

جامعة عبد الحميد بن باديس مستغانم

المرجع: .....

كلية الحقوق و العلوم السياسية

قسم : القانون العام

مذكرة نهاية الدراسة لنيل شهادة الماستر

## جريمة الدخول الغير المشروع لنظام المعالجة الالية للمعطيات

ميدان الحقوق و العلوم السياسية

التخصص: القانون الجنائي و العلوم الجنائية

تحت إشراف الأستاذة :

بوكر رشيدة

الشعبة: حقوق

من إعداد الطالبة :

الديزيري هيبية

أعضاء لجنة المناقشة

رئيسا

بوزيد خالد

الأستاذ

مشرفا مقرا

بوكر رشيدة

الأستاذة

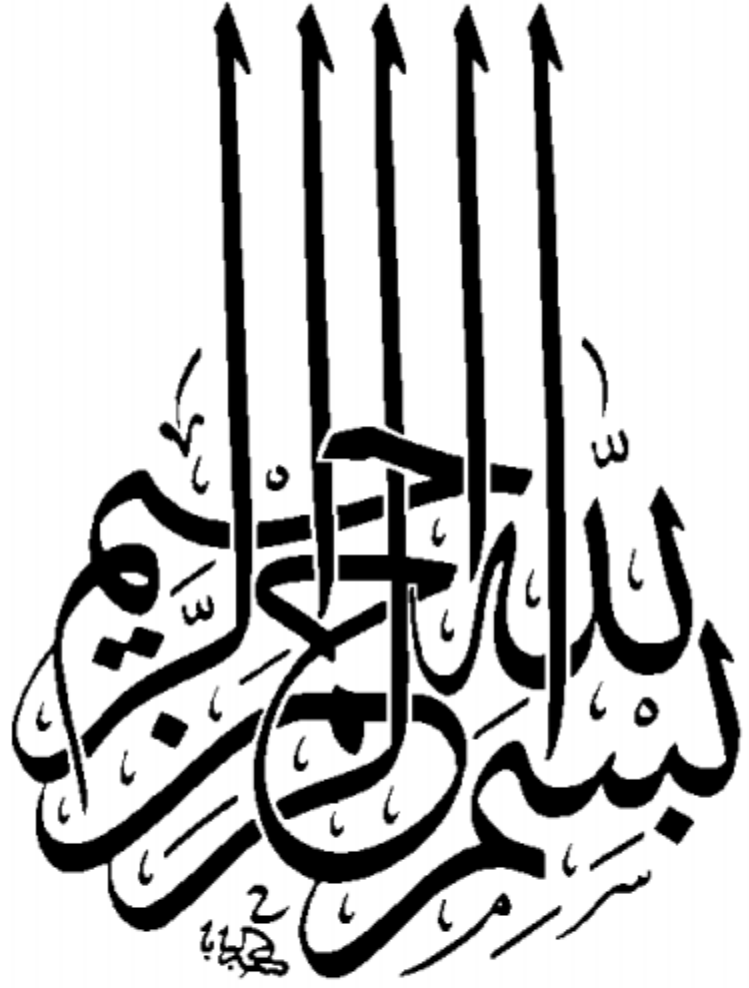
مناقشا

لطروش أمينة

الأستاذة

السنة الجامعية: 2020/2019

نوقشت يوم: 2020/06/20



# الإهداء

أهدي هذا العمل إلى أعز ما يملك الإنسان في هذه الدنيا إلى ثمرة نجاحي إلى من أوصى بهما  
الله سبحانه وتعالى :  
" وبالوالدين إحسانا "

إلى الشمعة التي تحترق من أجل أن تضيء أيامي إلى من ذاقت مرارة الحياة وحلوها، إلى  
قرة عيني وسبب نجاحي وتوفيقي في دراستي إلى امي  
"بورحلة زهرة"

أطال الله في عمرها

إلى الذي أحسن تربيتي وتعليمي وكان مصدر عوني ونور قلبي وجلاء حزني ورمز عطائي  
ووجهني نحو الصلاح والفلاح إلى ابي  
"دزيري فاتح "

أطال الله في عمره

إلى أخوتي حسام و أيمن و عماد وجميع أفراد عائلتي

إلى أستاذي " بوكري رشيدة " و جميع الأساتذة الأجلاء الذين أضاءوا طريقي بالعلم

وإلى كل أصدقاء الدراسة و العمل ومن كانوا برفقتي أثناء إنجاز هذا البحث إلى كل هؤلاء  
وغيرهم ممن تجاوزهم قلبي ولن يتجاوزهم قلبي أهدى ثمرة جهدي المتواضع

# شكر وتقدير

- الحمد لله على توفيقه وإحسانه، والحمد لله على فضله وإنعامه، والحمد لله على جوده وإكرامه، الحمد لله حمدا يوافي نعمه ويكافئ مزيده

أشكر الله عز وجل الذي أمدني بعونه ووهبني من فضله ومكنني من إنجاز هذا العمل ولا يسعني إلا أن أتقدم بشكري الجزيل إلى كل من ساهم في تكويني وأخص بالذكر أستاذتي الفاضلة " بوكر رشيدة "

الذي تكرمت بإشرافها على هذه المذكرة والتي لم تبخل علي بنصائحها الموجهة لخدمتي فكانت لي نعم الموجه والمرشد

كما لا يفوتني ان أشكر أعضاء لجنة المناقشة المحترمين الذين تشرفت لمعرفةهم وتقييمهم لمجهوداتي

كما أشكر كل من قدم لي يد العون والمساعدة ماديا أو معنويا من قريب أو بعيد إلى كل هؤلاء أتوجه بعظيم الامتنان وجزيل الشكر المشفع بأصدق الدعوات .

## قائمة المختصرات

ق: القانون.

الترميز : معنى الرمز.

ق.ع.ج : قانون العقوبات الجزائري

ج : جزء

ط : طبعة

ع : عدد

س : سنة

ص : صفحة

م : المادة

مقدمة

من خلال التطور التاريخي للإنسان واستغلاله للثروات الطبيعية ابتداء من اكتشاف الفحم كمصدر للطاقة واستعماله في تشغيل الآلة البخارية إلى اكتشاف البترول والكهرباء وما صاحبهما من تطور تكنولوجي وصولاً إلى الطاقة النووية التي تجسدت في الثورة الصناعية ، لكن رغم ما صاحب هذه الثورة من ظهور أشكال جديدة للطاقة وطرق حديثة للنقل والاتصال، فإن الثورة المعلوماتية أخذت **قدم السبق** بفضل الوسائل التكنولوجية المعلوماتية الحديثة والمتمثلة أساساً في الحاسوب الآلي (الكمبيوتر الذي ترك بصمات واضحة على حياتنا الحديثة، إذ أثر على تطور أنشطتنا اليومية من حيث الإنجاز والسرعة والشكل والمضمون والزمان والمكان<sup>1</sup> .

ومما لا شك فيه أن الحاسب الآلي أصبح على مدى العشرين عاماً الماضية ركيزة أساسية لأهداف التطور في كل مجالات الحياة لما فيها من أنشطة مختلفة سواء كانت اقتصادية أو علمية، اجتماعية أو صناعية أو زراعية، كما أن التطور الهائل الذي شهده كل من مجال تقنية المعلومات ومجال الاتصال و الاندماج المذهل الذي حدث بينهما فيما بعد، كان المحور الأساسي الذي قامت عليه تقنية المعلومات إذ أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لما تتميز به من عنصري السرعة و الدقة في تجميع المعلومات وتخزينها ومعالجتها ، ومن ثمة نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول، فبات يطلق على هذا العصر، عصر المعلومات ، فمنذ وقت قريب كان كم المعلومات المتولدة عن التفاعلات البشرية محدوداً إلى حد كبير، و لم يشكل حجمها أي مشكلة أمام عملية تجميعها و تخزينها، و إعادة استرجاعها إلا أنه ومع تقدم البشرية و تزايد معارف الإنسان وعلومه بدأ كم المعلومات يتزايد و يتكاثر وصارت الطرق التقليدية لتنظيم و تجميع المعلومات عاجزة عن تلبية احتياجات المستفيدين منها بكفاءة و فعالية ، و أصبح من

1- أمال قارة والحماية الجزائرية للمعلومات في التشريع الجزائري ودار هومة للطباعة و النشر و التوزيع و الجزائر الطبعة الأولى 2007 ، ص 3 .

الضروري اللجوء إلى استخدام أساليب علمية و تقنية متطورة لمواجهة هذه الطفرة فكان أن ظهرت الحاسبات الالكترونية، بالإضافة إلى ظهور مستحدثات تقنية كأقراص الفيديو الرقمية و أقراص الليزر وسائل الاتصال.....اخ وذلك من أجل تسهيل التحكم في المعلومات ومعالجتها و استرجاعها ، وفي مرحلة لاحقة من مراحل عصر تقنية المعلومات تم التوصل إلى فكرة الربط بين أجهزة الإعلام الآلي ووسائل الاتصال الأمر الذي أثمر على ظهور شبكات المعلومات ، و لعل أهمها على الإطلاق شبكة الانترنت .

ثم استتبع اتساع ونماء كل من تكنولوجيا الاتصال، والحاسبات من جهة، والبرمجيات بما تضمنته من هندسة البرمجيات و صناعاتها من جهة أخرى والاندماج المذهل الذي حدث بينهما للوصول إلى استحداثات تقنية نظم المعالجة الآلية للمعطيات، و من دون شك تضاعفت أهمية هذه التقنية و ازداد الاعتماد عليها في نقل و تبادل المعلومات بالصوت و الصورة عبر أنحاء العالم.

لكن وعلى الرغم من المزايا الهائلة التي تحققت ، و تتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة ، وفي شتى ميادين الحياة المعاصرة ،فإن هذه الثورة التكنولوجية المتنامية صاحبته في المقابل جملة من الانعكاسات السلبية والخطيرة جراء سوء استعمال هذه التقنية ، ذلك أن الآثار الإيجابية المشرقة لعصر تقنية المعلومات لا تقي الانعكاسات السلبية التي أفرزتها هذه التقنية نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع و بطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات والشئ الذي استتبعه ظهور أنماط جديدة من الاعتداءات على تلك المعلومات المخزنة في بيئة افتراضية ، فزادت هذه المخاطر تفاقما في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات ، كما أفرز نوعا جديدا من الجرائم لم يكن معهودا من قبل عرفت بالجرائم المعلوماتية أو جرائم تقنية المعلومات..

والخطورة التي تتميز بها هذه الجرائم المستحدثة، هي أنها سهلة الارتكاب نتيجة الاستخدام السلبي لتقنية المعلومات، بما توفره من تسهيلات و أن أثارها ليست محصورة في نطاق إقليمي لدولة بعينها فضلا على أن مرتكبيها يتسمون بالذكاء و الدراية في التعامل مع مجال المعالجة الآلية للمعطيات والإلمام بمهارات و معارف التقنية، ليس هذا فحسب بل أنها تستهدف محلا من طبيعة خاصة و نعني بذلك المعلومات التي يحتوي عليها نظام المعالجة الآلية<sup>1</sup>

و الذي هو عبارة عن إشارات و نبضات الكترونية تتساب عبر أجزاء نظام المعالجة الآلية، وشبكات الاتصال العالمية بصورة آلية والأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة وبالذات فيما يخص متابعة هذه الجرائم و آلية مباشرة الإجراءات للاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين و تقديمهم للعدالة.

و من هذا فان هذه الجرائم المستحدثة لا يمكن ارتكابها إلا من خلال ما يعرف بالدخول والبقاء في المنظومة المعلوماتية، و يعتبر هذين الفعلين من أهم العمليات التي يمكن من خلالها التعرض إلى محتويات النظام و من أخطر الجرائم التي تقع على نظام المعالجة الآلية للمعطيات، و لذلك أستشعر المشرع في دول عديدة الحاجة إلى إدخال تشريعات جديدة تحمي المعلومات داخل النظام من فعل الدخول و البقاء الغير مشروع الموجه إلى المنظومة المعلوماتية بما تحويه نظرا القصور القواعد التقليدية في قانون العقوبات عن حماية هذا النظام. ومن هذه النصوص ما يجرم فعل الدخول في المنظومة و منها ما يجرم إتلاف المعلومات و منها ما يجرم تغييرها.

ولقد أقر المشرع الجزائري هذه الحماية بداية في قانون العقوبات في الفصل السابع مكرر منه، و المتضمن المساس بنظم المعالجة الآلية للمعطيات، و الذي تضمن 8 مواد من

1- سمية مزغيش جرائم المساس بالأنظمة المعلوماتية مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، 2012-2013 ص 4.

المادة 394 مكرر إلى المادة 394 مكرر 7 كذلك من خلال القانون 09 / 04 لسنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها<sup>1</sup> و كذلك من خلال قانون الإجراءات الجزائية الجزائري<sup>2</sup> و ذلك لمتابعة مرتكبي جريمة الدخول و البقاء الغير مشروع إلى المنظومة المعلوماتية إذ خصهم بإجراءات تتفق و الطبيعة التقنية لهذه الجريمة .

و يعد هذا الموضوع من المواضيع الجديدة و المهمة أو من الموضوعات التي لا تزال بكرة و لم تتل حضاها من البحث و التمحيص على مستوى الفقه الجزائري كما أن أغلب الدراسات المنشورة في جريمة الدخول و البقاء الغير مشروع اقتصرت على البحث في ذكر بعض المفاهيم و العموميات للجريمة دون الغوص في أهم عناصرها ومشتملاتها. و إذا كانت جريمة الدخول و البقاء الغير مشروع إلى المنظومة المعلوماتية من الأنماط الإجرامية المستحدثة و التي لم تعرف سابقا في القانون الجنائي سواء الموضوعي أو الإجرائي , فمن المحتمل أن التعامل مع هذه الجريمة سوف يخلق إشكالات للأجهزة المكلفة بعملية البحث عن هذه الجرائم و متابعة مرتكبيها ومن هنا تأتي أهمية موضوع البحث الذي سنتطرق من خلاله إلى شرح جريمة الدخول والبقاء الغير مشروع إلى المنظومة المعلوماتية ثم بيان أركانها و كيفية متابعتها.

ولا يخفى أن سبب اختيارنا لهذا الموضوع هو أهميته باعتباره المنفذ الوحيد للجريمة المعلوماتية , والذي لا يمكن لأي شخص التطرق إلى المنظومة المعلوماتية بهدف الاستعمال الغير مشروع للمعلومات إلا من خلاله, و كذلك رغبة في الوقوف على حقيقة التعامل مع هذه الجريمة فكثير من الدراسات التي عنيت بهذه الجرائم باتت تركز على العموميات فيلاحظ أنه من النادر جدا ما تم التعرض لهذا الجانب و بالخصوص هذه الجريمة.

1- الجريدة الرسمية للجمهورية الجزائرية عدد 47 في 25 شعبان عام 1430 الموافق 16 غشت 2009 .

2- القانون 22 / 06 المؤرخ في 20 ديسمبر 2006 .

إن الهدف الأساسي من هذه الدراسة، هو محاولة تبيين هذه الجريمة من مختلف نواحيها والتعرف على كيفية متابعتها، ومما لا يخفى أن هذه الجريمة هي مقدمة كل الجرائم المعلوماتية، لذلك وجب على القائمين بمتابعتها فهم هذه الجريمة تحسبا لما يليها من تبعات، كما أن تحديد هذه الجريمة وإجراءات متابعتها تختلف عما هو الحال عليه في الجرائم التقليدية وتبدأ المشكلات في جريمة الدخول و البقاء الغير مشروع إلى المنظومة المعلوماتية، بتعلقها في كثير من الأحيان ببيانات المعالجة الإلكترونية و و كيانات منطقية غير مادية ، ومن ثمة يصعب الكشف عن هذه الجريمة وإثباتها نظرا للسرعة و الدقة العالية في تنفيذها خلافا للجرائم التقليدية التي ترتكب في عالم مادي ملموس ويلعب فيه السلوك المادي الدور الأكبر والأهم فجريمة الدخول و البقاء الغير مشروع ترتكب في مسرح إلكتروني غير مادي ويختلف كليا عن المسرح التقليدي، و انطلاقا من هذا يمكن طرح التساؤل الآتي :

كيف عالج المشرع الجزائري أحكام جريمة الدخول و البقاء الغير مشروع ؟

و إذ نحن بصدد البحث في الإشكالية الجوهرية تصادفنا تساؤلات يعتبر البحث فيها أمرا ضروريا للإجابة عن موضوع الدراسة و التي منها:

- ما مفهوم جريمة الدخول والبقاء الغير مشروع إلى المنظومة المعلوماتية ؟

- ما هي أركانها؟

ما هي الجزاءات المترتبة عن ارتكابها؟

و ما هي إجراءات متابعة هذه الجريمة؟

ولقد تطلب مني الأمر الاعتماد على المنهج التحليلي بالإضافة إلى مناهج أخرى كالمناهج الوصفي، والمنهج الاستقرائي، فالمنهج التحليلي يظهر من خلال تحليل بعض المفاهيم حول هذه الجريمة و طرحها بشكل من التفصيل أما المنهج الوصفي فيتجلى في وصف الجريمة وكذلك من خلال تبيين خصوصياتها و أخيرا المنهج الاستقرائي من جراء بيان النظام القانوني لهذه الجريمة

و الإجابة على هذه التساؤلات تقتضي قمنا بتقسيم البحث الى فصلين :

الفصل الأول تناولنا فيه خصوصية الجريمة المعلوماتية من الناحية الموضوعية الذي بدوره قسمناه الى مبحثين ماهية الجريمة المعلوماتية في المبحث الأول اما المبحث الثاني تناولنا فيه انواع الجرائم المعلوماتية.

أما الفصل الثاني تطرقنا إلى النظام القانوني لجريمة دخول غير مشروع قسمناه الى مبحثين الأول تناول أركان جريمة الدخول الغير مشروع أما المبحث الثاني العقوبات المقررة للجريمة دخول غير مشروع

## الفصل الاول

خصوصية الجريمة المعلوماتية من الناحية

الموضوعية

## تمهيد للفصل الاول

إن موضوع الجريمة المعلوماتية يعتبر بحد ذاته موضوع الساعة ومشكل كل الدول العالم ولا سيما الجزائر، بإعتبار أن هذه الجريمة أصبحت تمس حقوق الأشخاص من خلال التعديّ عليهم بمختلف الطرق والأساليب، باعتبار ان لشبكة الانترنت سلاح ذو حدين حيث يعكس وجهي الخير و الشر في الانسان، فهي وسيلة لربط و تقارب و تبادل المعلومات ،إلا انه يمكن ان تكون اداة تضليل و نشر للرديلة ،ومن خلال هذا الفصل سنحاول إستعراض في المبحث الأول ماهية الجريمة المعلوماتية الذي يتضمن مطلبين ، مطلب الأول تعريف الجريمة المعلوماتية و المطلب الثاني خصائص الجريمة المعلوماتية أما في المبحث الثاني فقد تطرقنا إلى أسس تصنيف الجريمة المعلوماتية و الذي يتضمن مطلبين المطلب الأول المعلوماتية وسيلة لإرتكاب الجرائم أما المطلب الثاني المعلوماتية هدفا من إرتكاب الجرائم .

**المبحث الأول : ماهية الجريمة المعلوماتية**

تعددت التعريفات الخاصة بالجريمة المعلوماتية وتباينت فيما بينها وتعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، وسوف نحاول من خلال هذا المبحث تعريف الجريمة المعلوماتية لننتقل فيما بعد إلى خصائصها.

**المطلب الأول : تعريف جريمة المعلوماتية**

إختلاف النظم القانونية والثقافية بين الدول، إنجر عنه تعريف للجريمة المعلوماتية تارة في المجال الضيق وتارة أخرى في المجال الموسع.

لذا سوف نتطرق إلى التعريف الفقهي الضيق لهذه الجريمة ثم التعريف الموسع.

**الفرع الأول : التعريف الضيق للجريمة المعلوماتية**

لا يوجد مصطلح قانوني موحد للدلالة على ظاهرة الإجرامية الناشئة في بيئة الكمبيوتر نشأت وفيما يعد بيئة الشبكات، بل تباينت هذه المصطلحات حيث رافق هذا التباين مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات<sup>5</sup> فظهرت عدة محاولات لتعريفها تعريفا ضيقا من بينها :

مأذهب إليه الفقيه (MERWE) حيث يرى أن الجريمة المعلوماتية ( جريمة الحاسب)

هي :

- الفعل الغير المشروع الذي يتورط في إرتكابه الحاسب الآلي وهي الفعل الإجرامي الذي يستخدم في إقترافه الحاسب الآلي كأداة رئيسة.<sup>6</sup>

<sup>5</sup> - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير كلية الحقوق ، جامعة الإسكندرية، سنة 2009، ص 26.

<sup>6</sup> - MARWE VANDER ,computer crimes and other grimes against information Technology in south Africa ,”R.I.D.P”,1993;p554.

- في رأي آخر ذهب ( Tièdement ) إلى أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعطيات <sup>7</sup>.
- فيما ذهب الفقيه (Rosblat) إلى تعريفها بأنها كل نشاط غير مشروع موجه لنسخ أو تغييرات أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تحول طريقه.
- أو أنها كما جاء في التعريف (David Tompson) هي الجرائم يكون متطلبا لإقترافها ان يتوافر لدى الفاعل معرفة بتقنية الحاسب.<sup>8</sup>
- وعرف (Leslie d ball) الجريمة المرتبطة بالحاسب بأنها فعل إجرامي يستخدم الحاسب في إرتكابه كأداة رئيسية .
- وعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية أنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا .
- والحقيقة ان هذه التعريفات كانت قاصرة على الإحاطة بأوجه ظاهرة الإجرام المعلوماتي ولذلك فقد أنقذت كون أن هذه التعريفات ركزت على وسيلة إرتكاب الجريمة لذا فهي ليست جامعة ولا مانعة.
- ومن أفضل التعريفات التي تدور حول الوسيلة هو تعريفها بأنها : تلك الجرائم التي يكون قد وقع في مراحل إرتكابها بعض العمليات الفعلية داخل نظام الحاسب، أي أنها الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا.
- وإزاء هذه الإنتقادات، حاول جانب من الفقه تعريف الجريمة المعلوماتية على نحو واسع لظاهرة الإجرام المعلوماتي.

<sup>7</sup> -Klaus Tiede man, Fraude et autres délits d'affaires commis a l'aide d'ordinateurs électroniques, Rev, drpén , crim, 1984, p 612.

<sup>8</sup> - د- هشام رستم، جرائم الحاسب كصورة من صور الجرائم الإقتصادية المستحدثة بحث مقدم إلى لجنة العلمية بمصر لمنع الجريمة المعلوماتية ومعاينة المجرمين، مجلة الدراسات القانونية، جامعة أسيوط ، العدد 17 ، سنة 1995 ص 107 - 108.

## الفرع الثاني : التعريف الموسع للجريمة المعلوماتية

وهو ما ذهب إليه الفقيهان (MICHEL & CREDO) من أن سوء استخدام الحاسب او جريمة الحاسب تشمل: استخدام الحاسب كأداة لإرتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج الغير المصرح به لحاسب المجني عليه أو بياناته كما تمتد جريمة الحاسب لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدلات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الإئتمان، وإنتهاك ماكينات الحساب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب.

وتناول رأي من الفقه تعريف الجريمة المعلوماتية بأنها : عمل أو إمتناع يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الإتصال الخاصة به التي يحميها قانون العقوبات ويفرض له عقاباً.

ويمتاز هذا التعريف بأنه يحتوي على كل صور الإعتداء الإيجابية والسلبية التي تقع إضراراً بمكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به. أنه يتضمن الأثر الجنائي المترتب على العمل أو الإمتناع غير المشروعين ويتمثل في الجزاء الجنائي بكافة صورته وأنواعه.<sup>9</sup>

بعد عرضنا لتعريف الجريمة المعلوماتية نضيف : أن شبكة الإنترنت بوصفها نتاج تطور النظم المعلوماتية كأداة للربط والإتصال بين مختلف شعوب العالم، تشكل أداة لإرتكاب الجريمة المعلوماتية أو محالاً لها وذلك بإساءة إستخدامها أو إستغلالها على نحو

<sup>9</sup> - د- طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر ، الإسكندرية، سنة 2009، ص 157-158.

غير مشروع، ولذلك ينبغي على الجهات التشريعية مواجهتها بتشريعات حاسمة لمكافحتها وتقديم مرتكبيها للعدالة.<sup>10</sup>

### المطلب الثاني : تصنيف المجرم المعلوماتي

الجريمة المعلوماتية إفراز ونتاج للتقنية المعلومات، وإتساع نطاق تطبيقها في المجتمع، مما يعطيها لونا او طابعا قانونيا خاصا، وبميزها مجموعة من الخصائص يمكن تجميعها حول العناصر الآتي ذكرها.

### الفرع الأول : خصوصية الجريمة المعلوماتية

#### أولا : صعوبة إكتشاف لجريمة المعلوماتية

تتسم الجرائم الناشئة عن إستخدام الأنترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، ولأن الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة .

مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة او إتلافها والتجسس وسرقة المكالمات وغيرها من الجرائم.<sup>11</sup>

كما أن وسيلة تنفيذها تتميز بالطابع الفني الذي يضيف عليها الكثير من التعقيد بالإضافة إلى عدم الإبلاغ عنها في حالة إكتشافها لخشية المجني عليهم من فقدان عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة ثانية واحدة.<sup>12</sup>

<sup>10</sup> - د- جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، سنة 2001، ص 04.

<sup>11</sup> - محمد عبيد الكعبي، الجرائم الناشئة عن الإستعمال الغير المشروع للشبكة الانترنت، دار النهضة العربية، القاهرة سنة 2000، ص 32.

<sup>12</sup> - نهلا عبد القادر المومني الجرائم المعلوماتية، الطبعة 2، دار الثقافة للنشر والتوزيع، سنة 2001، ص 54.

**ثانيا : صعوبة إثبات الجريمة المعلوماتية**

فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب و الأنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ونظرا لما تتطلبه هذه الجرائم من تقنية لإرتكابها فهي تستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحسين الجهاز الأمني والقضائي ضد هذه الظاهرة، حيث لم تعد قادة القوانين التقليدية على مواكبة السرعة الهائلة في التكنولوجيا والتي أدت إلى ظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها<sup>13</sup> مما يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية.

**ثالثا : أسلوب ارتكاب الجريمة المعلوماتية**

الجرائم الإلكترونية هي الجرائم هادئة، تحتاج إلى قدرة علمية في التعامل مع جهاز الحاسوب وشبكة المعلومات الدولية (الأنترنت) بما في ذلك بعض تقنيات ارتكاب هذه الجرائم كالإختراق سواء عن طريق إستعمال نظام التشغيل أو بإستخدام البرامج أو عن طرق تشمل كلمات السر وجمعها، كما ظهرت تقنيات السلامي *technique salami* ، أو حضان طروادة في ارتكاب عملية الإختلاس المالي وغيرها من الأساليب المتطورة التي أفرزتها التكنولوجيا<sup>14</sup>.

**رابعا: التعاون والتواطؤ على الإضرار**

وهو أكثر تكرارا في الجرائم المعلوماتية عنه في الأنماط الأخرى للجرائم الخاصة أو الجرائم أصحاب الياقات البيضاء، وهم ذوي المناصب الرفيعة المستوى في الإدارات وغالبا ما يكون متضمنا فيها متخصص في الحسابات، يقوم بالجانب الفني في المشروع الإجرامي،

<sup>13</sup> - محمد عبيد الكعبي، مرجع سابق، ص 40.

<sup>14</sup> - عائشة بن قارة مصطفى، مرجع سابق، ص 44.

وشخص آخر من المحيط أو من خارج المؤسسة ( المجني عليها) لتغطية عملية التلاعب وتحويل المكاسب إليه، كما أنها من عادة من يمارس التلصص على الحاسبات تبادل المعلومات بصفة منتظمة حول أنشطتهم.<sup>15</sup>

#### خامسا : أعراض النخبة

يعتقد بعض المختصين في تقنية الحاسبات والمعلوماتية أن من مزايا مراكزهم الوظيفية ومهارتهم الفنية، استخدام الحاسبات وبرامجها لأغراض شخصية أو ممارسة بعض الهويات الرائدة في فلك هذه التقنية وهو ما يعبر عنه بأعراض النخبة، ومن شأن ذلك تمادي بعضهم إلى استخدام نظم الحاسب بصورة غير مشروعة تصل إلى حد ارتكاب الجرائم الخطيرة.<sup>16</sup>

#### سادسا : الأضرار

تقع الجرائم المعلوماتية في نطاق تقنية متقدمة يتزايد يوما بعد يوم استخدامها في إدارة المعاملات الإقتصادية والمالية - الوطنية والدولية - الإعتماد عليها في تسيير معظم شؤون العامة لأكثر الحكومات بما في ذلك الأمن والدفاع، ومن شأن ذلك أن يضيف أبعادا مسبوقه على الخسائر و الأضرار التي تنجم عن هذه الجرائم. والأدل على ذلك من أن الخسائر المادية الناجمة عن هذه الجرائم تبلغ وفقا لتقديرات المركز الوطني لجرائم الحاسب في الولايات المتحدة الأمريكية (N.C.C.C.D) في نهاية القرن الماضي حوالي 500 مليون دولار في السنة.<sup>17</sup>

<sup>15</sup> - د - إبراهيم الدسوقي عطية، مرجع سابق، ص 169.

<sup>16</sup> - Jack Bologna, Corporate Fraud, hte Basic of prevention and Detction , Butter worth, 1984,p11.

<sup>17</sup> - WASIK Martin , computer crimes and other crimes against information tesnnology in the unit kingdom "R.I.D.P" , 1991,p19.

## سابعاً : الصفة الدولية للجريمة المعلوماتية

يمكن القول - وبحق- أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن ثم إكتسابها طبيعة دولية أو كما ذهب البعض أنها جريمة ذات طبيعة متعددة الحدود .

فمع ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، أدت إلى أن دول مختلفة قد تتأثر بالجريمة المعلوماتية المرتكبة في أن واحد.

وتظهر هذه المشكلة بصفة خاصة في مجال البنوك من خلال التوسع الكبير في إجراء المعاملات البنكية عبر الشبكات المعلومات الدولية ذلك أعطى بُعد دولي لجرائم الإحتيال المعلوماتي بصفة خاصة .

كما يمكن للجاني الذي يتواجد في دولة بالدخول إلى ذاكرة حاسب آلي موجود في دولة أخرى، للقيام بعمل إجرامي في نطاق المعلوماتية يضر بشخص آخر موجود في دولة ثالثة مثل جرائم النصب المعلوماتي .

ومن القضايا الهامة ذات البعد الدولي للجرائم المعلوماتية نذكر قضية " نقص المناعة المكتسبة" (الإيدز) وتتلخص وقائعها انه عام 1989 قام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج، الذي يهدف في ظاهره إعطاء بعض النصائح الخاصة بالمرض نقص المناعة المكتسبة إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس ( من أمثلة حضان طراودة) وكان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي، عن العمل ثم تظهر بعد ذلك على الشاشة عبارة يقوم الفاعل من خلالها بطلب مبلغ من المال، يرسل على عنوان بدولة (بنما)حتى يتمكن المجني عليه من الحصول على المضاد للفيروس، وفي عام 1990 تم إلقاء القبض على المتهم ويدعى ( جوزيف بوب) في

ولاية (أوهايو) USA وطلبت بريطانيا تسليمها المتهم لمحاكمته أمام القضاء الإنجليزي، وقد وافق القضاء الأمريكي على تسليم المتهم.

وتظهر أهمية هذه القضية من ناحيتين:

الأولى : أنها المرة الأولى التي يتم تسليم متهم في جريمة معلوماتية.

الثانية : أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد فيروس.<sup>18</sup>

### الفرع الثاني : سمات المجرم المعلوماتي

#### أولا : المعرفة والمهارة والذكاء

تعني المعرفة التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها وإحتمالات فشلها، فالجناة عادة يمهدون لإرتكاب جرائمهم بالتعرف على كافة الظروف المحيطة، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم، وتُميز المعرفة بمفهومها السابق مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يُكون تصورا كاملا لجريمته ويرجع ذلك إلى أن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.<sup>19</sup>

ويتمتع مجرمي الأنترنت بقدر لا يستهان به من المهارة بتقنيات الحاسوب والأنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات اليا، فتنفيذ جريمة الأنترنت يتطلب قدرا من المهارة لدى الفاعل الذي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال التكنولوجيا المعلومات.<sup>20</sup>

<sup>18</sup> - د - نائلة عادل فريد قورة، جرائم الحاسب الإقتصادية، دراسة نظرية تطبيقية، منشورات الحلبي القانونية القاهرة، سنة 2005، ص 48.

<sup>19</sup> - د - طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 176.

<sup>20</sup> - MASCALA Corinne , criminalité et contrat électronique, Travaux de l'association, CAPITANT Henir , journées National paris, 2000,p118.

**ثانيا : الوسيلة**

الوسيلة يراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته، وفيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بالانظمة الحاسب الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة والسهولة في الحصول عليها ، فالمجرم المعلوماتي يتميز بقدرته على الحصول على ما يحتاج إليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لأتمام النشاط الإجرامي.

**ثالثا : السلطة**

يقصد بالسلطة الحقوق أو مزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فالكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة .

وقد تتمثل هذه السلطة في معرفة الشيفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات بفتح الملفات وقراءتها ومحوها أو تعديلها، وقد تكون السلطة التي يتمتع بها الجاني غير شرعية كما الحال في حالة إستخدام شيفرة الدخول الخاصة بشخص آخر.<sup>21</sup>

**رابعا : التكيف الإجتماعي**

حيث ينشأ بين مجموعة لها صفات مشتركة فمثلا جماعة صغار نوابغ المعلوماتية لاشك أنهم يتكيفون في أفكارهم فيما بينهم وتنشأ بالتالي بينهم صفات وروابط تساعدهم على ارتكاب جرائمهم تتعدى تلك الروابط والصلات النطاق المحلي بحيث ينشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم، وتزداد خطورتهم الإجرامية إذا تزايد تكيفهم الإجتماعي مع وتوافر الشخصية الإجرامية لديهم.<sup>22</sup>

**خامسا : الباعث**

<sup>21</sup> - د - طارق إبراهيم الدسوقي عطية، مرجع سابق ، ص177.

<sup>22</sup> - ايمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار النشر، دون بلد النشر، سنة

2004، ص 17.

وأخيرا يأتي الباعث وراء ارتكاب الجريمة، ولا يختلف باعث الجاني على ارتكاب الجريمة المعلوماتية في كثير من الاحيان عن الباعث لإرتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية حوله، وأخيرا الإنتقام من رب العمل أو أحد الزملاء<sup>23</sup>.

ففي دراسة قديمة لإحدى المجالات المتخصصة في الأمن المعلوماتي تعرض لها الفقيه (PARKER) خلصت إلى أن 43% من حالات الإعتداء عاة نظم المعالجة الآلية المعلن عنها قد بوشرت بهدف إختلاس الأموال وأن 23% من أجل سرقة المعلومات وأن 19 % افعال الإلتاف وأن 15 % سرقة وقت الآلة، أي الإستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية.

أما فيما يتعلق بالرغبة في تحدي وقهر النظام فمن أشهر القضايا المتعلقة بهذه الحالة كان قد تعامل معها مكتب التحقيقات الفيدرالية، أطلق عليها إسم مجموعة الجحيم العالمي (GLOBAL HELL) تتلخص وقائعها في تمكن مجموعة من الأشخاص من إختراق مواقع البيت الأبيض والشركة الفيدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية، وقد أدين إثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة وقد ظهر من التحقيقات أن هذه المجموعات تهدف إلى مجرد الإختراق أكثر من التدمير او إلتقاط المعلومات الحساسة.

بالإضافة إلى باعث آخر يدفع إلى ارتكاب الجريمة المعلوماتية من قبيل ذلك أسباب تتعلق بالحياة المهنية، كالشعور بالحرمان من بعض الحقوق المهنية وخاصة ما يتعلق منها بالراتب ، ومن أمثلة ذلك قيام موظف فصل من الشركة التي كان يعمل بها وقبل يومين من

<sup>23</sup> – D.B.PARKER, comibattre la criminalité informatique , edoros,1987,p142.

تركه العمل قام ببرمجة كومبيوتر بالشركة زارعا نوعا من الفيروسات وبعد يومين حذفت معلومات هامة في الشركة .<sup>24</sup>

### الفرع الثالث : تصنيف المجرم المعلوماتي

#### أولا : المخترقون أو المتطفلون:

يتحدد في هذا الإطار نوعين من المخترقين أو المتطفلين :

#### 1- الهاكرز (Les hackers)

يعرف الهاكرز بأنه الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي<sup>25</sup> ويقصد بهم الشباب البالغ المفتون بالمعلوماتية، والحاسبات الآلية، أغلب هذه الطائفة هم من الطلبة والشباب حاصلين على المعرفة في مجال التقنية المعلوماتية والباعث الأساسي لهذه الطائفة هو الإستمتاع باللعب والمزاح بإستخدام هذه التقنية لإثبات مهارتهم وقدراتهم بإكتشاف وإظهار مواطن الضعف في الأنظمة المعلوماتية، دون أي إلحاق ضرر بها حيث لديهم الرغبة في المغامرة والتحري والرغبة في الإكتشاف.<sup>26</sup>

#### 2- الكراكرز (Les crakers) :

ويعني ذلك المقتحم وتعرف هذه الطائفة بالمجرمين البالغين أو المخربين المهنيين والكراكرز تتراوح أعمارهم بين 25-45 عاما ومن أبرز سمات وخصائص أفراد هذه الطائفة، أنهم ذوي مكانة في المجتمع وأنهم دائما ما يكونوا من المتخصصين في مجال التقنية

<sup>24</sup> - أ - رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، في التشريع الجزائري المقارن، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت ، لبنان، سنة، 2012، ص 95 - 96.

<sup>25</sup> - أسامة سمير حسين، الإختيال الإلكتروني ( الوجه القبيح للتكنولوجيا) ، الحنادرية للنشر والتوزيع ، الأردن الطبعة الأولى ، سنة 2011، ص 134.

<sup>26</sup> - د - عبد الفتاح البيومي الحجازي ، مبادئ الإجراءات الجنائية في الجرائم الكمبيوتر و الأنترنت، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى سنة 2006، ص 46.

الإلكترونية، أي أنهم يتمتعون بالمهارات، ومعارف فنية في مجال الأنظمة الإلكترونية أو المعلوماتية تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات.<sup>27</sup>

### ثانيا : مجرمو الكمبيوتر المحترفون :

تتميز هذه الطائفة بسعة الخبرة و الإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم و التخطيط للأنشطة التي تتركب من قبل أفرادها، لذا فإن هذه الطائفة تعد الأخطر من بين مجرمي التقنية حيث تهدف إلى اعتداءاتهم بالاساس إلى تحقيق الكسب المادي لها وللجهات التي كلفتهم وسخرتهم لإرتكاب جرائم الكمبيوتر كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي.<sup>28</sup>

وتعتبر هذه الفئة أكثر خطورة من الصنف الأول للأضرار الكبيرة التي يلحقونها بضحاياهم وباعتداءاتهم الإجرامية الخطيرة.

### ثالثا: الحاقدون :

هذه الطائفة لا يغلب عليها توافر الأهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين، فهم لا يسعون إلى إثبات القدرات التقنية والمهارتية وبنفس الوقت لا يسعون إلى مكاسب مادية او سياسية، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لصاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين أو على علاقة بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم.<sup>29</sup>

<sup>27</sup> - محمد دباس الحميد، ماركو إبراهيم نينو، حماية الأنظمة المعلومات، دار حامد للنشر والتوزيع، عمان ، الطبعة الأولى ، سنة 2007، ص 73.

<sup>28</sup> - جعفر حسين جاسم الطائي، جرائم تكنولوجيا المعلومات ( رؤية جديدة للجريمة المعلوماتية)، دار البداية ،عمان سنة 2007، ص 162.

<sup>29</sup> - نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف للنشر والتوزيع ، الأردن، دون سنة ، ص 42.

## رابعاً : الجماعات الإرهابية أو المتطرفون:

والتي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار إجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحياناً إلى النشاط الإجرامي، ويتركز نشاطهم بصفة عامة في إستخدام ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه .

ولقد بدأ إهتمام الجماعات الإرهابية، وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم، الاتجاه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة المعلوماتية .

فإعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في اغلب الأحوال، قد جعل من هذه الأنظمة هدفاً جذاباً لتلك الجماعات، حيث لا تزال الامثلة في هذا المجال قليلة وإن كان متوقفاً تزايدها مستقبلاً، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوروبا بإسم « The Red Brigades » بتدمير ما يزيد عن 60 مركزاً للمحاسبات الآلية خلال الثمانينات لتلفت الأنظار إلى أفكارها ومعتقداتها<sup>30</sup>.

## خامساً : صغار السن:

أو كما يسمون ( صغار نوابع المعلوماتية ) هم فئة لم تبلغ بعد سن الأهلية مفتونين كثيراً بالتقنيات الرقمية، وقد أثارت هذه الفئة جدلاً واسعاً في مجال الفقهي ففي حين كثر الحديث عن مخاطر هذه الطائفة، رأى جانب من الفقه أنه من أحسن عدم تصنيف هؤلاء ضمن دائرة الإجرام بحسبان أن لديهم ميلاً للمغامرة والرغبة في البحث والإستكشاف فقط.<sup>31</sup>

<sup>30</sup> - د - طارق إبراهيم الدسوقي عطية ، مرجع سابق، ص 181.

<sup>31</sup> - أ - رشيدة بوكر، مرجع سابق، 97.

**المبحث الثاني : انواع الجرائم المعلوماتية**

تعتبر الجرائم المرتكبة عبر الأنترنت من الجرائم المستحدثة، وهي تستهدف الكثير من القطاعات مما يجعل تحديدها وتصنيفها يتميز بالصعوبة على العكس الجريمة التقليدية، ولم يستقر الفقهاء على التصنيف موحدًا لصور الجريمة المعلوماتية لذ إرتأينا تقسيم وتصنيف الجريمة المعلوماتية على النحو التالي:

**المطلب الأول : جرائم الواقعة على نظام معلوماتي**

بعدها رأينا الجرائم التي تكون المعلوماتية وسيلة لإرتكاب الجرائم فيها، لا بد ان نعلم ان هنالك نوع آخر من الجرائم تكون فيه المعلوماتية هدفا من إرتكاب الجرائم، وقد تجسد ذلك في نوعين من الجرائم ، وهي الجرائم الواقعة على نظم المعالجة الآلية للمعطيات وكذلك الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الآلية للمعلومات وذلك ما سنتطرق إليه عبر الفرعين الآتيين:

**الفرع الأول : الجرائم الواقعة على نظم المعالجة الآلية للمعطيات**

**أولا : الجريمة الدخول أو البقاء غير المشروع في المنظومة المعلوماتية**

**1- جريمة الدخول غير المشروع:**

إن المشرع الجزائري جرم فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية وإعتبر هذا التصرف في حد ذاته يشكل جريمة، إذ يستخلص لأول وهلة أن مجرد إختراق جهاز الكمبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو مجرد التسلية يعد إنتهاكا لنظام المعلوماتي بطريقة غير مشروعة<sup>32</sup>.

والجريمة هنا تتحقق بالصور التالية :

- بمجرد الوصول إلى نظام معلوماتي لكن بطريق الغش، أي أنها جريمة عمدية تقوم بتوافر القصد الجنائي العام.

<sup>32</sup> - هدى حامد قشوش، جرائم الحاسب الإلكتروني في التشريع المقارن، الطبعة الأولى ، دار النهضة العربية ، سنة

1992 ، ص 62.

- أن يكون الجاني عالما بدخوله إلى منظومة معلومات لا تخصه ويتوضح معنا من نص المادة 394 ق.ع. أن الجريمة الدخول غير المشروع تصبح قائمة حتى لو لم يترتب عن ذلك أي أضرار بالمعلومات ودون تحديد للزمن، وذلك أنها جريمة وقتية.<sup>33</sup>

حيث نصت المادة 394 ق.ع. على ما يلي : " يعاقب بالحبس 03 أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية المعطيات أو يحاول ذلك"<sup>34</sup>.

## 2- جريمة البقاء في منظومة المعلوماتية :

لاحظنا نص المادة 394 ق.ع. يجرم الدخول وكذلك البقاء في المنظومة المعلوماتية ومما يتعين الوقوف عنه هنا هو أن المشرع فرق بين فعل الدخول غير المشروع وبين البقاء دون وجه قانوني أو مصلحة قانونية .

ويمكننا إيعاد ذلك إلى سبب بسيط يبرر هذه التفرقة وهو أنه إن كان الدخول عن طريق الخطأ ينتفى معه الجرم، فإن البقاء عن قصد يشكل جرماً قائماً بذاته يوحي عن إرادة الجاني في الإضرار بالغير .

وهذا ما يؤكد توافر القصد الجنائي لديه ولم نجد في القانون المقارن رأياً يحدد بدقة زمن إنتهاء جريمة الدخول وبداية جريمة البقاء في المنظومة أو في جزء منها.

غير أن البعض إعتبر بأن بدايتها تكون منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام المعلوماتي ويستهدف إعتدائه على المعطيات المخزنة او يستهدف المعدات المتصلة به، مما قد يترتب عليه حذف البيانات أو المعطيات أو تغييرها ، او تخريبها وتخریب نظام إستغلال المنظومة.<sup>35</sup>

<sup>33</sup> - أ - زبيجة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع عين مليلة، الجزائر، سنة 2011، ص 49.

<sup>34</sup> - المادة 394 من قانون العقوبات الجزائري المعدل والمتمم بموجب القانون رقم 15/04 المؤرخ في 10/11/2004.

<sup>35</sup> - أ - زبيجة زيدان، مرجع سابق، ص 50 - 51.

**ثانيا: جريمة التلاعب غير المصرح به بمعلومات نظام المعالجة الآلية**

وهي جريمة يقوم من خلالها الجاني بإدخال معطيات أو برامج جديدة أو معلومات وهمية أو مزيفة ومَعْلُومٌ أن أي تدخل في نطاق البيانات يعد تدخلا في الكيان المنطقي للحاسوب الآلي والذي يكون بغرض الوصول إلى نتيجة معينة هي بمثابة هدف الجاني لذلك فإن البرنامج الجديد إما أن يكون برنامجا وهميا يهدف إلى التمويه والتظليل في ارتكاب الجريمة وتغيير في الحقيقة وتعتبر مرحلة إدخال البيانات أو البرامج أو المعطيات الجديدة كما سماها المشرع الجزائري أهم المراحل في الجريمة الإلكترونية فهي التي تمهد لمرحلة أخطر وهي مرحلة إستغلال البيانات ، حيث نص المشرع الجزائري على هذه الجريمة في نص المادة 394 مكرر 1 ق.ع. والذي قام من خلالها بمضاعفة العقوبات المنصوص عليها في المادة 394 ق.ع آنفة الذكر.<sup>36</sup>

**ثالثا : جريمة التعامل في معلومات غير مشروعة .**

حرص المشرع الجزائري تبني سياسة جزائية تكفل الحماية لنظم المعالجة الآلية فأول ما قام به هو تجريمه لمجموعة من الفعال تصب كلها في التعامل في المعلومات صالحة لأن ترتكب بها إحدى الجرائم التي تمس سرية المعلومات أو سلامتها<sup>37</sup> وهذا ما جاء في المادة 394 مكرر 2 حيث أخذت هذه الجريمة صورتين بحيث تتضمن كل صورة منها مجموعة من الأفعال المكونة للركن المادي للجريمة التعامل في المعلومات غير مشروعة ويمكن توضيحها بشكل مختصر كالآتي<sup>38</sup> :

**1- الصورة الأولى : جاءت في المادة 394 مكرر 2 في الفقرة (1) وهي كالآتي :**

<sup>36</sup> - أ - زبيجة زيدان، مرجع سابق، ص 54 .

<sup>37</sup> - أ- رشيدة بوكري ، مرجع سابق، ص 274.

<sup>38</sup> - نصت المادة 394 مكرر 2 على الأتي : " يعاقب بالحبس من شهرين إلى 03 سنوات وبغرامة من 100.000 دج

إلى 500.000 دج كل من يقوم عمدا وعن طريق الغش للأفعال المكونة للركن المادي هذه الجريمة

أ- **التصميم** : وهو عملية تتمثل في إعداد معلومات صالحة للإرتكاب الجريمة، وهذا العمل يقوم به عادة المختصون في هذا المجال كالمبرمجين ومصممين البرامج مثل: تصميم برامج الفيروسية أو البرامج الإختراق.<sup>39</sup>

ب - **البحث** : وهو البحث عن المعلومات لمعرفة كيفية تصميم المعلومات وإعدادها لكي ترتكب بها الجرائم.

ج - **التجميع** : هو القيام بجمع قدر كبير من المعلومات التي تشكل خطرا كبيرا والتي من الممكن أن ترتكب بها إحدى جرائم الإعتداء على نظم المعالجة الآلية.<sup>40</sup>

د - **التوفير** : وهو عرض المعلومات وإتاحتها وجعلها في متناول الغير وتحت تصرفه وحيازته، لكي ترتكب بها جريمة الدخول أو البقاء أو جريمة التلاعب في الأنظمة.

هـ - **النشر** : وهو إذاعة المعلومات محل الجريمة وتمكين الغير من الإطلاع عليها، إذ من شأنه نقل هذه الأخيرة إلى عدد كبير من الأشخاص<sup>41</sup> وهذا ما يزيد من خطورة هذا الفعل.

و - **الإتجار**: وهو الإتجار بالمعلومات وتقديمها للغير بمقابل سواء كان بمقابل نقديا أو عينيا أو خدمة أو غيرها<sup>42</sup>.

2- **الصورة الثانية** : وقد جاءت في المادة 394 مكرر 2 الفقرة 2 وهي كالآتي :

أ - **الحيازة** : وهي سيطرة الحائز على المعلومات بنية إحتباسها لكي يعدل فيها، أو ينتفع بها، أو يستعملها، بطريقة غير مشروعة.

ب - **الإفشاء** : وهو الإفشاء الغير المشروع للمعلومات التي يحصل عليها بطريقة غير مشروعة عبر الوسائل التقنية الجديدة، وانتقال المعلومات من الحيازة الجاني الى غيره من الأشخاص .

39 - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الألي في القانون الجزائري والمقارن، دار الجامعية الجديدة الإسكندرية سنة 2007، ص 200.

40 - أ - رشيدة بوكري ، مرجع سابق، ص 281.

41 - أ - رشيدة بوكري ، مرجع سابق، ص 282 - 283.

42 - محمد خليفة ، مرجع سابق، ص 204.

ج - النشر : أصبحت نظم المعالجة الآلية ذاتها وسيلة فعالة في نشر المعلومات المتحصل عليها من جريمة من جرائم التي ذكرناها سابقا ، حيث يتم ذلك بسرعة وكفاءة عالتين ومثال ذلك قضية الفتى البالغ من العمر 21 سنة التي عرضت على مجلس قضاء باتنة والتي سوف نسرد وقائعها في الفصل الثاني.

د - الإستعمال : وهو الإستعمال الغير المشروع للمعلومات مهما كان الهدف منه في هذا الإستعمال، ومهما كان نوعه أو الوسائل المستخدمة في ذلك، وحتى لو تم هذا الإستعمال لمرة واحدة.<sup>43</sup>

### الفرع الثاني : الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الآلية لمعلومات

#### أولا : سرقة المال المعلوماتي

وهي عملية الإستلاء على المعلومات المخزنة داخل الجهاز دون وجه الحق أو نسخ هذه المعلومات، وهو ما يعبر عنه حاليا بالقرصنة و إن كان البعض قد عرفها بأنها : " سرقة المعلومات من برامج وبيانات مخزنة في دائرة الكمبيوتر بصورة غير شرعية أو نسخ برامج معلوماتية غير شرعية بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر أو بواسطة إلتقاط الموجات الكهرومغناطسية الصادرة عن الحاسب الآلي أثناء تشغيله وباستخدام هوائيات موصلة بحاسبة خاصة"<sup>44</sup>.

ونظرا لما تمثله القرصنة في وقتنا الحاضر من تهديد لمستقبل التقنية وصناعة المعلومات فأصبحت هذه الأخيرة تثير إشكالا يتعلق بطبيعة المعلومات الخاصة ذلك أن ليس لها كيان مادي محسوس وتبقى في حيازة مالكة وبالتالي يثور تساؤل حول ما إذا كانت المعلومات تصلح محلا لجريمة السرقة أم لا ؟

ومما لا شك فيه أن المعلومات وإذا كانت تثير إشكالا في مدى إعتبارها من الأموال التي يمكن سرقتها، إلا أنه من المسلم بيه أن هذه المعلومات إبتداءا يمكن أن تترجم إلى قيم

43 - أ - رشيدة بوكر ، مرجع سابق، ص285- 286 - 290.

44 - إنتصار نوري الغريب، أمن الكمبيوتر والقانون، دار الراتب الجامعية ، بيروت، سنة 1994، ص57.

مالية نظرا لقابليتها للإستغلال، مقارنة بالبرامج التي هي نوع من الإبداع الذهني والفكري، وبما أن البرامج عبارة عن أسلوب يضم العمل والمعالجة فإن إستخدام هذا الأسلوب بصورة غير مصرح بها من قبل مالكيها أو حائزها الشرعي يشكل إعتداء على حقوق الإستغلال المالي.

وكذلك فإن المعلومة بما تمثله من صفة السرية يمكن الإعتداء عليها بمجرد الإطلاع عليها دون إذن صاحبها لأن هذا يمثل إنتهاكا لسرية المعلومة .

وبتحليل عناصر جريمة السرقة كون المال فيها يكون منقولاً ومملوكاً للغير ونقل حيازته من حائزه الشرعي إلى سارق فإننا نرى وجوب عدم قياس نصوص السرقة التقليدية على السرقة المعلوماتية بإعتبار أن معظم التشريعات لا تعترف بسرقة المعلومات بل بالوصول غير المصرح لها وإختراقها وتقليدها والإستلاء عليها ونسخها نسخاً غير مشروعاً

45

وفي ظل الخلاف الفقهي الوارد بشأن قابلية هذه البرامج لتطبيق الأفعال المكونة لجريمة السرقة عليها عن عدمه مما يدعو بالتالي إقتراح أن يتدخل المشرع بنصوص صريحة لمواجهة هذه الظاهرة الجديدة للإجرام التي تعيش على هامش القانون مستغلة بذلك النقص والثغرات التي توجد بالتشريع القائم<sup>46</sup>.

### ثانياً : إتلاف معلومات وبرامج الحاسب الآلي

ويقصد بإتلاف برامج الحاسب الآلي ومعلوماته إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ويطلق عليها مصطلح تدمير نظم المعلومات *sabotage informatique* وعادة لا يستهدف مرتكب هذا الإعتداء فائدة مالية لنفسه بل مجرد إعاقة نظام المعلومات عن الأداء بوظائفه وإحداث الضرر.

<sup>45</sup> - محمود أحمد عابنة، مرجع سابق، ص 94 - 95.

<sup>46</sup> - أ - خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر 2010، ص 55 - 56.

والمقصود من الإتلاف في هذا المقام ليس الإتلاف المادي، وإنما ذلك الذي يوجه إلى جانب المنطقي والمعنوي في الحاسب الآلي الذي بات يشكل قيمة إقتصادية عالية فإتلاف برامج ومعلومات الحاسب الآلي فيه إفقاد لمنفعة هذه البرامج والمعلومات .

وترتكب جرائم إتلاف البرامج والمعلومات عن طريق قنابل منطقية<sup>47</sup>، أو عن طريق برامج الدودة والفيروس « virus » ، الذي يقصد به " برنامج ثم إعداده من قبل شخص أو أكثر على درجة متقدمة من العلم بالبرمجة باستخدام تقنيات متطورة، بحيث يكون من خصائص هذه البرامج الإنتقال الى أجهزة الحاسب الآلي والتكاثر والإنتشار فيها وهي برامج غير مرئية بالطرق العادية وتحتاج إلى أسلوب علمي للكشف عنها".<sup>48</sup>

وبسبب الفيروسات التي تنتشر في أجهزة الحاسب المتصلة بالشبكات العامة والخاصة المتعلقة بإتصال بين الحواسيب تدمر البرامج والمعلومات المخزنة داخل الجهاز، بحيث يتعطل عن العمل والقيام بوظائفه وتضليل مستخدميه وضياع بياناته وتحويله إلى آلة صماء لا فائدة منها.<sup>49</sup>

لذلك يستوجب الأمر توفير حماية للمكونات المعنوية عن طريق نصوص تشريعية خاصة تراعي خصوصيتها لأن العقوبات البسيطة التي وضعت في ق.ع. لا تحقق قمع وردع جريمة إتلاف المعلومات لأنها خاصة بإتلاف الأموال المادية الملموسة ليست معنوية.

50

47 - القنابل المنطقية أو الزمنية : تعرف بانها برامج أو جزء من برنامج ينفذ في لحظة محددة، أو كل فترة زمنية منتظمة، يوضع على شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل عمل غير مشروع. عن الدكتور محمد سامي الشوا، ثورة المعلومات وانعكساتها على القانون العقوبات، دار النهضة العربية، القاهرة، سنة 1994، ص 194.

48 - د - أسامة محمد محي الدين عوض، جرائم الكمبيوتر، بحث مقدم إلى مؤتمر السادس للجمعية العربية للقانون الجنائي ، ص 425.

49 - محمد أحمد عباينة، مرجع سابق ، ص 101.

50 - أ- رشيدة بوكر، مرجع سابق، ص 114.

## ثالثا : التزوير المعلوماتي

هو أي تزوير يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم بطريقة الطابعة أو كانت مرسومة عن طريق الراسم، ولذلك فالتزوير المعلوماتي قد يرد في محرر مكتوب بلغة سواء باللغة العربية أو بأية لغة أخرى مفهومة ولها دلالتها، وكذلك قد يتم في مخرجات ورقية غير مكتوبة أي مصورة ظلما كانت الصورة محل إعتبار في محرر أو مستند ويترتب عليها إثبات الحق أو أثر قانوني معين.<sup>51</sup>

كما عرفت المادة الرابعة جريمة التزوير المعلوماتي من القانون النموذجي العربي الموحد بشأن مكافحة الجريمة المعلوماتية على أنه: "كل من زور المستندات المعالجة آليا أو البيانات المخزنة في ذاكرة الحاسوب، أو على شريط أسطوانة مغنطة أو غيرها من الوسائط يعاقب ب .... وتترك العقوبة وفقا لكل دولة".

كما نصت الفقرة الثانية من المادة الرابعة من نفس القانون على أنه: "كل من إستخدم المستندات المزورة آليا مع علمه بتزويرها يعاقب بنفس عقوبة التزوير، فإذا كان المستخدم هو نفسه مرتكب فعل التزوير يعاقب وفقا للقواعد العامة المعمول بها في هذا الشأن".<sup>52</sup>

فالتزوير في صورته التقليدية هو تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون، تغييرا من شأنه أن يرتب ضررا للغير وبنية إستعمال هذا المحرر فيما أعد له.

أما التزوير المعلوماتي فهو تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية إستعمالها.<sup>53</sup>

<sup>51</sup> - د - خيرت علي محرز، التحقيق في الجرائم الحاسب الآلي، القاهرة، سنة 2012، ص 170 - 171.

<sup>52</sup> - المادة 2 و 4 من القانون النموذجي العربي الموحد لمكافحة الجرائم المعلوماتية وما في حكمها، الدورة 19 بقرار رقم 495 في 2003/10/08.

<sup>53</sup> - د فوزية عبد الستار، قانون العقوبات ( القسم الخاص ) ، دار النهضة العربية، بدون بلد النشر، سنة 1988 ص 244.

وما يمكن ملاحظته في جريمة التزوير المعلوماتي أنها أثارَت جدلا واسعا وتساؤلات كثيرة في الجانب الفقهي وكذا القضائي، وأبرزها كان القضاء الفرنسي وكانت تلك التساؤلات تدور حول مدى كفاية نصوص القوانين التقليدية للإلتحاق على التزوير المعلوماتي؟.

وعلى هذا الأساس وبعد صدور القانون الفرنسي الجديد في 16/12/1992 قرر المشرع لفرنسي عدم ضرورة الإبقاء على التجريم الخاص بتزوير المستندات المعالجة آليا وإستعمالها، والإكتفاء بإضافة إلى جريمة التزوير العادية، ولعل من أهم الأسباب التي أدت بالمشرع الفرنسي إلى إدراج هذه الجريمة ضمن جرائم التزوير العادية للمحررات هو أنه بصدور هذا القانون خرجت جريمتا تزوير المستندات المعالجة آليا وإستعمالها من بين جرائم الإعتداء على نظام المعالجة الآلية للمعطيات، وهو أمر منطقي يجد مبرر في إختلاف المصلحة المحمية بالقانون والتي تقف وراء تجريم كل منهما، فالمصلحة المحمية من تجريم الإعتداء على نظام المعالجة الآلية للمعطيات هي مصلحة فردية تخص صاحب هذا النظام المعلوماتي، في حين أن المصلحة التي يحميها القانون بصدد جريمة التزوير في المستندات والمحررات المعلوماتية فهي حماية الثقة العامة المقترحة في هذه المستندات أيّا كان شكلها، ومن خلال هذا المنطلق يمكن القول أن المشرع الفرنسي قد عاقب على جريمتي تزوير المستندات المعلوماتية من جهة، وإستعمالها من جهة أخرى<sup>54</sup>.

ونخلص إلى إن المشرع الجزائري رغم تداركه من خلال القانون 15/04 المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الإعتداءات الواردة على الأنظمة المعلوماتية بإستحداث نصوص خاصة إلا انه أغفل تجريم الإعتداءات الواردة على المنتوجات الإعلام الآلي، فلم يستحدث نصوصا خاصا بالتزوير المعلوماتي، ولم يتبنى

<sup>54</sup> - أ - خثير مسعود ، مرجع سابق، ص 132 - 133.

أُتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث، رغم أنها تعتبر من أخطر صور الغش المعلوماتية .<sup>55</sup>

---

<sup>55</sup> - آمال قارة ، الحماية الجزائرية للمعلوماتية في التشريع الجزائري ، الطبعة الثانية ، دار هومه للطباعة والنشر والتوزيع، الجزائر ، سنة 2007، ص 140.

**المطلب الثاني : المعلوماتية وسيلة لإرتكاب الجرائم**

صاحب ظهور شبكة الأنترنت تطورات كبيرة في شتى المجالات، ورغم الفوائد التي أتت بها إلا أنها أصبحت سلاح فتاك في يد المجرمين الذي يمس سلامة الأشخاص وحياتهم الخاصة، وكذا الجرائم التي تقع على الأموال والسطو عليها بل تعد الأمر إلى المساس بأمن الدولة وهذا ما سنتطرق إليه في الفروع الآتية:

**الفرع الأول : الجرائم الواقعة على الأشخاص****أولا : جريمة القذف والسب عبر الأنترنت**

تعد جرائم القذف والسب من الجرائم التي لها الأثر البالغ سلبا على الأشخاص وهي الأكثر شيوعا وانتشارا خاصة بعد ظهور شبكة الأنترنت، وإساءة إستخدامها لنيل من شرف الغير أو كرامته أو إعتباره.<sup>56</sup>

والقذف هو إسناد واقعة معينة تستوجب العقاب في حالة الصدق على من تنسب إليه وذلك بشكل علني.

أما السب هو الإسناد العمدي لواقعة غير معينة إلى المجني عليه خادشة بذلك لشرفه وإعتباره.<sup>57</sup>

هذا ما قد يعرض الضحية إلى بغض الناس وإحتقارهم بما تم إرساله للمجني عليه، على شكل رسالة بينات ويعني بذلك المعلومات التي تم إنشائها أو إرسالها بوسائل إلكترونية وبالتالي توافر عنصر العلنية في هذه الجرائم بسبب عرضها على المواقع والرسائل الإلكترونية تتسبب في أضرار كبيرة للأشخاص.<sup>58</sup>

<sup>56</sup> - د - خالد ممدوح إبراهيم، فن التحقيق الجنائي في جرائم الإليكترونية، الطبعة الاولى، دار الفكر الجامعي لشرف الإسكندرية، سنة 2009، ص 319.

<sup>57</sup> - د - فوزية عبد الستار، شرح القانون الإجراءات الجنائية، دار النهضة العربية، سنة 1979، ص 592.

<sup>58</sup> - د - خالد ممدوح إبراهيم/ مرجع سابق، ص 333.

**ثانيا : صناعة ونشر الإباحة**

إذا كان لشبكة الأنترنت وجه إيجابي فإن لها وجه سلبي أيضا، ومن هذه الأوجه وجود مواقع على شبكة الأنترنت تحرض على ممارسة الجنس لكبار والصغار على حد سواء، وتقوم هذه المواقع بنشر صور فاضحة للبالغين والأطفال<sup>59</sup>.

حيث يضر إستخدام الأطفال المستخدمين في إنتاج هذه المواد و الإعتداء عليهم في كل مرة يتم فيها عرض هذه صور.<sup>60</sup>

**ثالثا : إنتحال الشخصية والتغريب والإستدراج.**

يقصد بإنتحال الشخصية ما يعيد إليه المجرم من إستخدام شخصية شخص آخر للإستفادة من سمعته مثلا أو ماله أو صلاحياته، ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستخدمين على شبكة الأنترنت، وتتخذ جريمة إنتحال الشخصية عبر الأنترنت أحد الوجهين التاليين: إنتحال شخصية الفرد وإنتحال شخصية المواقع.

أما فيما يخص التغريب والإستدراج فغالبا ما يكون ضحيا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة، حيث يوهم المجرمين ضحاياهم برغبتهم في تكوين صداقة على الأنترنت والتي قد تتطور إلى إلتقاء مادي بين الطرفين.

إن مجرمي التغريب و الإستدراج على شبكة الانترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر ويكون معظم الضحايا هم من

<sup>59</sup> – FAUCHMOUX ، VINCENT Daprery pierre, le Droit de l'internet (loi ,contra et sage) , édition , lutec , paris ,2008,p215.

<sup>60</sup> – كريستينا سكولمان، عن جرائم الأنترنت طبيعتها وخصائصها، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر المملكة المغربية، سنة 2007، ص 40.

صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها، حيث لا يدري الكثير من الضحايا أنهم غرر بهم.<sup>61</sup>

### الفرع الثاني : الجرائم الواقعة على الموال

#### أولاً : السرقة عبر الأنترنت

تعرف السرقة بانها إختلاس الشيء منقول للغير دون رضاه بنية إمتلاكه<sup>62</sup>، وتتم سرقة - المال المعلوماتي - إن أمكن الوصف عن طريق إختلاس البيانات والمعلومات والأستفادة منها بإستخدام السارق للمعلومات الشخصية، مثل الإسم، العنوان، الأرقام الخاصة بالمجني عليهم والإستخدام غير شرعي لشخصية المجني عليه، ليبدأ عملية السرقة المتخفية عبر الأنترنت بحيث يؤدي بالغير إلى تقديم الأموال - الإلكترونية أو المادية- إلى الجاني عن طريق التحويل البنكي<sup>63</sup>.

تتجسد جريمة السطو على أموال البنوك عن طريق إستخدام الحاسب الآلي للدخول إلى شبكة الأنترنت والوصل غير المشروع إلى البنوك و المصارف والمؤسسات المالية<sup>64</sup>.  
ثانياً : الجرائم التي تنجر عن إساءة إستخدام البطاقة المصرفية .

نظراً للإنتشار الواسع لهذه البطاقات الممغنطة وعلى رأسها بطاقات السحب من المصارف، فقد أدى هذا إلى الزيادة في إساءة إستخدام هذه البطاقة من أجل الحصول على المنفعة المالية غير المشروعة سواء من قبل حاملها الشرعي أو من قبل الغير، وفي هذا شيء من التفصيل.

<sup>61</sup> - عمرو موسى الفقهي، الجرائم المعلوماتية، جرائم الحاسب الآلي و الأنترنت في مصر و الدول العربية، المكتب الجامعي الحديث، الإسكندرية، سنة 2006، ص 102.

<sup>62</sup> - نايف بن محمد المرواني ، جريمة السرقة ، دراسة نفسية إجتماعية ، جامعة نايف العربية للعلوم الأمنية، الرياض الطبعة الاولى، سنة 2011، ص 59.

<sup>63</sup> - د - محمد أمين أحمد الشوابكة ، جرائم الحاسوب و الأنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، سنة 2004، ص 138.

<sup>64</sup> - عباس أبو شامة عبد المحمود، عولمة الجريمة الإقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2007، ص 20.

**1- إساءة استخدام البطاقة من قبل حاملها الشرعي:**

ترتكب هذه الجريمة من قبل حامل البطاقة الشرعي الذي بإسمه وتتعلق بحسابه ويعلمه وبعده فروض، اما عن رصيده غير كافي لسحب المبلغ او أن الرصيد مغلق مستغلا إختراقه والتلاعب به وذلك بعد إشعاره من قبل المصرف بإلغائها او بعد إنتهاء مدة صلاحيتها.

**2- إساءة استخدام البطاقة المصرفية من قبل الغير:**

فقد يعمل الجاني على سرقتها من حاملها الشرعي، وقد يعثر عليها ومعها الرقم السري وتختلف بطاقة سحب النقود من أجهزة التوزيع التابعة للمصرف عن بطاقة الإئتمان والتي باتت في إطار الإنتشار الهائل مع زيادة الاستخدام لشبكة الأنترنت وإزدياد حجم التجارة الإلكترونية هدفا منشودا من قبل المجرمين.<sup>65</sup>

**ثالثا : جرائم غسيل الأموال عبر الأنترنت**

تعد جرائم غسيل الأموال من أخطر جرائم عصر الإقتصاد الرقمي، فهي التحدي الحقيقي أمام مؤسسات المال و الأعمال وتعد الإختبار الأمتل لقدرة القواعد القانونية على تحقيق الفعالية في مواجهة الأنشطة الإجرامية ومكافحة الأنماط المستحدثة منها : فهي كغيرها من الجرائم الإقتصادية جريمة ذوي الباقات البيضاء التي ترتكب من قبل محترفي الإجرام التي لا تتلائم سماتهم مع السمات الإجرامية التي عرفتها وحددتها النظريات الكلاسيكية المتعلقة بعلم الإجرام والعقاب.

وجريمة غسيل الاموال بعد تفجر ثورة الإتصالات وإزدهارها إتجه غاسيلوا الأموال القدرة إلى تطوير وسائلهم وإستحداث وسائل جديدة لغسل الأموال مستفدين في ذلك من وسائل التكنولوجيا الحديثة وعلى رأسها شبكة الأنترنت، كما لجأوا إلى الأنظمة الحولات الإلكترونية بدأ من البرقيات و الإيداعات والمسحوبات التقنية، وذلك عن طريق أجهزة

<sup>65</sup> - محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ماجستير في القانون الجنائي المعلوماتي، الطبعة الأولى دار الثقافة للنشر والتوزيع ، عمان، الأردن سنة 2009، ص 63 إلى 65.

الصرف الآلي وغيرها من الوسائط التكنولوجية الحديثة، ومن هنا برز ما يعرف بالغسيل الأموال الرقمي.<sup>66</sup>

### الفرع الثالث : الجرائم الواقعة على أمن الدولة

#### أولاً : الجرائم الماسة بالأمن الفكري

ينطوي الخوف من عواقب الثورة المعلوماتية والإتصال التي مست بثقافة وقيم ومفاهيم قواعد المجتمع المادية والتربوية بإعتبار ان الشبكة العالمية للإنترنت منحت المستخدم الكثير من الخيارات من خلال عدم خضوعها لأي رقابة وعبورها للحدود الجغرافية بين الدول، ونموها السريع والمتواصل، وإمكانية مشاركة الجميع من مختلف الدول العالم .

إضافة إلى الكم الهائل من المعلومات التي يمكن الحصول عليها من عدّة مصادر لا يمكن التحكم فيها ومتابعتها أو الإشراف عليها، كل ذلك جعل هذه الشبكة من أهم المقومات المجتمع المعلوماتي، والتي تؤدي إلى الإنحراف الفكري من خلال تعرض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العلمية للإنترنت، وتهدد الامن بأبعاده كافة.<sup>67</sup>

#### ثانياً : الجريمة المنظمة

الجريمة المنظمة ليست وليدة التقدم والسهولة وإن كانت إستفادت منه فالجريمة المنظمة وبسبب تقدم وسائل الإتصال والتكنولوجيا أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، بل أصبح إنتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود

<sup>66</sup> - د - خالد الممدوح إبراهيم، مرجع سابق، ص 452 - 455.

<sup>67</sup> - ناصر محمد البقهي، أثر التحويل المجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف عبد العزيز لدراسات الأمن الفكري بجامعة الملك سعود، المملكة العربية السعودية ، سنة 2009، ص 87.

سامي علي عياد، الجريمة المعلوماتية و الإنترنت ( الجرائم الإلكترونية)، الطبعة 1 ، منشورات الحلبي الحقوقية بيروت ، 2007، ص 83.

الجغرافية، كما إستغلت عصابات الجريمة المنظمة الإمكانات المتاحة في وسائل الأنترنت في تخطيط وتمير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بسهولة. وبذلك إكتشفت جماعات الجريمة المنظمة إستخدام التكنولوجيات بصفتها فرص للإستغلال وتحقيق الأرباح غير مشروعة، ويرجح أن الترابط بين الجريمة المنظمة وشبكة الأنترنت في تطور إلى حد بعيد في المستقبل في عالم الجريمة.<sup>68</sup>

ثالثا : الإرهاب

أصبح يتم بث الإرهاب في الوقت الراهن ظاهرة عالمية ترتبط بعوامل إجتماعية وثقافية وسياسية وتكنولوجية أفرزتها التطورات السريعة والمتلاحقة في العصر الحديث<sup>69</sup>، حيث أصبح بث ثقافة الإرهاب عبر الأنترنت عن طريق تأسيس مواقع إفتراضية تمثل المنظمات الإرهابية، وأصبحت الجماعات الإرهابية تجند عناصر جديدة من خلال الأنترنت فتعلن عبر مواقعها على الأنترنت حاجتها إلى عناصر إنتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب ، مستخدمة في ذلك الجانب إلى الجهاد وحثهم إلى الإستشهاد في سبيل الفور بالجنة.<sup>70</sup>

أضحت المواقع الإلكترونية تتيح للجماعات الإرهابية قدرا كبيرا من التحكم في المعلومات والرسائل الإعلامية التي تريد توجيهها لفئات مختلفة من الجمهور ورسم صورة ذهنية عن الجماعة عن أعدائها أيضا.<sup>71</sup>

<sup>68</sup> - سامي علي عياد، الجريمة المعلوماتية و الأنترنت ( الجرائم الإلكترونية)، الطبعة 1 ، منشورات الحلبي الحقوقية ، بيروت ، 2007،ص 83.

<sup>69</sup> - عبد الله بن عبد العزيز يوسف، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية، الرياض ، الطبعة الأولى ، سنة 2004، ص 25.

<sup>70</sup> - محمد سيد سلطان/ قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر والتوزيع الإلكتروني، 2004،ص 13.

<sup>71</sup> - Debray Stephan, internet face aux substances illicites, université de paris, 2002-2003,p13.

## رابعاً : جريمة التجسس الإلكتروني

عمليات التجسس والتنصت هي عملية قديمة قدم البشرية وبقدر النزعات، فمنذ قدم العصور كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم وخططهم ، إلا أنه وبظهور عصر المعلومات والاتصالات وإزدهاره تحولت وسائل التجسس والتنصت من الطرق التقليدية إلى الطرق الإلكترونية لا سيما مع استخدام شبكة الأنترنت وإنتشارها الواسع على مستوى العالم.

ويكمن الخطر الحقيقي في عمليات التجسس التي تقوم بها الأجهزة الإستخبارتية للحصول على أسرار أو معلومات الدولة، ومن ثم إفشائها لدول أخرى تكون عادة معادية لها، أو إستغلالها بما يضر بالمصلحة الوطنية للدول<sup>72</sup>.

وتستهدف عملية التجسس في عصر المعلومات ثلاثة أهداف رئيسية، وهي التجسس العسكري، التجسس السياسي ، التجسس الإقتصادي.<sup>73</sup>

<sup>72</sup> - د - خالد ممدوح إبراهيم، مرجع سابق، ص 338 و 339.

<sup>73</sup> - علي عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى ، منشورات زين الحقوقية ، دمشق، 2011، ص 96-97.

## الفصل الثاني

النظام القانوني لجريمة دخول غير

مشروع

**تمهيد**

تقوم الجريمة بشكل عام على توافر الأركان الأساسية لها، وهو ما يطبق أيضا على الجرائم المعلوماتية ففي هذا الصدد نقوم بدراسة جريمة الدخول والبقاء الى أنظمة المعالجة الآلية للمعطيات، وهذا من خلال تبيان وتوضيح ما جاء في نصوص القانون من ركن شرعي، إضافة إلى قيام الركن المفترض الذي يعني أساسا وجود نظام معالجة آلية، وتوافر الحماية لهذا النظام، إلى جانب الركن المادي، وزيادة على ذلك وجود نية لدى الجاني لإرتكاب هذا النوع من الجرائم، ذلك أن الجريمة لا تقوم إلا بتوافر القصد العام لإرتكابها وهذا ما ينطوي عليه الركن المعنوي.

وقد صادقت الكثير من الدول العربية والغربية على إتفاقية بودابست لمكافحة الجريمة المعلوماتية، وأصدرت هذه الدول عقوبات مختلفة لها.

ولكي يتضح لنا المجال القانوني الذي تدور فيه جريمة الدخول و البقاء لابد من دراسة محتواه من خلال الأركان و العقوبات، هذا ما سنتطرق إليه من خلال:

المبحث الأول: أركان جريمة الدخول والبقاء الغير مشروع

المبحث الثاني: العقوبات المقررة للجريمة دخول غير مشروع

**المبحث الاول : أركان جريمة الدخول الغير مشروع**

تبنى المشرع الجزائري بموجب الأمر 04/15 المؤرخ في 20 ربيع الثاني 1436هـ الموافق 10 / فبراير 2015 المعدل و المتمم للأمر 66 - 156 المتضمن قانون العقوبات نصوصا خاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، أو ما يصطلح عليها بالجريمة المعلوماتية أو الإلكترونية والتي تندرج ضمنها جريمة الدخول و البقاء الغير مشروع و التي تشكل بدورها كل فعل أو امتناع من شأنه الاعتداء على الكيانات المعنوية بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات ، ولقد ورد نص على هذه الجرائم والعقوبات المقررة لها في المواد 394 مكرر إلى 394 مكرر<sup>74</sup>.

و لقد نص المشرع الجزائري في المادة 394 مكرر من قانون العقوبات الجزائري على ما يلي : " يعاقب..... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات ، وتضاعف العقوبة إذ ترتب على ذلك حذف أو تغيير للمعطيات المنظومة ، وان ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة

**المطلب الأول : الركن المادي للجريمة**

يتكون الركن المادي لجريمة الدخول والبقاء الغير مشروع من سلوك ونتيجة وعلاقة السببية. من خلال استقراء نص المادة 394 مكرر من قانون العقوبات فإن الدخول إلى نظام المعالجة الآلية يتخذ صورة الدخول المنطقي وذلك بغرض فتح باب يؤدي إلى نظام المعالجة الآلية بمكوناته المختلفة وأحيانا يتخذ صورة البقاء و ينصب هذا الفعل المجرم على محل من نوع خاص و الذي يتمثل في النظام System, والذي يقصد به مجموعة البرامج التي تساعد في تشغيل الحاسب الي ذلك أن الأعمال الداخلية للحاسب معقدة للدرجة التي لا نستطيع معها التعامل مع الحارب مباشرة بدون استخدام برامج تساعدنا على التعامل معه , وهذا ما

<sup>74</sup> - الجريدة الرسمية للجمهورية الجزائرية وعدد06, للأمر 15 -04 المؤرخ في 10 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع و التسبق الإلكتروني

التعامل مع الحاسوب مباشرة بدون استخدام برامج تساعدنا على التعامل معه , وهذا ما تقوم به برامج النظام و هي تشمل نظام التشغيل operating system و البرامج المساعدة utility programs ونظم إدارة قواعد البيانات Data base management بالإضافة إلى برامج ترجمة اللغات compiler<sup>75</sup>.

و الواقع أن برامج النظام تقوم بالعديد من المهام ولعل من أهمها الإشراف ودعم التشغيل الرئيسي للجهاز الذي يشمل الخدمات الجوهرية التي تحتاج إليها و تستعملها برامج التطبيقات و كذلك للتحكم و السيطرة على مكونات الحاسوب و أداء العمليات الأساسية التي تساعد المستخدم على التعامل مع هذه المكونات.

و من مهام برامج النظام أيضا السماح لعدة مستخدمين بالتعامل مع نفس الحاسب في ذات الوقت بالإضافة إلى التعامل مع شبكات الحاسب التي تستخدم وحدات طرفية بعيدة (Remonte terminales), و قد ينصب الدخول و البقاء الغير مشروع على برامج التطبيقات ( Application program software ) وهي البرامج التي تصمم للقيام بمهام محددة , ومن أمثلة ذلك .....برامج معالجة الكلمات و النصوص ( ward processing)

spread sheet و هناك طائفتان من برامج التطبيقات , تتمثل الأولى في برامج التطبيقات سابقة التجهيز Ready made application pack ages و هي تلك البرامج التي خطت و كتبت لنتحكم في معالجة و حل مهمة خاصة , وتتقسم إلى البرامج التطبيقية ذات الوظائف المتكاملة و هو عبارة عن وحدة واحدة تحتوي على مجموعة من البرامج المركبة التي تؤدي وظائف يكمل بعضها بعضا .

<sup>75</sup> - عبد القادر القهوجي , الحماية الجنائية لبرامج الحاسب الآلي , دار الجامعة للطباعة و النشر , مصر , 1999 ص

أما الثانية فهي برامج التطبيقات طبقا لاحتياجات العميل Application programs و User developed وهي برامج يعدها خبير البرمجة Programmer و خصيصا العميل معين بناء على اتفاق مع هذا العميل لتكون صالحة للوفاء بحاجة منشأه , فهي برامج تفصل حسب رغبة و حاجة العميل .

لكن قبل ذلك : هل تعد الحماية عنصرا في المادي لهذه الجريمة أو بعبارة أخرى هل الحماية الفنية تعد شرطا حتى تسبغ الحماية الجزائية على نظام المعالجة الآلية ؟

لم ينص المشرع الجزائري لا من قريب ولا من بعيد إلى ذلك ، ومن المبادئ العامة والمستقرة في تفسير القانون الجزائري ، أنه لا يجوز إضافة عنصر ما لم ينص عليه القانون فإن عدم ذكر المشرع العنصر الحماية الفنية يعني أن المشرع أراد استبعاده والواقع العملي يكشف أن غالبية نظم المعالجة الآلية تتمتع بالحماية الفنية على درجة عالية من الكفاءة ، بل هناك شركات متخصصة في تقديم خدمات التأمين الفني المعلوماتي ، وذلك في ظل تنامي الاعتماد على نظام المعالجة الآلية وهو الرأي الذي استقر عليه القضاء الفرنسي وأكدته في عدة أحكام له من ذلك حكم محكمة استئناف باريس المشهور في 5 أبريل لعام 1994 بحيث جاء في حيثياته "من غير الضروري لقيام جريمة الدخول الغير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسؤول عن النظام<sup>76</sup> .

<sup>76</sup> - أبوكر رشيدة , جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن , منشورات حلبي الحقوقية , الطبعة الأولى 2012 .

وبناء على ذلك سوف نتعرض للركن المادي لهذه الجريمة من خلال الفرعين التاليين

### الفرع الأول : السلوك

ويمثل النشاط الجرمي المكون للركن المادي لهذه الجريمة ويتمثل إما في فعل الدخول إلى نظام المعالجة الآلية أو في جزء منه ، وإما في فعل البقاء في هذا النظام أو في جزء منه .

### أولاً : الدخول الغير مصرح به

لا يقصد بالدخول في هذه الحالة الدخول بمعناه المادي ، وإنما يجب أن ينظر إليه كظاهرة معنوية ، تشابه الدخول إلى فكر أو إلى ملكة تفكير لدى إنسان ووفقاً لهذا التصور المعنوي لفكرة الدخول فإنه يتحقق بأي صورة من صور التعدي سواء كان بطريق مباشر عن طريق نظام المعالجة الآلية للمعطيات الذي يحوي على المعلومات والنظام ، أو غير مباشر عندما يدخل الفاعل إلى هذه المعلومات أو النظام عن طريق نظام آخر يتصل بالأول بواسطة شبكة الإتصالات ويتم ذلك عن طريق اعتراض النظام الأول .

::

وتقع هذه الجريمة من كل إنسان أياً كانت صفاته ، وسواء تم الدخول إلى النظام كله أو جزء منه فقط ، لا كن لا يعني ذلك الدخول إلى جزء لا علاقة له بنظام المعالجة الآلية بل يجب أن يشارك فعلياً في نظام المعالجة الآلية . وتجدر الإشارة إلى أن الدخول غير مصرح به إلى نظام المعالجة الآلية يتحقق بأحد الأمرين:

- أولهما : ألا يكون هناك تصريح بالدخول بتاتا لدى من يقوم بالدخول .

- ثانيهما : ألا يوجد تصريح بالدخول ولكن المصرح له يقوم بتجاوز الحدود التي رسمت له في هذا التصريح.

وقد جرم قانون جرائم الكمبيوتر في ولاية (Tennessee) الأمريكية الدخول بدون وجه حق وبقوله كل من يتداخل أو بسبب تداخل الغير أو يحاول التداخل مع عمله بذلك في برامج الكمبيوتر أو البيانات التي يحتويها أو في نظام الكمبيوتر أو شبكة الكمبيوتر أو أي جزء منه بقصد الحصول على نقود أو أموال أو خدمات لنفسه أو للغير بالاستعانة بإدعاء كاذب أو انتحال شخصية الغير أو بوعود كاذبة<sup>77</sup>.

وقد عني قانون ولاية (Tennessee) سابق الذكر بتعريف الدخول بدون وجه حق أنه يعني كل وسيلة للإطلاع أو لإعطاء تعليمات أو للاتصال أو لتخزين بيانات أو لاستعادة بيانات أو للاتقاط بيانات من نظام الكمبيوتر أو شبكة الكمبيوتر ، غير أننا نخالف ما ذهب إليه قانون ولاية (Tennessee) من اعتبار التقاط إرسال الكمبيوتر عن بعد من قبيل الدخول ، ذلك أن المتهم لا يدخل في وظيفة من وظائف النظام عن بعد ويختلف عن المستخدم برنامجا يسمح له بالدخول إلى نظام والإطلاع على محتوى الجهاز, فالأمر عندئذ يشكل نوعا من التداخل<sup>78</sup>.

و تجدر الإشارة أن فعل الدخول يقع على حق من حقوق صاحب النظام على المعلومات فالجريمة من جرائم الأموال وقد عالجها المشرع الفرنسي في الكتاب الثالث من قانون العقوبات الفرنسي الذي خصه لجرائم الأموال بينما عالج تجميع البيانات الشخصية

<sup>77</sup> - د جميل عبد الباقي الصغير القانون الجنائي والتكنولوجيا الحديثة. الكتاب الأول , الجرائم الناشئة عن استخدام الحاسب الآلي) دار النهضة العربية, ص 44.

<sup>78</sup> -Martin wasik ,compter crimes and other crimes against , p 632.

في الكتاب الثاني الذي خصه لجرائم الأشخاص ، لذا فإن فعل الدخول يقع اعتداء على رضا المجني عليه .

و هذا الاتجاه الذي سار عليه المشرع الجزائري ، وتختلف فكرة الدخول عن استعمال النظام وبالتالي فإن المشرع جرم الدخول فإن ذلك لا يعني أن يقوم الفاعل باستعمال الجهاز فدائرة الدخول أضيق من دائرة الاستعمال فكل استعمال النظام دون رضا لصاحبه يعد دخولا بلا ريب فيه أما الدخول فإنه لا يعني بالضرورة استعمال النظام ، فقد يتصل الشخص بالنظام ومن ثمة يكون قائما بالدخول فيه ولكنه لا يستعمل إمكانيات النظام ، كأن يكتفي بالإطلاع على نظام بوسائل سلكية أو بوسائل غير سلكية أو باستعمال برامج خاصة بالافتحاح والفاعل عندئذ يكتفي بالإطلاع دون استعمال النظام .

لذلك حرصت بعض التشريعات مثل التشريع الكندي على تجريم استعمال النظام بدون رضا صاحبه .

ويتم الدخول على النظام بإحدى الوسائل الآتية :

#### أ- تشغيل كمبيوتر مقفل

وتتمثل هذه الطريقة في أن المتهم يقوم بفتح جهاز الكمبيوتر وتشغيله بعد أن كان مغلقا فإذا بدأ العمل فإن المتهم يعتبر قد دخل للنظام بدون وجه حق طالما تم ذلك دون موافقة صاحب الحق .

ونرى أن العبرة ليست هي بتشغيل الجهاز ولاكن بالتمكن من الدخول إلى الملفات ، إذ قد يتمكن المتهم من الدخول إلى الملفات الموجودة داخل النظام على الرغم من أن الجهاز مغلق كما أنه قد يتمكن من تشغيل الجهاز وذلك بإيصال الكهرباء إليه ، دون أن يتمكن من الدخول إلى الملفات ، عندئذ يعتبر نظام المعلومات المبرمجة مقفلا على الرغم من أن الجهاز في وضع (ON) بيد أنه في الحالة الأخيرة يعتبر المتهم قد حاول الدخول إلى الجهاز وهو ما تعتبره بعض التشريعات متساويا في وقوع الجريمة مثل فعل الدخول نفسه<sup>79</sup>.

أما إذا كان الجهاز يعمل بالفعل أي مفتوحا على ملف به معلومات ظاهرة على الشاشة فإن مجرد الإطلاع على تلك المعلومات دون تحريك لوحة المفاتيح لا يتوفر به الدخول الغير مشروع.

#### ب - استعمال كمبيوتر مفتوح

قد يكون جهاز الكمبيوتر قيد الاستعمال ممن له الحق في ذلك فإذا تغافل عنه أو انشغل وقام شخص آخر باستعماله وذلك بأن فتح الملفات المتواجدة فيه فإنه بذلك يكون قد دخل في هذا النظام ويقع منه السلوك وهو فعل الدخول . ويختلف هذا الفرض كما لو كان الكمبيوتر قيد الاستعمال واكتفى المتهم بالنظر إلى الملف الذي كان مفتوحا أمام المستخدم .

#### ج - الدخول عن طريق استعمال كارت تشغيل ينتمي إلى شخص آخر

قد يتمكن المتهم من الحصول على بطاقة الدخول إلى كمبيوتر إحدى الجهات لكن يحصل على خدمة معينة مقتصر تقديمها على أصحاب تلك البطاقات وهذا الدخول إلى النظام عن طريق بطاقة خاصة يحدث عادة في حالة سحب مبالغ من البنوك ، تطبيقا لذلك

قضت محكمة باريس بوقوع الجريمة ممن استخدم بطاقات السحب من ماكينات السحب الآلي مع الرقم السري الخاص بهذا الغير دون موافقته معتبرة ذلك من قبيل فعل الدخول المعاقب عليه<sup>80</sup>.

### ث - الدخول إلى الكمبيوتر عن طريق خط تلفزيوني

قد يتمكن المتهم من الموصل إلى نظام الكمبيوتر عن طريق العبث بخط تلفزيوني المربوط عليه هذا النظام ، فيمكنه هذا من الاتصال بنظام من أنظمة الكمبيوتر وعادة ما يقوم المتهم بذلك بغية التوصل إلى إعطاء أوامر لنظام الكمبيوتر لتحقيق غاية معينة. د- الدخول إلى كمبيوتر إلى كمبيوتر آخر

قد يتمكن المتهم ، وهو يستعمل جهاز بطريقة قانونية ، أن يدخل إلى معلومات في كمبيوتر آخر ، على الرغم من عدم وجود دائرة مشتركة بين الجهازين ويحدث ذلك باستعمال وسائل مختلفة ، منها إجراء توصيلة بدون موافقة صاحب الجهاز الثاني ، ومنها

80 -TGI paris ,26 juin 1995, petites affiches , les mars 1996, n 27, p 4.

التجسس عن بعد باستعمال وسائل تقنية حديثة ( برامج اختراق النظام مثلا ) ودون إجراء أية توصيلات .

وقد يتمكن المتهم من الدخول إلى نظام آخر من أنظمة الكمبيوتر بالاتصال عن بعد بهذا النظام والتوصل لمعرفة كلمة السر والدخول إلى النظام كله أو جزء منه<sup>81</sup>.

ومن التطبيقات على هذه الصورة من صور النشاط الإجرامي إذ يقوم المتهم بالدخول في نظام الكمبيوتر معين ليعطيه أمرا بطريقة مشتركة لتحويل مبلغ مالي إلى حساب معين . وبالمثل فإن المتهم قد يقوم بالدخول إلى أجهزة الكمبيوتر الخاصة بخدمة التلفزيون ويتمكن من الحصول على مكالمات تلفزيونية مجانية ، ومما هو ملاحظ أن شبكة الانترنت تسهل استعمال تلك الوسيلة في الدخول إلى أنظمة الغير التي تتصل بتلك الشبكة ، وفي نفس الوقت تجعل من الصعب تحديد شخصية المتداخل الذي قد يدخل جهاز آخر مرورا بجهاز ثالث كما انه قد يقوم بذلك من خارج البلاد.

#### هـ - الدخول إلى نظام متصل بنفس الكمبيوتر بدائرة واحدة

يقوم المتهم في هذه الحالة باستعمال جهاز كمبيوتر بطريقة قانونية فقد يكون جهازه وقد يكون جهاز شخص آخر يقوم باستعماله بموافقة منه لكنه يستعمل هذا الجهاز في الدخول إلى أنظمة أخرى يتصل بها هذا الجهاز ويتاح له الدخول فيها ، ويفترض هذا النشاط المعاقب عليه أن المتهم ليس من حقه الدخول في النظام فإذا كان من حقه هذا الدخول فلا جريمة تقع<sup>82</sup>.

81 - Aix, En, Provence , Gaz,Pal ,Latry Bonnat,Rev.Se.Cri .1998 ,p140

82 -Travaux De L'Institute Sciences Cri Min elles De Poitiers Informatique Et Droit Pénal ,Ed 1983 P 25.

## ثانيا : البقاء الغير المصرح به

جريمة البقاء تتحقق متى دخل الجاني عن طريق الخطأ أو الصدفة ، إلا انه يقرر البقاء داخل النظام وعدم قطع الاتصال به ، وعلى ذلك فإن الركن المادي يتمثل في نشاط إيجابي يتطلب من الجاني القيام به، هو قطع الاتصال ، وامتناعه عن قطع الاتصال مع النظام يحقق السلوك الإجرامي لقيام الجريمة ، ومن ثمة فإن الجريمة من جرائم النشاط الإيجابي الذي يتحقق بالترك أو الامتناع .

وتأسيسا على ما سبق ذكره يتضح لنا أن طبيعة البقاء هي نفس طبيعة الدخول ومن ثم ينطبق عليها كل ما قيل في طبيعة الدخول غير مصرح به لا كن ما يميزه عن الدخول أمه جريمة مستمرة ، فالسلوك الإجرامي في البقاء يستمر و يستمر معه الاعتداء على المصلحة القانونية ، أي سرية المعلومات بينما الدخول جريمة وقتية سواء كان مجردا أو أدى إلى نتائج معينة ، لأن الجريمة تكتمل في اللحظة التي يتم فيها الدخول إلى النظام وعليه إذ لم بنص المشرع صراحة على البقاء فلا يمكن سحب أحكام جريمة الدخول إليه .

وتجدر الإشارة أن لكل فعل من الأفعال التي نص عليها القانون نطاقه ومجاله الذي لا يتداخل فيه مع الآخر فإذا انتفت جريمة الدخول فإن جريمة البقاء لا تنتفي ، وإذا تحققت جريمة الدخول فلا تقع جريمة البقاء لأنها في تلك الحالة هي أثر من آثار الجريمة وليست فعلا إجراميا مستقلا

وكما ذكرنا آفا فإن النشاط الإجرامي يتمثل في بقاء المتهم داخل الكمبيوتر بعد دخوله عرضا أو بطريق الخطأ ، وهناك فرض آخر فقد يدخل المتهم النظام بطريق مشروع ولكنه يستمر بعد الوقت المحدد لبقائه فيه ، وكثيرا ما يحدث ذلك إذا كان استعمال النظام محددًا بوقت معين نظيرا أجر مالي ، فيتخطى المتهم هذا الوقت<sup>83</sup> .

<sup>83</sup> - أبوكر رشيدة ، مرجع سابق ص50 .

وقد أعمل القضاء الفرنسي تجريم البقاء في النظام في قضية تتخلص وقائعها في قيام بعض العاملين في شركة خطوط تلفزيونية باستعمال تلك الخطوط دون دفع مقابل مالي للقيام بألعاب فيديو ، جيم للحصول على جوائز مقررة لمن يستمر في اللعب مدة معينة ، وقد أعمل القضاء وصف البقاء في النظام بطريق الغش ، وليس وصف الدخول في النظام حيث أن هؤلاء العاملين كان من حقهم الدخول في النظام أصلاً لمراقبته والإشراف عليه واصطلاح أعطاله .

فيعد بقاء في النظام ما قام به المتهم من إرسال رسائل عديدة إلى إحدى الشركات المنافسة مثلاً، وذلك من جهاز واحد باستخدام برنامج لإيهام هذه الشركة بصدور هذه الرسائل من أجهزة مختلفة وذلك حتى يمتلأ صندوق الرسائل الخاص بهذه الشركة فلا يستقبل طلبات المتعاملين معها فيتعطل عملها بهذه الطريقة .

ويختلف نشاط الدخول عن البقاء في إحدى الأمرين :

#### أ- الأول أن جريمة البقاء قد لا تصدر دائما من الفاعل في جريمة الدخول

فلا تنسب جريمة البقاء إلى من قام بالدخول والأمر في ذلك يتمثل مع تجريم إخفاء الأشياء المسروقة بالنسبة لجريمة السرقة نفسها ، فالفاعل في جريمة السرقة الذي يحتفظ بالمسروقات بالنسبة لهذه الجريمة لا ينسب إليه أنه قام بارتكاب جريمة أخرى هي إخفاء المسروقات.

هذا التجريم الأخير يخاطب شخصا لم يساهم في جريمة السرقة.

#### ب - الثاني أن جريمة الدخول جريمة مؤقتة أما البقاء فهو جريمة مستمرة

وبذلك فإن فعل الدخول قد يكون مربوط بفترة زمنية قصيرة أما فعل البقاء فقد يمتد إلى وقت طويل نوعا ما .

#### محل النشاط الإجرامي :

تجرم المادة 394 مكرر فعل الدخول والبقاء عن طريق الغش في كل أو جزء من نظام المعالجة الآلية وفق التعريف الوارد في الفقرة ب من المادة الثانية من القانون رقم 09-04 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المترابطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين" و وفقا لهذا التعريف الموسع فإن المحل الذي ينصب عليه سلوك الجاني في جريمة الدخول والبقاء الغير مشروع يتسع

لاستيعاب المعلومات في نظام المعالجة الآلية خلال مرحلة المعالجة والتخزين والاسترجاع ، والنظام الذي يتضمنها فضلا عن الشبكات ذاتها أو المعلومات المنقولة عبرها <sup>84</sup>.

ولقد أصبحت المعلومات مصدر قوة ومصدر سلطة حتى قيل أن المعرفة هي سلطة وأن الحصول على المعرفة وحسن استخدامها عاملان أساسيان من عوامل التقدم ولذلك فإن التكنولوجيا الحديثة تتعلق بالمعرفة ثم السلطة <sup>85</sup>.

### الفرع الثاني : النتيجة

الأصل أن يتطلب المشرع القيام جريمة ما وجود ما يسمى بالنتيجة الإجرامية التي يربتها أو يحدثها النشاط الإجرامي وهذه النتيجة في الغالب من الأحيان ما تظهر بصورة أثر مادي ضار لكن في الأحيان الأخرى لا تظهر كذلك بل تمثل اعتداء على حق يحميه القانون فحسب .

ويسمى النوع الأول من الجرائم " بالجرائم المادية " بينما يسمى النوع الثاني " بالجرائم الشكلية " ، واتخاذ النتيجة الإجرامية صورة معينة وفق ما ورد ذكره وهو المعيار الذي يفرق بين هذين النوعين من الجرائم <sup>86</sup>.

إن أمر انتماء جريمة الدخول والبقاء الغير مشروع إلى هذه أو تلك يرد حسب ما إذا كانت بسيطة أو مشددة وذلك على النحو التالي :

<sup>84</sup> - بوكر رشيدة مرجع سابق، ص 45.

<sup>85</sup> - احسب عمرو حماية الحريات في مواجهة نظم المعلومات ، دار النهضة العربية ، الطبعة الأولى ، القاهرة 2000

ص30.

<sup>86</sup> - محمد حسام لطفي ، الجرائم التي تقع على الحاسوب ، بحث قدم إلى المؤتمر السادس للجمعية المصرية للقانون

الجنائي القاهرة خلال الفترة 25 الى 28 بتاريخ 1993/10/28

**أولاً : الدخول أو البقاء إلى نظام المعالجة الآلية في صورته البسيطة**

عاقب المشرع الجزائري على جريمة الدخول والبقاء عن طريق الغش بمجرد الدخول أو البقاء داخل النظام معالجة الآلية بذات المعاني السابقة لفعل الدخول والبقاء ولم يتطلب حدوث نتيجة معينة ضارة لها وجودها المحدد في العالم الخارجي كالحصول على المعلومات أو التلاعب فيها أو أي شكل من أشكال الضرر، وبذلك تكون هذه الجرائم من الجرائم الشكلية التي لا يلزم لتحقيقها نتيجة معينة منظور أليها وفقا لمدلولها المادي . ثانيا : الدخول أو البقاء المرتببات لنتيجة إجرامية

قد التجأ المشرع الجزائري إلى تشديد العقاب في حالة ما ترتب على الدخول أو البقاء الغير مشروع نتائج ضارة بالمعلومات أو النظم بصور مختلفة وذلك وفقا للفقرة الثانية من المادة 394 مكرر بقولها " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة " وهذه النتائج هي ذاتها المتطلبة في جريمة التلاعب بالمعلومات التي تناولها المشرع الجزائري بالتجريم بموجب المادة 394 مكرر 1 غير أن الفارق بين النتيجة المنصوص عليها في المادة 394 مكرر وجريمة التلاعب المنصوص عليها في المادة 394

مكرر 1 باعتبارها جريمة مستقلة يمكن في أن هذه الأخيرة تقع مقصودة، أي يريدتها الفاعل أو يقبلها على الأقل بينما في جريمة الدخول أو البقاء الغير مصرح به لا تقع كذلك إذا لا يريدتها الفاعل وكذا الفقرة الثالثة من نفس المادة بقولها " وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام الاشتغال المنظومة تكون العقوبة ...." ويقصد بتخريب النظام في هذا الإطار ممارسة أفعال عليه من شأنها جعله غير قابل الاستخدام أو الاستعمال<sup>87</sup>.

كما قد يترتب عن فعل الدخول والبقاء الغير مصرح به بعض النتائج السلبية التي تقع على النظام المعالجة الآلية للمعطيات وبالخصوص المعلومات والبيانات باعتبارها المستهدف الأول والتي سنوجزها كالآتي :

#### أ- إدخال تعديلات غير مرخص بها نتيجة البقاء في المنظومة المعلوماتية

قد يتمكن المتهم بعد الدخول على برنامج معين من الاحتيال والاستيلاء بواسطة برنامج حسان طروادة والقنابل المنطقية و برامج الدودة و الفيروسات و قد يترتب على ذلك تعطيل النظام و يستوي أن يكون التعطيل دائما أو مؤقتا فقد يؤدي إلى توقيف الدائم للنظام كما في حالة إدخال فيروس وقد يكون التوقف مؤقتا أو منقطعا على فترات منتظمة. كما أنه تم إدخال قنبلة معلوماتية زمنية مبرمجة ينجم عنها شل النظام عند البدء في تشغيله مثلا 2.

#### ب - الإفساد : Fausser

يقصد بالإفساد كل فعل وإن كان لا يؤدي إلى التعطيل، يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها ، والإفساد من هذه الزاوية يقترب من التعيب واللدان يعتبران كطرف مشدد لجريمة الدخول والبقاء الغير مشروع.

<sup>87</sup> - زكي أمين حسونة ، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنيك المعلوماتي و بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة 1993.

1 - استخدام القنبلة المعلوماتية التي يدخل عن طريقها معلومات تتكاثر داخل النظام مما يجعله غير صالح للاستعمال .

2- استخدام البرنامج الذي يحمل فيروس يطلق عليه ، اسم " حصان طروادة " والذي يقوم بتغيير غير محسوس في البرامج أو المعطيات وغير ذلك من الفيروسات التي تجعل مخرجات نظام غير تلك التي يجب علي أن يخرجها بل إن الإفساد يمكن أن يتحقق عن طريق إتلاف أو تخريب العناصر المادية في النظم<sup>88</sup>.

وفي الأخير فإن النشاط الإجرامي ،والذي تمثل في فعل الدخول والبقاء الغير مصرح به إلى نظام المعالجة الآلية للمعطيات هو الذي أدى إلى هذه النتيجة الإجرامية ولولاه لما تحقق كل ذلك .

### المطلب الثاني : الركن المعنوي

جريمة الدخول والبقاء داخل النظام جريمة عمديه يتخذ الركن المعنوي فيها صورة القصد الجنائي والقصد الجنائي يتكون من علم وإرادة فيلزم لتوافر الركن المعنوي أن نتيجة إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأن له الحق في الدخول إلى النظام والبقاء فيه وعليه لا يتوفر الركن المعنوي إن كان الدخول الجاني أو بقاءه داخل النظام مسموحا به أي مشروعاً.

كما لا يتوفر هذا الركن إذ وقع الجاني في خطأ سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق ، كان يجهل بوجود حظر للدخول أو البقاء أو كان يعتقد خطأ أنه مسموح له بالدخول فإذ توافر القصد الجنائي بعنصريه العلم و الإرادة

<sup>88</sup> - ( LE CHEVALE DE TROIDE )

هو برنامج خادع يخفي ظاهره لغرض غير مشروع بان يظهر كبرنامج عادي يؤدي برنامج حصان طروادة : بعض المهام المفيدة لمستخدمه و المألوفة لديه بينما تكون موجودة بعض الأوامر و التعليمات التي تؤدي عند تشغيله مهاماً ضارة غير متوقعة.

فإنه لا يتأثر الباعث على الدخول أو البقاء , فيظل القصد قائما حتى لو كان الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام .

ومن استقراء نص المادة 394 مكرر من قانون العقوبات نستنتج أن القصد الجنائي العام لا يكفي إنما يجب توافر قصد جنائي خاص و هو " الغش " ليس مقصود به نية الإضرار .

وعادة يبدو طابع الغش الذي تم به الدخول من خلال الجهاز الرقابي الذي يحمي النظام أما بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام .

وقد نص القانون صراحة على كون جريمة الدخول و البقاء الغير مشروع جريمة عمدية , و هذا ما يستشف صراحة من نص المادة 394 مكرر من قانون العقوبات الجزائي كما يلي : " كل من يدخل أو يبقى عن طريق الغش " .

و لذلك سوف نتعرض إلى العلم في فرع أول ثم الإرادة في فرع ثان .

### الفرع الأول : العلم

القيام القصد الجرمي لا بد أن ينصرف علم الجاني إلى واقعة ذات أهمية قانونية في تكوين الجريمة , أي كل واقعة يتطلبها لبناء أركان الجريمة و استكمال عناصرها و إضافة إلى ذلك لا بد أن يشمل العلم أيضا التكييف الذي تتصف به بعض هذه الوقائع و تكتسب به أهميتها في نظر القانون بحيث أن عددا من الوقائع التي تقوم بها الجريمة لا يمثل أهمية في نظر القانون , إلا إذ اكتسب وصفا معينا فإن تجرد من هذا الوصف , فقد تجرد من الأهمية القانونية و لم يعد صالحا لتقوم به الجريمة.

### الفرع الثاني : الإرادة

و تتمثل الإرادة في كونها ' حالة ذهنية و نفسية يكون عليها الجاني ساعة إقدامه على ارتكاب الجريمة, و يمكن تصور هذه الحالة بعزم الجاني على ارتكاب الجريمة أو اتخاذ

قرار بتنفيذها , ثم إصدار أمر إلى أعضاء جسمه القيام بالأفعال المكونة لها و قيادة هذه الأعضاء إلى تحقيق النتيجة المطلوبة ركن المعنوي .

و يتمثل الركن المعنوي للجريمة في صورتها المشددة من خلال نص المادة 394 مكرر على أنه " تضاعف العقوبة إذ ترتب على ذلك حذف أو تغيير لمعطيات المنظومة كما نص في الفقرة الثالثة من نفس المادة على أنه " ..... إذ ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة ..... .

فكما هو ملاحظ فإن المشرع الجزائري لم يستعمل كلمة غش « frauduleusement " وبناء على ذلك فإن هذه الجريمة تقع بطريق الخطأ بحيث أن الخطأ يعد كافيا لقيام الجريمة و من ثمة فإن هذه الجريمة تعد من جرائم الإهمال , وبالتالي فمجرد ارتكاب الفعل المادي يعد كافيا لقيام الجريمة إلا إذ استطاع الجاني إثبات حدوث قوة قاهرة أدت إلى حدوثها ومن ثمة لا يمكن تطبيق الظرف المشدد غد قصد الجاني النتيجة المشددة

**المبحث الثاني : العقوبات المقررة للجريمة دخول غير مشروع**

ان الجزاءات والعقوبات المقررة لجرائم الاعتداءات الماسة بالأنظمة المعلوماتية  
لقد نصت المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي بموجب أن تكون  
العقوبات المقررة نتيجة ارتكاب الجرائم المعلوماتية رادعة ومنتزعة لعقوبات سالبة للحرية،  
كما نصت على وجوب تطبيق عقوبات على الشخص المعنوي بناء على مبدأ له مساءلة  
الشخص المعنوي الوارد في المادة 12 من نفس الاتفاقية.  
وباستمرار نصوص المواد الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات  
الواردة في قانون العقوبات الجزائري، من المادة 394 مكرر إلى غاية المادة 394 مكرر 7  
نجد أن المشرع الجزائري قد تبنى هذا المبدأ في تقريره للجزاءات الواجبة على هذا النوع من  
الجرائم فسن عقوبات تطبق على الشخص الطبيعي وعقوبات تطبق على الشخص المعنوي  
وذلك ما سنتناوله فيمايلي:

**المطلب الأول: العقوبات المطبقة على الشخص الطبيعي****الفرع الأول: العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات.**

ومن خلال استقراء هذه النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية  
يتبين لنا وجود تدرج داخل النظام العقابي هذا التدرج في العقوبات يحدد الخطورة الإجرامية  
التي قدرها المشرع لهذه التصرفات إذا نجد سلم خطورة يتضمن ثلاثة درجات، جريمة الدخول  
أو البقاء بالغش في الدرجة الأولى، وبعدها الدرجة الثانية جريمة الدخول والبقاء المشددة، أما  
الدرجة الثالثة، فتحتملها الجريمة الخاصة بالمساس العمدي بالمعطيات<sup>90</sup>.

<sup>90</sup> - أمال قارة، مرجع سابق، ص 127

**أولاً: جريمة الدخول والبقاء**

أ ( الدخول والبقاء بالغش (الجريمة البسيطة العقوبة المقررة هي 03 اشهر على سنة حبس و 50.000 دج إلى 100.000 دج غرامة (المادة 394 مكرر).

ب) الدخول والبقاء بالغش (الجريمة المشددة) تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير المعطيات العقوبة من 06 أشهر إلى سنتين وغرامة من 50.000 دج على 150.000، إذا ترتب عن الدخول أو البقاء غير المشروع النظام اشتغال المنظومة (المادة 394 مكرر 03، 02) .

**ثانياً: جريمة التلاعب بالمعطيات**

نصت عليها المادة 394 مكرر 1، ق. ع. ج. بالحبس من 6 اشهر الى 03 سنوات وعقوبة الغرامة التي تتراوح من 500.000 دج إلى 2.000.000 دج. والملاحظ أن عقوبة التلاعب بالمعطيات تفوق جريمة الدخول والبقاء غير المصرح بهما سواء كانت هذه الأخيرة في صورتها البسيطة أو المشددة، لأن في صورتها البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو بنظام معالجتها وحتى في صورتها المشددة، وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي ازالة المعطيات أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجنائي بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشددة<sup>91</sup>.

<sup>91</sup> - د/ نائلة عادل محمد فريد فورة، المرجع السابق، ص228

**ثالثا: جريمة التعامل في معطيات غير مشروعة**

تعاقب المادة 394 مكرر 2 من ق. ع. ج. على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من شهرين إلى 3 سنوات وبالغرامة المالية من 1.000.000 دج إلى 5.000.000 دج

بهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول والبقاء غير المصرح بهما سواء في صورتها البسيطة أو المشددة وبين جريمة التلاعب بالمعطيات (غير أن حداها الأدنى يقل عن كلتا الجريمتين).

ذلك أن حداها الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء في صورتها سنة أو سنتين) وستساوى مع الحد الأقصى لجريمة التلاعب بالمعطيات (03 سنوات).

غير أن حداها الأدنى يقل عن الجريمتين معا، لأنه في جريمة الدخول أو البقاء البسيطة 3 أشهر وفي هذه الجريمة في صورتها المشددة وفي جريمة التلاعب هو 6 أشهر<sup>92</sup>.

**الفرع الثاني: العقوبات التكميلية**

نصت المادة 394 مكررة من ق. ع. ج. على العقوبات التكميلية، التي يمكن الحكم بها إلى جانب العقوبات الأصلية وجاء فيها مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها في هذا القسم، علاوة على اغلاق المحل أو مكان الاستعمال إذا كانت الجريمة قد ارتكبت بعلم مالکها ويستخلص من نص هذه المادة العقوبات التكميلية التالي:

92 - محمد خليفة، المرجع السابق، ص 219

## أولاً: مصادرة الأجهزة والوسائل والبرامج المستخدمة:

وذلك مع الاحتفاظ بحقوق الغير حسن النية، وتجدر الإشارة إلى أن المشرع نص فقط على مصادرة الأجهزة والبرامج والوسائل المستخدمة فقط، وأغفل مصادرة الوسائل الموجهة لإرتكاب الجريمة من المعطيات المخزنة أو المعالجة أو المرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في الفقرة الأولى من المادة 394 مكرر 2 قانون عقوبات جزائري، حيث أن عبارة المستخدمة الواردة في نص المادة 394 مكرر 6

الخاصة بالعقوبات التكميلية تفيد صيغة الماضي وهذا ما نصت عليه المادة 394 مكرر 6 من قانون عقوبات جزائري التي تنص على العقوبات التكميلية، وفي فقرتها الثالثة على المصادرة فنجد أنها تناولت مصادرة الشيء الذي كان موجها للقيام.

ثانياً: اغلاق المواقع التي تكون محلا للجريمة من جرائم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات<sup>93</sup>.

ثالثاً: اغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكاها واطاف المشرع شرط علم المالك إذا كان على سبيل المثال الجاني مستأجرا للمحل المالك مؤجر له، ويعلم خطورة الأفعال التي يقوم بها الجاني، كغلق نادي الانترنت الذي ترتكب فيه هذه الجرائم مع علم مالك أو مسير النادي بالافعال الخطيرة التي يقوم بها زبونه، ولكن المشرع لم يحدد المدة القصوى لغلق المحل أو مكان الاستغلال، مما يطرح مشكلا في تنفيذ هذه العقوبة فمن جهة يعتبر إغلاق المحل أو أماكن كعقوبة تكميلية للشخص الطبيعي المسؤول جزائياً، ومن جهة

<sup>93</sup> - د/ أحسن بوسقيعة، المرجع السابق، ص 448

أخرى لا يمكننا الرجوع الى القواعد العامة للمسؤولية الجزائية للشخص المعنوي لتحديد المدى المدة، لأنه في هذه الحالة تقع المسؤولية الجزائية على عاتق الشخص الطبيعي فيوجد حسب رأينا في توقيع الجزاء الجزاء، حيث تم توقيع جزاء خاص بالشخص المعنوي غلق المحل على الشخص الطبيعي.

- إن العقوبة التكميلية الواردة في المادة 394 مكرر 06، ق. ع. ج. غير كافية في مواجهة الحالات العديدة التي يمكن أن يرتكبها الشخص الطبيعي فمثلا تنص المادة على العقوبة التكميلية الخاصة بالموظف العمومي المصرح له بالدخول على نظام الآلية المعطيات لكنه يبتعد ذلك إلى ارتكاب جرائم أخرى متعلقة بالمنظومة المعالجة أليا، وكذلك الشيء بالنسبة للوظيفة المهنية

فيما يخص المحامين أو الأطباء مثلا، وكذلك الوظيفة الاجتماعية إذا ارتكبت الجريمة عند تأدية الوظيفة أو بمناسبةها وهذا ما جاءت به احكام المادة 323 - 05 من قانون العقوبات الفرنسي والتي نصت على تكميلية أخرى، تدعو المشرع الجزائري الى الأخذ بها وهي كمايلي:

- المنع لمدة أقصاها 5 سنوات من الحقوق المدنية والسياسية.
- المنع لمدة أقصاها 5 سنوات من ممارسة الوظيفة العمومية أو النشاط المهني أو الاجتماعي إذا ارتكبت الجريمة اثناء تأدية الوظيفة او بمناسبةها.
- مصادرة الشيء الذي استخدم أو الموجه لارتكاب الجريمة او الشيء محل الجريمة الغلق لمدة القصاها 5 سنوات للمؤسسات، أو لحد أو عدة مؤسسات المقاوله التي استعملت في ارتكابها الافعال المجرمة.
- الحرمان لمدة أقصاها 5 سنوات من الصفقات العمومية.

- المنع لمدة اقصاها خمس سنوات في اصدار الشيكات، بما فيها التي تسمح سحب الاموال من طرف الساحب لدى المسحوب له أو المرخص أو المرخص لهم بذلك. تقليل أو تشر الحكم أو القرار الصادر<sup>94</sup>.

### الفرع الثالث: الظروف المشددة.

نصت المادة 394 مكرر 2 - 03 على طرف التشديد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا الظرف عندما ينتج عن الدخول أو البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

- في الحالة الأولى تضاعف العقوبات المقررة فيا لفقرة الأولى من المادة 394 مكرر وفي الحالة الثانية تكون العقوبة الحبس ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج هذا الظرف المشدد هو طرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافر. نصت المادة 394 مكرر 3، على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام<sup>95</sup>.

94 - د/ أحسن بوسقيعة، المرجع السابق، ص 449

95 - نص المادة 394 مكرر ، من قانون العقوبات الجزائري

**المطلب الثاني: العقوبات المطبقة على الشخص المعنوي**

لقد كانت العقوبة إحدى أهم الحجج التي استند إليها المعارضون لمبدأ إقرار مسؤولية الشخص المعنوي حيث رأوا أنه لا يمكن تطبيقها على هذا الأخير خاصة تلك العقوبات السالبة والمقيدة للحرية، لكن وبعد اتساع تطبيق عقوبة الغرامة وابتكار عقوبات جديدة تتلاءم وطبيعة الشخص المعنوي لم لهذا الاعتراض محل، ولقد تضمنت المادة 18 مكرر من قانون العقوبات الجزائري بعد تعديله سنة 2004، أنواع العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجرح، وأول هذه العقوبات في الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى المقررة على الشخص الطبيعي، لكن المادة 394 مكرر 4، فهي غرامة ذات حد واحد أو جبن الأخذ بالحد الأقصى لهذه العقوبات، وهو خمس مرات فيما يتعلق بجرائم المعطيات، وفيما يخص القانون الفرنسي فقد نصت المادة 323 - 6 من قانون العقوبات بأن الأشخاص المعنوية يمكن أن يحكم عليها بالمسؤولية الجنائية وفقا للشروط التي حدتها المادة 121 - 2 وان العقوبات المقررة عليها هي<sup>96</sup> :

- الغرامة وفق ما تنص

عليه المادة 131-38

- العقوبات المحددة في المادة 131-39

- العقوبات المحددة في المادة 131 - 39 فقرة 2 بالنسبة للنشاط المهني الذي وقصت بمناسبة الجريمة. وتنقسم العقوبات المقررة على الشخص في قانون العقوبات الجزائري وكذا الفرنسي بالنظر الى طبيعة الحق الذي تمس أنواع:

<sup>96</sup> - نص المادة 121 وما يليها من قانون العقوبات الجزائري.

### الفرع الاول : العقوبات المطبقة على الشخص المعنوي

- العقوبات الماسة بوجود الشخص المعنوي أو حياته وتتمثل في الحل. العقوبات الماسة بالذمة المالية للشخص المعنوي وتتمثل في الغرامة والمصادرة
- العقوبات الماسة بالنشاط المهني للشخص المعنوي وتتمثل في اغلاق أو المؤسسة وكذا المنع من ممارسة النشاط المهني أو الاجتماعي.
- العقوبات الماسة بالسمعة و تتمثل في نشر الحكم وتعليقه.
- العقوبات الماسة بحق الشخص المعنوي في التعامل بحرية لتحقيق أهداف التي أنشء من اجلها، وتتمثل في الحراسة القضائية و الإقصاء من الصفقات العمومية وبضيف القانون الفرنسي المنع حتى الدعوى العام للإخار وكذلك المنع من اصدار الشيكات.
- وهذه العقوبات في القوانين الجزائري والفرنسي ليست خاصة بجرائم المعطيات وانما يمكن أن توقع على الجرائم التي يرتكبها الشخص المعنوي وليس هناك ما يميز جرائم المعطيات الا عقوبة الغرامة المشددة.

### الفرع الثاني : عقوبة جريمة الاتفاق والشروع الجنائي

نصت المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي على تجريم التحضير للجرائم الماسة بالأنظمة المعلوماتية، وقد تبني المشرع الجزائري مبدأ معاقبة الاتفاقية الجنائي بنص المادة 394 مكرر 05، من ق.ع. ج. إذ جاء فيها أن كل من شارك في مجموعة أو في اتفاق تالف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".

وإن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو اتفاق بغرض الإعداد الجريمة من الجرائم الماسة بالأنظمة المعلوماتية يتمثل في كون أن مثل هذه الجرائم تم عادة في إطار مجموعة، كما أن المشرع أراد توسيع نطاق العقوبة فأخضع الأعمال التحضيرية للعقوبة المقررة للجريمة التي تم التحضير لها إذا تمت في إطار اتفاق جنائي، بمعنى آخر أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص<sup>97</sup>. - ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا انعقدت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

- وشروط المعاقبة على الاتفاق الجنائي يمكن استخلاصها من نص المادة 394 مكرر 5 قي. ع. ج. والتي هي: أما الشروع فنصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وتبناه المشرع الجزائري في المادة 394 مكرر 7. ق. ع. ج. فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجرح إلا بنص. نصت المادة 394 مكرر 7، ق، ع. ج. يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها. يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة تشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة.

<sup>97</sup> - أمال قارة، المرجع السابق، ص130

ومن خلال استقراء نص المادة أن الجنحة الواردة بنص المادة 394 مكرر 5 من ق.ع. ج. مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبني فكرة الشروع في الاتفاق الجنائي<sup>98</sup>.

---

<sup>98</sup> - أمال قارة، المرجع السابق، ص 133

خاتمة

## الخاتمة

بعد هذا العرض لموضوع جريمة الدخول الغير المشروع لنظام المعالجة الآلية للمعطيات لاحظنا تشعب في الموضوع و صعوبته و خصوصا ما يتعلق منه بخصوصية جرائم المعطيات من حيث الإجراءات ثم أن هذه الأخيرة من الجرائم الحديثة نسبيا التي تستلزم دراسات مستقبلية محاولة لوضع المبادئ العامة بكل ما يتعلق من جرائم ترتبط بالتطور الإلكتروني و المعلوماتي ووسائل الاتصال الحديثة، وهذا ما يتطلب تدخلا تشريعا من اجل وضع حماية قانونية متكاملة و سد جميع الثغرات قانون العقوبات و التي تعد صالحة لمواكبة نظم المعلومات و لعل أبرز المشكلات التي أفرزتها هذه الجريمة تتمثل في:

- من ابرز المشكلات التي أثارها الجريمة المعلوماتية ان التحديات الإجرائية في ميدان التحري و التحقيق و المحاكمة من حيث الاختصاص و القانون الواجب التطبيق خاصة و أن الجريمة المعلوماتية كما سبق و أن وضحنا هي جريمة عالمية لا تعترف بالحدود الدولية و الإقليمية و أنه رغم توفر النصوص القانونية الموضوعية فإن مكافحة جرائم المعلوماتية رهين بالمعيقات الإجرائية التي أفرزتها هذه الجرائم، فبالنسبة لمرحلة التحري و التحقيق فإن أول معوق يواجهه حسن سيرها هو غياب القدرات التأهيلية و الوسائل الفنية التي تتيح سرعة إدراك ما حصل و أن غياب التأهيل قد يؤدي إلى إتلاف الدليل على الجريمة

فيكون الأثر هو إفلات مرتكبي هذه الجرائم من العقاب .

هذا إضافة إلى قصور النصوص الإجرائية التقليدية للضبط والتفتيش لتلاءم الجرائم المعلوماتية التي تتميز بسهولة إخفاء الدليل. و إلى حين انتهاء التحقيق تبدأ مشكلات المحاكمة و أولها هو الاختصاص، المتعلق بمكان وقوع الجريمة أو بناء على معيار إلحاق الضرر .

إضافة إلى القانون واجب التطبيق باعتبار أن الجريمة المعلوماتية جريمة عالمية

عابرة للحدود

لهذا يكون من الضروري الإسراع بسن قواعد إجرائية تتلاءم مع طبيعة الجريمة المعلوماتية حتى تكون القواعد الموضوعية المجرمة لها أكثر فعالية هذا من جهة ، و من جهة أخرى فإنه لا بد من تكاثف الجهود الدولية و الإقليمية في حقل جرائم المعلوماتية لتخطي العقبات التي تطرحها هذه الجرائم بعض

#### الاقتراحات:

ضرورة تدريب وتأهيل أفراد الضبطية القضائية من العاملين من الإدعاء العام (النيابة) و القضاء على كيفية التعامل مع هذا النوع من الإجرام و تحقيق التعاون مع التقنيين من أصحاب الخبرة ، وذلك بعقد دورات تدريبية بشكل دوري و دائم للاستفادة من خبراتهم و إرشاداتهم ابتداء من مرحلة الاستدلال و جمع الأدلة ، و انتهاء بقرارات المحاكم . تدريس مواد الأنظمة المعلوماتية و الجرائم التي قد تنشأ منها في كليات الحقوق والمعاهد

#### القضائية

- تفعيل دور الأسرة في متابعة الأبناء لوقايتهم من الآثار السلبية والمخاطر المترتبة عن الاستخدام الغير الأمن لشبكة الانترنت .

- التطور المستمر للتشريعات القائمة بما يحقق مرونتها و موكبتها للتطورات المتسارعة في مجال تكنولوجيا المعلومات

ضرورة التعاون الدولي لمواجهة الجرائم في البيئة المعلوماتية الإلكترونية و ذلك من خلال الدخول في اتفاقيات و معاهدات تجرم صور هذه الجرائم كلها و تبين كذلك الاختصاص المكاني في حال وقوعها، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات و المعلومات في المسائل المتعلقة بالجرائم المعلوماتية، وهذا ما يجب أن يحدث بالنسبة للجزائر و ضرورة انضمامها للاتفاقية بواديست 2001 لمكافحة الجريمة المعلوماتية

# قائمة المراجع

## المراجع باللغة الاجنبية

### اولا : الكتب

1. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير كلية الحقوق ، جامعة الإسكندرية، سنة 2009
2. طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر ، الإسكندرية، سنة 2009
3. جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية ، القاهرة، سنة 2001
4. محمد عبيد الكعبي، الجرائم الناشئة عن الإستعمال الغير المشروع للشبكة الانترنت، دار النهضة العربية، القاهرة سنة 2000
5. نهلا عبد القادر المومني الجرائم المعلوماتية، الطبعة 2 ، دار الثقافة للنشر والتوزيع، سنة 2001
6. نائلة عادل فريد قورة،، جرائم الحاسب الإقتصادية، دراسة نظرية تطبيقية، منشورات الحلبي القانونية القاهرة،؟ سنة 2005،
7. ايمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار النشر، دون بلد النشر، سنة 2004
8. رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، في التشريع الجزائري المقارن، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت ، لبنان، سنة، 2012
9. أسامة سمير حسين، الإحتيال الإلكتروني ( الوجه القبيح للتكنولوجيا ) ، الحنادرية للنشر والتوزيع ، الأردن الطبعة الأولى ، سنة 2011

10. عبد الفتاح البيومي الحجازي ، مبادئ الإجراءات الجنائية في الجرائم الكمبيوتر و الأنترنت، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى سنة 2006
11. محمد دباس الحميد، ماركو إبراهيم نينو، حماية الأنظمة المعلومات، دار حامد للنشر والتوزيع، عمان ، الطبعة الأولى ، سنة 2007
12. جعفر حسين جاسم الطائي، جرائم تكنولوجيا المعلومات ( رؤية جديدة للجريمة المعلوماتية)، دار البداية ،عمان سنة 2007،
13. نسرین عبد الحمید نبیه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف للنشر والتوزيع ، الأردن، دون سنة
14. هدى حامد قشوش، جرائم الحاسب الإلكتروني في التشريع المقارن، الطبعة الأولى ، دار النهضة العربية ، سنة 1992
15. زبيجة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع عين مليلة، الجزائر، سنة 2011
16. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية سنة 2007
17. إنتصار نوري الغريب، أمن الكمبيوتر والقانون، دار الراتب الجامعية ، بيروت، سنة 1994
18. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر 2010
19. عمرو موسى الفقهي، الجرائم المعلوماتية، جرائم الحاسب الآلي و الأنترنت في مصر و الدول العربية، المكتب الجامعي الحديث، الإسكندرية، سنة 2006
20. نايف بن محمد المرواني ، جريمة السرقة ، دراسة نفسية إجتماعية ، جامعة نايف العربية للعلوم الأمنية، الرياض الطبعة الاولى، سنة 2011

21. محمد أمين أحمد الشوابكة ، جرائم الحاسوب والأنترننت، مكتبة دار الثقافة للنشر والتوزيع، عمان، سنة 2004
22. عباس أبو شامة عبد المحمود، عولمة الجريمة الإقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2007
23. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ماجستير في القانون الجنائي المعلوماتي، الطبعة الأولى دار الثقافة للنشر والتوزيع ، عمان، الأردن سنة 2009
24. ناصر محمد البقهي، أثر التحويل المجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف عبد العزيز لدراسات الأمن الفكري بجامعة الملك سعود، المملكة العربية السعودية ، سنة 2009
25. سامي علي عياد، الجريمة المعلوماتية و الأنترننت ( الجرائم الإليكترونية)، الطبعة 1 ، منشورات الحلبي الحقوقية بيروت ، 2007
26. سامي علي عياد، الجريمة المعلوماتية و الأنترننت ( الجرائم الإليكترونية)، الطبعة 1 ، منشورات الحلبي الحقوقية ، بيروت ، 2007
27. عبد الله بن عبد العزيز يوسف، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية، الرياض ، الطبعة الأولى ، سنة 2004
28. محمد سيد سلطان/ قضايا قانونية في أمن المعلومات وحماية البيئة الإليكترونية، دار ناشري للنشر والتوزيع الإليكتروني، 2004
29. علي عدنان الفيل، الإجرام الإليكتروني، الطبعة الأولى ، منشورات زين الحقوقية ، دمشق، 2011<sup>1</sup>

30. عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعة للطباعة و النشر، مصر ، 1999
31. أبوكر رشيدة ، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن ، منشورات حلبي الحقوقية ، الطبعة الأولى 2012 .
32. جميل عبد الباقي الصغير القانون الجنائي والتكنولوجيا الحديثة. الكتاب الأول ، الجرائم الناشئة عن استخدام الحاسب الآلي) دار النهضة العربية، السنة 2011
33. احسب عمرو حماية الحريات في مواجهة نظم المعلومات ، دار النهضة العربية ، الطبعة الأولى ، القاهرة 2000
34. محمد حسام لطفي ، الجرائم التي تقع على الحاسوب ، بحث قدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة خلال الفترة 25 الى 28 بتاريخ 1993/10/28
35. زكي أمين حسونة ، جرائم الكمبيوتر و الجرائم الأخرى في مجال التكنيك المعلوماتي و بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة 1993.
36. خيرت عليّ محرز، التحقيق في الجرائم الحاسب الآلي، القاهرة، سنة 2012
37. د فوزية عبد الستار، قانون العقوبات ( القسم الخاص) ، دار النهضة العربية، بدون بلد النشر، سنة 1988
38. آمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الثانية ، دار هومه للطباعة والنشر والتوزيع، الجزائر ، سنة 2007
39. خالد ممدوح إبراهيم، فن التحقيق الجنائي في جرائم الإلكترونيّة، الطبعة الاولى ،دار الفكر الجامعي لنشر الإسكندرية ، سنة 2009
40. فوزية عبد الستار، شرح القانون الإجراءات الجنائية ، دار النهضة العربية ،سنة 1979.

41. محمد سامي الشوا، ثورة المعلومات وانعكساتها على القانون العقوبات، دار

النهضة العربية، القاهرة، سنة 1994

### المذكرات والرسائل العلمية

1. هشام رستم، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة بحث

مقدم إلى لجنة العلمية بمصر لمنع الجريمة المعلوماتية ومعاقبة المجرمين، مجلة

الدراسات القانونية، جامعة أسيوط ، العدد 17 ، سنة 1995

2. كريستينا سكولمان، عن جرائم الأنترنت طبيعتها وخصائصها، الندوة الإقليمية حول

الجرائم المتصلة بالكمبيوتر المملكة المغربية، سنة 2007

3. أسامة محمد محي الدين عوض، جرائم الكمبيوتر، بحث مقدم إلى مؤتمر السادس

للجمعية العربية للقانون الجنائي ،

### ثانيا : النصوص القانونية والمراسيم

1. قانون العقوبات الجزائري المعدل والمتمم بموجب القانون رقم 15/04 المؤرخ في

2004/11/10.

2. القانون النموذجي العربي الموحد لمكافحة الجرائم المعلوماتية وما في حكمها، الدورة

19 بقرار رقم 495 في 2003/10/08.

3. الأمر 04/15 المؤرخ في 20 ربيع الثاني 1436هـ الموافق 10 / فبراير 2015

المعدل و المتمم للأمر 66 - 156 المتضمن قانون العقوبات نصوصا خاصة

بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

4. للأمر 15 -04 المؤرخ في 10 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع

و التسبق الإلكتروني

5. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 ج.ر.71 ص.11 و 12 ب قسم

سابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن

المواد من 394 مكرر إلى المادة 394 مكرر 7

رابعاً : المراجع بلغة الاجنبية

1. MARWE VANDER ,computer crimes and other grimes against information Technology in south Africa ,”R.I.D.P”,1993;p554
2. Klaus Tiede man, Fraude et autres délits d’affaires commis a l’aide d’ordinateurs électroniques, Rev, drpén , crim, 1984, p 612.
3. Jack Bologna, Corporate Fraud, hte Basic of prevention and Detction , Butter worth, 1984,p11.
4. WASIK Martin , computer crimes and other crimes against information tesnnology in the unit kingdom “R.I.D.P” , 1991,p19
5. MASCALA Corinne , criminalité et contrat électronique, Travaux de l’association, CAPITANT Henir , journées National paris, 2000,p118.
6. D.B.PARKER, comibattre la criminalité informatique , edoros,1987,p142.
7. Debray Stephan, internet face aux substances illicites, université de paris, 2002-2003,p13.
8. Martin wasik ,compter crimes and other crimes agaist , p 632.
9. Alain Bensoussan , internet ,aspects juridiques ,ed herme 1998 p 198.
10. TGI paris ,26 juin 1995, petites affiches , les mars 1996, n 27, p 4.
11. Aix, En, Provence , Gaz,Pal ,Latry Bonnat,Rev.Se.Cri .1998 ,p140
12. Travaux De L’Institute Sciences Cri Min elles De Poitiers Informatique Et Droit Pénal ,Ed 1983 P 25.
13. FAUCHMOUX ‘ VINCENT Daprery pierre, le Droit de l’internet (loi ,contra et sage) , édition , lutec , paris ,2008,p215.

الفهرس

إهداء

الشكر

قائمة المختصرات

7.....	المقدمة
14.....	للفصل الاول خصوصية الجريمة المعلوماتية من الناحية الموضوعية.....
15.....	المبحث الأول : ماهية الجريمة المعلوماتية.....
15.....	المطلب الأول : تعريف جريمة المعلوماتية.....
15.....	الفرع الأول : التعريف الضيق للجريمة المعلوماتية.....
17.....	الفرع الثاني : التعريف الموسع للجريمة المعلوماتية.....
18.....	المطلب الثاني : تصنيف المجرم المعلوماتي.....
18.....	الفرع الأول : خصوصية الجريمة المعلوماتية.....
22.....	الفرع الثاني : سمات المجرم المعلوماتي.....
25.....	الفرع الثالث : تصنيف المجرم المعلوماتي.....
28.....	المبحث الثاني : انواع الجرائم المعلوماتية.....
28.....	المطلب الاول : جرائم الواقعة على نظام معلوماتي.....
28.....	الفرع الأول : الجرائم الواقعة على نظم المعالجة الآلية للمعطيات.....
32.....	الفرع الثاني : الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الآلية لمعلومات...
38.....	المطلب الثاني : المعلوماتية وسيلة لإرتكاب الجرائم.....
38.....	الفرع الأول : الجرائم الواقعة على الأشخاص.....
40.....	الفرع الثاني : الجرائم الواقعة على الاموال.....

42	الفرع الثالث : الجرائم الواقعة على أمن الدولة .....
46	الفصل الثاني : النظام القانوني لجريمة دخول غير مشروع.....
47	المبحث الاول : أركان جريمة الدخول الغير مشروع .....
50	الفرع الاول : السلوك .....
59	الفرع الثاني : النتيجة.....
62	المطلب الثاني : الركن المعنوي.....
63	الفرع الأول : العلم .....
63	الفرع الثاني : الإرادة .....
65	المبحث الثاني : العقوبات المقررة للجريمة دخول غير مشروع .....
65	المطلب الأول: العقوبات المطبقة على الشخص الطبيعي .....
65	الفرع الأول: العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات.....
67	الفرع الثاني: العقوبات التكميلية.....
70	الفرع الثالث: الظروف المشددة.....
	<b>Erreur ! Signet non défini.</b>
72	الفرع الاول : العقوبات المطبقة على الشخص المعنوي.....
72	الفرع الثاني: عقوبة جريمة الاتفاق والشروع الجنائي .....
76	الخاتمة .....
79	قائمة المراجع .....

## ملخص مذكرة الماستر

ان الدخول الغير المشروع لنظام المعالجة الآلية للمعطيات، جريمة ورد النص عليها بمختلف التشريعات المقارنة ولحقها التشريع الجزائري بالدراسة ضمن تعديل قانون العقوبات لسنة 2004 والمعالجة الآلية للمعطيات مصطلح غريب عن لغة قانون العقوبات، ظهر نتيجة تطور العالم الافتراضي، هذا الكيان المفترض يخضع إلى نظام قانوني خاص وأي خرق له وبأي صفة كانت قد ينتج عنه ضرر للغير سواء كان الدخول أو البقاء في نظام المعالجة الآلية للمعطيات عن طريق الصدفة ويتعدد الضرر ما بين المساس بالحياة الخاصة إلى زعزعة الأمن القومي، وتختلف العقوبة بالنظر إلى مرتكب الجريمة سواء كان شخصا طبيعيا أو معنويا.

الكلمات المفتاحية :

1/ الجريمة المعلوماتية 2/ المعالجة الآلية للمعطيات 3/ جريمة الدخول الغير المشروع

## Abstract of The master thesis

The illegal entry to the data processing system is considered to be a crime that was stipulated in various legislations, and the Algerian legislation has followed it with study within the amendment of the Penal code of the year 2004.

And the automatic processing of data and any violation in any capacity that might result in harm to others, whether by entering or staying in the system of data processing by accident.

And the damage varies between prejudice of the private life to the destabilization of national security,

And the punishment that requires the criminal varies whether it was natural or moral.

keywords:

1/ Information crime 2/ Automated data processing

3/ Crime Illegal entry