرق الاحتيالية التي يلجأ إليها الجاني، و التي يترتب عليها وقوع المجني عليه في غلط يدفعه إلى أن ينقل إليه شفهيا عن طريق القول محتويات برنامجه الذي يلتقطه الجاني و يحفظ في ذاكرته ؟ و بعبارة أخرى هل النقل من خلال القول يعادل التسليم بناءا على الغلط ؟ و هل الالتقاط أو سماع الجاني للمعلومات يعادل الاستيلاء[2] ؟

1 – لمعلومات أكثر أنظر د.أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ،الجزء الأول ,المرجع السابق ، ص 261 .

2 – د . علي عبد القادر القهوجي ، المرجع السابق ، ص 105 – 106.

والواقع أن مسألة إمكانية الاحتيال على نظام الحاسب و إيقاعه في غلط قد اختلف بشأنها الفقه و التشريع.

فذهب اتجاه من الفقه إلى عدم إمكانية وقوع فعل الاحتيال على الحاسب و إيقاعه في غلط إذ لابد لتتوافر هذه الجريمة أن يكون الجاني و المجني عليه أشخاصا طبيعية يتحقق بواسطتهما التسليم و الاستلام ؛ و بالتالي فهو متصور إذا تم خداع الشخص المكلف بمراقبة البيانات أو مراجعتها[1] .

و على العكس من ذلك يرى اتجاه آخر إمكانية وقوع فعل الاحتيال على الحاسب ، و من المتصور إيقاعه في غلط و هو ما تبنته الدول الأنجلوساكسونية و جانب من الفقه الفرنسي، و استندوا في ذلك إلى كون أن النصوص المتعلقة بجريمة النصب متسمة بالعموم و الشمول و من ثمة يمكن الاستناد على هذه السمة لمد تطبيق أحكام تلك النصوص على فعل الاحتيال الواقع على الحاسب .

أما عن وجوب حصول الاستيلاء على المال المنقول المملوك للغير بإحدى طرق الاحتيال فإن الاستيلاء على مال الغير هو النتيجة اللازمة قانونا لاكتمال تكوين الواقعة في الجريمة ؛ إلا أن تطبيق فكرة الاستيلاء في المجال المعلوماتي تثير مسألتين تتعلق إحداها بالنقود البنكية في حين أن الثانية تتعلق ببطاقات الائتمان.

أ- **النقود البنكية** : تقتضي جريمة النصب أن يقوم الجاني بحيازة المال محل الجريمة حيازة مادية، ، إلا أنه في حالة ما إذا كان محل تحقق الاستيلاء يتمثل فيما يعرف بالنقود الكتابية أو البنكية عن طريق إجراء ما يعرف بالقيد الكتابي بالتلاعب في البرامج و البيانات التي يترتب عليه تحويل بعض أو كل أرصدة أصحابها الشرعيين أو فوائدها على حساب المتلاعب، فبالرغم من

1 – د .هشام فريد رستم ، المرجع السابق ، ص 123.

عدم تحقق عنصر الحيازة في هذه الحالة إلا أن الفقه الراجح ذهب إلى اعتبار هذا التصرف من قبيل الاستيلاء المادي المتطلب في جريمة النصب[1] متى اعترف لهذه النقود بصفة المال.

ب- **بطاقات الائتمان** : إن استخدام هذه البطاقة للحصول على أموال عن الجهة المصدرة لها بطريق الغش قد يقع من طرف المالك الشرعي لهذه البطاقة أو من الغير في حالة عثوره عليها أو سرقتها من مالكها الشرعي و في هذا الصدد نفرق بين حالتين :

- **حالة استعمال البطاقة من مالكها الشرعي** ، و هذه الحالة بدورها تحتمل ثلاث فرضيات نتناولها كالآتي :

1- في حالة استعمال المالك بطاقة الائتمان لسحب النقود من منافذ السحب الآلي بما يتجاوز رصيده، في حال كون هذه البطاقة صحيحة فهناك من اعتبر هذا السلوك سرقة، وهناك من اعتبره نصبا، إلا أن محكمة النقض الفرنسية اعتبرته إخلال بالتزام تعاقدي.[2]

2- في حالة استعمال المالك البطاقة لسحب النقود بالرغم من إلغائها من قبل الجهة المصدرة لها، اعتبر البعض هذا السلوك جريمة نصب على أساس أن مجرد تقديم البطاقة يهدف إلى الإقناع بوجود ائتمان وهمي لا وجود له في الواقع خاصة وأن إلغاء البطاقة يخلع عنها قيمتها كأداة ائتمان.[3]

3- في حالة استعمال المالك البطاقة لسحب النقود بالرغم من انتهاء مدة صلاحيتها، اعتبر بعض الفقه هذا السلوك أنه جريمة خيانة الأمانة ، على أساس أن البطاقة تعد محرر يتم تسليمه للعميل على سبيل عارية الاستعمال.[4]

- **حالة استعمال بطاقة الائتمان من قبل الغير** ، و نميز في هذا الصدد بين فرضيتين :

1- محكمة النقض الفرنسية اعتبرت أن الإبراء من دفع الأجرة يقوم مقام التسليم على الرغم من أن الجاني لم يستلم أي شيء مادي، عن أمال قارة، المرجع السابق، ص 48-50.

2 – د . محمد سامي الشوا ، المرجع السابق ، ص 105.

3 – د. جميل عبد الباقي صغير، جرائم التكنولوجيا الحديثة ، دار النهضة العربية ، ص 114.

4 – د .محمد سامي الشوا ، المرجع السابق ، ص108 .

1- عند سرقة البطاقة أو العثور عليها و إجراء عملية سحب للنقود بموجبها اعتبر هذا الفعل جريمة نصب على أساس اتخاذ الجاني اسما كاذبا , بما يسوغ القول معه أنه قد استخدم وسيلة احتيالية يريد من وراءها إقناع المجني عليه بوجود ائتمان .

2- عند تزوير بطاقة الائتمان، يرى جانب من الفقه أنه في حالة قيام الغير بتزوير بطاقة الائتمان وقام باستغلالها في سحب مبالغ من أجهزة السحب الآلي للنقود يعتبر ذلك جريمة سرقة باستخدام مفتاح مصطنع ، كما استبعد بعض الفقه تطبيق جريمة التزوير على أساس أن بطاقة الائتمان لا تعتبر محررا كتابيا ، و قد اعتبر القضاء أن هذا السلوك لا يشكل جريمة النصب باعتبار أن هذه الجريمة تعترض علاقة مباشرة بين شخصين طبيعيين [1].

ثانيا : مدى خضوع البرامج للنشاط الإجرامي في جريمة خيانة الأمانة

تثور إشكالية في هذا الصدد مفادها مدى خضوع أموال الإعلام الآلي لأفعال الاختلاس والتبديد و الاستعمال المكونة للركن المادي لجريمة خيانة الأمانة كالآتي :

أ- **الاختلاس** : ومثال ذلك في المجال المعلوماتي الحالة التي يمتنع فيها العميل ردّ بطاقة الائتمان إلى البنك في حالة طلبها من جانب هذا الأخير سواء لانتهاء مدة صلاحيتها أو لإلغائها أثناء مدة صلاحيتها ، كون أن البنك يعتبر مالك البطاقة ، وأنها موجودة لدى العميل على سبيل عارية الاستعمال فقط [2] .

ب- **التبديد** : وهو تصرف الأمين في المال الذي أؤتمن عليه شرط أن يؤدي هذا التصرف إلى خروج المال من حيازته ، وقد اختلف الفقه حول مدى اعتبار الإتلاف تبديدا ، و ذهب أغلب الفقه إلى اعتبار الإتلاف تبديدا لأنه مظهر من مظاهر التصرف في المال الذي لا يثبت إلا للمالك وهو يتنافى تماما مع واجب الرد الذي يلتزم به الأمين[3].

1 – أمال قارة ، المرجع السابق ، ص 52.

2 – د . جميل عبد الباقي صغير ، المرجع السابق ، ص 129.

3 – أنظر في هذا المعنى د . أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، الجزء الأول ، المرجع السابق ، ص346 .

ج- **الاستعمال** : وهو استخدام الأمين المال استخداما يستنزف قيمته كلها أو بعضها مع بقاء مادته على حالها، فلا ينصب العقاب في هذا الصدد على مجرد إساءة استعمال الشيء ، وإنما ينصب على الاستعمال الذي يفترض أن يصدر إلا عن مالك الشيء[1].

وفيما يخص الاستخدام التعسفي لبطاقات الائتمان يرى الفقه الراجح أن هذا الفعل لا يشكل خيانة أمانة لأن العميل لم يبدد بطاقة الائتمان الممغنطة المسلمة إليه من البنك على سبيل عارية الاستعمال ولكنه استعملها فقط في سحب مبالغ تتجاوز رصيده في البنك.

وقد قضت محكمة استئناف هولندا ثبوت جريمة خيانة الأمانة في حق محلل للبرامج بإحدى الشركات كانت طبيعة عمله التردد على عملاء الشركة لصيانة برامجهم وبحوزته أقراص ممغنطة تخص الشركة تحتوي برامج وبيانات معينة لازمة لعمليات الصيانة، فقام بنسخها على أقراص تخصه بغرض إنشاء مشروع خاص به.[2]

ثالثا : مدى خضوع البرامج للنشاط الإجرامي في جريمة تحطيم ملك الغير[3]

لقد عرف الفقه الإتلاف بأنه التأثير على مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال بأي وسيلة كانت ، بشرط ألا تكون هذه الوسيلة مما يخضع لنص عقابي آخر[4], وذلك لكون المشرع لم يقيد النشاط الإجرامي في هذه الجريمة ولم يجرم نتيجة واحدة وإنما جرم فعل التخريب والإتلاف وعدم صلاحية الاستعمال ، وذلك بهدف حماية القيمة الاقتصادية للشيء .

1 – د. جميل عبد الباقي الصغير ، جرائم التكنولوجيا الحديثة , دار النهضة العربية ,ص 108.

2 – أمال قارة ، المرجع السابق ، ص 58.

3 – د . عبد القادر القهوجي ، المرجع السابق ، ص 119 .

4 – أمال قارة ، المرجع السابق ، ص 58.

وبالتالي يكفي لقيام هذه الجريمة الإنقاص من القيمة الاقتصادية لمادة الشيء بجعله غير صالح للاستعمال أوالتقليل من قوته في المبادلة التجارية [1] .

و مما سبق يتبين لنا بأن البرامج والمعلومات بالرغم من كونها شيئا معنويا إلا أنه وفقا للفقه الراجح يصدق عليها وصف المال لأن لها قيمة اقتصادية وتجارية,إلا أنه و على الرغم من أن النصوص التقليدية لجرائم الأموال المقررة في قانون العقوبات الجزائري لم تشترط أن يكون المال موضوع الجريمة ذو طبيعة مادية ، إلا أن النشاط الإجرامي لهذه الجرائم لا يتلاءم مع طبيعة المال المعلوماتي كما سبق تبيانه .

و مع ذلك لتفادي إفلات أفعال الاعتداء على المال المعلوماتي من العقاب على القاضي الجزائي أن يجتهد لإخضاع هذه الاعتداءات للنصوص التقليدية في بعض الحالات الممكنة والتي سبق بيانها ، دون المساس بمبدأ الشرعية و ذلك في انتظار تدخل تشريعي صريح لمحاولة إضفاء صفة المال على البرامج والمعلومات المعالجة آليا على غرار بعض التشريعات الحديثة.

المبحث الثاني: الحماية الجزائية المعلوماتية من خلال نصوص الملكية الفكرية

نظرا لنسبية الحماية الجزائية المقررة للمعلوماتية من خلال النصوص التقليدية لجرائم الأموال نتيجة للطبيعة المميزة للمال المعلوماتي كما سبق التطرق له في المبحث السابق ، و نظرا للحاجة الملحة و الضرورية لحماية برامج الحاسب الآلي في الوسط القانوني ، و نظرا للتوجه الفعلي لرجال القانون لوضع الأطر القانونية لهذه الحماية ، أدى كل ذلك إلى إثارة جدل فقهي وقضائي حول الحماية المناسبة لبرامج الحاسب الآلي، و استقر مؤخرا الفقه القانوني في الدول التي ترعرعت فيها برامج الحاسب الآلي على إخضاعها لقوانين الملكية الفكرية[2].

1 – جميل عبد الباقي الصغير ، المرجع السابق ، ص 156.

2 – أمال قارة ، المرجع السابق ، ص63.

وتجدر الإشارة إلى أن أحكام قانون براءة الاختراع يمكنها أن تطبق على المكونات المادية للحاسب الآلي متى توافرت فيها الشروط التي يتطلبها هذا القانون [1]، عكس المكونات غير المادية التي استبعدها المشرع الجزائري صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا لنص المادة 07 من الأمر 07/03 المتضمن براءة الاختراع " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب" .

ونظرا لاستبعاد نظام براءات الاختراع حماية البرامج ، و بالإضافة لصعوبة استحداث تشريع خاص بالبرامج تبنى المشرع الجزائري نظام الحماية وفقا لقانون حقوق المؤلف والحقوق المجاورة وهو ما سارت عليه غالبية التشريعات والاتفاقيات الدولية .

وعليه سنتطرق لأحكام حماية المعلوماتية وفقا لنصوص الملكية الأدبية والفنية من خلال مطلبين سنتطرق في أولهما إلى مدى اعتبار البرامج موضوع من موضوعات حق المؤلف لنصل في المطلب الثاني إلى تحليل فكرة مدى إمكانية حماية المعلوماتية وفقا لنصوص جرائم التقليد.

المطلب الأول : مدى اعتبار البرنامج موضوع من موضوعات حق المؤلف

لقد اختلف الفقه والتشريع في هذا الصدد بين مؤيد ومعارض لاعتبار البرامج كمصنفات خاضعة للحماية المقررة في قانون الملكية الأدبية والفنية وعليه سنفصل ذلك فيما يلي :

الفرع الأول : موقف الفقه من اعتبار البرنامج من مواضيع حق المؤلف

تباينت مواقف الفقهاء فيما يخص مدى اعتبار البرنامج مصنفا فكريا، لاختلاف نظرة كل واحد من الفقهاء إلى مفهوم البرنامج كالآتي :

1 – تنص المادة الثالثة من الأمر 03-07 المؤرخ في 19-07-2003 المتضمن براءة الاختراع أنه "يمكن أن تقع تحت حماية براءة الاختراع الاختراعات الجديدة الناتجة عن نشاط اختراعي والقابلة للتطبيق صناعيا " ، ومن ثم يتبين لنا حتى تضفى الحماية عن طريق براءة الاختراع يجب توفر الشروط الآتية:الابتكار، الجدة , القابلية للتطبيق الصناعي , و أخيرا المشروعية .

أولا : الرأي المؤيد لاعتبار البرنامج مصنفا فكريا[1]**:** ساد هذا الاتجاه في السنوات القليلة الماضية، و ذهب أنصاره إلى أن برامج الحاسوب في حقيقتها طرق للتعبير عن الأفكار ، فالبرامج تتناول أفكارا معينة مبتكرة أو متداولة، ويعبر عنها وفقا لطريقة أصيلة باستخدام التكنولوجيا الحديثة .

و منه يعد البرنامج كتابة بلغة البرمجة التي تعد من قبل الإنسان في صورة أولية ثم يتم تحويلها بعد ذلك إلى لغة الآلة بالصورة المنقوشة التي تستطيع الآلة قراءتها ، ومن ثم إخراجها إلى المستعمل للاستفادة منها.

ثانيا: الرأي المعارض لاعتبار البرنامج مصنفا فكريا : يذهب أنصار هذا الفريق إلى التشكيك في خضوع المكونات غير المادية للحاسب أو الكيان المنطقي للحماية من خلال النصوص المقررة لحماية حق المؤلف نظرا لبعض الصعوبات التي تتمثل أساسا في أن إضفاء أحكام قانون المؤلف على المكونات غير المادية للحاسب سيكون بلا فائدة باعتبار أنه يمكن لأي شخص يتمتع بقدر معقول من الخبرة في مجال تقنية المعلومات من أن يحدث ولو مجرد تعديل شكلي بسيط على الكيان المنطقي ، وبالتالي يحق له أن يطلب إضفاء الحماية القانونية له باعتباره الأب الشرعي للابتكار .

الفرع الثاني: موقف التشريع من اعتبار البرنامج من مواضيع حق المؤلف

إن الاتجاه الذي ساد بصدد حماية برامج الحاسوب هو إخضاعها إلى قوانين حماية حق المؤلف، وقد اتخذ هذا الاتجاه عدة مسارات في كيفية إخضاع البرامج بمختلف صورها لحقوق المؤلف[2].

1 – د. أحمد السمدان ، النظام القانوني لحماية برامج الكمبيوتر ، مجلة الحقوق ، الكويت ، العدد4 ، سنة 1987 ، ص 11-51 .

2 – د. محمد حسام لطفي ، النظام القانوني لحماية الحقوق الذهنية في مصر، بحث منشور في كتاب ندوة حقوق المؤلفات الفكرية في مصر ، ص 6 - 7.

لم ينص المشرع الجزائري صراحة قبل تعديل قانون حق المؤلف و الحقوق المجاورة سنة 2003 على حماية البرامج المعلوماتية في إطار حق المؤلف لكن رغم عدم التنصيص على ذلك ، ذهب بعض المختصين إلى إمكانية هذه الحماية بدليل الصياغة المرنة **للمادة الثانية** من **الأمر 14/73** و **المادة السابعة** من **الأمر 16/96** عند ذكرهما المصنفات المشمولة بالحماية ،إذ تفيدان بأن الحماية تشمل حماية المصنفات الجديدة التي لم تكن موجودة وقت صدور هذه النصوص .

إلا أنه بعد صدور تعديل **05/03** المؤرخ في **2003.07.19** المتعلق بحقوق المؤلف و الحقوق المجاورة تبنى المشرع الجزائري صراحة الاتجاه السائد القائل بحماية مصنفات الإعلام الآلي عن طريق قانون حقوق المؤلف .

و من خلال استقراء **الأمر 10/97 المعدل والمتمم بالأمر 05/03 المتعلق بحق المؤلف والحقوق المجاورة** نستخلص ما يلي :

- أنه وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصيلة بموجب المادة **04** من الأمر **10/97** والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي والتي تمكن من القيام بنشاط علمي أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم باندفاعات إلكترونية بالحاسوب، أما قواعد البيانات فهي عبارة عن مجموعة المصنفات والأساليب والقواعد كما يمكن أن تشمل الوثائق المتعلقة بسير ومعالجة المعطيات بموجب المادة **05** من الأمر **10/97**.[1]

1 – أمال قارة ، المرجع السابق ، ص 78.

- أن مدة الحماية تحدد من **25** سنة إلى **50** سنة بعد وفاة المبدع تماشيا مع **اتفاقية بارن BERNE** التي حددت كمدة دنيا للحماية **50** سنة ، وبالتالي هذه المدة تشمل حتى مصنفات الإعلام الآلي[1] طبقا للمادة **58 من الأمر 05/03** .
- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية بموجب أحكام المادة **153** من الأمر **05/03** و تقابلها المادة **151** من الأمر **10/97**[2].

- وتجدر الإشارة إلى أن **المادة الخامسة** من الأمر **05/03** قد عدلت تسمية مجموعات المعلومات البسيطة التي كانت واردة في المادة الخامسة من الأمر **10/97** وعوضتها بمصطلح قاعدة البيانات و اعتبرتها مصنفات أدبية مشتقة.
- اعتمد المشرع الجزائري فيما يخص نطاق حماية مصنفات الجزائريين المعيار الشخصي إذ نص أن الحماية تشمل مصنفات الجزائريين سواء نشرت في الجزائر أو في الخارج ؛ أما بالنسبة لمؤلفات الأجانب اعتمد المعيار الإقليمي إذ فرق بين المؤلفات التي لم يسبق لها أن نشرت و التي تنشر للمرة الأولى في الجزائر ، و شملها بنفس الحماية التي تتمتع بها مؤلفات الجزائريين، في حين أن مؤلفات الأجانب التي نشرت في الخارج من قبل فإنها لا تتمتع بالحماية إلا على أساس المعاملة بالمثل ، الشيء الذي يبرز ضرورة تنسيق الجزائر مع باقي الدول فيما يتعلق بالمصنفات المعلوماتية نظرا لكثرة تداولها .

و اعتمادا على المذكرة الإيضاحية للنصوص النموذجية التي وضعتها المنظمة العالمية للملكية الفكرية التي تقتصر الحماية على واقعة النقل المادي للبرامج بل نصت صراحة على صلاحية

1 – المادة السابعة من اتفاقية بارن تنص أن مدة الحماية التي تقرها الاتفاقية تشمل مدة حياة المؤلف و 50 سنة بعد الوفاة ، أنظر في هذا الصدد المادة 12 من اتفاق جوانب الملكية الفكرية المتعلقة بالتجارة .

2 – في السابق كانت الاعتداءات على حقوق الملكية الفكرية مجرمة بموجب المادتين 394 و 590 من قانون العقوبات و بعدها أصبحت منظمة بموجب الأمر 10/97 .

النقل المعنوي لها عن طريق شبكات الحاسب التي ترتبط العديد من الدول و يطلق عليها شبكات الانترنت.

و تجدر الإشارة إلى أن هذه المستجدات التي اعتمدها المشرع الجزائري من خلال الأمرين **10/97** و**05/03** تعود لأسباب أهمها أن من شروط الانضمام إلى المنظمة العالمية للتجارة ضرورة المصادقة على اتفاقية بارن وهو ما فعلته الجزائر بموجب **المرسوم الرئاسي 341/97**[1] ، إضافة إلى تبني أحكام الاتفاق المتضمن جوانب الملكية الفكرية المتعلقة بالتجارة المبرم بين المنظمة الدولية للملكية الفكرية والمنظمة العالمية للتجارة[2] .

ولقد نصت المادة العاشرة من الاتفاق على أن برامج الإعلام الآلي سواء كانت في صورة برنامج مصدر أو صورة منقوشة فهي محمية على أساس أنها مصنفات أدبية .

كما أن الاتفاقية المتعلقة بالإجرام المعلوماتي نصت على تجريم الاعتداءات الواقعة على حقوق المؤلف والحقوق المجاورة تطبيقا لأحكام اتفاق جوانب الملكية المتعلقة بالتجارة إذا ارتكبت هذه الاعتداءات عن طريق نظام معلوماتي في نطاق تجاري.

كما أشارت **معاهدة الويبو** بشأن حق المؤلف المؤرخة في **1996/06/20** في مادتها الرابعة على أن برامج الحاسوب تتمتع بالحماية باعتبارها مصنفات أدبية حسب مفهوم المادة الثانية من اتفاقية بارن، وتطبق تلك الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها ، و أضافت المادة الخامسة منها أن مجموعات البيانات أو المواد الأخرى تتمتع بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر ابتكارات فنية بسبب اختيار محتوياتها أو ترتيبها ولا تشمل هذه الحماية البيانات أو المواد في حد ذاتها.

المطلب الثاني: مدى إمكانية حماية المعلوماتية وفقا لنصوص جرائم التقليد

1 – المرسوم الرئاسي رقم 341/97 المؤرخ في 97/09/13 المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية بارن لحماية المصنفات الأدبية والفنية المؤرخة في 1896/06/09 والمتممة في باريس في 1896/05/04 والمعدلة في 1979/09/28 .

2 – أبرم هذا الاتفاق بتاريخ 1994.04.15 و أصبح ساري المفعول بتاريخ 1995.01.01 .

اتضح مما سبق أن القانون المتعلق بحق المؤلف والحقوق المجاورة يوفر الحماية الجزائية لمصنفات الإعلام الآلي بعد أن أدمجها صراحة ضمن المصنفات المحمية متبنيا بذلك بنود الاتفاق المتعلق بجوانب الملكية الفكرية الخاصة بالتجارة بهدف الانضمام للمنظمة العالمية للتجارة وعليه تدخل برامج الحاسوب تحت مظلة الحماية الجزائية لحق المؤلف ، الأمر الذي يقتضي دراسة جرائم تقليد المصنفات المعلوماتية والجزاءات المقررة نتيجة ذلك من خلال الفرعين المواليين.

الفرع الأول: جرائم تقليد المصنفات المعلوماتية

مادام أن المشرع الجزائري أدمج تطبيقات الحاسب الآلي ضمن قائمة المصنفات المحمية من حلال القانون المتعلق بحق المؤلف و الحقوق المجاورة فإن أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج يشكل فعلا من أفعال التقليد ، وقد نص المشرع الجزائري في الأمر **05/03** على جريمة التقليد والجرائم المشابهة لها[1], إذ نصت المادة **151 من الأمر 05/03** على قيام جنحة التقليد في حالة الكشف غير المشروع عن مصنف أو أداء فني أو في حالة المساس بسلامة مصنف أو أداء فني أو حالة استنساخ مصنف أو أداء فني بأي أسلوب من الأساليب في شكل نسخ مقلدة أو مزورة أو في حالة استيراد نسخ مقلدة أو تصديرها أو بيع نسخ مزورة من مصنف أو أداء فني و أخيرا في حالة تأجير مصنف أو أداء فني أو عرضه للتداول.

و سنتطرق فيما يأتي لأصناف جرائم التقليد و أركان جريمة التقليد لنصل أخيرا لأركان الجرائم المشابهة للتقليد.

أولا: أصناف جريمة التقليد : نستخلص من قراءة نص المادة **151** من الأمر **07/03** أن هناك ثلاثة أصناف لجنحة التقليد [2] .

1 – أمال قارة ، المرجع السابق ، ص 82،83 .

2 – د . عكاشة محي الدين ، محاضرات في الملكية الأدبية و الفنية ، ديوان المطبوعات الجامعية ،الجزائر 2001 .

يتمثل الصنف الأول في الجنح التي تمس بالحق المعنوي للمؤلف و يشمل حالتين تتعلق الأولى بالكشف غير المشروع عن مصنف أدبي أو أداء فني نصت عليها المادة **22** من الأمر **05/03** ، أما الحالة الثانية نصت عليها المادة **25** من الأمر **05/03** و تتعلق بالمساس بسلامة المصنف أو الأداء الفني .

أما الصنف الثاني يتعلق بالجنح المتعلقة بالحق المالي للمؤلف و يشمل بدوره حالتين تتمثل الأولى في استنساخ مصنف بأي أسلوب من الأساليب في شكل نسخ مقلدة، و تعد حالة استنساخ البرامج بصفة غير مشروعة الحالة الأكثر شيوعا في المجال المعلوماتي [1] ، و أما الحالة الثانية تخص إبلاغ المصنف أو الأداء الفني للجمهور عن طريق التمثيل أو الأداء العلني أو البث السمعي البصري أو بواسطة التوزيع أو أية وسيلة أخرى لبث الإشارة الحاملة للأصوات أو أي نظام للمعالجة الآلية.

و أخيرا الصنف الثالث يتعلق بالجنح المشابهة لجنحة التقليد و تشمل خمس جنح وتتمثل في جنحة استيراد النسخ المقلدة و تصديرها، جنحة بيع نسخ مزورة من المصنف ، جنحة تأجير مصنف مقلد أو عرضه للتداول ، إضافة إلى الجنحتين المتعلقتين بالمساعدة و المشاركة في المساس بحقوق المؤلف و الرفض عمدا دفع المكافأة المستحقة بمقتضى الحقوق المقررة للمؤلف .

ثانيا : أركان جريمة التقليد : إن كل أصناف جريمة التقليد السابق ذكرها تستلزم توافر ركنين لقيامها .

يتمثل الركن المادي في المصنف المحمي أي محل النشاط الإجرامي لجريمة التقليد بصفة عامة ، فقد سبق و أن ذكرنا أن المشرع الجزائري اعترف لبرامج الحاسوب بصفة المصنف المحمي بموجب نص المادة الرابعة من الأمر **03/ 05** إذ شمله بالحماية من كل اعتداء يمس بالحق في الكشف عن

1 – د . عكاشة محي الدين ، نفس المرجع ، ص 93.

المصنف و الاعتداء على الحق في سلامة المصنف و كذا الاعتداء على حق النسخ بالإضافة للاعتداء على حق المؤلف في إبلاغ المصنف أو الأداء إلى الجمهور[1] .

و تجدر الإشارة إلى أنه كان من الأفضل تجريم كل اعتداء واقع على أي حق من حقوق المؤلف حتى لا تفلت بعض الأفعال من العقاب كالاعتداء على حق الأبوة والاعتداء على الحق في تحويل المصنف بالترجمة أي نقل البرنامج إلى لغة أخرى دون ترخيص.

مع العلم أن كل حالات جريمة التقليد تشترط عدم وجود إذن من المؤلف أو خلفائه، إذ يشترط أن يكون هذا الإذن سابقا على أفعال الاعتداء أو معاصرا لها .

وكما أن الرضا لا يعد سببا من أسباب الإباحة، فالرضا لا يعد ظرف موضوعي يعاصر أفعال الاعتداء التي يتكون منها الركن المادي للجريمة، وإنما يشكل أحد عناصر هذا الركن الذي يتخلف بتخلفه و منه إذا كان البرنامج مشتركا، يصدر الإذن من جميع الشركاء، وإذا كان جماعيا فالموافقة تصدر عن ممثل الشخص المعنوي.

أما الركن المعنوي نعني به القصد الجنائي و يكون في جريمة التقليد مفترض ، فتوافر إحدى صور النشاط الإجرامي السابقة يعد قرينة على توافر القصد الجنائي ، وهذا يعني أن حسن النية لا يفترض وعلى الجاني إثبات حسن نيته و الاختصاص للفصل في ذلك يعود لمحكمة الموضوع .

ثالثا : أركان الجنح المشابهة للتقليد[2].

هناك بعض الجرائم تتشابه مع جريمة التقليد في صورها إلا أنها تخرج عن مجال جريمة التقليد و لقيام هذه الجرائم استوجب المشرع توافر ركنين على غرار جريمة التقليد .

يتمثل الركن المادي في صور التعامل المجرمة مع البرامج المقلدة سواء قلدت داخل أرض الوطن أو خارجها و يشمل أربع حالات تتمثل في حالة استيراد وتصدير نسخ مقلدة ، حالة بيع وتأجير

1 – إذ تنص المادة 150 من الأمر 05/03 أنه يعد مرتكبا لجريمة التقليد كل من يقوم بإبلاغ المصنف أو الأداء الفني للجمهور عن طريق التمثيل أو الأداء العلني أو البث السمعي أو السمعي البصري أو بواسطة التوزيع أو أية وسيلة أخرى لبث الإشارات الحاملة للأصوات أو الصور و الأصوات معا أو بأي نظام من نظم المعالجة المعلوماتية .

2 – د . عكاشة محي الدين ، المرجع السابق ، ص 94.

نسخ مقلدة و حالة عرض نسخ مقلدة للتداول و أخيرا حالة المساعدة و المشاركة في المساس بحق المؤلف والرفض العمدي لدفع المكافأة المستحقة .

أما الركن المعنوي يتمثل في القصد الجنائي و يكون مفترض على غرار القصد الجنائي في جريمة التقليد و منه على الجاني إثبات حسن نيته، و تجدر الإشارة أنه في حالة الاستيراد والتصدير فإلى جانب القصد الجنائي العام ، اشترط المشرع توافر قصد الاستغلال التجاري .

الفرع الثاني : الجزاءات المقررة لجرائم التقليد

لقد ربط المشرع الجزائري حماية المصنف بتاريخ الانتهاء من الابتكار أو تاريخ النشر أو التوزيع لأول مرة ، و بالتالي أصبحت الدعوى الجزائية أو المدنية مقبولة حتى ولو لم يتم الإيداع .

و قد نصت المادة **160** من الأمر **05/03** بالإضافة إلى الطرق التقليدية لتحريك الدعوى العمومية على حق مالك الحقوق المحمية ومن يمثله تقديم شكوى للجهة القضائية المختصة محليا في حالة ما إذا كان ضحية الأفعال المنصوص والمعاقب عليها بموجب الأمر **05/03** .

كما أن المشرع قد خول لصاحب المصنف المعتدى عليه القيام بإجراء تحفظي يتمثل في عملية حجز التقليد **La Saisie De La Contrefaçon** وهو إجراء يسهل إثبات عملية التقليد, فبواسطة هذا الإجراء التحفظي يمكن حجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع أو التقليد وذلك حتى في غياب ترخيص قضائي مسبق ، وقد حدد **الأمر 05/03** بموجب المادة **146** الجهات المخول لها القيام بإجراء حجز التقليد و حصرها في ضباط الشرطة القضائية و الأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف.

و اشترط لقيام هؤلاء الموظفون بحجز النسخ المقلدة من المصنفات أو من دعائم المصنفات أو الأداءات الفنية أن تكون النسخ موضوعة تحت حراسة الديوان الوطني لحقوق المؤلف و أن يتم الإخطار الفوري لرئيس الجهة القضائية المختصة بناءا على محضر مؤرخ و موقع قانونا يثبت النسخ المقلدة المحجوزة ، على أن تفصل الجهة القضائية المختصة في طلب الحجز التحفظي في خلال

ثلاثة أيام على الأكثر من تاريخ إخطارها، و الجهة القضائية المختصة هي المحكمة التي يوجد في دائرة اختصاصها موطن المدين أو مقر الأموال التي تم حجزها [1].

و الملاحظ أن دور رئيس المحكمة مهم في هذا الإجراء ، لاسيما إذا كانت عريضة المؤلف تحتوي على عدة طلبات فيجب على المحكمة الفصل فيها كلها [2]، فقد يطلب مالك الحقوق من رئيس الجهة القضائية اتخاذ عدة تدابير تحفظية ، و بالتالي قد يأمر بها رئيس الجهة القضائية بعد دفع كفالة من قبل المدعي.

وللقاضي سلطة اتخاذ إحدى التدابير النصوص عليها في المادة **147** من الأمر **05/03** و المتمثلة في الآتي:

-إيقاف كل عملية صنع جارية ترمي إلى الاستنساخ غير المشروع للمصنف أو للأداء المحمي أو تسويق دعائم مصنوعة بما يخالف حقوق المؤلفين والحقوق المجاورة.

-القيام ولو خارج الأوقات القانونية للعمل بحجز الدعائم المقلدة والإيرادات المتولدة من الاستغلال غير المشروع للمصنفات والأداءات.

-حجز كل عتاد أستخدم أساسا لصنع الدعائم المقلدة.

مع العلم أن للقاضي الاستعجالي سلطة رفع اليد أو رفض الحجز أو حصره أو رفع التدابير التحفظية أوتعيين حارس قضائي لمراقبة عمليات إعادة الصنع وإعادة التمثيل أو إعادة نشر المؤلفات وذلك بطلب من المتضرر من هذه التصرفات في خلال ثلاثين يوما من تاريخ صدور الأمر بالحجز التحفظي أو الأمر بالتدابير التحفظية[3] مقابل إيداع الطرف المتضرر مبالغ مالية كافية لتعويض مالك الحق في حالة ما إذا كانت دعواه غير مؤسسة .

1- المادة649 من قانون 08-09 المؤرخ في 25-02-2008 والمتضمن قانون الإجراءات المدنية والإدارية , مع الملاحظة أن الاختصاص كان طبقا للمادة 08 من الأمر 66-154 والمتضمن قانون الإجراءات المدنية يتحدد بحكمة المكان الذي تم فيه الحجز.

2 – عكس إذا كانت العريضة مختصرة فإن رئيس الجهة القضائية يوافق على الحجز دون تحديد التدابير التي يجب القيام بها .

3 – أنظر المادة 146 و 147 من الأمر 05/03 .

مع العلم أن يمكن للقاضي الاستعجالي رفع التدابير التحفظية بناءا على طلب المتضرر ودون إيداع هذا الأخير مبالغ وذلك إذا لم يقم المستفيد من التدابير خلال ثلاثين يوما ابتداء من تاريخ صدور الأمر بالحجز التحفظي أو الأمر بالتدابير التحفظية إخطار الجهة القضائية المختصة.

و قد نص المشرع على العقوبات المقررة للاعتداءات على حقوق الملكية الأدبية والفنية بموجب المواد **153-156-157-158-159 من الأمر 05/03** [1]، والملاحظ أن الأمر **05/03** شدد في العقوبات المقررة مقارنة بتلك المنصوص عليها سابقا في قانون العقوبات .

فقرر كعقوبة أصلية **الحبس من ستة أشهر** إلى **ثلاثة سنوات** و غرامة من **500.000 دج** إلى **1.000.000 دج** و ذلك سواء تمت عملية النشر داخل الجزائر أو خارجها .

كما منح للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي ، ومصادرة و إتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة ، والمصادرة في هذه الحالة تكون وجوبية.

بالإضافة لإمكانية الجهة القضائية الأمر بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك و الإيرادات موضوع المصادرة للمؤلف أو أي مالك حقوق آخر لتكون عند الحاجة بمثابة تعويض.

و للقاضي بناءا على طلب الطرف المدني الأمر بنشر أحكام الإدانة على نفقة المحكوم عليه على أن لا تتعدى المصاريف قيمة الغرامة المحكوم بها.

و أخيرا نص أنه يمكن للقاضي أن يضاعف العقوبات المقررة وذلك في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر.

و عليه نستخلص أن **الأمر 05/03** قد وسع من سلطة القاضي في تقرير العقوبة ، وذلك ضمانا وحماية لحق المؤلف ومالك الحق المجاور، عن طريق تشديد العقوبات الجزائية بإدراج إتلاف النسخ المقلدة والعتاد المنشأ خصيصا لصنعها في الترتيبات الردعية.

1 – و قد كانت المواد من 390 إلى 394 من قانون العقوبات على هذه العقوبات ، غير أن أحكام هذه المواد ألغيت بمقتضى المادة 165 من أمر 10/97 المعدل و المتمم بالأمر 05/03 ، إذ أخرجت من تحت مظلة قانون العقوبات و أصبح لها تجريم خاص في إطار قوانين حقوق المؤلفو الحقوق المجاورة.

إلا أنه و رغم اعتراف المشرع الجزائري لتطبيقات الإعلام الآلي بصفة المصنف المحمي بمقتضى **الأمر 10/97** تدارك في صلب التعديل الأخير بعض الأمور نخص بالذكر تلك المتعلقة بالمصنفات المعلوماتية في الآتي :

-احترام مقتضيات المادة العاشرة من اتفاق جوانب الملكية الفكرية المتعلقة بالتجارة باعتماد مفهوم برنامج الحاسوب كمفهوم أكثر شمولا للبرمجيات واستبدال مفهوم مجموعات المعطيات بمصطلح مجموعات المعلومات البسيطة المنصوص عليها **في المادة الخامسة من الأمر 10/97**.

-وضح الطبيعة القانونية للتأجير الخاضع للحق الإستئثاري لمؤلف برامج الحاسب و استبعد تطبيق حق التأجير عندما لا يكون البرنامج ذاته هو الموضوع الأساسي للتأجير على نحو ما هو منصوص عليه في المادة الحادية عشر من اتفاق **ADPIC**.

-إضافة ضمن التدابير التحفظية تدبير إيقاف عرض الدعائم المصنوعة على الوجه غير المشروع في السوق وحجزها مع العتاد الذي استخدم في صناعتها.

-شدد العقوبات الجزائية بإدراج إتلاف النسخ المقلدة والعتاد المنشئ خصيصا لصنعها في الترتيبات الردعية.

إلا أنه تجدر الإشارة إلى أنه رغم التعديلات الواردة في مضمون الأمر **05/03**[1] إلا أنه أغفل نقاطا هامة لكون بعض المفاهيم التقليدية لحقوق المؤلف لا تتماشى وطبيعة المصنفات المعلوماتية نجملها فيما يلي:

-مدة الحماية في التشريع الجزائري كانت مطابقة للحد الأدنى الوارد باتفاقية جنيف **25** سنة بعد الوفاة طبقا للأمر **14/73** المنصوص عليها بموجب المادة **60** ، أما في الأمر **10/97** أصبحت مدة الحماية محددة بخمسين سنة بعد الوفاة طبقا لتوصيات معاهدة بارن المنصوص عليها بموجب المادة **55** إلا أنه في نظرنا أن هذه المدة طويلة نسبيا وأنه ليس من مصلحة المجتمع وتقدمه احتكار

[1]- الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة.

أفراد تلك المعرفة التكنولوجيا الحديثة مدة طويلة، فالاحتكار في تطبيقات الإعلام الآلي يجب أن يكون قصير المدة كما هو الحال في جميع الوسائل التطبيقية.

– لم يضع المشرع معيار مميز لتحديد حصول الاعتداء على حقوق مؤلف البرنامج أو أي صاحب حق فيه، فيجب أن يكون هذا المعيار مختلف على معايير حقوق الملكية الفكرية التقليدية لتحديد الاعتداء لأن إخضاع البرامج لنفس المعايير التقليدية يعني أننا لا نحمي البرامج إلا بصورة الاعتداء المباشر الذي يتمثل في النسخ المجرد فيتم التحقق من الاعتداء في مدى التشابه الظاهر بين العمل الأصلي والعمل المنسوخ.

لكن برامج الحاسب الآلي قد تكون بصورة تظهر متطابقة تمام التطابق ولكنها تؤدي إلى نتائج تختلف عن بعضها لاسيما أن هناك برامج تكتب بصورة قد تظهر أنها مختلفة تماما ولكنها تأتي بنفس النتائج ، وتطبيق معيار قانون حق التأليف السابق يؤدي في مثل هذه الأحوال إلى تقرير الاعتداء في الأول حيث لا يوجد اعتداء، و تقدير عدم الاعتداء حيث أن هناك اعتداء بالفعل .

المبحث الثالث: الحماية الجزائية للمعلوماتية من خلال نصوص مستحدثة

لما كانت الحاجة ملحة وضرورية لحماية المال المعلوماتي ، استقر الفكر القانوني على ضرورة وجود نصوص خاصة لهذا الغرض ، وقد استجابت عدة دول لهذه الحاجة بسنها قوانين تناولت في طياتها تعريفات للجريمة المعلوماتية، أنواعها، خصائصها، أركان جرائمها، عقوبتها كما أقرت الحماية الجزائية للمعلوماتية .

وتعتبر الولايات المتحدة الأمريكية في هذا الصدد أول الدول التي سنت قوانين خاصة بالجريمة المعلوماتية من أجل حماية المعلوماتية ، و تليها بعد ذلك الكثير من الدول منها كندا، ألمانيا، أستراليا، النرويج، فرنسا، السويد، اليابان...الخ .

أما بالنسبة للتشريع الجزائري ، فقد تدارك المشرع مؤخرا و لو نسبيا الفراغ القانوني في مجال الجريمة المعلوماتية، و ذلك باستحداث نصوص تجريمية خاصة لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم **15/04** المتضمن تعديل قانون العقوبات.

غير أنه تجدر الإشارة و قبل الخوض في الحديث عن الحماية الجزائية المعلوماتية من خلال تعديل قانون العقوبات إلى أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية ، وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي أو ما يصطلح عليه فقها بالتزوير المعلوماتي ، و عليه ارتأينا حتى لا تتميز دراستنا بالقصور و تكون أكثر شمولية أن نتعرض للاعتداءات الواردة على المعلوماتية من خلال المطلبين المواليين ، نتطرق في أولهما إلى الاعتداءات الماسة بالأنظمة المعلوماتية لنصل في المطلب الثاني إلى الاعتداءات الماسة بمنتجات الإعلام الآلي .

المطلب الأول : الاعتداءات الماسة بالأنظمة المعلوماتية

تشير الإحصائيات إلى وقوع ما بين **200** إلى **250** حالة اعتداء يوميا على الأنظمة المعلوماتية في الجزائر[1].

و نظرا لتفاقم الاعتداءات الواقعة على الأنظمة المعلوماتية خاصة مع ضعف الحماية ظهرت ضرورة تدخل التشريع صراحة سواء على المستوى الدولي أو على المستوى الداخلي لحماية المعلوماتية .

فأما على المستوى الدولي تم وضع أول اتفاقية حول الإجرام المعلوماتي بتاريخ **2001/11/08** تضمنت مختلف أشكال الإجرام المعلوماتي[2] و التي تم التوقيع عليها بتاريخ **2001/11/23** ببودابست[3].

[1] -Benelkadi kamel : les sites algériens vulnerables journal el waten 23/12/2002 n°-3668.

[2] – الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

[3] - أنظر الملحق رقم 01 من المذكرة .

في حين أنه على المستوى الوطني فقد استدرك المشرع الجزائري الفراغ القانوني من خلال التعديل الأخير لقانون العقوبات الذي تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم **156/66** بإضافة القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" و تضمن ثمان مواد من المادة **394 مكرر** إلى غاية **المادة394 مكرر 7** و كذا القانون**04/09** المؤرخ في **2009.08.05** المتضمن القواعد الخاصة لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

و تجدر الإشارة أنه و إن كانت الجرائم الماسة بالأنظمة المعلوماتية تختلف في أركانها و عقوبتها إلا أنها تشترك مع بعضها البعض في مفهوم نظام المعالجة الآلية ، ولذلك فإن دراسة تلك الجرائم يقتضي منا أولا توضيح وبيان مفهوم نظام المعالجة الآلية للمعطيات، الأركان الأساسية لها، و أخيرا الجزاءات المقررة لها.

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام[1].

و يعتبر نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن أنه تعبير متطور يخضع للتطورات السريعة و المتلاحقة في مجال الحاسبات الآلية[2]، ولذلك فإن التشريع الفرنسي لم يقم بتعريف نظام المعالجة الآلية للمعطيات بل أوكل مهمة تعريفه لكل من الفقه و القضاء .

[1]–أمال قارة ، المرجع السابق ، ص 100.

[2] – راجع د . علي عبد القادر القهوجي ، المرجع السابق ، ص 119 – 120.

في حين أن التشريع الجزائري نجده أنه تبنى التعريف الذي جاءت به اتفاقية الدولية للإجرام المعلوماتي[1] بموجب أحكام المادة الثانية الفقرة ب من قانون **04/09** و أطلق عليه تسمية "**منظومة معلوماتية**" و عرفها بأنها " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ".

و عليه فإن نظام المعالجة الآلية يقوم على عنصرين [2]، يتمثل العنصر الأول في مركب يتكون من عناصر مادية و معنوية مختلفة ترتبط فيما بينها نتيجة علاقات توحدها بهدف تحقيق هدف محدد ، أما العنصر الثاني يتمثل في ضرورة خضوع النظام لحماية فنية ، نتطرق لذلك فيما يأتي بشكل من التفصيل .

أولا : مكونات نظام المعالجة الآلية للمعطيات : يتكون نظام المعالجة الآلية للمعطيات من العناصر المادية والمعنوية التي يتكون منها المركب مثل الذاكرة ، البرامج ، المعطيات ، أجهزة الربط...الخ,و بما أن هذه العناصر واردة على سبيل المثال لا الحصر فإن ذلك يفتح المجال لإضافة عناصر جديدة أو حذف بعضها حسبما يستوحيه التطور التقني في هذا المجال.

و عليه متى وقع اعتداء على عنصر بمفرده لا يشكل جزءا في هذا النظام ، فإن ذلك يفيد نفي قيام أية جريمة من جرائم الاعتداء على نظام المعالجة الآلية للمعطيات ، كما إذا وقع الاعتداء على برامج معروضة للبيع،أو على قطع الغيار أو حتى على الأنظمة التي خرجت من الخدمة تماما.

و لكن على العكس من ذلك، تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل، أو حتى لو كان النظام كله في حالة عطل تام و كان يمكن إصلاحه.

[1] – عرفت في مادتها الثانية النظام المعلوماتي على النحو التالي : « يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات الصلة بذلك ، و يقوم أحدها أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات » .

[2] – أمال قارة ، المرجع السابق ، ص 102.

ثانيا : ضرورة خضوع النظام لحماية فنية[1] : يسعى المتخصصون بأمن المعلومات إيجاد وسائل للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات ، و بالأخص حاليا شبكة الإنترنت، و لتأمين سرية الرسائل الالكترونية وسرية البيانات المتناقلة و خاصة منها تلك المتعلقة بالأعمال التجارية الرقمية و وصلوا إلى اعتبار أن التشفير يمثل أفضل وسيلة للحفاظ على سرية البيانات المتناقلة ، و عليه حث الخبراء على ضرورة استخدام أسلوب التشفير لمنع الآخرين من الإطلاع على الرسائل الالكترونية ، وهناك شكلين أساسيين للتشفير:

يتمثل الشكل الأول في **La cryptologie symétrique** و أساسه أن نفس المفتاح التشفيري يستعمل للتشفير، وفك الشفرة في آن واحد ، غير أن هذا الشكل يطرح مشكل إيجاد وسيلة لإرسال المفتاح بطريقة آمنة للمرسل إليه.

أما الشكل الثاني يتمثل في **la crytologie Asymètrique** و أساسه أن هناك مفتاحين واحد يستعمل للتشفير و الثاني يستعمل لفك الشفرة ، و منه المستعمل يملك مفتاحا خاصا و آخر عاما ، إذ يوزع المفتاح العام و يحتفظ بسرية المفتاح الخاص ، و بذلك لكل من يريد مراسلته أن يستعمل المفتاح العام، لكن المرسل إليه وحده بإمكانه الإطلاع على مضمون الرسالة المشفرة باستعماله المفتاح الخاص.

وإن مسألة الحماية الفنية للنظام تطرح إشكالية مفادها مدى ضرورة توافرها من أجل تمتع النظام المعلوماتي بالحماية الجزائية ؟

وتجدر الإشارة إلى أن الأنظمة المعلوماتية تنقسم من حيث الحماية الفنية إلى ثلاثة أنواع يتمثل النظام الأول في الأنظمة المفتوحة للجمهور ، في حين أن النظام الثاني يتمثل في الأنظمة القاصرة

[1]- المؤسسة الوطنية للأنظمة المعلوماتية أعدت عدة ملتقيات متعلقة بالحماية الفنية للأنظمة حيث نظمت ملتقى حول إستراتيجية الأمن المعلوماتي بتاريخ 2002/12/22 و ذلك بالتعاون مع الشركة السويسرية "Elwe et compass" و ملتقى في مارس 2003 بالتعاون مع Vip group خاص بطرق حماية المعطيات التشفير.

على أصحاب الحق فيها، و لكن بدون حماية فنية أما الاتجاه الثالث و الأخير يشمل الأنظمة القاصرة على أصحاب الحق فيها، و تتمتع هذه الأخيرة بحماية فنية[1] .

و قد عارضت الحكومتين البريطانية و الأمريكية استعمال التشفير لحماية أي نوع كان من الأنظمة بدعوى أن المعلومات المتناقلة عبر شبكة الانترنت لابد أن تكون مكشوفة [2] ، في حين أنه ذهب البعض الآخر من الفقه إلى اعتبار أن سوى النوع الثالث من الأنظمة المعلوماتية يتمتع بالحماية الجزائية ، كونهم يصرون على توفير الحماية الجزائية سوى للأنظمة المحمية فنيا ذلك أن القانون الجنائي يحمي سوى الأشخاص الحريصين على أموالهم لا الأشخاص الذين يهملون توفير الحد الأدنى لحماية أموالهم و هذا من شأنه أن يعزز دور القانون الجنائي الوقائي [3] .

و بالرجوع إلى النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية نجد أنها لا تتضمن شرط الحماية الفنية ، و من المبادئ العامة المستقرة في تفسير القانون الجنائي عدم جواز تقييد النص المطلق ، أو تخصيص النص العام، إلا إذا وجد نص خاص ، و عليه يستشف من عدم تطرق المشرع لشرط الحماية الفنية أنه أراد استبعاده و لو كانت غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام الحماية الفنية، كما أن دور الحماية الفنية يبرز جليا في إثبات أركان الجريمة ، و بصفة خاصة الركن المعنوي[4].

الفرع الثاني : أركان جرائم الاعتداءات الماسّة بالأنظمة المعلوماتية

بعد التطرق لمفهوم المعالجة المعلوماتية سنقوم بتحديد أركان جرائم الاعتداء على الأنظمة المعلوماتية فيما يأتي :

[1]-أمال قارة , المرجع السابق, ص 106.

[2]- Valérie Sedaillant Les problèmes poses par la législation française en matière de chiffrement .

[3] – أمال قارة ، المرجع السابق ، ص 105 .

[4]– د. علي عبد القادر القهوجي ، المرجع السابق ، ص 123.

أولا : الركن المادي : يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات و هناك ثلاثة أشكال للاعتداء نذكرها فيما يأتي :

1-الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات Accès et maintien frauduleux dans un système de traitement automatisé des données.

نصت عليه المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي بالإضافة للمادة **394 مكرر** من قانون العقوبات بقولها " يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من **50.000** دج إلى **100.000** دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ، **تضاعف العقوبة** إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة **الحبس من ستة أشهر إلى سنتين و الغرامة** من **50.000 دج إلى 150.000 دج**".

و عليه فإن هذا الشكل من الاعتداء على نظام المعالجة الآلية للمعطيات يتكون من صورة بسيطة للجريمة و أخرى مشددة.

فأما الصورة البسيطة تقوم بمجرد الدخول أو البقاء غير المشروع.

و يقصد **بفعل الدخول** ظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات و بالتالي لا نقصد بالدخول الدخول بمفهومه المادي .

و تجدر الملاحظة أن المشرع لم يحدد وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام ، و منه تقع الجريمة بأية وسيلة أو طريقة تمت بها الدخول ، فيستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[1].

1- د. عبد القادر القهوجي ، المرجع السابق ، ص 121.

كما أن هذه الجريمة تقع من كل إنسان أيا كانت صفته ، و كفاءته المهنية و الفنية ، فهذه الجريمة ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة.

في حين أنه يقصد بفعل **البقاء Le maintien** [1] التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.

و تجدر الإشارة إلى أنه قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام ، و قد يجتمعان, و يكون البقاء معاقبا عليه وحده حين يكون الدخول إلى النظام مشروعا، و من أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، و كان على الشخص قطع وجوده و انسحابه فورا ، أو في حالة تجاوزه للمدة المسموح له البقاء فيها بداخل النظام، أو في حالة طبعه لنسخة من المعلومات، في حين سمح له بالرؤية فقط فإنه يعاقب في هذه الحالة على جريمة البقاء غير المشروع متى توافرت أركانها لاسيما منها الركن المعنوي ، و يتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور كالخدمات التلفونية و التي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو في حالة تحصله على الخدمة هذه أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة.

وقد يجتمع الدخول غير المشروع و البقاء غير المشروع معا، في الحالة التي لا يكون فيها للجاني الحق في الدخول إلى النظام ، و يدخل إليه رغم ذلك ضد إرادة من له حق السيطرة عليه ، ثم يبقى داخل النظام بعد ذلك، و يتحقق في هذا العرض الاجتماع المادي للجريمتين الدخول و البقاء غير المشروعين [2].

و إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة ، فإنها تحقق أيضا ، وبصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها .

1- د . عبد القادر القهوجي، المرجع السابق ، ص 133.

2- أمال قارة , المرجع السابق , ص 110.

كما يمكن من خلالها تجريم سرقة وقت الآلة ، بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له حق السيطرة على النظام ، ويقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج[1]، بالإضافة إلى تطبيق هذا التجريم على الاستخدام غير المشروع للبطاقات الممغنطة إما لسرقتها أو تزويرها ثم استخدامها ، و لو تم استخدمها من طرف صاحبها في حالة سحب مبالغ دون أن يكون لديه رصيد كاف مع علمه بعدم كفاية رصيده فهذه الحالة الأخيرة ينطبق عليها وصف جريمة البقاء غير المشروع داخل النظام .و يمكن أيضا تطبيق هذا الوصف على التصنت على المحادثات الهاتفية طالما أن أرقام الهواتف معالجة آليا في نظام خاص بها.

و قد اتجه غالبية الفقه إلى اعتبار هذه الجريمة جريمة سلوك مجرد، أي أنها تقع و تكتمل بمجرد الانتهاء من السلوك المكون لها المتمثل في الدخول أو البقاء، أي أن الركن المادي لتلك الجريمة لا يشترط أن يضاف إليه ضرورة التقاط معلومات أو أي شكل من أشكال الضرر ، إذ لم يشترط المشرع في نموذجها القانوني أية نتيجة إجرامية[2].

إلا أن الفقه لم يتفق حول ما إذا كانت هذه الجريمة وقتية أو مستمرة أو متتابعة الأفعال ، غير أن الرأي الراجح ذهب إلى اعتبار جريمة البقاء جريمة مستمرة كون الفترة الزمنية التي تستمر فيها جريمة الدخول قصيرة نسبيا بحيث يكون اعتبارها مستمرة أو وقتية ذات أثر ممتد بدون أثر[3] ، كما اعتبر جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو يستمر في التجول بداخله بعد انتهاء الوقت المحدد المسموح به ،أما جريمة الدخول تقوم في حالة ما إذا كان الجاني يعلم أن ليس له الحق في الدخول للنظام ، فإذا دخل وظل ساكنا نكون بصدد جريمة الدخول إلى النظام ، أما إذا بدأ في التجول فهنا تقوم جريمة البقاء داخل النظام و تبدأ منذ

[1] -chamoux(B) la loi sur la fraude informatique ;de nouvelles incriminations J.C.P 1988 doct 3321.

2- د. جميل عبد الباقي صغير ، المرجع السابق ، ص 28.

[3]- د. علي عبد القادر القهوجي، المرجع السابق ، ص 135.

لحظة التجول في نظام يعلم مسبقا أن مبدأ دخوله فيه غير مشروع أو أن مبدأ استمراره فيه غير مشروع .

أما الصورة المشددة تتحقق بتوافر الظرف المشدد المتمثل في حصول نتيجة الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

و قد نصت المادة **394 مكرر /2+3** من قانون العقوبات على أن " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة، و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50.000 دج إلى150000دج " .

و عليه نستنتج من خلال ذلك أن هناك ظرفين تشدد بهما عقوبة جريمة الدخول و البقاء داخل النظام ، و تربط بين هذين الظرفين علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع و النتيجة الضارة و إن لم تكن مقصودة .

و منه فظرف التشديد يعتبر ظرف مادي يكفي أن توجد بينه و بين الجريمة الأساسية المتمثلة في الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره ، إلا إذا أثبت الجاني انتفاء تلك العلاقة و يثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ[1] .

2-الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات Atteintes volontaires au fonctionnement de STAD و قد نصت على هذا الشكل من الاعتداء المادتين الخامسة و الثامنة من الاتفاقية الدولية للإجرام المعلوماتي ، في حين أن المشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام و اكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام ,ويمكن رد ذلك لكون أن المشرع الجزائري قد إعتبر من خلال الفقرة ج من المادة

1 – أمال قارة ، المرجع السابق ، ص 114.

الثانية من القانون **09-04** على أن برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية.[1]

و قد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات و الاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية ، فإذا كان الاعتداء مجرد وسيلة فان الفعل يشكل جريمة الاعتداء العمدي على النظام ، أما إذا كان الاعتداء غاية فان الفعل يشكل جريمة الاعتداء العمدي على المعطيات.

و تشمل صورة الاعتداء العمدي على سير النظام فعلين يتمثلان في الآتي :

يتمثل الأول منها في فعل **التعطيل (العرقلة)** و الذي يفترض وجود عمل إيجابي ، مع العلم أن المشرع لم يشترط أن يتم التعطيل بوسيلة معينة فيستوي أن يتم التعطيل بوسيلة مادية ككسر الأجهزة المادية للنظام أو تحطيم أسطوانة أو عن طريق وسيلة معنوية تتم بموجب الاعتداء على الكيانات المنطقية للنظام كالبرامج و المعطيات و ذلك بإتباع إحدى التقنيات المستعملة في هذا المجال مثل إدخال برنامج فيروسي، استخدام قنابل منطقية مؤقتة ، جعل النظام يتباطأ في أدائه لوظائفه كما يستوي أن يقترن التعطيل بالعنف أم لا .

أما الفعل الثاني يتمثل في **الإفساد Fausser** و الذي يتم بكل فعل و إن كان لا يؤدي إلى تعطيل نظام المعالجة الآلية للمعطيات يؤدي إلى جعله غير صالح للاستعمال السليم وذلك من شأنه أن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

والإفساد من هذه الزاوية يقترب من التعييب الذي يعتبر ظرفا مشددا لجريمة الدخول والبقاء غير المشروع ، إلا أن الفارق بينهما يكمن في أنه لا يشترط أن يكون الإفساد عمديا بينما يتطلب هذا الشرط بالنسبة لجريمة الاعتداء العمدي على نظام المعالجة الآلية للمعطيات .

[1] _تنص الفقرة ج من المادة 02 من القانون 09-04 في تعريفها للمعطيات المعلوماتية بأنها"أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية , **بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها**".

و من بين صور الإفساد أو التعييب نجد تقنية استخدام القنبلة المعلوماتية التي تدخل عن طريقها مجموعة معطيات تتكاثر داخل النظام تجعله غير صالح للاستعمال كاستخدام البرنامج المسمى بـ "حصان الطرودة" و الذي يقوم بتغيير غير محسوس في البرامج أو المعطيات [1].

3-الاعتداءات العمدية على المعطيات و التي نصت عليها المواد **03، 04، 08**، من الاتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع الجزائري في المادة **394 مكرر 1** و **394 مكرر 2** من قانون العقوبات فجرم في المادة الأولى الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، وجرم في المادة الثانية المساس العمدي بالمعطيات الموجودة خارج النظام، وهذا ما سنبينه فيما يلي:

- **جرائم الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي**

باستقراء المادة **394 مكرر 1** والتي تنص " أنه يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، و بغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

وعليه فإن لهذه الجريمة صورتين تتمثل الأولى في الاعتداءات العمدية على المعطيات الموجودة داخل النظام أما الصورة الثانية تتمثل في المساس العمدي بالمعطيات خارج النظام ، نجد الاعتداءات العمدية على المعطيات الموجودة داخل النظام تتجسد في إحدى الأفعال الثلاثة التالية: **الإدخال L'intrusion** ، **المحوL'effacement** ،**التعديل La modification**.

مع الملاحظة أن المشرع لم يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يقوم الركن المادي.

[1]- د .علي عبد القادر القهوجي ، المرجع السابق ، ص 143.

كما أن أفعال الإدخال و المحو و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل[1] .

و يتحقق **فعل الإدخال** بإضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية أم كان يوجد عليها معطيات من قبل[2] ، و قد يتم ذلك في حالة الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير أو في حالة إدخال برامج غريبة (فيروس ، حصان طروادة ، قنبلة معلوماتية زمنية) تضيف معطيات جديدة.

أما فعل **المحو** يقصد به إزالة جزء من المعطيات المسجلة على الدعامة و الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[3].

في حين أن فعل **التعديل** يقصد به تغيير المعطيات الموجودة داخل النظام و استبدالها بمعطيات أخرى[4]، و قد يتم التلاعب في المعطيات عن طريق استبدالها أو عن طريق التلاعب في البرنامج و ذلك بإمداده بمعطيات مغايرة تؤدي إلى نتائج مغايرة عن تلك التي صمم البرنامج لأجلها.

و تجدر الإشارة إلى أن فعل المحو و التعديل يتحققان عادة عن طريق استعمال برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم بتعديلها كاستخدام القنبلة المعلوماتية الخاصة بالمعطيات و برنامج الممحاة Gomme d'effacement أو برامج الفيروسات بصفة عامة .

كما أن أفعال الإدخال و المحو و التعديل وردت على سبيل الحصر ، و منه لا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى و لو تضمن اعتداء على المعطيات الموجودة داخل نظام

1- أمال قارة، المرجع السابق ، ص 120.

2- د . علي عبد القادر القهوجي ، المرجع السابق ، ص60.

3- د .علي عبد القادر القهوجي ، المرجع السابق ، ص51.

4- د. علي عبد القادر القهوجي ، المرجع السابق ، ص 59.

المعالجة الآلية للمعطيات ، فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينها ، لأن كل تلك الأفعال لا تنطوي على إدخال أو تعديل بالمعنى السابق[1].

أما صورة **المساس العمدي بالمعطيات خارج النظام** نص عليها المشرع الجزائري بموجب أحكام المادة **394 مكرر 2من قانون العقوبات** ، و كرس بموجبها المشرع الحماية الجزائية للمعطيات في حد ذاتها لأنه لم يشترط أن تكون المعلومات داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا ،

إذ نصت الفقرة الأولى من المادة **394 مكرر 2** أن محل الجريمة يتمثل في المعطيات سواء كانت مخزنة في أشرطة أو أقراص أو معالجة آليا أو مرسلة عن طريق منظومة معلوماتية ، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

في حين أن الفقرة الثانية من المادة **394 مكرر 2** جرمت أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات فقد يكون الهدف من ذلك المنافسة غير المشروعة ، الجوسسة ، الإرهاب ، أو التحريض على الفسق... الخ.

ثانيا : الركن المعنوي

بعد التطرق للركن المادي لجرائم الاعتداء الماس بالأنظمة المعلوماتية بمختلف أشكاله نتطرق فيما يأتي للركن المعنوي الذي يتخذ في كل الأشكال السابق ذكرها صورة القصد الجنائي إضافة إلى نية الغش.

[1]-chamoux: la loi sur la fraude informatique de nouvelles Incriminations J C P 1988 doctors 3321 .

ففي صورة الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات فإن كل من فعل الولوج و التجول و البقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا إذا تما عمدا.

و قد نصت المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي في هذا الصدد أنه يمكن السماح للدولة العضو أن تشترط لقيام هذه الجريمة مجرد خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله.

و بالتالي يلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء مع علمه بأنه ليس له الحق في الدخول إلى النظام و البقاء فيه ، و عليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقائه داخل النظام مسموح به أو مشروع ، أو إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق كأن يجهل وجود خطر من جراء الدخول أو البقاء أو كان يعتقد خطأ أنه مسموح له بالدخول ، فإذا توافر القصد الجنائي بعنصريه العلم و الإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيضل القصد قائما حتى و لو كان الباعث هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظام[1].

و بالنسبة لنية الغش تبرز من خلال الطريقة التي يتم بها الدخول عن طريق خرق الجهاز الرقابي الذي يحمي النظام ، أما بالنسبة للبقاء فإنها تستنتج من خلال العمليات التي تمت داخل النظام.

أما جريمة الاعتداءات على سير نظام المعالجة الآلية للمعطيات فإنها تعد بطبيعتها جريمة عمدية ، إذ أنه من المفترض أن أفعال العرقلة و التعطيل لا تكون إلا عمدية و هذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول و البقاء غير المشروع داخل النظام .

[1] – د .علي عبد القادر القهوجي ، المرجع السابق ، ص136-137.

و عليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة[2] ، ويظهر ذالك جليا من خلال الأفعال المشكلة لهذه الجريمة إذ لا يتصور أن يقوم الفاعل بالاعتداء على سير نظام المعالجة الآلية للمعطيات بعرقلته أو تعطيله أو إفساده عن غير قصد .

كما أن جريمة الاعتداءات العمدية على المعطيات تعد بدورها جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم و الإرادة ، إذ يجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات ، و يعلم أيضا أن ليس له الحق في القيام بذلك ، و أنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته[3].

كما يشترط بالإضافة إلى القصد الجنائي العام نية الغش ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير، بل تتوافر الجريمة و يتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك و اتجاه الإرادة إليه ، و إن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة .

و أخيرا جريمة استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية التي تتم بالقيام بأحد الأفعال المنصوص عليها في المادة **394 مكرر 2** من قانون العقوبات المتمثلة إما في التصميم أوالبحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية أو حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية , فإنه لا يمكن أن يتم هذا الاستخدام بغير علم وإرادة الفاعل مما يجعله لامحالة عمديا , إلا أن المشرع اشترط أن يكون ذلك بطريق الغش , وبالتالي فإن المشرع الجزائري يشترط توافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش في هذه الصورة كذلك .

2- د علي عبد القادر القهوجي ، المرجع السابق ، ص 142.

3- د . علي عبد القادر القهوجي ، المرجع السابق ص145.

الفرع الثالث : الجزاءات المقررة لجرائم الاعتداءات الماسّة بالأنظمة المعلوماتية

لقد نصت المادة **13** من الاتفاقية الدولية للإجرام المعلوماتي بوجوب أن تكون العقوبات المقررة نتيجة ارتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات سالبة للحرية كما نصت على وجوب تطبيق عقوبات على الشخص المعنوي بناءا على مبدأ مساءلة الشخص المعنوي الوارد في المادة **12** من نفس الاتفاقية .

وباستقراء نصوص المواد الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات الجزائري من المادة **394 مكرر** إلى غاية المادة **394 مكرر 7** نجد أن المشرع الجزائري قد تبنى هذا المبدأ في تقريره الجزاءات الواجبة على هذا النوع من الجرائم فسن عقوبات تطبق على الشخص الطبيعي وعقوبات تطبق على الشخص المعنوي وذلك ما سنتناوله فيما يلي .

أولا : العقوبات المقررة للشخص الطبيعي

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا أن المشرع وضع تدرج فيما يتعلق بالعقوبات الأصلية ، و هذا التدرج في العقوبات يعكس الخطورة الإجرامية لهذا النوع من الجرائم ، مع العلم أن المشرع وضع سلم خطورة يتضمن ثلاثة درجات [1]، نجد في الدرجة الأولى جريمة الدخول أو البقاء بالغش ، و في الدرجة الثانية نجد جريمة الدخول و البقاء المشددة و في الدرجة الأخيرة نجد الجريمة الخاصة بالمساس العمدي بالمعطيات .

إذ قرر عقوبة الحبس من ثلاثة أشهر إلى سنة و غرامة من 50 000 دج إلى 100 000 دج بموجب المادة **394 مكرر** من قانون العقوبات لجريمة الدخول و البقاء و الغش في صورتها المبسطة .

1 – أمال قارة ، المرجع السابق ، ص 127.

و قرر لجريمة الدخول و البقاء بالغش في صورتها المشددة بموجب أحكام المادة **394 مكرر /02** و **03** عقوبة مضاعفة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة ونص على عقوبة الحبس من ستة أشهر إلى سنتين ، و غرامة من 50 000 دج إلى 150000 دج إذا ترتب عن الدخول أوالبقاء غير المشروع تخريب لنظام أشغال المنظومة .

في حين أنه قرر لجريمة الاعتداء العمدي على المعطيات بموجب نص المادة **394 مكرر 2** عقوبة الحبس من شهرين إلى ثلاث سنوات و غرامة من 1 000 000 دج إلى 5 000 000 دج إذا وقع الاعتداء العمدي على معطيات موجودة داخل النظام سواء كان الاعتداء عمديا أو عن طريق الغش و ذلك بتصميم أو بحث أو تجميع أو توفير أو نشر أو الادخار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها هاته الجرائم أو عن طريق حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها قانونا.

بالإضافة للعقوبات الأصلية نص المشرع الجزائري على العقوبات التكميلية بموجب أحكام المادة **394مكرر 6** من قانون العقوبات التي يحكم بها إلى جانب العقوبات الأصلية و تتمثل في:

أ- المصادرة و هي عقوبة تكميلية تشمل الأجهزة و البرامج و الوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية.

ب-إغلاق المواقع Les sites التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

ج-إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها كإغلاق المقهى الالكتروني Cyber café الذي ترتكب فيه مثل هذه الجرائم بشرط توافر عنصر العلم لدى مالكها.

كما نص المشرع الجزائري على الظروف المشددة بموجب أحكام المادة **394 مكرر الفقرة 2و3** إذ نص على ظرف تشدد فيه عقوبة جريمة الدخول و البقاء غير المشروع داخل النظام ، و

يتحقق هذا الظرف في حالة ما ينتج عن الدخول أو البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام و إما تخريب نظام اشتغال المنظومة.

ففي الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة **394 مكرر**، أما في الحالة الثانية تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 000 50 دج إلى 000 150 دج ، و يعد هذا الظرف المشدد كما سبق تبيانه ظرف مادي يكفي أن تقوم بينه و بين الجريمة الأساسية و هي الدخول أو البقاء غير المشروع علاقة السببية للقول بتوافره[1].

كما نصت المادة **394 مكرر 3** على أنه تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية متى استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، و ذلك دون الإخلال بتطبيق عقوبات النشر.

ثانيا : العقوبات المقررة للشخص المعنوي :

نصت المادة **12** من الاتفاقية الدولية للإجرام المعلوماتي على أنه يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا ، كما يسأل عن الجريمة التامة أو الشروع فيها بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه ، هذا مع الإشارة إلى أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي، و ذلك من خلال نص المادة **18 مكرر من قانون 15/04** المتضمن قانون العقوبات .

و قد نصت المادة **394 مكرر4** من قانون العقوبات أن عقوبة الشخص المعنوي الذي يرتكب إحدى الجرائم الماسة بالأنظمة المعلوماتية هي الغرامة التي تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

1- أمال قارة ، المرجع السابق ، ص 128.

ثالثا : عقوبة الاتفاق الجنائي (الاشتراك)

نصت المادة **11** من الاتفاقية الدولية للإجرام المعلوماتي على تجريم التحضير للجرائم الماسة بالأنظمة المعلوماتية، و قد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة **394 مكرر 5** من قانون العقوبات إذ جاء فيها أنه "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقرر للجريمة ذاتها".

و إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية يتمثل في كون أن مثل هذه الجرائم تتم عادة في إطار مجموعة ، كما أن المشرع أراد توسيع نطاق العقوبة فأخضع الأعمال التحضيرية للعقوبة المقررة للجريمة التي تم التحضير لها إذا تمت في إطار اتفاق جنائي ، بمعنى آخر أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص[1].

و بما أن المشرع الجزائري يعاقب على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها، فإنه في حالة تعدد الجرائم التي تم التحضير لها تكون العقوبة المقررة هي عقوبة الجريمة الأشد.

ويشترط لمعاقبة الاتفاق الجنائي أن نكون بصدد مجموعة أو اتفاق يهدف التحضير لجريمة من الجرائم الماسة بالأنظمة المعلوماتية و أن يتجسد هذا التحضير بفعل مادي و أن تتم فعلا المشاركة في هذا الاتفاق و أخيرا يشترط أن يتوفر القصد الجنائي.

1- أمال قارة ، المرجع السابق ، ص 131.

فبالنسبة للمجموعة أو الاتفاق يشترط أن يتم الاتفاق بين شخصين على الأقل فإذا ارتكب العمل التحضيري المادي شخص واحد بمفرده و بمعزل عن غيره فلا يعاقب في هذه الحالة ، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر و ذلك بغرض تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية .

و بالتالي يجب أن يحدد الهدف الإجرامي منذ البداية ، و عليه فإذا تم إنشاء نادي للمعلوماتية بهدف التكوين أو التسلية العلمية و يحول بعدها نشاطه لأهداف إجرامية لا يقع تحت طائلة المادة **394 مكرر 5** من قانون العقوبات هذا من جهة ، و من جهة أخرى و استنادا لنفس المادة فإنه لا يعاقب من اتفق بهدف ارتكاب جنحة تقليد البرامج المعاقب عليها بنصوص حق المؤلف و الحقوق المجاورة كونها لا تدخل ضمن الجنح الماسة بالأنظمة المعلوماتية .

كما أن التحضير لا يكف بل يجب أن يتم تجسيده بفعل مادي يتعلق بأعمال تحضيرية كتبادل المعلومات الهامة لارتكاب الجريمة ، الإعلان عن كلمة السر (المرور) أو رمز الدخول...الخ.

أما عن المشاركة فإن مجرد الانضمام أو الاتفاق لا يكف بل يجب توافر فعل إيجابي للمشاركة ، و يشترط بالإضافة لذلك لقيام القصد الجنائي لدى أعضاء الجماعة يستوجب توافر العلم لدى كل منهم بأنه عضو في الجماعة الإجرامية و أن تتجه إرادة كل عضو إلى تحقيق نشاط إجرامي معين يتمثل في العمل التحضيري.

رابعا : عقوبة الشروع في الجريمة

نصت عليه المادة **11** من الاتفاقية الدولية للإجرام و تبناه المشرع الجزائري في نص المادة **394 مكرر 7** من قانون العقوبات التي جاء فيها أنه "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم لعقوبات المقررة للجنحة ذاتها".

وعليه من خلال استقراء نص المادة المذكورة أعلاه نستنتج أن الجنحة الواردة بنص المادة **394 مكرر 5** من قانون العقوبات مشمولة بهذا النص أي أن المشرع الجزائري بهذا المنطق قد تبنى فكرة الشروع في الاتفاق الجنائي عكس التشريعات المقارنة بما فيها التشريع الفرنسي التي أخرجت الاتفاق الجنائي لتحضير الجرائم الماسة بالأنظمة المعلوماتية من نطاق الشروع لأنها تعتبر أن ذلك مساس بالنظرية العامة في القانون الجنائي كون تحضير الجرائم التي تتم في إطار الاتفاق تشكل في حد ذاتها محاولة أو عمل تحضيري مما يؤدي إلى تبني فكرة الشروع في الشروع[1].

المطلب الثاني : الاعتداءات على منتجات الإعلام الآلي –التزوير المعلوماتي–

إن الدعامات المادية للحاسب الآلي قد احتلت في الوقت الراهن مكانة المحررات و الصكوك، و نظرا لأهمية و خطورة ما تحتويه من بيانات قد تكون محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها الشيء الذي من شأنه إحداث أضرار مادية أو معنوية [2] كتزوير المستخرجات الالكترونية مثل الأوراق المالية ، أو السحب على الجوائز.

وتعد جريمة التزوير في المجال المعلوماتي من أخطر صور غش المعلوماتية نظرا للدور الهام و الخطير الذي أصبح يقوم به الحاسب الآلي الآن ، و الذي اقتحم كافة المجالات و أصبحت تجري من خلاله كم هائل من العمليات ذات الآثار القانونية الهامة و الخطيرة و التي لا يصدق عليها وصف "المكتوب" المنصوص عليه في القانونين المدني و الجنائي ، و قد أثار هذا الوضع الشك حول دلالتها في الإثبات و حول إمكانية وقوع جريمة التزوير العادية و لهذا كان التدخل التشريعي ذو أهمية بالغة.

1- أمال قارة،المرجع السابق، ص 133.

2- Roman (M) Faux Juris class,1996 art 441/1 à 441/12 n°19 P456

و تجدر الإشارة إلى أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، ربما اقتداء بما فعله المشرع الفرنسي الذي أخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير و ذلك بعد أن قام بتعديله بجعل موضوع التزوير دعامة مادية و ليس محررا .

في حين أن النصوص الواردة في قانون العقوبات الجزائري الخاصة بالتزوير تجعل التزوير يرد على محرر ، و عليه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير ، مما يستدعي تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي[1].

الفرع الأول : مفهوم منتجات الإعلام الآلي

سنتعرض للتفرقة بين مفهومين هما المستند المعالج آليا و المستند المعلوماتي.

أولا: المستند المعالج آليا: يقصد بالمستند في الاصطلاح القانوني كل دعامة مادية تصلح لأن تكون عليها معلومات أو آراء و التي هي بطبيعتها غير مادية.

في حين أنه يقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز (قرص أو شريط ممغنط أو خلافة)يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية.

و يعد المستند المعالج آليا كل دعامة مادية مهيأة لاستقبال المعلومات و التي تسجل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية للمعلوماتية ، أي هو الدعامة المادية التي تم تحويل المعطيات المسجلة عليها للغة الآلة[2].

ثانيا : المستند المعلوماتي: و هو ذلك المستند غير المعالج آليا ، و تعتبر مستندات معلوماتية الأوراق المعدة لتسطير المعلومات عليها و الأقراص الممغنطة التي لم يسجل عليها أي شيء

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

2 - د.محمد عقاد ، المرجع السابق، ص 36 .

بعد ، و الملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرنامج ، و كذا البطاقات البنكية التي لم تدخل الخدمة بعد.

الفرع الثاني: مدى خضوع منتجات الإعلام الآلي لنصوص التزوير

الاعتداء على منتجات الإعلام الآلي يتجسد في فعل التزوير المعلوماتي الذي نصت عليه المادة السابعة من الاتفاقية الدولية للإجرام المعلوماتي ، إذ أن التلاعب في المعطيات الذي من شأنه أن تنتج عنه معطيات غير أصلية يعد تزويرا.

و يقتضي الركن المادي لجريمة التزوير أن يكون تغيير الحقيقة حاصلا في محرر يشكل سندا ، هذا ما يستفاد منه من أحكام المواد **214** إلى **229 من قانون العقوبات** التي تنص على قيام التزوير في المحررات العمومية أو الرسمية أو في المحررات العرفية أو التجارية أو المصرفية أو في بعض الوثائق الإدارية و الشهادات ، و من هذا المنطلق نستنتج أن جريمة التزوير لا تقوم إذا كان تغيير الحقيقة قد تم بقول أو بفعل ،كما لا تقوم لو حصل تغيير الحقيقة في وثيقة لا يمكن الاستناد إليها لممارسة حق أو عمل[1] .

و يشترط بالإضافة لذلك أن يكون المحرر في شكل "كتابة" أو عبارات خطية، و على هذا الأساس لا يعد محررا كل ما هو غير مكتوب كالعداد الحاسب لاستهلاك الكهرباء أو المياه أو الغاز أو الأختام المنسوبة إلى فرد أو جهة.

و لنفس السبب أيضا لا تعد محررات الأفلام و الأسطوانات و أشرطة التسجيل و الأقراص الممغنطة أيا كانت أهميتها القانونية ، مما أدى بالمشرع الفرنسي ، نظرا للتطورات التقنية التي شهدها

[1] – د.أحسسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، الجزء الثاني، جرائم الفساد، جرائم المال و الأعمال، جرائم التزوير، الطبعة الثالثة منقحة و متممة في ضوء النصوص الجديدة لاسيما قانون 20 فبراير 2006 المتعلق بالوقاية من الفساد و مكافحته، دار هومه ، سنة 2006 ، ص 336 .

العالم في هذا المجال و للمكانة التي تحتلها هذه الوسائل في الحياة اليومية ، إلى إضافة إلى جانب مصطلح المحرر عبارة "كل سند آخر لتعبير الفكر" [1].

و عليه الإشكال الذي يطرح في هذا الصدد يتمثل في مدى إمكانية تطبيق نصوص التزوير الواردة في قانون العقوبات الجزائري على الاعتداءات الماسة بمنتجات الإعلام الآلي ؟

للإجابة على هذا الإشكال يجب التطرق أولا إلى مدى انطباق وصف المحرر على البيانات المعالجة آليا و مدى خضوعها لفعل تغيير الحقيقة في مرحلة لاحقة.

أولا : مدى انطباق وصف المحرر على منتجات الإعلام الآلي

يعد المحرر في مضمونه كتابة مركبة من حروف أو علامات تدل على معنى أو فكرة معينة تمكن القراءة البصرية لمحتواه و هو ما تفرضه نصوص التزوير التقليدية، و عليه يمكن إجمال خصائص المحرر في ثلاث نقاط:

1-اتخاذ المحرر شكلا كتابيا و إمكانية إدراك مضمونه بالنظر إليه أو لمسه، فإذا استحالت قراءته فلايصلح وسيلة للإثبات و لإعلان على ما احتواه من تغيير.

2-إمكانية نسب الكتابة لشخص معين.

3-إحداث المحرر آثارا قانونية.

وبإسقاط المفهوم التقليدي للمحرر على مجال المعالجة الآلية للبيانات، نجد أن تغيير الحقيقة الذي يكون محله الأشرطة الممغنطة لا ينطبق عليه وصف جريمة التزوير في المحررات، و ذلك لعدم وجود عنصر الكتابة،فجريمة التزوير تشترط الكتابة فأي تغيير في الوعاء المعلوماتي لا يعتبر تزويرا لانتفاء هذا الشرط.

و لذا قد ذهبت بعض التشريعات الحديثة لمواجهة القصور الموجود في النصوص التقليدية إلى استحداث نصوص تجريمية جديدة أو إدخال تعديلات على التشريعات التقليدية حتى لا تفلت

1 - د.أحسسن بوسقيعة ، المرجع السابق ، ص 336 .

جريمة التزوير الواقعة على المستندات المعلوماتية من العقاب ، و من أمثلة هذه التشريعات التشريع الفرنسي[1] .

أما بالنسبة للتشريع الجزائري يعد من التشريعات التقليدية، إذ لم يسد هذا الفراغ التشريعي رغم التطور الحاصل في مجال المعلوماتية فلا تزال النصوص المتعلقة بالتزوير المنصوص عليها في المواد من **214** إلى **229** من قانون العقوبات تشترط المحرر لتطبيق جريمة التزوير.

ثانيا: مدى خضوع منتجات الإعلام الآلي للنشاط الإجرامي لجريمة التزوير

النشاط الإجرامي المكون لجريمة التزوير يتمثل في فعل تغيير الحقيقة و يعني استبدالها بما يخالفه، و بالتالي إذا انتفى هذا التغيير انتفى معه التزوير, و المقصود بتغيير الحقيقة هو تغيير الحقيقة القانونية النسبية و ليس تغيير الحقيقة الواقعية المطلقة [2]، إذ يكفي لتغيير الحقيقة الذي تتطلبها جريمة التزوير أن يكون هناك مساس بحقوق الغير أو مراكزهم القانونية الثابتة في تلك المحررات، و عليه يمكن تصور تغيير الحقيقة في نظام المعالجة الآلية للمعطيات بالتلاعب في المعطيات مما يؤثر على أصالتها[3].

و تجدر الإشارة إلى أن تحويل البرنامج أو قواعد البيانات لا يعد تزويرا لكون البرامج والمعلومات لا ينطبق عليها وصف المحرر كما سبق تبيانه ، و لكن يمكن أن تقع هذه الأفعال تحت طائلة نصوص التقليد الواردة في قانون حق المؤلف و الحقوق المجاورة.

و تجدر الملاحظة أن التغيير المشترط لقيام جريمة التزوير يمكن أن ينصب على بطاقات الائتمان الممغنطة، و قد ميز الفقه في هذا الصدد بين التغيير المادي المنصب على البطاقة ذاتها فاعتبر

1 – لقد استحدث المشرع الفرنسي نصا خاصا بالتزوير المعلوماتي بموجب المادة 9/462 من قانون العقوبات الفرنسي المعدل سنة 1988 ، إلا أنه تراجع عن موقفه فألغى هذه المادة وأخضعه لنصوص التزوير كما سبق تبيانه وللمزيد من التفاصيل راجع أمال قارة ، مرجع سابق ، ص138-139.

2 – أمال قارة ,المرجع السابق , ص131.

3 – أسامة أحمد المناعسة ، جلال محمد الزعبين صايل فاضل الهواوشة ، جرائم الحاسب الآلي و الانترنت ، دار وائل للنشر ، الأردن، سنة 2004 ، ص159.

التغييرات المادية كتغيير اسم الحامل أو الرقم الخاص بالبطاقة أو تاريخ انتهاء صلاحيتها يشكل تزويرا وذلك لانطباق وصف المحرر على البطاقة الائتمانية لكونها تعبر عن مجموعة من الأفكار والمعاني مجسدة في شكل مادي ، بينما اختلف حول التغيير الذي ينصب على البيانات والمعلومات المبرمجة آليا فمنهم من أقر بعدم انطباق هذا الفعل على التزوير لعدم إمكانية قراءة هذه المعلومات بالعين المجردة وبالتالي انعدام انطباق وصف المحرر على البطاقة في هذه الحالة ، في حين أن البعض الآخر أقر بانطباق وصف جريمة التزوير على هذا الفعل لكون و إن كانت البيانات لا يمكن قراءتها بالعين المجردة فيمكن قراءتها وفقا للإجراءات الخاصة بها ، ومن ثم لا يمكن نفي عنها وصف المحرر ، إلا أن هذا الرأي الأخير مردود عليه لكون أن الفقه والقضاء مجمع على أنه يجب أن يكون المحرر مقروءا بمجرد الإطلاع عليه ، ومن ثم لا تعد من قبيل التزوير التعديلات التي تطرأ على المعلومات المعالجة آليا[1].

ومن هنا نلاحظ ضرورة تدخل من المشرع الجزائري لتحديد مفهوم المحرر الذي يكون محلا لجريمة التزوير.

و عليه نخلص في الأخير إلى القول أن المشرع الجزائري رغم تداركه من خلال القانون **15/04** المتضمن تعديل قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي و ذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة إلا أنه أغفل تجريم الاعتداءات الواردة على منتجات الإعلام الآلي ، فلم يستحدث نصا خاصا بالتزوير المعلوماتي و لم يتبنى الاتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

1- للمزيد من التفاصيل راجع د.نائلة عادل محمد فريد قورة , المرجع السابق , ص584-586.

الخاتمة

خاتمة

و في الأخير نخلص إلى القول أن دراسة موضوع الجريمة المعلوماتية تكتسي أهمية بالغة كونها تساهم في التعريف بظاهرة إجرامية جديدة بدأت في الظهور و الانتشار في معظم المجتمعات ، و نظرا لارتباطها بتكنولوجيا متطورة أدى إلى تميزها عن الجرائم التقليدية بدءا بتسميتها وصولا إلى الأفعال التي تدخل ضمن دائرتها .

و لا شك أن قانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تعديل قانون العقوبات بموجب قانون 15/04 كانت لهما أهمية في تدارك الفراغ التشريعي الذي كان يعتري القانون الجزائري و ذلك من خلال حسم المشرع الجدل الفقهي القائم حول طبيعة المعلوماتية باعتبارها مالا من نوع خاص باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات في الفصل الثالث من الباب الثاني من الكتاب الثالث من المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات لكون أن القسم السابع ورد تحت الكتاب الثالث المتعلق بالجنايات و الجنح ضد الأموال .

كما أن هذا التعديل يعد قفزة في مجال التشريع كونه واكب التشريعات المقارنة بتجسيده معظم أحكام الاتفاقية الدولية للإجرام المعلوماتي من خلال تجريم أفعال الدخول و البقاء غير المشروع داخل النظام المعلوماتي و تشديد العقوبة إذا ترتب عن ذلك مساس بالمعطيات أو نظام التشغيل للمنظومة المعلوماتية ، المساس بالمعطيات أو تغيرها ، استخدام المعطيات كوسيلة لارتكاب الجرائم المعلوماتية ، حيازة و إفشاء و نشر و استعمال المعطيات المحصلة من هذه الجرائم ، تجريم المساس بنظام التشغيل على أساس اعتبار المعطيات المعلوماتية من خلال الفقرة ج من المادة الثانية من قانون 09-04 تشمل برامج التشغيل.

كما أن المشرع الجزائري قد تبنى مبدأ مسؤولية الشخص المعنوي و وسع نطاق العقوبة بتجريم الشروع في هذه الجرائم بتجريمه حتى الأعمال التحضيرية في إطار الاتفاق الجنائي .

و بالمقابل فإنه بالرغم من مزايا هذين القانونين إلا أنهما لا يخلوان من بعض العيوب و النقائص و الانتقادات التي لاحظناها من خلال معالجتنا لهذا الموضوع ، نذكرها فيما يأتي محاولين بكل تواضع اقتراح بعض الحلول لها :

- بداية لم يذكر المشرع الخصائص التي يجب أن تتوفر عليها المعلومة حتى تتمتع بالحماية القانونية رغم أهمية الأمر ، و المتمثلة في صفات التحديد و الابتكار و السرية و الاستئثار ، لذا نحن في رأينا أنه من الأحسن لو يذكر المشرع ذلك صراحة لتفادي كل لبس فيما يخص التعريف بالمعلومة المحمية قانونا كونها غالبا ما تكون مستهدفة من خلال الجرائم المعلوماتية.
- اتسام تعريف المشرع الجزائري للجرائم المعلوماتية بالقصور لعدم تحديد صور السلوك الإجرامي و دور المنظومة المعلوماتية في النشاط المجرم ، و ذلك لتبنيه المفهوم الموسع للجرائم المعلوماتية من خلال أحكام المادة 02 من قانون 09-04 التي نصت على أن الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية ، و بما أن مبدأ الشرعية يحكم المجال الجزائي يجب تحديد بدقة الأفعال المجرمة ,و في رأينا التعريف الأنسب للجرائم المعلوماتية يتمثل في كل اعتداء على النظام المعلوماتي أو كل اعتداء يتم باستخدام النظام المعلوماتي وكان له دور رئيسي في السلوك المجرم .
- نظرا للطبيعة المتعدية الحدود للجريمة المعلوماتية و لما تثيره من إشكالات قانونية من حيث الاختصاص و المتابعة و الإثبات ، يتعين على الدول التدخل على محورين أولهما داخلي من خلال ملائمة تشريعاتها مع هذا النمط الجديد من الجرائم ، وثانيهما دولي عن طريق إبرام اتفاقيات دولية جماعية و ثنائية على حد سواء ، فإن كانت الجزائر قد تدخلت على المستوى الداخلي من خلال سن قانون 15/04 و 04/09 فإنها لا زالت مبادرتها على المستوى الدولي قاصرة .

- كما أنه و إن كانت بعض الصور الإجرامية للجرائم المعلوماتية يمكن أن تدخل ضمن الأفعال المجرمة وفق النصوص التشريعية التقليدية ، إلا أن الأمر يشتد صعوبة بالنسبة لبعض الصور الأخرى بسبب إشكالية تحديد طبيعة المال المعلوماتي و هو الأمر الذي يضعنا أمام أزمة القانون الجنائي في مواجهة واقع المعلوماتية لكون أن القانون الجنائي يحكمه مبدأ الشرعية الذي يتفرع عنه مبدئي التفسير الضيق للنص و حضر القياس في مجال التجريم ، و عليه حبذا لو يتدخل المشرع الجزائري بتعديل النصوص التقليدية المتعلقة بجرائم الأموال حتى تتلاءم و طبيعة المال المعلوماتي تفاديا لإفلات بعض المجرمين من العقاب و تضارب أحكام القضاء .
- رغم اعتبار أمر 05/03 المتعلق بحق المؤلف و الحقوق المجاورة تطبيقات الإعلام الآلي ضمن المصنفات المحمية من خلال المادة الرابعة ، إلا أن هذه الحماية المقررة بموجب هذا الأمر قاصرة لكون المفاهيم التقليدية لحق المؤلف لا تتماشى مع خصوصيات برامج الحاسب الآلي و من ثم وجب تعديل قانون الملكية الأدبية و الفنية فيما يخص تقليص مدة الحماية من خمسين سنة بعد وفاة المؤلف بما يتماشى و طبيعة برامج الحاسب الآلي مراعاة للتطور السريع الذي تشهده المعلوماتية و تقرير نصوص تجريمية خاصة لكل مساس بالمعلوماتية مراعاة لطبيعتها الخاصة .
- ضف إلى ذلك عدم تجريم المشرع الجزائري التزوير المعلوماتي ، ولذا في رأينا على المشرع تدارك هذا الفراغ التشريعي من خلال استحداث نص خاص به أو بتوسيع مجال التزوير عن طريق توسيع مفهوم المحرر ليشمل أية دعامة أخرى على غرار التشريعات الحديثة و منها التشريع الفرنسي.
- كما أهمل المشرع الجزائري تقرير نصوص خاصة للأفعال التي يكون النظام المعلوماتي وسيلة مسهلة لارتكابها كالجرائم الأخلاقية و الإرهابية المرتكبة عبر الأنظمة المعلوماتية و لذا يتعين تدخل المشرع من خلال تشديد العقوبات على الأفعال التي تكون فيها المعلوماتية وسيلة لارتكاب جرائم أخرى على النحو السابق ذكره .

- و في الأخير تجدر الإشارة كما أنه لا يكفي أن يتم مواكبة نصوص تشريعية للتشريعات المقارنة بدون تجسيدها من الناحية التطبيقية إذ يجب العمل على تكوين فرق من الضبطية القضائية و قضاة متخصصين في هذا النوع من الجرائم و مدها بكافة الوسائل المادية و التقنية اللازمة لأداء عملها .

و في الختام نسأل الله التوفيق و السداد ، و أن يزيدنا من فضله علما و خير ما نختم به قوله تعالى " و ما أوتيتم من العلم إلا قليلا" .

الملحـــق

I- المراجع العـــامة:

1. . د. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هـومة ، الطبعة الرابعة، 2007.
2. د. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص الجزء الأول، الجرائم ضد الأشخاص والجرائم ضد الأموال، الطبعة الخامسة منقحة ومتممة في ضوء النصوص الجديدة، دار هـومة، 2006.
3. د. أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص، الجزء الثاني، جرائم الفساد، جرائم المال والأعمال، جرائم التزوير، الطبعة الثالثة منقحة ومتممة في ضوء النصوص الجديدة، دار هـومة، 2006.
4. د. أحمد عبد الرزاق السنهوري ، الوسيط في شرح القانون المدني، حق الملكية، الجزء الثامن، دار إحياء التراث العربي، بيروت، 1952.
5. أحمد فتحي سرور، الوسيط في قانون العقوبات، الطبعة الرابعة، سنة 1991.
6. د. أحمد ضياء الدين خليل، الظاهرة الإجرامية بين الفهم والتحليل، دار الطوبجي للطباعة القاهرة، الطبعة الأولى، 1992.
7. د. عبد الرشيد مأمون شديد، الحق الأدبي للمؤلف، النظرية العامة وتطبيقاتها، دار النهضة، القاهرة، سنة 1978.
8. د. عكاشة محي الدين، محاضرات في الملكية الأدبية والفنية، ديوان المطبوعات الجامعية، الجزائر، 2001.
9. د. علي راشد، القانون الجنائي أصول النظرية العامة، القاهرة، مكتبة سيد عبد الله وهبة، 1970.
10. د. محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة و النشر،1984.

11. د. محمود محمود مصطفى، شرح قانون العقوبات، القيم الخاصة، الطبعة الثامنة، مطبعة جامعة القاهرة، سنة 1984.

II- المراجع المتخصصة:

أ-باللغة العربية :

1. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الطبعة الثالثة، 2006.
2. أسامة أحمد المناعسة، جلال محمد، فاضل الهواوشة، جرائم الحاسب الآلي والأنترنت، دار وائل للنشر، الأردن، 2004.
3. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائر ،دار هومة، الطبعة الثانية 2007.
4. جميل عبد الباقي صغير، جرائم التكنولوجيا الحديثة، دار النهضة العربية.
5. طارق إبراهيم الدسوقي عطيه،النظام القانوني للحماية المعلوماتية،دار الجامعة الجديدة للشرق،2009.
6. د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار الثقافة للطباعة والنشر1999.
7. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، سنة 1999.
8. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994.
9. د. محمد عقاد، جريمة التزوير في محررات الحاسب الآلي، دراسة مقارنة، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، دار النهضة العربية، القاهرة، 1995.
10. محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة غريب القاهرة، 1984.

11. د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005.

12. د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005.

13. نبيل صقر،موسوعة الفكر القانوني،جرائم الكمبيوتر و الأنترنت في التشريع الجزائري،دار الهلال للخدمات الإعلامية، طبعة 2005.

14. د.هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية القاهرة، الطبعة الأولى، 1992.

15. أ. هشام فريد رستم، قانون العقوبات مخاطر تقنية المعلومات، مكتبة الآلات الحديثة أسيوط، سنة 1995.

ب- باللغة الفرنسية :

1-André Lucas , le droit de l'informatique , Paris , PUF , 1987 .
2-Pierre Catala ,la propriété de l'informatique ,cité par F.Toubal,le logiciel-analyse juridique,FUDUL ;LGDJ .1986.
3- Rose Philipe, la criminalité informatique à l'horizon, 2005, analyse prospéctive,l'harmattan , 1992 .
4- Rose Philipe , la criminalité informatique, que sais je ? 1ére édition ,PUF1988.

ج-باللغة الإنجليزية:

5-- Parker(Donn B),Nycum(s)and Aura(s),Computer Abuse, Stanford Research institute , 1973.

III- رسائل الدكتوراه:

1-عزة محمود أحمد خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلـي، دراسة مقارنة في القانون المدني والشريعة الإسلامية، رسالة دكتوراه، 1994.

IV- المجلات والدوريات:

أ-باللغة العربية:

1.أحمد السمدان، النظام القانوني لحماية برامج الكمبيوتر،مجلة الحقوق الكويت،العدد الرابع،سنة 1987.

2.د.زكي أمين حسونة،جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنيك المعلوماتي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 1993.

3.د.محمد ناجي ،أمن المعلومات، من ينتصر في النهاية ، مجلة الشرطة، العدد 342،سنة 1999.

4.سيد عويس، ظاهرة الجريمة في مجتمعنا المتغير ، مجلة الأمن العام، 1996، العـدد 100.

5.هشام فريد رستم، جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين، مجلة الدراسات القانونية، جامعة أسيوط، العدد 17، سنة 1995.

ب- باللغة الفرنسية :

1-Carbonier :droit civil ,PUE Paris1973 T3 les biens N17 p54 .

2-Carbonier(M)droit civil , PUE Paris 1973 T3 les biens n17_18
Vivant à propos de bien informationnel JCP 1984 doct 3132.
3-Chamoux (B) , la loi sur la fraude informatique , de nouvelles incriminations JCP1988 , doctrine 3321.
4-Duleroy r et Rocco(A M) ,l'informatique nouvelle, avril1976,les escrocs à l'informatique,le nouvel économiste,octobre 1979.
5-Fidemann(k),fraudes et délits d'affaires commis à l'aide d'ordinateurs électroniques,Rev drpeu et crim 1984.
6-Pierre Catala ,Ebauche d'une théorie juridique de l'information, d,1984. comment se protéger contre le crime informatique,temps reels p264,1984.
7- Rollant , Réfléxions sur le vol d'usage , JCP.57 .doct 3269.p452.
8- Valérie Sedaillant ,les problèmes posés par la législation française en matière de chiffrement .

ج-باللغة الإنجليزية:

1-Equity fuding life insurence,l'informatique nouvelle,mai1976.
2-Law commission , working paper ,n110,computer misuse , HMSO, 1988.
3-Wasik (martin),crime and the computers,oxford university press 1991 .

V- النصوص القانونية:

1. دستور 1996 المعدل والمتمم بموجب القانون رقم: 03/02 المؤرخ في: 10 أفريل 2002 والقانون رقم: 19/08 المؤرخ في: 15 نوفمبر 2008.
2. الأمر رقم: 155/66 المؤرخ في 18 صفر 1386 الموافق لـ: 8 يونيو سنة: 1966 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمـم، ج ر العدد: 47 لسنة: 1966.
3. الأمر رقم: 156/66 المؤرخ في 18 صفر 1386 الموافق لـ: 8 يونيو سنة: 1966 الذي يتضمن قانون العقوبات المعدل والمتمـم، ج ر العدد: 47 لسنة: 1966.
4. الأمر رقم 02/75 المؤرخ في 1975/01/09 المتعلق بالمصادقة عل الاتفاقية الدولية المتضمنة إنشاء المنظمة العالمية للملكية الفكرية الموقعة بستوكهولم بتاريخ: 1967/07/14, ج ر العدد 13 لسنة 1975.
5. الأمر رقم 10/97 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة،ج ر العدد 13لسنة1997.
6. المرسوم الرئاسي رقم 341/97 المؤرخ في 1997/09/13 المتضمن انضمام الجزائر بتحفظ إلى الاتفاقية بارن لحماية المصنفات الأدبية والفنية،ج ر عدد 61لسنة1997.
7. الأمر رقم 05/03 المؤرخ في 2003/07/19 يتعلق بحقوق المؤلف والحقوق المجاورة, ج ر العدد 44 لسنة2003.
8. الأمر رقم 07/03 المؤرخ في 2003/07/19 يتعلق ببراءات الاختراع ج ر العدد 44 ،لسنة2003.
9. القانون رقم 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات،ج ر العدد71لسنة2004.

10. قانون رقم 09/08 المؤرخ في 2008/02/25 المتضمن قانون الإجراءات المدنية والإدارية.

11. القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،ج ر العدد 07لسنة2009.

الفهرس

مقدمـــة 1

الفصل الأول : ماهية الجريمة المعلوماتية 8

المبحث الأول : تعريف الجريمة المعلوماتية و خصائصها. 9

المطلب الأول : تعريف الجريمة المعلوماتية 9

الفرع الأول: الاتجاه المضيق من مفهوم الجريمة المعلوماتية..... 12

الفرع الثاني: الاتجاه الموسع من مفهوم الجريمة المعلوماتية 14

المطلب الثاني : خصائص الجريمة المعلوماتية 17

الفرع الأول: السمات الخاصة بالجريمة المعلوماتية..... 18

الفرع الأول: السمات الخاصة بالمجرم المعلوماتي 23

المبحث الثاني : دوافع ارتكاب الجريمة المعلوماتية. 26

المطلب الأول : الدوافع الشخصية 26

الفرع الأول: الدوافع المادية 26

الفرع الثاني: الدوافع الذهنية أو النمطية..... 28

المطلب الثاني : الدوافع الخارجية 29

الفرع الأول: دافع الانتقام و إلحاق الضرر برب العمل..... 29

الفرع الثاني: الدوافع الخاصة بالمنشأة..... 30

المبحث الثالث : أنواع الجرائم المعلوماتية 33

المطلب الأول : الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي.....34

الفرع الأول: الجرائم المعلوماتية الواقعة على الأشخاص الطبيعية..... 35

الفرع الثاني: الجرائم المعلوماتية الواقعة على النظم المعلوماتية الأخرى 37

الفرع الثالث: الجرائم المعلوماتية الواقعة على الأسرار 39

المطلب الثاني : الجرائم المعلوماتية الواقعة على النظام المعلوماتي.....40

الفرع الأول: جرائم الاعتداء على المكونات المادية للنظام المعلوماتي 41

الفرع الثاني: جرائم الاعتداء على المكونات المنطقية (البرامج) للنظام المعلوماتي 42

الفرع الثالث: جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي 44

الفصل الثاني : الحماية الجزائية للمعلوماتية في التشريع الجزائري 48

المبحث الأول : الحماية الجزائية للمعلوماتية من خلال نصوص جرائم الأموال 49

المطلب الأول : مدى اعتبار المعلوماتية موضوعا لجرائم الأموال 50

الفرع الأول: مدى انطباق وصف المال على المعلوماتية.....50

الفرع الثاني: مدى اعتبار المعلوماتية مالا بصدد جرائم الأموال.....55

المطلب الثاني : مدى خضوع المعلوماتية للنشاط الإجرامي لجرائم الأموال 63

الفرع الأول:مدى خضوع المعلوماتية للنشاط الإجرامي في جريمة السرقة 63

الفرع الثاني: مدى خضوع المعلوماتية للنشاط الإجرامي في جرائم النصب وخيانة

الأمانة و تحطيم ملك الغير 64

المبحث الثاني : الحماية الجزائية للمعلوماتية من خلال نصوص الملكية الفكرية

. 70

المطلب الأول : مدى اعتبار البرنامج موضوع من موضوعات حق المؤلف 71

الفرع الأول: موقف الفقه من اعتبار البرنامج من مواضيع حق المؤلف.....71

الفرع الثاني: موقف التشريع من اعتبار البرنامج من مواضيع حق المؤلف 72

المطلب الثاني : مدى إمكانية حماية المعلوماتية وفقا لنصوص جرائم التقليد 75

الفرع الأول: جرائم تقليد المصنفات المعلوماتية 75

الفرع الثاني: الجزاءات المقررة لجرائم التقليد 78

المبحث الثالث : الحماية الجزائية للمعلوماتية من خلال النصوص المستحدثة 86

المطلب الأول : الاعتداءات الماسّة بالأنظمة المعلوماتية 84

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات.....85

الفرع الثاني: أركان جرائم الاعتداءات الماسة بالأنظمة المعلوماتية 88

الفرع الثالث: الجزاءات المقررة لجرائم الاعتداءات الماسة بالأنظمة المعلوماتية 98

المطلب الثاني : الاعتداءات على منتجات الإعلام الآلي –التزوير المعلوماتي– 104

الفرع الأول: مفهوم منتجات الإعلام الآلي 105

الفرع الثاني: مدى خضوع منتجات الإعلام الآلي لنصوص التزوير 106

خاتمـــة.....110

قائمة المراجع.....114

الملحق

تناولنا بالدراسة في هذه المذكرة موضوع الجرائم المعلوماتية أين حاولنا التعريف بهذه الظاهرة الإجرامية الجديدة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة مبرزين أهم خصائصها والعنا صر الأساسية المكونة لها والعقوبات المقررة لها.

Nous avons traité dans ce mémoire les crimes informatiques où nous avons essayé de définir ce nouveau phénomène criminel qui s'est propagé ces derniers temps mettant l'accent sur les caractéristiques et les éléments essentiels qui les produisent et les sanctions arrêtées.

We had deal, in this dissertation, with computing crimes, trying to define this new criminal phenomenon that began to spread in wide area in the last time, clarifying the essential characteristics and elements that constitute it and sanctions decided.