الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم: القانون العام

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجريمة المعلوماتية في ظل التشريع الجزائري

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق.

التخصص: قانون جنائي وعلوم جنائية

من إعداد الطالب(ة):

عباسة محمد ياسين

تحت إشراف الأستاذ(ة):

أ / مزيود بصيفي

أعضاء لجنة المناقشة

الأستاذ(ة).....برابح هدى.....رئيسا

الأستاذ(ة).....مزيود بصيفي.....مشرفا مقررا

الأستاذ(ة).....بن عزوز سارة.....ممتحن

السنة الجامعية: 2021/2020

تاريخ المناقشة 2021/07/07

كلمة شكر

بداية الشكر لله عز وجل الذي وفقنا لإتمام هذا العمل المتواضع

كما أشكر الأستاذ المؤطر " مزيود بصيفي" والذي ساعدني كثيرا في إعداد مذكرتي جعلها في ميزان حسناته يوم لا ظل إلا ظله.

والشكر موصول لجميع أساتذة كلية الحقوق والعلوم السياسية عبد الحميد بن باديس جامعة مستغانم من درسني ومن لم يدرسني

وختاما أشكر كل من ساهم معي وساعدني في إنجاز هذا العمل من بعيد أو قريب ولو بالكلمة الطيبة والدعم المعنوي

ياسين

الإهداء

أهدي ثمرة جهدي وتعبي إلى :

الوالدين الكريمين أطال الله في عمرهما

الأخوة والأخوات أدامهم الله نعمة لا تزول

زملاء الدرب الدراسة أنار الله لهم الطريق

إلى كل طالب علم

ياسين

المقدمة

تمخض عن الفكر الإنساني في العقدين الرابع والخامس من القرن الماضي عن ابتكار أعظم ما قدمته الحضارة الإنسانية إلا وهو الحاسوب، مما أهل لحقبة جديدة بالغة الأهمية أحدثت تأثيرا في بنية المجتمع، حيث تطورت وذلك نتيجة لاكتساح جميع النواحي التي تتطلبها الحياة البشرية، مما جعل منها مصدرا أساسيا للأشخاص، وكذا المؤسسات للاعتماد عليه في كافة شئونهم نظرا للسرعة والدقة في تخزين المعلومات ومعالجتها في وقت قصير.

حيث عرفت هذه الفترة المعلوماتية تطورا مذهلان كما ساعد اقترانها بالتكنولوجيات أخرى على تعميم استعمالها وتعدد وظائفها، فالحديث اليوم لم يعد عن الحاسوب وقدراته في اختزال الوقت وتخزين المعلومات أو إنجاز العمليات المعقدة، وإنما عن تكنولوجيا الإعلام والاتصال، والفضاء الافتراضي الذي نشأ نتيجة ارتباط المعلومات بمختلف المواصلات السلكية واللاسلكية.

حيث أصبحت هذه الوسيلة ليست حكرا فقط على الدول المتقدمة، وإنما تعدت إلى غير ذلك (الدول النامية)، مما زاد من أهمية هذه التكنولوجيات، حيث عرفت بما يسمى بعصر المعلومات، ففي محاضرة ألقاها "كيراك أرثر" مدير إدارة السلامة العامة والعدل التابعة لشركة ميكروسوفت، خلال مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية بالدوحة خلال شهر أفريل 2005، أكد أن حجم البيانات الرقمية المتنامي سيبلغ بحلول عام 2020 أربعين عام زيتابايت، عد ما بلغ 1.8 زيتابيات عام 2012، إضافة إلى تأكيد أن 1.7 مليار شخص يستخدمون رسائل التواصل الاجتماعي وأن أكثر من 6.8 مليار شخص يستخدمون الهاتف النقال.

ومع التغلغل المتزايد للمعلومات وتكنولوجيا الاتصال في مختلف النشاطات البشرية، إذ اعتبرت فضاءا مفتوحا لا حدود له مقارنة بالحدود الإقليمية للدول، وذلك لكون جميع الدول والمنظمات والمؤسسات خاصة المالية المرتبطة ارتباط وثيق بها من أجل ممارسة أعمالهم ونشاطاتهم، وتقديم مختلف الخدمات لزبائنهم.

الأمر الذي أدى بأصحاب النوايا الإجرامية إلى الاتجاه إلى الاستعمال غير الشرعي لهذه المنظمات المعلوماتية، من أجل ارتكاب أعمالهم الإجرامية المختلفة، من جهة الانتفاع بها، ومن جهة أخرى التملص من لمسئولية الجزائية، وأمام هذا الزحف المتزايد للأنظمة المعلومات ظهر شكل جديد من الإجرام وهو ما يعرف بالإجرام أو الجرائم المعلوماتية.

إذ أنه وبظهور هذا النوع من الإجرام جعل من المجتمع الدولي التدخل من أجل وضع حد لانتشاره، فكان لا بد من وضع أطر قانونية ملائمة جديدة أو إدخال تعديلات على قوانين سارية المفعول بما يتلاءم والوضع الجديد، لتحديد شروط استعمال هذه الوسائل في مختلف المعاملات، من خلال نصوص جزائية لحماية الأنظمة المعلوماتية، وردع إساءة استعمالها سواء محليا أو دوليا في إطار الاتفاقيات الدولية.

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

وهو ما يوجب على القانون أن يمتد نصوصه إلى هذه الأنشطة الجديدة التي تفرزها التكنولوجيا حتى تتخذ الجريمة في نصوص منضبطة واحدة، إذ أصبحت النصوص التقليدية لا يمكن أن تسري أو تطبق على هذا النوع من الجرائم، مما أدى إلى ظهور مشكلات إجرامية في هذا المجال.

والجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا، فهي أيضا معينة بالمكافحة فكان لا بد من إيجاد إطار قانوني مناسبا لسد الفراغ الإجرائي، لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المعلوماتية عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة ومنها الجريمة المعلوماتية، ومنها إجراءات تطبق فقط على الجريمة المعلوماتية فقط، والتي تم النص عليها في قانون جديد يتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحته في القانون رقم 04/09 المؤرخ في أوت 2009.

أهمية البحث:

تكمن أهمية البحث أساسا في كون الجرائم المعلوماتية جريمة جديدة، بالتالي لا يمكن تطبيق الإجراءات التي تطبق على الجرائم التقليدية لأنها من الموضوعات لتي لم تنل حقها من البحث والتحقيق والمحاكمة، على المستوى الجزائي، حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها لاسيما أن هذا لموضوع يتسم بالحداثة وقلة المراجع التي يمكن الاعتماد عليها.

بالإضافة إلى كون الجرائم المعلوماتية حديثة النشأة، ويمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال، والتي تستخدم في جميع المجالات الحياة سواء من طرف الأفراد أو المؤسسات، إذ تجعل التعاملات معها صعبا ومعقدا، مما يحتم إيجاد طرق جديدة وتابعة لمكافحتها.

أسباب اختيار الموضوع:

1. الأسباب الذاتية:

- تكمن في اهتمامنا بمجال الجريمة المعلوماتية، وما يلقاها من جرائم، وكذا من إجراءات
- أنه موضوع يستحق البحث ويثير الفضول
- موضوع حيوي وجديد لأنه من الجرائم المستحدثة
- رغبة وميول شخصي لدراسة الموضوع

2. الأسباب الموضوعية:

- تسليط الضوء على الموضوع من خلال التعرف على مفهومه والوقوف على أسباب ارتكاب هذا النوع من الجرائم
- التعمق في تفاصيل الجرائم لمعلوماتية وما يحيط بها من اعتداء على نظم المعلوماتية ومعالجة الأنظمة الآلية وغيرها
- التعرف على القواعد الإجرائية والجزاءات التأديبية المترتبة عن ارتكاب الجريمة المعلوماتية .

ثم إنه وبظهور الإجرام المعلوماتي أثار العديد من المشاكل خاصة الإجرائية في مجال الجريمة المعلوماتية، باعتبار أن تلك الجرائم هي صعبة الكشف عنها ومتابعة مرتكبها، بالإضافة إلى أنها ترتكب على مسرح الإلكتروني غير مادي يختلف عن مسرح الجريمة التقليدي، مما يجعل قانون الإجراءات الجزائية قاصرا على إجراءات المتابعة في الجرائم التقليدية فقط، على الأمر الذي أدى إلى تدخل المشروع تعديل قانون الإجراءات الجزائية واستحداث قانون خاص يتضمن جميع القواعد الإجرائية التي يمكن من خلالها لجهات البحث والتحقيق والقضاء التحري من أجل الوصول إلى الدليل المناسب لإثبات الجريمة المعلوماتية، ومنه نطرح الإشكالية التالية:

كيف نظم المشرع الجزائري الجريمة المعلوماتية باعتبارها من الجرائم المستحدثة؟

أو بمعنى أخر: ما هي القواعد الإجرائية التي استحدثها المشرع الجزائري لمواجهة الجريمة المعلوماتية؟

ولقد اعتمدنا في دراستنا هذه على المنهج التحليلي والمنهج الوصفي لأنهما يعتبران الأنسب لمثل هذه الدراسات.

كما ارتأينا تقسيم البحث وفق الخطة الثنائية، حيث تطرقنا في الفصل الأول إلى مـاهية الجريمة المعلوماتية، بينما خصصنا الفصل الثاني إلى مكافحة الجريمة المعلوماتية في ظل التشريع الجزائري.

الفصل الأول

عرفت البشرية في نهاية القرن الماضي اتساعات وتزايدا مطردا لنطاق استخدام تقنية المعلوماتية في المجتمع، ونظرا للتطور السريع لهذه التقنية، فقد مكنت من استعمالات متعددة وفي جميع المجالات، مما أدى إلى ظهور نوع جديد من الجرائم أطلق عليها تسمية الجرائم المعلوماتية.

ولقد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة ونظرا لجسامة أخطارها وفداحة خسائرها وسرعة انتشارها، أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفئتين والمهتمين بأمن الصرح المعلوماتي، لتحديد مفهومها وخصائصها، والتمييز بينها وبين ما يقترب منها من ظواهر، ومعرفة العوامل المختلفة التي تتدخل في هذا التحديد.

المبحث الأول مفهوم الجريمة المعلوماتية

لقد ترتب على الاستخدام المتزايد لنظم المعلومات إلى نشوء ما يعرف بالجريمة المعلوماتية، ولقد استخدمت عدة مصطلحات للدلالة على هذه الظاهرة الإجرامية فمنهم من يطلق عليها: الغش المعلوماتي، والبعض الآخر يطلق عليها اسم جرائم الحاسب الآلي، والآخر جرائم الكمبيوتر والانترنت أو الجريمة الالكترونية.[1]

إن الجريمة المعلوماتية جريمة مستحدثة يعتمد مرتكبها على وسائل تقنية ويكون ذا دراية كافية باستخدام النظم المعلوماتية لذا فإن الإحاطة بمفهومها الدقيق لا يزال محل خلاف فقهي، فهي ظاهرة إجرامية مستحدثة تتميز عن الجريمة التقليدية، وتختلف عنها من حيث المفهوم، ولإزالة اللبس سنتعرض في هذا المبحث إلى مطلبين:

المطلب الأول تعريف الجريمة المعلوماتية

تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلي الخلاف الذي أثير بشأن تعريف هذه الجريمة، فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة، وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها. [2]

[1]: قربوز حليمة ،الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2006_2009، ص12.

[2] :أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الطبعة الرابعة، 2007، ص 104.

الفرع الأول التعاريف الفقهية

على الرغم من تنامي جهود التصدي لظاهرة الإجرام المعلوماتي إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق وجانب أخر عرفها على نحو موسع.

أولا: التعريف الموسع للجريمة المعلوماتية.

ذهب الفقيهان (Michel و Credo) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته.[1]

ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها:"كل سلوك اجرامى يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر".

ويعرفهاTièdementبأنها ":كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب " .

من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة المعلوماتية، حيث أن مجرد مشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة المعلوماتية.[2]

[1]: طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي ،جامعة الجزائر 1، كلية الحقوق ،2011،2012، ص6.

[2]: المرجع نفسه، ص 7.

ويعرفها (David Tompson):"جريمة يكون متطلبا لاقترافها أن يتوفر لدى فاعلها معرفة تقنية الحاسب".[1]

والدكتور هلالي عبد الله أحمد يرى أنها:"عمل أو امتناع يأتيه إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا".

ثانيا: التعريف الضيق للجريمة المعلوماتية

يعرف الفقيه الفرنسي (Mass) جريمة الكمبيوتر بأنها:" الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[2] وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال استخدم لهذا التعريف معيارين هما: الوسيلة، وتحقيق الربح المستمد من معيار محل الجريمة المتمثل في المال.

ويعرفها الفقيهان الفرنسيان (Vivant و Le Stant) بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب" هذا التعريف مستند من بين معيارية على احتمال جدارة الفعل بالعقاب وهو معيار غير منضبط ولا يستقيم مع تعريف قانوني وان كان يصلح هذا التعريف في نطاق علوم الاجتماع وغيرها.

وعرفها (كلاوس تايدومان) بأنها:"كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلي".[3]

---

[1]: عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002،ص4

[2]: ابرهيمي سهام،مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2004، 2007، ص7.

[3] :المرجع نفسه، ص 8.

ويرى البعض أن تعريف كلا من (Marwe)و(Ros Blat) جاءا مقصورين على الإحاطة بالظاهرة الإجرامية أما تعريف كلاوس تايدومان فيؤخذ عليه أنه بالغ في العمومية والاتساع، لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع.[1]

الفرع الثاني الجريمة المعلوماتية في الاتفاقيات الدولية

قدمت المادة الأولى من الاتفاقية الدولية للإجرام المعلوماتي تعريف للنظام المعلوماتي على النحو التالي:"يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات صلة بذلك ويقوم إحداهما أو أكثر من واحد منها تبعا للبرنامج بعمل معالجة آلية للبيانات ويقصد ببيانات الكمبيوتر أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها".

عرف المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين الجريمة المعلوماتية بأنها:"أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[2]

يذهب البعض إلى أنة عند وضع تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة اعتبارات مهمة منها:

- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.
- أن يراعى هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.

[1]: عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت،الطبعة الأولى، دار الفكر الجامعي، مصر ،2006،ص98.

[2]: عقد هذا المؤتمر في فيينا في الفترة ما بين (10-17) افريل2000.

- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الاجرامى.
- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.[1]

الفرع الثالث: موقف المشرع الجزائري من الجريمة المعلوماتية

تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون15/04المؤرخ في 2004/11/10 المتضمن تعديل قانون العقوبات[2]، ولكن المشرع تناول في النصوص المستحدثة الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي وسنبين بصفة موجزة الأفعال التي جرمها المشرع الجزائري بموجب القانون السالف الذكر:

1-جريمة التوصل أو الدخول غير المصرح به: نصت عليه المادة 394 مكرر من قانون العقوبات بقولها "يعاقب بالحبس و الغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة."[3]

---

[1]:أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الطبعة الثالثة، الجزائر، 2007، ص 73.

[2]: القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات (ج ر 71 بتاريخ 2004/11/10).

[3] :نبيل صقر، موسوعة الفكر القانوني، جرائم الكمبيوتر والانترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، طبعة 2005، ص 304.

فقد أورد المشرع ظرفي تشديد لعقوبة الدخول غير المشروع وهما: في حالة ما إذا ترتب عن الدخول غير المشروع حذف أو تغيير المعطيات، أو تخريب نظام اشتغال المنظومة، وقد نص المشرع في المادة المذكورة على تجريم فعل الشروع في جريمة الدخول غير المصرح به وذلك بقوله" أو يحاول ذلك."

2-جريمة التزوير المعلوماتي: نص عليها المشرع في نص المادة 394 مكرر 1 بقوله "يعاقب بالحبس وبالغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها[1]."

3-جريمة الاستيلاء على المعطيات:نصت عليها المادة 394 مكرر 2 بقولها" **كل من يقوم** عمدا و بطريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

4-جريمة إتلاف وتدمير المعطيات: نص عليها المشرع الجزائري بالمادة 394 مكرر 1 من قانون العقوبات" يعاقب بالحبس والغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها "وجريمة الإتلاف حسب نص المادة المذكورة تتمثل في إزالة معطيات نظام المعالجة الآلية عن طريق الفيروسات.[2]

---

[1]: تنص المادة 394مكرر2 من قانون العقوبات:"يعاقب بالحبس والغرامة 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 مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

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

[2] : أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري،الطبعة الأولى، دار هومة، ص99.

5. جريمة الاحتيال المعلوماتي:وهو ما نصت عليه المادة 394 مكرر 1/2 بقولها" يعاقب بالحبس وبالغرامة كل من قام بطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية "... أي أن يهدف مرتكبها إلى جني فوائد مالية من جراء ذلك.

6-أنشطة الانترنت المجسدة لجرائم المحتوى الضار والتصرف غير القانوني:نصت مواد القسم السابع مكرر من قانون العقوبات وخاصة المادة 394 مكرر2/2 على تجريم أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق، وجميع الأفعال غير المشروعة، وقد نصت المواد على توقيع عقوبتي الحبس والغرامة إضافة إلى ما نصت عليه المادة 394 مكرر6[1] بتوقيع عقوبة تكميلية تتمثل في غلق المواقع(sites les)التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات[2].

أما الجزاءات المقررة بموجب الفصل السابع مكرر فتتمثل في العقوبات الأصلية وهي عقوبة الحبس والغرامة.

وعقوبات تكميلية بموجب نص المادة 394 مكرر 6 والمتمثلة في: مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع والمحل أو أما الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الانترنت الذي ترتكب فيه هذه الجرائم بشرط علم مالكه. وقد أورد المشرع ظروفا تشدد بها عقوبة الجريمة وهي: في حالة الدخول والبقاء

[1]:تنص المادة 394 من قانون العقوبات:"مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها"

[2]: أمال قارة، المرجع السابق، ص 80.

غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ونص أيضا بموجب المادة 394 مكرر5 على تجريم الاشتراك(سواء شخص طبيعي أو معنوي) في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية – بعقوبة الجريمة –وكان التحضير لهذه الجرائم مجسدا بفعل أو بعدة أفعال مادية. [1]

كما نصت المادة 394 مكرر[2]4 على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع مكرر بغرامة تعادل 05 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي. غير أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة. والشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها وهو ما نصت عليه المادة 394 مكرر[3]7 من قانون العقوبات.

إلى جانب قانون العقوبات التي جاءت نصوصه المستحدثة مجرمة لبعض الاعتداءات على المعلوماتية فإن المشرع الجزائري وبموجب الأمر05/03 المؤرخ في 19.07.2003المتعلق بحقوق المؤلف والحقوق المجاورة قد عمد إلى توفير الحماية لبرامج الحاسب الآلي وإخضاعها لقوانين الملكية الفكرية وأقر عقوبة الحبس والغرامة على كل من يعتدي على هذه المصنفات.[4]

---

[1] :كحولة محمد وأخرون، جرائم المعلوماتية، مذكرة ماجيستير، جامعة أبي بكر بلقايد، تلمسان، 2010، ص 69.

[2]: تنص المادة 394مكرر4من قانون العقوبات:"يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 5مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

[3]: تنص المادة 394مكرر7من قانون العقوبات:"يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

[4]: أمال قارة، المرجع السابق، ص20.

المطلب الثاني: خصائص وأسباب الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي، وقد كان لظهور شبكة المعلومات وتطورها إلى الصورة التي أصبحت عليها الآن فيما يعرف بالانترنت أثره في إعطاء شكل جديد للجريمة المعلوماتية ،ولعل أهم ما أضفته شبكة المعلومات على الجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود.

الفرع الأول: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الألي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدة سمات وحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي، وقد كان ظهور شبكة المعلومات وتطورها إلى الصورة التي أصبحت الآن عليها فيما يعرف بالأنترنت أثره في إعطاء شكل جديد للجريمة المعلوماتية.[1]

أولا:السمات الخاصة بالجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح،سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة.

[1] : كحولة محمد وأخرون، جرائم المعلوماتية، مذكرة ماجيستير، مرجع سبق ذكره، ص 75.

- **خصوصية الجريمة المعلوماتية:** تتسم الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها، ويرجع ذلك إلى عدة أسباب من بينها:

وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.[1]

- **الطبيعة المتعدية الحدود للجريمة المعلوماتية:**

يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة.[2]

فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة بينها ألاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في أن واحد، كما أن السرعة الهائلة التي يتم من

[1] : كحولة محمد وأخرون، جرائم المعلوماتية، مذكرة ماجيستير، مرجع سبق ذكره، ص 76.

[2]: نائلة عادل، محمد فريد قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005، ص 29.

خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة.[1].

ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية".

تعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي التنسيق بين قوانين الدول المختلفة لضمان تحقق "مبدأ ازدواجية التجريم" فيما يتعلق بجرائم المعلوماتية.[2]

ونجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم. وإن كان المشرع قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات.

والذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

[1]: نائلة عادل، محمد فريد قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية وتطبيقية، المرجع السابق، ص 30.

[2] : المرجع نفسه، ص 31.

ثانيا/ السمات الخاصة بالمجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين، وقد اختلف الباحثون في تحديد هذه السمات، ويعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة ، بالمجرم المعلوماتي بصفة خاصة. إلا أنه لا يخرج في النهاية عن كونه مرتكبالفعل إجرامي يتطلب توقيع العقاب عليه.[1]

فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه على درجة من العلم و المعرفة، وإن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي.[1]

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و يرمز إليها الأستاذ Parker بكلمة S.K.R.A.M و هي تعني :[1]

1. **المهارة:**

المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي ،والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين. إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، بل إن الواقع العملي قد

[1] :محمد خربط، مذكرات في قانون الاجراءات الجزائية الجزائري، دار هومة للنشر والطباعة، الطبعة 4، الجزائر، 2009، ص 47.

أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.[1]

2. المعرفة:

فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته. كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي. فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

3. الوسيلة:

فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها.

4. السلطة:

فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها. وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات، وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر. [2]

[1] : حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2005_2006. ص9

[2] : المرجع نفسه، ص 10.

5. الباعث:

وراء ارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية،ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الانتقام من رب العمل أو أحد الزملاء، حيث يفرق مرتكبي هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية لأخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم،

الفرع الثاني: دوافع الجريمة المعلوماتية

الدافع والقصد يشكل أحد الركائز في جميع الجرائم، وبالنسبة لجرائم الحاسب الآلي والإنترنت فهي لا تختلف في وضعها العام عن أسباب أي جريمة أخرى تقليدية.

فثمة دوافع عديدة تحرك العينات لارتكاب أفعال الاعتداء المختلفة المنضوية تحت هذا المفهوم، ويمكن تلخيص هذه الدوافع فيما يلي:

أولا: الدوافع الشخصية

يقصد بالدوافع الشخصية تلك العوامل اللصيقة بشخصية المجرم المعلوماتي، والتي تدفعه لارتكاب الجريمة المعلوماتية.[1]

أ/الدوافع المادية:

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، وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتبط

[1] :أحمد شوقي الشلقاني، مبادئ الاجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، طبعة 5، الجزائر، 2008، ص 59.

بالحاسوب الذي يتيح تعزيز هذا الدافع بما تحققه من ثراء فاحش، والدليل على 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 أي ما يعادل أكثر من 38 مرة[1].

وهناك فئة من مرتكبي الجرائم المعلوماتية يرجع ارتكابهم لها إلى الديون الناتجة من المشاكل العائلية والخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، فقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه الحالات، فالغاية تبرر الوسيلة[2]

ب/ الدوافع الذهنية أو النمطية:

تعتبر الدوافع الذهنية أو الدوافع النمطية تلك العوامل النفسية اللصيقة بالمجرم 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 تقنية دون أن يكون له نوايا أثمة.

ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم، وعليه فإنه يرى البعض "أن الدافع إلى ارتكاب الجرائم المعلوماتية يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح".

ثانيا: الدوافع الخارجية

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

[1]: Rose philippe la criminalité informatique que sais je 1er édition PU 1988 P 490

[2] : أحمد شوقي الشلقاني، المرجع السابق، ص 61.

المنفردة في حالات معينة، وهذه العوامل قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة مثلت قوة محركة لبعض العاملين لارتكاب جرائم المعلوماتية، باعثها الانتقام من المنشأة أو رب العمل.

أ/ دافع الانتقام و إلحاق الضرر برب العمل

قد يكون الانتقام مؤثرا في ارتكاب تلك الجرائم، ومثال 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]

ولقد 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 معنية، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة، مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من المنشأة أو رب العمل، وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيسي والغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة.

ب/ الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية

يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجادها وغالبا ما يجدون الوسيلة التي تحيطها، ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم المعلوماتية الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات لإظهار تفوقهم على الوسائل التقنية.

[1]:comment se protéger contre le crime informatique. temps réels P264-1984

إن هذا الدافع هو أكثر الدوافع التي يجري استغلالها قبل المنظمات الإجرامية (مجموعات الجريمة المنظمة) لأجل استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة.هذا وإن كان الفعل الواحد قد يعكس دوافع متعددة وخاصة، فمحرك أنشطة الإرهاب الالكتروني وحروب المعلومات دوافعه سياسية وإيديولوجية، في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، وقد تتداخل وتشترك هذه الدوافع في الفعل الواحد فتتمازج دون إمكانية التفرقة بينها.[1]

ج. طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية والأدبية:

يمكن أن يكون النظام المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية والأدبية، ومثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج نظام معلوماتي أخر، أو حالة تخزين واستخدام هذه المعلومات أو التفريط فيها دون إذن صاحبها، ذلك أن استخدام معلومة معينة دون إذن صاحبها يتضمن اعتداء على حق من الحقوق المعنوية، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية و يندرج ضمن الحقوق الفكرية، كذلك براءات الاختراع إذ تمثل فكرة للمخترع تحتوي على حق معنوي، وأخر مالي للمخترع.[2]

وقد نص المشرع الجزائري على حقوق الملكية الفكرية والأدبية وبراءات الاختراع من خلال عدة نصوص قانونية نذكر من بينها:

- المادة 38 من الدستور الجزائري:" حرية الابتكار الفكري والفني و العلمي مضمونة للمواطن

حقوق المؤلف يحميها القانون.

[1]: سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجيستير، جامعة الحاج لخضر، باتنة، 2013، ص 147.

[2] : المرجع نفسه، ص 148.

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام، إلا بمقتضى أمر قضائي".

د. **طائفة الجرائم المعلوماتية الواقعة على الحياة الخاصة :**

لقد كفلت جل الدول الحياة الخاصة لمواطنيها بالحماية، وقد حذا الدستور الجزائري حذو الدساتير الدولية بحرصه على حماية الحياة الخاصة للمواطنين، بموجب المادة 39 من الدستور الجزائري:" لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"

ولا شك أن الحاسبات الألية بما لها قدرة فائقة على تخزين أكبر كم ممكن من المعلومات، أصبحت مخزنا لأهم المعلومات وأكثرها حساسية المتعلقة بالأفراد، ولأهمية المعلومات التي تحتويها أنظمة الحسابات الألية أصبح لهذه الحسابات دورا هاما في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة.

ومنه يمكن أن يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد، كأن يقوم الشخص يعمل بإعداد ملف يحتوي على هذه المعلومات تخص شخص أخر بدون علمه أو اذنه، أو أن يجمع المعلومات بعلم الشخص المعني، ولكن يقوم المكلف بحفظها بالاطلاع الغير عليها بدون إذن صاحبها، أو أن يقوم شخص باختراق معلومات تتمثل في أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص أخر.[1]

[1] :صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجيستير، جامعة مولود معمري، تيزي وزو، 2013، ص 88.

المبحث الثاني: أركان الجريمة المعلوماتية

تعد الجرائم المعلوماتية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الأونة الأخيرة، وذلك بسبب الاستعمال السيئ للثورة التكنولوجية، مما دفع الكثير من الحكومات إلى إظهار اهتمام متزايد لمكافحة الجرم المعلوماتي وسد ثغرات الأنظمة المعلوماتية، والجريمة المعلوماتية كغيرها من الجرائم التقليدية تقوم على أركان وأساس قانوني سوف نتعرف عليه من خلال :

المطلب الأول: الركن المفترض

يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان جريمة من جرائم الاعتداء على هذا النظام.

ويؤدي توافر هذا الشرط إلى الانتقال للمرحلة التالية، إذ أن هذا الشرط يعتبر عنصرا لازما، ولذلك يكون من الضروري تعريف نظام المعالجة الآلية للمعطيات ومدى خضوع هذا النظام لحماية فنية.

الفرع الأول:تعريف نظام المعالجة الآلية للمعطيات

هو تعبير فنِّ ي تقني متطور، يخضع للتطورات السريعة والمتلاحقة في مجال الإعلام الآلي، ولذلك لم يعرف المشرع الجزائري على غرار المشرع الفرنسي نظام المعالجة الآلية للمعطيات، فأوكل بذلك مهمة تعريفه لكل من الفقه و القضاء.

حيث قدمت المادة الأولى من الاتّفاقية الدولية للإجرام المعلوماتي تعريفا للنّظام المعلوماتي على النحو التالي:[1]

[1] :صغير يوسف، الجريمة المرتكبة عبر الأنترنت، المرجع السابق، ص 93.

"يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتّصلة ببعضها البعض أو ذات صلة بذلك، ويقوم إحداهما أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات". ويقصد بـ "بيانات الكمبيوتر" أية عملية عرض للوقائع ،أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر، بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها".

ويكون نظام المعالجة الآلية للمعطيات في طور التّشغيل عند إرسال إشارة كهربائية نحو وحدة المعالجة المركزية، والتي تقوم بدورها بإرسال البرنامج المسئول عن تشغيل ذاكرة القراءة، هذه الأخيرة تقوم بالبحث عن المعطيات التي تسمح بتشغيل النِّظام المسئول عن البحث، ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة التي تقوم بمتابعة المراحل اللاّحقة .[1]

الفرع الثاني الحماية الفنية لأنظمة المعالجة الآلية للمعطيات

تكفل بعض القواعد الأمنية الحماية لنظم المعالجة الآلية للمعطيات، كوضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من الأجهزة المختلفة، والتي يمكن عن طريقها معرفة محتوى المعلومات التي يتم نقلها، ويتأتّى ذلك عن طريق حماية الكابلات والوصلات الكهربائية لارتباطها بالأجهزة، ومن بين هذه القواعد، أُسلوب يعتمد على توزيع العمليّات التي يقوم بها نظام المعالجة الآلية للمعطيات ونقلها إلى نظام احتياطي (مركز للمساعدة) عند الضرورة، ويلجأ إلى هذا الأسلوب عادة البنوك وشركات التّأمين، ويظلّ هذا الموقع سرا ويخضع لدرجة عالية من الحماية، ومن الأساليب المستعملة كذلك، الاعتماد على الاختبارات الفيزيولوجية للدخول إلى النِّظام عن طريق التحقّق من شخصية

[1]: عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2003، ص 187.

القائم بعملية الدخول عن طريق بصمة الأصبع أو نبرة الصوت أو شكل الأذن أو شبكية العين .[1]

لكن يبقى نظام التشفير لحماية المعلومات هو الأسلوب الواسع الانتشار، خاصة البيانات المتناقلة عبر الشبكات، كشبكات الإنترنت، لما تنطوي عليه من سرية البيانات الشخصية كالرسائل الإلكترونية وكذا البيانات الخاصة بالأعمال التجارية الرقمية.

ويقوم نظام التّشفير على تحويل المعلومات والبيانات إلى شكل رمزي غير مفهوم بدون مفتاح لحلِّ رموزه، يعرفه عادةً مرسل المعلومات والمرسل إليه، وفي داخل جهاز الكمبيوتر توجد أجهزة مهمتها التحقُّق من شخصية القائم بعملية الدخول عن طريق الشفرة .

فبالرجوع إلى نص المادة 394 مكرر[2] من قانون العقوبات، لا نجد إشارة إلى ضرورة خضوع النّظام للحماية الفنية حتى يتمتع بالحماية الجنائية، وكذلك الشأن بالنسبة للمادة 323-1 من قانون العقوبات الفرنسي، و يظهر من خلال الأعمال التّحضيرية لقانون 1988، المتعِّ لق بالمعلوماتية والمقتبسة منه المادة 323-1 ، أنه كان من المقترح ضرورة شمول النّص بهذا الشرط، ولكن اشتراط وجود حماية أمنية في نظام المعالجة الآلية للمعطيات لم يتم الاتّفاق عليه في المناقشات الأخيرة في البرلمان الفرنسي، ولذلك جاء النص خالياً من هذا الشرط، ووجد أن هذا الشّرط قد يؤدي إلى الحد من الحماية الجنائية للنظم غير المشمولة بتجهيزات أمنية داخل النظام.

[1]: خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، طبعة 1، الاسكندرية، 2009، ص 280.

[2]: تنص المادة394مكرر من قانون العقوبات:"يعاقب بالحبس والغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

ولذلك اكتفى المشرع الفرنسي في النَّص النِّهائي بأن يكون التوصل قد تم "بطريق الغش"، وهذا التَّعبير يترك تفسيره لقاضي الموضوع.[1]

وهذا ما فتح أبواب النِّقاش حول هذه النُّقطة من خلال ظهور رأيين مختلفين:

الرأي الأول: يقول بعدم جدارة الأنظمة التي لا تحميها نظم أمنية بالحماية الجنائية ،كون أنه من غير المعقول حماية معلومات هامة تركها المسئولون عنها دون أي إجراءا تتكفل لها الحماية.

ويقيس أنصار هذا الرأي جريمة الدخول غير المشروع في أنظمة المعالجة الآلية للمعطيات على جريمة انتهاك حرمة المنزل، حيث لا تقوم الجريمة لمجرد أن الدخول إلى المسكن قد تم بغير رضاء صاحبه، كترك مسكنه دون حماية بسبب عدم وجود أقفال أو أبواب أو نوافذ، فيجب أن يكون الدخول مصحوباً باستعمال وسائل تدلّ على عدم رضا صاحب المسكن.[2]

ويستند أنصار هذا الرأي إلى عدة أسباب تنصب جميعها في اتجاه واحد هو ضرورة أن يكون هناك نظم أمنية يتم اختراقها لامتداد الحماية الجزائية للمعلومات، وأول هذه الأسباب يتعلّق بالمادة 28 من القانون 78-17 لسنة 1978 الخاص بالمعلوماتية وحماية الحريات الفرنسي، حيث تتطلّب أن تكون الأنظمة مشمولة بتدابير أمنية لحمايتها ،والسبب الثاني يكمن في إقامة الدليل على قيام الركن المادي للجريمة وكذا التّحقُّ ق من توافر القصد الجنائي لدى مرتكبها، لأن اختراق الأنظمة الأمنيّة من طرف الفاعل يترك أثراً، و يؤكِّد طريق الغش والاحتيال الذي سلكه.

[1]: صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،2003 ، ص117.

[2] : عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، مرجع سبق ذكره، ص189.

الرأي الثاني: فهو يذهب إلى أنه ينبغي حماية أنظمة المعالجة الآلية للمعطيات جزائيا بغض النظر إن كانت تتمتع بحماية النظم الأمنية من عدمه، ويقيس أنصار هذا الاتِّجاه جريمة الدخول غير المشروع على جريمة السرقة، حيث أن تمتُّع المال المسروق بحماية صاحبه أو عدم تمتُّ عه بهذه الحماية لا يؤثّر في قيام جريمة السرقة، بغض النظر عن مقدار الصعوبة التي واجهت الجاني في تنفيذها، كما أن تطُّلب مثل هذا الشرط يضيق من تطبيق الحماية الجزائية، ويتجاهل الحالات التي يتم فيها الدخول إلى النّظام نتيجة خطأٍ قام به المبرمجون، أو المسئولون عن أمن النِّظام.

هذا الرأي هو الأقرب إلى الصواب استنادا إلى المبادئ العامة المستقرة في القانون الجنائي كحرفية النص، وعدم جواز تقييد النص المطلق أو تخصيص النّص العام، إلاّ إذا وجد نص يجيز ذلك، ولا يوجد في حالتنا نص خاص يقيد إطلاق النّص أو يخصص عمومه، وبالتالي يجب التزام حرفية النّص في التّفسير، فعدم ذكر المشرع لشرط الحماية الفنّية يعني أن المشرع أراد استبعاده.[1]

وأكدت محكمة استئناف باريس في حكم صادر لها في 1994/04/05 ،على أنه من غير الضروري لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية، وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسئول عن النظام.

المطلب الثاني الأركان الأساسية للجريمة المعلوماتية

متى ثبت توفر الشرط الأولي لقيام الجريمة المعلوماتية ألا وهو نظام المعالجة الآلية للمعطيات أمكن الانتقال إلى المرحلة التالية وهي البحث في توافر أركان أية جريمة من جرائم المعلوماتية.

[1]: صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، المرجع السابق، ص118.

الفرع الأول الركن المادي

يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات وهناك ثلاثة أشكال للاعتداء نذكرها فيما يأتي:

أولا/ الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

نصت عليه المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي بالإضافة للمادة 394مكرر من قانون العقوبات بقولها: "يعاقب بالحبس من ثلاثة أشهر إلى سنة بغرامة من 50.00دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.0000 دج إلى 150.000دج ."

وعليه فإن هذا الشكل من الاعتداء على نظام المعالجة الآلية للمعطيات يتكون من صورة بسيطة للجريمة وأخرى مشددة، فأما الصورة البسيطة تقوم بمجرد الدخول أو البقاء غير المشروع.

ويقصد **بفعل الدخول** ظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات وبالتالي لا نقصد بالدخول الدخول بمفهومه المادي[1].

[1]:علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، مصر، 1999، ص120.

وتجدر الملاحظة أن المشرع لم يحدد وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ومنه تقع الجريمة بأية وسيلة أو طريقة تمت بها الدخول، فيستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر.

كما أن هذه الجريمة تقع من كل إنسان أيا كانت صفته، وكفاءته المهنية والفنية، فهذه الجريمة ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة.

في حين أنه يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.[1]

وتجدر الإشارة إلى أنه قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام، وقد يجتمعان، ويكون البقاء معاقبا عليه وحده حين يكون الدخول إلى النظام مشروعا.

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، في الحالة التي لا يكون فيها للجاني الحق في الدخول إلى النظام، ويدخل إليه رغم ذلك ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق الاجتماع المادي للجريمتين الدخول والبقاء غير المشروعين. [2]

إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، فإنها تحقق أيضا، وبصورة غير مباشرة حماية المعطيات أو المعلومات.[3]

[1] : عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، مرجع سبق ذكره، ص192.

[2]: علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص121.

[3]: عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، مرجع سبق ذكره، ص193.

أما الصورة المشددة تتحقق بتوافر الظرف المشدد المتمثل في حصول نتيجة الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

وقد نصت المادة 394 مكرر 2+3من قانون العقوبات على أن " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150000 دج."

وعليه نستنتج من خلال ذلك أن هناك ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، وتربط بين هذين الظرفين علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع والنتيجة الضارة وإن لم تكن مقصودة.

ومنه فظرف التشديد يعتبر ظرف مادي يكفي أن توجد بينه وبين الجريمة الأساسية المتمثلة في الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره، إلا إذا أثبت الجاني انتفاء تلك العلاقة ويثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ.[1]

ثانيا/ الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات

نصت على هذا الشكل من الاعتداء المادتين الخامسة والثامنة من الاتفاقية الدولية للإجرام المعلوماتي، في حين أن المشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام، ويمكن رد ذلك لكون أن المشرع الجزائري قد اعتبر من خلال الفقرة ج من المادة الثانية من القانون 04/09 على أن برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية. [2]

[1]: صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، مرجع سبق ذكره، ص122.

[2]: تنص الفقرة ج من المادة الثانية من القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 07 لـ 2009.على ما يلي:"منظومة معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"

وقد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات والاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية، فإذا كان الاعتداء مجرد **وسيلة** فان الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء **غاية** فان الفعل يشكل جريمة الاعتداء العمدي على المعطيات.

وتشمل صورة الاعتداء العمدي على سير النظام فعلين يتمثلان في الآتي:

يتمثل **الأول** منها في فعل التعطيل، والذي يفترض وجود عمل إيجابي، مع العلم أن المشرع لم يشترط أن يتم التعطيل بوسيلة معينة فيستوي أن يتم التعطيل بوسيلة مادية ككسر الأجهزة المادية للنظام أو تحطيم أسطوانة أو عن طريق وسيلة معنوية تتم بموجب الاعتداء على الكيانات المنطقية للنظام كالبرامج والمعطيات وذلك بإتباع إحدى التقنيات المستعملة في هذا المجال مثل إدخال برنامج فيروسي، استخدام قنابل منطقية مؤقتة، جعل النظام يتباطأ في أدائه لوظائفه كما يستوي أن يقترن التعطيل بالعنف أم لا. [1]

أما الفعل **الثاني** يتمثل في **الإفساد** الذي يتم بكل فعل إلى تعطيل نظام المعالجة الآلية للمعطيات يؤدي إلى جعله غير صالح للاستعمال السليم وذلك من شأنه أن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[2].

ثالثا_ الاعتداءات العمدية على المعطيات

نصت عليها المواد 03،40،08، من الاتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع الجزائري في المادة394مكرر 1و 394مكرر 2من قانون العقوبات فجرم في المادة الأولى الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، وجرم في المادة الثانية المساس العمدي بالمعطيات الموجودة خارج النظام، ويظهر هذا فيما يلي:

[1]: أحسن بوسقيعة، التحقيق القضائي، دار هومة للطبعة للنشر والطباعة، طبعة 10، الجزائر، 2009، ص 124.

[2]: المرجع نفسه، ص 125.

أ_ جرائم الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي

باستقراء المادة**394مكرر1**[2]نجد أن لهذه الجريمة صورتين تتمثل الأولى في الاعتداءات العمدية على المعطيات الموجودة داخل النظام أما الصورة الثانية تتمثل في المساس العمدي بالمعطيات خارج النظام نجد الاعتداءات العمدية على المعطيات الموجودة داخل النظام تتجسد في إحدى الأفعال الثلاثة:

الإدخال (L'intrusion)، المحو(L'effacement)، التعديل(modification La) **الإدخالl'intrusion:** يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل ويتحقق هذا الفعل في الفرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه وكذلك الحامل الشرعي لبطاقة الائتمان والتي يسدد عن طريقها مبلغا (التاجر أو شخص يتعامل معه) أكثر من المبلغ المحدد له.[1]

وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب(فيروس–حصان طروادة – قنبلة معلوماتية زمنية)يضيف معطيات جديدة.

المحوl'effacement :يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

[1] : www.desoace-univ.dz تم زيارة الموقع بتاريخ 2021/03/22 على الساعة 23:45.

التعديل modification: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة gomme d'effacementأو برامج الفيروسات بصفة عامة، وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل.

مع الملاحظة أن المشرع لم يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يقوم الركن المادي، كما أن أفعال الإدخال والمحو والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل.

ب_ أما صورة المساس العمدي بالمعطيات خارج النظام نص عليها المشرع الجزائري بموجب أحكام المادة394مكرر2 من قانون العقوبات[1]، وكرس بموجبها المشرع الحماية الجزائية للمعطيات في حد ذاتها لأنه لم يشترط أن تكون المعلومات داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا.

إذ نصت الفقرة الأولى من المادة394مكرر 2أن محل الجريمة يتمثل في المعطيات سواء كانت مخزنة في أشرطة أو أقراص أو معالجة آليا أو مرسلة عن طريق منظومة معلوماتية ، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

[1]: تنص المادة 394مكرر2من بقانون العقوبات:" يعاقب بالحبس وبغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي:
–تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات محزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
ـحيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

في حين أن الفقرة الثانية من المادة394مكرر 2جرمت أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات فقد يكون الهدف من ذلك المنافسة غير المشروعة ،الجوسسة، الإرهاب، أو التحريض على الفسق ...الخ.[1]

الفرع الثاني الركن المعنوي

بعد التطرق للركن المادي لجرائم الاعتداء الماس بالأنظمة المعلوماتية بمختلف أشكاله، نتطرق فيما يأتي للركن المعنوي الذي يتخذ كل الأشكال السابق ذكرها صورة القد الجنائي و نية الغش.

ففي صورة الدخول والبقاء غير المشروع داخل نظام المعالجة الألية للمعطيات فإن كل م فعل الولوج والتجول والبقاء داخل نظام المعالجة الألية للمعطيات لا يجرمان إلا إذا تم عدما، وقد نصت المادة الثانية من الاتفاقية الدولية للجرائم المعلوماتية في هذا الصدد أنه يمكن السماح للدولة العضو أن تشترط لقيام هذه الجريمة مجرد خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله.[2]

وبالتالي يلزم توفر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو فعل البقاء مع علمه بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوفر الركن المعنوي إذا كان دخول الجاني أو بقائه داخل النظام مسموح به، أو مشرع أو إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في البقاء أو نطاق هذا الحق كأن يجهل وجود خطر من جراء الدخول أو البقاء أو كان يعتقد أنه مسموح له بالدخول، فإذا توفر القصد الجنائي بعنصريه العلم والإرادة لا يتأثر بالباعث على الدخول أو البقاء فيضل

[1] : أحسن بوسقيعة، الوجيز في القانون الجنائي العام، دار هومة للنشر والطباعة، طبعة أولى، الجزائر، 2010، ص 34.

[2] : المرجع نفسه، ص 35.

القصد قائما ، حتى ولو كان الباعث هو الفضول أو اثبات القدرة على المهارة والانتصار على النظام.

وبالنسبة للنية تبرز من خلال طريقة التي يتم بها الدخول عن طريق خرق جهاز الرقابي الذي يحمي النظام، أما بالنسبة للبقاء فإنها تستنتج من خلال العمليات التي تمت داخل النظام، أما جريمة الاعتداءات على سير النظام المعالجة الآلية للمعطيات فإنها تعد بطبيعتها جريمة عمدية، إذ أنه من المفترض أن أفعال العرقلة لا تكون إلا عمدية، وهذا ما يميزه عن الاعتداء غير عمدي لسير النظام الذي يشكل ظرفا مشددا للجريمة والدخول والبقاء غير المشروع داخل النظام.

وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة، ويظهر ذلك جليا من خلال الأفعال المشكلة لهذه الجريمة، حيث لا يتصور أن يقوم الفاعل بالاعتداء على سير النظام المعالجة الآلية للمعطيات بعرقلته أو تعطيله أو إفساده عن غير قصد.[1]

كما أن جريمة الاعتداءات العمدية على المعطيات تعد بدورها جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم ولإرادة، إذ يجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، ويعلم أن ليس له الحق في القيام بذلك، وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.

كما يشترط بالإضافة إلى القصد الجنائي العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير، بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل، مع العلم بذلك واتجاه إرادة الجاني إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.[2]

[1] :خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سبق ذكره، ص 57.

[2] : أحسن بوسقيعة، التحقيق القضائي، مرجع سبق ذكره، ص 65.

وأخيرا جريمة استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية التي تتم بالقيام بأحد الأفعال المنصوص عليها في المادة 394 مكرر 2 من قانون العقوبات المتمثلة إما في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الانجاز في معطيات مخزنة أو معالجة مرسلة عن طريق منظومة معلوماتية أو حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، فإنه لا يمكن أن يتم هذا الاستخدام بغير علم وإرادة الفاعل مما يجعله لا محالة عمديا، إلا أن المشرع اشترط أن يكون ذلك بطريق الغش، وبالتالي فإن المشرع الجزائري يشترط توافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش في هذه الصورة كذلك.[1]

[1] : خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سبق ذكره، ص 63.

الفصل الثاني

لم تكتف التشريعات الحديثة بحماية معطيات الحاسب الآلي بصفة عامة من خلال تجريم صور الاعتداء عليها أي حماية موضوعية، وإنما نظرا لخطورة الإجرام الالكتروني في حد ذاته لكون حل الجريمة مجموعة معطيات هي عبارة في الحقيقة عن ذبذبات الكترونية يسهل على الجاني القيام بعمل إجرامي عليها دون ترك أثار، ودون أن يستغرق هذا العمل وقتا طويلا، وهو ما جعلها صعبة الاكتشاف والإثبات، لدى ذلك إلى ظهور مشكلات إجرائية في هذا النطاق، حيث أن المحقق أو ضابط الشرطة القضائية أو القاضي نفسه في حيرة أمام هذه الجرائم نظرا لقصور التشريع الإجرائي خاصة، وأن هذه الجرائم الحديثة، ولا يمكن تطبيق النصوص التقليدية من جهة، وعدم القدرة الكافية والفنية لرجال القانون لاكتسابها.

لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الماسة بالمعطيات، ومنها لا يطبق إلا على الجريمة المعلوماتية خاصة في مرحلة الاستدلالات والتحقيق.

المبحث الأول: الجوانب الموضوعية في نصوص الجريمة المعلوماتية

وضع المشرع الجزائري كغيره من التشريعات بعض الإجراءات والقواعد والضوابط التي تستهدف متابعة مرتكبي الجرم المعلوماتي حماية لمعطيات الحاسب الآلي، خاصة في مرحلة جمع الاستدلالات، حيث أن أجهزة الشرطة تقوم بدور فعال ورئيس حال وقوع الجريمة لمعاينة مكانها وضبط أدلتها، والقبض على مرتكبيها والقيام بكل ما يفيد في كشف الحقيقة، وذلك بعد مساعدة أجهزة التحقيق للتوصل إلى حقيقة الواقعة، ومعرفة مرتكبيها.

المطلب الأول: الحماية الجزائية للجريمة المعلوماتية في ظل قانون العقوبات

لقد نص المشرع الجزائري في قانون العقوبات على المساس بأنظمة المعالجة الآلية أو ما يعرف بالغش المعلوماتي بموجب التعديل الذي تم بالنسبة لقانون العقوبات بالقانون رقم23/06المؤرخ في 12/20/ 2006 المتضمن قانون العقوبات الجزائري في قسمه السابع مكرر، والذي شمل المواد من394مكرر إلى394مكرر7،متتبعا في ذلك خطى التشريعات الغربية التي اتجهت في وقت متقدم إلى إصدار تلك النصوص المتعلقة بالجريمة المعلوماتية.

أن مهمة تقرير الحماية الجزائية للمعلوماتية مهمة صعبة يعترضها صعوبة منهجية مصدرها تشعب الجوانب التي تتعلق بالمعلوماتية، وكذا حداثة الموضوع واتسامه بطبيعة علمية بحتة تخرج من مجال تكوين رجال القانون.

الفرع الأول: جريمة المساس بأنظمة المعالجة الآلية للمعطيات

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي وهو الفعل المنصوص والمعاقب عليه في المواد [1] 394 مكرر إلى المادة394مكرر7ونجد أن المشرع الجزائري لم يعرف لنا نظام المعالجة الآلية للمعطيات، بالرجوع إلى الاتفاقية الدولية الخاصة بالإجرام المعلوماتي قدمت تعريفا للنظام المعلوماتي في مادتها الثانية[1].

وبالعودة إلى قانون العقوبات الجزائري، نجد أن الغش المعلوماتي يأخذ صورتين أساسيتان وهما:

- الدخول في منظومة معلوماتية
- المساس بمنظومة معلوماتية
- صور أخرى من الغش المعلوماتي.

أولا: الدخول في منظومة معلوماتية.

ويشمل فعلين هما: الدخول والبقاء.

1_جريمة الدخول غير المشروع

تنص المادة394مكرر من قانون العقوبات الجزائري والتي تقابلها المادة1/323 قانون عقوبات فرنسي على معاقبة كل من يدخل عن طريق الغش في كل جزء.

2_جريمة البقاء غير المشروع:

نص المشرع الجزائري على هذه الجريمة في المادة394مكرر من قانون العقوبات الجزائري ويقصد بالبقاء الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم أتاء

[1] : المواد394 مكرر إلى المادة394مكرر7 من قانون العقوبات المعدل والمتمم بالقانون09/01 المؤرخ في26 يونيو 2001.

إتاوة، وتقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل بعد،كما يجرم البقاء حتى ولو تم بصفة عرضية.[1]

ثانيا:المساس بمنظومة معلوماتية.

تنص المادة394 مكرر 1 قانون العقوبات الجزائري ن "كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".[2]

ثالثا:صور أخرى للغش المعلوماتي:

جاء نص المادة 394 مكرر 2من قانون العقوبات الجزائري بتجريم الأعمال التالية:

- 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 إحدى جرائم الغش المعلوماتي السالفة الذكر.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم الغش المعلوماتي.

كما نصت الماد 6 من اتفاقية بودابست على جريمة الاستخدام غير المشروع للمعطيات على معاقبة كل من يقوم عمدا بإنتاج أو استعمال أو استيراد أو توزيع برنامج حاسوب بغرض ارتكاب أو كلمة سر أو رمز وصول أو بيانات مماثلة بغرض ارتكاب الجرائم المنصوص عليها في المواد2 إلى5، ولا يشترط اجتماع تلك الجرائم بل يكفي توافر إحدى تلك الجرائم. [3]

---

[1]: أحسن بوسقيعة، الوجيز في القانون الجزائي،الطبعة6، دار هومة، الجزائر، ص445.

[2]: مرزوق نسيمة، جرائم الانترنت مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2006_2009، ص10.

[3]: قربوز حليمة ،الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مرجع سبق ذكره، ص 62.

الفرع الثاني: جريمة التزوير المعلوماتي

إن التعديل أو التغيير الذي يقع على المعطيات أو البرامج من شأنه أن يشكل جريمة تزوير والتي تقوم على تغيير الحقيقة بقصد الغش تغييرا يترتب عليه إلحاق الضرر بالغير، ويلاحظ أن المشرع الفرنسي بعد تعديل قانون العقوبات لسنة1988 وصدور قانون العقوبات لسنة1994 عدل المادة1/441لكي تستوعب بجانب التزوير العادي جريمة التزوير المعلوماتي، حيث نصت بعد تعديلها على :

"إن كل تغيير للحقيقة بطريق الغش ....في محرر مكتوب أو في أي دعامة أخرى تحتوي تعبير عن الفكر"، فالمشرع فصل بذلك بين التزوير في البيانات المسجلة في ذاكرة الكمبيوتر وبين التزوير في محررات نظام المعالجة الآلية للمعلومات، حيث أفرد نص خاص، للصورة الأولى بينما احتوى الصورة الثانية في النص العام لجريمة التزوير.[1]

وقد تناولت المادة7 من اتفاقية بودابست جريمة التزوير المتصلة بالحاسوب واعتبرت أن الواقعـــة تعتبر تزويرا إذا تضمنت خلق أو تعديل لبيانات أو برامج غير مرخص بإنشائها أو تعديلها، حـــيث تصبح لها قيمة مختلفة في الإثبات فيما يتعلق بالمعاملات القانونية التي تقوم على الثقة في المعلومات القائمة على تلك البيانات التي تعرضت للتزوير.

ونجد المشرع الجزائري لم ينص عن التزوير المعلوماتي لذلك سنتطرق إلى تحديد جريمة التزوير المعلوماتي(الفقرة الأولى) وموقف المشرع الجزائري من التزوير المعلوماتي(الفقرة الثانـــية).[2]

[1]: قربوز حليمة ،الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، المرجع السابق، ص63.

[2]:نهلة القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، 2009، ص 37.

أولا:تحديد جريمة التزوير المعلوماتي

إن موضوع التزوير هو المحرر، الذي لا بد من توافر شروط فيه، تتمثل في الكتابة من قبل شخص وأن ينتج أثاره القانونية هذه من الناحية التقليدية لجريمة التزوير، لكن في مجال المعلوماتية فالأمر يختلف فجريمة التزوير المعلوماتي تقع على المستندات المعلوماتية.

كما أن الغاية من تجريم أفعال التزوير هو حماية الثقة العامة، التي تنشأ من تعامل الأفراد بالمحررات بمفهومها التقليدي، ووضع نص خاص بالتزوير المعلوماتي يحقق الحماية للنظام المعلوماتي فقط دون الحفاظ على الثقة العامة، وبذلك فإن المحررات المعلوماتية تخرج من المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها، لذلك فإن إلغاء النص يخضع المحررات المعلوماتية إلى النصوص التقليدية الخاصة بالتزوير، بالمفهوم الجديد للمحررات. [1]

إن النشاط الإجرامي المكون لجريمة التزوير المعلوماتي يتمثل في فعل تغيير الحقيقة ويعني استبدالها بما يخالفها وإذا انتفى هذا التغيير انتفى التزوير. وإن تحوير البرنامج أو قواعد البيانات لا يعد تزويرا بل يقع تحت طائلة نصوص قانون حقوق المؤلف والحقوق المجاورة.[2]

ثانيا: موقف المشرع الجزائري من جريمة التزوير المعلوماتي

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، الذي يعتبر من اخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسوب الآن.

[1]: سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجيستير، جامعة الحاج لخضر، باتنة، 2013، ص 55.

[2]: نهلة القادر المومني، الجرائم المعلوماتية، مرجع سبق ذكره، ص 38.

ونجد أن المشرع الجزائري نص على التزوير الخاص بالمحررات في القسم الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد214الى229التي تشترط المحرر لتطبيق جريمة التزوير، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من اجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير. [1]

لقد كان من الأفضل لو أضاف المشرع الجزائري نصا خاصا بالتزوير المعلوماتي مثلما قام به المشرع الفرنسي، ونخلص في النهاية أن المشرع الجزائري رغم تداركه من خلال القانون رقم 23/06 الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة إلا أنه أغفل تجريم التزوير المعلوماتي، ولم يتبنى الاتجاه الذي انتهجته التشريعات الحديثة التي قامت بتوسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث ليشمل المستند المعلوماتي.

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

نظرا لنسبية الحماية من خلال النصوص التقليدية لجرائم الأموال نتيجة للطبيعة المميزة للمال المعلوماتي، ولما كانت الحاجة ملحة وضرورية لحماية برامج الحاسب الآلي في الوسط القانوني والتوجه الفعلي من قبل رجال القانون نحو وضع الأطر القانونية لهذه الحماية مما أدى إلى إثارة جدل حول الحماية المناسبة لبرامج الحاسب الآلي، فقد استقر الفقه القانوني مؤخرا في الدول التي ترعرعت فيها برامج الحاسب الآلي على إخضاعها لقوانين الملكية الفكرية والصناعية.[1]

[1] : سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سبق ذكره، ص57.

الفرع الأول: الحماية الجزائية لبرامج الحاسوب من خلال نصوص قانون الملكية الفكرية

يعتبر حق المؤلف من ابرز صور الملكية الفكرية وأهمها، لذلك قامت العديد من الدول سواء عبر تشريعات داخلية أو اتفاقيات دولية بإقرار حماية قانونية لحق المؤلف وسايرها المشرع الجزائري في ذلك والذي اصدر عدة قوانين لحماية حق المؤلف أحدثها الأمر رقم05/03الموافق ل19يوليو2003.[1]

أولا:الاعتداءات الواردة على برامج الكمبيوتر

حماية لحقوق المؤلف لم تخلو اغلب التشريعات الخاصة بحماية حق المؤلف من نصوص تجـــريم الاعتداء على حق المؤلف، ومن تلك التشريعات التشريع الجزائري الذي جرم الاعتداء على حقوق المؤلف بما فيها حقوق مؤلفي البرامج، وذلك في المواد155،154،151،من الأمر05/03 المتعلق بحقوق المؤلف والحقوق المجاورة، أما المشرع الفرنسي فنص عليها في المادة02/335 من الأمر657/01 المتعلق بحقوق المؤلف والحقوق المجاورة، أما المشرع المصري فنص عليها في نص المادة 47من القانون38/92.

وأما بالنسبة للاتفاقيات الدولية كاتفاقية برن لعام 1979 فإنها أقرت مبادئ وأسس تحكم الجانب الجزائي للمساس بحق المؤلف، ولم تجرم بصفة صريحة تصرفات معينة لتترك أمر تحديد جرائم الاعتداء على حقوق المؤلف إلى التشريعات الداخلية للدول.

ويلاحظ أن المشرع أدخل جميع جرائم الاعتداء على حقوق المؤلف بما فيهم مؤلفي البرامج تحت وصف جنحة التقليد وإن كان لا يصدق عليها جميعها ذلك الوصف.[2]

---

[1] : الأمر رقم05/03الموافق ل19يوليو2003 المتعلق بحماية حقوق المؤلف.

[2]: أسامة أمحمد المناعسة، جلال محمد الزغبي، جرائم الحاسب الآلي ، دار وائل للنشر،الأردن،2004،ص44.

ثانيا: الجزاءات المقررة لجرائم الاعتداء على برامج الكمبيوتر

لقد قرر المشرع الجزائري بموجب المواد:159،158،157،156،153من الأمر 05/03المتعلق بحقوق المؤلف والحقوق المجاورة الجزاءات المقررة على كل من يعتدي على حقوق المؤلف.

غير أن الشروع أو المحاولة الذي يمكن تصوره بالنسبة لهذه الجرائم غير معاقب عليه بنص خاص، لان العقوبة المقررة لهذه الجرائم عقوبة جنحة والقاعدة تقضي بأن لا يعاقب على الشروع في الجنح إلا بنص خاص. [1]

1_العقوبات الأصلية

حدد المشرع الجزائري في المادة153من الأمر 05/03 عقوبة تتمثل في الحبس من 3اشهر إلى3سنوات وغرامة من 000.500دج إلى000.000.1دج سواء كان النشر قد حصل في الجزائر أو خارجها.

2_ العقوبات التكميلية وتدابير الأمن

تتمثل العقوبات التكميلية في التشريع الجزائري في المصادرة ونشر الحكم حيث نص على المصادرة في المادة157من الأمر 05/03 التي نصت على انه تقرر الجهة القضائية المختصة مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي للمصنف ومصادرة العتاد المخصص لمباشرة النشاط أو المشروع والنسخ.

[1] : أسامة أمحمد المناعسة، جلال محمد الزغبي، جرائم الحاسب الآلي، المرجع السابق، ص45.

أما عن عقوبة نشر الحكم فنص عليها المشرع الجزائري في المادة158من الأمر رقم05/03 والتي تقضي أنه يمكن للجهة القاضية المختصة بطلب من الطرف المدني، أن تأمر بنشر أحكام الإدانة كاملة أو مجزئة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها ومن ضمن ذلك على باب المسكن الخاص بالمحكوم عليه وكل مؤسسة أو قاعة حفلات يملكها على أن يكون ذلك على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها.

ويقصد بهذه العقوبة التشهير بالمحكوم عليه والتأثير على شخصيته الأدبية والمالية، وهي بذلك عقوبة ماسة بشرف الاعتبار.[1]

الفرع الثاني: الحماية الجزائية لبرامج الحاسوب في ظل نصوص الملكية الصناعية

إن قانون الملكية الفكرية يشمل عدة مجالات منها: العلامات التجارية براءة الاختراع، الرسوم والنماذج، تسمية المنشأ، وما يهمنا بصدد حماية برامج الكمبيوتر هو حمايتها من خلال براءة الاختراع. [2]

أولا: الشروط الواجب توافرها في براءة الاختراع

بصدور الأمر 07/03 المؤرخ في: 2003/07/19[3] المتضمن براءة الاختراع وبالعودة إلى نصوصه نجد المادة الثانية منه عرفت الاختراع بأنه:»فكرة المخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية«، وبشأن الشروط الواجب توافرها في الاختراع كي تطبق عليه أحكام المادة الثالثة من ذات الأمر التي تنص على ما يلي:

[1] : أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سبق ذكره، ص75.

[2] :سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في الحقوق، قانون جنائي، جامعة محمد خيضر، بسكرة، 2013، ص 51.

[3] : الأمر 07/03 المؤرخ في: 2003/07/19 المتضمن براءة الاختراع.

"يمكن إن تقع تحت براءة الاختراع الجديدة الناتجة عن نشاط الاختراعي والقابلة للتطبيق صناعيا"

ثانيا/مدى تطبيق نصوص براءة الاختراع على برامج الكمبيوتر.

حسبما يراه المختصون في الميدان فأنه من الصعب توفير حماية ناجحة للبرمجيات بالرجوع إلى قانون الملكية الصناعية، ويتعلق الأمر خاصة بشرطين لابد من توفرهما في العمل الإبداعي لكي يظفر صاحبه بالبراءة:

- ✓ *الجدية.
- ✓ القابلية لاستغلال الصناعي.[1]

المبحث الثاني: الجوانب الإجرائية في نصوص الجريمة المعلوماتية

إضافة إلى الجوانب الموضوعية التي تمت دراستها في المبحث الأول نخصص المبحث الثاني للجوانب الإجرائية في نصوص الجريمة المعلوماتية حيث يأتي المطلب الأول بعنوان قواعد الاختصاص المحلي وإجراءات التحقيق الابتدائي أما المطلب الثاني جاء بعنوان المكافحة الإجرائية في القانون الجزائري.

المطلب الأول: قواعد الاختصاص المحلي وإجراءات التحقيق الابتدائي

إن الطبيعة الخاصة للجرائم المعلوماتية لابد أن تنعكس على قانون الإجراءات الجزائية، فيلزم على المجتمع المعلوماتي في مجال قانون الإجراءات الجزائية أن تنشأ قواعد إجرائية حديثة إلى جانب القواعد الموضوعية، كانت هذه الجرائم المعلوماتية تتميز بصعوبة اكتشافها وإثباتها وتحتاج إلى خبرة فنية عالية للتعامل معها.[2]

[1] : سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مرجع سبق ذكره، ص 52.

[2] : المرجع نفسه، ص 52.

فإن ذلك أثار العديد من المشكلات العملية الإجرائية التي جعلت القواعد الإجرائية التقليدية قاصرة عن مواجهة تلك المشاكل، ولهذا اتجهت بعض التشريعات كالتشريع الانجليزي والأمريكي والجزائري إلى تعديل بعض قواعدها الإجرائية لجعلها قادرة على مواجهة تلك المشاكل الإجرائية كتلك المتعلقة بالاختصاص المحلي، وإجراءات التحقيق الابتدائي خاصة التي تهدف إلى جمع الأدلة. [1]

الفرع الأول:قواعد الاختصاص المحلي

عالج المشرع الاختصاص المحلي للجهات القضائية وذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه،وقد اعتمد على عناصر معينة تربط بين اختصاص الجهات القضائية بالنظر في الخصومة الجزائية، وهذا المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه، لكن لما كانت الجريمة المعلوماتية جرائم عابرة للإقليم، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه، لهذا فان المشرع الجزائري أجرى بعض التعديلات المتعلقة بالاختصاص المحلي في الجريمة المعلوماتية بموجب القانون 22/06المؤرخ في20ديسمبر2006المعدل والمتمم للأمر رقم155/66الموافق ل 08يونيو1966والمتضمن قانون الإجراءات الجزائية، لهذا سنتطرق لتلك القواعد على النحو التالي:[2]

[1] : صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة تخرج لنيل شهادة الماجيستير في القانون، جامعة مولود معمري، تيزي وزو، 2013، ص 83.

[2] : القانون 22/06المؤرخ في20ديسمبر2006المعدل والمتمم للأمر رقم155/66الموافق ل 08يونيو1966والمتضمن قانون الإجراءات الجزائية.

أولا/الاختصاص المحلي للنيابة العامة

يتحدد الاختصاص المحلي للنيابة العامة وفقا للمادة37من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة ومحل إقامة احد الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي في دائرته القبض على هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر. [1]

ويتعين على ضابط الشرطة القضائية طبقا للمادة40مكرر1من قانون الإجراءات الجزائية الجزائري[2] أن يبلغوا وكيل الجمهورية لدى المحكمة الكائن لها الجريمة بأصل ونسختين من إجراءات البحث ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة.

والذي يطالب طبقا للمادة40مكرر2من هذا القانون بالإجراءات فورا إذ اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة40مكرر من هذا القانون.

ثانيا:الاختصاص المحلي لقاضي التحقيق ومحاكم الجنح

1_الاختصاص المحلي لقاضي التحقيق

يقصد بالاختصاص المحلي لقاضي التحقيق المجال الذي يباشر فيه قاضي التحقيق، ويتحدد الاختصاص المحلي لقاضي التحقيق طبقا للمادة40 من قانون الإجراءات الجزائية لمكان وقوع الجريمة أو محل إقامة احد هؤلاء الأشخاص المشتبه في مساهمتهم في اقترافها أو محل القبض على احد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب أخر.

---

[1] : المادة 40 مكرر من القانون 22/06المؤرخ في20ديسمبر2006المعدل والمتمم للأمر رقم155/66الموافق ل 08يونيو1966والمتضمن قانون الإجراءات الجزائية.

[2]: تنص المادة 40مكرر1 من قانون الإجراءات الجزائية الجزائري على ما يلي:"يخبر ضباط الشرطة القضائية فورا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويبلغونه بأصل وبنسختين من إجراءات التحقيق ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة"

إلا أن المشرع ألغى في التعديل الجديد الفقرة2و3من المادة40، وأصبحت تنص الفقرة2 على انه:" يجوز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات".[1]

2_ الاختصاص المحلي لمحاكم الجنح.

يتحدد الاختصاص المحلي لمحاكم الجنح طبقا للمادة329من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة، أو بمحل إقامة احد الأشخاص المتهمين، أو شركائهم، أو بالمكان الذي تم في دائرته القبض على احد هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر، غير أن المشرع في التعديل الصادر بموجب القانون 14/04أضاف فقرة أخرى أجاز فيها في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم.[1]

الفرع الثاني:إجراءات التحقيق الابتدائي

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشان واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لذلك، والتحقيق مرحلة لاحقة لإجراءات جمع الاستدلال وتسبق مرحلة المحاكمة التي تقوم بها جهة الحكم، وعليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة. [2]

[1] :خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، الطبعة الأولى، دار الهدى، عين ميلة، 2010، ص 55.

[2] : المرجع نفسه، نفس الصفحة.

يهدف التحقيق الابتدائي إلى الكشف عن الحقيقة للوصول إلى هذا الغرض يلجا المحقق إلى مجموعة إجراءات بعضها يهدف للحصول على الدليل، وتسمى إجراءات جمع الدليل كالتفتيش والضبط والمعاينة والشهادة والخبرة، وبعضها الأخر يمهد للدليل ويؤدي إليه وتعرف بالإجراءات الاحتياطية ضد المتهم كالقبض والحبس المؤقت.[1]

أولا:التفتيش في مجال الجريمة المعلوماتية

لقد تعددت التعريفات التي أضافها الفقه على التفتيش، إلى أنها تجتمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل وذلك من اجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات القانونية المقررة، وقد أحاط القانون التفتيش بضمانات عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة. وإذا كان التفتيش للأشياء المادية بما فيها المكونات المادية للحاسوب لا يثير إشكالية، فما مدى خضوع البرامج والمعلومات.

1_مدى قابلية نظم الحاسوب للتفتيش:

يتكون الحاسوب من مكونات مادية ومكونات معنوية، ولا تثار أدنى صعوبة إذا كان محل جرائم الحاسوب الآلي مكونات مادية حيث ينطبق بصددها القواعد التقليدية دون صعوبة، فالواقع أن ولوج المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية قد وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وأنه يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو من الأماكن العامة أو الأماكن الخاصة إذ أن لصفة المكان أهمية خاصة في مجال التفتيش. [2]

[1]: رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، مستغانم 2012، ص 109.

[2]: المرجع نفسه، ص 110.

أما إذا كان محل جرائم الحاسوب الآلي مكونات غير مادية أي معنوية، كبرامج الحاسوب أو بياناته فقد ثار خلاف كبير في الفقه بين مؤيد ومعارض، حيث يذهب رأيانه إذا كانت الغاية من التفتيش هو جمع الأدلة المادية التي تفيد في كشف الحقيقة فإنهذا المفهوم يمتد ليشمل البرامج والبيانات.[1]

كما قرر المشرع الجزائري بموجب المادة45 من القانون رقم 22/06المؤرخ في 20ديسمبر 2006، التفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقرر له بعض الضوابط والقواعد سنراها لاحقا.[2]

زيادة على ذلك فإن المشرع في بعض الدول الأخرى لجأ إلى تقرير بعض القواعد القانونية بغية التغلب على الصعوبات التي قد تثار عند تفتيش الأنظمة المعلوماتية، وشاركه في ذلك الفقه، ومن تلك التشريعات التشريع الهولندي الذي أجاز في المادة25/أ منه للقائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق بذلك من قاضي التحقيق وهذا لتذليل الصعوبة الخاصة بوجود النهاية الطرفية للنظام المعلوماتي في منزل أخر غير منزل المتهم، كما أجاز بموجب المادة25منه إلزام غير المتهم كالشاهد والشخص القائم بالتشغيل القائم بتقديم كافة البيانات والمعلومات اللازمة لدخول نظام الحاسب الآلي والتعامل مع سلطة التحقيق في هذا الصدد، وأيضا اتجه المشرع الجزائري بموجب القانون السالف الذكر إلى وضع ضوابط للتفتيش في الجرائم المعلوماتية.[3]

[1]: المادة45 من القانون رقم 22/06المؤرخ في 20ديسمبر 2006، المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية.

[2]:أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الأولى، دار هومة للنشر والتوزيع، الجزائر، 2009، ص 114.

[3]: أحمد خليفة المط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، 2006، ص 66.

2_ ضوابط تفتيش نظم الحاسب الآلي

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات، بيد أن تحقيق تلك الغاية لا يكون بأي ثمن، ففي كل الحالات فإن الغاية لا تبرر الوسيلة، فالبحث عن الحقيقة القضائية لا ينبغي أن يكون طليقا من كل قيد، بل إن ذلك يخضع لضوابط معينة، ومن هذا المنطلق يجب أن يخضع التفتيش لضوابط يمكن تقسيمها إلى ضوابط موضوعية وضوابط شكلية:[1]

أ: الضوابط الموضوعية

تنحصر هذه الضوابط فيما يلي:

1/وقوع جريمة معلوماتية:والجريمة المعلوماتية هي كما سبق القول كل فعل غير مشروع يكون الحاسوب الآلي وسيلته أو محله وذلك لتحقيق أغراض غير مشروعة، وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا التي أصدرت قانون إساءة استخدام الكمبيوتر في 29يونيو1990، وفي فرنسا صدر قانون رقم19/88في 5يناير1988 وهو خاص بالغش المعلوماتي الذي تم تعديله مع صدور القانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من أول مارس 1994.[2]

[1] : علي عدنان الفيل، الإجرام الالكتروني، دراسة مقارنة، منشورات زين الحقوقية، الطبعة الأولى، 2011.

[2] : محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009، ص 90.

2/اتهام شخص أو أشخاص معينين بارتكاب الجريمة المعلوماتية أو المشاركة فيها:

فينبغي أن يتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية، سواء بصفته فاعلا أو شريكا، بحيث أنه إذا لم تتوافر هذه الدلائل كان على قاضي التحقيق أن يصدر أمر بأن لا وجه للمتابعة، وهذا ما تؤكده المادة 163من قانون الإجراءات الجزائية الجزائري[1]

وفي مجال المعلوماتية يمكن القول أن تعبير الدلائل الكافية يقصد به مجموعة المظاهر والدلائل التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش والتي تنسب الجريمة المعلوماتية إلى شخص معين سواء بصفته فاعلا أو شريكا.[2]

3/توافر قرائن على وجود أشياء لدى المتهم المعلوماتي أو غيره تفيد في كشف الحقيقة: فلا يكفي مجرد وقوع جناية أو جنحة بل يجب أن تتوافر قرائن قوية على وجود أشياء تفيد كشف الحقيقة،ويستوي أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله.

وهكذا فإن التفتيش لا يجري إلا إذا توافرت لذا المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء المتحصلة منها أو أية أشياء أخرى أو مستندات الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره.[3]

---

[1]: تنص المادة 163 من قانون الإجراءات الجزائية الجزائري على ما يلي:"إذا رأى قاضي التحقيق أن الوقائع لا تكون جنحة أو جناية أو مخالفة أو أنه لا توجد دلائل كافية ضد المتهم أو أن مقترف الجريمة ما يزال مجهولا، أصدر أمر بألا وجه لمتابعة المتهم.

[2]: خثير مسعود، الحماية الجزائية لبرامج الكمبيوتر، مرجع سبق ذكره، ص 69.

[3]: المرجع نفسه، ص 70.

4/إجراء التفتيش لنظم الحاسوب الآلي من قبل سلطة مختصة بالتحقيق:

يجب أن يقوم بتفتيش نظم الحاسوب الآلي سلطة مختصة بالتحقيق، وقد جعل المشرع المصري الاختصاص بالتفتيش كإجراء التحقيق في الجرائم التقليدية للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة وذلك على خلاف التشريع الفرنسي والجزائري الذين أناطا الاختصاص الأصيل بقاضي التحقيق، أما النيابة العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس، أما انجلترا فإن معظم الإجراءات الجنائية منوطة بالشرطة القضائية ما عدا بعض الجرائم التي تناط بالمدعي العام.[1]

ب/الضوابط الشكلية

بالإضافة إلى الضمانات الموضوعية لتفتيش نظم الحاسب الآلي، توجد ضمانات شكلية يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريات الفردية من التعسف أو الانحراف من استخدام السلطة وهي كالتالي:[2]

1/الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش الخاص بنظم الحاسوب الآلي:

والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط، وقد استوجب المشرع الجزائري في المادة 1/45أن يتم التفتيش في حضور صاحب المسكن الذي يجري فيه التفتيش وكذلك المشرع الفرنسي استوجب في الفقرة الأولى من المادة57من قانون الإجراءات الجنائية حضور صاحب المسكن الذي يجري فيه التفتيش وعدم حضوره يترتب عليه البطلان للتفتيش.[3]

---

[1]: علي محمد حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديثة، الطبعة الأولى، 2004، ص 33.

[2]: المرجع نفسه، ص 34.

[3]:عبد الماجد العكايلة، الوجيز في الضبطية القضائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2010، ص 44.

غير أن المشرع الجزائري بموجب المادة45من القانون رقم22/06المؤرخ في 20 ديسمبر2006استثنى إجراء الحضور لبعض الأشخاص، إذا تعلق الأمر بالتفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكنه اوجب الحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات، لكن إذا تعلق التفتيش بمسكن موقوف صاحبه للنظر أو محبوس في مكان أخر أوجب المشرع بموجب المادة 47 حضور شاهدين مسخرين أو بحضور ممثل يعينه صاحب المسكن محل التفتيش.[1]

2/محضر تفتيش نظم الحاسب الآلي :

فإن التفتيش من أعمال التحقيق فينبغي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سواء ما تستوجبه القواعد العامة في المحاضر عموما والتي تقضي بأن يكون المحضر مكتوب باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها.[2]

3/الميقات الزمني لإجراء تفتيش نظم الحاسوب الآلي:

حرصا على عدم التضييق من نطاق الاعتداء على الحرية الفردية وحرمة المسكن حرصت التشريعات الإجرائية على حضر القيام بتفتيش المنازل وما في حكمها في وقت معين، فالقانون الفرنسي ينص في المادة 59 من قانون الإجراءات الجزائية على أن التفتيش لا يمكن أن يبدأ قبل الساعة السادسة صباحا وبعد التاسعة مساءا، ولقد أخذت بعض التشريعات العربية بمبدأ عدم جواز تفتيش المنازل ليلا كقانون التونسي والجزائري،

[1]: المادة47 من القانون رقم22/06المؤرخ في 20 ديسمبر2006.

[2]: مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009، ص 11.

أما بالنسبة لتشريعات الدول الانجلسكسونية كالقانون الانجليزي والأمريكي فإنها لا تقيد التفتيش بوقت معين.[1]

لكن المشرع الجزائري بموجب المادة47 من قانون الإجراءات الجزائية الجزائري قرر إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات الليل والنهار أو الليل وفي كل محل سكني وغير سكني، بناء على إذن مسبق من وكيل الجمهورية المختص، إلا أنه أوجب الحفاظ على السر المهني.

4/أن يتم التفتيش بناءا على إذن مكتوب:إذا نصت المادة 44 من قانون

الإجراءات الجزائية الجزائري على ضرورة أن يكون التفتيش بناءا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا إذن قبل الدخول إلى المكان والشروع في تفتيش نظم الحاسوب الآلي.

إن التفتيش لنظم الحاسوب الآلي يتطلب مذكرة قضائية تجيز تفتيش أنظمة الكمبيوتر، فإجراء التفتيش دون تلك المذكرة مسالة تثير الكثير من المعارضة خاصة في ظل ما يتقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد.[2]

ثانيا:الضبط في مجال الجريمة المعلوماتية

منح المشرع في المادة 63[3]صلاحية القيام بالتحقيقات الابتدائية لأعوان الضبطية القضائية بشرط أن تكون تحت رقابة ضباط الشرطة القضائية.

---

[1]: مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص12.

[2] :ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة ماستر في القانون، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أمن البواقي، 2016، ص 47.

[3]: تنص المادة 63 من قانون الإجراءات الجزائية الجزائري على ما يلي:"يقوم ضباط الشرطة القضائية وتحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الابتدائية بمجرد علمهم بوقوع الجريمة إما بناء على تعليمات وكيل الجمهورية وإما من تلقاء نفسه"

1_ فيما يخص التوقيف للنظر.

إن التحقيق الابتدائي في الجرائم الخطيرة المذكورة في المادة16 من قانون الإجراءات الجزائية أصبح عسيرا وصعبا، خاصة وأن مرتكبي هذه الجرائم أصبحوا يستعملون أساليب متعددة، وحديثة و معقدة.

وأصبحت مدة الوضع تحت النظر لا تتماشى ومتطلبات التحقيق الأولي، مما جعل المشرع الجزائري يعدلها بالمادة51 والتي نصت على أنه:[1]

"يمكن تمديد أجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص:

–مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعـــــطيات".

2_ استعمال القوة لإحضار الأشخاص.

جاء بالمادة 65الفقرة1[2] أنه يجوز لضباط الشرطة القضائية بعد الحصول على إذن مسبق من وكيل الجمهورية المختص أن يستخدم القوة العمومية لإحضار الأشخاص الذين لم يستجيبوا لاستدعاء للمثول.

وإذا كانت الجرائم الواقعة على المكونات المادية للحاسوب الآلي لا يثير صعوبة للتقرير بصلاحية هذه الجرائم لضبط أدلتها، ذلك أن الضبط لا يرد بحسب الأصل إلا على أشياء مادية، إلا أن الأمر بالنسبة للجرائم الواقعة على المكونات المعنوية للحاسوب الآلي، يثير مشاكل بالنسبة لضبط أدلتها. وقد اختلف الفقهاء بين مؤيد ومعارض.[3]

---

[1] : المادة 51 1من قانون الإجراءات الجزائية الجزائري.

[2]: تنص الماد 1/65من قانون الإجراءات الجزائية الجزائري على ما يلي:"إذا دعت مقتضيات التحقيق الابتدائي ضابط الشرطة القضائية إلى أن يوقف للنظر شخصا مدة تزيد عن 48 ساعة فإنه يتعين عليه أن يقدم ذلك الشخص قبل انقضاء هذا الأجل إلى وكيل الجمهورية"

[3]: ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مرجع سبق ذكره، ص49.

ونجد المشرع الجزائري قد أجاز بموجب المادة 47الضبط أو الحجز في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في محل سكني أو غير سكني، وفي ساعة من ساعات النهار أو الليل بإذن مسبق من وكيل الجمهورية.

المطلب الثاني: المكافحة الإجرائية في القانون الجزائري

اقتدى المشرع الجزائري بالمشرعين الذين سبقوه، فسارع لمواكبة هذا التطور الذي لحق الجريمة بمكافحتها من الناحية الإجرائية وذلك بتعديل بعض المواد في قانون الإجراءات الجزائية وإصدار قوانين خاصة وجديدة في مجال الإجراءات.

الفرع الأول:المكافحة الإجرائية في القانون 04/09

نظم المشرع الجزائري في القانون رقم 04/09 المؤرخ في 05أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أحكاما جديدة وخاصة بمعالجة الجريمة المعلوماتية تتماشى والتطور الذي لحق بهذه الجريمة، من هذه القواعد ما نص عليه في المادة الثالثة منه التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات القضائية من ترتيبات تقنية،[1]الهدف منها هو:

- مراقبة الاتصالات الإلكترونية وتجميعها، حيث نجد أن المشرع الجزائري قد تبنى هذا الإجراء رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها بنص المادة 39 من الدستور الجزائري نظرا لخطورة بعض الجرائم المعلوماتية المحددة حصرا.[2]
- تسجيل الاتصالات الإلكترونية في حينها.

[1]: القانون 04/09 المؤرخ في 05أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[2] : المادة 39 من دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1966.

- القيام بإجراءات التفتيش والحجز للمنظومة المعلوماتية.

كما يبين القانون 04/09 في مادته الرابعة الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية وذلك على سبيل الحصر وهذه الحالات هي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الالكترونية.[1]

[1] : سوير سفيان، جرائم المعلوماتية، مذكرة ماجيستير في العلوم الجنائية وعلم الإجرام، جامعة أبي بكر بلقياد، تلمسان، 2010، ص 78.

• في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة تنص المادة16 من القانون 04/09 على إمكانية تبادل المساعدات القضائية على المستوى الدولي لنجاح عمليات التحقيق والتحريات لمكافحة الجرائم المعلوماتية.

كما أن المادة18 من القانون04/09 قد بينت الحالات التي لا تجوز فيها عملية المساعدة القضائية الدولية وحددتها بالحالات التالية:

- إذا كان فيها مساس بالسيادة الوطنية.
- إذا كان فيها مساس بالنظام العام. [1]

أما المادة الخامسة من القانون 04/09 [2] فهي تبين إجراءات التفتيش للمنظومة المعلوماتية يقصد بالتفتيش في مجال الجرائم المعلوماتية هو التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وان اختلف مضمونه عن التفتيش العادي بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة45 من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

غير أن القانون 04/09 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات التي يحتوي عليه هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها.[1]

[1] : المادة 18 من القانون 04/09 المؤرخ في 05أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[2] : المادة 05 من القانون 04/09 المؤرخ في 05أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

كما نص المشرع الجزائري في الفقرة الأخيرة من المادة الخامسة من القانون04/09 على إجراء أخر يسهل عملية التفتيش وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسبات لإجراء عمليات التفتيش على المنظومة المعلوماتية، وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات.

كما ألزمت المادة العاشرة من القانون04/09 [1] مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش وحفظ المعلومات طبقا للمادة 11 من نفس القانون التي من شأنها تمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب في المادة 12 على مقدمي الخدمات التزامات خاصة هي: [2]

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.
- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجودها.

[1]: المادة 10 من القانون 04/09 المؤرخ في 05أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[2]: المادة 12 من القانون 04/09 المؤرخ في 05أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الفرع الثاني: المكافحة الإجرائية في قانون الإجراءات الجزائية

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث أنه بتعديلي 09/01 و14/04 وضع قواعد وأحكام خاصة لسلطة المتابعة والاختصاص، الغرض منها هو مواجهتها، وهذه الأحكام هي:

- **جواز تمديد الاختصاص المحلي للمحكمة:** حيث نصت المادة 329من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

- **توسيع مجال اختصاص النيابة العامة:** حيث أنه بموجب المادة 37من قانون الإجراءات الجزائية تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها من قبل حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

- **العمل بنظام المشروعية في تحريك الدعوى العمومية:** حيث سحب نظام

الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، حيث يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في

[1] :أحسن بوسقيعة، الوجيز في القانون الجزائي العام، مرجع سبق ذكره، ص 100.

المواد144 مكرر ،144مكرر 1و2 من قانون العقوبات المعدل والمتمم بالقانون09/01 المؤرخ في26 يونيو 2001. [1]

• إضافة لما سبق ودائما في إطار المكافحة الإجرائية للجرائم المعلوماتية تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور حسب نص المادة 65 مكرر5 في إطار تعديل قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في 2006/12/20.[2]

• **التسرب:** إضافة لما سبق تجدر الإشارة إلى الإجراء الجديد الخاص بمكافحة الجرائم المعلوماتية والمنصوص عليه في المادة 65 مكرر11 من قانون الإجراءات الجزائية، وهو إجراء التسرب فتنص المادة 65 مكرر11 على أنه"عندما تنقضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر5، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد 65 مكرر12 و65مكرر18من قانون الإجراءات الجزائية.

[1]: قانون العقوبات المعدل والمتمم بالقانون09/01 المؤرخ في26 يونيو 2001.

[2]: قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في 2006/12/20.

وقد عرفت المادة 65مكرر12 التسرب على أنه "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة، بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"

كما سمحت الفقرة الثانية من المادة 65مكرر12 أن يستعمل لغرض إجراء التسرب هوية مستعارة أو أن يرتكب عند الضرورة الأفعال المنصوص عليها في المادة 65مكرر14 وهذه الأفعال هي:[1]

- اقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع ا لقانوني أو المالي وكذا وسائل النقل أو النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

ويمكن للمتسرب بإتيان هذه الأفعال دون أن تترتب عليه المسؤولية الجزائية لأنه مرخص له بهذه الأفعال بهدف الوصول إلى مرتكبي الجريمة.[2]

وقد بينت المادة 65مكرر15 الشروط الواجب توفرها في الإذن بالتسرب، وهي أن يكون مكتوبا ومسببا وأن يذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء ،وهوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته.

كما يجب أن يحدد في الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر كما أجازت المادة 65مكرر15 كإجراء جديد في مكافحة الجريمة المعلوماتية اعتبار ضابط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته كشاهد عن العملية في إجراءات التحقيق فيها.[3]

---

[1]: المادة 65مكرر15 من قانون العقوبات المعدل والمتمم بالقانون09/01 المؤرخ في26 يونيو.

[2]: سوير سفيان، جرائم المعلوماتية، مرجع سبق ذكره، ص 111.

[3]:أحسن بوسقيعة، الوجيز في القانون الجزائي العام، مرجع سبق ذكره، ص 109.

الخـــاتمة

لقد أضحى العالم اليوم يعيش في زمن التطور لتكنولوجي أو ما يعرف بالثورة المعلوماتية، حيث أصبحت حياتنا اليومية تستدعي اللجوء إليها، فقد مكنت طرق المعالجة الآلية للمعطيات المجتمعات من تجاوز فكرة الحدود الإقليمية،نظرا لكون التكنولوجيا أو العزيمة هي عبارة للحدود، وأما هذا التطور فقد ارتبطت به ظهور ما يعرف بالإجرام المعلوماتي، وذلك نتيجة لاستخدام السيئ للمعلوماتية أو الحاسوب الذي نتج عن هذا الأخير عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن لمعطيات من جهة وتمس بحرية الأفراد والمؤسسات من جهة أخرى.

ولأن الحماية الفنية مهما بلغت درجتها من لتعقيد، وصعوبة فهي لا تستطيع المقاومة أمام التطور التقني الذي تشهده تقنيات الاختراق، وكذا عجز النصوص التقليدية في توفير الحماية خاصة من الناحية الإجرائية، مما دفع العديد من الدول إلى إبرام اتفاقيات وسن قوانين داخلية من أجل توفير الحماية خاصة من الماحية الإجرائية.

وفي الأخير نخلص القول إلى القول أن دراسة موضوع الجريمة المعلوماتية في ظل التشريع الجزائري تكتسي أهمية بالغة كونها تساهم في التعريف بظاهرة إجرامية جديدة، بدأت في الظهور والانتشار في معظم المجتمعات من بينها الجزائر، ونظرا لارتباطها بتكنولوجيا متطورة أدت إلى تميزها عن الجرائم التقليدية بدءا بتسميتها وصولا إلى الأفعال التي تدخل ضمن دائرتها.

ولا شك أن لقانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، وتعديل قانون العقوبات بموجب قانون رقم 15/04 كانت لها أهمية في تدارك الفراغ التشريعي الذي كان يعتري القانون الجزائري، وذلك من خلال حسم لمشرع الجدل الفقهي حول طبيعة المعلوماتية باعتبارها مالا من نوع خاص باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الألية للمعطيات في الفصل الثالث من الباب

الثاني من الكتاب الثالث من المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات لكون أن القسم السابع ورد تحت الكتاب الثالث المتعلق بالجنايات والجنح ضد الأموال.

كما أن هذا التعديل يعد قفزة في مجال التشريع كونه واكب التشريعات المقارنة بتجسيده معظم أحكام الاتفاقية الدولية للإجرام المعلوماتي من خلال تجريم الأفعال الدخول والبقاء غير المشروع داخل النظام المعلوماتي وتشديد العقوبة، إذ ترتب على ذلك مساس بالمعطيات أو نظام التشغيل للمنظومة المعلوماتية، المساس بالمعطيات أو تغييرها، استخدام المعطيات كوسيلة لارتكاب الجرائم المعلوماتية، حيازة وإفشاء ونشر واستعمال المعطيات المحصلة من هذه الجرائم، تجريم المساس بنظام التشغيل على أساس اعتبار المعطيات المعلوماتية من خلال الفقرة ج من المادة الثانية من قانون 09-04 تشمل برامج التشغيل.

وتجدر الإشارة إلى أنه لا يكفي أن يتم مواكبة نصوص تشريعية للتشريعات المقارنة بدون تجسيدها من الناحية التطبيقية، إذ يجب العمل على تكوين فرق من الضبطية القضائية وقضاة متخصصين في هذا لنوع من الجرائم ومدها بكافة الوسائل المادية والتقنية اللازمة لأداء عملها.

قائمة المصادر و المراجع

قائمة المراجع

1. المراجع باللغة العربية

أولا: الكتب

1.أحسن بوسقيعة، التحقيق القضائي، دار هومة للطبعة للنشر والطباعة، طبعة 10، الجزائر، 2009.

2.أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الأولى، دار هومة للنشر والتوزيع، الجزائر، 2009.

3.أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الطبعة الرابعة، 2007.

4.أحسن بوسقيعة، الوجيز في القانون الجزائي،الطبعة6، دار هومة، الجزائر.

5.أحسن بوسقيعة، الوجيز في القانون الجنائي العام، دار هومة للنشر والطباعة، طبعة أولى، الجزائر، 2010.

6.أحمد خليفة المط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.

7.أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، طبعة 5، الجزائر، 2008.

8.أسامة أمحمد المناعسة، جلال محمد الزغبي، جرائم الحاسب الآلي ، دار وائل للنشر،الأردن،2004.

9.أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الطبعة الثالثة، الجزائر، 2007.

10. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، طبعة 1، الإسكندرية، 2009.

11.خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، الطبعة الأولى، دار الهدى، عين ميلة، 2010.

12.رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، مستغانم 2012.

13.صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،2003 .

14.طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي ،جامعة الجزائر1، كلية الحقوق ،2011،2012.

15.عبد الفتاح بيومي حجازي، الإثبات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2003.

16.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت،الطبعة الأولى، دار الفكر الجامعي، مصر ،2006.

17.عبد الماجد العكايلة، الوجيز في الضبطية القضائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2010.

18.علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، مصر، 1999.

19.علي عدنان الفيل، الإجرام الالكتروني، دراسة مقارنة، منشورات زين الحقوقية، الطبعة الأولى، 2011.

20.علي محمد حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديثة، الطبعة الأولى،

21.محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009.

22.محمد خريط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة للنشر والطباعة، الطبعة 4، الجزائر، 2009.

23.مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009.

24.نائلة عادل، محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005.

25.نبيل صقر، موسوعة الفكر القانوني، جرائم الكمبيوتر والأنترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، طبعة 2005.

26.نهلة القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، 2009.

ثانيا: الرسائل الجامعية والمذكرات

1.ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة ماستر في القانون، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أمن البواقي، 2016.

2.ابرهيمي سهام،مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2004، 2007.

3.حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2005_2006.

4.سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجيستير، جامعة الحاج لخضر، باتنة، 2013.

5.سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في الحقوق، قانون جنائي، جامعة محمد خيضر، بسكرة، 2013.

6.سوير سفيان، جرائم المعلوماتية، مذكرة ماجيستير في العلوم الجنائية وعلم الإجرام، جامعة أبي بكر بلقياد، تلمسان، 2010.

7.صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة تخرج لنيل شهادة الماجيستير في القانون، جامعة مولود معمري، تيزي وزو، 2013.

8.قربوز حليمة ،الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2006_2009.

9.كحولة محمد وآخرون، جرائم المعلوماتية، مذكرة ماجيستير، جامعة أبي بكر بلقايد، تلمسان، 2010.

10.مرزوق نسيمة، جرائم الانترنت مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2006_2009.

ثالثا: المجلات والملتقيات

1.عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002.

رابعا: النصوص القانونية

1.دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1966.

2004.

2.قانون العقوبات المعدل والمتمم بالقانون09/01 المؤرخ في26 يونيو 2001.

3.القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات (ج ر 71 بتاريخ 2004/11/10).

4.قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في 2006/12/20.

5.القانون رقم 22/06المؤرخ في 20ديسمبر 2006، المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية.

6.القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

خامسا: الأوامر

1.الأمر 07/03 المؤرخ في: 2003/07/19 المتضمن براءة الاختراع.

2.الأمر رقم05/03الموافق ل19يوليو2003 المتعلق بحماية حقوق المؤلف.

2. المراجع باللغة الأجنبية :

1. Rose philipe la criminalité informatique que sais je 1er édition PU 1988

المواقع الإلكترونية:

www.despace-univ.dz

الفهرس

الفهرس

الملخص

مـلخص مذكرة الماستر

تناولنا بالدراسة في هذه المذكرة موضوع الجريمة المعلوماتية أين حاولنا التعريف بهذه الظاهرة الإجرامية المستحدثة والجديدة التي بدأت في الظهور والانتشار بشكل واسع في الآونة الأخيرة مبرزين أسباب انتشارها والعقوبات المقررة لها في التشريع الجزائري.

الكلمات المفتاحية:
1/الجريمة المعلوماتية 2/المشرع الجزائري 3/قانون العقوبات 4/العقوبات الأصلية 5/العقوبات التكميلية 6/ نظم المعلومات

Abstract of The master thesis

Dans ce mémorandum, nous avons traité du sujet de la criminalité d'information, où nous avons tenté de définir ce phénomène criminel nouveau et émergent qui a commencé à apparaître et à se répandre largement ces derniers temps, en mettant en évidence les causes de sa propagation et les peines qui lui sont prescrites en algérien. législation

keywords:
1/ Crime informationne 2/ Législateur algérien3/ code pénal
4/ Pénalités originales 5 Pénalités supplémentaires/ 6 Systèmes d'information