وزرة التعليم العالي والبحث العلمي

Ministry of High Education and Scientific Research

جامعة محمد البشير الإبراهيمي برج بوعريريج

University of Mohamed el Bachir el Ibrahimi–Bba

كلية الحقوق والعلوم السياسية

Faculty of Law and Political Sciences

مذكرة مقدمة متطلبات لنيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون إعلام آالي وانترنات

الموسومة بـ:

إختراق النظم المعلوماتية

من إعداد الطالب:

- رغيس آسيا
- غربي لويزة

تحت إشراف الدكتور:

- رياح لخضر

لجنة المناقشة:

الإسم واللقب	الرتبة	الصفة
سي حمدي	أستاذ محاضر "ب"	رئيسا
رياح لخضر	أستاذ مساعد "أ"	مشرفا ومقررا
حاجي عبد الحليم	أستاذ مساعد "ب"	ممتحنا

السنة الجامعية: 2022/2021

تشكرات

قال تعالى في كتابه الكريم" ولئن شكرتم لأزيدنكم"

وقوله صلى الله عليه وسلم" من لا يشكر الناس لا يشكر الله "

وبناءا على هذا نشكر الله عز وجل الذي منى علينا بنعمة العلم وأنار لنا دربنا.

كما أخص بالشكر والتقدير و الاهتمام إلى الذي لم يبخل علينا بنصائحه وتوجيهاته من أجل إتمام هذا العمل:

الدكتور رياح لخضر

كما لا يفوتني أن أتقدم بأسمى آيات الشكر و التقدير والعرفان والاحترام للأساتذة أعضاء اللجنة الأفاضل وفي مقدمتهم الأستاذ سي حمدي عبد المؤمن لتفضله قبول رئاسة اللجنة لهذه المذكرة، وكذا الأستاذ حاجي عبد الحليم لقبولهم التقييم و المشاركة في هذه المذكرة ولما بذلوه من جهد ووقت. و أتقدم بشكر خاص إلى كل أساتذتي في كلية الحقوق والعلوم السياسية على دعمهم ومساندتهم طوال المشوار الدراسي.

رغيس آسيا

إهـــــــداء

سبحان الذي كان سببا في النجاح والتوفيق سبحان الذي خلقنا وأنار لنا السير في الطريق المستقيم.

أهدي ثمرة عملي هذا إلى من نزلت في حقهم هذه الآية" وقضى ربك ألا تعبدوا إلا إياه وبالوالدين احسانا".

إلى من أخرجتني إلى النور، وملئت حياتي حبا وحنانا إلى التي حملتني وهنا على وهن، وفصالي في عامين، إلى التي أفاضت علي من فضلها، وكرمها، وغمرتني بودها الصادق إلى أعز إنسانة إلى "**أمي العزيزة**"

إلى من عمل بكد في سبيلي وعلمني معنى الكفاح وأوصلني إلى ما أنا عليه، أدامه الله لي "**أبي الكريم**"

إلى من كن الرفيقات الصديقات والأخوات، "أخواتي" الكتابة لا تكفي لأصف كيف أشكركم، أراكم بسمتي وأرى جمال الأيام أنتم.

إلى الأخ الذي لم تلده أمي وله كل الشكر و التقدير زوج أختي .

إلى من ساهموا في مساعدتي في إتمام هذه المذكرة من قريب أو من بعيد، إلى أفراد أسرتي صغيرا و كبيرا كل واحد باسمه وإلى كل من سقط عن قلمي سهوا.

رغيس آسيا

قائمة المختصرات

ج ج د ش	الجمهورية الجزائرية الديمقراطية الشعبية
ج ر	الجريدة الرسمية
ص	الصفحة

مقدمـــــــة

مقدمة:

يولد الإنسان وهو على الفطرة السليمة التي لا تعرف الأذى أو الإجرام، وتساهم البيئة المحيطة به في تشكيل شخصيته والتأثير فيه، وقد يتعرض بعض الأشخاص لتأثير سلبي من قبل البيئة المحيطة بهم، مما يجعلهم ينحرفون نحو السلوكيات غير الجيدة، وارتكاب الممارسات غير المقبولة بالنسبة لإنسان سوي، مما يقودهم إلى الجرائم.

تعتبر الجريمة هي الانحراف عن المألوف والطبيعي في المجتمع بحيث تختلف العديد من المعايير الجمعية التي تتصف بكم كبير من الكلية والتوعية والجبرية، وهذا هو التعريف القانوني الأكاديمي للجريمة، وهي أيضا الاتيان بفعل يتنافى مع المعايير المعية والقانونية والدستور أيضا، مثل التعدي على حقوق الآخرين إما بالقتل والسرقة أو الجرائم المختلفة مثل الجرائم المالية و الجنسية، وهي جرائم يتم الاعتداء على الغير من خلالها وأيضا جرائم الانتقام، ويشار أن للجريمة نظريات أساسية، وارتبطت مع التحولات الجغرافية، والاقتصادية، والبيولوجية.

ومع ظهور الدولة تولت بنفسها سلطة تجريم الأفعال والعقاب عليها، حيث أصدرت تشريعات منها ما هو موضعي" قانون العقوبات"، الذي يجرم الأفعال ويحدد العقوبات عليها، ومنها ما هو إجرائي "قانون الإجراءات الجزائية" الذي يحدد الإجراءات الواجب إتباعها أمام الهيئات القضائية وكذا الضبطية القضائية، دون أن ننسى أن الشريعة الاسلامية المناسبة لكل مكان و زمان.

ومن التحولات التامة التي شهدها عصرنا والتي ساهمت في ارتقاء البشرية إلى المستويات عليا، ما يسمى بالثورة المعلوماتية، وهير الثورة التي تزاوجت فيها شبكات الاتصال بما وصلت إليه من تطور مع الحاسوب ذاك الجهاز الذي يمتلك قدرات هائلة للقيام بالعديد من المهام والوظائف في ظرف صغير وقياسي.

هذا التمازج الذي مكن الكثير من البشر الاتصال ببعضهم البعض وأتيح لهم الفرص للاطلاع على المعلومات وتبادلها، الاستطاعة على التفاوض وإبرام العقود والصفقات وظل بيئة تحاكي واقع البشرية وهي البيئة الافتراضية أو الرقمية ،وتقديم الخدمات كالاستشارات الاقتصادية والقانونية و الطبية والتجارية...مثل ما كان لها دورا ايجابي في تغيير نمط حياة الشعوب التي ساهمت في رقييها ،وحيث استطاعت أن تجمع بين مختلف وسائل الاعلام في وسيلة واحدة. كما أنها حولت عالمنا هذا إلى قرية صغيرة بدون حواجز يتبادل الناس فيها أخبارهم ويبدون أراءهم وتعليقاتهم بكل حرية ويحصلون فيها على أية معلومات عبر الأنترنت ونقصد بالأنترنت" هي شبكة عالمية تجمع بين وسائل الاتصالات والحواسيب، وهي مخصصة لتبادل البريد الالكتروني للمعلومات متعددة الوسائل و الملفات وهي تشتغل وفقا لبروتوكول مشترك ، يسمح بسيرورة إرسال الرسائل المنقسمة إلى طرود مستقلة" كما تعرف أيضا بأنها الشبكة المعلوماتية الدولية،" بقدر ما كان دورها ايجابيا بقدر ما يكون دورها سلبي أثر على حياة الناس ومصالحهم ومصالح الدول نتيجة اساءة البعض استخدام هذه التكنولوجيا وغيرها من الوسائل الالكترونية لارتكاب صور جديدة للإجرام كنسخ تلك المصنفات أو التعديل فيها وتوزيعها على الشبكة العنكبوتية دون ترخيص بذلك من صاحب الحق وهو ما سمي بالجرم المعلوماتي أو الجرائم الالكترونية وينجر عنها

إن الجرائم المعلوماتية أو الالكترونية هي ظاهرة من الظواهر الإجرامية تدق ناقوس الخطر لتنبيه المجتمع عن مدى وحجم المخاطر والخسائر التي من الممكن أن تنجر عنها وأنها من الجرائم التي تنشأ في بيئة معلوماتية تتميز بالتطور خلافا عن الجرائم التقليدية، والتي تتسم بالسرعة و التقدم وعلى إثر هذا تعددت أنواع الجرائم المعلوماتية من بينها الاختراق الالكتروني للنظم المعلوماتية.

أهمية البحث:

تكمن أهمية البحث في دراسة ظاهرة جديدة و هي الجريمة المعلوماتية وبالتي لا يمكن تخضع لإجراءات التي تطبق على الجريمة التقليدية من الناحية الإجرائية و الجزائية لاسيما يتميز هذا الموضوع بالحداثة والجدة كما هو الحال في أنواعها وهي الاختراق الذي يعد من بين الأنواع حديثة النشأة ويمتد تأثيرها لجميع الأصعدة لارتباطها بتطور تكنولوجيا الاعلام و الاتصال والتي تستخدم هذه الأخيرة في جميع المجالات الحياة سواء من طرف الأفراد أو المؤسسات إذ تجعل التعاملات معها صعبا و معقدا مما يحتم إيجاد طرق جديدة لمكافحته، على الرغم من الصعوبات التي واجهتنا في إعداد المذكرة نظرا لصعوبة الموضوع و حداثته و تشعبه.

أسباب اختيار الموضوع:

ومن بين أسباب اختيارنا للموضوع هذا ألا وهو جريمة اختراق النظم المعلوماتية يعود إلى عدة أسباب منها شخصية و أخرى موضوعية .

الأسباب الشخصية: تكمن في اهتمامنا بمجال الجريمة المعلوماتية وما يلقاها من جرائم سواء اختراق أو جرائم أخرى وكذا اجراءات خاصة وإن كانت اجراءات المتتابعة فيها كل الاختلاف بالنسبة إلى الاجراءات الجريمة التقليدية اضافة إلى أن اختراق النظم والجريمة المعلوماتية موضوع يتسم بالجدة والحداثة ورغبتها الشديدة في الغوص في مجال المعلوماتية وجرائمها وأخطارها وكذا مكافحتها والوقوف على حقيقة التعامل مع جريمة اختراق النظم المعلوماتية من الناحية الوقائية والاجرائية.

بالنسبة للأسباب الموضوعية فتكمن فيما يطرحه موضوع الاختراق و الحماية الاجرائية والوقائية من اشكاليات قانونية التي لابد من الوقوف نظرا لجدة الموضوع من الجانب الموضوعي للاختراق المعلوماتي والاعتداءات الماسة بأنظمة المعالجة الآلية

للمعطيات، والاجراءات الوقائية و الاجرائية التي جاء بها تعديل الاجراءات الجزائية و قانون العقوبات و قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحته[1].

أهدف من البحث:

يكمن الهدف هذه الدراسة إلى محاولة إعطاء نظرة عامة عن الجرائم الالكترونية وخاصصنا الدراسة لنوع من أنواع هذه الجرائم وهي اختراق النظم المعلوماتية ودور التشريعات الدولية و الداخلية في نظرتها حول هذه الجرائم المستحدثة، التعرف على الجهات المختصة على للحد من الجريمة الالكترونية و جرائم الاختراق المعلوماتي للنظم خاصة، و التعرض بشكل معمق للجوانب الوقائية و الاجرائية الحديثة للحد من جريمة الاختراق المعلوماتي للبيانات الالكتروني التي تختلف بشكل كبير على الجريمة التقليدية.

وكذا معرفة الجوانب الاجرائية المتطورة داخل المنظومة المعلوماتية بالتطرق إلى المراقبة الالكترونية وقواعد التفتيش داخل هذه المنظومة.

إيجاد حلول لتفعيل التعاون الدولي من أجل وضع اتفاقيات دولية لوضع تشريعات دولية لمكافحة اختراق النظم الالكترونية، ووضع معايير لتنظيم استخدام التكنولوجيا المعلومات سواء على المستوى الفردي أو الدولي أو المؤسسات من أجل التعاون الدولي لمنع وقوع الجرائم وتسليم المجرمين.

1 الجمهورية الجزائرية الديموقراطية الشعبية، القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق ل 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها، الجريدة الرسمية ، العدد 47.

الدراسات السابقة:

تناولت بعض الدراسات السابقة جريمة اختراق النظم المعلوماتية و نمن بين هذه الدراسات:

1/ دراسة جمال زين العابدين أمين أحمد (2020) :

بعنوان جرائم اختراق النظم الالكترونية بين التشريع المصري و المغربي.

تكمن أهمية تلك الدراسة في أن جريمة اختراق النظم الالكترونية أصبحت تشكل هاجسا مخيفا و كابوسا مزعجا للكثير من ذوي الشأن و غيرهم و صارت وبكل أسف ظاهرة بدأت بالتشعب وأخذت طريقها في الانتشار، كما يتوجب إعطاء هذه الجريمة أهمية لتوعية الآخرين بمخاطرها، و تتجلى أهميتها في أن الحاسب الآلي هو و الأنترنت من أولويات الحياة.

2/ دراسة إسلام عبد الله محمد عباس (2010):

بعنوان: أمن المعلومات على شبكة الأنترنت واستخدام طريقة حقن لغة الاستعلام الهيكلية في اختراق قواعد بيانات المواقع الالكترونية.

سلطت الضوء هذه الدراسة على ابراز خطورة الاعتداءات على المواقع في الشبكة العنكبوتية ومن أهم الأهداف التي هدفت إليها الدراسة هو: تصميم برامج الاختراق المواقع الالكترونية والتي تعتمد على دوال تصفية المعلومات، والوقوف على المخاطر التي تهدد أمن البيانات وكيفية التعامل معها، وبرزت أهمية هذه الدراسة السابقة إلى أن معظم التطبيقات و المواقع الالكترونية تعتمد على لغة الاستعلام الهيكلية. كما بينا مشكلة البحث أنه مع تطور واسع في استخدام التطبيقات الالكترونية واستعمالها لقواعد البيانات.

ولجدة الموضوع وحداثته مع التطور المعلوماتي الحاصل فإن جريمة اختراق النظم المعلوماتية جريمة مواكبة للعصر مع التقنيات الجديدة، واجهنا صعوبات متعددة في بحثنا وتتمثل قلة المصادر و المراجع نظرا لكونه من المواضيع الجديدة قلة الأبحاث و الدراسات سواء أكان من المنظور الدولي أو الداخلي.

إن كانت ظاهرة جريمة اختراق النظم أثارت بعض المشكلات فيما يتعلق في التشريع الجزائري بحثا عن امكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم، وقد أثارت في الوقت نفسه العديد من المشكلات في نطاق الوقائي و الاجرائي، كما تبدأ مشكلات الاجرائية في مجال اختراق النظم المعلوماتية بتعلقها في الكثير من الأحيان ببيانات المعالجة الالكترونية وكيانات تقنية ليست مادية، ومن ثم يصعب الكشف على هذه الجرائم واثباتها تحسبا للسرعة والدقة العالية غفي تنفيذها وكذا في امكانية مسحها واخفاء آثارها وأدلتها كما تكون اشكالية بحثنا ما مدى كفاية القواعد التقليدية على التحقيق ومكافحة جريمة اختراق النظم المعلوماتية؟ وتتفرع هذه الاشكالية على عدة إشكاليات أخرى:

- ما المقصود بالجريمة المعلوماتية وجريمة اختراق النظم المعلوماتية؟
- بماذا تتميز جريمة اختراق النظم المعلوماتية عن غيرها من الجرائم؟
- هل اجراءات التحري التقليدية المعتادة كافية لردع جريمة الاختراق المعلوماتي أو تم تطويرها؟
- ما هي التدابير الاجرائية والوقائية للكشف وردع جريمة اختراق النظم المعلوماتية؟

كما اعتمدنا في بحثنا المنهج الوصفي من خلال تعريف الجريمة المعلوماتية و مفهوم اختراق النظم المعلوماتية وتبيين مختلف خصائصها و أنواعها مع توضيح أركانها،

إضافة إلى المنهج التحليلي من خلال دراسة الجوانب القانونية مع ذكر التدابير الاجرائية و الوقائية.

وللإجابة على التساؤلات المطروحة في بحثنا انتهجنا خطة تتكون من فصلين في الفصل الأول تطرقنا فيه إلى الإطار المفاهمي للجريمة المعلوماتية، أما الفصل الثاني تناولنا الاختراق المعلوماتي.

خطة الدراسة

جريمة اختراق النظم المعلوماتية

✓ الفصل الأول: الإطار المفاهمي للجريمة المعلوماتية.

- المبحث الأول : مفهوم الجريمة المعلوماتية.
- المبحث الثاني: أركان الجريمة المعلوماتية.

✓ الفصل الثاني: الاختراق المعلوماتي.

- المبحث الأول: ماهية الاختراق المعلوماتي.
- المبحث الثاني: أساليب الحماية من جريمة الاختراق المعلوماتي.

الفصل الأول: الإطار المفاهيمي للجريمة المعلوماتية

تمهيد:

إن الجريمة هي إفراز للمجتمع ومظهر من مظاهره ومن ثم تعكس كافة ما تموج به المجتمعات من ظروف والذي يرجع إلى ما يحويه السلوك الإنساني في علاقاته المتشابكة من خير وشر وتصارعهما بصفة دائمة.

لذا فقد اقتحمت الجريمة و النشاط المعادي للمجتمع نوع جديد من المجرمين إلى جانب المجرم التقليدي والذي كانت تقتصر جرائمه على أبعاد فردية واجتماعية، فقد أدى التطور السريع والمذهل في وسائل الاتصال الى تطور الظاهرة الاجرامية سواء على الأشخاص الذين يرتكبونها.

عرفت البشرية في نهاية القرن الماضي اتساعا وتزايدا مطردا لنطاق استخدام تقنية المعلوماتية في المجتمع ونظرا للتطور السريع لهذه التقنية في جميع المجالات، بحيث أطلق عليها تسمية الجرائم المعلوماتية وهذه الأخيرة أثارت تساؤلات كثيرة باعتبارها ظاهرة جديدة ولخطورتها وفداحة خسائرها وسرعة انتشارها وذلك بتحديد مفهومها، وخصائصها، ومعرفة العوامل المختلفة التي تتدخل في هذا التحديد.

المبحث الأول: مفهوم الجريمة المعلوماتية.

إن بيان المشكلات القانونية والعملية التي تثيرها الجريمة الالكترونية تتطلب من الباحث أن يقوم ببحث مسألة أولية تتعلق بالتعريف بهذه الجريمة من خلال بيان معناها و طبيعتها القانونية سنسلط الضوء في المطلب الأول(تعريف الجريمة المعلوماتية).

المطلب الأول: تعريف الجريمة المعلوماتية.

لم يتناول المشرع الجزائري تعريفا للجريمة المعلوماتية في قانون العقوبات أو في الدستور بل أعطى تعريفات لبعض المصطلحات الخاصة بالحاسب الآلي ، وكذلك التشريع الكويتي و التشريع الأردني فلا يوجد قانونا يتناول التنظيم القانوني للجريمة المعلوماتية[1].

تناول الفقه القانوني تعاريفا مختلفة للجريمة قسمت إلى خمسة اتجاهات نقسمها إلى فرعين الفرع الأول (معنى الجريمة الإلكترونية من المنظور الفقهي) الفرع الثاني (تعريف الجريمة حسب الاتجاهين الموسع و الضيق).

الفرع الأول: معنى الجريمة الالكترونية من المنظور الفقهي.

لم يعطي الفقها تعريفا جامعا مانعا أو موحدا للجريمة المعلوماتية بل تعددت الإتجاهات من عدة زوايا وهي كما يأتي:

[1] شنتير خضرة، **آليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)**، أطروحة مقدمة لنيل شهادة الدكتوراه تخصص قانون جنائي، جامعة أحمد دراية، أدرار، 2020، ص09 .

أولا: الاتجاه الأول:

الجريمة الالكترونية هي كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الألي، ويلاحظ أن هذا التعريف يستند إلى الوسيلة المرتكب بها الجريمة الالكترونية باستخدام جهاز الكمبيوتر كي تعد جريمة الكترونية[1].

ثانيا: الإتجاه الثاني.

يعرف هذا الاتجاه الجريمة المعلوماتية نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه، يستند إلى وجوب أن يكون الحاسب الآلي هو محل الجريمة الالكترونية وقد فسر جانب من الفقه أن هذه الجريمة هي جريمة اعتداء على الأموال المعلوماتية، وهي عبارة عن الأدوات المكونة للحاسب الآلي، وبرامجه، ومعداته[2].

ثالثا: الإتجاه الثالث.

هي أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا.

يأخذ بموجب المام الفاعل بتقنية المعلومات الالكترونية من حيث استخدام الحاسب الآلي كي تعد جريمة من الجرائم الالكترونية[3].

---

[1] خالد ممدوح ابراهيم، **الجرائم المعلوماتية**، ط2، دار الفكر الجامعي، الاسكندرية، 2019، ص74.

[2] طارق عفيفي صادق أحمد، **الجرائم الالكترونية جرائم الهاتف المحمول**، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2015،ص 30.

[3] طارق عفيفي، المرجع نفسه، ص32.

رابعا: الاتجاه الرابع.

الاعتداءات القانونية التي تكون بواسطة الوسائل الالكترونية تكون بغرض تحقيق الربح. وقد عرفت منظمة التعاون الاقتصادي و التنمية التابعة للأمم المتحدة للجريمة المعلوماتية بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الالكترونية[1].

التعريف الأول اشترط أن يحقق الفاعل الربح وهذا الأمر برأينا غير محتمل دائما من الجريمة الالكترونية كما أن الفعل المرتكب قد لا يكون عمديا فقد يحصل بطريقة غير مباشرة أما التعريف الثاني فقد أدرج الأموال المادية، وهذه الأموال كما يرى البعض يمكن حمايتها بموجب نصوص قانون العقوبات التقليدية ولا حاجة لقانون الخاص وظهر لنا اتجاه خامس و أخير يرى أن الجريمة المعلوماتية هي كل فعل أو امتناع ، عبر فعل من مسألة الاعتداء على الأموال المعنوية " معطيات الحاسب الآلي" يكون ناتجا بطريقة مباشرة وغير مباشرة لتدخل التقنية الالكترونية[2].

يعد التعريف الأخير الذي جاء به الاتجاه الأخير موافقا مع التطور الأخير المستمر للجريمة الالكترونية ولوسائلها التقنية أو بخاصة أن شمل الأموال المعنوية دون الأموال المادية، وبذلك يكون هذا التعريف إلى حد ما قد جمع المعايير التي جاءت بها الاتجاهات الأربع سالفة الذكر[3].

وفي ظل مما سبق فالباحث يقترح تعريفا للجريمة المعلوماتية على أنها هي كل فعل أو امتناع يتم إعداده أو التخطيط له، ويتم بموجبه استخدام أي نوع من الحواسب الآلية سواء حاسب شخصي أو شبكات الحاسب الآلي أو الأنترنت أو وسائل التواصل

[1] صدام حسين ياسين العبيدي، **جرائم الأنترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية**، ط1، المركز العربي للنشر و التوزيع، القاهرة، 2018، ص40.
[2] طارق عفيفي، المرجع السابق، ص32.
[3] طارق عفيفي، المرجع السابق، ص33.

الاجتماعي لتسهيل ارتكاب الجريمة أو عملا مخالفا للقانون، أو تلك التي تقع على الشبكات نفسها عن طريق اختراقها بقصد تخزينها أو تعطيلها أو تعريف أو محو البيانات أو البرامج التي تحويها.[1]

الفرع الثاني: تعريف الجريمة الجريمة المعلوماتية حسب الاتجاه الضيق و الموسع.

ان الفقه اختلف في اعطاء تعريف الضيق أو الموسع للجريمة المعلوماتية فاعتمدوا على عدة معايير سنتطرق لها فيما يلي:

أولا: معيار وسيلة ارتكاب الجريمة.

يستند أنصار هذا الاتجاه في تعريفهم للجرائم الالكترونية إلى وسيلة الارتكاب ويشترطون وجوب ارتكابها بواسطة تقنية عالية لدى الجاني والحاسب الآلي وحسب ذلك تعريف الفقيه بايدن" بأنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي"، أما الفقيه دول فقد عرفها " هي كل فعل اجرامي يستخدم الحاسب الآلي لاتمامه[2].

أما **بالمكتب تقييم التقنية بالولايات المتحدة الأمريكية** فعرفها بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا" كما تعرف الجرائم الالكترونية بأنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتصلة بالكمبيوتر والأنترنت في أعمال وأنشطة إجرامية بهدف أن تحقيق عوائد مالية ضخمة في الاقتصاد الدولي عبر شبكة الأنترنت باستخدام النقود الالكترونية أو بطاقات السحب التي

[1] سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص قانون علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر،باتنة، 2013، ص112.

[2] خالد دوادي، **الجريمة المعلوماتية**، ط1، دار الأعصار العلمي للنشر، عمان، 2018، ص21.

تحمل أرقاما سرية بالشراء عبر الأنترنت أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة[1].

وقد عبر خبراء المنظمة الأوروبية للتعاون الاقتصادي عن الجريمة المعلوماتية بأنها كل سلوك غير مشروع ومناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها[2].

ولقي تعريف الجريمة المعلوماتية المعتمد على الوسيلة المستخدمة في ارتكابها على عدة انتقادات مفادها أن تعريف الجريمة يستوجب الرجوع إلى الفعل و الأساس المكون لها، وليس إلى الوسائل المستخدمة لتحقيقها فحسب، أو لمجرد أن الحاسب الآلي استخدم في الجريمة يتعين أن نعتبرها من جرائم الأنترنت[3].

ثانيا: معيار توافر المعرفة بتقنية المعلومات.

يعتمد أصحاب هذا الاتجاه على ضرورة إلمام الفاعل بتقنية المعلومات واستخدام الحاسوب للإمكانية اعتبارها من الجرائم المع ويعرف أنصار هذا الاتجاه الجرائم الالكترونية ومنها الدكتور ديفيد تومسيون " بأنها جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب[4] .

ومن بين التعريفات أيضا تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة عام 1989 حيث عرفت الجريمة بأنها "أية جريمة

---

[1] طارق عفيفي صادق أحمد، المرجع نفسه، ص 32.

[2] عبد الله عبد الكريم، **جرائم المعلوماتية والأنترنت (الجرائم الالكترونية)**،دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والأنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا،ط1، منشورات الحلبي الحقوقية، بيروت، 2007، 15.

[3] مصطفى يوسف كافي، **جرائم(الفساد-غسيل الأموال- السياحة- الإرهاب الإلكتروني- المعلوماتية)** ، ط1، مكتبة المجتمع العربي للنشر والتوزيع، عمان، 2014، ص165.

[4] آيت عبد المالك نادية، **التحقيق الجنائي للجرائم الالكترونية واثباتها في التشريع الجزائري**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجلالي بونعامة، خميس مليانة، المجلد 04، العدد 02، جانفي 2020، ص1692.

لفاعلها معرفة فنية بتقنية الحاسب يمكنه من ارتكابها، إن أصحاب هذا الرأي لا يستندون في تعريفهم على وجود الحاسب الآلي إنما على الشخص الجالس أمامه، أي الشخص الذي يستخدم الحاسوب لارتكاب هذا النوع من الجرائم[1].

حيث أن ما يميز الجريمة الالكترونية عن غيرها من الجرائم أن مرتكبيها يحيطون علما بتقنية المعلوماتية وفي غياب هذه المعرفة لا يمكنه ارتكاب هذه الجرائم[2].

ثالثا: المعيار الموضوعي.

يرى أنصار هذا الاتجاه أن الجريمة المرتكبة عبر الأنترنت ليست هي التي يكون النظام المعلوماتي أداة إرتكابها بل هي تقع عليه أو في نطاقه ومن أشهر الفقهاء روز بلات الذي عرف الجريمة الالكترونية على أنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول لمعلومات مخزنة داخل النظام أو التي تحول عن طريقه، كما أخذت بنفي الاتجاه الدكتورة هدى قشقوش حيث عرفت الجريمة المعلوماتية بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات وجرائم الحاسب الآلي هي الجرائم الناجمة عن ادخال البيانات المزورة في الأنظمة واساءة استخدام المخرجات اضافة إلى أفعال أخرى تجعل الجرائم أكثر تعقيدا من الناحية التقنية مثل: تعديل الكمبيوتر[3].

لا يعد المعيار الموضوعي كأساس لتعريف الجريمة بل يعد فقط من أهم المعايير وأكثرها قدرة على إيضاح طبيعة الجريمة محل التعريف إلا أنه هو الآخر ضيق من مفهومها وخرج من نطاقها جانب كبير من الأفعال الغير مشروعة[4].

---

[1] صدام حسين ياسين العبيدي، المرجع السابق، ص40.
[2] مصطفى يوسف كافي، المرجع السابق، ص165.
[3] عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والأنترنت والقانون العربي النموذجي**، منشأة المعارف، مصر، 2009، ص25.
[4] طارق عفيفي صادق أحمد، المرجع السابق، ص30.

كما يظهر لنا إتجاه آخر و هو الاتجاه الموسع يعد عكس الاتجاه السابق حيث يرون فرق أخرى من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة وتختلف مواقفهم حسب نظريتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية[1].

فعرف فريق من الفقهاء أن الجريمة المعلوماتية " كل سلوك اجرامي يتم بمساعدة الحاسب الآلي، أو هي كل جريمة تتم في محيط الحاسبات الآلية. كما يعرفها الفقيه الألماني تيادمان" هي كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب. وعرفها الأستاذEslie D.Ball: فعل اجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية.[2]

وقدم لها تعريف كل من الفقيهين توتي و هرد كستال" تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات الفعلية داخل نظام الحاسب، وبعبارة أخرى هي تلك الجرائم التي يكون فيها دور الحاسب فيها إيجابيا أكثر منه سلبيا[3].

ومن خلال هذه التعريفات يتبين لنا أن هذا الإتجاه يوسع من مفهوم الجريمة الالكترونية، حيث أن مجرد المشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة المعلوماتية ومن ثم يتضح لنا صعوبة قبول هذا التوجه، فجهاز الحاسب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم كسرقة الحاسب الآلي ذاته أو أقراص أو أسطوانات الممغنطة أو اللواحق على سبيل المثال ومن ثم لا يمكن اعطاء وصف للجريمة المعلوماتية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة، كما نلاحظ أن هناك تعريفات أخرى في إطار الاتجاه الموسع كانت أكثر تحديدا في تعريف الجريمة المعلوماتية ومن ذلك تعرفه بأنها كل

[1] ذياب موسى البداينة، **"الجرائم الالكترونية"**، مداخلة ضمن الملتقى العلمي حول: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان المملكة الأردنية الهاشمية، أيام 02، 03،04 سبتمبر 2014، 06.
[2] صدام حسين ياسين العبيدي، المرجع السابق، ص39.
[3] مصطفى يوسف كافي، المرجع السابق، ص165.

تلاعب بالحاسب الآلي ونظامه من أجل الحصول بطريقة غير مشروعة أو الحاق خسارة بالمجني عليه[1].

ويلاحظ من خلال التعريفات السابقة أنها قد أغفلت جانبا على قد كبير من الأهمية في تعريف الجريمة المعلوماتية ألا وهو الدور الكبير الذي يقوم به الحاسب الآلي في هذه الجريمة فإن كان من المتفق عليه أن الجريمة الالكترونية قد تتخذ أحد المظهرين، يتمثل الأول في استخدام الحاسب الآلي كوسيلة لارتكاب الجريمة، والثاني في الإعتداء على الحاسب الآلي ذاته.[2]

ونستخلص مما سبق أن اختلاف الفقه في وضع تعريف الجريمة المعلوماتية مرده الاختلاف في المعيار المعتمد عليه والزاوية التي ينظر إليها كل اتجاه إلى هاته الجريمة. وقد اصطلح المشرع الجزائري على تسمية الجرائم المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و عرفها بموجب أحكام المادة 02 من قانون 09-04 على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[3].

و يمكن استخلاص من خلال استقراء التعريف المعتمد من طرف المشرع الجزائري الملاحظات الآتية:

– أن المشرع الجزائري اصطلح على الجرائم المعلوماتية بتسمية الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال. وتبنى المشرع الجزائري معيار دور النظام المعلوماتي

[1] قارة أمال، **الجريمة المعلوماتية**، رسالة لنيل درجة الماجيستير في القانون، تخصص القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2002، ص19.

[2] مازيا عيساوي، سامية عزيز، **الجريمة من منظور سوسيولوجي –الأسباب والآثار-**، مجلة دراسات في سيكولوجية الإنحراف، جامعة محمد خيضر بسكرة، المجلد 06، العدد 01، السنة 2021، ص 130-131.

[3] ج ج د ش، قانون رقم 09-04 المؤرخ في 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها، ج.ر، العدد رقم 47، المادة 02، ص05.

لتحديد معالم الجريمة فسمى الجرائم الواقعة على النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر 07 [1]و ترك المجال واسع لأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية[2] أو نظام للاتصالات الإلكترونية.

أن المشرع الجزائري لم يقم بتحديد درجة دور المنظومة المعلوماتية أو نظام الاتصالات الإلكترونية في ارتكاب هذه الجرائم إذ حسب التعريف فإنه يكفي مجرد أن ترتكب الجريمة أو يسهل ارتكابها المنظومة المعلوماتية أو نظام الاتصالات الإلكترونية ، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم حتى تلك الجرائم التي يكون فيها للتقنية المعلوماتية دور ثانوي[3].

كما أنه لم يحدد صور السلوك المجرم الذي يرتكب أو يسهل ارتكابه منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

إن هذا التعريف تضمن تكرار كون أن مفهوم نظام الاتصالات الإلكترونية يندرج تحت مصطلح المنظومة المعلوماتية ذلك أن المشرع الجزائري عرف هذه الأخيرة بموجب أحكام المادة 02على أنها[4]:

"نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ".

[1] ج ج د ش ،الأمر رقم 66-156 ، مؤرخ في 18 صفر عام 1886 الموافق ل08 يونيو 1966، يتضمن قانون العقوبات ج.ر، العدد 49، صادر في 11يونيو 1966، معدل ومتمم ، المواد 394 مكرر إلى مكرر 07 ، ص157.

[2] أي نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

[3] وهيبة رابح، **الجريمة المعلوماتية في التشريع الإجرائي الجزائري**، مجلة الباحث للدراسات الأكاديمية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، ديسمبر 2014، ص 230-231-232.

[4] المادة 02،المرجع السابق، ص 157.

وحسب رأينا فإن تعريف الجريمة المعلوماتية الأقرب إلى الصواب هو كل اعتداء على النظام المعلوماتي أو كل اعتداء يتم باستخدام النظام المعلوماتي وكان له دور رئيسي في السلوك المجرم[1].

المطلب الثاني: خصائص الجريمة المعلوماتية.

تتميز الجريمة الإلكترونية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة لارتباطها بتقنية المعلومات والحاسب الآلي مع ما تتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من الخصائص والتي اكتست بدورها على مرتكب هذه الجريمة الذي يعرف بالمجرم الإلكتروني لتميزه أيضا عن المجرم التقليدي. وعليه سوف نحاول فيما يلي التطرق إلى بعض سمات الخاصة بالجريمة الإلكترونية (الفرع الأول) كما سنتناول دراسة أهم السمات الخاصة بالمجرم الإلكتروني (الفرع الثاني).

الفرع الأول: سمات خاصة بالجريمة بحد ذاتها.

تعتبر الجريمة المعلوماتية من الجرائم المستحدثة التي أتى بها التطور في مجال الإتصالات، فهي تختلف عن الجرائم التقليدية والتي ترتكب في العالم المادي، ولذلك فهي تتميز بخصائص و سمات جعلت منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل وسوف نبين أهم هذه الخصائص في هذا الفرع.

أولا: الجريمة الإلكترونية عابرة للدول أو عابرة للحدود.

ليس هناك في عالم اليوم حدود تقف حائلا أمام نقل المعطيات بين السياسات الآلية المتوزعة في مختلف دول العالم عبر شبكات المعلومات، فيمكن في بعض دقائق

[1] مصطفى يوسف كافي، المرجع السابق، ص151.

نقل كم هائل من المعطيات بين حاسب وآخر يبعد عنه آلاف الكيلومترات فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق بينهما بتحقق الفعل الإجرامي في دولة أخرى[1].

هذه الطبيعة الذي تتميز بها الجريمة الالكترونية كونها جريمة عابر للحدود خلفت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي لهذه الجريمة المعلوماتية، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بالإجراءات الملاحقة القضائية[2].

ثانيا: صعوبة إكتشاف الجريمة الالكترونية.

تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عامة، وما يؤكد ذلك قلة عدد الحالات التي يتم اكتشافها مقارنة في ضوء ما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء صعوبة في اكتشاف جريمة التقنية الحديثة إلى ارتكابها لا يشوبه أي عمل من أعمال العنف[3]، و عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، وكذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من ثانية واحدة يشكل عاملا اضافيا في صعوبة اكتشاف هذا النوع من الجرائم الحديثة.[4]

[1] نعيم مغبغب، **حماية الكمبيوتر الأساليب و الثغرات دراسة في القانون المقارن**، ط1، منشورات الحلبي الحقوقية، بيروت لبنان، 2006، ص218.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص77-78.

[3] محمد علي سالم، حسون عبيد عبد هجيج، **الجريمة المعلوماتية**، مجلة جامعة بابل، كلية العلوم الإنسانية، جامعة بابل، العراق، المجلد 14، العدد06،2007، ص92.

[4] عبد المؤمن بن صغير، **الطبعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن**، ورقة بحثية قدمت في الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، منظم من قبل قسم الحقوق ومخبر الحقوق، والحريات والأنظمة المقارنة، جامعة بسكرة، يومي 16-17 نوفمبر 2015، ص08.

وللمجني عليه دورا مهما في صعوبة اكتشاف وقوعها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له، و تكتفي عادة باتخاذ اجراءات ادارية داخلية دون الابلاغ عنها للسلطات المختصة، تجنبا للأضرار بسمعتها وهز الثقة في كفاءتها[1].

ثالثا: صعوبة اثبات الجريمة.

كما أن خصوصية الجريمة الالكترونية كما تبرز صعوبة اثباتها حتى في حالة اكتشاف وقوعها والإبلاغ عنها، فوسائل المعاينة طرقها التقليدية لا تصلح غالبا في اثبات هذه الجريمة، فهي تتم في بيئة غير تقليدية حيث لا تقع ناتج اطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والأنترنت، مما يجعل الأمور أكثر تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحظة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر ملمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة، وهذا خلافا للجريمة التقليدية التي لها مسرح تجري عليه الأحداث حيث تخلف آثار مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك من خلال المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة المعلوماتية[2].

إضافة إلى ذلك فإن نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الإدعاء والقضاء يشكل عائقا أساسيا أمام اثبات الجهات في مجال تقنية المعلومات، وكيفية جمع الأدلة والتفتيش في بيئة الحاسوب والأنترنت[3].

---

[1] نعيم مغبغب، المرجع السابق، ص22.

[2] حكيم سياب، **السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية**، مجلة الدراسات والأبحاث، جامعة زيان عاشور، الجلفة الجزائر، العدد الأول، 2009/09/15، ص 220.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص77.

رابعا: الجريمة الالكترونية سهلة الارتكاب.

تمتاز الجرائم الالكترونية بأنها جرائم لا تحتاج إلى أدنى مجهود عضلي ولا تحتاج إلى سلوكيات مادية فيزيائية متعددة لتحقيق النتيجة فيها، فطالما توافرت لدى الفاعل التقنية اللازمة والوسيلة المناسبة أصبح ارتكاب الجريمة من السهولة بمكان بما لا يحتاج إلى وقت ولا إلى الجهد[1].

الفرع الثاني: خصائص مرتكب الجريمة الالكترونية.

ان المجرم الالكتروني ليس له نموذج معين بل هناك عدة نماذج فمنهم من يستخدم الكمبيوتر في جرائمه وقد يقوم بأفعال إجرامية ضد الكمبيوتر نفسه فلماذا توجد صعوبة لتحديد سمات معينة له ويرجع ذلك الى تعدد الجرائم وتنوعها ورغم ذلك فان مرتكبها بالنسبة للمجموعة التقليدية هو شخصية مستقلة بذاتها فهو من جهة مثال منفرد للمجرم الذكي وهو من جهة أخرى اجتماعي بطبيعته وكذلك يتميز بصفات خاصة تميزه عن غيرة من مرتكبي الجرائم الواردة في قانون العقوبات[2].

أولا: مرتكب الجريمة مجرم ذكي

ان الجرم الالكتروني يصنف ضمن نوابغ المجرمين خاصة الأحداث الذين يخشى عليهم من الدخول من مجرد الهواية الى الاختراق في أفعال تسلل الى النظم، حيث يمتلك هذا المجرم من المهارات ما يؤهله أن يقوم بتعديل وتطور في الأنظمة الأمنية،

[1] محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت**، دار النهضة العربية القاهرة، مصر، 2009، ص31.

[2] سهام خليلي، **خصوصية المجرم الالكتروني**، مجلة المفكر، جامعة محمد خيضر بسكرة، العدد 15، جوان 2017، ص401- 414.

حتى لا تستطيع، ان تلاحقه وتتبع أعماله الاجرامية من خلال الشبكات أو داخل أجهزة الحواسيب[1].

ثانيا: مرتكب الجريمة الالكترونية متكيف اجتماعيا

بحيث لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به بل أنه انسان متكيف اجتماعيا ذلك أنه أصلا مرتفع الذكاء ويساعده في ذلك عملية التكيف وما الذكاء في رأي الكثيرين سوى القدرة على التكيف، ولا يعني ذلك التقليل من شأن المجرم بل خطورته الاجرامية تزيد اذا زاد تكيفه الاجتماعي، مع توافر الشخصية الاجرامية لديه ويذكر كذلك أن الاجرام الالكتروني تنتج عنه عوامل مستحدثة في أذهان مرتكبيه حيث لجأ العديد منهم الى ارتكاب هذه الجرائم بدافع اللهو أو لمجرد اظهار تفوقهم على الالة أو على البرامج المخصصة لأمن النظم المعلوماتية[2] .

ثالثا: مرتكب الجريمة الالكترونية متخصص

له قدرة فائقة في المهارة التقنية ويستقل مداركه ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الشفرات، ويسبح في عالم الشبكات ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة على أجهزة الحواسيب ومن خلال الشبكات.

[1] صدام حسين ياسين العبيدي، المرجع السابق، ص43.

[2] دليلة العوفي، **اشكالية مواكبة الجزائر لمجتمع المعلومات من الفجوة الرقمية إلى الجريمة المعلوماتية**، مجلة الحكمة للدراسات الإعلامية والاتصالية، كنوز الحكمة للنشر و التوزيع، مجلد 04، العدد 08، الجزائر، 2016، ص160.

رابعا: مرتكب الجريمة الالكترونية مجرم محترف.

ذلك أنه لا يسهل على الشخص المبتدئ في حالات قليلة أن يرتكب جرائمه عن طريق الكمبيوتر فالأمر يقتضي كثيرا من الدقة والتخصص في هذا المجال للتوصل إلى التقلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر[1].

خامسا: مرتكب الجريمة الالكترونية مجرم عائد في الإجرام.

فهو يوظف مهارته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات، فهو قد لا يحقق جريمة الاختراق بهدف الإيداع وإنما نتيجة شعوره بقدرته ومهارته في الاختراق[2].

المطلب الثالث: دوافع ارتكاب الجريمة الالكترونية.

الدافع وهو ما يعرف في القانون الجنائي بالقصد الخاص في الجريمة، وللجريمة المعلوماتية عدة دوافع تحث الجاني على ارتكابها، فبعضها يرجع إلى دافع شخصي و منها ما يرجع إلى الدافع الخارجي، وهذه الدوافع قد يكون مصدرها هو الرغبة الاجرامية

فالدافع والقصد يشكل الركن الاساسي في جميع الجرائم، وبالنسبة لجرائم الحاسب الآلي و الأنترنت فهي تختلف في وضعها العام عن أسباب أي جريمة أخرى تقليدية ومن الدوافع العديدة التي تحرك الأشخاص لارتكابها مثل هذا النوع من الجرائم[3] نذكر مايلي:

[1] اسراء جبريل رشاد مرعي، الجرائم الالكترونية" الأهداف- الأسباب- طرق الجريمة ومعالجتها"، **مجلة الدراسات الإعلامية**، المركز الديموقراطي العربي، العدد01، يناير 2018، ص429.
[2] صدام حسين ياسين، المرجع السابق، ص43.
[3] خالد ممدوح إبراهيم، المرجع السابق، ص138.

الفرع الأول: الدوافع المادية.

والدوافع المادية هي تلك التي يرجوا من ورائها مرتكب الجريمة الحصول على منافع مادية أو معنوية ذات مالية[1].

أولا: دوافع مالية.

ويعتبر هذا الدافع الهدف الرئيسي في أغلب الجرائم المعلوماتية في هذه الألفية، ذلك أن الربح الذي ينتج عن الاحتيال أو السرقة بواسطة الطرق المعلوماتية أكثر أمنا وحماية وربح عن السرقة التقليدية للأموال وغيرها.

كما أن استعمال التقنية المعلوماتية يسهل على المجرم القيام بجريمته ودون بذل مجهود بدني يذكر، بل أنها تمكنه حتى القيام بذلك دون التحرك من مكانه، إضافة إلى امكانية سرقة أموال ضخمة في عملية واحدة و بمفردة دون الحاجة إلى شركاء كان يقوم شخص ما بفتح حساب بنكي ثم يقوم بتحويل جزء من الأموال من كل حساب بنكي في تلك المؤسسة المالية إلى رصيده عن طريق الدخول إلى النظام المعلوماتي لذلك البنك أو المؤسسة المالية والتلاعب بها[2].

سهولة الفرار من المسؤولية الجزائية العقابية عن طريق مسح آثار الجريمة أو اتيانها من الفاعل ودون ترك أي دليل يدل على شخص مرتكب الجريمة أو استعمال صفة الغير أو شخصية خيالية أو شخص متوفى مما صعب معرفة الفاعل عند التحقيق.

صعوبة التحقيق في الجريمة، وامكانية القيام بها في أي مكان من العالم ومن أي دون عناء التنقل، دون القبض عليه من الدولة التي قام بالجريمة فيها[3].

---

[1] اسراء جبريل رشاد مرعي، المرجع السابق، ص 435.
[2] طارق عفيفي صادق أحمد، المرجع السابق، ص64.
[3] خالد ممدوح إبراهيم، المرجع السابق، ص138-139.

ثانيا: دوافع شخصية.

هناك فئة من مرتكبي الجرائم المعلوماتية يرجع ارتكابهم لها الديون الناتجة عن المشاكل العائلية والخسائر الضخمة من ألعاب القمار أو ادمان المخدرات، فقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه في الحالات أو حتى مساعدة الآخرين فيها، فالغاية تبرر الوسيلة.[1]

كما أن الرغبة في الاستئثار في مجال السوق أو التجارة قد تدفع بالشخص إلى اللجوء إلى هذا النوع من الجرائم من أجل تحطيم منافسة واخراجهم من السوق عن طريق القيام بحملات التشهير وتشويه سمعة المنافسين له.[2]

الفرع الثاني: الدوافع النفسية

وتتمثل هذه الدوافع في الأسباب النفيسة التي تدفع بالشخص إلى اتيان الأفعال الاجرامية ليس من أجل مكاسب مادية وإنما للإشباع رغباته نفسية أو الوصول إلى هدف ومبتغى معين.

أولا: دافع الانتقام

إن اللجوء إلى الجريمة قد يكون سبب الرغبة في الانتقام أو الكره والحقد الدفين اتجاه شخص ما، فقد يلجأ الشخص إلى اختراق الأنظمة المعلوماتية لصاحب العمل الذي كان يعمل لصالحه وقام بطرده أو تسبب له بأضرار مادية أو معنوية ويقوم بإتلاف البيانات الرئيسية أو نسخها وبيعها للشركة لشركة منافسة، كما يكون شخص اخترق صفحة أنترنت لصديقة تخلت عنه ويقوم بنشر معلومات الشخصية و صورها انتقاما منها[3].

[1] خالد دوادي، مرجع سابق ،37.
[2] شنتير خضرة، مرجع سابق، ص37.
[3] خالد ممدوح إبراهيم، المرجع السابق، ص140.

ثانيا: إثبات الذات

أحيانا يكون الدافع من وراءه الجريمة الرغبة في اثبات الذات وتحقيق انتصار على النظام المعلوماتي، مثال ذلك: الأشخاص الذين يقومون باختراق أنظمة معلوماتية من أجل التسلية أو المزاح مع الآخرين[1] أو من أجل القدرة على الإثبات على اختراق والوصول إلى أي نظام معلوماتي أو بدافع الفضول واكتساب الخبرة، أو حتى من أجل اثبات وجود خلل أو عيب أو ثغرة في النظام.[2]

وغالبا ما ينعدم للمجرم نية الإضرار بالغير، ذلك أن نيته من خلال ذلك هي الرغبة في قهر النظام ،ويدخل ضمن هذه الطائفة الهاكرز، فأغلب التشريعات عاقبت على مجرد الدخول إلى النظام المعلوماتي دون ترخيص حتى و لو كان للجاني نية حسنة، و لم يقم بأي تغييرات في المنظومة المعلوماتية وهذا ما سلكه المشرع الجزائري كذلك من أجل محاربة هذا النوع من الجرائم.[3]

[1] رمسيس بهنام، المجرم تكوينا و عقيدة، منشأة دار المعارف، الاسكندرية، 1982، ص175.
[2] شنتير خضرة، المرجع السابق، ص 39.
[3] خالد دوادي، المرجع السابق، ص 40-41.

المبحث الثاني: أركان الجريمة المعلوماتية.

إن الجريمة المعلوماتية ليست واحدة إنما تتخذ عدة أشكال مما يقضي دراسة أركانها بالتفصيل، وعليه سنتطرق للركن المفترض نبين فيه شروطه(نظام المعالجة الآلية) في المطلب الأول و تبين كيفية حمايته في المطلب الثاني.

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 الجريمة من جرائم الاعتداء على هذا النظام.

ويؤدي توافر هذا الشرط إلى الانتقال للمرحلة التالية إذ أن هذا الشرط يعتبر عنصرا لازما، لذلك يكون من الضروري تعريف نظام المعالجة الآلية للمعطيات ومدى خضوع هذا النظام لحماية فنية[1].

الفرع الأول: نظام المعالجة الآلية للمعطيات

هو تعبير فني تقني متطور، يخضع للتطورات الشريعة والمتلاحقة في الإعلام الآلي، وكذلك لم يعرف المشرع الجزائري على غرار المشرع الفرنسي نظام المعالجة الآلية للمعطيات، فأوكل بذلك مهمة تعريفه لكل من الفقه والقضاء.

انطلاقا من مبدأ الشرعية وفقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على:" لا جريمة ولا عقوبة أو تدابير أمن بغير قانون "[2]، كما جرم القانون المعدل لقانون العقوبات رقم 04-15 بعض صور الجريمة المعلوماتية ونص على

[1] نائلة عادل، المرجع السابق، ص331.

[2] قانون العقوبات الجزائري، الأمر رقم 66-155 المؤرخ في 1966/06/08، المتعلق بقانون العقوبات، المعدل و المتمم، المادة 01، ص01.

العقوبات المقررة لمرتكبيها في القسم السابع مكرر من قانون العقوبات تحت عنوان" المساس بأنظمة المعالجة للمعطيات" من الفصل الثالث المعنون" الجنايات والجنح ضد الأموال من الباب الثاني المتعلق بالجنايات والجنح ضد الأفراد وذلك في المواد من 394مكرر إلى مكرر 08 من قانون العقوبات المعدل و المتمم.

حيث لجأ المشرع إلى تقنين أو النص على مثل هذه الجرائم وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء إلى القياس، بمعنى عدم جواز لجوء القاضي الجنائي إلى قياس فعل لم يرد نص على تجريمه على فعل ورد نص تجريمه فيقرر القاضي الجنائي للأول عقوبة الثاني بسبب التشابه بين الفعلين[1]

حيث قدمت المادة الأولى من الاتفاقية الدولية للإجرام المعلوماتي تعريف النظام المعلوماتي[2] على النحو التالي:

يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من أجهزة 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 للعملية المعالجة داخل منظومة الكمبيوتر تؤدي وظائفها[3]

أما مجلس الشيوخ الفرنسي فقد عرف هذا النظام بأنه كل مجموعة مؤلفة من وحدة أو عدة وحدات لمعالجة المعلومات أو اختراقها أو اعداد البرامج و المعطيات وكل ما يؤدي الى ادخال واسترجاع المعلومات. هذا المفهوم يتضمن نظام المعالجة الألية المادية كالمعدات و الأجهزة الفكرية كالبرامج والمعلومات وأن توجد بين هذه العناصر علاقة لتحقيق هدف محدد، هو المعالجة الألية للمعلومات وهذه العناصر المادية والمعنوية التي

[1] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي للنشر و التوزيع، مصر،
[2] قارة أمال، المرجع السابق، ص102، ص 10.
[3] رامي حليم، **جرائم الاعتداء على الأنظمة الآلية للمعلومات**، جامعة سعد دحلب، الجلفة، 2017، ص34.

يتكون منها المركب واردة على سبيل المثال لا الحصر، فيمكن اضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال فاذا تم الاعتداء على أحد هذه العناصر بمعزل عن النظام، فلا تقوم الجريمة فلا بد من الاتصال بينها.

ويكون نظام المعالجة الالية للمعطيات في طور التشغيل عند ارسال اشارة كهربائية نحو وحدة المعالجة المركزية، والتي تقوم بدورها بإرسال البرنامج المسؤول عن تشغيل ذاكرة القراءة هذه الاخيرة تقوم بالبحث عن المعطيات التي تسمح بتشغيل النظام المسؤول عن البحث، ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة التي تقوم بمتابعة المراحل [1].

الفرع الثاني: الحماية الفنية لأنظمة المعالجة الألية للمعطيات.

تكفل بعض القواعد الأمنية لحماية لنظم المعالجة الألية للمعطيات، كوضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من الأجهزة المختلفة، والتي يمكن عن طريقها معرفة محتوى المعلومات التي يتم نقلها ، ويأتي ذلك عن طريق حماية الكابلات والوصلات الكهربائية لارتباطها بالأجهزة ومن بين هذه القواعد أسلوب يعتمد على توزيع العمليات التي يقوم بها نظام المعالجة الألية للمعطيات ونقلها الى نظام احتياطي (مركز للمساعدة) عند الضرورة، ويلجأ الى هذا الأسلوب عادة البنوك وشركات التأمين، ويظل هذا الموقع سرا ويخضع لدرجة عالية من الحماية، ومن الاساليب المستعملة كذلك الاعتداء على اختيارات الفيزيولوجية للدخول الى النظام عن طريق التحقق من شخصية القائم بعملية الدخول عن طريق البصمة أو نبرة الصوت أو شكل الأذن أو شبكية العين[2].

[1] لعاقل فريال، **الجريمة المعلوماتية في ظل التشريع الجزائري**، مذكرة لنيل شهادة الماستر في القانون العام، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق، جامعة أكلي محند أولحاج، البويرة،2015،ص28.

[2] رامي حليم، المرجع السابق، ص343.

لكن كل جريمة تستلزم وجود أعمال تحضيرية وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الاجرامي في الجرائم الالكترونية حتى و لو كان القانون لا يعاقب على الأعمال التحضيرية[1].

حيث تنص المادة 31 من القانون 06-23 المحاولة في الجنحة لا يعاقب عليها إلى بناءا على نص صريح في القانون، والمحاولة في لمخالفة عليها اطلاقا[2]، إلا أنه في مجال التكنولوجية المعلومات الأمر يختلف بعض الشيء، فشراء برنامج اختراق ومعدات لفك الشفرات والكلمات المرور وحيازة صور الدعارة.

وعليه فإن هذا الشكل من الاعتداء على نظام معالجة المعطيات الآلية للمعطيات يتكون من صورة بسيطة للجريمة وأخرى مشددة.

أولا: فعل 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 التقليدي.

كما أن المشرع لم يحدد وسيلة الدخول أو الطريقة التي يتم الدخول مباشرة أو عن طريق غير مباشر.

حيث أن الجريمة يقوم بها إنسان أيا كانت صفته، وكفاءته المهنية والفنية، فهذه الجريمة ليست من الجرائم ذوي الصفة[3].

[1] عبد الرحمان خلفي، محاضرات في القانون العام، دار الهدى للنشر و التوزيع، الجزائر، ص101.
[2] المادة 31 من القانون رقم 23/06 المؤرخ في 2006/12/20 المتعلق بالظروف المخففة وحالة العود المعدل و المتمم لقانون العقوبات الجزائري ،ج،ر العدد84، المؤرخة في 2006/12/24 ، ص17.
[3] أمال قارة، الحماية الجزائية المعلوماتية في التشريع الجزائري، ط1، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص121.

ثانيا: فعل البقاء.

التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على النظام. 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[1].

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا في الحالة التي لا يكون فيها الجاني 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.

إذا كانت تلك على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة حماية المعطيات أو المعلومات ذاتها[2].

المطلب الثاني: الأركان الأساسية للجريمة المعلوماتية.

بما أنه توفر الشرط الأولي لقيام الجريمة المعلوماتية ألا وهو نظام المعالجة للمعطيات، نستطيع الأن الانتقال إلى المرحلة التالية وهي لا بد من إيجاد وتوفر أركان أية جريمة من الجرائم المعلوماتية[3] وهذا من خلال تبين الركن المادي (الفرع الأول) ونوضح أيضا الركن المعنوي (الفرع الثاني).

[1] معاشي سميرة، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، جامعة محمد خيضر بسكرة، الجزائر ،العدد 7، 2011، ص280.

[2] لعاقل فريال، المرجع السابق، ص 33

[3] صدام حسين ياسين العبيدي، المرجع السابق، ص22.

الفرع الأول: الركن المادي.

يتكون الركن المادي في أشكال وصور الاعتداء على نظام المعالجة الآلية للمعطيات ونحدد ثلاث أشكال نذكرها:

أولا: الدخول والبقاء الغير المشروع في نظام المعالجة الآلية للمعطيات.

ونقصد هنا بالدخول الالكتروني عن طريق الأساليب والوسائل التقنية المتاحة كالدخول إلى مركز النظام المعلوماتي والاطلاع على المعلومات ولم يحدد المشرع الجزائري الطريقة التي تم بها الدخول وعليه فإن الجريمة تتحقق بأي وسيلة ومن أكثر التقنيات استعمالا لتحقيق الدخول إلى النظام:

1. نصت عليه المادة 394 مكرر من قانون العقوبات بنصها:" يعاقب بالحبس من ثلاثة أشهر إلى سنة بغرامة مالية من 50.000 إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعلومات الآلية للمعطيات أو يحاول ذلك.
2. تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الافعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين مع غرامة من 50.000 إلى 150.000 دج[1].

رجوعا لنص المادة 394 مكرر 3 من قانون العقوبات لا نجد اشارة إلى ضرورة خضوع النظام للحماية الفنية حتى يتمتع بالحماية الجنائية وذلك الشأن بالنسبة للمادة 323-1 من قانون العقوبات الفرنسي يظهر من خلال الأعمال التحضيرية لقانون 1988 المتعلق بالمعلومات والمقتبسة منه المادة 323-1 أنه كان من المقترح ضرورة شمول النص بهذا

[1] ج ج د ش، الأمر رقم 66-156 ، مؤرخ في 18 صفر عام 1886 الموافق ل08 يونيو 1966، يتضمن قانون العقوبات ج.ر، العدد 49، صادر في 11يونيو 1966، معدل ومتمم، المادة 394 مكرر، ص157.

الشرط، ولكن اشتراط وجود حماية أمنية في نظام المعالجة الآلية للمعطيات لم يتم الاتفاق عليه في المناقشات الأخيرة في البرلمان الفرنسي ولذلك جاء النص خاليا من هذا الشرط ووجد هذا الشرط قد يؤدي إلى الحد من الحماية الجانية للنظم غير المشمولة بتجهيزات أمنية داخل النظام[1].

ونصت المادة 394 مكرر 2 ومكرر3 من 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 عقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 إلى 150.000 دج[2].

هنا نجد أن هناك طرفين تشدد فيهما عقوبة جريمة الدخول والبقاء داخل النظام وتربط بين هذين الطرفين علاقة سببية بين الدخول غير المشروع و البقاء غير المشروع والنتيجة الضارة وإن لم تكن مقصودة.

ثانيا: الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات.

نصت على هذا الشكل من الاعتداء المادتين الخامسة و الثامنة 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 البرنامج سير النظام.[3]

[1] العاقل فريال، المرجع السابق، ص30

[2] ج ج د ش، ج ر، الأمر رقم 66-156، مؤرخ في 18 صفر عام 1886 الموافق ل08 يونيو 1966، يتضمن قانون العقوبات ، العدد 49، صادر في 11 يوليو 1966، معدل و متمم ، المادة 349 مكرر2 ومكرر3 ، ص157-158.

[3] ج ج د ش ، قانون رقم 09-04 المؤرخ في 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها، ج.ر ، العدد رقم 47، صادر في 16 أوت 2009.

وذكرت أيضا في نص المادة 3/323 من قانون العقوبات ولهذه الجريمة ثلاث صور منها: المحو والتعديل أما في ما يتعلق بجريمة إعاقة أو تحريف تشغيل نظم المعالجة الآلية للمعطيات فلم يرد نص خاص بها واكتفى المشرع بجريمة التلاعب في بيانات نظم المعالجة والتعطيل الذي يندرج ضمن اعاقة النظام المعلوماتي بأي وسيلة.[1]

وقد وضع الفقه معيار التفرقة بين الإعتداء وسيلة أم غاية، فإذا كان الاعتداء إلا وسيلة فإن الفعل يشكل جريمة اعتداء عمدي على النظام و من جهة أخرى إذا كان الاعتداء العمدي كما ذكرنا سابقا فعلين يتمثلان في الآتي:

1/يتمثل في التعطيل(العرقلة) والذي يفترض وجود عمل إيجابي مع العلم أن المشرع لم يذكر التعطيل بطريقة معينة بل يمكن أن يتم التعطيل بوسيلة مادية ككسر الأجهزة المادية للنظام أو كسر الأسطوانات، أو عن طريق أداة معنوية تتم بالإعتداء على الكيانات المنطقية للنظام كالبرامج والمعطيات وذلك باستعمال طرق أخرى كإدخال فيروسات، استعمال قنابل منطقية مؤقتة، جعل النظام يتعطل في أداءه لوظائفه كما يستوي ان يقترن التعطيل بالعنف أم لا.

2/يتمثل في الفساد الذي يتم بكل فعل إلى التعطيل نظام المعالجة الآلية للمعطيات يؤدي إلى جعله غير صالح للاستعمال السليم وذلك من شأنه يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[2].

[1] فلاح عبد القادر، أيت عبدالمالك نادية، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري،**مجلة الأستاذ الباحث للدراسات القانونية والسياسية** ، المجلد 04، العدد 02، 2019، ص1704.

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

ثالثا: الاعتداءات العمدية على المعطيات.

نصت عليها المواد03،04،08 من الاتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع الجزائري في المادة 394 مكرر 1 و394 مكرر 2 من قانون العقوبات فجرم المادة الأولى للاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، وجرم في المادة الثانية المساس العمدي للمعطيات الموجودة خارج النظام[1].

الفرع الثاني: الركن المعنوي.

يعتبر الركن المعنوي في الاعتداءات الماسة بأنظمة المعلوماتية تتخذ القصد الجنائي و هذا ما سنتناوله في هذا الفرع.

أولا: الركن المعنوي بالنسبة للدخول والبقاء غير المشروع داخل نظام المعالجة الآلية:

الركن المعنوي لجريمة الدخول والبقاء غير المشروعين يتخذ صور القصد الجنائي في الجريمة التقليدية من علم وارادة باعتبارها من الجرائم العمدية، وقد نصت المادة394 مكرر عن القصد الجنائي العام بتطلبه أن يكون الدخول أو البقاء: "عن طريق الغش" فاستخدام هذه العبارة يعني أن الفاعل على العلم بدخوله أو بقاءه في نظام المعالجة الآلية للمعطيات غير مشروع[2].

ويشترط القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، وبناءا على أركانها واستكمال عناصرها وخصوصا الركن المادي منها، وأول

[1] لعاقل فريال، المرجع السابق، ص35.
[2] سبع زيان، سلمى المفتي، صور و اركان الجريمة المنظمة دراسة مقارنة في القانون الإماراتي والقانون الجزائري، مجلة الحقوق والعلوم الإنسانية، العدد1، 2020/10/30، ص234.

هذه العناصر هو موضوع الحق المعتدي عليه، ويتعين توافر علم الجاني بأنه فعله ينصب على نظام المعالجة الآلية.

يتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة. كما أن في الجريمة المعلوماتية الركن المعنوي هو الحالة النفسية للجاني والعلاقة بين ماديات الجريمة وشخصية الجاني، برزت مشكلة الركن المعنوي في الجريمة المعلوماتية في قضية موريس[1]* الذي منهما في قضية الدخول غير المصرح به على جهاز الحاسب الفيدرالي وقد دفع محامي موريس على إنتقاء الركن المعنوي الأمر الذي جعل المحكمة تقول هل يلزم أن يقوم أن يقوم الادعاء بالثبات القصد الجنائي في جريمة الدخول غير المصرح به تثبت نية المتهم في تحدي الخطر الوارد على استخدام نظم المعلومات في الحاسب الآلي وتحقيق الخسائر[2] .

أما بالنسبة للقضاء الفرنسي فإن منطق سوء النية هو الأعم في الجرائم الالكترونية، حيث يشترط المشرع الفرنسي وجود نية في الاعتداء على البريد الالكتروني خاص بأحد الأشخاص.

أما المشرع الجزائري فقد نصت في المادة 394 مكرر 2 من جريمة المساس بأنظمة المعالجة الآلية للمعطيات[3]، على أنه كل من يقوم عمدا وعن طريق الغش، وهنا فقد تحقق عنصر العلم والارادة.

[1] قضية مورس: هذه الحادثة هي أحد أول الهجمات الكبيرة والخطرة في بيئة المعلوماتية ففي نوفمبر عام 1988 تمكن طالب يبلغ من العمر 23 سنة يدعى ROBER MORRIS من اطلاق فيروس عرف باسم(دودة موريس) عبر الأنترنت، أدى إلى إصابة 06 ألاف جهاز يرتبط معها حوالي، 60.000 نظام عبر الأنترنت ، من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة، بحوالي مئة مليون دولار، اضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم عليه بالسجن لمدة ثلاثة أعوام وعشرة ألاف دولار غرامة.

[2] سيباني عبد الكريم، **الحماية الجزائية والموضوعية للجريمة المعلوماتية**، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق، جامعة الطاهر مولاي، سعيدة، 2015،ص15.

[3] ج ج د ش الامر رقم 66-156 مؤرخ في 18 صفر عام 1886 الموافق ل08 يونيو 1966، يتضمن قانون العقوبات ج ر، العدد 49، صادر في 11 يونيو 1966، معدل ومتمم ،المادة 394 مكرر 2 ، المرجع ،ص157.

وأيضا يتطلب أن يعلم الجاني بخطورة الفعل الذي يقوم به، فإذا كان غير ذلك ينتفي القصد الجنائي، ويجب القصد الجاني أيضا أن يتوقع الجاني النتيجة الاجرامية التي ستترتب عن القيام بفعله، فتوقع النتيجة هو أساس النفي الذي تقوم عليه ارادتها فحيث يكون التوقع لا نتصور الارادة، والنتيجة التي يجب أن نتيجة إليها توقع الفاعل هي النتيجة التي يحددها القانون، وهي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات.[1]

وعليه إذا أثبت الجاني انتفاع العلاقة السببية بين السلوك الاجرامي ألا وهو الدخول أو البقاء غير المشروع، والنتيجة الاجرامية كأن يثبت أن التعديل أو محو معطيات أو عدم صلاحية النظام للقيام بوظائفه برجع إلى قوة قاهرة أو حادث مفاجئ انتفى السلوك الاجرامي والقصد الجنائي لدى الجاني. أما القصد الخاص فلا يبدوا من خلال نص المادة 394 مكرر ق.ع.ج[2].

وأخيرا بعد ما تطرقنا في هذا الفصل إلى ماهية الجرائم المعلوماتية ، حيث قمنا بدراسة مختلف الآراء الفقهية في تعريف الجريمة المعلوماتية انتهينا إلى أنها هي كل اعتداء على نظام الحاسب الآلي المعلوماتي أو يتم باستخدام النظام المعلوماتي بما أن له دور رئيسي في السلوك الاجرامي ، و هي بهذا المفهوم تتسم بعدة خصائص تميزها عن الجرائم الأخرى التقليدية إذا من أهم هذه السمات أو المميزات طبيعتها المتعدية الحدود و طابعها التقني الذي يعقد من مسألة إثباتها الشيء الذي يميز مرتكبيها و يجعل دوافع ارتكابهم للجريمة المعلوماتية بمختلف أنواعها تختلف عن المجرمين العاديين .

ورأينا أيضا أن لنظام المعلوماتي أهمية كبيرة باعتباره تقنية حديثة في عالم تكنولوجيا المعلومات ، إلا أنه غالبا ما يكون المصدر الرئيسي للجرائم التي تقع عليه و

[1] روزا جعفر محمد الخامري، مشكلات الطبيعة القانونية لبرامج الحاسب الآلي، الاسكندرية، ط1، المكتب الجامعي الحديث، 2006، ص 62.
[2] المادة 394 مكرر، الأمر السابق، ص 157.

بواسطته، و بذلك تعد الجرائم المعلوماتية أو الالكترونية من الجرائم الخطيرة و السريعة و المتطورة و في تزايد مستمر تبعا لازدياد استخدام تلك التقنية ، و لذا سنحاول من خلال الفصل الثاني أن نبرز ونكتشف نوع من أنواع الجريمة المعلوماتية هي الاختراق وندرس كل ما يخص هذا النوع من الجرائم الماسة بأنظمة معطيات الحاسب الآلي.

الفصل الثاني: الاختراق المعلوماتي.

تمهيد:

إثر التطور المتنوع في تقنيات التكنولوجية للاتصال أصبح الحاسب الآلي والمعلومات المحرك الأساسي في الاقتصاد العالمي الجديد، وأصبحت الحياة من حولنا تدار إلكترونيا فاليوم نجد البنوك تدار إلكترونيا وكل المعاملات و المجالات تدار معلوماتيا، على جراء هذا الأخير ظهرت جرائم مستحدثة أكثر خطورة من الجرائم التقليدية إذ تعد من أكثر الجرائم صعوبة فيما يتعلق في اكتشافها و التبليغ عنها، كما نرى مجموعة من المميزات التي تتسم بها عن الجرائم التقليدية وهي جريمة عابرة للحدود و تصعب في اثباتها هذه تعد من سمات التي تتميز بها الجريمة في حد ذاتها أما بالنسبة لمرتكب الجريمة فيجب أن يكون ذكي، متكيف اجتماعيا، ومتخصص في هذا المجال الالكتروني و التكنولوجي المتطور، كما أيضا الجريمة الالكترونية لديها عدة أنواع منها الاعتداء على البيانات و المعطيات الالكترونية والاختراق الالكتروني للنظم، تعد هذه الأخيرة من أخطر أنواع الجرائم الالكترونية المنتشرة مؤخرا.

المبحث الأول: ماهية الاختراق المعلوماتي.

يمكننا أن ندين لمن اخترعوا عموميات الشبكة العنكبوتية" الأنترنت" غير أننا أصبحنا نخاف من هتك و انتهاك المعطيات، حيث أن انتهاكها واختراقها بات هاجسا نخاف منه، هذا من جهة و من جهة أخرى فإن الاختراق أساس جل الجرائم الاعتداء على سرية المعطيات و المعلومات الالكترونية.

كلمات الاختراق والمخترقون أو الهاكرز تثير ذعر الكثير من الناس، وخاصة مستخدمي الأنترنت الذين يسعون إلى حماية أسرارهم من هؤلاء الهاكرز[1]، وكثيرا ما تكون عملية الاختراق تكون عشوائية، يعني أن المخترق لا يعرف جهاز من يقوم باختراقه.

المطلب الأول: مفهوم الاختراق المعلوماتي.

اختلفت التعريفات للاختراق المعلوماتي للنظم المعلوماتية ولم تضبط المفاهيم وهذا ما سنتناوله في هذا المطلب سنقوم بإعطاء تعاريف و تبين معنى الاختراق (الفرع الأول) وهذا الاختراق بدوره يقسم إلى أنواع وهذا ما سنتناوله في (الفرع الثاني).

الفرع الأول: تعريف الاختراق.

عرف الاختراق في القانون العربي النموذجي الموحد في شأن جرائم اساءة استخدام تقنية المعلومات بأنه "الدخول غير المصرح أو غير المشروع لنظام المعالجة الآلية للمعطيات وذلك عن طريق انتهاك الاجراءات الأمنية" هنا نسلط الضوء على أن الاختراق كسلوك فني لا نعني به جريمة الدخول غير المشروع به للنظام المعلوماتي كما

[1] الهاكرز جمع هاكر: هو شخص يعمل على تجاوز الحمايات الموضوعية على النظم الحاسوبية. ويهدف في المقام الأول إلى اختراق الحاسوب عن بعد عبر شبكات الاتصالات، ثمة مخترقون يعملون على الاختراق بقصد اكتشاف الثغرات الأمنية في نظام حاسوبي والعمل على اتلافها.

أن هنا الكثير من يخلط بينهما و لكن يمكن تعريفه أنه سلوك فني يترتب عليه الدخول الغير المصرح به للنظام المعلوماتي[1].

كما نعرف الاختراق أيضا أنه عمليات غير شرعية تتم عن طريق ثغرات موجودة في النظام يستطيع المخترق من خلالها الدخول إلى جهاز الضحية من أجل اتمام غرض معين يسعى إليه المخترع[2].

تتم عملية الاختراق الالكتروني عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الأنترنت وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص مخترع في الدولة التي تم فيها الاختراق، فالبعد الجغرافي لا أهمية له الحد من الاختراقات المعلوماتية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي تتصف به نظم تشغيل الحاسب الالكتروني والشبكات المعلوماتية[3].

فالاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق الثغرات في نظام الحماية الخاصة بالهدف، فالمخترق لديه القدرة على دخول أجهزة الآخرين عنوة دون الرغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي يحدثها سواء بأجهزتهم الشخصية أو نفسياتهم فما الفرق بين مخترق الأجهزة الالكترونية الشخصية ومقتحم البيوت الآمنة[4].

الفرع الثاني: أنواع الاختراق.

إن الاختراق يعد وسيلة من وسائل ارتكاب الجريمة المعلوماتية يشمل عدة أنواع من أهمها ما يلي:

[1] يمكن قول أن الاختراق هو التسلل والاقتحام

[2] جمال زين العابدين أمين أحمد، جرائم إختراق النظم الإلكترونية بين التشريع المصري و المغربي، **مجلة مستقبل العلوم الاجتماعية**، جامعة عبد الملك السعدي /المغرب، العدد الأول، أفريل 2020، ص115.

[3] علي عدنان الفيل، الاجرام الالكتروني دراسة مقارنة ، منشورات زين الحقوقية، ص87.

[4] نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف الاسكندرية، 2008، ص41.

أولا: اختراق المزودات:

مزودات الخدمة" أو الأجهزة الرئيسية للشركات أو المؤسسات أو الجهات الحكومية، وذلك باختراق الجدران النارية التي عادة ما توضع لحمايتها، وغالبا ما يتم ذلك باستخدام المحاكاة وهي مصطلح يطلق على عملية انتحال الشخصية للدخول إلى النظام[1].

ثانيا: التعرض للبيانات.

التعرض للبيانات أثناء انتقالها والتعرف على شفرتها إن كانت مشفرة وهذه الطريقة تستخدم في كشف بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية[2].

ثالثا: اختراق الأجهزة الشخصية.

وهي الطريقة الأكثر شيوعا نظرا لتوفر العديد من البرامج الاختراق سهلة الاستخدام.

كما يحتاج انتهاك البيانات إلى جهاز الضحية دون العلم بمجموعة من الأدوات والوسائل الخاصة، فهذه الأخيرة قد تكون بعض البرامج الموجودة داخل نظام التشغيل نفسه أو بعض البرامج التي صممت خصيصا لتسهيل عمليات الاختراق والتسلل وتجنب استخدام العديد من الأوامر المعقدة[3].

[1] جمال زين العابدين أحمد أمين، المرجع السابق، ص 117.
[2] نسرين عبد الحميد، المرجع السابق، ص 145.
[3] محمود نجيب حسني، جرائم الاعتداء على الأموال، ط3، منشورات حلبي الحقوقية، بيروت، ص 667-668.

المطلب الثاني: وسائل الاختراق الالكتروني وآثارها.

تتضمن المخاطر التي تتعرض لها النظم المعلوماتية إلى الاعتداء وزراعة نقاط ضعف ...إلخ ، و نسلط الضوء على الاختراق الالكتروني للنظم فيجب على المخترق استعمال عدة وسائل لنجاح عمله، ولابد من هذا الاختراق على وجود آثار سنتناولهما في فرعين، وسائل الاختراق المعلوماتي (الفرع الأول) ، والآثار التي تنجم عن الاختراق (الفرع الثاني).

الفرع الأول: وسائل الاختراق المعلوماتي.

يحتاج الاختراق لجهاز الضحية دون علمه إلى مجموعة من الأدوات والوسائل الخاصة ومن بين هذه الوسائل أهمها ما يلي:

أولا: الاختراق عن طريق استعمال نظام التشغيل

لأن نظم التشغيل مليئة بالثغرات، فإنه يتم استغلالها في عمليات الاختراق، ولكن الأهم هو القيام بذلك عن طريق بروتوكولات[1] التي يستخدمها النظام للتعامل مع شبكة الأنترنت أو الشبكات الداخلية بكل أنواعها.

كما يمر المنتهك عند التسلل بعدة مراحل يتمكن من خلالها اختراق الحاسب الآلي.

ثانيا: الاختراق باستخدام البرامج.

كما يجب لقيام الاختراق لا بد من وجود برنامجين، يكون واحد بجهاز الضحية ويسمى بالبرنامج الخادم لأنه بمثابة الخادم الذي يتأمر بأوامر المخترق وينفذ مهامه

[1] بروتوكول مفرد بروتوكولات: هو مجموعة من القواعد التي تستخدمها اجهزة الكمبيوتر للاتصال مع بعضها البعض عبر الشبكة، وهو وجود اتفاقية أو ضوابط القياسية التي تمكن من الاتصال ، ونقل البيانات بين نقاط النهاية الحوسبة في أبسط أشكالها.

الموكلة إليه داخل جهاز الضحية[1] و الجهاز الآخر برنامج يوجد بجهاز المخترق ويسمى ببرنامج المستفيد العميل، وليدنا أشهر مثال على هذه البرامج و أخطرها هو برنامج طروادة، فهو يتمتع بمجموعة من المميزات تجعل الأقدر على عملية الاختراق دون القدرة على كشفه وتتبعه والقضاء عليه[2].

برنامج حصان طروادة[3] في أبسط صوره، يقوم بتسجيل كل ما تقوم بكتابته على لوحة المفاتيح منذ أول لحظة للتشغيل، وتشمل كل البيانات السرية أو الحسابات المالية أو المحادثات الخاصة على الأنترنت أو رقم بطاقة الائتمان الخاصة أو حتى كلمات السر التي تستخدمها للولوج إلى الشبكة العنكبوتية، والتي قد يتم استخدامها بعد ذلك من قبل الجاسوس الذي قام بوضع البرنامج على الحاسب الشخصي للضحية[4].

ويتم إرسال هذا البرنامج إلى جهاز الضحية بعدة طرق، لعل أشهرها إرسال بالبريد الالكتروني، إذ يقوم المخترق بإرسال رسائل إلى الضحية يرفق بها ملفا يحمل حصان طروادة، ليقوم الضحية بفتحها وتحميل الملف المرفق على أنه أحد البرامج المفيدة ليكشف بعدها أنه لا يعمل فيظن أنه به عطلا ليقوم بإهماله، فيحتل حصان طروادة مكانه داخل النظام ويبدأ مهامه التجسسية و حتى لو قام الضحية بحذف البرنامج لمرة واحدة فقط حتى يقوم بمهامه[5].

[1] محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية الاسكندرية، 2003، ص137.
[2] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة للنشر، الاسكندرية، 2007، ص42
[3] شفرة صغيرة أو برنامج يتم تحميله مع برنامج رئيسي من البرامج ذات شعبية عالية، ويقوم ببعض المهام الخفية، غالبا ما تتركز على اضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته.
[4] رابحي عزيزة، **الأسرار المعلوماتية وحمايتها الجزائية**، رسالة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق و العلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2017، ص 114.
[5] محمد خليفة، المرجع نفسه، ص 43.

ثالثا: هجومات استغلال المزايا الاضافية.

إن هنا الأمر يتصل بواحد من أهم استراتيجيات الحماية فلدينا في الأصل أن مستخدم النظام يحدد له النطاق لاستخدام ونطاق الصلاحيات بالنسبة للنظام ولكن في الواقع العملي يحدث أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك أو دون علم الشخص نفسه أنه يحظى بمزايا تتجاوز اختصاصاته ورغباته[1]. وفي هذه الحالة فإن أي مخترق للنظام يكون قادرا فقط على تدمير معطيات المستخدم أو التلاعب بها من خلال اشتراكه أو عبر نقطة الدخول الخاصة به وبكل بساطة يتمكن من تدمير مختلف ملفات النظام حتى تلك غير المتصلة بالمدخل الدخل منه لأنهم استثمر المزايا الاضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله.

رابعا: التفتيش في مخلفات التقنية وانتحال شخصية الأفراد.

التفتيش في المخلفات التقنية و هو القيام بالبحث في بقايا المؤسسة من القمامة والمواد المتروكة بحثا عن أي شيء يساعد المخترق على اختراق النظام ،كالأوراق المكتوب عليها كلمات السر أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة أو الأقراص الصلبة المرمية بعد استبدالها أو غير ذلك من المواد المكتوبة أو الملاحظات أو أي أمر يستدل منه على أية معلومة تساهم في الاختراق.

بينما انتحال شخصية الأفراد هو قيام شخص باستخدام شخصية إنسان آخر للاستفادة من سمعته مثلا أو ماله وصلاحياته هذا الانتحال يمكنه القيام بذلك عن طريق المعلومات التي تتعلق بتلك الشخصية، كالاسم و العنوان ورقم الهوية حيث يستغلها استغلالا سيئا، والتي يحصل عليها من الانترنت[2] ويمكن أن تؤدي أن تؤدي هذه الجريمة

[1] محمد خليفة، المرجع السابق، ص45.
[2] نبيلة هبة هروال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، ط1، دار الفكر الجامعي، الاسكندرية، 2007، ص61.

إلى استنزاف رصيد الضحية في البنك أو السحب من البطاقة الائتمانية أو الإساءة إلى سمعة الضحية وقد تكون وسيلة المجرم إلى ارتكاب جريمة النصب، مستفيدا من السمعة الطيبة لتلك الشخصية أو شركة قد استغرقت السنوات الطوال لبناء تلك السمعة . وكثيرا ما يقوم المجرم بتغيير العنوان البريدي للضحية إلى عنوانه لكي يستقبل بنفسه الفواتير والمطالبات التي قد تنبه الضحية إلى أي شيء مريبا يحدث. [1]

وتعتبر وسيلة انتحال الشخصية من أسهل الطرق المستحدثة في الدخول إلى أنظمة الحاسب الآلي وهناك وسيلتان لانتحال الشخصية هما:

1-انتحال الشخصية باستخدام التقنيات غير عالية الكفاءة أو ما يطلق عليها الانتحال للشخصية بدائيا فقط، ويتم ذلك عن طريق استخدام المجرم لبطاقة أو كارت خاص بشخص مسموح له بالدخول وهذا النوع يعتبر بسيط من الناحية التقنية على الرغم مما يسببه من إخطار ونتائج ضارة.

2-انتحال الشخصية باستخدام التقنيات العالية، أو ما يطلق عليه التنكر الالكتروني بحيث ينتحل الشخص شخصية آخر باستخدام اسم هذا الشخص عن طريق إرسال بريد الكتروني مدعيا انه شخص آخر وهي من أسهل أنواع التنكر الالكتروني[2].

خامسا: انتحال شخصية المواقع.

هذا الأسلوب يعتبر حديثا نسبيا بين الجرائم المعلوماتية، ولكنه الأشد خطورة والأكثر صعوبة في اكتشافه من انتحال شخصية الأفراد، ويقوم الفاعل بهذه الجريمة من خلال وضع نفسه في موقع بيني بين البرنامج المستعرض Browser للحاسب الخاص بأحد مستخدمي الانترنت وبين الموقع Web ومن هذا الموقع البيني يستطيع حاسب المجرم أن

[1] رابحي عزيزة، المرجع السابق، ص117.
[2] يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والأنترنت، ط1، دار الكتاب العربي، القاهرة، 2010، ص 134.

يتصرف وكأنه صاحب الموقع الحقيقي، ويستطيع مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه كما يستطيع سرقة هذه المعلومات أو تغييره، ولكن القيام بهذه العملية حتى لو تم الاتصال بالموقع من خلال ما يسمى بالنظم الاتصال الآمنة. وكل ما يحتاجه من يقوم بهذه العملية هو السيطرة على أحد المواقع التي تتم زيارته بكثرة وتحويلها ليعمل كموقع بيني، وتحتاج عملية التحويل هذه إلى مهارة خاصة في برمجة المواقع أو إلى قيام المجرم باختراق موقع أحد مقدمي الخدمة المشهورين، ثم يقوم بتركيب البرنامج الخاص به هناك وبمجرد أن يكتب مستخدم الإنترنت اسم هذا الموقع فإنه يقع في المصيدة ويدخل إلى الموقع المشبوه الذي أعده المجرم، إذا أن هذا الأخير قام بتغيير أحد الروابط في الوسط بين المستفيد والموقع الشهير، ويستطيع من ذلك أن يتلصص على المعلومات المتبادلة بينها[1].

الفرع الثاني : أثار اختراق النظم الإلكترونية.

تترتب على جريمة الاختراق المعلوماتي عدة آثار نعدد منها مايلي:

أولا: آثار مادية.

تغيير الصفحة الرئيسية لموقع الويب كما حدث لموقع قناة الجزيرة الفضائية مؤخرا إثر عرضها لصور الأسر الأمريكية على شاشتها وموقعها حيث قامت جهة ما باختراق موقعها ونظامها وتعطيلهما وغيرت الصفحة الرئيسة لها بصورة العلم الأميركي.

السطو بقصد الكسب المادي كتحويل حسابات البنوك أو الحصول على خدمات مادية أو معلوماتية كأرقام بطاقات الائتمان والأرقام السرية الخاصة بالبطاقات البنكية[2] اقتناص كلمات السر التي يستخدمها الشخص للحصول على خدمات مختلفة كالدخول

[1] رابحي عزيزة، المرجع السابق، ص118.
[2] جمال زين العابدين أحمد أمين، المرجع السابق، ص 132.

إلى الإنترنت حيث يلاحظ الضحية أن ساعاته تنتهي دون أن يستخدمها وكذلك انتحال شخصية في منتديات الحوار، أو الاستلاء على بريد شخص ما[1].

ثانيا: أثار فردية

مما يترتب على الفرد من انتهاك الخصوصية وسرقة بياناته ومعلوماته.

ثالثا: أثار اجتماعية.

حيث فترتب على الاختراق العديد من الأضرار الاجتماعية مثل نشر الرذيلة والاتجار بالمخدرات والاتجار بالأطفال والنساء.

ترتبط بالحفاظ على الدولة ككل مثل التعدي على الأمن القومي الداخلي أو الخارجي.

رابعا: أثار إدارية.

مثل تدمير النظم الإدارية الإلكترونية للدولة أو المؤسسات الخاصة يؤدي الاختراق إلى تدمير البنية التحتية المعلوماتية للدولة[2] .

[1] البلوي، شيخة بنت مسعد عبد الله، المسؤولية الجنائية عن اختراق المواقع الالكترونية الرسمية دراسة مقارنة، أطروحة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص شريعة وقانون، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، السعودية، 2016، ص20.

[2] جمال زين العابدين أمين أحمد، المرجع السابق، 124.

المبحث الثاني: أساليب الحماية من جريمة الاختراق المعلوماتي.

إن الحد والردع الجنائي قام بتحديد مجموعة من العقوبات لجرائم المعلوماتية مسبقا تماشيا مع مبدأ الشرعية وإن كان يوفر حماية أساسية للنظام وللمعلومات ضد المخاطر والأضرار والاختراقات الناجمة عن هذه الجرائم الباهظة التكلفة في حالة الوصول إلى معلومات سرية سواء للشخص أو لأمن الدولة، إلا أنه غير كاف لوحده، فحتى تكون هناك الفعالية في الحركة والأداء والحماية لابد أن تعززها حماية فنية تعمل على وضع حاجز لعدم وقوع هذه الجرائم أو التخفيف من آثارها إذا وقعت[1].

إن تعرض الأنظمة المعلوماتية للانتهاك و التسلل اللامتناهي خاصة عند ارتباط الحاسوب بشبكة الانترنت[2] ما يتطلب ضرورة اتخاذ تدابير وطرق احترازية ووسائل حماية سرية لتلك الانظمة ، وجعلها في مأمن وبأمان وكثيرة هي الطرق والأساليب الفنية للحماية خاصة في عصرنا الحاضر، ويمكن إجمال أساليب الحماية في طرق حماية عن طريق البرامج (المطلب لأول)، وطرق حماية عن طريق نظام الرقابة الوقائية عبر الوسائل الالكترونية (المطلب الثاني).

المطلب الأول: طرق الحماية عن طريق البرامج.

من أجل الحد من الاختراقات الالكترونية وردعاها قامت التشريعات بوضع أساليب للحماية منها أساليب عن طريق البرامج و تنقسم أساليب الحماية الفنية عن طريق البرامج إلى أربعة فروع ، الوسائل المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعية (الفرع الأول) الوسائل المتعلقة بالتحكم في الدخول والنفاذ إلى الشبكة(الفرع

[1] بودابست، الاتفاقية المتعلقة بالجريمة المعلوماتية، مجموعة المعاهدات الأوروبية، رقم 185، أوروبا، ص 5-6.
[2] عبد الفتاح بيومبي حجازي، المرجع السابق، ص14.

الثاني) وسائل مراقبة الاستخدام وتتبع سجلات النفاذ (الفرع الثالث)، وسائل المنع من افشاء المعلومات لغير المخولين و وسائل متعلقة بمنع الانكار(الفرع الرابع).

الفرع الأول: الوسائل المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام والمشروعية.

هي وسائل تهدف إلى ضمان استخدام النظام المعلوماتي أو الشبكة من قبل الشخص المخول بهذا الاستخدام وتضم هذه الطائفة كلمات السر بأنواعها، البطاقات الذكية المستعملة للتعريف، وسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي كما تظم أيضا ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ[1].

الفرع الثاني: وسائل متعلقة بالتحكم في الدخول والنفاذ إلى الشبكة.

وهي الوسائل التي تساعد على التأكد من أن الشبكة قد استخدمت بطريقة شرعية ومن أهم الوسائل الفنية المعتمد عليها ما يعرف "بالجدران النارية"[2] والتي هي عبارة عن برامج تثبت داخل النظام بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الإنترنت، فيتم إجبار جميع عمليات الدخول إلى الشبكة أو الخروج منها بأن تمر من خلال هذا الجدار الناري والذي يمنع أي مخترق أو متطفل من الوصول إلى الشبكة. وذلك عن طريق مراقبة الحزم الذي يتم إرسالها واستقبالها من الحاسب الآلي الخاص بالمستخدم. وعند مراقبة الجدار الناري لهذه الحزم والمنافذ التي

[1] نائلة عادل محمد فريد، المرجع السابق، ص 94.

[2] الجدار الناري هو نظام يوفر الحماية للشبكة عبر ترشيح البيانات المرسلة والمستقبلة عبر الشبكة بناءا على قواعد حددها المستخدم عموما، الهدف من الجدار الناري هو تقليل أو إزالة وجود الاتصالات الشبكية غير المرغوب فيها والسماح في الوقت نفسه للاتصالات "الشرعية" أن تنقل بحرية، توفر الجدر النارية طبقة أساسية من الحماية التي عندما تدمج مع غيرها تمنع المهاجمين من الوصول خادموك بطرق خبيثة.

ترسل وتستقبل من خلالها فإن عليه السماح أو الاعتراض على دخول هذه البيانات أو خروجها، وتنبه الاستخدام لذلك. [1]

الفرع الثالث: وسائل مراقبة الاستخدام وتتبع سجلات النفاذ.

والأداء وهي التقنيات التي تستخدم لمراقبة مستخدمي النظام وتحديد الشخص الذي قام بالعمل المعين في الوقت المعين وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.

وهذه الوسيلة قد أشار إليها المشرع الجزائري في القانون /09 04 في المادة 10 منه، حينما ألزم مقدمي الخدمات العمل على حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة المتعلقة بتاريخ ووقت ومدة كل اتصال بالإضافة إلى حفظ المعطيات التي تسمح بالتعرف على المرسل إليه الاتصال وعنوان الموقع المطلع عليه[2].

الفرع الرابع: وسائل المنع من افشاء المعلومات لغير المخولين و وسائل متعلقة بمنع الانكار.

هي الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المخولين أو المصرح له بذلك وتهدف هذه الوسائل إلى ضمان سرية المعلومات وتشمل تقنيات تشفير المعطيات[3] والملفات، إجراءات حماية الموجات، نسخ الحفظ الاحتياطية، برامج الفلترات غيرها.

أما في ما يخص الوسائل المتعلقة بمنع الإنكار: وتهدف هذه الوسائل إلى ضمان عدم قدرة الشخص المستخدم على إنكار أنه هو الذي قام بالتصرف، وترتكز هذه

[1] أحمد خليفة الملط، المرجع السابق، 192.

[2] سعيداني نعيم، المرجع السابق، ص71-72.

[3] يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص حاليا فهم يسعون لتأمين السرية لرسائل الالكترونية وسرية البيانات المتناقلة وخاصة الأعمال التجارية الرقمية. ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على السائل الالكترونية.

الوسائل بصفة أساسية على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة من طرف ثالث.[1]

المطلب الثاني: طرق الحماية الوقائية و الاجرائية لمكافحة جريمة الاختراق عبر الوسائل الإلكترونية.

سن المشرع الجزائري مجموعة من القواعد الوقائية و الأنظمة التي تقي من الاختراق و الاعتداء على الأنظمة المعلوماتية و أيضا قواعد إجرائية للحد والمكافحة من الاختراق المعلوماتي وتتمثل هذي المنظومة في طرق حماية وقائية (الفرع الأول) و طرق اجرائية لمكافحة جريمة الاختراق المعلوماتي(الفرع الثاني).

الفرع الأول: طرق الحماية الوقائية من الاختراق المعلوماتي.

تعد وسائل الحماية الوقائية من بين الوسائل الأكثر أهمية لحماية النظام المعلوماتي في الاعتداء المعلوماتي وتعد الدرع الحامي لهذه النظم المعلوماتية و من بين هذه الطرق الأكثر أهمية نظام المراقبة الالكترونية.

المراقبة الالكترونية من القواعد الفنية الوقائية التي تسمح بالرصد المبكر للاعتداءات المخترقين المحتملة على النظام وتسمح بالتدخل السريع لتحديد مصدر هذا الاعتداء والتعرف على مرتكبيه ، حيث تعتبر من أهم البدائل العقوبات السالبة للحرية وأكثرها تطورا، استعملت مكافحة للجريمة، خاصة وإن المشرع أخذ بها مؤخرا وتزداد أهميتها في كونها جديدة، فالقليل من التشريعات من أخذت بنظام المراقبة الالكترونية وطبقتها[2]، إذ يعد هذا النظام من بين أهم آليات الوقاية من جرائم المعلوماتية وفي نفس الوقت تعتبر

[1] رابحي عزيزة، المرجع السابق، ص125.
[2] مهداوي محمد صالح، اسود ياسين، نظام المراقبة الالكترونية في التشريع الجزائري، دائرة البحوث والدراسات القانونية والسياسية، جامعة عين تيموشنت الجزائر، المجلد 05، العدد03، 2021، ص07.

من القواعد الإجرائية الخاصة باستخلاص الأدلة المعلوماتية ويسمح القانون بهذا الإجراء في مجال التحقيق الجنائي، فعن المشرع الجزائري نص بخصوص هذا الأخير في المواد من394 مكرر إلى394 مكرر8 من قانون العقوبات الجزائري [1].

كما نص المشرع المصري بالقانون رقم 82 لسنة 2002 لحماية حقوق الملكية الفكرية والحقوق المجاورة ففرض أسلوبا تقنيا جديدا للحماية الجنائية الفعلية لأصحاب الحقوق على المصنفات وذلك بمنع أي اعتداء على أي حق أدبي أو مالي من حقوق المؤلف أو الحقوق المجاورة في هذا القانون فقد نص عليه في ذلك القانون في المادة 181. كما تبنى الاتجاه التشريعي المختلط وهو الحماية القانونية للمعلومات وكذلك أنظمة المعلومات وشبكات المعلومات.

وشمل المشرع المغربي النظم الالكترونية بالحماية بالقانون رقم 34/05 المتعلق بحماية حقوق المؤلف و الحقوق المجاورة ومن ذلك القانون المشار اليه الحماية الجنائية الخاصة بالمعطيات من خلال حق المؤلف[2].

ويقصد بمراقبة الاتصالات الإلكترونية، العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني، والجدير بالكر أن المشرع الجزائري عرف الاتصالات الالكترونية من خلال نص المادة 02 من القانون /09 04 بأنها " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية"[3] .

[1] الجمهورية الجزائرية الديموقراطية الشعبية، الأمر رقم 16- 155 المؤرخ في 08 يونيو سنة 1966 ، المتعلق بقانون العقوبات الجزائري ، المعدل و المتمم، المواد 64 إلى 65 مكرر 10، ص157.
[2] جمال زين العابدين أمين أحمد، المرجع السابق، ص 127-128.
[3] ج ج د ش، قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر، العدد 47، المادة 2، ص5.

نص المشرع الجزائري على مراقبة الاتصالات الالكترونية في المادة 03 من القانون /09 04 المذكور سابقا حيث تنص على إمكانية وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، إذا تطلبت ذلك حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية، وذلك مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات.

ترجع ضرورة مراقبة الاتصالات الالكترونية من ناحية إلى ازدياد معدلات الجريمة ومن ناحية أخرى إلى كثرة استخدام المجرمين للتقنية المعلوماتية لإعداد وارتكاب جرائمهم، وما أقرها المشرع سوى لإقامة التوازن بين المجتمع في الأمن وردع الجريمة، وحفظ حق الأفراد السرية.

و من آليات المكافحة الفنية للجريمة المعلوماتية أيضا المرسوم الرئاسي رقم 228/15[1] المتعلق بالقواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو الذي بدوره قام في المساهمة بالوقاية من الأعمال الإجرامية وحماية الممتلكات والأشخاص بصفة عامة.

الفرع الثاني: طرق اجرائية لمكافحة جريمة الاختراق المعلومات.

كافح المشرع الجزائري الاختراق المعلوماتي للنظم المعلوماتية من خلال قانون الإجراءات الجنائية، ومن خلال قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها[2] وسنتطرق إلى هذا من خلال مايلي:

[1] ج ج د ش، مرسوم رئاسي رقم 228/15، المتعلق بالقواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو المؤرخ في 22 غشت 2015، ج ر، العدد 45، ص03.

[2] ج ج د ش، القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، ج ر ، العدد 47.

أولا: معالجة الجرائم المعلوماتية من خلال قانون الإجراءات الجزائية.

نص قانون الإجراءات الجزائية على مجموعة من إجراءات التحري والتحقيق في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والتي تتمثل في ما يلي : التفتيش، اعتراض المراسلات السلكية و اللاسلكية ،التقاط الصور [1] وندرس أهمها:

- **التفتيش وضبط جرائم الماسة بأنظمة المعالجة الآلية في حالات التلبس بجريمة الاختراق.**

يعتبر التفتيش من أهم الاجراءات التي جاءت في نص القانون 09-04 في المادة 5، ويكون التفتيش وفقا لقواعد متعددة منها الحصول على اذن مسبق من قبل سلطة قضائية مختصة فقد نصت المادة 44: لا يجوز لضابط شرطة قضائية الانتقال إلى مساكن الأشخاص التي يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع إلى التفتيش"، ويكون كذلك الأمر في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المذكورة في المادتين 37 و40 من هذا القانون[2].

كما يجب أن تتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم فيها زيارتها و تفتيشها. ويخضع التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة للمعطيات وبعض البرامج المنصوص غليها على سبيل الحصر في المادة 3/47 لقواعد خاصة تختلف عن القواعد العامة المقررة في البندين

[1] أحسن بوسقيعة، التحقيق الجنائي، دار هومة، الجزائر، ص113.
[2] ج ج د ش ، القانون رقم 06-22، المؤرخ في 20 ديسمبر سنة 2006، يعدل و يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ص6-7.

1و2 من المادة 1/45 إ ج نصت على ما يلي :" تتم عمليات التفتيش التي تجري طبقا لنص المادة 44 أعلاه على الوجه الآتي[1]:

1-إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له .وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته[2].

2-إذا جرى التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش، وان تعذر ذلك اتبع الإجراء المنصوص عليه في الفقرة السابقة[3].

وتختلف هذه القواعد حسب الحالتين:

الحالة الأولى :إذا تعلق الأمر بالتحقيق التمهيدي في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف ، فإن ضابط الشرطة القضائية بموجب الفقرة الأخيرة من المادة 45 إ ج لم يعد مقيدا عند إجراء تفتيش المساكن والمحلات بالشرط المتعلق بضرورة حضور المشتبه فيه أو من ينوبه أو شاهدين إذا حصل التفتيش بمسكنه، وكذلك الأمر إذا حصل التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالجريمة[4].

---

[1] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دون دار نشر ، دون طبعة، 2003، ص131. مشار إليه لدى ريتشارد مانسفيلد، ترجمة خالد العامري، دار الفاروق للنشر و التوزيع ، القاهرة ، 2001، ص46.

[2] خالد ممدوح ابراهيم، المرجع السابق، ص209.

[3] المادة 1/45، المرجع السابق، ص662

[4] خالد ممدوح ابراهيم، المرجع السابق، ص88.

الحالة الثانية :أصبح ضابط الشرطة القضائية إذا تعلق التحقيق التمهيدي الذي يجريه بجريمة متلبس بها أو تحقيق متعلق بإحدى أنواع الجرائم السالفة الذكر، يمكنه بموجب المادة 47 مكرر المستحدثة في قانون الإجراءات الجزائية أن يجري التفتيش بعد الموافقة المسبقة من وكيل الجمهورية بحضور شاهدين مسخرين من غير الموظفين الخاضعين لسلطته أو بحضور ممثل يعينه صاحب المسكن محل التفتيش، إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا أو في مكان آخر وأن الحال يقتضي عدم نقله إلى ذلك المكان بسبب مخاطر جسيمة قد تمس بالنظام العام أو احتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله[1].

ثانيا: معالجة الجرائم المعلوماتية من خلال قانون 09-04.

- كما نص المشرع الجزائري في المادة 5 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المذكور سابقا على ضرورة توافر حالات على سبيل الحصر، تجيز للسلطات القضائية وضباط الشرطة القضائية القيام بتفتيش المنظومة المعلوماتية في إطار قانون الاجراءات الجزائية، وهي للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة من الأبحاث الجارية،

[1] خالد ممدوح ابراهيم، المرجع السابق، ص92.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1].

غير أنه في حال الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها حصريا بإجراءات التفتيش.

كذلك يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارستهم لوظائفهم أو بمناسبتها، طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، لا سيما قانون الإجراءات الجزائية، تفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمها أنه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكتروني في الحالات سابقة الذكر يمكن الدخول بغرض التفتيش ولو عن بعد إلى:

أ –منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب –منظومة تخزين معلوماتية[2].

وختاما بعد دراستنا في هذا الفصل لنوع من أنواع الجرائم المعلوماتية ألا وهي الاختراق المعلوماتي للنظم المعلوماتية، قمنا بتسليط الضوء على ماهية هذا الاختراق الالكتروني للمعطيات المعلوماتية بينا أنواع الاختراق وتتمثل هذه الأنواع في " اختراق مزودات الخدمة" و "التعرض للبيانات" و"اختراق الأجهزة الشخصية" ،وقمنا بتوضيح وسائل الاختراق كلا على حدة المتمثلة في أدوات اختراق عبر البرامج المعلوماتية وأنظمة التشغيل، وذكرنا بعض الآثار المترتبة عن هذا الاختراق فتتعد حسب تعدد المجالات فاعتمدنا على الأثار المادية وشخصية واجتماعية...إلخ. و تهدف هذه الدراسة إلى توفير الحماية القانونية للنظم المعلوماتية من قبل التشريعات الوضعية و الاتفاقيات الدولية كما ركزنا عن أساليب الحماية سواء أكان من خلال الحماية على الصعيد الدولي أو على

[1] نائلة محمد فريد، المرجع السابق، ص306.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ط15، دار هومة الجزائر، 2013، ص 523.

الصعيد الداخلي وهذا ما تبناه المشرع الجزائري فقد أورد في قانون العقوبات من المواد 394 مكرر إلى 394 مكرر 8 حماية قانونية و جزاءات لمخترق الأنظمة المعلوماتية وكذلك تحدث في القانون 09-04 عن أساليب الحماية الوقائية و أساليب إجرائية تحد أو تمنع من هذه الاعتداءات المتمثلة في الاختراق الالكتروني للنظم المعلوماتية.

خاتمة:

جعل التطور الكبير والمتسارع للوسائل التكنولوجية الحديثة، والتحول إلى العالم الرقمي لخلق مجموعة من أخطر الجرائم يشهدها العالم اليوم، ألا وهي الجرائم الالكترونية التي بدورها تتفرع إلى عدة جرائم منها اختراق النظم المعلوماتية، التي أصبحت تهدد مختلف فئات المجتمع دون استثناء، الأمر الذي دفع أغلب الدول إلى تخصيص مجموعة من القوانين وبعض أليات للحد منها، إلا أن ذلك يردع و حد من انتشارها واستمرارها في المجتمعات، فتعتبر الجريمة المعلوماتية من الجرائم العابرة للحدود لم تكن الآليات المخصصة لها على المستوى الداخلي لوحدها قادرة على مجابهتها و مواجهتها بل استلزم الأمر إيجاد آليات مكافحة فعالة وفاعلة لهذه الآفة الإجرامية التي تتم بها أخطر الجرائم التي يشهدها عصرنا هذا الذي اصبحت فيه التكنولوجيا المتقدمة عصب الحيات و محركها، فكما استغلها البعض وخاصة مجرمو المعلوماتية.

وهذا ما أشرنا له في آخر المطاف فإننا حاولنا في بحثنا معالجة الموضوع من خلال فصلين أساسيين، حيث تعرضنا للفصل الأول الإطار المفاهيمي للجريمة المعلوماتية أو الالكترونية وذلك بالتطرق إلى مفهومها المتضمن الاتجاهات الفقهية و الاتجاهين الموسع والضيق، كما أن لديها سمات تجعلها تتميز عن نظيراتها التقليدية سواء تعلقت بالجريمة في حد ذاتها أو بالمجرم الالكتروني.

كما بينا أسباب و دوافع المؤدية لارتكاب هذه الجريمة المعلوماتية، سواء كانت دوافع شخصية أو نفسية أو متعلقة بإثبات الذات لشخص مرتكب الجريمة المتمثلة في الاختراق.

وبالنسبة للفصل الثاني فتوصلنا إلى تحديد المفهوم العام لنوع جديد من الجرائم ألا وهي الاختراق المعلوماتي للنظم المعلوماتية، مع توفير تدابير الاجرائية للحماية و طرق وقاية لمكافحة هذه الجريمة المستحدثة، كما أن هذا النمط من الجرائم يتنوع بتنوع ما هو واقع أو مستهدف للنظام المعلوماتي أو ما يرتكب باستخدامه هذه الطبيعة المتميزة للجريمة، جعلت من المشرع الجزائري يدرك مدى خطورة هذه الجريمة على الفرد والمجتمع على حد سواء والتصدي لها، كما يجب أن تكون هناك وسائل تقنية تقوم بمحاربتهم والتبليغ عنهم وكشف جرائمهم الالكترونية، وإلقاء القبض عليهم وذلك من خلال عدة أمور كاستغلال وسائل التواصل الاجتماعي والبريد الالكتروني والوسائل عير الهواتف من أجل التوعية بخطورة هذه الجرائم.

إذ قام المشرع الجزائري بتعديل قانون العقوبات رقم 04-15، ولكن محدوديته دفعت بالمشرع الجزائري إلى إصدار قانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال.

من خلال دراستنا هذه توصلنا لبعض النتائج نذكرها في مايلي:

- عدم وجود مفهوم أو تعريف جامع مانع للجريمة الالكترونية عامة ،والاختراق الالكترونية خاصة مما نتج عنه الاختلاف المتباين في الأفعال التي تعد من قبيل الجرائم الالكترونية، وقد يكون ذلك سبب الطبيعة المتسارعة والتطور الكبير الذي تشهده هذه الجريمة الخطيرة وعم قدرة التشريعات على مجاراتها، نظرا لما يتميز به هذا الأخير من جمود وبطء في اجراءات صدوره.
- للجريمة المعلوماتية مميزات تختلف بها عن الجرائم التقليدية الأخرى ومرد ذلك يعود للبيئة الرقمية التي ترتكب فيها، مما أكسبها وأكسب

مرتكبها أي المجرم الالكتروني سمات معينة، صعبت معها عملية المكافحة الإجرائية و المؤسساتية.

- لم يضع المشرع الجزائري نصا قانونا مخصصا بالجرائم الالكترونية رغم ما تسببه هذه الجرائم من مخاطر على المجتمع والدولة معا، خاصة و أن الجزائر تتجه نحو الرقمنة مما يتماشى مع العصرنة الحاصلة في العالم.
- سمح المشرع الجزائري بعمليات المراقبة الالكترونية كأسلوب من الأساليب الوقائية قبل وقوع الاختراق المعلوماتي، والاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أي عندما يكون من الصعب الوصول إلى النتيجة التي تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.
- حفاظا على النظام العام و محاولة ردع جريمة اختراق النظم المعلوماتية اتخذ تدابير اجرائية كالتفتيش و الحجز داخل منظومة معلوماتية، و أجاز تمديده بعد إعلام السلطة القضائية المختصة بذلك .

بعد ما تطرقنا إلى نتائج في بحثنا هذا نذكر بعض التوصيات التي من خلالها نجد حلا لهذه الجريمة من بين هذه التوصيات:

- ينبغي على المشرع الجزائري وضع أو سن قوانين خاصة تحمي المعلومة و المنظومة المعلوماتية من الاختراق عليا عن طريق الحاسب الآلي و الأنترنت في الآونة الأخيرة وضرورة الرجوع في ذلك إلى القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والأنترنت كنوع من التعاون الدولي من أجل التوفيق بين التشريعات الوطنية الخاصة بهذه الجريمة.

- تجريم الدخول الغير المشروع به إلى النظام المعلوماتي عن طريق اختراق أنظمة الأمن الخاصة بالحواسيب أو إذا أدى الدخول إلى إتلاف المعلومات سواك أكان هذا الإتلاف كليا أو جزئيا.
- ضرورة وضع قواعد و اجراءات تكفل لرجال القانون سواء من الشرطة أو القضاء أداء مهامهم كحالات الضبط و التفتيش مع عقد دورات تكوينية لهم حتى يتمكنوا من الفصل القضايا المعلوماتية المتعلقة بالاختراق المعلوماتي.
- يجب أن يتلاءم تعريف جريمة اختراق النظم المعلوماتية مع فكرة عالمية المعلومات والاتصالات، بحيث يكون متفقا عليه على المستوى العالمي خاصة مراعاة التطور التكنولوجي الحاصل يوما عن يوم، ويجب توضيح الدور الذي يقوم به الحاسب الآلي في إرتكاب هذه الجريمة.
- ضرورة التنسيق فيما يتعلق بالإجراءات الجزائية المتبعة في شأن الجريمة المعلوماتية عامة و جريمة اختراق النظم المعلوماتية خاصة بين الدول المختلفة خاصة مت تعلق منها بأعمال الاستدلال أو التحقيق.
- تأهيل القضاة وتكوينهم في مجال الجرائم المعلوماتية حتى يتسنى له الإلمام بكافة النصوص والاجراءات المتبعة في هذا النوع من الجرائم، خاصة في أحكام المستحدثة وتنشيط دورات تكوينية مستمرة من قبل خبراء وقوانين باعتبار أن هذا يؤثر على العدالة بصفة مباشرة.

قائمة المصادر والمراجع.

1/ النصوص القانونية:

أ- القوانين:

ب- الأوامر:

- الجمهورية الجزائرية الديموقراطية الشعبية، الأمر رقم 66-156 المؤرخ في 18 صفر عام 1886 الموافق ل08 يونيو 1966، يتضمن قانون العقوبات، الجريدة الرسمية، العدد 49 الصادرة في 11 يونيو 1966، معدل و متمم.

ت- المراسيم الرئاسية:

- المرسوم الرئاسي رقم 15-228، المتعلق بقواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو والمؤرخ في 22 غشت 2015، الجريدة الرسمية، العدد 45.
- الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 09-04 المؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، الجريدة الرسمية، العدد47، صادرة في 16 غشت سنة 2009.
- الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، يعدل و يتمم بالأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية.

2- الكتب:

- أحسن بوسقيعة، التحقيق الجنائي، دار هومة، الجزائر، 2013.

- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الطبعة 15، دار هومة، الجزائر، 2013.
- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية ، دار الفكر الجامعي للنشر و التوزيع ، مصر، 2006.
- أمال قارة، الحماية الجزائية المعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع الجزائر 2007.
- أمال قارة، الحماية الجزائية المعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة للطباعة والنشر و التوزيع، الجزائر، 2007.
- خالد دوادي، الجريمة المعلوماتية، الطبعة الأولى، دار الأعصار العلمي للنشر، عمان، 2018.
- خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، 2019.
- روزا جعفر محمد الخامري، مشكلات الطبيعية القانونية لبرامج الحاسب الآلي، الطبعة الأولى، المكتب الجامعي الحديث، الإسكندرية،2006.
- صدام حسين ياسين العبيدي، جرائم الأنترنت وعقوبتها في الشريعة الإسلامية والقوانين الوضعية، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، 2018.
- طارق عفيفي صادق أحمد، الجرائم الإلكترونية جرائم الهاتف المحمول، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015.
- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت والقانون العربي النموذجي، منشأة المعارف، مصر، 2009.
- عبد الله عبد الله عبد الكريم، جرائم المعلوماتية و الأنترنت الجرائم الالكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية و

الأنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007.

- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة و النشر، مصر، 1999.
- علي عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى، دراسة مقارنة، منشورات زين الحقوقية، 2011.
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الأنترنت، الطبعة الثانية، دار النهضة العربية القاهرة، مصر، 2009.
- محمود أمين الرومي، جرائم الأنترنت، دار المطبوعات الجامعية، الإسكندرية، 2007.
- محمود نجيب حسني، جرائم الإعتداء على الأموال، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، دون سنة نشر.
- مصطفى يوسف كافي، جرائم (الفساد-غسيل الأموال-السياحة-الإرهاب الإلكتروني، المعلوماتي)، الطبعة الأولى، مكتبة المجتمع العربي للنشر والتوزيع، عمان، 2014.
- نبيلة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، الطبعة الأولى، دار لفكر الجامعي، الإسكندرية،2007.
- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الاسكندرية، 2008.
- نعيم مغبغب، حماية الكمبيوتر لأساليب و الثغرات دراسة في القانون المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2006.
- يوسف أبو الحجاج، أشهر جرائم الكمبيوتر و الأنترنت، الطبعة الأولى، دار الكتاب العربي، القاهرة، 2010.

3- المقالات و المجلات:

- إسراء جبريل ورشاد مرعي، الجرائم الالكترونية " الأهداف- الأسباب- طرق الجريمة و معالجتها"، مجلة الدراسات الإعلامية، المركز الديموقراطي العربي، العدد 1، يناير، 2018.
- أيت عبد المالك نادية، التحقيق الجنائي للجرائم، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، المجلد 04، العدد 2، جانفي 2020.
- جمال زين العابدين أحمد أمين، جرائم اختراق النظم الإلكترونية بين التشريع المصري و المغربي، مجلة مستقبل العلوم الاجتماعية، جامعة عبد الملك، المغرب، العدد 1، أفريل 2020.
- حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة الدراسات والأبحاث، جامعة زيان عاشور، الجلفة الجزائر، العدد الأول ، 2009/09/15.
- دليلة العوفي، اشكالية مواكبة الجرائم لمجتمع المعلومات من الفجوة الرقمية إلى الجريمة المعلوماتية، مجلة الحكمة للدراسات الإعلامية و الاتصالية، كنوز الحكمة للنشر والتوزيع، مجلد 4، العدد 08، الجزائر، 2016.
- سبع زيان وسلمى المفتي، صور و أركان الجريمة المنظمة دراسة مقارنة في القانون الإماراتي والقانون الجزائري، مجلة الحقوق والعلوم الإنسانية، العدد1، 2020/10/30.
- سهام خليلي، خصوصية المجرم الإلكتروني، مجلة المفكر، جامعة محمد خيضر، بسكرة العدد ، جون 2017.

- فلاح عبد القادر و آيت عبد المالك نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 2019.
- مازيا عيساوي وسامية عزيز، الجريمة من المنظور السوسيولوجي –الأسباب والآثار–، مجلة الدراسات في سيكولوجية الانحراف، جامعة محمد خيضر بسكرة، المجلد 6، العدد 1، 2021.
- محمد علي سالم وحسون عبيد عبد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل، كلية العلوم الإنسانية، العراق، المجلد 14، العدد 6، 2007 .
- معاشي سميرة، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، جامعة محمد خيضر بسكرة ، الجزائر، العدد 7، 2011.
- مهداوي محمد صالح وأسود ياسين، نظام المراقبة الإلكترونية في التشريع الجزائري، دائرة البحوث والدراسات القانونية السياسية، جامعة عين تيموشنت الجزائر، المجلد 5، العدد ، 2021.
- وهيبة رابح، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر ديسمبر 2014.

4- المذكرات و الأطروحات العلمية:

أ/ الدكتوراه:

- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، رسالة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق و العلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2017.
- شنتير خضرة، آليات القانونية لمكافحة الجريمة الإلكترونية(دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه تخصص قانون جنائي، جامعة أحمد دارية، أدرار 2020.

ب/ الماجيستير:

- سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجيستير في العلوم القانونية، تخصص قانون علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013.

ت/ الماستر:

- لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق، أكلي محند أولحاج، البويرة، 2014.

الفهرس