جامعة الشيخ العربي التبسي –تبسة – الجزائر

كلية الحقوق و العلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تخصص:جريمة وأمن عمومي

بعنوان :

مكافحة الجريمة الالكترونية في التشريع الجزائري

من إعداد الطالب :

*عبد الرؤوف عبد اللطيف

تحت إشراف الأستاذة:

*خذيري عفاف

أعضاء لجنة المناقشة :

الاسم و اللقب	الرتبة العلمية	الصفة في البحث
أجعود سعاد	أستاذ محاضر أ	رئيسا
خذيري عفاف	أستاذ محاضر أ	مشرفا و مقررا
قحقاح وليد	أستاذ محاضر أ	ممتحنا

السنة الجامعية :2022/2021

جامعة الشيخ العربي التبسي –تبسة –الجزائر

كلية الحقوق و العلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تخصص:جريمة وأمن عمومي

بعنوان :

مكافحة الجريمة الالكترونية في التشريع الجزائري

من إعداد الطالب :

*عبد الرؤوف عبد اللطيف

تحت إشراف الأستاذة:

*خذيري عفاف

أعضاء لجنة المناقشة :

الاسم و اللقب	الرتبة العلمية	الصفة في البحث
أجعود سعاد	أستاذ محاضر أ	رئيسا
خذيري عفاف	أستاذ محاضر أ	مشرفا و مقررا
قحقاح وليد	أستاذ محاضر أ	ممتحنا

السنة الجامعية :2022/2021


بسم الله الرحمن الرحيم

﴿ فَتَعَالَى اللَّهُ الْمَلِكُ الْحَقُّ ۗ وَلَا تَعْجَلْ بِالْقُرْآنِ مِن قَبْلِ أَن يُقْضَىٰ إِلَيْكَ وَحْيُهُ ۖ وَقُل رَّبِّ زِدْنِي عِلْمًا ﴾

[سورة طه: 114]

الكلية لا تتحمل أي مسؤولية على ما

يرد في هذه المذكرة من آراء

شكر وعرفان

أولا نتقدم بجزيل الشكر والثناء لله عز وجل الذي أمدنا بالقوة والصبر والرحمة التي لولاها لما تمكنا من إنجاز هذا العمل.

أتقدم بجزيل الشكر وبأحر عبارات التقدير للأستاذة الفاضلة خذيري عفاف التي صبرت معي وأمدتني بكل ما أحتاج من نصائح وتوجيهات فكانت لي خير خير مشرف ومؤطر ونعم مرشد وأعضاء اللجنة الأفاضل.

كما أتقدم بأحر عبارات التقدير والعرفان بالجميل لأبي الثاني الذي لم يتوانى يوما في توجيهي ومساعدتي بكل ما أوتي عمي كمال أبجري

والشكر الجزيل وتحية إجلال وإكبار لعمي الحاج صالح جميعي الذي كان الوصي والأب العطوف والرجل الذي كان ولا يزال واقفا معي

شكرا لكم جميعا

الإهداء

لقد مرت قاطرتنا قاطرة البحث بالعديد من العوائق ولكن بعون من الله تعالى تجاوزتها وأكملت مذكرتي وعملي والأجمل أن نهدي ما تعبنا عليه للغوالي.

إلى من سهرت الليالي الى من فضلتني على نفسها إلى من ضحت من أجلي ولم تتوانى يوما في إسعادي وإعانتي إلى أمي أطال الله في عمرها وحفظها من كل مكروه.

إلى أبي العزيز الغالي رحمه الله تعالى وأسكنه الفردوس العالي.

إلى وحيدة أخيها اختي الكريمة المصون وكل أبنائها حفظهم الله

جميعكم كنتم خيرا سند لي فلكم أهدي ثمرة جهدي

عبد الرؤوف عبد اللطيف

مقدمة

تعد الجريمة نشاط إجرامي يستهدف المساس بالحياة العامة والكيانات العامة وهذا عندما يتعلق الأمر بالنظام العام،هذا من جهة، كما يستهدف أيضا المساس بالحياة الخاصة وهذا عندما يتعلق الأمر بالحرمة الشخصية المقدسة والمحمية قانونا بموجب النصوص القانونية بشكل عام.

وعليه عرفت الجريمة تطورا رهيبا في الآونة الأخيرة، ففي السابق لم يعرف من الجرائم إلا الجريمة الكلاسيكية التي تمثل تعدي بالوسائل التقليدية على النظام العام والحياة الخاصة.

أما في وقتنا الحالي فقد ظهر نوعا آخر من الجرائم تعرف بالجرائم الإلكترونية، والتي ترتكب عن طريق جهاز الحاسوب أو الأجهزة الإلكترونية العلمية المتطورة، فقد تمس هذه الجريمة الحياة الخاصة للفرد، كما قد تمس أيضا بالنظام العام للدولة بصفة عامة.

فلقد أصبحت الجريمة الالكترونية الآن هي ملجأ المجرمين خاصة مع انتشار الأجهزة الالكترونية التي سهلت المهمة وفي ظل الشبكة العنكبوتية التي لا غنى عنها، ففي الآونة الاخيرة ارتفعت معدلات التعدي على الحرمة الشخصية والحياة الشخصية للفرد بنسب عالية فاقت التوقع، ولا نجدها ضربت أطنابها في الجزائر فقط بل في جل العالم لكن الجزائر من بين الدول التي وقعت في فخ المعلوماتية.

وعليه عمل المشرع الجزائري على تجريم هذا النوع من الجرائم" الجريمة الإلكترونية " من خلال إصدار العديد من النصوص القانونية التي تحارب هذه الجريمة سواء من خلال الوقاية منها ، أو ردعها.

أهمية الموضوع:

تكمن أهمية دراستنا لهذا الموضوع في الوقوف على تحديد مفهوم الجريمة الإلكترونية باعتبار أن مفهوم هذه الجريمة يتطور بحسب نوع الجريمة والتطور التكنولوجي الحاصل في

العالم، بالإضافة إلى التعرف عن وسائل التي وضعها المشرع الجزائري من أجل مكافحة هذه الجريمة السيبريانية التي أصبحت من الجرائم الأكثر خطورة في الدولة.

دوافع اختيار الموضوع:

أما عن العوامل والدوافع التي حفزتنا على إختيار هذا الموضوع ، فيمكن إرجاعها إلى عوامل ذاتية وعوامل موضوعية. حيث تمثلت هذه الأخيرة في :

1/ الدوافع الموضوعية:

1- تسليط الضوء على مفهوم الجريمة الإلكترونية باعتبارها من الجرائم الحديثة.
2-معرفة الطرق القانونية التي وضعها المشرع الجزائري من أجل محاربة ومكافحة هذا النوع من الجرائم.

2/ الدوافع الذاتية:

1-الرغبة في البحث في الجرائم الخاصة والحديثة ، وهذا باعتبار الجريمة الإلكترونية من الجرائم المستحدثة والقابلة للتطور.
2-معرفة الطبيعة الجزائية للجريمة الإلكترونية الوقوف على مدى توفق المشرع الجزائري في الحد منها.
3-إثراء المكتبة القانونية ،نظرا لقلة الدراسات في هذا النوع من الجرائم الخاصة بالتحديد.

المنهج المتبع:

1-المنهج الوصفي : وهذا من أجل التعريف بالجريمة الإلكترونية والوقوف على خصائصها.
2-المنهج التحليلي: وهذا من أجل تحليل النصوص القانونية التي تحمي وتكافح الجرمية الإلكترونية.

أهداف الدراسة:

تنوعت أهداف التي نصبوا إليها في هذه الدراسة، إلى أهداف علمية، وأهداف عملية:

1- الأهداف العلمية: الوصول وتشخيص الدقيق لمفهوم الجريمة الإلكترونية وسبل مكافحتها في التشريع الجزائري.

2- الأهداف العملية: معرفة مدى قدرة النصوص القانونية التي وضعها المشرع الجزائري في احتواء هذه الجريمة السيبريانية .

الدراسات السابقة:

ومن الدراسات السابقة التي درست موضوع الجريمة الإلكترونية وفصلت فيه وجدنا العديد من فقهاء القانون المشارق ومنهم الدكتور خالد ممدوح إبراهيم والدكتور خالد عياد الحلبي والدكتور سامي علي حامد عياد .

أما بالنسبة للدراسات السابقة هنا في الجزائر وجدنا عدة أطروحات دكتوراه وعدة مقالات في مجالات قانونية مختلفة كالدكتور سعيداني نعيم والدكتورة سميرة معاشي والدكتور عبد القادر عمير

صعوبات البحث:

ونحن بصدد جمع المادة العلمية لإعداد هذه الدراسة فقد واجهتنا صعوبات، وتمثلت هذه الأخيرة في :قلة المراجع المتخصصة في هذا النوع من جرائم وهذا راجع لحداثة هذه الجريمة وتطورها واختلافها عن الجرائم السابق دراستها والمتعلق بالخصوص بالجريمة السيبريانية. بالإضافة إلى صعوبة الحصول على بعض المراجع الخاصة بهذه الدراسة نظرا لظروف شخصية.

الإشكالية:

حيث يتمحور موضع دراستنا حول إشكال أساسي مفاده:

ما هو النظام القانوني الذي يحكم الجريمة الإلكترونية في التشريع الجزائري؟

ويندرج تحت هذا التساؤل الأسئلة الفرعية الآتية:

1-ما هو مفهوم الجريمة الإلكترونية؟

2- ما هي سبل الوقاية منها ومكافحتها في التشريع الجزائري؟.

التصريح بالخطة:

بناءا على ما سبق طرحه، وتماشيا مع الدراسة التي تناولناها في موضوعنا هذا ، وللإجابة عن الإشكالية السابق طرحها فقد اعتمدنا على التقسيم الثنائي للخطة،وهذا وفق فصلين.

حيث جاء الفصل الأول تحت عنوان : الأحكام الموضوعية للجريمة الإلكترونية

أما الفصل الثاني فكان عنوانه: الأحكام الإجرائية للجريمة الإلكترونية

وعن سبب تقسيم دراستنا هذه لخطة ثنائية، فيعود السبب إلى طبيعة الموضوع والمعلومات المتوفرة لدينا.

الفصل الأول

الأحكام الموضوعية للجريمة الإلكترونية

إن التطور المشهود الذي عرفه مجال المعلوماتية والتقنية في العالم بأسره، أدى إلى اعتماد الحاسب الآلي والشبكة العنكبوتية في كل الجوانب العملياتية والإدارية خاصة ، فأصبح الكمبيوتر وسيلة لا غنى عنها في الوقت الحالي، وزاد تطوره في السنوات الأخيرة بشكل رهيب من خلال إنتاج بشكل يومي لبرامج وتطبيقات تسهل استخدامه وتعبد الطريق لمستعمليه ، لكن بالنظر من زاوية أخرى للكمبيوتر وشبكة الانترنت نجدهم نقمة لعدم الاستعمال الايجابي والصحيح لهما وإلحاق الضرر المادي أو المعنوي للناس لارتكاب جرائم لها علاقة وطيدة بمجال المعلوماتية وهذا بما يعرف اليوم بالجريمة الالكترونية (المعلوماتية) ، وتعتبر الجريمة الالكترونية جريمة مستحدثة لحداثة وسائل ارتكابها ، الأمر الذي أرق الفقهاء ومفسري القانون بوضع تعريف جامع وموحد لها ، كذلك تتسم بعدة خصائص جعلها من أخطر الجرائم في الآونة الأخيرة ، وسنعالجها من خلال مبحثين سنتناول ضمن المبحث الأول مفهوم الجريمة الالكترونية ويندرج تحته التعريف والخصائص وسنتطرق ضمن المبحث الثاني إلى أركان الجريمة الالكترونية (الركن المادي والركن المعنوي)

المبحث الأول : مفهوم الجريمة الالكترونية :

تعتبر الجريمة المعلوماتية من الظواهر الحديثة وذلك لارتباطها بتقنية حديثة هي تكنولوجيا المعلومات والاتصالات والكمبيوتر ، وقد أحاطت بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لهما ، ولكن الفقه لم يتفق على تعريف محدد ، بل إن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني

فالجرائم المعلوماتية هي صنف جديد من الجرائم ، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين ، انتقل بالجريمة من صورها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها ففي بداية ظهور هذه الجرائم كانت هناك إشكالية تواجه المختصين في كيفية مكافحتها لأنها تتعلق بالبيانات والمعلومات ، أي الكيان المنطقي للحاسب الآلي .

فنتيجة التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حتى الآن ، حال ذلك دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة المعلوماتية أو الإلكترونية ، وما ورد من تعريفات في الفقه إنما اقتصر على الناحية محل بحث الفقيه [1] ومما لا شك فيه أن عدم وضع تعريف للجريمة المعلوماتية يثير العديد من المشكلات العملية لعل أهمها ، صعوبة مواجهتها ، وتعذر إيجاد الحلول المناسبة لمكافحتها.

وسوف نقوم بتعريف الجريمة الالكترونية كمطلب أول ونتناول فيه عدة تعريفات منها تعريفات فقهية وتعريف منظمة التعاون الاقتصادي والتنمية وصولا للتعريف التشريعي الجزائري

وكمطلب ثاني سوف ندرس الخصائص التي تتميز بها الجريمة الالكترونية عن باقي الجرائم وسوف تفصل فيها الخاصية تلو الأخرى.

[1] – خالد ممدوح إبراهيم ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ، 2009، ص 73.

المطلب الأول : تعريف الجريمة الالكترونية

سنعرض بعض التعريفات الفقهية التي حاولت وضع تعريف للجريمة الالكترونية كالتالي:

تعرف جرائم الحاسب الآلي و الانترنت بأنها " ذلك النوع من الجرائم التي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها او التحقيق فيها ومقاضاة فاعليها ".

كما يمكن تعريفها بأنها " الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني ".

وهناك من عرفها بأنها " أي عمل غير قانوني يستخدم فيه الحاسب كأداة أو موضوع للجريمة".[1]

عرفها الخبير باركر بأنها " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الفاعل .[2]

وقريب منه هذا التعريف الذي وضعته **منظمة التعاون الاقتصادي والتنمية** الذي يعرفها بأنها .. " كل فعل أو امتناع من شانه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية .

وتعرف جرائم الحاسوب والانترنت بأنها " سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر " ، فالسلوك يشمل الفعل الايجابي والامتناع عن الفعل ، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ،

[1]– سامي علي حامد عياد ، الجريمة المعلوماتية وإجرام الانترنت ، دار الفكر الجامعي ، الاسكندرية ، 2007 ، ص12

[2] – عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة) ، منشورات الحلبي الحقوقية ، بيروت ، لبنان ، 2003، ص 32.

ومعاقب عليه قانونا لأن إصباغ الصفة الجرمية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفا للأخلاق .[1]

الجرائم الالكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت (مثل غرف الدردشة ، والبريد الالكتروني والموبايل) .

وتعتمد تعاريف الجريمة الالكترونية في الغالب على الغرض من استخدام هذا المصطلح . وتشمل عددا محددا من الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة . ويمثل جوهر الجريمة الالكترونية . أبعد من هذا الوصف ، ومع ذلك ، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر ، بما في ذلك أشكال الجرائم المتصلة بالهوية والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الالكترونية ".[2]

التعريف الدولي للجريمة الالكترونية :

– تعتمد تعريفات للجريمة الالكترونية في الغالب على الغرض من استخدام المصطلح

– هناك عدد من الأفعال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمته تمثل جوهر الجريمة الالكترونية.

[1]– الدكتور علي جبار الحسيناوي ، جرائم الحاسوب والإنترنت ، دار اليازوري العلمية للنشر والتوزيع ، عمان ، الأردن ، 2009، ص ،32

[2] – ذياب موسى البداينة ، كلية العلوم الإستراتيجية – الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية ، ورقة علمية بعنوان (الجرائم الإلكترونية : المفهوم والأسباب) ، 2014/09/04، ص 3–4.

– أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر ، بما في ذلك أشكال الأفعال المتصلة بجريمة الهوية ،وجرائم محتويات الكمبيوتر لا تصلح بسهولة للوصول إلى التعاريف القانونية للمصطلح الكلي .[1]

الجريمة الالكترونية عرفت كذلك بأنها " أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية .

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة المعلوماتية ، فهناك من يطلق عليها تسمية الجرائم الالكترونية ، وهناك من يطلق عليها تسمية جرائم المعلوماتية ، في حين يذهب آخرون إلى تسميتها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال ، ويسميها آخرون جرائم الكمبيوتر والانترنت ،وهناك من يطلق عليها تسمية الجرائم المستحدثة.

وبالنظر إليها من الزاوية الأولى نلاحظ أن الجاني يستخدم المعلوماتية لتنفيذ جرائمه سواء ما تعلق منها بجرائم الاعتداء على الأشخاص ... أو ما تعلق منها بجرائم الاعتداء على الأموال.أما إذا نظرنا لجرائم المعلوماتية من الزاوية الثانية ... نلاحظ أن الجاني يتجه قصده إلى الاعتداء على الشيء أو المال المعلوماتي ذاته – أي انه بالنسبة لهذه الجرائم يكون هذا الشيء أو المال المعلوماتي محلا أو موضوعا لها.[2]

بداية لابد أن نشير إلى انه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها : فالبعض يطلق عليها جريمة الغش المعلوماتي ، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي او الاحتيال المعلوماتي ، وآخرون يفضلون تسميتها بالجريمة المعلوماتية.[3]

---

[1] – ذياب موسى البداينة ، مرجع نفسه ، ص 4–5 .

[2] – عفيفي كامل عفيفي ، مرجع سابق ، ص 33

[3] – نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، الطبعة الثانية ، 2010 ، ص 46

تعريف الجريمة الالكترونية في اتفاقية ملس أوروبا للجريمة الالكترونية لعام 2001:

تم التوقيع على هذه الاتفاقية في 23 نوفمبر 2001 في بودابست وتضم في عضويتها 45 دولة أوروبية و17 دولة من خارج أوروبا حتى تاريخ 2014/10/05 ، وعرفت الاتفاقية جرائم الحاسب الآلي في الفصل الثاني بأنها الجرائم ضد السرية و النزاهة وتوافر البيانات وأنظمة الحاسب الآلي في المواد من 2 إلى 12 حيث تم بالترتيب تعريف الدخول الغير مشروع ، الاعتراض غير القانوني ، التدخل في البيانات التدخل في النظام إساءة استخدام الأجهزة .

ثانيا : الجرائم ذات الصلة بالحاسوب : الجرائم المتعلقة بالتزوير ، الجرائم المتعلقة بالغش .

ثالثا : الجرائم المتعلقة بالمحتوى : الجرائم المتعلقة بالمواد الإباحية عن الأطفال .[1]

رابعا : الجرائم المتعلقة بانتهاك حقوق الطبع والحقوق المجاورة : الجرائم المتعلقة بالتعدي على حقوق المؤلف والحقوق المجاورة .

خامسا : المسؤولية الإضافية : المحاولة والعون والتحريض والمسؤولية المؤسسية في المادة.

تعريف الجريمة الالكترونية في التشريع الجزائري :

رغم خلو بعض التشريعات من تعريف الجريمة المعلوماتية إلا ان هناك البعض من التشريعات من أشار إلى تعريفها كما هو الشأن بالنسبة للمشرع الجزائري من خلال المادة ½ من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أنها " كل الجرائم سواء المتعلق بالمساس بالأنظمة أو غيرها من الجرائم الأخرى التي ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو أي نوع آخر من نظم الاتصال الالكتروني ".

[1] – مجمع البحوث والدراسات ، أكاديمية السلطان قابوس لعلوم الشرطة نزوى عمان ، الجريمة الالكترونية في المجتمع الخليجي وكيفية مكافحتها ، مجلس التعاون لدول الخليج العربية ، ص 24

ويمكن أن أشير في هذا المقام أن المشرع الجزائري بداية بموجب القانون 04/15 المعدل والمتمم لقانون العقوبات قد عبر عن الجريمة المعلوماتية بالجرائم ضد الأنظمة المعلوماتية على أساس أنه قد قدر بذلك أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي ، فتحول إلى معلومات بعد معالجتها وتخزينها ، فقام بحماية هذه المعطيات من أوجه عدة . لذلك آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات ، ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلبتكنولوجيات الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها.[1]

وأما عن المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، وهو التعبير الذي استخدمه المشرع الجزائري للتدليل على الجريمة المعلوماتية. فإنه وقبل صدور القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كانت الجريمة المعلوماتية في النظام العقابي الجزائري تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وهي وفقا لدلالة الكلمة تنصرف إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات وهذه الأفعال في الحقيقة ما هي إلا جزء من الظاهرة الإجرامية.

لأجل هذا فقد تبنى المشرع الجزائري حديثا بموجب القانون 04/09 تعريفا موسعا للجرائم المعلوماتية واعتبر أنها تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 إلى المادة 394 مكرر 7 أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون

[1] – رابحي عزيزة ، الأسرار المعلوماتية وحمايتها الجزائية ، أطروحة مقدمة لنيل شهادة الدكتوراه ، جامعة ابو بكر بلقايد ، تلمسان ، 2018/2017، ص ص91.93.

فيها المنظومة المعلوماتية محلا للاعتداء بل توسع نطاقها لتشمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها.[1]

ومن جانبنا نرى بأن الجريمة المعلوماتية من الجرائم الحديثة الناشئة عن التكنولوجيا المتطورة وهذا التطور هو الذي نراه في مرونتها فهي جريمة متجددة بشكل يومي نستطيع القول وخاصة في مجال الحاسب الآلي وشبكة الانترنت وظهور أجهزة تقنية زادت من تطورها بشكل كبير الأمر الذي جعل تعريف الجرائم الالكترونية من قبل الفقهاء ودارسي القانون صعب جدا .

المطلب الثاني : خصائص الجريمة الالكترونية :

ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت أضفى عليها مجموعة من الخصائص والسمات للميزة لهذه الجريمة عن الجريمة التقليدية هي :

أولا : الجريمة المعلوماتية متعدية الحدود أو جريمة عابرة للدول :

المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود .

فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام المعلومات عبر الدول المختلفة ، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد . فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى.

[1] – رابحي عزيزة ، مرجع سابق، ص93.

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة ، وكذلك حول تحديد القانون الواجب التطبيق بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية ، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام .[1]

كانت القضية المعروفة باسم مرض نقص المناعة المكتسبة (الإيدز) من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية ، وتتلخص وقائع هذه القضية التي حدثت عام 1989 في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي في ظاهره إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة ، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس

(حصان طروادة)، إذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس ، وفي الثالث فبراير من عام 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية ، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي ،حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة ، وبالفعل وافق القضاء الأمريكي على تسليم المتهم ، وتم توجيه إحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة ، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية ، ومهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين :

الأولى : أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية

الثانية : أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث (فيروس).[2]

[1] – نهلا عبد القادر المومني ، مرجع سابق ، ص 50.51

[2] – نهلا عبد القادر المومني ، مرجع سابق ، ص 52

ولهذا فإن جرائم الحاسوب تشترك مع غيرها من الجرائم في أنها تتخطى حدود الدول ، كتجارة المخدرات وغسيل الأموال ، إلا أنها تتميز عن الأخيرة حيث يمكن ارتكابها دون مغادرة المقعد المقابل للحاسب الآلي بعكس جرائم المخدرات التي تتطلب حركة بين الدول .

ومن الأمثلة على أن هذه الجرائم عابرة للحدود ، تمكن احد الهواة في أوروبا من حل شفرة أحد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية) ومن ثم أصبح المجال أمامه مفتوحا للعبث ببيانات هذا المركز ، وكذلك الحال عليه في إنتاج الفيروسات.[1]

ثانيا : خطورة الجرائم الالكترونية :

وذلك لمساسها بالإنسان في فكره وحياته الخاصة ، وتمس المؤسسات في اقتصادها ، والبلاد في أمنها القومي والسياسي والاقتصادي . ومن شان ذلك أن يضفي أبعادا خطيرة غير مسبوقة على حجم الأضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات ولا أدل على ذلك من أن التي قيمت حجم الخسائر المادية الناجمة عن هذه الجرائم ، الجرائم قد بلغ وفقا لما بينته الإحصاءات في فرنسا طبقا للجمعية العمومية ضد الحرائق والمخاطر المختلفة سنة 1986 التي حددت قيمة الخسائر ب 7.3 مليار فرنك فرنسي ، كذلك في الولايات المتحدة الأمريكية أين قدمت نقابة المحامين الأمريكيين سنة 1984 تقريرا أشار إلى الحجم الهائل للخسائر التي لحقت بحوالي ثلاثمائة من أكبر الشركات هناك ، إذ يشير التقرير إلى معدل الخسارات السنوية لتلك الشركات الذي يتراوح من 2 إلى 15 مليون دولار سنويا . كما قدرت حجم الخسائر المادية لهذه الجرائم وفقا لتقديرات المركز الوطني لجرائم الحاسب الآلي في الولايات المتحدة الأمريكية حوالي 500 مليون دولار أمريكي سنويا بينما قدرتها مصادر أخرى بما يتراوح بين 3 و5 بليون دولار في السنة ، ولا شك أن هذه الخسائر قد فاقت بكثير تلك الأرقام في عصرنا الحالي.

[1] – محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، الطبعة الأولى الإصدار الثاني ، 2009 ، ص 34

وتعتبر البنوك الهدف الرئيسي للجيل الجديد من مجرمي تقنية المعلومات ، ذلك لاعتمادها كليا على أنظمة نقل التمويل إلكترونيا.[1]

ورغم استمرار تطور الظاهرة الالكترونية خلال حقبة السبعينيات ، إلا أن الحالات التي سجلت في تلك الفترة الزمنية كانت قليلة ، وقد تعود أسباب تلك القلة إلى كون مكمن الخطر كان داخليا ، ويكاد أن يكون خطرا ينحصر بين العاملين على الأنظمة الحاسوبية نفسها حيث كانوا هم فقط من يستطع الوصول إلى تلك الأنظمة بصورة مباشرة ولم يكن هناك اتصال بتلك الأنظمة من العالم الخارجي ، كما أن سبب قلتها أيضا يعود إلى عدم الإبلاغ عن الكثير من تلك الجرائم لكون الشركات والوكالات كانت تحرص على عدم اهتزاز الثقة بها وبأنظمتها الحديثة ، وأعقبت تلك الحقبة الزمنية إجراء دراسات ومقالات صحفية بشأن الجريمة الالكترونية من قبل كثير من الباحثين الصحفيين.

وفي السبعينيات أيضا شهد العالم بداية لظهور بعض التشريعات والقوانين التي تجرم بعض الممارسات ذات الصلة بإساءة استخدام الحاسوب وقررت لها عقوبات محددة كما حصل في السويد والتي اعتبرت بذلك أول دولة يصدر فيها قانون يجرم بعض الأفعال والممارسات المرتبطة بالحواسيب.

أما في عقد الثمانينات فقد حدث تغيرا ملحوظا في التعامل مع ظاهرة الجريمة الالكترونية وذلك من جانب الباحثين والعامة على السواء بسبب ارتفاع مؤشر عدد القضايا ذات الصلة بإساءة استخدام الحاسوب ولا سيما بعد اهتمام الصحافة وإبرازها لتلك القضايا حيث أصبح بعضها يؤرق المجتمع الدولي كقضايا الاختراق وقرصنة البرمجيات والتلاعب في أنظمة النقد الالكتروني وانتشار العديد من أنواع الفيروسات . كما شهد ذلك العهد الانطلاقة الأولى للقوانين والتشريعات الخاصة بحماية البرامج الحاسوبية والتي أطلق عليها قوانين حماية الملكية الفكرية واعتبرت من القوانين الأكثر وضوحا ونضجا.

[1] – سميرة معاشي ، ماهية الجريمة المعلوماتية ، مجلة المنتدى القانوني ، العدد السابع ، قسم الكفاءة المهنية للمحاماة ، جامعة محمد خيضر ، ص 281

وكذلك في تلك الفترة الزمنية ظهر الاهتمام العربي بظاهرة الجريمة الالكترونية وتمثل ذلك في صدور العديد من الدراسات العلمية والمؤلفات العربية ذات الشأن بالجريمة الالكترونية وعقد الندوات المختلفة ذات الصلة بذلك حيث عقدت سنة 1986 ندوة أمن المعلومات في الحاسبات الآلية والتي تبناها مركز المعلومات الوطني التابع لوزارة الداخلية السعودية .

وشهدت التسعينات والسنوات الأولى من القرن الحادي والعشرين تحولات في مجال الجريمة الالكترونية حيث ارتبط ذلك بتحول شبكة الانترنت في ذلك الوقت من شبكة أكاديمية إلى شبكة تعنى بخدمة المجالات التجارية و الفردية حيث بلغ مستخدميها في عام 1996 ما يقارب 40 مليون مستخدم ، وفي عام 2014 تجاوز عدد المستخدمين أكثر من ثلاثة مليار مستخدم الأمر الذي أدى إلى خلق عبئ كبير على المختصين بمكافحة الجريمة الالكترونية ، ولذلك وجد مفهوم جديد عرفها بالجرائم العابرة حيث يستطيع المجرمون تنفيذ مخططاتهم الإجرامية في دول متعددة دون الاكتراث بآية حدود دولية. [1]

ثالثا : يتطلب لارتكابها وجود جهاز الكتروني ومعرفة بتقنية استخدامه :

تتميز الجريمة الالكترونية عن غيرها أن الجهاز الالكتروني هو أداة الجريمة ووسيلة تنفيذها ، أو هو موضوع الجريمة كإتلاف أو سرقة البيانات والمعلومات وهنا تثور المشكلة ، أما لو كان موضوع الاعتداء هو الجهاز نفسه أو شاشته أو الكيانات المادية للحاسب الآلي فهنا تكفي نصوص التجريم التقليدية ، ويطبق قانون العقوبات على موضوع الجريمة ، فبدون الجهاز الالكتروني تنتفي الجريمة الالكترونية ، وتتطلب هذه الجريمة دراية كافية وخبرة فائقة بالكمبيوتر والانترنت في بعض الجرائم ، أو معرفة بسلوكيات الفعل المرتكب في الجرائم البسيطة منها ، كما أنها لا تمتاز بالعنف ، وأغلب الجرائم الالكترونية ترتكب عبر الانترنت.

ولذلك فإن ما يميز الجريمة الالكترونية عن غيرها من الجرائم ، أنها تتطلب وجود علم كافي بالجوانب الفنية والتقنية لاستخدام الحاسوب والانترنت ، وتعتبر العلاقة بين مدى الدراية

[1] – مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى سلطنة عمان ، مرجع سابق ، ص 25–27

بالجوانب الفنية والتقنية للحاسوب وبين الجريمة الالكترونية علاقة طردية ، فكلما زادت الخبرة لدى الأفراد بمعرفة تقنيات الحاسوب ، زاد احتمال استخدام خبرتهم بشكل غير مشروع.

وأثبت الواقع العلمي أن الجرائم الالكترونية قد ترتكب من خلال الهواتف المحمولة ، خاصة بعد ظهور أجهزة الهاتف الذكية والتي هي في الحقيقة عبارة عن أجهزة كمبيوتر صغيرة ، والتي من خلالها يتم الاتصال بشبكة الانترنت ، ويسهل تخزين ونقل المعلومات من خلالها ، وليس كما ذكر بعض الباحثين بأن الحاسب الآلي هو الأداة الوحيدة في ارتكاب الجريمة الالكترونية ، ففي أيامنا هذه نرى انه يمكن تصنيف هواتف المحمول الذكية ضمن أجهزة الكمبيوتر ، وذلك لأنه لا يختلف عن الحاسوب سواء في الحجم – بل أن الهواتف الذكية يمكن من خلالها الاتصال المباشر بخلاف الحاسب الآلي – أما بالنسبة للوظائف الأخرى فتتم ممارسة جميع وظائف الحاسب الآلي من خلال الهاتف الذكي.[1]

ويمثل علاج المشكلة السابقة من خلال وجود برامج حماية على كل أجهزة الحاسوب سواء المنزلية أو المتوافرة في أماكن العمل ، وذلك لضمان الحفاظ على الأسرار الشخصية والمهنية ، وعدم جعل الجهاز متصل بالإنترنت والتيار الكهربائي خارج وقت الاستخدام له .

رابعا : صعوبة الكشف عن الجريمة المعلوماتية وصعوبة إثباتها :

لا تحتاج برامج الاعتداء على برامج ومعلومات الحاسب الالكتروني إلى أي عنف أو جثث أو سفك للدماء او آثار اقتحام لسرقة الأموال ، وإنما هي بيانات ومعلومات تغير أو تعدل أو تمحى كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الالكتروني ، لذا يكون من الصعب اكتشافها ومن ثم تطبيق الجزاء الجنائي على مرتكبيها .

وهناك صعوبة أخرى تتعلق بإثبات الجرائم المعلوماتية حيث أن هذه الجرائم لا تترك أي أثر خارجي ومرئي لها ، ومما يزيد من صعوبة إثباتها ارتكابها في الخفاء وعدم وجود أي أثر

[1] – يوسف خليل يوسف العفيفي ، الجرائم الالكترونية في التشريع الفلسطيني (دراسة تحليلية مقارنة) ، الجامعة الإسلامية ، غزة ، 2013، ص 14

كتابي ملموس لما يجري خلال تنفيذها من عمليات وأفعال إجرامية حيث يتم استخدام النبضات الالكترونية في نقل المعلومات .

كما توجد صعوبات أخرى تكتنف إثبات هذه الجرائم تكمن في المجرمين الذين يخططون لمثل هذا النوع من الجرائم هم دائما أصحاب ذكاء ودهاء وخبرة ودراية واحتراف في مجال تقنية المعلومات وبالتالي فهم يخططون لهذه الجرائم بطرق محكمة تكفل نجاحهم في ارتكاب الجريمة وفرارهم من أعين السلطات كما يستخدم المجرمون المخططون لهذه الجريمة وسائل تقنية متطورة يصعب على الغير معرفتها والتعامل معها ، بالإضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي لإثبات هذه الجرائم ، بالشكل الذي يوجب البحث عن أدلة جديدة وحديثة ناتجة من ذات الحاسب الآلي ، وهنا تبدأ صعوبات البحث والتحري عن الدليل ، وجمع هذا الدليل ، وتبدأ إشكالية قبوله إن وجد ومدى مصداقيته على إثبات جريمة تنصب على عناصر غير مادية (معلومات وبرامج) .[1]

خامسا : الجرائم الالكترونية جرائم الأذكياء :

إن مرتكب الجريمة الالكترونية في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب وكيفية تشغيله ، وكيفية تخزين المعلومات والحصول عليها في حين أن مرتكب الجريمة التقليدية في الغالب شخص أمي بسيط متوسط التعليم .[2]

تعد المهارة التقنية المطلوبة لتنفيذ جرائم الانترنت أبرز خصائص مجرمي الانترنت ، فتنفيذ هذه الجرائم يتطلب قدرا من المهارات التقنية، سواء تم اكتسابها عن طريق الدراسات المتخصصة ، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات ، إلا أن ذلك لا

[1] – عادل يوسف عبد النبي شكري ، الجريمة المعلوماتية وأزمة الشرعية الجزائية ، مجلة الجريمة المعلوماتية (العدد السابع) ، جامعة الكوفة كلية القانون .

[2] – بوضياف اسمهان ، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، جامعة محمد بوضياف المسيلة ، ص356 .357

يعني ضرورة أن يكون مجرم الانترنت على قدر كبير من العلم في هذا المجال ، فالواقع العملي أثبت أن أشهر مجرمي الانترنت لم يحصلوا على مهاراتهم التقنية عن طريق التعليم او الخبرة المكتسبة من العمل في هذا المضمار.[1]

سادسا: الجرائم ترتكب عبر شبكة الانترنت :

تعد شبكة الانترنت هي حلقة وصل بين كافة الأهداف المحتملة لتلك الجرائم ، كالبنوك والشركات الصناعية وغيرها من الأهداف التي ما تكون غالبا الضحية لتلك الجرائم وهو ما دعا معظم تلك الأهداف على اللجوء على نظم الأمن الالكتروني في محاولة منها لتحمي نفسها من تلك الجرائم على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم.[2]

سابعا : عدم وجود مفهوم مشترك للجريمة الالكترونية :

لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها ، فالبعض يطلق عليها جريمة الغش المعلوماتي ، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي وآخرون يفضلون تسميتها بالجريمة المعلوماتية .

ومن وجهة نظر الباحث فإنه يفضل اصطلاح الجريمة الالكترونية للدلالة على الجرائم المرتكبة بواسطة الحاسوب والانترنت ، فاصطلاح الجريمة الالكترونية عام ويشتمل وسائل الاتصال الالكترونية الحالية والمستقبلية المستخدمة في التعامل مع البيانات وتبادلها.

كما أن التطور التكنولوجي نتج عنه تطور في طرق إثبات الجريمة والتعامل معها ، فالجرائم العادية يسهل غالبا تحديد مكان ارتكابها في حين انه من الصعوبة تحديد مكان وقوع الحادثة عند التعامل مع الجرائم الالكترونية ، لكون الرسائل وملفات الكمبيوتر تنتقل من نظام

[1] – محمد طارق عبد الرؤوف الخن ، جريمة الاحتيال عبر الانترنت ، منشورات الحلب الحقوقية ، بيروت ، لبنان، الطبعة الأولى ، 2011، ص 32

[2] – عبد الحكيم رشيد توبة ، جرائم تكنولوجيا المعلومات ، دار المستقبل للنشر والتوزيع ، الطبعة الأولى ، 2009، ص 140

معلوماتي إلى آخر في ثوان معدودة ، كما أنه لا يقف أمام انتقال الملفات والمستندات والرسائل عبر شبكة الانترنت آية حدود دولية أو جغرافية ، ونتيجة لذلك فإن تحديد أي محكمة تحدد أي قانون يطبق سوف يكون مشكلة بين الدول مما يستدعي التعاون بين دول العالم.

كما أن مشروعية الجريمة أمر نسبي من دولة إلى أخرى ، فمثلا تجارة المخدرات في الأردن والكويت والجزائر محرمة نهائيا ، بينما في الدول الاسكندينافية مصرح بها في حدود الاستعمال الشخصي فقط ، بل إن مشروعية الجريمة قد تختلف داخل البلد الواحد ، فمثلا نجد داخل الولايات المتحدة الأمريكية أن ألعاب القمار عبر الانترنت مسموح بها في ولاية لاس فيجاس بينما هي محرمة قانونا في ولاية نيويورك .[1]

ثامنا : خصوصية مجرم المعلومات : قد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة ، ولكن الأمر مختلف تماما بالنسبة للمجرم المعلوماتي والذي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات .

وقد تم تصنيف مجرمي الجرائم الالكترونية إلى المخترقين والمحترفين والحاقدين.

أ – **المخترقون :** مثل الهاكرز الذي يعد شخصا بارعا في استخدام الحاسب الآلي ولديه فضول في استخدام حسابات الآخرين بطرق غير مشروعة ، الأمر الذي يدل على أنهم أشخاص متطفلون وغير مرحب بهم لدى الغير ، وأغلبهم ما يكون جانبهم تحدي الشباب للدخول إلى المواقع الرسمية ، وبعض الأحيان الدخول إلى مواقع الحسابات من أجل إثبات الذات ، وغالبا ما تكون أعمارهم في سن المراهقة.

ب – **المحترفون :** وهم الأكثر خطورة بين مجرمي الانترنت ، حيث يهدف البعض منهم الى الاعتداء لتحقيق الكسب غير المشروع المتمثل في الناحية المادية وذلك عبر الدخول في

[1] – عبد الله دغش العجمي ، المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة ، رسالة ماجستير ، جامعة الشرق الأوسط ، 2014، ص 22.23

حسابات البنوك ، والبعض الآخر يدخل من أجل تحقيق أغراض سياسية والتعبير عن وجهة نظره او فكرة ، وغالبا أعمال هؤلاء تكون بين 25 و 40 سنة.

ج- **الحاقدون** : وهم الذين ليس لديهم أي أهداف للجريمة ولا يسعون لمكاسب سياسية او مادية ولكن يتحركون لرغبة في الانتقام والتأثر كالأمور الطائفية.[1]

تاسعا : وقوع الجريمة الالكترونية أثناء المعالجة الآلية للمعطيات :

من خصائص الجريمة الالكترونية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر ، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الالكترونية الخاصة بالتعدي على نظام البيانات ، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الالكترونية.

" وقد كان هناك اقتراح من قبل مجلس الشيوخ الفرنسي حال تعديل قانون العقوبات الحالي ، بوضع تعريف محدد لعملية المعالجة الآلية للبيانات أو المعطيات ، ولطن حذف هذا التعريف باعتبار أنها عملية فنية تخضع للتطور السريع ، وبالتالي سيكون أي تعريف لها قاصرا ، وكان هذا التعريف ينص على أنها: " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة ، والتي تتكون كل منها من الذاكرة ، والبرامج ، والمعطيات ، وأجهزة الإدخال والإخراج ، وأجهزة الربط والتي يربط بينها مجموعة من العلاقات والتي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام الحماية الفنية".

والجريمة الالكترونية قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات سواء عند مرحلة إدخال البيانات ، أو أثناء مرحلة المعالجة ، أو أثناء مرحلة إخراج المعلومات.[2]

عاشرا : جرائم يندمج فيها الفضاء الالكتروني مع العالم الواقعي :

[1] – عبد الله دغش العجمي ، مرجع سابق ، ص 21.22

[2] – عبد الله دغش العجمي ، مرجع سابق ، ص24

نتيجة لارتباط الفضاء الالكتروني الافتراضي مع العالم الواقعي افرز لنا هذا النوع من الجرائم الهجينة، فبمجرد الولوج للفضاء الالكتروني والبدء بتنفيذ الفعل المجرم فإننا نصبح أمام مسرح عمليات، ومن خلال هذا المسرح تتكون الجريمة الالكترونية وتتحقق أركانها لتجد الجريمة الالكترونية طريقها إلى الواقع بعد أن تتبلور على هيئة نتيجة إجرامية أو فعل غير مشروع، فهجوم إلكتروني واحد مكتمل الأركان عبر الشبكة المعلوماتية والعالم الافتراضي كالذي استهدف أنظمة المعلومات لشركة الخطوط الجوية البولندية وأدى إلى إلغاء العشرات من الرحلات كان يفترض أن تقلع من مطار شوبين في وارسو كانت نتيجته الإجرامية في العالم الواقعي هي تعطل حركة الملاحة في المطار وعدم تمكن ما يزيد عن ألف وأربعمائة مسافر من السفر لعدة ساعات بالإضافة إلى الخسائر المادية والمعنوية التي لحقت بالشركة جراء ذلك الهجوم.[1]

الحادي عشر : امتناع المجني عليهم عن التبليغ:

لا يتم في الغالب الأعم الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها إما خشية من التشهير، لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة، والعدد الذي تك اكتشافه، هو رقم خطير وبعبارة أخرى الفجوة بين عدد هذه الجرائم الحقيقي وما تم اكتشافه فجوة كبيرة.

تتبدى هذه الظاهرة على نحو أكثر حدة في المؤسسات المالية كالبنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة، حيث تخشى مجالس إدارتها عادة أن تؤدي الدعاية

[1] – إبراهيم محمد بن حمود الزنداني ، الجرائم الإلكترونية من منظور الشريعة الاسلامية وأحكامها في القانون القطري والقانون اليمني : دراسة مقارنة ، حقوق الطبع محفوظة لجامعة فطاني ، جامعة فطاني – 2018 ، ص 41

السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها.[1]

الثاني عشر : سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه:

تكون البيانات والمعلومات المتداولة عبر شبكة الانترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا لا سيما وأن الجاني يتعمد إلى عدم ترك أثر لجريمته، ضف إلى ذلك ما يتطلبه من فحص دقيق لموقع الجريمة من قبل مختصين في هذا المجال للوقوف على إمكانية وجود دليل ضد الجاني ، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة .

تتم الجريمة المرتكبة عبر الانترنت خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة.

يعيق المجرم في جرائم الانترنت سلطات التحقيق الوصول إلى الدليل بشتى الوسائل، كمسح برامج أو وضع كلمات سرية ورموز قد يلجأ لتشفير المعلومات لمنع إيجاد أي دليل يدينه.

يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم ذلك عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب، على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما إن يحس

[1] – صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، مذكرة لنيل شهادة الماجستير في القانون ، جامعة مولود معمري ، تيزي وزو ، 2013، ص 18

الجاني بأن أمره سينكشف حتى يبادر بإلغاء هذه الأوامر ، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبها أمرا في غاية الصعوبة.[1]

الثالث عشر : نقص الخبرة لدى الأجهزة الأمنية والقضائية وعدم كفاية القوانين السارية:

تتميز جرائم الانترنت بالكثير من السمات التي جعلتها تختلف عن غيرها من الجرائم ، الأمر الذي أدى إلى تغيير شامل في آلية التحقيق وطرق جمع الأدلة المتبعة من الجهات التي تقوم بعملية التحقيق، وإضافة أعباء تتعلق بكيفية الكشف عن هذه الجريمة وأدلتها، وكذا القضاء من خلال تعديل الكثير من مفاهيمه التقليدية سواء فيما يتعلق بالأدلة أو تطبيقاتها أو لقوتها في الإثبات.

ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلبه لاكتشافها والبحث عنها، وتستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي ضد هذه الظاهرة.

لم تعد قادرة القوانين على مواكبة هذه السرعة الهائلة في التكنولوجيا، والتي أدت إلى تطور الجريمة من خلالها، وظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها، مما تطلب تدخل المشرع لسن قوانين حديثة لمواجهة هذه الجرائم حفاظا على مبدأ الشرعية الجنائية، مع تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها.[2]

المبحث الثاني : أركان الجريمة الإلكترونية :

إن أركان الجريمة عموما هي تلك العناصر التي لا وجود للجريمة بدونها ، حيث تدور الجريمة معها وجودا وعدما ، وتتمثل الأركان العامة في العناصر المكونة للركن المادي ، من

[1] – صغير يوسف ، مرجع سابق ، ص 18.19.

[2] – صغير يوسف ، المرجع نفسه ، ص 19.20.

سلوك ونتيجة وعلاقة سببية ، وأخيرا الركن المعنوي القائم على العلم والإرادة ، أما الأركان الخاصة فهي ما يورده المشرع من عناصر في النص لقيام الجريمة بالإضافة إلى الأركان السابقة.

غير أن ما يميز الجريمة المعلوماتية عن غيرها ، من الجرائم – كما سبق الذكر– هو أن وجود نظام المعالجة الآلية للمعطيات يعد بمثابة الشرط الأولي أو الركن الخاص الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان آية جريمة من جرائم الاعتداء على هذا النظام ، وقد عرف المشرع الجزائري نظام المعالجة الآلية للمعطيات بأنه " كل نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة بعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين " ، وهو نفس التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي المبرمة ببودابست 2001.[1]

وكمطلب أول نقوم بدراسة الركن المادي المكون للجريمة الالكترونية وما يحتويه من سلوك إجرامي ونتيجة والعلاقة السببية بينهما

وكمطلب ثاني ندرس الركن المعنوي المكون للجريمة الالكترونية وما يتخلله من علم وإرادة كعنصرين أساسيين للركن المعنوي .

المطلب الأول : الركن المادي :

يتكون الركن المادي من السلوك الإجرامي المتمثل في < فعل الاستعمال > أي استعمال الجاني جهاز الحاسب استعمالا يضر بالغير سواء أفراد وشركات عامة أو خاصة أما النتيجة الإجرامية تتمثل في التدخل في خصوصيات الغير دون وجه مشروع بإتلاف للبيانات وتزوير للمعلومات ومشابه من قرصنة واختراق . أما العلاقة السببية فهي المشكلة وذلك لأن الفرق الرئيس بين الجريمة الالكترونية والجريمة العادية يظهر في علاقة سببية ودليل الإثبات الجنائي

[1] – زيوش عبد الرؤوف ، الجريمة المعلوماتية في التشريع الجزائري ، مجلة العلوم القانونية والاجتماعية جامعة زيان عاشور الجلفة ، 2019 ، ص 132.133

ما ذكره أحد القادة العسكريين < أثبت أنه أنا ليس أنا > فكل النظرية التي قال بها الفقهاء القانون يصعب تطبيقها على الجريمة الالكترونية سوء نظرية السببية الملائمة ونظرية تعدد الأسباب والسبب في ذلك صعوبة القبض على الجاني وصعوبة اكتشاف الدليل الجنائي الرقمي.[1]

جرائم المعلوماتية تتخذ عدة أشكال تتعدد بتعدد صور الاعتداء الواقع على نظام المعلوماتية بحد ذاته والتي نوردها كما يلي :

1- الدخول والبقاء غير المرخص بهما في النظام

يقصد بفعل الدخول هنا وهو الركن المادي لجريمة الاعتداء على نظام المعالجة الآلية للمعطيات ، ذلك الدخول المعنوي أو الالكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي ، ولا يعد فعل الدخول بحد ذاته سلوكا غير مشروع وإنما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص هو ما يستشف من المادة 394 مكرر من قانون العقوبات.

لاحظ من خلال هذه المادة أن المشرع الجزائري اعتبر جريمة الدخول غير المرخص به بمثابة جريمة شكلية التي لا يشترط لقيام الركن المادي فيها بتحقق النتيجة الإجرامية ، أي أنه جرم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات بأكمله أو إلى جزء منه فقط، بشرط ان يكون فعل الدخول بدون الترخيص مقصودا وليس صدفة أو خطأ.

نعتقد أن المشرع الجزائري قد أصاب كثيرا عندما جرم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش أي بدون ترخيص وبغض النظر عن ما إذا كان النظام المتعدى عليه محاطا بحماية فنية أم لا، لأنه بذلك يكون قد جعل من هذا التدبير بمثابة تدبير تحفظي وقائي سيساهم بشكل كبير في التصدي لظاهرة الإجرام المعلوماتي ، من خلال غلق الباب أمام المجرمين من التهرب من المسؤولية الجزائية عن فعل الاعتداء، بحجة أن

[1] – عبد الصبور عبد القوي علي المصري ، التنظيم القانوني للتجارة الالكترونية ، مكتبة القانون والاقتصاد ، الرياض ، السعودية ، د ط ، ص 94.

النظام المعتدى عليه لم يكن محاطا بحماية فنية ، وفي تفادي ارتكاب جرائم أكثر شدة على نظام المعالجة وبياناته كإتلاف النظام أو محو وتعديل معطيات النظام.[1]

أما فيما يخص البقاء غير المرخص به في نظام المعالجة الآلية للمعطيات فيقصد به استمرارية التواجد داخل نظام المعالجة دون إذن صاحبه أو من له السيطرة عليه، بمعنى آخر هو بقاء شخص داخل نظام المعالجة الآلية للمعطيات ملك الغير بعد الدخول إليه خطأ أو صدفة، رغم علمه بأن بقاءه فيه غير مرخص.

اعتبر المشرع الجزائري على غرار المشرع الفرنسي فعل البقاء الغير مرخص به في نظام المعالجة الآلية للمعطيات جريمة مثلها مثل جريمة الدخول الغير المرخص به وذلك بموجب المادة 394 مكرر من قانون العقوبات وحدد لهاتين الجريمتين نفس العقوبة.

ومن خلال نص نفس المادة أورد المشرع الجزائري ظرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية، بحيث يتحقق الظرف الأول إذا نتج عن الدخول أو البقاء تخريب نظام اشتغال المنظومة وإعاقته عن أداء وظيفته، وهذا بتوفر علاقة سببية بين فعل الدخول أو البقاء غير المرخص به والنتيجة الإجرامية التي حددتها المادة في محو أو تعديل بيانات النظام أو تخريب تشغيل النظام ذاته.[2]

2- الاعتداء على المعطيات الداخلية للنظام :

لقد جرم المشرع الجزائري أي اعتداء يقع على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات من خلال المادة 394 مكرر 1 قانون العقوبات، وحدد في ذات المادة صور الاعتداء على معطيات النظام الداخلية على سبيل الحصر ولم يدع أ مجال للاجتهاد فيها، مما يدل على أن أي اعتداء لا يحمل إحدى هذه الصور: الإدخال، المحو أو التعديل فهو مستبعد ولا يخضع لأحكام المادة 194 مكرر 1:

[1] – زيوش عبد الرؤوف ، مرجع سابق ، ص 133.134.

[2] – زيوش عبد الرؤوف ، المرجع نفسه ، ص 134

فبالنسبة للإدخال: يقصد به إضافة معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام والتي تمت معالجتها آليا.

وأما المحو: يعني إزالة من معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الآلية أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة.

أما التعديل: يعني تغيير المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات واستبدالها بمعطيات أخرى.

ولا يشترط اجتماع هذه الصور الثلاثة، بل يكفي أن يصدر عن الجاني إحداها لكي يكتمل الركن المادي لجريمة الاعتداء على معطيات نظام المعالجة.

يرجع سبب تجريم المشرع الجزائري للأفعال المذكورة أعلاه بنص مستقل عن جريمتي الدخول والبقاء غير المرخص بهما في نظام المعالجة، واللتان تمثلان الطريق العادي للوصول إلى المعطيات الموجودة داخل النظام وارتكاب جريمة محو أو إدخال أو تعديل ضدها، إلى وجود طرق أخرى لاقتراف هذه الأفعال عن بعد أي دون الدخول أو البقاء في النظام، كاستخدام مثلا القنابل المعلوماتية الخاصة بالمعطيات أو برامج الفيروسات.

وقد أصاب المشرع في ذلك لأنه بوضعه نص المادة 394 مكرر 1 يكون قد جرم أفعال المحو والإدخال والتعديل الواقع على معطيات النظام مهما كانت الوسيلة المستعملة والطريقة المتبعة لتحقيق ذلك .[1]

إن السلوك الإجرامي في الجريمة الالكترونية يرتبط دائما بالمعلومة المخزنة على الحاسب الآلي، أو تلك التي يتم إدخالها للحاسب الآلي، وصعوبة المشكلة أن السلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك أو إساءة استعمال بطاقات الائتمان.

[1] – زيوش عبد الرؤوف ، مرجع سابق ، ص 135.

إن السلوك الإجرامي بوصفه عنصرا في الركن المادي في الجريمة التقليدية يتم رؤيته رؤى العين والتأكد منه كفعل القتل أو السرقة أو التزوير، ولكن صعوبة الجريمة الالكترونية ، والركن المادي فيها خاصة أن الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي لا يمكن الإمساك ماديا بها، تماما مثل التيار الكهربائي الذي يسري في توصيلة دون أن نراه، لذلك يتعين تحليل السلوك الإجرامي في الجريمة الالكترونية خاصة ما يتعلق فيها بفكرة المال في جرائم الاعتداء على المال العام أو الخاص، كما لابد من العرض لصور السلوك الإجرامي في الجريمة الالكترونية.[1]

إن النشاط أو السلوك المادي في الجريمة الالكترونية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الانترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فعلى سبيل المثال يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن بقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها، وليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء ، فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال، فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

إن النشاط أو السلوك المادي في الجريمة الالكترونية يعد محلا لتساؤلات عديدة فيما يتعلق ببدايته أو الشروع في ارتكاب الجريمة، ومثل هذا النشاط يختلف عما هو الحال عليه في العالم المادي، فارتكاب الجريمة عبر الانترنت يحتاج بالضرورة إلى منطق تقني، وبدونه لا

[1] – عبد الله دغش العجمي ، مرجع سابق ، ص27.

يمكن للشخص حتى الاتصال بالإنترنت، سواء كان بقصد ارتكاب جريمة أم لمجرد التصفح أو الدخول في الاتصال المباشر كالمحادثة وغيرها.[1]

تثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة، فهل تقتصر على العالم الافتراضي، أم أن لها جزءا في العالم المادي، وهل تقتصر النتيجة على مكان واحد أو تمتد لتشمل دولا وأقاليم عدة، فعلى سبيل المثال إذا قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم أحد البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين.

تحديد رابطة السببية في مجال أضرار الانترنت يعد من المسائل الصعبة والمعقدة بالنظر إلى تعقيدات صناعة الحاسوب والانترنت، وتطور إمكانياتها وتسارع هذا التطور، إضافة إلى تعدد وتنوع أساليب الاتصال بين الأجهزة الالكترونية وتعدد المراحل التي تمر الأوامر المدخلة حتى تخرج وتنفذ النتيجة المراد الحصول عليها، كل ذلك سيؤدي حتما إلى صعوبة تحديد السبب أو الأسباب الحقيقية للإساءات المرتكبة في هذه المسؤولية.[2]

أولا : جريمة الغش المعلوماتي:

الركن المادي فيها هو تغير الحقيقة في مستند رسمي أو محرر رسمي ولكن المستند هنا ليس مستند عادي يدخل ضمن أدلة الإثبات بل هو عبارة عن تسجيلات الكترونية أو محررات الكترونية.

ثانيا : المواقع الإباحية :

[1] – عبد الله دغش العجمي ، مرجع سابق ، ص 27.28.

[2] – صغير يوسف ، مرجع سابق ، ص 68.

فتزود مواقعها بالصور وأفكار الشذوذ الجنسي وهناك مواقع تنشر فكرة الانتحار أو تشويه صور الإسلام.

ثالثا : مواقع القمار :

فهي لغسيل الأموال فالركن المادي هنا سلوك المجرم المعلوماتي في تزويد المواقع بالمعلومات اللازمة للانحراف أو القتل وهذا المجرم أقل من المخترق أو المتسلل هذا فيما يخص السلوك الإجرامي أما النتيجة فهي الأثر المادي المتمثل في انحراف المجتمع وتدمير الأخلاق والمعتقدات وظهور عادات غريبة على المجتمع وزيادة إلى تفشي العنف فتصبح المواقع من طرف المجرم مرتبطة بالتأثيرات الخطيرة التي يتحمل عبؤها المجتمع من انحراف وهذا ما يعرف بالعلاقة السببية.

إلا أن بعض الفقهاء يذهبون إلى تأييد انطباق نصوص التجريم التقليدية على الجرائم الواقعة على المعلومات الموجودة داخل الكمبيوتر إذا قام شخص بالدخول إلى جهاز الحاسوب واطلع على البرامج والمعلومات فهي سرقة ويستندون في ذلك إلى أن البرامج والمعلومات لها كيان مادي يمكن رؤيته على الشاشة مترجمة إلى أفكار ويمكن حيازتها عن طريق نسخها على قرص أو شريط ممغنط.[1]

رابعا : جريمة الإتلاف:

فإن الركن المادي يتمثل بالنشاط الإجرامي المتمثل للركن المادي، فلجريمة الإتلاف صور منها الإدخال غير المشروع للمعلومات أي إدخال معطيات لم تكن موجودة مسبقا يهدف للتشويش على صلة المعلومات والبيانات القائمة حيث أدانت محكمة استئناف باريس 1990 أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بإدخال معلومات وبيانات غير صحيحة إلى نظام الحاسب الآلي، وكذلك تدمير البيانات والمعلومات، فقد أوصى المؤتمر الخامس عشر للجمعية

[1] – حسنين خالد محمد ، الجرائم الالكترونية ، بحث مقدم الى مجلس كلية القانون والعلوم السياسية كجزء من متطلبات نيل درجة البكالوريوس في القانون ، جامعة ديالى ، العراق ، 2017 ، ص 17. 16.

الدولية لقانون العقوبات 1994 بتجريم الأفعال التي تؤدي إلى تدمير المعلومات، تمثل هذه الأفعال: المحو يعني(إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة) الإتلاف ويقصد به إفناء مادة الشيء أو هلاكه جزئيا أو كليا والتعطيل يقصد به (توقف الشيء عن القيام بوظيفة فترة مؤقتة) والتخريب يقصد به (توقف الشيء تماما عن أن يؤدي منفقة كليا أو جزئيا).[1]

خامسا : جريمة نشر الفيروسات :

فهي تتوفر على العقد الجنائي فالمجرم يهدف إلى تعطيل عمل الشبكة وفي جميع الحالات المشرع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص، ولكن هناك حالات لا يتوفر فيها القصد الجنائي في مجال الحاسبات الآلية لعدم توافر نية التملك المطلقة كقراءة المعلومات من خلال شاشة الحاسب الآلي أو سماعها من خلال مكبر الصوت أو الالتقاط للإشعاعات ، أما في مجال الحاسبات الآلية فإن محكمة النقض الفرنسية اكتشفت بتوافر نية التملك الوقتية وأقرت بها نظرية سرقة المنفعة وتحقق هذه النية من سلب حيازة المستندات خلال الوقت اللازم لإعادة نسخها بدون إرادة صاحب المشروع ومالكها أو حائزها منها بصفة دائمة أو وقتية وإنما مشاركة الانتفاع بها وهو الأمر الذي يتطلب تدخل المشرع لمواجهتها بنصوص خاصة.[2]

إن كل جريمة تحدث باستخدام الانترنت إنما تحدث كلها او بعضها حسب الأحوال في العالم الافتراضي، وإذا كان النشاط المادي يحدث كله في العالم الافتراضي بما يستتبع ذلك علاقة السببية كذلك فإن النتيجة الإجرامية لها كان منفصلا هنا حيث أنها تلك الجزئية التي تحدث بشكل انقسامي ما بين حدوثها في العالم المادي جزئيا أم كليا، وذلك أمر استفهامي يقودنا حتما إلى التقرير بالاهتمام بالنتيجة التي قررها المشرع تحديدا في نموذجه الإجرامي دون تمام التي تحدث تقنيا، فإذا تطلب المشرع القتل في جريمة اختراق قواعد بيانات المستشفيات مثلا

[1] – حسنين كامل محمد ، مرجع سابق ، ص 17.

[2] – حسنين كامل محمد ، المرجع نفسه ، ص 22.

بقصد ارتكاب جريمة قتل فإن تمام النتيجة تقنيا هو اكتمال تغيير بيانات الدواء، ويلزم هنا لكي يمكن القول بتمام الجريمة على وفق تطلب النموذج القانوني للجريمة أن يتم إعطاء المريض الدواء الخاطئ فعلا فإذا لم يتم إعطاء المريض الدواء الخاطئ فإن الجريمة ماديا تصل في حالة شروع شكلي ومن الناحية العملية فإن النتيجة الإجرامي التي يتم ارتكاب نشاط إجرامي ما عبر الانترنت بقصد الوصول إليها من الصعوبة بمكان إثبات القصد الإجرامي فيها توصلا إلى تحديد تسمية معينة للجريمة وذلك من الأمور التي تجعل الإثبات هنا قاصرا على التوصل إلى تحديدها بالدقة المتطلبة فقد يكتفي في مثل الجريمة السالفة بالاستعاضة عن جريمة الشروع بالقتل بجريمة تغيير أو تعديل بيانات اسمية أو العدوان على بيانات مرضية بما يشكل في النهاية عدوان على الحق في الخصوصية. سوف تظل مشكلة النتيجة الإجرامية في الجرائم الناشئة عن استخدام الانترنت محلا لجدل قانوني يجب أن يتم التطرق إليه من منطق التزاوج بين العالم المادي ونظيره الافتراضي بحيث يكون بناء معدلات الجريمة حين هيكلة ركنها المادي بالأخذ في الاعتبار هذا التزاوج.[1]

المطلب الثاني : الركن المعنوي:

عرف بأنه العلم بعناصر الجريمة وإرادة ارتكابها، وبالتالي يتكون هذا الركن من عنصرين هما العلم والإرادة، فالعلم هو إدراك الأمور على نحو مطابق للواقع، يسبق الإرادة، أما هذه الأخيرة فتتمثل في الاتجاه من أجل تحقيق السلوك الإجرامي، ويتخذ القصد الجنائي عدة صور منها القصد العام والقصد الخاص.

القصد الجنائي العام : هو الهدف الفوري والمباشر للسلوك الإجرامي، وينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها.

[1] – علي جبار الحسيناوي ، مرجع سابق ، ص 41.42.

القصد الجنائي الخاص : هو ما يتطلب توافره في بعض الجرائم فلا يكفي مجرد تحقيق الغرض من الجريمة بل هو أبعد من ذلك أي أنه يبحث في نوايا المجرم، من هنا نتساءل عن القصد الذي يجب توافره في الجريمة المعلوماتية.

إن المجرم الالكتروني يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بأركان الجريمة وبالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليين وأنهم قد تسللوا صدفة، فلا انتفاء للعلم كركن للقصد الجنائي، وكان يجب عليهم أن يتراجعوا بمجرد دخولهم ولا يستمروا في الاطلاع على أسرار الأفراد والمؤسسات لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية.

فالقصد الجنائي متوافر في جميع الجرائم المعلوماتية دون أي استثناء ولكن هذا لا يمنع أن هناك بعض الجرائم المعلوماتية تتطلب أن يتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الانترنت ، أما جرائم نشر الفيروسات عبر الشبكة فهي تتوفر على القصد الجنائي الخاص فالمجرم يهدف إلى تعطيل عمل الشبكة وفي جميع الظروف المشرع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص.[1]

إلا أن ما يثير اللبس حول ما إذا كان القصد الجنائي المطلوب توفره هو القصد العام أو القصد الخاص هو استعمال المشرع الجزائري لمصطلح عن طريق الغش، فأعتبر البعض أن هذه العبارة تعبر على نية المشرع في اشتراط توفر قصد خاص في هذه الجريمة وهو نية تسبيب ضرر للغير في ماله أو في حقوقه المختلفة، إلا أن هذا الرأي منتقد لأن عدم إضافة مصطلح الغش إلى نص التجريم يؤدي إلى فهم النص فهما خاطئا بما معناه تجريم فعل إدخال المعلومات وتعديلها ومحوها وهي من المهام الأساسية لمبرمجي الأنظمة المعلوماتية ومستخدميها، وبالتالي فعنصر الغش ضروري لقيام هذه الجريمة.

[1] – زيوش عبد الرؤوف ، مرجع سابق ، ص 136.137.

وهذا لا يعني اشتراط المشرع قصدا خاصا لقيام الجريمة لأنه ليست هناك وقائع أخرى يجب أن تتجه إليها قصد الجاني، على خلاف بعض التشريعات الأخرى كالقانون البرتغالي والقانون التركي، والفنلندي التي اشترطت لقيام الجريمة المعلوماتية توفر قصد الإضرار بالغير وقصد تحقيق ربح غير مشروع للجاني وللغير، على خلاف المشرعين الجزائري والفرنسي اللذين لم يشترطا توفر القصد الخاص لقيام هذه الجريمة.[1]

[1] – عبد القادر عمير ، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة) ، أطروحة لنيل شهادة دكتوراه علوم في القانون العام ، جامعة الجزائر 1 ، 2020/2019، ص 114.

من خلال ما تعرضنا له في دراستنا لماهية الجريمة الالكترونية، تبين لنا جليا بأنها من الجرائم التي تتسم بالخطورة المطلقة وفي نفس الوقت جرائم ناعمة، لكن تحقق النتيجة الإجرامية على أكمل وجه، فهي تلك الجريمة الرامية إلى عدم ترك أثر أو دليل قد يدين فاعلها فتميزها بهذا الطابع الفريد والأقل عنفا جعل الإقبال عليها متزايد خاصة ما نراه في السنين الأخيرة، فالربح كثير والجهد أقل و بثوان معدودة تتحقق الجريمة، فالبعد بينها وبين الجرائم العادية يكمن هنا، فتعد الأكثر فتكا ومنعدمة الوجود فتتحقق بلمسة زر واحدة، وأكثر من هذا عدم التقاء الجاني والمجني عليه وهذا ما يزيد من صعوبتها ومن صعوبة مكافحتها، وكذلك نصوص التجريم التي وضعها المشرع الجزائري لم تكن كافية فركز على الجريمة بحد ذاتها وأهمل نسبيا المجرم الذي يقوم بها (المجرم الالكتروني).

الفصل الثاني

الأحكام الإجرائية للجريمة الإلكترونية

بعد ما تطرقنا في الفصل الأول إلى الحماية الموضوعية للجريمة الالكترونية من ماهية الجريمة الالكترونية (مفهوم وتعريف وخصائص وأركان) سوف نتعرض من خلال الفصل الثاني إلى الحماية الإجرائية للجريمة الالكترونية ، وخاصة بعد ما تبنى المشرع الجزائري في القسم السابع مكرر نصوص الجريمة المعلوماتية، أو بما تعرف بجرائم المساس بأنظمة المعالجة الآلية للمعطيات وذلك بالقانون رقم 06/23 المؤرخ في 2006/12/20 المتضمن قانون العقوبات .

ومن خلال هذا الفصل سوف نتعرض وفق المبحث الأول إلى إجراءات التحقيق في الجريمة الالكترونية (الأعوان المكلفون بالتحري وجمع الأدلة وكذلك التفتيش في الجريمة الالكترونية)

أما المبحث الثاني فسوف نتعرض فيه إلى العقوبات المقررة في الجريمة الالكترونية سواء بالنسبة للشخص الطبيعي أو الشخص المعنوي عقوبات أصلية وأخرى تكميلية.

المبحث الأول : إجراءات التحقيق في الجريمة الالكترونية :

لعل خصوصية الجريمة المعلوماتية ، أبرزت مشكلة المكافحة الإجرائية للجريمة المعلوماتية خاصة من ناحية كيفية جمع الأدلة الالكترونية ومدى حجيتها، وحتى تتوفر في الدليل الإلكتروني المشروعية التي تشترطها القوانين في كافة التشريعات.

والمشرع الجزائري اقتدى بالمشرعين الذين سبقوه، سارع لمواكبة هذا التطور الذي لحق الجريمة بمكافحتها من الناحية الإجرائية، وذلك بتعديل بعض المواد في قانون الإجراءات الجزائية وإصدار قوانين خاصة وجديدة في مجال الإجراءات.[1]

فالمشرع الجزائري سارع إلى تبني الحماية من جرائم الإعلام الآلي في نصوص تجريمية في قانون العقوبات وقوانين خاصة من أجل الحد الأمثل والمحكم لهاته الجرائم خاصة وأن الإجراءات الكلاسيكية للتحري لم تعد تجدي نفعا ولم تكن نافعة وشافية بل أصبحت كوجودها كعدمها مما حتم للمشرع الجزائري الذي اقتدى بالمشرعين السابقين ضرورة مواكبة التطورات التي آلت إليها الجرائم الالكترونية.

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعوانها ، حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية .[2]

[1]- أمحمدي بوزينة آمنة ، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام) ، كلية الحقوق والعلوم السياسية ، الشلف ، كتاب أعمال ملتقى آليات مكافحة الجرائم الالكترونية في التشريع الجزائري المنعقد في الجزائر العاصمة في 2017/03/29 ، ص 57.

[2] - عثماني عز الدين ، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية ، مجلة دائرة البحوث والدراسات القانونية والسياسية ، مخبر المؤسسات الدستورية والنظم السياسية ، العدد الرابع ، جانفي 2018 ، ص 50-51.

حيث منح قانون 04/09 دورا إيجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم الماسة بأنظمة الاتصال والمعلوماتية وكشف مرتكبيها حيث تنص المادة الثالثة منه على وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

ونص ذات القانون في مادته الرابعة على أربعة حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية، عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية وفي إطار تنفيذ طلبات المساعدة القضائية والدولية المتبادلة.

وعلى هذا الأساس ، يجوز للجهات القضائية وضباط الشرطة القضائية الدخول بغرض معلوماتية أو جزء منها ، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من اجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها ذلك أن ملاحقة الجناة وكشف جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم هذا الإجراء في نطاق إقليم دولة أخرى .[1]

وسوف نتعرض من خلال المطلب الأول إلى الأعوان المكلفون بالتحري وجمع الأدلة في الجريمة الالكترونية ومعرفة اختصاصاتهم في مجال الجرائم المعلوماتية والسيبيرانية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

ومن خلال المطلب الثاني سوف نعالج التفتيش في الجريمة الالكترونية.

[1] - عثماني عز الدين ، مرجع السابق ، ص 51.52.

المطلب الأول : الأعوان المكلفون بالتحري وجمع الأدلة في الجريمة الالكترونية :

وضع المشرع الجزائري كغيره من التشريعات بعض القواعد والضوابط التي تستهدف متابعة مرتكبي الجرم المعلوماتي حماية لمعطيات الحاسب الآلي خاصة في مرحلة جمع الاستدلالات، حيث أن أجهزة الشرطة تقوم بدور فعال ورئيس حال وقوع الجريمة لمعاينة مكانها وضبط أدلتها والقبض على مرتكبيها والقيام بكل ما يفيد في كشف الحقيقة .[1]

حيث يتبين أن الشرطة القضائية أو ضباط الشرطة القضائية والأعوان هم الجهاز الأول المكلف بالتحري والتحقيق وجمع الأدلة في الجرائم التي تتسم بالمعلوماتية والجرائم ذات النطاق الواسع والمفتوح والجرائم التي يدخل فيها الحاسب الآلي كجهاز رئيس دون غيره في ارتكابها فأصبحت الآن الجرائم الأكثر إقبالا عليها في ظل تطور الشعوب والمجتمعات وغزو الالكترونيات وسوف نتفصل في الأجهزة المختصة بالبحث والتحري وجمع الأدلة والتحقيق في الجرائم الالكترونية .

الفرع الأول : التحقيق في الجريمة المعلوماتية :

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة ، لما له أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها ، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.

[1] - خالد عياد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، ط1- دار الثقافة للنشر والتوزيع ، عمان ، 2011، ص 147.

والثابت أن الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة ،وتمر مرحلة التحقيق بمرحلتين أيضا مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي ، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق، وإننا نؤيد الرأي أو الاتجاه الذي يقسم التحقيق إلى:

تحقيق أولي والذي يناط به رجال الضبطية القضائية.

تحقيق قضائي ويناط به رجال القضاء، وهذا الأخير يقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق وتحقيق نهائي يكون في مرحلة المحاكمة من طرف قضاة الحكم .[1]

وفي كل جميع أنواع التحقيق هذه، يكون للقائمين عليه من ضبطية قضائية وقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية، وهو الأمر الذي يفهم صراحة من خلال استقراء نص المادتين 12 و 38 من قانون الإجراءات الجزائية الواردتين في الباب الأول من هذا القانون تحت عنوان " في البحث والتحري عن الجرائم" حيث تنص المادة 12 الفقرة الثالثة أنه "يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات..." وتنص في نفس الوقت المادة 38 من نفس القانون أنه " يناط بقاضي التحقيق إجراءات البحث والتحري..."

وعليه فأنه يمكن القول أن إجراءات البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أم ابتدائيا، وبهذا المفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولى بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا.

وإذا كان التحقيق عموما يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة، فإن التحقيق في البيئة الالكترونية يستوجب

[1] - سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، 2013/2012-ص102.

بالإضافة إلى كل هذا تطويرا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة.[1]

ويتميز التحقيق في الجريمة الالكترونية بمجموعة من الصفات وهي :

01 – السرية : وهي عدم إطلاع الغير على مجريات التحقيق وفقا لما نصت عليه المادة 11 من قانون الإجراءات الجزائية.

02 – التدوين : تدون جميع إجراءات التحقيق في محاضر ويصادق عليها في محضر رسمي حتى تكون حجة في الإثبات.

03 – وضع خطة للتحقيق : بحيث تبدأ مهمة المحقق بجمع الاستدلالات، وفي الجريمة الالكترونية يساعد المحقق في أعمال التحقيق فريق فني مؤهل.[2]

الفرع الثاني : الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الماسة بأنظمة الاتصال والمعلوماتيـــــــة :

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها ، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الاستثناء إلى بعض الجهات والهيآت الخاصة بحكم خبرتها في مجال معين وباعتبارها الأقدر من غيرها على كشف الجرائم الواقعة ضمن حدود اختصاصها الفني أو

[1] - سعيداني نعيم ، المرجع نفسه ، ص 102-103.

[2] - أيت عبد المالك نادية ، فلاح عبد القادر ، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، جامعة الجيلالي بونعامة ، خميس مليانة ، العدد 2 ، المجلد 4 ، 2019، ص 1695.

التقني، والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال ضبط الجرائم والتحري بشأنها.[1]

ومن أجل إشراك مزودي خدمات الانترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم التكنولوجية، يلزم القانون 04/09 هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات الملزمين بحفظها، وتشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات المستعملة في الاتصال والخصائص التقنية وتاريخ وزمن ومدة كل اتصال والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وعناوين المواقع المطلعة عليهم.

ويتضمن القانون أيضا إجراءات عقابية حيث أنه ولتفادي أي تهرب من التزامات القانون 04/09 يسلط هذا الأخير على الأشخاص الطبيعيين الذين يعرقلون سير التحريات القضائية عقوبة السجن من خمس إلى ستة سنوات وغرامة مالية تتراوح ما بين خمسة ملايين إلى خمسين مليون سنتيم، مع معاقبة المؤسسات المخالفة بالغرامات المالية المنصوص عليها في قانون العقوبات.[2]

أولا : الضبطية القضائية : تعتبر الضبطية القضائية صاحبة الاختصاص الأصيل في كل الجرائم بما فيها الجريمة الالكترونية، وقد منحها القانون أساليب تحري جديدة نبينها فيما يلي :

01 – على مستوى جهاز الشرطة :

أنشأت المديرية العامة للأمن الوطني مخبر مركزي بمركز الشرطة بشاطوناف بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة ووهران تحتوي على فروع تقنية من بينها خلية الإعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف عن جرائم الانترنت، بالإضافة إلى

[1] - عثماني عز الدين ، مرجع سابق ، ص 52
[2] - عثماني عز الدين ، مرجع سابق ، ص 53/52.

إنشائها ثلاث مخابر على مستوى بشار – ورقلة – تمنراست قيد الإنجاز لأجل تعميم هذا النشاط على كافة ربوع الوطن. كما يضم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران مخبرا خاصا يتولى مهمة التحقيق في الجريمة الالكترونية تحت اسم " دائرة الأدلة الرقمية والآثار التكنولوجية والتي تضم ثلاث أقسام هي :

– قسم استغلال الرقمية الناتجة عن الحواسيب والشبكات .

– قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

– قسم تحليل الأصوات ، وذلك بالاستعانة بأجهزة مادية للكشف عن الجرائم الالكترونية.[1]

02 – على مستوى جهاز الدرك الوطني :

تعمل مؤسسات الدرك الوطني على مكافحة الجريمة الالكترونية بواسطة المعهد الوطني للأدلة الجنائية وعلم الإجرام الكائن مقره ببوشاوي التابع لقيادة الدرك العامة قسم الإعلام والإلكترونيك الذي يختص بالتحقيق والكشف عن الجرائم الإلكترونية وأيضا بواسطة مديرية الأمن العمومي والاستغلال والمصلحة المركزية للتحريات الجنائية، وهي هيئة ذات اختصاص وطني مهمتها التصدي للجريمة الالكترونية.[2]

ثانيا : دور مقدمي الخدمات في التحري والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية:

إن تكنولوجيات الإعلام والاتصال متنوعة خاصة ما يتعلق منها بخدمات الاتصال السلكية واللاسلكية كالهواتف النقالة والشبكات الرقمية المتمثلة في الإنترنت وهو ما يجعل عملية توصيل الخدمات المتنوعة لهذه التكنولوجيا إلى مستعمليها يتطلب توافر مجموعة من الفاعلين على رأسهم مقدمي الخدمات، المنصوص عليهم في القانون 04/09 الذي يعرفهم على أنهم:

[1] - أيت عبد المالك نادية ، فلاح عبد القادر ، مرجع سابق ، ص 1696/1695.
[2] - أيت عبد المالك نادية ، فلاح عبد القادر ، المرجع نفسه ، ص 1696.

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

2 – أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لقائدة خدمة الاتصال المذكورة أو لمستعمليها.[1]

ثالثا : مركز الوقاية من جرائم الإعلام الآلي والجرائم الالكترونية :

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم الالكترونية عن طريق المرسوم الرئاسي رقم 15–261 ومقره بئر مراد رايس، وهو تابع لمديرية الأمن والدرك الوطني، وقد حددت المادة الأولى منه تشكيلة وتنظيم سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتمارس هذه الهيئة العديد من المهام في مجال التصدي للجريمة الالكترونية ورد النص عليها في المادة 14 من قانون 04/09 سالف الذكر وهي:

– ضمان المراقبة المستمرة لشبكة الانترنت

– القيام بمراقبة الاتصالات الالكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني.

– المشاركة في عمليات البحث والتحري عن الجرائم الالكترونية.[2]

رابعا : الهيآت القضائية الجزائية المتخصصة :

إن السلطة القضائية ستتعامل تأكيدا في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ولا سيما بعد اللجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين، بينما

[1] - عثماني عز الدين ، مرجع سابق ، ص 53.
[2] - أيت عبد المالك نادية ، فلاح عبد القادر ، مرجع سابق ، ص 1697/1696.

يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي.

ومنذ سنة 2003 وفي إطار إصلاح العدالة، قامت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة.[1] ليواكب التطور القانوني الجاري الخاص بجرائم المعلوماتية لأجل هذا تم إجراء :

أولا : دمج مادة (الجريمة المعلوماتية) في برنامج تكوين طلبة المدرسة الوطنية للقضاء على شكل ملتقيات ينشطها خبراء ، والعديد من دورات التكوين في مختلف مجالات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منظمة بالخارج لصالح القضاة وإطارات وزارة العدل في إطار التعاون الثنائي ومنها : التعاون الجزائري الفرنسي – التعاون الجزائري البلجيكي – التعاون الجزائري الأمريكي الذي تناول خاصة التكوين المتخصص في الملكية الفكرية المتمحورة حول التزوير المتصل بالبيئة الرقمية ولا شك أن تخصيص جهات القضاء وتخصص القضاة هما من السمات الحديثة البارزة للتنظيم القضائي الجزائري، وقد جاء اتفاقية التمويل الجزائرية الأوروبية لمشروع دعم إصلاح العدالة في الجزائر أن : هذا المشروع يهدف إلى دعم التخصيص وتكوين القضاة داخل وخارج الوطن للاستجابة للمتطلبات المستجدة الناتجة عن التزايد المستمر للمنازعات التي يجب عليهم الفصل فيها. ونظرا لأهمية التخصص القضائي فقد عقد له عدة مؤتمرات دولية منها : مؤتمر روما سنة 1958 ، مؤتمر نيس سنة 1972 ، مؤتمر ريو دي جانيرو سنة 1978 ، وقد أكدت هذه المؤتمرات أن التخصص في مجال القضاء له أهمية كبيرة ودور فعال في رفع مستوى العمل القضائي ، ولنظام التخصص جانبين هما : تخصص القضاة وتخصص جهات القضاء.[2]

ويتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص، وما يؤكد ذلك ما نص عليه القانون رقم 04/14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون

[1] - بوضياف اسمهان ، مرجع سابق ، ص 370
[2] - بوضياف أسمهان ، مرجع سابق ، ص 370

الإجراءات الجزائية على أنه يجوز تمديد دائرة الاختصاص للمحكمة وكذا لوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم في جرائم المخدرات والجرائم المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، كما نصت المادة 40 مكرر من قانون الإجراءات الجزائية على أنه " يطبق قواعد هذا القانون المتعلق بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي يتم توسيع اختصاصها المحلي طبقا للمواد 37- 40- 329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر1 إلى 40 مكرر 5 أدناه".[1]

وإذا كان للقضاء المتخصص جانبين هما تخصص القضاة وتخصص الأجهزة القضائية المتخصصة فإن هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة. وهو الأمر الذي نعتقد أنه جعل المشرع الجزائري لتلاقي هذه العقبات التي تواجه القضاء المتخصص يختار أسلوب الأقطاب القضائية، فيتجنب أنشاء هيآت قضائية جديدة لكنه يوسع من دائرة الاختصاص الإقليمي للمحاكم لتشكل أقطاب قضائية ويمنحها اختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن اختصاصها العادي، وهذا ما يجعلنا نعتقد من جانب آخر أن التخصص الذي سيسود التنظيم القضائي الجزائري سيرتكز أكثر على الجانب البشري أي تخصص القضاة، ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية

هذه الأقطاب الجزائية المتخصصة طبقا لنصوص المرسوم التنفيذي رقم 348/06 المؤرخ في 5 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق(جريدة رسمية رقم 63) في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم ريع الخاص بالصرف، ولأن الجريمة المنظمة تشمل جرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع متنوعة تتعلق بسلوكيات خطيرة لأنها تستهدف الأشخاص والممتلكات والدولة، وترتكب من طرف عدة أفراد يتصرفون بطريقة منظمة، تعد الجرائم المعلوماتية بشكل من

[1] - بوضياف أسمهان ، المرجع نفسه ، ص 371/370.

الأشكال جريمة منظمة ترتكب عن طريق الشبكات الرقمية، والتي يمكن معالجتها عن طريق الأقطاب الجزائية المتخصصة، وكما لاحظنا سابقا فإن الحركة المتزايدة والضرورية أدت إلى تركيز الاختصاص القضائي في إطار الاهتمام بجدوى وفاعلية الجهاز القضائي في مكافحة الجرائم المستحدثة.[1]

الفرع الثالث : الوسائل المستخدمة في البحث والتحري :

عند القيام بالتحقيق في جريمة ما، فإنه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة، وقواعد فنية تحقق الشرعية، وسهولة الوصول إلى الجاني، وحيث أن للجرائم المعلوماتية طابعها الخاص المميز لها، فإن التحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة وبالتالي حل لغزها والوصول إلى الجاني، وفي سبيل ذلك يعتمد المحقق على مجموعة من الوسائل المختلفة.

أولا : الوسائل المادية :

وهي الأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها :

–عناوين IP – البريد الالكتروني، وبرامج المحادثة.[2]

– البر وكسي : حيث يعمل البر وكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات وقدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة (cash Memory) .

– برامج التتبع : حيث تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث

[1] - بوضياف اسمهان ، مرجع سابق ، ص 371.
[2] - عثماني عز الدين ، مرجع سابق ، ص 54

وتاريخه وتاريخ حدوثه وعنوان (IP) الذي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى، ومن الأمثلة على هذه البرامج برنامج (2، hack tracer vl) .

نظام كشف الاختراق (intrusion detection system) : ويرمز له اختصارا بالأحرف (IDS) وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي تجري حدوثها على أجهزة الحاسبة الالكترونية أو الشبكة مع تحليلها بحثا عن آية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسبة الالكترونية أو الشبكة.

ويتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسبة الالكترونية، أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة، والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها.

– أدوات تدقيق ومراجعة العمليات الحاسوبية.

– أدوات فحص ومراقبة الشبكات : هذه الأدوات تستخدم في فحص بروتوكول ما وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات أدوات (ARP) وظيفتها تحديد مكان الحاسبة الالكترونية فيزيائيا على الشبكة.[1]

ثانيا : الوسائل الإجرائية :

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة والغير محددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها.

[1] - عثماني عز الدين ، مرجع سابق ، ص 55.

1 – اقتفاء الأثر :

يمكن تقصي الأثر بطرق عدة سواء عن طريق بريد الكتروني تم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

2- الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.

3 – الاستعانة بالذكاء الاصطناعي، من خلال استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الالكترونية، وفق برامج صممت خصيصا لهذا الغرض.

4 – مراقبة الاتصالات الالكترونية : لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الاتصالات الالكترونية، على عكس بعض التشريعات التي عرفتها مثل التشريع الأمريكي والكندي.[1]

5 – توسيع دائرة اختصاص الهيآت القضائية الجزائرية لشمل النظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية والدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة.

6 – السماح للسلطات الجزائرية المختصة اللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال عبر الوطنية ومرتكبيها، وذلك عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل.[2]

لكن وبالنظر للوسائل المستخدمة في البحث والتحري وجمع الأدلة في الجرائم التي تتسم بالمعلوماتية إلا أنها لم تكن كافية في جمع وضبط الأدلة وقد واجهتها عدة صعوبات ومعوقات

[1] - عثماني عز الدين ، المرجع نفسه ، ص 55.
[2] - بوضياف اسمهان ، مرجع سابق ، ص 367.

جمة أثرت عليها بشكل سلبي حال دون جمع الأدلة وضبطها وسوف نبين الصعوبات والمعوقات التي واجهت الوسائل المستخدمة للبحث والتحري وكذا الأجهزة المختصة بهما .

المطلب الثاني : التفتيش في الجريمة الالكترونية :

01- تعريف التفتيش اللغوي : اشتق من الفعل فتش، وفتش الشيء تصفحه، وفتش عنه سأل واستقصى في الطلب .

02 – تعريف التفتيش الاصطلاحي : هو السؤال عن الشيء ، والاستقصاء في طلبه، بالسعي والبحث والتنقيب والتقليب ، وهو بهذا المعنى يتصرف إلى كل بحث يجريه الإنسان.

03 – تعريف التفتيش القانوني : البحث الذي نظم القانون قواعده، وضبط حالاته، وجهل لرجال الضبط القضائي، ولمن حولهم سلطة التحقيق حق مباشرته في حدود القانون.

04 – تعريف التفتيش الإجرائي : قيام رجال الضبط الجنائي بإجراءات بالتفتيش على السرقات الالكترونية، التي تتم بواسطة الحاسب الآلي، والشبكة العالمية الانترنت.[1]

تعريف التفتيش بصفة عامة :

يعرف التفتيش بوجه عام بأنه عبارة عن " إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة".

وعرفه البعض بأنه " البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون ".

[1] - عبد الله بن عبد العزيز بن عبد الله الخثعمي ، التفتيش في الجرائم المعلوماتية في النظام السعودي (دراسة تطبيقية) ، مذكرة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، 2011 ، ص 9/8.

وعرفه آخرون بأنه هو " البحث عن الحقيقة التي تتمثل في ثبوت أو انتفاء ارتكاب شخص معين لجريمة معينة وقعت بالفعل وأتهم هذا الشخص بارتكابها على أساس من الجدية التي تؤيدها أمارات قوية".[1]

ونخلص مما سبق أن المقصود بالتفتيش القانوني هو:

– الذي ينصرف على تفتيش الشخص أو المسكن وبالتالي تفتيش المحال العامة والتفتيش تلك الحالة يعد إجراء إداري.

– التفتيش عملا وإجراء من إجراءات التحقيق أي لابد من وقوع جريمة وأن يؤدي إلى التوصل لحقيقتها وفاعلها.

– التفتيش عمل قضائي لا يجوز أن يقوم به إلا من خوله القانون صفة الضبطية القضائية.

وتكمن الفكرة الأساسية للتفتيش في إباحة انتهاك الحق في الخصوصية طالما أن هناك مبررا في القانون لهذا الانتهاك، لذا فهو يعد من بين أقصى الصلاحيات التي قد تمارسها الدولة ضد المواطن وبعد أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الكبرى الأساسية في دعم المحافظة عليها.[2]

الفرع الأول : الاستعانة بنظم المعالجة الآلية للبيانات بحثا عن الأدلة :

التنقيب و البحث في البرامج المستحدثة وملفات البيانات المخزنة للبحث عما يتعلق بجريمة وقعت للوصول إلى كشف الحقيقة عن تلك الجريمة وعن مرتكبيها قد تفرضها مصلحة وظروف التحقيق في جرائم الحاسبات .

وهذا الإجراء جائز قانونا، ولو لم ينص صراحة على استخدامه باعتباره مما يدخل في نطاق التفتيش بالمعنى القانوني ويندرج تحت مفهومه.

[1] - خالد ممدوح إبراهيم ، مرجع سابق ، ص 83
[2] - خالد ممدوح إبراهيم ، مرجع سابق، ص 84

وهذا الإجراء قد استخدمته بعض التقنيات المعاصرة، ونصت عليه صراحة كالمادة 251 من التقنين الإجرائي اليوناني، والتي تقضي بصلاحية اتخاذ أي إجراء لازم لجمع أدلة الجريمة وضبطها والمحافظة عليها .

لذا فإنه وعملا بالمواد من 183 حتى 207 من التقنين ذاته فإن التقنين والضبط المنصب على البيانات المسجلة في وسائط وأوعية مادية أو المخزنة في الذاكرة الداخلية للحاسبات تواجهه مشكلات تستلزم استعانة المحقق بخبير لجمع تلك البيانات يعد كدليل أمام القضاء.

لذا قال بعض الفقهاء عن التفتيش أنه إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون بهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص[1]

يتمتع بالخصوصية بصرف النظر عن إرادة صاحبه، أو هو إجراء من بين إجراءات التحقيق التي تهدف إلى التوصل إلى أدلة جريمة ارتكبت فعلا، وذلك بالبحث في مستودع السر سواء تم هذا التفتيش على المتهم شخصيا أو في منزله دون توقف على رضائه.[2]

الفرع الثاني : مدى قابلية نظام الحاسوب للتفتيش :

يتكون الحاسب الآلي من ومكونات مادية Hard ware ومكونات منطقية Soft ware، كما أن له شبكات اتصال بصرية سلكية ولاسلكية، سواء كان ذلك على المستوى المحلي أو على المستوى الدولي.

- خضوع مكونات الحاسوب المادية للتفتيش :

يرى جانب من الفقه الجنائي أن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فبالتالي فإن تفتيش المكونات المادية للحاسب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة إلكترونية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، يدخل في نطاق

[1] - محمد علي سكيكر ، الجريمة المعلوماتية وكيفية التصدي لها ، دار الجمهورية للصحافة ، ط1 – 2010 – ص 70
[2] - محمد علي سكيكر ، مرجع سابق ، ص71.

التفتيش طالما تم وفقا للإجراءات القانونية المقررة، مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها.

إلا أن حكم هذه المكونات يتوقف على طبيعة المكان الموجودة فيه، سواء في الأماكن العامة أو الأماكن الخاصة، إذ للمكان أهمية خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أد ملحقاته كان لها حكمه.[1]

- خضوع مكونات الحاسوب المعنوية للتفتيش :

إذا كان الأمر قد انتهى بنا إلى صلاحية المكونات المادية للنظم المعلوماتية كمحل يرد عليه التفتيش فإن امتداد ذلك إلى مكوناته غير المادية، هو محل جدل كبير حول مدى صلاحيتها كي تكون موضوعا للتفتيش.

وقد ذهب الفقه في هذا الشأن إلى مسارين رئيسيين :

المسار الأول : يلخص أصحاب هذا المسار في تفسيره إلى الاستناد على الربط بين النصوص الإجرائية والعلوم الطبيعية ومفهومها في البيانات المنطقية أو البرامج، حيث أن كلمة الشيء هو المادة بمعنى كل ما يشغل فراغ معين يمكن قياسه والتحكم فيه، بناء على ذلك أن الكيان المنطقي للحاسوب – الذاكرة – تشغل حيزا ماديا يمكن قياس سعتها وحجمها والحروف التي يمكن خزنها فيه.

[1] - ليندا بن طالب ، التفتيش في الجريمة المعلوماتية ، مجلة العلوم القانونية والسياسية ، عدد 16 ، 2017 ، ص 490/489.

ويتضح موقف المشرع الجزائري من خلال المادة 5 من القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث أجاز صراحة تفتيش المنظومة المعلوماتية.

المسار الثاني :يذهب إلى عدم إمكانية انسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث وتنقيب عن الأدلة في برامج الحاسوب وبياناته.

ولذلك يقترح هذا الجانب الفقهي إزاء النقص التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش إمكانية البحث والضبط للمواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي، لتصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هو البحث عن الأدلة المادية وآية مادة معالجة بواسطة الحاسب الآلي.[1]

مدى خضوع شبكات الحاسوب للتفتيش " التفتيش عن بعد"

مع التطور التكنولوجي لثورة الاتصالات لم يعد نطاق الاتصالات محدودا في إقليم دولة واحدة، بل امتد ليشمل كل أرجاء العالم وذلك بعد ظهور شبكة الانترنت وهي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لا مركزية، ويدخل في تركيب هذه الشبكة ملايين الحواسب الموزعة عبر مختلف دول العالم.

إن طبيعة التكنولوجيا الرقمية عقدت التحدي أمام أعمال التفتيش والضبط، بسبب امتداد الأدلة الالكترونية عبر شبكات الحاسوب في أماكن بعيدة عن الموقع المادي للتفتيش، وإن كان من الممكن الوصول إليها من خلال الحاسوب بعد أخذ إذن تفتيشه، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، وهو ما يزيد المسألة تعقيدا باعتبار أن الشبكة المعلوماتية ممتدة في أرجاء العالم تقريبا.

[1] - ليندا بن طالب ، مرجع سابق ، ص 490.

وبالتالي فإن الحاسوب الذي يمكن أن ترتكب عليه أو بواسطته الجريمة المعلوماتية يخضع للقانون الإجرائي الخاص بتلك المنطقة.[1]

فالسؤال المطروح : هل يمكن تفتيش الأنظمة المتصلة بالنظام المسموح بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة أو حتى خارج البلاد؟ وللإجابة عن هذا التساؤل يجب التفرقة بين الفرضيتين التاليتين:

الفرضية الأولى : اتصال حاسب المشتبه فيه أو المتهم بحاسب آخر موجود في مكان آخر داخل الدولة:

نجد المشرع الجزائري أجاز تمديد التفتيش وذلك في نص المادة 05 الفقرة الثانية من القانون 04/09 بأنه في حالة تفتيش منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، ويجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وانطلاقا مما سبق ذكره، نلاحظ أن ذاتية تفتيش الحاسوب وقصور القواعد الإجرائية التقليدية تظهر بصورة جلية أثناء امتداد التفتيش إلى الأجهزة المرتبطة به، فالانتقال غير مهم إلى مكان الجهاز الثاني، بل إن ذلك يتم باستعمال وسائل تقنية حديثة " برامج الدخول" وهنا يبقى السؤال مطروحا ألا يعد استعمال هذه البرامج اعتداء على حرمة الحياة الخاصة للأفراد، خاصة وأن الأجهزة الأخرى تنتمي إلى أشخاص غير المتهم؟.[2]

الفرضية الثانية : اتصال حاسب المشتبه فيه أو المتهم بحاسب موجود في مكان آخر خارج الدولة:

[1] - ليندا بن طالب ، مرجع سابق ، ص 491/490.
[2] - ليندا بن طالب ، مرجع سابق، ص 491.

إن لامتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي أهمية في إمكانية الحصول على دليل عن بعد وفي بضع ثوان، إلا أن بعض الفقه يتحفظ على القيام بذلك لأنه يعتبر انتهاك لسيادة الدولة الأجنبية، وإذا اقتضت ضرورة التحقيق القيام بذلك ينبغي مراعاة العديد من الضمانات يكون متفقا عليها سلفا عن طريق اتفاقيات ومعاهدات في هذا المجال، وهذا ما يؤكد أهمية التعاون الدولي في مكافحة الجرائم الالكترونية.

إن المشرع الجزائري أخذ نفس مسار المشرع الفرنسي حيث أجاز هو ذلك تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، وهذا ما نصت عليه المادة 05 فقرة 3 من القانون 04/09 < ... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل>.[1]

الفرع الثالث : ضمانات التفتيش :

رغم اعتبار التفتيش من الإجراءات الجوهرية في عملية تحقيق البحث عن حقيقة الجرائم إلا أن معظم القوانين الإجرائية حرصت على إحاطته بجملة من الضمانات القانونية، وذلك تفاديا لتعسف سلطات البحث والاستدلال وما يمكن أن يحدثه من اعتداء على حقوق وحريات الأفراد وحرمة مساكنهم وحياتهم الخاصة من جهة، وإحقاقا لحق الدولة ممثلة المجتمع في كشف غموض الجرائم ومتابعة مرتكبيها وتوقيع العقاب عليهم من جهة أخرى.

ويمكن تقسيم هذه الضمانات إلى ضمانات موضوعية وأخرى شكلية أو إجرائية نذكرها على النحو التالي:

أولا : الضمانات الموضوعية للتفتيش الإلكتروني:

[1] - ليندا بن طالب ، المرجع نفسه ، ص 491

تتمثل هذه الضمانات في الشروط الواجب توفرها حتى يكون التفتيش صحيحا، وتتلخص في ثلاثة شروط أساسية وهي : سبب التفتيش، محل التفتيش والسلطة المختصة بالتفتيش.

أ – سبب التفتيش :

يعتبر عنصر السبب ضمانة قانونية لصحة ومشروعية إجراء التفتيش، يتحقق بوقوع جريمة ما يتم بموجبها توجيه الاتهام إلى الشخص أو الأشخاص المراد تفتيشهم بناء على أدلة أو قرائن قوية تفيد تورطهم في هذه الجريمة، عملا بمبدأ الشرعية الجزائية للقاضي بأنه " **لا جريمة ولا عقوبة إلا بنص**" . إذ بدون وقوع جريمة، وتوجيه اتهام إلى شخص أو أشخاص معينين وفقا لأدلة كافية، يكون التفتيش باطلا لانتفاء السبب الذي يبرره.[1]

وتطبيقا لما سبق، فإن التفتيش في الجرائم الالكترونية لا يتحقق إلا بتحقق العناصر الثلاثة التالية:

1 – وقوع جريمة الكترونية تحمل وصف جناية أو جنحة :

اتفقت معظم تشريعات الدول على أنه لا يجوز لهيآت التحقيق مباشرة إجراءات التفتيش إلا بعد التأكد من الوقوع الفعلي لجريمة الكترونية نص عليها القانون في نصوص التجريم والعقاب، وأي تفتيش في جريمة محتملة الوقوع مستقبلا ولو أيقنت التحريات والدلائل الجدية على أنها ستقع بالفعل يعد إجراء غير مشروع مآله البطلان .[2]

ولا يكفي وقوع جريمة الكترونية للقول بمشروعية إجراء التفتيش طبقا للقواعد العامة، بل لابد أن تحمل هذه الجريمة بمنظور القانون وصف جناية أو جنحة، ويستثنى من ذلك

[1] - براهيمي جمال ، التحقيق الجنائي في الجرائم الإلكترونية ، أطروحة لنيل شهادة الدكتوراه في العلوم القانونية ، جامعة مولود معمري ، تيزي وزو ، 2018 ، ص 31.
[2] - براهيمي جمال ، مرجع سابق ، ص 32

المخالفات بسبب ضعف خطورتها التي لا تستحق انتهاك حرمة الحياة الخاصة للأشخاص وسرية اتصالاتهم وحرمة منازلهم من أجلها.

والجدير بالذكر، أن مسألة وقوع الجريمة من عدمها تثير مشكلة كبيرة عندما يتعلق الأمر بتفتيش جرائم الحاسب الآلي وشبكات المعلومات، خاصة في الدول التي لم تسن حتى الآن قوانين تصنف فيها هذه الجرائم، وتحدد وصفها القانوني، عناصر أو أركان كل جريمة وكذا العقوبات المقررة لها، مع العلم أن إجراء التفتيش لا يكون مشروعا إلا إذا بني على سبب جدي يتمثل في الوقوع الفعلي للجريمة، وأن وقوع هذه الأخيرة من عدمه يتوقف أساسا [1]

على مدى تحقق أركانها مجتمعة. فعلى سبيل المثال، ما زالت العديد من الجرائم المتعلقة بنظم المعالجة الآلية وشبكة الانترنت خارج نطاق التجريم في التشريع الجزائري مثل جرائم الاعتداء على المواقع الالكترونية، وحجبها، وتدميرها، وجرائم الاستغلال الجنسي للأطفال وغيرها من الجرائم الإباحية، وتبعا لذلك فإن اتخاذ أي إجراء من إجراءات التحقيق إزاء هذه الجرائم بما في ذلك التفتيش، قد يكون مصيره البطلان طالما لم يرتكز على سبب مقبول قانونا، ناهيك عما تتطلبه الإجراءات التقنية في حالة النص على تلك الجرائم من نصوص تتناسب مع حداثتها.[2]

2 – اتهام شخص أو أكثر بمساهمته في ارتكاب الجريمة الإلكترونية:

يشترط لقيام سبب التفتيش إلى جانب وقوع جريمة الكترونية تحمل وصف جناية أو جنحة، أن تتوفر في حق الشخص المراد تفتيشه أو تفتيش حاسبه أو مسكنه دلائل كافية توحي إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة بوصفه فاعلا أصليا أو ثانويا، مما يستوجب اتهامه بها. ومن هنا كان عدم اكتشاف قاضي التحقيق لهوية المتهم في الشكوى ضد مجهول سببا لحفظ ملف القضية وإصداره لأمر بأن لا وجه للمتابعة.

[1] - براهيمي جمال ، المرجع نفسه، ص 32
[2] - براهيمي جمال ، مرجع سابق ، ص 33.

وقد أجمع الفقه الجنائي على أن المقصود بالدلائل الكافية بصفة عامة هو " الشبهات المستمدة من الواقع والقرائن التي تنبئ عن اقتراف الشخص جريمة من الجرائم" ، أما في الجرائم الالكترونية فيقصد بها " مجموعة من المظاهر أو الأمارات المعينة القائمة على العقل والمنطق والخبرة الفنية والحرفية للمحقق والتي ترجح نسبة الجريمة الالكترونية إلى شخص معين باعتباره فاعلا أصليا أو شريكا " .

وعلى هذا الأساس فسبب التفتيش في البيئة الالكترونية لا يتوقف على وقوع جريمة من الجرائم الالكترونية فقط، إنما لابد أن يكون ذلك الوقوع مقترنا بنسبتها إلى شخص أو أشخاص معينين إما بصفتهم فاعلين أصليين أو شركاء.

3 – توافر أمارات قوية توحي إلى وجود أدلة مادية تفيد في كشف الجريمة:

لا يكفي وقوع جريمة من نوع جناية أو جنحة منصوص عليها في القانون، وتوجيه الاتهام إلى شخص أو أشخاص معينين بمساهمتهم في ارتكابها لقيام سبب التفتيش في الجرائم الالكترونية، إنما ينبغي أن تتوافر كذلك لدى المحقق أدلة قوية وقرائن كافية على وجود لدى شخص المتهم أو في الموقع المراد تفتيشه أجهزة أو أدوات استعملت في الجريمة أو أشياء متحصل منها، أو آية معلومات أو بيانات أو مستندات إلكترونية تفيد في استجلاء الحقيقة.[1]

ويتم الحصول عادة على هذه القرائن والأمارات من خلال مختلف التحريات الجدية التي تجريها سلطات الضبط في مرحلة الاستدلال، بعدما يتم إخضاعها للسلطة المختصة بإصدار الإذن بالتفتيش التي تتأكد من مدى توفر هذه القرائن لمصداقية كافية تبرر اللجوء إلى إجراء التفتيش.

وينطبق على هذه الضمانة ما قيل في سابقتها بأنها لا تجدي في مجال الجرائم الالكترونية، بخلاف ما هي عليه في الجرائم التقليدية. لأن التوصل إلى قرائن أو أمارات قوية كسبب لقيام التفتيش في جريمة الكترونية ليس بالأمر الهين، نظرا للصعوبات الكثيرة والعقبات

[1] - براهيمي جمال ، مرجع سابق ، ص 34

الجمة التي تواجه سلطات التحري والاستدلال في ذلك، كنقص خبرتها في تقنيات التحري في العالم الالكتروني الافتراضي، مقابل ما تتسم به تلك الأدلة من طبيعة معنوية يمكن إخفاؤها، تغييرها وإتلافها بكل سهولة وبسرعة فائقة. وهو ما قد يشكل دافعا كافيا لانتفاء سبب التفتيش الذي يعتبر شرطا جوهريا لصحة إجراء التفتيش.[1]

ب – محل التفتيش :

يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره في الجريمة التقليدية فإن التفتيش ينصب على شخص المتهم أو غير المتهم، وكذلك على مسكن المتهم وما في حكمه وملحقاته، أو على مسكن غير المتهم وما في حكمه وملحقاته.

لكن في الجريمة المعلوماتية فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به.[2]

ولكي يتم التفتيش على هذه الحال، ينبغي الإشارة إلى أن هذه الأخيرة لا تكون قائمة بذاتها، بل تكون إما موضوعية في مكان ما كالمسكن أو المكتب، أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو الهاتف النقال الذكي.[3]

ويشترط في الذي يقع عليه التفتيش، أن يكون معينا تعيينا نافيا للجهالة، ويكون مما يجوز تفتيشه.

فأما الشرط الأول فهو نتيجة منطقية للمحافظة على حقوق وحرمات وحريات الأفراد، لذا لا يمكن القيام بتفتيش كل الحواسيب المتواجدة في شركة ما أو الحواسيب المحمولة أو الهواتف النقالة الخاصة بكل أفراد العائلة الواحدة.

[1] - براهيمي جمال ، المرجع نفسه ، ص 35.
[2] - ليندا بن طالب ، مرجع سابق ، ص 492.
[3] - ليندا بن طالب ، مرجع سابق ، ص 492.

وأما الشرط الثاني فلأن القانون يستثني من التفتيش بعض الأشخاص والأماكن مثل أشخاص ومساكن وسيارات أعضاء السلك الدبلوماسي وأعضاء المجالس النيابية، وكذا مكتب المحامين لتمتعهم بالحصانة، وعليه فأي تفتيش لأجهزة الحواسيب أو الوسائل الالكترونية الأخرى الموجودة بحوزة هذه الفئة من الأشخاص أو في منازلهم أو على متن سياراتهم يعد منافيا للقانون ومآله البطلان.[1]

ج – السلطة المختصة بالتفتيش:

كما هو معلوم فإنه لا يعتبر التفتيش الالكتروني صحيحا ومنتجا لآثاره إلا إذا تم القيام به من طرف الأشخاص أو الجهات المخول لها قانونا صلاحيات إجرائه، وقد اختلفت التشريعات الإجرائية في هذا الشأن، فمنها من أسند هذه المهمة إلى المدعي العام وهناك من منحها لقاضي التحقيق أو ضباط الشرطة القضائية، وبالنسبة للمشرع الجزائري فقد أوكل صلاحية إجراء التفتيش إلى السلطات القضائية الممثلة في النيابة أو التحقيق وكذا ضباط الشرطة القضائية وفقا لأحكام المادة 05 من القانون رقم 04/09.

وبالنظر إلى المهارات الفنية التي تتطلبها الجريمة المعلوماتية فقد أجاز المشرع الجزائري للسلطات المكلفة بالتفتيش الاستعانة بخبير له دراية بالمعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها بهدف مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، وذلك طبقا لمقتضيات المادة 05 الفقرة الأخيرة منها، ويتمثل دور الخبير في تقديم التوضيحات الكافية حول كيفية تشغيل هذه الأنظمة وطريقة النفاذ إليها أو إلى المعطيات المخزنة أو المعالجة أو المنقولة في شكل يمكن فهمه أو إدراكه.[2]

د – الإذن بالتفتيش :

[1] - براهيمي جمال ، مرجع سابق ، ص 36.

[2] - عربوز فاطمة الزهراء ، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية ، مجلة جيل الأبحاث القانونية المعمقة ، العدد 34 ، ص 103.

غالبا ما يصدر الإذن بتفتيش مسكن المتهم وينصرف هذا الإذن إلى كل ما يتواجد في المسكن، ومن ثم هل يجوز بمقتضى هذا الإذن لضباط الشرطة القضائية الولوج إلى البيئة الرقمية والتغلغل في المنظومة المعلوماتية للبحث عن أدلة إثبات التي يمكن أن تكون محل الضبط ؟

وفي هذه الحالة يرى أغلب الفقهاء أنه يجب أن يحدد إذن التفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها (أجهزة الحاسوب، صور جنسية إلكترونية خاصة بالأطفال، مصنفات إلكترونية مقلدة ...)، والهدف من هذا التحديد في إذن التفتيش لا هو تجنب التفتيش الاستكشافي، بحيث لا يترك للمأذون بالتفتيش أي سلطة تقديرية في ذلك، إلا أن هناك صعوبة في احترام هذا الشرط أثناء الممارسة العملية في تفتيش أجهزة الكمبيوتر، ويرجع ذلك إلى الطبيعة الخاصة لهذه الأخيرة، فالكمبيوتر يحتوي على عدد كبير من الملفات، بالإضافة إلى أن أسماء هذه الملفات لا تدل بالضرورة على ما تحتويها، بالتالي هنا تثار الصعوبات فهل يعتبر كل ملف " صندوقا مغلقا " يحتاج إلى إذن قضائي مستقل عن الآخر؟ خاصة وقد يعمد المتهم إلى وضع أسماء مستعارة لملفات تحتوي على مواد غير مشروعة.

أما المشرع الجزائري في القواعد الخاصة بأجراء التفتيش المعلوماتي الواردة في قانون رقم 04/09، لا نجده يتحدث عن هذا الشرط، كل ما في الأمر أنه تحدث عن إعلام جهات السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى.[1]

ثانيا : الضمانات الشكلية للتفتيش الإلكتروني :

يتطلب القانون شروطا شكلية معينة ينبغي مراعاتها عند مباشرة التفتيش، والغرض من تلك الإجراءات إحاطة المتهم بضمانات لحماية حريته، ومن المتعارف عليه أن الإجراءات الشكلية لأي إجراء ومنها التفتيش لا ترمي إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجميع الأدلة بل تهدف إلى حماية الحريات الفردية والحقوق الخاصة للأفراد وضمان صيانتها.

[1] - ليندا بن طالب ، مرجع سابق ، ص 493/492.

01 – أن يجري التفتيش بحضور أشخاص يحددهم القانون :

تشترط معظم التشريعات للقيام بعملية التفتيش حضور أشخاص معينين يحددهم المشرع، وتختلف هذه الأشخاص حسب كل تشريع فهناك من يشترط ضرورة حضور المتهم أو من ينوبه أو صاحب المسكن أو شاهدين يحددهم القائم بالتفتيش أو من يأمر به ولحضور هؤلاء الأشخاص أهمية مزدوجة، فهو من جهة يعد بمثابة رقابة على القائم به، ومن جهة ثانية يوفر جوا من الطمأنينة والثقة لدى من يجري تفتيش مسكنه.

وبالنسبة للمشرع الجزائري فقد اشترط لإجراء عملية التفتيش في المعطيات المخزنة في المنظومة المعلوماتية، إعمال قاعدة الحضور تطبيقا لأحكام المادة 05 من القانون 04/09 التي تحيل الأحكام العامة المنصوص عليها في قانون الإجراءات الجزائية، ومن ثم فإنه يشترط ضرورة حضور صاحب مسكن المشتبه به في ارتكابه الجريمة أو صاحب مسكن شخص من الغير يحوز أوراقا أو أشياء تتعلق بالجريمة لعملية التفتيش أو من ينوبهما أو حضور شاهدين إذا تعذر حضورهما بحسب ما نصت عليه أحكام المادة 45 من قانون الإجراءات الجزائية.[1]

ومما سبق ذكره، يمكننا القول أنه في حال ارتكاب أحد الجرائم المتصلة بتكنولوجيا الإعلام والاتصال يسمح إذن التفتيش للشخص المكلف بتنفيذه سلطة تفتيش المكان للبحث عن الأشياء، وأيضا البحث في داخل النظام المعلوماتي الموجود في المكان المحدد للحصول على معلومات يمكن أن تستخدم كدليل على ارتكاب الجريمة وضبط هذه المعلومات وحفظها.

02 – الميعاد الزمني لإجراء التفتيش :

اختلفت التشريعات الإجرائية في وقت تنفيذ التفتيش، فمنها ما يحظر تفتيش المساكن ليلا إلا في أحوال معينة، ومنها لم يقيد القيام بهذا الإجراء بوقت معين وترك الأمر لتقدير القائم بالتفتيش لاختيار الوقت الملائم لتنفيذه ضمن المدة المحددة بالإذن.

[1] - رضا هميسي ، تفتيش المنظومات المعلوماتية في القانون الجزائري ، مجلة العلوم القانونية والسياسية ، عدد 5 ، 2012 ، ص 169/168.

والمشرع الجزائري ذهب إلى حظر تفتيش المساكن وما في حكمها في أوقات معينة وحدد ميقات تنفيذ هذا الإجراء من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا، وهناك حالات استثنائية يجوز فيها الخروج عن هذا الميقات ويصح إجراؤه في أي ساعة من ساعات الليل والنهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها بالمواد 342 إلى 348 من قانون العقوبات المرتكبة في أماكن معينة، أو في حالة رضا صاحب المسكن صراحة.

وفي نطاق التفتيش المتعلق بالجرائم المعلوماتية فإن الاستثناء الوارد بالفقرة الثالثة من المادة 47 قانون الإجراءات الجزائية والمتعلق بجواز إجراء ضابط الشرطة القضائية للتفتيش في كل ساعة من ساعات الليل أو النهار عندما يتعلق التحقيق بنوع معين من الجرائم، فقد شمل هذا الاستثناء الجرائم المعلوماتية حيث جاء في نصها " ... عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و ... فإنه يجوز إجراء التفتيش ... في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص.".[1]

03 – أن يتم تحرير محضر خاص بعملية التفتيش :

لما كان التفتيش عملا من أعمال التحقيق فإنه يتوجب تدوينه، ويكون ذلك بإعداد محضر يثبت فيه ما تم من إجراءات بشأنه وما أسفر عنه من أدلة، ويجب أن يتضمن المحضر المحرر عن عملية التفتيش وصف العملية من بدايتها إلى نهايتها، مع تبيان وقت بداية العملية ونهايتها وكذا جرد الأشياء وضبطها التي يتم حجزها أثناء العملية التفتيش، ويجب أن يمضى هذا المحضر من طرف القائم بالتفتيش ومن الأشخاص الذين يحدد القانون ضرورة إمضائهم لذلك المحضر.

[1] - سعيداني نعيم ، مرجع سابق ، ص 154/153.

ويشترط القانون الجزائري حضور كاتب أثناء إجراء التفتيش طبقا لنص المادة 79 من قانون الإجراءات الجزائية على قاضي التحقيق أثناء قيامه بعملية التفتيش أن يصطحب معه كاتب ويتعين عليه تحرير محضر يمضى من طرفه ومن طرف الكاتب.

ولا تشترط التشريعات عادة شكلا معينا لمحاضر التفتيش وإنما تشترط فيها أن تتضمن بيانات معينة تختلف من تشريع إلى آخر كضرورة إمضائها من طرف القائم بالتفتيش والكاتب أحيانا.

وفيما يخص شكل المحضر فإن المشرع الجزائري لم يشترط شكلا خاصا في محضر التفتيش، وبالتالي فهو لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر بشكل عام أي يجب أن يتضمن كافة البيانات المتعلقة بعملية التفتيش وبيان صفة القائم بالتفتيش ومن حضر التفتيش.[1]

ويختلف الأمر عادة عما إذا كان التفتيش تم من طرف ضابط الشرطة القضائية الذي يخضع للقواعد العامة التي يجب أن تتضمنها المحاضر المحررة من طرف الضبطية القضائية، عنه إذا كان قد أجرى من طرف قاضي التحقيق الذي يشترط أن يكون مصحوبا بكاتب وأن يمضي المحضر من الكاتب وإلا كان باطلا.[2]

ونرى أن تحرير محضر عن عملية التفتيش هي لازمة وذلك لتمكين الجهات القضائية المختصة بنظر مدى احترام الإجراءات المتطلبة في عملية التفتيش ومن ثم بسط رقابتها على شرعية الإجراء، لذلك ففي حالة عدم إتباع هذه المتطلبات فقد رتب المشرع الجزائري البطلان على عدم احترام الإجراءات المنصوص عليها في المواد 48 من قانون الإجراءات الجزائية وأنه من المعلوم أن بطلان إجراءات التفتيش يؤدي إلى بطلان واستبعاد الدليل المحصل من هذه العملية.[3]

04 – أن يكون الأمر بالتفتيش مسببا :

[1] - رضا هميسي ، مرجع سابق ، ص 170
[2] - رضا هميسي ، المرجع نفسه ، ص 170.
[3] - رضا هميسي ، مرجع سابق ، ص 171.

يعتبر من الضمانات المقررة في التشريعات الإجرائية الجزائية تسبيب أمر التفتيش، ويقصد بالتسبيب أن الأمر الصادر لابد وأن ينبنى على عدة قرائن ودلائل تدل على أن في المكان المراد تفتيشه أو الشخص المراد تفتيشه ما يفيد في كشف الحقيقة.

05 – أن يكون الإذن بالتفتيش مكتوبا :ويجب أن يتضمن أمر الندب من أصدره ووظيفته وتاريخ وساعة صدوره واسم أو أسماء المقصودين بالتفتيش وأن يحدد له فترة معقولة ويمكن تجديدها عند انقضائها بغير تنفيذ ويذيل الأمر من أصدره.[1]

المبحث الثاني : الجزاءات المقررة في الجريمة المعلوماتية :

بعد التطرق إلى إجراءات التحقيق وما شملته من وسائل مادية وبشرية للبحث والتحري والتحقيق في الجريمة الالكترونية وكذلك التفتيش ومدى قابلية نظام الحاسوب الآلي للتفتيش وكذلك ضمانات التفتيش الآن سوف نتطرق إلى الجزاءات المقررة للجريمة الالكترونية في القانون الجزائري

سوف ندرس العقوبات المقررة للشخص الطبيعي كمطلب أول و في المطلب الثاني سوف ندرس العقوبات المقررة للشخص المعنوي.

المطلب الأول : العقوبات المقررة للشخص الطبيعي :

نص المشرع الجزائري على مجموعة من العقوبات الأصلية والتكميلية المقررة للشخص الطبيعي والمتمثلة في :

أولا : العقوبات الأصلية : تمثل العقوبات الأصلية المطبقة على الشخص الطبيعي في إطار الجريمة الالكترونية المؤشر الصريح لخطورة هذه الجريمة والتي أقرها المشرع على الأفعال التي يجرمها قانون العقوبات والمتمثلة فيما يلي[1] :

[1] - عادل عبد الله خميس المعمري ، التفتيش في الجرائم المعلوماتية ، مجلة الفكر الشرطي ، المجلد 22 ، العدد86، الشارقة ، الإمارات ، 2013 ، ص265.

1 – العقوبات المقررة لجريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي :

تعتبر هذه الجريمة من أهم الجرائم الالكترونية وأخطرها على المؤسسات والأفراد لكونها تشكل انتهاكا صارخا ومباشرا للحقوق والحريات ويختلف الفقه في طبيعة هذه الجريمة بين من يعتبرها جريمة واحدة تؤدي نفس النتيجة وبين من يقسمها إلى جريمتين بحيث يفصل رواد هذا المذهب بين الدخول إلى النظام المعلوماتي كجريمة أولى والبقاء غير المشروع في النظام كجريمة ثانية.

ويقصد بجريمة الدخول إلى الأنظمة تحقيق فعل الدخول إلى النظام وتشير الكلمة إلى كل

" **الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والسيطرة على المعطيات أو المعلومات التي يتكون منها**" . **كما يقصد به** " **الدخول إلى محتويات جهاز الكمبيوتر والقيام بأي عملية اتصال بالنظام محل الحماية دون أي ترخيص أو وجه حق**".

أما جريمة البقاء غير المشروع داخل النظام المعلوماتي فتعتبر من الجرائم المستمرة وتبقى قائمة مستوفية أركانها ما دام الجاني لا يزال على اتصال بنظام المعلومات الذي تم الدخول إليه بطريقة غير مشروعة ودون ترخيص.[2]

ويقصد بالبقاء **كفعل** " **التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام والتصرف فيه** " واستقر أغلب الفقه على أن جريمة البقاء غير المشروع داخل النظام المعلوماتي تعتبر بشكل عام من الجرائم التي يصعب تقديم دليل على إثباتها وكثيرا ما تقترن الجريمتان (أي الدخول غير المشروع والبقاء غير المشروع) ببعضهما البعض وهو الأمر الذي جعل الكثير من الفقه المقارن وأغلب التشريعات الجنائية تجمع الصورتين في جريمة واحدة تحت مسمى **الدخول والبقاء غير المشروع في النظام المعلوماتي**، وقد قرر المشرع في إطار قانون

[1] - دمان ذبيح عماد/ بهلول سمية ، الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري ، مجلة الحقوق والعلوم السياسية ، جامعة عباس لغرور *خنشلة ، 2020 ، ص 145

[2] - دمان ذبيح عماد/ بهلول سمية ، مرجع نفسه ، ص146

العقوبات وبموجب المادة 394 مكرر عقوبتين أصليتين لجريمة الدخول أو البقاء غير المشروع.

- العقوبة المقررة للجريمة في صورتها البسيطة :

يعاقب القانون على هذه الجريمة في صورتها البسيطة بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من خمسين ألف (50.000) إلى مائة ألف (100.000) وفتح في هذا المجال للقاضي السلطة التقديرية بأن جعل له حدا أدنى وحدا أقصى في تقدير العقوبة بالعودة إلى الحيثيات والوقائع، وبالنظر للباعث الذي دفع الشخص لارتكاب الجريمة.

العقوبة المقررة للجريمة في صورتها المشددة :

تضاعف عقوبة الجريمة إذا ترتب عنها حذف أو تغيير في المعطيات، بحد أدنى يقدر بستة أشهر بعدما كان ثلاثة أشهر، وحد أقصى يقدر بسنتين بعدما كان سنة واحدة، ويعاقب على هذه الصورة بغرامة مالية تقدر بمائة ألف (100.000) دينار إلى مائتي ألف (200.000) دينار وفي حال ما تم القيام بتخريب نظام المعالجة الآلية فيعاقب عليها بالحبس من ستة أشهر إلى سنتين وبغرامة من خمسين ألف (50.000) دينار إلى مئة وخمسين ألف (150.000) دينار [1].

2 – العقوبات المقررة لجريمة إفساد أو تعطيل سير النظام :

وتسمى أيضا جريمة " **الاعتداء على سير نظام المعالجة الآلية للمعطيات** " حيث أغفل المشرع الجزائري وضع نص صريح خاص بتجريم الاعتداء على جريمة سير نظام المعالجة الآلية للمعطيات، إلا أنه يمكن استخلاص التجريم من خلال النصوص القانونية المستحدثة في

[1] - دمان ذبيح عماد/ بهلول سمية ، مرجع سابق ، ص 147.

إطار تجريم الاعتداءات الواقعة على أنظمة المعالجة أو على معطيات الأنظمة الداخلية أو الخارجية.

وعلى الرغم من أن هناك من يذهب إلى جريمة الاعتداء العمدي على المعطيات مثل جريمة الاعتداء العمدي على نظام المعالجة الآلية للبيانات تهدف إلى القيام بأفعال تخريب وقرصنة، إلا أن هناك من يذهب إلى أن الفرق بينهما يكمن في أن جريمة الاعتداء العمدي على النظام وإن كانت لا تقع بصفة أساسية على البرامج والشبكات إلا أنها تصيب المعطيات كنتيجة لأفعال الإفساد والتوقيف في حين أن الاعتداء على المعطيات الذي تقوم عليه جريمة الاعتداء العمدي على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه سواء على البرامج أو شبكات النقل والاتصال، وفي سبيل التفرقة بين الجريمتين تم الاتفاق على أن المعيار الأساسي هو المحل الذي يقع عليه الاعتداء ففي حال وقوع الجرم على العناصر المادية للنظام فإن الجريمة هي جريمة الاعتداء العمدي على نظام المعالجة الآلية للمعطيات، أما إذا كان يقع على العناصر المعنوية فإننا نكون في هذه الحالة أمام جريمة الاعتداء العمدي على المعطيات.[1]

3 – العقوبات المقررة لجريمة الاعتداء العمدي على المعطيات :

يقصد بالاعتداء على المعطيات " **التجاوز الذي يهدف إلى الإضرار بمعلومات الكمبيوتر أو وظائفه سواء بالمساس بسريتها أو المساس بسلامة محتوياتها وتكاملها أو بتعطيل قدرة وكفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بشكل سليم**" ويتحقق الاعتداء على معطيات النظام عادة بعد تجاوز مرحلة الدخول والبقاء في نظام المعالجة الآلي للمعطيات، ويتخذ وفق ما نص عليه المشرع الجزائري صورتين " **الاعتداء على المعطيات الداخلية للنظام** " **أو** " **الاعتداء على المعطيات الخارجية للنظام**" .

تنص المادة 394 مكرر من قانون العقوبات أنه " **يعاقب بالحبس من ستة أشهر (06) إلى ثلاث (03) سنوات وبغرامة مالية من 500.000 إلى 2.000.000 دج كل من أدخل**

[1] - دمان ذبيح عماد/ بهلول سمية ، مرجع سابق، ص 147.

بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها" وما يسجل أن عقوبة الاعتداء العمدي على المعطيات تفوق عقوبة الدخول أو البقاء غير المشروع سواء في صورتها المشددة أو البسيطة ذلك أن جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة لا تؤدي إلى حدوث أضرار معينة تلحق بالمعطيات أو النظام، أما الصورة المشددة وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة الاعتداء العمدي على المعطيات وإن كانت تؤدي إلى نفس النتائج فإن عقوبتها أكبر لأنها جريمة عمدية يجب فيها توافر القصد الجنائي لدى مرتكب جريمة الدخول أو البقاء غير المشروع في صورتها المشددة.[1]

ثانيا : العقوبات التكميلية :

يقدر المشرع في العديد من الحالات عدم كفاية العقوبة الأصلية التي قررها كجزاء على اقتراف الجريمة في ردع الجاني أو في حماية المصلحة التي قرر حمايتها، فيأتي بالعديد من العقوبات الفرعية لتدعيم الحماية المقررة للمصلحة المعنية، فالعقوبات التكميلية هي عقوبات تضاف إلى العقوبات الأصلية، وقد حددها المشرع في نص المادة 09 المعدلة بموجب القانون23/06 المعدل والمتمم لقانون العقوبات، وإن كانت هذه العقوبات مرتبطة بالعقوبة الأصلية، إلا أنها لا يحكم بها على المحكوم عليه بقوة القانون، إذ لا توقع إلا بالنطق بها وتتمثل هذه العقوبات في المصادرة والغلق ونشر الحكم وستتم مناقشتها كالتالي:[2]

01 – المصادرة :

[1] - دمان ذبيح عماد/ بهلول سمية ، مرجع سابق ، ص148.
[2] - رابحي عزيزة ، مرجع سابق ، ص 246

يقصد بالمصادرة تجريد الشخص من ملكية مال أو من حيازة شيء معين له صلة بجريمة وقعت أو يخشى وقوعها، ثم إضافتها إلى جانب الدولة بلا مقابل بناء على حكم من القاضي الجنائي كما عرفها المشرع الجزائري من خلال المادة 15 من قانون العقوبات.

فأحيانا العقوبات الأصلية لا تكن كافية كما هو الشأن بالنسبة للجرائم الماسة بالسرية المعلوماتية، إذ أنه من الممكن أن يرتكب الجاني في هاته الجرائم جرائم أخرى بحيازته لبعض الوسائل التي ارتكب بها جرائمه ومنه يعاود ارتكاب جرائم أخرى تمس السرية أو سلامة أو وفرة المعلومات لهذا يكون بالنسبة لهؤلاء من الضروري اتخاذ تدابير عملية لمنع وقع جريمة أخرى من نفس الشخص ويتحقق ذلك بمصادرة تلك الوسائل وهذا ما نصت عليه المادة 394 مكرر 6 كالتالي " مع الاحتفاظ بحقوق الغير حسن النية يحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة" والملاحظ على النص أن المشرع أخذ بعين الاعتبار حسن النية وبذلك يكون قد انسجم مع مبدأ الشرعية

02 – الغلق :

فإلى جانب عقوبة المصادرة نص المشرع على عقوبة تكميلية وجوبية أخرى هي الغلق وذلك بموجب المادة 394 مكرر 6 كما يلي " مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها"، ويكون بذلك المشرع جعل لعقوبة الغلق محلين هما المواقع محل ارتكاب الجريمة ومحل أو مكان الاستغلال.[1]

ولكن المادة لم تنص على مدة الغلق وبالتالي فإننا نرجع القواعد العامة لقانون العقوبات حيث تكون مؤبدة أو مؤقتة وذلك وفقا للمادة 16 مكرر 1 في فقرتها الأولى " يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي ارتكبت الجريمة

[1] - رابحي عزيزة ، مرجع سابق ، ص 246

بمناسبته ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة لا تزيد عن عشر سنوات في حالة الإدانة لارتكاب جناية أو خمس سنوات في حالة الإدانة لارتكاب جنحة...".[1]

المطلب الثاني : العقوبات المقررة للشخص المعنوي :

تبنى قانون العقوبات الجزائري مبدأ المسؤولية الجزائية للأشخاص المعنوية بموجب القانون15/04 في نص المادة 18 مكرر ليعزز ذلك بالقانون رقم 23 لسنة 2006 بنص المادة 51 مكرر وفي مضمون هذا النص استثنى المشرع الأشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية وعلى رأسها الدولة، ومن خلال استقراء المادة 18 مكرر فالعقوبات التي تطبق على الشخص المعنوي في الجنايات والجنح كالتالي:[2]

1 – الغرامة التي تساوي مرة إلى خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

2 – واحدة أو أكثر من العقوبات التكميلية التالية :

– حل الشخص المعنوي.

– غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.

– الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.

– المنع من مزاولة نشاط أو أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات.

– مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

– نشر وتعليق حكم الإدانة.

[1] - رابحي عزيزة ، مرجع سابق ، ص247

[2] - رابحي عزيزة ، المرجع نفسه، ص 248.

– الوضع تحت التصرف لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى جريمة أو الذي ارتكبت الجريمة بمناسبته.

ومما تجدر الإشارة إليه في هذا المقام أن هذه العقوبات ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية فحسب، بل تقع على كل الجرائم التي يرتكبها الشخص المعنوي، بينما ما يتعلق بالجرائم ضد الأنظمة المعلوماتية المحددة في المواد 394 مكرر وما بعدها فإن الغرامة المطابقة على هذا الأخير هي 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وذلك تطبيقا للمادة 394 مكرر 4 في قانون العقوبات الجزائري .

حيث أن المشرع الجزائري شدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية وهي الطائفة التي تنتمي إليها جل جرائم الدراسة، غذ نصت المادة 394 مكرر 4 بمضاعفة قيمة الغرامة 5 أضعاف ما قررته للشخص الطبيعي ونصت على الآتي " بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي ".

أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة فتضاعف الغرامة في التشريع الجزائري مرتين، إذ تضاعف إلى خمس(05) مرات عما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من شخص معنوي، وثم يضاعف ذلك إلى ضعفين لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة عشرة (10) مرات أضعاف عما هو مقرر على الشخص العادي.[1]

[1] - رابحي عزيزة ، مرجع سابق ، ص 248.

من خلال دراستنا للحماية الإجرائية للجريمة الالكترونية في الفصل الثاني تعرفنا بـــأن الجريمة الالكترونية جريمة لا محدودة ومتطورة ومرنة لذلك أعطت لهـــا التشـــريعات ســـواء العربية منها أو العالمية إجراءات تحقيق ومتابعة خاصة ، فلقد تعرضنا من خلال المبحث إلـــى الإجراءات المتبعة في الجريمة الالكترونية بصفة عامة والأعوان المنوطة بهم هذه الإجـــراءات وتطبيقها حسب ما جاء به القانون كذلك التحقيق في الجريمة الإلكترونية وكذا الوسائل المتخـــذة في البحث والتحري حولها كما تعرضا في دراستنا إلى التفتيش في البيئة الالكترونية واتخاذ نظم المعالجة الآلية للبيانات كحالة للتفتيش وكذلك ما يتطلبه التفتيش من ضمانات وفي نهاية الفصل ضمن المبحث الثاني تعرضنا إلى العقوبات المطبقة على الشخصين الطبيعي والمعنـــوي مـــن عقوبات أصلية وأخرى تكميلية، واستنتجنا بأن الجرائم التي تتسم بالالكترونية والمرتكبة بأحدث الوسائل التقنية والمعلوماتية أصبحت تشكل خطرا محدقا كل يوم يكبر ويهدد أمن البشرية بعدم الثقة في المواقع وفي المعلوماتية بشكل عام فلذلك كان لزاما على كل الدول في العالم بأسره بأن تكثف الجهود وتتخـــذ إجـــراءات صـــارمة وردعيـــة بشـــأن هـــذه الجريمـــة الالكترونيـــة.

الخاتمة

في نهاية دراستنا لموضوع الجريمة الإلكترونية، فإنني حاولت معالجة الموضوع من خلال فصلين أساسيين، حيث تناولت في الفصل الأول إلى الحماية الموضوعية للجريمة الالكترونية وما تحتويه من عناصر من ماهية الجريمة الالكترونية التي من خلالها درست مفهومها الموسع والضيق والمفهوم التشريعي، ودرست الخصائص المميزة لهذه الجريمة التي جعلتها تنفرد عن الجريمة التقليدية، سواء تعلقت خصائصها بالجريمة بذاتها، أو مرتكبها، كما أن هذا النوع من الجرائم يتنوع بحسب ما هو واقع أو مستهدف النظام المعلوماتي، أو ما يرتكب باستخدام النظام المعلوماتي.

كذلك تناولت بالتفصيل أركان الجريمة الالكترونية على التوالي الركن المادي والركن المعنوي، الركنين المكونين للجريمة وما يحتويه كل ركن.

وكفصل ثاني تناولت مليا الحماية الإجرائية للجريمة الالكترونية وما تحتويه، حيث كمبحث أول تعرضت لإجراءات التحقيق المتخذة في الجريمة الالكترونية والأعوان المكلفون بالبحث والتحري فيها ، كذلك كل الوسائل المادية والبشرية المستعملة في التحري عن الجريمة الالكترونية ، كما لا يفتني أهم عنصر وهو التفتيش في البيئة الالكترونية وما يحتويه من ضمانات.

وأخيرا فصلت جيدا في العقوبات المطبقة على الشخص الطبيعي والشخص المعنوي من عقوبات أصلية وأخرى تكميلية .

وعليه من خلال دراستنا هذه توصلنا لمجموعة من النتائج تمثلت في :

- ❖ مفهوم الجريمة الإلكترونية مفهوم يتغير ويتطور حسب تطور التكنولوجي، مما قد يعطي وصف جديد لبعض الجرائم التي يمكن أن تستجد بفعل واقعة إجرامية جديدة.

- ❖ أنواع الجرائم الإلكترونية يتغير بحسب الاستخدام ممكن أن تكون على الفـــرد، أو مؤسسات الدولة .
- ❖ المشرع الجزائري لم يحط تماما بأنواع الجرائم الإلكترونية.
- ❖ الأحكام الإجرائية من الجرائم الإلكترونية غير كافي تماما، وهـــذا بســـب غيـــاب النصوص التشريعية الكافية لمكافحة هذا النوع من الجرائم.
- ❖ غموض بعض النصوص الخاصة والتي تهدف لمكافحة الجريمة الإلكترونية، وهذا نظرا الكلاسيكية هذه النصوص وعدم شمولها لبعض الجرائم الحديثة.

على ضوء النتائج السابق ذكرها يمكن أن نقترح بعض التوصيات التي يمكن أن تســـاعد في مكافحة الجريمة الإلكترونية، وتمثلت هذه التوصيات في:

- ❖ وجوب إعادة تكييف المفهوم العام للجريمة الإلكترونية لجعله شموليا أكثر، وقـــابلا لأن يشمل بعض الجرائم المستحدثة في هذا الجانب وهذا لتسهيل محاربتها.
- ❖ وجوب إعادة النظر في قانون العقوبات الجزائري، خاصة في ما يخص هذا النوع من الجرائم وهذا من أجل مكافحتها.
- ❖ وجوب إعطاء حماية إجرائية لهذه الجريمة بهدف تقليل من مخاطر هذه الجريمة .
- ❖ وجوب إنشاء قيام بحملات توعية من أجل تقليل من هذا النوع من الجرائم وتحسيس من مخاطر هذه الأخيرة.
- ❖ وجوب إتباع المشرع الجزائري نهج المشرع الفرنسي في معالجة وتشريع عقوبة لجريمة نشر الفيروسات.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

المصادر :

01 – القرآن الكريم

02- أمر رقم 66-155 مؤرخ في 8 يونيو سنة 1966 يتضمن قانون العقوبات ، معدل ومتمم لا سيما بالقانون رقم 16-02 مؤرخ في 19يونيو سنة 2016.

03 - رقم 66-155 مؤرخ في 8 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية، معدل ومتمم، لا سيما بالقانون رقم 07/17 المؤرخ في 27 مارس سنة 2017.

المراجع

الكتب

1. إبراهيم محمد بن حمود الزنداني – الجرائم الإلكترونية من منظور الشريعة الاسلامية وأحكامها في القانون القطري والقانون اليمني : دراسة مقارنة – حقوق الطبع محفوظة لجامعة فطاني – جامعة فطاني – 2018.
2. أمحمدي بوزينة آمنة – إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام) – كلية الحقوق والعلوم السياسية – الشلف – كتاب أعمال ملتقى آليات مكافحة الجرائم الالكترونية في التشريع الجزائري المنعقد في الجزائر العاصمة في 2017/03/29.
3. خالد عياد الحلبي – إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت – ط1- دار الثقافة للنشر والتوزيع – عمان – 2011.

4. خالد ممدوم إبراهيم – الجرائم المعلوماتية – دار الفكر الجامعي – الاسكندرية – الطبعة الأولى – 2009.

5. سامي علي حامد عياد – الجريمة المعلوماتية وإجرام الانترنت – دار الفكر الجامعي – الاسكندرية – 2007.

6. عبد الحكيم رشيد توبة – جرائم تكنولوجيا المعلومات – دار المستقبل للنشر والتوزيع – الطبعة الأولى – 2009.

7. عبد الصبور عبد القوي علي المصري – التنظيم القانوني للتجارة الالكترونية – مكتبة القانون والاقتصاد – الرياض – السعودية.

8. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة) – منشورات الحلبي الحقوقية – بيروت – لبنان – 2003.

9. علي جبار الحسيناوي – جرائم الحاسوب والإنترنت – دار اليازوري العلمية للنشر والتوزيع – عمان – الأردن – 2009.

الاطروحات والمذكرات

10. براهيمي جمال – التحقيق الجنائي في الجرائم الإلكترونية – أطروحة لنيل شهادة الدكتوراه في العلوم القانونية – جامعة مولود معمري – تيزي وزو – 2018.

11. رابحي عزيزة – الأسرار المعلوماتية وحمايتها الجزائية – أطروحة مقدمة لنيل شهادة الدكتوراه – جامعة ابو بكر بلقايد – تلمسان – 2018/2017.

12. عبد القادر عمير – آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة) – أطروحة لنيل شهادة دكتوراه علوم في القانون العام – جامعة الجزائر 1 – 2020/2019.

13. عبد الله دغش العجمي – المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة – رسالة ماجستير – جامعة الشرق الأوسط – 2014.

14. عبد الله دغش العجمي – المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة – رسالة ماجستير – جامعة الشرق الأوسط – 2014.

15. صغير يوسف – الجريمة المرتكبة عبر الانترنت – مذكرة لنيل شهادة الماجيستير في القانون– جامعة مولود معمري – تيزي وزو – 2013.

16. سعيداني نعيم – آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري – مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية – 2013/2012.

17. حسنين خالد محمد – الجرلئم الالكترونية – بحث مقدم الى مجلس كلية القانون والعلوم السياسية كجزء من متطلبات نيل درجة البكالوريوس في القانون – جامعة ديالى – العراق – 2017.

18. ذياب موسى البداينة – كلية العلوم الإستراتيجية – الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية – ورقة علمية بعنوان (الجرائم الإلكترونية : المفهوم والأسباب) – 2014/09/04.

19. عبد الله بن عبد العزيز بن عبد الله الخثعمي – التفتيش في الجرائم المعلوماتية في النظام السعودي (دراسة تطبيقية) – مذكرة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية – جامعة نايف العربية للعلوم الأمنية – 2011.

المجلات

20. أيت عبد المالك نادية – فلاح عبد القادر – التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري – مجلة الأستاذ الباحث للدراسات القانونية والسياسية – جامعة الجيلالي بونعامة – خميس مليانة – العدد 2 – المجلد 4 – 2019.

21. بوضياف اسمهان – الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر – مجلة الأستاذ الباحث للدراسات القانونية والسياسية – جامعة محمد بوضياف المسيلة.

22. دمان ذبيح عماد/ بهلول سمية – الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري – مجلة الحقوق والعلوم السياسية – جامعة عباس لغرور *خنشلة – 2020.

23. رضا هميسي – تفتيش المنظومات المعلوماتية في القانون الجزائري – مجلة العلوم القانونية والسياسية – عدد 5 – 2012.

24. زيوش عبد الرؤوف – الجريمة المعلوماتية في التشريع الجزائري – مجلة العلوم القانونية والاجتماعية جامعة زيان عاشور الجلفة – 2019.

25. سميرة معاشي – ماهية الجريمة المعلوماتية – مجلة المنتدى القانوني – العدد السابع – قسم الكفاءة المهنية للمحاماة – جامعة محمد خيضر.

26. عادل عبد الله خميس المعمري – التفتيش في الجرائم المعلوماتية – مجلة الفكر الشرطي – المجلد 22 – العدد86– الشارقة – الإمارات – 2013.

27. عادل يوسف عبد النبي شكري – الجريمة المعلوماتية وأزمة الشرعية الجزائية – مجلة الجريمة المعلوماتية (العدد السابع) – جامعة الكوفة كلية القانون.

28. عثماني عز الدين – إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية – مجلة دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية – العدد الرابع – جانفي 2018.

29. عربوز فاطمة الزهراء – التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية – مجلة جيل الأبحاث القانونية المعمقة – العدد 34.

30. ليندا بن طالب – التفتيش في الجريمة المعلوماتية – مجلة العلوم القانونية والسياسية – عدد 16 – 2017.

31. مجمع البحوث والدراسات – أكاديمية السلطان قابوس لعلوم الشرطة نزوى عمان – الجريمة الالكترونية في المجتمع الخليجي وكيفية مكافحتها– مجلس التعاون لدول الخليج العربية.

32. محمد طارق عبد الرؤوف الخن – جريمة الاحتيال عبر الانترنت – منشورات الحلب الحقوقية – بيروت – لبنان– الطبعة الأولى – 2011.

محمد علي سكيكر – الجريمة المعلوماتية وكيفية التصدي لها – دار الجمهورية للصحافة – ط1 – 2010.

33. محمود أحمد عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر والتوزيع – عمان – الأردن – الطبعة الأولى الإصدار الثاني – 2009.

34. نهلا عبد القادر المومني – الجرائم المعلوماتية – دار الثقافة للنشر والتوزيع – عمان – الأردن – الطبعة الثانية – 2010.

يوسف خليل يوسف العفيفي – الجرائم الالكترونية في التشريع الفلسطيني (دراسة تحليلية مقارنة) – الجامعة الإسلامية – غزة – 2013.

فهرس

المحتويات

الملاحق

الملخص:

الجريمة الإلكترونية هي تلك الجريمة التي تعاقبت على أزمان ومدد متعاقبة لتصل إلى ما هي عليه اليوم من التطور الهائل الذي نشهده، وبهذا الانتشار الرهيب، وبهذا التغير المستمر والتطور الكبير جعل من تحديد مفهوم موحد لها مشكلة واجهت التشريعات واختلفت الآراء وتباينت بين مفهوم موسع ومفهوم ضيق، أما المشرع الجزائري الذي أطلق تسمية جريمة المساس بأنظمة المعالجة الآلية للمعطيات على الجريمة الالكترونية في تعريفه لها وقد اتخذ نفس المفهوم المتداول.

أما فيما يخص الأركان المكونة للجريمة التقليدية هي نفسها الأركان المكونة للجريمة الالكترونية (الركن المادي والركن المعنوي).

ولقد اتخذت التشريعات المقارنة ومن بينها التشريع الجزائري عدة أجهزة خولتها خصيصا لمكافحة ومتابعة الجريمة الالكترونية وكذلك تقوم بالبحث والتحري عن مرتكبيها نخص بالذكر على المستوى الدولي المخابرات المركزية بالولايات المتحدة الأمريكية ومباحث أمن الدولة في مصر، أما على المستوى المحلي فنجد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال زيادة على القوانين الداخلية لكل دولة من تجريم في قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة .

لكن مع زيادة معدلات تلك الجرائم التي تتسم بالمعلوماتية كان لابد على التشريعات أن تقوم بترشيد تلك النصوص التقليدية كي تصبح نافذة في مواجهة الجرائم الالكترونية، إلى حين بعث وإرساء قوانين جديدة تتلائم والجريمة المعلوماتية.

Résumé

Le crime électronique est ce crime qui a suivi des époques et des périodes successives pour atteindre ce qu'il est aujourd'hui du formidable développement auquel nous assistons, et avec cette terrible propagation, et avec ce changement continu et ce grand développement, il en a fait la définition d'un concept unifié un problème auquel se sont heurtées des législations et des avis divergents et oscillant entre une notion élargie et une notion étroite, Quant au législateur algérien, qui a donné le nom de délit de violation des systèmes de traitement automatisé de données à la délinquance électronique dans sa définition de celle-ci, il a adopté la même concept en circulation.

Quant aux éléments constitutifs de la délinquance traditionnelle, ils sont les mêmes que les éléments constitutifs de la cybercriminalité (l'élément physique et l'élément moral).

La législation comparée, y compris la législation algérienne, a pris plusieurs agences spécifiquement autorisées à combattre et à suivre la cybercriminalité, ainsi qu'à rechercher et enquêter sur ses auteurs, notamment au niveau international, la Central Intelligence des États-Unis d'Amérique et l'État Enquêtes de sécurité en Égypte En plus des lois internes de chaque pays, les médias et la communication sont criminalisés dans le Code pénal, le Code de procédure pénale et les lois spéciales.

Mais avec l'augmentation des taux de délits caractérisés par les technologies de l'information, il était nécessaire que la législation rationalise ces textes traditionnels pour devenir efficace face aux délits électroniques, jusqu'à ce que de nouvelles lois soient promulguées et établies, compatibles avec délit d'information.