جامعة عمار ثليجي الأغــواط

كلية الحقوق و العلوم السياسية

قسم الحقــوق

المكافحة الموضوعية للجريمة المعلوماتية و مردودها على الإقتصاد الوطني

مذكرة مكملة ضمن مقتضيات نيل شهادة الماستر في الحقوق

تخصص: قانـون أعمـال

إعـــداد: داودي محمد

إشـــراف : د.الفحلة مديحـة

لجنـة المناقشــة

الأستاذ(ة):– أ.د رزق الله العربي بن مهيدي.....رئيسا

الأستاذ(ة):– د. الفحلة مديحة.....مشرفا و مقررا

الأستاذ(ة):– أ.خطوي مسعود.....عضوا مناقشاً

السنة الجامعيــة: 2020-2021

بسم الله الرحمان الرحيم

قال الله تعالــى

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا يَسْخَرْ قَومٌ مِنْ قَوْمٍ عَسَى أَنْ يَكُونُوا خَيْرًا مِنْهُمْ

وَ لَا نِسَاءٌ مِنْ نِسَاءٍ عَسَى أَنْ يَكُنَّ خَيْرًا مِنْهُنَّ وَ لَا تَلْمِزُوا أَنْفُسَكُمْ

وَ لَا تَنَابَزُوا بِالْأَلْقَابِ بِئْسَ الِاسْمُ الْفُسُوقُ بَعْدَ الْإِيمَانِ

وَ مَنْ لَمْ يَتُبْ فَأُولَئِكَ هُمُ الظَّالِمُونَ (الحجرات)

يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ

وَ لَا تَجَسَّسُوا وَ لَا يَغْتَب بَّعْضُكُم بَعْضًا

أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ

وَ اتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ"

صدق الله العظيم

قال رسول الله صل الله عليه و سلم

" كل المسلم على المسلم حرام دمه و ماله و عرضه"

"المسلم من سلم الناس من لسانه و يده".

صدق رسول الله صل الله عليه و سلم

الإهـــــداء

الحمد لله على منه و جوده و كرمه الذي وفقني لإتمام هذا العمل المتواضع
و الصلاة و السلام على سيدنا محمد صلاة تخرجنا بها من ظلمات الوهم
و تكرمنا بها بنور الفهم و تُوضح بها عنا ما أشكل حتى يعلم
فانك تعلم و لا نعلم و أنت علام الغيوب.

أهدي ثمرة جهدي هذا إلى من كان سببا في تعليمي و اخذ بيدي
إلى طريق العلم حتى وصلت إلى ما انأ عليه اليوم
روح أبـي تغمده الله برحمته الواسعة...
إلـى من أكرمنا الله بوجودها و كان دعائها سر نجاحي
أمي الغالية حفظها الله و رعاهـا
و أطال عمرها بخير و عافية، و رزقني الله طاعتها و برهـا
إلى إخوتـــي : أنسي في هذه الحياة و سندي في كل المقتضيات
إلى زوجتي و أولادي الذين أخذت من وقتهم و ساندوني بصبرهم و دعمهم
إلى أهلـي كبيرهم و صغيرهم الذين أهمهم أمري و ثبتوا عزيمتي و صبري
إلى أسرتي الكبيرة التي احتضنتني و أحبتني كل واحد باسمه
إلى من أشرفت على انجاز هذا العمل و شجعتني و دعمتني أستاذتي الفاضلة
.....إلى أصدقائي الأوفياء.....
إلى زملائ في الوظيفة و رفقاء دربي في العمل
إلى كل من ساعدوني بالنصح و التوجيه
و مدوا إلي يد العون أهديكم نجاحي

محمـــــد

شكر وعـرفان

أشكر الله تعالى و أحمده حمدا كثيرا على منه و جوده و كرمه

الذي هداني و وفقني في انجاز هذا العمل المتواضع

و أصلي و أسلم على سيدنا محمد و على آله وصحبه و من تبعهم

بإحسان إلى يوم الدين.

لا يسعني في هذا المقام و بعد سنين قضيناها في الجامعة إلى أن أتقدم بجزيل الشكر إلى أساتذتنا الكرام الأفاضل الذين بذلوا ما في وسعهم من أجل تنويرنا بما ينفع و تأهيلنا لحياة أفضل و مقام أرفع. و أخص بالشكر و التقدير الدكتورة الفحلة مديحة التي لم تبخل علي بنصائحها و توجيهها

و كذلك نشكر كل من ساعد على إتمام هذا العمل و قدم لنا يد المساعدة وزودنا بالمعلومات اللازمة لإتمامه هذا البحث : أساتذتنا الكرام على تواضعهم

و مرافقتهم لنا بكل صدق

إلى الدكتور غريبـي علي على نصائحه المفيدة و توجيهاته القيمة

شكري موصول إلى موظفي و عمال المكتبة المركزية و مكتبة الحقوق

محمـــــد

قائمـــــة المختصـــرات

- ق ع ج : قانون العقوبات الجزائري
- ق م ج : ال قانون المدني الجزائري
- ج ر : جريدة رسمية
- ج م : جريمة معلوماتية
- ص : صفحة

مقدمــة

شهد عصرنا الحالي تطورا كبيرا مس مختلف مناحي الحياة الاقتصادية و الإجتماعية و الثقافية و الذي تحقق بفضل ثورات عديدة منها الثورة الزراعية و الثورة الصناعية على اثر المجهودات الفكرية و العضلية التي بذلتها البشرية من أجل تحسين المستوى المعيشي للفرد و المجتمع و السير قدما نحو الرقي و الازدهار.

و من أشهر الاختراعات التي توصل إليه الإنسان عبر سنين طويلة من الإستثمار الضخم و البحث المضني، هو الحاسب الآلي ، و كان استعماله مقتصرا و محتكرا أولا على الجهات العسكرية ثم الحكومية، فالمؤسسات الكبرى، فالطبقات الراقية من المجتمع، ثم الإدارات العمومية و المؤسسات، نظرا لتكلفته الباهظة و تعقيدات استعماله من طرف الأشخاص.

هذه الثورة المعلوماتية، أحدثت نقلة نوعية في المجتمع و حولته من المجتمع التقليدي، المتباعد إلى المجتمع المعلوماتي المتقارب ، و وفرت على الإنسان الوقت و المال و الجهد الذي كان يبذله في سبيل تحصيل المعلومة و تدوينها على الورق ، فأصبحت تعالج بصفة رقمية.

لقد أصبحت المعلوماتية علما قائما بذاته، و أدى استعمالها إلى تدفق كم هائل من المعلومات، تم توظيفها و معالجتها بفضل إنتاج و تطوير البرمجيات، و القيام بمختلف العمليات في بيئة رقمية يطلق عليها المعالجة الآلية للمعلومات، و التي تعرف لدى الدارسين بالنظام المعلوماتي.

و في هذا المجال تسابقت الدول إلى اكتساب هذه التكنولوجيا من اجل توظيفها و استغلالها في مختلف المجالات الاقتصادية و الاجتماعية و الطبية و الثقافية و السياسية... لما تمتاز به من تسهيلات من حيث الدقة و السرعة في جمع و تخزين و معالجة و استرجاع و تبادل المعلومات بين الأشخاص، حيث أصبحت هذه المعلومات تحمل أسرارهم الشخصية أو طبيعة معاملاتهم المختلفة المالية منها على الخصوص و الاقتصادية كالبيع و الشراء الإلكتروني و الأسهم، كما تعتبر هذه المعلومات وعاء أسرار الدولة و المؤسسات الاقتصادية و البنوك.

هذا التطور في مجال الإعلام و الاتصال و ما حققه من منافع كبيرة للبشرية، عبر مراحل عديدة من العمل المتواصل و البحث من طرف علماء و خبراء، رافقه بروز خبراء جدد لم تعهدهم البشرية من قبل يتمتعون بالخبرة و الحرفية في تطوير هذه التقنية للقيام بأعمال إجرامية أفرزت إلى جانب الجريمة التقليدية جرائم معاصرة، و حولت هذه الجريمة من صفتها العادية و أبعادها المحدودة، إلى أبعاد جديدة تستعمل التقنية في تنفيذ الفعل المجرم و بأساليب مبتكرة و طرق جديدة لم تكن معروفة من قبل أصبحت تهد النظام المعلوماتي و التسبب في خلق شلل كامل للأنظمة المدنية و العسكرية، الأرضية و الفضائية و تعطيل المعدات الإلكترونية و اختراق النظم المصرفية، و إرباك حركة الطيران و شلل محطات الطاقة و غيرها بواسطة قنابل موقوتة ترسل عن طريق الكمبيوتر على مسافات تتعدى الحدود، و دون أن يترك المجرم المعلوماتي اثر ملموسا للملاحقة أو معرفة مصدر ارتكاب الجريمة.

فعبر الإبحار في الشبكة المعلوماتية يستطيع المجرم أن يصل إلى أي مكان في العالم، و يتصل و يتفاعل مع من شاء متى شاء و كيف ما شاء فلا مكان و لا زمان يستطيع وضع حدود لهذه الشبكة.

لقد احدث هذا التطور تقاربا مفروضا بين الدول بحكم العولمة و المصالح المشتركة رغم الفوارق و الاختلاف الإيديولوجي و النظام السياسي المتبع. و الجزائر شانها شان باقي الدول لم تكن في منئ عما يحث في العالم، حيث سعت منذ استقلالها إلى رفع تحديات على مختلف الأصعدة عن طريق جلب الخبرات و التكنولوجيا و تعميمها في جميع القطاعات و خاصة ما تعلق بمجال المعلومات الذي عرف تطورا عبر عدة مراحل، فمنذ سنة 1970 اعترفت الدولة بالرهانات الكبرى الخاصة بمستقبل البلاد في مجال المعلوماتية، فبادرت إلى إنشاء المعهد الوطني للأعلام الآلي (INI) و مركز التكوين و البحث في الإعلام الآلي(CERIST) من اجل إثبات مكانتها بين البلدان النامية في مجال المعلوماتية بإنشاء المؤسسات و الحصول على النتائج عن طريق التكوين، و تصميم نظم المعلوماتية و انجاز البرمجيات و حتى تركيب العتاد الخاص بالإعلام الآلي.

و قد سمحت هذه السياسة من الانطلاق في إدخال النظام المعلوماتي على التسيير داخل المؤسسات و الإدارات و انجاز أولى شبكات التسيير المعلوماتي مركز الحساب الجاري(CCP) ،شركة سوناطراك، الخطوط الجوية الجزائرية، و الخطوط الجوية الجزائرية و تكوين مئات المهندسين و التقيين في الإعلام الآلي.

و قد أصبحت الجزائر جزئا لا يتجزأ من المنظومة المعلوماتية العالمية و الافتراضية الرقمية و زادت حدودها اتساعا و لم تعد تلك الحدود المتعارف عليها دوليا، بل أصبحت افتراضية و الجريمة لم تعد تلك الجريمة التقليدية المتعارف عليها بل ازدادت خطورتها و انتقلت عبر شبكة الإنترنت و تفشت و أصبحت تؤرق الجميع.

و لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة المعلوماتية، حيث تعدَّدت ألفاظ ومفردات وصِيَغ و مصطلحات تعريفها، فأُطْلِقَ على عليها مسمَّى الجرائم المستحدثة و جرائم إساءة إستخدام تكنولوجيا المعلومات و الإتصال، و جرائم الكمبيوتر والإنترنت و الجرائم المعلوماتيّة و الجرائم الرقمية و الجريمة السيبيرية.

و تتمثل خطورة هذه الجرائم المتعددة الصور و الأشكال، في أنها عابرة للحدود سهلة الارتكاب و صعبة الإثبات، لا تتطلب الجهد و العنف و تتم بسرعة و سرية ، بالإضافة إلى ما يتميز به المجرم الم‌علوماتي من ذكاء و معرفة تقنية و الذي وجد ضالته في هذه البيئة الرقمية و وسط معلوماتي منفتح، و له دوافع لارتكاب هذا النوع من الجرائم كالرغبة في تحقيق مكاسب مالية خاصة إذا علمنا أن المعلومة في حد ذاتها ثروة، أو من اجل إثبات الذات أو دواع سياسية كالهجمات التي حدثت بين حزب الله و إسرائيل أو نشر الأفكار و الآراء و الرسائل الاحتجاجية عن طريق مجموعات الأنونيموس كما حدث في تونس و مصر و غيرها من الدول أثناء ما سمي بثورات الربيع العربي.

فهذه الجريمة مست كل الجوانب الأخلاقية الفكرية السياسية و الاقتصادية خاصة المعلومة التي تعد مالا لأصحابها، و هي تكبد العالم في كل لحظة خسائر كبيرة، فحسب بعض الإحصائيات فإن الاقتصاد العالمي يتضرر جراء الجريمة الإلكترونية تريليون دولار سنويا، حيث أصبحت هذه الجريمة تمثل ضريبة عن ممارسة الأعمال المعتمدة على الانترنت.

و أمام تفشي هذه الظاهرة و استفحالها، و التي فرضت تحديات جديدة للمنظومة القانونية على المستوى الدولي، كان لا بد من تظارف الجهود الدولية للبحث عن وسائل كفيلة بمكافحتها، عن طريق عقد الاتفاقيات و إقامة المؤتمرات و الندوات و الملتقيات و سن التشريعات، من قبل العديد من الهيئات الدولية على رأسها منظمة الأمم المتحدة من خلال مؤتمراتها(المؤتمر السابع 1985-المؤتمر الثاني عشر 2010)، كما كان للمنظمة العالمية للملكية الفكرية دور بارز في هذا المجال، و ذلك من خلال خلقها لنصوص قانونية خاصة بحماية برامج الحاسب الآلي و هذا من خلال المادة 04 و 05 من اتفاقية تريبس. و اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية سنة 2001، أما على المستوى العربي فكانت الاتفاقية العربية لمكافحة جرائم المعلومات بالقاهرة لسنة 2010، بالإضافة إلى المؤتمر الأول و الثاني لمكافحة جرائم تقنية المعلومات (2002 و 2008) بالإمارات، و مؤتمر التحديات التشريعية في عصر تكنولوجيا المعلومات و الإتصال(2009) بالقاهرة و المؤتمر المغاربي الأول حول المعلوماتية و القانون (2009) بليبيا، هذا على المستوى الدولي و الإقليمي، أما على المستوى الوطني و نتيجة للنمو المتسارع لإستعمال المعلوماتية و التي ينمو معها الإجرام المعلوماتي و يتفشى، فقد بادر المشرع بالإسراع إلى التصدي لهذه الظاهرة عن طريق سد الفراغ التشريعي من خلال القانون رقم 04-15 المؤرخ في 2004/04/11 المعدل و المتمم لقانون العقوبات الذي ينص على الحماية الجزائية للأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، إضافة إلى إصداره للقانون رقم 09-04 المؤرخ في 2009/08/05 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها. محاولا بذلك وضع إطار قانوني يتلاءم مع خصوصية الجريمة الافتراضية و يجمع بين القواعد الموضوعية و الإجرائية و كذا القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و التعرف على مرتكبيها.

و من هنا يبرز **سبب اختياري للموضوع** و هي الرغبة و الفضول في اكتشاف هذه الظاهرة المستجدة نسبيا و ما تنطوي عليه من غموض و معرفة أبعادها و مخاطرها و التي

لا تزال موضوع الإهتمام و البحث و الدراسة نظرا لتطورها المرتبط بتطور المعلوماتية، كذلك لاكتساب ثقافة تقنية و قانونية تمكنني من الاحتراز و الوقاية منها.

و من خلال ما سبق ذكره تتجلي **أهمية الموضوع** في الخطورة و الخصوصية التي تميز الجريمة المعلوماتية كونها تحدث في عالم افتراضي و وفق تقنية معقدة و بوسائل متطورة، عن طريق الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات و التلاعب بمعطيات اللآلي بنشر الفيروسات و إتلاف البرامج و تزوير المستندات و مهاجمة المراكز المالية و البنوك و نشر الشائعات و النيل من هيبة الدولة و الاعتداء على خصوصية الأفراد. و تزداد أهمية الموضوع للأثر الجسيم على الاقتصاد الوطني المتنامي، كل هذا يتطلب ضرورة رصد آليات قانونية كفيلة لمعالجتها و تجنب الآثار المترتبة عنها.

و نهدف من خلال هذه الدراسة الى التعريف بالجريمة المعلوماتية و خصوصيتها و صورها و المخاطر المترتبة عنها و الوقوف على الآليات التي رصدها المشرع لمكافحتها و مدى فعاليتها في كبح جماحها و مسايرة تطورها.

لا شك أنه ما من موضوع جدير بالدراسة و البحث إلا و **تكتنفه صعوبات** في سبيل تحقيق ما يصبو إليه الدارس من نتائج و لو جزئية لاستكمال بحثه و من الصعوبات التي اعترضتني ارتباط الموضوع بجوانب تقنية و مصطلحات مختلفة متعلقة بالتكنولوجيا المتطورة و ما تتسم به من صبغة علمية بحتة، تتطلب جهدا و وقتا إضافيين، بالإضافة إلى نقص المراجع التي تناولت الموضوع، و كذا ندرة المراجع التي تناولت الجريمة المعلوماتية من الجانب الجانب الاقتصادي.

و قد استعنا في دراستنا هذه ببعض **البحوث السابقة** في جانب من موضوعنا، منها مذكرة لنيل شهادة الماجستير في القانون الدولي بعنوان "الجريمة المرتكبة عبر الأنترنت" من انجاز صغير يوسف لسنة 2013، و مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، سوير سفيان بعنوان الجريمة المعلوماتية 2011، و كذلك أطروحة لنيل شهادة الدكتوراه علوم قانونية في القانون الخاص بعنوان الأسرار المعلوماتية و حمايتها الجزائية" من انجاز رابحي عزيزة لسنة 2018.

و مع مرونة الجريمة المعلوماتية و تعدد صورها و سرعة انتشارها و جمود النصوص التقليدية و قصورها و عجزها عن ضبطها و كبح جماحها نطرح الإشكال التالي :

إلى أي مدى وفق المشرع الجزائري في مكافحة الجريمة المعلوماتية؟ و ما أثر ذلك على الاقتصاد الوطني؟

منهج الدراسة

و للإجابة على هذه الإشكالية اعتمدت على بعض المناهج الملائمة لطبيعة الموضوع منها المنهج الإستقرائي في جمع المادة العلمية من مختلف المراجع ذات الصلة ثم المنهج الوصفي و التحليلي لوصف الظاهرة و بيان المفاهيم القانونية و شرحها

متبعاً في ذلك خطة ثنائية الفصول، حيث خصصت الفصل الأول إلى **الإطار المفاهيمي للجريمة المعلوماتية** من خلال تناول مفهوم الجريمة في المبحث الأول و خصائصها و أنواعها في المبحث الثاني أما الفصل الثاني فتطرقنا من خلاله إلى **الآليات الموضوعية لمكافحة الجرائم المعلوماتية** في مبحثين المبحث الأول خصص لآليات المكافحة في قانون العقوبات أما المبحث الثاني فتناول لآليات المكافحة في بعض القوانين الخاصة، و أنهيت البحث بخاتمة تضمنت النتائج المتوصل إليها و اقتراح بعض التوصيات.

بالرغم من المزايا التي جاءت بها ثورة المعلوماتية باستعمال أجهزة الإعلام الآلي المتطورة و شبكة الانترنت، في جميع المجالات الاقتصادية و الاجتماعية و التي ساهمت في آدائها و تطويرها ، إلا أنها أحدثت كذلك تطورا في الجرائم التقليدية و ذلك عن طريق الاستخدام السيئ لهذه التكنولوجيا، حيث استغلها البعض لمآرب أخرى بارتكابهم جرائم لها علاقة بهذا المجال، عرفت بالجريمة المعلوماتية و نظرا لحداثة هذه الجريمة و تطورها المستمر، فقد اختلف الفقه في وضع تعريف موحد لها، كما اتسمت بمجموعة من الخصائص، و عرفت نوعا جديدا من المجرمين لهم عدة دوافع لارتكابها و سأحاول التطرق في هذا الفصل إلى مفهوم الجريمة المعلوماتية في المبحث الأول، و بيان خصائص و أنواع الجريمة المعلوماتية في المبحث الثاني.

المبحث الأول : مفهوم الجريمة المعلوماتية

من خلال هذا المبحث سأحاول التطرق إلى التعاريف المختلفة للجريمة المعلوماتية و كذا الأركان التي ترتكز عليها و بيان الدوافع المؤدية لارتكابها، نظرا لطبيعتها الخاصة باعتبارها تقع في العالم الافتراضي، على خلاف الجريمة التقليدية التي تقع في الواقع الملموس، و ذلك من خلال المطلبين المواليين:

المطلب الأول : تعريف الجريمة المعلوماتية و أركانــها

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة المعلوماتية، حيث تعدَّدت ألفاظ ومفردات وصِيَغ ومصطلحات تعريفها، فأُطْلِقَ على عليها مسمَّى الجرائم المستحدثة و جرائم إساءة إستخدام تكنولوجيا المعلومات و الإتصال، و جرائم الكمبيوتر والإنترنت و جرائم الحاسب الآلي (Computer Crimes)، و جرائم التقنية العالية (High-tech) الجرائم المعلوماتيّة (Information Crimes)، و الجرائم الرقمية (Digital Crimes) و الجريمة السيبيرية (Cyber Crime) ، و الجرائم الناعمة [1](Soft Crimes) و الجرائم النظيفة.[2] (Crimes Clean).

---

[1]. فهي جرائم لا تتصف بالعنف أو القوة عند ارتكابها، و لكنها تتسم بلمسات بسيطة لا تستغرق ثوان معدودة. انظر: د. ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، مجلة العدل، العدد 31 رجب 1427.

[2]. و ذلك لصعوبة اكتشاف دليل ثبوتها؛ فلا أثر فيها لأيَّ عنف أو دماء، و إنما مجرد أرقام و بيانات. انظر: محمد علي العريان، الجرائم المعلوماتية، (ص35- 36)، نقلا عن أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، 19- 20 يونيو،2007، المملكة المغربية (ص52).

و تجدر الإشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الأنترنت، فبينما تتحقق الأولى بالإعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه والمعلومات المخزنة به، فإن جرائم الأنترنت تتحقق بنقل المعلومات و البيانات بين أجهزة الحاسب الآلي عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميدانين الحوسبة و الإتصالات وظهور مصطلح Cyber Crimeأو Information Crime. كما أن للجريمة المعلوماتية أركان لا تقوم الجريمة إلا بتوافرها، وهذا ما سأتناوله في الفرعين المواليين.

الفرع الأول : تعريف الجريمة المعلوماتية

من الملاحظ انه لا يوجد اتفاق على مصطلح معين للدلالة على ظاهرة الجريمة المعلوماتية كونها من الظواهر الحديثة لارتباطها بتكنولوجيا المعلومات و الإتصالات و أجهزتها المختلفة و لذلك من الصعوبة و ضع تعريف لهذه الظاهرة خشية حصرها في مجال ضيق في ظل التطور المعلوماتي الحاصل على مستوى العالم و سنحاول عرض بعض التعاريف الفقهية باتجاهيها الضيق و الموسع في بندين و نخصص البند الثالث للتعريف القانوني لهذه الظاهرة.

البند الأول : التعريف الواسع للجريمة المعلوماتية

هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية و بالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، و ذلك باستخدام شبكات الأنترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الاجتماعية قصد إلحاق الضرر بالفرد أو المجتمع أو الدول لاستهداف أمنها العسكري أو الاقتصادي عن طريق التوغل و كشف الأسرار و نشر معلومات و تسريبها لأطراف معينة و سنعرض التعريفات التي وردت في هذا المفهوم:

" كل سلوك إجرامي يتم بمساعدة الكمبيوتر" أو هي" كل جريمة تتم في محيط أجهزة الكمبيوتر " أو هي " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".[1]

[1] . خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، الإسكندرية، طبعة أولى 2011، ص 357

أو هي : " كل فعل أو امتناع عمدي، ينشأ عن الإستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الإعتداء على الأموال أو الأشياء المعنوية"[1].

و يعطي الخبير الأمريكي Parker مفهوما موسعا للجريمة المعلوماتية بقوله : " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل"[2]

و يعرف الأستاذ Le Stanc, Vivant الجريمة المعلوماتية أنها :" مجموعة من الأفعال المرتبطة بالمعلوماتية و التي يمكن أن تكون جديرة بالعقاب".

و من التعريفات الموسعة ما يقوله الفقيهان Credo، Micel من أن سوء استخدام الحاسب أو جريمة الحاسب تشمل كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحساب المجني عليه أو بياناته كما تمتد جريمة الحاسب ذاته أو المعدات المتصلة به و كذلك الإستخدام غير المشروع لبطاقات الائتمان و انتهاك ماكينات الحاسبات الآلية بما تتضمنه من شبكات تمويل الحسابات المالية بطريقة الكترونية و تزييف المكونات المادية و المعنوية للحاسب بل و سرقة جهاز الحاسب في حد ذاته أو مكون من مكوناته "[3] .

و في تقرير الجرائم المتعلقة بالحاسوب، أقرا المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها تغيير معطيات، أو بيانات، أو برامج، أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات، أو معالجتها , و تبعا لذلك تسببت في ضرر إقتصادي، أو فقد حيازة ملكية شخص أو قصد الحصول على كسب إقتصادي غير مشروع له، أو لشخص آخر[4] . و دائما حسب أنصار هذا الإتجاه يرى البعض أن الجريمة المعلوماتية هي : " كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية

---

[1]. غانم مرضي الشمري، الجرائم المعلوماتية (ماهيتها، خصائصها، كيفية التصدي لها)، الدار العلمية الدولية للنشر و التوزيع، عمان، الأردن، ط1، 2016، ص 26

[2] . محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية مصر، طبعة 2011، ص 54

[3]. غانم مرضي الشمري، نفس المرجع ص26

[4] . مليكة عطوي، **الجريمة المعلوماتية**، حوليات جامعة الجزائر، مجلة علمية، 2012 ، العدد 21 ، ص 08

الحاسوب نظاما حاسوبيا، أو شبكة حاسوبية، للوصول إلى البيانات، والبرامج بغية نسخها أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها أو جعلها غير صالحة، أو حيازتها أو توزيعها بصورة غير مشروعة" [1] .

أما بعض الفقهاء يعرفونها بأنها " كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[2]

و من خلال هذه التعاريف يتضح لنا أنها اتسمت بالعموم و تناولت موضوع الجريمة المعلوماتية من زاوية دون أخرى و لم تعطي تعريفا جامعا مانعاَ سواء بسبب خصوصية الجريمة في حد ذاتها أو الوسائل المستعملة في ارتكابها، لأن جهاز الحاسوب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه، أو الأقراص الممغنطة، أو الأسطوانات الممغنطة على سبيل المثال. و من ثم لا يمكن إعطاء و صف الجريمة على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة، و قد ترتكب الجريمة باستعمال الحاسب الآلي، من طرف شخص للإتصال بشركائه في ارتكاب جريمة السطو على بنك.و لا نكون أمام جريمة معلوماتية.

البند الثاني : التعريف الضيق للجريمة المعلوماتية

من التعريفات التي وضعها أصحاب الاتجاه المضيق أن الجريمة المعلوماتية هي " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لإرتكابه من ناحية و ملاحقته و تحقيقه من ناحية أخرى" [3] حسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة، بل كذلك لملاحقتها، و التحقيق فيها. و هذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية ، بمعنى يجب أن يتوافر قدر كبير من العلم لدى الجناة و المختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم.

---

[1]. كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية و مجتمع المعلوماتية، – الجمعية السورية للمعلوماتية – فرع حلب، 21–23 تشرين الأول، 2000 ، بدون صفحة

[2]. غانم مرضي الشمري، مرجع سابق ص26

[3]. خالد ممدوح إبراهيم، مرجع سابق ص 357

و يقترب منه تعريف David Thompson حيث يعرفها على أنها " أي جريمة يكون متطلبا لاقترافها أن يتوافر لدى فاعلها معرفة تقنية الحاسب" و هذا الفقيه إرتكز كذلك في تعريفه على توافر المعرفة بتقنية المعلومات.

يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف جريمة الحاسب Computer Crime بأنها : الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا"[1].

بينما يعرف الفقيه الألماني Tiedemann " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بإستخدام الحاسوب"[2]. حيث ارتكز التعريفان على وسيلة إرتكاب الجريمة.

و هناك من يعرفها على أنها " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية".

و هناك جانب من الفقه الفرنسي، يحاول وضع تعريف لظاهرة الغش المعلوماتي، حيث يرى الأستاذ Massa أن المقصود بالجريمة المعلوماتية : " الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"[3].

و جرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال، و هو في هذا التعريف يستخدم معيارين : أولهما الوسيلة، (بواسطة المعلوماتية) و الأصوب استعمال مصطلح (تقنية المعلومات) لأن العملية هي المعالجة الآلية للبيانات لا وسيلة تنفيذها، أما المعيار الثاني و المتمثل في معيار محل الجريمة، و المتمثل بتحقيق الربح، أي الحصول على المال فينتقد هذا الفقيه في هذه النقطة لأن الاعتداء في كثير من جرائم الكمبيوتر ينصب على المعلومات في حد ذاتها دون السعي لتحقيق الربح و دونما أن تكون المعلومات مجسدة

[1]. غانم مرضي الشمري، مرجع سابق ص29

[2]. محمد على العريان، مرجع سابق ص 54

[3]. نفس المرجع، ص 54

لأموال أو أصول، عوضا عن عدم صواب اعتبار المعلومات في ذاتها مالا ما لم يقر النظام القانوني هذا الحكم لها لدى سعيه لتوخي الحماية للمعلومات[1].

يرى بعض الفقهاء انه من أجل تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة اعتبارات هامة و هي :

- أن يكون هذا التعريف مقبول و مفهوم على المستوى العالمي .
- ان يراعي في وضع التعريف التطور السريع و المتلاحق لتكنولوجيا المعلومات و الإتصالات.
- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي.

و يقتضي الأمر عند التعرض لمفهوم الجريمة المعلوماتية تقسيم هذا المصطلح إلى مقطعين، الأول : الجريمة و الثاني المعلوماتية حيث نتناول تعريف ماهية الجريمة و ماهية المعلوماتية

عرف بعض الفقه الجريمة بأنها : " فعل أو امتناع يحظره القانون و يقرر عقوبة لمرتكبه"[2] و عرفها البعض الآخر بأنها " فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازياً[3].

أما المعلوماتية فيقصد بها المعالجة الآلية للمعلومات و هي ترجمة المصطلح الفرنسي Informatique، و تعني تكنولوجيا تجميع و معالجة و إرسال المعلومات بواسطة الكمبيوتر، و قد استعمل مصطلح traitement automatisé de données و تعني المعالجة الآلية للبيانات.

و مصطلح Télématique يعني من الناحية اللغوية " تقنيات بث المعلومات عبر شبكات اتصالات بعدية" و هي اختصار ناتج عن اندماج كل من اللفظين Informatique أي المعلوماتية، و Télécommunication أي اتصالات.

---

[1]. شرف الدين وردة، بلجراف سامية، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث و الدراسات القانونية و السياسية جامعة يحي فارس، المدية، العدد الثالث ديسمبر 2017، ص 30 .

[2] . محمد زكي أبو عامر، قانون العقوبات– القسم العام، دار المطبوعات الجامعية الطبعة الأولى 1986، ص 35

[3] .محمود نجيب حسني، شرح قانون العقوبات– القسم العام، ط 76، دار النهضة ، 1989، ص 40

البند الثالث : التعريف القانوني للجريمة المعلوماتية

عرفها التشريع السعودي من خلال نص المادة 01 من نظام مكافحة جرائم المعلوماتية السعودي، بأنها: "أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.[1]

أما المشرع الجزائري فقد اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام و الإتصال، وعرفها بموجب الفقرة(أ) المادة 02 من القانون 09-04 على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية"[2]

و بهذا يكون المشرع الجزائري قد اعتمد على دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الألية للمعطيات، كما بينها في قانون العقوبات[3] من المادة 394 مكرر إلى 394 مكرر 7 و بذلك يترك المجال واسعا لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

و حسب المشرع الجزائري فإنه قد تتحقق الجريمة المعلوماتية بمجرد أن ترتكب أو يسهلا ارتكابها عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية، حيث يشمل هذا التعريف عدد كبير من الجرائم.

الملاحظ على تعريف المشرع الجزائري أنه قد إعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية، أولها معيار وسيلة الجريمة و هو نظام الإتصالات الإلكتروني و ثانيها معيار موضوع الجريمة و هو المساس بأنظمة المعالجة الآلية للمعطيات، و ثالثها

---

[1]. هيئة الاتصالات و تقنية المعلومات، نظام مكافحة الجرائم المعلوماتية عن موقع : https://www.citc.gov.sa/ar/ ، تاريخ الإطلاع 2021/05/04. سا 18:50

[2]. القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها.

[3]. القانون 04-15 الصادر في 10 نوفمبر 2004 يعدل و يتمم الأمر 156/66 الصادر 08 جوان 1966 المتضمن قانون العقوبات، ج.ر العدد 71

معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

كما إعتمد المشرع على معيار رابع لتحديد نطاق الجريمة المعلوماتية، حيث نص على أن الجريمة المعلوماتية ترتكب في نظام معلوماتي أو يسهل إرتكابها عليه، كما ذكرنا بحيث وسع من دائرة التجريم في مجال الإجرام المعلوماتي في القانون الجزائري.

الفرع الثاني : أركان الجريمة المعلوماتية

بعد أن تطرقنا في بداية بحثنا إلى مفهوم الجريمة المعلوماتية في الفقه و التشريع نتناول في هذا الفرع أركان الجريمة المعلوماتية الأساسية و المتمثلة في الركن الشرعي و المتمثل في نصوص القانونية و الركن المادي و المتمثل في السلوكات المادية المجرمة و الركن المعنوي المتمثل في الإرادة التي يقترن بها الفعل أو القصد الجنائي للجريمة.

إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان، و التي تدخل المشرع لتجريمها بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم و العقوبة المقررة لارتكابه[1].

أولا الركن الشرعي:

و هو الصفة غير المشروعة للفعل، فالركن الشرعي عامة يعرف على أنه: " عدم إمكانية متابعة أي شخص جزائيا إلّا إذا ما وجد نص صريح يجرم السلوك المرتكب قبل ارتكابه وفقا لمبدأ الشرعية الجنائية، فلا جريمة و لا عقوبة إلا بقانون[2]. الأمر الذي من خلاله تنتج مجموعة أحكام أساسية تحمل الصفة الإلزامية و لا مجال للتخلي عنها و المتمثلة في انفراد التشريع بالتجريم، حظر التفسير الواسع للنص الجنائي الموضوعي حظر القياس في المسائل الجنائية، و عدم رجعية النص الجنائي إلا ما كان منه أقل شدة.

و انطلاقا من مبدأ الشرعية، يرى الفقه أن المعلوماتية خلقت العديد من الإشكالات من حيث تطبيق نص جنائي تقليدي شرع في زمن لم تعرف فيه المعلوماتية على سلوكات

[1] . أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومه، الجزائر، ط 10، 2011 ، ص27 .

[2]. انظر المادة 01 من القانون رقم 15/04 المؤرخ في 2004/11/10 المعدّل و المتمّم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن : قانون العقوبات ج ر عدد 71 بتاريخ 2004/11/10.

ارتكبت باستعمالها، مثل سب شخص على موقع شبكي، و كذا عدم مواكبة التشريع للتطور السريع في مجال المعلوماتية.

ثانيا الركن المادي :

ينطلق مبدأ تحديد الفعل غير المشروع و إعطائه صفة الجريمة بتحديد الركن المادي فيه، فلا جريمة دون ركن مادي، الذي يتمثل في سلوك الجاني من أجل تحقيق غاية ما و يحدّد له القانون العقاب اللازم و هو يتباين بتباين الجرائم المرتكبة من قبل الجاني، بشرط أن يكون له مظهر خارجي ملموس. و يتخد الركن المادي عدة صور بحسب كل فعل إيجابي مرتكب مثلا: جريمة التجسس الركن المادي فيها هو الحصول مباشرة على الدعامة الإلكترونية الحاوية لهذا السر أو المعلومات، كالحصول على " CD" مخزنة فيه الأسرار و الوثائق.

إن النشاط أو السلوك المادي للجريمة المعلوماتية يتطلب وجود بيئة رقمية و جهاز كمبيوتر و اتصال بشبكة الأنترنت و/أو وجود أحد البرامج الخارقة للمواقع أو الفيروسات على الحاسب[1]. و لأن الجرائم المعلوماتية تفرض أنماط جديدة فقد تغير الركن المادي عن المألوف بعض الشئ. مثلًا بصدد جريمه تسمى بـ"إعداد الفيروسات على الحاسب تمهيداً لبثها" تدخل الأعمال التحضيرية في ركن الجريمة المادي، بخلاف ما جري عليه القول في الجرائم العادية؛ لا تعتبر الأعمال التحضيرية جزء من الركن المادي للجريمة.

ثالثا الركن المعنوي :

و هو الحالة النفسية للجاني، و يطلق عليه الركن الأدبي أو الشخصي و يمكن تعريفه بأنه : "العلاقة التي تربط بين ما ديات الجريمة و شخصية الجاني مرتكبها، و هذه العلاقة هي محل الإذناب في معني استحقاق العقاب و من يوجه إليها لوم القانون و عقابه"[2]

[1]. خالد ممدوح إبراهيم، مرجع سابق ص 382

[2]. محمود نجيب حسني، النظرية العامة للقصد الجنائي،دار النهضة العربية، الطبعة الثانية، 1970 في القانون الجزائي العام ، دار هومه، الجزائر، ط 10، 2011 ، ص27 .

و يقوم الركن المعنوي في الجريمة المعلوماتية بتوافر الإرادة الآثمة لدى الفاعل للقيام بعمل غير مشروع جرّمه القانون، كسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الإجرامية المترتبة على الأفعال السابقة، فتكسب إرادة الجاني الصفة الإجرامية من العمل غير المشروع الذي له النية على ارتكابه، و هو عالم بالآثار الضارة الناشئة عنه.

المطلب الثاني : دوافع إرتكاب الجريمة المعلوماتية

إن من أهم ما يتميز به الإجرام المعلوماتي عن الإجرام التقليدي هو تقنية المعلوماتية و ثورة المعلومات و توجد العديد من الأسباب أو الدوافع لارتكاب أفعال الاعتداء المختلفة المنطوية تحت مفهوم الإجرام المعلوماتي منها الشخصية و الموضوعية و سنذكر بعضها كالأتي:

الفرع الأول : الدوافع الشخصية

من الدوافع الشخصية هناك دوافع مادية و أخرى ذهنية حيث يندفع الشخص لارتكاب الجريمة، تحت تأثير العنصر المادي لتحقيق كسب مالي أو تأثير العنصر الذهني لمآرب أخرى نفسية.

البند الأول: الدوافع المادية الربح أو كسب المال:

تعد الدوافع المادية من أهم البواعث على ارتكاب الجرائم المعلوماتية لما تحققه من كسب مادي أو ثراء، عن طريق إتاحة الإطلاع على معلومات معينة أساسية و ذات أهمية لمن يطلبها ، و قد يكون إرتكابها بسبب ضغوط الديون الناتجة من المشاكل العائلية أو الخسائر الضخمة من ألعاب القمار

مثال مبرمج يعمل لدى إحدى الشركات الألمانية على 22 شريطا تحوي معلومات بخصوص عملاء و إنتاج الشركة و قد هدد السارق ببيعها لشركات منافسة ما لم تدفع له فدية مقدارها 200 ألف دولار و قامت الشركة بدفع المبلغ من أجل استرداد الشرائط الممغنطة المسروقة بعد أن قدرت أن الخسائر التي تنشا عن إفشاء محتواها تفوق بكثير المبلغ المطلوب[1].

[1]. محمد على العريان، مرجع سابق ص 54

البند الثاني: الدوافـع الذهنيـة

هناك الكثير من الدوافع المرتبطة بذهنية مستعملي أجهزة الكمبيوتر و رواد الأنترنت قصد المتعة و التحدي و الرغبة في فهم النظام المعلوماتي و إثبات الذات. و قد تكون هذه الدوافع مجرد شغف بالإلكترونيات و الرغبة في التعلم و تحدي و قهر النظام والتفوق على تعقيد وسائل التقنية، فقد يجد الكثير من مرتكبي هذه الجرائم في اخترق الأنظمة الإلكترونية و كسر الحواجز الأمنية المحيطة متعة كبيرة و تسلية تملا أوقات فراغهم، و قد يمثل ذلك آفة نفسية يصاب بها البعض و يتفاخرون بما قاموا به من جرائم من أجل تفوقهم على الأنظمة المعلوماتية[1].

ففي الوقت تعزز فيه الهيئات و أمن أنظمة المعلومات ببرمجيات التشفير و غيرها يتسابق أصحاب الشغف الإلكتروني لخرق هذه الأنظمة و إظهار تفوقهم عليها.

الفرع الثاني : الدوافع الخارجية لارتكاب الجريمة المعلوماتية.

قد تكون هناك دوافع أخرى غير الكسب المادي و التسلية، نتيجة مؤثرات أخرى و وجود البيئة الرقمية، تدفع بالإنسان إلى ارتكاب هذا النوع من الجرائم

البند الأول : دافع الإنتقام و إلحاق الضرر برب العمل.

قد يكون الدافع نحو ارتكاب الجريمة المعلوماتية هو عامل الانتقام و هو من أخطر لدوافع التي لارتكاب الجريمة، مثلا فصل عامل من عمله أو تعرضه لمواقف تعسفية أو الطرد من الوظيفة، من شان ذلك أن يهيئ له المناخ لارتكاب جريمته فهو يملك معلومات كثيرة عن المؤسسة التي يعمل بها، فيتولد لديه الرغبة في الانتقام من رب العمل. كان يتلاعب بالبرامج المعلوماتية أو يقوم بزر فيروسات خطيرة تحدث أضرارا جسيمة.

البند الثاني : دوافع سياسية

توجد العديد من المواقع غير المرغوب فيها على شبكة الانترنت و التي تكون معادية لسياسة دولة أو اتجاه سياسي أو عقائدي معين قصد إلحاق الأذى و تشويه السمعة أو إثارة

[1]. محمد على العريان، نفس المرجع ص 83

البلبلة و تقويض النظام، و ذلك عن طريق تلفيق الأخبار و المعلومات الكاذبة و لو استناد إلى جزء بسيط من الحقيقة ومن ثم نسخ الأخبار الملفقة حولها، و تعد الدوافع السياسية من ابرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم . و أصبحت شبكة الأنترنت مجالا خصبا للكثير من الأفراد و المجموعات لترويج الأخبار و أمور كثيرة تمس بأمن الدولة أو أحد رموزها عن طريق الذم و التشهير[1].

المبحث الثاني : خصائص و أنواع الجريمة المعلوماتية

بعد أن عرفنا في المبحث الأول مفهوم الجريمة المعلوماتية، نتطرق من خلال هذا المبحث إلى خصائص هذه الجريمة التي جعلت منها ظاهرة إجرامية جديدة ، لم يعرفها العالم من قبل سواء من حيث خطورتها أو حجم الأضرار التي تنشأ عنها حيث تطال الفرد في كيانه و الموئسة في اقتصادها و البلد في أمنه كما أنها تستعمل التقنية الحديثة ليسهل ارتكابها و هي عابرة للحدود و لا تتطلب عنفا و لا تترك أثراً، و سنتناول في المطلب الأول خصائص الجريمة المعلوماتية و نتطرق إلى أنواعها في المطلب الثاني.

المطلب الأول : خصائص الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من الجرائم المستحدثة التي أتت بها التقنية الحديثة في مجال المعلوماتية و الإتصال لذلك فهي تتميز بخصائصها عن الجريمة التقليدية المرتكبة في العالم الملموس، كما أن لمرتكبيها خصائص تميزهم عن غيرهم من المجرمين في عالم الإجرام و سوف نتناول في هذا المطلب كل من سمات الجريمة المعلوماتية و سمات المجرم المعلوماتي.

[1]. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، 2013، ص 40

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.

من أهم خصائص الجريمة المعلوماتية :

أولا : الجرائم المعلوماتية تتطلب وجود حاسب آلي

يعني ذلك وجود الحاسب الآلي و أن يستعان به كوسيلة لتنفيذ هذه الجرائم [1]. حيث أن الحاسب الآلي يعد أداة أساسية لتمكين الشخص من الدخول على شبكة الإنترنت و قيامه بتنفيذ جريمته أي كان نوعها عبر شبكة الإنترنت. فهذه الجريمة ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية، و أجهزة و معدات، (Hardware) وتجهيزات الحاسب الآلي، بمعنى تتم بواسطة المكونات المادية للحاسوب و مكوناته المعنوية البرمجيات (Software).

ثانيا : الجريمة المعلوماتية متعدية للحدود أو جريمة عابرة للدول (Transnational):

تتسم الجريمة المعلوماتية بالطابع الدولي الذي لا يعترف بالحدود الجغرافية، فالمجتمع متفتح و في اتصال دائم على الخط On line عبر شبكات تخترق الزمان و المكان بفضل شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام عملية نقل المعلومات عبر مختلف دول المعمورة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم، مثل التعدي على قواعد البيانات، و تزوير و إتلاف المستندات الإلكترونية و الاحتيال المعلوماتي، و سرقة بطاقات الائتمان، و القرصنة، و غسيل الأموال[2].

فأصبح المجرم المعلوماتي بفضل هذه التقنية التي قربت المسافات يقوم بالفعل الإجرامي دون عناء التنقل إلى مسرح الجريمة، فقد يكون الجاني في بلد و المجني عليه بلد

[1]. غانم مرضي الشمري، الجرائم المعلوماتية (ماهيتها، خصائصها، كيفية التصدي لها)، مرجع سابق ص 38

[2]. خالد ممدوح إبراهيم، مرجع سابق ص 360

أخر و قد يكون الضرر المحتمل في بلد ثالث، و هو ما يعني عدم التواجد المادي للمجرم في مكان الجريمة.

و تثير عالمية الجريمة المعلوماتية إشكالات عدة من حيث القانون الواجب التطبيق و اختصاص المحاكم و الملاحقة و التفتيش و قواعد التسليم.

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)[1]، 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 و كانت المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية، و الأولى أيضا التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث(فيروس)[2].

ثالثا صعوبة إكتشاف و إثبات الجرائم المعلوماتية:

تمتاز الجرائم المعلوماتية بصعوبة الإكتشاف والإثبات و ذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فهي جرائم تتم بواسطة إدخال أرقام و رموز دقيقة يصعب إكتشافها وإثباتها لهذا عادة ما يتم إكتشافها بالصدفة .

و ترجع صعوبة إثباتها إلى عدة أمور منها :

[1]. 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,ص

[2]. سوير سفيان، الجريمة المعلوماتية، ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، جامعة أبو بكر بلقايد، تلمسان،2011، ص 20

أ. أنها لا تترك أي آثار مادية لها بع ارتكابها يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات و تداولها بالنبضات الكترونية غير مرئية و لا توجد مستندات ورقية. فهي لا تترك آثارا ملموسة و شهودا يمكن الاستدلال بأقوالهم.

ب. صعوبة الإحتفاظ الفني بدليل الجريمة المعلوماتية إذ يستطيع المجرم المعلوماتي أن يمحو أو يحرف أو يغير البيانات و المعلومات الموجودة في الكمبيوتر في وقت وجيز جدا، لذا فان المصادفة و سوء الحظ يلعب دور في اكتشافها[1]

ت. حرفية ارتكابها مما يتطلب قدرا كبير من الذكاء و المعرفة من جانب مرتكبيها و قدرا أكبر من الحرفية من جانب من يتولى الإشراف على جهود المكافحة[2].

رابعا :الجريمة المعلوماتية جريمة ناعمة

إذا كانت الجريمة التقليدية تتطلب توفر الوسائل المادية، و العنف غالبا كما هو الحال في جريمة السطو المسلح، المخدرات، و السرقة و الإرهاب.

فان الجرائم المعلوماتية توصف بأنها جرائم ناعمة أي لا تحتاج إلى العنف، فتنقل البيانات من حاسوب لآخر وسرقة الأرصدة البنكية لا يتطلب ممارسة العنف و الإيذاء و لا يشترط استعمال أو إطلاق النار على رجال الشرطة.

فالمجرم المعلوماتي يحتاج جهاز الحاسوب و يوظف مستواه التقني في أفعال غير مشروعة، عبر شبكة المعلومات الدولية، إضافة إلى الإرادة في تحقيق الغرض الإجرامي و ذلك بدون بذل أي جهد عضلي أو عنف، كالتجسس و اختراق خصوصيات الغير و التغرير بالقاصرين.

و بهذا تكون الجريمة المرتكبة عبر الانترنت من الجرائم النظيفة فلا أثر فيها لأي عنف أو دماء و إنما مجرد أرقام و بيانات و رموز يتم تغييرها في ذاكرة الحاسب الآلي دون ترك أثر مادي خارجي.

---

[1]. خالد ممدوح إبراهيم، حوكمة الإنترنت، مرجع سابق ص 363

[2]. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الإنترنت(الجرائم الإلكترونية)– دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية و الإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2007، ص32

خامسا : قلة الإبلاغ عن الجريمة المعلوماتية

لا يتم في غالب الأحيان الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها و إما خشية من التشهير. [1] كما أن معظم الأشخاص يحجمون عن الإبلاغ تحت تأثير التهديد و الابتزاز من طرف المجرمون سواء تعلق الأمر بالأشخاص العاديين أو البنوك و الشركات و مؤسسات الأعمال تجنبا للأساة إلى السمعة و هز ثقة العملاء فيها، و كذلك إخفاء أسلوب ارتكاب الجريمة خوفا من قيام آخرين بإتباع نفس أسلوب الجريمة، و عدم إبلاغ السلطات المختصة عن الجريمة في حينه يزيد من فرص إفلات المجرم المعلوماتي من العقاب.

لذا نجد أن معظم الجرائم يتم اكتشافها بعد وقت طويل من ارتكابها و عن طريق الصدفة، كما أن عدد الجرائم التي لم تكتشف هو أكبر بكثير من عدد الجرائم التي يتم اكتشافها و الإعلان عنها.

سادسا : الجريمة المعلوماتية جريمة سهلة الإركاب

يسهل ارتكاب هذه الجريمة نظرا لأنها ذات طابع تقني، كما انه من السهل إخفاء معالم الجريمة و صعوبة تتبع مرتكبيها[2].

لقد سهل تعميم استعمال وسائل المعلوماتية بلوتياد الأشخاص من مختلف المستويات للمواقع المختلفة باختلاف مقاصدهم التعليمية و الترفيهية و البحثية وقوع الكثير منهم تحت مؤثرات نفسية و أخرى خارجية تدفعنهم و تحت مغريات مختلفة إلى تحقيق مآربهم، فينصرف سلوك الكثير منهم إلى إساءة استخدام أجهزة الحاسب الآلي سواء عن قصد أو عن طريق الخطأ فينحرف سلوكهم إلى إحداث تغير في طبيعة النظام المعلوماتي القائم بإحداث أضرار بالغير بارتكاب الفعل غير المشروع الذي يجرمه القانون و المتمثل في جريمة معلوماتية.

[1]. عبد الله عبد الكريم عبد الله، نفس المرجع ص 33

[2]. نفس المرجع ص 33

سابعا : وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للنظام

من خصائص الجريمة المعلوماتية أنها تقع أثناء عملية المعالجة الآلية للبيانات و المعطيات الخاصة بالكمبيوتر و يمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام الجريمة المعلوماتية الخاصة بالتعدي على نظام معالجة البيانات، و في حالة تخلف هذا الشرط تنتفي الجريمة المعلوماتية.[1]

و قد تقع الجريمة المعلوماتية في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات أثناء عملية المعالجة، سواء عند مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج المعلومات.

و تعرف عملية المعالجة الآلية للبيانات أو المعطيات بأنها " كل مركب يتكون من وحدة أو مجموعة و حدات معالجة، و التي تتكون كلا منها من الذاكرة والبرامج والمعطيات و أجهزة الإدخال و الإخراج و أجهزة الربط، و التي يربط بينها مجموعة من العلاقات و التي عن طريقها يتم تحقيق نتيجة معينة.[2]

ففي مرحلة الإدخال حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة، و يكون من السهل إدخال بيانات جديدة لا علاقة لها بالمعطيات القائمة و محو البيانات الأساسية المطلوب إدخالها، و في مرحلة المعالجة حيث يمكن إدخال أية تعديلات عن البرنامج، يمكن التلاعب في برامج النظام المعلوماتي فيتم إدخال بيانات غير مصرح بها و أما المرحلة الأخيرة المتعلقة بالمخرجات، و فيها يتم التلاعب في النتائج التي يخرجها النظام المعلوماتي بشأن بيانات غير صحيحة[3].

---

[1]. خالد ممدوح إبراهيم، حوكمة الإنترنت، مرجع سابق ص 367

[2]. سيد طنطاوى محمد سيد، الجريمة المعلوماتية و الصعوبات التي تواجه التعاون الوطني والدولي و كيفية مكافحتها، المركز الديمقراطي العربي للدراسات الإستراتيجية،الإقتصادية و السياسية، https://democraticac.de/. اطلع عليه الثلاثاء 11 ماي 2021 سا 17:50

[3]. خالد ممدوح إبراهيم، مرجع سابق ص 369

ثامنا : خفاء الجريمة و سرعة التطور في ارتكابها

حيث لا يمكن للضحية الشعور بها و كشفها حتى أثناء تواجده على الشبكة لأنها خفية و مستترة في أغلبها و لأن الجاني يتمتع بقدرات فنية و مهارة و دقة في تنفيذها، حيث تتسم بإخفاء الجريمة و سرعة التطور في ارتكابا قد تقع أثناء وجوده على شبكة الإتصالات، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة، مثلا عند إرسال الفيروسات المدمرة و سرقة الأموال و البيانات الخاصة أو إتلافها، و التجسس و سرقة المكالمات وغيرها من الجرائم.

و كون هذه الجرائم تقع في الخفاء و تنفذ بسرعة فائقة فانها لا تترك أي اثر خارجي و مرئي لها فيصعب اثباتها و الكشف عتها في حينها،كما انها تستعمل التقنية المتطورة حيث يتم استخدام النبضات الالكترونية في نقل المعلومات.

كما أن روادها و المخططين لها على قدر من الذكاء و خبرة و دراية و احتراف في مجال تقنية المعلومات، و بالتالي يخططون بطرق محكمة تمكنهم من النجاح في ارتكاب هذه الجرائم و فرارهم من قبضة السلطات كما يستخدم المجرمون المخططون لهذه الجريمة وسائل تقنية متطورة يصعب على الغير معرفتها والتعامل معها بالاضافة الى عدم ملائمة الأدلة التقليدية في القانون الجنائي لإثبات هذه الجرائم.

و يستفيد المجرمين في مختلف أنحاء العالم مم الشبكة المعلوماتية من تبادل الخبرات و الأفكار الإجرامية فيما بينهم، عبر مواقع الكترونية ومنتديات القراصنة(Hackers).[1]

و نظرا للتطور التكنولوجي الهائل و المتسارع الذي توفر شبكة الأنترنت، جعلت وتيرة ارتكاب الجريمة و تطورها أسرع من تطور التشريعات بفارغ زمني كبير، بالإضافة إلى المؤتمرات التي يعقدها القراصنة و التي تمكنهم من ابتكار وسائل و طرق معقدة لارتكاب جرائمهم يصعب على التشريعات معرفتها و حل ألغازها و بالتالي مكافحتها.

[1]. صغير يوسف، مرجع سابق، ص 15

تاسعاً : أضرار جرائم المعلوماتية

تساير الجرائم المعلوماتية التطور المضطرد و السريع لتكنولوجيا الحاسب الآلي و الأتصال التي عم استخدامها في إدارة مختلف المعاملات الاقتصادية و المالية حيث تمس هذه الجرائم المركز الحسابي و الإداري و تنقلات الأموال والاستثمارات سواء في المنشآت العامة أو الخاصة ، كما تمس المعلومات الشخصية المخزونة في ذاكرة الحواسيب الآلية للبنوك وشركات التأمين ولدى المحامين والمستشفيات و مراكز الشرطة و الأحزاب و قد تهدد هذه الاعتداءات مباشرة قدسية وسرية الحياة الخاصة أو الحرية السياسية، ناهيك عن الخطورة التي تشكلها هذه الجرائم إذا ما تعلقت بالمعلومات الخاصة بإدارة الدولة و عمل الحكومة وخاصة في ميادين الأمن والدفاع والمشروعات النووية والتصنيع الحديث للأسلحة.

و يبدو أن هذه المعلومات هي الأكثر رواجاً في (سوق المعلومات السوداء)[1].

و عليه فالجريمة المعلوماتية تعتبر من أحدث أنواع الجرائم، مسرحها العالم الإفتراضي غير ملموس بعيدة عن أي مظهر من مظاهر الجريمة التقليدية فهي جريمة عابرة للحدود يرتكبها مجرمون ذو مستوى عالي، أذكياء و متميزون في المجال التقني، مما يؤدي إلى تشتيت الجهود الدولية في محاولة تعقبها التحري عنها، أو الوصول إلى مرتكبها.

الفرع الثانـــي : السمات الخاصة بالمجرم المعلوماتي

بعد أن عرفنا فيما سبق خصائص جرائم المعلوماتية التي تميزها عن غيرها، فان لمرتكبيها كذلك سمات و خصائص تميزهم عن سواهم من الجناة المتورطين في أنماط الانحراف الأخرى، و لعل من ابرز هذه السمات:

أولا : المعرفة و المهارة و الذكاء

فالمعرفة هي الإحاطة بكافة الظروف الخاصة بالجريمة المراد تنفيذها، و احتمالات نجاحها أو فشلها و تجنب الظروف التي يمكن أن تكشف أفعالهم، فعن طريق هذه المعرفة يرسم المجرم تصورا كاملا للجريمة في مختلف مراحلها.

[1]. عادل يوسف عبد النبي الشكري، المعلوماتية و أزمة الشرعية الجزائية، جامعة الكوفة/ كلية القانون، العدد السابع ، 2008، ص 116

كما يتمتع مجرم المعلوماتية بالمهارة و المعرفة بتقنيات الحاسوب و الإنترنت، التي اكتسبها عن طريق الدراسة المتخصصة أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلوماتية، فبعض من هؤلاء المجرمين هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ الجريمة المعلوماتية يتطلب قدرا من المهارة لدى الفاعل، بحيث يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها(محاكاة) و يكون ذلك قبل تنفيذ جريمته، حتى لا يفاجأ بأمور غير متوقعة من شأنها أن تؤدي إلى إفشال مخططات أو الكشف عنها [1].

يوصف الإجرام المعلوماتي بأنه إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم المعلوماتي إنسان على مستوى من الذكاء، إضافة إلى انه مجرم متكيف اجتماعياً لا يناصب العداء للمجتمع.[2]

و يلعب الذكاء المتمثل في المقدرة العقلية و الذهنية العميقة التي تتطلبها الجرائم المعلوماتية خاصة منها الجرائم المالية التي تلحق بالمجني عليه خسائر مادية معتبرة، حيث يتجنب المجرم المعلوماتي استخدام العنف أو الإتلاف المادي، بل يستخدم مقدرته العقلية و يحاول تحقيق أهدافه بهدوء، عكس المجرم التقليدي الذي يميل إلى العنف.

كالتلاعب في بيانات و برامج الحاسب الآلي كمسح البيانات أو تعطيل استخدام البرامج، عن طريق زرع الفيروسات أو باستخدام البرامج المنطقية أو الزمنية لكي يشل حركة النظام المعلوماتي و يجعله غير قادر على القيام بوظائفه الطبيعية.[3]

ثانيا : المجرم المعلوماتي يبرر ارتكاب جريمته

إذ يوجد شعور لدى كل مرتكب فعل إجرامي أن ما يقوم به لا يدخل في قائمة الجرائم خاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبوا هذه الجرائم بين الإضرار بالأشخاص الذي يعدونه

[1]. ريم عمیار، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي كلية الحقوق و العلوم السياسية قسم الحقوق، 2018 ، ص 19

[2]. عادل يوسف عبد النبي الشكري، مرجع سابق، ص 117

[3]. محمد على العريان، مرجع سابق، ص 78

غاية في اللاخلاقية، و بين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم .

و نجد في كثير من الأحيان أن العاملون بالمؤسسات يستعلمون الانترنت لأغراض شخصية، حيث يعتبر ذلك سلوكا شائعا بين الناس و لا ينظرون إليه انه فعلاً إجراميا و عدم الشعور بعدم أخلاقية هذه الأفعال لدى فئة كبيرة من مرتكبيها لا ينفي وجود مجرمين يرتكبون هذه الجرائم و هم على علم و أدراك بعدم مشروعية هذا الفعل.[1]

ثالثا : الخوف من كشق الجريمة المعلوماتية

الخوف من كشف أمر الجرائم صفة مشتركة بين جميع أصناف المجرمين، غير أن هذه الخشية تصاحب المجرم المعلوماتي بصفة خاصة، خوفا من فقدان المركز الوظيفي و ما يترتب عن ذلك من ارتباك مالي و تشويه للسمعة، كما أن طبيعة الأنظمة المعلوماتية تساعد الجاني على الحفاظ على سرية أفعاله، ذلك أن كثير ما يعرض اكتشاف أمره، هو أن يطرأ أثناء تنفيذ جريمته عوامل غير متوقعة لا يمكن التنبأ بها.

رابعاً الميل إلى التقليد :

يميل المجرم المعلوماتي إلى تقليد غيره داخل الوسط الذي يرتاده، إذ يكون عندئذ أسهل و أسرع انسياقا لتأثير الغير عليه، و يكون ذلك التقليد لاكتساب المهارات الفنية، مما يشجعه على اقتحام عالم المعلوماتية و التوق إلى مزيد من التفوق و فرض الذات و اكتساب مركز داخل بيئته، فيؤدي به إلى الأمر إلى ارتكاب الجريمة.

خامسا المجرم المعلوماتي مجرم عائد:

يتميز المجرم المعلوماتي بأنه عائد للإجرا م دائما، باستخدام مهاراته و خبراته و طريقة عمل الحواسيب، فهو قد لا يرتكب الجريمة بهدف الإيذاء أو سرقة البيانات، إنما هو نوع من أنوع التحدي بهدف إختبار مهاراته و رغبته في تطويرها أكثر فأكثر، خاصة ما لم يكشف أمره و لم يتم القبض عليه.

[1]. صغير يوسف، مرجع سابق، ص 34

فغالباً ما يعود إلى ارتكاب جرائم أخرى في مجال المعلوماتية قصد تدارك الأخطاء التي أدت إلى التعرف عليه و تقديمه إلى العدالة في المرة الأولى، فيؤدي ذلك إلى العود لارتكاب الجريمة فينتهي بهم الأمر في المرة الثانية إلى كشفهم و تقديمهم للمحاكمة.[1]

سادسا المجرم المعلوماتي إنسان اجتماعي:

يتميز المجرم المعلوماتي بأنه قادر على التكيف في بيئته الاجتماعية بالإضافة إلى انه لا يوقع نفسه في حالة عداء مع المجتمع الذي يحيط به فهو قادر على التوافق و التصالح مع المجتمع.

و ما يميز المجرم المعلوماتي عن المجرم التقليدي أن للمجرم المعلوماتي يعيش وسط المجتمع و يمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى، فهو إنسان اجتماعي وجِدُ متعايش في بيئته الاجتماعية لذلك فالجريمة المعلوماتية ترتكب لعدة دوافع منها دافع الكبرياء (مستخدم طرد من عمله فيقوم بارتكاب جريمته) أو دافع النصب أو الحسد أو بدافع اللهو لإظهار قدراته على التفوق على أمن الأنظمة المعلوماتية.[2]

و بالتالي فهو يكتفي بالتفاخر بين أقرانه أو لمجرد الحصول على منفعة مالية من وراء جرائمهم.

سابعاً القيام بالتخطيط و التنظيم

ترتكب أغلب الجرائم المعلوماتية في العالم الإفتراضي (شبكات الأنترنت) كما هو الحال في العالم الحقيقي من طرف أفراد أو مجموعات صغيرة ، حيث يقوم بمعظم الأعمال الإجرامية مجموعة متكونة من عدة أشخاص يحدد لكل شخص دور معين، و يتم العمل بينهم وفقا لتخطيط و تنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون أحد أعضائها متخصص في الحاسب الآلي يقوم بالجانب الفني من المشروع الإجرامي و شخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب و لتحويل المكاسب إليه.

[1]. عادل يوسف عبد النبي الشكري، المعلوماتية و أزمة الشرعية الجزائية، ص 117

[2]. محمد على العريان، مرجع سابق، ص 77

ثامنا التخصص و الاحتراف

مرتكبو هذه الجرائم لهم صفات مميزة من حيث الثقافة و العلم التكنولوجي، فالمجرم في هذا النوع من الجرائم ليس إنسانا عاديا فهو يرتكب جريمة متخصصة خاصة إذا تعلقت بسرقة معلومات مشفرة تتطلب منه خبرة تقنية عالية في هذا المجال [1]، للتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسوب كما في البنوك أو المفاعلات النووية و المؤسسات العسكرية.

تاسعا الوسيلة و السلطة :

تتمثل الوسيلة في الإمكانيات التي يتزود بها الفاعل لارتكاب جريمته، أما بالنسبة للمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية في أغلب الحالات تتميز نسبيا بالبساطة و بسهولة الحصول عليها، و قد يستطيع حتى ابتكارها نظرا لمهارته و قدرته.

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 لقد لخص الأستاذ **Parker** معظم هذه الخصائص بكلمة **S.K.R.A.M** و تعني المهارة، **Skills المعرفة Knowledge، الوسيلة Resources ، السلطة Authority** ، و أخيرا الباعث **Motives**.

و يقسم مجرمي المعلوماتية (Cyber Criminals) إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال إلي وجود عدد من الأنماط المختلفة لمجرمي المعلومات، نرصدها فيما يلى[2] :

---

[1]. عبد الله عبد الكريم عبد الله، مرجع سابق ص 32

[2]. عبد العال الديربى، المجرم المعلوماتى: تصنيفات متنوعة ومهارات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني abdelaald200594@yahoo.com،

1. المازحون (Pranksters):

و هم الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم. و من أمثلة هذة الطائفة و من بينهم فئة لم تبلغ بعد سن الأهلية مفتونين كثيرا بالتقنيات الرقمية و هم غالبا ما يكونون في مرحلة المراهقة، وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة المعلوماتية.

2. القراصنة الهواة (Hackers):

هذا المصطلح أطلقه مجموعة من طلبة الجامعات الأمريكية على من يتميزون بقدر عال من الكفاءة و التقنية و اغلبهم من صغار السن و لهم شغف بعلوم الحاسبات و تقنياته[1].

و يقوم هؤلاء بالدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول إليها لكسر الحواجز الأمنية بهدف اكتساب الخبرة و بدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذة الأنظمة.

فعلى سبيل المثال خرق استشاري تقنية معلومات أحد الأنظمة الأممية للإنترنت البريطانية لمجرد كشف القنوات الأممية بها و لقد نجح في الحصول على أسماء لأكثر من 24 ألف شخص وعناوينهم وكلمات السر و معلومات البطاقات الإئتمانية من بينهم خبراء عسكريون و موظفون حكوميون وكبار مديري الشركات[2].

3. القراصنة المحترفون (Crackers):

هم أشخاص تتراوح أعمارهم ما بين 25 و40 سنة و غالبا ما يتم ارتكاب هذه الجرائم المعلوماتية من أشخاص يعملون في منشأة ما، أو مسؤولون عن أنظمة معلوماتية، فهم يملكون المعرفة اللازمة و التقنية الكافية للتلاعب بالحاسبات الآليةّ، و عندئذ يقومون بتنفيذ

[1]. غانم مرضي الشمري، مرجع سابق ص 42

[2]. ريم عمیار، مرجع سابق ص 24

أفعالهم غير المشروعة بأنفسهم أو بمشاركة أو مساعدة أشخاص آخرين سواء كانوا فنيين أو مجرد وسطاء[1].

فهدفهم سحب الأموال من الأرصدة، و الوصول إلى أخطر المواقع و أكثرها حساسية و اختراقها و التلاعب ببياناتها، فهذه الفئة من المجرمين وبالنظر إلى السلوكات المرتكبة من طرفهم نجد أن لهم ميول إجرامية خطيرة و واضحة، تفصح عن رغبتهم في إحداث التخريب و السرقة و النهب.

4. **القراصنة المجرمون (Malicious Hackers):**

و هم أشخاص هدفهم إلحاق خسائر بالمجني عليهم، دون أن يكون الحصول على مكاسب مالية ضمن هذة الأهداف، و يندرج تحت هذة الطائفة الكثير من مخترعي فيروسات الحاسبات الآلية و موزعيها.

5. **ممتهنوا الإجرام (Career Criminals):**

هم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية و يعمل المنتمون لهذه الطائفة في أغلب الأحوال بطريقة منظمة حيث ينطبق على أفعالهم وصف الجريمة المنظمة.

و هم مجرمي المعلوماتية الذين يهدفون من وراء نشاطهم الاجرامى تحقيق ربح مادي بطريق غير مشروع، و يقترب المجرم المعلوماتى من هذه الطائفة في سماتة إلى المجرم التقليدي.

6. **المتجسسين**

و تقوم هذه الفئة بالعمل على سرقة الأسرار الاقتصادية و السياسية، و يندرجون في عداد مجرمي المعلوماتية، فهم يسرقون معلومات سرعان ما تتحول إلى أموال، بعد بيعها أول استخدامها أذا كانت هذه المعلومات تتمثل في رقم بطاقة ائتمان على سبيل المثال أو رقم استخدام إحدى شبكات الحاسب الآلي، كما أنهم لا يتورعون في عرض أي سر من الأسرار قد يحصلون عليه بالصدفة للبيع.

[1]. محمد على العريان، مرجع سابق، ص 80

و قد تمكن بعضهم من الدخول إلى هاتف سكوتلانديارد و هو المقر الرئيسي للبوليس البريطاني و اجروا مكالمات هاتفية على حساب هذا الهاتف و شبكته وصلت إلى مبلغ مليون دولار أمريكي[1].

7. المدافع المتطرف (Extreme Advocates)

تتكون هذه الفئة من الجماعات الإرهابية أو المتطرفة، و التي تتبنى معتقدات و أفكار اجتماعية أو سياسية أو دينية، و يحاولون فرضها باللجوء إلى النشاط الإجرامي، و استعمال العنف من أجل لفت الأنظار إلى ما يدعون إليه. و مع التطور التكنولوجي و امتلاكهم للوسائل العصرية في مجال تقنية المعلومات و الإنترنت اتجه اهتمامهم إلى نوع جديد من النشاط الإجرامي ألا و هو الجريمة المعلوماتية.

و بما أن المؤسسات المختلفة داخل الدول تعتمد على أنظمة الحاسبات الآلية في إنجاز أعمالهما و ما تمثله المعلومات التي تحتويها من أهمية، جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات. لأحداث الخسائر المعتبرة بهذه المؤسسات و لفت الأنظار إلى أفكارها و معتقداتها.

[1]. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية المعلوماتية)، دار الفكر الجامعي، الإسكندرية، مصر، الطبعة الأولى 2007، ص 143

المطلـــب الثانـــي : أنـــواع الجرائـــم المعلوماتية

تعتبر الجريمة المعلوماتية من الجرائم المستحدثة و هي تستهدف العديد من القطاعات، ممّا جعل تصنيفها من قبل الفقهاء يتميّز بالصعوبة على عكس الجرائم التقليدية التي يمكن تصنيفها بسهولة.

و لم يستقر الفقهاء على معيار واحد لتصنيف الجريمة المعلوماتية و ذلك لتشعب هذه الجرائم و سرعة تطوّرها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة أو دافع المجرم، أو على أساس محل الجريمة.

و على هذا الأساس نعتمد في تقسيم هذا المطلب على مختلف معايير التصنيف و هي الجرائم الواقعة على الأموال و الجرائم الواقعة على الأشخاص(الفرع الأول) ثم الجرائم الواقعة على أمن الدول(الفرع الثاني.)

الفرع الأول : جرائم تسبب الأذى للأفراد و للمؤسسات.

أولا : جرائم تسبب الأذى للأفراد

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

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

و من خلالها يتم استهداف فئة من الأفراد أو فرد بعينه من أجل الحصول على معلومات هامة تخص حساباته سواء البنكية أو على الإنترنت، و تتمثل هذه الجرائم في:

1. **انتحال الشخصية :**

و يقصد بانتحال الشخصية ما يعمد إليه المجرم من استخدام شخصية شخص أخر للإستفادة من سمعنه أو ماله أو صلاحياته [1]. و قد يكون انتحال شخصية الفرد أو شخصية المواقع.

و فيها يستدرج المجرم الضحية و يستخلص منها المعلومات بطرق غير مباشرة و يستهدف فيها معلومات خاصة من أجل الإستفادة منها و استغلالها لتحقيق مكاسب مادية أو التشهير بسمعة أشخاص بعينهم، و إفساد العلاقات سواء الإجتماعية أو علاقات العمل.

2. **تهديد الأفراد:** يصل المجرم من خلال القرصنة وسرقة المعلومات إلى معلومات شخصية وخاصة جداً بالنسبة للضحية، ثم يقوم بابتزازه من أجل كسب الأموال و تحريضه للقيام بأفعال غير مشروعة قد يصاب فيها بأذى.

3. **تشويه السمعة :**

يقوم المجرم باستخدام المعلومات المسروقة وإضافة بعض المعلومات المغلوطة، ثم يقوم بإرسالها عبر الوسائط الإجتماعية أو عبر البريد الإلكتروني للعديد من الأفراد بغرض تشويه سمعة الضحية و تدميرهم نفسياً.

ثانيا : جرائم تسبب الأذى للمؤسسات.

1. **اختراق الأنظمة:**

و تتسبب الجرائم المعلوماتية بخسائر كبيرة للمؤسسات و الشركات المتمثلة في الخسائر المادية و الخسائر في النظم، بحيث يقوم المجرم باختراق أنظمة الشبكات و الحصول على معلومات قيمة خاصة بأنظمة الشركات، و من ثم يقوم باستخدام ها في سرقة الأموال و تدمير أنظمة الشركة الداعمة في عملية الإدارة ، كما يمكن سرقة المعلومات الخاصة بموظفين المؤسسات و الشركات و تحريضهم و ابتزازهم من أجل

[1]. صغير يوسف، مرجع سابق، ص 50

تدمير الأنظمة الداخلية للمؤسسات، و تثبيت أجهزة التجسس على الحسابات و الأنظمة و السعي لاختراقها و السيطرة عليها لتحقيق مكاسب مادية وسياسية.

و تؤثر الجرائم المعلوماتية الخاصة باختراق الشبكات و الحسابات و الأنظمة بشكل سلبي على حالة الإقتصاد في البلاد، كما تهدد الأمن القومي للبلاد إذا ما لم يتم السيطرة عليها و مكافحاتها ، و تمثل الجرائم المعلوماتية أكبر نسبة حول العالم ، و هي في تزايد مستمر مما يشكل خطورة على المجتمع، بسبب الإنتهاكات و اختراق الأنظمة و الحسابات. و يعود ذلك لضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات و الشبكات.[1]

2. تدمير النظم:

عن طريق الفيروسات الإلكترونية والتي تنتشر في النظام وتسبب الفوضى والتدمير، ويتسبب ذلك في العديد من الخسائر المرتبطة بالملفات المدمرة ومدى أهميتها في إدارة وتنظيم الشركات و المؤسسات.

و يتم كذلك من خلال اختراق حسابات الموظفين بالمؤسسة الخاصة بالشبكة المعلوماتية للمؤسسة و الدخول على الحسابات جميعاً في نفس ذات الوقت، و يتسبب ذلك في عطل تام للخادم مما يؤدي إلى تدميره و بالتالي تعطل الأعمال بالشركات و المؤسسات.

[1]. غانم مرضي الشمري، مرجع سابق ص 86

الفرع الثاني : جرائـــم تمس الأمـــوال و أمن الدولة

أولا : جرائـــم الأمـــوال

1. **الإستيلاء على حسابات البنوك:**

و هي اختراق الحسابات البنكية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات الخاصة، كما يتم أيضاً سرقة البطاقات الإئتمانية، و من ثم الإستيلاء عليها و سرقة ما بها من أموال.

2. **انتهاك حقوق الملكية الفكرية والأدبية:**

و هي صناعة نسخ غير أصلية من البرامج وملفات الملتيميديا ونشرها من خلال الإنترنت، ويتسبب ذلك في خسائر فادحة في مؤسسات صناعة البرامج والصوتيات.

ثانيا : الجرائم التي تستهدف أمن الدولة.

1. **برامج التجسس :**

تنتشر العديد من برامج التجسس والمستخدمة في أسباب سياسية و اقتصادية [1] و التي تهدد أمن وسلامة الدولة، ويقوم المجرم بزرع برنامج التجسس داخل الأنظمة الإلكترونية للمؤسسات، فيقوم أعداء الوطن بهدم أنظمة النظام والإطلاع على مخططات عسكرية تخص أمن البلاد، لذلك فهي تعتبر من أخطر الجرائم المعلوماتية.

2. **استخدام المنظمات الإرهابية لأسلوب التضليل:**

و يعتمد الإرهابيون على استخدام وسائل الإتصال الحديثة وشبكة الإنترنت من أجل بث ونشر معلومات مغلوطة، والتي قد تؤدي لزعزعة الإستقرار في البلاد وإحداث الفوضى من أجل تنفيذ مصالح سياسية ومخططات إرهابية، وتضليل عقول الشباب من أجل الإنتفاع بمصالح شخصية.

[1]. عبد الفتاح بيومي حجازي، مرجع سابق، 2007، ص 142

خلاصة الفصل الأول

تناولنا في هذا الفصل الإطار المفاهيمي للجريمة المعلوماتية من خلال تعريفها حسب تناولها من جانب الفقه الذي لم يتفق في إعطاء تعريف جامع مانع لها نظرا لخصوصيتها و ما يميزها عن الجريمة التقليدية ، من حيث حداثتها و مرونتها و الاستمرارية و السرعة في التطور. فهناك جانب من الفقه ضيق من مفهومها و يعاب عليه أنه وضع المشرع في زاوية ضيق مقارنة مع طبيعة الجريمة الخاصة التي تتطلب الإحاطة بها من مختلف جوانبها بينما الإتجاه الموسع لمفهومها كان تحسبا لاحتواء أي تغيير أو تطور يحدث في شانها

و قد المشرع الجزائري في هذا الإتجاه بالإضافة إلى اعتماده على معايير أخرى جريمة، كما تطرقنا إلى صور و أنواع هذه الجريمة وسمات المجرم المعلوماتي وكذا أساليب و دوافع ارتكاب الجريمة المعلوماتية.

بعد أن تطرقنا في الفصل الأول لظاهرة الجريمة المعلوماتية و حاولنا إبراز مفهومها و الدوافع المؤدية لارتكابها و خصائصها و كذا سمات مرتكبيها و الصور التي تتخذها نحاول في هذا الفصل التطرق للجانب الحمائي عن طريق مكافحة هذه الظاهرة.

إن التطور الهائل مجال تكنولوجيا المعلومات و الإتصال الذي مس مختلف الميادين الاقتصادية و الإجتماعية و السياسية، و اتجاه المؤسسات إلى زيادة الإستثمار في التكنولوجيا و التعامل بالتجارة الالكترونية من أجل زيادة أرباحها من جهة و البيئة الأكثر التنافسية التي أصبحت تعيشها من جهة أخرى؛ خلفت أثرا سلبيا من خلال تعاظم تقديم الخدمات عبر شبكة الإنترنت التي أصبحت مجالا خصبا لارتكاب ما اصطلح على تسميتها بالجريمة المعلوماتية، التي بدأت تنمو و تتسارع في التطور في ظل تأخر الآليات القانونية و البشرية و الفنية.

و نظرا لخصوصية هذه الجريمة التي تهدد الفرد في أمنه و شرفه و المجتمع في استقراره و وحدته و الدولة في سيادتها و أمنها، فهذه الجرائم المالية تكبد الإقتصاد الوطني خسائر معتبرة بحكم توسيع استعمال المعلوماتية في جميع المؤسسات خاصة الإقتصادية و المالية. و أمام قصور القواعد التقليدية في مواجهة الجريمة كان لزاما على المشرع الجزائري التدخل من أجل توفير الحماية القانونية للنظام المعلوماتي من خلال تفعيل و تحديث مختلف التشريعات التي تناولت الجريمة المعلوماتية، و باستحداث و إصدار قوانين خاصة تتلاءم و طبيعة هذه الجرائم، و في هذا الإطار سارع المشرع الجزائر لتدارك هذا الفراغ التشريعي بإصدار القانون 04-15 المعدل و المتمم للأمر 156/66 المتضمن قانون العقوبات[1] و الذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية، كما قام بتعديل آخر على قانون العقوبات بموجب قانون 06-23 المؤرخ في 20 ديسمبر 2006 و ذلك بتشديد العقوبة المقررة لهذه الجرائم دون المساس بالنصوص. و حرصا منه على سد كل الثغرات و الذرائع في مجال التجريم عزز هذه الحماية بتوسيع دائرة التجريم بإصدار القانون رقم 04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم

[1]. الأمر 156/66 الصادر في 08 جوان 1966 المتضمن قانون العقوبات ،ج.ر عدد 71

المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها كجانب إجرائي و إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال كجانب وقائي.

و هذا ما سيتم توضيحه في المبحثين الآتيين، حيث نتناول في المبحث الأول مكافحة الجريمة المعلوماتية من خلال قانون العقوبات و نخصص المبحث الثاني للقوانين الخاصة المستحدثة لمكافحة هذه الجريمة.

المبحث الأول : مكافحة الجريمة المعلوماتية في قانون العقوبات

أمام التطور المذهل و المتسارع في مجال التكنولوجيا و العولمة الاقتصادية و ما صاحبه من سوء استغلال بطرق غير مشروعة لتكنولجيا الحاسب الآلي و الإنترنت إضافة إلى ارتكاب الجرائم المخلة بالآداب و الأخلاق العامة.

و نظرا لخصوصية هذا النوع من الجرائم و خطورتها على غرار التشريعات الدولية و العربية و الاتفاقيات و المعاهدات، سارع المشرع الجزائري لتدارك الفراغ التشريعي في مجال الإجرام المعلوماتي، حيث يعتبر قانون العقوبات الجزائري من القوانين العربية السباقة إلى هذا الموضوع في مواكبة التشريعات الغربية مثل التشريع الأمريكي و الإنجليزي و الفرنسي، و بادر إلى إصدار القانون 15/04 المتضمن تعديل قانون العقوبات و سنتناول في هذا المبحث أهم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و المنصوص عليها في القسم السابع مكرر من قانون العقوبات، من خلال المطلبين : (المطلب الأول) **جريمتي الدخول أو البقاء غير المصرح به و جريمة التلاعب بمعطيات الحاسب الآلي**، (المطلب الثاني) **جريمتي التعامل في معطيات غير مشروعة و جريمة التزوير المعلومـــاتـــي.**

المطلب الأول : الجرائم المنصوص عليها في المواد 394 مكرر و 394 مكرر1

الفرع الأول : جريمة الدخول أو البقاء غير المصرح به

قبل أن نتطرق لهذه الجريمة نعطي تعريف موجز لنظام المعالجة الآلية للبيانات أول المعطيات لأنه علم قائم بذاته و بالمختصر فإن كلمة معلوماتية و هي ترجمة المصطلح الفرنسي Informatique و هي مزج مختصر لكلمتي : معلومة : Information و كلمة آلية : Automatique،و يقصد بها المعالجة الآلية للمعلومات [1]، Traitement Automatisé de Données و تعني تكنولوجيا تجميع و معالجة و إرسال المعلومات بواسطة الكمبيوتر.

نظام المعلومات عبارة عن آلية و إجراءات منظمة تسمح بتجميع و تصنيف و فرز البيانات (Data) و معالجتها، ومن ثم تحويلها إلــى معلومات يسترجعها الإنسان عند الحاجة إليها، ليتمكن من إنجاز عمل أو اتخاذ قرار أو القيام بأية وظيفة.[2].

و يفهم من المعطيات الفكرية المعالجة آليا هي عمل البرامج و البيانات الموجودة في الكمبيوتر و على شبكة الإنترنت سواءً كانت فنية أو أدبية أو علمية أو تجارية أو صناعية فهي تصنف كإنتاج فكري لأصحابها ، فللفكرة (المعلومة) قيمة مادية معتبرة و بذلك تصبح محل حماية قانونية في مواجهة الانتهاكات التي تتم من جراء الدخول غير المشروع في أنظمة المعالجة الآلية للبيانات أو البقاء فيها.

يعد الاعتداء على نظام المعالجة الآلية للمعطيات عن طريق الدخول أو البقاء غير المصرح به، أول صور من صور المساس بأنظمة المعالجة التي نص عليها المشرع الجزائري في قانون العقوبات من خلال نص المادة 349 مكرر، في الفقرة الأول منها.

---

[1]. خالد ممدوح إبراهيم، مرجع سابق ص 359

[2]. محمد القاسمي إبراهيم، **جرائم الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية** (وفقا للمرسوم بقانون اتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات و تعديلاته"، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام.جامعة الإمارات العربية المتحدة، كلية القانون، قسم القانون العام، 2018 ص 16 ، https://scholarworks.uaeu.ac.ae/public_law_theses/12

فللدخول إلى نظام المعالجة الآلية للمعطيات أو البقاء فيه من الجرائم التي تقوم بتوافر القصد الجنائي العام بعنصريه العلم و الإرادة، حيث يتوجب أن يكون الجاني عالما بعدم أحقيته في دخول النظام أو البقاء فيه، و أن هذا الفعل مخالف لإرادة صاحب النظام و مع ذلك يقدم على دخول النظام أو البقاء فيه[1].

أولا فعل الدخول غير المشروع

لقد جرم المشرع الجزائري فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية أي مجرد اختراق جهاز الكمبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية يعد انتهاكا للنظام المعلوماتي بطريقة غير مشروعة.

و لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب و نظامه، بل يقصد به الدخول باستخدام الوسائل الفنية و التقنية إلى النظام المعلوماتي، أي الدخول المعنوي أو الالكتروني إلى العمليات الذهنية التي يقوم نظام المعالجة الآلية للمعطيات [2] سواءً كان مباشر إلى المعلومات أو تم عن طريق الإعتراض غير المشروع لعمليات الاتصال.

و يكون الدخول إلى النظام المعلوماتي سلوكا غير مشروع، إذا تم دون وجه حق، أي دون تصريح، أو مصرحا بالدخول إلى جزء من النظام فقط و يتجاوز الدخول إلى كامل النظام أو أجزاء أخرى يحظر الدخول اليها.

فالدخول و البقاء غير المصرح بهما، لهما تبعات مادية تتمثل في خسائر مالية معتبرة، من حيث تكوين الخبراء الاستشاريين في المجال المعلوماتي يعملون لدى شركات مختلفة عبر العالم تنفق ملايين الدولارات على خدمات الاستشارة المعلوماتية، و ذلك من أجل ضمان امن المبادلات الالكترونية.

---

[1]. خضراوي الهادي، عبد الحليم بوقرين، تجربة الجزائر في مكافحة الجريمة الإلكترونية، المؤتمر الدولي الأول لمكافحة جرائم المعلوماتية، ICACC، كلية علوم الحاسب و المعلومات،جامعة الإمام محمد بن سعود الإسلامية،الرياض السعودية نوفمبر 2015 ص .156 http://search.mandumah.com/Record/609635

[2]. مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات و قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال، مجلة القانون، المجلد 09، العدد 01(2020)، 109-133، تاريخ النشر 2020/06/01

ثانيا فعل البقاء غير المشروع

لقد سبق و أن رأينا أن المشرع قد جرم الدخول و كذلك البقاء أو المكوث عن طريق الغش إلى النظام المعلوماتي بنص المادة 394 مكرر من ق.ع.ج.

يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[1] و لا يختلف الدخول إلى نظام الكمبيوتر عن طريق الخطأ، عن الدخول غير المصرح به من حيث و جوب التجريم، غير أن المشرع فرق بين فعل الدخول غير المشروع و بين البقاء دون وجه قانوني أو مصلحة قانونية و يرجع ذلك إلى سبب بسيط يبرر هذه التفرقة و هو و أن كان الدخول عن طريق الخطأ ينتفي معه الجرم فإن البقاء عن قصد يشكل جرماً، أي إرادة الجاني الإضرار بالغير (سوء النية عن طريق الغش). و لا يوجد هناك رأي يحدد بدقة زمن انتهاء جريمة الدخول و بداية جريمة البقاء في المنظومةأو جزء منها، و اعتبر بعض الفقه أن بدايتها تكون لحظة بداية التجول داخل النظام المعلوماتي[2].

و قد يجتمع الدخول و البقاء غير المشروع معا، و ذلك في و قد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في النظام و قد يجتمعان، فإذا دخل الشخص إلى النظام بالصدفة أو عن طريق الخطأ وجب عليه قطع الإتصال و الإنسحاب ، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع، كأن يطبع الشخص نسخة من المعلومات في الوقت الذي سمح له بالإطلاع فقط، و يتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، كالحصول على الخدمة دون أن دفع المقابل الواجب دفعه أو الحصول على مدة أطول من المدة التي دفع مقابلها ، ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد، و ذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية.

---

[1]. رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان،2018

[2]. زيبحــة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي،دار هومة، عين ميلة، الجزائر، ط 2011، ص 50

ثالثـــــا : الجزاء أو العقوبة المقـــــرة

يعد الإعتداء على أنظمة المعالجة الآلية للمعطيات عن طريق الدخول و البقاء من أخطر الجرائم لما يسببه من مساس بالمصالح المحمية للأشخاص الطبيعية و المعنوية و التي خصها المشرع بقواعد تحميها من أي اعتداء و بأي وسيلة كان.

حيث في هذا الشأن نصت المادة 394 مكرر من قانون العقوبات على ما يلي : "**يعاقب بالحبس من (03) أشهر إلى سنة(1) و بغرامة من 50.000 إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك .**"

و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة من ستة (06) أشهر إلى سنتين (02) و الغرامة من 50.000 إلى 150.000 دج ".

و قد شدد المشرع في العقوبة و جعلها مضاعفة بنص المادة 394 مكرر من ق.ع.ج إذا ترتب على البقاء أو الدخول في النظام حذف أو تغيير لمعطيات المنظومة بنص الفقرة الثانية من المادة المشار أليها، و يتضح من ذلك أن الحرص على حماية نظام المعلوماتية لم يقتصر على تجريم فعل الدخول إليه أو البقاء فيه بل في مواجهة ما هو أخطر منها و هو ما يترتب عنها كحذف البيانات أو المعطيات أو تغييرها ، و تخريب نظام اشتغال المنظومة

فعملية التحريف و التخريب و التغيير في المنظومة تعد أبرز صور الجريمة التي تجسد الركن المادي لها بإحداث تغيير في البيانات، و ذلك بمحوها كليا أو جزئيا أو تشويهها و تجعلها غير صالحة للاستعمال و يتحقق الركن المعنوي لهذه الجريمة بتوافر العلم بان تتجه إرادة الجاني لتحقيق نتيجة تصرفه ، فجريمة الإتلاف و التخريب عمدية و هي لا تقتصر على تغيير في البيانات بل قد تصل إلى تخريب نظام اشتغال المنظومة كليا، كما تصورها نص المادة 394 مكرر من ق.ع.ج. و بصدد ذلك ضاعف المشرع العقوبة[1].

[1]. زيبحـــة زيدان، مرجع سابق، ص 51

الفرع الثانـــي : جريمة التلاعب بمعطيات الحاسب الآلي

هي الجريمة الثانية التي نص عليها قانون العقوبات الجزائري بعد جريمة الدخول و البقاء غير المصرح بها، و يطلق عليها أيضا اسم "جريمة التلاعب في بيانات نظم المعلومات" أو " جريمة المساس العمدي للمعطيات"، و المنصوص عليها في المادة 394 مكرر1 من قانون العقوبات، و نظرا لعالمية الجريمة المعلوماتية فانه بإمكان أي شخص الدخول و التلاعب بمحتوى المعلومات المخزنة في الحاسب الآلي عن بعد و دون التواجد في مكان ارتكاب الجريمة [1].

و قد وسع المشرع الجزائري من مفهوم الحماية الجنائية للمنظومة المعلوماتية بوضع تصور للسلوكات التي يمكن أن يقوم بها الجناة و تشكل خرقا و مساسا بقدسية الحياة الخاصة للأفراد و المؤسسات أو الدولة الموجودة بشبكة نظام المعلوماتية من بيانات و معطيات و برامج و ما يتبعها من نتاج فكري.

و على خلاف المادة 394 مكرر حيث اعتبر مجرد الدخول إلى المنظومة أو جز منها أو البقاء فيها بطرق تدليسية يشكل جريمة دون اقترانه بأي تصرف آخر، بادر المشرع الجزائري برفع العقوبة و تشديدها في الماد 394 مكرر 1 و ذلك تحسبا منه لما قد يترتب عن فعل الدخول أو البقاء من المساس بالمعطيات أو البيانات المخزنة من خلال التجوال في النظام سواء كان هذا المساس عن عمد أو عن غير عمد.

و يتمثل النشاط الإجرامي في هذه الجريمة في أفعال الإدخال أو المحو أو التعديل، و لا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها، و من ثم قيام الركن المادي في الجريمة، و يكفي توافر احدها لقيام الجريمة، لأن القاسم المشترك فيها هو انطوائها على تلاعب في المعلومات التي يتضمنا نظام المعالجة الآلية للبيانات بإدخال أخرى جديدة غير صحيحة أو محو أو تعديل أخرى قائمة.[2]

[1]. محمد على العريان، مرجع سابق ص 97

[2]. عبد الفتاح بيومي حجازي، مرجع سابق ص 91

الركن المادي:

كما سبق و أن رأينا قسم المشرع الاعتداءات إلى ثلاثة أفعال الإدخال غير المصرح به للمعطيات داخل نظام المعالجة الآلية للمعطيات أو إزالة هذه المعطيات أو تعديلها و هي أفعال تؤدي إلى المساس بسلامة المعطيات.

أولا فعل الإدخال :L'intrusion

يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التقليد أو في حالة إدخال برامج غريبة و هي عبارة عن تعليمات بلغة ما توجه إل ى الحاسوب بغرض الوصول إلى نتيجة معينة حسب هدف الجاني فان البرنامج الجديد إما أن يكون برنامجا وهميا يهدف إلى التمويه و التضليل في ارتكاب الجريمة، أو زرع (فيروس حصان طروادة، قنبلة معلوماتية زمنية)، و تعتبر مرحلة إدخال البيانات أو البرامج أو المعطيات الجديدة أهم المراحل في الجريمة المعلوماتية و التي تمهد لمرحلة اخطر و هي مرحلة استغلال البيانات. فقد يعمد المجرم إلى إدخال بيانات جديدة عن فاتورة هاتف قبل طبعها و إرسالها أو بيانات حول حساب بنكي، كما أن يقوم طالب مثلا بتغيير درجاته المسجلة على الحاسوب أو القيام بالتسجيل مكان طالب آخر في الجامعة بواسطة اقتناص البيانات[1]،

و ترتبط هذه الجريمة بالمصارف و البنوك، حيث يمكن لأي شخص يشغل مركزا على قدر من الأهمية و لديه كفاءة فنية أن يتلاعب بالمعلومات الموجودة في الحاسب الآلي الخاص بهذه المؤسسات[2].

[1]. هذا ما حدث فعلا بالنسبة للتلميذ الناجح في الرتبة الأولى في شهادة البكالوريا لسنة 2008 من ولاية قالمة الذي اكتشف بان شخصا آخر انتحل صفته و سرق بياناته و سجل نفسة مكانه في اختيار لا يرغب فيه في الجامعة ، جريدة الشروق اليومية عدد 2362 ليوم السبت 2008/07/26.

[2]. خضراوي الهادي، عبد الحليم بوقرين، مرجع سابق، ص 159

ثانيا فعل المـــحو : L'effacement

و هو إزالة جزء من المعطيات المسجلة على دعامة داخل النظام أو تحطيم تلك الدعامة، أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة"[1]

و عرفته اتفاقية بودابيست لسنة 2001 في المادة 04 منها عند تجريمها لمختلف أشكال العدوان على سلامة المعطيات بعدة مصطلحات تنصب في نفس المعنى و هي: الإضرار الإتلاف الطمس و الإزالة.

و مما يلاحظ أن المشرع قصد بإزالة المعطيات المخزنة إتلافها أو محوها كليا فالنص لم يستثن بان تكون الإزالة جزئيا أو كليا و الأرجح أن يشمل المعنيين معا طالما أن كليهما يشكل فعل ينطوي على خطورة كبيرة من شانه أن يلحق الأذى بالغير.

ثالثا التعديل Modification

تعديل المعطيات هو تغيير غير مشروع لحالة المعطيات الموجودة بدون تغيير الطبيعة الممغنطة، و يتحقق هذا الفعل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم بتعديلها و ذلك باستخدام القنبلة المعلوماتية للمعطيات و برامج الممحاة Gomme d'effacement أو برامج الفيروسات بصفة عامة و قد وردت أفعال الإدخال و المحو و التعديل على سبيل الحصر ، فلا يخضع لهذه الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق فيما بينها، لأن هذه الأفعال لا تنطوي على إدخال أو تعديل[2].

من خلال العرض السابق لهذه الجريمة، نجد أن المشرع قد نص على معظم الأفعال التي يمكن أن تمثل الركن المادي لهذه الجريمة، كما أكد على عمدية هذه الجريمة بتكرار مصطلح " بطريق الغش"، لكن و بالرغم من خطورة هذه الجريمة و ما ينجر عنها من خسائر خاصة في مجال المعاملات التجارية الإلكترونية التي تتم بين الشركات و المؤسسات، نجد أن العقوبة المقررة لها لا تتلائم و جسامتها، لذلك كان من الأولى ترقيتها إلى مصاف الجنايات[3]

---

[1]. أمال قارة،" الحماية الجزائية للمعلوماتية في التشريع الجزائري"، دار هومة للطباعة و النشر و التوزيع،الجزائر، ط 02، 2007 ص 132

[2]. نفس المرجع ص 123

[3]. خضراوي الهادي، عبد الحليم بوقرين، مرجع سابق ص 160

الركن المعنوي: و يتكون من القصد العام و الخاص.

أ – القصد الجنائي العام:

و يتوفر بعنصريه العلم و الإرادة، فلا بد من علم الجاني أنه قام بإدخاله أو إزالة أو تعديل غير مصرح به لمعطيات و أن من شأن أفعاله تؤدي إلى نتيجة و هي تغيير حالتها و بالرغم من ذلك تتجه إرادته إلى إحداث النتيجة.

ب – القصد الخاص:

يستشف لنا من نص المادة 394 مكرر 01 من قانون العقوبات الجزائري يشترط المشرع توافر القصد الخاص لدى الجاني، و ذلك من خلال استعماله لفظ " الغش" الذي يعني إرادة تسبيب ضرر للغير في ماله أو في حقوقه على اختلاف طبيعتها.

العقوبـــة :

تم النص على عقوبة التلاعب بالمعطيات في نص المادة 394 مكرر 01 و تتمثل في عقوبة أصلية إضافة إلى العقوبة التكميلية في نص المادة 394 مكرر 06

أ – العقوبة الأصلية:

تتمثل عقوبة جريمة التلاعب بالمعطيات في عقوبة الحبس من 06 أشهر إلى ثلاث سنوات و عقوبة الغرامة التي تتراوح 500,000 دج إلـــى 2 مليون دينـــار.

ب – العقوبة التكميلية: هي العقوبات المقررة لباقي الجرائم المعطيات المصادرة و الغلق

ج – عقوبة الشخص المعنوي:

العقوبة المقررة للشخص المعنوي هي الغرامة المضاعفة إلى خمس مرات كما هو مقرر للشخص الطبيعي و هو ما نصت عليه المادة 394 مكرر 04 من قانون العقوبات.

المطلب الثانـي : جريمة التعامل في معطيات غير مشروعة و جريمة التزوير المعلوماتي

من أهم و أخطر الجرائم التي تمس بالنظام المعلوماتي، نتيجة الكم الهائل من المعلومات المتداول بين المتعاملين في محتلف المؤسسات، و كذلك الدور الذي تلعبه المحررات في مختلف التعاملات كونها مصدر ثقة كالعقود و الصفقات و غيرها.

الفرع الأول : جريمة التعامل في معطيات غير مشروعة

تعد جريمة التعامل في معطيات غير مشروعة الصورة الثالثة من صور جرائم المساس بأنظمة المعالجة الآلية للمعطيات، و التي تناولها المشرع الجزائري في المادة 394 مكرر 02 و التي تنص على ما يلي " يعاقب بالحبس من شهرين..... كل من يقوم عمدا أو عن طريق الغش بما يأتـي:

1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

و تعتبر من أهم الجرائم ضد المعلومات و أخطرها جرمها المشرع الجزائري على غرار المشرع الفرنسي الذي نص عليها في المادة 323-3-1 من ق.ع.ف، و قد أشارت إليها المذكرة التفسيرية لاتفاقية بودابيست سنة 2001.[1] و لقد سعى المشرع الجزائري لمنع وقوع الجريمة أو التخفيف من آثارها إن وقعت.

و يتخذ السلوك الإجرامي في جريمة التعامل معطيات غير مشروعة صورتين :

[1]. بقولها إن جرائم المعطيات يتطلب لارتكابها حيازة وسائل الولوج كأدوات القرصنة أو أي أدوات أخرى و أن هناك دافعا قويا للحصول على هذه الوسائل لأغراض إجرامية مما يؤدي إلى خلق نوع من السوق السوداء لإنتاج وتوزيع مثل هذه الأدوات من أجل وقاية أكثر فعالية من هذه المخاطر فانه يجب على قانون العقوبات أن يحظر الأفعال قبل ارتكاب هذه الجرائم، من أجل الحفاظ على سرية المعلومات المتحصل عليها بطريقة غير مشروعة.

- التعامل في معطيات صالحة لارتكاب جريمة من الجرائم التي سبقت دراستها
-التعامل في معلومات متحصله منها

و هي كلها صور شكلية تقع و تكتمل بمجرد اكتمال الفعل دون تطلب نتيجة.

أولا : التعامل في معطيات صالحة لارتكاب جريمة:

ينطوي التعامل في المعطيات على العديد من الأفعال و العمليات السابقة لاستعمال المعلومات مثل تصميمها و بحثها و تجميعها، وصولا إلى توفيرها أو نشرها أو الاتجار فيها، و لا تشترط أن تقوم مجتمعة بل يكفي أيا منها إحداها لقيام السلوك المادي للجريمة و نبين معنى هذه الأفعال كالأتـــي :

1. **التصميم** La conception :

و هو إيجاد معطيات صالحة لإرتكاب الجريمة وعادة ما يقوم بهذا العمل أشخاص متخصصين مثل مصممي البرامج ومثال ذلك برنامج يحمل فيروس أو برنامج اختراق أو برامج خبيثة.

2. **البحث** : La recherche

و هو كيفية تصميم المعلومات و إعدادها، أي البحث عن المعلومات من أجل تصميمها لأغراض إجرامية مثل البحث عن الشفرات و البيانات التي تمكن من الاستيلاء على التوقيع الإكتروني للشخص أو فك شفرات تعاملاته المالية الإكترونية.

3. **التجميع** le rassemblement :

هو القيام بجمع قدر من المعطيات التي بحيث تشكل خطرا، يمكن أن ترتكب الجرائم المعلوماتية بواسطتها و يكون عن طريق الدخول غير المصرح به أي التلاعب بالمعطيات، وقد عبر عنها المشرع الفرنسي بالحيازة Détiens ، فالتجميع يقتضي وجو الحيازة لأكبر قدر من المعلومات دون نية استخدامها فبمجرد توافرها لدى الجاني يكون قد ارتكب الجريمة المعاقب عليها بالمادة 394 مكرر2.[1]

[1]. القانون 04-15 الصادر في 10 نوفمبر 2004 يعدل و يتمم الأمر 156/66 الصادر 08 جوان 1966 المتضمن قانون العقوبات، ج.ر العدد 71

4. **التوفير Mettre en disposition :**

يقصد به الوضع تحت التصرف و المراد بذلك هو تقديم المعطيات و عرضها و إتاحتها لمن يريدها أي جعلها في متناول الغير، و وضعها تحت تصرفه و يمكن أن ترتكب بها جرائم الحاسب الآلي، مثل كلمة المرور الشفرة أو الكود أو بيانات تسمح بالدخول لكل أو جز من النظام المعلوماتي، كذلك الكشف أو الإفشاء العلني للثغرات الأمنية في النظام المعلوماتي.

5. **النشـر La diffusion:**

يكون بنشر و إذاعة المعطيات محل الجريمة حتى يتمكن الغير من الإطلاع عليها بمختلف وسائل النشر، و يعد النشر يعد من أخطر الأفعال كونه ينقل هذه المعلومات إلى اكبر قد ممكن الأشخاص.

6.الإتجـار Commercialisation :

يقصد به تقديم معطيات للغير و يكون ذلك بالمقابل أيا كان هذا المقابل، و هو يختلف عن التوفير الذي قد يكون بدون مقابل، لهذا فالاتجار قد يكون جزء من التوفير الذي قد يكون بمقابل أو بدون مقابل. و بذلك يكون المشرع الجزائري قد وسع في تجريم التعامل في المعلومات التي يمكن أن ترتكب بها جرائم المعلوماتية، من أجل الوقاية المسبقة منها.

ثانياً التعامل في معطيات متحصلة من الجريمة:

و هي الصورة الثانية للتعامل غير الشرعي في معطبات النظام المعلوماتي تقوم بأحد الأفعال التي حددتها نص المادة 394 مكرر 04 الفقرة الثانية (02) من ق.ع.ج، و تتم هذه الجريمة عن طريق الحيازة ، الإفشاء ، النشر و الإستعمال. و أي من هذه الأفعال كاف لتحقيق الركن المادي للجريمة، سنحاول شرحها كما يلي :

1. **الحيازة** La détention : تعرف الحيازة بأنها "سيطرة فعلية على شيء يجوز التعامل فيه أو يستعمل بالفعل حقا من الحقوق[1]"،

[1]. رابحي عزيزة، مرجع سابق ص 173

و يقصد بها سيطرة واقعية وإرادية على المنقول تمكنه من الانتفاع به أو تعديل كيانه أو تحطيمه أو نقله و هذا ما عرفه Garçon و في جريمة التعامل بالمعطيات تكون الحيازة متحصلة من إحدى جرائم المعطيات[1].

2. **النشـــر :**

لم يحدد المشرع وسيلة النشر فقد تكون عن طريق شبكة الإنترنت أو الأقراص المضغوطة...الخ أو إن كان النشر بمقابل أو غير مقابل ومثال ذلك يقوم الهاكرز باختراق مواقع معينة و حصولهم على كلمات العبور فيها و القيام بنشرها بسرعة على الجميع باستعمال وسائل التقنية الحديثة.

3. **الإفشـــاء La révélation :**

و يقصد بها أن شخص يتحصل على معطيات بطريقة غير مشروعة ثم يقدمها إلى أشخاص آخرين. و الإفشاء هو انتقال المعلومات من حيازة الجاني إلى الغير.

4. **الإستعمال :**

جرم المشرع سلوك الإستعمال لأي غرض كان للمعلومات المتحصل عليها من جرائم المعلوماتية، و مثال ذلك تستعمل شركة ما معطيات أو معلومات تم الحصول عليها بطريقة غير مشروعة عن شركة منافسة لها و هي من أخطر الأفعال التي يمكن تسبب خسائر للشركة أو تؤدي بها إلى الإفلاس.

ثالثا : العقوبـــــة

فيما يخص عقوبة" التعامل في معطيات غير مشروعة"، هو الحبس من شهرين إلى ثلاث سنوات غرامة من 1.000.000 إلى 5.000.000 دج، و هو ما نص عليه المشرع الجزائري في نص المادة 394 مكرر 02 ، إضافة إلى العقوبات التكميلية المنصوص عليها في المادة 394 مكرر 06.

[1]. فيصل نسيغة، الآليات القانونية الموضوعية، لمكافحة الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية 11 جوان 2017

و إلى جانب الجرائم المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر2 بين المشرع الجزائري مسألة الشروع في إركاب الجريمة المعلوماتـية و عقوبة الشريك فيها و غيرها، كما أورد أيضا عقوبة تكميلية خاصة تطبق وجوبا على هذا النوع من الجرائم.

- **الشروع في إرتكاب الجريمة المعلومـاتــية**

إن فعل الشروع أو البدء في إرتكاب الجنحة بحسب نص المادة 31[1] من قانون العقوبات، لا يعاقب عليه إلا بناء على نص صريح في القانون، و نظرا لكون جرائم الإعتداء على نظام المعالجة الآلية ذات وصف جنحي، فإن المشرع أقر لها بنص خاص نفس العقوبة المقررة للجريمة و هو نص المادة 394 مكرر 7 من نفس القانون.

- **الظروف المشددة للجريمة المعلوماتية**

اعتبر المشرع بنص المادة 394 مكرر3 من قانون العقوبات أن الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي مؤسسة رسمية، بمثابة ظرف تشديد، "ارتكاب الجرائم سالفة الذكر إضرار بالدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام"[2]

حيث حرص المشرع الجزائري على ضمان حماية مطلقة لهيئات الدفاع الوطني و المؤسسات التابعة للدولة الجزائرية و وسع هذه الحماية و ذلك بنصه على مضاعفة العقوبة المنصوص عليها.

- **الشريك في الجريمة المعلوماتية**

تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي[3] بنص المادة 394 مكرر5 بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية و لم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار، حيث تنص المادة 394 مكرر5 من قانون

---

[1]. المادة 31 من الأمر 66-155 " المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون ." ج ر عدد 49 ص 704

[2]. شرف الدين وردة و آخرون، "الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري" مجلة المنار للبحوث والدراسات القانونية و السياسية، مجلد 2 العدد 3 ديسمبر 2017 ص 32

[3]. نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي.

العقوبات : "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية يعاقب بالعقوبات المقررة بالجريمة ذاتها".

- **الجرائم المعلوماتية المرتكبة من طرف الشخص المعنوي**

طبقا للمادة 394 مكرر 4 من قانون العقوبات، يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا، و يكون ذلك إذا ارتكبت الجريمة لحسابه أو بواسطة أحد أعضائه أو ممثليه.

- **العقوبات التكميلية في الجرائم المعلوماتية**

نص المشرع الجزائري في الماد 394 مكرر 6 على عقوبات تكميلية وجوبية، تطبق على الجرائم السالف ذكرها، و تتمثل في مصادرة الأجهزة و البرامج و الوسائل المستعملة، إضافة إلى غلق المواقع و أماكن الإستغلال، على أن يكون صاحبها على علم بالجريمة مع حفظ حق الغير حسن النية.

الفرع الثانـــي : جريمـــة التزويـــــر المعلوماتـــي

تكتسي المحررات بمختلف أنوعها أهمية بالغة للبشرية لما تحتويه من مواضيع في مختلف المجالات العلمية و الثقافية و الفنية و الإقتصادية، قوامها المعلومة و ما تحمله من معنى و دلائل و ما لها من قيمة خاصة في المجال الإقتصادي، حيث مع التطور التكنولوجي تحولت دعامتها المادية من القالب الورقي إلى الحاسب الآلـي الذي سهل جمعها و معالجتها و تخزينها و من ثم توظيفها في مختلف في مختلف المجالات.

و بذلك خلفت دعامة الحاسب الآلي هذه المحررات و الصكوك و غيرها في المعاملات المختلفة للأشخاص الطبيعية و المعنوية، و نظرا لأهمية هذه البيانات، فإنها تكون محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها، و الذي من شانه إحداث أضرار مادية و معنوية معتبرة.

و تعد جريمة التزوير المعلوماتي من أخطر صور غش المعلوماتية بتوظيفها الحاسب الآلي الذي اقتحم كافة المجالات من خلال الكم الهائل للعمليات ذات الآثار القانونية الهامة و الخطيرة و التي لا يصدق عليها وصف "المكتوب" [1] في القانونين المدني و الجنائي، مما أثار الشك حول دلالتها في الإثبات و حول إمكانية اعتبارها جريمة عادية، خاصة و أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي الذي يعتبر من أخطر صور الغش المعلوماتي، و لم يتخذ أي موقف لتوسيع مفهوم المحرّر من أجل إدماج مستندات المعلوماتية ضمن المحرّرات محل جريمة التزوير. بل اكتفى بالنص على التزوير الخاص بالمحررات في القسم الثالث و الرابع و الخامس من الفصل السابع من الباب الأوّل من الكتاب الثالث من قانون العقوبات في المواد من 214 إلـى 229 التي تشترط المحرّر لتطبيق جريمة التزوير.

و من التعاريف السائدة في الفقه تعريف إميل جارسون التزوير في المحررات بأنه " تغيير الحقيقة بقص الغش في محرر بإحدى الطرق التي بينها القانون تغييرا من شانه أن يسبب ضرارً "[2]

كما عرف التزوير المعلوماتي بأنه : " تغيير للحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة أو سند له طالما أن هذه الدعامة ذات أثر في إنشاء حق أو لها شان في إحداث نتيجة معينة".

و عرف أيضا بأنه:" تغيير الحقيقة في البيانات أو المعلومات المعالجة عن طريق الحاسب الآلي، و التي أصبحت كيانا ماديا ملموسا يقابل أصل المحرر المكتوب"[3].

و حسب هذا التعريف فلا بد أن يرد التزوير المعلوماتي على البيانات أو معلومات معالجة عن طريق الحاسب الآلي و تدون على كتاب مادي ملموس قدي يكون ورقة مطبوعة، أو نسخ على شريط ممغنط أو قرص مدمج، في هذه الحالة فقط، يمكن القول بوقوع التزوير.

---

[1]. زيبحــة زيدان، مرجع سابق ، ص 50

[2]. محمد على العريان، مرجع سابق ص 162

[3]. عبد الفتاح بيومي حجازي، مرجع سابق ص 101

و سنحاول تعريف منتجات الإعلام الآلي الذي يندرج تحته التزوير المعلوماتي و الذي اغفل عنه المشرع الجزائري و لم يخصه بنصوص مستحدثة تضبطه.

أولا مفهوم منتجات الإعلام الآلـــــي

سنعرض هذا المفهوم من خلال محاولة التفرقة بين معنى المستند المعالج آليا و المستند المعلوماتي

1. 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 خلافه) 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[1]

2. المستند المعلوماتـــــي :

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 بعد و الملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرنامج، و كذا البطاقات البنكية التي لم تدخل الخدمة بعد، و إن كانت مسجلة عليها معلومات مكتوبة بخط اليد أو مطبوعة أو محفورة، إلا انه لم يتم معالجتها بعد، إذ أنها مازالت في مرحلة الإعداد فقط[2].

[1]. سوير سفيان، الجريمة المعلوماتية، ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، جامعة أبو بكر بلقايد، تلمسان،2011، ص 104

[2]. أمال قارة، مرجع سابق ، ص 132

ثانيـــــا : مدى خضوع منتجات الإعلام الآلي لنصوص التزويـــر

نصت المادة السابعة 07 من الاتفاقية الدولية للإجرام المعلوماتي على فعل التزوير المعلوماتي، الذي هو صورة من صور الاعتداء على منتجات الإعلام الآلي، إذ أن التلاعب في المعطيات الذي من شأنه أن ينتج معطيات غير أصلية يعد تزويرا.

و يقتضي الركن المادي لجريمة التزوير أن يكون تغيير الحقيقة حاصلا في محرر يشكل سندا، كما ورد في 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 يشترط بالإضافة لذلك أن يكون المحرر في شكل" كتابة "أو عبارات خطية، [1]

و السؤال الذي يطرح هو مدى قابلية تطبيق نصوص التزوير الواردة في ق.ع.ج على الاعتداءات الماسة بمنتوجات الإعلام الآلي؟.

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

1. مدى انطباق وصف المحرر على منتجات الإعلام الآلي

المحرر هو عبارة عن 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 فلا يصلح وسيلة للإثبات و لإعلان على ما احتواه من تغبير.
2. إمكانية نسب الكتابة لشخص معين.
3. إحداث المحرر آثارا قانونية.

[1]. أمال قارة، مرجع سابق ، ص 137

و بإسقاط 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.

لذلك قامت بعض التشريعات باستحداث نصوص تجريمية لمواجهة القصور الموجود في النصوص التقليدية أو تعديلها حتى لا تفلت جريمة التزوير الواقعة على المستندات المعلوماتية من العقاب[1].

غير أن التشريع الجزائري، و رغم التطور الحاصل في مجال المعلوماتية، فلم يستحدث و لم يجر أي تعديل بخصوص النصوص المتعلقة بالتزوير، حيث مازالت تشترط المحرر لتطبيق جريمة التزوير حسب ما جاء في المواد من 214 إلى 229 من قانون العقوبات.

2. مدى خضوع منتجات الإعلام الآلي للنشاط الإجرامي لجريمة التزوير

يتمثل النشاط الإجرامي المكون لجريمة التزوير في فعل تغيير الحقيقة أو استبدالها بما يخالفها، و بالتالي إذا انتفى هذا التغيير انتفى معه التزوير, و المقصود بتغيير الحقيقة هو تغيير الحقيقة القانونية النسبية و ليس تغيير الحقيقة الواقعية المطلقة، 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.[2]

و تجدر الإشارة إلى أن تحويل البرنامج أو قواعد البيانات لا يعد تزويرا لكون البرامج و المعلومات 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.

---

[1]. إلهام بن خليفة، الإشكالات التي تثيرها الفقرة" أ "في المادة الثانية من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، مجلة العلوم القانونية والسياسية، عدد 10 - جانفي 2015 . ص 173

[2]. أمال قارة، مرجع سابق ، ص 139

و بالتالي فتغيير الحقيقة كعنصر من عناصر الركن المادي لجريمة التزوير المعلوماتي تقع على البيانات و المعلومات بأي لغة كانت و بأي طريقة و جدت، حيث لا يهم المادة التي كانت عليها و لا يهم شكلها سواء كانت صور أو رموز أو إعلانات و إذا كان لا يشترط في تغيير الحقيقة التقليدية أن تكون بطريقة معينة، فانه يشترط في تغيير الحقيقة في التزوير المعلوماتي أن تتم باستخدام الحاسب الآلـي، لغرض تمييزها عن جريمة التزوير التقليدية [1]

و بالرغم من المجهودات التي بذلها المشرع الجزائري في سبيل سد الفراغ القانوني بخصوص الإجرام المعلوماتي من خلال القانون 15/04 المتضمن قانون العقوبات و ذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة إلا انه اغفل الاعتداءات الواردة على منتوجات الإعلام الآلـي. فلم يستحدث نصا خاصا بالتزوير المعلوماتي و لم يقم بتوسيع مفهوم المحرر ليشمل كافة صور التزوير، كما فعلت التشريعات الأخرى.

مما يستدعي تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي.

[1]. حفصي عباس، جرائم التزوير الإلكترونية،(دراسة مقارنة)، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم الإسلامية، تخصص شريعة و قانون، كلية العلوم الإنسانية و العلوم الإسلامية، جامعة احمد بن بله، وهران، 2015

المبحث الثانـي: آليات مكافحة الجرائم المعلوماتية في إطار القوانين الخاصة

لقد خص المشرع الجزائري الجرائم المعلوماتية بمجموعة من القوانين حرصا منه على الحماية منها و التصدي لها و من ذلك ما جاء في القسم السابع مكرر من قانون العقوبات كما رأينا في المبحث الأول، كما نص أيضا في بعض القوانين الخاصة على تجريم بعض السلوكات المعتبرة من ضمن الجرائم المعلوماتية، من خلال بعض المواد و النصوص المحتشمة في القوانين الخاصة كالتأمينات و البريد و المواصلات السلكية و اللاسلكية و الملكية الأدبية و الفنية، التجارة الالكترونية، و يرجع ذلك إلى بطئ الوتيرة التي سارت عليها تكنولوجيا المعلوماتية في بلادنا و مدى توظيفها و توسعها في مختلف القطاعات غير أن التطور السريع في مجال الجريمة المعلوماتية يفرض على المشرع مسايرة هذا التطور بتطوير المنظومة القانونية خاصة و أن هذه الجرائم جلها تمس الجانب المالي سواء لأفراد أو المؤسسات، مما يترتب عنها من خسائر جسيمة تؤثر سلبا على الجانب الإقتصادي و التنموي للبلاد.

و سنحاول من خلال هذا المبحث استعراض هذه القوانين و ما جاءت به بخصوص الحماية من الجريمة المعلوماتية.

المطلب الأول : قانــون الملكيــة الفكرية

نصت المادة الأولى من اتفاقية باريس لحماية الملكية الصناعية " تشمل حماية الملكية الصناعية براءات الاختراع ونماذج المنفعة و الرسوم و النماذج الصناعية و العلامات الصناعية أو التجارية وعلامات الخدمة والاسم التجاري و بيانات المصدر أو تسميات المنشأ وكذلك قمع المنافسة غير المشروعة[1]".

لقد كفل الدستور الجزائري لسنة 1996 و كذا تعديله لسنة 2016 الحقوق الأساسية و الحريات الفردية مع ضمان عدم إنتهاك حرمة الإنسان من خلال العديد من المواد منها

[1]. اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 20 مارس 1883 المعدلة ببروكسل سنة 1925 و لندن 1934، انضمت إليها الجزائر بموجب الأمر رقم 02-75

المادة رقم 44 التي تنص على ": حرية الإبتكار الفكري و الفني و العلمي مضمونة للمواطن و حقوق المؤلف يضمنها القانون.

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

تعتبر الملكية الفكرية من الحقوق التي خصها القانون بالحماية، و هي حق الإنسان فيما ينتجه من اختراعات علمية و إبداعات فنية وأدبية وتقنية وتجارية، تخول لصاحبها حق الاستئثار و التصرف فيه.

كما أن هذه المنتجات الفكرية لها قيمة مادية مثل المنتجات الأخرى التي تحمل قيما مالية و التي تكون عرضة للإعتداء عن طريق الإجرام المعلوماتي.

الفرع الأول : الحماية المقررة في قانون الملكية الصناعية

أولا : في الأمر 06-03 المتعلق بالعلامات التجارية

نظم المشرع الجزائري أحكام العلامات التجارية من خلال عدة قوانين أخرها الأمر 06-03 المؤرخ في 19-07-2003 و المتعلق بالعلامات التجارية و هي التسميات و الرموز و الأشكال و التي توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج و ذلك لتمييزها عن بقية المنتجات أو المصنوعات [1]، و يشترط أن تكون العلامة مميزة و جديدة و غير مخالفة للنظام العام.

لكن الإشكال المطروح في ظل التعامل بالمعلوماتية في مدى خضوع برنامج الحاسب الآلي لهذه الحماية المقررة في قانون الملكية الفكرية؟

تحمل برامج الحاسوب أسماء تميزها عن بعضها، حيث يقوم أصحاب هذه البرامج تسجيل هذا الاسم كعلامة تجارية للبرنامج، و لما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجأ أصحاب البرامج إلى وضع الأسم مقترنا به.

[1]. خالد ممدوح إبراهيم، مرجع سابق ص 449

و بالرغم من الحماية توفرها العلامات التجارية لبرنامج الحاسوب، إلا أن مجال هذه الحماية يظل محدودا و سوف يتقلص باتساع استخدام البرمجيات في التجارة الالكترونية وقد رتب القانون جزاءات مدنية و جنائية في حالة المساس بالعلامة لسيما في جريمة التقليد للعلامة المسجلة من خلال المواد 26 إلى 33 من المر 03-06 و هو ذات الأمر المنصوص عليه في اتفاقية تربس.

ثانيا : في الأمر 03-07 المتعلق ببراءة الاختراع

تعرف براءة الاختراع على أنها شهادة تمنحها الدولة و يتمتع صاحبها بحق احتكار استغلال اختراعه لمدة معينة و بمعايير معينة، فهذه الوثيقة لحماية الاختراع[1].

عرفت المادة 02 من الأمر 07/03 بأنه" فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية"، و وفق شروط فتتمثل في شرط الابتكار،شرط الجدة إن التشريعات المعاصرة بصفة عامة استبعدت البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع لأحد سببين: إما تجرد البرامج من أي طابع صناعي، أو صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة.

إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا.

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة الاختراع، نظرا للتكلفة العالية و المدد الطويلة التي يستغرقها هذا التسجيل، فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة سنوات بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر و عليه يمكن للغير الوصول إلى سر البرنامج واستغلاله قبل صدور البراءة.

وقد سلك المشرع نفس نهج التشريعات الأخرى حيث استبعد البرامج المعلوماتية صراحة من مجال الحماية، بواسطة براءات الإختراع وفقا للمادة 07 من الأمر 03-07 المتضمن براءة الإحتراع." **لا تعد من قبيل الإختراعات في مفهوم هذا الأمر برامج الحاسوب**"

[1]. زيبحـــة زيدان، مرجع سابق، ص 90

و نظرا لاستبعاد نظام براءات الإختراع للأسباب السالف ذكرها و عدم وجود تشريع خاص بالبرمجيات تبنى المشرع الجزائري نظام الحماية وفقا لحقوق المؤلف و الحقوق المجاورة و هو ما سارت عليه غالبية التشريعات و الإتفاقيات الدولية.

الفرع الثاني : الحماية المقررة في قانون الملكية الأدبية و الفنية

تناولت اتفاقية تربس حماية برامج الحاسوب في المادة 1/10 و التي تنص على تمتع " برامج الحاسب الآلي الكمبيوتر " سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن 1971.

اتجه المشرع الجزائري على غرار معظم التشريعات الغربية إلي الإقرار بالحماية القانونية لبرامج الحاسب الآلي من خلال إخضاعها لقوانين حماية حقوق المؤلف، بحيث اعترف صراحة في الأمر 03-05 المؤرخ 2003/07/19 المتعلق بحقوق المؤلف و الحقوق المجاورة بوصف المصنف المحمي لمصنفات الإعلام، حيث نص في المادة 4 من نفس الأمر على اعتبار "برنامج الحاسب الآلي كمصنف أدبي مكتوب".[1]

و هو ما ترتب عنه اعتبار أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج و البيانات يشكل فعلا من أفعال التقليد المنصوص عليها في المادة 151 من الأمر 03-05 المذكور سالفا، يترتب عليها العقوبات المقررة في المواد 153،156،157،158 من نفس الأمر[2].

و تنقسم جنح التقليد التي تمس مصنف برامج الحاسب الآلي إلى ثلاثة أنواع هي:

1. **الجنح المرتبطة بالحق المعنوي للمؤلف** : و هي محددة في المادة 1/151 من نفس الأمر و تتمثل في :

أ -الكشف غير المشروع عن المصنف الأدبي و الفني ، كأن يتم الكشف عن برنامج في الوقت أو بطريقة يرى المؤلف أنها غير مناسبة.

[1]. زيبحـــة زيدان، مرجع سابق، ص 88

[2]. أمال قارة،" مرجع سابق ص 91

ب- المساس بسلامة المصنف الأدبي أو الفني : كأن يقوم شخص بتعديل أو تغيير أو حذف أو إضافة أو تحويل على البرنامج أو بيانات الحاسب دون إذن من المؤلف.

2. **الجنح المرتبطة بالحق الأدبي للمؤلف** تتمثل فيـــي:

أ- الاستنساخ غير الشرعي للمصنف)و هي محددة في المادة 1/151 كأن يقوم شخص باستنساخ برنامج أو بيانات الحاسب بأي أسلوب .

ب- الإبلاغ غير الشرعي للمصنف المادة 152 كان يقوم شخص بإبلاغ و إعلام عموم الجمهور بمصنف برنامج و بيانات الحاسب دون علم و ترخيص من المؤلف.

3. **الجنح المرتبطة بالمصنف المقلد:**

تتعلق هذه الجنح بالتصرفات و التعاملات التي ترد على المصنف المقلد الذي يمكن أن يكون برنامج أو بيانات الحاسب الآلي و هي كالتالي.

-استيراد أو تصدير نسخ مقلدة من المصنف، بيع نسخ مزورة من المصنف، تأجير مصنف مقلد أو عرضه للتداول، الرفض عمدا دفع المكافأة المستحقة بمقتضى الحقوق المقررة للمؤلف تجدر الإشارة في الأخير أن المشرع الجزائري جرّم الإشتراك بالفعل أو بالوسائل في جرائم التقليد الواقعة على مصنف برامج وقواعد بيانات الحاسب الآلي و جعل العقوبة عليه هي نفسها العقوبة المقررة للفاعل الأصلي .

العقوبات المقررة لجنح تقليد معطيات الحاسب الآلي

لقد حدد المشرع الجزائري العقوبات التي توقع على جنح تقليد المصنفات المعلوماتية (برامج وقواعد بيانات الحاسب الآلي) في صنفين هما:

العقوبات الأصلية :حددت هذه العقوبات في نص المادة 153 من الأمر 03-5على النحو التالي:

أ **-عقوبة الحبس** : تتمثل في الحبس من 06 أشهر إلى 03 سنوات على كل من ارتكب جنحة تقليد مصنف بما فيه المصنفات المعلوماتية.

ب **عقوبة الغرامة:** علاوة على عقوبة الحبس يمكن للقاضي أن يحكم بغرامة مالية تتراوح بين 500000 دج و 1000000 دج

2- العقوبات التكميلية : للقاضي سلطة تقديرية للنطق بعقوبة واحدة أو أكثر من العقوبات التكميلية المقررة لجنح تقليد المصنفات التالية:

- مصادرة المبالغ المساوية لإقساط الإرادات المحصلة من الاستغلال غير المشروع للمصنف البرنامج المادة 157

- الأمر بتسليم العتاد و النسخ المقلدة أو قيمة ذلك و كذلك الإرادات موضوع المصادرة للمؤلف أو أي مالك حقوق أخرى لتكون عند الحاجة بمثابة تعويض المادة 159

-الأمر بطلب من المتضرر بتعليق و نشر أحكام الإدانة على نفقة المحكوم المادة 158

-الأمر بحجز الوثائق و النسخ الناتجة عن الاستنساخ غير المشروع أو التقليد أو حجز الدعائم المقلدة و الإرادات الناتجة عن الاستغلال غير المشروع للمصنفات.

و يتضح من خلال ما سبق أن المشرع الجزائري قد واكب التطورات الحاصلة في المجال المعلوماتي بان أخضع المعلوماتية لقانون الملكية الفكرية موسعا بذلك من سلطة القاضي في تقرير العقوبة و ذلك ضمانا لحقوق المؤلف[1].

و في الخلاصة يمكن القول بان التشريعات الحديثة في مجال الملكية الفكرية أخذت في الإتساع محاولة السيطرة على الموضوع في ظل الصراع االقانوني المتزايد بين الاقتصاد و التكنولوجيا. و من ذلك اعتبار **الموقع الإلكتروني مصنف متعدد الأغراض** "، من حيث إستخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسويق أو الدعاية عن غيرها على شبكة الأنترنت، أو كإسم تجاري أو شعار لجذب الجمهور، كما يمكن أن يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو لوحاتهم الزيتية أو ألعاب الفيديو ...و غيره.

[1]. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، المرجع السابق، ص 107

المطلب الثانـــي : الحماية في بعض القوانين الخاصة الأخرى

الفرع الأول : في قانوني البريد و المواصلات و قانون التأمينات

أولا : قانون البريد و المواصلات السلكية و اللاسلكية

لاشك أن الجزائر و رغم ما يسجل عليها من نقائص سواء في اكتساب التكنولوجيا أو الإستغلال العقلاني لها خاصة في القطاعات الحساسة، تبذل العديد من الجهود من اجل عصرنه هذه القطاعات و النهوض بها بغية مسايرة التطور التكنولوجي الذي يشهد العالم من حولنا و قد حققت الجزائر قفزة نوعية خاصة في مجال الاتصالات السلكية و اللاسلكية التي تعتبر العصب النابض لسير مختلف التعاملات، و لا يمكن تحقيق ذلك ألا من خلال سن تشريعات تضمن هذه التعاملات و تحمي الحقوق المترتبة عنها، و هذا ما اقره المشرع من خلال الأمر رقم 2000-03 المؤرخ في 2000/08/05 المحدد للقواعد المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، و نظرا لأهمية التعاملات التي ينظمها هذا القطاع و التطورات المتسارعة في تكنولوجيا الإعلام و الإتصال، سارع هذا القانون إلى تسهيل هذه العمليات خاصة ما تعلق بالتحويلات المالية عن طريق توظيف المعلوماتية.

و هذا ما نصت عليه المادة 87 بالقول" يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن التعامل و المحولة بالبريد أو البرق أو عن الطريق الإلكتروني" و نظرا لخطورة عمليات تحويل الأموال بواسطة الحوالات عن الطريق الإلكتروني و ما قد ينجم عنها من جرائم تستهدف شبكة الأنترنت، فقد رتب هذا القانون مسؤولية مدنية على عاتق المتعامل على المبالغ المحولة إلى حوالات إلى حين دفعها و هو ما أكدته المادة 89 و أوجبته المادة 2/84 بنصها " تطبق أحكام المادة 89 من هذا القانون عن إستعمال حوالات دفع عادية أو إلكترونية أو برقية"[1]

و قد أحاط القانون سرية المراسلات بحماية خاصة من أي انتهاك و ذلك حفاظا على الحياة الخاصة للأفراد و المؤسسات و كذا أجهزة الدولة و هذا ما ورد في نص الفقرة الأخيرة من المادة 105 كما يلي " لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات".

[1]. . زيبحـــة زيدان، مرجع سابق، ص 76

و نص على كل من تسول له نفسه و بحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات خاصة و قد أحالت المادة 127 منه العقوبات المترتبة عن ذلك على المادة 137 من ق.ع.ج بنصها : " كل موظف او عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم بفض أو اختلاس أو إتلاف رسائل مسلمة إلى البريد او يسهل فضها أو اختلاسها أو إتلافها يعاقب بالحبس من ثلاثة(03) أشهر إلى خمس (05) سنوات و بغرامة من 30.000 إلى 500.000 دج و يعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق يختلس أو يتلف برقية أو يذيع محتواها.[1]

بالإضافة إلى ذلك يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.

و يطبق هذا النص على كل شخص مرخص له بتقديم خدمة البريد السريع أو الدولي أو كل عون يعمل لديه و الذي يتولى في إطار ممارسته لمهامه فتح أو تحويل أو تخريب أو انتهاك سرية المراسلات.

ثانيا : قانـــون التأمينـــات الاجتماعية(ق. 01/08)

شهد قطاع التأمينات في الجزائر عدة تحولات في مجال تحسين الخدمات من أجل التكفل الجيد بالمؤن له اجتماعيا عن طريق إدخال كل ما هو جديد من التكنولوجيا و توظيفها و تعميم استعمال المعلوماتية في مختلف المجالات، حيث نص على أن صفة المؤمن اجتماعيا تثبت ببطاقة الكترونية و حددت المادة 06 مكرر 1 منه على أن البطاقة الإلكترونية تسلم للمؤمن مجانا من طرف هيئات الضمان الأجتماعي و هي صالحة في كل التراب الوطنيو تقدم لكل مقدم خدمات مرتبطة بالعلاج و هذا الأخير يزود بمفتاح الكتروني يسمى " المفتاح الإلكتروني لهيكل العلاج" حسب نص الماد 65 مكرر.

و بما البطاقة الالكترونية تحتوي معلومات خصوصية و متعلقة بالحياة الخاصة للفرد سواء شخصية للصيقة به أو وطنية فقد أولاها المشرع بالحماية من خلال القانون 01/08 المؤرخ في 2008/01/23 المعدل و المتمم للقانون 11/83 المتعلق بالتأمينات لتنظيم

[1]. زيبحـــة زيدان، مرجع سابق، ص 88

الجريمة المعلوماتية من خلال هيئات الضمان الإجتماعي، و ذلك بمعاقبة كل من يسلمها أو يستلمها بغرض استعمالها بطريقة غير مشروعة، عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية، أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له إجتماعيا.

و قد حدد القانون الجزاءات المقررة لهه الجرائم بنص المادة 93 على أنه " : دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة من 100.000 د ج إلى 200.000 د ج كل من يسلم أو يستلم بهدف الإستعمال غير المشروع البطاقة الإلكترونية للمؤمن له إجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة"[1].

كما اهتم المشرع كذلك بالمعطيات و البيانات التي تحتويها البطاقة الإلكترونية سواء كانت تلك المعطيات تقنية معالجة آليا أو إدارية محضة كمما شملت تلك الحماية البرمجيات و ذلك بتشديد العقوبة على كل من قام بنسخ أو تعديل فيها بطريقة غير مشروعة.و هذا ما جاء في نص المادة 93 مكرر 3 من ذات القانون.

و بما أن صناديق الضمان الإجتماعي تدير تعاملات مالية ضخمة فهي عرضة للجرائم المعلوماتية التي يسعى أصحابها إلـى تحقيق عوائد مالية عن طريق وسائل غير مشروعة ناتجه عن عمليات التزوير و الإحتيال و الغش.

و هذا ما لوحظ في السنوات الأخيرة حيث سجلت هذه الصناديق عجزا بعد أن كانت من أقوى المؤسسات و التي كان يلجا إليها لتغطية العجز المسجل في القطاعات الأخرى و لجأت تغيير بعض القوانين و التي أثرت سلبا على المؤمنين اجتماعيا خاصة ففئة المتقاعدين و كذلك حذف الكثير من الأدوية من قائمة التعويض، و لربما أن الكثير من هذه المشاكل ناتج عن علميات غير مشروعة مثل التلاعب بمعطيات الحاسب الآلي عن سواء من داخل المؤسسة أو خارجها و عدم التزام المتعاملين و أرباب العمل بالتصريحات السنوية للأجراء، بالرغم من التحديثات التي شهدها القطاع بإنشاء قاعدة بيانات و منصات تحاوريه

[1]. زيبحــة زيدان، نفس المصدر، ص 78

و إمكانية التصريح عن بعد، لتسهيل هذه العملية و ضمان التصريحات في وقتها كذلك تهرب بعض الجهات التي ترصد مبالغ ضخمة من الأموال لا تقوم بدفع مستحقاتها السنوية المترتبة عن اقتطاعات الضمان االإجتماعي لموظفيها، و هذا كله بسبب عجز منظومة الضمان الاجتماعي عن مراقبة و إحصاء مستحقاتها لدى الغير و تحصيلها في وقتها من اجل استثمارها في أبوابها المشروعة. و هذا كله راجع لعدم تفعيل و تامين استعمال المعلوماتية في هذا المجال.

الذي يضمن تحصيل المستحقات ففي وقتها و ضمان السرية الأزمة للتعاملات المختلفة حتى لا تصبح عرضة للتلاعب و القرصنة و السرقة من طرف مجرمي المعلوماتية.

الفرع الثانـــي : في قانوني التجارة الإلكترونية (18-05)

تعد السوق المحلية سوقا محدودة الأمر الذي فرض البحث عن خيارات أكثر تطوراَ و توازنا تتناسب مع تلبية الحاجيات، الحالية و المستقبلية، عن طريق التشابك الدولي تحقيقا للرفاهية الإقتصادية.[1]

أولا : مفهوم التجارة الإلكترونية

لم تعد التجارة الإلكترونية مصطلحا يتداوله الناس بل واقعا ملموسا يعايشه البشر [2]، أصبح يستخدم في العديد من الأنشطة المرتبطة بثورة تكنولوجيا المعلومات و الاتصالات، و يتكون هذا المصطلح من مقطعين: الأول " **التجارة**"، و التي تشير إلى نشاط اقتصادي من خلال التداول السلع و الخدمات ، و الذي تحكمه عدة قواعد و أنظمة معترف بها دولياً، أما المقطع الثاني " **الإلكترونية**" فهو يشير إلى و يقصد به أداء النشاط التجاري باستخدام الوسائط و الأساليب الإلكترونية مثل الإنترنت و الحاسب الآلي و غيرها من الوسائل الحديثة التي تخدم هذا الغرض.

[1]. ناصر محمد الحلالمة، التجارة الإلكترونية في القانون،دار الثقافة للنشر و التوزيع، عمان الأردن، الطبعة الأولى 2012، ص 50

[2]. زيبحــة زيدان، نفس المصدر، ص 28

فهي تلك التجارة التي تتم من خلال وسيط الكتروني (الانترنيت) سواء أكان داخل حدود الدولة الجغرافية أو خارجها، و بصرف النظر عن نوعية السلع محل التجارة أو مدى مشروعيتها، أو القانون الذي تخضع له. من دون استخدام أية وثائق ورقية.

و تقوم التجارة التجارة الإلكترونية على آلية شبكة الأنترنت في مختلف النشاطات و على مبدأ كسب الثقة بين المتعاملين في تبادل السلع و الخدمات، و بما إن النشاط التجاري يقوم على ركني السرعة و الائتمان، و إذا كانت السرعة قد ضمنتها تكنولوجيا الإتصال، فان ضمان الائتمان يقع على عاتق المشرع من حيث توفير الحماية في ظل التطور السريع و المهول في مجال التجارة الإلكترونية و ما توفره من تسهيلات للمتعاملين الاقتصاديين، غير أن هذه التسهيلات تبقى مشوبة بالكثير من المخاطر التي تتربصها عن طريق الإجرام المعلوماتي فما هي هذه الجرائم التي تقع على التجارة الإلكترونية و كيف تعامل معها المشرع الجزائري؟

إذا كان ظاهر التعاملات التجارية يبدو سهلا بما يضمن سرعتها و أريحيتها في التعامل فان ما تخفيه التكنولوجيا المستعملة في التجارة الإلكترونية من تعقيدات تقنية تتطلب خبرة لفهما و فك رموزها من اجل التعامل معها و إيجاد الحلول المناسبة عند الضرورة، و هذا ما يقع على عاتق المختصين و الخبراء و التقنيين في مجال المعلوماتية و قد يتمكن هؤلاء من توفير الحماية الفنية لهذه للأنظمة من المخاطر التي تداهمها عن طريق الإجرام المعلوماتي الذي يكون له السبق في فك التشفير و اختراق البرامج، غير أن العبئ الكبير يقع على عاتق رجال القانون من أجل إيجاد السبل الكفيلة لتوفير الحماية القانونية الموضوعية و الإجرائية الوقائية لتمكين التجارة الإلكترونية من النماء و الازدهار في بلادنا و التي تعاني و تبقى رهينة قصور التشريع.

إن المشرع الجزائري على عكس التشريعات الأجنبية و بعض التشريعات العربية و التي حققت نقلة نوعية في إصدار قوانين خاصة بالتجارة الإلكترونية ، فانه تأخر في إصدار قانون خاص في هذا المجال، إلا بعد إلحاح من طرف رجال القانون و الاقتصاد،

بضرورة تنظيم هذا المجال، فقام المشرع بإصدار قانون التجارة الإلكترونية(ق. 18-05)[1] الجزائري و تنظيم بعض المسائل المتعلقة بها، حيث عرفها في نص المادة 06 منه بأنها "هي تلك النشاط الذي يقوم بموجبه مورد الكتروني باقتراح أو ضمان توفير سلع و خدمات عن بعد بمستهلك الكتروني عن طريق الاتصالات الإلكترونية"[2].

و يأتي قانون 18-05 الصادر في 10 ماي 2018 كخطوة لمحاولة مسايرة ركب الدول التي خصت التجارة الإلكترونية بقانون خاص و نظرا للنقائص التي شابت هذا القانون من حيث قصره و اقتضابه و عدم شموليته و إحاطته بجوانب التجارة الإلكترونية، فقد أحيلت جرائم التجارة الإلكترونية لقانون العقوبات المعدل و المتمم بالقانون 04-15(المواد 394 مكرر الى 394 مكرر 7) و قانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم الإلكترونية المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها و كذلك القانون المدني 05-10 فيما تعلق بالعقد الإلكتروني و التوقيع الإلكتروني و الإعتداد بالتوقيع الإلكتروني في التشريع الجزائري، و هذا ما نضمته المواد 323 مكرر 1 و 324 مكرر 7.

ثانيا : جرائم الاعتداء على التجارة الإلكترونية

من الضروري توفير الحماية الجنائية للأموال المتداولة في نطاق التجارة الإلكترونية هذه الأموال يمكن أن تكون محلا لجرائم السرقة و النصب و خيانة الأمانة و الإتلاف العمدي، فالتحويل الإلكتروني للأموال و البطاقات الإلكترونية و النقود الرقمية و قد تتعرض لجرائم الاستخدام غير المشروع لتلك البطاقات مثل استخدام بطاقة انتهت صلاحيتها أو استعمال البطاقة المسروقة أو المفقودة بواسطة الغير أو السحب ببطاقة ائتمان مزورة.

و سنذكر بعض الجرائم التي تعترض سبيل التجارة الالكترونية، و تستدعي رفع حالة تأمين و حماية المبادلات التجارية الالكترونية.

---

[1]. قانون التجارة الالكترونية الصادر بموجب القانون 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018 المتضمن قانون التجارة الالكترونية.

[2]. سعيدي عزوز، (التجارة الإلكترونية و تحديات الجريمة المعلوماتية) مجلة الدراسات والبحوث القانونية، المجلد 04 – العدد01، 01 جوان 2019

1.جريمة اختراق مواقع التجارة الالكترونية

يستطيع قراصنة الحاسب الآلي "Hackers" التوصل إلى المعلومات المالية والشخصية واختراق الخصوصية، و سرية المعلومات بسهولة، و تتم هذه القرصنة من خلال الحصول على معلومات و بيانات التاجر الالكتروني و من ثم استخدامها لأغراض غير مشروعة، و هو يعد من قبيل انتهاك حرمة الحياة الخاصة للأفراد.

و قد نص ق.ع.ج على جرائم الاعتداء على بيانات المواقع و تمثلت في التلاعب بالمعطيات، و التعامل بمعطيات غير مشروعة(المادة 394 مكرر1 و 2)[1].

2.جريمة الاتجار بمعطيات غير مشروعة

و يقصد بها هو الاتجار عمدا بمعلومات غير مشروعة و مخزنة في أنظمة إلكترونية، قصد الربح غير المشروع منها، و ذلك باستخدامها لارتكاب جرائم من ورائها و هو ما نصت عليه المادة 394 مكرر 2 ، بحيث تكون العقوبة في هذه الحالة الحبس من شهرين إلى 3 سنوات، وبغرامة من 1000000 دج إلى 5000000 دج.

3.سرقة بيانات البطاقات الائتمانية:

و يتم الحصول على أرقام بطاقة الائتمان الخاصة بالغير بسرقة البطاقة ذاتها أو سرقة بياناتها خارج الوسط الإلكتروني (سرقة تقليدية)، وقد يتم الحصول على تلك البيانات عبر الوسط الإلكتروني أي الإنترنت وذلك بأحد الأساليب التجسس(الخداع تفجير الموقع) ، ثم يقوم الجاني باستخدام بيانات البطاقة المملوكة للغير في شراء سلع أو خدمات عبر الإنترنت.

[1]. العقوبة المحددة بنص المادة 394 مكرر 1 و 2 ، "الحبس من 6 أشهر3 سنوات وبغرامة من 500000 دج إلى 2000000 دج، كل من يدخل أو يبقى عن الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، كما أن العقوبة تتغير من 6 أشهر إلى سنتين، و الغرامة من دج 50000 إلى 150000 دج إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام(اشتغال المنظومة).

4.استخدام الأسماء و العلامات التجارية المتشابهة:

بعض المواقع الالكترونية تقوم بتقليد العلامات التجارية المشهورة على الشبكة بغرض جذب المستهلك والاحتيال عليه و لا يجوز الاعتداء على العلامة التجارية المشهورة، فإن ذلك يعد تقليدا يتطلب شطب الموقع و يعد منافسة غير مشروعة.

5. طلب شراء السلع عبر الاحتيال:

و يتمثل في شحن البضائع الإلكترونية و السلع الفاخرة المشتراة ببطاقات الائتمان المسروقة، إلى بلاد بعيدة عن محيط السرقة، حيث يحصل المجرمون على هذه السلع بأسعار أقل داخل الولايات المتحدة وأوروبا على سبيل المثال، ثم يقومون بشحنها إلى الخارج بأسعار أعلى بقليل من قيمتها الحقيقية و لكنها تظل في نفس الوقت أقل من أسعارها في البلاد المرسلة إليها، بعد ذلك تتحول البضائع إلى نقود يتم تقاسمها بين المحتالين.

6. حوالات المبالغ غير المصرح بها:

بات تحويل المبالغ الكترونيا إحدى الممارسات الشائعة في المجتمعات الغربية الصناعية، حيث يسعى المجرمون إلى تحويل حوالات المبالغ المشروعة، أو تدبير تحويل المبالغ النقدية من الحسابات المشروعة بهدف الكسب عن طريق قنوات إجرامية، و يمكن أيضا سرقة أو تزوير البطاقات الائتمانية (أو بياناتها) وتستخدم لشراء البضائع، أو الخدمات سواء عن طريق الأشخاص أو عبر الانترنت، كما يمكن أن تتعرض بيانات حسابات البنوك للخطر عبر استخدامها من قبل أشخاص غير مصرح لهم بغرض التأثير على المعاملات.

7. جريمة إتلاف أو تدمير المواقع الالكترونية عن طريق الفيروسات:

و هو الاعتداء على مواقع يرتادها المستهلكون، بتدميرها و تخريبها عن طريق إطلاق فيروسات، و كأنه تخريب و تدمير للمحل التجاري و الذي تعرض فيه السلع و الخدمات الموجهة للزبائن. و هو ما يستشف من مضمون المادة 394 مكرر[1].

و بما أن الفيروسات هي عملية إدخال نظام للجهاز هدفه تدمير نظام آخر فهو يدخل في إطار الجرائم الموجهة للتجارة الإلكترونية.

[1]. " يعاقب كل بالحبس من 06 أشهر إلى 03 سنوات و بغرامة من 500.000 دج إلى 2.000.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ".

خلاصـــــة الفصـــــــل

بعد ما عرفنا في الفصل الأول الجريمة المعلوماتية و مدى خطورتها كونها تمس بالفرد و المجتمع كافة و كذا المؤسسات خاصة المالية و الإقتصادية منها، و أن النصوص التشريعية التقليدية لم تعد قادرة على رصدها و تنظيمها و كبح جماحها مما يوجب على المشرع إيجاد حلول جذرية ضمن إصدار قواعد قانونية فعالة تتماشى و طبيعتها المتغيرة و هذا ما تحق نسبيا من خلال المجهودات التي بذلها المشرع من اجل إحداث توازن بين تطور الجريمة المستمر من جهة و مسايرة المنطومة التشريعية لهذا التطور من جهة أخرى و هذا ما رأيناه من خلال آليات المكافحة الموضوعية التي رصدها المشرع الجزائري لذلك منها ما تعلق بقانون العقوبات عن طريق تعديله بموجب القانون 04-15 أو عن طريق القوانين الخاصة كقانون الملكية الفكرية كالبريد و المواصلات و التأمينات الاجتماعية و التجارة الإلكترونية، غيرن أنها تبقى غير كافية أو عاجزة عن ضبط هذه الظاهرة.

خاتمـــــة

بعد الانتهاء من هذا العمل المتواضع بحمد الله و فضله و الذي كان ثمرة جهد طيلة المدة التي منحت لإنجازه و في حدود الإمكانيات المتاحة، حيث قمت بمعالجة الموضوع من خلال فصلين أساسيين، تعرضت في الفصل الأول إلى مفهوم الجريمة المعلوماتية، و التي اختلف الفقه في إعطاء تعريف جامع مانع لها ، بل تعدد الآراء و الإتجاهات حولها و قد تطرقنا إلى مفهومها باتجاهيه المضيق الذي افترض أن يكون متطلبا لاقترافها قدرا من معرفة التقنية لمرتكبها، غير أن المجرم يمكن أن يكون شخصا عاديا أي من الهواة.

أما مفهومها في الاتجاه الموسع فيتلخص في " كل سلوك إجرامي يتم بمساعدة الكمبيوتر" و يكون بذلك وسع من مفهومها خشية حصرها في إطار ضيق، و عرفنا أن المشرع الجزائري قد تبنى التعريف الموسع للجريمة بما جاء في مادته 02 من القانون 09-04 كما اعتمد على معايير أخرى و هذا ما ميزه عن غير هبحيث فسح المجال لتوقع أي جريمة قد تقع مستقبلاً، ثم بينا خصائصها و أشكالها حسب أهدافها و التي قد تقع على النظام المعلوماتي أو بواسطته، ما يميزها عن نظيرتها التقليدية، كما أن المجرم المعلوماتي يتميز بسمات خاصة اكتسبها بحكم البيئة الرقمية التي يتعامل فيها و التي جعلت منه شخصا محترفا يتمتع بقدر من الذكاء و المهارة و الخبرة ، تمكنه من ارتكاب جريمة دون جهد و عناء و عند بعد و في سرية تامة و دون اللجوء إلى العنف، و بسهولة عن طريق لمسات خفيفة للوحة المفاتيح لجهازه الموصول بالأنترنت و هو يترشف فنجان قهوة غير آبه بما ينجر عن سوء استعماله لهذه التقنية و ما تمثله من مخاطر و تسببه من أضرار للغير و دون أن يترك وراءه أي اثر للجريمة، فيصعب بذلك كشفها و تتبعها و معاقبة المسؤولين عنها، و قد تكون الدوافع من وراء ارتكاب هذه الجريمة شخصية من اجل تحقيق مكاسب مادية لظروف معينة أو ذهنية من اجل الفضول و التسلية و إثبات الذات من اجل تطويع التكنولوجيا و اكتساب الخبرة و قد تكون للانتقام و إلحاق الضرر بالغير كما قد تكون سياسية معادية بين الدول أو منظمات ضد دولة معينة عن طريق اختراق الأنظمة و تدميرها و إفشاء الأسرار.

و أمام خطورة هذه الجريمة التي تمس بأمن الأشخاص و المؤسسات و الدول و التي يصعب السيطرة عليها نظرا لتطورها المتسارع و بما أن استعمال المعلوماتية قد أصبح

ضرورة لا بد منها في جميع المجالات الاقتصادية و الاجتماعية و الصناعية و ساهم في آدائها و تطويرها و نظرا لطبيعتها الخاصة ، كان لابد من تجند المجتمع الدولي للتصدي لمخاطرها ليس بحشد الجنود و العتاد العسكري ، و إنما بإيجاد الآليات القانونية الكفيلة بردعها و تكييفها بما يتناسب مع طبيعتها و خصوصيتها ، و لا يتأتى هذا إلا بتكاتف الجهود الدولية و الإقليمية و كذا تجميع الخبرات و التعاون بين التقنيين و الخبراء في مختلف التخصصات لإلهام رجال القانون بكل ما يتعلق بهذه الظاهرة المرتبطة بالتقنية العالية التي ليست من تخصصهم من أجل الوصول إلي نتائج مرضية بإحاطة هذه الظاهرة المستجدة بقواعد تضمن للبشرية العيش الآمن في هذا الفضاء الإفتراضي.

و هذا ما تناولناه في الفصل الثاني من موضوعنا من خلال معرفة اللآليات القانونية الموضوعية التي رصدت في هذا المجال.

إذا كانت الدول المتقدة قد سبقتنا بحقب من الزمن في مجال التطور و ما حققته من ازدهار بفضل استعمال و تطوير تكنولوجيا المعلوماتية و الاتصال و دمج الوسائل المتطور بتغذية نظم معلوماتية لتسيير كم هائل من المعطيات الذي بلغ أربعين(40) زيتابايت[1] عام 2020، بين حوالي 1.7 مليار شخص يستخدمون رسائل التواصل الاجتماعي و أن أكثر من 6.8 مليار شخص يستخدمون الهاتف النقال[2]، مع تصور ما يمكنه أن يصاحب هذا كله من جرائم معلوماتية، و ما رصد لها من آليات مكافحة.

فالجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي بالإستعمال الموسع للتقنية المعلوماتية في جميع القطاعات، سواء كان إيجابيا أو سلبيا فهي معنية أيضا بالمكافحة، فكان لابد من إيجاد إطار قانوني متين و متكامل الجوانب لاحتواء الجريمة المعلوماتية، في ظل جمود النصوص التقليدية و قص ورها في ضبطها من جهة و مرونة الجريمة السريعة التطور من جهة أخرى.

---

[1]. زيتابايت :زيتا و تعني سيكتليون وهو الف مليار مليار هي وحدة قياس سعة تخزين ذاكرة حاسوبية

1ZB =10000000000000000000 bites

[2]- حسب محاضرة ألقاها " كيرك أرثر " مدير إدارة السلامة العامة والعدل التابعة لشركة ميكروسوفت، خلال مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية بالدوحة خلال شهر أفريل.

و هذا ما سارع إليه المشرع الجزائري من خلال رصد ما لديه من إمكانات مادية و بشرية بهذا الخصوص فمن خلال آليات المكافحة الموضوعية التي تطرقنها لها نخلص إلى النتائج التالية :

-لم يتفق العرف على تعريف جامع مانع للجريمة الإلكترونية

-لا شك أن هذه الجرائم تمس الاقتصاد الوطني بما فيها القطاع العام و الخاص و كذا المنظومة الأخلاقية للمجتمع.

-تبين من خلال دراسة خصائص الجريمة الإلكترونية أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية و قصور القوانين التقليدية أمام هذه الجرائم المستحدثة.

-خص المشرع الجزائري الجريمة المعلوماتية بنصوص مستحدثة من خلال تعديل قانون العقوبات بالقانون 04-15 الذي تضمن تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطي و التي نص عليها في المواد من (394 مكرر إلى 394 مكرر 7) منها جريمة الدخول أو البقاء في النظام المعلوماتي ما تمثله من خطورة على النظام المعلوماتي بحيث يعتبر مفتاح كل جريمة، كذلك جريمتي التلاعب بالمعطيات و التعامل في معطيات غير مشروعة بالإضافة إلى ذلك حاول المشرع توسيع هذه الحماية من خلال استحداث بعض القواعد الخاصة نذكر منها :

- قانون الملكية الفكرية أين اعتبر المشرع برامج الكمبيوتر من المصنفات المشمولة بالحماية في المادة 02 من قانون 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة أما بـالبريد و المواصلات و قانون التأمينات الاجتماعية لم يأت بجديد ما عدا ما تعلق بحوالات الدفع الإلكترونية و البطاقات الإلكترونية أما التجارة الإلكترونية بالرغم من أهميتها كونها عماد الاقتصاد الوطني تبقى رهينة القواعد التقليدية.

-و رغم اجتهاد المشرع الجزائري للتصدي لهذه الجريمة، إلا أنه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة.

-إن المشرع الجزائر تطرق للجريمة الواقعة على النظام المعلوماتي، و أغفل الجرائم الماسة بمنتوجات الحاسب الآلي، حيث لم ينص على جريمة التزوير المعلوماتي، وإنما أخضعها

للنصوص التقليدية الخاصة بتزوير المحرر، و لم يوسع من مفهوم المحرر ليشمل المستند المعلوماتي.

من خلال هذه النتائج يمكن اقتراح التوصيات الآتية :

- ضرورة استصدار قانون خاص بالجريمة المعلوماتية و تعهده بالتحيين و التعديل كلما دعت الضرورة إلى ذلك مسايرة لكل تطور يحصل بشان الجرائم المتعلقة بالجريمة المعلوماتية لأن قانون العقوبات و بالرغم من التعديلات الطارئة عليه في بعض جوانبه إلا أنه يبقى رهين مبادئه و أصوله و على رأسها مبدأ الشرعية و ما يتفرع عنه من مبدأ التفسير الضيق و حضر القياس في مجال التجريم.
- إدراج مقاييس لها علاقة بالتقنية الجديدة و ربطها بالتوعية من مخاطر الجريمة الإلكترونية في بعض الأطوار التربوية خاصة الجامعات و في كل التخصصات و خصوصا العلوم القانونية.
- الاستفادة من الطاقات و الكفاءات الجزائرية المتخصصة في مجال التقنية و رجالات القانون لتبادل الخبرات و متابعة كل ما هو جديدة بخصوص التقنية المتطورة و الإستشعار المبكر بما قد تحدثه من نتائج سلبية و الإحاطة بها عن طريق خلق القواعد الموضوعية و الإجرائية و الوقائية اللازمة لها.
- ضرورة مسايرة الجزائر لكل جديد من خلال ما يحدث حولها من تطورات تقنية و ما يتعلق بها من اطر قانونية تنظم ما يصاحبها من إجرام معلوماتي.
- انضمام الجزائر إلى المزيد من الاتفاقيات الدولية و العربية للتعاون على مكافحة الجريمة المعلوماتية.
- استحضار المشرع عند إصدار القانونين لكل ما يتوقع مستقبلا من جرائم وفق التغييرات المستجدة على جميع الأصعدة
- توعية المؤسسات و الأفراد و الشركات بمدى الأخطار التي تسببها جرائم المعلوماتية و التحذير منها
- تطوير برمجيات الأمن المعلوماتي بشكل دوري و مستمر و سد الثغرات و تأمين جميع وسائل التحويل الإلكتروني و البطاقات الإتمانية و برامج و أجهزة البنوك و المؤسسات الإقتصادية و المالية.

❖ **الكتب**

أ. الكتب العامة

1.أحسن بوسقيعة، الوجيز في القانون الجزائي العام ، دار هومه، الجزائر، ط 10، 2011.

2.عمر كامل السواعدة، الأساس القانوني لحماية الأسرار التجارية (دراسة مقارنة) دار حامد للنشر و التوزيع، عمان–الأردن، ط 1، 2009.

3.فاضلي إدريس، الملكية الصناعية في القانون الجزائري، ديوان المطبوعات لجامعية الجزائر، ط 2، 2011.

4.محمد أزهر سعيد السماك، طرق البحث العلمي (أسس و تطبيقات)،دار اليازوري العلمية للنشر و التوزيع، الأردن، ط 1، 2011.

5.محمد خالد جمال رستم، التنظيم القانوني للتجارة و الإثبات الإلكتروني في العالم منشورات الحلبي الحقوقية، بيروت، لبنان، ط 1، 2006.

6.محمد زكي أبو عامر، قانون العقوبات– القسم العام، دار المطبوعات الجامعية الطبعة الأولى 1986.

7.محمود نجيب حسني، النظرية العامة للقصد الجنائي،دار النهضة العربية، الطبعة الثانية 1970 في القانون الجزائي العام ، دار هومه، الجزائر، ط 10، 2011.

8.مختار شبيلي، الإجرام الإقتصادي و المالي الدولي و سبل مكافحته، دار هومة للطباعة و النشر و التوزيع، الجزائر ، ط 2، 2011.

9.شوربجي عبد المولى، مواجهة الجرائم الإقتصادية في الدول العربية، دار الحامد للنشر و التوزيع، الأردن، ط 1، 2014.

ب. الكتب الخاصة

1.أمال قارة، " الحماية الجزائية للمعلوماتية في التشريع الجزائري"، دار هومة للطباعة و النشر و التوزيع،الجزائر، ط 02، 2007.

2.خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، الإسكندرية، طبعة أولى 2011، ص 357

3.زيبحـــة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار هومة عين ميلة الجزائر، ط 2011، ص 50

4. محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية مصر طبعة 2011،
5. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية المعلوماتية)، دار الفكر الجامعي، الإسكندرية، مصر، الطبعة الأولى 2007.
6. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الإنترنت(الجرائم الإلكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية و الإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2007.
7. غانم مرضي الشمري، الجرائم المعلوماتية(ماهيتها، خصائصها، كيفية التصدي لها) الدار العلمية الدولية للنشر و التوزيع، عمان، الأردن، ط1، 2016،
8. عادل يوسف عبد النبي الشكري، المعلوماتية و أزمة الشرعية الجزائية، جامعة الكوفة/ كلية القانون، العدد السابع ،2008
9. ناصر محمد الحلالمة، التجارة الإلكترونية في القانون، دار الثقافة للنشر و التوزيع عمان الأردن، الطبعة الأولى 2012.
10. محمد فهيم درويش، الجريمة و عصر العولمة، المركز القومي للإصدارات القانونية مصر، ط 1، 2008.
11. محمد فتحي عيد، الإجرام المعاصر، دار الحامد للنشر و التوزيع، ط 1، 2014.
12. عجة الجيلالي، العلامة التجارية، خصائصها و حمايتها، منشورين زين الحقوقية(الجزء الأول)، بيروت، لبنان، ط 1، 2015

❖ الرسائل و المذكرات الجامعية

أ. الرسائل الجامعية

1. حفصي عباس، جرائم التزوير الإلكترونية،(دراسة مقارنة)، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم الإسلامية، تخصص شريعة و قانون، كلية العلوم الإنسانية و العلوم الإسلامية، جامعة احمد بن بله، وهران، 2015
2. رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان،2018

ب. مذكرات الماجستير

1. محمد القاسمي إبراهيم، جرائم الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون اتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات و تعديلاته"، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام.جامعة الإمارات العربية المتحدة كلية القانون، قسم القانون العام، 2018 موقع: https://scholarworks.uaeu.ac.ae/public_law_theses/
2. سوير سفيان، الجريمة المعلوماتية، ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، جامعة أبو بكر بلقايد، تلمسان،2011
3. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، 2013.

ت. مذكرات الماستـــر

1. ريم عمیار، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص جنائي للأعمال جامعة العربي بن مهيدي، أم البواقي كلية الحقوق و العلوم السياسية قسم الحقوق 2018.
2. دليلة مرزوق، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص : قانون جنائي للأعمال"

❖ المقـــــــالات

1. فيصل نسيغة، الآليات القانونية الموضوعية عبير بعقيقي، لمكافحة الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية 11 جوان 2017
2. مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات و قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال، مجلة القانون، المجلد 09، العدد 01(2020)، 109-133، تاريخ النشر 2020/06/01
3. مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر،مجلة علمية، 2012 العدد 21
4. سعيدي عزوز،(التجارة الإلكترونية و تحديات الجريمة المعلوماتية) مجلة الدراسات والبحوث القانونية، المجلد 04 – العدد01، 01 جوان 2019

5. شرف الدين وردة، بلجراف سامية، الجوانب الموضوعية و الإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث و الدراسات القانونية و لسياسية جامعة يحي فارس، المدية، مجلد 2 العدد 3 ديسمبر 2017.
6. إلهام بن خليفة، الإشكالات التي تثيرها الفقرة" أ "في المادة الثانية من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، مجلة العلوم القانونية والسياسية، عدد 10 – جانفي 2015.

❖ المؤتمرات و الندوات

1. كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية و مجتمع المعلوماتية الجمعية السورية للمعلوماتية – فرع حلب، 21-23 تشرين الأول، 2000
2. خضراوي الهادي، عبد الحليم بوقرين، تجربة الجزائر في مكافحة الجريمة الإلكترونية المؤتمر الدولي الأول لمكافحة جرائم المعلوماتية، ICACC،كلية علوم الحاسب و المعلومات،جامعة الإمام محمد بن سعود الإسلامية، الري اض السعودية، نوفمبر 2015.
http://search.mandumah.com/Record/609635

❖ النصوص القانونية

أ. الدستور و الاتفاقيات الدولية

1. دستور 1996 ، المعدل بموجب القانون رقم 16-01 المؤرخ في 06 مارس 2016 الجريدة الرسمية العدد 14 ، المؤرخة في 07 مارس 2016.
2. الاتفاقية الخاصة بالإجرام المعلوماتي بودابست، الصادرة في 23 نوفمبر 2001.
3. اتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة في 21 ديسمبر 2010
4. اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 20 مارس 1883 المعدلة ببروكسل سنة 1925 و لندن 1934، انضمت إليها الجزائر بموجب الأمر رقم02-75

ب. النصوص التشريعية

1.القانون 04-15 الصادر في 10 نوفمبر 2004 يعدل و يتمم الأمر 156/66 الصادر 08 جوان 1966 المتضمن قانون العقوبات، ج.ر العدد 71 بتاريخ 2004/11/10.

2.القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها.

3.الأمر 03-06 المؤرخ في 19-07-2003 و المتعلق بالعلامات التجارية

4.الأمر 03-07 المتعلق ببراءة الاختراع

5.الأمر 03-05 المؤرخ 2003/07/19 المتعلق بحقوق المؤلف و الحقوق المجاورة

6.الأمر رقم 2000-03 المؤرخ في 2000/08/05 المحدد للقواعد المتعلقة بالبريد و المواصلات السلكية و اللاسلكية

7. القانون 01/08 المؤرخ في 2008/01/23 المعدل و المتمم للقانون 11/83 المتعلق بالتأمينات

8.قانون 18-05 الصادر في 10 ماي 2018 المتعلق بلتجارة الإلكترونية

❖ **المواقع الإلكترونية** :

1.سيد طنطاوى محمد سيد، الجريمة المعلوماتية الصعوبات التي تواجه التعاون الوطني والدولي و كيفية مكافحتها،– المركز الديمقراطي العربي للدراسات الإستراتيجية، الإقتصادية و السياسية، موقع : https://democraticac.de/ تم الإطلاع عليه يوم : 2021/05/11

2.هيئة الاتصالات و تقنية المعلومات، نظام مكافحة الجرائم المعلوماتية عن موقع : https://www.citc.gov.sa/ar/ ، تاريخ الإطلاع 2021/05/04. سا 18:50

3.عبد العال الديربى، المجرم المعلوماتى: تصنيفات متنوعة ومهارات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني، **abdelaald200594@yahoo.com** أطلع عليه يوم : 2021/05/12

العنـــــــوان	الصفحة
إهـــــــداء	
شكر و عرفان	
مقدمـــــــة	
الفصل الأول : الإطار المفاهيمي للجريمة المعلوماتية	8- 38
المبحث الأول: مفهوم الجريمة المعلوماتية	8
المطلب الأول: تعريف الجريمة المعلوماتية و أركانـها	8
الفـرع الأول: تعريف الجريمة المعلوماتية	9
الفـرع الثانـي: أركان الجريمة المعلوماتية	15
المطلب الثاني: دوافع إرتكاب الجريمة المعلوماتية	17
الفـرع الأول: الدوافع الشخصية	17
الفـرع الثانـي: الدوافع الخارجية لارتكاب الجريمة المعلوماتية	18
المبحث الثاني: خصائص و أنواع الجريمة المعلوماتية	19
المطلب الأول: خصائص الجريمة المعلوماتية	19
الفـرع الأول: السمات الخاصة بالجريمة المعلوماتية	20
الفـرع الثانـي: السمات الخاصة بالمجرم المعلوماتي	27
المطلب الثاني: أنـواع الجرائـم المعلوماتية	34
الفـرع الأول: جرائم تسبب الأذى للأفراد و للمؤسسات.	34
الفـرع الثانـي: جرائـم تمس الأمـوال و أمن الدولة	37
خلاصة الفصل الأول	38

الفصل الثاني: الآليات القانونية الموضوعية لمكافحة الجريمة المعلوماتية في التشريع الجزائري	75-40
المبحث الأول: مكافحة الجريمة المعلوماتية في قانون العقوبات	41
المطلب الأول: الجرائم المنصوص عليها في المواد 394 مكرر و 394 مكرر 1	42
الفـرع الأول: جريمة الدخول أو البقاء غير المصرح به	42
الفـرع الثانـي: جريمة التلاعب بمعطيات الحاسب الآلي	46
المطلب الثاني: جريمة التعامل في معطيات غير مشروعة و جريمة التزوير المعلوماتي	50
الفـرع الأول: جريمة التعامل في معطيات غير مشروعة	50
الفـرع الثانـي: جريمـة التزويـر المعلوماتـي	55
المبحث الثاني: آليات مكافحة الجرائم المعلوماتية في إطار القوانين الخاصة	61
المطلب الأول: قانـون الملكيـة الفكرية	61
الفـرع الأول: الحماية المقررة في قانون الملكية الصناعية	62
الفـرع الثانـي: الحماية المقررة في قانون الملكية الأدبية و الفنية	64
المطلب الثاني: الحماية في بعض القوانين الخاصة الأخرى	67
الفـرع الأول: في قانوني البريد و المواصلات و قانون التأمينات	67
الفـرع الثانـي: في قانوني التجارة الإلكترونية	70
خلاصة الفصل الثاني	75
الخاتمـــة	77
ملخـــص	81
قائمة المراجـــع	83
فهرس المحتويات	89

ملخـــــص

أحدثت الثورة المعلوماتية تطورا ملحوظا بواسطة جهاز الحاسب الآلي و شبكة الأنترنت، و ذلك باستثمار المعلومة كمادة أولية في مختلف التعاملات خاصة الإقتصادية منها و التبادلات التجارية و المالية في فلك شبكة الإنترت، و استخدامها بما يحقق الرقي و الإزدهار للبشرية جمعاء، و قد نتج عن سوء استخدام هذه التقنية جرائم مستحدثة عرفت بالجرائم المعلوماتية.

و أمام خطورة هذه الظاهرة و استفحالها، و تهديدها للأمن الاجتماعي و الإقتصادي من خلال عمليات الإحتيال و السرقة و القرصنة، كان لابد من إيجاد الأطر القانونية الكفيلة بردعها بما يتناسب مع خصوصيتها، و هذا ما تجسد من خلال تدخل المشرع الجزائري عبر العديد النصوص القانونية الموضوعية لمواجهة الجريمة المعلوماتية و المجرم المعلوماتي، غير أنها تبقى غير كافية لضمان العيش في بيئة رقمية أمنة.

الكلمات المفتاحية: الجريمة المعلوماتية، المكافحة الموضوعية، الإقتصاد

Résumé : La révolution de l'information a entraîné un développement remarquable grâce à Internet, et l'investissement de l'information comme matière première dans diverses transactions économiques, y compris les échanges commerciaux et financiers dans l'orbite d'Internet, et son utilisation afin d'atteindre le progrès et la prospérité pour toute l'humanité, et l'utilisation abusive de cette technologie a entraîné de nouveaux crimes connus sous le nom de crimes informatiques.

Face à la gravité et à l'exacerbation de ce phénomène, et à sa menace pour la sécurité sociale et économique, à travers les opérations de fraude, de vol et de piraterie, il a fallu trouver des cadres juridiques pour le dissuader en proportion de sa nature, et cela s'est concrétisé à travers l'intervention du législateur algérien à travers de nombreux textes législatives objectives pour lutter contre la criminalité informatique et les cybercriminels, mais elle reste insuffisante pour assurer de Vivre dans un environnement numérique sécurisé.

Mots-clés : délit de l'information, contrôle objectif, économie

Abstract : The information revolution has brought about a remarkable development thanks to the Internet, and the investment of information as a raw material in various economic transactions, including commercial and financial exchanges in the orbit of the Internet, and its use in order to achieve progress and prosperity for all mankind, and the misuse of this technology has resulted in new crimes known as crimes informatics.

In the face of the seriousness and exacerbation of this phenomenon, and its threat to social and economic security, through fraud, theft and piracy operations, it was necessary to find legal frameworks to deter it in proportion to its nature, and this was embodied through the intervention of the Algerian legislator through many texts Objective legality to confront information crime, however, it remains insufficient to ensure living in a secure digital environment.

Keywords: information crime, objective control, economics

مقدمـــة

الفصل الأول

الإطـــار المفاهيمي

للجريمة المعلوماتية

الفصل الثاني

الآليات القانونيـــة الموضوعية المكافحة للجريمة المعلوماتية

خاتمـــــة

قائمة المراجـع

فهرس المحتويات