جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

خصوصية الجريمة الإلكترونية و مدى تأثيرها على التشريع العقابي الجزائري

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: القانون الجنائي و العلوم الجنائية

من إعداد الطالب:

بن براهيم محمد المختار

عادم فاروق عبد اللطيف

تحت إشراف الأستاذ:

د. لريد محمد أحمد

أعضاء لجنة المناقشة

الدكتور اللقب والاسم	الرتبة العلمية	جامعة الانتماء	رئيساً
الدكتور اللقب والاسم	الرتبة العلمية	جامعة الانتماء	مشرفاً ومقرراً
الدكتور اللقب والاسم	الرتبة العلمية	جامعة الانتماء	عضواً

السنة الجامعية: 2025/2024

جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

خصوصية الجريمة الإلكترونية و مدى تأثيرها على التشريع العقابي الجزائري

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: القانون الجنائي و العلوم الجنائية

من إعداد الطالب:

بن براهيم محمد المختار

عادم فاروق عبد اللطيف

تحت إشراف الأستاذ:

الدكتور لريد محمد أحمد

أعضاء لجنة المناقشة

الدكتور اللقب والاسم	الرتبة العلمية	جامعة الانتماء	رئيساً
الدكتور اللقب والاسم	الرتبة العلمية	جامعة الانتماء	مشرفاً ومقرراً
الدكتور اللقب والاسم	الرتبة العلمية	جامعة الانتماء	عضواً

السنة الجامعية: 2025/2024

إهداء:

بسم الله والصلاة والسلام على من بعث رحمة للعالمين،

أشرف المرسلين:

والحمد لله الذي منحنا الصبر والقوة لنتم هذا العمل؛ أما بعد:

نهذي ثمرة جهدنا هذا إلى من قال فيهما ربنا ﷻ:

"وقل ربي إرحمهما كما ربياني صغيرا"

ونهدي هذا العمل إلى كل الإخوة، الأقارب، الزملاء والأصدقاء..

الشـــكـــر والـعـــرفـــان:

بعد الشكر لله وحده على ما أنعم علينا

من الصبر لإتمام هذا العمل المتواضع في أحسن الأحوال.

نشكره ونحمده حمدا كثيراً يليق بجلال وجهه وعظيم سلطانه؛

كما نتوجه بجزيل الشكر وأسمى العبارات إلى الأستاذ الدكتور المشرف

"لريد مُحَّد أحمد"

الذي أشرف على مذكرتنا ويسره وإرشاده في إنجاز هذا الموضوع.

ونشكر أعضاء لجنة المناقشة

"....." "....."

كما نتقدم بالشكر الجزيل إلى كل أساتذة قسم الحقوق،

وموظفي الإدارة والمكتبة

و إلى كل من ساعدنا من قريب أو بعيد.

قائمة المختصرات

- ق ع ج = قانون العقوبات الجزائري.
- ق إ ج ج = قانون الإجراءات الجزائية الجزائري.
- ج ر ج ج د ش = الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية

مقدمة

بعد الثورة الصناعية في القرن الثامن عشر تميز القرن العشرين باختراعات هائلة و ذلك في ظل الثورة الرقمية و التكنولوجية المعتمدة أساسا على الرققات الإلكترونية وتطور قدراتها ، حيث دخلت المجتمعات بسرعات متزايدة في تطبيق هذه الإختراعات في مختلف ممجالات الحياة (الإقتصادية و الإجتماعية و التعليمية و الصحية إلخ..) ، فغزت الحواسيب الآلية و الانترنيت جميع مجالات الحياة، و أضحى استخدامها ضرورة لا غنى عنها بالنسبة للدول و الحكومات و مؤسسات الدولة(في الجزائر مثلا :برنامج أسرتك، الحكومة الرقمية إلخ..) ، ساهم تطور هذه التقنيات في تسهيل التواصل و تبادل المعلومات و المراسلات و إبرام مختلف الصفقات مما جعل العالم عبارة عن قرية صغيرة مما يمكن التواصل و التعامل بين مجتمعات مختلفة و أجناس متنوعة في مدة زمنية قصيرة و استطاعت هذه القفزة تقديم خدمات جليلة للأمم و الشعوب، وبدأ العالم يدخل عصرا جديدا هو عصر المعلوماتية .

على الرغم من أهمية الوسائل الالكترونية و ايجابيات استعمالها على الفرد و المجتمع إلا أن هذا التقدم واكبه من جهة أخرى تطور الفكر و الفعل الإجرامي حيث تستخدم هذه الأنظمة المتطورة لمعالجة المعطيات لتحقيق أهذاف غير مشروعة، هذا ما أدى إلى ظهور نوع جديد من الجرائم سميت بالجرائم الالكترونية أو المعلوماتية أو جرائم التعدي غلى أنظمة معالجة المعطيات ، هذا النوع الحديث من السلوكات الإجرامية الماسة بأمن الدولة و سلامة النظم المعلوماتية و بحقوق الغير تشكل خطر بالغا ،كجرائم التحويل غير المشروع للأموال و جرائم المعلومات المخزنة .

بتزايد معدلات هذا النوع من الجريمة و تطور أشكالها و تهديداتها المباشرة التي مست المجتمعات المعاصرة و الأضرار الناجمة عن هذه الجرائم التي تستهدف الاعتداء على المعطيات في حد ذاتها أو إستخدام أنظمة معالجة المعطيات في إرتكاب الجرائم مما دفع بالمشرع الجزائري إلى محاولة مواكبة ال سرعة التي تتطور بها تكنولوجيا الإعلام و الإتصال للتكييف مع الواقع الحالي .

قام المشرع الجزائري بسن مجموعة من التدابير و إصدار قوانين جديدة لمواجهة و مكافحة الجرائم الألكترونية في الجزائر ،كما قام بتعديل بعض قوانينه القائمة كغيره من التشريعات الدولية الأخرى لمسايرة هذا التطور الحاصل في ميدان تكنولوجيا الإعلاوم و الإتصال ، بحيث أجري تعديل لقانون العقوبات الجزائري بإصداره عدة قوانين كالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 و الذي تم من خلاله استحداث نصوص خاصة متعلقة بالجرائم الماس ة بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 394 مكرر 7 و عدلت بالقانون 24-06 المعدل و المتمم لقانون العقوبات ، و الأمر رقم 03-05 المؤرخ في 19/07/2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، ، و قد أصدر كذلك القانون رقم 09-04 المؤرخ في 5/8/2009 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ،كما أجرى تعديلات على قانون الأجراءات الجزائية مثل الأمر رقم 11/21 الصادر بتاريخ 26 أوت 2021.

بناءا على ما سبق تبرز أهمية دراسة هذا الموضوع في الرغبة الملحة لتحليل الجرائمالإلكترونية و دراستها من مختلف جوانبها بإبراز خطورتها على المجتمع و كذلك التمعن في موقف المشرع الجزائري من هذه الجريمة الحديثة و معرفة كيفية تأثير خصوصيتها في كيفية تصدى المشرع لها من خلال النصوص الموضوعية و الإجرائية و بالتالي إظهاره مختلف السبل و الآليات المستجدة المعتمدة للحد منها .

ككل بحث علمي يعني بالبحث و الدراسة نجده لا يخلو من بعض الصعوبات و لعل أبرزها قلة المراجع الوطنية الحديثة المعالجة لموضوع الجريمة الإلكترونية و كذلك بصفة أدق قانون العقوبات و قانون الإجراءات الجزائية هو الأمر الذي شدنا إلى الخوض فيه و محاولة دراسة لكونه يتميز بكثير من المستجدات خاصة على الواقع العلمي .

تم الاعتماد في دراسة موضوع البحث على منهجين أوليان أولهما المنهج الوصفي، للجانب الفني

من الدراسة مع الاستعانة بالمنهج التحليلي في بعض مراحل البحث لمختلف القواعد و السنن القانونية المرتبطة بعناصر البحث .

و عليه من خلال هذه الدراسة سيتم محاولة تبيان أبرز النقاط المهمة المتعلقة بخصوصية الجريمة الإلكترونية و ذلك من خلال طرح الإشكالية التالية: إلى أي مدى تأثر التشريع الجزائي لجزائري بخصوصية الجريمة الإلكترونية؟

من أجل الكشف عن مختلف خ فليا الموضوع وكذا إيجاد أجوبة لكل التساؤلات المطروحة عبر الإشكال العام .

تم تقسيم الدراسة إلى فصلين أولهما عني بدراسة الخصوصية الموضوعية للجريمة الإلكترونية حيث تم تقسيمه بدوره إلى مبحثين أثنين أولهما معنون بمفهوم الجريمة الإلكترونية حيث تم التطرق عبر مطالبه الاثنان إلى تعريفها ودوافع ارتكابها أما المبحث الثاني فقد خصص إلى دراسة أنواع و خصائص الجرائم الإلكترونية في التشريع الجزائري .

بالنسبة للفصل الثاني تمت دراسة الجانب الاجرائي من خلال استعراض آليات مكافحة الجريمة الالكترونية والحد منها في التشريع الجزائري الذي قسم إلى مبحثين اثنين بالاعتماد على خطة ثنائية بسيطة حيث أوردنا

في المبحث الأول القواعد الموضوعية لمكافحة الجريمة الالكترونية قسمناه بدوره إلى مطلبين تعرضنا في أولهما إلى الحماية الجزائية للمعلوماتية من خلال نصوص قانون العقوبات وأوردنا في الثاني الحماية الجزائية للجريمة الالكترونية من خلال القوانين والتنظيمات الأخرى .

أما في المبحث الثاني تم التطرق من خلاله إلى مختلف القواعد الإجرائية لمكافحة الجريمة الالكترونية الذي تمت دراستها من خلال مطلبين أولهما يتمحور حول القواعد المنصوص عليها في قانون الإجراءات الجزائية و الثاني تطرق إلى الحماية الجزائية للمعلوماتية في ظل الأمر ر قم 11/21 المتضمن تعديل قانون الإجراءات الجزائية .

الفصل الأول

الخصوصية الموضوعية للجريمة الإلكترونية

شهد العالم في عقود الأخيرة تطورًا علميا متسارعا في مجال تكنولوجيا الإعلام و الإتصال ، لاسيما في مجال معالجة البيانات و قدرات الاتصال ، مما أدى إلى انتشار استخدام الحواسيب وشبكة الإنترنت في مجالات متعددة.

و رغم الفوائد الكبيرة التي توفرها الوسائل الإلكترونية ، فإن سوء استخدامها أدى إلى بروز نوع جديد من الجرائم يُعرف بالجرائم الإلكترونية . و بسبب حداثة هذا النوع من الجرائم، لم يتفق الفقهاء بعد على تعريف موحد لها ، كما أنها تتميز بخصائص فريدة و بتعدد أشكالها، إلى جانب ظهور فئة جديدة من المجرمين تختلف دوافعهم و أساليبهم في ارتكاب هذه الجرائم، حيث سيتم التطرق في هذا الفصل إلى مفهوم الجريمة الإلكترونية (**المبحث الأول**)، و بيان أنواع و خصائص الجريمة الإلكترونية (**المبحث الثاني**)

المبحث الأول

مفهوم الجريمة الإلكترونية

من خلال هذا المبحث سيتم تحديد التعاريف المختلفة للجريمة الإلكترونية و كذا الأركان التي ترتكز عليها و منه الدافع المؤدية إلى ارتكابها باعتبارها تقع في العالم الافتراضي على خلاف الجريمة التقليدية التي تقع في الواقع الملموس .

سيتم التعرض في هذا المبحث إلى مطلبين تعريف الجريمة الإلكترونية و أركانها (مطلب أول)، و دوافع الجريمة المعلوماتية (مطلب ثاني) .

المطلب الأول

تعريف الجريمة الإلكترونية و أركانها.

لم يجمع الفقه الجنائي على تسمية موحدة للجريمة المعلوماتية، فهناك عدة تسميات لهذه الجريمة، منها الغش المعلوماتي و البعض الآخر يطلق عليها إسم جرائم الحاسوب الآلي والآخر جرائم الكمبيوتر و الإنترنيت أو الجريمة الإلكترونية أو جرائم المعلوماتية أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات و فقا للمشرع الجزائري .

ظهر اتجاهين من الفقهاء منهم من ينظر إلى الجريمة الإلكترونية بمفهوم ضيق و منهم من ينظر إليها بمفهوم واسع ، كما أن للجريمة المعلوماتية أركان لا تقوم إلا بتوافرها و هذا ما سنتطرق إليه من خلال هذين الفرعين المواليين .

الفرع الأول:

تعريف الجريمة الإلكترونية

بالرغم من الجهود المبذولة لمكافحة و التصدي لهذه الظاهرة الإجرامية المعلوماتية ، إلا أنه لا يوجد تعريف شامل و محدد ومتفق عليه بين الفقهاء ، فقد اتجه جانب من الفقه إلى تناولها بالتعريف على النحو الضيق و جانب آخر على النحو الموسع .

أولا: التعريف الفقهي للجريمة المعلوماتية

تعددت التعريفات التي تناولت الجريمة المعلوماتية بسبب الخلاف الذي أثير في تعريف الجريمة و المعلومة ، فالجرائم المعلوماتية هي صنف جديد من الجرائم و المجرم المعلوماتي هو أيضا نوع جديد من المجرمين الذين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها لارتباطها بالتكنولوجيا الحديثة. لذلك لم

يجتمع الفقه على وضع تعريف محدد لها و متفق عليه، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق و جانب آخر عرفها على نحو موسع .

1.التعريف الضيق للجريمة الإلكترونية

من التعريفات المضيقة لمفهوم الجريمة المعلوماتية تعريف الفقيه « Rosenblatt [1] » **" كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الألي و إلى تحويل طريقه".**

كما عرفها الفقيه « Van der Merwe[2]» على أنها " **الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية** ". و عرفها "كلاوس تايدومان" بأنها **"كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلي."[3]**

و عرفت أيضا على أنها " **كل فعل غير مشروع يكون العلم بتكنولوجيا الحواسيب الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته من ناحية أخرى** "[4] ، حسب هذا التعريف أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها و التحقيق فيها ، و هذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية .

---

[1] ألبرت روزنبلات ولد بأمريكا سنة 1939 انتخب كنائب عام سنة 1969 ،تولى منصب قاضي في محكمة نيويورك سنة 1975 ثم قاضي بالمحمة العليا لولاية نيويرك سنة 1989 ، له عدة مؤلفات و محاضرات في القانون الجنائي .

2دانا فان دير ميروي. بكالوريوس في القانون (جامعة إيست أنجليا)، بكالوريوس في الحقوق، وماجستير في القانون العام (جامعة جنوب أفريقيا). أستاذة سابقة في القانون العام بجامعة جنوب أفريقيا، وحاليًا باحثة في الجامعة نفسها.

[3] عبد العال الديربي و محمد صادق اسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية و الانترنيت، ط1، المركز القومي للإصدارات القانوني، القاهرة، 2012، ص 40.

[4] نائلة قورة، جرائم الحاسوب الاقتصادية، ط1، دارالنهضة العربية، القاهرة، 2003، ص 21.

و عرفت أيضا بأنها " **الجرائم التي تلعب فيها بيانات الكمبيوتر و البرامج المعلوماتية دورا هاما، أو هي كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية**"[1].

ما يأخذ على التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام الإلكتروني، فالبعض من فقهاء هذا الاتجاه ركز على معيار موضوع الجريمة، و البعض الآخر ركز على وسيلة ارتكابها و البعض على معيار النتيجة.

و يدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة، تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها" **الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا**".[2]

2.التعريف الواسع للجريمة الإلكترونية :

في المقابل هناك تعريفات حاولت التوسع في مفهوم هذه الجريمة ذلك نتيجة الانتقادات الموجهة للاتجاه الأول ، فحاول الفقهاء تقديم تعريف واسع لهذه الجريمة لتفادي أوجه القصور التي شابت تعريفات الاتجاه المضيق للتصدي لظاهرة الإجرام المعلوماتي .

ذهب الفقيهان (Michel & Credo) "إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة، هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته."

كما قد تمتد هذه الجريمة لتشمل الاعتداءات المادية سواءا كانت على جهاز الحاسوب ذاته أو المعدات المتصلة به، و كذلك الاستخدام غير المشروع البطاقات الائتمان و انتهاك ماكينات الحسابات الآلية بما يتضمنه

[1] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، ط1، منشورات الحلبي الحقوقية، بيروت، 2014، ص 25.
[2] عبد العال الديربي و محمد صادق اسماعيل، مرجع سابق، ص 41.

من شيكات تمويل الحسابات المالية بطريقة إلكترونية و تزييف المكونات المادية و المعنوية للحاسوب بل و سرقة الحاسوب في حد ذاته أو مكون من مكوناته[1].

فتناول رأي آخر من الفقه تعريف الجريمة الإلكترونية بأنها " **عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسوب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقابا**"

و يرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها " **كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر**".[2]

كما عرفت في إطار المنظمات الأوروبية للتعاون و التنمية الاقتصادية على أنها "**كل فعل أو امتناع من شأنه أن يؤدي إلى الاعتداء على الأموال المادية و المعنوية، يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية**"[3]

لا شك أن هذا الاتجاه ينطوي على توسيع كبير لمفهوم الجريمة الإلكترونية لذا يأخذ عليه هذا التوسع الذي من شأنه أن يسقط وصف الجريمة الإلكترونية على أفعال قد لا تكون كذلك المجرد مشاركة الحاسوب الآلي في النشاط الإجرامي ، فبعض الجرائم كسرقة الحاسوب الآلي أو الأقراص مثلا لا يمكن إعطاء وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسوب أو أحد مكوناته المادية كانت محل لفعل الاختلاس .

[1] ونوغي نبيل، زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور بالجلفة الجزائر، المجلد الرابع، العدد الثالث، سبتمبر 2019، ص 130.

[2] عبد العال الديربي و مُحَمَّد صادق اسماعيل، مرجع سابق، ص41.

[3] حنان ريحان مبارك المضاحكي، مرجع سابق، ص130.

ثانيا : التعريف التشريعي للجريمة المعلوماتية

تأثر المشرع الجزائري بغيره من التشريعات الأجنبية الأوروبية منها و العربية فيما يخص القواعد التي استند أو اعتمد عليها و أتى بها لمكافحة الجرائم المعلوماتية، حيث اتجه إلى خلق نصوص جديدة و خاصة تتعلق بهذا النوع من الجرائم رغبة منه في تأمين أنظمة المعلومات من اعتداءات المجرمين، إذ نجد أنه ضمن موضوع الجريمة المعلوماتية في قانون العقوبات أو بموجب نصوص خاصة على حد السواء .

المشرع الجزائري على غرار ال تشريعات الأخرى لم يقم بتعريف الجريمة الالكترونية بل أوكل مهمة تعريفه إلى الفقه و القضاء[1] ، و إستقر المشرع على تسمية الجريمة المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجية الإعلام و الاتصال ، و تبنى في ذلك التعريف الذي ورد في الاتفاقيات الدولية للإجرام المعلوماتي بموجب المادة الثانية من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام و الاتصال و مكافحتها ، و عرفها على أنها "**جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية**[2] . "

و بالتالي تكون الجريمة المعلوماتية أيضا تلك الجرائم المرتكبة عن طريق أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين[3] ، و المرتكبة عن طريق أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[4].

يلاحظ على هذا التعريف ما يلي :

---

[1] قارة أمال ، الحماية الجنائية للمعلوماتية في التشريع الجزائري، ط 1، دارهومة، الجزائر، 2006، ص 101.

[2] المادة الثانية الفقرة أ من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والإتصال ومكافحته المؤرخ في 05 أوت 2009،ج رعدد 47، الصادرة في 16 أوت 2009،ص5.

[3] المادة الثانية الفقرة "ب"من القانون نفسه،المرجع نفسه.

[4] .المادة الثانية الفقرة "و" من القانون نفسه، المرجع نفسه.

أن المشرع الجزائري قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية أولها معيار وسيلة الجريمة و هو نظام الاتصالات الإلكترونية، ثانيها معيار موضوع الجريمة و المتمثل في المساس بأنظمة المعالجة الآلية للمعطيات ، و ثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات[1].

كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة المعلوماتية كونه أقر أن هذه الجريمة ترتكب في نظام معلوماتي أو يسهل ارتكابها فيه، وهذا ما يوسع نطاق مجال الجرائم المعلوماتية في القانون الجزائري .

و ترتيبا على كل هذه التعاريف الفقهية و التشريعية يمكننا القول أن الجريمة المعلوماتية هي كل سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته و يمس بالأشخاص أو الأموال أو أمن الدولة ، و هي على غرار الجرائم التقليدية تعرف من خلال أركانها بتوافر القصد الجنائي الارتكاب هذه الجريمة و الركن المادي للجريمة و ركنها المعنوي[2].

الفرع الثاني

أركان الجريمة الإلكترونية

تقوم الجريمة الإلكترونية شأنها في ذلك شأن أي جريمة على أركان أساسية، حيث سيتم دراسة هذه الأركان بصفة عامة من خلال الإشارة إلى كل ركن على حدى وفقا لما يلي:

أولا : الركن الشرعي في الجريمة الإلكترونية

يقصد به اعتراف المشرع و نصه قانونا على تجريم الفعل المرتكب، حيث أنه تطبيقا للقانون العقوبات الجزائري لا جريمة و لا عقوبة إلا بنص ، و تأكيدا على ذلك فإن المشرع الجزائري قد أحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الأموال تحت عنوان المساس بأنظمة

[1] ونوغي نبيل،زيوش عبد الرؤوف، مرجع سابق، ص 132.

[2] أنظر المادة 02 فقرة 2 من القانون رقم 09-04، مرجع سابق.

المعالجة الآلية للمعطيات[1]، و يشتمل على ثمانية (08) مواد تهتم بكل أنواع الاعتداءات على الأنظمة المعلوماتية، لذا فقد عمد المشرع على وضع نصوص خاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لتساير بذلك كل الاتجاهات التشريعية المعاصرة في هذا الشأن.

ثانيا : الركن المادي في الجريمة الإلكترونية

إن الركن المادي في هذه الجريمة يختلف من حال لآخر حسب التصنيف الذي يقع على الفعل، و عليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة و التي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض و بشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر، و هذا لا يسبب إشكالا، إذ تطبيق نصوص قانون العقوبات على هذه السلوكات التقليدية، إلا أنه هناك أنواعا أخرى من السلوك يتطلب التمييز بينها و بين سابقتها و هذا ما يدعو للتدخل التشريعي [2] ، فيتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي و النتيجة ، كالتبليغ عن الجريمة قبل تحققها[3].

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب و هو أغلب صور الجرائم الإلكترونية (مثلا : جريمة الغش الإلكتروني: الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية و المحررات الإلكترونية [4] ، أو كأن يقوم باختراق شبكة الاتصال يحصل على بيانات سرية و يقوم بنشرها .

---

[1] أنظر المادة 394 مكرر من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، الجريدة الرسمية، عدد 44 ،ص11.

[2] بن غدقة شريفة والقص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الانترنيت وطرق محاربتها، أعمال الملتقى الوطني، " آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس، ص 48.

[3] بوضياف أسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة الجزائر،العدد 11 ،2018، ص 354.

[4] عاقلي فضيلة، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية، طرابلس بتاريخ 24/ 25 مارس، 2017، ص 12.

و قد يكون السلوك الإجرامي سلبيا و هو الامتناع عن فعل كان من الواجب إتيانه مثل: امتناع موظف أمن عن حماية بيانات و معلومات الشركة التي يعمل بها و هو نادر الحدوث و في الغالب يرتكب من قبل موظفين مختصين .

ثالثا : الركن المعنوي في الجريمة الإلكترونية

تعد الجرائم الإلكترونية كغيرها من الجرائم و التي تفترض بالأساس وجود القصد العام أي العلم و الإرادة لتحديد المسؤولية الجنائية، و لا يمكن تصور وجود قصد خاص بالجريمة دون أن يسبقه القصد العام، أما عن وجود قصد خاص في الجرائم المعلوماتية فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة و النية الخاصة لدى الجاني من وراء قيام بالفعل غير المشروع أو ارتكاب الجريمة .

فيكون الركن المعنوي للجريمة الإلكترونية من عنصرين العلم و الإرادة، فالعلم هو إدراك الفاعل للجرم أو الفعل المجرم، أما الإرادة فهي توجه السلوك الإجرامي أي الرغبة لتحقيق النتيجة و بالرجوع إلى المبادئ العامة في قانون العقوبات الجزائري قد يكون القصد الجنائي عاما أو خاصا، فالقصد الجنائي العام هو : الهدف المباشر للسلوك الإجرامي، و ينحصر في حدود ارتكاب الفعل[1].

أما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه الجريمة بل يذهب إلى التأكد من تحقيق النتيجة مثلا في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه.

[1] بوضياف أسمهان،المرجع السابق، ص 354

أما فيما يتعلق بالجريمة الإلكترونية فالأصل أن الفاعل في هذه الجريمة يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه و قاصدا ذلك، و مهما يكن فلا يمكن انتفاء علمه كركن للقصد الجنائي العام[1].

و عليه فالقصد الجنائي العام متوفر في جميع الجرائم الإلكترونية دون أي استثناء، و لكن هذا لا يمنع أن بعض الجرائم الإلكترونية يتوفر فيها القصد الجنائي الخاص (مثلا جرائم تشويه السمعة غبر الانترنيت) و يبقى الأمر للسلطة التقديرية للقاضي في ذلك[2].

المطلب الثاني

دوافع ارتكاب الجريمة الإلكترونية

إن الباعث أو الدوافع هو العامل المحرك لإرادة توجيه السلوك الإجرامي و غالباً ما تتجه التشريعات العقابية إلى اعتبار الدافع عنصراً من عناصر التجريم إلا في الأحوال التي يحددها القانون صراحة، فالجريمة تقوم بتحقيق عناصرها و أركانها أيا كان الدافع من وراء ارتكبها، حيث ستم دراسة الدوافع الشخصية (**الفرع الأول**) و أخرى موضوعية لارتكاب الجريمة الإلكترونية (**الفرع الثاني**).

الفرع الأول

الدوافع الشخصية لارتكاب الجريمة الإلكترونية

إن الدوافع الداخلية الشخصية هي المحرك الذي يدفع الإنسان إلى الإقدام على السلوك الإجرامي و هي تتعلق بشخصيته حيث يسعى من خلالها لتحقيق أهدافه الذاتية الخاصة و التي تتمثل في كل من الدوافع المادية (**أولاً**) و كذا الدوافع المعنوية (**ثانياً**) .

---

[1] سوبرسفيان،الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبوبكر بلقايد، تلمسان، الجزائر، 2010، ص 12.

[2] محمود نجيب حسني،شرح قانون العقوبات، دار النهضة العربية، القاهرة، 1992، ص 4.

أولاً: الدوافع المادية

يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة المعلوماتية و ذلك أن الربح الكبير و الممكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على النفسية المعلوماتية و استغلال الفرص و السعي إلى الاحتراف بغية تحقيق مكاسب بأقل جهد دون ترك أي أثر وراءه[1].

فالإنسان بغية تلبية حاجياته الأساسية الفيزيولوجية كانت أو الاجتماعية فإنه يحتاج إلى المال الذي يعد عصب الحياة من أجل تحقيق و تلبية هذه الحاجيات مما يجعل مرتكبي الجريمة التكنولوجيا وفر الكثير من المعلومات التي يمكن لمرتكبي الجرائم الإلكترونية استغلالها و استخدامها عن طريق بيعها في ظل عصر بيع المعلومات و الجوسرة التي ساهمت في تطور سوق المعلومات باختراق أنظمة و بيانات الدول و الهيئات و المؤسسات، و هذا ما مثل دافعاً أساسياً لارتكاب مثل هذه الجرائم بل يعد المحرك الأول و الأساسي لأي جريمة إلكترونية في ظل عصر المعلومات اليوم[2].

و يجدر منا الإشارة في هذا المجال إلى أن هناك مجلة تسمى بالأمن الآلي التي تختص في الأمن المعلوماتي حيث أن الإحصائيات المعلن عنها في حالات الغش تتمثل في 43 % أما حالات اختلاس الأموال هي 23 % و كذا 15% لاستغلال غير مشروع للحاسوب من أجل تحقيق منافع شخصية [3]، غير أن هذا لا ينكر أن هناك دوافع و أسباب أخرى تدفع الأفراد لارتكاب هذه الجريمة لتحقيق أهداف أخرى قد تكون مادية أو معنوية [4] .

---

[1] وضاح محمود نشأت، مقضي المجالي، جرائم الأنترنيت، دارالمنارة للنشر، عمان، 2005، ص 30.

[2] صابر بحري،خرموش مني، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات فيسيكولوجية الانحراف، المجلد 06، العدد 01، جامعة محمد لمين، دباغين، سطيف، الجزائر 2021، ص48.

[3] الرومي محمد أمين، الكمبيوتر والأنترنت، دارالمطبوعات الجامعية الإسكندرية، مصر، 2004، ص 90

[4] بوخبزة عائشة، الحماية الزائية من الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجيستير في القانون الجنائي،كلية الحقوق، جامعة وهران، 2012 – 2013، ص 61.

ثانيا : الدوافع المعنوية

تتمثل هذه الدوافع المعنوية في دافع الحصول على معلومات جديدة، كما أن هنالك من يرتكب جرائم الحاسوب بغية الحصول على الجديد من المعلومات، بالإضافة إلى أنه نجد أشخاص يقومون بالبحث و اكتشاف الأنظمة و العمل من خلال الجماعة و تعليم بعضهم، حيث يفضل هؤلاء القراصنة البقاء مجهولين أكثر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة فالكثير من مرتكبي الجريمة الإلكترونية يكون دافعهم حبا لاطلاع و الحصول على المعلومة، ضف إلى دافع الاستلاء على المعلومة، كما نجد دافعاً آخر يتمثل في الرغبة على فهم النظام الإلكتروني و التغلب عليه، و ذلك بسبب ميول هؤلاء الأشخاص بإبراز على تفوقهم على وسائل التكنولوجيا الحديثة ، إذ أن هذه الرغبة و إثبات الذات و تحقيق الانتصار الشخصي على الأنظمة الإلكترونية من الدوافع النمطية لارتكاب الجريمة ، فالمجرم الإلكتروني في حال تمكنه من الانتصار على النظام المعلوماتي يشعر بتقدير الذات و تعزيز الثقة لديه ، حيث أن في ارتكابه للجريمة الإلكترونية يحقق دوافع نفسية، و من الدوافع المعنوية دافع التسلية و لعل الكثير من مرتكبي الجرائم الإلكترونية يكون دافعهم الأول هو المزاح و التسلية و بمجرد احترافهم فيها يصبحون مجرد هاوين لهذه الجرائم إلى محترفين خطرين ، كما يعتبر أيضا دافع الإثارة و المتعة دافعاً معنويا لارتكاب الجريمة الإلكترونية [1].

الفرع الثاني

الدوافع الموضوعية لارتكاب الجريمة الإلكترونية

تتمثل الدوافع الموضوعية في تلك الدوافع الخارجية أي كل الأسباب و العوامل التي تكون خارجة عن ذات الفرد و التي ليس لها علاقة بشخصيته، و لهذه الأسباب أهمية كبيرة في مجال الجريمة الإلكترونية، بحيث قد يتأثر المجرم الإلكتروني ببعض المواقف التي قد تكون دافعه لارتكاب الفعل الإجرامي الإلكتروني، كما أنه لا يسعى فيها المجرم

[1] صابر بحري،خرموش مني، المرجع السابق،ص55.

الإلكتروني حينها لكسب المال و لا التسلية و لا حتى الإثارة و المتعة، ضف إلى أن هذه الدوافع تتعلق بدافع الانتقام و إلحاق الضرر بالغير (**أولاً**) ، وكذا دافع التعاون والتواطؤ (**ثانياً**)، بالإضافة إلى الضغوطات العامة (**ثالثاً**).

أولاً: دافع الانتقام وإلحاق الضرر بالغير

تُعد الدوافع النفسية من أهم العوامل المؤثرة في سلوك الجريمة الإلكترونية، و يأتي دافع الانتقام في مقدمة هذه العوامل لما له من أثر بالغ على السلوك الإجرامي . إذ يُعتبر الشعور بالظلم أو الحرمان الوظيفي من المحفزات الأساسية التي تدفع الأفراد ذوي المعرفة التقنية إلى استغلال قدراتهم و معلوماتهم ضد المؤسسات التي كانوا يعملون بها.

يرتبط دافع الانتقام ارتباطًا وثيقًا بالوظيفة التي يشغلها الفرد داخل المؤسسة، حيث قد ينشأ نتيجة الطرد من العمل ، الإقصاء المهني، أو الشعور بالحرمان من الحقوق المشروعة. و عادةً ما يكون مرتكب هذا النوع من الجرائم مطلعًا بشكل دقيق على أنظمة المؤسسة و إجراءاتها الداخلية، مما يمكنه من إحداث أضرار ملموسة[1].

و تبرز حالة محاسب قام بالتلاعب ببرامج الحسابات الإلكترونية الخاصة بالشركة التي كان يعمل بها كمثال على ذلك ، حيث عمد إلى برمجة الأنظمة بطريقة تسمح بإخفاء كافة البيانات المتعلقة بديون الشركة، محددًا تاريخًا معينًا لتنفيذ عملية الإخفاء بعد مغادرته للعمل. وقد أدى هذا الفعل إلى إلحاق أضرار مادية جسيمة بالمؤسسة ، مما يعكس خطورة دافع الانتقام حين يقترن بمهارات تقنية متقدمة.

تُظهر هذه الحالة أهمية تبني المؤسسات لسياسات أمنية مشددة فيما يخص إدارة المعلومات الحساسة، لاسيما خلال فترات إنهاء الخدمة أو انتقال الموظفين ، مع تعزيز أنظمة الرقابة الداخلية للحد من احتمالات استغلال المعلومات لأغراض إجرامية[2].

[1] صابر بحري، خرموش منى، مرجع سابق، ص 52.

[2] سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، شهادة الماجستير في العلوم القانونية، تخصص علوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013 ، ص42.

كما نجد كذلك أسباب تدفع المجرم الإلكتروني لإتيان الفعل الإجرامي بغية الانتقام من الضحايا كتشويه سمعة الضحية من خلال نشر معلوماته الشخصية السرية ، تتبعه خلاف مع الضحية لأسباب شخصية أو مهنية، فشخصية المجرم الإلكتروني لها دور في تحديد البعد الانتقامي لديه ، فالكثير من الجرائم يكون دافع الانتقام المنجز من المجرم الإلكتروني لا يستحق ذلك الانتقام ، فالمجرم الإلكتروني حفظاً عنه عن ذاته وتحقيق لها هذا ما يدفع لإتيان السلوك الإجرامي[1].

ثانيا : دافع التعاون و التواطؤ

تشير الدراسات إلى أن عدداً كبيراً من مرتكبي الجرائم الإلكترونية يميلون إلى تشكيل جماعات متخصصة في هذا المجال ، حيث يتعاونون بشكل منظم لتنفيذ الأفعال الإجرامية بدقة عالية، بهدف تحقيق مصالح مشتركة قد تكون ذات طبيعة شخصية أو نفسية[2].

و يُلاحظ أن هذا النمط الإجرامي يتكرر بصفة ملحوظة في الفضاء الإلكتروني ، إذ تتوزع الأدوار بين أفراد المجموعة بما يضمن فاعلية العمليات الإجرامية؛ حيث يتكفل المتخصصون في الأنظمة المعلوماتية بالجانب الفني للعملية ، في حين يتولى عناصر آخرون من خارج المجال التقني عمليات التلاعب و تحويل المكاسب المالية الناتجة عن هذه الجرائم . كما يتميز هذا النوع من الجماعات بتبادل منتظم و دقيق للمعلومات المتعلقة بأنشطتهم ، فضلاً عن ممارستهم المستمرة للتجسس على الأنظمة الإلكترونية المستهدفة[3] .

ثالثاً : الضغوطات العامة

تتمثل هذه الضغوط في البطالة ، الفقر، و الظروف الاقتصادية الصعبة، حيث تُعد من أبرز العوامل التي تضغط على المجتمع بشكل عام ، و على فئة الشباب بشكل خاص. و ينتج عن هذه الضغوط مشاعر سلبية لدى

[1] صابر بحري، خرموش منى، مرجع سابق، ص 53.
[2] المرجع نفسه، ص 54.
[3] سعيداني نعيم،المرجع سابق، ص 61.

فئات واسعة من الناس تجاه المجتمع و ظروفهم المعيشية ، مما يدفع بهم إلى التأقلم السلبي مع هذه الظروف الصعبة منها الإتجار الإلكتروني بالبشر و الجنس و غيرها ، ترتبط الجريمة الإلكترونية ارتباطًا مباشرًا بالضغوط النفسية التي يعاني منها الفرد ، مما قد يدفعه إلى ارتكاب أفعال إجرامية بمختلف أشكالها . و عندما يمتلك الشخص مهارات تقنية في المجال الإلكتروني ، فقد تدفعه هذه الضغوط ، الناتجة عن عوامل اجتماعية مثل الفقر و البطالة و التهميش، إلى التفكير في الجريمة الإلكترونية كوسيلة لحل مشكلاته . فقد يسعى من خلالها إلى تحقيق مكاسب مادية لتلبية احتياجاته الأساسية، أو للتغلب على مشاعر الفراغ و الوحدة . كما أن تأثره بالآخرين و دعمهم له قد يعزز لديه هذا السلوك الإجرامي ، بحثًا عن الشعور بالانتماء و المساندة[1].

المبحث الثاني

أنواع و خصائص الجرائم الإلكترونية في القانون الجزائري

تعد الجرائم الإلكترونية من الجرائم المستحدثة حيث اختلف الفقه حول تصنيفها إلى عدة تقسيمات، إذ لم تراع أغلب التقسيمات خصائص الجرائم الإلكترونية و موضوعها ، إذ نجد أهم ما يميز الجرائم الإلكترونية عن غيرها هو أن هذه الجريمة تستهدف البيانات و أنظمة التشغيل للحاسوب الآلي و ترتكب بواسطة جهاز الإلكتروني ، كما اختلف الفقهاء في تقسيم الجرائم الإلكترونية نتيجة ظهور جرائم جديدة من حين إلى آخر، أي أن الجرائم الإلكترونية غير محصورة فلا يمكننا أن نجمل أصنفها و أشكالها و خصائصها فهي متغيرة و متجددة ، فكلما ظهرت وسيلة جديدة لاستخدام الحاسب الألي ظهرت معها جريمة جديدة، غير أن الفقهاء لم يستقروا على معيار واحد لتصنيف الجرائم الإلكترونية و هذا راجع إلى كثرة هذه الجرائم و سرعة تطورها، و هذا التصنيف يعود إلى الوسيلة التي يتم بها ارتكاب الجريمة أو على أساس محلها ، ضف إلى أن المجرم المعلوماتي له تميزه معينة عن المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي و معرفي للمجرم في عملية ارتكابها فإن الأمر يختلف

[1] نياب موسى، الجرائم الإلكترونية المفهوم والأسباب، الملتقى العلمي للجرائم المستحدثة في ظلال تغيرات و التحولات الإقليمية و الدولية، كلية العلوم الاستراتيجية، الأردن، 2014، ص 15.

بالنسبة للجرائم المعلوماتية، فهي جرائم فنية حيث يكون مرتكبها ذو قدرة في المجال الإلكتروني و مختص في مجال الشبكة الإلكترونية .

المطلب الأول

أنواع الجرائم الالكترونية في القانون الجزائري

لقد اختلف الفقه في تقسيم و تصنيف الجرائم الالكترونية و ذلك نتيجة ظهور جرائم جديدة و مستحدثة من حين لأخر، فكلما ظهرت وسيلة جديدة لاستخدام الحاسوب الآلي و الانترنيت ظهرت معه جريمة جديدة [1]، فهناك من يصنفها بحسب طبيعتها إلى جريمة عادية و جريمة سياسية، جريمة عسكرية و أخرى إرهابية، حيث أن البعض يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو على أساس محل الجريمة، أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الالكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع و لم يحددها و بالتالي: تتمثل في كل من الجرائم المرتكبة بواسطة تكنولوجيا الإعلام و الاتصال، أما النوع الآخر يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع الجزائري بموجب قانون العقوبات و هذا ما سيتم تناوله في الفروع الموالية .[2]

الفرع الأول

الجرائم المرتكبة باستخدام النظام المعلوماتي

تتنوع الجرائم التي ترتكب بواسطة النظام المعلوماتي ما بين جرائم اقتصادية أو قرصنة المعلومات أو ذات طابع سياسي أو متعلقة بالأمن القومي و قد تقع هذه الجرائم على الأشخاص الطبيعة أو الاعتبارية و الجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار [3] ، سيوضح كل نوع منها في البنود الآتية :

---

[1] يوسف خليل يوسف العفيفي، الجرائم الالكترونية في التشريع الفلسطيني دراسة تحليلية مقارنة، رسالة لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون الجامعة الإسلامية، غزة، 2013، ص 13

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي العام الديوان الوطني للأشغال التربوية، ط1، الجزائر، 2002، ص 24.

[3] المادة 394 مكرر 3 من قانون العقوبات الجزائري المعدل و المتمم.

أولا: الجريمة الإلكترونية الواقعة على الأشخاص

و هي من الجرائم المتعلقة بإتلاف و تعطيل الممتلكات الخاصة بالناس على الانترنيت، و يطلق بعض الفقهاء على هذا النوع من الجرائم مصطلح جريمة الاعتداء على الحياة الخاصة للأفراد باعتبار حق حماية الحياة الخاصة من أهم الحقوق و ذلك لما له من ارتباط وثيق بحرية الفرد، و قد جاء تجريم هذا النوع من الأفعال كحماية من التهديد الحقيقي الذي تشكله تكنولوجيات المعلومات لحق الأفراد في احترام حياتهم الخاصة مع انتشار ما يسمى ببنوك المعلومات بمختلف أنواعها الأمنية المالية، السياسية، الطبية العسكرية ... إلخ.[1]

و عليه يمكن أن يستخدم النظام المعلومات في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد بصور متعددة من أهمها:

- جمع البيانات وتخزينها على نحو غير مشروع .
- إساءة استعمال البيانات أو المعلومات الاسمية .
- الإفشاء غير المشروع للبيانات و المعلومات الاسمية .
- الاعتداء على سرية الاتصالات و المراسلات .

و من خلال هذا العنصر سيتم التعرض إلى بعض الجرائم التي ترتكب بواسطة النظام المعلوماتي عن طريق الانترنيت من بينها ما يلي :

1.جرائم السب والقذف عبر الانترنيت

عرفت المادة 297 من قانون العقوبات الجزائري السبب قولها: يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا، أو قدحا لا ينطوي على إسناد واقعة .

[1] سوير سفيان، جرائم المعلوماتية، مذكرة ماجيستر في العلوم الجنائية، جامعة أبوبكر بلقايد، تلمسان،2010، ص 35.

كما يعرف القذف على أنه: " إسناد واقعة محددة تستوجب عقاب من تنسب إليه أو احتقاره إسنادا علينا يفيد نسبة الأمر إلى الشخص على سب التوكيد . و يتضح من النصوص السابقة أن السب و القذف يتطلب أن بكل وضوح العلانية كما نص القانون على ذلك صراحة أي نشر السب و القذف عن طريق الانترنيت تتحقق به العلانية .

لقد اعتبر المشرع الجزائري صراحة من بين مكونات الركن المادي لارتكاب هذه الجريمة أن تكون موجهة لشخص الرئيس لاعتبار هذا الأخير من رموز السيادة الوطنية و هذا ما نصت عليه المادة 144 مكرر من قانون العقوبات الجزائري، يعاقب بغرامة من 100.000 دج إلى 500.000 دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان عن طريق الكتابة أو الرسم أو التصريح أو بأية آلة لبث الصوت أو الصورة أو بأية وسيلة الكترونية أو معلوماتية أو إعلامية ."

2.جرائم الاعتداء على الحياة الخاصة

فقد عني المشرع الجزائري بإضفاء الحماية على الحياة الخاصة سواء بالدستور أو بالقانون ، و قد يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة كما لو قام شخص بعمل بالنظام المعلوماتي بإعداء ملف يحتوي على معلومات تخص شخص بدون علمه و بغير إذنه و قام هذا الشخص بإطلاع الغير عليها بدون إذن صاحبها كما في حالة الأسرار المودعة لدى المحاسبين أو لدى الأطباء. فكل هذه الأسرار يحميها القانون و يجرم إفشاءها غير المشروع و بدون موافقة صاحبها ، و جريمة التعدي على الحياة الخاصة و الاطلاع على الأسرار أو إفشاءها قد تتم بنشر المعلومات على الكومبيوتر و فتح السجلات الالكترونية و الإطلاع عليها من خلال شاشة الكمبيوتر .

و يدخل كذلك في نطاق جرائم التعدي على الحياة الخاصة جريمة تسجيل المحادثات الشخصية أو مراقبتها بأية وسيلة حيث نجد بعض المتسللين يستطيعون اختراق شبكة الإنترنيت بطرق غير مشروعة و التنصت على هذه المكالمات.

و على هذا فقد نص المشرع الجزائري في المادة 303 مكرر[1]، يعاقب بالحبس من ستة (6) أشهر إلى 3 سنوات و بغرامة من 50.000 دج إلى 300.000 دج ، كل من تعمد المساس بحرمه الحياة الخاصة للأشخاص بأية تقنية كانت و ذلك :

أ – بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه .

ب – بالتقاط أو تسجيل صورة الشخص في مكانه خاص، بغير إذن صاحبها أو رضاه .

3. الجريمة الالكترونية الواقعة على حقوق الملكية الفكرية

إن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى أنه يصنفك اعتداء على قيمته المالية كون أن المعلوماتية ذو قيمة أدبية و مادية، كما تندرج براءات الاختراع ضمن الحقوق الفكرية، فقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية خاصة في الأمر رقم 03-05 الصادر في 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، و الأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الاختراع .

مع هذا التطور فقد ظهرت مشاكل التعامل مع نوع جديد من أنواع الملكية الفكرية يمكن وصفها بالملكية الرقمية و هي تلك الملكية التي تنصب على برامج الحاسوب و بياناتها و المصنفات الرقمية المنشورة على شبكة الانترنيت فقد أشار المشرع الجزائري إلى مفهوم المصنفات الرقمية في الأمر رقم 05/03 المؤرخ في 19/07/2003[2] في نصوص المواد 02،03،04،05 إضافة إلى نص المادة 03 و المادة 27 من الأمر 08/03 المؤرخ في 23/07/2003 [3]إن جرائم المعلوماتية هي من أكثر الجرائم التي تمس بحق المؤلف من خلال ما يعرف بجرائم التقليد (La contrefaçon) مثل جرائم التحميل غير المشروع عبر شبكة الانترنيت، فملايين المتصفحين الشبكة الانترنيت اعتادوا على تحميل الأفلام

[1] المادة 303 مكرر من القانون 06-23 المعدل و المتمم لقانون العقوبات.

[2] الأمر رقم 03-05 مؤرخ في 19 جمادى الأول عام 1424 الموافق لـ 19 يوليو 2003،المتعلق بحماية المؤلف من الحقوق المجاورة، ج ر،عدد 44.

[3] الأمر رقم 03-08 المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، صادر في تاريخ 23/07/2003، الجريدة 44 الرسمية، عدد 36، ص35

و الموسيقى دون شرائها من مصدرها الأساسي، معتمدين في ذلك على برامج متخصصة في فك شفرات الحماية و ذلك إما بغرض استعمالها الشخصي أو بغرض إعادة نشرها و طرحها للغير على شبكة الانترنيت أو للبيع على وسائط تخزين خارجية كالأقراص المضغوط[1] .

ثانيا : الجرائم الواقعة على النظم المعلوماتية الأخرى

تتحقق هذه الجريمة باستخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات و التنصت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدام البطاقة الإئتمانية [2] .

بالنسبة للجريمة الولوج غير المشروع للمعلومات المعالجة أليا تنقسم إلى الولوج المباشر بها يستطيع الجاني الإستلاء على المعلومات المخزنة بعدة طرق هي :

1- باستخدام آلة طباعة لاستخراج المكتوب على ورق .

2-استخدام شاشة النظام و الإطلاع بالقراءة على ما هو مكتوب عليها .

3-باستخدام مكبر الصوت أو سماعات لالتقاط المعلومات و البيانات المعالجة كما هناك كذلك الولوج غير المباشر و يكون ذلك باستعمال شبكات الاتصال البعيدة و المعالجة عن بعد إلى مخاطر تتمثل في التقاط و التسجيل غير المشروع للمعلومات أثناء بثها و حركتها[3].

أما الحالة الثانية تكون في حالة إساءة استخدام العميل البطاقة الائتمانية، و ذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الائتمانية و شروط العقد المبرم بينه و بين البنك، كاستعماله بطاقة الائتمانية انتهت مدة

[1] فليح نور الدين،الجريمة الالكترونية و آليات مكافحتها في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص قانون جنائي و العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر، سعيدة،2019/2018، ص40.

[2] ناير عائشة، الجريمة الإلكترونية في التشريع الجزائري،مذكرة لنيل شهادة الماستر في القانون الإداري،جامعة أحمد دراية،أدرار،الجزائر،2016-2017،ص26.

[3] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، دون بلد النشر، 2006، ص190.

الصلاحية أو تم إلغائها أو بعد الإبلاغ بضياعها، و كذلك إساءة استخدام الغير لهذه البطاقات كاستعماله لبطاقة مسروقة للحصول على الخدمات و السلع أو سحب مبالغ بموجبها، أو السحب باستخدام بطاقة مزورة[1].

ثالثا : الجريمة الإلكترونية الواقعة على الأسرار

إن أنظمة المعلوماتية أصبحت أيضا تستخدم في إفشاء الأسرار ،خاصة تلك التي تخص الدولة مثل أسرار المالية أو العسكرية أو الاقتصادية أو أسرار مهنية مثل الأسرار المتعلقة بالمحامين و القضاة فكل موظف يباشر النظام المعلوماتي يدرك قيمة السرية فهو مطالب بحمايتها و كل إفشاء يعتبر جريمة[2]، في حين تكون هذه الأسرار إما أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات الخاصة، فيتخذ هذا النوع من الجرائم صورتين، الأولى تتعلق بالجرائم الواقعة على أسرار الدولة، من بينها الإطلاع على مختلف الأسرار خاصة العسكرية منها و الاقتصادية[3]، و الثانية متعلقة بالجرائم الواقعة على الأسرار المهنية، و الهدف من ارتكاب هذه الجريمة هو سرقة معلومات الغير قصد التشهير أو بيع هذه المعلومات لتحقيق المصلحة الخاصة.[4]

هذا ما جعل المشرع الجزائري حريص على حماية هذه الأسرار من خلال نصوصه في الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات و ذلك بالإضافة إلى المادة 394 مكرر 03 التي تنص على: تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام .[5]

[1] أحمد خليفة الملط، المرجع السابق، ص 197.

[2] أحمد خليفة الملط ،لمرجع نفسه، ص 198.

[3] صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 57.

[4] سوير سفيان، المرجع السابق، ص38

[5] القانون 04-15 ،مرجع سابق.

الفرع الثاني

الجريمة الإلكترونية الواقعة على النظام المعلوماتي

تعتبر هذه الصورة بدون شك أكثر الصور خطورة و انتشارا حيث يتم بواسطة الاحتيال إدخال معطيات في نظم المعالجة الآلية للمعطيات أو إتلافها أو حذفها أو تغيير المعطيات المدرجة فيها [1]

و قد عالج المشرع الجزائري هذا النمط من الجرائم من خلال القانون رقم 04-15 الصادر في 10 نوفمبر 2004 المتضمن قانون العقوبات، و ذلك بتجريم كل أنواع الاعتداءات التي تمس بالأنظمة المعالجة الآلية للمعطيات، و قد ورد نص التجريم في القسم السابع مكرر من قانون العقوبات المعدل و المتمم بالقانون رقم 24-06 المؤرخ في 2024/04/28 ، و ذلك بعنوان المساس بأنظمة المعالجة الآلية للمعطيات ذلك في المواد 394 مكرر إلى 394 مكرر 07 ، فالاعتداء يأخذ صورتين هما: الدخول و البقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية و أفعال إجرامية أخرى[2]، و هذا ما سنتناوله فيما يلي :

أولا : جريمة الدخول أو البقاء في منظومة معلوماتية

إن قانون العقوبات الجزائري من القوانين العربية السباقة إلى دراسة هذا الموضوع، خطى المشرع الجزائري هذه الخطوة بتعديل قانون العقوبات، و ذلك بإضافة القسم السابع مكرر . بمحتوى المواد 394 مكرر إلى 394 مكرر 7 ، و قد نصت المادة 394 مكرر منه على ما يلي: (يعاقب بالحبس من ست (6) أشهر إلى سنتين (2) و بغرامة من

[1] سومية عكور، الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانون والأمني المتلقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، الأردن،02-04-09-2016،ص 12.

[2] زبيدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، داراالهدى، الجزائر، 2011، ص 46.

60.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك[1] .

فالملاحظ على هذا النوع من الجرائم ، أنها ليست من الجرائم التي يطلق عليها جرائم ذو الصفة، مثل الرشوة أو الاختلاس أو الزنا . بل تقع و ترتكب ضد كل شخص أي كانت صفته سواء كان يعمل في مجال الأنظمة الآلية لمعالجة المعطيات أم لا، سواء كان يفهم أم لا طريقة تشغيل النظام و سواء كان يستطيع أن يستفيد من الدخول أم لا[2]

1.فعل الدخول إلى النظام

إن مدلول كلمة الدخول تنصرف إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي ، أو السيطرة على المعطيات و المعلومات التي يتكون منها ، لم يحدد المشرع الوسيلة التي يتم بها الدخول إلى النظام ، و لذلك تقع الجريمة بأية وسيلة أو طريقة ، فقد يلجأ الجاني إلى التلاعب بعناصر النظام المادي لكي يصل إلى هدفه و هو الدخول أو يربط بجهاز تنصت يستطيع من خلاله اختراق النظام و استقبال المعلومات، كما قد يكون عن طريق فيروس مثل فيروس حصان طروادة [3]، أو عن طريق استخدام أرقام سرية لشخص أخر أو عن طريق تجاوز نظام الحماية ، ويتم بطرق غير مباشرة أم مباشرة ،كما هو الحال في الدخول عن بعد من خلال شبكات الهاتف النقال و يكون الدخول

[1]قانون رقم 24-06 المؤرخ في 19 شوال 1445 الموافق ل 28 أبريل 2024 المعدل و المتمم لقانون العقوبات،ج.ر.ج.ج.د.ش،العدد30،الصادرة في 30 أفريل 2024.

[2]قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، 2004، ص 343

[3]فيروس حصان طروادة، وهو برنامج فيروس لديه قدرة على الاختفاء في البرنامج الأصلي للمستخدم، وعندما يتم تشغيل البرنامج الأصلي ينشط هذا الفيروس وينتشر ليبدأ في نشاط التدمير، وهو ما يؤدي إلى تعطيل البرنامج وتزويد المعلومات ومحو بعضها وقد يصل إلى تدمير النظام بأكمله.

غير مشروع مثال ذلك الأنظمة المتعلقة بأسرار الدولة أو دفاع اتها و كذلك إذا كانت فعل يتطلب الدخول إليه دفع المال ، و تم الدخول إليه دون دفع المال. [1]

ففعل دخول يتسع ليشمل كل فنيات الدخول الاحتيالية في منظومة محمية كانت أو غير محمية ، كما يشمل استعمال من لاحق في ذلك المفتاح للدخول إلى المنظومة .

2.فعل البقاء داخل النظام

هو كل تواجد غير عادي داخل نظام المعالجة الآلية للمعطيات ضد إدارة من له حق في السيطرة على هذا النظام ، أي الدخول والنظر فيه و في المعطيات التي يتضمنها و غيرها من التصرفات الغير المسموح بها و التي تشكل بدورها بقاء احتياليا[2].

يتحقق الركن المادي لهذه الجريمة في الحالة التي يجد فيها الشخص نفسه داخل النظام المعلوماتي عن طريق الخطأ أو الصدفة إلا أنه يقرر البقاء ، داخل النظام و عدم قطع الاتصال به و يمكن تصور ذلك في الحالة التي يكون فيها الشخص يريد الدخول إلى نظام معلوماتي له الحق في الدخول إليه إلا أنه يجد نفسه لسبب ما دخل نظام أخر، كما لا يشترط لقيام هذه الجريمة حدوث نتيجة جرمية معينة، فيكفي البقاء غير المصرح به داخل النظام المعلوماتي ليقوم الركن المادي [3] . أما الركن المعنوي لا يتوفر متى كان دخول الجاني أو بقاءه داخل النظام مسموح به أي مشروعا، كما يمكن أن تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يجرم البقاء حتى و لو حصل الدخول بصفة عرضة[4]

[1] محمد حماد مرهجال هيبتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، 2005، ص 183.
[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر و الانترنيت، دار الكتب، القاهرة،2002، ص -235
[3] نهلا عبد القادر المومني، مرجع سابق، ص 161.
[4] حمزة بن عفون، مرجع سابق، ص 184.

ثانيا : جريمة المساس بمنظومة معلوماتية

جرم المشرع الجزائري كل فعل يهدف إلى إعاقة أو تحريف أو إفساد تشغيل نظام معالجة البيانات و ذلك في نص المادة 394 مكرر 01 قانون العقوبات و يشرط بالإضافة إلى فعل الدخول للنظام أو البقاء فيه ، إحداث استمرار في تخريب نظام تشغيل معالجة المعطيات سواء بتعطيله ، بإفسادها و تغييه، و يكون ذلك بأية طريقة تكن، سواء بالإعاقة المادية كإتيان أعمال عنف على أجهزة الحاسوب ، أو بالإعاقة المعنوية كإدخال فيروس على البرامج ، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكتفي أن يصدر من الجاني إحداهما فقط لكي يتوافر الركن المادي. [1]

تجدر الإشارة إلى أن المشرع الجزائري جرم كل من الاشتراك و الشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية ، و جعل العقوبة لها تساوي العقوبات المقررة للجريمة ذاتها .

ثالثا : أفعال إجرامية أخرى

جرمت المادة 394 مكرر 2 من قانون العقوبات الأفعال التالية : تصميم أو بحث أو تجميع أو الاتجار أو توفير أو استعمال أو نشر في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابق الذكر[2].

يقصد بفعل التوفير ومفاد ذلك تقديم المعطيات لمن يريدها وجعلها في متناول الجميع إلى جانب فعل التوفير نجد النشر المتمثل في إذاعة المعطيات محل الجريمة و يعتبر هذا السلوك خطيرا جدا كونه ينقل المعطيات إلى عدد كبير الأشخاص مما يزيد احتمال وقوع الجريمة ، كما جرمت المادة سالفة الذكر فعل الاتجار بمعطيات لها علاقة بالجرائم الماسة بنظام المعالجة الآلية للمعطيات، و يتم ذلك عن طريق تقديمها للغير.

[1] حمزة بن عفون، مرجع سابق، ص 184

[2] حمزة بن عفون، مرجع سابق، ص 184

و يشترط للعقاب على هذه الأفعال أن تقع على معطيات مخزنة داخل أقراص أو ما شابه، أو معالجة في نظام للمعالجة أو مرسلة عن طريق إحدى المنظومات المعلوماتية ، مع إمكانية أن ترتكب بهذه المعطيات جرائم بها هذه الجرائم فلا تقوم الجريمة[1].

قد يقوم الجاني باستعمال هذه المعطيات و يشمل للتجريم كل استعمال للمعطيات السالفة الذكر مهما كان الهدف منها ، و مثال ذلك قيام شركة ما باستعمال معلومات أو معطيات متحصل عليها بطريقة غير شرعية بإحدى الجرائم المذكورة آنفا تتعلق بشركة منافسة للإضرار به[2].

المطلب الثاني

خصائص الجريمة الإلكترونية

نتج عن ارتباط الجريمة المعلوماتية بجهاز الحاسوب و شبكة الأنترنت مجموعة من الخصائص التي تجعلها منفردة عن غيرها من الجرائم التقليدية سواء من حيث الجريمة ذاتها أو من حيث مرتكبي هذه الجريمة و هذا ما سيتبين من خلال الفرعين التاليين.

الفرع الأول

الخصائص المتعلقة بالجريمة الإلكترونية

بالرجوع للطبيعة المميزة للجريمة الإلكترونية باعتبارها تمس المعلومات مما جعلها تتميز عن الجرائم التقليدية بمجموعة من الخصائص و المميزات و هذا ما يساعد على التعرف على خصائص الجريمة الإلكترونية للوصول إلى الحلول لمكافحة حيث يمكن ابراز أهم هذه السمات فيما يلي :

[1] الهادي حضراوي، تجربة الجزائر في مكافحة الجريمة الالكترونية، المؤتمر الدولي لمكافحة الجرائم المعلوماتية ICACC ،كلية علوم الحاسب والمعلومات جامعة الإمام محمد بن سعود الإسلامية، السعودية، 2015، ص 161

[2] الهادي حضراوي ،المرجع السابق ، ص 162.

أولا – الجريمة المعلوماتية متعددة الحدود

هي جريمة عابرة للحدود ، فالمجرم المعلوماتي لا يعترف بالحدود الجغرافية و لا يعيرها اهتمام إذ هو مجتمع منفتح عبر شبكات تخترق المكان و الزمان دون خضوعها لحرس الحدود، فبظهور شبكات الأنترنت لم يعد هنالك حدود مرئية أو ملموسة ، ما جعل نقل المعلومات عبر الدول المختلفة سهلة في حركة المعلومات عبر أنظمة و برامج تقنية حديثة مما سهل إرتكاب الجريمة الإلكترونية عن طريق الحاسوب موجود في دول معينة بينما يتحقق الفعل الإجرامي في دول أخرى ، فهذه الميزة التي تتسم بها الجريمة الإلكترونية خلقت العديد من المشاكل حول تحديد الدولة صاحب الاختصاص القضائي و كذا تحديد القانون الواجب التطبيق ، كما نجد ظهور إشكاليات تتعلق بإجراء الملاحقة القضائية ، غير أن ذلك من النقاط التي تتسم بها الجرائم العابرة للحدود بصفة عامة[1] .

ثانيا – صعوبة اكتشاف الجريمة الإلكترونية

تتميز الجرائم الإلكترونية بصعوبة اكتشافها، حيث الحالات التي يتم اكتشاف هذا النوع من الجرائم قليلة و بمحض بالصدفة ، و ترجع أسباب صعوبة اكتشاف الجريمة المعلوماتية إلى ترك هذه لأي أثر خارجي بصورة مرئية، فلا يوجد جثث لقتلى أو للدماء ، كما أن المجرم المعلوماتي يمكن له ارتكاب هذه الجريمة في دول وقدرات مختلفة، ضف إلى صعوبة الحصول على الدليل المتوفر [2] ، و لعل صعوبة كشف الدليل المتزايد بصورة خاصة من ارتكبت هذه الجرائم في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة بين هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا أثار تدل عليهم[3].

---

[1] حمزة بن عفون، السلوك الإجرامي، المجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2011/2012، ص 17-18

[2] عبد الناصر محمود فرغلي محمد عبيد سيف السماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول للعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007، ص 10.

[3] موسى مسعود أرحومة، الإشكاليات الإجرائية التي تسيرها الجريمة المعلوماتية عبر الوظيفة، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظيمه أكاديمية الدراسات العليا، طرابلس، 26، -29/10/2009، ص 03.

ثالثا : صعوبة إثبات الجريمة المعلوماتية

يعتبر اكتشاف الجريمة الإلكترونية صعبا، إلا في حالة اكتشافها و الإبلاغ عنها، فإن إثباتها أمر يحيط بها الكثير من الصعاب ، باعتبار أن الجريمة الإلكترونية غير تقليد ية و وقوعها في إطار غير ملموس و غير مادي ، لتقوم أركانها في بيئة الحاسوب و الأنترنت مما يجعل الأمر يزداد صعوبة و تعقيداً لدى سلطات الأمن و أجهزة التحري و التحقيق و الملاحظة كون البيانات و المعلومات في هذه البيئة عبارة عن نبضات إلكترونية غير مرئية ، كما أن وسائل المعاينة و طرقها التقليديتي لا تفلح في أغلب الأحيان في إثبات هذه الجريمة نظراً لطبيعتها الخاصة التي تميزها عن الجرائم التقليدية ، فالمجرم الإلكترونية لا يخلف أثار مادية يركن الى موثوقيتها بسبب قدرت المجرمين العالية على التمويه ، كما أن هذه الجريمة يصعب فنياً الاحتفاظ بأثارها و إذا تركت أثاراً فإن هذه الجريمة الإلكترونية على التضليل و الخداع في ارتكابها و التعرف على مرتكبها، كما أن الجريمة الإلكترونية تعتمد على قمة الذكاء في ارتكابها ، إذ يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية و ما تخلفه من أثار غير مرئية .

رابعا: أسلوب ارتكاب الجريمة الإلكترونية

الجرائم المعلوماتية تتسم بالهدوء بطبيعتها ، لا تحتاج إلى العنف بل كل ما تحتاج إليه هي القدرة على التعامل مع أنظمة معالجة المعطيات بمستوى تقني سخر لارتكاب الأفعال الغير المشروعة[1]، كما تحتاج أيضا إلى وجود شبكة الأنترنت مع وجود مجرم يوظف خبراته و قدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كاختراق خصوصيات الغير أو التجسس ، فكل ذلك دون الحاجة إلى سفك الدماء على عكس الجرائم التقليدية التي تتطلب نوعاً من الجهد العضلي الذي قد يكون في صورة ممارسة العنف و الإيذاء، كما هو الحال في جريمة القتل أو في صورة الكسر في جريمة السرقة[2].

خامسا : الجريمة الإلكترونية تتم بتعاون عدة أشخاص

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة لنشر والتوزيع، عمان، 2008، ص 55.

[2] نهلا عبد القادر المؤمني ،المرجع نفسه، ص 56.

تتم عادة بتورط اكثر من شخص في تنفيذج الجريمة لتعدد الاختصاصات التقنية المطلوبة لإ خراج الجريمة إلى الواقع حيث يقوم مختص بالجانب الفني من المشروع الإجرامي و شخص أخر من المحيط لتغطية عملية التلاعب و تحويل المكاسب إليه و الاشتراك في الجريمة الإلكترونية له صورتين أولهما اشتراكا سلبياً المتمثل على من يعلم لتسهل لإتمام ارتكاب الجريمة أما الجانب الآخر فهو إيجابي الذي يتمثل في الكثير من الجرائم و يتمثل في المساعدة الفنية و المادية.

الفرع الثاني

الخصائص المتعلقة بالمجرم المعلوماتي

المجرم المعلوماتي كإنسان يتمتع بالمهارة و المعرفة و الذكاء بمعنى التعرف على كافة الظروف التي تحيط بالجريمة و تنفذها و إمكانية نجاحها و فشلها ، فالجناة يمهدون لارتكاب جرمتهم بالتعرف على كافة الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة و التي يمكن أن يتم ضبط أفعالهم و الكشف عنهم من خلالها، كما أن المجرم الإلكتروني يتمتع بقدرة فائقة في مجال تقنية الحاسوب و الأنترنت ، فتنفيذ مثل هذه الجرائم يتطلب قدراً من المهارة لدى الجناة الذين يكتسبونها عن طريق الخبرة في المجال المعلوماتي ، فالجريمة الإلكترونية تعد جريمة الأذكياء بالمقارنة مع الجرائم التقليدية التي تتسم بالميل إلى العنف ، فالمجرم المعلوماتي دائم البحث و السعي إلى طرق جديدة و حديثة التي لا يعلم بها سواء بهدف اختراق كل الحواجز الأمنية في البيئة المعلوماتية لتحقيق أهدافه و نيل مبتغاه[1].

أولا: المجرم المعلوماتي إنسان اجتماعي

يمكن القول أن المجرم المعلوماتي يتصف بالذكاء فهو إنسان يستطيع التوافق و التصالح مع مجتمعه ، الأمر الذي يساعده على تنفيذ عملية التكيف في مجتمعه مما يؤدي الى زيادة خطورته الإجرامية مع توافر الشخصية

[1] سمية مزعيش، جرائم المساس بالأنظمة المعلوماتية،مذكرة شهادة الماستر في الحقوق ،كلية الحقوق،جامعة مُحَّد خيضر،الجزائر2013-2014، ص18.

الإجرامية لديه ، فشعور المجرم المعلوماتي بأنه محل ثقة في مجتمعه و مجموعته و أنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا يتم الكشف عنها ، و حتى إذا ما تم اكتشافها فأنها تواجه صعوبة الإثبات.

ثانيا : المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي

بمعنى بسلطة الحقوق و المزايا التي يتمتع بها المجرم الإلكتروني و التي من خلالها يستطيع من القيام بالسلوك الإجرامي ، فالمجرم المعلوماتي يتمتع بالسلطة المباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة المتمثلة في الرقم السري الخاص للدخول إلى النظام يحتوي على المعلومات و التي تمتد للفاعل الجاني بمزاياً كفتح ملفات محو المعلومات أو تعديلها ، و قراءة الملفات و كتابتها و قد تتمثل هذه السلطة في الحق في استعمال الأنظمة المعلوماتية أو القيام ببعض المعلومات ، و كذا الدخول إلى الأماكن التي تحتوي على الأنظمة المعلوماتية، فإنه القيام بالتخطيط و التنظيم ففي علم الانترنت و الشبكات الإلكترونية ، فيقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة، كما هو الحال في الواقع المادي حيث ترتكب مجموعات متكونة من عدة أفراد يحدد لكل شخص دوره، و يتم ذلك وفقا لتنظيم و تخطيط مسبق على ارتكاب الجريمة، حيث تتكون هذه المجموعة الإجرامية من متخصص في المجال الفني للحاسب الآلي الذي يتولى الجانب الفني من المشروع الإجرامي إلى جانب شخص أخر من المحيط أو من خلال مؤسسة المجني عليه لتغطية التلاعب .

ثالثا : المجرم المعلوماتي يبرر ارتكابه للجريمة

يتولد لدى مرتكب فعل المجرم المعلوماتي إحساس و شعور بأن ما يقوم به لا يعتبر من عداد الجرائم[1]، حيث يميز مرتكبو هذه الجرائم بالإضرار بالأشخاص الأمر الذي يعدونه غاية من الأخلاقية و بين الأضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم[2].

[1] تايرب عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، جامعة أحمد درارية، أدرار، 2016/2017، ص 12.

[2] الزبدي وليد، القراصنة على الأنترنت والحاسوب، الطبعة الأولى، دار سامة للنشر، عمان،2003، ص 40.

رابعا: التطور في السلوك الإجرامي

يعني وجود المجرم الإلكتروني ضمن جماعة إجرامية تساعده في سرعة اكتساب المهارة الفنية التي تؤدي إلى المراد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة، و بناء على ما تقدم يمكن تقسيم المجرم الإلكتروني إلى عدة طوائف مختلفة متمثلة فيما يلي :

أ.المخترقون أو المتطفلون :نجد في هذا الإطار نوعين من المجرمين

1 –القراصنة الهواة العابثون هذا القسم من القراصنة يرون في اختراق الأنظمة المعلوماتية تحدياً لقدراتهم الذاتية، و هم يمثلون طائفة هواة الحاسوب فيقومون بأعمالهم هذه لمجرد إظهار قدراتهم على اقتحام المواقع الأمنية و يدعون هؤلاء أنه لا يوجد هنالك دوافع تخزينية وراء أعمالهم، و أصحاب هذه الفئة لديهم الكفاءة الخاصة ، المعرفة و المهارة المطلوبة في المجال الجواسيس و الشبكات إلكترونية.

2–كما نجد كذلك النوع الثاني المسمى بقراصنة الأخلاقية ينتقلون أنهم يعملون من أجل المصلحة العامة، فقاموا بتشكيل منظمات خاصة مثل منظمة القراصنة ضد المواقع الإباحية للأطفال التي قامت و استطاعت بالقيام بحملات تحسيسية و تأديبية لإبطال و تعطيل قدرة بعض المواقع الإلكترونية عن عرض مواد غير أخلاقية[1] .

ب – القراصنة المحترفون

تعرف هذه الطائفة بالمجرمين البالغين و أعمارهم تتراوح بين 25 و 45 سنة فمن أهم نواتهم أنهم يتمتعون بمكانة بالمجتمع وأنهم غالباً من المتخصصين في المجالات التقنية أي أنهم يتمتعون بمهارات فنية في مجال الأنظمة الإلكترونية[2] .

1 **بن مكي نجاة ،السياسة الجنائية لمكافحة جرائم المعلوماتية ،دار الخلدونية،الجزائر، 2017،ص41** .

2 عيمور راضية،الجريمة الإلكترونية و آليات مكافحتها في التشريع الجزائري،"المجلة الأكاديمية للبحوث القانونية"،المجلد السادس،العدد الأول،2022،ص87.

ج – طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية

بحكم المام هؤلاء بالنظام المعلوماتي كونه مجال عملهم الأساسي، و نظراً لمهاراتهم التقنية، فإنهم يرتكبون الجرائم المعلوماتية بهدف تحقيق أهدافهم الشخصية، و تكمن غايتهم القصوى هو تحقيق الكسب المادي فهنا نستنتج أنه بسبب العلاقة الوظيفية التي تربط بين المجني عليه و الموظف ولحكم الثقة بينهما، هذا ما يسهل عملية ارتكاب الجريمة المعلوماتية، هذا من جهة و من جهة أخرى نجد أن هنالك فئة من الحاقدين على عملهم و على الشركات التي يعملون فيها، فإن هنا تكون العمليات الإجرامية ليس بهدف تحقيق الكسب المادي و إنما بدافع الثأر والانتقام، و يطلق على هذه الفئة بمجرمي المعلوماتية الحاقدين أحياناً أو مجرد ترك بصماتهم التي تثبت وصولهم إلى ذلك المواقع، و يدعي هؤلاء أنه لا يوجد هنالك دوافع تخريبية وراء أعمالهم، و هذه الفئة لديهم الكفاءة الخاصة ، المعرفة و المهارة المطلوبة في المجال الحواسيب و الشبكات إلكترونية [1] .

د – مجرمون ذوي دوافع سياسية

هذه الفئة لها ميول و دوافع سياسية، لاختراق نظم الحاسب الآلي غير المصرح بالدخول إليها ،و التي تتضمن بيانات و معلومات سرية تخص الدفاع و الأمن ، و بعد المساس بها غاية في الخطورة .

هـ – صغار السن :

يمثلون فئة من صغار السن دون سن الأهلية ، تتسم هذه الفئة بأنهم متحمسين لحاسوب و دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب . فالإجرام الإلكتروني يتسم بالذكاء دون الحاجة إلى استخدام القوة والضعف و الذكاء لديهم هو مفتاح المجرم الإلكتروني لاختراق البرامج المحصنة و من المميزات التي يشترك فيها مجرمو

[1] رشاد خالد عمر ، مرجع سابق ،ص 53.

المعلوماتية أن أعمارهم تتراوح بين 18 و 45 سنة و الثقة الزائدة بالنفس ،كما يتسمون بالمهارة التقنية و الإلمام و القدرة بالنظام المعلوماتي ضف إلى الإلمام التام بمسرح الجريمة[1] .

[1] محمود أحمد عبابنة ،جرائم الحاسوب و ابعادها الدولية ،دار الثقافة للنشر و التوزيع 2005،الأردن،ص41.

الفصل الثاني

الخصوصية الإجرائية للجريمة الإلكترونية

بعد التطرق في الفصل الأول إلى ماهية الجريمة الإلكترونية من خلال تقديم تعريفها و أنواعها و الدوافع لارتكابها ، نتعرض في الفصل الثاني إلى الخصوصية الإجرائية لجريمة الإلكترونية و مدى تأثريها على المشرع الجزائري، وذلك عن طريق ما أقره المشرع من وسائل قانونية و قضائية لمكافحة هذه الجريمة بإصداره قوانين عامة و خاصة و انشاء هياكل و أجهزة للتصدي للجرائم الإلكترونية و توفير الحماية للأنظمة المعلوماتية و مستخدميها، و ذلك من خلال مختلف النصوص التشريعية خاصة المستحدثة منها و التي تناولت الجريمة المعلوماتية، و هذا سوف يتم توضحه عن طريق القواعد الموضوعية لقمع الجريمة الإلكترونية في التشريع الجزائي (المبحث الأول) و القواعد الإجرائية لقمع الجريمة الالكترونية في التشريع الجزائري (المبحث الثاني) .

المبحث الأول

القواعد الموضوعية لقمع الجريمة الإلكترونية في التشريع الجزائري

إن تتبع و الكشف عن الجرائم المعلوماتية التي تُعرف على أنها كل اعتداء على الأموال المادية و المعنوية يكون ناتجًا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ، و أمام قصور القواعد التقليدية في التصدي لهذه الجرائم التي باتت في تطور سريع مُسايرةً للتطور المعلوماتي ، فكان لابد من تدخل المشرع الجزائري بنصوص قانونية لقمع هذا النوع من الجرائم ، و إصدار قوانين خاصة تتلاءم مع طبيعة الجريمة و مستلزمات مكافحتها التي تستدعي التعاون بين الجهات القانونية و المختصين في المعلوماتية .

وعليه سريتم تناول في المطلب الأول الحماية الجزائية المعلوماتية من خلال نصوص قانون العقوبات و في المطلب الثاني الحماية الجزائية للمعلوماتية من خلال القوانين و التنظيمات الأخرى .

المطلب الأول

الحماية الجزائية للمعطيات في قانون العقوبات الجزائري

لم يتضمن التشريع الجزائري قبل سنة 2004 قوانين تطبق على الأنظمة المعلوماتية لكن أمام الإنتشار السريع للمعلوماتية و الجرائم المتعلقة بها ، حرص المشرع الجزائري على خلق الإطار القانوني المناسب الذي يقمع هذا الاعتداء و لسد الفراغ القانوني و الإقتداء بأغلب دول العالم لذا قام بإصدار قوانين معدلة و متممة لقانون العقوبات تارة و إصدار قوانين خاصة أهمها القانون رقم 09-04 المؤرخ المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها[1] في نصوص متعلقة بجرائم الأموال المقررة في قانون العقوبات .

الفرع الأول

الحماية الجزائية للمعطيات في قانون العقوبات الجزائري

إن التطور المعلوماتي و تطبيقاته المتعددة أدى إلى ظهور مشاكل مستحدثة و هذا ما أدى إلى البحث في مدى ملائمة الأوضاع القانونية في التصدي لهذه المشاكل، بإعتبارها تهتم بالجانب المادي المعلوماتي، من هنا يجب البحث عن مدى إمكانية القاضي الاستعانة بقانون العقوبات لتوفير الحماية لهذه القيمة الاقتصادية الجديدة ألا و هي أموال الإعلام في ظل النصوص التقليدية ، ولهذا الغرض تم التركيز على على نقطتين أساسيتين و هما :

أولا: مدى اعتبار المعلوماتية موضوع لجرائم الأموال

لمعرفة مدى إمكانية إخضاع الاعتداءات الواردة على أموال الإعلام الآلي للنصوص التقليدية الجرائم الأموال وجب أولا تحديد ما يلي:

1- مدى انطباق وصف المال على المعلوماتية

[1] القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والإتصال ومكافحته المؤرخ في05 أوت 2009،ج ر عدد 47، الصادرة في 16 أوت 2009،ص5.

يقصد بالمال المعلوماتي للحاسوب كل مكوناته و التي هي عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات و تخزينها و معالجتها و إعادة استرجاعها عند الحاجة إليها و هي تتكون من كيانين هما :

الكيان المادي (Hardware) الذي يشتمل على الأجهزة المادية المختلفة و من بينها أجهزة الإدخال و أجهزة الإخراج و وحدات التشغيل المركزية التي يتم من خلالها معالجة المعطيات و البيانات و تخزينها و إخراجها، أما فيما يخص الكيان المعنوي (Software) فيضم كل من نظام التشغيل و مختلف البرامج التي يحتاجها الحاسب للقيام بوظائف مختلفة بالإضافة إلى البيانات المطلوب معالجتها بالفعل [1]، فإذا كانت الأجهزة المادية للحواسيب لا تحتاج إلى نصوص خاصة لحمايتها جزائيا، فهذا الأمر يختلف بالنسبة للكيان المعنوي لتلك الحواسيب. الآن في جرائم الاعتداء على الأموال يجب عادة أن يكون موضوعها شيئا ماديا، و طبيعة الكيان المعنوي ليست مادية، و عليه يجب التساؤل عن مدى اعتبار الكيان المعنوي للحاسوب مالا[2].

يعتبر المال كل ما يصلح أن يكون محلا لحق ذو قيمة مالية، و يعتبر الشيء هو محل الحق، و تقسم هذه الأشياء إلى أشياء مادية و أخرى معنوية ، و بما أن الأموال بالنسبة للنصوص التقليدية لا ترد على الأشياء و لهذا فقد تم تعريف المال بصدد جرائم الأموال على أنه: كل شيء مادي يصلح لأن يكون محلا لحق من الحقوق المالية [3]، لكن مع التطور ازدادت الأشياء المعنوية عددا و تفوق بعضها من حيث قيمتها على الأشياء المادية هذا ما استدعى البحث لإيجاد معيار أخر لِيرد عليه الحق المالي غير طبيعة الشيء حتى يمكن إسباغ صفة الشيء المعنوي .

و من بين هذه الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسب الآلي ، تكون هذه البرامج مثبتة على دعامة أو حامل مثال ذلك الأقراص أو الشرائط الممغنطة من البلاستيك أو الأقراص الصلبة .

---

[1] مُحَمَّد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة عزيب، القاهرة، 1984، ص217.

[2] أمال قورة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص12.

[3] أحمد عبد الرزاق السنهوري، الوسيط في شرح القانون المدني حق الملكية، الجزء الثاني، دار أحياء التراث العربي، بيروت، 1952،ص09.

يعتبر البرنامج المستقل عن دعامته شيء معنوي و بالتالي لا يصدق عليه وصف المال، أما إذا سجل البرنامج أو نقش على دعامته فإن تلك الدعامة بما عليها من برامج تصلح لأن تكون محلا لجرائم الأموال على الرغم من أن الدعامة منفصلة عن البرامج تعتبر ضئيلة القيمة إذ ما قيست بقيمة البرامج و على الرغم من أن الاعتداء عليها ليس في غاية في ذاتها ، و إنما الباعث على ذلك هو البرنامج نفسه لا دعامته و مع ذلك لا تأثير لهذه البواعث في القانون الجنائي.[1]

2-مدى اعتبار المعلوماتية مالا في جرائم الأموال

أ- مدى اعتبار البرنامج كمحل لجريمة السرقة

نبدأ أولا في دراسة مدى اعتبار البرنامج مالا بصدد جريمة السرقة هذا ما ذهبت إليه المادة 350 من قانون العقوبات الجزائري المعدل و المتمم على أنه " كل من أختلس شيئا غير مملوك له يعد سارقا فالمادة 350 لم تشترط ضرورة أن يكون المال موضوع للجريمة ماديا مما يجعل وقوع جريمة السرقة على مال معنوي أمر لا يصطدم بمبدأ شرعية الجرائم و العقوبات ، و لكن يبقى اعتبار البرنامج كمحل للسرقة غير قطعي و من باب الإمكان لا غير .

ب- مدى اعتبار البرامج كمحل لجريمة النصب

حسب المادة 372 من قانون العقوبات فإن كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية و وعود أو مخالصات أو إبراء من التزامات أو الحصول على أي منها أو شرع و كان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي أو بإحداث الأمل في الفور بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية

[1] د. علي عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق الذكر، ص7.

من وقوع الشيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر بغرامة من 100.000 إلى 500.000دج .[1]

يستنتج من نص هذه المادة أنه ليس كل شيء مادي و منقول يصلح أن يكون محلا لجريمة النصب بل يجب أن يكون ضمن الأشياء التي حصرتها المادة 372 من ق ع المعدل و المتمم فالنص على المنقول في هذه المادة ورد دون تحديد طبيعته و دون أن يقيده المشرع بأن يكون ماديا هذا ما يسمح بإدخال برامج الحاسوب ضمن الأشياء التي تقع عليها جريمة النصب.[2]

ج- مدى اعتبار البرنامج كمحل لجريمة خيانة الأمانة

طبقا للمادة 376 من قانون العقوبات كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سلمت إليه على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر يشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين و ذلك إضرار بمالكيها أو واضعي اليد عليها أو حائزيها بعد مرتكبا لجريمة خيانة الأمانة.[3]

و عليه يستنتج من هذا النص أن الاختلاس يقع على أموال منقولة سلمت إلى الجاني وذلك بعقد من عقود الأمانة ، و عليه لا تقع جريمة خيانة الأمانة على غير المنقولات المادية، كما حددت المادة الأشياء التي تصلح محلا لهذه الجريمة و هي مذكورة على سبيل الحصر (الأوراق التجارية، النقود أو أوراقا مالية، مخالصات، محررات تتضمن أو تثبت التزاما أو إبراء) و عليه فإن إخضاع الاعتداءات الواردة على المال المعلوماتي إلى نصوص للأمانة يثير بعض

[1] أمر رقم 66-156 مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات،ج. ر. ج. ج. د. ش، عدد49، صادر في 10 جوان ،المعدل و المتمم.

[2] فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، المنعقد بأكاديمية الدراسات العليا بليبيا في أكتوبر 2009، ص 5.

[3] أمر رقم 66-156 مؤرخ في 08 جوان 1966،المرجع السابق.

المشاكل القانونية و ذلك لطبيعة الغير المادية للقيم المعلوماتية و عليه فإن تطبيق نصوص خيانة الأمانة في مجال المعلوماتية يكون في نطاق محدد و من باب الإمكان لا غير.[1]

د مدى اعتبار البرنامج كمحل الجريمة الاتلاف

فحسبما نصت عليه المادة 407 من قانون العقوبات الجزائري المعدل و المتمم كل من خرب أو أتلف عمدا أموال غير المنصوص عليها في المادة 396 بأية وسيلة كليا أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة 20.000 إلى 100.000 دج[2] .

كما تنص المادة 412 من قانون العقوبات الجزائري المعدل و المتمم كل من أتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة و ذلك بواسطة مواد من شأنها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 20.000 دج إلى 100.000 دج.[3] بالرجوع إلى نص المادة 412 نجدها قد حددت الأشياء الخاضعة للإتلاف وبالتالي فإنها تشمل المكونات المادية للحاسوب سواء بوصفها أجهزة أو بضائع.

ثانيا: مدى خضوع المعلوماتية للنشاط الإجرامي في جرائم الأموال

يختلف مدى خضوع برامج الحاسب الآلي أو المعلومات بصفة عامة للسلوك الإجرامي الذي يتحقق به الركن المادي في جرائم السرقة و النصب و خيانة الأمانة و الإتلاف .

1-مدى خضوع المعلوماتية للنشاط الإجرامي في جريمة السرقة

[1] فشار عطاء الله، مرجع نفسه، ص6.

[2] أمر رقم 66-156 مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات،ج. ر. ج. ج. د. ش، عدد49، صادر في 10 جوان ،المعدل و المتمم.

[3] أمر رقم 66-156 مؤرخ في 08 جوان 1966، المرجع نفسه.

الركن المادي للسرقة هو الاختلاس، أي أن الجاني و إن كان يدخل في ذمته ما استولى عليه من برامج إلا أنه في نفس الوقت تخرج هذه البرامج من ذمة صاحبها الشرعي إذ تظل رغم مباشرة الاختلاس تحت سيطر هذا الأخير دون إنقاص من محتواها، ما يمكن ملاحظته أن الإستلاء على البرامج بإعتبارها معلومات لا يتصور من الوهلة الأولى إلا إذا انتقلت هذه المعلومات ذهن أو من الحرة إلى ذاكرة.[1]

كما يلاحظ أيضا أن المعلومات التي تحتويها البرامج من طبيعة غير مادية أي أنها شيء معنوي فلا يمكن تصور فعل الاختلاس على شيء معنوي وهذه تعتبر عقبة ثالثة، فحسب هذه العقبات فليس من السهل تطبيق أحكام السرقة على برامج الحاسب الآلي وخاصة في الحالات الآتية:

أ- سرقة المعلومات عن طريق النسخ غير المشروع للبيانات المخزنة إلكترونيا

ويتم ذلك بإعادة إنتاج الوثيقة أو الدعامة التي تحتويها ، و لشرح حالات النسخ غير المشروع يمكننا الاعتماد الاجتهاد القضائي الفرنسي و ذلك عن طريق إعلانه أن المعلومات التي نسخت أو أعيد إنتاجها هي التي سرقت، حيث حافظ على مبدأ مادية الاختلاس و علاوة على ذلك فإن قرار الحكم باختلاس المعلومات عن طريق إعادة إنتاج المستند يتسمح بالعقاب على إعادة الإنتاج الذي لا يمكن أن يقع تحت طائلة الجريمة التقليدية .

فهناك اختلاف بين جريمة سرقة المعلومات عن طريق النسخ غير المشروع و بين الجريمة التقليدية لأن السرقة تحتوي على بيانات في ذاتها بينما الحماية التي يكفلها المشرع للمصنفات بتجريم تقليدها على طريقة التعبير عن أفكار المؤلف.[2]

[1] د. علي عبد الله القهوجي، مرجع سابق، ص95

[2] أمال قورة، مرجع سابق، ص 26

ب – سرقة وقت الآلة

يكيفها فقهاء القانون الجنائي على أنها سرقة ، وفي هذه الحالة ليس من السهل بسط أحكام جريمة السرقة على وقت الآلة لذلك فالمشرع الجزائري يأخذ بما يسمى سرقة الخدمة و عليه تتطلب تدخلا تشريعيا ، فإذا كانت هذه الجريمة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة إلا أنها تحقق أيضا و بصورة غير مباشرة حماية للمعلومات ذاتها .

ج – الالتقاط الذهني للبيانات

و ذلك بأن يقوم شخص بالتقاط معلومات ظهرت على شاشة الحاسوب و قام بحفظها في ذاكرته، فهذا الفعل يمكن أن يكون اختلاسا رغم أنه يرد على ذات المادة المستند و إنما اقتصر الشيء المختلس على مضمون المستند مع بقائه في حيازة صاحبه، لأن هذا المضمون شيء منقول مملوك للغير، إلا أن المشرع الجزائري لا يأخذ بسرقة الاستعمال و عليه ضرورة تدخل تشريعي يشمل حالتي الالتقاط الذهني و حالة سرقة المعطيات دون استنساخها و دون المساس بسلامتها و أصالتها.[1]

د – تكييف الالتقاط الهوائي للبيانات المعالجة أو المنقولة إلكترونيا

إن الطاقة و القوة الطبيعية أو الصناعية تعد من الأموال المنقولة و تصلح لأن تكون محلا للسرقة إلا أنه لا يمكننا أن نطبق أحكام سرقة الطاقة على الإشعاعات و الموجات و النبضات المنبعثة من الحواسيب الآلية أثناء تشغيلها رغم أنها كهربائية قابلة للقياس و التقدير الكمي .

[1] أمال قورة، المرجع السابق، ص 23.

إن عدم وقوع السرقة في الحالات السابقة لأن طبيعة البرامج لا تحقق الأخذ و الاختلاس بمعناه الدقيق في جريمة السرقة و الذي يعني الاستلاء على الحيازة الكاملة لشيء بدون رضا صاحبها أو حائزه السابق لأنه إذا تصورنا وقوع الاختلاس من خلال النسخ و التصوير على المعلومات الأصلية ذاتها تظل في نفس الوقت كما كانت من قبل تحت سيطرة صاحبها الأصلي و لا تخرج من حيازته، لما كان قانون العقوبات الجزائري لا يجرم سرقة الاستعمال بصفة عامة ، فإن الحل الوحيد لا يكون إلا بتدخل صريح من هذا الأخير، لتفادي الجدال موضوع سرقة المعلومات وقت الآلة أو سرقة استعمال الأصل و تحقق الحماية للبرامج المعلوماتية .

2-مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي في جرائم النصب و خيانة الأمانة

أ. بتطبيق النشاط الإجرامي لجريمة النصب في المجال المعلوماتي

إن لجوء الجاني إلى إحدى الطرق الاحتيالية و حمل المجني عليه على تسليم هدعامة مادية مثبت عليها أحد البرامج ثم استلاء الجاني عليها فإن النشاط الإجرامي في هذه الحالة يتحقق، لكن الأمر الذي يطرح إشكالا هو هل يمكن تصور أن يتحقق النشاط الإجرامي في جريمة النصب من خلال الطرق الاحتيالية التي يقوم بها الجاني و التي يترتب عليها إيقاع المجني عليه في غلط الذي يتم من خلاله نقل محتويات برامجه شفويا و التي يلتقطها الجاني و يحفظها في ذاكرته.

لا وجود لنشاط مادي يتحقق به التسليم و الإستلام في جريمة النصب، و لو فرضنا إمكانية وقوع التسليم فإنه لن ينتج عن ذلك حرمان المجني عليه من المعلومات التي نقلها بالقول بل تظل تحت سيطرة من نقلها، إلا أنه لا

يتفق هذا مع طبيعة النشاط الإجرامي في جريمة النصب و هذا يعني عدم صلاحية البرامج للخضوع للنشاط الإجرامي في جريمة النصب.[1]

ب. بتطبيق النشاط الإجرامي لجريمة خيانة الأمانة في المجال المعلوماتي

لا جدال في وقوع جريمة خيانة الأمانة بالنسبة للدعامات المثبت عليها البرامج و المعلومات و ذلك في الحالة التي يقوم فيها الأمين بنسخ البرامج لحسابه متجاوز ا الاتفاق الذي يربطه مع صاحب البرنامج إذ يحقق هذا النسخ فعل الاستعمال و الذي يقصد به استخدام الأمين المال استخداما يستنزف قيمته كلها أو بعضها رغم بقاء المادة على حالها ، و هذا ما يصعب قيام جريمة خيانة الأمانة في حالة البرامج و المعلومات المستقلة عن الدعامة و ذلك لعدم قيام النشاط الإجرامي و هو التسليم بناء على عقد الأمانة لعدم وجود النشاط المادي مجسم لتحقق فعل الإستلام ، مما يحول دون صلاحية البرامج و المعلومات للخضوع للنشاط الإجرامي في جريمة خيانة الأمانة.[2]

ج. بتطبيق النشاط الإجرامي لجريمة الإتلاف في المجال المعلوماتي

إن المشرع الجزائري لا يقيد النشاط الإجرامي في جريمة الإتلاف بوسيلة معينة إذ هي من الجرائم ذات القالب الحر و لهذا لا يوجد ما يحول دون وقوع جريمة الإتلاف على برامج الحاسب الآلي خاصة و أن المشرع الجزائري لم يحدد طريقة بعينها لوقوع الجريمة و لم يحدد نتيجة وحيدة محددة لقيامها، فإنه من المتصور أن يتجه الجاني بنشاطه الإجرامي إلى البرامج و الدعامة المسجل عليها معا، أو إلى البرامج فقط دون الدعامة و قد تقع الجريمة عن طريق الاتصال المباشر بالجهاز كما قد تقع من خلال الاتصال عن بعد .

[1] فشار عطاء الله،مرجع سابق، ص 10

[2] أمال قورة، المرجع نفسه، ص 45-60.

و عليه فإن جريمة الإتلاف المنصوص عليها في قانون العقوبات تحقق حماية جنائية كاملة لبرامج الحاسب الآلي على خلاف جرائم الأموال التي توفر حماية نسبية.[1]

الفرع الثاني

الحماية الجزائية للمعطيات من خلال النصوص المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات ت ع ج

عزز المشرع الجزائري الترسانة القانونية في مجال الإجرام المعلوماتي و ذلك عن طريق إستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية ، و ذلك بموجب القانون رقم 04-15 المتضمن تعديل قانون العقوبات، لكن المشرع الجزائري ركز على الاعتداءات الماسة بالأنظمة المعلوماتية ، و أغفل الاعتداءات التي تخص منتجات الإعلام الآلي و المتمثلة في التزوير المعلوماتي .

نص المشرع الجزائري من خلال القانون رقم 04-15 على العقوبات المقرر للجرائم التي تمس الأنظمة المعلوماتية و هي كما يلي :

أولا: العقوبات المقررة لشخص الطبيعي

أ- العقوبات الأصلية

نص المشرع الجزائري في القانون رقم 04-15 المعدل و المتمم لقانون العقوبات على عقوبات أصلية لجريمتي الدخول أو البقاء الغير المشروعان للنظام المعلوماتي و كذا جريمة المساس بمنظومة معلوماتية وفقا لما يلي :

عقوبة الدخول أو البقاء غير المشروعان للنظام

الدخول الغير المشروع من طرف المجرم المعلوماتي للنظام كله أو جزء منه أو متى كان مسموح له الدخول إلى جزء معين من ذلك النظام و تجاوزه ، و متى كان دخوله للنظام المعلوماتي مخالف لارادة صاحب ذلك النظام، تكون العقوبة المقررة في هذا الشأن الحبس من ستة أشهر إلى سنتين و غرامة مالية تقدر بقيمة 60.000 دج إلى

[1] فشار عطاء الله، مرجع سابق، ص 10

200.000 دج و ذلك طبقا للمادة 394 مكرر من تعديل قانون العقوبات رقم 06/24. إن العقوبة تضاعف في حالة إذا ترتب عن هذه الأفعال تغيير أو حذف معطيات المنظومة المعلوماتية مما يشكل ظرفا مشددا، و تصبح العقوبة بالحبس من سنة إلى أربع سنوات و غرامة من 120.000 دج إلى 400.000 دج،و ذلك وفقا للمادة 394 مكرر من قانون العقوبات السابق الذكر .

عقوبة المساس بمنظومة معلوماتية

نص المشرع الجزائري في المادة 394 مكرر01 من قانون العقوبات المعدل و المتمم على عقوبة الاعتداء العمدي على المعطيات الموجودة داخل النظام المعلوماتي، و ذلك بالحبس من سنة إلى 03 سنوات و غرامة من 500.000 دج إلى 2.000.000 دج، و ذلك في حالة ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، و في حالة حيازة و إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية تكون العقوبة بالحبس من سنة إلى 05 سنوات و غرامة من 1.000.000 دج إلى 5.000.000 دج [1].

ثانيا : العقوبات المقررة للشخص المعنوي

لقد نص المشرع الجزائري في المادة 51 مكرر من القانون العقوبات بعد تعديله ا بموجب القانون 24-06 على موضوع الشخص المعنوي فيما يخص ارتكابه لهذه الجرائم و ذلك و فقا لشروط منها :

- يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه القانونيين أو الحائزين على تفويض سلطات ، و لتمنع هذه المسؤلية الجزائية من مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعل.
- تستثنى الدولة و الجماعات المحلية و الأشخاص المعنوية الخاضعة للقانون العام.

[1] خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر،2010، ص99.

كما نصت المادة 394 مكرر 04 من القانون 24-06 المعدل و المتمم لقانون العقوبات على أن العقوبة المطبقة على الشخص المعنوي في حالة ارتكابه لإحدى جرائم الإعتداء على نظام المعالجة الآلية للمعطيات هي غرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.[1]

ثالثا : عقوبة الاشتراك و الشروع في الجريمة

أ- عقوبة الاشتراك

نصت المادة 394 مكرر5 من القانون العقوبات على أنه: "كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم ، و كان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها .

ب- عقوبة الشروع

نصت المادة 394 مكرر 07 من القانون العقوبات على أنه " **يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقرر للجنحة ذاتها**[2] ."

رابعا : العقوبات التكميلية

لقد نصت المادة 394 مكرر 06 من نفس القانون على مجموعة من العقوبات التكميلية يعتمد عليها قاضي الحكم في حكمه إلى جانب العقوبات الأصلية دون المساس بحقوق الغير حسن النية و هي كالتالي :

المصادرة: تشتمل على الأجهزة و البرامج و الوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية[1] مع مراعاة حقوق الغير حسن النية.

[1] خثير مسعود ،**المرجع نفسه**، ص100.

[2] القانون رقم 04-15 ،مرجع سابق.

إغلاق المواقع: تلك التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية [2]، أي إغلاق مواقع الأنترنيت أو الموقع الإلكتروني بصفة عامة التي كانت وسيلة لإرتكاب هذه الجرائم أو ساهمت في ارتكابها .

إغلاق المحل أو مكان الاستغلال: في حالة إرتكاب الجريمة بعلم مالك المحل أو مكان الإستغلال كإغلاق مقهى إلكتروني .

المطلب الثاني

الحماية الجزائية للمعلوماتية ضد الجريمة الإلكترونية من خلال القوانين و التنظيمات الأخرى

نص المشرع الجزائري على بعض القوانين و التنظيمات من شأنها إضافة نوع من الحماية الجزائية للمعلوماتية، و ذلك من خلال استحداث قواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية و هو ما سنفصله من خلال الفرع الأتي :

الفرع الأول

القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية

بإستقراء القانون 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد و التصالات الالكترونية لاحظنا أن هناك تسارع في مواكبة التطور الذي شهدته التشريعات العالمية مسايرة للتطور التكنولوجي، لذلك بات من السهولة إجراء التحويلات المالية عن طريق الدفع الإلكتروني وفق المادة 46 منه، كما نصت المادة 60 منه على استعمال حولات دفع عادية أو إلكترونية أو برقية ، كما نصت المادة 105 من نفس القانون على احترام المراسلات [3] ، و قد تناول المشرع في الباب الاول الفصل الثاني القسم الأول و الثاني من القانون رقم 18-04 المؤرخ في 10 ماي

---

[1] صالح شنين، **الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني** ، عدد 01، الجزائر، 2010، ص74.

[2] سوير سفيان، **مرجع سابق**، ص 99.

[3] فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مرجع سابق، ص131.

2018[1]، تعاريف تتعلق بالاتصالات الالكترونية منها الأمواج اللاسلكية و اللاسلكية الشبكة الخاصة، و الشبكة العامة و خدمة الانترنت و الاتصالات الالكترونية و الخدمات البريدية و أطرافها عن مرسل و مرسل إليه و غيرها من المصطلحات التي تم استعمالها في هذا القانون، كما تضمن الجرائم المعلوماتية و العقوبات و خصصت المواد من 164 إلى المادة 188 للنص على العقوبات المقررة للجرائم المتعلقة بها و من السلوكات المجرمة بنص هذا القانون نذكر ما يلي :

- يعاقب بالحبس من سنة إلى خمس سنوات و بغرامة من 500.000 دج إلى 1.000.000 دج كل شخص ينتهك سرية المراسلات البريدية أو الإتصالات الإلكترونية أو يفشي مضمونها ...أو يخبر بوجدها وفقا للمادة 164 من نفس القانون.
- فتح أو تحويل أو تخريب البريد أو التصالات الإلكترونية أو المساعدة على ارتكاب هذه الأفعال من قبل كل متعامل للبريد أو متعامل للإتصالات الإلكترونية، يعاقب من قام بهذه الأفعال بالحبس من سنة إلى ثلاث سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج أو بإحدى هاتين العقوبتين وفقا للمادة 165 من نفس القانون.
- كل شخص يقوم بقطع عمدا و في غياب الضروف القاهرة كابل بحريا أو يسبب له تلفا قد يوقف الاتصالات الالكترونية كليا أو جزئيا، يعاقب بالحبس من 05 سنوات إلى 10 سنوات و بغرامة مالية 5.000.000 دج إلى 10.000.000 دج حسب المادة 179 من القانون السابق الذكر .

[1]قانون رقم 2000-03 المؤرخ في أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالواصلات السلكية واللاسلكية، العدد 48، الصادر في 06 أوت 2000.

-يعاقب بالحبس من سنة إلى ثلاث سنوات و بغرامة من 1500.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين، كل من ينشئ أو يستغل شبكة إتصالات إلكترونية مفتوحة للجمهور دون الرخص القانونية و المنصوص عليها في المادة 123.[1]

يعتبر الشخص المعنوي مسؤولا جزائيا عن الجرائم المذكورة في هذا القانون طبقا للقواعد المنصوص عليها في قانون العقوبات و في حالة العود تضاعف العقوبة .

الفرع الثاني :

تقرير حماية جزائية لمعطيات الحاسب في قانون الملكية الفنية و الأدبية

الهدف من وضع قوانين الملكية الفكرية و حماية حق الإنسان في التفكير و الإبداع و الإبتكار الذي يعد بمثابة العامل الأساسي لتقدم المجتمعات و تطورها،و لما كانت المكونات المعنوية لمنظومة المعالجة الآلية للمعطيات (برامج ، قواعد البيانات ، نظام التشغيل إلخ...)ثمرة جهد فكري للإنسان،كان لزوما على المشرع اشتمال هذه المكونات المعنوية بالحماية المقررة في قانون الملكية الفنية و الأدبية و ذلك بتجريم الأفعال التي تشكل اعتداءا عليها و إقرار ما يقابلها من عقوبات جزائية.[2]

إتجه المشرع الجزائري على غرار معظم التشريعات الغربية إلى إقرار الحماية القانونية لبرامج منظومة المعالجة الآلية للمعطيات من خلال إخضاعها لقوانين حماية حقوق المؤلف،بحيث أعترف صراحة في الأمر رقم 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف و الحقوق المجاورة بوصف المصنف المحمي لمصنفات الإعلام الآلي.

ترتب عن جعل المشرع الجزائري برامج و بيانات منظومة المعالجة الآلية للمعطيات مصنفا فكريا دمجها ضمن المصنفات الأصلية و اعتبار أي اعتداء على الحق المالي و الأدبي لمؤلف البرنامج و البيانات يشكل فعلا من أفعال

[1] فليح نور الدين، مرجع سبق ذكره، ص 106.

[2] عيمور راضية،المرجع السابق،ص103.

التقليد المنصوص عليها في المادة 151 من الأمر 03-05 المذكور سالفا يترتب عليها العقوبات الجزائية المقررة في المواد 153،156،157،158 من نفس الأمر .

أولا:تقسيم جنح تقليد معطيات الحاسب الآلي

و تنقسم جنح التقليد التي تمس بمصنف البرامج و بيانات الحاسب الآلي الى ثلاث أنواع هي :

1 -**الجنح المرتبطة بالحق المعنوي للمؤلف** : و هي محددة في المادة 151 فقرة 1 من الأمر 03-05 السالف الذكر.

2 -**الجنح المرتبطة بالحق الأدبي للمؤلف** :تتمثل في :

أ - الإستنساخ الغير الشرعي للمصنف : حسب المادة 151 فقرة 1 من الأمر 03-05 السالف الذكر

ب -الإبلاغ الغير الشرعي للمصنف : حسب المادة 152 من الأمر 03-05 السالف الذكر

3 -**الجنح المرتبطة بالمصنف المقلد.**

ثانيا:العقوبات المقررة لجنح تقليد معطيات الحاسب الآلي

حدد المشرع الجزائري العقوبات التي توقع على جنح تقليد المصنفات المعلوماتية (قواعد البيانات، التطبيقات ، أنظمة التشغيل الخ...) في صنفين هما :

1 - **العقوبات الأصلية** : حددت هذه العقوبات في نص المادة المادة 153 من الأمر 03-05 على النحو التالي :

أ - عقوبة الحبس : للقاضي أن ينطق بعقوبة أصلية تتمثل في الحبس من 06 أشهر إلى 03 سنوات ضد كل من ارتكب جنحة تقليد مصنف بما فيه المصنفات المعلوماتية.

ب – عقوبة الغرامة :علاوة على عقوبة الحبس يمكن للقاضي أن يكم بغرامية مالية تتراوح بين 500.000دج و 1.000.000دج .[1]

2 – **العقوبات التكميلية**:لقد أعطى المشرع الجزائري سلطة تقديرية للقاضي للنطق بعقوبة واحدة أو أكثر من العقوبات التكميلية المقررة لجنح تقليد المصنفات.

المبحث الثاني

القواعد الإجرائية لمكافحة الجرائم الإلكترونية

إن المشرع الجزائري قام بإصدار نصوص قانونية لقمع الجريمة المعلوماتية و ذلك بسبب تزايد الإعتداءات على أنظمة المعلوماتية في الجزائر، كذا استعمال المنظومة المعلوماتية للأغراض إجرامية .

المطلب الأول

القواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية

إن خصوصية الجرائم الإلكترونية لابد أن تنعكس على قانون الإجراءات الجزائية الأمر الذي يفرض على المشرع الجزائري إنشاء قواعد إجرائية حديثة إلى جانب القواعد الموضوعية و نظرا لإتسام هذه الجرائم الإلكترونية بصعوبة اكتشافها و إثباتها و تحتاج إلى خبرة فنية عالية للتعامل معها ، فإن ذلك أثار العديد من المشكلات الإجرائية و التي جعلت القواعد الإجرائية التقليدية قاصرة في مواجهة تلك المشاكل، لهذا قام المشرع الجزائري بتعديل بعض القواعد الإجرائية لجعلها قادرة على مواجهة تلك المشاكل الإجرائية خاصة المتعلقة بالاختصاص المحلي و إجراءات البحث و التحري.[2]

[1]الأمر رقم 03-05 مؤرخ في 19 جمادى الأول عام 1424 الموافق لـ 19 يوليو 2003،المتعلق بحماية المؤلف من الحقوق المجاورة، ج ر،عدد 44.

[2]أحمد شوقي الشلفاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء 2 طبعة 5، ديوان المطبوعات الجامعية الجزائر، ص 159.

الفرع الأول

قواعد الاختصاص المحلي

إن الاختصاص المحلي هو المجال الإقليمي الذي يمارس فيه ض باط الشرطة القضائية مهامه م في البحث و التحري عن الجريمة أي في حدود الدائرة التي يباشر ون وظيفته م و ذلك يتحد بمكان وقوع الجريمة أو محل القبض على المتهم أو مكان إقامته [1]، حيث عالج المشرع الجزائري الاختصاص المحلي للجهات القضائية و ذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه ، و قام بالاعتماد على عناصر تربط إختصاص الجهات القضائية بالنظر في الخصومة الجزائية و تتمثل في المجال الجغرافي ، و نظرا لإعتبار أن الجريمة الإلكترونية جريمة عابرة للحدود فغالبا ما يكون الجاني في بلد و المجني عليه في بلد آخر ،كما قد يحصل الضرر في بلد ثالث في الوقت نفسه لهذا السبب نجد المشرع الجزائري قد أجرى بعض التعديلات المتعلقة بالاختصاص المحلي في الجريمة الإلكترونية بموجب القانون 22/06 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم للأمر رقم 155/66 المتضمن قانون الإجراءات الجزائية، لهذا سنتطرق في هذا الفرع إلى دراسة هذه القواعد .

أولاً: الاختصاص المحلي للنيابة العامة

وفقاً لنص المادة 37 من قانون الإجراءات الجزائية الجزائري فإنه يتحدد الاختصاص المحلي للنيابة بمكان وقوع الجريمة و محل القبض على أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو القبض على هؤلاء الأشخاص حتى و لو تم القبض عليهم لسبب أخر، و بالتالي فإن اختصاص وكيل الجمهورية لا يتعدى مكان وقوع الجريمة أو مكان القبض على الأشخاص المشتبه في مساهمتهم في الجريمة أو محل إقامة أحد هؤلاء الأشخاص ، لما كانت الجريمة المعلوماتية جريمة قد ترتكب في مكان معين و تكون أثارها في مكان أخر ، فإن المشرع الجزائري أجاز بتمديد الاختصاص المحلي

[1] فليح نور الدين، مرجع سابق،ص ص 107-108

لوكيل الجمهورية بموجب المادة 37 فقرة 2 من قانون الإجراءات الجزائية إلى دائرة الاختصاص المحاكم الأخرى مع ترك كيفية تطبيق ذلك عن طريق التنظيم الذي سيحدد المحاكم التي يمتد إليها الاختصاص[1] .

كما أن المشرع قضى في أحكام نص المادة 40 مكرر فقرة 2 من قانون الإجراءات الجزائية على أنه يتعين على ضابط الشرطة القضائية إخبار وكيل الجمهورية لدى المحكمة الكائن في مكان الجريمة و يبلغونه بأصل ويستحسن بإجراءات البحث و يرسل هذا الأخير فوراً بنسخة ثانية إلى النائب العام لدى محكمة المجلس القضائي التابعة له المحكمة المختصة ، و الذي يطالب وفق المادة 40 مكرر1 من قانون الإجراءات الجزائية التي تتعلق بإجراءات تحريك الدعوى العمومية أو مباشرتها أو رفعها بمجرد أن يتبين للنائب العام أن الجريمة ضمن المحكمة المختصة التابعة لها و هذا ما نصت عليه المادة 40 في الفقرة 03 من نفس القانون.[2]

ثانياً: الاختصاص المحلي لقاضي التحقيق

الاختصاص المحلي لقاضي التحقيق يقصد به التحقيق في المجال الذي يباشر فيه قاضي التحقيق مهامه و الذي يتحدد طبقاً للمادة 40 من قانون الإجراءات الجزائية بمكان وقوع الجريمة أو محل إقامة أحد هؤلاء الأشخاص المشتبه في مساهمتهم على اقترافها أو محل القبض على أحد من هؤلاء الأشخاص حتى و لو كان هذا القبض حصل لسبب أخر ، غير أن المشرع الجزائري قام بإلغاء في التعديل الجديد الفقرة 2 و 3 من المادة 40 و أصبحت تنص الفقرة 2 على جواز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، و نستخلص من هذا أن المشرع أجاز إمكانية تمديد الاختصاص المحلي

1

[2] أمر رقم 66-155 مؤرخ في 18 جوان 1966، يتضمن قانون الإجراءات الجزائية، ج. ر. ج. ج. ر. ش، عدد 48، صادر في 11 جوان 1966، معدل ومتمم بموجب أمر رقم 21-11 مؤرخ في 25 غشت 2021،ج. ر. ج. ج. د. ش،عدد 65، صادر في 26 أوت 2015.

القاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم أخرى مع ترك كيفية تطبيق تلك الإجراءات لتنظيم الذي سيصدر بعد ذلك .

ثالثا : الاختصاص المحلي لمحاكم الجنح

يتحدد الاختصاص المحلي للمحاكم الجنح طبقاً للمادة 329 من ق، إ، ج، ج، بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المتهمين أو شركائهم أو بمكان الذي في دائرته القبض على أحد هؤلاء الأشخاص حتى و لو تم القبض لسبب أخر و بعد التعديل الصادر بموجب القانون 14/04 ،كما أضاف المشرع الجزائري فقرة أخرى أجاز فيها تمديد الاختصاص المحلي للمحاكم إلى اختصاص محاكم أخرى عن طريق التنظيم في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات . و بالتالي فإن المشرع الجزائري أجاز في حالة ارتكاب جريمة من جرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد الاختصاص لوكيل الجمهورية و اختصاص قاضي التحقيق و اختصاص محاكم الجنح و لكنه ترك ذلك للتنظيم الذي سيصدر لاحقاً و الذي يحدد تلك المحاكم الذي يمتد إليها الاختصاص و تطبيق القواعد المتعلقة بالدعوى العمومية و التحقيق والمحاكم أمام الجهات القضائية في المادة 40 مكرر[1]، و التي تم توسيع اختصاصها المحلي طبقاً للمواد 37 .40، 329 من ق. إ، ج، ج المعدل و المتمم.

تعد مشكلة الاختصاص القضائي في الجريمة المعلوماتية من المشكلات التي تصعب الحصول على الدليل، ذلك أن هذه الجريمة قد ترتكب في مكان معين و تنتج أثارها في مكان أخر داخل الدولة أو خارجها، و إذا كانت مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس معيار القبض على المتهم أو محل إقام ته أو مكان وقوع الجريمة ، في أي مكان من هذه الأماكن ينعقد الاختصاص الجنائي لسلطات التحقيق و المحاكمة في الجريمة

[1] فليح نور الدين، مرجع سابق، ص 110.

المعلوماتية، لكن على المستوى الدولي فإن الأمر بحاجة إلى اتفاقيات دولية، فقد شرعت بعض الدول في عقد اتفاقيات قضائية لتسهيل مهمة التحقيق في جرائم المعلوماتية .[1]

الفرع الثاني

إجراءات البحث والتحري

يقصد بإجراءات التحقيق الإبتدائي مجموعة الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشأن واقعة جنائية معروضة عليها ويكون ذلك بالبحث عن الأدلة الثابتة لذلك، و هو مرحلة لاحقة لإجراءات جمع الإستدلالات و تسبق مرحلة المحاكمة و التي تكون من اختصاص جهة الحكم، فالتحقيق يهدف إلى تمهيد الطريق أمام القضاة باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة.[2]

أما أهداف التحقيق الابتدائي فهي تكشف عن الحقيقة للوصول إلى هذا الغرض يلجأ المحقق إلى مجموعة إجراءات بعضها بهدف للحصول على الدليل و يطلق عليها تسمية إجراءات جمع الدليل كالتفتيش و الضبط و المعاينة و الشهادة و الخبرة ، و بعضها الآخر يمهد للدليل و يؤدي إليه و تعرف بالإجراءات الاحتياطية ضد المتهم كالقبض و الحبس المؤقت .

أما بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع في الجريمة التقليدية كالتفتيش و المعاينة و استجواب المتهم و الضبط و الشهادة و الخبرة ، حيث أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من ق،إ،ج،ج المعدل و المتمم،كما نص على التفتيش في المادة 45 في الفقرة الأخيرة من نفس القانون ، حيث أعتبر التفتيش الذي يكون على المنظومة المعلوماتية يختلف عن التفتيش

[1] محمد الأمين البشري، التحقيق في جرائم الحاسوب الآلي والأنترنت، المجلة العربية للدراسات الأمنية والتدريب،العدد 30، نوفمبر2000، ص373.

[2] عبد الله أوهابية، محاضرات في قانون الإجراءات الجزائية، ألقيت على طلبة سنة ثانية حقوق، جامعة، الجزائر، 2009-2010،ص53.

المتعارف عليه في القواعد الإجرائية من حيث الشروط الشكلية و الموضوعية، فالتفتيش و إذ كان إجراء من إجراءات التحقيق قد أحاطه المشرع بقواعد صارمة و لهذا لا تطبق الأحكام الواردة في المادة 45 فقرة الأخيرة من نفس القانون إذ تعلق الأمر بالجرائم الإلكترونية ، ضف إلى ذلك نص على التوقيف للنظر في جريمة المساس بأنظمة المعالجة في المادة 51 بالإضافة إلى " **اعتراض المراسلات و تسجيل الأصوات و التقاط الصور** "، إذ نجد أن المشرع الجزائري مدركا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية و تحفظية، و التي من شأنها أن من الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها و هو ما استدركه المشرع يتضمن القانون رقم 22/06 المعدل لقانون الإجراءات الجزائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية بتسجيلها و التسرب[1]

يقصد باعتراض المراسلات أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج و التوزيع ، التخزين الاستقبال التي تتم عن طريق قنوات أو وسائل الاتصال السلكية و اللاسلكية في إطار البحث والتحري عن الجريمة و جمع الأدلة عنها [2] ، فهنا قام المشرع الجزائري بالإشارة إلى ظروف و كيفية اللجوء لهذا الإجراء في المادة 65 مكرر05 من قانون الإجراءات الجزائية على النحو الآتي " **إذا اقتضت ضروريات التحدي في الجريمة المتلبس بها أو التحقيق الابتدائي في... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكي وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط و تثبيت و تسجيل الكلام المتفوه به، بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص**

[1] فضيلة عاقلي، مرجع سابق، ص 364.

[2] بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر" ، المرجع السابق، ص364.

أو عدة أشخاص يتواجدون في مكان خاص ." نستخلص من هذه المادة أن المشرع الجزائري يسمح لسلطات التحقيق و الاستدلال إذ استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الإلكترونية اللجوء إلى إجراء اعتراض المراسلات السلكية و اللاسلكية و تسجيل المحادثات و الأصوات و الصور، و الاستعانة بكل الترتيبات التقنية اللازمة للوصول إلى الكشف عن ملابسات الجريمة و إثباتها دون أن يتقيدوا بقواعد التفتيش و الضوابط المألوفة مع وضع المشرع الجزائري مجموعة من الضمانات القانونية التي تحد من تعسف سلطات البحث و التحري و تصون الحقوق و الحريات العامة و الحياة الخاصة للأفراد و دون الإخلال بضمانات المحاكمة العادلة.[1]

المطلب الثاني

الحماية الجزائية للمعلوماتية في ظل الأمر رقم 11/21 المتضمن تعديل قانون الإجراءات الجزائية

إن الإجرام الإلكتروني من أخطر الظواهر الإجرامية المستحدثة في المجتمع الجزائري، نظراً للأضرار التي تتسبب فيها ، مما أدى بالمشرع الجزائري إلى إصدار مجموعة من القواعد القانونية بغية ردع مثل هذه السلوكات الغير شرعية لما تشكل من خطورة و مساس بالنظام العام و أمن الدولة .

الفرع الأول

أسباب صدور القانون 11/21 ومضمونه

أولاً: أسباب صدور الأمر 11/21

نظراً لخطورة الجرائم الإلكترونية باعتبارها من الجرائم الحديثة ذات طبيعة خاصة لكونها ترتبط بوجود العالم الافتراضي و مع صعوبة أثباتها و إكتشافها مما دفع بالمشرع الجزائري إلى التدخل بإصدار قواعد قانونية تحضر الفعل الإجرامي المعلوماتي التي يترتب عليها أثاراً خطيرة تهدد الفرد و المجتمع ، هذا ما يتطلب إلى وجود نصوص تجرمها

[1] براهيمي جمال، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية مولود معمري، تيزى وزو، العدد 2، الصادر بتاريخ 15/11/2016، ص138.

و تعاقب مرتكبها ، فكان إلزاماً سد الفراغ القانوني الذي عرفه المجال الإلكتروني بصدور قانون 11/21 المؤرخ في 25 غشت 2021 [1] من الباب السادس منه على إنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال الذي ينص على الحماية الجزائية للأنظمة المعلوماتية و تجريم كل الأفعال المنصوص عليها في هذا الباب إذا كانت تشكل جنحاً ، بحيث يختص هذا القطب بالمتابعة و التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال والمرتبطة بها ، بمعنى أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى ذات صلة بتكنولوجيات الإعلام و الاتصال ، و تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية و بين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و التعرف على مرتكبها، كما يختص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال الأكثر تعقيداً و هي الجريمة المستحدثة وفقاً لهذا القانون و هي الجريمة التي يتعدد فيها الفاعلين أو الشركاء أو المتضررين أو بسبب إتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام و الأمن العموميين ، و تتطلب وسائل تحري خاصة و خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي .

ثانيا : مضمون القانون 11/21

يقضي الدستور الجزائري [2]، الذي يعتبر القانون الأسمى في البلاد و إستنادا إلى أحكام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بتاريخ 15 نوفمبر2000 المصادق عليها بالتحفظ وفق مرسوم رئاسي رقم 55/02 المؤرخ في في 05 فيفري 2002، و وفقا لـلأمر رقم 155/66 المعدل و المتمم ،كذلك في هذا المسار نجد ما جاء في

[1] أمر رقم 21-11، مؤرخ في 16 محرم عام 1443 الموافق ل 25 غشت سنة 2021، المتعلق بجرائم المتصلة بتكنولوجيات الإعلام والاتصال،ج. ر. ج. ج. د. ش، العدد 65، صادر في 26 غشت 2021

[2] دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي رقم 96-438، مؤرخ في 07 ديسمبر 1996، ج. ر. ج. ج. د. ش، عدد 76 ، صادر في 07 مارس 1996، المعدل المتمم.

الأحكام المتواجدة في الأمر رقم 156/66 المتضمن قانون العقوبات[1]، كما نجد العديد من القوانين كقانون 04/09 المتعلق بالقواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجياً الإعلام و الاتصال و مكافحتها ، بالإضافة إلى القانون رقم 04/18[2]، الذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية، و بمقتضى القانون رقم 05/20 [3] و المتعلق بالوقاية من التميز و الكراهية و مكافحتها عمد المشرع الجزائري على إصدار أمر رقم 11/21 الذي يهدف إلى إتمام الأمر رقم 156/66 المتضمن قانون الإجراءات الجزائية ، و ذلك بإنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المتواجد مقره على مستوى مجلس قضاء الجزائر الذي يختص في متابعة و التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و المرتبطة بها، كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحاً ، حيث يقصد بمفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، إذ تتمحور الحماية الجزائية من خلال هذا القانون بمكافحة و معاقبة كل شخص يرتكب أو يشترك في ارتكاب الجريمة التي تمس بأمن الدولة و الدفاع الوطني كجرائم النشر و الترويج لأخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع ، و كذا جرائم الإتجار بالأشخاص و الأعضاء البشرية أو تهريب المهاجرين، بالإضافة إلى جرائم التميز و خطاب الكراهية ضف إلى المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات و المؤسسات العمومية ، بمعني أنه أي جريمة ترتكب أو يسهل ارتكبها باستعمال منظومة معلوماتية أو نظام الاتصالات الإلكترونية أو أي وسيلة أخرى ذات صلة بتكنولوجيا الإعلام و الاتصال ، كما استحدث المشرع الجزائري نوعاً ثانياً من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال في القانون

[1] أمر رقم 66-156 مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات،ج. ر. ج. ج. د. ش، عدد 49، صادر في 10 جوان 1966 معدل ومتمم بالقانون 16-02 مؤرخ في 16 جوان 2016، ج.ر.ج.ج.د.ش، عدد37، صادر في 22 جوان 2016.

[2] القانون رقم 18-04 المؤرخ في 24 شعبان 1439 الموافق ل 10 مايو 2018، المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية.

[3] القانون رقم 20-05 المؤرخ في 05 رمضان 1441 الموافق ل 28 أبريل 2020، المتعلق بالوقاية من التميز وخطاب الكراهية و مكافحتها.

21/ 11 و أطلق عليها إسم الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال الأكثر تعقيداً و التي ينظر لها من حيث تعدد الأشخاص الفاعلين و الشركاء في إرتكابها و كذا اتساع الرقعة الجغرافية لمكان ارتكابها، بالإضافة إلى مدى جسامة أضرارها ، و ما مدى مساسها بالنظام و الأمن العمومين حيث أعطى المشرع الجزائري للضبطية القضائية استعمال وسائل خاصة للتحري فيها .

الفرع الثاني

القطب الجزائي الوطني المختص المستحدث بموجب الأمر 11/21

حرص المشرع الجزائري على استحدث عدة إجراءات بموجب القانون رقم 11/21 تزامناً مع كثرة الجرائم الإلكترونية داخل المجتمع الجزائري حيث تم استحداث في الباب السادس من هذا القانون قطب الجزائي المتخصص في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و التوسيع من اختصاص من هذا القطب ، بمعني أي وسيلة تستحدث فيما بعد تكون من اختصاص القطب الجزائي ، و التي تكون لها علاقة بالاتصال و الإعلام و هذا ما يظهر لنا من خلال ما يلي:

أولاً: الاختصاص المحلي

إن اختصاص القطب الجزائي المتخصص بالجرائم المتصلة بالإعلام و الاتصال و الجرائم المرتبطة بها، فإن الاختصاص يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و كذا قاضي التحقيق و رئيس محكمة جنح القطب صلاحيتهم في كامل الإقليم الوطني وفق نص المادة 211 مكرر 23 من هذا القانون.[1]

[1] أنظر المادة 211 مكرر 23 من الأمر رقم 21-11، المتعلق بجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ثانيا : الاختصاص النوعي للقطب الجزائي الوطني

إن النوعي للمحاكم يتحد على أساس نوع الجريمة، و يتحدد نوع الجريمة على أساس مقدار العقوبة المقررة لها في قانون العقوبات ، أو القوانين المكملة له ، أي أن الإختصاص النوعي يفترض أولا تحديد الواقعة و تطابقها مع نموذج القانوني خاص بجريمة بعينها ثم تحديد نوعها على أساس مقدار العقوبة.[1]

يختص القطب المستحدث عبر الإقليم الوطني و دون سواه قانونا و حصرا وفق المادة 211 مكرر24 بالجرائم التالية:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني .
- جرائم نشر و ترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع .
- جرائم نشر وترويج أنباء معرضة تمس بالنظام و الأمن العمومين ذات الطابع المنظم أو العابرة للحدود الوطنية .
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات و المؤسسات العمومية.
- جرائم الإتجار بالأشخاص أو الأعضاء البشرية أو تهريب المهاجرين .
- جرائم التميز و خطاب الكراهية .

كما يختص أيضا القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال حصريا بالمتابعة و التحقيق و الحكم في الجرائم المتصلة بالإعلام و الاتصال الأكثر تعقيداً و الجرائم المرتبطة بها وفقا لنص

[1] علي عبد القادر القهوجي،شرح أصول المحاكمات الجزائية دراسة مقارنة،الكتاب الثاني،منشورات حلب الحقوقية،لبنان،2007،ص410.

المادة 211مكرر25، حيث يختص هذا القطب بالمتابعة و التحقيق و الحكم في القضايا الموصوفة بالجرائم الإلكترونية الأكثر تعقيدا .

ثالثا: حالة الاشتراك في الاختصاص

تتم معالجة حالات الإشتراك في الإختصاص وفقا لوضعيات التالية:

- تطبق في هذه الحالة الإجراءات المنصوص عليها في المادة 211 مكرر 4 إلى 211 مكرر 14 من هذا القانون أمام القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال .
- يمارس هذا القطب الجزائي الوطني اختصاصا مشتركاً مع الاختصاص الناتج من تطبيق المواد 37 و 40 و 329 من ق ، ج، ج ج [1] بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها المتعلقة في الجرائم المتمثلة في المخدرات، الفساد، تبيض الأموال، الجريمة التي تمس بمعالجة الآلية للمعطيات جريمة الصرف ، فالاختصاص هنا مشترك بين هذه الأقطاب و هذا ما قضت به المادة 211 مكرر27 من هذا القانون .
- إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال مع اختصاص القطب الاقتصادي و المالي ، يتنازل القطب الجزائي الوطني المكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال حيث يؤول الاختصاص للقطب الاقتصادي و المالي وجوباً حسب نص المادة 211 مكرر 28 من قانون 11/21 مثل :
  - الجرائم المنصوص عليها في المواد 119 مكرر 1 و 389 مكرر 2 و 3 من قانون العقوبات .
  - الجرائم المنصوص عليها في القانون 01/06 المتعلقة بالوقاية من الفساد و مكافحته[2]

[1] أنظر المواد 37، 40، 329 من الأمر رقم 66-155، المتعلق بقانون الإجراءات الجزائية، المعدل و المتمم .

[2] قانون رقم 06-01 مؤرخ في 20 فيفري 2006، يتعلق بالوقاية من الفساد ومكافحته، ج. ر. ج. ج. د،ش، عدد 14، صادر في 08 مارس 2006، معدل ومتمم بأمر رقم 10-105 مؤرخ في 26 أوت 2010،ج،ر. ج. ج. د. ش، عدد 50، صادر في 01 ديسمبر 2010

- الجرائم المنصوص عليها في الأمر رقم 22/96 المتعلقة بقمع مخالفة التشريع و التنظيم الخاص بالصرف و حركة رؤوس الأموال من و إلى الخارج.[1]
- الجرائم المنصوص عليها في المواد 11، 12، 13، 14، 15 من الأمر رقم 06/05 المتعلق بمكافحة التهريب .

- إذا كان الاختصاص مشتركا بين القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و الجرائم المرتبطة بها مع اختصاص محكمة مقر مجلس قضاء الجزائر طبقاً للأحكام المواد 211 مكرر 16 إلى 211 مكرر 21 من هذا القانون ، فإن الاختصاص يؤول لمحكمة مقر المجلس قضاء الجزائر وفق المادة 211 مكرر 29 من القانون 21/ 11المتمم لقانون الاجراءات الجزائية

[1] أمر رقم 96-22 مؤرخ في 09 يوليو 1966، المتعلق بقمع مخالفة التشريع والتنظيم الخاص بالصرف وحركة رؤوس الأموال من و إلى الخارج ، المعدل والمتمم.

خـــــاتمة

الخاتمة

أخيرا و على ضوء ما سبق يتضح بأن خصوصية الجرائم الإلكترونية شكلت إشكالية للوصول إلى تعريف شامل و جامع رغم كل المحاولات المبذولة ، و تشكل تحديا لـلمشرع الجزائري في مجال قمع هذه الجريمة رغم ترسانة القوانين و مواكبته المستمرة لتطورها بسبب التطور السريع و الكبيرة في مختلف مجالات علوم تكنولوجيا الإعلام و الإتصال.

تتسم الجرائم الإلكترونية بطبيعة تميزها عن الحرائم التقليدية من حيث سرعة تنفيذها و خصائص المجرم المعلوماتي و سهولة تنفيذها عبر حدود الدول مما يصعب إكتشافها و كذا جمع الأدلة و بالتالي قمعها و هو ما يشكل خطورة على الأفراد و المجتمع .

لقد تجاوب المشرع الجزائري مع خصوصية الجرائم الإلكترونية بمجموعة من النصوص الموضوعية و الإجرائية لقمع هذه الجرائم المستحدثة من خلال تعديله لقانون العقوبات و قانون الإجراءات الجزائية ، كما أنه شرع نصوص مستقلة مثل قانون قواعد البريد و الإتصالات الرقمية.

رغم كل هذه المجهودات التي بذلها المشرع الجزائري لقمع الجرائم الإلكترونية إلا أنها غير كافية و من خلال ما سبق يمكن تقديم الاقتراحات التالية:

- العمل على وضع بروتوكولات تعاون مشترك بين الهيئة الوطنية للوقاية و مكافحة من جرائم الإعلام و الاتصال و باقي الهيئات المتخصصة، كالهيئة الوطنية للوقاية و مكافحة جرائم الفساد، الديوان الوطني لقمع الفساد ، المجلس الوطني الحقوق الإنسان .
- التكوين المتخصص و المتواصل للعاملين في مجال مكافحة الجريمة الإلكترونية.

- التأكيد على وجوب الحصول على إذن مسبق من طرف القاضي المكلف بإجراءات المراقبة عند تحديد المراقبة .
- توفير الإمكانات البشرية و المادية و التقنية الحديثة للجهات المتخصصة في مكافحة الجرائم الإلكترونية .
- وضع قواعد واضحة حول سرية البيانات المتحصل عليها أثناء التفتيش و حجز الأدلة .
- ضرورة تكثيف الجهود الوطنية لنشر المعرفة و زيادة الوعي بالجرائم الإلكترونية و مدى خطورتها و وسائل الوقاية منها و سبل مواجهتها.
- من الأفضل أن يسن المشرع قانون موحد لمكافحة الجرائم الإلكترونية، ملم بكل النصوص الموضوعية و الإجرائية و التنظيمية ، و هو يسهل عمل ضابط الشرطة القضائية و وكلاء الجمهورية و قضاة التحقيق و قضاة الحكم ، و يساعد رجال القانون من الإلمام بكل ما يخص هذه النوع المستحدث من الجرائم .
- ضرورة استقطاب هذا النوع من المجرمين و محاولة الاستفادة من خبراتهم في مكافحة الجرائم الإلكترونية.
- ضرورة تقنين نشاط شركات الناشطة في مجال المعلوماتية و فرض الرقابة على نشاطها في ما يخص المستخدمين.
- تشجيع الجامعات و المراكز البحثية على العمل على إنشاء نظام تشغيل جزائري و بديل لمختلف التطبيقات و الخدمات الرقمية
- ضرور توطين تخزين بيانات المستخدمين في الجزائر.

قائمة المصادر والمراجع

أولا/ المصادر:

1) دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي رقم 98-36 ، مؤرخ في 01 ديسمبر 1996، ج. ر. ج. ج. د. ش، عدد 76، صادر في 08 ديسمبر1996 المعدل و المتمم.
2) القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، الجريدة الرسمية، عدد 44.
3) القانون رقم 06-01 مؤرخ في 20 فيفري 2006، يتعلق بالوقاية من الفساد ومكافحته، ج. ر. ج .ج. د،ش، عدد 14، صادر في 08 مارس 2006، المعدل و المتمم
4) القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام و الإتصال و مكافحته المؤرخ في 05 أوت 2009،ج رعدد 47، الصادرة في 16 أوت 2009.
5) القانون رقم 18-04 المؤرخ في 24 شعبان 1439 الموافق ل 10 مايو 2018، المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية.
6) القانون رقم 20-05 المؤرخ في 05 رمضان 1441 الموافق ل 28 أبريل 2020، المتعلق بالوقاية من التميز وخطاب الكراهية ومكافحتها.
7) القانون رقم 24-06 المؤرخ في 19 شوال 1445 الموافق ل 28 أبريل 2024 المعدل و المتمم لقانون العقوبات،ج.ر.ج.ج.د.ش،العدد30،الصادرة في 30 أفريل 2024.
8) الأمر رقم 96-22 مؤرخ في 23 صفر 1386،الموافق ل 09 يوليو 1966، المتعلق بقمع مخالفة التشريع والتنظيم الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، المعدل والمتمم.
9) الأمر رقم 03-05 مؤرخ في 19 جمادى الأول عام 1424 الموافق لـ 19 يوليو 2003،المتعلق بحماية المؤلف من الحقوق المجاورة،ج ر،عدد 44.
10) الأمر رقم 03-08 المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، صادر في تاريخ 2003/07/23 ، الجريدة 44 الرسمية، عدد 36.
11) الأمر رقم 21-11، مؤرخ في 16 محرم عام 1443 الموافق ل 25 غشت سنة 2021، المتعلق بجرائم المتصلة بتكنولوجيات الإعلام والاتصال،ج. ر. ج. ج. د. ش، العدد 65، صادر في 26 غشت 2021
12) الأمر رقم 66-155 مؤرخ في 18 جوان 1966، يتضمن قانون الإجراءات الجزائية، ج. ر. ج. ج .ر. ش، عدد 48، صادر في 11 جوان 1966 المعدل والمتمم.
13) الأمر رقم 66-156 مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات،ج. ر. ج. ج. د. ش، عدد 49، صادر في 10 جوان 1966 المعدل والمتمم

ثانيا/ المراجع العامة :

41) أحسن بوسقيعة، الوجيز في القانون الجزائي العام الديوان الوطني للأشغال التربوية، ط1، الجزائر، 2002
51) أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، دون بلد النشر، 2006
61) أحمد شوقي الشلفاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء 2 طبعة 5، ديوان المطبوعات الجامعية الجزائر
71) أحمد عبد الرزاق السنهوري، الوسيط في شرح القانون المدني حق الملكية، الجزء الثاني، دار أحياء التراث العربي، بيروت، 1952.
81) محمود نجيب حسني،شرح قانون العقوبات، دار النهضة العربية، القاهرة، 1992

ثالثا/المراجع المتخصصة:

91) الرومي مُحَمَّد أمين، الكمبيوتر والأنترنت، دارالمطبوعات الجامعية الإسكندرية، مصر، 2004
02) الزبدي وليد، القراصنة على الأنترنت والحاسوب، الطبعة الأولى، دار سامة للنشر، عمان، 2003
12) بن مكي نجاة ،السياسة الجنائية لمكافحة جرائم المعلوماتية ،دار الخلدونية،الجزائر،2017
22) حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، ط1، منشورات الحلبي الحقوقية، بيروت، 2014
32) خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، 2010
42) رشاد خالد عمر، المشاكل القانونية و الفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة، ، ط2، المكتب الجامعي الحديث، مصر، 2018
52) زبيدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دارالهدى، الجزائر، 2011
62) عبد العال الديربي و مُحَمَّد صادق اسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية و الانترنيت، ط1، المركز القومي للإصدارات القانوني، القاهرة، 2012
72) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، دارالكتب، القاهرة، 2002
82) علي عبد القادر القهوجي،شرح أصول المحاكمات الجزائية دراسة مقارنة،الكتاب الثاني،منشورات حلب الحقوقية،لبنان،2007
92) قارة أمال،الحماية الجنائية للمعلوماتية في التشريع الجزائري، ط 1، دار هومة، الجزائر، 2006
03) قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة،2004
13) مُحَمَّد حماد مرهجال هيبتي، جرائم الحاسوب، دار المناهج للنشر و التوزيع، عمان، 2005

23) مُحَمَّد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة عزيب، القاهرة، 1984
33) محمود أحمد عبابنة ،جرائم الحاسوب و ابعادها الدولية ،دار الثقافة للنشر و التوزيع ،الأردن،2005
43) نائلة قورة، جرائم الحاسوب الاقتصادية، ط1، دارالنهضة العربية، القاهرة، 2003
53) نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة لنشر والتوزيع، عمان، 2008
63) وضاح محمود نشأت، مقضي المجالي، جرائم الأنترنيت، دارالمنارة للنشر، عمان، 2005

رابعا / الأطروحات و المذكرات :

37) بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجيستير في القانون الجنائي،كلية الحقوق، جامعة وهران، 2012 – 2013
38) تايرب عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، جامعة أحمد درارية، أدرار، 2016/2017
39) حمزة بن عفون، السلوك الإجرامي، المجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2011/2012
40) سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، شهادة الماجستير في العلوم القانونية، تخصص علوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013
41) سمية مزعيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات مذكرة هادة الماستر في الحقوق، تخصص قانون جنائي،جامعة مُحَمَّد خيضر، بسكرة،الجزائر، 2013-2014.
42) سوبر سفيان،الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبوبكر بلقايد، تلمسان، الجزائر، 2010
43) صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013
44) فليح نور الدين الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر، سعيدة، 2019/2018.
45) يوسف خليل يوسف العفيفي، الجرائم الالكترونية في التشريع الفلسطيني دراسة تحليلية مقارنة،رسالة لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون الجامعة الإسلامية،غزة، 2013

خامسا / المقالات العلمية:

46) الهادي حضراوي، تجربة الجزائر في مكافحة الجريمة الالكترونية، المؤتمر الدولي لمكافحة الجرائم المعلوماتية ICACC كلية علوم الحاسب والمعلومات جامعة الإمام مُحَمَّد بن سعود الإسلامية، السعودية، 2015

47) براهيمي جمال، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية مولود معمري، تيزى وزو، العدد 2، الصادر بتاريخ 15/11/2016

48) بن غدقة شريفة و القص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الانترنيت و طرق محاربتها، أعمال الملتقى الوطني،آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري،الجزائر، 29 مارس2017.

49) بوضياف أسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة مُحَمَّد بوضياف المسيلة الجزائر،العدد 11 ،2018

50) حمودي ناصر، التنظيم القانوني لظاهرة المعلوماتية في الجزائر الانجازات والتحديات المجلة النقدية للقانون والعلوم السياسية، عدد 2 كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012

51) سومية عكور، الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانون والأمني، المتلقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، الأردن، 02 أفريل 2016

52) عاقلي فضيلة، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية، طرابلس بتاريخ 24/ 25 مارس، 2017.

53) عبد الناصر محمود فرغلي مُحَمَّد عبيد سيف السماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول للعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007

54) عيمور راضية،الجريمة الإلكترونية و آليات مكافحتها في التشريع الجزائري ،"المجلة الأكاديمية للبحوث القانونية"،المجلد السادس،العدد الأول،2022.

55) فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، المنعقد بأكاديمية الدراسات العليا بليبيا في أكتوبر 2009

56) مُحَمَّد الأمين البشري،التحقيق في جرائم الحاسوب الآلي والأنترنت،"المجلة العربية للدراسات الأمنية والتدريب"، العدد 30، نوفمبر2000

57) موسى مسعود أرحومة، الإشكاليات الإجرائية التي تسيرها الجريمة المعلوماتية عبر الوظيفة، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظيمه أكاديمية الدراسات العليا، طرابلس، 26، – 29/10/2009، ص 03.

58) نياب موسى، الجرائم الإلكترونية المفهوم والأسباب، الملتقى العلمي للجرائم المستحدثة في ظلال تغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، الأردن، 2014

59) ونوغي نبيل، زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور بالجلفة الجزائر، المجلد الرابع، العدد الثالث، سبتمبر 2019

60) صابر بحري و خرموش مني، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات فيسيكولوجية الانحراف، المجلد 06، العدد 01، جامعة مُحَّد لمين، دباغين، سطيف، الجزائر، 2021.

61) صالح شنين، الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، عدد 01، الجزائر، 2010.

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات