جامعة محمد خيضر– بسكرة

كلية الحقوق والعلوم السياسية

قسم الحقوق

جريمة المساس بأنظمة المعالجة الآلية للمعطيات

مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق

تخصص: قانون جنائي

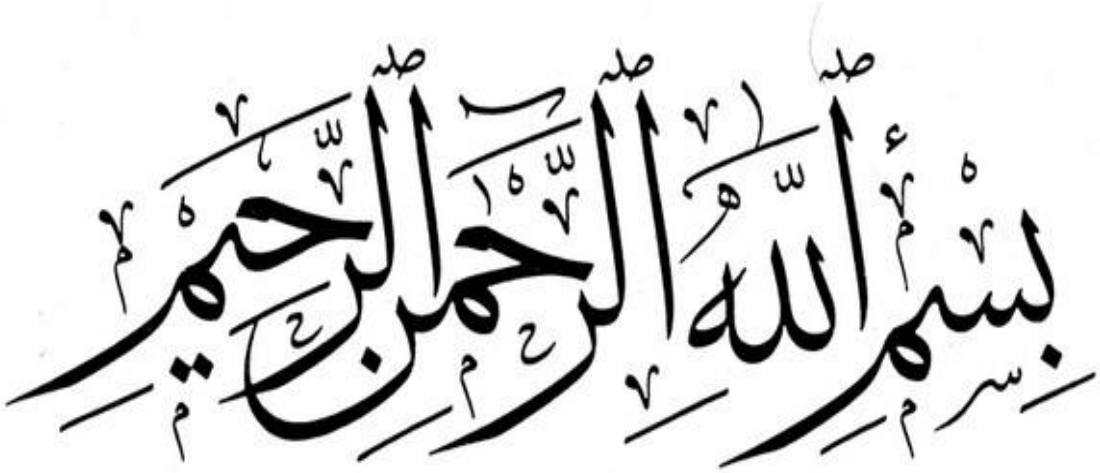
إعداد الطالبة:

– دليلة مزرقن

تحت إشراف:

– أ.د عادل رزيق

السنة الجامعية: 2016/2015


بسم الله الرحمن الرحيم

الإهداء

أهدي ثمرة جهدي

إلى من تنحني هامتي له خجلا **أبي**

إلى من حملتني وهنا على وهن **أمي**

إلى من أشد بهم أزري أخوتي وأخواتي

إلى رفقاء دربي أصدقائي

إلى من تحلو بالإخاء وتميزوا بالوفاء والعطاء إلى ينابيع الصدق الصافي

إلى من كانوا معي على طريق النجاح والخير

أصدقائي طلبة الحقوق وتخصص القانون الجنائي

أهدي هذا البحث.

شكر وعرفان

أشكر الله العلي القدير أن يسر لي السير في بحثي هذا و ذلل لي كل عسير بعزته ورحمته فلك يا الله عظيم الشكر يا واسع النعم ولك كثير الحمد على ما أنعمت به علينا بجـــودك و كرمك.

وأتقدم بالشكر الجزيل إلى الأستاذ الدكتورعادل رزيق على تفضله بالإشراف على هذه الدراسة و على الاهتمام الكبير و المتابعة المستمرة في كل المراحل.

فبفضل نصائحه و توجيهاته القيمة استطعت الوصول إلى تحقيق الأفضل في هذا العمل.

كما أتقدم بالشكر الخالص إلى أعضاء لجنة المناقشة لقبولهم مناقشة هذا العمل.

وإلى كل الأساتذة الذين عرفنا من معينهم و تشرفت بالدراسة على أيديهم خلال فترة دراستي بكلية الحقوق و في جميع أطوار حياتي الدراسية.

هذا و لا يفوتنا أن أتقدم بجزيل الشكر إلى كل من ساهم و لو بكلمة طيبة في انجاز هذا العمل.

مقدمة

تعتبر الجرائم الماسة بالأنظمة المعلوماتية وليدة عصر العولمة، ذلك أن هذا النوع من الجرائم الواقعة على الحاسب الآلي بكل مكوناته المادية أو المعنوية لم تكن في الحسبان حتى يتسنى دراستها ووضع قواعد و أسس تسييرها قبل انتشارها وتطورها.

وهذه الجرائم ولدت نتيجة الاستخدام الهائل للحاسوب في شتى المجالات الخاصة والعامة، بالإضافة إلى الانتشار الواسع للشبكات العنكبوتية التي ظهرت على الساحة الدولية، حيث لم يكن لها وجود قبل ذلك، ونتيجة لظهور تلك الشبكة فقد ظهرت معها الجرائم المعلوماتية التي تمثلت في جرائم الاعتداء على الكمبيوتر، سواء كان هذا الاعتداء يقع على ذات الجهاز أو كان على البيانات (المعطيات) التي يحتويها أو على الشبكة ذاتها.

ولم يعد يخف على أحد ما أصبحت تمثله هذه المعلومات من أهمية حتى باتت سلعة رائجة في سوق المعلومات، فقد غزت مختلف جوانب الحياة وارتبطت بمختلف الأنشطة والأعمال، فبات لزاما على كل الدول والمجتمعات التي تنشد التطور والازدهار ومواكبة التطورات الهائلة أن تولي لها الاهتمام وأن تحقق لها التدفق والانسياب مما يكفل الاستفادة القصوى منها.

وبهذا تعد جرائم المساس بأنظمة المعالجة الآلية للمعطيات من أهم موضوعات البحث التي فرضت نفسها للدراسة والبحث، كونها من الجرائم التي تمس بالفرد والدولة بمؤسساتها العامة والخاصة، وليس على المستوى الداخلي فحسب بل يمتد أثرها على المستوى الدولي مما جعل الدول تلجأ لإبرام اتفاقيات دولية ثنائية ومشتركة لمواجهة هذه الجرائم.

كما تسعى الدول من خلال تشريعاتها الداخلية لسن قوانين لتجريم هذا النوع من الاعتداءات ووضع عقوبات من شأنها حماية المجتمع منها، والأمر لا يتوقف على صدور تشريع ثابت بشأن هذه الجرائم نظرا لما تتسم به من تطور و تغير إذ تتنوع سبل ارتكاب الجريمة وتتعدد صورها مع تطور التكنولوجيا المعلوماتية، وعليه وجب على المشرع

بالمقابل أيضا الحرص على مواكبة النصوص التجريمية والعقابية لتشمل كل الأفعال المستحدثة، ووضع إستراتيجية حمائية جزائية للوقاية من هذه الجرائم.

وبهذا فقد قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون 22/06 المؤرخ في 20 ديسمبر 2006، بالإضافة إلى إصداره للقانون 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال، ومن خلالهما أوجد المشرع طرقا إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية.

أما فيما يخص تبني المشرع لقواعد قانون خاصة بتكنولوجيات الإعلام و الاتصال فقد ظهر جليا بعد تعديل الأمر رقم 156/66 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات وهذا بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 ، بحيث كرس هذا الأخير لأول مرة قواعد تتعلق بحماية أنظمة المعالجة الآلية للمعطيات وهذه القواعد تم وضعها في القسم السابع مكرر المعنون بـ "المساس بأنظمة المعالجة الآلية للمعطيات" من الفصل الثالث المتعلق بالجنايات والجنح ضد الأموال.

أهمية الدراسة:

يكتسي موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات أهمية بالغة، إذ يعد من الموضوعات الجديدة والمهمة في إطار القسم الإجرائي من القانون الجزائي، وهو من الموضوعات التي لا تزال بِكرا ولم تنل حظها من البحث والتمحيص على مستوى الفقه الجزائي، وهدف دراستنا الرئيسي هو التعرف على هذا النوع من الجرائم والخصوصية التي تتميز بها عن غيرها من الجرائم.

أسباب الدراسة:

تعد الجرائم الماسة بالأنظمة المعلوماتية من الجرائم التي لها طابع عابر للحدود حيث أنها تتميز عن غير من الجرائم التقليدية سواء في الأفعال الإجرامية أو في طبيعة الدليل

الصعب الإثبات، وهذا ما جعلنا معالجة هذا الموضوع الحديث من حيث جوانبه الموضوعية والإجرائية.

إشكالية الدراسة:

لقد اتجه المشرع الجزائري كغيره من التشريعات الأخرى إلى التدخل لحماية المنظومة المعلوماتية وذلك بتجريم في قانون العقوبات كل فعل قد يشكل مساسا وعدوانا بالأنظمة المعلوماتية، ومن هنا نطرح الإشكال التالي: هل وفق المشرع الجزائري في إقرار الحماية الجزائية لنظام المعالجة الآلية للمعطيات؟

ويتفرع عن هذه الإشكالية عدة أسئلة فرعية يستوجب الإجابة عنها من خلال هذه الدراسة وهي:

- ما المقصود بجريمة المساس بأنظمة المعالجة الآلية للمعطيات؟ وما هي الخصائص التي تتميز بها عن غيرها من الجرائم التقليدية؟

- ما هي الآليات المتبعة لمكافحة جريمة المساس بالأنظمة المعلوماتية؟

- كيف تعامل المشرع مع الدليل الرقمي في مجال الإثبات الجزائي من حيث كونه دليلا علميا وأثر هذه الخاصية على مبدأ الاقتناع الشخصي للقاضي الجزائي؟

أهداف الدراسة:

تهدف هذه الدراسة بشكل عام إلى تسليط الضوء على الجرائم الماسة بالأنظمة المعلوماتية، ومحاولة المساهمة في وضع الخطوط العريضة للتعرف على طرق التحقيق في هذا النوع من الجرائم، ذلك أن جدة وحداثة الجرائم المعلوماتية وما تتسم به من خصائص سوف يجد معه المحقق نفسه في حيرة أمامها وكيفية التعامل معها وأسلوب التحقيق فيها.

المنهج المتبع:

لقد اعتمدنا من خلال دراستنا لهذا الموضوع والإلمام بمختلف جوانبه على المنهج "**التحليلي الوصفي**"، وذلك من أجل بيان وكذا تحليل ب عض المفاهيم والغوص في جزئيا ته ا وطرحها بشكل من التفصيل والتشريح لما بدا لنا من أهميتها، وكذا وصف ظاهرة الجريمة المعلوماتية وتحديد بعض المفاهيم التي تقوم عليها، وكذا قيامنا بوصف المفاهيم الخاصة بالإجراءات المستعملة في استخلاص الدليل والصعوبات التي تواجهها.

صعوبات الدراسة:

لا يكاد يخلو أي بحث علمي من صعوبات تواجه الباحث، وهذا الأخير يستطيع تذليلها بإرادة وقناعة شخصية نابعة من إيمانه العميق بأن هناك فكرة نيرة قد تغير مجرى الحياة.

ومن الصعوبات التي واجهتنا قلة المراجع الوطنية التي تبحث في هذا الموضوع، وهذا الأمر لا يعد حاجزا للتواصل في البحث في هذا الموضوع.

التقسيم العام للدراسة:

للإجابة على الإشكالية السالفة الذكر فقد اعتمدنا على التقسيم الثنائي، أي تقسيم الدراسة إلى فصلين الفصل الأول تناولنا فيه **ماهية جريمة المساس بأنظمة المعالجة الآلية للمعطيات** والذي قسم إلى ثلاثة مباحث، حيث تم بيان مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات في المبحث الأول، ثم الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات في المبحث الثاني، أما المبحث الثالث فقد تطرقنا من خلاله عن أهم صور جريمة المساس بأنظمة المعالجة الآلية للمعطيات، وأما الفصل الثاني فقد جاء بعنوان: آليات قمع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، وقد قسم إلى مبحثين، الأول تناولنا فيه الاختصاص والتحري في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، أما المبحث الثاني فقد تعرضنا للإثبات في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجزاءات المقررة لها.

الفصل الأول

ماهية جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تمهيد:

إن التطور السريع لتقنيات الإعلام والاتصال وتنوع شبكات الربط أدى بطبيعة الحال إلى توسع ميادين استعمال هذه التقنيات سواء على المستوى الثقافي أو الاقتصادي أو الاجتماعي أو الإداري...إلخ، وقد واكب هذا التوسع في استعمال هذه التقنيات ارتفاع في أرقام الإجرام المرتكب بواسطتها، وهو ما يصطلح عليه بالجرائم الالكترونية أو الجرائم المعلوماتية، الأمر الذي أثر على حقوق الأفراد وحرياتهم حيث وفرت الأنظمة المعلوماتية وسيلة جديدة في أيدي مجرمي المعلوماتية لتسهيل ارتكاب العديد من الجرائم.

وإن حداثة الجرائم الماسة بالأنظمة المعلوماتية أدت إلى إثارة ضجة في الأوساط الفقهية بخصوص مفهومها وخصائصها ودوافع ارتكابها، وكذا موضوعها والأفعال المجرمة التي تدخل في نطاقها كون هذه الجريمة ظاهرة إجرامية تستهدف استخدام التطورات التكنولوجية بدلالتها الواسعة.

لذا ارتأينا تقسيم هذا الفصل إلى ثلاث مباحث، تناولنا في المبحث الأول مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات، وقد فصلنا ذلك في مطلبين المطلب الأول تطرقنا عن تعريف وخصائص جريمة المساس بالأنظمة المعلوماتية، وعن دوافعها في المطلب الثاني، وفي المطلب الثالث تطرقنا إلى أساليب ارتكاب مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات، أما المبحث الثاني جاء بعنوان الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات، وقسمناه إلى مطلبين المطلب الأول تناولنا فيه بواعث حماية أنظمة الآلية للمعطيات، ووسائل الحماية الجزائية من الجرائم الماسة بالأنظمة المعلوماتية في المطلب الثاني،أما المبحث الثالث فقد تطرقنا من خلاله عن أهم صور جريمة المساس بأنظمة المعالجة الآلية للمعطيات في ثلاث مطالب مستقلة.

المبحث الأول:

مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تعتبر الجرائم الماسة بالأنظمة المعلوماتية أحد أهم ثمار التقدم السريع في مختلف المجالات العملية التي يتميز بها الوقت الحاضر، وإن هذا التقدم صاحبه تقدم آخر موازي له في مجال الجريمة الماسة بالمعلومات وأنظمة المعالجة الآلية للمعطيات أو ما يطلق عليها بالغش المعلوماتي أو جريمة الاختلاس أو الاحتيال المعلوماتي مما يصعب إيجاد تعريف جامع وموحد لها باعتبارها ظاهرة حديثة نسبيا.

وفي هذا المبحث حاولنا إعطاء تعريف لجريمة المساس بأنظمة المعالجة الآلية للمعطيات وذلك بالتطرق إلى أهم التعريفات التي أسندت إليها وكذا أهم ما تتميز به هذه الجريمة من خصائص تميزها عن غيرها من الجرائم في المطلب الأول، أما المطلب الثاني فقد تناولنا فيه دوافع جريمة المساس بأنظمة المعالجة الآلية للمعطيات، أما المطلب الثالث فقد تطرقنا إلى أساليب ارتكابها.

المطلب الأول: تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات وخصائصها

لقد عرفت الجريمة بصفة عامة على أنها كل عمل أو امتناع يعاقب عليه القانون بعقوبة جزائية، أو بعبارة أخرى هي كل فعل غير مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدبيرا احترازيا، وبهذا تعتمد الجرائم الناشئة على الاستخدام غير المشروع لشبكة الانترنت على المعلومة بشكل رئيسي، وهذا ما أدى إلى إطلاق عليها مصطلح الجريمة المعلوماتية[1] والتي اختلفت العديد من الآراء حول تعريفها (الفرع الأول)، كما أن هذه

[1]– محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت**، دار النهضة العربية، القاهرة، 2009، ص 32.

الجريمة اتسمت بجملة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم (الفرع الثاني).

الفرع الأول: تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات

قبل التطرق إلى تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات كان لابد من توضيح معنى المعلوماتية.

أولا/ تعريف المعلوماتية:

إن امتلاك المعلومة يعني القدرة على امتلاك الحاضر والمستقبل، لأنها هي الأداة لتنظيم المعرفة، والمعرفة هي مجموعة المعاني والمعتقدات والمفاهيم والتصورات الفكرية التي تتكون لدى الإنسان نتيجة المحاولات المتكررة لفهم الظواهر والأشياء المحيطة به، وتمثل حصيلة خبرة ومعلومات ودراسة طويلة يمتلكها الشخص في وقت معين.

المعلومات من حيث مدلولها اللغوي مشتقة من المادة اللغوية" علم"، وهي مادة غنية بالكثير من المعاني كالعلم والإحاطة بباطن الأمور والوعي والإدراك واليقين والإرشاد والإعلام والشهرة، والتميز والتيسير، وتحديد المعالم، والمعرفة، والتعليم والتعلم، والدراية إلى آخر ذلك من المعاني المتصلة بوظائف العقل.

وترجع كذلك إلى كلمة " مَعْلَم" ، أي الأثر الذي يستدل به على الطريق وInformation هي المقابل الانجليزي لكلمة معلومات، وهذه الكلمة الانجليزية مشتقة من اللاتينية Information والتي كانت تعني في الأصل الاتصال والتلقي[1].

وتعرف المعلومات اصطلاحا على أنها:" مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة.[2]

---

[1]– رصاع فتيحة، **الحماية الجنائية للمعلومات على شبكة الانترنت** (مذكرة ماجستير في القانون العام)، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2011، ص 26.

[2]– رئلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي، ط1، بيروت، 2005، ص 97.

وعرفها الأستاذ Catala على أنها: " رسالة ما معبر عنها في شكلٍ يجعلها قابلة للنقل أو الإبلاغ للغير".[1]

وفي هذا الإطار عرف المشرع الأمريكي المعلومات في قانون المعاملات التجارية الإلكترونية لسنة 1999 بالمادة الثانية الفقرة العاشرة منه بأ نها " تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر والبرامج الموضوعة في الأقراص المرنة وقواعد البيانات أو ما شابه ذلك.

وأشار المشرع الفرنسي وفقا للقانون رقم 652/82 الصادر في 1982/07/26 الخاص بالاتصالات السمعية والبصرية إلى المعلومة على أ نها "صور الوثائق والبيانات والرسائل من أي نوع.

وبهذا يمكننا القول أن المشرع الفرنسي والأمريكي قد وفقا نوعا ما في إعطاء تعريف موسع من خلال إضافتها لعبارة "**من أي نوع**" كما في تعريف القانون الفرنسي أو بعبارة "ما شابه ذلك" كما في تعريف القانون الأمريكي، وذلك لما قد يظهر من أشكال جديدة للمعلومات وذلك لارتباطها بتقنية الحاسوب والتطور التكنولوجي.

ويرى الكثير من الباحثين في هذا المجال أن هناك اختلاف بين المعلومات والمعطيات، إذ أن هذه الأخيرة تعبر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض ولم تخضع بعد للتفسير أو التجهيز للاستخدام، أما عن المعلومات فهي المعنى الذي يستخلص من هذه المعطيات.[2]

وقد عرفت اتفاقية بودابست للجريمة المعلوماتية نفس التعريف الذي ذهبت إليه هي ئة التوصيف العالمية الإيزو، حيث نصت في ماد تها الأولى على أن المعطيات هي كل تمثيل

---

[1]– رشيدة بوكر، **جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن** ، منشورات الحلبي الحقوقية الطبعة الأولى، بيروت، 2012، ص65.

[2]– هشام محمد فريد رستم، **قانون العقوبات ومخاطر تقنية المعلومات**، مكتبة الآلات الحديثة، مصر ،1992، ص26 .

للوقائع أو للمعلومات أو المفاهيم تحت أي شكل وتكون مهيأة للمعالجة بما في ذلك برنامج معد من ذات الطبيعة ويجعل الحاسب يؤدي المهمة.[1]

وبهذا فإن المعطيات تعتبر المواد الخام التي تستخرج منها المعلومات باستخدام معالجة آلية في عملية الاستخراج، إذ يتم تجميع وتشغيل المعطيات للحصول على المعلومات ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من المعطيات والتي يحصل تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية.[2]

وعلى غير العادة عمد المشرع الجزائري إلى وضع تعريف للمعطيات بموجب المادة الثانية من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بنصه في الفقرة ج من هذه المادة على أن المعطيات المعلوماتية:" هي أي عملية عرض للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".[3]

وقد فرق بعض الباحثين بين المعلومات والبرامج حيث عرف هذا الأخير على أنه "مجموعة من التعليمات المتتابعة بصفة منطقية توجه إلى الكمبيوتر لأداء العمليات المنطقية المطلوبة".[4]

ومن التعريفات القانونية للبرنامج أنه: "مجموعة من التعليمات الموجهة من الإنسان إلى الآلة والتي تسمح بتنفيذ مهمة معينة".[5]

---

[1]– مفتاح محمد دباب، **معجم المصطلحات وتكنولوجيا المعلومات والاتصالات** ، الدار الدولية للنشر ، القاهرة، 1995، ص42 .

[2]– انتصار غريب، **أمن الكمبيوتر والقانون**، دار الراتب الجامعية، بيروت، 1998، 81.

[3]– قانون 04/09المؤرخ في 14شعبان 1430الموافق لـــ 5أوت 2009المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، العدد 47، سنة 2009.

[4]– محمد محمد الهادي، **تكنولوجيا المعلومات وتطبيقاتها**، الطبعة الأولى دار الشروق، القاهرة، 1989، ص 110.

[5]– عماد محمد سلامة، **الحماية القانونية لبرنامج الحاسب الآلي ومشكلة قرصنة البرنامج الأول** ، دار وائل للنشر، عمان، 2005، ص 48.

أما عن القرار الوزاري الصادر عن وزير الصناعة والتعليم الوطني في 1982/11/22 بخصوص إثراء اللغة الفرنسية، فقد عرف البرنامج على أنه : " مجموعة الخطوات والإجراءات التي تهدف إلى تشغيل نظام متكامل لأنظمة المعالجة المعلوماتية وتوظيفها وفقا لهذا الغرض الذي من أجله تم وضع هذا البرنامج".

ومن خلال الجدل الفقه حول التمييز والتفرقة بين المعطيات والمعلومات والبرامج، إلا أنه هناك جانب آخر من الفقه يرى عدم وجود أهمية في التمييز بينها، طالما أن المعلومات هي المعنى المستخلص من المعطيات بعد معالجتها ، وأن البرنامج هو المستودع الذي يتم فيه معالجة هذه المعطيات، فالعلاقة بينها إذن هي علاقة الجزء بالكل.

أما عن المشرع الجزائري فقد أدرج برامج الحاسوب ضمن مفهوم المعطيات ولم يأبه لهذا الجدل الفقهي من حيث التمييز بينها، وهذا ما جاء في نص المادة الثانية من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال في تعريفها للمعطيات أنها: "أي عملية عرض للوقائع أو المعلومات.بما في ذلك البرامج المناسبة التي من شانها أن تجعل المنظومة المعلوماتية تؤدي وظيفتها ."

ثانيا/ تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات:

تمخض عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالكمبيوتر والانترنت، الجريمة المعلوماتية أو الالكترونية أو الجريمة الماسة أنظمة المعالجة الآلية للمعطيات والتي أشاب تعريفها كثير من الإبهام والغموض، حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لهما، ولكن الفقه لم يتفق على تعريف محدد، بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب الكتروني[1].

فهذه الجرائم هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين، حيث انتقل بالجريمة من صورها التقليدية إلى أخرى الكترونية قد يصعب التعامل معها.[2]

---

[1]– نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، ط 1، عمان، 2008، ص46.

[2]– خالد ممدوح إبراهيم، **أمن المعلومات الإلكترونية**، الدار الجامعية، الإسكندرية، 2008، ص 41.

وبالرجوع لنصوص قانون العقوبات الجزائري خاصة في المواد من 394 مكرر إلى 394 مكرر7، فإنه لم يرد تعريف لنظام المعالجة الآلية للمعطيات، ونفس الشيء بالنسبة المشرع الفرنسي بالرغم من اقتراح البرلمان الفرنسي لوضع تعريف وذلك خلال مناقشة تعديل قانون التجريم، ولم يتم الموافقة على تضمين هذا التعريف في نصوص التعديل بحجة أنه لا يمكن ربط التجريم في هذه الأنظمة بحالة تقنية متغيرة قد لا يشملها التعريف الموضوع لها لاحقا.

أما القانون رقم 09/04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أورد تعريفا للمنظومة المعلوماتية في المادة 02/ ب على أنها: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

في حين الاجتهاد القضائي الفرنسي فقد أورد في قراراته كل مرة تحديد لمفاهيم عدة مصطلحات معلوماتية، كما ورد تعريفها في منظمة " أنكسيكلوبيديا يونيفارسال" بأن نظام المعلوماتية هو كل شيء مركب يتكون من عدة معطيات مرتبطة ببعضها بعدد معين من الروابط.

وعرفه الفقيه خالد ممدوح إبراهيم على أنه:" مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها البعض والتي تعمل على جمع البيانات والمعلومات ومعالجتها وتخزينها وبثها وتوزيعها بغرض دعم صناعة القرارات و التنسيق و تأمين السيطرة على المنظومة إضافة لتحليل المشكلات للموضوعات المعقدة".[1]

وقد عرفه مجلس الشيوخ الفرنسي على أنه:" نظام المعالجة الآلية للمعطيات هو كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تكون كل منها الذاكرة، المعطيات ، أجهزة الإدخال و الإخراج، أجهزة الربط التي تربط بينها مجموعة من العلاقات التي عن طريقها تم تحقيق نسخة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية.[2]

---

[1]– خالد ممدوح إبراهيم، **التقاضي الإلكتروني**، دار الفكر الجامعي، الإسكندرية، 2009، ص 29.

[2]– محمد خليفة ، **الحماية الجنائية لمعطيات الحاسب الآلي** ، دار الجامعة الجديدة الإسكندرية، مصر، 2007، ص26.

وعرفت تعرفها المادة 1/14من القانون العربي النموذجي الموحد بأن ها: " كل مجموعة مركبة من وحدة أو عدة وحدات الإدخال والإخراج و الاتصال التي تساهم في الحصول على نتيجة معينة".[1]

أما في المذكرة التفسيرية للاتفاقية الدولية للإجرام المعلوماتي فقد جاء أن المقصود بالنظام المعلوماتي هو: جهاز يتكون من مكونات مادية و منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية و هو يشتمل على وسائل للإدخال وإخراج وتخزين البيانات، و هذا الجهاز قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة.

ومن خلال هذا التعريف نستشف أن لأنظمة المعالجة نوعين من المكونات مادية وغير مادية يتكون الحاسب الآلي من المكونات المادية الآتية:

أولا / المكونات المادية:

1- وحدات الإدخال: هي الوحدات المصمّمة للقيام بإدخال المعلومات و المعطيات المطلوب معالجتها إلى وحدة المعالجة الرئيسية مثل لوحة المفاتيح، الأقراص المغناطيسية، مشغل شرائط التخزين، الأقراص الصلبة، الفأرة، شاشات الكمبيوتر التي تعمل باللمس، أجهزة المسح الإلكتروني.

2- **وحدات الإخراج:** تستخدم وحدات الإخراج لعرض نتائج العمليات التي أتمها الكمبيوتر على المعطيات التي تم إدخالها إليه عن طريق وحدات الإدخال مثل الطابعات والشاشات، الأقراص و الشرائط الممغنطة.

3- **وحدة المعالجة المركزية:** تعتبر أهم أجزاء الحاسب الآلي وهي بمثابة العقل في الجهاز تعمل على إنجاز كافة العمليات الحسابية بسرعة مذهلة بالإضافة إلى معالجة مختلف أنواع المعطيات، و التنسيق بين جميع أجزاء الحاسب، وتنقسم وحدة المعالجة المركزية إلى ثلاثة أقسام و هي:

---

[1]- جباري عبد المجيد، **دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة**، دار هومة للنشر والتوزيع، الجزائر، 2012، ص 10.

- وحدة التحكم
- وحدة الحساب و المنطق
- وحدة الذاكرة بنوعيها الذاكرة الداخلية و الذاكرة الخارجية.[1]

ثانيا/ المكونات غير المادية للحاسب الآلي: وهي تمثل الروح بالنسبة للحاسب الآلي ويطلق عليها الكيان المنطقي أو البرمجيات، وتنقسم هذه المكونات إلى:

1-**البرامج:** وهي التقديم الكامل المفصل بصورة كافية للعمليات في شكل شفوي أو خطي أو غيره بغية تحديد مجموعة التعليمات المشكلة لبرنامج الحاسب الآلي وصلة كل منها بالأخرى تكون موجهة من الإنسان إلى الآلة والتي تسمح لها بتنفيذ مهمة معينة، كذلك يتضمن المستندات الملحقة وهي المستندات التي ليست ببرامج الحاسب الآلي تهدف إلى تبسيط مفهوم وتطبيق البرنامج.

2/ **المعطيات:** وهي معلومات تمّ تنظيمها و معالجتها داخل نظام المعالجة الآلية للمعطيات وتخزينها بغية استرجاعها عند طلبها، فضلا عن عنصر إضافي أعطى بعدا جديدا للنظام المعلوماتي وهو يعد الاتصال بالنظم الأخرى من خلال شبكات الاتصال المعلوماتية المختلفة.[2]

ثالثا/ ضرورة خضوع نظام المعالجة الآلية للمعطيات لحماية فنية:

مع تعدد شبكات الاتصال السلكية واللاسلكية التي أصبحت من خلالها الحواسيب في كل أنحاء العالم متصلة بشبكة عالمية، وأصبح تناقل المعلومات خلال هذه الأنظمة يفرض تأمين بقاء المعطيات سرية وهذا ما أدى بالمختصين في هذا المجال البحث لإيجاد برامج تشفير لنقلها وحمايتها في سرية تامة.

---

[1]- رشا علي الدين ، **النظام القانوني لحماية البرمجيات بين نظرية تنازع القوانين و القانون الدولي الإتفاقي** ، الطبعة الأولى، مصر، 2004، ص80 .

[2]- محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن**، دار الجامعة الجديدة، مصر، ص25.

وفي هذا الصدد اختلفت الآراء فهناك من يرى ضرورة تقييد الحماية الجزائية بوجوب توافر عنصر الحماية الفنية، فيجب أن تخضع الأنظمة والمعطيات لنظام أمني.

أما الرأي الغالب في الفقه الفرنسي يرى وجوب خضوع النظام لحماية فنية ذلك أن وجوب الشرط لا يكون له سوى دور واحد هو إثبات سوء نية من قام بانتهاك النظام والدخول إليه بطريقة غير مشروعة ويدخل ذلك في عبء إثبات القصد الجنائي.[1]

الرأي الثاني يرى بوجوب تمتع كل الأنظمة و المعطيات بالحماية الجزائية بغض النظر على احتوائها على نظام أمان، هذا الرأي أخذت به محكمة الاستئناف في باريس في إحدى قراراتها الصادر 1994 حيث أشارت في حيثياته أنه: ليس من اللازم لقيام جريمة الدخول الغير شرعي أن يكون الفعل قد تم مخالفا لتدابير أمنية، بل يكفي لقيام الجريمة أن يتم ذلك ضد إرادة المسؤول عن النظام.

أما في قانون العقوبات الجزائري نجد أن المشرع الجزائري لم ينص على ضرورة أن تكون أنظمة المعالجة الآلية للمعطيات محمية فنيا لتتمتع بالحماية الجزائية عند المساس بها، حيث أستبعد هذا الشرط لأنه من الناحية العملية أغلب الأنظمة تتمتع بنظام حماية فنية إلا ما كان منها ومنذ البداية موضوع للجمهور.

الفرع الثاني: خصائص جريمة المساس بأنظمة المعالجة الآلية للمعطيات

نظرا لوقوع هذه الجريمة في أغلب الأحيان في بيئة المعالجة الآلية للبيانات والتي تكون المعلومات محل الاعتداء فيها، فهي من الجرائم التي تتم بسرعة وتتسم في التطور في أساليب ارتكابها، وتعد أقل عنفا في التنفيذ مما يجعلها تتميز بخصائص عن غيرها من الجرائم التقليدية ويمكن إجمالها فيما يلي:

أولا/ جريمة المساس بأنظمة المعالجة الآلية للمعطيات جريمة عابرة للحدود:

تعتبر جريمة ذات طابع دولي حيث أنها لا تعترف بالحدود، فبعد ظهور شبكات المعلومات لم يعد هناك حدود لا مرئية ولا ملموسة تقف أمام نقل المعلومات عبر الدول

[1]– جباري عبد المجيد، مرجع سابق، ص 109.

والمختلفة، إذ تقع بدولة لا يمتد أثرها لدولة أخرى أو أكثر، و تثير الطبيعة الدولية لهذه الجرائم العديد من المشاكل، كمشكلة السيادة والاختصاص القضائي وقبول الأدلة المتحصل عليها في دولة ما أمام قضاء دولة أخرى.[1]

والحقيقة أن عملية التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر الوسائل التي تثيرها الإشكالات في مجال الحاسوب وبشكل خاص الإجراءات الجنائية والاختصاص والقانون الواجب التطبيق، وهذا بدوره عامل رئيسي في نماء دعواته تضافر الجهود الدولية لمكافحة هذا النوع من الجرائم.[2]

ثانيا/ صعوبة اكتشاف جريمة المساس بأنظمة المعالجة الآلية للمعطيات:

يتسم هذا النوع من الجرائم بأنها خفية ومستمرة في أغلبها، ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجرائم الناشئة عن استخدام الحاسوب إلى عدم ترك أثر خارجي بصورة مرئية، كما أن المجرم يمكنه ارتكاب هذه الجريمة في دول وقارات مختلفة، حيث أنها جريمة عابرة للحدود، كما للجاني قدرة هائلة في تدمير دليل الإدانة في لمح البصر.[3]

ويكون للمجني عليه دورا أساسيا كذلك في صعوبة اكتشاف وتحديد نوع الجريمة، حيث تحرص أغلب الجهات التي تتعرض أنظمتها المعلوماتية للقرصنة والانتهاك على عدم الكشف حتى بين موظفها عما تعرضت له، وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها، وتشير بعض التقديرات إلى أن ما يتراوح بين 20 و 25 % من جرائم الحسابات لا يتم الإبلاغ عنها مطلقا، خشية الإساءة إلى سمعة المؤسسة أو المصنع.[4]

---

[1]– محمد خليفة، المرجع السابق، ص37.

[2]– جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة**، دار البداية ناشرون وموزعون، عمان، 2007، ص 142.

[3]– جميل عبد الباقي، **القانون الجنائي والتكنولوجيا الحديثة**، دار النهضة العربية، مصر، 1992، ص17.

[4]– نهلا عبد القادر مومني، مرجع سابق ، ص 55.

ثالثا/ صعوبة اثبات جريمة المساس بأنظمة المعالجة الآلية للمعطيات:

إن اكتشاف جريمة المساس بأنظمة المعالجة الآلية للمعطيات كما سبق وأشرنا ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها، فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب ، فما يزيد من صعوبة إثبات هذه الجرائم هو ارتكا بها عادة في الخفاء، وعدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من عمليات أو أفعال إجرامية، حيث يتم بالنبضات الالكترونية نقل المعلومات، أضف إلى ذلك إحجام مجتمع الأعمال عن الإبلاغ عنها تجنباً للإساءة إلى السمعة وهز الثقة في كفاءة المنظمات والمؤسسات ا لمجني عليها، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الزمنية.[1]

وتجدر الإشارة إلى أن وسائل المعاينة التقليدية لا تفلح غالبا في إثبات هذا النوع من الجرائم نظرا لطبيعتها الخاصة تختلف عن الجرائم التقليدية التي لها مسرح تجري عليه الأحداث، حيث تخلف آثار مادية تقوم عليها الأدلة، وهذا ما يعطي المجال أمام السلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة [2]، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة المعلوماتية يتضاءل ويتلاشى دوره في إظهار الكشف عن الحقيقة، ويرجع ذلك لسببين اثنين هما:

1- الجريمة المعلوماتية لا تخلف آثارا مادية.

2- إن الكثير من الأشخاص يتعاقبون على مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي مدة طويلة نسبيا، الأمر الذي يعطي مجالا واسعا للجاني وللآخرين أن يغيروا أو يتلفوا الآثار المادية إن وجدت، وهذا ما يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية.

---

[1]- محمد علي العريان، مرجع سابق، ص 54/53.

[2]- حجازي عبد الفتاح بيومي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت** ، دار الكتب القانونية، مصر، 2002، ص 59.

ومن الأمور التي زادت تعقيدا نقص الخبرة الفنية والتقنية لدى السلطات المختصة من ضباط الشرطة القضائية وقضاة التحقيق وقضاة الحكم، فهذا الأمر يشكل عائقا أساسيا أمام إثبات هذه الجريمة.[1]

رابعا/ أسلوب جريمة المساس بأنظمة المعالجة الآلية للمعطيات:

تتطلب الجرائم التقليدية نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو في جريمة السرقة أو الاختطاف أو القتل...الخ، فإن الجرائم الماسة بالأنظمة المعلوماتية لا عنف لها ولا قتل ولا آثار دماء إنما تحتاج القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.

خامسا/ خصوصية مجرمي المعلوماتية:

يتصف المجرم المعلوماتي بخصائص تميزه عن المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي ومعرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة للجرائم المعلوماتي، فهي جرائم فنية تقنية في الغالب الأعم، والأشخاص الذين يقومون بارتكابها عادة يكونون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال الحاسوب والتعامل مع شبكة الانترنت.[2]

وبهذا فقد لخص الفقه سمات المجرم المعلوماتي في الآتي:

1- المجرم المعلوماتي مجرم متخصص فقد ثبت في العديد من القضايا أن عددا من المجرمين لا يرتكبون إلا جرائم الكمبيوتر.

2- المجرم المعلوماتي مجرم عائد إلى الإجرام انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف على هو تقديمه للمحاكمة في المرة السابقة.

---

[1]- حجازي عبد الفتاح بيومي، مرجع سابق، ص 59.

[2]- نهلا عبد القادر المومني، مرجع سابق، ص 55.

3- المجرم المعلوماتي مجرم محترف ذلك أنه لا يسهل على الشخص العادي أن يرتكب هذه الجرائم إلا في حالات قليلة فالأمر يقتضي كثيرا من الدقة والتخصص في هذا المجال وذلك لأجل التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر.[1]

وقد صنف الفقيه **دون باركر** المختص بالجريمة المعلوماتية بمعهد ستانفورد أشكال ظهور الجاني إلى سبع فئات:

1- الهواة

2- المهووسون: وهم الذين يرتكبون الجريمة باستخدام العنف الذي من الصعب تصوره في المجال المعلوماتي .

3-الجريمة المنظمة: فالحاسوب و ما يتضمنه من أنظمة أصبح وسيلة في تنفيذ الجرائم كقاعدة البيانات التي تملكها عائلة (جيمبرتو رودر بوفيه) في كولومبيا المختصة في تجارة الكوكايين.

4- الحكومات الأجنبية: تستغل الأنظمة للجوسسة.[2]

5- النخبة: هم متخصصون في أجهزة الإعلام الآلي وأنظمته الذين يسود الاعتقاد لديهم أن سمات وظائفهم المرموقة و خبرتهم في استعمال الأنظمة لأهداف شخصية أو للتنافس مما يؤدي بهم للتمادي في استخدامها بطرق غير مشروعة تصل لحد ارتكابهم الجرائم.

6- المتطرفون: الذين يستخدمون الأنظمة لنشر أفكار بدافع أو لمذهب ديني معين أو سياسي أو اقتصادي مثل مجموعة (الألوية الحمراء) بإيطاليا.

7- المخربون: هم الذين يرتكبون الجريمة إرضاء لرغبتهم.[3]

---

[1]- عبد الفتاح بيومي حجازي ، **الإثبات الجنائي في جرائم الكمبيوتر و الانترنت** ، دار الكتب القانونية مصر ، 2007، ص 80.

[2]- جدي نسيمة، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات** (مذكرة ماجستير في القانون الجنائي)، كلية الحقوق ، جامعة وهران، 2014، ص 30.

[3]- جدي نسيمة، مرجع سابق، ص 31.

المطلب الثاني: دوافع ارتكاب جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تختلف الجريمة المرتكبة باستخدام الحاسب الآلي عن الجرائم التقليدية من حيث الدوافع، حيث أن المجرم المعلوماتي يسعى من خلال ارتكابه لجريمة بالإضافة إلى تحقيق المكسب المادي إلى تحقيق أغراض معنوية مثل التعلم أو بدافع الانتقام، ويمكن حصر هذه الدوافع فيما يلي:

الفرع الأول: الدوافع الشخصية

يقصد بالدوافع الشخصية تلك العوامل اللصيقة بشخصية ا لمجرم المعلوماتي والتي تدفعه لارتكاب الجريمة المعلوماتية.

ويمكن رد الدوافع الشخصية لدى مرتكب الجرائم المعلوماتية إلى دوافع مالية وأخرى ذهنية أو نمطية.

أولا/ الدوافع المالية:

يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل، وهو من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم المعلوماتية، ذلك أن خصائص هذه الجرائم [1]، وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع بما يحققه من ثراء فاحش.

ومن أمثلة ذلك ما حدث في فرنسا سنة 1986 حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو 70000 فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670.000 فرنك فرنسي.[2]

---

[1]– سوير سفيان، **جرائم المعلوماتية** (مذكرة ماجستير في العلوم الجنائية وعلم الإجرام)، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2010، ص 26.

[2]– سوير سفيان، مرجع سابق، ص 26.

فمعظم الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر هو تحقيق الكسب المادي، ففي دراسة تعرض لها الفقيه Parcker يظهر أن 43 % من حالات الغش المعلن عنها قد تمت من أجل اختلاس الأموال، و 23 % من أجل سرقة المعلومات، و19 % من أجل أفعال إتلاف، أما 15 % فلسرقة وقت الآلة، أي استعمال غير مشروع للحاسوب لأجل تحقيق منافع شخصية.[1]

ثانيا/ الدوافع الذهنية أو النمطية:

يتصور لمرتكب الجرائم المعلوماتية صورة ذهنية على أنه هو البطل الذكي الذي يستحق الإعجاب، فمرتكبو هذا النوع من الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقائهم ببراعتهم، لدرجة أنه عند ظهور لأي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغب الآلة، يحاولون إيجاد وسيلة إلى تحطيمها أو التفوق عليها.[2]

وبهذا فللدوافع الذهنية أو الدوافع النمطية هي تلك العوامل النفسية اللصيقة با لمجرم المعلوماتي تدفعه إلى ارتكاب الجريمة المعلوماتية بهدف الرغبة في إثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية والرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية دون أن يكون له نوايا آثمة.[3]

ويرى البعض أن الدافع إلى ارتكاب الجرائم المعلوماتية يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح.[4]

---

[1] – عبد الله حسين علي محمود، **سرقة المعلومات المخزنة في الحاسب الآلي**، دار النهضة العربية، مصر، 2001، ص 70

[2] – نسرين عبد الحميد نبيه، **الجريمة المعلوماتية والمجرم المعلوماتي**، منشأة المعارف، الأردن، د س ن، ص 44.

[3] – أحمد خليفة الملط، مرجع سابق، ص 89.

[4] – أحمد خليفة الملط، مرجع سابق، ص 89.

الفرع الثاني: الدوافع الخارجية

في بعض الأحيان يكون الدافع لارتكاب الجريمة هو نتاج تأثر الجاني بعوامل خارج بيئة أثناء تواجده في بيئة لمعالجة المعطيات و عليه يؤول الأمر لارتكاب الجريمة إما بدافع الانتقام، التعاون، التواطؤ مع شخص آخر أثر عليه أو إضرارا بالغير أو أن يرتكبها تحت التهديد.

أولا/ دافع الانتقام أو إلحاق الضرر برب العمل:

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

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

ثانيا/ الرغبة في كسر النظام والتفوق على تعقيد وسائل تقنية:

إن اختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بها والتفوق عليها قد يشكل متعة كبيرة لدى مرتكبي جرائم المساس بالأنظمة المعلوماتية، وهذا ما صرح به أحد قراصنة الحاسوب:" كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد كنت أعود إلى البيت بعد يوم آخر في الدراسة أدير تشغيل جهاز الحاسوب وأصبحت عضوا في لجنة قراصنة الأنظمة".[2]

---

[1]– محمد أمين الرومي، **جرائم الكمبيوتر والانترنت**، دار المطبوعات الجامعية، الإسكندرية، 2003، ص 24.

[2]– نهلا عبد القادر المومني، مرجع سابق، ص 92.

وبهذا فإن مجرم المعلوماتية يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته التقنية لإدارة المنشأة لارتكاب الجريمة المعلوماتية.

المطلب الثالث: أساليب ارتكاب جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تتنوع الوسائل التي تستخدم في الاعتداء على معطيات الحاسب الآلي حيث يستخدم المجرمين تقنيات مختلفة وعديدة لتنفيذ جرائمهم، ولم يعد الحصول على هذه التقنيات حكرا على جهات أو أشخاص معينين، بل أصبحت متاحة للجميع نظرا لانتشار الكثير من المواقع والكتب التي تتيح معرفة مختلف التقنيات والأساليب المبتكرة التي يمكن استعمالها في هذه الجرائم ، ورغم تعدد هذه التقنيات فان أهدافها تنحصر في إلحاق الضرر بالمعطيات إما بهتك سريتها أو محوها أو تشوّيهها أو تعطيل أنظمة معالجتها، ومن خلال هذا المطلب سنتناول في فروعه أهم هذه التقنيات.

الفرع الأول: الاعتداءات المنطقية

تتحقق الاعتداءات المنطقية عندما تكون مكونات الحاسب المعلوماتي غ ي مادي مثل: البرامج المستخدمة والمعطيات المخزنة محلا أو موضوعا للجريمة.

أولا/ الفيروس: هو برنامج ي كاثر لهدف ضار هو تدمي الأنظمة المعلوماتي، ي مي بالقدرة الهائلة على الاختراق و الانتشار و التدمي بك في لا ي كن م عها استرجاع الملفات إذ ي م مسرحها نهائيا و ي لأ مكانها بالنفايات، إذ ي عمل على نسخ نفسه في البرنامج الذي ي صيبه و ي حكم به كما ي مي البرامج المصابة بالعدوى بتحكم بعد إصابتها مرة أخرى، و لدرء مخاطر الفي وسات ي تم صنع البرامج المضادة للف ي وسات (anti-virus) ورغم ذلك تضل الفي وسات تتسلل ببرامج مقرصنة.[1]

[1]– أمي فرج ي سف، **الجرائم المعلوماتي على شبكة الانترنت**، دار المطبوعات الجامعي، مصر،2009 ، ص6.

- **أنواع فيروسات الحاسوب وطرق انتشارها** :هناك العديد من التقسيمات والتسميات لأنواع فيروسات الحاسوب، وطرق انتشارها كل حسب الزاوية التي ينظر إليها ، ومن أهم أنواع الفيروسات نذكر:

- **فيروس السرطان:** وهذا الفيروس يقوم بمسح أجزاء من شاشة الحاسب بصورة تدريجية حتى يصل في النهاية إلى القضاء عليها كليا. ويطلق العاملون في مجال الحاسبات على هذه العملية Zeroing أي مسح البيانات وتحويلها إلى حرف (0) Zéro.

- **فيروس الجنس:** يمثل مجموعة من الصور الجنسية مثيرة للغرائز لجلب انتباه القائم على النظام، وأثناء ذلك ينسخ البرنامج نفسه، ويمسح جدول توزيع الملفات .

- **فيروس القردة :** ويتمثل في صور لمجموعة من القردة تمارس ألعاب بهلوانية أثناء قيام البرنامج بنسخ نفسه بنفسه في أكثر من موقع، وتدمير الفهرس الرئيسي للقرص الصلب.[1]

- **فيروس الحب Love:** يتمثل هذا الفيروس في شكل رسالة أو صورة مثيرة للإغراء، ترسل إلى البريد الالكتروني للمستخدم لحثه على فتحها وتكون ملحقة برسالة عادية، ويتنكر الفيروس في شكل رسالة بريدية آمنة، وبمجرد فتح الرسالة يقوم الفيروس بنسخ نفسه مرات عديدة، مما يضاعف قدرته على الانتشار لحذف الملفات أو إخفائها ويستبدلها بنسخ منه، ويقوم أيضا بإرسال رسالة بريد إلكتروني لكافة العناوين الالكترونية الموجودة في سجل العناوين الالكترونية.[2]

- **فيروس سارز:** تزامن ظهور هذا الفيروس الالكتروني مع ظهور فيروس سارز البيولوجي، وينتشر هذا الفيروس عبر البريد الالكتروني حيث يأتي برسالة إلكترونية بعنوان (أنا أحتاج إليك ساعدني) باللغة الانجليزية، وبمجرد فتح المستخدم هذه الرسالة يقوم الفيروس

---

[1]- مليكة عطوي، **الجريمة المعلوماتية**، حوليات جامعة الجزائر، العدد 21، جوان 2011، ص16.

[2]- هدى حامد قشقوش، **جرائم الحاسب الإلكتروني في التشريع المقارن**، دار النهضة العربية، القاهرة ،1992، ص05.

بنسخ نفسه عدة مرات، وإرسال رسائل إلكترونية إلى كافة العناوين الموجودة في قائمة العناوين لالكترونية، وهكذا يضمن انتشارا سريعا وخرابا مدمرا.

لعل خطورة هذا الفيروس تكمن في حمله اسم المرض الخطير الذي يهتم الكثير من الناس لمعرفة المزيد عنه في ذلك الوقت.

- **فيروس مايكل أنجلو:** أطلق هذا الفيروس يوم 06 مارس 1992 بمناسبة الاحتفال بذكرى ميلاد الرسام الإيطالي الشهير مايكل أنجلو، وأصاب هذا الفيروس العديد من أجهزة الحاسوب الشخصية في عدد كبير من دول العالم.

- **فيروس ناسا:** وهو فيروس أطلق احتجاجا على إنتاج الأسلحة النووية، فهو عبارة عن برنامج يحمل رسالة مناهضة للأسلحة النووية، وتظل هذه الرسالة تكرر نفسها وتتكاثر بشكل مدمر للبرامج الأخرى.[1]

ثانيا/ حصان طروادة : وهو عبارة عن شفرة صغ يرة يتم تحم يلها لبرنامج رئ يسي من البرامج ذات الشعبية العالية و يقوم ببعض المهام الخفية غالبا ما تتركز على إضعاف قوى الدفاع لدى الضحية أو تقويضها ليسهل اختراق جهازه وسرقة بياناته.[2]

و مثال ذلك في الولايات المتحدة الأم ريكية وجد برنامج عرف باسم (zoxoon) يبدو عند بداية تشغيله أنه ألعاب تسلية إلا أ نه يقوم بذات الوقت بمحو أقراص النظام، أ يضا برنامج (filer) الذي يبدو ظاهريا كبرنامج لتنظيم الملفات في حين يقوم في الحقيقة بمحوها وعادة ما توجد برامج أحصنة طروادة في برامج العمال كبرامج معالجة النصوص والجداول للتلاعب بروابتهم ومستحقاتهم وتعطي نتائج غ ير صحيحة وهي بخلاف الفيروسات لا تنسخ نفسها وهي بالغة الصعوبة لاكتشافها.[3]

---

[1]- مليكة عطوي، مرجع سابق، ص 16.

[2]- بوذراع عبد العزيز، مرجع سابق، ص 33.

[3]- جدي نسيمة، مرجع سابق، ص 35-36.

ثالثا/ ديدان الحاسوب(برنامج الدودة): وهي البرامج التي تتصف بامتلاكها قدرة تعطيل أو إيقاف نظام الحاسب بصورة كاملة، وذلك عن طريق استغلال فجوة في نظام تشغيل الحواسيب، متنقلة من حاسب لآخر لتغطي شبكة بأكملها ، وقد يتكاثر عددها عن طريق إنتاج نسخ منها وهي تشبه البكتريا في تكاثرها ، كما تهدف هذه البرامج إلى احتلال أكبر نطاق ممكن من سعة الشبكة، مما يؤدي إلى التقليل أو الخفض من قدرتها وقد تتجاوز ذلك في بعض الأحيان، وتقوم بأعمال تخريب حقيقية للملفات والبرامج وأنظمة تشغيل الحاسب.[1]

رابعا/ القنبلة العلوماتية: وهو برنامج يعده مصمم معلوماتي و يثبته على أن يعمل بعد انقضاء مدة محددة على استعمال النظام بهدف تدميره أو تعطيله أو محو بياناته وهي نوعان: القنابل المنطقية والقنابل الزمنية.

فالقنابل المنطقية تهدف إلى تدمير أو تغيير برامج ومعلومات النظام في لحظة محددة أو في فترة زمنية منتظمة عند إنجاز أمر معين في الحاسب الآلي أو برنامج معين.[2]

ومثال ذلك وضع قنبلة منطق ية تسعى للبحث حول حرف أبجدي مع ين في أي سجل يتضمن أمرا بالدفع وعندما تكتش فه تتحرك متتال ية ومنطق ية وتز يل كل اسم يتضمن هذا الحرف من السجل.

أما القنابل الزمن ية فتقوم بعم لها التخريبي في وقت محدد مسبقا، كق يام موظف مفصول من العمل بوضع قنبلة معلومات ية زمن ية تتلف كل المعط يات بعد شهر أو شهر ين مثلا من فصلة بدافع الانتقام.[3]

ومن أمثلتها قض ية حادثة شركة أوم يغا أن قام موظف بدافع الانتقام بوضع برنامج لإتلاف بيانات الشركة التي طرد منها لي تم ذلك بعد ستة أشهر من مغادرته.[4]

---

[1]– مليكة عطوي، مرجع سابق، ص 17.

[2]– محمد أمين أحمد الشوابكة، **جرائم الحاسوب و الانترنت**، مكتبة دار الثقافة للنشر والتوزيع، الأردن، 2004، ص240.

[3]– بوذراع عبد العزيز، مرجع سابق، ص 34.

[4]– جدي نسيمة، مرجع سابق، ص 33.

الفرع الأول: الاعتداءات المادية

وتتمثل هذه الاعتداءات في:

- اعتراض المجرم المعلوماتي للمعط يات عمدا عن طر يق رصد الإشارات الكهرومغناطيسية في الأنظمة المعلوماتية و تحليلها بغية استخراج المعلومات الم فهومة أو المقروءة منها.

- التشويش : و يكون الغرض م نه إعاقة المستوى التشغ يلي للنظام المعلوماتي مما يؤثر على سرعته وسلامة المعطيات التي يحتويها.

- التخريب: هو أخطر من التشو يش لأ نه يضع نظام المعالجة الآل ي خارج الخدمة .

- التصنت: وهو التمركز في موقع مع ي داخل شبكات الاتصالات وتسج يل وحفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية.[1]

- التجسس: و يهدف إلى الحصول على معلومات إستترات يجية سواء كانت عسكرية أو اقتصادية أو سياسية أو معطيات سكانية واجتماعية.

[1]- بوذراع عبد العزيز، مرجع سابق، ص 35.

المبحث الثاني:

الحماية الجزائية للأنظمة الآلية للمعطيات

لقد تباينت إتجاهات الدول المختلفة في التعامل مع ظاهرة الج رائم الماسة بالأنظمة المعلوماتية، ويرجع ذلك إلى اختلاف الأنظمة القانونية لهذه الدول ، وكذا إلى اختلاف تجربة كل منها مع الجريمة المعلوماتية، و أيضا إلى النتائج الاقتصادية المترتبة عن هذا النوع من الجرائم والذي يختلف من دولة إلى أخرى، وهو ما ينعكس على أشكال السلوكات التي تلقى اهتماما من قبل المشرعين.

وبهذا جميع الدول تدعو إلى ضرورة سن نصوص تشريعية صارمة التشريعي لمواجهة جريمة المساس بأنظمة المعالجة الآلية للمعطيات، إلا أنها تختلف من حيث الأساس الذي يرتكز عليه التدخل التشريعي، وبهذا نجد اختلاف في المفاهيم القانونية التي لها تأثير على النظام القانوني بشكل عام.

وإن تدخل التشريعات في مختلف الدول يأخذ عدة أنماط والتي تتمثل إما في خلق نصوص قانونية جديدة يضاف إليها البعد الخاص بالنظم المعلوماتية، وإما بتعديل النصوص القانونية القائمة حيث تكون أكثر ملائمة مع تطور هذا النوع من الجرائم.

وإن خطورة هذه الجريمة وطبيعتها الدولية وعجز الدول عن التصدي لها جعل منها شأنا دوليا دفع با لمجتمع الدولي إلى توحيد جهوده وحشد قواه لمكافحة هذه الجرائم، وذلك بعقد المؤتمرات وسن الاتفاقيات.

وهذا ما سنتطرق إليه في هذا المبحث، حيث قسمناها إلى مطلبين حيث تناولنا في المطلب الأول الحماية الجزائية على المستوى الدولي، أما المطلب الثاني فقد جاء بعنوان الحماية الجزائية على المستوى الداخلي.

المطلب الأول: الحماية الجزائية على المستوى الدولي

بعد تنامي هذا النوع من الجرائم و نظرا لطبيعتها الدولية وآثارها الممتدة العابرة للحدود أدركت الدول أن إيجاد نظام قانوني داخلي غير كافي لمواجهة الجريمة إذ تعجز كل دولة منفردة على التصدي لها، مما دفع المجتمع الدولي للسعي لتوحيد الجهود لمكافحتها وإبرام اتفاقيات تعاون ولإصدار توصيات نذكر منها:

الفرع الأول: منظمة الأمم المتحدة

لا يستهان بالمجهودات المبذولة من طرف منظمة الأمم المتحدة في مجال مكافحة الجريمة الماسة بالأنظمة المعلوماتية، فهي دائمة الحرص على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل الحد من انتشار هذا النوع من الجرائم وذلك من خلال متابعتها وإشرافها على عقد المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين.[1]

أصدرت منظمة الأمم المتحدة عدة توصيات خلال مؤتمراتها المنعقدة باستمرار لمواجهة هذه الظاهرة الإجرامية منها:

المؤتمر السابع المنعقد بميلانو عام 1985 الذي كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والاعتداء على الحاسب الآلي وإعداد تقرير يعرضه على المؤتمر الثامن، وقد عقد هذا الأخير في هافانا عام 1990 وقد خرج العديد من التوصيات منها التأكيد على ضرورة الاستفادة من التطورات العلمية والتكنولوجية في مواجهة الجريمة المعلوماتية، كما أكد على ضرورة تحديث القوانين التي تتناول هذه الجرائم وتحسين تدابير الأمن والوقاية المتعلقة بها، وكذا التعاون مع المنظمات المهتمة بهذه الظاهرة.[2]

---

[1]– محمود أحمد عبابنه، **جرائم الحاسوب و أبعادها الدولية**، دار الثقافة للنشر و التوزيع، الأردن، 2009، ص 155.

[2]– سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري** (مذكرة ماجستير في القانون تخصص علوم جنائية)، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2012، ص 83–84.

وفي سنة 1995 عقد مؤتمر آخر للأمم المتحدة لمنع الجريمة ومعاملة المجرمين في القاهرة، حيث أوصي فيه على وجوب حماية حياة الإنسان الخاصة وملكيته الفكرية من تزايد خطر التكنولوجيا، وأوصى كذلك على وجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة، وجاء المؤتمر العاشر المنعقد في بودابست عام 2000 الذي أوصى بوجوب العمل الجاد من أجل الحد من جرائم تقنية المعلومات المتزايدة والتي اعتبرت نمطا من الجرائم المستحدثة والعمل على اتخاذ تدابير مناسبة للحد من أعمال القرصنة.[1]

الفرع الثاني: المجلس الأوروبي

لعب المجلس الأوروبي دورا مهما في محاولة الحد من الجرائم الماسة بالأنظمة المعلوماتية، وذلك من خلال إقراره العديد من التوصيات الخاصة بحماية البيانات ذات الصبغة الشخصية من سوء الاستخدام وحماية تدفق المعلومات.

وللمجلس الأوروبي اتفاقيتين بارزتين الأولى اتفاقية الجرائم المعلوماتية وقعت عليها 32 دولة وتم المصادقة عليها من 9 دول ودخلت حيز النفاذ اعتبارا من أول جويلية 2004 وتعتبر الاتفاقية الوحيدة الملزمة وتضمنت النص على الجرائم التالية:

- الجرائم المرتكبة ضد سرية وتكامل وتوافر البيانات أو نظم الكمبيوتر (التدخل، الاختراق التعدي على أجهزة الكمبيوتر) الجرائم المتصلة بالمحتوى.
- الجرائم التي تتضمن انتهاكا لحقوق الملكية الفكرية وما يتصل بها.[2]

---

[1]- محمود أحمد عبانه، مرجع سابق، ص 159.

[2]- طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي: النظام القانوني للحماية المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2009، ص 334.

أما الاتفاقية الثانية فقد كانت ببودابست الموقعة في 2001/22/23 والتي اعتبرت قفزة نوعية في مجال التعاون الدولي لمحاربة الجرائم المعلوماتية، قد تضمنت هذه الاتفاقية 48 مادة غطت في مضمونها ثلاث أقسام كبرى:[1]

- القسم الأول تناول مجموعة الجرائم التي يمكن أن تتعرض لها النظم المعلوماتية
- القسم الثاني: تناول مجموعة الإجراءات الجنائية التي يمكن أن تتخذ في مواجهة هذا النوع من الجرائم خصوصا تفتيش وضبط البيانات المخزنة في الحاسوب
- القسم الثالث: تناول موضوع التعاون الدولي بين الدول الأعضاء الموقعة على الاتفاقية.

الفرع الثالث: القانون الجنائي العرب الموحد

هو قانون نموذجي تم اعتماده من مجلس وزراء العدل العرب بموجب القرار رقم 229 سنة 1996 لمواجهة جرائم معطيات الحاسب الآلي الذي نص على الاعتداءات في نظام المعالجة المعلوماتية و عاقبت المادة 464 منه على الدخول بطريق الغش إلى نظام المعالجة الآلية للمعطيات و عرقلة أو إفساد نظام التشغيل و تخريب المعلومات داخل النظام.[2]

وإضافة إلى ذلك ونذكر القانون العربي الاسترشادي الذي اعتمدت عليه جامعة الدول العربية عبر الأمانة العامة لمجلس وزراء العرب لمكافحة جرائم تقنية المعلومات وما في حكمها، حيث مت اعتماده من قبل مجلس وزارة العدل في دورته التاسعة عشر بالقرار رقم 495 د- 19-2013/10/08، ويعد هذا القانون من أبرز الجهود العربية المبذولة في مجال الحماية من الجرائم الماسة بالأنظمة المعلوماتية من الناحية التشريعية، حيث تضمن هذا القانون على 27 مادة موزعة على أربعة أبواب، إذ يعالج الباب الأول الجرائم المعلوماتية والتي تنص عليها المواد من 03 إلى غاية 22 ومن أهمها:

---

[1]- هلالي عبد الله أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست**، دار النهضة العربية، القاهرة، 2003، ص 23.

[2]- جدي نسيمة، مرجع سابق، ص 46-47.

– جريمة الدخول بغير حق إلى موقع أو نظام معلوماتي، مع تشديد العقوبة إذا كان بغرض إلغاء أو إتلاف أو إعادة نشر بيانات أو معلومات شخصية .

– جريمة تزوير المستندات المعالجة في نظام معلوماتي واستعماله.

– جريمة الإدخال الذي من شأنه إيقاف الشبكة المعلوماتية عن العمل، أو إتلاف البرامج أو البيانات فيها.

– جريمة التنصت دون وجه حق على ما هو مرسل عن طريق الشبكة المعلوماتية.[1]

المطلب الثاني: الحماية الجزائية على المستوى الداخلي

لقد ألقت الثورة المعلوماتية بضلالها على قوانين العقوبات لمختلف الدول بالتصدي للجانب السلبي منها مع ضرورة مراعاة تحقيق هدفين أساسيين هما: عدم تفويت الفرصة في الاستفادة من تطور التقنية المعلوماتية ومن ناحية أخرى ضرورة حماية الاقتصاد والأمن الوطني وحقوق وحريات الأفراد من جراء اللجوء إلى الاستخدام غير الشرعي لهذه التقنية .

والملاحظ في هذا الصدد أنه كلما كان الاعتماد أكبر على التقنية المعلوماتية كلما كانت الحاجة أكثر إلحاحا لوضع نصوص قانونية لحماية هذه المعلوماتية.[2]

وفي هذا المطلب سنتناول في الفرع الأول مواجهة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الفرنسي، ثم نعرج إلى تجربة المشرع الجزائري ومجهوداته في مكافحة ومحاربة جريمة المساس بالأنظمة المعلوماتية في الفرع الثاني.

الفرع الأول: مواجهة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الفرنسي

كانت أولى المحاولات لمد سلطان قانون العقوبات لحماية المال المعلوماتي بفرنسا من طرف وزيرها للعدل عام 1985عندما تقدم بمشروع قانون عقوبات جديد أضاف بموجبه بابا

[1]– سعيداني نعيم، مرجع سابق، ص 86.

[2]– محمد خليفة، مرجع سابق، ص 61.

رابعا للكتاب الثالث منه بعنوان "الجرائم في المادة المعلوماتية " تناول بالتجريم الموضوعات التالية:

- الالتقاط العمدي للبرامج أو أي عنصر آخر من النظام المعلوماتي.
- استخدام برنامج أو معطيات أو أي عنصر من عناصر النظام المعلوماتي دون موافقة من لهم الحق فيه.
- تخريب أو عرقلة أداء كل أو جزء من نظام المعالجة الآلية للمعلومات.[1]

لكن هذا المشروع لم يكتب له النجاح، ولم يجد سبيله للتطبيق إلى أن تقدم النائب codfrain Jacques في 1986/08/05 ونواب آخرون في الجمعية الوطنية باقتراح مشروع قانون عن الغش المعلوماتي حاول من خلاله تطويع بعض النصوص القائمة في قانون العقوبات والتي تتناول جرائم تقليدية كالسرقة وخيانة الأمانة والتزوير والإتلاف... وذلك لتشمل العدوان على المال المعلوماتي.

وبعد المناقشات في البرلمان أسفرت عن قانون اختلف تماما عن ذلك المشروع الذي قدم لأول مرة بل تشابه إلى حد كبير مع المشروع الأول الذي تقدم به وزير العدل 1985 سنة فصدر بذلك القانون رقم 19 لسنة 1988 المتعلق بحماية نظم المعالجة الآلية للبيانات ثم تم إدراجه في قانون العقوبات لعام 1992 وطبق بعدها في 1994/03/01، وقد تضمن النص على مجموعة من الجرائم في المواد من 2/462 إلى 9/462 وهي:

- الدخول أو البقاء غير المشروع في نظام معالجة آلية المعطيات أو في جزء منه .
- محو أو تعديل المعطيات الموجودة داخل النظام المعلوماتي.
- كل فعل عمدي من شأنه أن يعرقل أو يفسد أداء النظام لوظيفته.
- تزوير المستندات المعالجة آليا أيا كان شكلها واستعمال هذه المستندات.

[1]- سعيداني نعيم، مرجع سابق، ص 81.

أما المحطة التالية من محطات التجريم المعلوماتي في فرنسا فكانت عام 2004 عندما أضاف المشرع الفرنسي بموجبه جريمة أخرى هي جريمة التعامل في الوسائل التي تصلح أن ترتكب بها جريمة الدخول أو البقاء غير المصرح بها أو جريمة التلاعب بالمعطيات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات.[1]

الفرع الثاني: تجربة المشرع الجزائري في مكافحة جريمة المساس بأنظمة المعالجة الآلية للمعطيات

على غرار باقي الدول و تطبيقا للتوصيات الدولية التي شددت على وجوب النص في القوانين الداخلية وتجريم هذا النوع من الاعتداءات، كذلك فعل المشرع الجزائري بتعديله لقانون العقوبات بموجب الأمر 15/04 المؤرخ 2004/11/10 المعدل والمتمم بالأمر رقم 155/06 والذي أفرد القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات الذي يحوي ثماني مواد من 394 مكرر إلى 394 مكرر 7 أو ما يسمى بجرائم الغش المعلوماتي.[2]

والملاحظ أن تخصيص المشرع الجزائري لهذه الجرائم قسما خاصا في قانون العقوبات دلالة على إقراره بأنها ظاهرة مستجدة ومتميزة عن الجرائم التقليدية الأخرى من حيث المصالح التي تطالها وكذا من حيث مبناها وطبيعتها ومحلها، ومن ثم لا يمكن إدراجها تحت أي نوع من الجرائم التقليدية.

كما أنه لم يميز في وضعه لهذه النصوص القانونية نوعية المعلومات التي تطالها الجريمة في إذا كانت معلومات تتصل بمصالح اقتصادية أو مالية أو مسائل أمنية، وذلك سعيا من المشرع الجزائري إلى تعميم الحماية للمعلومات بكافة أنواعها ما عدى تشديد العقوبة إذا كانت المعلومات المستهدفة متعلقة بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.[3]

---

[1]– سعيداني نعيم، مرجع سابق، ص 81.

[2]– أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص** ، ج1، دار هومة ، ط 3، الجزائر، 2011، ص 447.

[3]– سعيداني نعيم، مرجع سابق، ص 79.

إضافة للجانب الإجرائي إذ نص المشرع على إجراءات للوقاية من الجريمة ومكافحتها بالقانون 04/09[1] المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، الذي تضمن في الفصل السادس النص على التعاون والمساعدة القضائية الدولية فيما يتعلق بهذه الجرائم.

والجدير بالذكر أنه بموجب القانون السالف الذكر الفصل الخامس منه تم استحداث ما يسمى:" الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحته"، في انتظار تحديد تشكيلة هيئتها وكيفيات تسييرها عن طريق التنظيم طبقا للمادة 13 من هذا القانون.

[1]– القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، ج ر، العدد 47، الصادرة سنة 2009.

المبحث الثالث:

صور المساس بأنظمة المعالجة الآلية للمعطيات

إن أي نظام معالجة آلية للمعطيات هدفه حماية تقنية للحفاظ وتأمين سرية الرسائل الالكترونية والبيانات المتناقلة خاصة في ميدان أعمال التجارة الالكترونية مثل البنوك تعتمد على شبكة الحاسب الآلي داخل البنك الواحد أو بين مختلف فروعه في دولة واحدة أو عدة دول أين تتم التحويلات المالية وغيرها من العمليات المصرفية داخل هاته الشبكة، وهو ما يستلزم حماية تقنية للمعلومات المتداولة ذات قيمة مالية حتى لا تكون في متناول قراصنة ومخترقي الشبكات المعلوماتية الذين لهم القدرة على الدخول للحسابات المالية الشخصية وتحويلهم لصالحهم.

وبهذا نجد أن المشرع الجزائري على غرار التشريعات الأخرى قد نص على أحكام خاصة لمحاربة الاعتداءات المتعلقة بأنظمة المعالجة الآلية للمعطيات، إذ نص على أربعة صور ماسة بالأنظمة المعلوماتية وهي:

1- جريمة الدخول والبقاء الغير شرعي في نظام المعالجة الآلية البسيط.

2- جريمة الإتلاف الغير عمدي للمعطيات.

3- جريمة المساس العمدي بالمعطيات.

4- جريمة التعامل في المعطيات غير المشروعة.

المطلب الأول: جريمة الدخول والبقاء الغير شرعي في نظام المعالجة الآلية

وهي الصورة التي نصت المادة 394 مكرر/1 من قانون العقوبات[1] على صور الدخول والبقاء الغير شرعي في نظام المعالجة الآلية وجاء في المادة المذكورة أعلاه على أنه:

"يعاقب بالحبس من ثلاث أ شهر إلى سنة و بغرامة من 50.000 دج إلى 200.000 دج

[1]- الأمر 66 - 156، المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 15-19 المؤرخ في 30 ديسمبر 2015، الجريدة الرسمية، العدد 71، سنة 2016.

كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

الفرع الأول: تعريف جريمة الدخول الغير الشرعي في نظام معالجة آلية للمعطيات

يعني الدخول كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي و يتحقق بالوصول إلى المعلومات والبيانات المخزونة داخل نظام معلوماتي دون رضا المسؤول عنه من شخص غير مرخص له باستخدامها.[1]

فالدخول الغير شرعي هو سلوك إيجابي ولم يحدد المشرع وسيلة الدخول، ومن هنا نقول أن المشرع قد وفق فيذلك لأنه يتعامل مع جريمة قد تكون أركانها متغيرة ومتطورة بتطور تكنولوجيا المعلومات، وبهذا تتحقق الجريمة في كل حالة يكون فيها الدخول مخالفا لشروط الدخول التي نص عليها القانون أو الاتفاق أو بمخالفة إرادة من له الحق في السيطرة على النظام الذي تم الدخول له.

وعليه فإن عملية الدخول في النظام المعلوماتي تتم بعدة طرق أهمها:

1- استخدام البرامج المخصصة لاختراق أنظمة الحماية الفنية في الحالات الطارئة، لأن إدارة و تشغيل هذه الحواسيب تقتضي وجود نوع من البرامج يمكن استخدمها لتخطي حواجز الحماية في الحالات الطارئة، وفي حالة اختلال وظائف الحاسب أو توقفه عن العمل و أشهرها برنامج يسمى (superzap)،[2] إلا أن هذا النوع من الأنظمة إذا ما وقع في أيدي غير مصرح لها باستخدامها فإن هذا يسمح لها بالتغلغل في منظومة الحاسب الآلي و لو كان محمي.

---

[1]- خالد ممدوح إبراهيم، **أمن المستندات الإلكترونية**، الدار الجامعية، الإسكندرية، 2008، ص 148.

[2]- جدي نسيمة، مرجع سابق، ص 51.

2- أبواب المصيدة (trap-doors) ويقصد بها الفواصل التي يتعمد واضعي البرامج تركها أثناء إعداده لتستخدم في إضافة ما يحلو لهم لاحقا.

3- استعمال ما يسمى بصناديق القمامة دون حذفه نهائيا.

4- طريقة المختصرات (raccourci) تتم باستغلال نقاط ضعف بالنظام للدخول إليه.[1]

5- القناع: وذلك أن يقوم الفاعل بإقناع الحاسوب بأنه شخص مرخص له بالدخول.

6- استخدام برامج خبيثة يتم دمجها في إحدى البرامج الأصلية للحاسب الآلي بحيث يعمل في جزء منه ليقوم بتسجيل الشفرات.

7- استخدام آلة طابعة مرفقة بجهاز الحاسب الآلي لاستخراج قائمة البرامج الموجودة داخل النظام.

8- التصنت على المعلومة المخزنة عن طريق التقاط المعلومات والبيانات المعالجة آليا بواسطة مكبر أو ميكروفون صغير أو مركز تنصت مما يسهل جميع الاتصالات المتداولة داخل النظام المعلوماتي.[2]

الفرع الثاني: مفهوم البقاء الغير الشرعي في نظام معالجة آلية للمعطيات

يعرف فعل البقاء الغير مشروع في نظام المعالجة الآلية للمعطيات بأنه التواجد فيه ضد إرادة من له الحق بالبقاء فيه، إذ يقترن فعل البقاء مع فعل الدخول، لهذا فتجريم الأول هدفه بالنسبة للجاني الذي لم يقصد الدخول عن طريق الغش في النظام لكن يبقى داخله وتنصرف إرادته إلى ذلك حيث كان بإمكانه مغادرة النظام.[3]

---

[1]- جدي نسيمة، مرجع سابق، ص 51.

[2]- بن دعاس فيصل، **إشكالات الجريمة المعلوماتية في التشريع الجزائري**، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة، 2010، ص 10.

[3]- عبد الفتاح بيومي حجازي، **الجريمة في عصر العولمة : دراسة في الظاهرة الإجرام ية المعلوماتية**، دار الفكر الجامعي، الإسكندرية، 2008، ص 83 .

وبهذا فإن سلوك البقاء في هذه الجريمة هو سلوك سلبي، حيث أن الجاني هنا يتعمد البقاء بالرغم من علمه أنه غير مصرح له بالبقاء داخل النظام ككل أو في جزء منه ويرفض الخروج، ومثال ذلك استعمال الجاني لخدمة الانترنت لمدة تطول عن تلك التي دفع مقابل استخدامها بواسطة الغش أو وسائل أخرى غير مشروعة.

الفرع الثالث: الجمع بين الدخول و البقاء الغير الشرعي في نظام معالجة آلية للمعطيات

قد تجتمع الجر يمتين في آن واحد بأن يتم الدخول عن طر يق الغش إلى نظام معلوماتي معين والبقاء فيه دون مغادرته، فتتوافر هنا أركان كل من الجريمتين معا، لكن نص المادة 394 مكرر من قانون العقوبات جعل من الدخول والبقاء جريمتين منفصلتين حيث نص على أنه كل من دخل أو بقي لو تأت العبارة مثلا:(كل من دخل وبقي)، فمعنى العبارة الأولى يختلف عن الثانية فهذه الأخيرة تتعلق بوصف جريمة واحدة، أما عن المعنى الأول فيتحدث عن جريمتين مستقلتين.[1]

ومنه نستنتج أن جريمة الدخول وقتية في حين جريمة البقاء مستمرة، فبهذا يمكن متابعة الجاني بجريمتي الدخول والبقاء في النظام المعلوماتي بطريق غير مشروعة على أساس التعدد الفعلي للجرائم.

المطلب الثاني: جريمة الإتلاف الغير عمدي للمعطيات

جاء في نص المادة 394 مكرر في الفقرة الثانية والثالثة من قانون العقوبات، حيث يشدد المشرع العقوبة في حالة ارتكاب الأفعال المتمثلة في حذف أو تغيير لمعطيات المنظومة، وهذه تمثل الصورة للمشددة لجريمتي الدخول والبقاء الغير شرعي في نظام المعالجة الآلية.

[1]– جدي نسيمة، مرجع سابق، ص 56.

الفرع الأول: الركن المادي لجريمة الإتلاف الغير عمدي للمعطيات

وبهذا فإن الجريمة الدخول أو البقاء في نظام المعالجة الآلية للمعطيات يترتب عليها إحدى النتائج الثلاث، وقد حددها المشرع على سبيل الحصر في نص المادة 394 مكرر/2 و3 ق وهي:[1]

-حذف المعطيات وذلك بإزالتها كليا عن طريق المحو أو الإلغاء.

-تغيير المعطيات أي المساس بالحالة الأصلية بحيث لا تبقى على ما كانت بعمليات عشوائية غير مدروسة.

-تخريب نظام التشغيل وجعله غير قابل للاستعمال.

ولكي تتحقق الجريمة يكفي أن تكون هناك علاقة سببية بين الدخول والبقاء الغير شرعي في النظام وبين النتيجة التي تحققت وهي إما بحذف المعطيات أو عدم قدرته على أداء وظيفته أو تغيير البيانات والمعطيات.[2]

الفرع الثاني: الركن المعنوي لجريمة الإتلاف الغير عمدي للمعطيات

إن جريمة الإتلاف الغير عمدي للمعطيات لا يشترط فيها القصد العمدي فهي من الجرائم الغير عمدية حيث تتحقق النتيجة فيها بغير قصد من الجاني عن طريق الخطأ دون سوء نية.

فظرف التشديد هنا ظرف مادي، فيكفي أن توجد بين الفعل الإجرامي والنتيجة علاقة سببية لكي نكون أمام جريمة عمدية، إلا إذا أثبت الجاني انتفاء تلك العلاقة كأن يثبت أن ذلك التغيير أو الإلغاء الذي حدث على مستوى النظام كانت سببه قوة قاهرة أو حادث مفاجئ.[3]

---

[1]- بن دعاس فيصل، مرجع سابق، ص 11.

[2]- جميل عبد الباقي الصغير، مرجع سابق، ص 20.

[3]- بن دعاس فيصل، مرجع سابق، ص 11.

المطلب الثالث: جريمة المساس العمدي بالمعطيات

وهي جريمة التلاعب بمعطيات أنظمة المعالجة الآلية المنصوص عليها في المادة 394 مكرر من ق ع حيث نصت على:" يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات و بغرامة مالية من 500.000 دج إلى 2.000.000 كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

كما نصت عليه المادة 5 و 8 من الاتفاقية الدولية للإجرام المعلوماتي على جريمة الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات، غير أن المشرع الجزائري اكتفى بالنص على الاعتداء العمدي للمعطيات الموجودة بداخل النظام والاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية، فإذا كان مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء غاية فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات.[1]

الفرع الأول: الركن المادي لجريمة المساس العمدي بالمعطيات

يتحقق السلوك الإجرامي في الجريمة المساس العمدي بالمعطيات يتحقق بإتيان الجاني لفعل من الصور الثلاث التالية عن طريق: فعل الإدخال، وفعل المحو أو الإزالة، وفعل التعديل وهي الصور التي منصوص عليها في المادة 394 مكرر 1 ق ع.

فلا يشترط الركن المادي توافر الصور الثلاث ، بل يكفي أن يقوم الجاني بإدخال معطيات مغلوطة جديدة لم تكن موجودة أو محو معطيات موجودة أو تعديل أخرى كانت موجودة أصلا يحتويها النظام، فغاية الأمر أن يرد الأمر على معطيات بإحدى الصور الثلاث التي سنأتي على شرحها تفصيلا و التي تشكل جزءا من النظام.[2]

---

[1]– أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، دار هومة، ط 2، الجزائر، 2007، ص 113.

[2]– جدي نسيمة، مرجع سابق، ص 63.

أولا/ فعل الإدخال: ويعني بإضافة معطيات جديدة على الدعامة الأساسية للنظام به سواء كانت خالية أم يوجد عليها معطيات من قبل البيانات والغاية من ذلك التشويش على صحّة البيانات القائمة، وإدخال معلومات مزورة ووضع معلومات غير للمعلومات الحقيقية.[1]

وقد يقوم بفعل الإدخال شخص أجنبي لا يحق له التواجد و استعمال النظام و أن يكون من المصرح لهم باستعمال النظام إلا أنه يعمد لإدخال معطيات خاطئة تخرج عن الاستعمال المنوط بمهامهم.

ويسهل ارتكاب هذه الصورة عند التشغ يل الأولي لأي نظام معالجة عند إدخال المعطيات لحفظها في المراحل الأولى للتشغ يل أ ي يقبل النظام أي معلومات صح يحة أو مغلوطة و يعمل على ح فظها ومثال ذلك حالة إدخال ف يروس الهدف منه إضافة معلومات جد يدة لم تكن موجودة وهذا النوع من ال فيروسات يصطلح عليه بفيروس حصان طروادة[2] والقنابل المعلوماتية.

وهناك طر يقة يطلق عليها اسم (بلوف) تتمثل في استخدام النظام من أجل طبع فواتي مصطنعة يقوم العملاء بتسد يدها، أ يضا في حالة أخرى قام المدعو فلادم يي بورليت و هو مهاجر روسي بإدخال فواتي وهمية لا حصر لها و تحو يل ما تم تسد يده لحساب شركات وهمية اصطنعها أيضا.[3]

---

[1]– عبد الفتاح بيومي حجازي، مرجع سابق، ص 92.

[2]– حصان طروادة هو برنامج يتم تشغيله داخل جهاز حاسوب الضحية ليقوم بأراض التجسس على أعماله حيث يقوم البرنامج منذ بداية التشغيل حتى إغلاق النظام بتسجيل كل طرقة على لوحة المفاتيح قام بها المعتدي عليه، كذلك يعمل هذا الفيروس على تغيير البرامج والبيانات والمعلومات داخل الحاسوب.

[3]– أحمد خليفة الملط، المرجع السابق، ص 182.

ثانيا/ المحو أو الإزالة: تعرف على أنها اقتطاع خصائص مسجلة على دعامة ممغنطة بمحوها أو طمسها أو عن طريق تحويل خصائص أخرى فوقها أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.[1]

وتكون عملية الإزالة ومحوها للمعطيات لاحقة لعملية الإدخال و تتمّ بواسطة برامج غريبة تقوم بالتلاعب بهذه المعطيات إما بمحوها كليا أو جزئيا من الذاكرة.[2]

والمشرع الجزائري لم ينص على طريقة المحو أو الوسائل المستخدمة للإزالة أو شرح صورها بل اكتفى بتعدادها في نص المادة 394 مكرر 1 ق ع، وبهذا فإن فعل الإزالة أو المحو يتحقق عند اختفاء المعطيات التي كانت داخل النظام.

ثالثا/ التعديل: وهو تغيير لحالة المعطيات الموجودة بدون تغيير الطبيعة الممغنطة لها، كما يعرف على أنّه كل تغيير غير مشروع للمعلومات و البرامج يتمّ عن طريق استخدام إحدى وظائف الحاسب الآلي.[3]

ويقصد بالتعديل أيها هو تغيير المعطيات الموجودة داخل النظام و استبدالها بأخرى جزئيا أو كليا ويتم هذا التعديل عن طريق استبدالها أو التلاعب بالبرنامج بإمداده بمعطيات مغايرة عن تلك التي صمم لأجلها.[4]

وجاء في التوصيات الصادرة عن المجلس الأوروبي المتعلقة بالجرائم المعلوماتية التفريق بين التعديلات التي تؤدي إلى نتائج سلبية، والتعديلات التي تساعد على تحسين النظام، حيث كانت من التوصيات إدراج التعديلات الأولى ضمن قائمة الجرائم المعلوماتية، أما التي لها آثار إيجابية فتكون ضمن القائمة الاختيارية، لكن معظم التشريعات لم تأخذ بهذا

---

[1]- محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2007، ص 184.

[2]- عبد الفتاح بيومي حجازي، **الجريمة في عصر العولمة**، مرجع سابق، ص 93.

[3]- محمد أمين الشوابكة، **جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)**، مكتبة دار الثقافة للنشر والتوزيع، الأردن، 2004، ص 232.

[4]- عبد الفتاح بيومي حجازي، **الجريمة في عصر العولمة**، مرجع سابق، ص 95.

التفريق بعين الاعتبار، من بينهم المشرع الجزائري الذي جرم صورة التعديل على مطلقها بغض النظر عن الآثار التي تترتب عليها سواء كانت إيجابية أو سلبية، فيكفي أن يتحقق فعل تعديل أو تغيير المعطيات داخل النظام لتقوم جريمة الاعتداء العمدي على المعطيات.[1]

الفرع الثاني: الركن المعنوي لجريمة المساس العمدي بالمعطيات

جريمة المساس العمري بالمعطيات هي جريمة عمدية تتطلب قصد جنائي عام بعنصريه العلم والإرادة، وهذا ما يستشف من نص المادة 394 مكرر1 ق ع، حيث أن إرادة الجاني تتجه إلى ارتكاب صورة من صور جريمة المساس أو التلاعب العمدي بالمعطيات، فيقوم بإزالة بيانات ومعطيات متواجدة داخل النظام أو تعديلها أو إدخال معطيات داخل نظام المعالجة الآلية للمعطيات، وهو يعلم أن سلوكه قد يؤدي لا محالة إلى نتيجة معينة.

وبهذا فإن هذه الجريمة لا تتطلب قصد جنائي خاص إذ تقوم بمجرد قصد الجاني بالتلاعب والمساس بالمعطيات المتضمنة بنظام المعالجة الآلية للمعطيات.[2]

المطلب الرابع: جريمة التعامل في المعطيات غير المشروعة

نصت عليها المواد 03 و04 و08 من الاتفاقية الدولية للإجرام المعلوماتي ويقابلها نص المادة 394 مكرر 02 من قانون العقوبات التي نصت على أنه:" يعاقب بالحبس من شهرين(02) إلى ثلاثة(03) سنوات وبغرامة من 1.000.000 إلى 10.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

---

[1]– خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، دار الفكر الجامعي، الإسكندرية، 2010، ص 68.

[2]– جدي نسيمة، مرجع سابق، ص 69.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من أحدى الجرائم المنصوص عليها في هذا القسم".

وبهذا فإن المادة المذكورة أعلاه تستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هي المعطيات مثل: التصميم، البحث، التجميع، التوفير، النشر والاتجار في معطيات المعالجة أو مخزنة أو مرسلة موجودة خارج النظام...، وأن تكون فيه المعطيات محصلة أو نتيجة لارتكاب جريمة الاعتداءات الماسة بنظام المعالجة الآلية للمعطيات وتتحقق بإتيان أحد الأفعال المتمثلة في حيازتها أو إفشاؤها أو نشرها أو استعمالها مثل أعمال الجوسسة، الإرهاب، التحريض على الفسق وفساد الأخلاق.[1]

الفرع الأول: الركن المادي لجريمة التعامل في المعطيات غير المشروعة

من خلال هذا الفرع سنقسمه إلى نقطتين هامتين:

1- محل الجريمة

2- السلوك الإجرامي المتمثل في فئيتين:

-التعامل في معطيات صالحة لارتكاب جريمة

- التعامل في معطيات متحصلة من جريمة

أولا/ محل جريمة التعامل في المعطيات غير المشروعة:

طبقا لنص المادة 394 مكرر 02 من قانون العقوبات أن محل جريمة التعامل في المعطيات غير المشروعة يكون إما:

1-معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية.

[1]- بن دعاس فيصل، مرجع سابق، ص 12.

2- معطيات متحصل عليها من إحدى الجرائم المنصوص عليها بالمواد 394 مكرر و 394 مكرر 01 من ق ع. [1]

نجد المشرع الجزائري قد وسع من دائرة التجريم بهذا التعداد وكان هدفه من ذلك حماية المعطيات مهما كانت حالتها سواء كانت مرسلة أو مخزنة أو معالجة على اعتبار إمكانية ارتكاب جرائم حتى باستعمال معطيات موجودة على وسائط تخزين خارجية، ولم يشترط أيضا في قيام الجريمة أن تكون المعطيات المعدة خصيصا لارتكاب الجريمة من جرائم الماسة بالأنظمة المعلوماتية بل يكفي أن تكون صالحة أو قابلة لأن ترتكب بها الجريمة. [2]

ثانيا/ السلوك الإجرامي:

1- **التعامل في معطيات صالحة لارتكاب جريمة:** محل جريمة التعامل في معطيات صالحة لارتكاب جريمة كما هو مبين في نص المادة 394 مكرر02 من ق.ع.ج هو المعطيات المحزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، فالمعطيات تمر بالعديد من المراحل حتى تصل إلى يد الجاني فيرتكب بها جريمته، و هذه المراحل هي:

أ- **التصميم والبحث:** التصميم هو إيجاد وخلق معطيات صالحة لارتكاب جريمة وهذا العمل يقوم به المتخصصون كالمبرمجين و مصممي البرامج مثلا : تصميم فيروس، برامج خبيثة، برامج اختراق و قرصنة ...، ففعل التصميم جرمه المشرع بصورة مستقلة إذا كان بإمكانه أن يستعمل لاحقا في ارتكاب أحد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات السالف ذكرها كالدخول أو البقاء أو الإدخال أو الإزالة أو التعديل، وبالتالي فالمشرع أراد أن يلعب دورا وقائيا للحد من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أما البحث فهو كيفية تصميم المعطيات و إعدادها من أجل ارتكاب الجريمة و ليس مجرد البحث عن المعطيات بتشغيل أحد محركات البحث الموجودة داخل الشبكة.

---

[1]- جدي نسيمة، مرجع سابق، ص 72.

[2]- بن دعاس فيصل، مرجع سابق، ص 12.

ب- التجميع والتوفير: هو جمع عدد من المعلومات التي يمكن أن ترتكب بها جرائم الدخول أو البقاء في المنظمة بطريق الغش أو التلاعب في المعطيات، و يفترض ذلك أن يحتفظ الجاني بمجموعة من المعطيات التي تشكل خطرا و التي من الممكن استعمالها في ارتكاب تلك الجرائم.[1]

أما التوفير فقد ورد بالنص الفرنسي عبارة (met a disposition) والترجمة الحرفية لها هي "الوضع تحت التصرف "وهو ذات المصطلح الوارد في اتفاقية بودابست وهو المعنى الأدق والأكثر ملائمة وعليه يقصد بالتوفير وضع المعطيات الممكن استخدامها في ارتكاب جريمة تحت تصرف الغير و إتاحتها لمن يريد استخدامها.[2]

جـ- النشر والاتجار : النشر هو إذاعة المعطيات وتمكين الغير من الاطلاع عليها، وهو تصرف خطير باعتباره يسمح بأن تكون هذه المعطيات في متناول عدد كبير من الأشخاص.[3]

ومصطلح الاتجار يشير مباشرة للمقابل لقاء الحصول على المعطيات من أجل استخدامها و قد يكون المقابل نقدي أو عيني أو خدماتي.

2- **التعامل في معطيات متحصلة من جريمة :** وهي الأفعال التي نصت عليها الفقرة الثانية من المادة 394 مكرر 02 من قانون العقوبات، وتشمل: حيازة، إفشاء، نشر، استعمال لأي غرض كان المعطيات المتحصل عليها من أحد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أ- الحيازة: و تعرف الحيازة في نطاق القانون الجنائي على أنها رابطة واقعية بين شخص و مال (منقول) تتيح للأول أن يسيطر على الثاني سيطرة مستقلة مقترنة بنيّة

---

[1]- محمد خليفة، مرجع سابق، ص 201.

[2]- بوذراع عبد العزيز، **خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** (مذكرة ماجستير في القانون الجنائي والعلوم الجنائية)، كلية الحقوق، جامعة الجزائر1، 2011، ص 68.

[3]- بوذراع عبد العزيز، مرجع سابق، ص 68.

الاحتباس و تكون السيطرة على المال مستقلة إذا كان يمكن للشخص أن يمارس أي عمل على الشيء بدون رقابة من شخص آخر له على المال سلطة قانونية أعلى بمقتضى حق من الحقوق.[1]

والحيازة في جريمة التعامل في المعطيات غير المشروعة هي مركز واقعي يكون دائما يستند لسبب غير شرعي، و يشترط في الحيازة ما يلي :

- أن تكون متحصله من إحدى جرائم المعطيات.
- أن تكون بسيطرة الحائز على المعطيات سيطرة مطلقة بإفنائها أو تعديلها أو استعمالها، أو سيطرة واقعية محدودة و ذلك بالانتفاع بها.
- اقتران السيطرة على المعطيات بنيّة التملك و الاحتباس الدائم.

ب- الإفشاء: يقصد بالإفشاء نقل المعطيات من حيازة الشخص الذي تحصل عليها بطريقة غير مشروعة إلى غيره ومن يقوم بذلك ليس مؤتمنا على المعطيات فقد لا يكون ملزما قانونا بكتمانها التي قام بإفشائها إنما تحصل عليها أيضا بطريقة غير مشروعة و نشرها.

جـ- النشر: سبق وتطرقنا للنشر بصدد التعامل في المعطيات الصالحة لارتكاب جريمة و هي صورة مشتركة بين هذه الأخيرة والتعامل في معطيات متحصلة من جريمة وهو ذات المفهوم باختلاف المحل والمقصود منه إذاعة المعطيات والتمكين من الإطلاع عليها بأي وسيلة من وسائل النشر.[2]

د- الاستعمال: وهو يشمل أي استعمال للمعطيات المتحصل عليها من إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مهما كان نوعه و هدفه ولا يهم عدد المرات التي تم فيها الاستعمال، إذ يمكن أن يكون لمرة واحدة أو عدة مرات.[3]

---

[1] - محمد خليفة، المرجع السابق، ص 205.

[2]- جدي نسيمة، مرجع سابق، ص 75.

[3]- بوذراع عبد العزيز، مرجع سابق، ص 69.

الفرع الثاني: الركن المعنوي لجريمة التعامل في المعطيات غير المشروعة

جريمة التلاعب بالمعطيات داخل نظام المعالجة الآلية للمعطيات تعتبر من الجرائم العمدية فيجب توافر قصد جنائي عام وقصد جنائي خاص ، ففي القصد العام يجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم أن سلوكه الإجرامي يترتب عليه التلاعب في المعطيات وأنه ليس له الحق في القيام بهاته الأفعال، وأنه يعتدي على صاحب حق في السيطرة على تلك المعطيات أو بدون موافقته.

وحتى تقوم الركن المعنوي كذلك لابد أن يتوافر قصد جنائي خاص وهو نية الغش فلا تقوم الجريمة إلا إذا قام الجاني بهذه العملية بنية الغش وخارج الاستعمال المرخص به.

وفي جريمة الاعتداء على المعطيات خارج النظام فهذه الجريمة عمدية فيجب توافر القصد الجنائي العام وهي: اتجاه النية إلى التصميم أو البحث أو تجميع أو توفير أو شراء أو الاتجار أو حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، كما يجب أن يعلم بأن هاته الأفعال يمكن أن تؤدي إلى حذف أو تغيير أو تخريب أو إفشاء لأي منظومة معطيات.

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجاني العام قصد جنائي خاص وهي بنية الغش، هذا لا يعني بالضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق هذا عن طريق بنية الغش.[1]

[1]– لحمر نبيل، **دور الأقطاب الجزائية المتخصصة في مكافحة الجريمة** (مذكرة ماجستير في قانون العقوبات والعلوم الجنائية)، كلية الحقوق، جامعة قسنطينة 1، 2014، ص 135.

الفصل الثاني :

آليات قمع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تمهيد:

نظرا للخصوصية التي تتميز بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات عن باقي الجرائم الأخرى إذ أنها ذات طابع دولي، هذا ما جعل جل التشريعات الوطنية تسعى إلى الوصول إلى حلول ناجعة وذلك بتخصيص نصوص موضوعية وإجرائية لقمع هذا النوع من الجرائم، ولتنظيم اختصاص الهيئات القضائية والتحري والمتابعة، وكذا جمع الأدلة الرقمية.

وفي ذلك فقد وسعت الدول الجهود في مجال التعاون الدولي لمكافحة الجريمة وخصتها بقواعد وإجراءات فعالة، حيث نجد أن المشرع الجزائري قد اعتمد على توصيات الاتفاقية الدولية للإجرام المعلوماتي وذلك باستحداث مواد تنص على هذه الجرائم وتعاقب على الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، إضافة إلى مواد أخرى تنص على قواعد إجرائية لمكافحة وقمع هذه الجرائم.

وستناول في هذا الفصل التطرق إلى آليات قمع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في مبحثين مستقلين، حيث تناولنا في المبحث الأول الاختصاص والتحري في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أما المبحث الثاني فقد خصصناه الإثبات في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجزاءات المقررة لها.

المبحث الأول:

الاختصاص والتحري في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

إن طبيعة الجرائم الماسة بالأنظمة المعلوماتية وعناصرها ووسائل ارتكابها دفعت بالمشرع الجزائري إلى تكريس قواعد إجرائية يمكن الاعتماد عليها في الوصول إلى الدليل المناسب لإثبات هذا النوع من الجرائم، على عكس تلك القواعد الإجرائية التقليدية التي لا تستطيع استخلاص الدليل، إذ أن هذا النوع من الجرائم يتطلب أن تكون هناك إجراءات ذات طبيعة تقنية وتقتضي السرعة في التحري والتحقيق فيها خشية ضياع الدليل.

ومنه فإن هذه الجرائم تتم في بطيعة خاصة يتوجب لمواجهتها تأهيل نوع خاص من رجال الضبطية والقضاة من نيابة وتحقيق وحكم، خاصة مع استحداث الأقطاب الجزائية المتخصصة.

وبهذا سنتناول فقد قسمنا هذا المبحث إلى مطلبين مستقلين، تناولنا في المطلب الأول مسألة الاختصاص في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أما المطلب الثاني فقد تطرقنا إلى التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

المطلب الأول: مسألة الاختصاص في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

الاختصاص هو مباشرة سلطة المتابعة والتحقيق والحكم في الجريمة وفقا للقواعد التي رسمها القانون والحدود التي تبناها المشرع لهذه السلطات أثناء ممارسة مهامها، و حدد المشرع الجزائري معايير الاختصاص المحلي في قانون الإجراءات الجزائية في المواد 37، 40، 329.

وقبل كل هذا سنتعرف على القانون الواجب التطبيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الفرع الأول: القانون الواجب التطبيق بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

جاء في نص المادة 22 من القانون العربي النموذجي الموحد لمكافحة جرائم الكمبيوتر والانترنت على أ نه تسري أحكام التشر يع الجنائي للدولة على الجر يمة المعلوماتية إذا ارتكبت كلها أو جزء م نها داخل حدود ها، كما تختص المحاكم فـيها بنظر الدعوى المترتبة عن تلك الجرائم وعلى الدول العرب ية عقد اتفاقات لتبني المع يار الأول في حالة تنازع الاختصاص بين الدول، كما يسري التشريع الجنائي للدولة على الجرائم المعلوماتية التي تقع خارج الحدود إذا كانت مخلة بأم نها وفقا للقواعد العامة المنصوص عل يها في قانون العقوبات.[1]

أما المادة 03 من قانون العقوبات الجزائري فقد نصت على أنه يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الج مهورية، كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائر ية طبقا لأحكام قانون الإجراءات الجزائية وبهذا فإن القانون الجزائري يطبق في حالتين هما:

- حالة ارتكاب الجريمة فوق الإقليم الوطني.
- حالة ارتكاب الجر يمة في الخارج و لك نها تدخل ضمن اختصاص الجهات القضائية الجزائرية استنادا لأحكام قانون الإجراءات الجزائية.

1- **الجرائم المرتكبة فوق الإقل يم الوطني :** كرست المادة 03 من قانون العقوبات الجزائري مبدأ إقليمية القانون الذي يرتكز على مبدأ أساسي وهو سيادة الدولة، أي بسط الدولة لسيادتها وسلطانها فوق إقليمها والذي يتخذ عدة مظاهر من بينها تطبيق قانون الدولة فوق إقليمها.

[1]- عبد الفتاح بيومي حجازي، مرجع سابق، ص 49.

فإذا وقعت الجريمة فوق إقليم الدولة الجزائري، فقانون العقوبات الجزائري يفرض نفسه سواء حصلت النتيجة داخل الإقليم الوطني أو خارجه، المهم هو أن يكون أحد العناصر المكونة لأركان الجريمة قد حصل داخل الإقليم الجزائري، وهذا ما كرسته المادة 586 من قانون الإجراءات الجزائية التي تنص على أنه :" تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المذكورة لها قد تم في الجزائر".

ويتكون لإقليم من المجال البري والجوي والبحري للدولة [1](المادة 13 من الدستور التي تنص على أنه:" تمارس سيادة الدولة على مجالها البري، ومجالها الجوي، وعلى مياهها. كما تمارس الدولة حقها السيد الذي يقره القانون الدولي على كل منطقة من مختلف مناطق المجال البحري التي ترجع إليها)[2]، وبهذا ففي حالة ارتكاب شخص جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فوق إقليم الدولة الجزائري فقانون العقوبات الجزائري يطبق عليه مهما كانت جنسيته.

2- **الجرائم المرتكبة في الخارج :** تنص المادة 03 من قانون العقوبات على مبدأ إقليمية قانون العقوبات، وبهذا أن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي ترتكب خارج الإقليم الوطني لا يسري عليها قانون العقوبات الجزائري كأصل عام ، وكاستثناء نجد أن المشرع الجزائري قد كرس مبدأين لا يقل عن الآخر أهمية وهما مبدأ الشخصية والذي بمقتضاه يطبق النص الجزائي على كل من يحمل جنسية الدولة ولو ارتكب جريمته في خارج إقليمها، ومبدأ العينية الذي بمقتضاه يطبق على الجاني الأجنبي الذي ارتكب الجرم في الخرج لكن مس بالمصالح الأساسية الجزائرية.[3]

---

[1]– أحسن بوسقيعة، **الوجيز في القانون الجزائي العام**، دار هومة، ط 10، الجزائري، 2011، ص 89.

[2]– القانون رقم 16–01 المؤرخ في 06 مارس 2016 المعدل للدستور الجزائري، ج ر، رقم 14، المؤرخة في 7 مارس 2016، ص 16.

[3]– أحسن بوسقيعة، مرجع سابق، ص 93.

وتبعا لما سبقا تثار مسألة التعاون الدولي في مجال مكافحة الجر يمة المعلوماتي الذي صار مهما للغاي في ظل العولمة والعالمي التي أصبحت تتم ي بها الجر يمة المنظمة والتي من بينها جرائم المعلوماتي، فالاعتداء على سر ي المعلومات وخصوصيتها بقصد الاستيلاء أو التخر يب أو التجسس أصبح هاجسا للشركات العالمية و الهيئات الحكومية وغ ي الحكومي.

ونظرا لتبادل المعلومات المشفرة التي قد يكون لها صلة بالتجسس السياسي أو العسكري أو الاقتصادي أو نشاطات إجرام ي أخرى ناد ى الكثي بضرورة إنشاء وحدات خاصة بمكافحة الجر يمة المعلوماتي موازاة بالشرطة الدولي "أنتربول"، وهو ما يعني إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات الخاصة في الانترنت وتبادل الخبرات والمعلومات، ولكن الخصوصي التي تتمتع بها الجر يمة المعلوماتي وضعت عراقيل في سبي تحقيق تعاون دولي ناجع، وتظهر على مستوي ين وهما:

المستوى الأول: يتعلق بمشكل الاختصاص الناتج عن التداخل بين شبكات المعلومات، فكما سبق ذكره يمكن أن ترتكب الجر مة في الدولة (أ) و يتحقق الضرر في الدولة (ب).

المستوى الثاني: يتعلق بمشكل انعدام نموذج واحد متفق عليه يتعلق بالنشاط الإجرامي في الجريمة المعلوماتي الذي يغري القراصنة على تنو ع الأسالي المستعملة في ارتكاب جرائمهم دون تقي بالحدود الجغرافي، إلى جانب إخفاء الشخصي الذي يستفيدون منه ويسهل لهم ممارسة نشاطا تهم وصعوبة الوصول إل يهم خاصة في ظل عدم تكييف بعض الدول لتشريعاتها و تحيينها.[1]

الفرع الأول: الاختصاص القضائي للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

[1]– بوذراع عبد العزيز، مرجع سابق، ص ص 101–102.

الاختصاص هو مباشرة سلطة المتابعة والتحقيق والحكم في الجرائم وفقا للقواعد التي رسمها القانون والحدود التي تبناها المشرع لهذه السلطات أثناء ممارسة مهامها، وبهذا سنحاول في هذا الفرع التطرق إلى الاختصاص المحلي لمختلف الجهات القضائية والجهات المختصة في البحث والتحري في الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات.

أولا/ الاختصاص المحلي لضباط الشرطة القضائية:

منح المشرع الجزائري للضبطية القضائية مهمة البحث والتحري عن الجرائم المحددة قانونا، وذلك في مرحلة أولية قبل أن يباشر بشأنها التحقيق القضائي وهذا ما نستشفه في نص المادة 12/ 3 من قانون الإجراءات الجزائية والتي تنص على أنه:" يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها بتحقيق قضائي".[1]

وبهذا فإن الاختصاص المحلي لضباط الشرطة القضائية يقصد به المجال الإقليمي الذي يباشر فيه ضباط الشرطة القضائية مهامه في التحري والبحث عن الجريمة، ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة، إلا أنه وفي الحالة الاستثنائية يجوز لهم أن يباشروا مهمتهم في كافة التقليم الوطني [2]، إذا طلب منهم ذلك قاضي المختص قانونا، ويجب أن يساعدهم في ذلك ضابط الشرطة القضائية الذي يمارس وظائفهم في المجموعة السكنية المعنية، وفي ذلك يجب أن يخبروا مسبقا وكيل الجمهورية الذين يباشرون مهمتهم في دائرة اختصاصه.[3]

---

[1]- الأمر 66 - 155، المؤرخ في 8 جوان 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بالقانون رقم 15-22 المؤرخ في 13 مارس 2016، الجريدة الرسمية، العدد40 سنة 2016.

[2]- زيبخة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي** ، دار الهدى، الجزائر، 2011، ص ص 106-107.

[3]- محمد حزيط، **مذكرات في قانون الإجراءات الجزائية الجزائري**، دار هومة، الجزائر، ط 8، 2013، ص 90.

إذا تعلقت الأبحاث والمعاينات بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة للمعطيات وجرائم تبييض الأموال وجرائم الإرهابية والجرائم المتعلقة بالتشريع الخاص بالصرف، إذ نجد أن قانون الإجراءات الجزائية قد وسع من دائرة الاختصاص المحلي لضباط الشرطة القضائية وجعلها وطنيا، بعض النظر إلى الجهة التي ينتمي إليها فيكفي أن يحمل صفة الضبطية القضائية، وهذا بطبيعة الحال يكون تحت إشراف النائب العام بالمجلس القضائي المختص إقليميا ويعلم وكيل الجهورية المختص إقليميا بجميع الحالات.

عليه فإنه يمكن القول أن إجراءات البحث و التحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أم ابتدائيا، و هذا المفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولي، بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا.

ثانيا/ الاختصاص المحلي لوكيل الجمهورية:

أما عن الاختصاص المحلي لوكيل الجمهورية يتحدد بمكان وقوع الجريمة أو بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر، هذا ما جاء في نص المادة 37 من قانون الإجراءات الجزائية.[1]

ثالثا/ الاختصاص المحلي لقاضي التحقيق:

[1]– المادة 37 من قانون الإجراءات الجزائية.

جاء في نص المادة 1/40 ق إ ج على الاختصاص المحلي لقاضي التحقيق والذي يتحدد بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المش تبه في مسا همتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.[1]

رابعا/ الاختصاص المحلي لجهات الحكم:

و أما فيما يخص جهات الحكم في مواد الجنح فتنص المادة 329 على أنه تختص محليا بالنظر في الجنحة المحكمة محل ارتكاب الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر.

كما تختص محكمة محل حبس المحكوم عليه استثناء طبقا لأحكام المواد 552 و553 من قانون الإجراءات الجزائية، إذا كان المحكوم محبوسا بحكم نهائي أولا عليه بعقوبة سالبة للحرية بنظر القضايا المنسوبة إليه فيما يخرج عن المواد 40، 37 و329 ق إ ج، وفي ذلك تختص المحكمة في نظر الجنح والمخالفات الغير قابلة للتجزئة أو المرتبطة.

ويرجع الاختصاص للمحكمة التي ارتكبت في نطاق دائ رتها المخالفة أو المحكمة الموجودة في بلد إقامة مرتكب المخالفة بالنظر في تلك المخالفة.

ونوعيا بالنسبة للأحداث فإن قسم الأحداث المختص إقل يميا هو المحكمة التي ارتكبت الجريمة بدائرة اختصاصها أو بها محل إقامة الحدث أو واليه أو وصيه، أو محكمة المكان الذي عثر فيه على الحدث أو المكان الذي أودع به الحدث سواء بصفة مؤقتة أو نهائية طبقا لأحكام المادة 451/ 3 ق إ ج.[2]

وعن معيار مكان وقوع الجر يمة فهو يختلف حسب ط بيعة الجريمة إذ يتحدد بالنسبة للجريمة الوقتية بالمكان الذي وقع فيه تنفيذ الفعل، وبالنسبة للجر يمة المستمرة يتحدد المكان

[1]– المادة 1/40 من قانون الإجراءات الجزائية.

[2]– جدي نسيمة، مرجع سابق، ص ص 84–85. ،

بكل مكان قامت فيه حالة استمرار الفعل، وبالنسبة للجرائم المتتابعة يعتبر مكان ارتكاب الجريمة كل مكان تقع فيه أحد الأفعال.

أما عن محل إقامة المتهم فالعبرة بالمحل الذي كان يقيم فيه المتهم وقت اتخاذ إجراءات المتابعة بغض النظر عن التغييرات التي تحدث به.[1]

خامسا/ توسيع الاختصاص:

كما هو معروف أن تختص جهة قضائية معينة بالفصل في الدعوى العمومية الرامية إلى توقيع العقاب على الجاني، إذ تكون مختصة إقليميا إما: بمكان وقوع الجريمة، أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها، أو مكان إلقاء القبض على أحد هؤلاء الأشخاص حتى ولو حصل القبض لسبب آخر.

إلا أنه عند تعديله لقانون الإجراءات الجزائية بموجب القانون رقم 14/04[2] المؤرخ في 2004/11/10 تم تمديد الاختصاص الإقليمي لوكلاء الجمهورية وقضاة التحقيق وقضاة الحكم لجهات قضائية معينة لتشمل دوائر اختصاص جهات قضائية أخرى في جرائم محددة ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وترك المجال للتنظيم لتحديد هذه الجهات القضائية ذات الاختصاص الموسع.

وبعد ذلك تم إصدار المرسوم التنفيذي رقم 06/348 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[3]، وبهذا تم إنشاء جهات قضائية موسعة أي ذات اختصاص موسع أو ما يعرف في العرف

---

[1]– جيلالي بغدادي ، **التحقيق دراسة مقارنة وتطبيقية**، الديوان الوطني للأشغال التربوية، الجزائر1999، ص 108.

[2]– المادة 2/37 من القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية، ج ر، العدد 72، الصادرة بتاريخ 10 نوفمبر 2004.

[3]– المرسوم التنفيذي رقم 348–06 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر، العدد 63، الصادرة بتاريخ 08 أكتوبر 2006.

القضائي بالأقطاب الجزائية المتخصصة والتي تم تفعيلها سنة 2008، وتكون في أربع جهات تشمل:

- **محكمة سيدي أمحمد التابعة لمجلس قضاء الجزائر** : يتوسع اختصاصها الإقليمي طبقا للمادة 02 من المرسوم ليشمل دوائر اختصاص المحاكم التابعة لمجالس قضاء: الجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة، عين الدفلى (أي 12 مجلس قضائي).[1]

- **محكمة قسنطينة التابعة لمجلس قضاء قسنطينة:** يتوسع اختصاصها الإقليمي طبقا للمادة 03 من المرسوم ليشمل دوائر اختصاص المحاكم التابعة لمجالس قضاء : قسنطينة، أم البواقي، باتنة، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق أهراس، ميلة (أي 17 مجلس قضائي).[2]

- **محكمة وهران التابعة لمجلس قضاء وهران:** يتوسع اختصاصها الإقليمي طبقا للمادة 05 من المرسوم ليشمل دوائر اختصاص المحاكم التابعة لمجالس قضاء: وهران، بشار، تلمسان، تيارت، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تموشنت، وغليزان (أي 13 مجلس قضائي).

- **محكمة ورقلة التابعة لمجلس قضاء ورقلة** : يتوسع اختصاصها الإقليمي طبقا للمادة 04 من المرسوم ليشمل دوائر اختصاص المحاكم التابعة لمجالس قضاء : ورقلة، أدرار، تمنراست، إليزي، تندوف، وغرداية (أي 06 مجالس قضائية).

يسير هذه الأقطاب 37 قاضيا موزعين على حسب اختصاصهم من نيابة وقضاة تحقيق وقضاة حكم[3]، يتم اختيارهم من ضمن القضاة الأكثر كفاءة والذين تلقوا تكوينا متخصصا في

---

[1]– المادة 02 من المرسوم التنفيذي رقم 348–06.

[2]– المادة 03 من المرسوم نفسه.

[3] - **La réforme de la justice en Algérie piétine**, http://www.algerie-dz.com/article9990.html, تاريخ الاطلاع: 2017/05/04، الساعة : 20:57.

الجرائم التي خولهم القانون سلطة النظر فيها نذكر منها: جريمة تبييض الأموال، جرائم الصرف، جرائم الفساد، جرائم المخدرات، الجرائم الإرهابية، الجرائم الماسة بأنظمة المعالجة الآلية، والجريمة المنظمة العابرة للحدود.

ولتوضيح ذلك، إذا ارتكب شخص مقيم بمدينة البويرة جريمة ماسة بأنظمة المعالجة الآلية للمعطيات بهذه المدينة، فالأصل هو أن تختص محكمة البويرة محليا بالنظر في القضية ولكن ما دام أن الأمر يتعلق بجريمة تدخل ضمن اختصاص الجهة القضائية ذات الاختصاص الموسع فإنه يجوز لمحكمة سيدي أمحمد النظر في القضية، وبالتالي فكلتا الجهتين القضائيتين (البويرة وسيدي أمحمد) مختصتين، الأولى استنادا للقواعد العامة للاختصاص المحلي والثانية استنادا لطبيعة الجرم المرتكب وتمديد الاختصاص لهذه الجهة بنص قانوني خاص.

وتجدر الإشارة إلى أن تمديد الاختصاص للجهة القضائية ذات الاختصاص الموسع هو أمر جوازي وليس إجباري كون المواد 37، 40، 329 من قانون الإجراءات الجزائية استعملت عبارة "يجوز تمديد الاختصاص المحلي..."، بمعنى أنه إذا نظرت المحكمة الأصلية في الدعوى فهذا جائز، أما إذا نظرت فيها الجهة القضائية ذات الاختصاص الموسع فهذا جائز أيضا.[1]

المطلب الثاني: التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة أن إجراءات البحث و التحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أم ابتدائيا.

[1]– بوذراع عبد العزيز، مرجع سابق، ص ص 105–106.

وبهذا نجد أن المشرع الجزائري قد أرسى قواعد ذات طبيعة خاصة وفعالة في مكافحة جريمة المساس بأنظمة المعالجة الآلية للمعطيات، فقد جاء قانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث جاء في نص المادة 03[1] من نفس القانون على أنه مما تتطلبه مستلزمات التحريات أو التحقيقات القضائية وهي وضع ترتيبات تقنية هدفها مراقبة الاتصالات الإلكترونية وتجميعها وتسجيلها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، وشروط صحة هذه الإجراءات ومهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وفي ذلك نجد أن المادة 10 من القانون المذكور أعلاه قد ألزمت على تقديم المساعدة لسلطات التحري القضائية لجمع وتسجيل المعطيات ومحتوى الاتصالات التي يتعين عليهم حفظها وذلك طبقا للمادة 11 من نفس القانون.

أما المادة 11 هي الأخرى قد ألزمت مقدمي الخدمات حفظ البيانات لمدة سنة من تاريخ التسجيل، بالتعرف على مستعمل الخدمة، المعطيات المتعلقة بالتجهيزات، الخصائص التقنية من تاريخ ووقت ومدة كل اتصال، المعطيات التي تسمح بالتعرف على المرسل و المرسل إليه...[2]

وبهذا سنتطرق في هذا المطلب على الاختصاصات العادية وغير العادية في التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

[1]- المادة 03 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، العدد 47، الصادرة بتاريخ 16 أوت 2009.

[2]- المادة 10 و11 من القانون نفسه.

الفرع الأول: الاختصاصات العادية في التحري والتحقيق

الاختصاصات العادية في التحقيق والتحري في الجرائم الماسة بالأنظمة المعلوماتية تعتبر أساليب من شأنها أن تساعد في كشف الحقيقة والتعرف على هوية الجاني، وتشمل الانتقال إلى مسرح الجريمة ومعاينته، وكذا التفتيش أي تفتيش المنظومة المعلوماتية، التوقيف للنظر.

أولا/ الانتقال والمعاينة: جاء في نص المادة 79 ق إ ج أنه يجوز لقاضي التحقيق الانتقال إلى مكان وقوع الجريمة وذلك لإجراء المعاينات اللازمة، ويخطر في ذلك وكيل الجمهورية الذي يملك كل الصلاحيات للتنقل إلى عين المكان مستعينا معه كاتب التحقيق الذي يقوم بدوره بتحرير محضر بما يقوم به من إجراءات.[1]

وبهذا فالمعاينة يقصد بها رؤية محل ارتكاب الوقائع الجنائية و إثبات حالتها بالشكل الذي تركها عليها الجاني عقب ارتكاب الجريمة كما تنصرف إلى فحص و إثبات ما يوجد من آثار[2]، وبهذا فهي فحص مكان الجريمة أو شيء أو شخص له علاقة بالجريمة.

وعند تطبيق إجراء المعاينة على الجرائم الماسة بالأنظمة المعلوماتية يطرح إشكال حول مدى ملائمة مسرح الجريمة الخاص بهذه الجرائم للمعاينة، ومدى جدوى هذا الإجراء بالنسبة لهذه الجرائم التي تعتبر صعبة الإثبات وذلك لعدم ترك أثرا ماديا لها.

وفي ذلك نجد أن الفقه يفرق بين حالتين هما:

1- إذا تمت معاينة المكونات المادية للحاسب الآلي وبما أنها محسوسة فإنها لا تثير صعوبة مادية لمعاينتها والتحفظ على الأدلة المادية ووضعها في أحراز مختومة و ضبطها للرجوع إليها.

---

[1]- المادة 79 من قانون الإجراءات الجزائية.

[2]- خالد ممدوح إبراهيم، مرجع سابق، ص 147.

2- أما إذا وقعت الجريمة على مكون غير مادي كإتلاف معطيات برنامج هنا يصطدم المحقق بإشكال عدم وجود آثار للجريمة لمعاينتها وعدم إمكانية حصر عدد المتردد في على مسرح الجريمة.

وبهذا تتم المعاينة بالاستعانة بذوي الخبرة الفنية في مجال الإعلام الآلي حيث يمكنهم من استرجاع المعلومات والتعامل معها وذلك بحفظ الأدلة الالكترونية وما تبقى من آثارها.[1]

ولسرعة فقد هذا النوع من الأدلة وإمكانية تعديلها نجد أن المادة 16 من اتفاقية بودابست على أنه:" يجوز لكل طرف اتخاذ كل إجراء قانوني يسمح بطريقة السرعة لحفظ المعلومات الإلكترونية وعلى الأخص إذا وجد سبب يدعو للاعتقاد أن تلك المعلومات عرضة للفقد أو التعديل".[2]

و ما يعني هذه الجرائم أن المشرع أجاز المعاينة في أي ساعة لأي محل كان بعد أخذ إذن وكيل الجمهورية المختص على امتداد التراب الوطني، و يجوز لقاضي التحقيق القيام بذلك أو أمر ضابط شرطة قضائية طبقا للمادة 40 مكرر 2 من قانون الإجراءات الجزائية

ثانيا/ التفتيش وحجز المعطيات المعلوماتية:

التفتيش هو إجراء من إجراءات التحقيق يهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل من اجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا للإجراءات القانونية المقررة.

فالتفتيش هو وسيلة لغاية تتمثل فيما يمكن الوصول إليه من خلاله إلى أدلة مادية تسهم في بيان و ظهور الحقيقة[3]، غير أنه تنطوي عليه مساس بحرية الأشخاص وحرمة ممتلكاتهم

---

[1]- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، 2003، ص 338.

[2]- جدي نسيمة، مرجع سابق، ص 93.

[3]- عفيفي كامل عفيفي، مرجع سابق، ص 358.

ومسالكهم، لكن الهدف منه البحث عن الأدلة متى وجدت قرائن على حيازة الخاضع لهذا الإجراء لها.[1]

أما التفتيش في المنظومة المعلوماتية يقصد به وإجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للمعطيات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة مرتكبة تشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم.[2]

ويكون التفتيش في جرائم الماسة بالأنظمة المعلوماتية إما التفتيش المكونات المادية للكمبيوتر المتمثلة في وحدات لكل منها وظيفة معينة وهي متصلة ببعضها في شكل نظام متكامل منها وحدات الإدخال ومهمتها استقبال البيانات المعلوماتية غير المعالجة، وأيضا لها في داخل جهاز الحاسوب وحدة الذاكرة والتي تقول بتخزين البرامج والمعلومات، وما يحتويه من ذاكرة رئيسية وعشوائية وذاكرة القراءة ثم وحدة الحساب والمنطق، ووحدة الذاكرة ووحدة التحكم ووحدة لذاكرة المساعدة ووحدة الإخراج والتي تحتوي على أجهزة الشاشة والطابعة ومشغلات الأقراص... [3]، أي كل ما يتصل بالجريمة ويفيد وقوعها للكشف عنها وعن مرتكبيها.

أما عن تفتيش المكونات المعنوية فهو مسألة تثير عدة إشكالات تتعلق بمحل التفتيش الذي يقع على معنويات و ليس ماديات، وكأصل يهدف التفتيش للحصول على دليل مادي، وقد أجاز والمشرع الجزائري التفتيش عن أي شيء و لم يحدد الطبيعة المادية كشرط، وعليه يطبق التفتيش على هذا النوع من المكونات المعنوية من برامج ومعطيات مخزنة لعدم وجود

---

[1]– أحسن بوسقيعة، **التحقيق القضائي**، دار هومة، ط 5، الجزائر، 2000، 87.

[2]– هلالي عبد الله أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي**، دار النهضة العربية، مصر، 2006، ص 73.

[3]– زيبخة زيدان، مرجع سابق، ص ص 131–132.

وفي على ذلك، إضافة لوسائط الحفظ والتخز ين والوحدات المركز ية وكل ما يتعلق بالحاسب الآلي.

وإن تفتيش البيانات المخزنة آل يا يتطلب عون مؤ هل للتعامل بالبرامج وحفظ الملفات و فك الشيفرات وكلمات المرور للتمكن من الحصول على الأدلة وحفظها.[1]

وبهذا إذا كانت مكونات الحاسوب موجودة في مكان خاص كمسكن المشتبه فيه أو أحد ملحقاته فلا يجوز التفتيش إلا بتطبيق الضمانات المقررة قانونا و هي الحصول على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق.

أما بالنسبة للاماكن العامة سواء كانت بطب يعتها كالطرق العامة والشوارع أو كانت بالتخصيص كالمقا هي والمطاعم والسيارات العامة فان الشخص إذ وجد في هذه الأماكن وهو يحمل مكونات ماد ية للحاسوب أو كان مس يطرا أو حائزا لها فان التفتيش لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والق يود المنصوص عليها في هذا الصدد.[2]

أما في حالة ما إذا كان محل جرائم الحاسوب مكونات معنو ية أي عبارة عن برامج، فقد ثار خلاف في ذلك، وقد لجأ الفقه في العديد من الدول استنادا إلى عمومية نصوص التفتيش إلى التوسع في تفسيرها وذلك بتمد يد حكمها إلى البرامج والب يانات المخزنة في أنظمة المعالجة الآلية للمعطيات، حيث ذهب الفقه الكندي إلى توسيع من تفسير المادة 487 من قانون العقوبات الكندي والتي تنص على إمكانية إصدار أمر قضائي لتفتيش أي شيء تتوافر بشأنه أسس أو مبررات معقولة تدعو للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها أو

[1]– جدي نسيمة، مرجع سابق، ص 95.

[2]– هلالي عبد الله أحمد، مرجع سابق، ص 74.

أن هناك نية لاستخدامه في ارتكاب جريمة أو أنه سيتم دليلا على ارتكاب الجريمة، وهكذا فإن هذا النص يفسر على أنه يسمح بضبط وبتفتيش البيانات وبرامج الحاسب الآلي.[1]

وفي ذلك نجد أن المشرع الجزائري قد حرص على أن تكون إجراءات التفتيش بالنسبة لهذا النوع من الجرائم ذات طبيعة خاصة وأعطاها مكانة متميزة عن باقي الجرائم، ونجده أيضا قد أجاز تفتيش المنظومة عن بعد وذلك من خلال القانون رقم 09-04 إذ يكون الدخول إليها بدون صاحبها والولوج إلى الكيان المنطقي للحاسوب، فالتفتيش هنا يستهدف أشياء معنوية وفنية وليست مادية لأن هذه قد تكون وسيلة لارتكاب جريمة أو تخزين معلومة بشأنها، وفي ذلك قد أجاز إفراغ أو نسخ المعلومات المشكوك فيها أو التي من شأنها الإفادة في الكشف عن الجريمة أو عن مرتكبيها، ويكون بنسخها على دعامة إلكترونية تكون قابلة للحجز.[2]

فالتفتيش في المنظومة المعلوماتية عن بعد يكون إما بطريق مباشرة أو عن طريق الولوج عن بعد وفي ذلك يأخذ طريقين:

- إما الدخول إلى المنظومة المعلوماتية أو جزء منها وكذا المعطيات أو البيانات المخزنة فيها.
- أو الدخول إلى منظومة تخزين معلوماتية.[3]

أما بخصوص تمديد التفتيش إلى المنظومة المعلوماتية نجد أن المشرع الجزائري قد تفطن إلى تقنية بالغة في الأهمية في عالم المعلوماتية، يتعلق الأمر بارتباط شبكة الحواسيب ببعضها البعض، فهناك ترابط بين الأنظمة المعلوماتية، وأن شبكة الأنترنت هي أيضا شبكة ممتدة من خلال اتصال أجهزة الحواسيب الآلية اتصالا سلكيا ولا سلكيا يطلق عليها الشبكة

[1]- عفيفي كامل عفيفي، مرجع سابق، ص 366.

[2]- المادة 06 من القانون رقم 09-04.

[3]- زيبخة زيدان، مرجع سابق، ص 136.

الممتدة، وتحسبا لما قد يقبل عليه المجرم المعلوماتي مستعملا ومستغلا هذا الترابط بين الحواسيب وذلك بمحاولة تهريب المعلومات وتسريبها من جهاز لآخر، نجد أن المشرع قد أشار إلى ذلك في المادة 05 من القانون 09-04 على أنه[1]:"...في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك".

ومن المشاكل التي تواجه عملية جمع الأدلة حالة امتداد التفتيش إلى خارج الإقليم الجغرافي للدولة لدولة أخرى وهو ما يسمى بالولوج أو التفتيش عبر الحدود وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها وحدودها الإقليمية.[2]

وللتخلص من هذا الإشكال يجب تفعيل آليات التعاون الدولي الذي من شأنه كما ذكرنا سابقا لتسهيل إجراءات البحث والتحري بعقد اتفاقيات تبادل معلومات بين الدول، وهو ما ضمنه المجلس الأوروبي في إحدى تقاريره الذي ورد فيه أن التفتيش بالاختراق المباشر يعتبر انتهاكا لسيادة الدولة الأخرى ما لم توجد اتفاقية دولية في هذا الشأن.[3]

وهذا ما أشار إليه المشرع الجزائري في المادة 16 من القانون رقم 09-04 على أنه:" يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني".[4]

---

[1]- المادة 05 من القانون رقم 09-04.

[2]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الالكترونية**، مرجع سابق، ص 205.

[3]- جدي نسيمة، مرجع سابق، ص 98.

[4]- المادة 16 من القانون رقم 09-04.

وطبقا للمادة المذكورة أعلاه يمكن الاعتماد على الاتفاقيات الدولية ومبدأ المعاملة بالمثل وذلك بقبول المساعدة القضائية لجمع أدلة بشكل إلكتروني

ثالثا/ التوقيف للنظر:

وهو إجراء بوليسي يأمر به ضابط الشرطة القضائية بوضع شخص يراد التحفظ عليه فيقف في مركز الشرطة أو الدرك لمدة 48 ساعة كلما دعت مقتضيات التحقيق لذلك.[1]

و طبقا للمواد 64، 63، 51 و65 من قانون الإجراءات الجزائية لا يجوز أن تتجاوز مدة التوقيف للنظر 48 ساعة، و أن الأشخاص الذين لا توجد أي دلائل ضدهم لا يجوز توقيفهم فوق المدة الكافية لأخذ أقوالهم، و لأن إجراء التوقيف للنظر إجراء خطير يمس بحرية الأشخاص لابد أن يأمر به ضابط شرطة قضائية تحت إشراف وكيل الجمهورية، ولا تمدد المدة إلا بأمر منه.

وبالنسبة للجرائم الماسة بالأنظمة المعلوماتية فلا يتم تمديد التوقيف للنظر إلى مرة واحدة مع وجوب تقديم المتهم خلال 48 ساعة، وذلك بعد تحرير محضر يتضمن الوقائع إضافة لمدة استجوابه وأوقات الراحة وساعة التقديم أو إطلاق سراحه مع توقيع الموقوف أو الإشارة لذلك في حال امتناعه والتي يجب أن تدون في السجل الخاص الذي يلزم ضابط الشرطة القضائية بإمساكه تحت طائلة قانون العقوبات في مادته 110 مكرر ق إ ج.[2]

الفرع الأول: الاختصاصات غير العادية في التحري والتحقيق

لقد أستحدث القانون رقم 06-22 إلى أساليب التحري والتحقيق تخص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وتتمثل في:

- المراقبة والتتبع.
- اعتراض المراسلات و تسجيل الأصوات و التقاط الصور.

---

[1]- أوهايبية، **شرح قانون الإجراءات الجزائية الجزائري**- التحري و التحقيق- ، دار هومة الجزائر، 2004، ص 239.

[2]- جدي نسيمة، مرجع سابق، ص 100.

- التسرب.

1- **المراقبة والتتبع:** بالرجوع إلى نص المادة 16 مكرر من ق إ ج فإنه يمكن لضباط الشرطة القضائية وتحت سلطتهم أعوان الشرطة القضائية الحق في القيام بعملية مراقبة الأشخاص وتنقل الأشياء والأموال ومتحصلات الجريمة، وذلك على امتداد التراب الوطني، ولكن وفق شروط معينة.

وبهذا فالمراقبة هي وضع شخص أو وسائل نقل أو أماكن أو مواد تحت رقابة سرية ودورية، بهدف الحصول على معلومات لها علاقة بالشخص محل الاشتباه أو بأمواله أو بالنشاط الذي يقوم به.

2- **اعتراض المراسلات وتجيل الأصوات والتقاط الصور:** لقد مكن المشرع الجزائري ضباط الشرطة القضائية من اختصاصات بالغة الخطورة فيها مساسا بالحريات الفردية، وتتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور[1] وذلك في جرائم محددة على سبيل الحصر وهي المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالصرف والجرائم محل الدراسة الماسة بأنظمة المعالجة الآلية للمعطيات.

و قد أثير إشكال إمكانية التصنت على المحادثات الهاتفية إذ لم ترد في نصوص قانون الإجراءات الجزائية، إذ يتعلق الأمر بمسألة بالغة الأهمية لكونها تشكل انتهاكا لحرمة المراسلات التي كفلها الدستور بنص المادة 46 بقولها:" سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

وفي فرنسا أيضا أثير هذا الإشكال وقضت محكمة النقض الفرنسية بشرعية أمر أصدره قاضي التحقيق بالتصنت على محادثات هاتفية و هو ما أكدته المادة 08 من الاتفاقية

[1]- عبد الرحمن خلفي، **الإجراءات الجزائية في التشريع الجزائري والمقارن**، دار بلقيس، الجزائر، 2015، ص 99.

الأوروبية التي تحضر كل تدخل من جانب السلطات في الحياة الخاصة إلا بنص القانون و لضرورة الوقاية من الجرائم.[1]

وبصدور القانون 09-04 تم حل الإشكال المطروح هول مراقبة الاتصالات، حيث حددت المادة 04 منه الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الإلكترونية الواردة بالمادة 03 من ذات القانون بوضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، وورد ضمن الحالات المسموح اللجوء فيها بهذا الإجراء بالبند ب من المادة 04 وهي حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.[2]

أما عن إجراء اعتراض المراسلات و تسجيل الأصوات والتقاط الصور فقد أجازت المادة 65 مكرر 5 من قانون الإجراءات الجزائية[3] لوكيل الجمهورية أن يأذن بـ:

- اعتراض المراسلات التي تتم عن طريق وسائل سلكية ولا سلكية .

- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط و تثبيت وبث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص أو بالدخول إلى المحلات السكنية أو غيرها و لو خارج المواعيد المحددة في المادة 47 ق إ ج و بغير علم أو رضا الأشخاص الذين لهم الحق طبقا للمادة 65 مكرر 5 فقرة 4.

وتتم هذه العمليات تحت الإشراف والمراقبة المستمرة لوكيل الجمهورية أو قاضي التحقيق بعد فتح تحقيق طبقا للمادة 65 مكرر 5 فقرة 5 و6 والتي حددت البيانات الواجب توافرها في الإذن و الذي يسلم لمدة أقصاها أربعة (04) أشهر قابلة للتجديد.

---

[1]- أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص 89.

[2]- جدي نسيمة، مرجع سابق، ص 102.

[3]- المادة 65 مكرر 05 من قانون الإجراءات الجزائية.

وفي ذلك يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية أو قاضي التحقيق أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية.[1]

و إذا اكتشفت جرائم أخرى غير تلك التي ورد ذكرها بإذن القاضي المختص فهذا لا يعد سببا لبطلان الإجراءات.[2]

ويتم تحرير محضر من طرف ضابط الشرطة القضائية يذكر فيه تاريخ وساعة بداية العملية وانتهائها، ويصف في المحضر وينسخ المراسلات والصور والمحادثات المسجلة التي من شانها إظهار الحقيقة، ويودع هذا المحضر بملف الإجراءات.

3- **التسرب:**

التسرب تقنية جديدة بالغة الخطورة على أمن الضبطية القضائية وتتطلب جرأة وكفاءة ودقة في العمل، قننها المشرع الجزائري في التعديل الحاصل على مستوى قانون الإجراءات الجزائية لسنة 2006 في المادة 65 مكرر 12، فهو يسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية على تقديم المتسرب لنفسه على أنه فاعل أو شريك.[3]

و لا يجوز القيام بالإجراء قبل الحصول على إذن مكتوب يشار فيه للجريمة و هوية الضابط المنفذ للعملية على ألا يتجاوز مدة أربعة (04) أشهر قابلة للتجديد، كما يجوز للقاضي توقيف العملية في أي وقت يراه مناسبا طبقا للمادة 65 مكرر 15 ق إ ج، إذ تتم العملية منذ بدايتها تحت إشرافه طبقا للمادة 65 مكرر 11.

---

[1]- المادة 65 مكرر 08 من قانون الإجراءات الجزائية.

[2]- المادة 65 مكرر 06 فقرة 2 من قانون الإجراءات الجزائية.

[3]- عبد الرحمن خلفي، مرجع سابق، ص 103.

و حماية للمتسرب وضمانا لسلامته لا يمكن أن يعتبر أي من الأعمال التي يرتكبها بمناسبة القيام بالمهمة المسندة إليه تحريضا على ارتكاب جرائم، كما ولا يسأل عن إخفاء هوية و له استعمال هوية مستعارة كما لا يسأل عما يرتكبه من جرائم طبقا للمواد 65 مكرر 12و14 ق إ ج.[1]

كما نص المشرع على أحكام جزائية بالمادة 65 مكرر 16 توقع على كل من يكشف عن هوية المتسرب فيعاقب بالحبس من عام إلى خمس سنوات و غرامة من 50000 دج إلى 200.000 دج.[2]

و إذا تسبب الكشف في أعمال عنف أو ضرب عليه أو زوجه أو أبناءه أو أصوله تكون العقوبة هي الحبس من 5 سنوات إلى 10 سنوات وغرامة من 200.000 دج إلى 500.000 دج غرامة نافذة.

و إذا تسبب الكشف في وفاة أحد هؤلاء الأشخاص تكون العقوبة هي الحبس من عشر إلى عشرين سنة وغرامة من 500.000 دج إلى 1.000.000 دج.

و عند انتهاء المهمة أو توقيفها من القاضي المختص يقوم المكلف بالمهمة بإنجاز تقرير يتضمن كل المعلومات التي توصل لها دون الإشارة لهوية المنجز و يودع ملف الإجراءات رفقة الإذن الأولي، ولا يمكن بأي حال من الأحوال الإشارة لـ هوية المتسرب خلال كل مراحل الدعوى إذ أن الضابط المنسق وحده من يمكن سماعه كشاهد تحت مسؤوليته الشخصية طبقا للمادة 65 مكرر 18 من قانون الإجراءات الجزائية.[3]

الفرع الثالث: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

لقد تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومن خلال نص المادة 13 من القانون رقم 09-04، حيث أنشأت هذه اللجنة من

---

[1]- جدي نسيمة، مرجع سابق، ص 104.

[2]- المادة 65 مكرر 16 قانون الإجراءات الجزائية.

[3]- جدي نسيمة، مرجع سابق، 104.

أجل تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، وكذا لمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، إضافة إلى ذلك تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعطيات المساعدة في التعرف على مرتكبي الجرائم المعلوماتية وتحديد مكان تواجدهم.[1]

[1]- المادة 13 و14 من القانون 09-04.

المبحث الثاني:

مسألة الإثبات في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تتميز الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كالجرائم المعلوماتية بصعوبة إثباتها لما تتميز به من خصائص كونها تتعلق في غالبها بمعنوي يسهل محو أثرها وتدميرها، لذا تثور مسألة استخلاص الدليل الذي تثبت به هذه الجريمة.

ولا شك أن هذا الدليل سيتم استخلاصه من البيئة الرقمية، والتي تعتبر مسرح الجريمة المعلوماتية مما يجعله يتميز بخصائصها (خصائص البيئة الرقمية)، وهذا ما إلى الحديث عن مسالة قبول هذا الدليل أمام القضاء ومدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف والتحريف والأخطاء، بل وحتى مع ضمان مصداقية هذا الدليل وكذا مشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة أكبر أهمية تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي إعمالا لمبدأ الاقتناع الشخصي للقاضي الجزائي الذي يشكل جوهر أي حكم.

وبهذا فقد قسمنا هذا المبحث إلى ثلاث مطالب، المطلب الأول تناولنا فيه سرية الدليل الالكتروني وخصوصيته، أما المطلب الثاني فقد تطرقنا إلى إجراءات الحصول على الدليل الالكتروني، والمطلب الثالث فقد كان بعنوان القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي، أما المطلب الرابع فقد تناولنا فيها الجزاءات المقررة للجرائم الماسة بالأنظمة المعلوماتية.

المطلب الأول: سرية الدليل الالكتروني وخصوصيته

يعد الدليل الإلكتروني الوسيلة لإثبات الجرائم التي ترتكب بوسائل معلوماتية والتي تقع إما بتحريف البيانات المعالجة آليا عن طريق أجهزة الإعلام الآلي أثناء إدخال البيانات أو

تخزينها أو أخراجها و للوصول إلى الأدلة على ذلك فإن الأمر يحتاج إلى أدلة علمية تثبت وقوعها و إسنادها

الفرع الأول: مفهوم الدليل الالكتروني أو الرقمي

كانت هناك العديد من المحاولات الفقهية والتشريعية لتعريفه، فكان من اللزوم معرفة معنى الدليل الإلكتروني ومفهومه حتى يسهل توضيح كل الجوانب المتعلقة به.

أولا/ تعريف الدليل الالكتروني:

إن الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء.[1]

وقد عرفت المنظمة العالمية لدليل الكمبيوتر الدليل الرقمي على أنه:" المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية".[2]

أو هو عبارة عن بيانات يمكن إعدادها وتراسلها وتخزينها رقميا، بحيث يمكن الحاسوب من تأدية مهامها.

وبهذا فإن الدليل هو أي معلومات سواء كانت من صنع الإنسان أو تم استخلاصها من الحاسوب يقبلها المنطق والعقل ويعتمدها العلم ويتم الحصول عليها إجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه.[3]

---

[1]– ممدوح عبد الحميد عبد المطلب، **البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت**، دار الفكر القانونية.مصر، 2006، ص 88.

[2]– مصطفى محمد موسى، **التحقيق الجنائي في الجرائم الإلكترونية**، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2009، ص 213.

[3]– سعيداني نعيم، مرجع سابق، ص 122.

ثانيا/ خصائص الدليل الالكتروني:

يمتاز الدليل الرقمي عن الدليل المادي المأخوذ من مسرح الجريمة بالخصائص التالية:

1- **الدليل الرقمي هو دليل علمي**: إن الدليل الرقمي يحتاج إلى بيئته التقنية التي يتكون فيها، لكونه من طبيعة تقنية المعلومات ذات المبنى العلمي ومن ثمة فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي، فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة أن القانون مسعاه العدالة وأما العلم فمسعاه الحقيقة.

وإذا كان للدليل العلمي منطقه الذي يجب ألا يخرج عليه، إذ يستبعد تعارضه مع القواعد العلمية السليمة فإن الدليل الرقمي له ذات الطبيعة فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه.[1]

2- **الدليل الالكتروني من طبيعة تقنية**: الدليل الإلكتروني كما سبق تبيانه هو الواقعة التي تنبئ عن وقوع جريمة أو فعل غير مشروع، وهذه الواقعة مرجعها أو مبناها علمي، باعتبار أن مبنى العالم الافتراضي علمي أيضا، و هذه الخاصية مفادها أن الدليل الإلكتروني لا يمكن الحصول عليه ولا الإطلاع على ما يحتويه إلا باستخدام طرق علمية.[2]

نتيجة للطبيعة التقنية للدليل الرقمي فإنه أكتسب مميزات عن الدليل المادي من حيث قابليته للنسخ، بحيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى مما يشكل ضمانة شديدة

---

[1]– سعيداني نعيم، مرجع سابق، ص 123.

[2]– فتحي محمد أنور عزت ، **الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية و التجارية**، دار الفكر والقانون للنشر والتوزيع، مصر 2010، ص648.

الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير ، الإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة.[1]

3- **الدليل الرقمي صعب التخلص منه** : إن القاعدة التي تسري على كافة ما يتعلق بهيكلة تكنولوجيا المعلومات، هي أنه كلما حدث اتصال بتكنولوجيا المعلومات في معنى إدخال بيانات إلى ذلك العالم (Input) فإنه من الصعب التخلص منها ولو كان ذلك باستخدام أعتى أدوات الإلغاء، فمحاولة التخلص من الدليل الرقمي باستخدام خصائص التخلص من الملفات في الحاسوب كخاصية (Erase. Remove.Delete....) لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة إذ تتوافر برمجيات ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب.[2]

4- **الدليل الرقمي دليل متنوع ومتطور :** على الرغم من أن الدليل الإلكتروني في أساسه يعتبر متحدا في تكوينه، أي في مجال الحوسبة والرقمية، إلا أنه يتخذ أشكالا مختلفة، فمصطلح الدليل الإلكتروني يشمل كافة أنواع البيانات الإلكترونية الممكن تداولها رقميا، ويكون بينها و بين الجريمة رابطة من نوع ما، بالإضافة إلى أن تكون متصلة بالضحية مما يتحقق معه وجود رابطة بينها و بين الجاني ففيما يخص التنوع المتعلق بالدليل الإلكتروني، نجد أنه قد يظهر بطريقة علانية في هيئات مختلفة الأشكال، كأن يكون بيانات غير مقروءة، كما هو الأمر في حالة المراقبة عبر الشبكات والملقمات أو الخوادم، و قد يكون الدليل الإلكتروني مفهوما للأشخاص كما لو كان وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة، أو معدة بنظام التسجيل السمعي المرئي، أو أن تكون

[1]– سعيداني نعيم، مرجع سابق، ص 123.

[2]– سعيداني نعيم، مرجع سابق، ص 124.

مخزنة في نظام البر ي الإلكتروني، و هذه الخاصية تستوجب مواكبة التطور في عالم التكنولوجيات.[1]

الفرع الثاني: أنواع الدليل الرقمي

يأخذ الدليل الرقمي نوعين رئيسيين أدلة أعدت لتكون وسيلة إثبات وأدلة لم تعد لتكون وسيلة إثبات، فأما النوع الأول فيمكن إجماله فيما يلي:

1- السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا، وتعتبر هذه السجلات من مخرجات الجهاز ولم يساهم الإنسان في إنشائها.

2- السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الجهاز، ومن أمثلة ذلك البيانات التي تم إدخالها إلى الأدلة وتتم معالجتها من خلال برنامج خاص.

وأما النوع الثاني أي الأدلة الرقمية التي لم تعد لتكون وسيلة إثبات فهي تلك الأدلة التي تنشأ دون إرادة الشخص بمعنى أنها أي أثر يتركه دون أن يكون راغبا في وجودها، ويسمى هذا النوع من الأدلة بالبصمة الرقمية أو الآثار المعلوماتية للرقمية ، وهي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال النظام المعلوماتي وشبكة الاتصالات، والواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من طرف من صدر عنه غير أن الوسائل التقنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها فالاتصالات التي عبر المنظومة المعلوماتية المرتبطة بشبكة الاتصالات وكذا المراسلات الصادر عن الشخص أو التي يتلقاها يمكن ضبطها بواسطة تقنية خاصة بذلك.

وتبدو أهمية التمييز بين هذين النوعين في كون أن النوع الأول من الأدلة الرقمية قد أعد سلفا كوسيلة لإثبات بعض الوقائع التي يتضمنها، لذلك فإن عادة ما يعمد إلى حفظه للاحتجاج به لاحقا وهو ما يقلل من إمكانية فقدانه كما يكون من السهل الحصول عليه، بينما

[1]- فتحي محمد أنور عزت، مرجع سابق، ص ص 651-652.

النوع الثاني من الأدلة الرقمية فلكونه لم يعد أصلا ليكون أثرا لمن صدر عنه لذا فهو في الغالب ما يتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها ويكون الحصول عليه بإتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد، وهو على العكس من النوع الأول إذ لم يعد ليحفظ مما يجعله عرضة للفقدان بسهولة.[1]

ويلاحظ أن هذا التنوع في الدليل الرقمي يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه وإنما تتعدد هذه الوسائل أيضا، ويضل في كل الأحوال الدليل المستمد بواسطتها.[2]

المطلب الثاني: إجراءات الحصول على الدليل الإلكتروني

إن إجراءات الحصول على الدليل الإلكتروني لها خصوصية تختلف عن الإجراءات التقليدية، وتتمثل خصوصية هاته الإجراءات في العقبات التي تواجهها للحصول على الدليل وحجزه وحفظه في ملف الدعوى وذلك باستعمال مختلف أساليب التحري والتحقيق السالفة الذكر وذلك بالاستعانة بأساليب التحقيق الأخرى منها الاستجواب وشهادة الشهود والاستعانة بخبير وذلك بغية الحصول على الدليل الالكتروني واستكمال إجراءات التحقيق للكشف عن الجريمة ومرتكبيها.

الفرع الأول: الاستجواب

الاستجواب هو مناقشة المتهم في التهمة المنسوبة إليه، ومواجهته بالأدلة القائمة ضده ومناقشته في إجابته لاستظهار الحقيقة، إما بإنكار التهمة ودحض هذه الأدلة أو الاعتراف بالجريمة المنسوبة إليه.[3]

فالاستجواب يعد إجراء من إجراءات التحقيق القضائي وهو من اختصاص قاضي التحقيق طبقا لنص المادة 100 من قانون الإجراءات الجزائية.

---

[1]– سعيداني نعيم، مرجع سابق، ص 129.

[2]– سعيداني نعيم، مرجع سابق، ص 130.

[3]– عبد الرحمن خلفي، مرجع سابق، ص 234.

و يهدف الاستجواب لهدفين الأول إثبات شخصية المتهم و مناقشته تفصيلا في الاتهام الموجه له، والثاني تحقيق حقوق الدفاع فمناقشة المتهم للأدلة قد يؤدي لاعترافه كما تفتح له المجال لإثبات براءته[1]، لذلك فالاستجواب ذو طبيعة مختلطة فهو وسيلة إثبات ودفاع في نفس الوقت و استجواب المتهم فيما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تحكمه القواعد العامة إلا أن الفرق يكمن في وجوب أن يكون المحقق مؤهلا للتحقيق في هذا النوع من الجرائم و يكون مستوعبا لمفرداتها فالمجرم المعلوماتي خبير في الحاسوب واستخدام تقنياته.

ومن خلال الاستجواب يتم التحقيق في الأدلة التهم المنسوبة ضد المتهم والتي يقدمها لصالحه حتى الوصول إلى الحقيقة أما بالإحالة إلى المحاكمة أو صدور أمر بألا وجه للمتابعة، وكما جرت العادة فقد أحاط المشرع الجزائري المتهم بمجموعة من الضمانات وذلك استنادا إلى مبدأ الأصل في الإنسان البراءة ومن هذه الضمانات حق المتهم في التزام الصمت، حق الاستعانة بمحامي(المادة 100 ق إ ج).

الفرع الثاني: الاستعانة بالخبرة الالكترونية

يجوز لكل جهة قضائية تعرض عليها مسألة ذات طابع تقني أن تأمر بإجراء خبرة سواء من تلقاء نفسها أو بناء على طلب النيابة العامة أو أحد الأطراف الآخرين من متهم أو طرف مدني، وهذا ما نصت عليه المادة 143 من قانون الإجراءات الجزائية.

و بالنسبة للجريمة المعلوماتية فإن دور الخبراء التقنيين في هذا المجال أصبح أكثر من مهم، وبالتالي فإن الخبراء الإلكترون يين الرقم يين صاروا في الوقت الرا هن أهم أعوان المحقق ويشكلون بما يقدمونه من أعمال واحدا من أ هم مصادر الأدلة الجنائية الإلكترونية، وعلى المحقق توطيد علاقته بهم لأنهم من أ هم عوامل نجاحه في مجال التحقيق الجنائي الالكتروني نتيجة تزا يد الأسال يب الإجرام ية الإلكترون ية الرقم ية، ففي مجال الجرائم

[1]– جدي نسيمة، مرجع سابق، ص 113.

المعلوماتية يتم اللجوء للخبير من أجل القيام بمهام تحليل و تفسير العناصر المشكلة للدليل، بل ويلعب دورا هاما للحفاظ على هذه العناصر.[1]

والخبير في الجريمة المعلوماتية هو الفني المتخصص في التقنية الالكترونية الرقمية و شبكاتها، و هو المتمكن من الدخول في نظام المعالجة الآلية الرقمية للمعطيات إذا كانت ضرورة التحقيق تحتم ذلك، ولقاضي التحقيق أو جهة الحكم سلطة ندب الخبراء.

ولعل أهم النقاط الواجب أن تشملها الخبرة الالكترونية هو بيان تركيب الحاسب و أنظمة تشغيله والشبكة المرتبطة به، وسائط الاتصال به والموضع المحتمل للأدلة والشكل والهيئة التي تكون عليها، إمكانية نقل الأدلة لوسائط تخزين خارجية حتى يمكن الرجوع لها دون إتلافها وحتى لا يتم تدميرها لاحقا وإمكانية تجسيد الأدلة في صورة مادية بنقلها من الدعائم الممغنطة إلى نسخ ورقية حتى يمكن الإطلاع عليها من القاضي مباشرة وضمها للملف دون الحاجة لإعادة تشغيل النظام.

ورغم ما يناط بالخبير من مهام حيث أجاز له القانون تلقى أي تصريح مفيد من الغير يبقى الخبير مجرد مساعد للقاضي، تنحصر مهمته في إنارة القاضي بخصوص مسألة فنية، ولا يجوز له بأي حال من الأحوال أن يحل محل القاضي أو ينوب عنه.[2]

المشرع الجزائري لم يتخلف عن هذه التشريعات حينما أشار في المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير

[1]– بوذراع عبد العزيز، مرجع سابق، ص 116.

[2]– أحسن بوسقيعة، **التحقيق القضائي**، مرجع سابق، ص 116.

المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.[1]

الفرع الثالث: شهادة الشهود

الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام التحقيق أو الحكم بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم وتسمى حينها بشهادة الإثبات أو براءته منها وتسمى حينها بشهادة النفي أي نفي التهمة.

والشاهد في جريمة المساس بأنظمة المعالجة الآلية للمعطيات يمكن سماعه وذلك بغية تحصيل الدليل من مشغلي الحاسب الآلي وذوي الخبرة بمعداته واستخدامه وخبراء البرمجة ومحللي البرامج وأنظمة المعالجة، وكذا مهندسي الصيانة الذين بطبيعة الحال يكونون عونا للقاضي أثناء الإدلاء بالشهادة للكشف عن بعض الغموض في تلك الأنظمة من شيفرات وكلمات سر وتحليل كل دليل رقمي موجود، ويمكن الاعتماد على آرائهم التي يبدونها باعتبارهم أصحاب خبرة في مجال المعلوماتية هذا ما يطلق عليه بالشاهد الخبير أو الشاهد المعلوماتي.[2]

ويحصر قانون الدليل الخاص بولاية كاليفورنيا شهود الجريمة المعلوماتية في:

- محلل النظم الذي صمم وحدد برنامج الكمبيوتر الذي أنتج الدليل.
- المبرمج الذي قام بتحرير البرنامج واختباره.
- المشغل الذي يقوم بتشغيل البرامج.

[1]- سعيداني نعيم، مرجع سابق، ص 167.

[2]- جدي نسيمة، مرجع سابق، ص 116.

– طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة).

– أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة أو الأسطوانات التي تشتمل على البيانات المصدرية الصحيحة.[1]

– مهندس الصيانة الالكترونية الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة.

– موظفو المدخلات والمخرجات والمسؤولون عن معالجة المدخلات المستخدم في تنفيذ برامجه.

– المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نواتجها.

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للدخول في نظام المعالجة الآلية للمعطيات سعيا للتنقيب عن أدلة الجريمة بداخله

وهي ذلك فقد اتجه الفقه إلى اتجاهان:

الاتجاه الأول: ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة ان يقوم بطبع ملف البيانات أو الافصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل إلى هذا الاتجاه الفقه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب.

وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة.

[1]– عبد الله حسين علي محمود، بحث بعنوان **إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات**، مأخوذ من الموقع الإلكتروني http://www.f-law.net/law/threads/11338، تاريخ الإطلاع: 2017/05/15، ساعة الإطلاع: 18:07.

الاتجاه الثاني: ويرى أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم[1] (المواد 62، 109، 138 من قانون الإجراءات الجنائية الفرنسية) ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة.

وهذا الرأي يتماشى مع التزامات ال شهادة التي يفرضها قانون الإجراءات الجزائية الجزائري إذ تنص المادة 97 منه على أن : "كل شخص استدعي لسماع شهادته ملزم بالحضور وحلف اليمين وأداء الشهادة مع مراعاة السر المهني.."، إلى جانب المادة 98 من نفس القانون التي تفرض عقوبة جنحية على كل شخص يرفض الإجابة عن الأسئلة الموجهة إليه من طرف قاضي التحقيق، وهذا بعد إحالته إلى المحكمة المختصة.[2]

المطلب الثالث: القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي

نظرا لما تتميز به الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و بالتبعية الطبيعة الخاصة للدليل الإلكتروني وصعوبة الحصول عليه، يثار إشكال حول قيمته القانونية ومدى مصداقيته في مجال الإثبات الجنائي.

وبهذا سنتناول في الفرع الأول مشروعية الدليل الالكتروني، أما الفرع الثاني فستطرق إلى حجية هذا الدليل في إطار نظرية الإثبات الجنائي، وأخيرا ستناول موقف المشرع الجزائري من الدليل الالكتروني في مجال الإثبات الجنائي.

الفرع الأول: مشروعية الدليل الالكتروني في مجال الإثبات الجنائي

[1]- عبد الله حسين علي محمود، مرجع سابق، http://www.f-law.net/law/threads/11338.

[2]- بوذراع عبد العزيز، مرجع سابق، ص 123.

يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا من حيث وجوده ومن حيث الحصول عليه، والأمر نفسه بالنسبة للدليل الإلكتروني الذي يثير إشكال في مسألة مصداقيته وحجيته في تعبيره عن الحقيقة.

أولا/ مشروعية الدليل الالكتروني: تعرف المشروعية بأنها التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام، إذ تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حريا تهم وحقوقهم الشخصية ضد تعسف السلطة ومن التطاول عليها في غير الحالات التي رخص فيها القانون بذلك، من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته.[1]

وبهذا فإن مشروعية وجود الدليل الرقمي تقتضي أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثبات الجنائي، وتشمل هذه المشروعية في مشروعية وجود الدليل الرقمي أو الالكتروني ومشروعية الحصول عليه.

1- **مشروعية وجود الدليل الالكتروني:** يعترف المشرع بالدليل الرقمي أو الالكتروني، وذلك من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الاستناد إليه في تكوين عقيدته، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الرقمي يتمثل في طبيعة نظام الإثبات السائد في الدولة، إذ تختلف النظم القانونية في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات.

[1]-هلالي عبد الله أحمد، **حجية المخرجات الكومبيوترية في المواد الجنائية** ، دار النهضة العربية، ط 2، مصر، 2008، ص 104.

فللنظم القانونية التي تتبنى نظام الأدلة القانونية لا يمكن في ظلها الاعتراف للدليل الرقمي بأية قي إثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الإثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين قناعته.[1]

أما بالنسبة للنظم القانونية التي تعتمد نظام الإثبات الحر كما هو الحال عليه في القانون الجزائري(المادة 212 من قانون الإجراءات الجزائية[2]) والقانون الفرنسي (المادة 427 قانون الإجراءات الجزائية الفرنسي)، فإنه لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود، على اعتبار أن المشرع لا يعتمد سياسة النص على قائمة لأدلة الإثبات فالأساس هو حرية الأدلة، لذلك فمسألة قبول الدليل الرقمي لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه لتقدير القاضي.

2- **مشروعية الحصول على الدليل الالكتروني:** من المقرر أن الإدانة في أي جريمة لابد وأن تكون مبنية على أدلة مشروعة تم الحصول عليها وفق قواعد الأخلاق والنزاهة واحترام القانون من طرف الجهة المختصة بجمع الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية، و لا يكون مشروعا إلا إذا أجرى التنقيب عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء أو إقامته أمامه بالطرق التي رسمها القانون، فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته.

[1]– سعيداني نعيم، مرجع سابق، ص 209.

[2]– تنص المادة 212 من قانون الإجراءات الجزائية على أنه:"يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا في الأحوال التي ينص فيها القانون على خلاف ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص".

وبهذا فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإ نها تكون باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية.[1]

الفرع الثاني: حجية الدليل الرقمي في إطار نظرية الإثبات الجنائي

إن الوصول إلى الحقيقة في مرحلة الحكم، هي المرحلة الحاسمة في الدعوى الجنائية، وهذا الأمر يتم عن طريق الأدلة المتوفرة لدى القاضي الجنائي التي يمارس عليها سلطته التقديرية، و في مجال الجريمة الإلكترونية يكون الدليل الإلكتروني هو الأوفر.

والدليل الإلكتروني كباقي الأدلة الجنائية يخضع للقواعد المقررة لباقي الأدلة فيما يخص حجيته، من حيث مقبوليته على مستوى أنظمة الإثبات الجنائي، سواء تعلق الأمر بنظام الإثبات الحر أو المقيد أو المختلط، و فيما يتعلق بسلطة القاضي الجنائي في قبول هذا النوع من الأدلة و تقديره والاقتناع به، وهذا باعتبار أن القاضي لا يقدر إلا الدليل المقبول، وهذا على مستوى القضاء الجنائي.

و نظرا للطبيعة الخاصة للدليل الإلكتروني فإن حجيته على مستوى الإثبات الجنائي، قد تثير العديد من المشاكل، خاصة فما تعلق بمصداقية الدليل الإلكتروني.

وعليه سنتناول فيما يلي شروط قبول الدليل الرقمي ومدى تأثير ذلك على الاقتناع الشخصي للقاضي الجزائي.

أولا/ شروط قبول الدليل الإلكتروني: لقبول الدليل الالكتروني يطلب وجوب توافر مجموعة من الشروط فيه:

1- **وجوب يقينية الأدلة الالكترونية وغير قابلتها للشك :** يجب أن تكون الأدلة المستخرجة من المنظومة المعلوماتية غير قابلة للشك وذلك ليتمكن الحكم بموجبها، حيث أنه لا مجال لدحض قرينة البراءة أو افتراض الإدانة إلى أن يصل قاضي الموضوع إلى اقتناع يقيني وجزمي.[1]

[1]– سعيداني نعيم، مرجع سابق، ص 210.

ويمكن التوصل إلى اقتناع القاضي وذلك من خلال ما يعرض من الأدلة الرقمية على اختلاف أشكالها التي تتوافر عن طريق الوصول المباشر إليها أو بمجرد عرضها كمخرجات على شاشة الحاسوب، ويستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية وما ينطبع في ذمته من حتما تصورات تمكنه من الاقتناع و نسبة الجريمة المعلوماتية إلى شخص معين من عدمه، وكذا عن طريق المعرفة العقلية من خلال ما يقوم به من استقراء واستنتاج ليصل إلى الحقيقة التي يهدف إليها ويجب أن يصدر حكمه استنادا إليها.[2]

ويتحقق من يقين الأدلة الالكترونية بإخضاعها للتقييم الفني وذلك بوسائل مختلفة ذات طبيعة فنية بغية التأكد من صحة هذه الأدلة وسلامتها، وتتمثل هذه الوسائل الفنية في:

أ- تقييم الدليل الالكتروني للتحقق من سلامته: ويتم ذلك بعدة طرق أهمها:

- فكرة التحليل التناظري الرقمي إذ يتم من خلالها مقارنة الدليل الالكتروني المقدم للقضاء والمدرج بالآلة الرقمية، ومن خلاله يتم التأكد من مدى حصول هذا الدليل للعبث في النسخة المستخرجة ويستعان في ذلك بلعم الكمبيوتر الذي يكشف مدى التلاعب بمضمون هذا الدليل.

- استخدام عمليات حسابية خاصة تسمى الخوارزميات ويتم اللجوء إلى مثل هذه التقنية في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي، أو حالة العبث الذي حصل على مستوى النسخة الأصلية، فمن خلالها يتم التأكد من سلامة الدليل الرقمي من الاستبدال والتحريف أو التغيير.

---

[1]- علي حسن محمد الطوالبة ، **التفتيش الجنائي على نظم الحاسوب والإنترنت**، عالم الكتب الحديثة، الأردن، 2004، ص 190.

[2]- هلالي عبد الله أحمد، **حجية المخرجات الكومبيوترية في المواد الجنائية**، مرجع سابق، ص91.

– استعمال الدليل المحايد وهو نوع من الأدلة الرقمية المخزون في البيئة الافتراضية لا علاقة له بموضوع الجريمة، ولكنه يساعد في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول أي تعديل عليه في النظام الكومبيوتري.[1]

ب- تقييم الدليل الرقمي من حيث السلامة الفنية للإجراءات المستخدمة في الحصول عليه : ويتم ذلك بـــ:

– إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج ويكون ذلك بإتباع اختبارين أساسيين يتم التأكد من خلالهما أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الرقمي ، وهذه الاختبارات تتمثل في: اختبار السلبيات الزائفة ومفاده أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي [2]، أما الاختبار الثاني والذي يعرف باختبار الإيجابيات الزائفة فمفاده إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي لاختبار يمكن من التأكد من أن هذه الأداة لا تعرض معطيات إضافية جديدة.

– لاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل، إذ تبين الدراسات العلمية والبحوث المنشورة في مجال تقنية المعلومات الطرق السليمة التي يجب إتباعها في الحصول على الدليل الرقمي وفي المقابل بينت تلك الدراسات أيضا الأدوات المشكوك في كفاءتها وهو ما يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات.

2- **وجوب مناقشة الأدلة الرقمية المستخرجة من الحاسوب** : إن الأدلة الرقمية المتحصلة لإثبات الجرائم المعلوماتية سواء كانت مطبوعة أم اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مصورات فلمية، كلها ستكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام

[1]– خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة للنشر والتوزيع، 2011، ص 249.

[2]– سعيداني نعيم، مرجع سابق، ص 218.

المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال البيئة الإلكترونية يجب أن يعرض في جلسة المحكمة ليس من خلال ملف الدعوى في التحقيق الابتدائي وإنما يعرض بصفة مباشرة أمام القاضي.[1]

ما سبق فإن هناك من يذهب إلى الاعتقاد بأنه بمقدار أتساع مساحة الأدلة العلمية بمقدار ما يكون انكماش وتضاؤل دور القاضي الجزائي في التقدير، خاصة أمام غياب الثقافة المعلوماتية للقاضي وقد يستتبع ذلك بالقول أن التطور العلمي من شأنه أن يطغى على نظام الاقتناع القضائي ولا يبقى للقاضي سوى الإذعان لرأي الخبراء المختصين دون أي تقدير من جانبه فمثل هذا الأمر يدفعنا إلى بحث مدى تأثير القيمة العلمية للدليل الرقمي على مبدأ اقتناع القاضي الجزائي.[2]

الفرع الثالث: موقف المشرع الجزائري من الدليل الالكتروني في مجال الإثبات الجنائي

الإثبات الجزائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف غموض الجريمة ونسبتها إلى المتهم.

وبهذا نجد أن الفقه قد وضع أنظمة إجرائية في مجال الإثبات الجنائي، كل نظام يختلف عن الآخر من حيث الأسس التي يقوم عليها.

إن نظام الإثبات الجنائي المقيد كان يقوم على تقييد سلطة القاضي الجنائي، بوضع الأدلة من قبل المشرع وما على القاضي الجنائي إلا رؤية مدى توفر هذه الأدلة و الأخذ بها، دون

[1]– سعيداني نعيم، مرجع سابق، ص 218.

[2]– مرجع نفسه، ص 219.

تدخل من قبله، فدور القاضي كان سلبيا بحتا، ولا يخرج عن نطاق تطبيق القانون و ما جاء به القاضي دون زيادة أو نقصان عن ما جاء به المشرع.[1]

نظام الإثبات المقيد بصفة عامة هو ذلك النظام الذي يطلق عليه نظام الأدلة القانونية، أو نظام الإثبات المحدد، بمعنى آخر أن المشرع هو الذي يحدد فيه الأدلة مسبقا، و القاضي بدوره لا يجوز له أن يخرج عن هذه الأدلة المحددة من قبل المشرع.

فالقاضي دوره في هذا النظام يظهر كمطبق للقانون، بمراعاة توافر الدليل أو شروطه، حيث أنه إذا لم تكن هذه الشروط والشكل المطلوب من القانون للدليل، فإن القاضي لا يستطيع أن يحكم على أساسه، كما أنه لابد أن يصرف النظر عن اقتناعه الشخصي حتى ولو اقتنع يقينيا بما هو متوفر أمامه.[2]

يواجه الدليل الإلكتروني في ظل هذا النظام العديد من المشاكل، خاصة فيما يتعلق بقواعده التي تخص مضمون الأدلة كقاعدة استبعاد شهادة السماع، ومادام الدليل الإلكتروني في أصله يمثل شهادة سماع، و هذا باعتبار أنه يتكون من جمل وكلمات أدخلها شخص إلى جهاز الكمبيوتر، سواء تمت معالجة تلك البيانات أم لا، و هذا الأمر من شأنه أن يخلق اعتراضا على قبول المستندات المطبوعة التي يخرجها الحاسوب في الإثبات أمام القضاء الجنائي.

أما فيما يخص القواعد المتعلقة بكيفية تقديم الأدلة إلى القضاء، وكذا تحديد مدى قبولها كأدلة إثبات في المواد الجنائية، هناك قاعدة الدليل الأفضل أو المحرر الأصلي، و لو تم تطبيق هذه القاعدة على الدليل الإلكتروني لتم استبعاده كوسيلة إثبات في هذا النظام، و هذا الأمر أدى إلى تخوف رجال الضبط القضائي والمدعين العموميين من أن تكون مخرجات

---

[1]– بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي**، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، العدد، سنة 2014، ص 287.

[2]– مروك نصر الدين، **محاضرات في الإثبات الجنائي**، ج 1، دار هومة، ط 3، الجزائر،2009، ص 56.

طابعة ملف إلكتروني مخزن على الحاسوب غير أصلية، ولا تعني عين النسخة الحقيقية و التي تكون قيمتها أكثر من النسخة.

و منه يمكن أن نقول أن الدليل الإلكتروني له حجية و قوة ثبوتية بالنسبة للتشريعات التي تأخذ بنظام الإثبات المقيد، وقد حاولت بشكل كبير إعطاء القوة الثبوتية لهذا النوع من الأدلة وبالرغم من أن الدليل الإلكتروني يتعارض بسبب طبيعته مع أهم قواعد نظام الإثبات الجنائي المقيد، إلا أنه كان من الضروري الخروج عن الأصل العام في هذه القواعد وإيراد استثناءات عليها حتى يكون في الإمكان الأخذ بالدليل الإلكتروني، و هذا تماشيا مع التكنولوجيا الحديثة و إثبات الجريمة الإلكترونية.

أما عن نظام الإثبات الحر فقد جاء مناقضا للنظام الأول من خلال إعطاء الحرية التامة للقاضي الجنائي، في الأخذ بالأدلة الجنائية والأخذ بها وتقديرها، فدور القاضي الجنائي إيجابي في ظل هذا النظام بصفة عامة نظام الإثبات الحر يكرس مبدأ حرية القاضي في الاقتناع ، بمعنى أن القاضي حر في تكوين عقيدته من أي دليل يراه يفيد و يقتنع به.[1]

هذا النظام لا يحدد طرقا معينة للإثبات، وإنما يكون للخصوم حرية كاملة في اختيار الأدلة المؤدية إلى اقتناع القاضي ومساعدته في الوصول إلى الحقيقة، دون التقيد بطرق محددة، فالقاضي في هذا النظام له دور إيجابي في تسيير الدعوى وتكوين الأدلة والحكم بناءا على ما يصل إليه من حقائق.[2]

وفيما يتعلق بالدليل الإلكتروني فإن التشريعات التي تأخذ بهذا النظام لم تفرد نصوصا خاصة فيما يتعلق بقبول هذا الدليل، على أساس أن هذه التشريعات تستند لمبدأ حرية الإثبات في المسائل الجنائية، هذا المبدأ الذي يمثل أساس نظام الإثبات الحر، فمن خصائص هذا النظام عدم تحديد الأدلة، و كذا حرية القاضي في الأخذ بالأدلة و تقديرها و هذا ما يبين أن

[1]– محمد مروان، **نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري** ، ج 1، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 39.

[2]– محمد حسين منصور، **قانون الإثبات**، دار الجامعة الجديدة للنشر، مصر، 2002، ص 08.

القاضي الجنائي يمكنه أن يستند إلى الدليل الإلكتروني لإثبات الفعل الجنائي في سائر الجرائم بصفة عامة، والجرائم الإلكترونية بصفة خاصة في ظل هذا النظام.

بالنسبة لنظام الإثبات المختلط فقد حاول التوفيق بين النظامين السابقين، عن طريق الأخذ بإيجابيات كل منهما فهذا النظام يسعى إلى الجمع بين مفهومي كل من نظام الإثبات المقيد وكذا الحر للوصول إلى الحقيقة القضائية، و كذا محاولة التوفيق بينهما، أي إعمال كلا من النظامين معا.[1]

إن هذا النظام يقوم على تحديد أدلة الإثبات مسبقا من قبل المشرع، بحيث يتقيد القاضي بهذه الأدلة المحددة سلفا، و يقوم بتحديد قيمة وحجية كل من تلك الأدلة، كما أن ه يقوم على إعطاء القاضي حرية في تقدير الأدلة الموجودة في القضية المعروضة أمامه[2].

وبالنسبة للدليل الإلكتروني وفيما يتعلق بمبدأ تحدد الأدلة مسبقا فقد بينا فيما سبق أن التشريعات لم تنص على الدليل الإلكتروني باعتباره دليلا مستحدثا لجريمة مستحدثة كذلك، إلا أن هذه التشريعات وفي إطار مواكبة التكنولوجيا وتماشيا مع هذا النوع المستحدث من الأدلة والجرائم، فقد قامت بوضع استثناءات حتى تشمل هذا الدليل في تشريعاتها.

وبالنسبة لمبدأ حرية القاضي الجنائي فإنه لا يثير إشكالا باعتبار أن كل الأدلة الجنائية خاضعة لحرية وتقدير القاضي الجنائي، والدليل الإلكتروني دليل من أدلة الإثبات الجنائي، و بالتالي فهو خاضع لحرية القاضي وتقديره واقتناعه كغيره من الأدلة.[3]

وبهذا فإن المشرع الجزائري قد تبنى كقاعدة عامة نظام الاقتناع الشخصي للقاضي الجزائي، إلا واستثناء نجده أخذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محددة مسبقا وعلى سبيل الحصر.[1]

---

[1]– سامي جلال فقي حسين، **الأدلة المتحصلة من الحاسوب و حجيتها في الإثبات الجنائي**، دار الكتب القانونية، مصر، 2011، ص ص 79–80.

[2]– مرجع نفسه، ص 95.

[3]– سامي جلال فقي حسين، مرجع سابق، ص 95.

ويتضح ذلك من خلال المادتين المادة 212 من قانون الإجراءات الجزائية والتي تنص على أنه " يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص..." كما نصت المادة 307 من قانون الإجراءات الجزائية أيضا " أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم...".[2]

ومما سبق يطرح الإشكال التالي وذلك في حالة تطبيق نص المادة 212 من قانون الإجراءات الجزائية، نقول أنه إذا كان الدليل الإلكتروني ذو الأصالة العلمية هو الأوفر والأنسب في إثبات الجريمة المعلوماتية ، فما مدى إمكانية إعمال القاضي الجزائي لمبدأ الاقتناع الشخصي حيال هذا الدليل طبقا لأحكام المادة 212 من قانون الإجراءات الجزائية.

أولا/ مفهوم الاقتناع الشخصي للقاضي الجزائي : عرف فقهاء القانون الجنائي الاقتناع بأنه حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث، أو بمعنى آخر هو حالة ذهنية ذو خاصية ذاتية نتيجة تفاعل ضمير القاضي وأدلة الإثبات المطروحة والتي يثيرها الخصوم إما لإثبات أو إنكار اتهام.[3]

ثانيا/ سلطة القاضي الجزائي في تقدير الدليل الرقمي : لقد ثار خلاف حول سلطة القاضي الجزائي في تقدير الدليل الإلكتروني إذ أن هناك من يرى أن الدليل العلمي ومنه الدليل الرقمي له قوته الثبوتية الملزمة حتى للقاضي، مستندين في رأيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين وهناك من يرى أن مبدأ حرية القاضي في الاقتناع يجب أن يبسط سلطانه على كل الأدلة دون استثناء حتى على الدليل الرقمي،

---

[1]– المادتين 339 و 341 من قانون العقوبات الجزائري.

[2]– المادتين 212 و 307 من قانون الإجراءات الجزائية الجزائري.

[3]– مروك نصر الدين، مرجع سابق، ص620.

معتبرين أن إعطاء الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني (المقيد).

والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الجرائم التي قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن إليه.[1]

الطبيعة العلمية والتقنية للجريمة المعلوماتية غالبا ما تفرض على القاضي الاستناد في تكوين اقتناعه على الخبرة الفنية والتقيد بالنتيجة المتوصل إليها الخبير في تقرير خبرته ولا يمكنه طرحها واستبعادها إلا إذا قدر أن ما تحمله من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة العلمية ، فحسب الاجتهاد القضائي أنه أحيانا ما تكون الخبرة وحدها كافية بالنسبة للقاضي عندما يكون مطالبا للفصل في وقائع ذات طابع تقني دون أن يحتاج إلى مناقشتها.[2]

المطلب الرابع: الجزاءات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

سنتناول في هذا المطلب على الجزاءات المقررة لجريمة المساس بأنظمة المعالجة الآلية للمعطيات بالنسبة للشخص الطبيعي وكذا المعنوي.

الفرع الأول: العقوبات المقررة للشخص الطبيعي

نتناول في هذا المطلب العقوبات الأصلية والعقوبات التكميلية ثم ظروف تشديد العقوبة.

أولا/ العقوبات الأصلية: من خلال الإطلاع على المواد النصوص العقابية الخاصة بهذا النوع من الجرائم يلاحظ أن المشرع الجزائري اعتمد سلما تصاعديا للعقوبات حسب خطورة الجريمة والتي يمكن تقسيمها إلى ثلاث فئات.

---

[1]– سعيداني نعيم، مرجع سابق، ص 229.

[2]– قرار المحكمة العليا الغرفة الجنائية مؤرخ في 2002/06/04، نشرة القضاة رقم 58، لسنة 2006، ص25.

1- **جريمة الدخول أو البقاء الغ يرشرعي في صورتها البسيطة :** حسب نص المادة 394 مكرر من قانون العقوبات فإن العقوبة المقررة هي الحبس من 03 ثلاثة أشهر إلى سنة وغرامة من 50.000 دج إلى 100.000 دج.

2- **جريمة الدخول أو البقاء الغيرشرعي في صورتها المشددة :** حسب نص المادة 394 مكرر الفقرة 2 و 3 من قانون العقوبات تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة وتكون العقوبة من 06 ستة أشهر إلى سنتين 02 وغرامة من 50.000دج إلى 150.000 دج، إذا ترتب عن الدخول أو البقاء غير المشروع تخريب نظام اشتغال المنظومة.[1]

3- **جريمة المساس العمدي بالمعطيات والتعامل بمعطيات غير مشروعة :** طبقا لنص المادة 394 مكرر 1 ق ع فالعقوبة المقررة على جريمة التلاعب في بيانات تظم المعالجة للمعطيات هي الحبس من ستة أشهر إلى ثلاثة سنوات وغرامة من 500.000 دج إلى 2.000.000دج[2]، أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وذلك بتصميم أو بحث أو تجميع أو توفير أ نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية أو عن طريق حيازة أو إفشاء أو نشر أو استعمار لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها فعقوبتها هي الحبس من شهرين إلى ثلاثة سنوات وغرامة من 1.000.000 دج إلى 5.000.000 دج.

وقد اعتبر المشرع الجزائري الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي من المؤسسات الرسمية بمثابة طرف مشدد، وذلك من خلال نص المادة 394 مكرر 3 ق ع أن العقوبة المشددة تنصرف على جميع الجرائم المنصوص عليها في نص المادة 394 مكرر والمادة 394 مكرر 1 ومكرر 2.

---

[1]– نبيل صقر، أحمد لعور، **موسوعة الفكر القانوني قانون العقوبات نصا وتطبيقا** ، دار الهدى، الجزائر، 2007، ص 270.

[2]– المادة 394 مكرر 1 من قانون العقوبات الجزائري.

أما في حالة الاتفاق الجنائي بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية فقد عاقب عليها المشرع بموجب نص المادة 394 مكرر 5 والحكمة من ذلك هو توسيع نطاق العقوبة بإخضاع الأعمال التحضيرية التي تسبق البدء في التنفيذ، بهذا فإن عقوبة الاتفاق الجنائي هي نفسها عقوبة الجريمة ذاتها.

أما عن الجزاء المقرر في حالة الشروع فقد نصت المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وبالرجوع إلى نص المادة 394 مكرر 7 من قانون العقوبات فإنه يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم الخاص بالمساس بالمعالجة الآلية للمعطيات بالعقوبات المقررة للجنحة ذاتها.[1]

ثانيا/ العقوبات التكميلية: من خلال نص المادة 394 مكرر 6 استثنت الغير حسن النية بحفظ حقوقه، ونصت على العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصلية والمتمثلة في:[2]

1- **المصادرة:** وتشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية.

2- **إغلاق المواقع** : يتعلق الأمر بالمواقع التي تكون محل لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

3- **إغلاق المحل أول مكان الاستغلال:** إذا كانت الجريمة قد ارتكبت بعلم مالكها مثلا إغلاق المقهى الانترنت الذي ترتكب فيه مثل هذه الجرائم.

الفرع الأول: العقوبات المقررة للشخص الطبيعي

بموجب نص المادة 18 مكرر من قانون العقوبات يقرر المشرع الجزائري المسؤولية الجزائية للشخص المعنوي سواء كان فاعلا أصليا أو شريكا، كما أنه يسأل جزائيا عن

[1]- المادة 394 مكرر 7 من قانون العقوبات الجزائري.

[2]- المادة 394 مكرر 6 من قانون العقوبات الجزائري.

الشروع، لكن بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي أو بواسطة أحد ممثليه أو أعضائه.[1]

وبهذا فالعقوبات المقررة للشخص المعنوي في مواد الجنايات والجنح هي:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.
- الاقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر وتعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة على النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

تساوي الغرامة من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة مع إمكانية الحكم بمصادرة الشيء الذي استعمل في ارتكاب الجريمة أو ما نتج عنها.[2]

[1]- المادة 18 مكرر من قانون العقوبات الجزائري.

[2]- زيبخة زيدان، مرجع سابق، ص 102.

الخاتمة

من خلال هذه الدراسة حاولنا قدر الإمكان من معالجة كل الجوانب الخاصة بالجرائم الماسة بالأنظمة المعلوماتية، وبهذا فإن هذا النوع من الجرائم يشكل تهديدا مباشرا وغير مباشرا لتقدم البشرية، حيث يقوم بارتكابها أشخاص على درجة عالية من الذكاء يستعملون التكنولوجيا هدفهم في ذلك إضرار المجتمع وليس خدمته.

وبهذا فهي جرائم تتميز بقدر عال من التعقيد، يزداد تعقيدها كلما تطورت التكنولوجيا، فالتطور التكنولوجي سلاح ذو حدين يستفيد منه الجاني أيضا لتطوير وسائل ارتكاب الجرائم واتخاذ صور جديدة منها، مما يجعل متابعة الجرائم والتحقيق فيها لا يخلو من العراقيل والعقبات المادية والقانونية، هذا الذي يفرض تكوين فئة معينة من رجال القانون متمكنين من المادة التي يبحثون فيها لجمع الآلة والحفاظ عليها وتتبع آثار الجريمة التي تكاد تنعدم مما يحتم بحثا احترافيا.

خصوصية هذه الجرائم استوجبت كذلك على المشرع أن يدعم رجال الضبطية القضائية بإجراءات جديدة للبحث والتحري لم تكن معروفة في ظل الإجرام التقليدي ومنها التسرب، اعتراض المراسلات، التقاط الصور وتسجيل الأصوات، إلى جانب بقاء الإجراءات المعروفة سابقا سارية المفعول (كالمعاينة، جمع وضبط الأدلة، التوقيف للنظر،التفتيش)، مع منح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات نوع من الخصوصية تظهر من حيث تمديد مدة التوقيف للنظر المسموح بها، و تظهر كذلك من خلال إجراء التفتيش الذي يسمح بالقيام به ليلا و نهارا و دون اشتراط حضور صاحب المسكن أو رضاه.

تظهر أيضا الخصوصية من خلال الاختصاص المحلي الموسع الذي منحه المشرع الجزائري لأربع جهات قضائية في مجال المتابعة والتحقيق والحكم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بحيث جعله يمتد لدائرة اختصاص جهات قضائية أخرى، وهذه الجهات القضائية ذات الاختصاص الموسع أو ما يعرف أيضا بالأقطاب الجزائية

المتخصصة تتطلب تخصصا للقضاة في مجال جرائم المعلومات حتى يكون تعاطيهم مع هذه الملفات أسهل، وهذا ما تم استلهامه من التشريع الفرنسي.

وأهم خصوصية أيضا تبرز في صعوبة الإثبات، لأن مسرح الجريمة المعلوماتية هو مسرح افتراضي غير محسوس، و لهذا فالدليل تحول و صار رقميا، و دور الخبراء مهم في هذا النوع من الجرائم نظرا لطابعها التقني الذي يحتاج ندب خبراء مختصين في المجال، حتى أنه و لطغيان التقنية على القانون صار يخشى من تأثر القضاة بالخبراء.

نتائج الدراسة:

من خلال دراستنا لهذا الموضوع يمكننا التوصل إلى نتائج أهمها:

– قصور النصوص التشريعية الخاصة بهذه الجرائم من الناحية الموضوعية مما يترتب ضعف الحماية الجزائية للفرد والمجتمع من هذه الجرائم، و أيضا من الناحية الإجرائية مما ينعكس سلبا على إجراءات التحري، المتابعة، التحقيق والمحاكمة والبحث عن الدليل في ظل جرائم صعبة الإثبات لا اثر لها.

– إن أهم مميزات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات،أنها تنصب على محل من نوع خاص يختلف تماما على محل الجرائم التقليدية فهذه الجرائم تستهدف المساس بالمعلومات الإلكترونية المتواجدة في البيئة الرقمية على هيئة إشارات ونبضات غير مرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الاتصال العالمية.

– طبيعة هذه الجرائم وارتباطها بمستوى رفيع من التكنولوجيا المعلوماتية يحتم تأهيل بشري بذات المستوى، سواء من رجال الضبطية أو القضاة في مراحل التحقيق أو المحاكمة، وهي الجرائم التي غيب فيها دور القاضي في البحث عن الأدلة نسبيا وأصبح الخبير المعلوماتي هو من يلعب الدور الرئيسي في إيجاد الدليل.

– أن الدليل المناسب والأوفر في إثبات الجريمة المعلوماتية هو الدليل الرقمي والذي هو عبارة عن معلومات مخزنة في النظم المعلوماتية في شكل نبضات مغناطيسية أو كهربائية من الممكن من الناحية التقنية استخلاصه من البيئة الرقمية التي يتواجد بها، وتجميعه باستخدام برامج وتطبيقات تقنية، ليظهر بعد ذلك في شكل مخرجات إلكترونية أو حتى ورقية بعد طبعه.

– إن بحث حول مسألة تقدير القيمة القانونية للدليل الرقمي أنه يجب التمييز بين أمرين الأول : القيمة العلمية القاطعة للدليل الرقمي والثاني : الظروف والملابسات التي تحيط هذا الدليل، فالقاضي ليس له أن ينازع فيما أسفرت عليه تكنولوجيا المعلوماتية والعلوم التقنية من الناحية العلمية وإنما له أن يقدر الظروف والملابسات التي أحاطت هذا الدليل، ويمكن له في سبيل ذلك الاستعانة بطرق الإثبات التقليدية التي توجد عادة إلى جانب الدليل الرقمي، وله في ذلك أن يرفض هذا الدليل إذا لم يقتنع بظروف القضية وملابساتها.

اقتراحات الدراسة :

من خلال معالجتنا لجريمة المساس بأنظمة المعالجة الآلية للمعطيات نرى ضرورة دعم هذه الدراسة بالاقتراحات التالية:

1– استحداث قانون جنائي للمعلوماتية مستقل يحدد ويجرم كل أنواع جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وتحديد الجهات المختصة بمراقبة هذه الجرائم.

2– من بين المميزات التي تتميز بها الجرائم الماسة بالأنظمة المعلوماتية طابعها العابر للحدود الوطنية مما ينتج صعوبة كشفها وكشف مرتكبيها والقانون الواجب التطبيق، فكان لابد من تعزيز التعاون الدولي فيما بين الدول للقضاء على هذه الظاهرة وإخضاع إجراءات البحث والتحري إلى السرعة قبل طمس أدلة الإثبات.

3- ضرورة استحداث قواعد مناسبة في مجال الإجراءات الجزائية لعدم ملائمة الإجراءات الجزائية الحالية في محال التحقيق في جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

4- العمل على تكوين متخصصين وخبراء قادرين على تشخيص الجريمة قبل عرضها على المحكمة للفصل فيها.

5- ضرورة استحداث استراتيجيات عقابية وتقنية لحماية ضحايا هذه الجريمةـ خاصة فئة الأطفال ورجال المال كونهم الأكثر عرضة لها.

قائمة المصادر والمراجع

أولا : المصادر

1- الأمر 66 - 155، المؤرخ في 8 جوان 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بالقانون رقم 15-22 المؤرخ في 13 مارس 2016، الجريدة الرسمية، العدد40 سنة 2016.

2- الأمر 66 - 156، المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 15-19 المؤرخ في 30 ديسمبر 2015، الجريدة الرسمية، العدد 71، سنة 2016.

3- المرسوم التنفيذي رقم 348-06 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجهورية وقضاة التحقيق، ج ر، العدد 63، الصادرة بتاريخ 08 أكتوبر 2006.

4- القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، ج ر، العدد 47، الصادرة سنة 2009.

5- القانون رقم 16-01 المؤرخ في 06 مارس 2016 المعدل للدستور الجزائري، ج ر، رقم 14، المؤرخة في 7 مارس 2016، ص 16.

ثانيا: المراجع

1- الكتب:

1- أحسن بوسقيعة، **التحقيق القضائي**، دار هومة، ط 5، الجزائر، 2000.

2- ــــــــــــ، **الوجيز في القانون الجزائي الخاص** ، ج1، دار هومة ، ط 3، الجزائر، 2011.

3- ـــــــــــــ، **الوجيز في القانون الجزائي العام** ، دار هومة، ط 10، الجزائري، 2011.

4- أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري** ، دار هومة، ط 2، الجزائر، 2007.

5- أمير فرج يوسف، **الجرائم المعلوماتية على شبكة الانترنت** ، دار المطبوعات الجامعية، مصر،2009 .

6- انتصار غريب، **أمن الكمبيوتر والقانون**، دار الراتب الجامعية، بيروت، 1998.

7- جباري عبد المجيد ، **دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة** ، دار هومة للنشر والتوزيع، الجزائر، 2012.

8- جعفر حسن جاسم الطائي ، **جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة**، دار البداية ناشرون وموزعون، عمان، 2007.

9- جميل عبد الباقي، **القانون الجنائي والتكنولوجيا الحديثة**، دار النهضة العربية، مصر، 1992.

10- جميلالي بغدادي، **التحقيق دراسة مقارنة وتطبيقية**، الديوان الوطني للأشغال التربوية، الجزائر1999.

11- حجازي عبد الفتاح بيومي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت**، دار الكتب القانونية، مصر، 2002.

12- خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت** ، دار الثقافة للنشر والتوزيع، 2011.

13- خالد ممدوح إبراهيم، **التقاضي الإلكتروني** ، دار الفكر الجامعي ، الإسكندرية، 2009.

14- ـــــــــــــــ ، **أمن المستندات الإلكترونية**، الدار الجامعية، الإسكندرية، 2008.

15- ـــــــــــــــ، **أمن المعلومات الإلكترونية** ، الدار الجامعية ، الإسكندرية، 2008.

16- ـــــــــــــــ، **فن التحقيق الجنائي في الجرائم الإلكترونية**، دار الفكر الجامعي، الإسكندرية، 2010.

17- رشا علي الدين ، **النظام القانوني لحماية البرمجيات بين نظرية تنازع القوانين و القانون الدولي الإتفاقي**، الطبعة الأولى، مصر، 2004.

18- رشيدة بوكر، **جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن**، منشورات الحلبي الحقوقية الطبعة الأولى، بيروت، 2012.

19- عبد الله أوهايبية، **شرح قانون الإجراءات الجزائية الجزائري**- التحري والتحقيق، دار هومة الجزائر، 2004.

20- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، 2003.

21- علي حسن محمد الطوالبة ، **التفتيش الجنائي على نظم الحاسوب والإنترنت** ، عالم الكتب الحديثة، الأردن، 2004.

22- عماد محمد سلامة، **الحماية القانونية لبرنامج الحاسب الآلي ومشكلة قرصنة البرنامج الأول**، دار وائل للنشر، عمان، 2005.

23- فتحي محمد أنور عزت ، **الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية**، دار الفكر والقانون للنشر والتوزيع، مصر 2010.

24- محمد أمين أحمد الشوابكة ، **جرائم الحاسوب و الانترنت** ، مكتبة دار الثقافة للنشر والتوزيع، الأردن، 2004.

25- محمد أمين الرومي، **جرائم الكمبيوتر والانترنت** ، دار المطبوعات الجامعية، الإسكندرية، 2003.

26- محمد حزيط، **مذكرات في قانون الإجراءات الجزائية الجزائري** ، دار هومة، الجزائر، ط 8، 2013.

27- محمد حسين منصور، **قانون الإثبات**، دار الجامعة الجديدة للنشر، مصر، 2002.

28- محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2007.

29- محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت**، دار النهضة العربية، القاهرة، 2009.

30- محمد محمد الهادي، **تكنولوجيا المعلومات وتطبيقا تها**، الطبعة الأولى دار الشروق، القاهرة، 1989.

31- محمد مروان، **نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري** ، ج 1، ديوان المطبوعات الجامعية، الجزائر، 1999.

32- محمود أحمد عبانه ، **جرائم الحاسوب و أبعادها الدولية** ، دار الثقافة للنشر و التوزيع، الأردن، 2009.

33- زيبخة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي** ، دار الهدى، الجزائر، 2011.

سامي جلال فقي حسين، **الأدلة المتحصلة من الحاسوب و حجيتها في الإثبات الجنائي**، دار الكتب القانونية، مصر، 2011، ص ص 79-80.

34- عبد الله حسين علي محمود، **سرقة المعلومات المخزنة في الحاسب الآلي** ، دار النهضة العربية، مصر، 2001.

35- مروك نصر الد ين، **محاضرات في الإثبات الجنائي** ، ج 1، دار هومة ، ط 3، الجزائر،2009.

36- مصطفى محمد موسى ، **التحقيق الجنائي في الجرائم الإلكترونية**، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2009.

37- مفتاح محمد دباب، **معجم المصطلحات وتكنولوجيا المعلومات والاتصالات** ، الدار الدولية للنشر، القاهرة، 1995.

38- ممدوح عبد الحميد عبد المطلب، **البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت**، دار الفكر القانونية.مصر، 2006.

39- زائلة عادل محمد فريد قورة ، **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي، ط1، بيروت، 2005.

40- نبيل صقر، أحمد لعور، **موسوعة الفكر القانوني قانون العقوبات نصا وتطبيقا** ، دار الهدى، الجزائر، 2007.

41- نسرين عبد الحميد نبيه، **الجريمة المعلوماتية والمجرم المعلوماتي** ، منشأة المعارف، الأردن، 2008.

42- نهلا عبد القادر المومني ، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، ط 1، عمان، 2008.

43- هدى حامد قشقوش، **جرائم الحاسب الإلكتروني في التشريع المقارن** ، دار النهضة العربية، القاهرة ،1992، ص05.

44- هشام محمد فريد رستم ، **قانون العقوبات ومخاطر تقنية المعلومات** ، مكتبة الآلات الحديثة، مصر ،1992.

45- هلالي عبد الله أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست**، دار النهضة العربية، القاهرة، 2003.

46- ه لالي عبد الله أحمد، **تفتيش نظم الحاسب الآلي وضمانات الم تهم المعلوماتي**، دار النهضة العربية، مصر، 2006.

47- ـــــــــــــــ ، **حجية المخرجات الكومبيوترية في المواد الجنائية** ، دار النهضة العربية، ط 2، مصر، 2008.

ب- الرسائل الجامعية:

1- بوذراع عبد العزيز، **خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** (مذكرة ماجستير في القانون الجنائي والعلوم الجنائية)، كلية الحقوق، جامعة الجزائر 1، 2011.

2- جدي نسيمة، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات** (مذكرة ماجستير في القانون الجنائي)، كلية الحقوق ، جامعة وهران، .

3- رصاع فتيحة، **الحماية الجنائية للمعلومات على شبكة الانترنت** (مذكرة ماجستير في القانون العام)، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2011.

4- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**(مذكرة ماجستير في القانون تخصص علوم جنائية)، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2012.

5- سوير سفيان، **جرائم المعلوماتية** (مذكرة ماجستير في العلوم الجنائية وعلم الإجرام)، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2010.

6- لحمر نبيل، **دور الأقطاب الجزائية المتخصصة في مكافحة الجريمة** (مذكرة ماجستير في قانون العقوبات والعلوم الجنائية)، كلية الحقوق، جامعة قسنطينة 1، 2014.

ج- المقالات العلمية:

1- بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي**، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، العدد، سنة 2014.

2- مليكة عطوي، **الجريمة المعلوماتية**، حوليات جامعة الجزائر، العدد 21، جوان 2011.

2- المواقع الإلكترونية:

1- La réforme de la justice en Algérie piétine, http://www.algerie-dz.com/article9990.html,.20:57 : الساعة ،2017/05/04 تاريخ الاطلاع:

2- عبد الله حسين علي محمود، بحث بعنوان **إجراءات جمع الأدلة في مجال جرائم سرقة المعلومات**، مأخوذ من الموقع الإلكتروني http://www.f-law.net/law/threads/1133، تاريخ الإطلاع: 2017/05/15، ساعة الإطلاع: 18:07.

3- المجلات القضائية:

1- قرار المحكمة العليا الغرفة الجنائية مؤرخ في 2002/06/04، نشرة القضاة رقم 58، لسنة 2006.

الفهرس

ملخص:

تعد جرائم المساس بأنظمة المعالجة الآلية للمعطيات من أهم موضوعات البحث التي فرضت نفسها للدراسة والبحث، كونها من الجرائم التي تمس بالفرد والدولة بمؤسساتها العامة والخاصة، وليس على المستوى الداخلي فحسب بل يمتد أثرها على المستوى الدولي مما جعل الدول تلجأ لإبرام اتفاقيات دولية ثنائية ومشتركة لمواجهة هذه الجرائم.

يكتسي هذا الموضوع أهمية بالغة، إذ يعد من الموضوعات الجديدة والمهمة في الجانب الإجرائي والخصوصيات التي تشمل هذا النوع من الجرائم من حيث القانون الواجب التحقيق والاختصاص القضائي من جهة، وأساليب التحري الخاصة بهذه الفئة من الجرائم دون غيرها المنصوص عليها بقانون الإجراءات الجزائية، وكذا بعض الأحكام الخاصة المنصوص عليها بالقانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال للحصول على ما يسمى بالدليل الإلكتروني، إلى جانب الأحكام المتعلقة بالجزاءات المقررة للشخص المعنوي والطبيعي، وكذا عقوبة الشروع والاتفاق الجنائي، إضافة للدور الذي يلعبه التعاون الدولي في مكافحة هذه الجرائم المتسمة بطابع دولي عابر للحدود.

الكلمات المفتاحية: الجريمة المعلوماتية – جريمة المساس بأنظمة المعالجة للمعطيات– الدليل الرقمي– القانون رقم 04/09– قانون العقوبات