الـجمهورية الـجزائرية الـديمقراطية الـشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الدكتور الطاهر مولاي – سعيدة –
كلية الحقوق والعلوم السياسية
– قسم الحقوق –

مذكرة التخرج لنيل متطلبات شهادة الماستر في الحقوق
تخصص:قانون جنائي
المـوضوع:

سرقة المعلومات المخزنة في الحاسب الآلي

إعداد الطالبة:
زقير زهرة

اشراف الأستاذة:
بوسماحة أمينة

لجنة المناقشة.

الدكتور فليح كمال محمد عبد المجيد	رئيسا
الدكتورة بوسماحة أمينة	مشرفا و مقررا
الدكتورة عز الين غالية	عضوا مناقشا

الموسم الجامعي: 2020/2019

بسم الله الرحمن الرحيم

شكر و تقدير

قال رسول الله صلى الله عليه وسلم:"إذا ساعدكم أحد فكافئوه فإن لم تجدوا بما تكافئوه فأثنوا عليه."

كما أخص بالشكر والتقدير إلى الأستاذة " بوسماحة أمينة" التي تفضلت بالإشراف على هذه المذكرة، وتقديم النصح والإرشاد طوال فترة إعداد هذه المذكرة، فلها مني فائق الإحترام والتقدير وإلى كل أعضاء اللجنة المحترمة.

زكير زهرة

الإهداء

أهدي هذا المجهود إلى عائلتي الكريمة خاصة الوالدين الكريمين أطال الله في عمرهما ورفيقة دربي كريمة ديداوي وجميع الأساتذة الكرام.

زكير زهرة

المقدمة

مقدمة

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة، اصطلح على تسميتها بالثورة المعلوماتية وذلك إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن، فقد أمست قوة لا يستهان بها في أيدي الدول والأفراد وكان التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات والاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه هذه الثورة.[1]

ومما لاشك فيه أن الثورة المعلوماتية ونتيجة للتقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب والشبكات المعلوماتية التي تربط بينها قد تركت آثارا ايجابية وشكلت قفزة حضارية نوعية في حياة الأفراد والدول، وعلى الرغم من أهمية الوسائل الإلكترونية وإيجابياتها وإستعمالها، إلا أن الإستخدام غير المشروع لها، قد أدى إلى ظهور نوع جديد من الجرائم سميت "بالجرائم الإلكترونية" وهذه الأخيرة مرتبطة بأجهزة الحواسيب الآلية بإعتبارها أداة لإختزال الوقت وتخزين المعلومات وإنجاز العمليات المعقدة بساهمة من الفضاء الإفتراضي الذي نشأ نتيجة ارتباط المعلومات بمختلف الإتصالات السلكية واللاسلكية.[2]

حيث أن 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"، ومع النشاط المتزايد للمعلومات وتكنولوجيا الإتصال في مختلف النشاطات البشرية إذا 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 الأمر الذي أدى بأصحاب النوايا الإجرامية إلى الإتجاه إلى الإستعمال غير الشرعي لهذه المنظمات المعلوماتية من أجل ارتكاب أعمالهم الإجرامية المختلفة، فأفضى ظهور الكمبيوتر بكفاءته العالية في تجميع وتركيب وترتيب وإسترجاع المعلومات في ثوان معدودة وبدقة متناهية في عصر جديد اصطلح عليه عصر المعلوماتية ،[3]نظرا لما

---

[1] زبيدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر،2011،ص07.

[2] زبيدة زيدان، مرجع نفسه، ص09.

[3] علي جبار الحسناوي ، جرائم الحاسوب والإنترنت، الطبعة العربية دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2009، ص03.

اكتسبته المعلومات فيه من أهمية فائقة ولما أصبح لها من تأثير هائل على البشر ومن هنا تعددت الجرائم المعلوماتية والتي يستخدم فيها الكمبيوتر لأغراض غير شرعية، مثل سرقة المعلومات عن طريق اختراق شبكة إتصالات معلوماتية، كما أن هذا الإختراق يكون قصد تحقيق أهداف معينة لمجرمي المعلوماتية.

وقد كثرت هذه الجرائم في الأونة الأخيرة بإزدياد إستخدام الكمبيوتر من قبل عدد كبير من الناس في معظم دول العالم وإزدياد عدد شبكة الإتصالات المعلوماتية. [1] فالتقدم العلمي والتكنولوجي 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 أداة لإرتكاب الجريمة إذا أسيئ استخدامه.

والجزائر بإعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا فهي دولة معينة بالمكافحة، فكان لابد من إيجاد إطار قانوني مناسبا لسد الفراغ الإجرائي، لذلك وضعت مجموعة من الإجراءات للجرائم المعلوماتية تتماشى وطبيعة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته 04/09 المؤرخ في أوت 2009[2] تكمن أهمية البحث أساسا في كون الجرائم المعلوماتية جرائم مستحدثة وبالتالي لابد من قانون يتسم بالحداثة في مجال التكنولوجيا بالإضافة إلى كون الجرائم المعلوماتية حديثة النشأة ويمتد تأثيرها إلى جميع الأصعدة لإرتباطها بتطور تكنولوجيا الإعلام والإتصال.

إختيار موضوع "سرقة المعلومات المخزنة في الحاسب الآلي" يرجع إلى سببين أولهما شخصي والآخر موضوعي ، كذلك سبب إختيار هدا الموضوع التعريف بظاهرة جديدة هي الجريمة المعلوماتية التي بدأت في الظهور و الإنتشار وإرتبطت بتكنولوجيات الحاسبات الآلية، مما أسفر عن تميزها بمجموعة من الخصائص تختلف عن غيرها من الجرائم مما يستوجب ضرورة التعامل معها بما يتلائم مع هذه الخصوصية.

---

[1] علي جبار الحسناوي، المرجع السابق، ص04.

[2] القانون 04/09 الوقاية المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، المؤرخ في أوت ،2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال و مكافحتها، الجريدة الرسمية رقم8 العدد 47.

تم ما يزيد من أهمية هذا الموضوع صدور القانون رقم 04/09 المعدل والمتمم للأمر رقم المتضمن قانون العقوبات الجزائري الذي إستحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية.

ولمعالجة هذا الموضوع الذي أثار مشاكل صعبت إكتشاف الجرائم المعلوماتية ، تم طرح الإكتشاف التالية: ما موقف المشرع الجزائري من الجريمة المعلوماتية؟

ومن هنا نطرح تساؤلات فرعية تتمثل في:

- هل قانون العقوبات الجزائري كفيل بتجريم هذه الأفعال؟
- ما هي الاجراءات المتخذة لمكافحة الجرائم المعلوماتية في القانون الجزائري؟

واعتمدنا في دراستنا هذه على المنهج التحليلي الوصفي، كونه الأنسب لمثل هذه الدراسات من خلال تحليل ووصف المواد و الإتفاقيات الدولية من أجل مكافحة هذا النوع من الإجرام.

لقد تطرقت إلى دراسات سابقة إلى الجرائم المعلوماتية من الناحية الموضوعية، فقط ومن بين هذه الدراسات:

– رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبوبكر بلقايد، تلمسان.

و لمعالجة الإشكالية التي سبق طرحها وجب تقسيم هذه الدراسة وفقا لخطة منهجية تتمثل في:

فصلين تطرقنا في الفصل الأول إلى ماهية الجريمة المعلوماتية، و قسم إلى مبحثين هما:

المبحث الأول: ماهية المجرم المعلوماتي

المبحث الثاني: المجرم المعلوماتي

وفي كل مبحث إلى مطلبين وفروع.

الفصل الأول

الجريمة المعلوماتية وسماتها العامة

الفصل الأول

الإطار المفاهيمي للجريمة المعلوماتية

لقد ترتب على الإستخدام المتزايد لنظم المعلومات إلى نشوئها يعرف بالجريمة المعلوماتية، ولقد استخدمت عدة مصطلحات للدلالة على هذه الظاهرة الإجرامية، فمنهم من يطلق عليها اسم جرائم الحاسب الآلي، والآخر جرائم الكمبيوتر والإنترنت، فالجريمة المعلوماتية هي جريمة مستحدثة يعتمد مرتكبيها على وسائل تقنية ويكون ذا دراية كافية بإستخدام النظم المعلوماتية، لذا فإن الإحاطة بمفهومها الدقيق لا يزال محل خلاف فقهي، ولإزالة اللبس سنتطرق في هذا الفصل الأول: ماهية الجريمة المعلوماتية في المبحث الأول، وفي المبحث الثاني إلى المجرم المعلوماتي.

المبحث الأول :ماهية الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من الجرائم المستحدثة الناشئة عن التقدم التكنولوجي ،فقد شكلت هذه الأخيرة ثورة اقتحام المعلومات وذلك عن طريق استخدام تقنيات عالية، والمتمثلة أساسا في سرقة المعلومات المخزنة في جهاز الكمبيوتر [1] بطريقة فائقة السرعة،مما أدى إلى صعوبة معرفة مرتكبيها وفي هذا الصدد تعددت التعاريف بخصوص الجريمة المعلوماتية، وبخصوص هذه الظاهرة المستحدثة [2] سنتطرق إلى إزالة اللبس بخصوص مفهومها وهدا من خلال:

المطلب الأول: مفهوم الجريمة المعلوماتية:

لقد ترتب على الإستخدام المتزايد للنظم المعلوماتية، إلى نشوء ما يعرف بالجريمة المعلوماتية فقد تعددت التعريفات التي تناولت هذه الجريمة، كونها صنف جديد من الجرائم المستحدثة

الفرع الأول :التعريف القانوني للجريمة المعلوماتية:

اختلفت أراء الفقهاء في وضع تعريف جامع للجريمة المعلوماتية، فظهر اتجاهين مختلفين هما:

أولا: الاتجاه المضيق:

عرف أنصار هذا الاتجاه الجريمة المعلوماتية على أنها"كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية ملاحقته وتحقيقه من ناحية أخرى." [3] وعرفها (mass) بأنها :"الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح" [4]

ومن بين التعريفات الضيقة للجريمة المعلوماتية أنها "تلك التي يكون الغرض مناه موجه ضد أموال المعلوماتية متى كانت مرتبطة باستخدام نظام المعالجة الآلية للمعطيات، مع إقصاء تلك الأفعال المتمثل في استخدام الإعلام الآلي كوسيلة للاعتداءات أو الثقة العامة."[5]

---

[1] زينات طلعت شحادة مرجع سابق ص22

[2] زينات طلعت شحادة مرجع نفسه ص 23-24

[3] نائلة عادل محمد فريد قورة،جرائم الحاسب الآلي الاقتصادية،ط1، منشورات الحلبي الحقوقية ،بيروت،2005 ،ص28 .

[4] أمين لعباش،الحماية الجنائية للمعاملات الالكترونية،ط1،، مكتبة الوفاء القانونية الإسكندرية، 2015، ص17.

[5] أمين لعباش، مرجع نفسه، ص17 .

وتبقى جانب من الفقه الفرنسي تعريف أضيف من ذلك في أنها:"كل الأفعال غير المشروعة ضد نظام المعالجة الآلية للمعطيات."[1]

ثانيا: الاتجاه الموسع:

يرى أنصار هذا الاتجاه أن مفهوم الجريمة المعلوماتية يمتد حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية وعرفت هذه الأخيرة حسب أنصار الاتجاه الموسع بأنها " كل عمل أو امتناع يأتيه الإنسان أضرار بمكونات الحاسب المادية والمعنوية وشبكات الإيصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد نصوص قانون العقوبات لحمايتها"[2]

كما تبين الخبير الأمريكي (poker) مفهوما واسعا للجريمة المعلوماتية حيث عرفها " كل فعل إجرامي معتمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه كسبا يحققه الفاعل"[3]

ويذهب فريق آخر من الفقهاء لتعريف الجريمة المعلوماتية بأنها" كل سلوك إجرامي يتم بمساعدة الحاسب الآلي، أو هي كل جريمة تتم في محيط الحاسبات الآلية"[4]

وعرفه أيضا بأنها "كل سلوك إجرامي يتم بمساعدة الكمبيوتر"[5]

الفرع الثاني: موقف المشرع الجزائري من الجريمة المعلوماتية:

نص عليها المشرع الجزائري في نص المادة 394 مكرر 2 من قانون العقوبات الجزائري ، والتي يستخلص منها أن المشرع الجزائري جرم الاتجار في المعطيات سواء كانت مخزنة في جهاز الحاسوب أو إحدى الوسائل التقنية المرتبطة به أو مرسلة بواسطة الشبكة المعلوماتية، كما جرم كذلك في الفقرة الثانية من نفس المادة حيازة المعلومات أو المعطيات، ومما لا شك فيه أن المشرع الجزائري أدرك الأهمية الاقتصادية و التجارية في ظل التطور العلمي والتقني الذي يشهده العالم المعاصر [6]، وهذا من خلال وجوب حماية الأموال المعنوية وهي أمر ضروري ويقصد بهذا المعطيات والبيانات المعالجة آليا والتي يتم تبادلها عبر شبكة الانترنت ،وبالتالي المعلومات

---

[1] أمين لعباش، مرجع نفسه، ص 18 .

[2] أمين لعباش، مرجع نفسه، ص 16.

[3] نهلا عبد القادر المومني، لجرائم المعلوماتية،طبعة 2، دار الثقافة للنشر والتوزيع، الأردن ،2010، ص49.

[4] أمين لعباش، مرجع سابق، ص30.

[5] نهلا عبد القادر المومني ،مرجع سابق، ص49.

[6] لحسن بوسقيعة، الوجيز في القانون الجزائي القسم العام،طبعة 1، دار هومة للنشر والتوزيع، الجزائر،2010 ، ص3

يمكن حيازتها وتكون محلا للسرقة أو الإتلاف، سواء كانت هذه المعلومات معالجة آليا مخزنة في الوحدة المركزية للحاسوب أو مرسلة بواسطة الشبكة المعلوماتية[1].

الفرع الثالث: أركان الجريمة المعلوماتية وخصائصها:

أضافت المعلوماتية الكثير من الجوانب الإيجابية إلى حياتنا إلا أنها في المقابل جلبت معها الكثير من المخاطر، وحتى يتم التمييز بين الجريمة المعلوماتية وغيرها من الجرائم المشابهة لها ، شرعت لهذه الأخيرة أركان خاصة بها[2] ، والمعلوماتية ينظر إليها دائما بوصفها أداة محايدة وأن مصدر انتهاكها هو الإنسان نفسه، الذي غالبا ما يهيئ فرصة استغلال الوسيلة المعلوماتية عن حسن أو سوء نية فجوهر المشكلة يرتبط بالإنسان وشخصيته ودوافعه كما هو معروف لا يمكن لأي عقوبة هدفها تحقيق ردع عام أو ردع خاص ما لم تضع في الاعتبار شخصية المجرم[3]، و هذه الأركان هي:

أولا:**الركن المادي:**

يتمثل الركن المادي في أشكال الاعتداء على نظام المعالجة الآلية للمعطيات وهي ثلاثة أشكال:

1/ **الدخول أو البقاء غير الشرعي في نظام المعالجة الآلية للمعطيات:**

يتمثل شكل الاعتداء على نظام المعالجة الآلية للمعطيات من صورة بسيطة وأخرى مشددة.

أ/ **صورة بسيطة:** تقوم بمجرد الدخول أو البقاء غير المشروع، ويقصد بالدخول ظاهرة معنوية، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات، وبالتالي لا نقد بالدخول، الدخول بمفهومه المادي.

وتجدر الإشارة إلى أن المشرع الجزائري 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 بطريقة مباشرة أو غير مباشرة ، في حين أنه يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام. وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، في الحالة التي لا يكون فيها للجاني

[1] زبيدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي،طبعة 1، الجزائر، ص84.

[2] أمين لعباش ، مرجع سابق،ص 69.

[3] أمين لعباش، مرجع نفسه، ص 70.

الحق في الدخول إلى النظام، ويدخل إليه رغم ذلك ضد إرادة من له حق السيطرة عليه، سيبقى الدخول داخل النظام ويتحقق الاجتماع المادي للجريمتين الدخول والبقاء غير المشروعين [1].

ب/ صورة مشددة : تتحقق بتوافر الظرف المشدد المتمثل في حصول نتيجة الدخول أو البقاء غير المشروع ويخضع إما بمحو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

وقد نصت عليها المادة 394 مكرر2 من قانون العقوبات الجزائري على أن "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج، وعليه تستنتج من خلال ذلك أن هناك ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام وتربط هذين الظرفين علاقة سببية بين الدخول غير المشروع والنتيجة الضارة وإن لم تكن مقصودة " [2] ، 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 انتقاء تلك العلاقة ويثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ[3] .

ب: الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

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 أن برامج سير نظام المعالجة الآلية المعطيات تدخل ضمن المعطيات المعلوماتية[4] .

---

[1] زبيدة زيدان، مرجع سابق، ص 46.

[2] آمال قارة، مرجع سابق، ص 75.

[3] تنص المادة 394مكرر 1 من قانون العقوبات"يعاقب بالحبس وبغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي تصميم أو بحث أو بحث أو تجميع أو توفير أو أكثر أو الاتجار في معطيات مخزنة أو مرسلة عن طريق منظومة معلوماتية يمكن أن يرتكب بها الجرائم" .

[4] آمال قارة، مرجع سابق" ص 55.

ج: **الاعتداءات العمدية على المعطيات:**

نص عليها المشرع الجزائري في المادة 394 مكرر1 قانون العقوبات ،فجرم الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، كما نجد أن المشرع جرم المساس العمدي بالمعطيات الموجودة خارج النظام

ثانيا:الركن المعنوي:

باعتبار أن الجرائم المعلوماتية من الجرائم العمدية اشترط لقيامها توفر القصد الجنائي، فالركن المعنوي لجريمتي الدخول والبقاء غير المشروع يجب أن يعلم الفاعل بأن دخوله أو بقائه داخل النظام غير المشروع أو غير مصرح به أي اتجاه إرادته إلى ذلك" [1].

كما أن الركن المعنوي في جرائم الاعتداءات العمدية على المعطيات داخل وخارج النظام يجب أن يتوفر علم الجاني بأن نشاطه ذلك يترتب عليه تلاعب في المعطيات سواء داخل أو خارج النظام من خلال تصميمه أو بحثه أو نشره أو الاتجار في هذه المعطيات، ففي جرائم الاعتداءات على سير نظام المعالجة الآلية للمعطيات والتي ضمن من الجرائم العمدية تتطلب قصدا جنائيا خاصا، مما يجعلها تختلف عن الاعتداءات غير العمدية لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول أو البقاء غير المشروع .

وبالتالي يجب توافر العلم والإرادة لدى الجاني لقيام الركن المعنوي ، فيجب أن يكون عالما أن المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، ويعلم بخطورة الفعل الذي يقوم به [2].

المطلب الثاني: خصائص الجريمة المعلوماتية:

الجريمة المعلوماتية جريمة حديثة فهي مرتبطة بتكنولوجيا متطورة تتمثل في تكنولوجيا المعلومات ،ونتيجة لذلك هذه الأخيرة بجملة من الخصائص وهي:

[1] نائلة عادل محمد قورة، مرجع سابق، ص 35.

[2] أمين لعيلش، مرجع نفسه، ص 80.

الفرع الأول: الجريمة المعلوماتية عابرة للحدود:

المجتمع المعلوماتي لا يعترف بالحدود الجغرافية ،فهو مجتمع منفتح متسع عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود، فبعد ظهور شبكات المعلوماتية لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة ،فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات يفصل بينها آلاف الأميال، وبالتالي المساهمة في ارتكاب جرائم معلوماتية دون ترك أثر [1].

الفرع الثاني: صعوبة اكتشاف الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بصعوبة اكتشافها ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية كما أن الجاني يمكنه ارتكاب هذه الجرائم لأي وسيلة، لأن أكثر صورها خفية لا يلاحظها المجني عليه و لا يدري حتى بوقوعها [2].

الفرع الثالث: إنفراد الجريمة المعلوماتية عن الجرائم الأخرى:

تتميز جرائم الحاسب الآلي بخصائص تنفرد بها لوحدها وتتطلب لارتكابها وجود حاسب آلي ومعرفة تقنية باستخدامه و المقصود هنا ، أن يستعان بالحاسب الآلي كوسيلة لتنفيذ هذه الجرائم ، كما سبقت الإشارة إليه أن الحاسب الآلي و إن كان موضوعا للاعتداء ،كالإتلاف أو سرقة الجهاز نفسه أو شاشته فلا تثور أية مشكلة وذلك لأن قانون العقوبات كفيل بردع الجاني ولكن تثور المشكلة عندما يطال الاعتداء على ما يمكن أن يسمى بفن الحاسب الآلي، كتدمير برامجه وسرقتها وتدميرها وهذا ما جعل هذه الجريمة تنفرد عن غيرها من الجرائم [3].

الفرع الرابع: تتطلب لارتكابها وجود حاسب آلي ومعرفة تقنية باستخدامه:

تكتسب دراسة جرائم الحاسب الآلي أهمية خاصة، نظرا لخطورتها ذلك أنها تمس الإنسان في فكره وحياته الخاصة وتمس المؤسسات في اقتصادها القومي والسياسي والاقتصادي، ومن هذا المقصود أنه يستعان بالحاسب الآلي كوسيلة لتنفيذ هذه الجرائم، فتطلب هذه الأخيرة وجود حاسب آلي و معرفة تقنية استخدامه [4].

---

[1] نهلا عبد القادر،مرجع سابق، ص 24.

[2] زبيدة زيدان، مرجع سابق،ص36.

[3] نهلا عبد القادر، مرجع سابق، ص 63.

[4] نهلا عبد القادر ،مرجع نفسه،ص 65-66.

المطلب الثالث: الفيروسات المعلوماتية

تعتبر الفيروسات المعلوماتية من أهم وسائل المساس بالأنظمة المعلوماتية والمعطيات وأكثرها استعمالا، فهي تعد بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب في كلتا الحالتين بفائدتها، وفيروس الحاسب الآلي يشبه الفيروس الذي يصيب الإنسان إلى حد كبير فإنتقاله من حاسب إلى آخر، كما أن هذه الفيروسات كثيرة ومتنوعة، وقد أنشئت شركات ضخمة تقوم بتصنيع برامج للحماية منها وما أدى إلى إنتشار هذه الفيروسات هو الإستخدام الواسع للحاسب الآلي ومع التطور العلمي ظهرت فيروسات جديدة محصنة ضد هذه البرامج وفيما يلي سنتطرق إلى تعريف الفيروس المعلوماتي وخصائصه وهذا في "الفرع الأول" وإلى آثار الإصابة بالفيروس وهذا في "أولا" أما "ثانيا" سنتطرق إلى أنواع الفيروسات المعلوماتية.

أولا: تعريف الفيروس المعلوماتي و أنواعه:

الفيروس هو برنامج يكرر نفسه على نظام الكمبيوتر عن طريق دمج نفسه في البرامج الأخرى وكما أن الفيروسات قد تقضي على جهاز الحاسوب [1] وقد تأتي في مختلف الأشكال و الأحجام وهناك بعض الفيروسات ليست خطيرة وإنما مزعجة.

فالفيروس عبارة عن برنامج يحتوي على مجموعة من الأوامر الخاصة بكيفية انتشاره داخل الملفات، ويتم كتابة هذا البرنامج لإحداث آثار تخريبية [2] أو هو برنامج أو جزء في الشفرة التي تدخل إلى الحاسب الآلي بهدف التخريب وتتميز بقدرتها على نسخ نفسها إلى نسخ كثيرة وقدرتها على الإنتقال من مكان إلى آخر أو من حاسب إلى حاسب والإختفاء وتغطية محتوياتها.

وهناك فرق بين فيروس الحاسب الآلي وفيروس الإنترنت، حيث يتميز فيروس الإنترنت بإمكانية انتشار هائلة وغير محدودة كونه متميز في الإنتشار ولو لم يتم إغلاق الحاسب الآلي أو النظام كله، كما يختلفان من حيث الدور حيث يقوم فيروس الإنترنت بدور المخرب والمختلس للمعلومات خلافا لفيروس الحاسب الآلي الذي يقتصر دوره على التخريب فقط.

ومن خلال هذا التعريف يمكن استخلاص أهم الخصائص التقنية للفيروس المعلوماتي:

[1] أمير فرج يوسف، الجرائم المعلوماتية عبر الإنترنت، دار المطبوعات الجامعية الإسكندرية، 2008، ص68

[2] عمرو عبسي الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث،ص230.

- هو عبارة عن برنامج صغير يختفي بسهولة على النظام المعلوماتي، حيث استغل المجرمون المعلوماتيون هذه الخاصية حيث وضعوا فيروسات من الصعب العثور عليها بالبرامج المضادة للفيروسات.
- له قدرة فائقة على مهاجمة المكونات المعنوية لجهاز الحاسب الآلي والشبكات المعلوماتية التي تربطها فيما بينها مما يزيد في قدرته على الإنتشار والسرعة في تنفيذ أهدافها.[1]
- حذف ملفات (fat) مما يعني حذف جميع المعطيات الموجودة داخل الصلب وهو الأمر الأكثر خطورة.

ثانيا: أنواع الفيروسات المعلوماتية

الفيروسات كثيرة جدا لا يمكن حصرها ذلك أن الإنترنت ساهمت بشكل كبير في انتشارها وكثرتها إذ أصبحت قادرة على الإنتقال بكل سهولة من أي مكان دون تلقي أي عوائق تمنع تنقلها وتتمثل هذه الفيروسات في (أولا) حصان طروادة،(ثانيا)القنبلة المنطقية،(ثالثا) القنبلة الزمنية.

أولا:حصان طروادة:

سمي بهذا الإسم للدلالة على خطورته، وآثاره المدمرة وقدرته على الخداع [2] والمفاجأة والتضليل لديه القدرة على الإختفاء في البرنامج الأصلي للمستخدم وعندما يتم تشغيل هذا الأخير وينشط هذا الفيروس ويبدأ نشاطه التدميري، ومن آثاره السيئة تزوير المعلومات ومحو بعضها.

ثانيا: القنبلة المنطقية:

هي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة ويتم وضعه في شبكة المعلومات بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع وهذا النوع ينشط بمجرد بدأ تشغيل برنامج معين.[3]

---

[1] محمد سامي الشوا،ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة1993، ص189.

[2] بلال أمين زين،جرائم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية،2008،ص383.

[3] بن مكي نجاة، مرجع سابق، ص70

ثالثا:القنبلة الزمنية:

هي عكس القنبلة المنطقية، فهي تنطلق أو تنفجر في زمن وتاريخ محدد من السنة، فهي مرتبطة بالزمن، ويمكن إدخالها في برنامج وضبطها لكي تنفجر في يوم ووقت محدد وذلك بغرض تحويل نقود من حساب شخص معين إلى آخر.[1]

المبحث الثاني: المجرم المعلوماتي

أضافت المعلوماتية الكثير من الجوانب الايجابية إلى حياتنا إلا أنها في المقابل جلبت معها فئة جديدة من المجرمين اصطلح على تسميتهم "بمجرمي المعلوماتية [2].

والمعلوماتية ينظر إليها دائما بوصفها أداة محايدة وأن مصدر ضعفها وقوتها هو الإنسان ذاته، والذي غالبا ما يهيئ فرصة استغلال الوسيلة المعلوماتية عن حسن أو سوء نية، فجوهر المشكلة يرتبط بالإنسان وشخصيته ودوافعه وكما هو معروف فإنه لا يمكن لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام أو الردع الخاص ما لم تضع في الاعتبار شخصية المجرم [3]، ومن خلال هذا المبحث سنتطرق إلى:

المطلب الأول: السمات الخاصة بالمجرم المعلوماتي

يتميز المجرم المعلوماتي عن غيره من المجرمين بسمات معينة جعلت منه محلا للعديد من الأبحاث والدراسات، فلم يكن لارتباط الجريمة المعلوماتية بالحاسوب والانترنت أثرا على تمييز الجريمة المعلوماتية عن غيرها من الجرائم المعلومات التقليدية فحسب، وإنما للمجرم المعلوماتي سمات تميزه وهي:

الفرع الأول: المجرم المعلوماتي يتمتع بالمهارة والمعرفة و الذكاء

أولا: يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والانترنت [4]، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا .

فتنفيذ الجريمة المعلوماتية يتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات.

---

[1] بن مكي نجاة،مرجع نفسه،ص71.

[2] نائلة محمد قورة، مرجع سابق،ص60.

[3] نائلة محمد قورة، مرجع نفسه، ص61.

[4] أيمن عبد الحفيظ،الاتجاهات الأمنية والفنية لمواجهة الجرائم المعلوماتيةط1، دار النشر،2005،ص13.

ثانيا: إن المجرم المعلوماتي يمكن أن يكون تصورا كاملا لجريمته ، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها قبل تنفيذ جريمته ،وذلك حتى لا يفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها[1] .

ثالثا: غالبا ما يتميز المجرم المعلوماتي بالذكاء،حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة تلحق بالمجني عليه، فالمجرم المعلوماتي يستخدم مقدرته العقلية و لا يلجأ إلى استخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء.

فالإجرام المعلوماتي هو إجرام الأذكياء مقارنة بالإجرام التقليدي الذي يميل إلى العنف[2] .

الفرع الثاني: المجرم المعلوماتي يبرر ارتكاب جريمته:

أولا: يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم،أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله،حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية [3].

ثانيا: هؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب ويبدو أن الاستخدام المتزايد للأنظمة المعلوماتية ، قد أنشأ مناخا نفسيا لاستبعاد تصور فكرة الخير والشر وقد ساعد على ذلك عدم وجود احتكاك مباشر بالأشخاص، ومما لاشك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع [4]

الفرع الثالث: المجرم المعلوماتي إنسان اجتماعي:

المجرم المعلوماتي هو عادة إنسان اجتماعي قادر على التكيف في بيئته الاجتماعية بل إن بعضهم يتمتع بثقة كبيرة في مجال عمله، فالمجرم المعلوماتي يتميز بأنه لا يضع نفسه في حالة عداء مع المجتمع الذي يحيطه بل إنه إنسان قادر على التوافق والتصالح مع مجتمعه.

---

[1] أيمن عبد الحفيظ ، مرجع نفسه، ص14

[2] نهلا عبد القادر المومني، مرجع سابق، ص78

[3] أمين لعباش،مرجع سابق،ص53.

[4] أمين لعباش،مرجع نفسه،ص54.

فهو إنسان مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع ،و لا يعني ذلك التقليل من شأن المجرم المعلوماتي، بل إن خطورته الإجرامية قد تزداد إذا زاد تكيفه مع الاجتماعي مع توافر الشخصية الإجرامية لديه.

الفرع الرابع: خوف المجرم المعلوماتي من كشف جريمته:

يتصف مجرمو المعلوماتية بالخوف من كشف جرائمهم وافتضاح أمرهم بالرغم من أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقدان المركز الوظيفي في كثير من الأحيان.

ويساعد مجرمو المعلوماتية على الحفاظ على سرية أفعالهم طبيعة الأنظمة المعلوماتية نفسها، ذلك أن أكثر ما يعرض المجرم إلى اكتشاف أمره هو أن يطرأ أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها [1].

الفرع الخامس: المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي:

ويقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي التي تمكنه من ارتكاب جريمته، فكثير من مجرمو المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، والتي تعطي الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها [2].

المطلب الثاني: أسباب ارتكاب الجريمة المعلوماتية:

هناك عدة أسباب تدفع المجرم المعلوماتي لارتكاب الجريمة المعلوماتية، خصوصا في الآونة الأخيرة التي شهدت مثل هذه الظواهر بكثرة، في ظل هذه التطورات التي شهدتها الثورة التكنولوجية الحديثة [3] ، وقد تعددت الأسباب الدافعة لارتكاب الجريمة المعلوماتية من ناحية إلى أخرى وهي كالتالي:

الفرع الأول: الرغبة في التعلم:

الرغبة الشديدة في تعلم كل ما يتعلق بأنظمة الحاسوب والشبكات الالكترونية،قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية ويشير الأستاذ(ليفي) مؤلف كتاب قراصنة الأنظمة إلى أخلاقيات هؤلاء القراصنة التي ترتكز على مبدأين:

---

[1] نهلا عبد القادر المومني،مرجع سابق،ص82.

[2] نهلا عبد القادر المومنى، مرجع نفسه،ص 83.

[3] نهلا عبد القادر المومني، مرجع سابق، ص90-91.

أولا: إن الدخول إلى أنظمة الحاسوب يمكن أن يعلمك كيف يسير العالم

ثانيا: إن عملية جمع المعلومات يجب أن تكون غير خاضعة للقيود.

1/ فهناك من يرتكب جرائم الحاسوب بغية الحصول على الجديد من المعلومات،وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم [1] ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة من أجل تعلم المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية.

الفرع الثاني: الدوافع المادية:

الرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتران جرائمهم، من أجل تحقيق المكاسب المالية هذه يتم اللجوء إلى ارتكاب الجريمة المعلوماتية: إما عن طريق المساومة على البرامج أو ن طريق استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية[2]، ومثاله: سرقة معلومات أو إتلافها.

الفرع الثالث:المتعة والتحدي:

اختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فارغة، وعلى صعيد آخر قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية هو الرغبة في قهر الأنظمة الالكترونية والتغلب عليها، إذ يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة : فمجرمو المعلوماتية يتملكهم شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم المعلوماتية بواسطة الوسائل التقنية الحديثة [3].

الفرع الرابع: الرغبة في الانتقام:

الباعث على ارتكاب الجريمة المعلوماتية قد يكون الرغبة في الانتقام من شخص ما أو مؤسسة ما أو حتى من بعض الأنظمة السياسية في بعض الدول أو الانتقام من رب العمل.[4]

---

[1] أيمن عبد الحفيظ،مرجع سابق، ص63.

[2] نهلا عبد القادر المومني،مرجع سابق، ص65.

[3] نائلة عادل محمد فريد قورة، مرجع سابق، ص49.

[4] زينات طلعت شحادة، مرجع سابق، ص48.

الفرع الخامس: دوافع أخرى:

الدوافع السابقة ليست هي الوحيدة بل إن هناك دوافع أخرى تدفع لارتكاب الجريمة المعلوماتية.

فمثلا التنافس السياسي والاقتصادي قد يكون دافعا لارتكاب هذه الأفعال: كما يعد التسابق القضائي والعسكري بين الدول دافعا لهذه الجريمة، ومن ثم مناهضة العولمة قد تكون إحدى الدوافع لارتكاب هذا الفعل[1].

المطلب الثالث: الشبكة العالمية للمعلومات

أظهرت الشبكة العالمية للمعلومات قيمة إقتصادية كبرى للمعلومات، بحيث أصبحت المعلومات في العصر الحالي تمثل قوة كبيرة وبالتالي الإعتداءات الموجهة ضدها وذلك بالإعتداء على المعلومات المبتكرة والمحمية بموجب قوانين حقوق الملكية الفكرية كذلك الإعتداء على البيانات الإسمية ، سرقة المعلومات الخاصة وغيرها من أشكال الإعتداءات الماسة خصوصا بسلامة وإتاحة المعلومات، ورغم تلك الإعتداءات إلا أنه لا يمكن لأحد أن ينكر خدمات الإنترنت، ذلك يعني أن لهذه الأخيرة دورها السلبي و الإيجابي وقبل التطرق إليها سنتطرق إلى تعريف الشبكة الدولية للمعلومات وهذا في (الفرع الأول) وفي (الفرع الثاني) سنتطرق إلى نشأتها وتطورها.

الفرع الأول: تعريف الشبكة الدولية للمعلومات:

تعرف الشبكة الدولية للمعلومات أو الإنترنت بصفة عامة بأنها توصيات تعاونية لعدد من شبكات الحاسبات الآلية وهي مكونة من كلمتين Interconnection وكلمة network وهذا يعني أن مئات الشبكات المربوطة مع بعضها البعض بطريقة بسيطة وسهلة بحيث تبدو وكأنها قطعة واحدة أو نظام واحد دون إحساس أي من الأطراف أنه يختلف عن الآخر.[2]

فالإنترنت عبارة عن حاسب آلي يتحدث إلى حاسب آلي آخر يرتبطان بواسطة سلك أو فرع من الكوابل، وإذا كانت الحواسيب موجودة في أماكن بعيدة ومتفرقة فيمكن استخدام الأقمار الصناعية للربط بينها ليتحقق بذلك الإتصال الدولي عبر الإنترنت على الوصلات الوسيطة بين نقطتين.

[1] أيمن عبد الحفيظ، مرجع سابق،ص40.

[2] عبد الله ذيب محمود،حماية المستهلك في التعاقد الإلكتروني- دراسة مقارنة-، دار الثقافة للتوزيع والنشر عمان الأردن، الطبعة الأولى،2012،ص59.

الفرع الثاني: نشأة وتطور الشبكة العالمية للمعلومات

الشبكة المعلوماتية أو الإنترنت كفكرة عن وزارة الدفاع الأمريكية وتم تطبيقه كتجربة داخل المتحدة بمعرفة الهيئات العلمية المتخصصة عام 1969م فكانت الفكرة في البداية تقوم على ربط الحواسيب الآلية ببعضها البعض في مراكز البحث وفي كل منطقة إلى أن قامت مؤسسة العلوم القومية(NSF) بشراء حواسيب آلية عملاقة وتزويد مراكز الحاسب الآلي العملاق بها، تم توزيعها على كل مناطق الولايات المتحدة الأمريكية حتى تعمل إقليميا مع بعضها البعض في شكل شبكة قومية وفي كل المراحل كانت شبكة الإنترنت مخصصة لأغراض البحث العلمي وتتعامل مع مراكز البحث ومع الجامعات وتسيير العلماء، للإستفادة من إمكاناتها الهائلة في القيام بالعمليات الرياضية المعقدة والتي تعجز الحاسبات الآلية عن القيام بها[1]، وعندما استقرت الشبكة على مدى عشرين عاما على هذا النمط، ظهرت الحاجة الماسة إلى استخدام نفس الشبكات لأغراض تجارية يستفيد منها الأفراد والمؤسسات والشركات ورغم عدم إرتياح " NSF" وبعض المشتغلين بالشبكات الرسمية لهذا التطور، إلا أن الشركات استطاعت من خلال نفوذها داخل الحكومة الفدرالية ودوائر الحكومة الأمريكية أن تفتح المجال للإستخدام التجاري للشبكة محليا وعالميا، ولذلك يمكن القول أن الشبكة بدأت تعمل بشكل تجاري عام 1993.

والإنترنت لا يملكها أحد، ولا يسيطر عليها أحد، إنما هي ملكية تعاونية للبشرية بقدر إسهامهم فيها، وقد كانت خدمات شبكة الإنترنت في البداية مجانية وبغير مقابل و قد كانت قاصرة على الإستخدامات العلمية والبحثية وليس لها الصفة التجارية.[2]

وفي الوقت الحالي تقوم شركات تجارية بإدارة شبكة الإنترنت على أسس تجارية، لذلك فمن الضروري أن يدفع المشترك مبلغا من المال مقابل إستخدامه للمعلومات، وكذلك لتطوير الشبكة نفسها والمحافظة على تطويرها وتحسين استخداماتها، وذلك بالطبع إضافة إلى ما يدفعه المشترك في الشبكة إلى شبكة المعلومات مقابل استخدامه لبرامجها والإستفادة من المعلومات التي تبيعها للمستهلك مقابل إنتاجها وما بذله من جهد للحصول عليها مع تحقيق الربح المعقول.

[1] عبد الله ذيب محمود، مرجع نفسه، 64.

[2] خالد عباد الحلبي،إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت،طبعة 1، دار الثقافة للنشر والتوزيع، ص50-51.

وشبكة الإنترنت أو كما يطلق عليها الشبكة العالمية الإلكترونية أو الشبكة العنكبوتية نقدم للفرد والمجتمع كل ما تقدمه وسائل المعرفة. فالإنترنت هو الشبكة الدولية للمعلومات وتعرف أيضا أنها شبكة عالمية من الحاسبات الآلية تحتوي على شبكات منفصلة بعضها مع البعض عبر العالم مما يعطي لكل مستخدم للإنترنت القدرة على الإتصال بحاسب آلي في أي مكان في العالم له إتصال بالشبكة.

الفرع الثالث: خدمات الشبكة الدولية العالمية

إن سهولة استخدام شبكة الإنترنت والخدمات المتعددة والمتنوعة التي تقدمها في جميع مجالات الحياة ساهم بشكل فعال في زيادة أعداد المستفيدين منها وسنقوم بإستعراض أهم الخدمات الإلكترونية التي تقدمها الشبكة العالمية للمعلومات "الإنترنت" ومن أهمها البريد الإلكتروني وشبكة الويب العالمية في(أولا) محركات البحث والتخاطب في (ثانيا).

أولا: البريد الإلكتروني وشبكة الويب العالمية

يعتبر البريد الإلكتروني من الإستخدامات الشائعة التي توفر إمكانية الإتصال بملايين البشر حول العالم كبديل للبريد التقليدي والبريد الإلكتروني عبارة عن رسالة لكنها تتم بطريقة إلكترونية يكتبها المستخدم على جهاز الحاسوب وذلك بعد أن يفتح الصفحة الخاصة ببريده الإلكتروني والتي لها رقم سري وإسم المستخدم ولا يمكن لغيره الدخول إليها وبعد إتمام كتابة الرسالة التي يقوم المستخدم بالضغط على أمر معين في الصفحة وهو(SNED)أي أرسل وفي حال إتمام الرسالة يظهر على جهاز الحاسوب ما يفيد إتمام العملية بنجاح، وإذا كان هناك خطأ ما يظهر للمرسل رسالة موجزة تشير إلى موضع الخطأ.[1]

أما عن شبكة الويب العالمية والمعروفة بـ (WWW) يمكن أن تعرف أنها عبارة عن كم هائل من المستندات المحفوظة في شبكة الحاسوب والتي تتيح لأي شخص أو أي جهة على معلومات تخص جهات أخرى أو أشخاص آخرين قاموا بوضعها على هذه الخدمة أي تفيد للمستخدم تصفح مواقع المعلومات وهذه الخدمة تجمع النصوص والصور والأصوات والأفلام المتحركة مما يتيح للمستخدم الحصول على المعلومات التي يريدها في أسرع وقت.

[1] خالد عباد الحلي، مرجع سابق،ص53.

ثانيا: محركات البحث والتخاطب عبر الإنترنت:

محركات البحث عبارة عن برامج تساعد في الحصول على المعلومات، فكما هو معروف هناك كم هائل من المعلومات في شبكة الإنترنت يرغب المستخدم في معرفة المواقع التي تمكنه من الوصول مباشرة إلى مبتغاه فيتم في هذه الحالة اختيار خدمة البحث بإسم الموضوع الذي يهم المستخدم ومن ثم يتم تزويده بقائمة المواقع التي تتطابق مع المعلومات التي يرغب في الحصول عليها، وهناك عدة محركات بحث كل منها يستخدم طريقة معينة أو خاصة في إجراء محركات بحث كل منها يستخدم طريقة معينة أو خاصة في إجراء عملية البحث.[1]

أما عن التخاطب عبر الإنترنت، فيقوم المستخدم في عملية التخاطب بكتابة رسالة يجري عرضها مباشرة أمام شخص آخر في أي مكان في العالم، الذي يقوم بدوره في الرد على الرسالة مباشرة، يشغل التخاطب عبر الإنترنت مساحة كبيرة من حزمة البيانات التي يتم تبادلها بين مستخدمي هذه الشبكة العالمية، ومن مزايا التخاطب عبر شبكة الإنترنت أنه نوع من الخطاب الفكري الذي إذا تم بالشكل والأسلوب الصحيحين فإنه سيؤدي إلى التبادل الثقافي بين الحضارات.[2]

[1] خالد عباد الحلي، مرجع سابق، ص53.

[2] عبد الله ذيب محمود، مرجع سابق، ص69.

الفصل الثاني

الجرائم الواقعة بواسطة النظام المعلوماتي

الفصل الثاني: الجرائم الواقعة بواسطة النظام المعلوماتي:

مما لاشك فيه أن التقدم التكنولوجي الهائل في كافة مناحي الحياة ولاسيما في مجال تبادل المعلومات والمعلوماتية و الاتصالات والاعتماد المطرد على الحاسوب والنظم المعلوماتية بصفة عامة في مختلف جوانب الحياة أدى إلى تعرض المعلومات لأخطار كثيرة، دفع العديد من الدول إلى سن قوانين داخلية ودولية لملاحقة كل منتهكات المعلومات، كما ارتبطت جرائم الحاسبات الآلية للمعطيات، وهي ظاهرة إجرامية حديثة النشأة لتعلقها بتكنولوجيا الحاسبات الآلية، الأمر الذي صعب مكافحتها خصوصا في ظل التطور التكنولوجي الذي تشهده البشرية، وقد تم تقسيم هذا الفصل إلى مبحثين تطرقنا في "المبحث الأول" إلى دور الحاسب الآلي في ارتكاب الجريمة المعلوماتية، أما "المبحث الثاني" فقد تطرقنا إلى جرائم المعالجة الآلية للمعطيات.

المبحث الأول: الحاسب الآلي ودوره في ارتكاب الجريمة المعلوماتية

يعتبر الحاسب الآلي من أبدع ما ابتكره عقل الإنسان على مدى الأزمان، هذه الآلة الصغيرة التي ارتبطت بها معظم نشاطات الإنسان وباتت تقدم له خدمات هائلة، كانت تتطلب منه في الماضي الكثير من الجهد والمال والوقت وأصبح من غير الممكن أن يستغني الإنسان عنها في مجالات شتى بالنظر للخدمات الكبيرة التي تقدمها له هذه الآلة، وهو في نفس الوقت وعلى وجه الخصوص الأساس الذي يبنى عليه أي نظام معلوماتي، والحاسوب بكل مكوناته، عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها واسترجاعها عند الطلب[1]، وهو ما سنتطرق له في "المطلب الأول" للتعريف بجهاز الحاسوب أما "المطلب الثاني" نسلط الضوء على أساليب الاعتداء على المعلومات المخزنة في الحاسوب.

المطلب الأول: تعريف جهاز الحاسوب:

يتفق الباحثون في مجال تسمية وتعريف الحاسب الآلي،هذا الجهاز الذي يتولى معالجة المعلومات بشكل آلي وقد جرت العادة على إطلاق اسم الحاسب الآلي أو الحاسب الالكتروني على ذلك الجهاز الذي أصبح ضرورة عصرية، وهناك من يسميه أيضا بالعقل الإلكتروني [2]، ويتكون الحاسوب من كيان مادي وآخر معنوي، ويضم الكيان المادي الأجهزة المادية المختلفة، وهي جهاز الإدخال، جهاز الإخراج، ووحدات التشغيل المركزية التي يتم من خلالها معالجة المعلومات وتخزينها وإخراجها.

[1] د.أحمد عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، حق الملكية، بدون طبعة، الجزء الثاني، دار إحياء التراث العربي، بيروت 1952،ص09.

[2] آمال قارة / مرجع سابق،ص34.

الكيان المعنوي يشمل البرامج المختلفة التي تحقق من خلالها قيام الحاسب بوظائفه المختلفة، بالإضافة إلى المعلومات المطلوب معالجتها بالفعل.[1]

سنحاول التفصيل في هذا من خلال: "الفرع الأول" مكونات الحاسب الآلي، "الفرع الثاني" دور الحاسب الآلي في ارتكاب الجريمة المعلوماتية، "الفرع الثالث" التعدي على برامج الحاسب الآلي.

الفرع الأول:مكونات الحاسب الآلي:

تتألف مكونات الحاسب الآلي من مكونات مادية وأخرى من عناصر رئيسية أهمها: وحدة التشغيل، وحدات الإدخال والإخراج، وحدات التخزين، وحدة التحكم، وحدة الذاكرة المساعدة، وحدات الحساب والمنطق وسنفصل للبعض منها كالتالي:

وحدات الإخراج والإدخال:

وهي تستخدم في إدخال البيانات والأوامر والمعلومات إلى وحدة التشغيل أو المعالجة المركزية في الحاسب الآلي، أو إخراجها منها لاستخدامها بواسطة مستخدم الحاسب وذلك بتوجيه من وحدة التحكم.

أولا: وحدات الإدخال:

هي الوحدات المصممة للقيام بإدخال المعلومات إلى الحاسب الآلي ومعالجتها، إلى وحدة المعالجة الرئيسية، وتتألف هذه الوحدات بدورها من العديد من المكونات، من بينها لوحة المفاتيح، الماسح، الفأرة، مشغل الأقراص.[2]

ثانيا: وحدات الإخراج:

بعد أن يتم إدخال البيانات والأوامر والمعلومات إلى الحاسب الآلي ومعالجتها، فإنه يمكن من خلال ذلك الحصول على المعلومات وناتج معالجة البيانات بواسطة وحدات الإخراج المختلفة فوحدات الإخراج هي الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات الموجودة في الحاسب الالي .[3]

---

[1] تعريف الكمبيوتر لغة: "من حسبها فالحسب العد وما عد والحساب والحسابة عدك للشيء وحسب الشيء يحسبه"/ عن خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى للطباعة والنشر والتوزيع، عين مليلة الجزائر2010، ص21.

[2] د. أحمد عبد الرزاق السنهوري، مرجع سابق، ص22.

[3] محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف بالإسكندرية،2006، ص23.

فتستخدم وحدات الإخراج لعرض نتائج العمليات التي أتمها الكمبيوتر على المعطيات التي تم إدخالها إليه عن طريق وحدات الإدخال، فهي مجموعة الوحدات المسؤولة عن إظهار ما يحتاجه المستخدم للتفاعل مع الحاسوب، ومن أمثلتها الطابعات والشاشات، ومن أمثلة وحدات الإخراج أيضا وحدة تخزين البيانات على الأقراص الممغنطة أو على الشرائط الممغنطة والتي تستخدم كوحدة إدخال أيضا.[1]

ثانيا: وحدة الذاكرة والتحكم:

أ- وحدة **الذاكرة:** وتقوم هذه الوحدة بتخزين البرامج والبيانات التي تقع تحت الوحدة صنفين:

- وحدة الذاكرة الرئيسية: تستخدم لتخزين البرامج والبيانات التي تقع تحت المعالجة.
- وحدة ذاكرة القراءة فقط: حيث تتم برمجة هذه الذاكرة أثناء مرحلة التصنيع ويمكن قرائتها عند الحاجة، ولا يمكن تخزين أي معلومات جديدة أثناء استخدامها.

ب- وحدة التحكم: تنظم علاقة وحدة المعالجة المركزية مع الوحدات الأخرى لاستلام البيانات وإرسال النتائج بعد المعالجة فتقوم بالتحكيم بعمل وحدات الحاسوب وتنسيق تبادل البيانات والأوامر، وتحتوي على مجموعة من السجلات والعدادات ودوائر فك الرموز وتحليلها ومولدات إشارات التزامن والتحكم.

ثالثا:الكيان المعنوي: يتمثل في البرامج والمعطيات، اللذان يشكلان معا المكونات غير المادية لنظام المعالجة الآلية إذ بدونها يعتبر الحاسب الآلي مجرد آلة كباقي الآلات، والتعدي عليها هو الذي يشكل الجريمة المعلوماتية بالمعنى الدقيق.[2]

[1] محمد عبد الله أبو بكر سلامة، مرجع سابق، ص30.

[2] محمد عبد الله أبو بكر سلامة،مرجع نفسه، ص31.

الفرع الثاني: دور الحاسب الآلي في ارتكاب الجريمة المعلوماتية:

يلعب الحاسب الآلي دورا مهما في الجريمة المعلوماتية، فقد يكون له دور في ارتكابها، فإما يكون الهدف المباشر للاعتداء أو موضوع الاعتداء أو وسيلة الاعتداء لتحقيق نتيجة إجرامية، كما قد يكون له دور في اكتشافها، وهذا ما سيتم التطرق له "أولا" أن يكون الكمبيوتر هدفا أو موضوعا للجريمة،" ثانيا" استخدام الحاسب الآلي كأداة لارتكاب الجريمة.

أولا:أن يكون الكمبيوتر هدفا أو موضوعا للجريمة : يمثل في حالة الدخول غير المصرح به إلى النظام المعلوماتي أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، كحالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم.[1]

ومن أوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في مجال التصرفات غير القانونية أن توجه الاعتداءات إلى معلوماته أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، وهدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام، ودون أن يدفع الشخص مقابل الاستخدام.[2]

ثانيا: استخدام الحاسب الآلي كأداة لارتكاب الجريمة : في هذه الحالة لا يكون الحاسب الآلي محلا أو موضوعا للجريمة، ولكن تقع الجريمة في هذه الحالة بواسطته أي أنه يستخدم كأداة لارتكابها، ومن الناحية النظرية يمكن أن تقع بعض الجرائم بواسطة الحاسب مثل:الجرائم التي تقع على الذمة المالية من سرقة ونصب وخيانة الأمانة والتزوير في عمليات السحب على الجوائز وانتهاك حرمة الحياة الخاصة، ففي الحالة الحاسب يستخدم كأداة لارتكاب الجريمة.

إن ظهور مثل هذا النوع الخطير من الإجرام المعلوماتي ينجم عنه مخاطر جسيمة، ذلك لأنها

[1] بن مكي نجاة، مرجع سابق، ص36.

[2] د.أحمد عبد الرزاق السنهوري، مرجع سابق، ص26.

تمس خاصة الكيان المعنوي للحاسب الآلي، بالإضافة إلى أن هذا راجع بالدرجة الأولى إلى تدخل الإنسان في هذا الخطر المعلوماتي، ونظرا إلى تزايد نطاق جرائم الكمبيوتر واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة، أصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها.[1]

[1] د.أحمد عبد الرزاق السنهوري، مرجع نفسه، ص27-28.

الفرع الثالث: التعدي على برامج الحاسب الآلي:

يستلزم هذا النمط من الإجرام معرفة فنية كبيرة في مجال البرمجة والتنفيذ، وإن كان من الصعوبة بمكان، إلا أنه يمكن أن يتحقق في مراحل مختلفة ومن صنع برامج التشغيل أو التطبيق أو في لحظة صيانتها وفيما يلي سيتم التطرق إلى: التعديل في البرنامج التطبيقي وهذا " أولا " أما " ثانيا " سيتم التطرق إلى التعديل في برنامج التشغيل.

أولا:التعديل في البرنامج التطبيقي: يمثل هذا النوع من التعديل نسبة 15% من مجموع حالات الغش المعلوماتي، يكون الهدف الرئيسي للتعديل هذه البرامج هو اختلاس النقود وتكثر تلك الجرائم في مجال الحسابات [1]، وهناك نظام أكثر خطورة وانتشارا وتقوم فكرة هذا النظام، على اقتراف الاختلاس عن طريق اقتطاعات مبالغ زهيدة وعلى فترات زمنية طويلة ومتباينة من خلال صفقات عديدة يترتب عليها تحقيق فائدة كبيرة ومبالغ طائلة.

ثانيا: التعديل في برنامج التشغيل: تعتبر برامج التشغيل هي البرامج المسؤولية عن عمل النظام المعلوماتي، من حيث قيامها بتنظيم وضبط توالي التعليمات الخاصة بالنظام، والجريمة تتحقق في هذه الحالة بتزويد البرنامج بمجوعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تتيح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي ويأخذ الاعتداد على برامج التشغيل إحدى الصورتين، الصورة الأولى المصيدة أما الصورة الثانية تصميم برنامج وهمي أو إعداد برنامج.[2]

الصورة الأولى : المصيدة: تتمثل في المداخل وهي تعني أن أي برنامج يتضمن عند إعداده أخطاء و عيوب قد لا تكتشف كلها أو بعضها إلا عند استعمال هذه البرامج عن طريق ما يعرف بالمداخل المميزة التي يجب أن يستبعدها المبرمج بمجرد الانتهاء من التصحيح النهائي للبرامج، وتتمثل خطورة المصيدة في أنه عن طريقها يمكن الولوج إلى كل المعلومات المخزنة بالحاسب الآلي والتوصل إلى التعليمات والشفرات الخاصة بها.

[1] بن مكي نجاة، مرجع سابق، ص50.

[2] بن مكي نجاة ،مرجع نفسه، ص 52-53.

الصورة الثانية : تصميم برنامج وهمي أو اصطناع برنامج: يقوم المبرمجون من خلال برامج تشغيل النظام المعلوماتي وضع برنامج مصمم خصيصا لارتكاب الجريمة ومراقبة تنفيذها، التي يرى الخبراء والباحثون أنها لا تكتشف إلا صدفة.[1]

ومن الملاحظ النظام المعلوماتي في هذه الاعتداءات يكون محلا أو موضوعا للجريمة المعلوماتية لأن الاعتداء يستهدف المكونات المعنوية للحاسب الآلي بما تشمله من برامج ومعلومات، وهذا ما استدعى جلب اهتمام المجتمع الدولي، وإبرامه عدة اتفاقيات دولية تهدف إلى إقرار الحماية القانونية لهذه البرامج نظرا لما تشمله من قيمة اقتصادية عالية، تشجيعا للابتكار وحفاظا عليها من التقليد.[2]

[1] محمد عبد الله أبوبكر سلامة، مرجع سابق، ص43.

[2] د.أحمد عبد الرزاق السنهوري، مرجع سابق، ص18.

المطلب الثاني: طرق الاعتداء على المعلومات المخزنة في الحاسوب:

أصبحت المعلومة مصدر قوة ومصدر سلطة لما تقدمه من إيجابيات إلا أنها تبقى قاصرة أمام التطور التكنولوجي الذي يشهده العالم، خاصة المعلومات المخزنة في برامج الحاسوب والتي تتعرض للإعتداء بطرق وتقنيات عالية. [1] ومن خلال هذا سيتم التطرق لدراسة هذه الإعتداءات على المعلومات كالتالي:

الفرع الأول: سرقة المعلومات المخزنة في الحاسوب ، و الفرع الثاني: الاختراق ،ثم في الفرع الثالث تم التطرق الى حماية المعلومات وفق القوانين المستحدثة.

الفرع الأول: سرقة المعلومات من الحاسوب:

يعرف الأستاذ "باركر" المعلومات بأنها:"هي مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال، أو التفسير أو المعالجة بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها أو جمعها أو نقلها بوسائل وأشكال مختلفة[2].

ونظرا لما تشغله المعلومات من قيمة اقتصادية كبيرة كان هناك تهافت من قبل الأفراد والمؤسسات المختلفة، وحتى الدول للحصول عليها، و تسريع عملية التقدم في كل المجالات، وبالمقابل كانت هناك طائفة متواجدة دائما للقيام بالاستغلال غير المشروع لهذه المعلومات وبكل الأساليب المتاحة للقيام بسرقة المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر الشبكة العالمية الإنترنت، فأصبحت إحدى أكثر الأساليب انتشارا في مجال الاعتداء على المعلومات، ويطلق البعض على هذه الجريمة: " جريمة قرصنة المعلومات" [3]، وتجري عملية السرقة من خلال وصول الأفراد غير المرخص لهم إلى المعلومات والبيانات وبرامج الحاسوب ويقصد بالقرصنة المعلوماتية نسخ البرامج على نحو غير مشروع

[1] نهلا عبد القادر المومني، مرجع سابق، ص 101.

[2] محمد عبد الله أبو بكر سلامة، مرجع سابق، ص33.

[3] نهلا عبد القادر المومني، مرجع نفسه، ص99.

أو الحصول دون وجه حق على معلومات مخزنة في ذاكرة الحاسوب بطريقة مباشرة أو غير مباشرة

1-اختلاس النقود ويتم عن طريق عمل تحويلات لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك وتسجيلها وإعادة إرسالها إلى حساب آخر في بنك آخر.

2- إتلاف المعلومات وتعد من أخطر الجرائم المعلوماتية لأضرارها الجسيمة والبالغة نظرا إلى أن جميع مؤسسات الدولة وكذلك المؤسسات الخاصة أصبحت تدار عبر برامج وقاعدة بيانات مدرجة على الكمبيوتر.[1]

3- تسريب المعلومات: هناك أنواع كثيرة من الجرائم المتعلقة بالحاسب الآلي يحتاج تنفيذها إلى إخراج البيانات أو نسخها من الحاسب الآلي أو من مراكز المعلومات الخاصة بالحاسب، حيث يقوم مرتكب هذه الجريمة بإعداد وتحضير الجوانب الفنية لجريمته داخل الجهاز أثناء عمله العادي، ودون أن يدرك أحد ما يسعى إليه الجاني، كما تتحقق هذه الأخيرة بإخراج البيانات وتسريبها إلى مكان آخر أو باستخدام ما يعرف بتقنيات حصان طروادة.[2]

ثانيا: سرقة منفعة الحاسب الآلي: يقصد بسرقة منفعة الحاسوب استخدامه لأغراض شخصية أو تجارية دون علم مالكه أو حائزه القانوني، ويعد هذا الفعل غير المشروع من أكثر الجرائم المعلوماتية تعارفا وقد يرتكب إما بواسطة مستخدمي الشركات الخاصة أو المرافق العامة، ومن الأمثلة التي تشير إلى حدوث هذا في جميع أنحاء العالم كأن يتوصل شخص إلى الحاسب الآلي للغير بطريق التحايل كالقرصان، وبالتالي يتم الحصول على المعلومات بطريقة غير شرعية وانتهاك أسرار ذات أهمية خاصة أو خطورة أمنية.

الفرع الثاني: الشروط الواجب توافرها في المعلومات لتمتع بالحماية القانونية:

هناك شروط لابد من توافرها في المعلومة بصفة عامة، سواء كان التعبير عنها يتم من خلال وسيط مادي أم كانت بمعزل عن هذا الوسيط حتى يمكن أن تتمتع بالحماية القانونية وتتجلى هذه

[1] بن مكي نجاة، مرجع سابق، ص52.

[2] بن مكي نجاة، مرجع سابق، ص53.

الشروط فيما يلي:

أولا: أن يتوافر في المعلومة التحديد والابتكار.

ثانيا: أن يتوافر في المعلومة السرية والاستثمار.

أولا: أن يتوافر في المعلومة التحديد والإبتكار:

إن المعلومة التي تفتقر لصفة التحديد لا يمكن أن تكون معلومة حقيقية، فالمعلومة بوصفها رسالة مخصصة للتبليغ يجب أن تكون محددة،لأن التبليغ الحقيق يفترض التحديد [1] كما أن المعلومة المحددة هي التي يمكن حصرها في دائرة خاصة بها من الأشخاص.

أما فيما يتعلق بالإبتكار فإنه ينبغي أن تنصب هذه الصفة على الرسالة التي تحملها المعلومة، فمعلومة غير مبتكرة هي معلومة شائعة ومتاحة للجميع ويمكن للجميع الوصول إليها ولا يمكن نسبتها إلى شخص محدد.[2]

ثانيا:أن يتوافر في المعلومة السرية والإستئثار:

كلما اتسمت المعلومة بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها هذه المعلومة محددا بمجموعة معينة من الأشخاص، ودون هذا التحديد لا يمكن أن تكون المعلومة محلا يعتدي عليه بالسرقة أو النصب أو الإتلاف على سبيل المثال، فالمعلومة غير السرية تكون صالحة للتداول ومن ثم تكون بمنأى عن أي حيازة، وهذا ما ينطبق على المعلومات التي تتعلق بحقيقة معينة كدرجة الحرارة في وقت معين أو تلك المعلومات التي ترد على حوادث معينة كالبراكين، فهي تبدو كأنماط قابلة بسهولة بين كل الأشخاص والوصول إلى المعلومة بسهولة يتعارض والطابع السري لها.

قد تستمد المعلومة سريتها من طبيعتها كإكتشاف في أحد المجالات التي تتميز بالسرية، أو قد الإئتمان.[3]

[1] زينات طلعت شحادة، مرجع سابق، ص208.

[2] زينات طلعت شحادة، مرجع نفسه،ص209.

[3] بن مكي نجاة، مرجع سابق، ص16.

و تعد خاصية الاستئثار بالمعلومة أمرا ضروريا لأنه في جميع الجرائم التي تنطوي على اعتداء قانوني على القيم يستأثر الفاعل بسلطة تخص الغير وعلى نحو مطلق، وتتوافر للمعلومة صفة الاستئثار إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين.

الإجراءات بحماية معطيات الحاسب الآلي:

أولا: التحفظ المعجل على البيانات المخزنة: إن هذا الإجراء يعد أداة تحقيق مستحدثة ويقصد به السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته وتحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها.

ثانيا: الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك: الأصل أن البيانات الشخصية المتعلقة بمستخدمي الشبكة تدخل في إطار الحق في الخصوصية غير أنه يسمح لرجال الضبط القضائي بأن يأمر الأشخاص بتسليم ما تحت أيديهم من موضوعات يطلب تقديمها كدليل، ومن بينها البيانات المتعلقة بالمشترك التي يحوزها مزودو الخدمات[1].

اعتراض المراسلات الالكترونية:

يقصد بهذا الإجراء مراقبة الاتصالات الالكترونية أثناء بثها وليس الحصول على اتصالات الكترونية مخزنة، وقد استحدث المشرع الجزائري هذا الأمر عن طريق قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، غير أنه حدد الحالات التي يسمح فيها باللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو مؤسسات الدولة أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[2]

[1] بن مكي نجاة، مرجع سابق، ص230.

[2] بن مكي نجاة، المرجع نفسه، ص231.

الفرع الثالث: الاختراق:

إن معظم الجرائم المعلوماتية تقوم على تقنية الاختراق وذلك بغرض الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، والاختراق بصفة عامة هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف للوصول إلى البيانات الموجودة في أجهزة شخصية بوسائل غير مشروعة، كما يحتاج التسلل إلى جهاز الضحية دون علمه إلى مجموعة من الوسائل، فقد تم الاختراق عن طريق استعمال نظم التشغيل لكونها مليئة بالثغرات من خلال البروتوكولات التي يستخدمها نظام التعامل مع شبكة الإنترنت فيقوم المجرم بالبحث عن الضحية وذلك من خلال معرفة رقم (AD)[1] الخاص به ويتم البحث عن هذا الرقم بمجموعة من الخطوات يقوم بها المخترق على الجهاز الذي يشترط أن يكون متصلا بجهاز الضحية عبر شبكة الإنترنت، وفي نفس اللحظة لأن هذا الرقم يتغير مع كل اتصال جديد.[2]

وللحد من تزايد عمليات الاختراق وهي الاستعانة بخبرات بعض محترفي التسلل ذلك لأن المتسللون عادة يطورون تقنياتهم بصفة مستمرة ويملكون مهارات متقدمة ، لهذا فقد اضطر مسؤولي أمن الحاسبات الآلية وشبكات الإنترنت وكذلك رجال الأمن بالاستعانة بخبرة هؤلاء المحترفون ليستطيعوا تطوير الحماية ضد هذه الفئة من المتسللين.

[1] (AD): Adresse هو الرقم الخاص بصاحب النظام أو الحاسوب ويشترط الوصول إلى هذا الرقم بمجموعة من الخطوات، لأن هذا الرقم يتغير مع كل إتصال جديد، ويتطلب تشغيل نظم اتصالات الكمبيوتر أن تكون هناك آلية من أجل عنونة الأجهزة سواء المرسلة أو المستقبلة كما يتطلب أن تكون آلية من أجل لضمان وصول أو التحقق من وصول اتصال أو الرسالة للجهة المقصودة والتحق من جهة الإرسال، بن مكي نجاة، مرجع سابق، ص56.

[2] بن مكي نجاة، مرجع نفسه، ص56-57.

المبحث الثاني: حماية المعلومات وفقا للقوانين المستحدثة:

نظرا إلى الطبيعة الخاصة التي تمتاز بها الجرائم الماسة بالمعلومات، فإن القواعد العادية للحماية لن تحقق ثمارها وذلك بسبب عدم تماشي القواعد التقليدية للحماية مع التطور المستمر لهذا النوع من تقنية المعلومات، وتطور وسائل وطرق الاعتداءات،فقد تأثر المشرع الجزائري بالجدال العالمي الذي أفرزته التطورات المذهلة لأنظمة المعلوماتية واعتبر المساس بها جرائم أدرجها في القسم السابع مكرر من قانون العقوبات المعدل والمتمم بالقانون (05/04) المؤرخ في 2004/11/10[1] المساس بأنظمة المعالجة الآلية للمعطيات وذلك في المواد من 394 مكرر إلى 394 مكرر 7، لذا سيتم التعرف على أنواع هذه الجرائم، و العقوبات المقررة لها وذلك في المطلب الأول، أما المطلب الثاني سيتم التطرق فيه إلى جريمة التلاعب بمعطيات الحاسب الآلي والعقوبات المقررة لها.

[1] القانون رقم (15/04) المؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم (66-156) المتعلق بقانون العقوبات الجزائري، الجريدة الرسمية رقم71.

المطلب الأول: جريمة الدخول أو البقاء غير المشروع:

لقد تم تصنيف هذه الجريمة تحت باب الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي، وتم البدء بهذه الجريمة في هذه الدراسة لأنها تعتبر أهم الجرائم أو بالأحرى يعد الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي المرحلة السابقة والضرورية لارتكاب الجرائم المعلوماتية الأخرى مثل سرقة المعلومات، وللتفصيل في هذه الجريمة سنتطرق إلى جريمة البقاء غير المشروع في الفرع الثاني أما الفرع الثالث فسنتطرق إلى العقوبات المقررة لجريمة الدخول أو البقاء غير المشروع.

الفرع الأول: جريمة الدخول غير المشروع:

تنص المادة 394 مكرر من قانون العقوبات الجزائري على معاقبة كل من يدخل عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك [1]، وتضاعف العقوبة إذا ترتب على الدخول أو البقاء حذف أو تغيير معطيات المنظومة أو تخريب النظام، كما نصت "اتفاقية بودابست"[2] على هذه الجريمة في المادة الثانية تحت عنوان "الدخول غير القانوني" والتي تشير إلى أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقا للقانون الداخلي الولوج العمدي لكل أو جزء من جهاز الحاسب الآلي دون حق.

و للتعرف أكثر على هذه الجريمة وجب التطرق إلى ركنيها المادي وكذا المعنوي فيما يلي:

أولا: الركن المادي:

يتكون الركن المادي لهذه الجريمة من نشاط إجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه، ولم يحدد المشرع الجزائري المقصود بالدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات.حيث يتمثل الدخول في الاتصال بنظام الكمبيوتر بأي طريقة كانت وعادة ما يقصد الفاعل بذلك الاطلاع على المعلومات التي يحتويها هذا النظام.[3]

---

[1] المادة 394 مكرر من قانون العقوبات.

[2] اتفاقية بودابست المبرمة في 08 نوفمبر سنة 2001 والخاصة بحماية المعلوماتية ومنع وقمع الإجرام المعلوماتي.

[3] بن مكي نجاة، مرجع سابق، ص179.

ويتحقق الدخول غير المشروع كذلك متى كان مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه، كذلك الأنظمة المتعلقة بأسرار الدولة أو دفاعها أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة ولا يجوز الاطلاع عليها، ومن صور الدخول غير المشروع كذلك أن يكون مالك النظام قد وضع قيودا للدخول إلى ذلك النظام ولم يحترم الجاني هذه القيود أو كان الأمر يتطلب سداد مبلغ من النقود والجاني لم يسدده، وقام بالدخول غير المشروع إلى هذا النظام.[1]

فالمشرع في هذه الجريمة يعاقب على الدخول المجرد إلى النظام المعلوماتي وفق ما يلي:

- بمجرد الدخول تقوم به جريمة حتى ولو لم يترتب على دخوله ضرر، أو يتحقق من وراء الدخول فائدة كسرقة معلومات مثلا، طالما أن ذلك غير مشروع أي عن طريق الغش، فالدخول في حد ذاته يجب أن يكون عن طريق الغش.
- و الملاحظ أن هذه الجريمة من جرائم السلوك الشكلية، أي يتحقق الجرم بمجرد ارتكاب الفعل المجرم دون اشتراط تحقق نتيجة معينة، فالسلوك مجرم في حد ذاته.
- جريمة الدخول غير المرخص به تتحقق بمجرد الدخول أو محاولة الدخول من ليس له الحق أيا كانت صفته في كل أو جزء من نظام المعالجة الآلية للمعطيات، وإذا ترتب على الدخول غير المرخص به حذف أو تغيير لمعطيات المنظومة أو تخريب أشغالها فإن المادة 394 مكرر 21 نصت على مضاعفة العقوبة.[2]

[1] نهلا عبد القادر المومني، مرجع سابق،ص158.

[2] علي محمد جعفر، شرح قانون العقوبات، طبعة 2، مجد المؤسسة الجامعية النشر والتوزيع ،بيروت،2004، ص224.

ثانيا: الركن المعنوي:

تنص المادة 394 مكرر من القانون صراحة على وجوب كون جريمة الدخول، جريمة عمدية ويستشف ذلك من قولها:" كل من يدخل أو يبقى عن طريق الغش، فالقصد الجنائي المطلوب في هذه الجريمة هو القصد الجنائي العام بعنصريه العلم والإرادة."

1. **العلم** : هو أن ينصرف علم الجاني إلى كل واقعة تدخل في تكوين جريمة الدخول وأول ما يجب أن ينصرف إليه علمه هو موضوع الحق المعتدي عليه، فلابد أن يعلم الجاني أن فعله ينصب على نظام المعالجة الآلية للمعطيات وليس على شيء آخر. و كذلك لابد أن يعلم هذا الأخير أنه يقوم بالدخول إلى هذا النظام من غير تصريح أي بصفة غير مشروعة.

2. **الإرادة:** هي التي تبين الموقف النفسي للفاعل من سلوكه ومن النتيجة المترتبة عليه، وبما أن جريمة الدخول غير المصرح به ، جريمة شكلية لا يتطلب لقيامها نتيجة معينة،فإن الإرادة فيها تقتصر على السلوك الإجرامي فتستغرقه بكل مقوماته.[1]

اعتبر المشرع الجزائري مجرد الدخول إلى برنامج أو نظام معلوماتي دون موافقة صاحب البرنامج وبطريقة غير شرعية، جريمة تستوجب العقاب لأن فيه اعتداء على صاحب الحق وبرامجه.

الفرع الثاني:جريمة البقاء غير المشروع:

يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام وقد يجتمعان معا، ويكون البقاء معاقبا عله استقلالا حين يكون الدخول إلى النظام مشروعا،و مثال ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السمو في هذه الحالة يجب على المتدخل أن يقطع وجوده وينسحب فورا، ولقيام هذه الجريمة لابد من توافر ركنيها المادي والمعنوي فيما يلي:

أولا: الركن المادي: يتخذ النشاط الإجرامي الذي يتكون منه هذا الركن في جريمة البقاء صورة الوجود داخل نظام المعالجة الآلية للمعطيات بالمخالفة لإرادة الشخص صاحب النظام، أو من له السيطرة عليه.[2]

[1] علي محمد جعفر، مرجع سابق، ص226.

[2] بن مكي نجاة، مرجع سابق، ص183.

وفقا لهذا يعد من صور فعل البقاء المعاقب عليه أن يظل الجني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله، أو في حالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والاطلاع فقط.

ثانيا: الركن المعنوي : هذه الجريمة مثل جريمة الدخول غير المصرح به لابد من توافر القصد الجنائي العام فيجب أن يعلم الجاني أنه يتحول في نظام المعالجة الآلية للمعطيات و أن تتجه إرادته إلى البقاء في هذا النظام.[1]

ويتوافر الركن المادي الذي يتخذ صورة البقاء داخل النظام المعلوماتي والركن المعنوي المتمثل في القصد الجنائي تقوم جريمة البقاء غير المصرح به، فإن عملية الدخول إلى أنظمة الحاسبات الآلية.

والبقاء فيها هي عمليات تنكر بشكل مذهل في اليوم الواحد، ولو كانت جريمة الدخول أو البقاء غير عمدية لوقع الكثير من مستعملي هذه الشبكة والحاسب الآلي تحت طائلة العقاب، وعلى هذا كان من اللازم أن تكون هذه الجريمة عمدية من أجل الموازنة بين حماية خصوصية الأنظمة المعلوماتية وحماية حرية الأفراد في استخدام الإنترنت.[2]

[1] آمال قارة، مرجع سابق، ص 121.

[2] نائلة محمد فريد قورة، مرجع سابق،ص 317.

الفرع الثالث: العقوبات المقررة لجريمة الدخول أو البقاء غير المصرح بهما:

تتخذ جريمة الدخول أو البقاء غير المصرح بهما صورتين لكل منهما عقوبتها الأولى بسيطة أو مجردة والثانية مشددة، وعليه سنتطرق إلى العقوبات الأصلية لهذه الجريمة في صورتها "أولا" أما "ثانيا" سنتطرق إلى العقوبات التكميلية.

أولا: العقوبات الأصلية : تقرر الفقرة الأولى من المادة 394 مكرر عقوبتين أصليتين لمرتكب جريمة الدخول أو البقاء غير المصرح بهما، وتشدد الفقرة الثانية من نفس المادة عقوبة هذه الجريمة، إذا نجمت عنها نتائج معينة، لذا سيتم التطرق إلى العقوبات في الجريمة البسيطة ثم في الجريمة المشددة.[1]

1- العقوبات الأصلية لجريمة الدخول أو البقاء غير المصرح بهما في صورتها البسيطة:

بالرجوع إلى المادة 394 مكرر من قانون العقوبات الجزائري نجد للاعتداء العمدي على المعطيات الموجودة داخل النظام المعلوماتي هي الحبس من 6 أشهر إلى 3 سنوات وعقوبة الغرامة التي تتراوح بين 500.000 إلى 2.000.000 دينار جزائري.

و الملاحظ أن جريمة التلاعب بالمعطيات تفوق عقوبة جريمة الدخول أو البقاء غير المصرح بهما سواء كانت هذه الأخيرة في صورتها البسيطة أم المشددة، لأن في صورتها البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو نظام معالجتها، وحتى في صورتها المشددة وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي إزالة المعطيات أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب بالمعطيات تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجنائي للتلاعب، فالموقف النفسي لكل واحد منهما له اتجاه مختلف للتلاعب.[2]

ثانيا: عقوبات تكميلية: أقر المشرع الجزائري عقوبة تكميلية لجريمة التلاعب بالمعطيات وهذا وفق غرامة مالية قدرها ما بين 500.000 و2.000.000 دينار جزائري.[3]

---

[1] بن مكي نجاة، مرجع سابق، ص185.

[2] عبد الفتاح بيومي حجازي، مرجع سابق، ص54.

[3] آمال قارة، مرجع سابق، ص125-126.

المطلب الثاني: جريمة التلاعب بمعطيات الحاسب الآلي:

نصت عليها المادة 394 مكرر 1 من قانون العقوبات بعد جريمة الدخول والبقاء غير المصرح بهما، لأن جريمة التلاعب الحاسب الآلي ثاني أهم أخطر الجرائم الواقعة على النظام المعلوماتي بمعطيات الحاسب في "الفرع الأول" وإلى العقوبات المقررة لها في "الفرع الثاني"وإلى المواجهة وفقا للقانون 04/09 في "الفرع الثالث" أما "الفرع الرابع "إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال.

الفرع الأول: أركان جريمة التلاعب بمعطيات الحاسب الآلي:

يعتبر التلاعب بمعطيات الحاسوب جريمة عمدية معقب عليها قانونا وتقوم هذه الأخيرة على ركنين أولهما مادي وثانيهما معنوي.

أولا: الركن المادي:

يقوم الركن المادي لجريمة التلاعب بمعطيات الحاسوب على السلوك الإجرامي الذي ينحصر في أفعال الإدخال، والمحو والتعديل، ويكفي توافر أحدهما لقيام الجريمة، فلا يشترط اجتماعهما معا حتى يتوافر النشاط الإجرامي فيها، لكن القاسم المشترك في هذه الأفعال جميعها هو انطوائها على التلاعب في المعطيات التي ينظمها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل أخرى قائمة.[1]

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص44.

وسيتم التطرق فيما يلي إلى كل واحد من هذه الأفعال والنتيجة المترتبة عليه:

- **فعل الإدخال:** يقصد به إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أم يوجد عليها معطيات من قبل ويتحقق فعل الإدخال كل حالة يتم فيها إدخال برنامج غريب مثل فيروس حصان طروادة.
- **فعل التعديل** : يقصد بالتعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، وذلك بإمداده بمعطيات مغايرة تؤدي لنتائج عن تلك التي صمم البرنامج لأجلها.
- **فعل الإزالة:** تعرف الإزالة بأنها محو جزء من المعطيات المسجلة عل دعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.[1]

وعملية إزالة المعطيات هي مرحلة لاحقة على عملية إدخال المعطيات، فالإزالة تفترض الوجود السابق لعملية الإدخال، وكقاعدة عامة،فإن صور الركن المادي في جريمة الاعتداء على نظام المعالجة الآلية للمعطيات، يتم عن طريق برامج تتلاعب هذه في المعطيات وذلك بمحوها كليا أو جزئيا، أو تعديلها عن طريق برامج الفيروسات، لاسيما أن الفيروس يصممه مجرم معلوماتي على درجة عالية من الذكاء.

وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل جاءت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر.[2]

النتيجة الإجرامية: إن معظم الجرائم الواقعة على المعطيات جرائم خطر لا يشترط لوقوعها بأن يترتب على السلوك الإجرامي عدوان فعلي على المعطيات، وإنما يكتفي التهديد بالخطر الفعلي على المعطيات في سريتها أو إتاحتها، إذ لا يكتفي أن تهدد سلامة المعطيات بخطر الإزالة أو

[1] عبد الفتاح بيومي الحجازي، مرجع سابق، ص51.

[2] عبد الفتاح بيومي حجازي، مرجع نفسه،ص54.

التعديل أو الإدخال وإنما لابد أن يقع ضرر فعلي على هذه المعطيات يتمثل في تغيير حالتها. فالمشرع يتطلب نتيجة معينة من خلال السلوك الإجرامي في هذه الجريمة وهو تغيير حالة المعطيات.

ثانيا:الركن المعنوي:

هذه الجريمة من الجرائم العمدية التي يقوم عليها القصد الجنائي العام بركنيه العلم والإرادة فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، ويعلم بأن نشاطه غير مشروع وأنه يعتدي على صاحب الحق في المعطيات محل الاعتداء ومع ذلك تتجه إرادته رغما عن إرادة صاحب الحق في المعطيات أو من له السيطرة عليها.[1]

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام، نية الغش إذن هذا لا يعني ضرورة توافر قصد الإضرار بالغير، بل تتوافر الجريمة ويتحقق ركناها بمجرد الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إلى ذلك.

مما سبق يتضح أن المشرع الجزائري من خلال نص المادة 394 مكرر 1 من قانون العقوبات الجزائري أراد أن يوفر الحماية الجنائية للمعطيات الموجودة بالنظام المعلوماتي ضد أي نشاط إجرامي.

الفرع الثاني: العقوبات المقررة لجريمة التلاعب بالمعطيات:

يقرر قانون العقوبات الجزائري في مادته 394 مكرر 1 على مرتكب جريمة التلاعب بالمعطيات عقوبة أصلية تتمثل في الحبس والغرامة، كما تقرر عليه المادة 394 مكرر 6 عقوبة تكميلية تشترك فيها مع باقي جرائم المعطيات، فيما يلي سيتم التطرق إلى العقوبات الأصلية في "أولا" لتليها العقوبات التكميلية في "ثانيا" .

أولا: العقوبات الأصلية: طبقا لنص المادة 394 مكرر1 [2] فالعقوبة الأصلية المقررة أن كلا من الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات والبرامج والتلاعب بها لا يتطلبان نتيجة

[1] عمر أبو الفتوح عبد العظيم المحامي، الحماية الجنائية المسجلة إلكترونيا، دون طبعة، دار النهضة العربية، 2016، ص560.
[2] بن مكي نجاة، مرجع سابق، ص186.

معينة كالوصول إلى المعطيات والتلاعب بها، فإذا لم ينجم عن الدخول أو البقاء غير المصرح بهما إعاقة أو إفساد نظام المعالجة الآلية للمعطيات أو إزالة أو تعديل لمعطياته، فإن العقوبة تكون الحبس من ثلاثة أشهر إلى سنة والغرامة من 50.000 إلى 10.000 دينار جزائري.

وقد جعل المشرع للقاضي حدا أدنى وحد أقصى للعقوبة حتى تكون له سلطة تقديرية في تفردها.

بحسب ما تتطلبه الحالة المعروضة أمامه، ذلك بواعث ارتكاب هذه الجريمة كثيرة، وليس باعث الاكتشاف والفضول كباعث الربح، وغيرها كثير من الظروف الخاصة بكل فاعل وبكل جريمة مما يقتضي أن تفرد العقوبة.

و الملاحظ أيضا أن الحد الأدنى وكذا الحد الأقصى منخفض، وتفسير ذلك أن المشرع يسمح بفترة تحذير للناس بلغة يفهمها الجميع حول المستهدف من القانون ورد الفعل حال تخطي حدوده، ولأن هذه الجرائم حديثة تستدعي المرور بفترة التحذير.[1]

ثانيا: العقوبات الأصلية لجريمة الدخول أو البقاء غير المصرح بهما في صورتها المشددة: تشدد الفقرتين الثانية والثالثة من المادة 394 مكرر من قانون العقوبات الجزائري عقوبة جريمة الدخول أو البقاء غير المصرح بها إذا نجم عن هذا الفعل، إما محو أو تعديل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه.

فترفع العقوبة إلى ضعف تلك المقررة للجريمة البسطة، سواء في حدها الأدنى الذي تضاعف من ثلاثة أشهر إلى 06 أشهر، أو في حدها الأقصى الذي تضاعف كذلك من سنة واحدة إلى سنتين، أما الغرامة فثبت حدها الأدنى عند 50.000 دينار جزائري وارتفع حدها الأقصى إلى 150.000 دينار جزائري وذلك فيما إذا أدى الدخول والبقاء إلى حذف أو تغيير المعطيات، أما إذا أدى الدخول أو البقاء إلى تخريب النظام فالغرامة تشدد إلى لضعف أي تتراوح من 100.000 إلى 200.000 دينار جزائري.

[1] آمال قارة، مرجع سابق، ص113.

انطلاقا مما سبق ذكره يتبين جريمة الدخول أو البقاء غير المصرح بهما لابد لقيامهما أن يكون النظام مفتوحا لأشخاص محددين كما أن نص المادة 394 مكرر تتضمن صورتين للركن المادي لهذه

الجريمة هي الصورة البسيطة للدخول أو البقاء غير المشروع، وكذا صورة مشددة للعقاب عليها تتضمن ضعف العقوبة المقررة للجريمة في صورتها البسيطة.[1]

الفرع الثالث:المواجهة وفقا للقانون 04/09 المتضمن القواعد العامة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

إن تفاقم الاعتداءات على معطيات الحاسب الآلي خاصة مع ضعف الحماية الفنية، استدعى تدخل تشريع صريح، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]

وتضمن هذا القانون 19 مادة في ستة فصول وفيما يلي سيتم التطرق إلى الإجراءات الخاصة بحماية معطيات الحاسب الآلي وفق: "أولا" التحفظ المعجل على البيانات المخزنة، "ثانيا" الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك.

أولا: التحفظ المعجل على البيانات المخزنة: هذا الإجراء يعد أداة تحقيق مستحدثة ويقصد به توجيه السلطة المختصة لمزودي الخدمات، الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته وتحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش، أو الأمر بتقديم بيانات معلوماتية ويتضح أن التحفظ هو إجراء تمهيدي الهدف منه هو محاولة الإحتفاظ بالبيانات قبل فقدانها.

ثانيا: الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك: الأصل أن البيانات الشخصية المتعلقة بمستخدمي الشبكة تدخل في إطار الحق في الخصوصية غير أنه يسمح لرجال الضبط القضائي بأن يأمر الأشخاص بتسليم ما تحت أيديهم من موضوعات يطلب تقديمها كدليل ومن بينها البيانات المتعلقة بالمشترك التي يحوزها مزودو الخدمات.

[1] آمال قارة، مرجع سابق، ص114.

[2] القانون رقم 09-04 مؤرخ في 14شعبان عام 1430 الموافق لـ 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية العدد 47.

الفرع الرابع: إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

نصت المادة 13 من القانون 09-04 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والتي تعد سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أعضاء من الحكومة معنيين بالموضوع و مسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، وتضم الهيئة قضاة وضباطا وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك الوطني والأمن الوطني ، وتكلف الهيئة بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وضمان مراقبة الاتصالات الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئة وطنية أخرى.[1]

التعاون والمساعدة القضائية الدولية: من أجل مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ساهمت الجزائر كغيرها من الدول بدورها الفعال من خلال ما سيتم التطرق له في "أولا" الاختصاص القضائي، "ثانيا" المساعدة القضائية الدولية المتبادلة.

أولا: الاختصاص القضائي: أشارت المادة 15 من القانون 04/09 إلى أن المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.[2]

ثانيا: المساعدة القضائية الدولية المتبادلة: نصت المادة 16 من ذات القانون إلى أنه في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

[1] المادة 14: تتولى الهيئة المذكورة في المادة 13 أعلاه خصوصا المهام التالية:أ- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكافحته. ب- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال.

[2] المادة 14 من قانون العقوبات 04/09.

وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، كما يمكن في حالة الاستعجال ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية.[1]

[1] بن مكي نجاة، مرجع سابق، ص232-233.

الخاتمة

الـخاتمة

أصبحت المعلوماتية سمة العصر، وبات استخدام الأنظمة المعلوماتية من قبل الأفراد المقياس الذي يحدد مدى تطور الشعوب وتقدمها فتكنولوجيا المعلومات تساهم في تسريع انجاز الأعمال، الأمر الذي يعني تنفيذ الأهداف والخطط التي ترسمها الدول لتحقيق التنمية الاقتصادية والاجتماعية والسياسية في وقت قياسي ومن هنا أصبح لزاما على الدول من أجل ضمان نهضتها وتماشيا مع عصر المعلوماتية ، أن يعمل على مواكبة التطور التكنولوجي والالكتروني الذي نجم عن تحويل العديد من المجتمعات إلى مجتمعات معلوماتية تعتمد على التقنية الرقمية في أداء أعمالها.

إلا أن عصر المعلوماتية خلف ورائه آثارا سلبية نجمت عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية في غير الغرض الذي خلقت من أجله، الأمر الذي أثر على حقوق الأفراد وحرياتهم، حيث وفرت الأنظمة المعلوماتية وسيلة جديدة في أيدي مجرمي المعلوماتية، لتسهيل ارتكاب العديد من الجرائم، كما أضحى النظام المعلوماتي ذاته محلا للاعتداء عليه وإساءة استخدامه.

هدد وبالفعل الحياة العامة والخاصة للأشخاص من خلال جرائم مستحدثة مست معلومات الشخص أو ما يعرف بأسراره، والتي لا يرغب في أن يعلم بها غيره، وبالرغم من ذلك توالت التعديلات القانونية اللازمة لمواجهة تلك الجرائم المستحدثة المتعلقة بكل أشكال الاعتداء على المعلومات، فعلى المستوى الوطني فقد أصدر المشرع الجزائري نصوص خاصة في قانون العقوبات قصد مواجهة هذا النوع الخطير من العقاب، كما تم استصدار القانون 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الذي بدوره يتضمن عدة نصوص للحد من الجرائم المعلوماتية، كذلك على المستوى الدولي نجد "اتفاقية بودابست" التي أبرزت معظم أصناف هذا الإجرام، و على هذا الأساس، و من خلال دراسة موضوع سرقة المعلومات المخزنة في الحاسب الألي تم التوصل الى أهم النتائج كمايلي:

-ان سرقة المعلومات المخزنة في الحاسب الألي تعد من أخطر الجرائم، اذ تتم هذه الجريمة بسرعة فائقة، و دون سابق انذار، مما يصعب معرفة مرتكبيها.

-تعتبر جريمة المعلوماتية وسيلة اعتداء، و فعل غير مشروع ضد نظام المعالجة الألية للمعطيات.

-تختلف الجريمة المعلوماتية عن غيرها من الجرائم، و ذلك لأنها تتطلب لارتكابها وجود حاسب ألي، و هذا الأخير يعتبر وسيلة اتصال و تواصل، هذا ما يجعله عرضة لمثل هذه الجرائم من السرقة.

-لقد وفق المشرع الجزائري حينما نص على الجريمة المعلوماتية و سماها بجرائم الاعتداء على نظام المعالجة الألية للمعطيات.

-يتصف الجرم المعلوماتي بمهارة لا مثيل لها، حيث أنه يستخدم قدرته العقليةفي سرقة المعلومات المخزنة، الهدف منها الرغبة في التعلم، أو الرغبة في تحقيق مكاسب مادية، أو الرغبة في الانتقام، الى غير ذلك من الأهداف المتوخاة من ارتكاب هذه الجريمة.

و على اثر هذه النتائج المتوصل اليها، فانه يمكننا تقديم بعض التوصيات منها:

-يجب على المشرع تخصيص مواد ردعية و أكثر صرامة للحد من هذه الجريمة التي أضحت خطرا على الحياة الاجتماعية و الاقتصادية.

-تكوين دوري للخبراء في مجال التكنولوجيا حتى يتماشى مع التطور المعلوماتي.

-العمل على تطوير البرامج خاصة بالفيروسات، و وضع برامج للانذار على وجود خطر.

-انشاء هيئات متخصصة في التصدي لجريمة السرقة المعلوماتية.

-توعية المجتمع من خلال حصص تلفزيونية، أو عن طريق وسائل الاتصال على اختلافها، و حتى المدارس و الجامعات عن طريق ندوات، بخطورة الجرائم المعوماتية، و ضرورة اعطاء حلول للتصدي لها.

ملخص الدراسة

تطرقنا في هذه الدراسة إلى موضوع حديث وهو سرقة المعلومات المخزنة في الحاسب الآلي، والتي تعتبر جريمة معلوماتية خطيرة، وتهدف هذه الدراسة إلى التعرف على الجريمة المعلوماتية من حيث ماهيتها وخصائصها وسماتها المتمثلة في المجرم المعلوماتي، كما تم تسليط الضوء في هذا البحث على الحاسب الآلي بإعتباره أداة فعالة لارتكاب الجريمة المعلوماتية، وأهم الجرائم الواقعة على نظم المعالجة الآلية للمعطيات والعقوبات المقررة لها، وتجلى محور هذا البحث دور المشرع الجزائري في
مكافحة الجرائم المعلوماتية من خلال استصداره لعقوبات رادعة في هذا المجال.

Study summary

In this study we dealt with the optic of stealing information stored from the computer ,which is considred an information crime in terms of what it is and its characteristics and characteristics represented by the information criminal.
The automatic processing of data and the penalities prescribed for them. The focus of this research revealed the role of the algerian legislator in combating information crimes by calling him for deterrent penalties in this field.

المصادر والمراجع

1/-قائمة المصادر

- القرآن الكريم

- القانون 15/04 المؤرخ في 10 نوفمبر2004، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد 47 بتاريخ 16 أوت 2009.

- القانون 15/04 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات.

- القانون رقم 04/09المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 المتضمن القواعد الخاصة بتكنولوجيات الإعلام والإتصال ومكافحتها.

- القانون رقم 05/04 المؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم (156//66) المتعلق بقانون العقوبات الجزائري الجريمة الرسمية رقم 71.

الإتفاقيـــات

-اتفاقية بودابست المبرمة في 08 نوفمبر 2001 والخاصة بحماية المعلومات ومنع وقمع الإجرام المعلوماتي.

الكتب العامة

- أحسن بوسقيعة، الوجيز في القانون الجنائي القسم العام، دار هومة للنشر والتوزيع، الجزائر، 2010.

- أيمن عبد الحفيظ ، *الإتجاهات الأمنية والفنية لمواجهة الجرائم المعلوماتية.* دار النشر.2005.

- أمين لعياش. *الحماية الجنائية للمعاملات الإلكترونية .* مكتبة الوفاء القانونية الإسكندرية.مصر.

- أحمد عبد الرزاق السنهوري، *الوسيط في شرح القانون المدني، حق الملكية، الجزء الثاني.* بيروت: دار إحياء،1952 .

- بن مكي نجاة ، *السياسة الجنائية لمكافحة الجرائم المعلوماتية.* خنشلة ،جامعة عباس لغرور، 2017.

الكتب المتخصصة

– آمال قارة. *الحماية الجزائية للمعلوماتية في التشريع الجزائري والدولي* ، دار الهدى – الجزائر–.

– خثير مسعود. *الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات*. عين مليلة – الجزائر–: دار الهدى للطباعة والنشر والتوزيع.2010.

– رابحي عزيزة.الأسرار المعلوماتية وحمايتها الجزائرية . أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص . أبو بكر بلقايد – تلمسان –: كلية الحقوق والعلوم السياسية– قسم القانون الخاص –2018 .

– زبيدة زيدان. *الجريمة المعلوماتية في التشريع الجزائري والدولي*. الجزائر.

– زينات طلعت شحادة. *الأعمال الجرمية التي تستهدف الجريمة المعلوماتية*. لبنان: المنشوررات الحقوقية.2006.

– عبد الفتاح بيومي حجازي. *مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي*. الإسكندرية، الطبعة الأولى: دار النهضة العربية،2009.

– علي عبد القادر القهوجي. *الحماية الجنائية لبرامج الحاسب الآلي*. الإسكندرية: الدار الجامعية للنشر والتوزيع،1992.

– علي محمد جعفر. *قانون العقوبات، الطبعة الثانية*. بيروت: مجد المؤسسة الجامعية للنشر و التوزيع.،2004.

– عمر أبو الفتوح عبد العظيم المحامي. *الحماية الجنائية المسجلة الكترونيا*. دار النهضة العربية.2016.

– محمد احمد عباينة. *جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى*. عمان الأردن: دار الثقافة للنشر والتوزيع.2009.

– محمد عبد الله بو بكر سلامة. *جرائم الكمبيوتر والإنترنت*. الإسكندرية: منشأة المعارف.مصر.2006.

– نائلة محمد فريد قورة. ***جرائم الحاسب الآلي الإقتصادية.*** **منشورات الحلبي الحقوقية.بيروت.2005.**

– نهلا عبد القادر المومني. ***الجرائم المعلوماتية.*** **دار الثقافة للنشر والتوزيع.الأردن،2010.**

فهرس المحتويـات

شكرو تقدير	**ا**
الإهداء	**II**
مقدمة عامة	**أ-ه**
الفصل الأول:االجريمة المعلوماتية وسماتها العامة	
المبحث الأول:ماهية الجريمة المعلوماتية	**9**
المطلب الأول: تعريف الجريمة المعلوماتية	**10**
الفرع الأول:التعريف الفقهي للجريمة المعلوماتية	**10**
الفرع الثاني:موقف المشرع الجزائري من الجريمة المعلوماتية	**11**
الفرع الثالث:أركان الجريمة المعلوماتية وخصائصها	**12**
المطلب الثاني:خصائص الجريمة المعلوماتية	**15**
الفرع الأول:الجريمة المعلوماتية متعددة الدول	**15**
الفرع الثاني:إنفراد الجريمة المعلوماتية عن الجرائم الأخرى	**10**
الفرع الثالث:تتطلب لارتكابها وجود حاسب آلي ومعرفة تقنية باستخدامه	**16**
المطلب الثالث: الفيروسات المعلوماتية	**16**
الفرع الأول: تعريف الفيروس المعلوماتي وخصائصه	**16**
الفرع الثالث:أنواع الفيروسات المعلوماتية	**17**
المبحث الثاني:الـمجرم الــمعلوماتي	**19**
المطلب الأول:السمات الخاصة بالمجرم المعلوماتي	**20**
الفرع الأول:المجرم المعلوماتي يتمتع بالمهارة والمعرفة و الذكاء	**20**
الفرع الثاني:المجرم المعلوماتي يبرر ارتكاب جريمته	**20**
الفرع الثالث:المجرم المعلوماتي إنسان اجتماعي	**21**
الفرع الرابع:خوف المجرم المعلوماتي من كشف جريمته	**21**
الفرع الخامس:المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي	**22**
المطلب الثاني:الأسباب الدافعة لارتكاب الجريمة المعلوماتية	**22**
الفرع الأول:الرغبة في التعلم	**22**
الفرع الثاني:الدوافع المادية	**23**
الفرع الثالث: المتعة والتحدي	**23**
الفرع الرابع:الرغبة في الانتقام	**23**
الفرع الخامس:دوافع أخرى	**24**
المطلب الثالث:الشبكة العالمية للمعلومات	**24**

الفرع الأول:تعريف الشبكة الدولية للمعلومات.....	24
الفرع الثاني:نشأة وتطور الشبكة العالمية للمعلومات.....	25
الفرع الثالث:خدمات الشبكة الدولية للمعلومات.....	26
خلاصة الفصل الأول.....	28
الفصل الثاني:الجرائم الواقعة بواسطة النظام المعلومات	
المبحث الأول:الحاسب الآلي ودوره في ارتكاب الجريمة المعلوماتية.....	**30**
المطلب الأول:تعريف جهاز الحاسوب.....	30
الفرع الأول:مكونات الحاسب الآلي.....	31
الفرع الثاني:دور الحاسب الآلي في ارتكاب الجريمة المعلوماتية.....	33
الفرع الثالث:التعدي على برامج الحاسب الآلي.....	35
المطلب الثاني:أساليب الاعتداء على المعلومات المخزنة في الحاسوب.....	37
الفرع الأول: سرقة المعلومات من الحاسوب.....	37
الفرع الثاني: الشروط الواجب توافرها في المعلومات لتتمتع بالحماية القانونية.....	38
الفرع الثالث:الاختراق.....	41
المبحث الثاني:حماية المعلومات وفقا للقوانين المستحدثة.....	**42**
المطلب الأول:جريمة الدخول أو البقاء غير المشروع.....	43
الفرع الأول:جريمة الدخول غير المشروع.....	43
الفرع الثاني:جريمة البقاء غير المشروع.....	46
الفرع الثالث:العقوبات المقررة لجريمة الدخول أو البقاء غير المصرح بهما.....	47
المطلب الثاني:جريمة التلاعب بمعطيات الحاسب الآلي.....	49
الفرع الأول:أركان جريمة التلاعب بمعطيات الحاسب الآلي.....	49
الفرع الثاني:العقوبات المقررة لجريمة التلاعب بالمعطيات.....	51
الفرع الثالث: المواجهة وفقا للقانون 04/09 المتضمن القواعد العامة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....	53
الفرع الرابع:إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.....	54
خلاصة الفصل الثاني :.....	55
الخـــــاتمة	58
الــنتائج والتوصيـــات	60
ملخص الدراسة	61
قائمة المصادر والمراجع	62