وزارة التعليم العالي و البحث العلمي

جامعة غرداية

كلية الحقوق و العلوم السياسية

قسم الحقوق

عنوان المذكرة

الحماية الجزائية للمؤسسة من جريمة الغش المعلوماتي

مذكرة مقدمة لإستكمال متطلبات شهادة ماستر أكاديمي في مسار الحقوق

تخصص : قانون جنائي و العلوم الجنائية

من إعداد الطالبة :

- أولاد سعيد محمد
- يعقوب عبد العزيز

إشراف الأستاذ:

- د بن فردية محمد

لجنة المناقشة:

إسم و لقب الأستاذ	الرتبة	الجامعة	الصفة
بن عودة مصطفى	أستاذ محاضر ب	غرداية	رئيسا
بن فردية محمد	أستاذ محاضر أ	غرداية	مشرفا
هوام نسيم	أستاذ مساعد ب	غرداية	مناقشا

- السنة الجامعية: 2020/2019 -

بسم الله الرحمن الرحيـم

﴿يوم تجد كل نفس ما عملت من خير محضرا و ما عملت من سوء تود لو أنها بينها و بينه أمدا بعيدا و يحذركم الله نفسه و الله رؤوف بالعباد ﴾

آل عمران .30

الإهداء

كن عالما فان لم تستطع،فكن متعلما فان لم تستطع فأحب العلماء

ربي إذا أعطيتني نجاحا فلا تأخذ تواضعي،وإذا أعطيتني تواضعا فلا تأخذ اعتزازي بكرامتي.

بمناسبة تخرجي سأرفع قبعتي مودعا السنين التي مضت

اهدي ثمرة هذا الجهد إلى ابي، الرجل الذي علمني أن أكون رجلا والى من أشعل لي أول شمعة في حياتي،إلى من تحمل مصاعب الحياة من اجلي، أطال الله في عمره.

والى الصدر الدافئ،والقلب العطوف رمز الصبر والتضحية " أمي" أطال الله في عمرها وأمدها بالصحة والعافية ودامت تاجا فوق رؤوسنا.

إلى تيجان راسي وفخري إخوتي وأخواتي هواري وابنه وفوزية وابناها وزوجها وسعيدة وولديها وزوجها وإيمان ومروة وعبد القادر وكل عائلة يعقوب ولشهب.

والى اصدقائي السنة وعماد الدين وفارس واحمد و صالح وعيسى والإمام الفاضل مختار رمضاني وبوعمامة ويوسف وإسماعيل وعيسى زرباني وحمزة وفتح الله وبلقاسم.

واخص بالشكر والامتنان والعرفان إلى الدكتور الفاضل أولاد النوي مراد الذي لم يكن أستاذا بل كان أخ وصديق والى الدكتور زرباني عبد الله (ا) والدكتور بوحميدة عبد الكريم والدكتور زرباني عبد الله (ب)

والى كل الأهل والأحباب، والى كل من كان له الفضل والمساعدة في هذا العمل.إلى جميع طلبة السنة ثانية ماستر جنائي.

والى زميلي و أخي في انجاز هذه المذكرة أولاد سعيد محمد وأخته التي ساعدتنا أم الخير .

الإهداء

أصل البداية فكرة واصل الفكرة دوافع

وما أصعب تجسيد الأفكار على ارض الواقع

إلى من أكن له بالوقار ومن علمني العطاء دون انتظار،الذي احمل اسمه بكل افتخار والدي العزيز (رحمه الله واسكنه فسيح جنانه).

إلى التي أهدتني نور الحياة وسقتني من دفقات حبها ورعايتها وكان دعائها سر نجاحي "أمي" الغالية أطال الله في عمرها وأدامها نبعا صافيا وعزا

إلى الذين ساعدوني وجعلو الفكرة واقعا

إلى أخي مبارك وزوجته الكريمة وولديهما امجد ورفيدة

إلى أخواتي أم الخير وليلى وخضراء وزوجها وأولادها ، سيف الدين_ يوسف_عبدا لرحمان_منصف

والى عائلة ظاهر مسعود وخاصة احمد.وعائلة راكش الياس.

-دون أن أنسى زميلات وزملاء الدراسة ابنة عمي أولاد سعيد جمعة ولصقع أمباركة والى الزميل صالح خنان و بوحميدة إسماعيل.

واخص بالشكر الدكاترة زرباني عبدا لله (ا) ،بوحميدة عبدا لكريم ،زرباني عبدا لله (ب)،الراعي العيد.لغلام عزوز.

والى زميلي في انجاز هذه المذكرة يعقوب عبد العزيز.

والى كل من كان له الفضل والعون في مشواري الدراسي من قريب أو بعيد

شكر و عرفان

انطلاقا من الأثر النبوي الكريم (**من لايشكر الناس لا يشكر الله**)

الشكر لله الذي خلق الكون فنظمه وخلق الإنسان فكرمه، فالق الحب والنوى منزل التوراة والإنجيل والفرقان.

نتقدم بالشكر الجزيل إلى أستاذنا والدكتور الفاضل "**بن فردية محمد**" على نصائحه وتوجيهاته القيمة التي أنارت دربنا، والذي لم يبخل علينا بمراجعه التي قدمها إلينا ومعلوماته القيمة.

كما نتوجه بالشكر إلى كل الزملاء والأصدقاء خاصة الدكتور **لشهب السنة** ، صاحب مكتبة الوفاء الأستاذ **بوحفص عماد الدين** اللذين كانت لهما لمسة في هذا الانجاز .

دون أن أنسى جميع الأساتذة الكرام و الإداريين العاملين على مستوى كلية الحقوق .

الملخص

من خلال دراستنا هذه التي جاءت مع التطورات الحديثة الحاصلة في مجال المعلوماتية ، حيث أدت هذه التطورات إلى ظهور ما يعرف بجريمة الغش المعلوماتي الذي أخذ عدة صور منها الاعتداء على المعلومات واستخدامها على النحو غير مشروع وقد سعينا من خلال هذا البحث إلى تحديد مفهوم جريمة الغش المعلوماتي وذلك بأخذ تعريفات التي صاغها الفقه الجنائي للجريمة وبعض التشريعات العربية والغربية ،وكذا الصيغة القانونية الخاصة التي تميز جريمة الغش المعلوماتي وكذا أصناف المجرمين اللذين ينتمون إليها ومن خلال الدراسة تطرقنا إلى بعض النماذج جريمة الغش المعلوماتي .

أما في الفصل الثاني حاولنا التعرف على طرق وآليات البحث في الغش المعلوماتي وكذا الإجراءات المقررة لها من خلال قانون العقوبات وكذا قانون 04/09

الكلمات المفتاحية :الغش المعلوماتي ,المؤسسة ,العمل.

Abstract

Through our study, which came with recent developments in the field of informatics, as these developments led to the emergence of what is known as the crime of information fraud, which took several forms, including assault on information and its unlawful use, and we sought through this research to define the concept of the crime of information fraud. By taking definitions formulated by criminal jurisprudence for crime and some Arab and Western legislation, as well as the special legal formula that distinguishes the crime of information fraud, as well as the types of criminals to which they belong, and through the study we touched upon some models of the crime of information fraud.

As for the second chapter, we tried to identify the methods and mechanisms for researching information fraud, as well as the procedures prescribed for them through the Penal Code, as well as the 04/09 Law.

Keywords : Information fraud, institution, business.

قائمة المختصرات :

ق إ ج ج	قانون الاجرءات الجزائية الجزائرية
ق ع	قانون العقوبات
ق إ ج الألماني	قانون الإجراءات الجزائية الألماني
ق إ ج الفرنسي	قانون الإجراءات الجزائية الفرنسي
ج 1	الجزء الأول
ص	الصفحة
ط	الطبعة
دج	دينار جزائري
إلخ	إلى آخره

المقدمة

ظهرت في الآونة الأخيرة –في القرن الواحد والعشرين – استخدامات الحاسب الآلي عبر شبكة المعلوماتية الدولية وهو ما تطلب بسط القانون على هذه الأنشطة المعلوماتية بالشكل الذي يحمي حياة الأفراد والمؤسسات،فلقد أضحت المعلومات تمثل 07بالمئة من قيمة التجارة الدولية العالمية،وهو ما جعل المعلومات أهم وأثمن الموارد على الإطلاق .

وبالرغم من المنافع التي أفرزتها تكنولوجيا المعلومات وشبكات المعلومات من خلال إدخال العصرنة في مجال العمل وتسريع وتيرته واستبدال النظام الالكتروني لليد العاملة، وتسهيل العمل للمؤسسات،كما أوجدت سلبيات لعلى أهمها ما يعرف بالغش المعلوماتي.وجب على المشرع أن يحمي هذه المؤسسات من هذه الجريمة بوضع قوانين تمنع استفحال ظاهرة الغش المعلوماتي.

وغني عن البيان إن ثورة تكنولوجيا الاتصالات والتوسع في استخدام شبكة الانترنت جعل من مختلف القطاعات ومن بينها ميدان العمل تعتمد في عملها على استخدام هذه الأنظمة المعلوماتية لما تتميز به من سرعة ودقة في تجميع المعلومات وتخزينها ومن ثم نقلها بين الأفراد والمؤسسات المختلفة سواء داخل دولة أو بين عدة دول أخرى،مما أدت إلى تطور وسائل ارتكاب الجرائم، حيث ظهرت نوعية جديدة من الجرائم المستحدثة يتم ارتكابها من خلال استخدام التقنيات الحديثة والحاسبات الآلية عن طريق شبكة الانترنت ،أطلق عليها الجرائم المعلوماتية.ومع التغلغل المتزايد للمعلوماتية وتكنولوجيا الاتصال في مختلف مجالات النشاطات البشرية والتي أفرزت العديد من الأشخاص الذين يتعاملون معها بشكل سوي ويستغلون معارفهم وقدراتهم في مجال المعلوماتية للقيام بأفعال غير قانونية ومنتفية للأخلاق بلغت حد المساس بالأمن العام في العديد من الدول.

وعلى الرغم من الأهمية البالغة للمعلوماتية إلا أنها خلفت انتشارا سريعا لهذا النوع من الإجرام مما جعل من المجتمع الدولي يتدخل من اجل وضع حد لانتشارها،فكان لابد من وضع اطر قانونية سارية المفعول بما يتلائم والوضع الجديد وذلك لتحديد شروط استعمال هذه الوسائل في مختلف المعاملات،من خلال نصوص جزائية لحماية الأنظمة المعلوماتية،وردع إساءة استعمالها محليا ودوليا.

فالتقدم العلمي والتكنولوجي لا يمكن أن يسير أو يعمل وحده بمعزل عن أي تقدم قانوني يواكبه ويقوم بالمحافظة عليه ويكفل حماية ويضع الحلول لما قد يطرأ من مشاكل بسبب استعماله،ففي هذه الحالة يمكن للتقدم التكنولوجي أن يصبح أداة للبناء وأساس لكل تطور ويمكن أن يكون أداة لارتكاب الجريمة إذا أسيء استخدامه.

ونظرا للخطورة التي تتميز بها هذه الجرائم المستحدثة هي أنها سهلة الارتكاب نتيجة للاستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات،وان أثارها ليست محصورة في النطاق الإقليمي لدولة بعينها ،فضلا على أن مرتكبيها يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الآلية، للمعطيات والإلمام بالمهارات والمعارف التقنية،ليس هذا فحسب بل أنها تستهدف من طبيعة خاصة وتعني بذلك التي يحتوي عليها نظام المعالجة الآلية،الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة وبالذات فيما يخص إثبات هذه الجرائم والية مباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمهم للعدالة.

وعليه فان هذا النوع من الجرائم المستحدثة صعب الاكتشاف والإثبات فلا اثر فيها لأي عنف أو دماء وإنما مجرد أرقام وبيانات تتواجد على اسطوانة صلبة أو مرنة أو على أي دعامة مادية منقولة أو على الذاكرة الحية للحاسوب،مما يمكن القول معه أن البحث في الإثبات ووسائله في إطار رصد مدى اتفاقه مع التقنية الحديثة يبدو غير ذي معني إذا لم يكن مدعما بتوافق من قبل التقنية ذاتها،غير أن المشكلات الإجرائية في مجال الجرائم المعلوماتية بتعلقها في كثير ممن الأحيان ببيانات معالجة الكترونيا وكيانات غير ملموسة،وبالتالي يصعب من ناحية كشف هذه الجرائم،ويصعب من ناحية أخرى في بعض الأحيان كجمع الأدلة بشأنها،ومما يزيد صعوبة في هذا الإجراءات في هذا المجال،سرعة ودقة تنفيذ الجرائم المعلوماتية وإمكانية محو أثارها،وإخفاء الأدلة المتحصل عنها عقب التنفيذ مباشرة،ويواجه التفتيش وجمع الأدلة صعوبات كثيرة في هذا المجال،وقد يتعلقان ببيانات مخزنة في أنظمة أو شبكات الكترونية موجودة بالخارج.

والجزائر كغيرها من الدول الأخرى وباعتبارها واحدة البلدان التي عرفت هذا النوع من التطور التكنولوجي سواء كان ايجابي أو سلبي فهي أيضا معنية بمكافحة هذه الظاهرة الحديثة،فكان لابد لها من إيجاد إطار قانوني مناسبا لسد الفراغ الإجرائي، لذلك سعى المشرع الجزائري إلى وضع مجموعة من القوانين منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المعلوماتية عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل وإجراءات خاصة تتماشى مع طبيعة الجرائم المستحدثة ومنها الجرائم المعلوماتية وتخصيص آليات وإجراءات تطبق عليها فقط والتي تم النص عليها في قانون جديد يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال قانون 04/09.

كما تدخل من جهته لحماية أهم المصالح المتعلقة الأنظمة المعلوماتية من خلال تعديله لقانون العقوبات سنة 2004 واستحدث بموجبه قسم سابع مكرر يحمل عنوان (المساس بأنظمة المعالجة الآلية للمعطيات) يتضمن طائفة من النصوص التي جرم من خلالها العديد من الأفعال التي تشكل عدوانا على أنظمة المعالجة الآلية للمعطيات أو احد أجزائها واقر لمرتكبيها الجزاء المناسب.

أهمية الدراسة

ينبع الهدف من هذه الدراسة هو محاولتنا لإثراء هذا الموضوع المستحدث للتعرف على نوع من الجرائم التي تقع داخل المؤسسات التي باتت تعرف بجريمة الغش المعلوماتي،ذلك أن حداثة الجرائم المعلوماتية جعلت المشرع في حيرة في كيفية وضع قوانين تحمي المؤسسات من الانتهاك من قبل الآخرين.

أسباب اختيار الموضوع

سبب اختيارنا لهذا البحث، هو رغبتنا في التعرف على جريمة الغش المعلوماتي التي ترتكب في ميدان العمل، وكشف حقيقة التعامل مع هذه الجريمة من الناحية الإجرائية لان الكثير من الدراسات باتت ترتكز على الجانب الموضوعي فقط،ونظرا لقلة المؤلفات التي تتحدث عن الجانب الإجرائي حاولنا من خلال بحثنا إثراء النقاش القانوني حول هذا الموضوع الهام.

الصعوبات:

يمكن القول بان أهم الصعوبات التي واجهتنا خلال إعدادنا لمذكرة التخرج :

- غلق المؤسسات الجامعية عبر التراب الوطني جراء جائحة كورونا (covid19) التي اجتاحت العالم عامة والجزائر خاصة الأمر الذي صعب علينا جمع عدة مراجع .
- غلق جميع المكتبات العمومية وصعوبة التنقل بين الولايات لاقتناء مراجع وكتب.
- تأثر الجانب النفسي جراء هذا الوباء مما صعب علينا مزاولة البحث.
- أما من ناحية لب الموضوع وجدنا قلة نادرة في المؤلفات نظرا لان جريمة الغش المعلوماتي موضوع مستحدث ومتطور مما صعب على التشريعات وضع قوانين للتصدي لهذه الجريمة.

مناهج البحث

تطلب منا هذا البحث الاعتماد على المنهج الوصفي بالإضافة إلى المنهج التحليلي و المنهج المقارن .

المنهج الوصفي يظهر من خلال وصفنا لجريمة الغش المعلوماتي وتحديد بعض المفاهيم التي تقوم عليها،أما المنهج التحليلي فحاولنا تحليل بعض المفاهيم وتبيان جزئياتها مثل ماكان الحال في طرق إثبات الجريمة وذكر الجزاءات المقررة لها أما بخصوص المنهج المقارن فقد قمنا بمقارنة النصوص الوطنية وواقع هذا الجريمة مع القوانين وواقع الدول الأخرى.

الإشكالية

إن بحث الحماية الجزائية التي يوفرها القانون في المجال المعلوماتي للمؤسسة عن طريق تجريم ظاهرة الغش المعلوماتي يتطلب منا طرح الإشكالية التالية : **هل القوانين التي أقرها المشرع الجزائري كافية للتصدي لجريمة الغش المعلوماتي ؟**

ومنه كان لزاما علينا طرح التساؤلات التالية:

- ما مفهوم جريمة الغش المعلوماتي ؟
- ما هي خصائص جريمة الغش المعلوماتي و ما مميزات الجرم المعلوماتي ؟
- ما هي طرق و آليات البحث في جريمة الغش المعلوماتي ؟

- ما هي الجزاءات المقررة من خلال التلاعب بأنظمة المعالجة الآلية للمعطيات؟

و للإجابة عن هذه الإشكالية ارتأينا إتباع خطة البحث التالية :

خطة البحث

حاولنا من خلال بحثنا أن نحصر نطاق الدراسة ضمن خطة تتكون من فصلين:

في الفصل الأول :ماهية جريمة الغش المعلوماتي والذي يضم مبحثين،المبحث الأول حول مفهوم جريمة الغش المعلوماتي في التشريعات المقارنة،والمبحث الثاني حول أركان وأنواع جريمة الغش المعلوماتي.

الفصل الثاني: طرق إثبات جريمة الغش المعلوماتي والجزاءات المقررة لها والذي يضم مبحثين، المبحث الأول حول طرق إثبات جريمة الغش المعلوماتي،والمبحث الثاني حول الجزاءات المقررة لهذه الجريمة.

الفصل الأول : ماهية جريمة الغش المعلوماتي

لقد عرف العالم في الفترة الراهنة ازديادا كبيرا في نطاق استخدام فقهية المعلومات مما أدى إلى الاعتماد عليها في تسيير شؤونه وهو الأمر الذي صاحبه في المقابل ازديادا موازيا للإجرام لمعلوماتي.

وقد أثارت هـذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة و نظرا لجسامة أخطارها وفداحة خسارتها وسرعة انتشارها أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الغنيين والمهنيين بأمن الصرح المعلوماتي .

وتعد جريمة الغش المعلوماتي من الظواهر الإجرامية الحديثة وتحديد مفهومها بعد الخطوة الأولى للتعرف على هذه الظاهرة الجريمة من جميع جوانبها القانونية ، خاصة إذا علمنا انه لا يوجد مصطلح قانوني موحد للدلالة على هـذه الظاهرة الإجرامية الناشئة في بيته الكمبيوتر بسبب ذاتيتها وتميزها عن الجرائم التقليدية .

وسوف نحاول من خلال هـذا الفصل تحديد ماهية جريمة المعلوماتي بإلقاء الضوء على تعريف جريمة الغش المعلوماتي وتبيان خصائصها ، أما في المبحث الثاني سنتناول أركان وأنواع الغش المعلوماتي :

المبحث الأول : مفهوم جريمة الغش المعلوماتي

تعددت تعريفات جريمة الغش المعلوماتي وتباين بين فيما بينها لتعريفات وظيفية واسعة وواسعة وقد أسفرت ذلك عن تعذر إيجاد فهم مشترك لظاهرة جريمة الغش المعلوماتي ،مما ينتج عدا ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها ، وسوف نحاول من خلال هـذا المبحث الوصول إلى تعريف يتلائم مع طبيعة جريمة الغش المعلوماتي في العمل(مط1) ومنه نتنقل بعد ذلك إلى ذكر خصائصها وأنواع الجريمة الغش المعلوماتي (م ط 2)

المطلب الأول : تعريف جريمة الغش المعلوماتي

إن جريمة الغش المعلوماتي جريمة مستحدثه يعتمد مرتكبها على وسائل فقهية ويكون ذا دراية كافية باستخدام النظم المعلوماتية لذا فان الإحاطة بمفهوم الدقيق لا يزال محل خلاف فقهي،[1] فالجرائم المعلوماتية فهي صنف جديد من الجرائم ذلك انه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى الكترونية قد يصعب التعامل معها ، إن جريمة الغش المعلوماتي هي من الظواهر الحديثة وذلك ارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصال. وقد أحاط بتعريف جريمة الغش المعلوماتي الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها.[2]

الفرع الأول: التعريف الفقهي

نتناول فيما يلي بعض التعريفات الفقهية التي قيلت في تعريف جريمة الغش المعلوماتي باعتبارها تعاريف تبين لنا مفهوم الغش داخل المؤسسات والتي يكون فيها المتضرر المؤسسة سواء مديرا أو رئيس المؤسسة،والتي يكون الفاعل فيها إما العامل أو الأجير أو شخص أجنبي خارج المؤسسة و أخذوا باعتبار المعلوماتية كموضوع للجريمة أو كوسيلة لارتكاب الجريمة، وذلك النحو التالي:

أ)– الاتجاه الضيق من مفهوم جريمة الغش المعلوماتي (وسيلة الجريمة):

هذا نوع من التعريفات يستند إلى اعتبار الحاسب الآلي كوسيلة لارتكاب الجريمة، إذ عرفها الفقيه الألماني تديمان بأنها: كل أشكال السلوك غير المشروع (أو الضار بالمجتمع)الذي يرتكب باستخدام الحاسب.

1 أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، الطبعة الثالثة 2006، دار هومة ، ص3

2 قربوز حليمة ، الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن ،مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء الجزائر ، ص 57. 2009

وقد عرفها مكتب التقنية في الولايات المتحدة الأمريكية، من خلال تعريف جريمة الحاسب بأنها:"الجرائم التي تلعب فيها بيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا ".كما عرفتها الأستاذة ESLIF.DBALL

بأنها:"فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"[1]

وعرفها الأستاذ ASTAR SOLAR نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبط بتقنية المعلومات، وهو يشابه التعريف الذي أتى بها الباحث DAVID THOMPSONبأنها:" جرائم يكون متطلبا لاقترافها أن يتوفر لدى الفاعل معرفة بتقنية الحاسب. أما الفقيه (MERWE) فقد عرفها بأنها ذلك الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات.[2]

ومن هذه خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يضيق من مفهوم جريمة الغش المعلوماتي ، حيث إن مجرد مشاركة الحاسب الآلي في سلوك الإجرامي يضيف عليه وصف الجريمة المعلوماتية ومن ثم يتضح لنا صعوبة هذا التوجه ، فجهاز الحاسب الآلي قد لا يخلو إن يكون محلا تقليديا وبعض الجرائم كسرقة الحاسب الآلي ذاته أو الأقراص أو الاسطوانات الممغنطة أو اللواحق على سبيل المثال ، ومن ثم لا يمكن إعطاء وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد إن الحاسب الآلي أو أي من مكونات كانوا للجريمة كما يلاحظ من خلال التعريفات السابقة قد أغفلت جانبا على قدر كبير من الأهمية في تعريف جريمة الغش المعلوماتي إلا وهو الدور الكبير الذي يقوم به

1 رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات الدولية والمواثيق الدولية، دار النهضة العربية، الطبعة الأولى 2011، ص 18, 19.

2 محمد بن فردية , الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية , أطروحة لنيل شهادة الدكتوراه ,فرع القانون الجنائي وعلوم الجنائية ,الحقوق , طلية الحقوق, جامعة الجزائر 1 ,2015/2014 ,ص 35.

الحاسب الآلي في هذه الجريمة ، فان كان من المتفق عليه أن جريمة الغش المعلوماتي قد تتخذ احد المظهرين ، ويتمثل الأول في استخدام الحاسب الآلي كوسيلة لارتكاب الجريمة والثاني في الاعتداء على الحاسب الآلي ذاته ، فانه يثور أمامنا التساؤل الأتي هل تعد جريمة الغش معلوماتي في كل الحالات التي يستخدم فيها نظام الحاسب الآلي من اجل ارتكاب الجريمة، وفي كل الحالات التي يقع فيها اعتداء على الحالات التي يقع فيها اعتداء على الحاسب الآلي ونظامه ؟

لا شك إن الإجابة على هذا التساؤل تكون بالنفي ، إذا قد ترتكب الجريمة و يستعمل الحاسب الآلي ولا نكون أمام جريمة معلوماتية كمن يقوم بالاتصال بواسطة حاسب ألي بشركاته في ارتكاب جريمة السرقة أو السطو على بنك لارتكاب جريمة أخرى ، كما انه قد لا نكون بالضرورة أمام جريمة معلوماتية إذا ما تم الاعتداء على الحاسب الآلي ونظامه كمن يقوم بتخريب الوحدة المركزية لجهاز الحاسب الآلي أو أحد مكوناته المادية. [1]

ب)– الاتجاه الموسع من مفهوم جريمة الغش المعلوماتي (موضوع الجريمة) :

ارتكز جانب كبير من الفقه الجنائي في تعريف جريمة الغش المعلوماتي على التقنية المعلوماتية كموضوع أو وسيلة اعتداء ،[2] كما يرى هذا الجانب من الفقه أن تعريف جريمة الغش المعلوماتي إنما يرجع إلى محل هذه الجريمة وغير متعلق بالوسيلة المرتكبة التي ذكرها السابقون حيث يرى هؤلاء إن جريمة الغش المعلوماتي هي تلك التي يكون موضوعها أو محلها المعلومات دون النظر فيما إذا كان الحاسوب هو الأداة المستخدمة في الجريمة من عدمه[3] ومن أنصار هذا الاتجاه الفقيه روز بلات rose blatt إذ عرفها بأنها : كل فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغييرات أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب ، أو تلك التي تحول من طريقة وقد عرفها جانب ثالث بأنها كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية ويهدف إلى

1 PDF.SWI…., dispace.univ.tlemcen.dz جرائم المعلوماتية , مذكرة لنيل شهادة الماجيستر في العلوم الجنائية و علم الإجرام ,2020/04/21 , س 20:30

2 رامي متولي القاضي، مرجع سابق, ص 18

3 محمد بن فردية ,مرجع سابق ,ص 54

الاعتداء على أية مصلحة مشروعة سواء كانت مادية أو معنوية,[1] أو هي "كل جريمة تتم في محيط أجهزة الكمبيوتر" . أو هي "كل سلوك غير مشروع أو غير أخلاقي أو غير المصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".[2]

كما عرفها مكتب المحاسبة العامة ل.م.أ GOA بأنها : الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات ، وإضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر وكذلك عرفها الدكتور عبد القدر قهوجي بأنها : سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها ويعرف الباحثان محمود فرغلي وسعد المسماري الجريمة بأنها : فعل أو أفعال غير مشروعة تتم بواسطة أو تستهدف النظم البرامجية أو نظم المعالجة الالكترونية للحاسب الآلي أو الشبكات الحاسوبية أو شبكة الانترنت وما على شكلها ، وعلى ذلك فتنوع الجرائم المعلوماتية وتعدد لدرجة تصعب حصرها ، مابين التزوير والتزييف الرقمي أو المعلوماتي ، وتدمير و إتلاف البرامج والبيانات والمعلومات، والسطو على البيانات والمعلومات ، والاحتيال الرقمي ، والتجسس [3]

وقد انتقد هذا التعريف لكونه يجهر الجريمة في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكبها ، إذا انه في كثير من الحالات يرتكب الفعل دون الحاجة إلى هذا القدر من المعرفة ورغم ذلك لا يمكننا إنكارا إن هذه الأفعال تدخل في عداد الجرائم المعلوماتية كإتلاف في البيانات المخزنة داخل المعلوماتي ، كما أن هذا الفعل مجرما قانونا عند معظم التشريعات بما فيها التشريع الجزائري كما تجدر الملاحظة أن جانب من هذا الاتجاه يرى إن الجرائم المعلوماتية ليس هي التي يكون الحاسب الآلي أداة لارتكابها ، بل هي التي تقع على الحاسب الآلي أو على نظامه المعلوماتي فقط يعرفون هذه الجريمة بأنها : نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة

1 رامي متولي القاضي، مرجع سابق, ص 19.

2 خالد ممدوح إبراهيم, الجرائم المعلوماتية, دار الفكر الجامعي, الإسكندرية, الطبعة الأولى, سنة 2009, ص74

3 محمد بن فردية ,مرجع سابق ,ص 55

داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقة ، ويعاب على هذا التعريف انه يخرج من نطاق الجريمة المعلوماتية عدد كبير من الأفعال غير مشروعة والتي يستخدم فيها الحاسب الآلي كأداة لارتكابها كالاحتيال المعلوماتي[1]

الفرع الثاني : التعريف التشريعي لجريمة الغش المعلوماتي :

خلوها لبينة التشريعات من وضع تعريفا للجرائم المعلوماتية : بداية نود أن نشير إلى مدونة الأمم المتحدة بشأن الجرائم المعلوماتية قد أشارت إلى عدم توصل الخبراء الدوليين إلى وضع تعريفا محددا للجرائم المعلوماتية ، كما أن اللجنة الأوروبية لمشاكل الجريمة التابعة للمجلس الأوروبي عام 1989 لم تشتري الإرشادات العامة بشأن الجرائم المعلوماتية وتصنيفها إلى تعريف أوروبي موحد ، وتركت ذلك للدول المعنية .

وقد تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا للجرائم المعلوماتية ، حيث عرفها بأنها :" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوب أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية ."

إلا أن هناك جانبا من التشريعات المقارنة التي أشارت إلى تعريف الجريمة المعلوماتية ، نذكر منها القانون السعودي ، القانون الأميركي .

أ)– تعريف القانون السعودي

تضمن نظام مكافحة جرائم المعلوماتية السعودي الصادر بمقتضى المرسوم الملكي رقم (م (17)في 1428/3/8هـ على تعريف جريمة المعلوماتية بأنها:[2]

1 PDF.SWI…., dispace.univ.tlemcen.dz جرائم المعلوماتية , مذكرة لنيل شهادة الماجيستر في العلوم الجنائية و علم الإجرام ,2020/04/21 , س 20:30

2 رامي متولي القاضي، مرجع سابق، ص 20

أي فعل يرتكب متضمن استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لإحكام هذا النظام (م1 من نظام مكافحة الجرائم المعلوماتية السعودي).

ب)– تعريف القانون الأمريكي

نص القانون الأمريكي رقم (1213) لسنة 1982 الخاص بمواجهة جرائم الكمبيوتر على تعريف جريمة الغش المعلوماتي بأنها : الاستخدام الغير صحيح لأنظمة به الكمبيوتر المحمية أو الملفات البيانات أو الاستخدام الغير صحيح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات ، وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة[1].

ج)– مفهوم جريمة الغش المعلوماتي في التشريع الجزائري

هناك عدة مفاهيم لجريمة الغش المعلوماتي من بينها:

هي جريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال و في كل عمل أو امتناع عن عمل يقوم به شخص يتمثل بإضرار بمكونات الحاسب المادية أو المعنوية ، وشبكات الاتصال الخاصة به ، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها .

أو هي استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال أو احد ملحقاتها أو برامجها في التنفيذ لأغراض مشبوهة أو أمور غير أخلاقية لا يرضاها المجتمع.[2]

كما تأثر المشرع الجزائري بغيره من التشريعات الأجنبية الأوروبية منها والعربية ، فيما يخص القواعد التي استند إليها أو اثر بها لمكافحة الجرائم المعلوماتية ، حيث اتجه إلى خلق نصوص جديدة وخاصة تتعلق بهذا النوع من الإجرام ، رغبة منه في تامين أنظمة المعلومات من اعتداءات المجرمين .

1 رامي متولي القاضي، مرجع سابق، ص 20

2 زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى ، عين مليلة ، الجزائر ، (ط) ، 2011 ، ص12

إذ نجد انه ضمن موضوع جريمة الغش المعلوماتي في قانون العقوبات أو بموجب نصوص خاصة على السواء.[1] وقد جاء المشرع الجزائري على تسمية جريمة الغش المعلوماتي بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، وتبين في ذلك التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي ، بموجب المادة الثانية من القانون 09- 04 المتضمنة القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، و عرفها على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن منظومة معلوماتية أو نظام الاتصالات الالكترونية

وبالتي تكون الجريمة معلوماتية أيضا : تلك الجرائم المرتكبة عن طريق أي نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبط ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ، والمرتكبة عن طريق أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات[2].

من خلال ما تقدم من تعريفات حول الجريمة المعلوماتية في التشريع الجزائري نستنتج موقف المشرع من هذه الجريمة ، وهذا الموقف متمثل في أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة من الإجرام ، مما دفع الكثير من الدول للنص على معاقبة هذا النوع من الجرائم ، تسعى من خلال هذا المشروع إلى توفير الحماية الجزائية للأنظمة المعلوماتية وأساليب المعالج الآلية للمعطيات ، وبالتالي قام المشرع الجزائري بتعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال وكان ذلك بموجب القانون رقم 04-1 المؤرخ في 2004/11/10 المتمم والمعدل لأمر 66/154 المتضمن لقانون العقوبات والذي اقر له القسم السابع مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ، فقد أشار المشرع الجزائري باستخدامه للمصطلح

1 ونوغي نبيل / ط , زيوش عبد الرؤوف ، الجريمة المعلوماتية في التشريع الجزائري ,مجلة العلوم القانونية والاجتماعية,جامعة زيان عاشور ,الجلفة ,الجزائر ، 2019, ص 45

2 القانون رقم 09- 04 المؤرخ في 14 شعبان 1430هـ الموافق 05اوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتمثلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، ج ر ص 47 ، الصادر بتاريخ 2009/08/16 .

للدلالة على كلمة المعلومات والنظام الذي يحتوي عليها ويخرج بذلك من نطاق تجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة ارتكابها وحصرها فقط في صور الأفعال التي في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي ، أي الجرائم التي يكون النظام المعلوماتي محلا لها.[1]

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها، وقام بحماية هذه المعطيات من أوجه عدة.

تم في مرحلة لاحقة اختيار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن لطرق مكافحتها.[2]

1 سعيد نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية ، جامعة الحاج لخضر ، باتنة ، 2013/2012 ، ص 41.

2 سعيد نعيم، المرجع نفسه، ص41.

المطلب الثاني : الطبيعة القانونية لجرائم الغش المعلوماتي

تتميز جرائم الغش المعلوماتي بطبيعة خاصة كونها ترد على معلومات وتعود هذه الطبيعة على المعلومات لكي يشملها القانون بحماية خاصة من خلال التعدي عليها،وقد اتجه الفقه إلى اتجاهين في تحديد الطبيعة القانونية فهناك من يرى المعلومات لها طبيعة من نوع خاص،في حين يرى الاتجاه الأخر أن المعلومة مجموعة من القيم المستحدثة وهذا ما سنتناوله من خلال الفرعين التاليين:

الفرع الأول: المعلومات لها طبيعة من نوع خاص

يرى جانب من الفقه أن المعلومات تعد أموال منقولة وانه يمكن تقويمها بالمال انطلاقا من القيمة الاقتصادية لها ، وبالتالي يصح أن يكون محلا للحقوق المالية وعلى الأخص حق الملكية ،على أساس انه يمكن استغلالها في تحقيق عوائد مادية أو تحسين أداء المشروعات الإنتاجية ، وبالتالي يجوز أن يرد عليها جميع أنواع التعاملات التجارية ، وتتمتع المعلومات بحماية القانون باعتبارها مال مقوم يستوي في ذلك أن تكون مبتكرة أو غير مبتكرة ، لأنها إذا كانت مبتكرة فهي محمية بمقتضى قانون حماية الملكية الفكرية ، وإذا لم تكن كذلك فهي تعد محمية طبقا للقواعد العامة في القانون المدني .[1]

ويعتبر الفقه الفرنسي إن المعلومات أموالا ذات طبيعة خاصة انطلاقا من أن غياب الكيان المادي للمعلومات لا يجعلها محلا لحق مالي من نوع الحقوق المتعارف عليها في الفقه والتي ترد على كيانات مادية ، وان جاز اعتبارها محلا لحق ملكية أدبية أو فنية أو الصناعية التي تأبى بطبيعتها عن أن تكون محلا لمثل هذه الحقوق ، يلزم بالضرورة استبعادها من طائفة الأموال وليس من مقتضى هذا الاستبعاد أن تظل هذه المعلومات عارية من أية حماية إذا ما جرى الاستيلاء عليها أو استخدامها استخداما غير مشروع ، فهذه المسؤولية تتحرك وفق قواعد المسؤولية المدنية المستندة التي نص المادة 1382 من القانون المدني الفرنسي ، وبالاعتراف بالخطأ تكون المحكمة قد اعترفت بوجود الحق وهو

1 خالد ممدوح إبراهيم, مرجع سابق, ص 20

" الحق في المعلومات " مما مؤداه أن يكون للمعلومات طبيعة خاصة تسمح بان يكون الحق الوارد عليها من نوع الملكية العلمية .

فصناعة المعلومات أصبحت هي المجال الأهم لجذب الاستثمارات خصوصا مع تحقيق التزاوج بين المعلوماتية والاتصال ، فهي تعتبر مالا لأنها ذات قيمة اقتصادية حيث تمثل مصدر حقيقي لتحقيق عائد مادي لصاحبها ، ومن ثم فإنها يمكن أن تكون محلا للتعاقد والانتقال من شخص إلى أخر ، فكل عمل إنساني مفيد ينتج فائدة اقتصادية يجب أن يتم تكييفه مالا ، ولذلك فهم يقترحون لحماية المعلومات أدوات جديدة وذلك من خلال النظرية التي ابتدعها القضاء الفرنسي وهي نظرية الأعمال الطفيلية.[1]

الفرع الثاني: المعلومات مجموعة مستحدثة من القيم

يرى الفقه الحديث أن المعلومات مجموعة مستحدثة من القيم، ويرجع الفضل في إضفاء صفة القيمة على المعلومة إلى الأستاذين VIVANT. CATALA وقد ارتكز الأستاذ CATALA إلى حجتين لإضفاء وصف القيمة على المعلومة الأولى قيمة اقتصادية مستندا لرأي الأستاذ CARBONNIER والذي يبين في دراسة صلة القيمة بدعامتها المادية ، حيث يشير إلى أن أي قانون يرفض أن يرى قيمة في شيء له أهمية اقتصادية سيبقى بمعزل عن الحقيقة ، وعليه فمن المقبول إن ينطبق وصف القيمة على المعلومة وهو كذلك ا أكده الأستاذ ZANATI في رسالته الخاصة " الطبيعة القانونية لحق الملكية

إذ يرى انه إذا ما وضع في الاعتبار الرابطة التي تجمع ما بين المعلومة ومؤلفها فيجوز الإقرار بإمكانية الحيازة للمعلومة بوصفها قيمة ، وهو ما ذهب إليه الأستاذ VIVANT وأسس رأيه على حجتين الأولى مستمدة من رأي الأستاذ RIPERT PILANIOL وهي أن فكرة الشيء أو قيمة معنوية ذات طابع اقتصادي تكون جديرة بالحماية القانونية ، أما الحجة الثانية وهي أن كل الأشياء المملوكة ملكية معنوية من قبيل حق الملكية والرسم والنماذج الصناعية تركز بان

1 خالد ممدوح إبراهيم, مرجع سابق, ص 21.22

للمعلومة قيمة ، والإنسان الذي يطلع المجموعة على شيء ما يصرف النظر عن الشكل والفكر فهو يقدم لهم معلومة ولكنها خاصة به ويجب أن تعامل هذه الأخيرة بوصفها قيمة وتصبح بدورها محل للحق ، وفلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية ، ويستخلص من ذلك أن المعلومة بوصفها قيمة فهي تدرج تحت القيم المستحدثة وتصبح بذلك قيمة معلوماتية وتدرج تحت الملكية التي تعتبر أنها قيمة قانونية وان الاستيلاء عليها بدون وجه حق يستوجب العقاب.[1]

المطلب الثالث: خصائص جريمة الغش المعلوماتي :

تتميز جريمة الغش المعلوماتي داخل المؤسسات أو في مجال العمل بخصائص تميزها عن الجرائم التقليدية والتي تأخذ خصائص الجريمة المعلوماتية ولعلى من أهمها ما يلي:

الفرع الأول : السمات الخاصة بجريمة الغش المعلوماتي

أ)– جريمة الغش المعلوماتي جريمة عابرة للحدود الجريمة :

جريمة الغش المعلوماتي تتسم غالبا بالطابع الدولي ذلك لان الطابع العالمي لشبكة الانترانت وما يتميز به من جعل معظم دول العالم في حالة اتصال دائم على خط ONLINE،يسهلا ارتكاب الجريمة من دولة إلى دولة أخرى ، فالجريمة المعلوماتية لا تعرف بالحدود بين الدول والقارات ولذلك فهي جريمة عابرة للقارات ، فهي تعتبر شكلا جديدا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم **مثال** : التعدي على قواعد البيانات وتزوير إتلاف المستندات الالكترونية .....الخ

فالجريمة المعلوماتية ، هي من نوع الجرائم التي يتم ارتكابها عن بعد online عبر المسافات ، حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمة عن بعد ، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر الفاعل وبين النتيجة أي المعطيات محل الاعتداء ، إن الجرائم المعلوماتية تتميز

1 محمد بن فردية ,مرجع سابق ,ص 58.59

بالتباعد الجغرافي بين الفاعل المجني عليه ، ومن جهة التقنية ، بين الكمبيوتر أداة الجريمة وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدفة بالاعتداء .[1]

ب)- جرائم ترتكب عبر شبكة الانترانت :

تعد شبكة الانترانت internet هي حلقة الوصول بين كافة الأهداف المحتملة لذلك الجرائم AIMOF CRIMES كالبنوك و الحركات الصناعية وغيرها من بالأهداف إلى ما تكون عاليا الضحية لتلك الجرائم وهو ما دعا معظم تلك الأهداف إلى اللجوء نظم الأمن الالكترونية ELECTRONIC Security Systems في محاولة منها لنحمي نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم[2]

ج)- صعوبة إثبات الجريمة المعلوماتية

فالجرائم المعلوماتية تتصف بالخفاء أي عدم وجود أثار مادية يمكن متابعتها وهي خطيرة وصعبة الاكتشاف أو هي صعبة في تحديد مكان وقوعها، أو مكان التعامل معها بسبب اتساع نطاقها المكاني وضخامة البيانات، ترجع صعوبة إثبات الجريمة المعلوماتية إلى عدة أمور منها.[3]

- أنها كجريمة لا تترك أي أثار مادية لها بعد ارتكابها
- صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية
- نحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها :

الفرع الثاني : سمات وأنماط المجرم المعلوماتي

أ)- سمات المجرم المعلوماتي:

1 خالد ممدوح ,مرجع سابق ,ص 77.78

2 خالد ممدوح ,المرجع نفسه ,ص 79

3 رامي متولي القاضي، مرجع سابق، ص 43

- **مجرم متخصص:** فقد تبت من عدد من القضايا أن عدد من المجرمين لا يرتكبون الجرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم

- **مجرم عائد إلى الإجرام:** يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخري في مجال الكمبيوتر انطلاقا من الرغبة في الثغرات إني أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة، ونودي ذلك إلى العود إلى الجرائم وقد ينهي بهم الأمر مع ذلك في المرة الثانية إلى تقديمهم إلى المحاكمة.[1]

- **مجرم محترف:** لا يسهل على الشخص الهاوي، إلا في حالات قليلة أن يرتكب جرائم بطريقة الكمبيوتر، فالأمر يقتضي كثيرا من الدقة و التخصص في هذا المجال للتواصل إلى التغلب على العقاب التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما يحدث في البنوك مثلا.

- **مجرم ذكي** : لا يمكن أن يحمي المجرم المعلوماتي إلى طائفة المجرمين الأغبياء فالمجرم المعلوماتي دائما ما ينسب بالذكاء ، ويتمتع بمهارة و قدرة فائقة على التعامل مع الحاسب الآلي وشبكات المعلومات ولديه قدرة على اختراقها ، والوصول إلى البيانات والمعلومات المطلوبة .

- **مجرم غير عفيف** : ينتمي الإجرامي المعلوماتي إلى جرائم الحيلة ، فلا يلجأ المجرم المعلوماتي إلى العنف في ارتكاب جرائمه ، هذا النوع من الجرائم لا يستلزم مقدرا من العنف للقيام به .

- **مجرم متكيف اجتماعيا** : لا يضع المجرم المعلوماتي نفسه في حالة عداء سافر مع المجتمع الذي يحيط به ، بل انه إنسان متكيف معه ، ذلك انه أصلا إنسان مرتفع الذكاء ويساعده ذلك على عملية التكييف.[2]

ب)- من حيث أنماط مجرمي المعلوماتية:

1 منير محمد الجنيمي ,ممدوح محمد الجنيدي,جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها, دار الفكر الجامعي, الإسكندرية ,2006 ص 24
2 رامي متولي القاضي، مرجع سابق، ص 44

يمكن تصنيف مرتكبي الجرائم الالكترونية على أساس أعراض الاعتداء إلى الفئات التالية : الفئة الأولى ، المحترفون وتضم نوعين من المتطفلين الهاكرز والكراكز ، أما الفئة الثانية فتشمل المحترفون ، وقد تعد الأخطر من بين مجرمي التقنية حيث تهدف اعتداء اتهم أساسيا إلى تحقيق الكسب المادي ، أو تحقيق أغراض سياسية .أما فئة الحاقدين لا يسعون إلى إثبات قدراتهم الفنية ولا إلى مكاسب مادية فما يحرك نشاطهم سوى الرغبة بالانتقام والثار من رب العمل . وهناك طائفة ظهرت حديثا هي فئة صغار نوابغ المعلوماتية أو (المد لعثمين)

- **أسلوب ارتكاب الجريمة المعلوماتية:** الطبيعة الخاصة بالجريمة المعلوماتية تبرز بصورة ممارسة في أسلوب ارتكابها[1] فإذا كانت بعض الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي يكون في صورة ممارسة العنف و الإيذاء كما هو في جريمة القتل والاختطاف مثلا ، فالجرائم الالكترونية هي جرائم هادئة ، كل ما تطلبه عدد من اللمسات على أزرار لوحة المفاتيح حتى تؤدي إلى إسقاط الحواجز الأمنية للنظم والشبكات ، حيث تحتاج إلى قدرة علمية في مجال التعامل مع جهاز الحاسوب وشبكة المعلومات الدولية "الانترنت" بما في ذلك بعض تقنيات ارتكاب هذه الجرائم كالاحتراق سواء عن طريق استعمال نظم التشغيل أو باستخدام البرامج أو عن طريق كشف كلمات السر وجمعها ، أيضا ظهرت تقنيات ألسلامي (SALAMI TECHNIQUE) أو حصان طروادة (TROIAN HORS) في ارتكاب عملية الاختلاس المالي ،و غيرها من الأساليب المتطورة التي أفرزتها التكنولوجيا . فهاته الأفعال التي تعتبر أحدث أنواع الإجرام المعلوماتي من شانها أن تضع مستقبل المؤسسة الضحية، وخاصة مستقبل علاقات العمل محل تساءل ، مما يوضح بأن جرائم الغش المعلوماتي هي اخطر بكثير من الجرائم التقليدية [2]

1 بن قارة مصطفى عائشة ,الحماية الجزائية للمجال المعلوماتي للمؤسسة من جريمة الغش المعلوماتي قارة مجلة الحقوق و العلوم السياسية ,جامعة عباس لغرور خنشلة ,العدد11 جانفي 2019, ص 115,130.

2بن قارة مصطفى عائشة, نفس المرجع ,ص 122.

الفرع الثالث : نماذج جريمة الغش المعلوماتي في العمل .

أ)– لإعطاء توضيح أكثر لمفهوم جرائم الغش المعلوماتي في العمل ينبغي تقديم نماذج عملية عن هذه الجرائم وهي كالتالي :

- عرضت قضية على أنظار القضاء الألماني : حيث تمت متابعة عامل بوكالة مكلفة بمنح تعويضات عن الأطفال ، الذي قام بإدخال بيانات مزيفة لبرامج المؤسسة المعلوماتي ، خولته تعويضات له ولإفراد عائلته مستغلا في ذلك عدة حسابات تعود لأشخاص آخرين ، فأخذ الحاسوب بصرف وتنفيذ دفعات التعويضات لهذا العامل بصفة منتظمة ، ظرف 10 أشهر قام الجاني بـ 29 استعمال معلوماتي من هذا النوع اكسبه هو وأبويه مبلغا ماليا كبيرا ، وقد تمت متابعته بتهمة خيانته الأمانة المتكررة ، وتزييف المستندات تمت متابعة أجير مكلف بعملية البرمجة المعلوماتية داخل شركة مساهمة ، والذي تمكن من إدخال بيانات إعلامية خاصة بأجور أشخاص وهميين في الشبكة المعلوماتية الخاصة بالمؤسسة ، لتحويل هاته الأجور في الأخير إلى حسابه الخاص فهذه الاستعمالات المعلوماتية الغير مشروعة على الأجور يمكن انجازها بنجاح في العديد من المؤسسات ، إلا انه من السهل اكتشافها ، لان الحاسوب ينجز وثائق وبطاقات الأداء ولوائح المراقبة وجداول محاسبية، و لأجل الحيلولة دون اكتشاف هذه الاستعمالات يعمل الجاني إلى تعديل برامج أداء الأجور ،كجعل الحاسوب لا يطبع ، وبالتالي لا تظهر هذه الأداءات على لائحة المراقبة[1]

1 بن قارة مصطفى عائشة, نفس المرجع ,ص 122

المبحث الثاني: أركان وأنواع الجريمة الغش المعلومات

لكي يصح القول بوجود جريمة غش داخل مؤسسة ما فان المشرع يتطلب وجود أركان كأي جريمة عادية التي تتكون من ثلاثة أركان : الركن المادي ، الركن المعنوي ، والركن الشرعي ، كما هو الحال بالنسبة لجريمة الغش المعلوماتي وحاليا المجال مفتوح لكل أنواع الجرائم المعلوماتية يصعب حصرها أو تعدادها نظرا لازديادها وتنوع أساليبها كما يصعب تقسيمها و من خلال هذا المبحث سنتناول في المطلب الأول أركان جريمة الغش المعلوماتي أما في المطلب الثاني سنتناول أنواع جريمة الغش المعلوماتي.

المطلب الأول : أركان جريمة الغش المعلوماتي

يقصد بأركان الجريمة عناصرها الأساسية التي يتطلبها القانون لقيام الجريمة و هي أركان خاصة التي ينص عليها المشرع بصدد كل جريمة و هي واجب توافرها أي كان نوع الجريمة كما سنتناول كل ركن على حدة.

الفرع الأول: الركن المادي

اتي النشاط أو السلوك المادي في الجريمة المعلوماتية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الانترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه والنتيجة.[1]

إن جرائم المعلوماتية تتخذ عدة أشكال تعدد بتعدد صور الاعتداء الواقعة على نظام المعلوماتية بحد ذاته والتي يمكن حصرها في :

- **الدخول والبقاء غير المرخص بهما في النظام** : ويقصد بفعل الدخول هنا وهو الركن المادي لجريمة الاعتداء على نظام المعالجة الآلية للمعطيات ، ذلك إن الدخول المعنوي أو الالكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي.

1 خالد ممدوح إبراهيم، مرجع سابق، ص 98

- **الاعتداء على المعطيات المعالجة الآلية:** ويقصد بالاعتداء هنا ذلك الاعتداء الذي يهدف إلى الإضرار بمعلومات الكمبيوتر أو طائفة سواء المساس بسير بتها أو المساس بسلامة محتوياتها

الفرع الثاني: الركن المعنوي

هو الجانب الشخصي أو النفسي للجريمة فلا تقوم ، الجريمة بمجرد قيام الواقعة المادية التي تخضع لنص التجريم بل لابد أن تصدر هذه الواقعة من إرادة فاعلها وترتبط بها ارتباطا معنويا.[1]

وعناصر الركن المعنوي القصد الجنائي وهو العلم وعناصر الجريمة وإرادة ارتكابها وهما العلم والإرادة، في الجريمة المعلوماتية.

الركن المعنوي هو الحالة النفسية للجاني والعلاقة بين ماديات الجريمة وشخصية الجاني ، حيث برزت مشكلة الركن المعنوي في الجريمة المعلوماتية في قضية موريس الذي اتهم في دخول غير مصرح به على جهاز الحاسب الفيدرالي وقدم محامي موريس على انتفاء الركن المعنوي الأمر الذي جعل المحكمة تقول هل يلزم أن يقوم الادعاء بالثبات القصد الجنائي في جريمة الدخول الغير مصرح به حيث تبث نية المتهم في تحدي الخطر الوارد على استخدام نضم المعلومات في الحاسب وتحقيق خسائر

أما بالنسبة للقضاء الفرنسي فان منطق سوء النية هو الأهم في الجرائم الالكترونية ، حيث يشترط المشرع الفرنسي وجود سوء النية في الاعتداء على بريد الالكتروني خاص بأحد الأشخاص أما المشرع الجزائري فقد نص في 394مكرر 2 من جريمة المساس بأنظمة المعالجة الآلية ،على انه كل من يقوم عمدا وعن طريق الغش ، وهنا فقد تحقق عنصر العلم والإرادة.[2]

1 عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزائر، الطبعة السادسة، 2005، ص 65.

2 قانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016 المعدل والمتمم للأمر رقم 66 – 156 المتضمن قانون العقوبات و المؤرخ في 8 يونيو 1966

الفرع الثالث: الركن الشرعي

الركن الشرعي يعني إقرار المشرع والنص على تجريم الفعل المرتكب وهو ما تحدث عليه م 1 من ق ع ج " لا جريمة ولا عقوبة أو تدابير بغير نص قانوني.[1]

في الجرائم المعلوماتية الركن الشرعي هو المادة القانونية التي تحدد أبعاد الجريمة وما يترتب على الإثبات بها عقاب ويكون ذالك مدرجا في قانون العقوبات ويعتبر وجوده إلزاميا إلى جانب كل جريمة وذلك وفقا لقاعدة لا جريمة ولا عقوبة دون نص قانوني ويرتكز الركن الشرعي على ركيزتان

- مطابقة الفعل لنص التجريم ويعيق تطابق الأفعال المجرمة قانونا في النصوص التشريعية الموجودة
- عدم خضوع الفعل المرتكب لسبب من أسباب الإباحة ومن هنا نرى اجتهاد المحكمة العليا ذهب إلى تطبيق نظرية العقوبة المقررة إلا انه لا بد أن يكون النص الواجب التطبيق بقرار العقوبة .2

1 أحسن بوسقيعة ،الوجيز في القانون الجزائي العام , مرجع سابق، ص 27

2 بالعليات ابراهيم ، أركان الجريمة الالكترونية وطرق إثباتها في قانون العقوبات الجزائري ، ط 1 ، دار بريتي ، للنشر ، الجزائر ، 2007 ، ص 94. 95

المطلب الثاني: أنواع جرائم الغش المعلوماتي

حاول عديد الفقهاء ، تحديد أنواع الجرائم المعلوماتية وذلك لصعوبة حصر هذه الأنواع بصفة مميزة ويرجع ذلك لحداثة ظهور هذه الجريمة وكذا عدم وجود تعريف عام متفق عليه للجريمة المعلوماتية وتحديد مجالها وكذا بالنظر للتطور التكنولوجي في كل صورة للارتباط الوثيق بينهما فبعضهم يقسمها إلى جرائم ترتكب على نضم الحاسب الآلي وأخرى ترتكب بواسطة وبعضهم يصفها ضمن فئات بالإسناد إلى أسلوب المتبع في الجريمة ، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء ، وكذا تعدد الحق المعتدي عليه ، فتوزع الجرائم المعلوماتية حسب هذا التقسيم إلى جرائم تقع على الأموال وجرائم تقع على الأشخاص ونجد هذا التقسيم الشائع من خلال الدراسات والأبحاث الأمريكية ، ويلاحظ انه يقوم على فكرة الغرض النهائي أو المحل الذي يستهدف الاعتداء.[1]

الفرع الأول : الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

هذا التصنيف هو الأهم حيث يشمل الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي في هذه الطائفة من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا بجسامتها ويهدف الجاني عادة من وراء ارتكاب هذه الجرائم لتحقيق ربح مادي بطريقة غير مشروعة.[2]

إذ تهدف هذه الجرائم الاعتداء على أموال الغير ،فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته أو برامجه أو نظمه كوسيلة لتنفيذ الجريمة

أ)- الجرائم المعلوماتية الواقعة على الأشخاص :

هي الجرائم التي تتمثل بالاعتداء أو التهديد بالخطر على الحقوق ذات الطابع الشخصي البحث، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي ومن أهم هذه الحقوق الحق في الحياة والحق في سلامة الجسم.

---

1 يونس عرب ، دليل امن المعلومات والخصومة جرائم الكمبيوتر والانترنت, إصدار اتحاد المصارف العربية, الجزء الأول, بيروت، 2001 ، ص 15 .

2 نائلة عادل محمد فريدة قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية ، منشورات الجنائي الحقوقية ، الطبعة الأولى ، 2005 ، ص 265 .

ب)- الجرائم المعلوماتية الواقعة على الحياة الخاصة :

لقد كفلت جل الدول الحياة الخاصة لمواطنيها بالحماية وقد حذا الدستور الجزائري حذو الدساتير الدولية بحرصه على حماية الخاصة للمواطنين لموجب المادة 46 من أخر تعديل دستوري مؤرخ في 06 مارس 2016 والتي تنص على:

" لا يجوز انتهاك حرمة حياة الموطن الخاصة وحرمة شرفه ويحميها القانون.

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة " [1]

ولا شك أن الحاسبات الآلية لها من قدرة فائقة على تخزين اكبر كم ممكن المعلومات أصبحت مخزنا هاما للمعلومات وأكثر حساسية المتعلقة بالأفراد والأهمية المعلومات التي تحتويها أنظمة الحاسبات الآلية أصبح له لهذه الحسابات دورا هاما في تسهيل الحصول على المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة.[2]

الفرع الثاني: الجرائم المعلوماتية الواقعة على النظام المعلوماتية الأخرى

يقتصر هذا النوع من الجرائم في غالب الأحيان على الولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أذلة الكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها.

- **الولوج غير المشروع للمعلومات المعالجة آليا:**

هنا يكون المجرم المعلوماتي داخل احد المراكز المعلوماتية بهدف الولوج إلى المعلومات التي تمت معالجتها أليا والاطلاع عليها من دون تصريح وقد يكون هذا الولوج إما مباشرا أو غير مباشر فأما الولوج المباشر فيعد من أكثر الأفعال المرتكبة وأسهلها تنفيذا ويتخذ عدة صور إذا يستطيع الجاني الاستيلاء على المعلومات المخزونة لدى الأنظمة المعلوماتية بحدة طرف باستخدام آلة الطباعة أو

1 نص المادة 46 من الدستور الجزائري

2 نائلة محمد عادل فريد قورة ، مرجع سابق ، 275.

استخدام شاشة النظام آو الاطلاع على المعلومات بالقراءة على ما هو مكتوب عليها أو باستخدام مكبر الصوت.[1]

- **أما الولوج الغير مباشر**

هو عبارة عن تقنيات مستحدثة لها صلة بالنظام المعلوماتي كالمعالجة عن بعد إذ أن هذه التقنيات أدت إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للدخول أو الاستفسار عن بعد من مراكز المعلوماتية ، إذ انه أثناء حركتها وبثها تكون مهددة للالتقاط والتسجيل غير المشروعين في كل لحظة كتوصيل خطوط تحويلية لالتقاط المعلومات المتواجدة ما بين النظام المعلوماتي والنهاية الطرفية و إرسال المعلومات المختلفة إلى النهاية الطرفية عن طريق إشارات الكترونية أو الدخول غير المشروع عن طريق نهاية طرفية بعيدة عن طريق نظام معلوماتي ومعرفة كلمة السر أو مفتاح الشفرة المناسب.[2]

- **إساءة استخدام البطاقات الائتمانية**

أدى استخدام النظام المعلوماتي في العمليات المصرفية والبنكية إلى ظهور نوع جديد من الجرائم المعلوماتية ويعد هذا من الجرائم من اخطر الجرائم المعلوماتية لا سيما في المجتمعات التي تتسم نظامها البنكي بدرجة عالية التطور والحداثة ، ويتخذ هذا النوع صورتين

– إساءة استخدام العميل لبطاقات الائتمانية وذلك عن طريق عدم احترام شروط العقد المبرم بينه وبين البنك كان يستعمل بطاقة ائتمانية انتهت مدة صلاحيتها أو بطاقة تم إلغاؤها أو شراء بأكثر من قيمتها

1 احمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي ,الإسكندرية، الطبعة الثانية ، سنة 2006 ، ص 190

2 احمد خليفة الملط ، المرجع نفسه ، ص 192

– إساءة استخدام الغير البطاقات الائتمانية كان يقوم سارق باستعمال البطاقة الائتمانية للحصول على السلع والخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة (01)

ج)– الجرائم المعلوماتية الواقعة على الأسرار :

إفشاء الأسرار باستعمال النظام المعلوماتي سواء كانت أسرار عامة تخص مصالح الدولة ونظام الدفاع عنها أو أسرار خاصة تتعلق بالأفراد أو المصالح الاقتصادية للمؤسسات المختلفة أو كما يطلق عليها أسرار مهنية وهنا تكون أمام نوعين من الجرائم 1

الأولى تقع على أسرار الدولة والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية . وتقع هذه الجريمة لسرقة معلومات قصد التشهير بشخص أو جماعة معينة أو بيعها لتحقيق مصالح ي كالحصول على عائد مادي ممن يهمه الأمر أو يستخدم للضغط على أصحابها من اجل القيام بعمل أو الامتناع عن القيام بعمل.

لقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 إلى 96 مكرر من قانون العقوبات بالإضافة للمادة 394 مكرر من قانون العقوبات التي نصت " تضاعف العقوبات المنصوص عليها في هذا القس ماذا استهدف الدفاع الوطني أو الهيئات والمؤسسات الخاصة للقانون العام ، دون إخلال بتطبيق عقوبات اشد" وبذلك قد يكون حدا حذو مختلف التشريعات الأول.2

1 احمد خليفة الملط / المرجع السابق ، ص 196

2 الأمر 66 /156المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم بتاريخ 2 غشت 2011 . القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الإلية للمعطيات.

الفرع الثالث : الجرائم المعلوماتية الواقعة على النظام المعلوماتي

هناك نوع آخر من الجرائم المعلوماتية بالاعتماد على التصنيف الذي يقوم على المحل الجريمة المعلوماتية يتمثل في الجرائم الواقعة على النظام المعلوماتي الذي قد تستهدف إما المكونات المادية للنظام أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي

أ)- جراء الاعتداء على المكونات المادية للنظام المعلوماتي

يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة والمعدات الملحقة بها والتي تستخدم في تشغيله كالاسطوانات والشرائط .....الخ

فالاعتداء عليها يكون عن طريق عادية وتقليدية.[1] كأن محلا للسرقة أو خيانة الأمانة أو الإتلاف العمدي وإفساد اسطوانات التشغيل مغناطيسيا بتعريضها إلى أي مجال مغناطيس متلف ويترتب على هذا الإتلاف خسائر كبيرة.[2]

ومن أمثلة ما حدث في فرنسا حيث أدى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيق المعلومات الحساسة إلى خسائر مالية معتبرة

ب)- جرائم الاعتداء على المكونات المنطقية (البرامج)للنظام المعلوماتي

هذا النوع من الجرائم المعلوماتية يستلزم معرفة فنية عالية في مجال البرمجة، وقد تقع هذه الجرائم إما على البرامج التطبيقية أو على برامج التشغيل

- **الجرائم المعلوماتية الواقعة على البرامج التطبيقية**

- **تعديل البرامج:** ويهدف من وراء تعديل هذه البرامج في اختلاس النقود وتكتر هذه الجرائم في مجال الحسابات.[3] ومثال على ذلك قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل

1 ذكي ذكي أمين حسونة ,جرائم الكمبيوتر و الجرائم الأخرى في المجال التكنيك المعلوماتي ,المؤتمر السادس للجمعية المصرية للقانون الجنائي, القاهرة 1993 في الفترة من 25 إلى 28 أكتوبر 1993 تقرير مصر ,ص 471

2 Rose (Philippe), op, cit, p58 .59

3 احمد خليفة الملط ، المرجع السابق ، ص 173 .

برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم zzwiek وحصل على اثر ذلك على مئات الدولارات كل شهر مكان من الممكن أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وأخر عميل له ليكشف عدم وجود ما يدعى zzwiek.[1]

- **الجرائم المعلوماتية الواقعة على برامج التشغيل** : برامج التشغيل هي تلك البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام وهي طريقة تزويد البرامج مجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي.[2]

و تأخذ هذه الجرائم شكلين

أ) المصيدة : هي إعداد المبرمج ببرامج به أخطاء وعيوب عمدا ،فلا يكتشف بعضها عند استخدام البرامج ، إذ يترك المبرمج ممرات خالية وفواصل وفراغات في البرامج كي يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال إضافات و إحداث مخارج وسيطة للولوج داخل النظام المعلومات والوصول إلى كل المعلومات التي تحتويها الذاكرة وبذلك يصبح هو المهيمن على النظام وعلى صاحب العمل المعتدي عليه.[3]

ب) تصميم برنامج وهمي : هنا يقوم المبرمج بوضع برنامج يصعب اكتشافه مختص لارتكاب الجريمة ومراقبة تنفيذها وكمثال على ذلك قيام إحدى شركات التامين الأمريكي في مدينة لوس انجلوس بواسطة مبرمجيها تصميم برنامج وهمي يقوم بتصنيع وثائق تامين لأشخاص وهميين بلغ عددهم 46000 لهدف تقاضي هذه الشركة من اتحاد شركات التامين عمولات من نظيرتها.[4]

1 Duteroy r et Rocco (a ; m) l'informatique

2 احمد خليفة الملط ، المرجع السابق ، ص 175

3 محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، 1994، ص82.

4 Equity fuding life insurence l'informatique nouvelle ; naï 1976

ج) جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي :تعتبر المعلومات المعالجة أليا أساسيا في النظام المعلوماتي ولها قيمة اقتصادية ، وهي تعد هدف لجرائم المعلوماتية من خلال التلاعب فيها عن طريق إتلافها

د) التلاعب في المعلومات : يمكن التلاعب في المعلومات الموجودة داخل النظام المعلوماتي بشتى الطرق إما مباشر أو غير مباشر يتم التلاعب المباشر عن طريق إدخال معلومات لمعرفة المسؤول عن القسم المعلوماتي ويأخذ هذا التلاعب عدة صور كضم مستخدمين غير موجودين بالعمل لا سيما المنشات التي لها عدد كبير من العاملين المؤقتين ودائمي التغيير بهدف الحصول على مرتباتهم عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي.[1] ومن ناحية أخرى هناك تلاعب الغير مباشر يكون عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام احد وسائط التخزين أو بواسطة أو بالتلاعب عن بعد باستخدام أدوات معينة ومعرفة أرقام وشفرات الحسابات كما يكون التلاعب باستخدام الجاني لكلمة السر أو مفتاح الشفرة أو أداة ربط بالمركز المعلوماتي لأي جهة والحصول على المنفعة المراد تحقيقها .

د) إتلاف المعلومات المخزنة : تهدف هذه الجريمة إلى إتلاف المعلومات المخزنة في النظام المعلوماتي ويكون إما عادي كالحريق أو ضرب أو التكسير أو السرقة أو عن طريق استبدال المعلومات أو محوها ويكون استبدال المعلومات نوع من الجرائم الغش أو التزوير المعلوماتي وهو على درجة كبيرة من الخطورة لأنه في حالة نجاحه يستمر لمدة طويلة قبل اكتشافه ويتولد عنه مكاسب كبيرة بمجرد استبدال رقم باخ راو إحلال رقم مكان أخر.[2]

[1] احمد خليفة الملط ، المرجع السابق ، ص 179.

[2] احمد خليفة الملط ، مرجع سابق ، 180

ملخص الفصل الأول:

يمكن القول في هذا الفصل بأننا تطرقنا إلى مفهوم جريمة الغش المعلوماتي من الجانب الفقهي والتشريعي وقد انقسم الجانب الفقهي في تعريف الجريمة إلى اتجاهين اتجاه ضيق من مفهوم الجريمة واسند إلى اعتبار الحاسب الآلي كوسيلة لارتكاب الجريمة،أما الاتجاه الثاني (الموسع) فقد اعتبر أن الأمر لا يتعلق بالوسيلة في حد ذاتها وإنما يرجع إلى محل الجريمة وهي التي يكون محلها أو موضوعها المعلومات أما الاتجاه الثالث يرى أن جريمة الغش المعلوماتي هي التي تقع على الحاسب الآلي أو نظامه المعلوماتي ولا يكون الحاسب الآلي أداة لارتكابها،أما بخصوص التعريفات التشريعية نرى عدم التوصل إلى تعريف جامع مانع لتعريف جريمة الغش المعلوماتي على غرار المشرع السعودي والأمريكي الذي أشار نوعا ما إلى تعريف الجريمة ،أما المشرع الجزائري فقد تأثر بمختلف التشريعات العربية والغربية واخذ بعدة تعاريف نجدها ضمن موضوع الجريمة المعلوماتية في قانون العقوبات إذ نجد تسمية جريمة الغش المعلوماتي بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وجاء تعريفها بموجب المادة الثانية من ق 09/04 المتضمنة القواعد الخاصة بتكنولوجيا الإعلام والاتصال ومكافحتها وعرفها بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات،أما بخصوص خصائص الجريمة يتضح أن هناك سمات تتعلق بالجريمة في حد ذاتها وسمات تتعلق بالمجرم المعلوماتي،وعلى غرار جميع الجرائم نجد أن الجريمة المعلوماتية مثل باقي الجرائم و لإنساب الفعل أو (الجرم) إلى صاحبه يجب توفر الأركان الثلاثة لقيام الجريمة (المادي،المعنوي،الشرعي) إلى جانب القصد الجنائي.

الفصل الثاني:

طرق إثبات جريمة الغش المعلوماتي والجزاءات المقررة لها

بعد التطرق إلى ماهية جريمة الغش المعلوماتي من خلال تعريفها و خصائصها وأركانها وأنواعها وككل الجرائم الأخرى أن لكل جريمة من هذه الجرائم عقاب وحماية قانونية ولقد ارتأينا في الفصل الثاني هذا أن نقسمه إلى قسمين أي مبحثين:

المبحث الأول طرق آليات هذه النوع من الجرائم كونها جرائم مستحدثة ومعقدة ليست كالجرائم العادية وهي مرتبطة بالجانب التكنولوجي والحاسب الآلي ومن هنا وجب اتخاذ طرق خاصة للكشف عنها أما في المبحث الثاني نتكلم عن الحماية القانونية للجرائم المعلوماتية في ظل القوانين الداخلية منها قانون الملكية الفكرية وقانون العقوبات والقانون 09-04.

المبحث الأول : طرق و آليات إثبات جريمة الغش المعلوماتي

إن الإثبات الجنائي هو احد الموضوعات الهامة لهذا الموضوع،فقد تأثر بدوره بالتطور الهائل الذي لحق الأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة،الأمر الذي يتعين معه تغيير النظرة إلى طرق الإثبات الجنائي لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية.

فإثبات الجرائم التي تقع على العمليات المعلوماتية باستخدام الوسائل الالكترونية سيتأثر بطبيعة هذه الجرائم،وبالوسائل العلمية التي قد ترتكب بها،مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها،وعدم الوصول إلى الجناة المرتكبين لها أو تعذر وسائل إثباتها. و هذا ما سنحاول التطرق إليه من خلال مطلبين : المطلب الأول طرق جمع الأدلة التقليدية أما في المطلب الثاني فتناولنا طرق جمع الأدلة الحديثة.

المطلب الأول: طرق جمع الأدلة التقليدية

تكمن مشكلة البحث في مدى الصعوبة التي تواجهها إجراءات التحقيق في هذا النوع من الجرائم و المتمثلة في إخفاء الجريمة و سهولة و سرعة محو أو تدمير أدلة أو معالم الجريمة وتبرز هذه الصعوبات في مسائل جمع الأدلة من المعاينة و التفتيش و الضبط و غيرها من الإجراءات كون أن

جريمة الغش المعلوماتي ذات طابع عالمي لما تمتاز هذه الجريمة التي تتجاوز عنصر الزمان و المكان و هذا ما سنتناول من خلال الفروع التالية من طرق جمع الأدلة الخاصة بهذه الجريمة

الفرع الأول: المعاينة

معاينة مسرح الجريمة المعلوماتية : يقصد بالمعاينة فحص مكان أو شيء أو شخص له علاقة بالجريمة واثبات حالته، كمعاينة مكان ارتكاب الجريمة ، أو أداة ارتكابها أو محلها أو معاينة جسم أو ملابسة الجاني أو المجني عليه لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من تمزق أو ثقوب هذا ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية ومرد ذلك إلى :

- إن الجرائم التي تقع على نضم المعلومات قلما يترتب على ارتكابها أثار مادية
- إن عددا كبيرا من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة ارتكاب الجريمة واكتشافها مما يهيئ الفرصة لحدوث تغيير أو إتلاف أو عبت بالآثار المادية. [1]

كما يمكن تعريفها بأنها إجراء من إجراءات الاستدلال ، أو التحقيق ليقوم بها أشخاص محددون في القانون (ضباط الشرطة القضائية ، والنيابة العامة أو قضاة التحقيق) بغية المحافظة على مسرح الجريمة واستخلاص الأدلة منه ، في سبيل التوصل لإثبات الجريمة.

وتختلف المعاينة في إطار قانون الإجراءات الجزائية عنها في إطار القانون المدني ، فيتولى إجراؤها الخبير أو المحضر القضائي كما يمكن للقاضي أيضا إجراء المعاينة بنفسه وهذا طبقا للمادة 146 من ق .إ.إ الجزائري، [2] إما في إطار الجرائم فإن المعاينة تتولاها النيابة العامة وقضاة التحقيق وهو ما يتضح من خلال المادة 79 من ق.إ .ج الجزائري. [3]

---

1 الشحات إبراهيم محمد منصور ، الجرائم الالكترونية في الشريعة الإسلامية والقوانين الوضعية ، دار الفكر الجامعي ، الإسكندرية ، 2011، ص 195.

2 أنظر قانون الإجراءات المدنية والإدارية الجزائري ، المادة 146

3 أنظر قانون الإجراءات الجزائية ، المادة79

وتكمن أهمية المعاينة في أمرين الأول جمع الأدلة الناتجة عن الجريمة (أثار الجريمة) والثانية وقوف المحقق بنفسه على مسرح الجريمة لتتكون لديه فكرة واضحة عن كيفية وقوع الجريمة ، وبهذا توصف المعاينة بأنها دليل مباشر تفوق في أهميتها اعتراف المتهم إذا هي أقوى الأدلة الجنائية التي يطمئن إليها المحقق لكونها لا تكذب ولا تحابي وتعبر عن الواقع تعبيرا صادقا.

والمعاينة رقم أهميتها ليست لازمة في كل الجرائم ، فهي ليست إجراء تلقائي في مباشرتها بل إجراء هادف غايته الكشف عن العناصر المادية التي تتعلق بالجريمة فإذا انعدم ذلك الهدف كما هو الحال في جريمة السب مثل لم يكن ثمن مجال لإجراءاتها.[1]

الفرع الثاني : التفتيش في مجال جريمة الغش المعلوماتي.

كما تعودنا فإن مهمة التعريف غير منوط بالمشرع الجزائري و الذي اكتفى في هذه الحالة بالتطرق إلى انه إجراء من إجراءات التحقيق الأمر الذي استلزم منا دراسة أهم ما ورد عن رجال الفقه القانوني ، فبعض منهم عرف التفتيش بقوله " التفتيش احد إجراءات التحقيق والمسعى من اللجوء إليه هو ضبط الأدلة وما يتعلق بالجريمة حتى يتم نسب الجرم إلى فاعله وإنصاف صاحب الحق . وكذلك فعل الدكتور علالي عبد الله أحمد "التفتيش إجراء من إجراءات التحقيق هدفه جمع الأدلة المتعلقة بجناية أو جنحة في محل يتمتع بحرمة المسكن ويسعى المحققون من خلاله نسب الجرم لمرتكبه " وهو تعريف أدرج عمارة حرمة المسكن وكان الأصح في نظرنا لو كانت العبارة ينتهك خصوصية الشخص ولا يقتصر الأمر فقط على المسكن لان الجرائم قد ترتكب في محل آخر غير المسكن كمحل المعدل ، والذي يكون الشخص خصوصية فيه بعدم الغلق ليتصرف بحريته في عد أرباحه والبضائع ....الخ.

بينما التفتيش في جرائم المعلوماتية يمكن القول بخصوصه انه " إجراء من إجراءات تحقيقها وتقوم به سلطة مختصة بهذا المجال " مجال المعلوماتية " للدخول إلى نظم المعالجة الآلية للبيانات بما

1 محمد حماد الهيتي ، التحقيق الجنائي والأدلة الجريمة ، الطبعة 1 ، دار المناهج للنشر عمان 2010 ، ص 75 .

تشمله من مدخلات ومخرجات بحثا عن أثار الجرم التي قد يخلفها الفاعل كل هذا لتجميع الأدلة ضده وبالتالي نسب الجرم له ".[1]

أ)– مدى قابلية مكونات وشبكات الحاسب الآلي التفتيش

- **المكونات المادية للحاسب الآلي ومدى خضوعها للتفتيش:** يجمع الفقهاء على أن مكونات الحاسب المادية تصلح أن تكون محلا للتفتيش ، بحثا عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع الإجراءات القانونية الخاصة بالتفتيش ، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هو من الأماكن العامة أو من الأماكن الخاصة ، حيث أن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش ، فإذا كانت موجودة في مكان خاص لمسكن المتهم أو احد ملحقاته كان لها حكمة فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانونا في التشريعات المختلفة مع مراعاة التمييز بين ما إذا كانت مكونات الحاسب المراد تفتيشها منعزلة عن غيرها من الحاسب الأخرى ثم إنها متصلة بحاسب آلي أخر وبنهايته ظرفية في مكان أخر كمسكن غير المتهم مثلا ، أما إذا كانت موجودة في أماكن عامة سواء كانت عامة بطبيعتها كالطرق العامة والميادين والشوارع ، أو كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة ، فإن تفتيشها لا يجوز إلا في الحالات التي يجوز فيها تفتيش الأشخاص.[2]
- **المكونات المنطقية للحاسب الآلي ومدى خضوعها للتفتيش** : أثار تفتيش المكونات المنطقية للحاسب الآلي خلافا كبيرا في الفقه بشأن جواز تفتيشها ، فذهب رأي إلى جواز ضبط البيانات الالكترونية بمختلف أشكالها ، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي شيء فان ذلك يجب تفسيره بحيث يشمل بيانات الحاسب الآلي المحسوسة بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو

1 فيصل نسيغة ، عبير بعقيقي ، الإثبات في الجرائم المعلوماتية على ضوء القانون 09/04 ، المجلد 9 ، العدد 2 جوان 2018، ص 34- 49.

2حسنين بن سعيد الغافوري ، السياسة الجنائية في مواجهة جرائم الانترنت ، دراسة مقارنة ، دار النهضة العربية ، 2009 ص 476.

غير ملموسة ، وذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن التفتيش الحاسب الآلي لابد أن يشمل " المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي ".

بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب.

وذلك نجد أن القسم 94 من قانون الإجراءات الجنائية الألمانية ينص على الأدلة المضبوطة يجب أن تكون ملموسة ، وهي على هذا النحو تشمل ليس فقط نظم الحاسب بل أيضا الدعامات التي تحمل عليها البيانات ويترتب على ذلك أن البيانات منفردة عن الدعامات لا تعد أشياء لكي يمكن ضبطها ، ولكن إذا تم طبع هذه البيانات فإن مطبوعاتها تقدمن الأشياء الملموسة وبالتالي يمكن ضبطها.

وفي رومانيا فإن التفتيش والضبط ينصب على الدعامة المادية المدون ، بيانات الحاسب كالأشرطة المغناطيسية آو الأقراص، أما البيانات فلا يتم ضبطها ، ونفس الأمر في اليابان حيث إن السجلات الالكترومغناطسية تكون غير مرئية و من تم لا يمكن ضبطها إلا إذا حولت إلى صورة مرئية عن طريق مخرجات الحاسب مثل الطابعة وبهذا المفهوم أخد كل من الفقه في البرازيل والمجر وفنلندا وفرنسا ، حيث أن بعض الفقهاء يرون أن النبضات المغناطيسية والإشارات الالكترونية لا تعد من قبيل الأشياء المادية وبالتالي لا تكون مثلا للتفتيش .[1]

ومن التشريعات العربية التي أجازت صراحة التفتيش في نظم المعالجة الآلية للبيانات القانون الأردني في نص المادة 1/31 من ق.إ.ج . وجاء فيها العدلية : " مع مراعاة الشروط والأحكام المقررة في التشريعات ذات العلاقة يجوز لموظفي الضابطة العدلية الدخول إلى أي مكان يشتبه باستخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل المشتبه في استخدامها ....."."[2]

1 حسين عبد الغافوري ، مرجع سابق ، ص 477, 479

2 رامي متولي القاضي، مرجع سابق، ص 96.

أما المشرع الجزائري فتناول هذا الإجراء في المادة 11 من القانون 09- 04 المؤرخ سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها في الفصل الثالث المادة 05 بعنوان القواعد الجزائية تفتيش المنظومات المعلوماتية ، حيث أشارت المادة إلى انه يجوز للسلطات القضائية المختصة ولضباط الشرطة القضائية في الحالات المنصوص عليها في المادة 04 من هذا القانون التفتيش ولو عن بعد في منظومة معلوماتية أو معطيات معلوماتية مخزنة فيها ، منظومة تخزين المعلوماتية . وهنا إشارة صريحة إلى التفتيش في المكونات المعنوية للحاسب.[1]

- **مدى قابلية شبكات الحاسب للتفتيش** : تعرف الشبكة المعلوماتية بأنها مجموعة مكونة من اثنين فأكثر من أجهزة الحاسوب والمتصلة يبعضها البعض اتصال سلكيا أو لا سلكيا . و قد تكون الأجهزة موجودة في نفس الموقع وتسمى بالشبكة المحلية وقد تكون موزعة في أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف وتسمى بالشبكة بعيدة المدى. ومع التطور التكنولوجي لثورة الاتصالات لم يعد نطاق الاتصالات محدودا في إقليم دولة واحدة، بل امتد ليشمل كل أرجاء العالم بعد ظهور شبكة انترنت.[2]

والتي هي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسبية المتصلة مع بعض بطريقة لا مركزية ، ويدخل في تركيب هذه الشبكة ملايين الحواسب الموزعة عبر مختلف دول العالم .

كما أن طبيعة التكنولوجيا الرقمية قد عقدت من التحدي أمام أعمال التفتيش والضبط. فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدا تماما عن الموقع المادي للتفتيش ، فقد يكون الموقع الفعلي للشبكات داخل اختصاص قضائي آخر وحتى في بلد أخر والتي بواسطتها تخضع الجريمة المعلوماتية للقانون الإجرائي الخاص بتلك المنطقة ، وتستطيع أن تميز في هذه الصورة بين احتمالين على النحو التالي :

- اتصال حاسب المتهم بحاسب أخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة : يثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم ؟

---

1 قانون رقم 09- 04 السالف الذكر

2علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت ، عالم الكتب الحديثة ، الأردن2004 ، ص 148

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخري في مجال الكمبيوتر انطلاقا من الرغبة في الثغرات إني أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة، ونودي ذلك إلى العود إلى الجرائم وقد ينهي بهم الأمر مع ذلك في المرة الثانية إلى تقديمهم إلى المحاكمة.[1]

ويعتبر المشرع الجزائري من بين التشريعات حيث نصت الفقرة الثانية في المادة 05 من ق 09- 04 بأنه في حالة التفتيش منظومة معلوماتية أو جزء منها.[2]

وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وان هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة غلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك .[3]

كما نجد إلى جانب المشرع الجزائري المشرع الألماني في المادة 103 من ق. إ . ج الألماني ينص على إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر والمشرع الفرنسي حسم هذه المسألة أيضا بمناسبة تعديله ق.إ.ج بموجب القانون 239/ 2003 المتعلق بالأمن الداخلي الصادر في 2003/03/18 الذي أجازت المادة 17 منه لضباط الشرطة القضائية أو تحت مسؤولياتهم أعوان الشرطة القضائية في إطار التفتيش المنصوص عليه الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي فيها التفتيش على المعطيات التي تهم التحقيق والمخزنة في النظام المذكور أو في نظام معلوماتي آخر.[4]

❖ اتصال حاسب المتهم بحساب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة وهنا من المتصور طبقا لهذا الاحتمال أن يقوم مرتكبو الجرائم بتخزين بياناتهم في أنظمة معلوماتية خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف وعرقلة سلطات التحقيق في جميع الأدلة ، وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من

1 منير محمد الجنيمي ,ممدوح محمد لجنيدي,نفس المرجع , ص 103

2 على حسن محمد الطوالبة ، مرجع سابق ، ص 42

3 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي, الإسكندرية, 2009، ص203.

4 Voire plus Myriam quener.joel ferry .cybercriminalité defi mondial 2 em édition .2009. p2.

وجهتها المختصة الإذن ودخوله في المجال الجغرافي للدولة أخرى . وهو ما يسمى بالتفتيش العابر للحدود، وقد يتعذر القيام به بسبب تتمسك كل دولة بسيادتها.

لذا فإن جانبا من الفقه يرى بأن التفتيش الالكتروني العابر للحدود لابد وان يتم في إطار اتفاقية خاصة ثنائية أو دولية تجيز هذا الامتداد تعقد بين الدول المعنية، وبالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في غياب تلك الاتفاقية.[1] ولمواجهة هذا الاحتمال نجد أن المشرع الجزائري قد أجاز تفتيش الأنظمة حتى ولو كانت متواجدة خارج الإقليم الوطني، وهو الوارد في الفقرة الثالثة من نص المادة 05من ق 09-04 ..... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ،فإن الحصول علها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل ولعل هذه الفقرة مأخوذ نصها من الفقرة الثانية من المادة الثانية57- 1 من ق.إ.ج الفرنسي .[2]

ومع ذلك أجازت المادة 32 من الاتفاقية الأوروبية بشأن الجرائم المعلوماتية و التي أعدها المجلس الأوربي وتم التوقيع عليها في بودابست في 2001/11/23 إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين :

الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.[3]

1حسين بن سعيد الغافري، مرجع سابق، ص 484

2 المادة 57 -2/1 من ق .إ.ج الفرنسي مضافة بموجب 2/17 من ق 2003/239 : 1و2 تبني مسبق أن هذه المعطيات مخزنة في نظام معلوماتي للموجود خارج الإقليم الوطني وانه يمكن الدخول إليها وأنها متاحة انطلاقا من النظام الرئيسي فإنه يمكن الحصول عليها من طرف ضباط الشرطة القضائية مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية

3 علي حسن محمد طوالبة ،مرجع سابق ، ص47.

الفرع الثالث : الخبرة في مجال جريمة الغش المعلوماتي

الخبرة هي عبارة عن استشارة فنية يستعين بها قاضي في التحقيق لتقدير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو إدارية علمية لا تتوفر لدى قاضي التحقيق بحكم تكوينه.[1]

ولقد نص المشرع الجزائري على الخبرة في المواد من 143إلى 156 من ق.إ.ج و تنص المادة 143 على أنه : " الجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع في أن تأمر بندب خبير إما بناء على طلب النيابة العامة أو من تلقاء نفسها أو من الخصوم ،وإذا رأى قاضي التحقيق انه لا موجب الاستجابة لطلب الخبرة فعلية أن يصدر في ذلك أمرا مسببا في اجل 30 يوما من تاريخ استلامه الطلب.[2]

كما أن تطورات التكنولوجيا وتعددها في مجال الحسابات الرقمية و الوسائل التكنولوجية الفنية وتعدد وسائل الاتصال الحديثة ودور الانترنت كقوة مؤثرة من جهة وفشل جهات التحقيق في جميع الأدلة لعدم درايتها بالدليل الفني كل هذه الأسباب أدت بالخبرة إلى أن تكون ضرورة لا يمكن الاستغناء عنها في هذا الإطار . فالخبرة التقنية في مجال الانترنت والعالم الافتراضي لا تشمل بالضرورة تلك النوعية من الخبرة الدراسة ، فالدراسات الحاسب الآلي والانترنت لا تربط بمنهج دراسي أو بحثي معين أو حتى مدة زمنية يقضيها المرء دارسا في الجامعات والمعاهد المتخصصة ، وإنما ترتبط بماهرات خاصة وبموهبة الاستعمال الحاسوب والانترنت والتعامل مع تقنية المعلومات إذ أن امهر مبرمجي نظم التشغيل حتى الآن بيل غايتس لم يكن تحصيله العلمي يتجاوز المرحلة الثانوية ، وذات الأمر ينطبق عتاة الهكرز ومخترق الأنظمة فإن أعمارهم لا تتجاوز مرحلة التعليم الثانوي والسنوات الجامعية الأولى في أحسن الأحوال .[3]

1احسن بوسقيعة ، التحقيق القضائي ، ط 6 ، دار هومة الجزائر ، 2006، ص112

2أنظر قانون الإجراءات الجزائية ، المواد قانون143إلى 156.

3 فلاك مراد، آيات الحصول على الأدلة الرقمية لوسائل إثبات في الجرائم المعلوماتية، دكتوراه علوم في القانون العام مجلة الفكر القانوني والسياسي ,العدد الخامس ، ص 214 .

أ)- **أهمية الخبرة التقنية:** يشير الفقيه الجنائي إلى أهمية الخبرة في كشف و تحقيق الجرائم المعلوماتية ، إذا تستعين أجهزة العدالة الجنائية (الشرطة والنيابة والقضاء) بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي بغية كشف الغموض في هذه الجرائم ، وتجمع أدلتها والتحفظ عليها ، ومساعدة المحقق فيها من استجلاء غموضها.[1]

خاصة في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق ، فالجرائم المعلوماتية تتعلق بمسائل فنية غاية في تعقيد . يصعب على المحقق أن يسبق طريقة فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات ، ويلاحظ أن نجاح الاستدلالات و أعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء ، فإجرام الذكاء والفن لا يكشفه إلا ذكاء وفن مماثلين ، وتبرز أهمية الاستعانة بالخبير في مجال الجرائم المعلوماتية عند غيابه فقد تعجز الضبطية في كشف غموض الجريمة لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة ، وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجمل أو الإهمال عند التعامل معه.[2]

والمشرع الجزائري لم يختلف عن هذه التشريعات حينما أشار في المادة 05 الفقرة الأخيرة من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجية الإعلام والاتصال ومكافحتها انه يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية بتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها .[3]

ب)- **شروط صحة الخبرة ومدى حجيتها:** إن الفقه الجنائي يقدر أن الخبرة تستدعي توافر ركنين أساسين هما : الركن الشكلي والركن الموضوعي فالركن الشكلي فيها يمثل التخصص والعلم

1رامي متولي القاضي، مرجع سابق، ص90

2محمد أبو العلاء عقيدة ، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية ،بدون طبعة ,ص 63

3أنظر قانون 09-04 السالف الذكر

الذي أكتسبه الخبير ، إذا يشترط في الخبير حقيقة الجمع بين العلم ذوي الاختصاص والخبرة العلمية ، فلا يكفي فقط كفاءة علمية في مجال التخصص بل يضاف إليها سنوات من أعمال الخبرة في المجال ، ومن الشروط التي درجت اغلب التشريعات على تحديدها منها ما يتعلق بالخبير ومنها ما يتعلق بتقرير الخبرة . أما فيما يتعلق بالخبير فإنه يشترط:

- اختياره من قائمة الخبراء المحددة أسماؤهم ضمن الجدول المعد مسبقا وهو ما نصت عليه المادة 144 من ق.إ. ج
- حلف اليمين القانونية ،إذا يجب لصحة عمل الخبير أداء اليمين القانونية وذلك لحمله على الصدق والأمانة في عمله وبث الطمأنينة في آرائه التي يقدمها سواء بالنسبة لتقدير القاضي او لثقة بقية أطراف الدعوى

أما الشروط المتعلقة بتقرير الخبرة فإن الخبير بعد انتهائه من أبحاثه وفحوصاته يعد تقريرا يضمنه ليتوصل إليه من نتائج بعد تطبيق الأسس والقواعد العلمية على المسألة محل البحث.[1]

ويشترط أيضا فيما يتعلق بتقرير الخبرة أن يقوم الخبير بإيداع تقريره خلال المدة المحددة له في أمر أو حكم الندب، فإن لم يودع تقريره خلال هذه المدة أجاز للقاضي استبداله بغيره ما لم يقدم الخبير طلبا بتمديد هذه المهلة وذلك نظرا لما تتسم به الإجراءات الجزائية من طابع السرعة سيما إذا تعلق الأمر بالجريمة المعلوماتية.[2]

ج)– أساليب عمل الخبير التقني:للخبير التقني في سبيل تحري الحقيقة أن يقوم بكل ما يمكن التوصل إليها. وهو في إطار القيام بعمله عليه أن يستخدم الأساليب العلمية التي يقوم عليها تخصص وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسببا بشكل منطقي وإلا تعرض حكمها للنقض. ويرى بعض المختصين أن عمل الخبير المعلوماتي في اشتقاق وتجميع الأدلة الرقمية يتم عبر ثلاث (3) مراحل :

1 خالدممدوح إبراهيم، مرجع سابق، ص 292

2 هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ,أسيوط ,مصر ، ط 1، 2001 ، ص 142-143.

- **المرحلة الأولى** : تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحسابات الخادمة التي دخل منها المجرم المعلوماتي ومحاولة إيجاد أثر له
- **المرحلة الثانية:** مرحلة المراقبة ويتم ذلك بطرق مختلفة أهمها استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع.[1]
- **المرحلة الثالثة** : فحص النظام المعلوماتي المشتبه فيه بعد ضبطه من طرف جهات التحقيق بمكوناته المادية والمعنوية لاشتقاق الدليل وتقديمه لجهات التحقيق وتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه ، وعلى الخبرة أن يتبع خطوات أساسية لجمع الأدلة ثم فحصها ومن ثم تحليلها وأخيرا كتابة النتائج المتوصل إليها في تقرير ، ويمكن إيجار هذه الخطوات في المراحل التالية :

❖ خطوات ما قبل التشغيل والفحص

- التأكد من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها
- التأكد من صلاحية وحدات نظام التشغيل
- تسجيل معطيات وحدات المكونات المضبوطة

❖ خطوات التشغيل الفحص:

- استكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز
- عمل نسخة من كل وسائط التخزين المضبوط وهذا حفاظا على الأصل أثناء الفحص المبدئي
- تحديد أسماء وأنواع المجموعات البرامجية التي لها دلالة بموضوع الجريمة
- إظهار الملفات المخبأة والنصوص المخفية داخل الصور والتي تم محوها.
- تحويل الدليل الالكتروني إلى هيأة مادية وذلك عن طريق طباعة الملفات أو تصوير محتواها أو وضعها في أي وعاء آخر حسب نوع المعطيات والمعلومات المكونة للدليل.[2]

---

1 فلاك مراد، آليات الحصول على الأدلة الرقمية، مرجع سابق، ص78

2 عائشة بن قارة، مرجع سابق، 148- 149.

الفرع الرابع: الشهادة

يقصد بالشهادة بأنها : تقرير الشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بالحواس ويقصد بالشاهد في جرائم المعلوماتية بأنه الشخص الفني صاحب الخبرة المعلوماتية والتخصص في تقنية وعلوم الحاسب الآلي وشبكاته ، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي le témoin informatique تميزا له عن الشاهد التقليدي ، ويشمل الشاهد في المعلوماتية عدة طوائف أهمها :[1]

- ❖ القائم على تشغيل الحاسب الآلي : وهو المسؤول عن التشغيل الحاسب الآلي والمعدات المتصلة به ويجب أن تكون لديه الخبرة الكبيرة في استخدام الجهاز ، كما يجب أن لديه معلومات عن قواعد كتابة البرامج .
- ❖ المبرمجون: وهم الأشخاص الذين يأخذون على عاتقهم كتابة البرامج، وينقسمون إلى فئتين.

- الفئة الأولى: هم مخططو البرامج التطبيقية ويقومون بالحصول على خصائص النظام المطلوب
- الفئة الثانية: هم مخططو برامج النظم ويقومون باختيار تعديل وتصحيح برامج النظام الحاسب الداخلية وإدخال أي تعديلات آو إضافات لها.

- ❖ مهندسو الصيانة والاتصالات : وهم المؤولون عن الأعمال الصيانة الخاصة بتقنيات الحاسب وبمكوناته وشبكات الاتصال المتعلقة به.
- ❖ المحللون: وهم الأشخاص الذين تأتي على عاتقهم مهمة التحليل بيانات نظام معين إلى وحدات مفصلة واستنتاج العلاقة الوظيفية منها
- ❖ مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية
- ❖ طاقم عمليات البيانات: الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة)

1فلاك مراد، آليات الحصول على الأدلة الرقمية، مرجع سابق، ص216.

- مهندس الصيانة الالكترونية: الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة

المطلب الثاني: طرق جمع الأدلة الحديثة

بعد الانتهاء من الإجراءات التقليدية المستعملة لإثبات جريمة الغش المعلوماتي و أما قصور هذا النوع من الإجراءات في كشف جرائم الغش المعلوماتي و إثباتها جاءت إجراءات جديدة تهدف إلى إثبات هذا النوع من الجرائم المستحدثة للحصول على أدلة تثبتها و هذا ما سنتطرق إليه من خلال الفروع الآتية

الفرع الأول: التسرب واعتراض المراسلات

تعتبر جريمة الغش المعلوماتي من بين الجرائم التي يمكن فيها اللجوء إلى إجراء التسرب أو اعتراض المراسلات إذا اقتضت ذلك ضرورة إن التحري أو التحقيق بشأنها

أ)– **التسرب**:لقد حدد المشرع الجزائري نطاق هذا الإجراء بالجرائم المذكورة على سبيل الحصر في المادة مكرر من ق. إ. ج .ج والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .[1]

- مفهوم التسرب وشروطه : لقد نظم المشرع هذا الإجراء في قانون الإجراءات الجزائية وفق ثمانية مواد من المادة 65 مكرر 11 إلى المادة 65 مكرر 18 تناول خلالها تحديد مفهوم هذا الإجراء وشروطه .

❖ مفهوم التسرب في مجال الإجرام المعلوماتي : تكون عملية التسرب في الجرائم الالكترونية بدخول ضابط أو عون شرطة إلى العالم الافتراضي وذلك عن طريق اشتراكه في محادثات أو اختراق مواقع معينة مستخدما في ذلك أسماء أوصفات وهيئات مستعارة وهمية سعيا منه للاستفادة منهم في كيفية اقتحام الباكر للموقع ، أو القيام بحلقات اتصال مع المشتبه فيهم عن طريق البريد الالكتروني.[2]

1انظر نص المادة 65 مكرر 05 و65 مكرر 11 ق. إ . ج

2 عبير بعقيقي ، فيصل نسيغة ، مرجع سابق ، ص 43.

❖ شروطه:

- الحصول على إذن مكتوب ومسبق من طرف وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية
- يتضمن الإذن الجريمة التي تبرر اللجوء للتسرب وهوية ضابط الشرطة المنسق للعملية وتحديد المادة إذ لا تتجاوز 4 أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق
- أن تكون الجريمة ضمن الجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 05 من ق.إ . ج ومن ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

ثانيا: اعتراض المراسلات: يتعلق الأمر بمسألة بالغة الأهمية كونها تشكل انتهاكا لجريمة المراسلات التي كفلها الدستور الجزائري، غير أن المشرع الجزائري قد سمح بموجب المادة 65 مكرر 05 من ق. إ. ج باعتبار المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وذلك إذا اقتضت ضرورة التحري والجريمة المتلبس بها في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.....الخ

ونلاحظ من نص هذه المادة أن المشرع الجزائري قد يسمح بهذا الإجراء في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حتى تتمكن جهات التحقيق من استخلاص أدلة الإثبات والوصول إلى الحقيقة[1].

ب)– مفهوم اعتراض المراسلات وتسجيل الأصوات والتقاط الصور :الاعتراض والتسجيل و التقاط الصور والتسرب :هي عدة تسميات يمكن اختزالها في مصطلح " المراقبة " التي لا تخرج عن كونها رقابة مشروعة لشخص أو مكان أو أحاديث أو مرسلات مكتوبة أو مسموعة أو مرئية ، نتيجة الانتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير بمباشرتها لطابع السرية التي

1 فيصل نسيغة ، عبير بعقيقي، الاثباث في الجرائم المعلوماتية على ضوء القانون 09/04 ,مجلة العلوم القانونية و السياسية ,العدد 02 ,جوان 2018 ، ص44

يكتنفها . على أن تكون مؤقتة مع اقتصارها على جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالمصرف وكذا جرائم الفساد.

- **اعتراض المراسلات:** الاعتراض يعني الاستيلاء لغته والمشرع الجزائري في المادة 65 مكرر 05 من ق.إ.ج.ج خص بالذكر المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، دون الرسائل والخطابات و المطبوعات والطرود لدى مكاتب البريد.[1]
- **التسجيل الصوتي** : يقصد به تسجيل المحدثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان خاص أو عام الحديث هو كل صوت له دلالة التعبير عن معنى و لا يشترط لغة ينتفي عنه وصف الحديث لو كان لحنا موسيقيا أو صيحات ليس لها دلالة لغوية ، أما التسجيل فيقصد به حفظ الحديث على الجهاز معد لذلك للاستمتاع إليه مرة أخرى .

وأجاز المشرع وضع الترتيبات التقنية دون موافقة المعنيين من اجل تسجيل الحديث المتفوه به في المحلات السكنية وكل توابعها كما هي واردة في قانون العقوبات و الأماكن العامة التي تعد لاستقبال العامة وكذا الأماكن الخاصة غير معدة للسكن وتستعمل لممارسة نشاطات كالمحلات التجارية و اخذ المشرع الجزائري بالمعيار الموضوعي صراحة فأجاز التسجيل الصوتي للأحاديث بصفة خاصة أو سرية في أماكن خاصة أو عامة حيث تعد طبيعة الحديث أساس الحماية الجنائية بغض النظر عن المكان الذي تجوز فيه عام أو خاص وهو المعيار الذي أخد به كل من المشرع الفرنسي والمصري .

- **التقاط الصور** : أجاز المشرع الجزائري التقاط الصور لشخص أو عدة أشخاص يتواجدون في مكان خاص ، باستخدام أساليب علمية حديثة للحد من تفاقم معدلات الجريمة ، أما

1 فوزي عمارة ، اعتراض المرسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجنائية ، مجلة العلوم الإنسانية ،جامعة منتوري قسنطينة , الجزائر , العدد 33 ، جوان 2010 ،ص 236 -237 .

أجهزة المراقبة فمتعددة ومتنوعة منها ما يتعلق بالرؤيا ، المشاهدة وتسجيل الصورة وهي تمثل انتهاكا خطيرا لحياة الأفراد الخاصة سواء في الأماكن الخاصة أو العامة .[1]

- **الشروط والضمانات المقررة لاعتراض المراسلات** : مما لا شك فيه أن أسلوب اعتراض المراسلات دون علم أصحابها بقدر ما يفيد في كشف الحقيقة و يسهل إثبات كثيرة من الغمضة كتلك المتعلقة بالجرائم المعلوماتية ، فهو من جانب آخر يمثل انتهاكا لحرمة الحياة الخاصة لأفراد واعتداء على على سرية واتصالاتهم مرسلاتهم التي كفلتها الدساتير والتشريعات العقابية .

والمشرع الجزائري في هذا الصدد أعطى لسلطات التحقيق مكنة اعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائم وإخفاء أي أثر يدل عليهم ، فمن ناحية أخرى لم يفتح الباب على مصرعيه في اللجوء إلى هذه الوسيلة بل أحاط استخدام بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في: [2]

❖ **السلطة المختصة بإجراء هذه العمليات**: طبقا للمادة 65 مكررا 5 من ق.إ.ج.ج فإنه لا يمكن لضباط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات ألا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي ، فالسلطة القضائية هي وحدها المختصة هي وحدها بإصدار هذا الإذن وهو ما يعد ضمانه لازمة لمشروعية هذا الإجراء ، ولكن السؤال الذي يطرح هنا ، إذا كان قاضي التحقيق بإمكانه أنتدب من يقوم بمثل هذه العمليات ، هل له أن ينتدب في إطار الإنابة القضائية من يتولى مراقبتها ؟

بالنظر لحداثة مثل هذه الإجراءات في ق.إ.ج.ج، فإنها نقول انطلاقا من الفقرة الرابعة من مادة 65 مكرر 5 المراقبة المباشرة لهذه العمليات ينبغي أن تبقى حكرا على قاضي التحقيق لخطورتها وتعلقها مباشرة بالحريات والحق في الخصوصية التي حماها الدستور. فلا مجال لتركها بين أيدي ضباط الشرطة القضائية تنفيذا وإشرافا ، لأن ميولات الشرطي بصفة عامة معروفة بتوجهها نحو

1 جميلة محلق، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور ق.إ.ج.ج ، مجلة التواصل في الاقتصاد والإدارة والقانون ,جامعة باجي مختار عنابة ، العدد 42، جوان 2015 ، ص 178- ص 179

2 الحماية على مستوى الدساتير أنظر المادة 46 من الدستور الجزائري التي تنص...." أن سرية المراسلات والاتصالات الخاصة بكل أشكالها محمية "والحماية على مستوى النصوص العقابية أنظر المادة 303 مكرر من ق..ا.ج.ج

البحث عن أدلة الإثبات أكثر من البحث عن أدلة النفي ، وهو ما قد يترتب عليه تجاوزات تكون ضحيتها الأولى الحريات والحرمات الخاصة .[1]

وعليه فحسب رأينا ينبغي أن لا يمس الانتداب في إطار الإنابة القضائية عملية المراقبة المباشرة لهذه العمليات، وهو ما يترتب عليه وجوب تعديل الفقرة الأخيرة من المادة 139 من ق.إ.ج.ج المتعلقة بالإنابة القضائية لكي تصبح على النحو التالي: " ولا يجوز لضباط الشرطة القضائية استجواب المتهم أو القيام بمواجهة أو سماع أقوال المدعي المدني أو المراقبة المباشرة لعمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور و التسرب "

وإذا كان المشرع خص قاضي التحقيق بالإشراف على المراقبة المباشرة لهذه العمليات، فإنه بالمقابل فيما يخص إجراءها أجاز صراحة لقاضي أن ينتدب لهذا الغرض أحد ضباط الشرطة (م) 65 مكرر 8 و65 مكرر 9 من ق.إ.ج.ج.[2]

❖ **تحديد طبيعة المراسلة ومدة الاعتراض**: طبقا للمادة 65 مكرر 7 التي نصت على انه يجب أن يتضمن الإذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصالات آو المرسلات المطلوب اعتراضها. كما استجوب المشرع أن لا تتجاوز مدة هذا الإجراء 4 أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق

❖ **محضر العمليات** : استجوب المشرع الجزائري في المادة 65 مكرر 9 على ضابط الشرطة القضائية المأذون له أو المناب من طرف قاضي التحقيق المختص أن يحرر محضرا عن كل عملية اعتراض و تسجيل مراسلات و كذا عن العمليات وضع الترتيبات التقنية و عمليات الالتقاط و التثبيت و التسجيل الصوتي أو السمعي البصري و يذكر بالمحضر أيضا بتاريخ و ساعة بداية هذه العمليات و الانتهاء منها.

كما اوجب عليه في المادة 65 مكرر 10 وصف أو نسخ المراسلات آو الصور أو المحادثات المسجلة و المفيدة في إظهار الحقيقة كمرفقات تودع بالملف , و تنسخ و تترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهذا الغرض.

1د فوزي عمارة، مرجع سابق، ص 238- ص239.

2 أنظر قانون الإجراءات الجزائية المادة 139

ولا يكون لهذه المحاضر قوة في الإثبات إلى إذا كانت صحيحة في الشكل طبقا للمادة 214 من ق.إ.ج الجزائري و الأدلة الواردة بها لها حجة نسبية , أي صحيحة ما لم يقدم ما يخالفها , على خلاف الأدلة الواردة بالمحاضر المنصوص عليها بالمادة 216 من قانون الإجراءات الجزائية .[1]

الفرع الثاني: التسرب واعتراض المراسلات

ألزم المشرع الجزائري مزودي الخدمات بحفظ المعطيات،وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف،وضعها في ترتيب معين،في حين اتخاذ إجراءات قانونية محتملة كالتفتيش وغيره،وقد حصر المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة،وهي المعطيات المتعلقة بحركة السير (معطيات المرور)،وهي كما عرفتها المادة الثانية من قانون 09-04 تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة،باعتبارها جزءا في حلقة الاتصال،الوجهة المرسل إليها،والطريق الذي يسلكه،ووقت وحجم ومدة الاتصال ونوع الخدمة،وفد حصر المشرع الجزائري معطيات المرور التي ألزم بحفظها في المادة 11 من القانون 04/09 وتتضمن:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها
- المعطيات التي تسمح بالتعرف على المرسل إليه،الاتصال وكذا عناوين المواقع المطلع عليها وبما أن حفظ المعطيات إجراء وقتي،واحتراما للحق في الخصوصية،فان المشرع الجزائري فرض على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها بعد سنة من تاريخ التسجيل،أن مزودي الخدمات

1 أنظر قانون الإجراءات الجزائية المادة 65 مكرر 5 .... المدة 65 مكرر 10

يعتبرون مصدرا لجهات التحقيق،للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمون بحفظها وفي نفس الوقت ملزمين بوضعها تحت تصرف هذه الجهات إذا تم طلبها .[1]

1 سعيداني نعيم , آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية ، جامعة الحاج لخضر ، باتنة ، 2013/2012 , ص 128

المبحث الثاني : الجزاءات المقررة لجريمة الغش المعلوماتي

لا بد من الاعتراف أن الإسهام في الحلول التي يجب أن تعالج موضوع الجزاءات المقررة لجريمة الغش المعلوماتي التي اقرها المشرع الجزائري في مجموعة من النصوص القانونية و هذا ما سوف نتعرف عليه في هذا المبحث من خلال المطلبين التاليين :المطلب الأول الحماية الجزائية في ظل نصوص قانون الملكية الفكرية و الصناعية أما المطلب الثاني الجزاء الجنائي لجريمة الغش المعلوماتي في قانون العقوبات.

المطلب الأول: الحماية الجزائية في ظل نصوص قانون الملكية الفكرية والصناعية

تعتبر الحقوق الفكرية و الذهنية على أنها حقوق ملكية معنوية ترد على الأشياء غير المادية, و يمكن تقسيمها إلى ثلاثة أقسام:

- حق الملكية الصناعية : و يرد على الابتكارات الجديدة و تمكين صاحبها من الاحتكار و استغلال ابتكاره قبل الكل , و هي حقوق تتعلق بابتكار جديد من حيث الشكل و المظهر الخارجي للمنتجات (الرسوم , التصميمات , النماذج الصناعية , حقوق تتعلق بابتكار جديد من حيث الموضوع كالاختراعات , حقوق ترد على شارات مميزة تمكن صاحبها من احتكار استغلال علامة تستخدم لتمييز المنشآت كالاسم التجاري.
- حقوق الملكية التجارية: و هي تتضمن ما للتاجر من حق على محله التجاري, باعتباره مال منقول.
- حقوق الملكية الأدبية و الفنية: و تعني ما للمؤلف من حق على إنتاجه الذهني في الأدب و الفنون و العلوم.[1]

و قد اعتمد المشرع الجزائري من اجل حماية المصنفات الفكرية أولا ثم عدم مخالفته للنظام العام ثانيا, و أخرى خاصة و هي وجود ابتكار جديد في المصنف أولا ثم القيام بإيداعه القانوني ثانيا.[1]

1 محمد عبد الرحيم الناغي , الحماية الجنائية للرسوم و النماذج الصناعية , دراسة مقارنة , دار النهضة العربية , القاهرة ,2009 ,ص 12.13

الفرع الأول:مدى خضوع برامج الحاسب الآلي للنصوص الملكية الصناعية:

تعتبر حقوق الملكية الصناعية من المبتكرات الجديدة كالاختراعات , و معنى الاختراع إيجاد شيء لم يكن موجودا من قبل أو اكتشاف شيء كان موجودا و لكنه كان مجهولا و غير ملحوظ ثم أبرزه في المجال الصناعي , فالاختراع الذي لا يؤذي إلى تقدم ملموس في الفن الصناعي لا يستحق براءة عنه.[2]

و لما كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ عملية لتشغيل الحاسب الآلي, فهي من هذه الزاوية تصبح قابلة للبراءة.[3]

و قد نص عليها الأمر رقم 03/07 الصادر في 2003, حيث نصت المادة الثالثة منه على الشروط الواجب توفرها حتى يحظى الاختراع بالحماية بقولها: "يمكن أن تحمي بواسطة براءة الاختراع, الاختراعات الجديدة و الناتجة عن نشاط اختراعي و القابلة للتطبيق الصناعي..." [4]

و عليه يمكن القول انه حتى يحظى أي اختراع ما بالحماية ضمن نطاق براءات الاختراع, وجب توفر شرطي الابتكار الجديد و القابلية للتطبيق الصناعي. [5]

يمكن القول إلى انه يمكن الحصول على براءة الاختراع بخصوص برامج الإعلام الآلي في حالتين:

- أن يكون البرنامج جزءا من ذاكرة الحاسوب نفسه و مثاله البرنامج المبني.

---

1 بن زيطة عبد الهادي ,حماية برامج الحاسوب ف التشريع الجزائري ,دار الخلدونية للنشر و التوزيع , الجزائر ,2007. الطبعة الأولى, ص51

2 عفيفي كامل عفيفي, جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفكرية و دور الشرطة و القانون, دراسة مقارنة,2000,ص02 ص51

3 بوعناد فاطمة الزهراء , مكافحة الجريمة الالكترونية في التشريع الجزائري , مجلة الندوة للدراسات القانونية , سيدي بلعباس, العدد 01 , 2013 , ص 68

4 الأمر رقم 07/03 الصادر في 19 يوليو 2003, المتعلق ببراءة الاختراع, الجريدة الرسمية, العدد 44

5 خثير مسعود ,الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات ,دار الهدى عين مليلة الجزائر ,2010 , ص69

– أن يكون البرنامج جزءا أي أن طلب البراءة ينصب على وسيلة صناعة جديدة, يستخدم البرنامج في تحقيق إحدى مراحلها والحماية تبقى رهينة توافر الشرطان المذكوران, مما يصعب توفره. فالمشرع الجزائري استبعد صراحة المعطيات في مجال الحماية بواسطة براءات الاختراع.[1]

طبقا للمادة 07 من الأمر رقم 03/07 التي تنص على "لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب".

الفرع الثاني: مدى إخضاع برامج الحاسب الآلي لنصوص الملكية الأدبية والفنية.

تعتبر الملكية الأدبية والفنية حق من حقوق المؤلف ، وهو حق استئثاري بمنحة القانون لمؤلف أي مصنف للكشف عنه ، كابتكار له أو استنساخه أو توزيع أو نشره على الجمهور الإذن للغير باستخدامه أو توزيع أو نشره على الجمهور ، الإذن للغير باستعماله على وجه محدد.[2]

وقد انقسم الفقه إلى طريقتين هما:

يرى أن برنامج الحاسب الآلي مصنفة ضمن قانون حق المؤلف وانه لا حاجة لتعديل النصوص التقليدية في قانون حق المؤلف، باعتبار برامج الحاسب الآلي ما هي إلا طلاق مختلفة للتعبير عن الأفكار الإنسانية وهو مثل سائر المصنفات.

أما الاتجاه الآخر أفرز برامج الجانب الآلي الصفة المميزة عن سائر المصنفات الأخرى المحمية بموجب قانون حماية حق المؤلف ، وتبني هذا التوجه العديد من الدول التي عدلت قوانينها بما ينسجم والصفة المميزة لبرامج الحاسب الآلي.[3] ومنهم الجزائر حيث جاء الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة باستخلاص ما يلي : "إن المشرع ومع قائمة المؤلفات المحمية ، حيث ادمج

1 بوعناد فاطمة الزهراء ,مرجع سابق, الصفحة 68

2 عفيفي كمال عفيفي, مرجع سابق, ص 75

3 جلال محمد الزغبي ، أسامة احمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية ، دراسة مقارنة ، دار الثقافة للنشر والتوزيع ، عمان الأردن ، 2010، ط 1، ص 189 .

تطبيقات الإعلام الآلي ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد التبات وبرامج الإعلام الآلي تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين ، لا سيما المصنفات المعلوماتية".

حيث نصت المادة 05 من القانون رقم 03-05 على انه: "تعتبر أيضا مصنفات محمية الأعمال الآتية..... مجموعات من المصنفات التراث الثقافي التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى.....تكفل الحماية للمؤلف.[1]

المصنفات المشتقة دون المساس بحقوق مؤلفي المصنفات الأصلية والمادة 4 من نفس القانون نصت على انه "تعتبر على الخصوص لمصنفات أدبية المكتوبة مثال المحاولات الأدبية .....

وبرامج الحاسوب والمصنفات الشفوية ...." كما أن مدة الحماية تحدد بـ 50 سنة بعد وفاة صاحب المصنف أو المبدع وذلك ما جاءت به المادة 58 الفقرة الأولى من نفس القانون، ويعتبر كل اعتداء على الحق المالي أو الأدبي لمؤلف برنامج فعلا من الأفعال التقليد.، حيث نصت على ذلك المادة 161من الأمر 03-05 " يعتبر مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية:

- الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف.
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة
- استيراد أو تصدير نسخ مقلدة من مصنف أو أداء.
- بيع نسخ مقلدة لمصنف أو أداء
- تأخير أو وضع رهن التداول لنسخ مقلدة أو أداء

وقد قرر المشرع جزاءات لجرائم التقليد كما جاء في المادة 58 الفقرة الأولى يربط حماية المصنف بتاريخ النشر أو التوزيع لأول مرة ، كما خول المشرع لصاحب المصنف المعتدي عليه القيام بإجراء تحفظي يتمثل في حجز التقليد ، بواسطة يتم حجز الوثائق والنسخ الناتجة عن الاستنساخ غير مشروع أو التقليد ، والعقوبات المقررة للاعتداء على حقوق الملكية الأدبية والفنية تشمل المواد من

1الأمر 03- 05 الصادر في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج 1، العدد 44

153- 156 إلى 159 من نفس القانون السابق الذكر حيث تقدر العقوبة الأصلية بالحبس من (06) أشهر إلى (03) سنوات وغرامة مالية من 500.000 دج إلى 1.000.000 سواء تمت عملية النشر داخل الجزائر أو خارجها ، وفي حالة العود. خول المشرع للقاضي السلطة تقدير وتقرير عقوبات تكميلية تتمثل في إمكانية غلق المؤسسات التي يشغلها المقلد أو شريكه مدة لا تتعدى ستة (06) أشهر. كما يمكن للجهة القضائية المختصة مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي، ومصادرة وإتلاف كل عتاد خصيصا لمباشرة النشاط غير مشروع.[1]

1 سوير سفيان ، جرائم المعلوماتية ، مذكرة نيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام ، جامعة بوبكر بلقايد ، تلمسان ، 2010 - 2011 ، ص78- ص80 .

المطلب الثاني: الجزاء الجنائي لجريمة الغش المعلوماتي في قانون العقوبات

إن المشرع الجزائري أقر عقوبات بالنسبة لجريمة الغش المعلوماتي بموجب قانون العقوبات والذي افرد القسم السابع مكرر منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات "من المواد 394مكرر إلى 394 مكرر 7، وقد نص على جريمة الغش المعلوماتي بالتحديد في المواد 394 مكرر والمادة 394مكرر1 من ق.ع.ج .كما أن المشرع الجزائري تدرج في العقوبات من خلال هذه المواد والتي نص على العقوبات المترتبة عن هذه الجريمة من عقوبات أصلية وأخرى تكميلية وهذا ماسنتناوله من خلال الفروع التالية:

الفرع الأول: العقوبات المقررة للشخص الطبيعي

إن المشرع الجزائري ومن خلال النصوص القانونية التي اقرها نلاحظ انه قام بوضع العقوبات الأصلية ، ومع هذا التدرج في العقوبات حدد الخطورة الإجرامية التي تنتج عن هذه التصرفات إذ نجد سلم الخطورة يتضمن ثلاثة درجات:

- جريمة الدخول أو البقاء عن طريق الغش
- جريمة الدخول والبقاء المشددة
- جريمة المساس العمدي بالمعطيات

أ)– العقوبات المقررة لجريمة الدخول أو البقاء بطريق الغش للأنظمة المعلوماتية: تقرر الفقرة الأولى من المادة 394 مكرر عقوبة أصلية لجريمة الدخول أو البقاء غير مصرح بهما تتمثل في الحبس من 3 أشهر إلى سنة وغرامة من خمسين ألف دينار جزائري(50000 دج) إلى مئتين ألف دينار(200000 دج).[1]

وقد جعل المشرع الجزائري لهذه العقوبة حد ادني وأقصى تاركا للقاضي السلطة التقديرية في تقريرها حسب ما تتطلبه ملابسات كل قضية

1 المادة 394 ، الأمر رقم 66 .156 مؤرخ في 8 يونيو 1966 حسب آخر تعديل له القانون رقم 14/11 المؤرخ في 02 غشت 2011

وقد كان المشرع الفرنسي في تعديل قانون العقوبات لسنة 1988 الذي أدرج بموجبه لأول مرة جرائم المعطيات واضعا حد لعقوبتي الحبس والغرامة ، إلا انه تراجع عن هذا الموقف ليشدد عقوبة تلك الجرائم إذا انه جعل لها حدا واحدا مند تعديل قانون العقوبات لسنة 1994 وهو الحبس لمدة سنة وغرامة تقدر بخمسة عشر ألف اورو ، أما قانون العقوبات الفرنسي لسنة 2004 فقد رفع معه عقوبة الحبس لمدة سنتين (2) والغرامة لقيمة ثلاثون ألف اورو.[1]

ب)– العقوبات المقررة لجريمتي الدخول أو البقاء بطريق الغش للأنظمة المعلوماتية (مشددة):تضاعف المادة 394 مكرر من قانون العقوبات في فقرتها الثانية والثالثة من عقوبة جريمة الدخول أو البقاء غير مصرح بهما ، إذا نجم عن هذا الدخول أو البقاء إلى حذف أو تغيير أو تخريب لنظام تشغيل نظام المعالجة الآلية للمعطيات.

في حالتي حذف أو تغيير المعطيات ترفع العقوبة إلى ضعف تلك المقررة للجريمة في صورتها البسيطة فتصبح الحبس من ستة أشهر إلى سنتين والغرامة من مائتي ألف (200.000 دج) إلى أربعمائة ألف (400.000 دج) دينار جزائري

أما في حالة ما إذا أدت الجريمة إلى تخريب نظام اشتغال المنظومة فان العقوبة تكون الحبس من ستة أشهر إلى سنتين والغرامة من خمسين ألف (50.000دج) إلى ثلاثمائة ألف (300.000 دج) دينار جزائري

وبالنسبة لقانون العقوبات الفرنسي لسنة 2004 فيعاقب بموجب نص المادة 323 في فقرتها الأولى على حذف أو تغيير المعطيات كطرف تشديد لجريمة الدخول أو البقاء غير المصرح بهما إذا كانت غير عمديه بثلاث سنوات حبس وبغرامة مالية تقدر بخمسة وأربعون ألف (45000 اورو)

1 alaim ben soussam .l informatique et le droit .tome1. hernnes1.1995. p372

، أما إذا تم تخريب نظام اشتغال المنظومة المعلوماتية فيعاقب عليها بالحبس لمدة خمسة سنوات و بالغرامة بخمسة وسبعون ألف اورو (75000).[1]

ج)– جرائم التلاعب بمعطيات الحاسب الآلي: تقرر المادة 394 مكرر 1 من قانون العقوبات على عقوبتي الحبس والغرامة لجريمة التلاعب بمعطيات الحاسب الآلي فتتراوح مدة الحبس من ستة أشهر إلى ثلاثة سنوات والغرامة ما بين (500.000دج) و (400.000دج) دينار جزائري

د)– جرائم الاعتداء العمدي على المعطيات: أن المادة 394 مكرر 2 من قانون العقوبات أوردة بالذكر العقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من شهرين إلى ثلاثة سنوات وغرامة (1.000.000دج) إلى (10.000.000دج)

سواء كان الاعتداء عمدي أو عن طريق الغش وذلك بتصميم أو بحث أو تجميع أو توفير أو نشر أو الادخار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية ويمكن أن ترتكب بها هذه الجرائم أو عن طريق حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها قانونا .

أما بالنسبة للمشرع الفرنسي فقد قرر لهذه الجريمة نفس العقوبة المقررة للجريمة التي يمكن أن تؤدي الوسائل المتعامل فيها لارتكابها.[2]

الفرع الثاني: العقوبات المقررة للشخص المعنوي

نصت المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي على انه يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا ، كما يسأل عن الجريمة التامة او الشروع فيها يشترط أن تكون الجريمة قد ارتكبت لحساب الشخص بواسطة احد أعضائه أو ممثلة هذا مع الإشارة إلى أن المسؤولية الجزائية لشخص المعنوي لا يستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة .

1 Alan ben soussan, cip cit ; p373

2 Alan ben soussan, cip cit ; p373

كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي ،وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات. أما بالنسبة للشخص المعنوي الذي يرتكب جريمة الغش المعلوماتي في ميدان العمل،يلاحظ أن المشرع حدد العقوبة الأصلية للشخص المعنوي في المادة 394 مكرر 4، وأن عقوبته تكون الغرامة التي تعادل خمسة مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي،وبالتالي تكون الغرامة المقررة عليه في جريمة الدخول والبقاء البسيطة تتراوح ما بين 250.000دج و500.000دج في حين تكون عقوبة جريمة الدخول أو البقاء غير المصرح بهما إذا نجم عن هذا الدخول أو البقاء تخريب لنظام اشتغال منظومة المعالجة الآلية للمعطيات آو حذف أو تغيير لمعطياته فترفع العقوبة إلى ضعف تلك المقررة للجريمة المجردة أو البسيطة،فتكون قيمتها في ق.ع.ج بين 250.000دج و 750.000دج.

أما عقوبة جريمة التلاعب بالمعطيات سواء بإدخال معطيات عن طريق الغش إلى نظام المعالجة الآلية للمعطيات،أم بالحذف أم التعديل للمعطيات التي يتضمنها النظام من 2.500.000دج إلى 10.000.000دج.

الفرع الثالث : عقوبة الاشتراك والشروع في جريمة الغش المعلوماتي

نصت على عقوبة الشروع في جريمة الغش المعلوماتي المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وثناه المشرع الجزائري في نص المادة 394 مكرر 7 من قانون العقوبات " يعاقب على الشروع في ارتكاب الجنح النصوص عليها في هذا القسم لعقوبات المقررة للجنحة دائما ".

فالجنحة الواردة بنص المادة 394 مكرر5 من قانون العقوبات مشمولة بهذا النص أي أن المشرع الجزائري بتبنيه لهذا المنطق قد تبنى معه فكرة الشروع في الاتفاق الجنائي عكس التشريعات المقارنة بما فيها التشريع الفرنسي التي أخرجت الاتفاق الجنائي لتحضير الجرائم الماسة بالأنظمة المعلوماتية من نطاق الشروع لأنها تعتبر ماسة بالنظرية العامة في القانون الجنائي كون تحضير الجرائم

التي تتم في إطار الاتفاق تشكل في حد ذاتها محاولة أو عمل تحضيرهما مما يؤدي إلى تبني فكرة الشروع في الشروع.[1]

فالمشرع الجزائري ومن خلال المادة 394مكرر 5 من ق. ع جرم مرحلة الاتفاق الجنائي بصفتها مرحلة من مراحل الجريمة التي تسبق الشروع، وعليه كان لزاما أن يجرم الشروع بوصفه مرحلة لاحقة عليها فلا يعقل أن يجرم مرحلة ويبيح أخرى لاحقة عليها.[2]

اختلف الفقه والتشريعات في تحديد مقدار العقوبة المقررة للشروع في الجريمة وانقسمت في ذلك إلى أربعة اتجاهات مختلفة ، فالاتجاه الأول يقضي بالمساواة بين عقوبة الشروع و عقوبة الجريمة التامة وهو الموقف الذي تبناه المشرع الفرنسي متفقا بذلك مع المذهب الشخص الذي يعتمد بخطورة الجاني لا بالخطر الناجم عن فعله قصد الردع العام عن ارتكاب الجريمة ، أما الاتجاه الثاني فيذهب لجواز تحقق عقوبة الشروع عن عقوبة الجريمة التامة وتذهب هذه التشريعات إلى أفراد عقوبة مخففة للشروع وهو الموقف الذي تبناه كل من التشريع الألماني والسويسري.[3]

أما الاتجاه الثالث اوجب تحقيق عقوبة الشروع .ومن هذا المنطلق فهناك تشريعات تميز بين الجريمة الموقوفة تجعلها اخف من الجريمة الخائبة ، في حيث ينص الاتجاه الرابع على أن عقوبة الشروع تكون خاصة بكل جريمة على حذ وهو ما تبناه المشرع السويدي.[4]

إن موقف المشرع الجزائري في تحديد عقوبة الشروع في الجريمة وجعلها مساوية لعقوبة الجريمة المشروعة في ارتكابها متبنيا في ذلك نفس موقف المشرع الفرنسي السابق ذكره ، كما انه لم يميز بدوره بين الجريمة الخائبة والموقوفة.[5]

---

1 أمال قارة، مرجع سابق، ص133

2 محمد خليفة , الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن,دار الجامعة الجديدة ,الإسكندرية ,2007 , ص 118

3 عباوي نجاة ، جرائم المعلوماتية في التشريع الجزائري ، مذكرة ماستر ، المركز الجامعي بشار ، معهد العلوم القانونية والإدارية ، السنة الجامعية 2008/2007 ، ص 313.

4 احمد فتحي سرور ، الوسيط في قانون الإجراءات الجزائية ، دار النهضة العربية ، طبعة 1943، ص320.

5 عباوي نجاة ، المرجع السابق ، ص 314.

الفرع الرابع: العقوبات التكميلية

أورد المشرع الجرائم الماسة بأنظمة المعالجة للمعطيات بعقوبات تكميلية تشترك فيها جميع هذه الجرائم بالإضافة إلى العقوبات الأصلية التي تم ذكرها سالفا والمقررة لكل جريمة على حدا وهي على التوالي المصادرة والغلق

أ)– **المصادرة**:عرفت المادة 15 من قانون العقوبات المصادرة كما يلي:" الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة أو ما يعادل قيمتها عند الاقتضاء "

وتنصب المصادرة على الأشياء التي استعملت أو كانت تستعمل في تنفيذ أو تلك التي تحصلت منها.

نص المشرع الجزائري على عقوبة المصادرة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب المادة 394 مكرر 6 من قانون العقوبات التي نصها : "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المتخذة " معتبرا بذلك عقوبة مصادرة تكميلية وجوبية ويقع لزاما على القاضي الحكم بها إذا ما توافرت شروط قيامها المقررة قانونا

ويمكن حصر شروط تطبيق عقوبة المصادرة في:

- أن يحكم على المتهم بالعقوبة الأصلية لإحدى الجرائم الواقعة على المعطيات الآلي بعقوبة الحبس الغرامة مهما كانت قيمتها
- أن يحكم على المتهم بالعقوبة الأصلية لإحدى الجرائم الواقعة على معطيات الحاسب الآلي
- أن تكون الأشياء التي يحكم بمصادرتها قد استخدمت في ارتكاب الجريمة فالمادة 394 مكرر 06 من قانون العقوبات جعلت محلا للمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة والتي حصر جاءت على سبيل المثال لا للحصر
- بدليل أن المشرع نص على عبارة " الوسائل المستخدمة " وهي كفيلة باستيعاب انه وسيلة أخرى

- يجب أن لا تخل المصادر بحقوق الغير حسن النية ، وهذا الشرط يتعلق بالأشياء المملوكة لشخص غير المتهم يعني للغير الذي هو كل أجنبي عن الجريمة أي كل من لا يدان فيها سواء بوصفه فاعلا أو شريكا وتبثث ملكيته للشيء المضبوط فهو حسن النية .[1]

وقد عرفت المادة 15 مكرر 2 من قانون العقوبات الغير حسن النية كالآتي: يعتبر من الغير الحسن النية الأشخاص الدين لم يكونوا شخصيا محل متابعة أو إدانة من اجل الوقائع التي أدت إلى المصادرة ، ومن الذين لديهم سند ملكية أو سند حيازة صحيح ومشروع على الأشياء القابلة للمصادرة.[2]

وحتى يكون الغير حسن النية حق المطالبة باسترداد الشيء القابل للمصادرة لابد من توافر شرطان:

❖ أن يكون ذلك الشخص محل المتابعة أو إدانة من أجل الوقائع التي أدت للمصادرة ومن تم لا يكون حسن النية الشخص الذي كان محل متابعة واستفادة من البراءة

- أن يكون لديه سند ملكية آو سند حيازة صحيح ومشروع على الشيء القابل للمصادرة ومن ثم لا يكون حسن النية الشخص الذي يحوز الشيء حيازة غير شرعية أو بدون سند.[3]

- كما أن المشرع الفرنسي قد أورد مجموعة من العقوبات التكميلية لجرائم المعطيات التي اعتبرها اختيارية وخاصة بالأشخاص الطبيعيين هي:

- الحرمان لمدة خمس سنوات (05) أو أكثر من الحقوق الوطنية والحقوق المدنية وحقوق الأسرة
- الحرمان لمدة خمس سنوات (05) أو أكثر من ممارسة وظيفة عامة.

أو ممارسة نشاط مهني أو اجتماعي في المجال الذي ارتكب فيه الجريمة ، مصادرة الأشياء التي استخدمت في الجريمة أو كانت معدة لاستخدامها فيها الغلق لمدة خمس سنوات (05) أو أكثر

1 محمد نجيب حسني، شرح قانون العقوبات، القسم العام، دار النهضة العربية، طبعة 1993، ص 841.

2 محمد خليفة، المرجع السابق، ص 120.

3 أحسن بوسقيعة ، نفس المرجع ، ص 251

للمؤسسات أو لأحد فروعها أو أكثر الذي استخدمت في ارتكاب الجريمة ، الإقصاء لمدة خمس سنوات (05) أو أكثر من الصفقات العمومية ، المنع لمدة خمس سنوات (05) أو أكثر من إصدار شيكات ، نشر أو تعليق الحكم.[1]

ب)– الغلق: كما أن المشرع الجزائري اقر عقوبة الغلق كعقوبة تكميلية وذلك طبقا لنص المادة 394 مكرر 6 من قانون العقوبات والتي تشمل إغلاق المواقع (les sites)والتي تكون محلا لجريمة الغش كما تشمل كذلك إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها بإغلاق المقهى الالكتروني (cyber café) عنصر العلم لأي مالك المقهى

وما يلاحظ على المشرع الجزائري استعماله لعبارة " المواقع التي تكون محلا لارتكاب الجريمة " والتي أوردها بالذكر في النص القانوني السابق ذكره والتي يقصد بها المواقع التي تتسبب في ارتكاب الجريمة ، وكان بالإمكان استعمال عبارة " المواقع التي تستعمل في ارتكاب الجريمة " والتي تعني المواقع التي وقعت فيها الجريمة .

وقد تقرره عقوبة الغلق كذلك لتشمل غلق المحل أو مكان الاستغلال ، ويمكن تعريفه بأنه المكان الذي استعمله الجناة في ارتكاب الجريمة ويمكن معها أن يحوي الأجهزة التي استعملت في عملية الدخول غير مصرح ب هاو في عملية التلاعب بالمعطيات أو في التعامل في المعطيات غير مشروعة ، ويمكن أن يحوي المحل المعطيات الصالحة لارتكاب جريمة أو معطيات المتحصلة من جريمة دون أن يحوي أجهزة ما ، وفي كل الأحوال يراعي في تطبيق العقوبة الغير حسن النية شأنها في ذلك شأن عقوبة المصادر.[2]

ولم تحدد المادة 394 مكرر 6 مدة الغلق وعليه فقد يكون بصفة نهائية أو مؤقتة، وذلك على عكس المادة 323/ 5 من قانون العقوبات الفرنسي التي حددت مدة الغلق كعقوبة تكميلية مقررة لأشخاص الطبيعيين بخمس سنوات (05) أو أكثر.

1 علي عبد القادر القهوجي ، الحماية الجنائية لبرنامج الحاسب الآلي ، الدار الجامعية للطباعة والنشر ,بيروت 1996 ، ص 125 .
2 محمد خليفة، المرجع السابق، ص 123.

الفرع الخامس : الحماية في ظل قانون الوقاية من جرائم المتصلة بتكنولوجيا الإعلام .

صدر القانون رقم 04/09 الصادر في 05 أوت 2009 ويتضمن 19 مادة موزعة على ستة فصول ، وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحداث القوانين وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء.

ومهنيين متخصين في مجال الإعلام الالكتروني من كافة القطاعات المهنية ، كما يتضمن القانون أحكام خاصة بالمراقبة الالكترونية التي لا يجوز إجراءها إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها وهي أفعال الموصوفة بجرائم الإرهاب والتخريب ، وجرائم بالماسة بأمن الدولة أو حالة توفير معلومات عن اعتداء محتمل يهدد منظومة من المنظومات لمؤسسات الدولة أو الدفاع الوطني أو النظام العام ، و ينص القانون على إنشاء هيئة وطنية الوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال مكافحته ، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم الالكترونية ومساعدة مصالح الشرطة القضائية في التحريات التي تجريها بشان هذه الجرائم ، كما تتكفل اللجنة أيضا بتبادل المعلومات مع نظيرتها في الخارج، علما بان القانون أكد على مبدأ التعاون الدولي من منطق المعاملة بالمثل كالمعاينة.[1]

1 القانون 04/09 المؤرخ في 05 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحته.

ملخص الفصل الثاني

نظرا لتطور وتنوع الجرائم المعلوماتية وصعوبة اكتشافها وهذا التطور الحاصل في الأنظمة المعلوماتية انعكس بطبيعة الحال على النظام الاثباتي،مما أدى إلى ظهور أدلة مستحدثة،تختلف عن الأدلة التقليدية وهذا التطور في الإثبات الجنائي جعل نصوص ق.ا.ج عاجزة عن إثبات هذا النوع من الجرائم الذي يحتاج إلى طرق تقنية وفنية تتناسب مع طبيعته الخاصة بحيث يمكن فك رموزها وشفراتها .

ولهذا تدارك المشرع الجزائري هذا النقص وفقا لخطته في مكافحة الجريمة المعلوماتية وتدخل من جهته لحماية أهم المصالح المتعلقة بالأنظمة المعلوماتية من خلال تعديله لقانون العقوبات سنة 2004 واستحدث بموجبه قسم سابع مكرر يحمل عنوان المساس بأنظمة المعالجة الآلية للمعطيات يتضمن طائفة من النصوص التي جرم من خلالها العديد من الأفعال التي تشكل عدوانا على أنظمة المعالجة الآلية للمعطيات واقر لمرتكبيها الجزاء المناسب.

ومع هذا التدارك اقر المشرع الجزائري من هذه الخطوة التي خطها بالحماية الجزائية من هذه الجريمة في جانبها الموضوعي وعززها بحماية إجرائية بتعديل ق.ا.ج بموجب القانون 22/06 المؤرخ في 20-12-2006 وإصدار قانون إجرائي خاص وهو القانون 09/04 والمتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهذا من اجل استنباط طرق إجرائية ذات طبيعة تقنية تتلائم مع هذه الجرائم.

الخاتمة

يمكن القول أن جريمة الغش المعلوماتي أصبحت آفة العصر نظرا للتطور التكنولوجي الحاصل ، فجريمة الغش المعلوماتي لست مجرد جرائم تقليدية بل هي جريمة بثوب جديد من حيث طبيعتها ومضمونها ونطاقها وتأثيرها وحتى من ناحية مرتكبيها . ونظرا لإساءة هذه التكنولوجي من طرف المجرمين المعلوماتيين والتي يكون فيها المتضرر المؤسسة الأمر الذي استدعى تدخل القانون الجنائي لوضع حماية للمجال المعلوماتي للمؤسسة هذا التدخل جعل من المشرع الجزائري تدارك الفراغ القانوني ، حيث عمد على تجريم أنواع الاعتداءات على هذه الأنظمة ، وحمى المصلحة السرية من خلال جريمة الدخول والبقاء غير المصرح بهما ،أما مصلحة السلامة فقد وضع لها الحماية من خلال تجريم التلاعب بالمعطيات ، كما جرم الشروع في جرائم المعطيات والاشتراك الجنائي للقيام بأفعال مادية تحضيرا لتلك الجرائم

كما قام المشرع الجزائري بتخصيصه قسم في قانون العقوبات تحت تسمية الجرائم الماسة بالأنظمة المعلوماتية رغبتا منه في حماية أهم المصالح المتعلقة بهذه من خلال نصوص قانون العقوبات تبقى مجرد حماية موضوعية لن تحقق نتائجها إلا إذا اقترنت بحماية إجرائية وفقا لقواعد الواردة بقانون الإجراءات الجزائية والمكملة فيما جاء به قانون 04/09 المتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بنصه مع أساليب جديدة لإجراءات البحث والتحري ..

وكل هذا تبقى هذه النصوص التي سنها قاصرة وحبذا لو وضع نصوص قانونية خاصة تحمي المؤسسة من الانتهاك وللحد من هذه الجرائم على مستوى المؤسسات.

و بناءا على هذا البحث توصلنا إلى ما يلي:

النتائج:

- لم يتفق على تعريف موحد جامع مانع للجريمة الغش المعلوماتي
- رغم اجتهاد المشرع الجزائري لتصدي لهذه الجريمة إلا أنه لم يحميها بقانون قائم بذاته للتحكم فيها بطرقه

- أن التطور التكنولوجي والفني ي حتم على المشرع تعديل القواعد القانونية، خاصة لحماية المؤسسات
- قصور القوانين أمام هذه الجريمة المستحدثة

إقتراحات

وعلى ضوء هذه النتائج توصلنا إلى جملة من الإقتراحات التي يمكن حصرها في:

- ضرورة وضع تعريف واضح لجريمة الغش المعلوماتي يتواكب مع التطور الحاصل في مجال المعلوماتية
- ينبغي على المشرع الجزائري وضع سياسة لحماية المؤسسات من جريمة الغش المعلوماتي حتى لا يبقى تطبيقها محدود في الجزائر .
- يجب وضع تشريعات وقوانين خاصة لحماية المؤسسات من الانتهاك
- ضرورة جعل صفة العامل كمتهم في جريمة الغش المعلوماتي الواقعة على المؤسسات.

قائمة المراجع

النصوص التشريعية

01 الدستور الجزائري سنة 2016

02 قانون العقوبات المعدل و المتمم

03 قانون الإجراءات الجزائية الجزائري المعدل و المتمم

04 قانون الإجراءات المدنية والإدارية الجزائري المعدل و المتمم

05 القانون رقم 09- 04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

06 قانون رقم 16-02 المؤرخ في 19 فيفري 2016 المعدل والمتمم للأمر رقم 66 – 156 مؤرخ في 8 يونيو 1966

07 الأمر رقم 07/03 الصادر في 19 يوليو 2003, المتعلق ببراءة الاختراع

08 الأمر 03/ 05 الصادر في 19 جويلية 2003، يتعلق بحقوق المؤلف والحقوق المجاورة

09 المادة 57 -2/1 من ق .إ.ج الفرنسي مضافة بموجب 2/17 من ق 2003/239

الكتب

1 احمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الطبعة الثانية ، سنة 2006

2 احسن بوسقيعة ، التحقيق القضائي ، ط 6 ، دار هومة الجزائر ، 2006،

3 احمد فتحي سرور ، الوسيط في قانون الإجراءات الجزائية ، دار النهضة العربية ، طبعة 1943

4 الشحات إبراهيم محمد منصور ، الجرائم الالكترونية في الشريعة الإسلامية والقوانين الوضعية ، دار الفكر الجامعي ، الإسكندرية ، 2011

5 أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، الطبعة الثالثة 2006، دار هومة

6 بالعليات ابراهيم ، أركان الجريمة الالكترونية وطرق إثباتها في قانون العقوبات الجزائري ، ط 1 ، دار برتي ، للنشر ، الجزائر ، 2007

7 بن زيطة عبد الهادي ,حماية برامح الحاسوب ف التشريع الجزائري ,دار الخلدونية للنشر و التوزيع , الجزائر ,2007. الطبعة الأولى

8 بوعناد فاطمة الزهراء , مكافحة الجريمة الالكترونية في التشريع الجزائري , مجلة الندوة للدراسات القانونية , سيدي بلعباس

9 جلال محمد الزغبي ، أسامة احمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية ، دراسة مقارنة ، دار الثقافة للنشر والتوزيع ، عمان الأردن ، 2010، ط 1

10 حسنين بن سعيد الغافوري ، السياسة الجنائية في مواجهة جرائم الانترنت ، دراسة مقارنة ، دار النهضة العربية ، 2009

11 خالد ممدوح إبراهيم, الجرائم المعلوماتية, دار الفكر الجامعي, الإسكندرية, الطبعة الأولى, سنة 2009

12 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي ,الاسكندرية 2009,

13 خثير مسعود,الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات , دار الهدى عين مليلة الجزائر , 2010.

14 رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات الدولية والمواثيق الدولية، دار النهضة العربية، الطبعة الأولى 2011

15 زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى ، عين مليلة ، الجزائر ، (ط) ، 2011

16 عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزائر، الطبعة السادسة، 2005

17 عفيفي كامل عفيفي, جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفكرية و دور الشرطة و القانون, دراسة مقارنة,2000

18 علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت ، عالم الكتب الحديثة ، الأردن2004

19 علي عبد القادر القهوجي ، الحماية الجنائية لبرنامج الحاسب الآلي ، الدار الجامعية للطباعة والنشر ,بيروت 1996

20 محمد حماد الهيتي ، التحقيق الجنائي والأدلة الجريمة ، الطبعة 1 ، دار المناهج للنشر عمان 2010

21 محمد خليفة , الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن,دار الجامعة الجديدة ,الإسكندرية ,2007

22 محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، 1994

23 محمد عبد الرحيم الناغي , الحماية الجنائية للرسوم و النماذج الصناعية , دراسة مقارنة , دار النهضة العربية , القاهرة ,2009

24 محمد نجيب حسني، شرح قانون العقوبات، القسم العام، دار النهضة العربية، طبعة 1993

25 فلاك مراد، آيات الحصول على الأدلة الرقمية لوسائل إثبات في الجرائم المعلوماتية، دكتوراه علوم في القانون العام مجلة الفكر القانوني والسياسي ، العدد الخامس

26 منير محمد الجنيمي ,ممدوح محمد الجنيدي,جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها, دار الفكر الجامعي, الإسكندرية ،.2006

27 نائلة عادل محمد فريدة قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية ، منشورات الجنائي الحقوقية ، الطبعة الأولى ، 2005

28 هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، ط 1، 2001

29 يونس عرب ، دليل امن المعلومات والخصومة جرائم الكمبيوتر والانترنت, إصدار اتحاد المصارف العربية الجزء الأول ، 2001

المذكرات و الرسائل

01 سعيد نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية ، جامعة الحاج لخضر ، باتنة ، 2013/2012

02 سوير سفيان ، جرائم المعلوماتية ، مذكرة نيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام ، جامعة بوبكر بلقايد ، تلمسان ، 2010 -2011

03 عباوي نجاة ، جرائم المعلوماتية في التشريع الجزائري ، مذكرة ماستر ، المركز الجامعي بشار ، معهد العلوم القانونية والإدارية ، السنة الجامعية 2008/2007

04 قربوز حليمة ، الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن ،مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء الجزائر ، ص2006 ـ 2009

05 محمد بن فردية , الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية , أطروحة لنيل شهادة الدكتوراه ,فرع القانون الجنائي وعلوم الجنائية ,الحقوق ,كلية الحقوق, جامعة الجزائر 1 ,2015/2014

المقالات العلمية

01 بن قارة مصطفى عائشة ,الحماية الجزائية للمجال المعلوماتي للمؤسسة من جريمة الغش المعلوماتي , مجلة الحقوق و العلوم السياسية ,جامعة عباس لغرور خنشلة ,العدد11 جانفي 2019

02 جميلة محلق، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور ق.إ.ج.ج ، محلية التواصل في الاقتصاد والإدارة والقانون ، العدد 42، جوان 2015

03 ذكي ذكي أمين حسونة ,جرائم الكمبيوتر و الجرائم الأخرى في المجال التكنيك المعلوماتي ,المؤتمر السادس للجمعية المصرية للقانون الجنائي, القاهرة 1993 في الفترة من 25 إلى 28 أكتوبر 1993 تقرير مصر

04 فوزي عمارة ، اعتراض المرسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجنائية ، مجلة العلوم الإنسانية ، العدد 33 ، جوان 2010

05 فيصل نسيغة ، ط .د عبير بعقيقي ، الإثبات في الجرائم المعلوماتية على ضوء القانون 09/04 ، المجلد 9 ، العدد 2 جوان 2018،

06 ونوغي نبيل / ط ,د زيوش عبد الرؤوف ، الجريمة المعلوماتية في التشريع الجزائري مجلة العلوم القانونية والاجتماعية ، 2019/09/01

المراجع باللغة الأجنبية

01 Alaim ben soussam .l informatique et le droit .tome1. hernnes1.1995. p372

02 Duteroy r et Rocco (a ; m) linformatique

03 Equity fuding life insurence l'informatique nouvelle ; nai 1976

04 Rose (Philippe), op, cit, p58 .59

05 Voire plus Myriam quener.joel ferry .cybercriminalité defi mondial 2 em édition .2009

الفهرس

شكر و عرفان ..... ب
إهداء ..... ب
الملخص ..... ج
قائمة المختصرات ..... د
المقدمة ..... ج
الفصل الأول : ماهية جريمة الغش المعلوماتي 12
المبحث الأول : مفهوم جريمة الغش المعلوماتي 13
المطلب الأول : تعريف جريمة الغش المعلوماتي 14
الفرع الأول: التعريف الفقهي 14
الفرع الثاني : التعريف التشريعي لجريمة الغش المعلوماتي 18
المطلب الثاني : الطبيعة القانونية لجرائم الغش المعلوماتي 22
الفرع الأول: المعلومات لها طبيعة من نوع خاص 22
الفرع الثاني: المعلومات مجموعة مستحدثة من القيم..... 23
المطلب الثالث: خصائص جريمة الغش المعلوماتي 24
الفرع الأول : السمات الخاصة بجريمة الغش المعلوماتي 24
الفرع الثاني : سمات وأنماط المجرم المعلوماتي 25
الفرع الثالث : نماذج جريمة الغش المعلوماتي في العمل 28

المبحث الثاني: أركان وأنواع الجريمة الغش المعلومات	29
المطلب الأول : أركان جريمة الغش المعلوماتي	29
الفرع الأول: الركن المادي	29
الفرع الثاني: الركن المعنوي	30
الفرع الثالث: الركن الشرعي	31
المطلب الثاني: أنواع جرائم الغش المعلوماتي	32
الفرع الأول : الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي	32
الفرع الثاني: الجرائم المعلوماتية الواقعة على النظام المعلوماتية الأخرى	33
الفرع الثالث : الجرائم المعلوماتية الواقعة على النظام المعلوماتي	36
ملخص الفصل الأول	39
الفصل الثاني: طرق إثبات جريمة الغش المعلوماتي والجزاءات المقررة لها	40
المبحث الأول : طرق و آليات إثبات جريمة الغش المعلوماتي	41
المطلب الأول: طرق جمع الأدلة التقليدية	41
الفرع الأول: المعاينة	42
الفرع الثاني : التفتيش في مجال جريمة الغش المعلوماتي.	43
الفرع الثالث : الخبرة في مجال جريمة الغش المعلوماتي	49
الفرع الرابع: الشهادة	53
المطلب الثاني: طرق جمع الأدلة الحديثة	55

الفرع الأول: التسرب واعتراض المراسلات 55
الفرع الثاني: التسرب واعتراض المراسلات 60
المبحث الثاني : الجزاءات المقررة لجريمة الغش المعلوماتي 62
المطلب الأول: الحماية الجزائية في ظل نصوص قانون الملكية الفكرية والصناعية 62
الفرع الأول:مدى خضوع برامج الحاسب الآلي للنصوص الملكية الصناعية 63
الفرع الثاني: مدى إخضاع برامج الحاسب الآلي لنصوص الملكية الأدبية والفنية 64
المطلب الثاني: الجزاء الجنائي لجريمة الغش المعلوماتي في قانون العقوبات 67
الفرع الأول: العقوبات المقررة للشخص الطبيعي 67
الفرع الثاني: العقوبات المقررة للشخص المعنوي 69
الفرع الثالث : عقوبة الاشتراك والشروع في جريمة الغش المعلوماتي 70
الفرع الرابع: العقوبات التكميلية 72
الفرع الخامس : الحماية في ظل قانون الوقاية من جرائم المتصلة بتكنولوجيا الإعلام 75
ملخص الفصل الثاني 76
الخاتمة 77
قائمة المراجع 80
الفهرس 85