وزارة التعليم العالـي والبحث العلمي

جامعة العربي التبســي - تبسة

كلية الحقوق و العلوم السياسية

قسم:الحقوق

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي (ل م د)

دفعـــة: 2020

التخصص:قانون جنائي

الموضوع:

الحماية الجزائية للمعلومات عبر شبكة الأنترنت

إعــداد الطالــب:

- نباشي رياض

تحت إ شرا ف الأستاذ(ة):

- عثماني عز الدين

نوقشت أمام اللجنة المكونة من الأساتذة:

الاســـم واللقـــب	الرتبـــة العلميـــة	الصفـــة
أجعود سعاد	أستاذ محاضر قسم - أ-	رئيســـا
عثماني عز الدين	أستاذ محاضر قسم - أ-	مشرفـــا ومقررا
ملاك وردة	أستاذ محاضر قسم - ب-	عضـــوا منـاقشا

السنة الجامعية: 2020/2019

وزارة التعليم العالي والبحث العلمي

جامعة العربي التبسي - تبسة

كلية الحقوق و العلوم السياسية

قسم:الحقوق

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي (ل م د)

دفعـــة: 2020

التخصص:قانون جنائي

الموضوع:

الحماية الجزائية للمعلومات عبر شبكة الأنترنت

إعـداد الطالـب

- نباشي رياض

تحت إشراف الأستاذ(ة):

- عثماني عز الدين

نوقشت أمام اللجنة المكونة من الأساتذة:

الاســـم واللقـــب	الرتبـــة العلميـــة	الصفـــة
أجعود سعاد	أستاذ محاضر قسم - أ-	رئيســـا
عثماني عز الدين	أستاذ محاضر قسم - أ-	مشرفـــا ومقررا
ملاك وردة	أستاذ محاضر قسم - ب-	عضـــوا منـاقشا

السنة الجامعية: 2020/2019

الكلية لا تتحمل ما

يرد في هذه المذكرة

من أراء

♦ (فَتَعَالَى اللَّهُ الْمَلِكُ الْحَقُّ وَلَا تَعْجَلْ بِالْقُرْآنِ مِنْ قَبْلِ أَنْ يُقْضَى إِلَيْكَ وَحْيُهُ وَقُلْ رَبِّ زِدْنِي عِلْمًا)

صدق الله العظيم

سورة طه، الآية 114.

شكر وعرفان:

الحمد لله الذي هو اولى المحمودين بالحمد واولى المحمودين بالثناء والمجد.

الشكر جزيل الشكر لله رب العالمين صاحب الفضل على الناس اجمعين.

ابدأ بشكره وانتهي بشكره واستوسط بشكر من رافقني في هذا المشوار ومد لي يد العون في انجاز هذا العمل.

اخص بالذكر الاستاذ **عثماني عز الدين** الذي تفضل وقبل الاشراف على هذه الرسالة فكان لي نعم المعلم والموجه والناصح ادامه الله لنا.

كما اعبر عن عميق شكري وخالص تقديري الى الاساتذة الافاضل اعضاء لجنة المناقشة الاستاذة **أجعود سعاد** ، والاستاذة **ملاك وردة** جزاهم الله عني وعن طلاب العلم خير جزاء،

كما لا يسعني الا ان اشكر عمادة كلية الحقوق بتبسة كل باسمه وصفته بداية من اساتذتها الى كامل موظفيها الكرام.

الاهداء

الى اللذين قال الله فيهم: "واخفض لهما جناح الذل من الرحمة وقل ربي ارحمهما كما ربياني صغيرا"

الاسراء، 24.

وعرفانا لفضلهما ودعواتهما اهدي هذا العمل المتواضع للوالدين الكريمين، اطال الله عز وجل في عمرهما.

الى اخوتي واخواتي، لما قدموه لي من مساعدة ودعم وتشجيع حفظهم الله ورعاهم

الى اصدقاء الخير وكل من وقف الى جانبي

اهدي اليهم هذا العمل المتواضع

راجيا المولى عز وجل ان ينفعنا من علمنا وان يزدنا علما.

والله الموفق.

قائمة المختصرات.

ص: الصفحة.

ج: الجزء.

د ط: دون طبعة.

د د ن: دون دار نشر.

د ب ن: دون بلد نشر.

د س ن: دون سنة نشر.

UNODC: Office des Nations Unies contre les Drogues et le Crime.

مقدمة

تعاني المجتمعات في الآونة الأخيرة من انتهاك للحقوق والخصوصيات الإلكترونية، وذلك في ظل انتشار الجريمة الإلكترونية، وجاء تطوّر هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا التي يسرت سبل التواصل وانتقال المعلومات بين مختلف الشعوب والحضارات وسهلت حركة المعاملات.

ورغم تطور المنظومة القانونية للجريمة الالكترونية في فرنسا والجزائر والقوانين المقارنة، إلا أن هذا النوع من الجرائم قد أثار إشكالات قانونية من حيث تعريفها وتحديد مصطلحاتها وأنواعها، في مقابل قلة الأحكام والاجتهادات القضائية في هذا الشأن.

فهي جريمة تقنية تنشأ في الخفاء و توجه للنيل من الحق في المعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت ، وتظهر مدى خطورتها في الإعتداءت التي تمس الحياة الخاصة للأفراد وتهدد الأمن والسيادة الوطنيين وتشيع فقدان الثقة بالتقنية وتهدد ابداع العقل البشري.

اهمية الموضوع:

نهدف من خلال دراستنا لموضوع الحماية الجزائية للجرائم الالكترونية عبر شبكة الانترنت إلى تحقيق جملة من الأهداف العلمية والعملية أهمها:

1- الأهداف العلمية:

ومع تطور الانترنت وتوسع استخداماته وازدياد أعداد المستخدمين له في العالم أصبح الانترنت وسطا ملائما للتخطيط والتنفيذ عدد من الجرائم بعيدا عن رقابة وأعين الجهات الأمنية، إضافة إلى أنه ثبت أن المجرمين المعلوماتيين ليسوا بأشخاص عاديين فهم يتمتعون بقدر كبير من الذكاء والدهاء، ويتحكمون في التقنيات التكنولوجية الحديثة وهم قادرون على الذهاب بعيدا في ممارسة الإجرام عن طريق الانترنت، مما يستدعي توفير الأمن المعلوماتي

فعند ذكر كلمة أمن المعلومات فإن أول ما يتبادر إلى الذهن غالبا هو كشف معلومات كان يجب أن تبقى سرا، والحقيقة أن الحفاظ على سرية المعلومات لا يعدو أن يكون جانبا واحدا من جوانب الأمن حيث أن فكرة الأمن المعلوماتي وتطويره بات أمرا حتميا أمام قيام إمبراطورية المعلوماتية

يعتبر الحق في الخصوصية من بين الحقوق المكفولة دستوريا و المحمية في القوانين الوطنية وحتى القوانين الدولية ، و مع التطور العلمي و التكنولوجي الحديث تم اختراع وسائل الإتصال الحديثة كالهواتف الذكية و أجهزة الاعلام الآلي ، وأدى ذلك بدوره إلى اقتحام البريد الإلكتروني و كسر الشيفرات الخاصة به و العبث بالملفات الخاصة بالافراد بتغيير البيانات ، و المعطيات الخاصة بهم ولم يتوقف الأمر عند هذا الحد بل وصل إلى سب و قذف و تشويه سمعة هؤلاء الافراد.

2- الأهداف العملية:

بعد دراسة موضوع الحماية الجزائية للمعلومات عبر شبكة الانترنت فإن ذلك يساعد على الفهم الأكاديمي لأنواع الجرائم الالكترونية و الوقوف على وسائل مكافحة هذه الجرائم.

ورغم استحداث نصوص خاصة بالجرائم المعلوماتية إلا أنه في حالة غياب النص في بعض الأحوال فإنه لا مانع من تطبيق النصوص التقليدية في حالة ارتكاب جرائم تقليدية بواسطة تقنية معلوماتية، إذ أن الجرائم الالكترونية التي تستدعي تطبيق نصوص عقابية خاصة هي التي استحدث لها نصوصا.

وقد **دفعتنا لاختيار هذا الموضوع** مجموعة من الدوافع الشخصية والدوافع الموضوعية، فأما **الدوافع الشخصية** فنجملها فيما يلي:

ـ السعي إلى إثراء المكتبة الجامعية بمرجع متواضع حول الاجراءات الجزائية للجرائم الالكترونية عبر شبكة الانترنات.

ـ مواصلة دراسات تحسين المستوى والاستفادة .

أما عن **الدوافع الموضوعية** لاختيار الموضوع فيمكن أن نستعرضها كالاتي:

ـ مواكبة توجه سياسة الدولة نحو مكافحة السرقة المعلوماتية و الجرائم الالكترونية عبر شبكة الانترنت مثلا يمكن تجريمها من خلال النصوص العقابية التقليدية، ذلك لأن المشرع الجزائري وغيره من غالبية المشرعين لم يخصصوا لها نصا عقابيا مستحدثا .

الأمر الذي دفع بالدول إلى العمل ملياً للحد من هذه الجرائم من خلال التوعية والوسائل الوقائيّة الأمنية وغيرها ،بحيث بات لازما أن يواكب تطور الجريمة و أساليبها تطورا في مجال السياسة التشريعية عموما و السياسة الجنائية على وجه الخصوص ، بعد أن أصبح واضحا التهديد المباشر للمنظومة الحقوقية الذي يتسبب فيه إساءة استخدام شبكة المعلوماتية، لهذا الاعتبار تكاثفت الجهود الدولية لمواجهة الآثار السلبية المترتبة على إساءة استخدام تقنية الاتصالات و المعلومات.

إشكالية البحث:

لقد أثارت هذه الأنماط الإجرامية المستحدثة على شبكة الانترنت عدة مشاكل نظرا لأنه من الصعب السيطرة على هذه الشبكة، وعلى الجرائم التي ترتكب عبرها، هذا من جهة، ومن جهة أخرى من الصعب اكتشاف هذه الجرائم أو تحديد مصدرها، لأن الجاني يستخدم اسما مستعارا أوغير حقيقي.

ومن الصعب أيضا إيقاف ارتكاب الجريمة عبر الشبكة بسبب سرعة نشر المعلومات

و تسجيلها على الحاسبات الخادمة في الخارج مما يجعلها تجوب العالم في لحظات .

وذكرنا بأن هذه الجرائم ترتكب عن طريق أنماط إجرامية مستحدثة، وتتمثل هذه الأنماط الإجرامية في الفيروسات و سرقة الأسرار السياسية و التجارية وهذا يدفعنا إلى التساؤلات التالية:

– على اي اساس تحظى المعلومة بالحماية الجنائية و ما مدى نجاعة المشرع الجزائري في مواجهة الجريمة المعلوماتية ؟

و في سبيل الإجابة على هذه الإشكالية تثور مجموعة من الإشكاليات الفرعية على النحو التالي:

– ماهي الجرائم الإلكترونية عبر شبكة الانترنت ؟

- أنواع هذه الجريمة ومجال تحقيقها؟

- ما هو الاختصاص بنظر هذه الجرائم ؟

أهداف البحث:

التعريف بهذه الجريمة من أجل تجنبها.

- التوعية من مخاطر الوقوع ضحية للجريمة الإلكترونية.

- التعريف بالوسائل الكفيلة التي تضمن وتحفظ المعلومة المنشورة إلكترونيا.

- محاولة الوصول إلى معرفة طرق التعامل مع البيئة الإلكترونية للتصدي للجريمة الإلكترونية.

المنهج المتبع:

إعتمدنا للإجابة عن الإشكالية المطروحة في هذه الدراسة على المنهج التحليلي والمنهج الوصفي ،وهذا ما تتطلبه الدراسة في مثل هذه المواضيع:

المنهج الوصفي : باعتبار أن الجرائم الالكترونية عبر شبكة الانترنت من الجرائم الحديثة ولذلك تطرقنا إلى ماهية الجرائم الالكترونية

المنهج التحليلي: باعتباره المنهج المناسب لمعالجة مختلف العناصر الأساسية للبحث من تحليل و شرح للنصوص القانونية محل الدراسة لبيان حقيقة هذا البحث أهداف علمية ، كما أن إتباع هذا المنهج سيكون ضروريا لتحليل بعض النصوص القانونية الخاصة بالتشريع الجزائري و مدى كفاية هذه النصوص في تحقيق حماية الجرائم الالكترونية، وتتخلل هذه الدراسة بعض التشريعات المقارنة و ذلك بسبب ندرة النصوص القانونية الجزائرية في هذه المادة من جهة أخرى.

ولقد واجهتنا ونحن بصدد اعداد هذا البحث مجموعة من **الصعوبات** اهمها عدم القدرة على التنقل من اجل الحصول على المراجع وغلق المكتبات العامة

والخاصة بسبب اجراءات الحجر الصحي الذي فرضته الحكومة كاجراء وقائي للحد من انتشار فيروس كورونا المستجد" كوفيد19" الذي لا يزال الى حين طباعة هذه الكلمات يحصد الارواح عبر مختلف بقاع العالم.

هذا بالاضافة الى قلة وندرة المراجع والدراسات المتخصصة في الموضوع رغم اهميته البالغة .

أسباب إختيار الموضوع:

ترجع أسباب إختياري لموضوع الحماية الجزائية للمعلومات عبر شبكة الانترنت إلى مجموعة من الأسباب الموضوعية و الذاتية على النحو التالي:

أ- الأسباب الموضوعية:

أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدت إلى بروز أشكال جديدة للإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول سعت من خلال قانونها إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، وكان التعديل بموجب القانون رقم04/151، والذي أدخل إلى قانون العقوبات بقسم سابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، والذي تضمن ثمانية مواد (من المادة 394 مكرر إلى المادة 394 مكرر 07).

إذن لم يقف المشرع الجزائري بالطبع متفرجا، حيث سارع هو أيضا إلى سن قوانين تتلائم وطبيعة الجرم المستحدث، فقد استدرك الفراغ القانوني من خلال القانون رقم 04-15 سالف الذكر.

ب- الاسباب الذاتية:

– اثراء المكتبة القانونية بمراجع تخص التكنولوجيا الرقمية خاصة فيما يخص التشريع الجنائي الجزائري

رغبتي الشخصية في البحث في مجال تكنولوجيا المعلومات وذلك بالإطلاع على أن هناك اختراقات و إعتداءات تقع عبر الإنترنت دون أن تسلم منها الدول سواء الدول المتقدمة أوالسائرة في طريق التقدم كما تمس الفرد.

كما وجدنا **صعوبة** في حصر المعلومات الواردة في الاحكام القانونية لمختلف القوانين بسبب كثرة التعديلات المدرجة كل سنة ، حيث لاحظنا استحداث احكام جديدة والغاء احكام اخرى ثم اعادة ادراجها مرة ثانية .

و للإلمام بجميع جوانب الموضوع والتوصل الى اجابة على الاشكالية المطروحة ،ارتأينا تقسيم بحثنا الى فصلين اثنين نتعرض في الفصل الأول الاحكام الموضوعية للحماية الجزائية للمعلومات عبر شبكة الانترنت ،في المبحث الاول وفي المبحث الثاني نتعرض الى الجريمة الإلكترونية و الإطار القانوني للجريمة الإلكترونية ، اما الفصل الثاني فقد خصصناه للاحكام الاجرائية للجريمة الإلكترونية وقسمناه بدوره الى مبحثين لنتعرض لضبط الجريمة المعلوماتية و اثباتها في المبحث الاول والاختصاص بنظر الجريمة الالكترونية في المبحث الثاني..

الفصل الأول: الاحكام الموضوعية للحماية الجزائية للمعلومات عبر شبكة الانترنت.

المبحث الأول: تعريف الجريمة الإلكترونية.

المبحث الثاني: الإطار القانوني للجريمة الإلكترونية.

الفصل الأول: الاحكام الموضوعية للحماية الجزائية للمعلومات عبر شبكة الانترنت:

ان ظاهرة جرائم الكمبيوتر والانترنت ، او جرائم التقنية العالية ، او الجريمة الإلكترونية ، ظاهرة اجرامية مستجدة نسبيا بحيث تعاني المجتمعات في الآونة الأخيرة من انتهاك للحقوق والخصوصيات الإلكترونية، وذلك في ظل انتشار الجريمة الإلكترونية، وجاء تطوّر هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا التي يسرت سبل التواصل وانتقال المعلومات بين مختلف الشعوب والحضارات وسهلت حركة المعاملات، إلا أن هذا التقدم المذهل والمميز لايخلو من عيوب لأن استخدامه لايقتصر على الإنسان الخير بل الإنسان الشرير الذي قد يوصف كمجرم لسعيه وراء أطماعه واقتناصه الفرص لتحقيق أغراضه غير المشروعة ، فلم يتوان عن استغلال التقنية لتطوير قدراته الإجرامية باستخدام شبكة المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية ، مما يلحق ضررا بالآخرين .

و بتنامي معدلات الجريمة وتطور أشكالها و تهديدها المباشر قد دق ناقوس مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن هذه الجرائم التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة.

فهي جريمة تقنية تنشأ في الخفاء و توجه للنيل من الحق في المعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت ، وتظهر مدى خطورتها في الإعتداءت التي تمس الحياة الخاصة للأفراد وتهدد الأمن والسيادة الوطنيين وتشيع فقدان الثقة بالتقنية وتهدد ابداع العقل البشري.

وأصبح يواجه المؤلفون في البيئة الرقمية المتشابكة العديد من المشاكل بسبب سهولة الوصول إلى مؤلفاتهم واستنساخها،في ظل تقاعس أو عدم مواكبة التشريعات التقليدية للسرعة التي تتطور بها التكنولوجيا الحديثة وعصر المعلوماتية، وعدم قدرتها على التكيف مع الوضع الحالي.

الأمر الذي دفع بالدول إلى العمل ملياً للحد من هذه الجرائم من خلال التوعية والوسائل الوقائيّة الأمنية وغيرها ،بحيث بات لازاما أن يواكب تطور الجريمة و أساليبها تطورا في مجال السياسة التشريعية عموما و السياسة الجنائية علي وجه الخصوص ،

بعد أن أصبح واضحا التهديد المباشر للمنظومة الحقوقية الذي يتسبب فيه إساءة استخدام شبكة المعلوماتية ، لهذا الاعتبار تكاثفت الجهود الدولية لمواجهة الآثار السلبية المترتبة على إساءة استخدام تقنية الاتصالات و المعلومات.

يتطلب دراسة مفهوم الجريمة الإلكترونية أن يتناول الباحث التعريف بهذه الجريمة، و كذلك بيان إطارها القانوني، وسيتم تناول هذا الفصل في مبحثين:

المبحث الأول: تعريف الجريمة الإلكترونية

إن جرائم الحاسبات الالكترونية أو كما تسمى بجرائم المعلوماتية لارتباطها بنظم المعالجة الآلية للمعطيات هي ظاهرة إجرامية حديثة النشأة؛ لتعلقها بتكنولوجيا الحاسبات الآلية فقد اكتنفها الغموض مما صعب عملية تحديد مفهومها وإن بيان المشكلات القانونية و العملية التي تثيرها الجريمة الإلكترونية تتطلب من الباحث أن يقوم يبحث مسألة أولية تتعلق بالتعريف بهذه الجريمة من خلال بيان معناها، و طبيعتها القانونية، و كذلك خصائصها، و سأقسم هذا المبحث إلى ثلاثة مطالب.

المطلب الأول: المعنى الإصطلاحي واللغوي للجريمة الإلكترونية

الجريمة الالكترونية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة وقد اختلف الفقهاء في تعريفها؛ فهناك من عرفها على أنها كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية. كما وقع اختلاف في تسميتها إلى أن المصطلحات الأكثر شيوعا ودقة هي جرائم الكمبيوتر والجرائم الالكترونية. كما يتسم مجرم الجريمة الالكترونية بأنه متخصص وله القدرة الفائقة والمهارة التقنية.

أما فيما يتعلق بالحماية الجزائية للمعلوماتية فقد تبناها المشرع الجزائري بموجب القانون رقم 04-05 المعدل والمتمم لقانون العقوبات فقد جرم الدخول والبقاء الغير مشروع في نظام المعالجة الآلية للمعطيات وجريمة الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي وحدد لكل نوع من الجرائم السابق الذكر أركانها والعقوبة المقررة لها.

لم يتناول المشرع الأردني تعريفا للجريمة الإلكترونية في قانون جرائم أنظمة المعلومات المؤقت رقم (30) سنة 2010م، كما انه لا يوجد في التشريع الكويتي قانونا يتناول التنظيم القانوني للجريمة الإلكترونية.

و قد تناول الفقه القانوني تعريفات مختلفة للجريمة الإلكترونية، و يمكن ردها إلى خمسة إتجاهات، على النحو الآتي:

الإتجاه الأول: يعرف الجريمة الإلكترونية بأنها: كل أشكال السلوك غير المشروع الذي يرتكب بإستخدام الحاسب[1].

يلاحظ الباحث أن هذا التعريف يستند إلى ارتكاب الجريمة الإلكترونية بإستخدام الحاسب الآلي كي تعد جريمة إلكترونية.

الإتجاه الثاني : يعرف الجريمة الإلكترونية بأنها : نشاط غير المشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه[2].

يلاحظ أن هذا التعريف يستند إلى أن يكون الحاسب الآلي هو محل الجريمة الإلكترونية، و قد فسر جانب من الفقه أن هذه الجريمة هي جريمة إعتداء على الأموال المعلوماتية، و هي عبارة عن الأدوات المكونة للحاسب الآلي، و برامجه، و معداته[3].

---

[1] أنظر: الجنيهي، منير محمد، و الجنيهي، ممدوح (2006) ، جرائم الإنترنت و الحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي ،الإسكندرية ، ط1، ص14، و كذلك : رستم، هشام محمد (1999)، جرائم الحاسب المستحدثة، دار الكتب القانونية ، مصر ، ط1، ص 110.

[2] قشقوش، هدى حامد (1992)، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية ، القاهرة ، ص 5.

[3] العريان، محمد علي (2009)، الجرائم المعلوماتية، دار الجامعة الجديدة ، الإسكندرية ، ط2، ص170.

الإتجاه الثالث : يعرف الجريمة الإلكترونية بأنها : أي فعل غير المشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه و التحقيق فيه و ملاحقته قضائيا[1].

يلاحظ أن هذا التعريف يأخذ بوجوب إلمام الفعل بتقنية المعلوماتية الإلكترونية من حيث إستخدام الحاسب الآلي كي تعد جريمته من الجرائم الإلكترونية .

الإتجاه الرابع: يعرف هذا الإتجاه الجريمة الإلكترونية بأنها: الإعتداءات القانونية التي يمكن أن ترتكب بواسطة الوسائل الإلكترونية بغرض تحقيق الربح[2].

و قد عرفت منظمة التعاون الإقتصادي و التنمية التابعة للأمم المتحدة الجريمة الإلكترونية بأنها: كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية[3].

ما يلاحظ على هذان التعريفين أن التعريف الأول إشترط أن يحقق الفاعل ربحا، و هذا الأمر برأي غير متحصل دائما من الجرائم الإلكترونية، كما أن الفعل المرتكب قد لا يكون عمديا فقد يحصل بطريقة غير مباشرة، كما أن تعريف منظمة التعاون الإقتصادي و التنمية أدرج الأموال المادية، و غير المادية – كما يرى البعض[4] – يمكن حمايتها بموجب نصوص قانون العقوبات التقليدية و لا حاجة لقانون خاص لحمايتها.

الإتجاه الخامس: يعرف الجريمة الإلكترونية بأنها: كل فعل أو إمتناع من مسألة الإعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجا بطريقة مباشرة و غير مباشرة لتدخل التقنية الإلكترونية[5].

---

[1] الشوا، سامي، (1993)، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية للقانون الجنائي ، القاهرة، 25-28 أكتوبر، ص 516.

[2] عبد الله عبد الكريم (2011)، جرائم المعلوماتية و الإنترنيت – الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ط1، ص15.

[3] أورد هذا التعريف د. عبابنة، محمود أحمد (2005)، جرائم الحاسوب و أبعادها الدولية، دار الثقافة، عمان، ط1، ص 17.

[4] عبابنة، محمود أحمد ، مرجع سابق، ص 19.

[5] عبابنة، محمود أحمد ، مرجع سابق، ص 19.

و برأي الباحث فإن الإتجاه الأخير يعد التعريف الذي جاء به متوافقا مع التطور المستمر للجرائم الإلكترونية و لوسائلها التقنية ، و بخاصة أنه شمل الأموال المعنوية دون الأموال المادية، و بذلك يكون هذا التعريف إلى حد ما قد جمع المعايير التي جاءت بها الإتجاهات الأربعة سالفة الذكر.

و في ضوء ما سبق ، فإن الباحث يقترح تعريفا للجريمة الإلكترونية بأنها: كل فعل أو إمتناع يتم إعداده أو التخطيط له، و يتم بموجبه إستخدام أي نوع من الحواسيب الالية سواء حاسب شخصي أو شبكات الحاسب الآلي أو الأنترنت أو وسائل التواصل الإجتماعي لتسهيل إرتكاب جريمة أو عمل مخالف للقانون، أو تلك التي تقع على الشبكات نفسها عن طريق إختراقها بقصد تخزينها أو تعطيلها أو تحريف أو محو البيانات أو البرامج التي تم تحويلها.

المطلب الثاني: الطبيعة القانونية للجريمة الإلكترونية:

يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج و المعلومات، و هل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للإستثناء يمكن الإعتداء عليها بأية طريقة كانت؟

إنقسم الفقه إلى إتجاهين: الأول يرى أنه وفقا للقواعد العامة فإن الأشياء المادية وحدها هي التي تقبل الحيازة و الإستحواذ، و أن الشيء موضوع السرقة يجب أن يكون ماديا أي له كيان مادي ملموس حتى يمكن إنتقاله و حيازته عن طريق الإختلاس المكون للركن المادي في جريمة السرقة ، و لما كانت المعلومات لها طبيعة معنوية و لا يمكن إعتبارها من قبيل القيم القابلة للحيازة و الإستحواذ ، إلا في ضوء حقوق الملكية الفكرية ، لذلك تستبعد المعلومات و مجرد الأفكار من مجال السرقة، و ما لم تكن مسجلة على إسطوانة أو شريط ، فإذا ما تم سرقة إحدى هاتين الدعامتين الخارجية، فلا تثور مشكلة قانونية في تكييف الواقعة على أنها سرقة مال معلوماتي ذو طبيعة مادية،

و إنما المشكلة تثور عندما تكون أمام سرقة مال معلوماتي مادي غير مادي[1] ، و الإتجاه الثاني يرى المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للإستحواذ مستقلة عن دعامتها المادية، و ذلك أن المعلومات لها قيمة إقتصادية قابلة لأن تحاز حيازة غير مشروعة، و أنها ترتبط كما يقول الأستاذان(Vivant & Catala) بمؤلفها عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للتملك أو الإستغلال على قيمته الإقتصادية ، و ليس على أساس كيانه المادي ، و لذلك فهو يستحق الحماية القانونية و معاملته معاملة المال[2].

و هناك من يقول: " إنه يجب أن نفرق بأن هناك مالا معلوماتيا ماديا فقط و لا يمكن أن يخرج عن هذه الطبيعة و هي آلات و أدوات الحاسب الآلي مثل وحدة لعرض البصري، ووحدة الإدخال، و أن هناك من المال المعلوماتي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية و هي المال المادي الشريط الممغنط أو الإسطوانة الممغنطة أو الذاكرة أو السلك التي تنتقل منها الإشارات من على بعد، كما هو الحال في جرائم التجسس عن بعد، إذن من المنطق القول إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة و البرامج لقيمته المادية و هي ثمن الشريط أو ثمن الإسطوانة، و إنما يسرق ما هو مسجل عليهما من معلومات و برامج[3].

" إن التحليل المنطقي يفرض الإعداد بفكرة الكيان المادي للشيء الناتج عنه إختلاس المال المعنوي للبرامج و المعلومات، و أنها لا يمكن أن تكون شيئا ملموسا محسوسا، و لكن لهما كيان مادي قابل للإنتقال و الإستحواذ عليه بتشغيل الجهاز و رؤيتهما على الشاشة مترجما إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي، و إنتقال

---

[1] المطردي، مفتاح بوبكر (2012)، الجريمة الإلكترونية، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 23-25 أيلول، ص 17.

[2] نقلا عن : محمد عبد الله (2007)، موسوعة جرائم المعلوماتية – جرائم الكومبيوتر و الأنترنيت، المكتب العربي الحديث، الإسكندرية، ص 43-44.

[3] الزعبي، جلال محمد و المناعسة، أسامة محمد (2013)، جرائم تقنية نظم المعلومات الإلكترونية ، دار الثقافة ، عمان،ط1، الإصدار الرابع، ص 36-37.

المعلومات يتم عن طريق إنتقال نبضات و رموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادرة عنه يمكن سرقته، و بالتالي لها كيان مادي يمكن الإستحواذ عليه (البرامج و المعلومات)، و طالما أن موضوع الحيازة (أي المعلومات) غير مادي، فإن واقعة الحيازة تكون من نفس الطبيعة أي غير مادية (ذهنية)، و بالتالي يمكن حيازة المعلومات بواسطة الإلتقاط الذهني عن طريق البصر"[1].

و عند حديثنا عن طبيعة الجرائم الإلكترونية يجب علينا أن نتحدث أيضا عن ذلك من خلال الحديث عن أكثر الصور شيوعا لإختلاف كل منها في تكييفها عن الأخرى.

أولا: الجرائم الإلكترونية جرائم أموال:

إن الجرائم الإلكترونية وفقا للمفهوم الذي بيناه آنفا، تظهر بصورتين[2]:

<u>الأولى:</u> جرائم واقعة بإستخدام الحاسب الآلي، و منها إستخدام الحاسب الآلي لتزييف العملة، أو التزوير في محررات رسمية، أو الإختلاس[3]، أو إستخدام الحاسب الالي لأغراض الدخول غير المشروع للبيانات و المعلومات المخزنة على حاسب آلي آخر، و

[1] قشقوش ، هدى حامد، مرجع سابق، ص 51-52.

[2] المومني، نهلا، مرجع سابق، ص64.

[3] من الأمثلة الواقعية على الإختلاس بواسطة الحاسب الالي قيام أحد الموظفين في مكتب محاسبة في أمريكا/كاليفورنيا بإختلاس أكثر من مليون دولار عن طريق التلاعب بالحسابات التي يريها بالمكتب لشركة شحن خضار و فواكه إذ لاحظ بحكم كونه محاسبا أن عملية التدفق و المراجعة على حسابات شركة الشحن غير دقيقة، و غير كاملة ، فقام بإختلاق سبع عشرة شركة وهمية جعل لها في حسابا شركة الشحن مستحقات مالية عن خدمات تؤديها، بحيث يقوم هو بالإستيلاء على تلك المبالغ، مع حرصه على ألا يتجاوز نسبة ما يختلسه النسب المعقولة حتى لا تثار حوله المشاكل، فقام بإعداد برنامج خاص يتولى وفقا لمعايير حسابية – تراعي مختلف الظروف الواقعية لإيرادات الشركة و مصروفاتها – تحديد مقدار الإختلاس دون أن يكشف أمره في عمليات التدفق و المراجعة، و من العجيب أن أمر هذا المجرم لم يكتشف إلا بمحض الصدفة نتيجة لضخامة قيمة الشيكات ، فصدر على المختلس حكم بالسجن عشر سنوات، أنظر: الهيتي، محمد حماد مرهج (2004)، التكنولوجيا الحديثة و القانون الجنائي، دار الثقافة، عمان، ط1، ص 46.

ذلك عبر شبكات الإتصال الدولية، أو بصورة مباشرة بغية الحصول على منافع نقدية أو غيرها، أو اخذ المعلومات و البيانات.

الثانية: جرائم واقعة على الحاسب الآلي بمشتملاته المتعلقة بالجانب المادي، أو الجانب المعنوي كجرائم تعديل أو تحويل أو تقليد برامج الحاسب الآلي، و جرائم تدمير المعلومات و البيانات الخاصة بالحاسب الالي نفسه، بالإضافة إلى الجرائم التقليدية العادية التي تطال الجانب المادي للحاسب الآلي كالسرقة و الإتلاف.

و في كلتا الحالتين يمكن أن توصف الجرائم الإلكترونية بانها جرائم أموال . إذ موضوعها دائما هو المال، هذا مع التسليم بأن الجانب المعنوي للحاسب الآلي و ما يشتمل عليه المال بالمعنى الفني و القانوني.

و لعل ما يدعم وجهة النظر هذه من ان الجرائم الإلكترونية هي جرائم أموال و ضخامة السلوكيات غير المشروعة و الناتجة عن إستخدام الحاسب الالي لتحقيق مكاسب مالية سواء تم ذلك الغش أو الإحتيال أو اعمال التخريب و الهدم أو المضاربات غير المشروعة، و كلها جرائم تقع على الأموال من منظور قانون العقوبات[1].

و في هذه الحالة من الممكن أن تكون الكثير من جرائم الأموال التقليدية جرائم أموال إلكترونية، فقد تكون الجريمة الإلكترونية جريمة سرقة، و قد تكون جريمة إحتيال ، و قد تكون أيضا جريمة إساءة إئتمان(خيانة)، و قد تكون جريمة إتلاف لمال الغير[2].

ثانيا : الجرائم الإلكترونية جرائم اشخاص:

من الممكن وقوع جرائم أشخاص من خلال النظام الإلكتروني، و لكن هذا الشكل لا يجد الكثير من التطبيقات العملية على أرض الواقع، إذ ينحصر أثرها في مجموعة ضيقة من جرائم الأشخاص و ذلك في جرائم الذم، و القدح، و التحقير، و جريمة إفشاء

[1] أنظر مثلا، المواد(399-458) عقوبات أردني.

[2] الزعبي، جلال محمد و المناعسة، أسامة محمد ، مرجع سابق، ص 38.

الأسرار سواء التجارية أو الشخصية ، و كذلك جرائم التهديد ، و التحريض ، و جرائم الإعتداء على الحياة الخاصة عبر الإنترنت.

ثالثا: الجرائم الإلكترونية جرائم أمن دولة و جرائم مخلة بالثقة العامة و الآداب العامة:

نظرا للطبيعة الخاصة التي تتمتع بها جرائم أمن الدولة و إمكانية وقوع الكثير منها عن طريق الوسائل المحكية أو المقروءة ، فهي بذلك تعد جريمة ملائمة لتقع عبر الوسائل الإلكترونية سواء فيما يخص أمن الدولة الداخلي أو الخارجي، مثل جرائم التجسس ، و جرائم الإتصال بالعدو، و جرائم إثارة الفتن، و الحض عليها، و الجرائم الماسة بالوحدة الوطنية، و تعكير صفو الأمة.[1]

أما الجرائم المخلة بالثقة العامة و الآداب العامة فهي أيضا قابلة للوقوع عبر الوسائل الإلكترونية و ذلك مثل جرائم التزوير، و تقليد الأختام، و تزوير الأوراق البنكية، و المسكوكات، و إنتحال الشخصية[2].

و بالرجوع إلى قانون جرائم أنظمة المعلومات الأردني، يجد الباحث أن المشرع الأردني أحسن حينما تدخل و حسم الجدل الفقهي في طبيعة الجرائم الإلكترونية، إذ أنه عالج صورا متعددة من هذه الجرائم و حدد لها عقوبات ، و هي : الجرائم المرتبطة بالذمة المالية ، و التي تتعلق ببطاقات الإئتمان، أو بالبيانات، أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بموجب المادة (6) منه، و كذلك جرائم غش الحاسب الآلي(التحايل المعلوماتي)، بموجب المادتين (4 ،3) من القانون المذكور، و أيضا عالج الجرائم المتصلة بالحياة الخاصة لجريمة إلتقاط أو إعتراض أو التنصت على المرسل من خلال النظام الإلكتروني في المادة (5) من القانون المذكور، و كذلك جريمة نشر أعمال إباحية تتعلق بالإستغلال الجنسي لمن لم يكتمل الثامنة عشرة من العمر، أو ترويج هذه الأعمال بمقتضى المادة (8) من نفس

[1] منصور، محمد حسين (2010)، المسؤولية الإلكترونية، دار المعارف، الإسكندرية، ط2، ص148.

[2] حجازي، عبد الفتاح بيومي (2008)، التزوير في جرائم الكمبيوتر و الأنترنت، دار الكتب القانونية ، مصر ، ط1، ص 58 – 59.

القانون، و كذلك جريمة ترويج الدعارة بموجب المادة (9) من ذات القانون، و كذلك القيام بأعمال إرهابية أو دعم لجماعة ، أو تنظيم ، أو جمعية تقوم بأعمال إرهابية، أو تمويلها بموجب المادة (10) من نفس القانون، و كذلك أي إطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني ، أو العلاقات الخارجية للمملكة الأردنية ، أو السلامة العامة ، أو الإقتصاد الوطني، و ذلك بموجب المادة (11) من القانون المذكور.

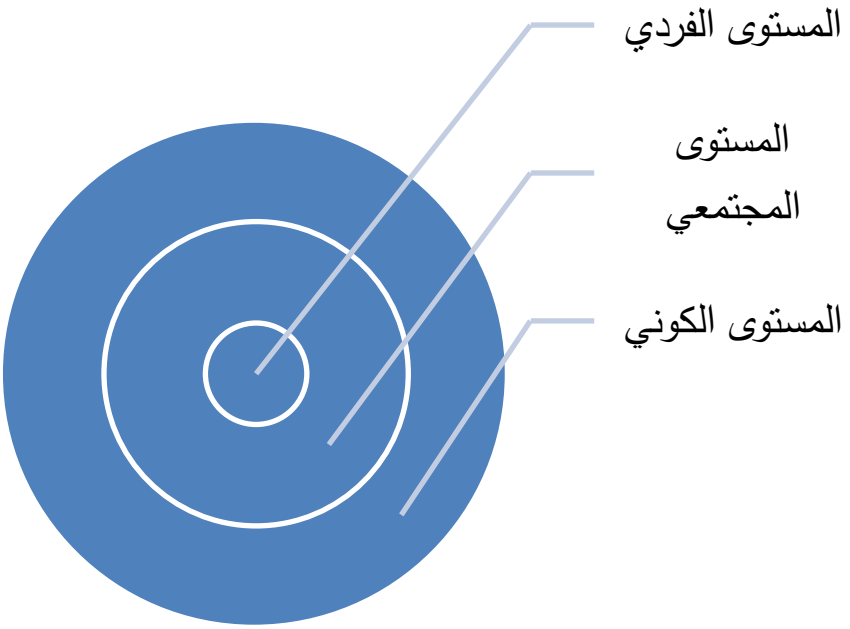
أما بالنسبة للمشرع الكويتي ، فحتى وقتنا الحالي لم يدخل قانونا خاصا بالجرائم الإلكترونية ، رغم أهميته القانونية و العملية لمكافحة هذا النوع من الجرائم، و في هذا الصدد يرى جانبا من الفقه القانوني الكويتي أن : عقوبة الجرائم الإلكترونية و الإختراقات غير المشروعة بالكويت تصل إلى التكييف القانوني للجريمة الإلكترونية لإختلاف الوقائع التي تم إرتطابها ، و على سبيل المثال: إذا كان الدخول على حسابات الأشخاص لدى البنوك، و الإستيلاء على أموال منها، فإن الوقائع قد تشكل جنحة السرقة وفقا للمادة (221) من قانون الجزاء الكويتي ، أو جنحة السرقة المنصوص عليها بالمواد (222 ، 223 ، 224 ، 225 ، 226 ، 227) من القانون الجزائي ، حيث تصل العقوبة إلى 3 سنوات، أما إذا كان الدخول إلى الحسابات و المواقع الشخصية على شبكة الأنترنت ، فإن كان ذلك بنشر عبارات أو ألفاظ تشكل قذفا أو سبا يكون ذلك معاقبا بالجنحة المؤثمة بالمادتين(209 ، 210) من القانون الجزائي الكويتي رقم (16) لسنة 1960م.

و قد تشكل الأفعال إحدى الجنايات المتعلقة بأمن الدولة الخارجي أو أمن الدولة الداخلي المنصوص عليها في القانون رقم(31) لسنة 1970م بتعديل لبعض أحكام القانون الجزائي، فضلا عن الجنح المؤثمة بالقانون رقم (9) لسنة 2011 بشأن إساءة إستعمال أجهزة الإتصالات الهاتفية و أجهزة التنصت[1].

[1] الكندري، عبد الله (2013)، مقال قانوني بعنوان: " الجرائم الإلكترونية في التشريع الكويتي" ، جريدة الأنباء، جريدة كويتية يومية شاملة، العدد الصادر يوم الإثنين 22 يوليو 2013م، ص7، موقع الجريدة: www.alanba.com.km.

المطلب الثالث: أسباب الجريمة الإلكترونية:

هناك عدة من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية منها ما يقع على مستوى كوني، و منها ما يقع على مستوى مجتمعي، و منها ما يقع على مستوى فردي أو شخصي، كما أن أسباب الجريمة الإلكترونية تتفاوت وفق نوعها و نوع المستهدف و مستوى تنفيذه (فردي، مجتمعي، كوني) ، فجرائم الشباب و الهواة و الصغار تختلف عن أسباب جرائم المحترفين، و تختلف وفق هدفها سرقة معلومات أو تجارة بالمعلومات أومعلومات شخصية..... الخ.



شكل رقم (1) أسباب الجريمة الإلكترونية وفق مستوى التحليل

أسباب الجريمة على المستوى الفردي

البحث عن التقدير: (sake of recognition):

هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش و صغار سن، و ذلك من باب التحدي، وحب الظهور في الإعلام، و غالبا ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينات.

الفرصة: (**opportunity**) : لقد وفرت التقنيات الحديثة و الأنترنت فرصا غير مسبوقة لإنتشار الجريمة الإلكترونية، إذ أن الفرصة تنتج الجريمة (Felson & Clark, 1998)، و تلعب البيئة و ترتيباتها دورا كبيرا في إنتاج الجريمة و الخروج على قواعد الإجتماعية، فوقفت الإنحراف عن قواعد الإمتثال ليلا نهارا و في أي مكان، و عدم وجود رقابة، كلها عوامل تزيد من فرصة إرتكاب الجريمة الإلكترونية، و قد تشكل المعلومات هدفا سهل المنال ، و يحقق المنفعة السريعة، و بالتالي يمكن سرقتها أو سرقة محتوياتها، فهي فرصة مربحة و قليلة المخاطر، و إحتمالية الكشف للفاعل فيها ضئيلة (Rice & Smith, 2002)[1].

إن تكنولوجيا المعلومات و الإتصالات و الإستخدام المتزايد للأنترنت قد خلق فرص جديدة للمجرمين و سهلت نمو الجريمة، أن جرائم الأنترنت تمثل " شكلا جديدا و مميز للجريمة، و قد خلقت تحديات لتوقع التطورات، و الوقائع منها، (UNODC, 2013) .

ضبط الذات المنخفض: تنطلق هذه الدراسة من النظرية العامة في السلوك الطائش (gottfredson & hirdchi, 1990) ، و تؤكد هذه النظرية أن إحتمالية إنخراط الأفراد في فعل إجرامي تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض ، و قد عرف كل من جودفردسون و هيرشي السلوك الطائش بأنه: " كل فعل يقوم على القوة و الخداع لتحقيق الرغبات الذاتية، و بناء على هذا التعريف الذي يستدل على طبيعة السلوك الطائش من خصائص الأشخاص، فإن السلوك الطائش يعد مظهرا من مظاهر الضبط الذاتي المنخفض ، و كما في نظرية الضبط الإجتماعي لهيرشي ، فالدوافع لإرتكاب السلوك الطائش ليست متغيرة ، و ذلك لأن كل فرد قد يندفع لتحقيق مصالحه الشخصية بما في ذلك السلوك الطائش، فالسلوك الطائش يعد عملا سهلا و قد يحقق المصالح الخاصة بسرعة مثل (الرشوة، السرقة) و نحوهما من الأعمال الإجرامية التي تحقق بسرعة و سهولة دون إنتظار أو بذل جهد ، و لكن

[1] عبد الحميد ابراهيم، العلاقة بين الإرهاب المعلوماتي و الجرائم المنظمة، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية خلال الفترة. من 24 9 مارس 1222 بالقنطيرة بالمغرب، ص، ص 1.2.4

الإختلاف بين الأفراد يعود إلى مستوى ضبط الذات، ووجود الفرصة لإرتكاب السلوك المنحرف (البداينة و الرشيد و المهيرغ ، 2005).

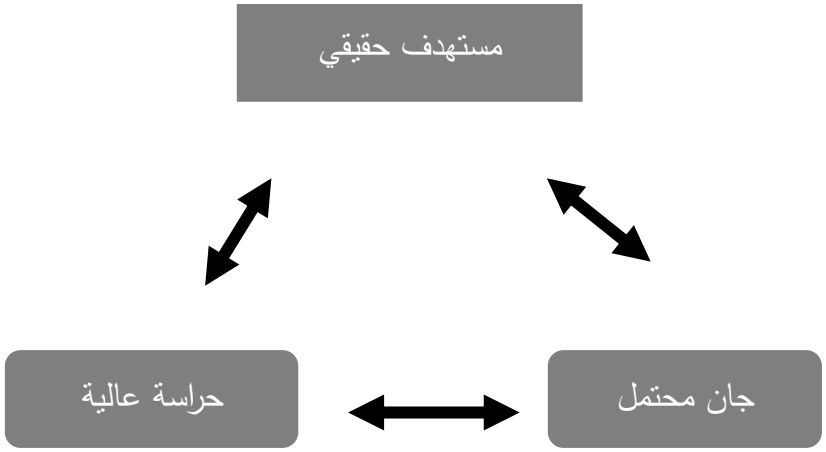
إن توفر الضبط الذاتي المنخفض مع وجود الفرصة لإرتكاب السلوك الطائش يعدان عاملين مؤثرين في إرتكاب السلوك الطائش، فتأثير هذين العاملين يكون نتيجة لإتحادهما ، و التفاعل بينهما هو المؤدي للسلوك الطائش، و قد حاول كل من جودفردسون و هيرشي غزو الإختلاف بين المجرمين و غيرهم إلى الإختلافات في مستوى ضبط الذات، إن نقص ضبط الذات قوة طبيعية تظهر في غياب الخطوات من أجل تطويره، أي أنه نتاج للتنشئة الإجتماعية الناقصة، حيث يفشل الآباء في مراقبة سلوك الطفل، و لا يلاحظون السلوك المنحرف عندما يحدث ، و إهمال معاقبة الطفل عندما يقترف سلوكا منحرفا، و عندما يتكون الضبط الذاتي في المراحل الأولى عند الأفراد، فإن الإختلافات في ضبط الذات تبقى ثابتة بشكل معقول من الوقت الذي تم تحديده عبر أطوار الحياة غير متأثر بالمؤسسات الإجتماعية (البداينة و الرشيد و المهيرغ ، 2005) بل على العكس فإن ضبط الذات قد يؤثر على أداء الأفراد في هذه المؤسسات، مثل المدرسة و العمل و الزواج، و الأشخاص ذو الضبط المنخفض لا يميلون إلى السلوكات المنحرفة فقط، بل أنهم في الأغلب غير ناجحين في المدرسة أو العمل أو الزواج (البداينة و التوابهة ، 2010).

أظهرت الدراسات أيضا أن ضبط الذات المنخفض و الإستعداد لتحمل المخاطر من أجل تحقيق مكاسب قصيرة الأجل، و هذا قد ينطبق على الأفعال التي يمكن أن تسهل أو تتعزز بواسطة وسائط الإتصالات الإلكترونية و الأنترنت، بالإضافة إلى ذلك، يتعرض الأفراد على الأنترنت لنماذج التعلم الإجرامي و الأقران قد يكونون أكثر ميلا للإنخراط في الجريمة الإلكترونية، و نظرية التعلم الإجتماعي " نظرية قد يكون لها تطبيق خاص عندما يتعلق الأمر بالجرائم الإلكترونية، فالمجرمين غالبا ما يحتاجون إلى تعلم تقنيات الكمبيوتر و الإجراءات، فالنظرية العامة للجريمة و نظرية التعلم الإجتماعي، تريان أن الأفراد يتصرفون في البيئة الإفتراضية كما يشاؤون في العالم الحقيقي.

الضغوط العامة: (General Sttrain) : ترجع نظرية الضغوط العامة للإنحراف و خرق القانون إلى دافع ناجم عن قوى البناء الإجتماعي أو إستجاباته النفسية و الإجتماعية للحوادث و الظروف و التي تعمل كضغوطات أو مقلقات خاصة عندما لا تتاح للأفراد الفرصة لتحقيق أهدافهم المقبولة إجتماعيا(merton, 1938: agnew, 1992)، و أن مصادر الضغوط لا تتوقف على الإحباط الذي يجبره الفرد عندما تسد الطرق لتحقيق هدف ما، و إنما يشمل المشاعر السلبية التي تحدث في المواقف الإجتماعية (paternoster & mazerolle, 1994.) كما قد تلعب العوامل الإجتماعية و الإقتصادية أيضا دورا هاما في زيادة الجريمة الإلكترونية، فالضغط على مؤسسات القطاع الخاص لخفض الإنفاق و خفض مستويات التوظيف يمكن أن يؤدي على سبيل المثال إلى تخفيضات في الأمن و إلى فرص لإستغلال ثغرات و ضعف تكنولوجيا المعلومات و الإتصالات و الشركات، مما يضطر لتوظيف المتعاقدين من الخارج أو المؤقتين، أو يصبح هناك موظفين ساخطين بسبب إنخفاض في الأجور و الخوف من فقدان الوظيفة، و الخطر يزداد من الأعمال الإجرامية و النفوذ من قبل منظمة إجرامية (UNODC, 2013).[1]

النشاط الروتيني: و يمكن تفسير زيادة ضحايا الجريمة الإلكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية، فمع ظهور شبكة الأنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الاخرين في العلاقات الشخصية ، و الترفيه، و التجارة، ... الخ، أن التغيرات في أنشطة الناس الروتينية ، من مثل إستخدام النت و شبكات التفاعل الإجتماعي مثل الفيس بوك و الإيميل و المواقع و غيرها قد خلقت للجناة المتحفزين مع وجود أهداف قيمة و سهلة في الحيز الفضائي مع غياب الحراسة، و يرى كوهين و فيلسون (cohen and felson, 1979) إلى أنه من المرجح أن تحدث الجريمة عندما تتلاقى ثلاث عوامل هي:: الجاني المتحفز(motivated offender) و الهدف المناسب (suitqble tqrgets) و غياب الحراسة (absence of capable guardians) .

[1] WWW.UNODC.COM? اطلع عليه بتاريخ 04/04/2020 على الساعة 13:45



شكل رقم (2) نظرية الفرصة المصدر: البداينة و آخرون 2009

أنه لا بد من توافر هذه العوامل الثلاثة من أجل أن تحدث الجريمة ، و عدم وجود واحد من هذه العوامل هو " كافي لمنع حدوث ناجح لإكمال الإتصال المباشر في جريمة السلب (cohen and felson, 1979, p 589) و يعطي إهتمام إلى التقارب في الزمان و المكان ، و أن هذا التلاقي يمكن أن يؤدي إلى زيادة كبيرة في معدلات الجريمة من دون أي تغيير في "الحالة الظرفية" التي تحفز المجرمين(cohen and felson, 1979)، المبدأ الأساسي هو أن التغيرات الهيكلية في النشاط الروتيني تؤثر على التقارب في العناصر الثلاثة من الناحية النظرية، و بالتالي تؤثر على معدل الجريمة (meithe, mark, and dcott, 1987)[1] .

يبين الشكل أدناه عناصر النظرية الثلاثة الرئيسية في العالم الإفتراضي في الجريمة الإلكترونية ، حيث الجاني المتحفز(قد يكون) و المستهدف المناسب(

[1] تم اقتباسها في عدد: 452 مقالات ذات صلة الإصدارات الـ 9كلها (COHEN AND FELDON)

إستهداف الهوية أو المال) ، و لكن الحراسة القادرة (برامج الحماية و برامج المضادة للفيروسات).

أسباب الجريمة على المستوى المجتمعي:

التحضر(urbanization): يعد التحضر أحد أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة و غلاء المناطق الحضرية و المدن الكبيرة، و عادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية، باهضة التكاليف، و التي تتطلب مهارات عالية أحيانا، مما يجعل شرائح كبيرة من المهاجرين غير قادرة على تلبية متطلبات الحياة الحضرية، مما يجعلهم يعيشون في مدن الصفيح و الحياء الطرفية و الهامشية و كنتيجة يجد الناس أنفسهم في تنافس غير قادرين على مجاراته، مما يجعلهم يلتفتون إلى الإستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير و التي تعرف " أولا الياهو" (yahoo bays) ، و كما يرى ميك(mek,2012)، فإن التحضر سبب رئيسي للجرائم الإلكترونية في نيجيريا، و أن التحضر بدون الجريمة مستحيل، و كنتيجة بينهم قد وجدوا أن صفقة الإستثمار في الجريمة الإلكترونية مربحة(lucrative).

البطالة: (unemployment): ترتبط الجريمة الإلكترونية شأنها شان الجريمة التقليدية بالبطالة و الظروف الإقتصادية الصعبة، و ترتكز البطالة بين قطاعات كبيرة من الشباب، و كما يقول المثل النيجيري " العقل العاطل عن العمل هو ورشة عمل للشيطان " و لذا فان الشباب الذين يملكون المعرفة سيستثمرون ذلك في النشاط الإجرامي الإلكتروني.[1]

الضغوط العامة(Strains): تعد الضغوط العامة التي يتعرض لها المجتمع من فقر و بطالة و أمية و ظروف إقتصادية صعبة عوامل ضاغطة على المجتمع عامة و خاصة قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف و ضد

[11] https://www.nw3c.org/ اطلع عليه بتاريخ 05/04/2020 على الساعة 09:10

المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الإتجار بالبشر و الجنس و الجريمة الإلكترونية و غيرها.

البحث عن الثراء: (Quest for wealth): يسعى الإنسان إلى المتعة و يتجنب الألم هكذا تقول النظرية العامة في الجريمة لجوتفردسون و هيرشي (gottfredson and hirschi, 1990)، و يسعى الناس إلى الوسائل غير المقبولة إجتماعيا لتحقيق أهداف مقبولة إجتماعيا كما ترى نظرية الأنومي لميرتون، فالرغبة في الثراء تواجه صعوبات بالغة في تحقيقه بالطرق المقبولة إجتماعيا و قانونيا، و لذا يلجأ بعض الناس إلى الجرائم الإلكترونية حيث المستهدف يجمع أكبر مع سهولة التنفيذ و سرعة المردود و قلة الخطورة.

ضغط إنفاذ القانون و تطبيقه في الجريمة الإلكترونية(lack of law enforcement and implementation)، هناك الكثير من الدول التي لم تطور تشريعاتها و أجهزة العدالة فيها لكي تتمكن من مجازاة التقدم في الجرائم الإلكترونية و أساليبها، و هذا لا يتوقف عند التشريعات و إنما يشمل الشرطة و التحقيق و القضاء، و كيفية التعامل مع الأدلة الرقمية على المستوى الوطني، كما هو الحال على المستوى الدولي، فمما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية و الجنائية و ضعف الممارسات العدلية و الشرطية و القضائية في محاكمة و التحقيق في الجرائم الإلكترونية، و غالبا ما تجد في دول كثيرة تواضع التقنيات المتوافرة و كذلك الخبراء القادرون على متابعة و رصد و ملاحقة الجريمة الالكترونية داخل المجتمع و العابرة منها للحدود الوطنية.[1]

أسباب الجريمة على المستوى الكوني:

التحول للمجتمع الرقمي: إن من أهم سمات عصر المعلومات السمات الثلاثة الرئيسية: 1- تغير كمية في مقدار المعلومات المتدفقة و نوعيها، فبفعل تكنولوجيا الإتصالات و المواصلات فإن الصور و المعلومات تغطي كافة المعمورة بسرعة و دقة.2- إرسال المعلومات إلى العديد من مكان الحدث.3- وجود الشبكات

[1] عبد الحميد ابراهيم، المرجع السابق الذكر، ص14.

NETWORKING حيث يتم تداول المعلومات بين جميع الأطراف من مثل البريد الإلكتروني، الجوال ، ..... الخ (كوهين ، 2001) (البداينة ، 2008)، ففي القضاء الإفتراضي، تكونت التفاعلات الإفتراضية و حلت محل التفاعل وجها لوجه و تكونت السلوكيات الإفتراضية و المجتمع المحلي الإفتراضي (al-badayneb, 2012).

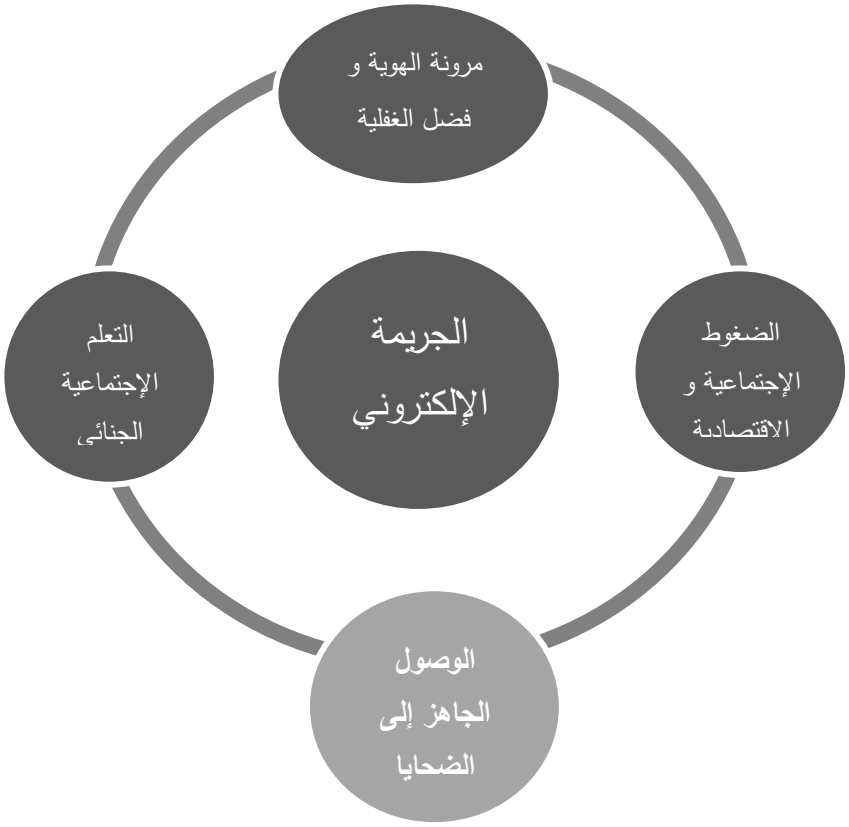
لقد دخلنا عصر المعلوماتية الجديدة (أي الفضاء الإلكتروني أو العالم الإفتراضي)، فالناس يقضون جزءا من حياتهم اليومية في الفضاء الإلكتروني، ينشؤون الشبكات و المواقع و يتمتعون بأنواع جديدة من العلاقات الإجتماعية ، و هم على تواصل مع ما يجري في العالم الخارجي ، و القيم ببعض الأعمال ، كل من هذه الانشطة قد جعلت من الممكن للجميع و بوجود جهاز كمبيوتر أو موديم مع معرفة التقنية القليلة و بعبارة أخرى فإن شبكة الأنترنت هي من خلقت ما يعرف الآن بإسم الفضاء الإلكتروني، أو العالم الإفتراضي، يحتاج المجتمع لكي يقوم بوظائفه إلى أن يعم الأمن و الأمان و أن يتحقق النظام و الإستمرارية ، و لا يتوقف توفر الأمن و الأمان في الواقع المادي للمجتمع بل أنتقل ليشمل العالم الإفتراضي (cyber space)(stol, 2008, leukfeld, and stol, 2013)

العولمة:

إن ظهور "الفضاء الإلكتروني" يخلق ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر نفسها، و الفرص المباشرة للجريمة و التي وفرتها أجهزة الكمبيوتر الآن، ضمن الفضاء الإلكتروني، قد يظهر الأشخاص الفروق في إمتثالهم الخاص (القانوني) و عدم الإمتثال(غير القانوني) مقارنة مع سلوكهم في العالم المادي[1].

فالأشخاص على سبيل المثال ، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم و موقعهم، بالإضافة إلى ذلك فمرونة الهوية(identity flexibility)، و عدم ظهور الهوية و ضعف عوامل الردع تحفز السلوك الإجرامي في العالم الإفتراضي (UNODC, 2013)

[1] https://drive.google.com/file/d/0B7Xzn6q9WBfsbGxHXzNBb080Umc/view?usp=sharing



UNODC, 2013m p.8

شكل رقم (3) تصور لبعض أسباب الجريمة الإلكترونية في الفضاء التخيلي.

هذا العصر يتطلب مؤسسات أمنية مصممة للتعامل مع التغير السريع، تركز على الإبداع و الشفافية و إرضاء العملاء(المجتمع بأسره)، مؤسسات ذات سرعة عالية في نشر المعلومات و إعلام الجمهور، مؤسسات قادرة على إعادة تصميماتها (الهندرةre-elgineering) لمواجهة المستجدات السريعة وسريعة التغير في عالم الجريمة الإلكترونية (البداينة ، 2004).

الترابط الكوني: و هناك عامل يمكن أن يساهم في دفع مستويات الجريمة هو في ظهور الترابط العالمي في سياق تحولات العالم الإقتصادية و الديمقراطية ، بحلول عام 2050 ، فإن العالم سوف يشهد تضاعف عدد سكان الحضر إلى 6.2 مليار – 80 في المئة من سكان العالم المتوقع من 8.9 مليار UNODC, 2013 ، أكد تقرير صدر عن المركز الوطني لجريمة الياقات البيضاء(national white collar crime centre (nw3c)(2002)(nw3c, 2002 [1] يؤكد أن فضاء الأنترنت قد خلق فرصا جديدة للمجرمين في التواصل مع الضحايا ، هو و قد بين أن السمات الفريدة للأنترنت ، و هي الكشف عن إسم الشخص و سهولة الإستخدام ، قد وفرت طرق جدية للمجرمين لإرتكاب جرائمهم ، بالإضافة إلى ذلك يتيح الأنترنت للمجرمين على التواصل بسرعة و بكفاءة نقل كميات كبيرة من المعلومات إلى العديد من الضحايا عبر غرف الدردشة ، البريد الإلكتروني، و لوحات الرسائل ، أو مواقع ويب(NW3C, 2002) ، و كل الذي يحتاجونه هو مهارات الحاسوب الأساسية و أجهزة الكمبيوتر المتصلة بالأنترنت، و بناءا على ذلك يوفر جهاز كمبيوتر واحد وسائل متنوعة لإجراء مجموعة من الجرائم، و يمكن للمجرمين إستخدام الكمبيوتر لبدء تواصل مع الضحايا و إدامته عن طريق شبكة الإنترنت، لإجراء المعاملات المالية الإحتيالية(nw3c, 2002)، يشير في مخططات المصرفية على الأنترنت المجرمين جمع المعلومات الشخصية السرية بـ " إنتحال موقع ويب صحيح ، إنشاء مواقع ويب الخادعة، حتى يروج المشروعية للإحتيال في غرفة دردشة" عندما يحصل مجرم على معلومات الحساب المصرفي ، التحولات غير المشروعة من المال، على سبيل المثال، يمكن أن يحدث في صفقة واحدة سريعة(nw3c()).

إنكشاف البنية التحتية المعلوماتية الكونية: تتفاوت البنى التحتية المعلوماتية بدرجة إنكشافها إلى الكوارث الطبيعية، و الإهمال البشري، و سوء التصرف الإنساني، حدد التقرير الرئاسي بخصوص حماية البنية التحتية الحساسة (PCCIP,1997) خمسة قطاعات بناءا على الخصائص المشتركة لها، و هذه القطاعات هي:

[1] https://www.nw3c.org/ اطلع عليه بتاريخ 05/04/2020 على الساعة 09:10

1- قطاع الإتصالات و المعلومات: information and) communication: و تشمل شبكات الإتصالات العامة(PIN)، و الأنترنت، و الحاسبات في المنازل، و الإستخدام الأكاديمي ، و الحكومي ، و التجاري .

2- قطاع التوزيع المادي(الفيزيقي)(phisical distribution)، و يشمل الطرق السريعة للمواصلات، و خطوط السكك الحديدية، و الموانئ، و خطوط المياه، و المطارات، و شركات النقل، و خدمات الشحن التي تسهل إنتقال الأفراد و البضائع.

3- قطاع الطاقة (energy): و تشمل الصناعات التي تنتج الطاقة، و توزع الطاقة الكهربائية، و البترول، و الغاز الطبيعي

4- قطاع المال و البنوك: (banking and finance)، و تشمل البنوك، و شركات الخدمات المالية من غير البنوك، و نظم الرواتب، و شركات الإستثمار، و القروض المتبادلة، و التبادلات الأمنية و المادية.

5- قطاع الخدمات الإنسانية الحيوية: (vital human dervices)، و تشمل نظم التزويد بالمياه ، و خدمات الطوارئ و الخدمات الحكومية(البطالة، الضمان الإجتماعي، و تحوي الإعاقات، و إدارة سجلات المواليد، ..... الخ)

من الصعب ربط التهديدات الإلكترونية بمكان أو زمان أو جماعة ، فقد تصدر من هاو أو من طفل أو محترف أو جماعة إرهابية أو جماعة تنافسية أو إستخبارات أجنبية و لقد حددت وكالة مشاريع البحوث الدفاعية المتقدمة (DARPA) مهددت البناء المعلوماتي في (5) فئات.

1-التهديدات الخارجية المحايدة (external positive attack) [التنصت، و تحليل الإشارات، و تحليل الذروة].

2-التهديدات الخارجية النشطة (external active attack)) [مثل الدخول، و الحمولة الزائدة ، و الإزدحام]

3-الهجوم على نظام عام(running system attack)

4-الهجوم الداخلي(internal attack)

5-الهجمات للوصول إلى تعديل النظام [إختراق حماية الدخول للنظم ، الإكتشاف](موثق في البداينة 2002)(DARPA, 1997, appendixC).

أسباب تتعلق بخصائص الجريمة الإلكترونية:

فيما يلي مجموعة من خصائص الجرائم الإلكترونية و التي تؤدي إلى ارتكاب الجريمة الإلكترونية منها:

1-**الإزالة(Removable)**: الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط

2-**التوافر(Available)**: المعلومات في كل مكان ، جاهزة لتستهدف من الجريمة

3-**القيمة(valuable)**: معلومات بطاقة الإئتمان و الحسابات المصرفية و التصاميم... قيمة

4-**المتعة(enjoyable)**: كثير من الجرائم الإلكترونية ممتعة مثل سرقة الموسيقى و المال.

5-**الديمومة(durable)**: المعدات و البرامج المسروقة يمكن أن تستخدم لفترة طويلة[1].

6-**سرعة التنفيذ** : لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر، و هذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو إستخدام معدات و برامج معينة.

7-**التنفيذ عن بعد:** لا تتطلب الجريمة الإلكترونية في أغلبها (إلا جرائم سرقة معدات الحاسب) وجود الفاعل في مكان الجريمة، بل يمكن الفاعل تنفيذ جريمته و هو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول

[1] محمد لمين دباغين سطيف 2 الجزائر. كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، ص 95

للشبكة المعنية أو إعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب ... إلخ.

8-**إخفاء الجريمة:** إن الجرائم التي تقع على الحاسبات الآلية أو بواسطتها (كجرائم الأنترنت) جرائم مخيفة ، إلا أنه يلاحظ آثارها و التخمين بوقوعها.

9-**الجاذبية** : نظرا لما تمثله سوق المعلومات و الحاسب و الأنترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم ، فقد عدت أكثر جذبا لإستثمار الأموال و غسيلها و توظيف الكثير منها في تطوير تقنيات و أساليب تمكن الدخول إلى الشبكات و سرقة المعلومات و بيعها أو سرقة البنوك أو إعتراض العمليات المالية و تحويل مسارها أو إستخدام أرقام البطاقات .... الخ.

10-**عبرة للحدود الدولية: (tranndnational)** : إن ربط العالم بشبكة من اتصالات من خلال الأقمار الصناعية و الفضائية و الأنترنت جعل الإنتشار الثقافي و عولمة الثقافة و الجريمة أمرا ممكنا و شائعا ، لا يعترف بالحدود الإقليمية للدول، و لا بالمكان، و لا بالزمان، أصبحت ساحتها العالم أجمع (البداينة ، 1997 "ج") ، (البداينة ، 1999 "د").

11-**جرائم ناعمة:** تتطلب الجريمة التقليدية إستخدام الأدوات و العنف أحيانا كما في جرائم الإرهاب و المخدرات،[1] و السرقة و السطو المسلح، إلا أن الجريمة الإلكترونية تمتاز بأنها جرائم ناعمة لا تتطلب عنفا ، فنقل بيانات من حاسب إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن(سليم، 1998).

12-**صعوبة إثباتها:** تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات، و هذ راجع إلى افتقاد وجود الآثار التقليدية للجريمة، و غياب الدليل الفيزيقي(بصمات ، تخريب، شواهد مادية) و سهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة و النظام العدلي ، و عدم كفاية القوانين القائمة (البحر، 1999).

[1] غادة نصار، الارهاب والجريمة الالكترونية، ط 1، العربي للنشر والتوزيع، د ب ن، 2017، ص163.

تصنيف مرتكبوا الجرائم الإلكترونية:

- **المثاليين(indealists) (المراهقين)** : عادة ما يكونون غير مدربين أو مهرة، و هم الشباب الذين تتراوح أعمارهم من 13 إلى 26 سنة و الذين يسعون إلى الإعتراف الإجتماعي، و هم يريدون أن يكونون في بؤرة الضوء في وسائل الإعلام، و تمتاز أفعالهم بأنها تسبب الخراب عالميا و لكنها لا تذكر على المستوى الفردي، من " مثل الحرمان الكثير من خوادم هامة في التجارة الدولية في شهر فبراير عام 2000 و التي سببت أضرار عالية لهذه الشركة" و في معظم الأحيان يهاجم المثاليون أنظمة المعلومات بفيروسات طوروها ، و ضررهم الفعلي على كل فرد لا يكاد يذكر، و عادة ما يتوقفون في سن 22-26 عندما ينضجون و يفهمون نتائج أعمالهم.
- **الجشع – المدفوع(greed-motivated) (المجرمون المهنيون):** و هذا النوع من مجرمي الأنترنت خطير ، و هذه الفئة عادة ما تكون عديمة الضمير و هم على إستعداد لإرتكاب أي نوع من الجرائم، طالما أنها تجلب لهم المال، حيث " بدأوا في إنتاج المواد الإباحية و غالبا ما تسمى السيبرانية للمواد الإباحية و التي تشمل الإباحية القانونية و غير القانونية على شبكة الأنترنت" أنهم عادة ما يكونوا أذكياء جدا و منظمون و يعرفون كيفية الهروب من وكالات إنفاذ القانون ، و مجرموا الأنترنت هؤلاء يرتكبون الجرائم الخطيرة ، و خاصة في جرائم إباحية الأطفال و الأقمار الإلكترونية و هذه تشكل تهديدا خطيرا للمجتمع.[1]
- **الإفتراضي –** الإرهابي (the cyber-terrorists): هم مجموعة الاحداث و الأكثر خطورة ، و الدافع الأساسي لهم ليس المال فقط و لكن أيضا لديهم قضية ما و التي يدافعون عنها، و عادة ما ينغمسون في إرسال رسائل التهديد و تدمير

[1] ذياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، ورقة علمية بعنوان الجرائم الالكترونية: المفهوم والاسباب، الملتقى العلمي في الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، خلال الفترة من 02 الى 0 سبتمبر 201، الاردن، ص95.

البيانات المخزنة في الغالب في نظم المعلومات الحكومية لمجرد أن يسجلوا وجهة نظهرهم ، و يمكن مقارنة تهديد الإرهاب الإلكتروني بتهديدات السلاح النووي، و البكتربولجيا أو الكيميائية، هذه المسالة المثبطة للهمم هي أنهم لا يعملون داخل حدود الدولة ، بل يمكن أن يعملوا من أي مكان في العالم ، و هذا يجعل من الصعب إقتناصهم(chizoba, 2005) .

ففي مجال الإرهاب أظهرت دراسة سالم وريد وشين (salem, reid, and chen, 2008) و التي درسوا فيها محتوى فيديوهات للجماعات المتطرفة الإرهابية بإستخدام تحليل المحتوى و أدوات الترميز في الوسائط المتعددة و تحليل أنماط الفيديوهات و طريقة العمل (modus operandi) و خصائص المنتج الذي قاد إلى دعم هذه الجماعات المتطرفة، أظهرت الدراسة أن هذه الفيديوهات قد مررت رسائل قوية و كافية لتعبئة الأفراد(mobilize) و المتعاطفين و حتى لتنفيذ هجمات مثل التي يحويها الفيديو و نشرها عالميا من خلال النت ، وهذه الفيديوهات مهمة للجماعات الجهادية في مجالات التعليم و التدريب و التجنيد ، بالإضافة إن جمع هذه الفيديوهات و تحليلها مفيد لصناع القرار و محللي الإستخبارات ، و الباحثين في فهم أفضل حملات الإرهاب للجماعات المتطرفة و طرق عملها ، كما أنها تساعد في إستراتيجيات مكافحة الإرهاب في تدريب تكتيكات للجيش ، و يظهر الجدول التالي تحليل لهذه الفيديوهات.[1]

لقد كان متوسط مدة الفيديو في ال 60 فيديو جهادي 6:32 دقيقة أظهر التحليل وجود نوعين من الفيديوهات : الفيديوهات العنيفة و تتضمن الفيديوهات الوثائقية ، و الهجمات الإنتحارية، و قطع الرأس و الإختطاف، التي تستخدم لدعم الحرب النفسية للجهاديين و إستراتيجيات التعبئة، و الفيديوهات الأخرى و تتضمن الجزية ، و الفدية، و الرسائل ، و الدعاية، و النشرات الإخبارية، و محتويات خاصة من مثل اسماء المجموعات و عمل المجموعات (مثل التكتيكات و المستهدفين و الأسلحة) و التي تمكن الجماعات المتطرفة من : (أ) تعميم إفتعالهم

[1] ملحق رقم 01 جدول فيديوهات الشبكة المظلمة

إلى مجموعة متنوعة من الداعمين و المتعاطفين و جماعات الإعلام و الأعداء (ب) إدعاء تحمل المسؤولية، (ج) نشر رسائلهم عالميا للحصول على الشرعية لأعمالهم.

أهم طرق الجريمة الإلكترونية:

و تشمل و ليس حصرا في :

1-**تخريب المعلومات و إساءة إستخدامها:** و يشمل ذلك قواعد المعلومات ، المكتبات ، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية، الخ.

2-**سرقة المعلومات:** و يشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني، أو الصناعي ، أو العسكري، أو تخريبها، و تدميرها، الخ.

3-**تزوير المعلومات:** و يشمل الدخول لقواعد في النظام التعليمي و تغيير المعلومات و تحريفها ، مثل تغيير علامات الطلاب.

4-**تزييف المعلومات** : و تشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي و إصدارها.

5-**إنتهاك الخصوصية** : و يشمل نشر معلومات ذات طبيعة خاصة من الأفراد أو الدخول لحسابات الأفراد الإلكترونية و نشر معلومات عنهم ، أو وضع معلومات تخص الأفراد و نشرها.[1]

6-**التصنت:** و تشمل الدخول لقواعد المعلومات و سرقة المحادثات عبر الهاتف

7-**التجسس:** و يشمل إعتراض المعلومات و محاولة معرفة ما يقوم به الأفراد

8-**التشهير:** و يشمل إستخدام المعلومات الخاصة أو ذات الصلة بالإنحراف أو الجريمة و نشرها بشكل القصد منه إغتيال شخصية الأفراد أو الإساءة[1]

[1] إبراهيم رمضان إبراهيم عطايا ، الجريمة الإلكترونية وسبل مواجهتها فـــي الشريعة الإسلامية والأنظمة الدولية كلية الشريعة و القانون بطنطا، الاردن، 2014، ص32.

9-**السرقة العلمية:** الكتب و البحوث العلمية الأكاديمية و خاصة ذات الطبيعة التجريبية و التطبيقية.

10-سرقة الإختراعات: و خاصة في المجالات العلمية لإستخدامها أو بيعها

11-الدخول غير القانوني: للشبكات بقصد إساءة الإستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات

12-قرصنة البرمجيات: و يشمل النسخ غير القانوني للبرمجيات و إستخدامها أو بيعها مرة أخرى

13-**قرصنة البيانات و المعلومات :** و تشمل إعتراض البيانات و خطفها بقصد الإستفادة منها و خاصة أرقام البطاقة الإئتمانية و أرقام الحسابات و كلمات الدخول و كلمات السر.

14-**خلاعة الأطفال:** و تشمل نشر صور خاصة للأطفال " الجنس السياحي" للأطفال خاصة ، و للإناث بشكل عام، و نشر الجنس التخيلي(CYBER SIX) على الشبكات

15-القنابل البريدية: و تشمل إرسال فيروسات لتدمير البيانات من خلال رسالة مقومة إلكترونية

16-إفشاء الأسرار: و تشمل الحصول على معلومات خاصة جدا و نشرها على الشبكة.

17-الإحتيال المالي: بالبطاقات و هذا ناتج عن إستخدام غير شرعي لبطاقات التسويق أو المالية أو الهاتف .... الخ.

18-سرقة الأرقام و المتاجرة: بها و خاصة أرقام الهواتف السرية و إستخدامها في الإتصالات الدولية أو أرقام بطاقات الإئتمان

19-**التحرش الجنسي :** و يقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة، أو الملامسة.

---

[1] ابراهيم رمضان ابراهيم عطايا، المرجع السابق ذكره، ص33.

20- **المطاردة و الملاحقة و الإبتزاز:** و تشمل ملاحقة الذكور للإناث أو العكس و التتبع بقصد فرض إقامة علاقة ما ، و ذلك من خلال إستخدام البريد الإلكتروني و إرسال الرسائل.

الإرهاب الإلكتروني: يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة و التي تؤثر على فرص الإرهاب و مصادرة هذه التغيرات تؤثر على تكتيكات الإرهاب و أسلحته و أهدافه و من التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني

اهداف الجريمة الالكترونية:

نستطيع تلخيص بعض أهداف الجرائم الإلكترونية ببضعة نقاط أهمها:

1- التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.

2- التمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات و تعطيلها.

3- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات و البنوك و الجهات الحكومية و الأفراد و إبتزازهم بواسطتها.

4- الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات إختراق و هدم الموقع على الشبكة العنكبوتية و تزوير بطاقات الإئتمان و سرقة الحسابات المصرفية .... الخ.[1]

[1] رفد عيادة الهاشمي، الارهاب الالكتروني القانوني، دار أمجد للنشر والتوزيع، العراق، 2020، ص140.

المبحث الثاني : الإطار القانوني للجريمة الإلكترونية.

استقر الفكر القانوني على ضرورة إيجاد نصوص خاصة لحماية المال المعلوماتي؛ وقد استجابت عدة دول لهذه الحاجة بسنها قوانين تناولت في طياتها تعريف الجريمة المعلوماتية وأنواعها وخصائصها وأركانها والعقوبات المقررة لها. وتُعتبر الولايات المتحدة الأمريكية أول الدول التي سنت قوانين خاصة بالجريمة المعلوماتية من أجل حماية المعلوماتية وتليها بعد ذلك الكثير من الدول منها كندا وألمانيا وأستراليا.

أما بالنسبة للمشرع الجزائري فقد تدارك مؤخرا الفراغ القانوني في مجال الجريمة المعلوماتية وذلك باستحداث نصوص تجريمية خاصة لقمع الاعتداءات الواردة على المعلوماتية بموجب تعديل قانون العقوبات الذي تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 66-156 بإضافة القسم السابع المكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" من المادة 394 مكرر إلى 394 مكرر 7 من قانون العقوبات؛ وكذا القانون رقم 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته. أما على المستوى الدولي فنجد أول اتفاقية حول الإجرام المعلوماتي كان بتاريخ 08-11-2011 التي تضمن مختلف أشكال الإجرام المعلوماتي.[20] أما المشرع الفرنسي فقد تناولها في المواد 323-1 إلى 323-7 من قانون العقوبات الفرنسي.

نجد أن المشرع الجزائري اتخذ هذه الإجراءات اللازمة من أجل مقاومة الجريمة المعلوماتية المنصوص عليها في الاتفاقية الأورومتوسطة المؤرخة في 22 أفريل 2002، التي كانت تهدف إلى ربط الجهود بين الوحدة الأوربية والدول الأعضاء فيها ومابين الحكومة الجزائرية من جهة أخرى. وقد صادقت الجزائر مع الدولة الفرنسية في مجال الأمن ومكافحة الإجرام المنظم وذلك بتاريخ 25 أكتوبر 2003 ودخلت حيز التنفيذ بموجب المرسوم الرئاسي رقم 07-375

المطلب الأول: أركان الجريمة المعلوماتية:

إن الجريمة المعلوماتية ليست واحدة، إنما تتخذ عدة أشكال مما يقتضي دراسة أركانها بالتفصيل ، و هذا من خلال المطلبين التاليين:

الركن المفترض (نظام المعالجة الآلية للمعطيات) في المطلب الأول

الأركان الأساسية في المطلب الثاني

الركن المفترض

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

و يؤدي توافر هذا الشرط إلى الإنتقال للمرحلة التالية، إذ أن هذا الشرط يعتبر عنصرا لازما، و لذلك يكون من الضروري تعريف نظام المعالجة الآلية للمعطيات و مدى خضوع هذا النظام لحماية فنية.

الفرع الأول: تعريف نظام المعالجة الآلية للمعطيات :

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

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

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

[1] أمال قارة، المرجع السابق، ص 102.

أما الفقه الفرنسي فقد عرفه من خلال الأعمال التحضيرية للمادة 323-1 قانون العقوبات الفرنسي، الذي تبنى التعريف الوارد في القانون الفرنسي، الذي تبنى التعريف الوارد في القانون الخاص بالمعلوماتية و حماية الحريات لسنة 1978، بأنه كل مركب من وحدة أو مجموعة وحدات للمعالجة ، و التي تتكون كل منها من الذاكرة و البرامج و المعطيات و أجهزة الإدخال و الإخراج، و أجهزة الربط التي تربط بين العناصر المختلفة للنظام، كالشاشة و لوحة المفاتيح و الطابعة و البطاقات المغناطيسية التي تشكل وسيلة للدخول، و التي تربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة، و هي معالجة المعطيات، على أن يكون هذا المركب خاضع لنظام الحماية الفنية" [1]

و هذه العناصر المادية و المعنوية التي تكون منها المركب، واردة على سبيل المثال لا الحصر، فيمكن إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال، فإذا تم الإعتداء على أحد هذه العناصر بمعزل عن النظام، فلا تقوم الجريمة ، فلا بد من الإتصال بينها.

و يكون نظام المعالجة الآلية للمعطيات في طور التشغيل عند إرسال إشارة كهربائية نحو وحدة المعالجة المركزية، و التي تقوم بدورها بإرسال البرنامج المسؤول عن تشغيل ذاكرة القراءة، هذه الأخيرة تقوم بالبحث عن المعطيات التي تسمح بتشغيل النظام المسؤول عن البحث، ثم تقوم بتسجيلها في ذاكرة القراءة و الكتابة التي تقوم بمتابعة المراحل اللاحقة[2]

الفرع الثاني: الحماية الفنية لأنظمة المعالجة الآلية للمعطيات:

تكفل بعض القواعد الأمنية لنظم المعالجة الآلية للمعطيات، كوضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من الأجهزة المختلفة، و التي يمكن عن طريقها معرفة محتوى المعلومات التي يتم نقلها ، و يتأتى ذلك عن طريق حماية الكابلات و الوصلات الكهربائية لإرتباطها بالأجهزة، و من بين هذه القواعد، أسلوب يعتمد على

[1] نائلة عادل، المرجع السابق، ص 331.

[2] المرجع نفسه ، ص 331.

توزيع العمليات التي يقوم بها نظام المعالجة الآلية للمعطيات و نقلها إلى نظام إحتياطي (مركز للمساعدة) عند الضرورة ، و يلجأ إلى هذا الأسلوب عادة البنوك و شركات التأمين، و يظل هذا الموقع سرا و يخضع لدرجة عالية من الحماية، و من الأساليب المستعملة كذلك، الإعتماد على الإختبارات الفيزيولوجية للدخول إلى النظام عن طريق التحقق من شخصية القائم بعملية الدخول عن طريق بصمة الأصبع أو نبرة الصوت أو شكل الأذن أو شبكية العين[1].

لكن يبقى نظام التشفير لحماية المعلومات هو الأسلوب الواسع الإنتشار، خاصة البيانات المتناقلة عبر الشبكات، كشبكات الإنترنت، لما تنطوي عليه من سرية البيانات الشخصية كالرسائل الإلكترونية الخاصة بالأعمال التجارية الرقمية[2].

و يقوم نظام التشفير على تحويل المعلومات و البيانات إلى شكل رمزي غير مفهوم بدون مفتاح لحل رموزه ، يعرفه عادة مرسل المعلومات و المرسل إليه، و في داخل جهاز الكمبيوتر توجد أجهزة مهمتها التحقق من شخصية القائم بعملية الدخول عن طريق الشفرة.

و قد ثار التساؤل حول ضرورة وجود أو عدم حماية النظام كشرط للتمتع بالحماية الجنائية؟

فبالرجوع إلى نص المادة 394 [3]مكرر1 من قانون العقوبات، لا نجد إشارة إلى ضرورة خضوع النظام للحماية الفنية حتى يتمتع بالحماية الجنائية، و كذلك الشأن بالنسبة للمادة 323-1 من قانون العقوبات الفرنسي، و يظهر من خلال الأعمال التحضيرية لقانون 1988، المتعلق بالمعلوماتية و المقتبسة منه المادة 323-1، أنه من المقترح ضرورة شمول النص بهذا الشرط، و لكن إشترط وجود حماية أمنية في نظام المعالجة الآلية للمعلومات لم يتم الإتفاق عليه في المناقشات الأخيرة في البرلمان

[1] نائلة عادل، المرجع السابق، 353

[2] أمال قارة، المرجع السابق، ص 103.

[3] **تنص المادة 394 مكرر من قانون العقوبات:" يعاقب بالحبس و الغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات"**

الفرنسي، و لذلك جاء النص خاليا من هذا الشرط، ووجد أن هذا الشرط قد يؤدي إلى الحد من الحماية الجنائية للنظم غير المشمولة بتجهيزات أمنية داخل النظام.

و لذلك إكتفى المشرع الفرنسي في النص النهائي بأن يكون التوصل قد تم بطريق الغش، و هذا يترك تفسيره لقاضي الموضوع[1].

و هذا ما فتح أبواب النقاش حول هذه النقطة من خلال ظهور رأيين مختلفين:

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

و يقيس أنصار هذا الرأي جريمة الدخول غير المشروع في أنظمة المعالجة الآلية للمعطيات على جريمة إنتهاك حرمة المنزل، حيث لا تقوم الجريمة لمجرد أن الدخول إلى المسكن قد تم بغير رضاء صاحبه، كترك مسكنه دون حماية بسبب عدم وجود أقفال أو أبواب أو نوافذ، فيجب أن يكون الدخول مصحوبا بإستعمال وسائل تدل على عدم رضا صاحب المسكن.

و يستند أنصار هذا الرأي إلى عدة أسباب تنصب جميعها في إتجاه واحد هو ضرورة أن يكون هناك نظم أمنية يتم إختراقها لإمتداد الحماية الجزائية للمعلومات، و أول هذه الأسباب يتعلق بالمادة 28 من القانون 78-17 لسنة 1978 الخاص بالمعلوماتية و حماية الحريات الفرنسية، حيث تتطلب أن تكون الأنظمة مشمولة بتدابير لحمايتها، و السبب الثاني يكمن في إقامة الدليل على قيام الركن المادي للجريمة و كذا التحقق من توافر القصد الجنائي لدى مرتكبها، لأن إختراق الأنظمة الأمنية من طرف الفاعل يترك أثرا، و يؤكد طريق الغش و الإحتيال الذي سلكه.

الرأي الثاني: فهو يذهب إلى أنه ينبغي حماية أنظمة المعالجة الآلية للمعطيات جزائيا بغض النظر إن كانت تتمتع بحماية النظم الأمنية من عدمه ، و يقيس أنصار هذا الإتجاه جريمة الدخول غير المشروع على جريمة السرقة، حيث أن تمتع المال المسروق بحماية صاحبه أو عدم تمتعه بهذه الحماية لا يؤثر في قيام جريمة السرقة، بغض

[1].صلاح سالم، تكنولوجيا المعلومات و الإتصالات و الأمن القومي للمجتمع، الطبعة الأولى، 2003، ص117

النظر عن مقدار الصعوبة التي واجهت الجاني في تنفيذها، كما أن تطلب مثل هذا الشرط يضيق من تطبيق الحماية الجزائية ، و يتجاهل الحالات التي يتم فيها الدخول إلى النظام نتيجة خطأ قام به المبرمجون، أو المسؤولون عن أمن النظام[1].

هذا الرأي هو الأقرب إلى الصواب إستنادا إلى المبادئ العامة المستقرة في القانون الجنائي كحرفية النص، و عدم جواز تقييد النص المطلق أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك، و لا يوجد في حالتنا نص خاص يقيد إطلاق النص أو يخصص عمومه، و بالتالي يجب إلتزام حرفية النص في التفسير، فعدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع أراد إستبعاده.[2]

و أكدت محكمة إستئناف باريس في حكم صادر لها في 1994/04/05، على أنه من غير الضروري لقيم جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية، و أنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسؤول عن النظام.

المطلب الثاني: الأركان الأساسية للجريمة المعلوماتية:

متى ثبت توفر الشرط الأولي لقيام الجريمة المعلوماتية ألا و هو نظام المعالجة الآلية للمعطيات أمكن الإنتقال إلى المرحلة التالية و هي البحث في توافر أركان أية جريمة من جرائم المعلوماتية.

الفرع الأول: الركن المادي:

يتمثل الركن المادي في أشكال الإعتداء على نظم المعالجة الآلية للمعطيات، و هناك ثلاثة أشكال للإعتداء نذكرها فيما يأتي:

أولا: الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

[1] نائلة عادل، المرجع السابق، 355

[2] أمال قارة، المرجع السابق، ص 105

نصت عليه المادة الثانية من الإتفاقية الدولية للإجرام المعلوماتي بالإضافة للمادة 394 مكرر من قانون العقوبات بقولها: يعاقب بالحبس من ثلاثة أشهر إلى سنة بغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ، تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50.000 دج إلى 150.000 دج.

و عليه فإن هذا الشكل من الإعتداء على نظام المعالجة الآلية للمعطيات يتكون من صورة بسيطة للجريمة و أخرى مشددة.

فأما الصورة البسيطة تقوم بمجرد الدخول أو البقاء غير المشروع و يقصد بفعل الدخول ظاهرة معنوية تشابه تلك التي تعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات و بالتالي لا نقصد بالدخول بمفهومه المادي[1].

و تجدر الملاحظة أن المشرع لم يحدد وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام ، و منه تقع الجريمة بأية وسيلة أو طريقة تمت بها الدخول، فيستوجب أن يتم الدخول مباشرة أو عن طريق غير مباشر[2].

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

في حين أنه يقصد بفعل البقاء[3] التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.

---

[1] علي عبد القادر القهوجي، الجماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة و النشر ، مصر ، 1999 ، ص 120.

[2] علي عبد القادر القهوجي، المرجع نفسه ، ص 121

[3] علي القهوجي، المرجع نفسه ، ص 133.

و تجدر الإشارة إلى أنه قد يتحقق البقاء عليه داخل النظام مستقلا عن الدخول إلى النظام، و قد يجتمعان، و يكون البقاء معاقبا عليه وحده حين يكون الدخول إلى النظام مشروعا.

و قد يجتمع الدخول غير المشروع و البقاء غير المشروع معا ، في الحالة التي لا يكون فيها للجاني الحق في الدخول إلى النظام ، و يدخل إليه رغم ذلك ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، و يتحقق الإجتماع المادي للجريمتين الدخول و البقاء غير المشروعين.[1]

إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة ، فإنها تحقق أيضا، و بصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها أما الصورة المشددة تتحقق بتوافر الظرف المشددة المتمثلة في حصول نتيجة الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب إشتغال المنظومة

و قد نصت المادة 394 مكرر 2 و3 من قانون العقوبات على أن:" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة، إذا ترتب الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50.000 دج إلى 150.000دج"

و عليه نستنتج من خلال ذلك أن هناك ظرفين تشدد بهما عقوبة جريمة الدخول و القاء داخل النظام، و تربط بين هذين الظرفين علاقة سببية بين الدخول عير المشروع أو البقاء غير المشروع و النتيجة الضارة و إن لم تكن مقصودة

و منه فظرف التشديد يعتبر ظرف مادي يكفي أن توجد بينه و بين الجريمة الأساسية المتمثلة في الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافرها. إلا إذا أثبت الجاني إنتقاء تلك العلاقة و يثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ[2]

[1] أمال قارة، المرجع السابق، ص 110.

[2] أمال قارة، المرجع نفسه ، ص 110.

ثانيا: الإعتداء العمدي على سير نظام المعالجة الالية للمعطيات

نصت على هذا الشكل من الإعتداء المادتين الخامسة و الثامنة من الاتفاقية الدولية للإجرام المعلوماتي، في حين أن المشرع الجزائري لم يورد نصا خاصا بالإعتداء العمدي على سير النظام و إكتفى بالنص على الإعتداء على المعطيات الموجودة بداخل النظام، و يمكن رد ذلك لكون أن المشرع الجزائري قد إعتبر من خلال الفقرة ج من المادة الثانية[1] من القانون 04/09 على أن برامج سير نظام المعالجة الآلية للمتدخل ضمن المعطيات المعلوماتية.

و قد وضع الفقه معيارا للتفرقة بين الإعتداء على المعطيات و الإعتداء على النظام على أساس ما إذا كان الإعتداء مجرد وسيلة فإن الفعل يشكل جريمة الإعتداء العمدي على النظام، أما إذا كان الإعتداء وسيلة أم غاية، فإذا كان الإعتداء غاية فإن الفعل يشكل جريمة الإعتداء العمدي على المعطيات.

و تشمل صورة الإعتداء العمدي على سير النظام فعلين يتمثلان في الآتي:

يتمثل الأول منها في فعل التعطيل(العرقلة) و الذي يفترض وجود عمل إيجابي ، مع العلم أن المشرع لم يشترط أن يتم التعطيل بوسيلة معينة فيستوجب أن يتم التعطيل بوسيلة مادية ككسر الأجهزة المادية للنظام أو تحطيم اسطوانة أو عن طريق وسيلة معنوية تتم بموجب الإعتداء على الكيانات المنطقية للنظام كالبرامج و المعطيات و ذلك بإتباع إحدى التقنيات المستعملة في هذا المجال مثل إدخال برنامج فيروسي، إستخدام قنابل منطقية مؤقتة، جعل النظام يتباطأ في أدائه لوظائفه كما يستوجب أن يقترن التعطيل بالعنف أم لا.

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

أما الفعل الثاني يتمثل في الإفساد الذي يتم بكل فعل إلى تعطيل نظام المعالجة الآلية للمعطيات يؤدي إلى جعله غير صالح للإستعمال السليم و ذلك من شأنه أن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[1].

ثالثا: الإعتداءات العمدية على المعطيات:

نصت عليها المواد 03، 04، 08 من الإتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع الجزائري في المادة 394 مكرر 1 و 394 مكرر 2 من قانون العقوبات مجرم المادة الأولى الإعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، و جرم في المادة الثانية المساس بالمعطيات الموجودة بالنظام ، و يظهر فيما يلي:

أ- جرائم الإعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي:

بإستقرار المادة 394 مكرر 1 [2]نجد أن لهذه الجريمة صورتين تتمثل الأولى في الإعتداءات العمدية على المعطيات الموجودة داخل النظام أما الصورة الثانية تتمثل في المساس العمدي على الموجودات خارج النظام نجد أن الإعتداءات العمدية على المعطيات الموجودة داخل النظام في إحدى الأفعال الثلاثة: الإدخال(l'intrusion)، المحو(l'effacement)، التعديل(modification) و يقصد بها:

الإدخال l'intrusion: يقصد بهذا الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل و يتحقق هذا الفعل في القرص الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي و ذلك حين إستخدام رقمه الخاص و السري لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه و من ذلك

[1] عبد القادر القهوجي، المرجع السابق ص، 143.

[2] تنص **المادة 394 مكرر 1 من قانون العقوبات:" يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات و بغرامة 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"**

الحامل الشرعي لبطاقة الإئتمان و التي يسدد عن طريقها مبلغا (التاجر أو شخص يتعامل معه) أكثر من المبلغ المحدد له.

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

المحوl'effacement: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة و الموجودة داخل النظام ، أو تحطيم تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[1].

التعديلmodification: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام و إستبدالها بمعطيات أخرى، و يتحقق فعل المحو و التعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم تعديلها و ذلك بإستخدام القنبلة المعلوماتية الخاصة بالمعطيات و برامج الممحاةgomme d'effacement أو برامج الفيروسات بصفة عامة و هذه الأفعال المتمثلة في الإدخال و المحو و التعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى و لو تضمن إعتداء المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لكن تلك الأفعال لا تنطوي لا على إدخال و لا على تعديل بالمعنى السابق،

مع الملاحظ أن المشرع لم يشترط إجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يقوم الركن المادي.

كما أن أفعال الإدخال و المحو و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل.[2]

[1] علي عبد القادر القهوجي، المرجع السابق، ص 144.

[2] أمال قارة ، المرجع السابق، ص 120.

ب- أما صورة المساس العمدي بالمعطيات: نص عليها المشرع الجزائري بموجب أحكام المادة 394 مكرر 2 من قانون العقوبات[1]، و كرس بموجبها المشرع الحماية الجزائية للمعطيات في حد ذاتها لأنه يشترط أن تكون خارج النظام المعلومات داخل النظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا.

إذ نصت الفقرة الأولى من المادة 394 مكرر 2 أن محل الجريمة يتمثل في المعطيات سواء كانت مخزنة في أشرطة أو اقراص أو معالجة آليا أو مرسلة عن طريق منظومة معلوماتية ، ما دامت قد تستعمل كوسيلة لإرتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

في حين أن الفقرة الثانية من المادة 394 مكرر 2 جرمت أفعال الحيازة ، الإفشاء، النشر، الإستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات فقد يكون الهدف من ذلك المنافسة غير المشروعة، الجوسسة ، الإرهاب ، أو التحريض على الفسق، .... الخ.

الفرع الثاني: الركن المعنوي:

إن الركن المعنوي في الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات تتخذ صورة القصد الجنائي

أولا: الركن المعنوي بالنسبة للدخول و البقاء غير المشروع داخل نظام المعالجة الالية للمعطيات:

[1] تنص المادة 394 مكرر 2 من قانون العقوبات:" يعاقب بالحبس و بغرامة كل من يقوم عمدا و عن طريق الغش ما يلي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو مرسلة عن طريق منظومة معلوماتية يمكن أن رتتكب بها الجرائم المنصوص عليها في هذا القسم.

-حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

إن الركن المعنوي لجريمة الدخول و البقاء غير المشروعين، يتخذ صورة القصد الجنائي من علم و إرادة من الجرائم العمدية، و قد عبر نص المادة 394 مكرر 2 عن القصد الجنائي العام بتطلبه أن يكون الدخول أو البقاء" عن طريق الغش، فإستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله أو بقاءه في نظام المعالجة الآلية للمعطيات غير مشروع ، و هو نفس ما عبر عنه المشرع الفرنسي في نص المادة 323 -1 بعبارة " fraduleudemet".

يتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، و بناء أركانها، و إستكمال عناصرها، و خاصة الركن المادي منها، و أول هذه العناصر هو موضوع الحق المعتدى عليه، فيتعين توافر علم الجاني بأن فعله ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات و برامج، بإعتباره محل الحق الذي يحميه المشرع، فإذا إعتقد الفاعل بناء على أسباب معقولة بأنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي، دون أن يتجه علمه إلى أنه يقوم بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات، فإن قصد الدخول أو البقاء لا يتوفر فيه[1].

كذلك يتعين أن يعلم بخطورة الفعل الذي يقوم به، فإذا كان غير ذلك ينتفي القصد الجنائي، و يتطلب القصد الجنائي أيضا أن يتوقع الجاني النتيجة الإجرامية التي ستترتب عن القيام بفعله، فتوقع النتيجة هو أساس النفي الذي تقوم عليه إرادتها، فحيث لا يكون التوقع لا نتصور الإرادة، و النتيجة التي يجب أن يتجه إليها توقع الفاعل هي النتيجة التي يحددها القانون، و هي الدخول و البقاء غير المشروع لنظام المعالجة الآلية للمعطيات.

و لا يشترط أن يتوقع الضرر الذي سوف يلحق النظام أو صاحبه من جراء هذا الدخول[2]، فإذا توقع الفاعل أنه بصدد الدخول إلى نظام معين ، ثم ترتب على فعله الدخول إلى نظام آخر، فإن القصد الجنائي يظل متوافرا لديه.

[1] نائلة عادل محمد فريد قورة ، المرجع السابق، ص 365

[2] نائلة عادل محمد فريد قورة ، المرجع نفسه ، ص 366

و هناك وقائع يسأل فيها الجاني عن الجريمة دون أن يتطلب القانون علمه بها فحين يقرر القانون لبعض الجرائم عقابا معينا إذا أحدث الفعل نتيجة ذات جسامة معينة، و إذا إزدادت جسامة هذه النتيجة فأفضت إلى نتيجة جسامة شدد القانون العقاب، و يتطلب المشرع إنصراف القصد الجنائي إلى النتيجة الأقل جسامة، و لكنه لا يتطلب إنصرافه إلى النتيجة الأشد جسامة، بحيث يسأل الجاني عنها بالرغم من عدم توقعها لها[1].

و هذا ما ينطبق على الفقرة الثانية و الثالثة من المادة 394 مكرر من قانون العقوبات، حيث يعاقب الجاني على النتيجة الأشد بمجرد ترتبها عن الدخول أو البقاء غير المشروع الذي قصده.

و يجب أن يعلم مرتكب جريمة الدخول أو البقاء غير المشروعين داخل نظم المعالجة الآلية للمعطيات، أن دخوله إلى هذا النظم غير مشروع أو غير مصرح به، فلا يتوافر القصد الجنائي إذا وقع الجاني في خطأ ، كأن يجهل وجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول أو البقاء.

أما بالنسبة لإرادة الجاني فيجب أن تتجه إلى الدخول أو البقاء غير المشروعين داخل النظام، أي أن تتجه إرادته لتحقيق هذه النتيجة ، و لا عبرة بعد ذلك للباعث أو الغاية من وراء هذا الدخول سواء هذا الباعث هو الفضول، أو إثبات القدرة على المهارة و الإتصال على النظام ، حتى و إن كانت الغاية نبيلة كمن يدخل إلى النظام غير المصرح له بالدخول رغبة في الكشف عن أوجه القصور التي تعتري النظام الذي تمكن من الدخول إليه، و ذلك لتجنب هذا القصور مستقبلا[2].

ثانيا: الركن المعنوي للإعتداءات على سير نظام المعالجة الآلية للمعطيات و الإعتداءات على المعطيات خارج و داخل النظام:

إن الإعتداءات على سير نظام المعالجة الآلية للمعطيات بصورتيها التعطيل أو العرقلة، و إفساد النظام، لا تكون إلا عمدية هذا ما يميزها عن الإعتداء غير العمدي

[1] نفس المرجع، ص 367.

[2] نائلة عادل محمد فريد قورة ، المرجع نفسه ، ص 368

لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول و البقاء غير المشروعين داخل النظام[1].

و هذه الإعتداءات تتطلب القصد الجنائي العام من علم و إرادة ، شأنها شأن الإعتداءات العمدية على المعطيات، فيجب أن يعلم الفاعل بأنه يقوم بإحدى هذه الأعمال التي أوردها النص القانوني، و التي من شأنها إتلاف المعلومات فيعلم بأنه يقوم بفعل الإدخال أو المحو أو التعديل، و يعلم خطورة النشاط الإجرامي الذي يقوم به و ما يترتب عليه من عقاب

كما يجب أن تتجه إرادة الفاعل إلى فعل الإدخال أو المحو أو التعديل، فلا يسأل من قام بذلك خطا أو عن غير قصد، بل يسأل طبقا للمادة 394 مكرر 3/2 التي تتناول الصورة المشددة لجريمة الدخول أو البقاء غير المشروعين في نظام المعالجة الالية للمعطيات، كونها تعاقب الفاعل عن الحذف و التغيير المترتب عن الدخول أو البقاء غير المشروعين حتى و إن كان خطأ ، كون أن نص المادة 394 مكرر 1 من قانون العقوبات إشترط أن ترتكب هذه الأفعال " بطريق الغش".

و هي العبارة المستعملة كذلك في نص المادة 323-3 من قانون العقوبات الفرنسي " Frauduleusement"، أي أن يعلم أنه ليس له الحق في القيام بذلك، و أنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات دون موافقته، و لا يتطلب نص المادة 394 مكرر 1 قصدا جنائيا ، إذ لا يوجد فيه ما يشير إلى ذلك، عكس بعض التشريعات المقارنة التي إشترطت قصدا خاصا إلى جانب القصد العام، يتمثل في إتجاه نية المتهم إلى الإضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير، و هو ما كان عليه النص الفرنسي القديم قبل تعديله، و يبرز ذلك في عبارة " إرتكاب الفعل دون مراعاة حقوق الآخرين"، و قد إنتقدت هذه المادة قبل تعديلها بشدة لتطلبها القصد الجنائي الخاص ، كون أن إشتراط هذا القصد الخاص سوف يؤدي إلى اللاعقاب في

1 أمال قارة، المرجع السابق، ص 124.

الحالات التي لا تتجه فيها نية الفاعل إلى تحقيق ربح على الرغم من أهمية المعلومات التي يتم إتلافها كمعلومات علمية[1].

و هو ما دعا المشرع الفرنسي إلى إستبعاد القصد الخاص من هذه الإعتداءت العمدية، حيث إقتبس المشرع الجزائري نص المادة 394 مكرر 1 من نص المادة 323-3 المعدلة من قانون العقوبات الفرنسي.

أما بالنسبة للإعتداءات العمدية الماسة بالمعطيات الموجودة خارج النظام، فيجب لقيام الركن المعنوي أن يتوافر القصد الجنائي العام، و هو ما عبرت عنه المادة 294 مكرر 2 بعبارة "كل من يقوم عمدا و عن طريق الغش."

و بالتالي يجب توافر العلم و الإرادة لدى الجاني لقيام الركن المعنوي، فيجب أن يكون عالما أن المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، و ذلك بتصميمه أو بحثه أو تجميعه أو توفيره أو نشره أو الإتجار في هذه المعطيات، أي علمه بأن هذه المعطيات يمكن أن تكون وسيلة لإرتكاب الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

و يجب أن يعلم الجاني كذلك، أن إثباته أحد الأفعال السابقة ينصب على معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، كذلك أن يعلم بخطورة الفعل الذي يقوم به، و أن يتوقع النتيجة المترتبة عن القيام بأحد الأفعال السابقة.

المطلب الثالث: خصائص الجريمة الإلكترونية:

نظرا لإرتباط الجريمة الإلكترونية بجهاز الحاسوب، و شبكة الإنترنت بصفة عامة، ووسائل التواصل الإجتماعي بصفة خاصة، قد أضفى عليها ذلك مجموعة من الخصائص المميزة لها عن خصائص الجريمة التقليدية، و من هذه الخصائص ما يلي:

[1] نائلة عادل محمد فريد قورة ، المرجع السابق، ص 368

أولا: جريمة عابرة للحدود:

أعطى إنتشار شبكة الإنترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان و المكان، لذلك فإن من السهولة بمكان أن يكون المجرم في بلد ما و المجني عليه مقيم في بلد آخر، و هنا تظهر الحاجة لوجود تنظيم قانوني دولي و داخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم و ضبط فاعليها، و حيث إن التشريعات الداخلية متفاوتة فيما بين كل دولة من دول العالم، تظهر العديد من المشاكل حول صاحب الإختصاص القضائي لهذه الجريمة و إشكالات أخرى متعلقة بإجراءات الملاحقة القضائية ، و تتشابه الجرائم الإلكترونية في هذه الخاصية مع بعض الجرائم مثل غسيل الأموال، و جرائم المخدرات[1].

ثانيا: جريمة صعبة الإثبات و الإكتشاف:

تكمن صعوبة إثبات مثل هذه الجريمة أنها لا تترك في الغالب أثرا ماديا ظاهرا يمكن ضبطه ، فضلا عن التباعد الجغرافي الذي يثير الإشكال بداية، حيث تشير الدراسات أن ما يتم إكتشافه من جرائم المعلومات يصل إلى نسبة 1 % و الذي يتم الإبلاغ عنه من هذه النسبة لا يكاد يصل إلى 5 % فقط[2].

و الوسيلة المستخدمة لإرتكاب الجريمة هي نبضة إلكترونية ينتهي دورها خلال أقل من ثانية واحدة، و كان الجاني يقوم بتدمير الدليل بمجرد إستعماله و يقوم بذلك بكل هدوء و دون إحداث أية ضجة، و ذلك على خلال الكثير من الجرائم التي تعرف[3].

ثالثا: خصوصية مجرم المعلومات:

[1] القطاونة، مصعب (2010)، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن، ص 5

[2] القطاونة، مصعب، المرجع نفسه ، ص 6

[3] المطردي، مفتاح بوبكر، مرجع سابق، ص 8

قد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة، و لكن الأمر مختلف تماما بالنسبة للمجرم المعلوماتي و الذي يكون عادة من ذوي الإختصاص و المعرفة في مجال تقنية المعلومات.

و قد تم تصنيف مجرمي الجرائم الإلكترونية إلى المخترقين و المحترفين و الحاقدين.

أ- المخترقون: مثل الهاكرز الذي يعد شخصا بارعا في إستخدام الحاسب الالي و لديه فضول في إستخدام حسابات الآخرين بطرق غير مشروعة، الأمر الذي يدل على أنهم أشخاص متطفلون و غير مرحب بهم لدى الغير، و أغلبهم ما يكون جانبهم تحدي الشباب للدخول إلى المواقع الرسمية، و بعض الأحيان الدخول إلى مواقع الحسابات من أجل إثبات الذات ، و غالبا تكون أعمارهم في سن المراهقة[1].

ب- المحترفين: و هم الأكثر خطورة بين مجرمي الإنترنت، حيث يهدف البعض منهم إلى الإعتداء لتحقيق الكسب غير المشروع المتمثل في الناحية المادية و ذلك عبر الدخول في حسابات البنوك، و البعض الآخر يدخل من أجل تحقيق أغراض سياسية و التعبير عن وجهة نظره أو فكرة، و غالبا أعمال هؤلاء تكون بين 25 و 40 سنة [2].

ج- الحاقدون: و هم الذين ليس لديهم أي أهداف للجريمة و لا يسعون لمكاسب سياسية أو مادية و لكن يتحركون لرغبة في الإنتقام و التأثر كالأمور الطائفية[3].

رابعا: جريمة مغرية للمجرمين[4]:

نظرا للصفات التي تتمتع بها مثل هذه الجريمة، و الصعوبات التي تثور عند محاولة إكتشافها أو ملاحقتها، فإن ذلك يشكل إغراءً كبيرا للمجرمين و خصوصا أنه

[1] قورة، نائلة عادل (2012) ، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي الحقوقية، بيروت، ط1، ص178.

[2] إبراهيم ، خالد ممدوح (2009)، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، ص 78.

[3] إبراهيم ، خالد ممدوح ، المرجع نفسه، ص 79 .

[4] إبراهيم ، خالد ممدوح، المرجع نفسه، ص 30

يمكن تحقيق مكاسب طائلة من وراء مثل هذا النوع من الجرائم، و نتيجة لكل ما سبق تعد هذه الجرائم جريمة تستهوي الكثيرين لسهولتها، و كثرة مكاسبها.

خامسا: عدم وجود مفهوم مشترك للجريمة الإلكترونية:

لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن إستغلال تقنية المعلومات و إستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي، و البعض الآخر يطلق عليها جريمة الإختلاس المعلوماتي، أو الإحتيال المعلوماتي، و آخرون يفضلون تسميتها بالجريمة المعلوماتية[1].

و من وجهة نظر الباحث فإنه يفضل إصطلاح الجريمة الإلكترونية للدلالة على الجرائم المرتكبة بواسطة الحاسوب و الإنترنت، فإصطلاح الجريمة الإلكترونية عام و يشتمل وسائل الإتصال الإلكترونية الحالية و المستقبلية المستخدمة في التعامل مع البيانات و تبادلها.

كما أن التطور التكنولوجي نتج عنه تطور في طرق إثبات الجريمة و التعامل معها، فالجرائم العادية يسهل – غالبا– تحديد مكان إرتكابها، في حين أنه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع الجرائم الإلكترونية، لكون الرسائل و ملفات الكمبيوتر تنتقل من نظام معلومات إلى آخر في ثوان معدودة، كما أنه لا يقف أمام إنتقال الملفات و المستندات و الرسائل عبر شبكة الإنترنت أي حدود دولية أو جغرافية و نتيجة لذلك فإن تحديد أي محكمة تحدد أي قانون يطبق سوف يكون مشكلة بين الدول مما يستدعي التعاون بين دول العالم.[2]

كما أن مشروعية الجريمة أمر نسبي من دولة إلى أخرى، فمثلا تجارة المخدرات في الأردن و الكويت محرمة نهائيا، بينما في الدول الإسكندنافية مصرح بها في حدود الإستعمال الشخصي فقط، بل إن مشروعية الجريمة قد تختلف داخل البلد الواحد، فمثلا

[1] تفصيلا أنظر، الزعبي، جلال و المناعسة، أسامة، مرجع سابق، ص 86– 87

[2] حجازي، عبد الفتاح بيومي (2004)، جرائم الكمبيوتر و الإنترنيت، دار الكتب القانونية، مصر، 148.

نجد داخل الولايات المتحدة الأمريكية أن ألعاب القمار عبر الإنترنت مسموح بها في لاس فيغاس بينما هي محرمة قانونا في ولاية نيويورك[1]

سادسا: وقوع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات:

من خصائص الجريمة الإلكترونية أنها تقع أثناء عملية المعالجة الآلية للبيانات و المعطيات الخاصة بالكمبيوتر، و يمثل هذا النظام الشرط الأساسي الذي توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الإلكترونية[2].

" و قد كان هناك إقتراح من قبل مجلس الشيوخ الفرنسي حال تعديل قانون العقوبات الحالي، بوضع تعريف محدد لعملية المعالجة الآلية للبيانات أو المعطيات، و لكن حذف هذا التعريف بإعتبار أنها فنية تخضع للتطور السريع، و بالتالي سيكون أي تعريف لها قاصرا، و كان هذا التعريف ينص على أنها:" كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، و التي تتكون منها من الذاكرات، و البرامج، و المعطيات، و أجهزة الإدخال، و الإخراج، و أجهزة الربط، و التي يربط بينها مجموعة من العلاقات و التي عن طريقها يتم تحقيق نتيجة معينة و هي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام الحماية الفنية[3].

و الجريمة الإلكترونية قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات.

سابعا: الجريمة الإلكترونية جريمة مستحدثة:

[1] عفيفي، كامل عفيفي (2010)، جرائم الكمبيوتر، دار النهضة العربية، القاهرة، ص 76

[2] قورة، نائلة مرجع سابق، ص 55

[3] نقلا عن: القهوجي ، علي عبد القادر(2000)، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الإنترنت و الذي عقد خلال الفترة من 1 – 3 مايو ، كلية الشريعة و القانون، جامعة الإمارات العربية، ص 43.

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة ، فلا غرابة أن تعد الجرائم الإلكترونية – سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في إرتكابها – من الجرائم المستحدثة ، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته و إمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها و أمن مواطنيها[1].

ثامنا: إحتمال تعدد الأوصاف القانونية لمحل الجريمة الإلكترونية:

إن محل الجريمة الإلكترونية قد يظهر بمظهرين أحدهما مادي و الثاني معنوي ، كما هو الحال بالنسبة للمعلومات فقد تكون في حالة إنتقال أو موجودة في ذاكرة النظام الإلكتروني أي أنها في حالة غير مادية ، و الشكل الاخر أن تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة إلكترونية ، حتى أن المعلومات غير المادية بطبيعتها يمكن أن تخضع لأكثر من نص قانوني، وفقا لما إذا كانت في شكل مادي أو غير مادي ، و في الشكل الأخير يوجد لها أكثر من نص قانوني يمكن أن تخضع له، مثل ذلك إعتبارها مصنف أدبي مما يثير مشكلة تعدد الأوصاف القانونية على ذات المحل.[2]

[1] إبراهيم ، خالد ممدوح ،مرجع سابق، ص 86

[2] إبراهيم ، خالد ممدوح ، المرجع سابق ، ص 87-88.

الفصل الثاني: الاحكام الاجرائية للجريمة الإلكترونية.

المبحث الاول: ضبط الجريمة المعلوماتية و اثباتهـــا.

المبحث الثاني: الاختصاص بنظر الجريمة الالكترونية

الفصل الثاني: الاحكام الاجرائية للجريمة الإلكترونية

اتضح لنا من الفصل السابق أن الجريمة المعلوماتية ترتكب باستخدام التقنية المعلوماتية مما يعني أنها ترتكب في فضاء افتراضي مفرغ cyberspace، سواء ارتكبت عبر شبكة الإنترنت أم في داخل نطاق ذات المؤسسة التي يتم الاعتداء عليها، أو ارتكاب الجريمة من خلالها، و تعرضنا في الفصل السابق أيضاً إلى المشكلات الموضوعية التي تثيرها هذه الجرائم في تطبيق القواعد التقليدية لقانون العقوبات الذي صيغت جل نصوصه ونظمه الأساسية لتواجه سلوكاً مادياً يرتكب في عالم مادي ملموس، فإذا كان ذلك هو حال القواعد الموضوعية للتجريم و العقاب، فما هو حال القواعد الإجرائية لهذا الفرع من القانون الجنائي[1] ؟ وهو ذلك الفرع الذي يتأسس في كل النظم القانونية المختلفة على مبدأ دستوري هو الشرعية ،أي شرعية التجريم و العقاب، الذي تنبثق عنه قاعدة الشرعية الإجرائية، و ما يميز هذه الجريمة هو أنها ترتكب في مسرح الكتروني أو مجال مفرغ يختلف كلياً عن المسرح التقليدي الذي ترتكب فيه الجريمة حيث يتم الاستدلال عليها وضبطها و اثباتها بالوسائل التقليدية المتمثلة في اجراءات الاستدلال و التحقيق ، فهي اجراءات صيغت لضبط و اثبات جرائم ترتكب في عاالم ملموس مادياً، يلعب فيه السلوك المادي الدور الأكبر و الأهم، وهنا يثور التساؤل

[1] د.احمد السيد عفيفي – الاحكام العامة للعلانية في قانون العقوبات – دراسة مقارنة – – 2001 – 2002– دار النهضة العربية، القاهرة .ص32

حول مدى صلاحية هذه الإجراءآت لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس [1]؟ أما إذا ارتكبت الجريمة عبر الشبكة العنكبوتية الدولية (الانترنت) تزداد العقبات القانونية صعوبة، فلا نكون أمام مشكلات اجرائية تخص ضبط الجريمة و اثباتها فحسب، بل نجد انفسنا أمام مشكلة أكثر تعقيداً تتمثل في تحديد الاختصاص القضائي المرتبط بتحديد القانون الواجب التطبيق على هذه الجريمة، فقواعد الاختصاص القضائي التقليدية صيغت لكي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة، وهي قواعد ترتكز على مبدأ الإقليمية، وهو ما يرتبط بسيادة الدولة على إقليهما، فلا يكون الخروج عليه بقبول اختصاص قضائي أجنبي إلا في حالات استثنائية يجب النص عليها صراحة، وهنا تثور امامنا مدى امكانية الاعتماد على هذه القواعد لتحديد الاختصاص القضائي لجريمة ترتكب في مجال تنعدم فيه الحدود الجغرافية، وكثيرا ما يكون مرتكبيها في بلاد مختلفة و من جنسيات متعددة، و كثيرا ايضا ما يتعلق السلوك الاجرامي باكثر من دولة: الدولة التي ارتكب فيها السلوك و الدولة التي تم فيها القبض على الجاني و تلك التي حدثت فيها النتيجة الاجرامية و هو ما يتطلب منا التطرق الى مشكلات ضبط الجريمة المعلوماتية و اثباتها في مبحث أول قبل التطرق إلى الحديث عن مشكلات الاختصاص بنظر الجريمة المعلوماتية في مبحث ثانٍ .

[1] أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة 1994.ص 55

المبحث الأول: ضبط الجريمة المعلوماتية و اثباتها

يعتمد ضبط الجريمة و اثباتها في المقام الأول على جمع الأدلة التي حدد المشرع وسائل اثباتها على سبيل الحصر ، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية، و تتمثل في وسائل الاثبات الرئيسية في و في المعاينة و الخبرة و التفتيش و ضبط الأشياء المتعلقة بالجريمة، أما غيرها من وسائل الاثبات كالاستجواب و المواجهة و سماع الشهود فهي مرحلة تالية من إجراءات التحقيق و جمع الأدلة ، ولما كنا بصدد تناول الجريمة المعلوماتية و ما تثيره من مشكلات إجرائية، فسنتعرض للمشكلات القانونية التي يثيرها اثبات هذه الجرائم دون غيرها من الاجراءات كالاستجواب و المواجهة و سماع الشهود، لأن هذه الأخيرة تتم في مواجهة البشر، أما المعاينة و الخبرة و التفتيش ،فهي إجراءات فنية محلها الأشياء لا الافراد وهو ما يهمنا في هذا الموضوع .[1]

[1] د.جميل عبد الباقي الصغير – الانترنت و القانون الجنائي – دار النهضة العربية –2001 .ص33

لما كان ذلك فسوف نقسم هذا المبحث إلى مطلبين، نتناول في الأول الحديث على حجية المخرجات الالكترونية في الاثبات الجنائي، قبل أن ننتقل لتناول اشكاليات المعاينة و الخبرة في المسائل المعلوماتية في المبحث الثاني.

المطلب الأول: حجية المخرجات الالكترونية في الاثبات:

تخضع المحررات كغيرها من الأدلة التي تقدم أثناء نظر الدعوى إلى تقدير المحكمة حيث يسود مبدأ حرية القاضي في تكوين عقيدته، وهو ما يختلف فيه القاضي المدني حيث يتقيد هذا الاخير بطرق معينة في الاثبات، فالقاضي الجنائي له مطلق الحرية في تقدير الدليل المطروح أمامه ،وله أن يأخذ به أويطرحه ولا يجوز تقييده بأي قرائن أو افتراضات[1] .

ولما كانت المحررات أحد الأدلة التي قد يلجأ اليها القاضي في الاثبات فهي تخضع كغيرها من الادلة لتقدير المحكمة، الا إذا كان الاثبات متعلقاً بمواد غير جنائية، ففي هذه الحالة يكون على القاضي الجنائي أن يتقيد بطرق الاثبات المحددة في ذلك الفرع من القانون مثال ذلك حق الملكية في جريمة السرقة ، والعقود التي تثبت التصرف في الحق في جريمة خيانة الامانة أو صفة التاجر في جريمة التفليس بالتدليس[2] .

[1] مأمون سلامة – الاجراءات الجنائية في التشريع الليبي – ج 2ط2000– منشورات المكتبة الجامعة – ص151.

[2] مأمون سلامة – المرجع السابق – ص160

وهنا تثور مشكلة مدى حجية المخرجات الالكترونية في الاثبات الجنائي في هذه الحالات، فللمخرجات الالكترونية انواع مختلفة، فهي تتنوع بين مخرجات ورقية، و مخرجات لاورقية و هي المعلومات المسجلة على الأوعية الممغنطة كالاشرطة و الاقراص المرنة Floppy Disk و القرص الصلب Hard Disk وغيرها من الاوعية التي اصبحت في تطور مستمر حتى وصلت الى اقراص الflash discs التي اصبحت تتميز بسعات كبيرة للتخزين، خاصة أنه تواجهنا مشكلة اساسية تتعلق بصعوبة التمييز بين المحرر و صورته أو بين الاصل و الصورة ، ذلك لأننا نتعامل مع بيئة الكترونية تعمل بالنبضات و و الذبذبات و الرموز و الأرقام وهو ما يستحيل معه تطبيق القواعد الخاصة بالمحررات العرفية [1]

ولما كان المشرع الليبي لا يزال عازفاً عن التدخل التشريعي في هذه المسألة فلا بد من تطبيق القواعد العامة في هذا الصدد، ولما كان ذلك، فالمشرع الليبي لايزال يعتمد على مبدأ سيادة الدليل الكتابي على غيره من الادلة ولا يجوز الاعتماد على الدليل غير الكتابي في غير المسائل الجنائية،الا على سبيل الاستئناس، ولا يخفى ما يؤدي ذلك من تقييد للقاضي الجنائي لأن الإثبات في المسائل الجنائية كثيراً ما يعتمد على مسائل غير جنائية ، وهو ما سبقت الاشارة اليه عند تناول جريمة التزوير في هذا البحث التي

[1] احمد شرف الدين– حجية الرسائل الاليكترونية في الاثبات – شبكة المعلومات القانونية العربية – East Law .com – 2007-ص111

اعتمدت على مدى اعتبار هذه الاوعية من قبيل المستندات او المحررات موضوع جريمة التزوير ، فمواجهة الجرائم المعلوماتية لا تتأتى الا عن طريق نظام قانوني متكامل أهم عناصره التدخل لضبط المعاملات و التجارة الاكترونية واضفاء الحجية القانونية على المستندات الالكترونية شأنها شأن المستندات الورقية، حتى يتاح للقاضي الجنائي الاعتماد عليها و اتخاذها دليلاً جنائياً، كغيره من الادلة، وقد كان المشرع التونسي من السباقين بين أقرانه على المستوى العربي في هذا المجال، حيث صدر في تونس قانون التجارة و المعاملات الالكترونية الذي اعترف للمستندات الالكترونية سنة 2000 بحجيتها في الاثبات، كما أصدرت امارة دبي قانون التجارة الالكترونية سنة 2002 ، وتبعهما بعد ذلك المشرع المصري سنة 2004 الذي اصدر قانون نظم التوقيع الكتروني، وتجدر الاشارة في هذا الصدد إلى القانون العربي النموذجي السابق الاشارة اليه سنة 2003، وكل هذه القوانين اعطت للمستند الالكتروني ذات الحجية التي يتمتع بها المحرر الورقي، تجدر الاشارة ايضاً إلى أن لجنة الأمم المتحدة للقانون التجاري الدولي United Nation Commission on International Trade Law (UNCITRAL) على هذه الحجية و قد كان ذلك سنة 2000 أما القانون العربي النموذجي فنص في المادة الأولى منه على تعريف الكتابة بأنها كل(عملية تسجيل للبيانات على وسيط لتخزينها)، و المقصود بالوسيط في هذه الحالة هو الوسيط الالكتروني لأن الوسيط الورقي المتمثل في الأوراق التقليدية لا يحتاج إلى تعريف، وإن كنا نتحفظ على استخدام عبارة الوسيط دون تحديده

بالالكتروني، مادام الأمر متعلقاً بالتجريم و العقاب، أما المادة 6 من قانون الاونسترال النموذجي السابق الاشارة اليه [1].

اذا كان المشرع التونسي يعد سباقاً إلى اللحاق بهذا التطور التشريعي فإن المشرع السنغافوري أصدر قانوناً للاثبات أقر فيه حجية المستندات المعلوماتية في الاثبات منذ سنة 1997م وهو ما يبين مدى تأخر المشرع الليبي في مواكبة هذا التطور[2].

المطلب الثاني: الخبرة و المعاينة في الجرائم المعلوماتية

تعتبر كل من الخبرة و المعاينة أكبر العقبات التي تواجه الاثبات في الجرائم المعلوماتية، فالمعاينة اجراء بمقتضاه ينتقل المحقق الى مكان وقوع الجريمة ليشاهد اثارها بنفسه ، فيقوم بجمعها وجمع أي شيء يفيد في كشف الحقيقة، وتقتضي المعاينة اثبات حالة الأشخاص و الأشياء الموجودة بمكان الجريمة و رفع الآثار المتعلقة بها كالبصمات و الدماء و غيرها مما يفيد التحقيق، و المعاينة تكون شخصية إذا تعلقت بشخص المجني عليه، أو مكانية اذا تعلقت بالمكان الذي تمت فيه الجريمة، ووضع الشهود و المتهم و المجني عليه، أما المعاينة العينية فهي التي تتعلق بالأشياء أو

[1] مرجع سابق – ص88

[2] عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – القاهرة 2007 .ص44

الأدوات المستخدمة في ارتكاب الجريمة وقد يقتضي الامر الاستعانة بخبير للتعرف على طبيعة المادة او نوعها إذا كان ذلك يحتاج لرأي المتخصص، وفي هذه الحالة يتم ارسال هذه الاشياء الى الخبير لنكون بصدد اجراء آخر من اجراءات التحقيق و هو الخبرة ، فالخبرة هي أحد أهم وسائل جمع الأدلة، يلجأ اليها المحقق عند وجود واقعة مادية أوشيء مادي يحتاج االتعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الاثبات[1].

يثور التساؤل هنا عن مدى امكانية معاينة الجريمة المعلوماتية، واذا كانت المادة 74 اجراءات جنائية ليبي تنص على انتقال المحقق لأي مكان ليثبت حالة الامكنة و الاشياء و الاشخاص ووجود الجريمة مادياً، فهل يكون للجريمة المعلوماتية وجود مادي، يمكن للمحقق الليبي معاينته؟ نجد في هذه المادة أن المشرع سن هذا النص لضبط جريمة لها وجود مادي محسوس في العالم الخارجي، وما يؤكد ذلك هو أن المادة 44 من ذات القانون تنص على أن (توضع الاشياء و الاوراق التي تضبط في حرز مغلق وتربط كلما أمكن) فالحرز المغلق الذي يتم ربطه هو الاجراء العام الذي تخضع له كل الاشياء المضبوطة، وهنا نصطدم بالعقبة الاساسية أمام معاينة الجريمة المعلوماتية التي ترتكب داخل الفضاء المعلوماتي أو السيبراني، فالمحقق في هذه الحالة

[1] حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الاسكندرية مصر 1991 .ص57

يتعامل مع بيئة مليئة بالنبضات الالكترومغناطيسية و البيانات المخزنة داخل نظام معلوماتية شديدة الحساسية ولا يتعامل مع أوراق او اسلحة أو اشياء قابلة للربط وهو ما يؤكد القواعد الاجرائية التقليدية سنت لتواجه سلوكاً ماديا يرتكب بواسطة الات و ادوات قابلة للربط و التحريز .

أما السلوك الاجرامي ففي الجريمة المعلوماتية فهو عبارة عن بيانات مخزنة في نظام معلوماتي يتطلب اثباته انتقال محقق متخصص حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الاسطوانة الصلبة الخاصة بالجهاز، ويجب على المحقق أو ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة. وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الانترنت ،ولكي ينجح المحققون في عملهم يجب أن يقتفوا أثر الاتصالات منذ الحاسب المصدر إلى الحاسب أو المعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل ودولة. كما يقتضي ذلك ايضاً ان يعمل المحقق على الوصول إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات. من أين صدرت؟ ومن الذي يحتمل إجراؤها، بالاضافة الى ضرورة المام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز

أو الاكتفاء بأخذ نسخة من الاسطوانة الصلبة للحاسب ، والاوقات التي يستخدم فيها برامج استعادة المعلومات التي تم الغاؤها (1)

فالمحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملماً بمهرات هذه التقنية، مثل القدرة على استخدام برامج Time stamp وهي البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الاجرامي، لأن ذلك لا يكون متاحاً في جميع الانظمة المعلوماتية ،أما الخبير ففي هذه الحالة يجب ان يكون ملماً بمهارات تحليل البيانات و مهارات التشفير cryptanalysis skills التي تتيح له فك الرموز استعادة البيانات لملغية .

ولما كانت الجرائم ترتكب عبر الشبكة الدولية فقد نصت المادة 23 على أن (تتعاون كل الأطراف، وفقاً لنصوص هذا الفصل، على تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وكذلك بشأن الحصول على الأدلة في الشكل الإلكتروني لمثل هذه الجرائم) كما نصت

(1) Recommandations sur le dépistage des communications électroniques transfrontalière dans le cadre des enquêtes sur les activités criminelles www G8 Mont tremblant Canada 21 mai 2002. اشار اليه أ.د. صالح أحمد البربري دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية –الموقعة في بودابست في 2001/11/3www.arablawinfo@.com-

المادة 30 من الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على : أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله. كما أشارت المادة 31 إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة . حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة 29من الاتفاقية[1] .

وهو ما نصل معه الى حقيقة مؤداها اننا نواجه اليوم اخطر مظاهر العولمة ، فالتعاون الدولي في المجال الجنائي لم يعد مقتصراً على نظام الانتربول ، فأصبح على الدولة أن تستخدم بروتوكولات موحدة لنظم التخزين و الحماية المعلوماتية كما حدث على مستوى الاتصالات الهاتفية ، لأن التعاون بين دولة واخرى سوف يتم بين أجهزة الخبرة

[1] عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والانترنت – دار الكتب القانونية – القاهرة 2005.ص22

الجنائية بشكل مباشر وبطريقة متشابكة ، وهو مانصل معه إلى ان تطوير البنية التحتية المعلوماتية لأي دولة اليوم اصبح ضرورة ملحة ، ومطلباً أساسياً قد يترتب على غيابه انعزال الدولة وسيرورة نظامها المعلوماتي – اذا كان متواضعاً – مباحاً لمجرمي المعلوماتية[1] .

نخلص من كل ما تقدم إلى أن الخبرة و المعاينة الجنائية في الجرائم المعلوماتية اليوم تحتاج إلى ادارة خاصة يعمل بها متخصصون في أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية ، وهوما يتطلب انشاء ادارة خاصة للخبرة و المعاينة في الجرائم المعلوماتية ، ولا يجب الاكتفاء بمجرد تدريب القائمين على إدارة الخبرة الجنائية ، أما رجال القضاء و النيابة والضبطية القضائية فلا شك أنهم يحتاجون للتدريب على استخدام مهارات الحاسب لآلي و الموسوعات القانونية التي تتطلب ربط كافة المؤسسات القضائية بقواعد بيانات قانونية مثل أحكام المحاكم و القوانين المختلفة ، لتوفير امكانية استخدام موسوعات القوانين و مجموعات الأحكام القانونية العربية المختلفة و تعليمات النائب العام ، لرفع مستوى الكفاءة القانونية لدى رجال القضاء و النيابة العامة .

[1] عبد الفتاح بيومي حجازي– مرجع نفسه–ص27

المبحث الثاني: الاختصاص بنظر الجريمة الالكترونية

خلصنا من المبحث السابق إلى عدم كفاية القواعد التقليدية للخبرة و المعاينة، وعدم ملائمتها لاثبات الجرائم المعلوماتية، فهل تستجيب القواعد الخاصة بتحديد نطاق تطبيق القانون من حيث المكان، فكيف يمكن تحديد مكان وقوع الجريمة المعلوماتية ؟ واذا كانت هذه الجريمة ترتكب في مجال افتراضي غير محدد جغرافياً فهل يمكن ربط هذه الجريمة بدولة ما دون اخرى؟ للاجابة على هذا التساؤل تتطلب ضرورة الحديث عن لامركزية القضاء المعلوماتي في مطلب أول، قبل تناول التعاون الدولي لملاحقة الجريمة المعلوماتية في المطلب الثاني[1]

المطلب الأول: لامركزية القضاء و عالمية الجريمة الالكترونية.

فقدت الحدود الجغرافية كل اثر لها في القضاء الشبكي او الآلي، فهو لا يعترف بالحدود الجغرافية حيث يتم تبادل البيانات في شكل حزم الكترونية توجه الى عنوان افتراضي ليس له صلة بالمكان الجغرافي، فهو قضاء ذو طبيعة لا مركزية DESSENTRALI ZED NATURE و يمكن اجمال اهم خصائصه في عدم التبعية لأي

[1] فهد بن عبدالله اللحيدان، – الإنترنت، شبكة المعلومات العالمية – الطبعة الأولى– الناشر غير معروف – 1996.ص78

سلطة حاكمة [1].فالقضاء الالي : نظام الكتروني معقد لانه عبارة عن شبكة اتصال لا متناهية غير مجسدة و غير مرئية متاحة لاي شخص حول العالم و غير تابعة لاي سلطة حاكمة فالسلوك المرتكب فيها يتجاوز الأماكن بمعناه التقليدي له وجود حقيقي وواقعي غير محدد المكان لكنه حقيقة واقعا.

فالشبكة عالمية النشاط و الخدمات لا تخضع لأي قوة مهيمنة الا في بدايتها حيث كان تمويل هذه الشبكة حكوميا يعتمد على المؤسسة العسكرية الامريكية، أما الان فقد اصبح التمويل ياتي من القطاع الخاص حيث الشركات الاقليمية ذات الغرض التجاري التي تبحث عن كافة السبل للاستفادة من خدماتها بمقابل مالي 2.

والجريمة المرتكبة عبر شبكة الانترنت جريمة تعبر الحدود و القارات ،وهو ما يدرجها ضمن موضوعات القانون الجنائي الدولي ، الذي يقابل القانون الدولي الخاص في القانون المدني، و هو ذلك الفرع من القانون الذي يحدد ضوابط مجالات التعاون الدولي في مجال مكافحة الجريمة بالتزام الدول الموقعة على الاتفاقيات بالعمل بمقتضاها في مكافحة الجريمة.

[1] فتوح الشاذلي – القانون الدولي الجنائي – دار المطبوعات الجامعية – الاسكندرية – 2001 –ص31

[2] – منير الجنبهي – ممدوح الجنبهي – صراخ الانترنت وسائل مكافحتها – المرجع السابق –ص 9

[2] فتوح الشاذلي – المرجع السابق – ص 34

و قد ازدادت اهمية القانون الجنائي الدولي بعدما تطورت الجريمة المنظمة في وقت تقلص فيه المفهوم التقليدي للسيادة ، حيث اتسع نظام المعاهدات الدولية لمكافحة الجرائم العابرة للحدود فالجانب الدولي للجريمة المعلوماتية لا يعد عنصرا من عناصرها كما هو الحال في الجريمة الدولية بل يعد هو نطاقها المكاني.

ان القواعد العامة التي تحكم نطاق تطبيق النصوص الجنائية – التي تتمثل في مبدأ اقليمية النص الجنائي و الاستثناءات الواردة عليه – تقتضي تطبيق النص الجنائي على كل الجرائم الواقعة في اقليمه، الا في احوال خاصة نص عليها المشرع في المواد 4 و ما بعدها تبين حالات يطبق فيها القانون الليبي على جرائم ارتكبت خارج اقليمه.

المطلب الثاني: التعاون الدولي لملاحقة الجرائم المعلوماتية:

يعتمد النظام القانوني السابق على جريمة ترتكب في مكان قابل للتحديد الجغرافي، اما الجريمة المعلوماتية فهي جريمة ترتكب في مسرح غير قابل للتحديد الجغرافي، الا انه يضم اكبر تجمع إنساني يتميز بارتباط و تشابك معقد، و تتمثل اهم خصائصه في خلق آليات خاصة لفرض الالتزامات و الاذعان لها مثل قطع الاتصال على مخترقي بعض القواعد او طردهم من المنتديات، لكن هذا التجمع الانساني الضخم يفتقر الى المعايير الاخلاقية المشتركة.

و هو ما أدى بالمجلس الاروبي الى عقد اتفاقية بوداست COUNCILالسابق الاشارة اليها، و التي قدمت صورا لمكافحة هذه الجرائم و نصت المادة 22 منها على "أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التي يراها لازمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقاً لما هو وارد في المواد من 2 إلى 11 من الاتفاقية الحالية عندما تقع الجريمة:

1. أ- داخل النطاق المحلي للدولة

ب- على ظهر سفينة تحمل علم تلك الدولة.

ج- على متن طائرة مسجلة في هذه الدولة.

د- بواسطة أحد رعاياها، إذا كانت الجريمة معاقباً عليها جنائياً في المكان الذي ارتكبت فيه أو إذا كانت الجريمة لا تدخل في أي اختصاص مكاني لأي دولة أخرى.

ولكل طرف أن يحتفظ لنفسه بالحق في عدم تطبيق، أو عدم التطبيق إلا في حالات وفي ظل شروط خاصة، قواعد الاختصاص المنصوص عليها في الفقرة الأولى (ب و د) من هذه المادة أو في أي جزء من هذه الفقرات.[1]

[1] مبدر سليمان لويس – أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية ، رسالة الدكتوراة – حقوق القاهرة.–ص13

و تنص الفقرة 4 من المادة على عدم استبعاد اي اختصاص ينعقد للقضاء الوطني طبقا للقانون المحلي الفقرة 5 تنص على انه في حالة حدوث تنازع في الاختصاص فانه يجب ان يتم حله بالتشاور بين الدول الاطراف حول المكان الاكثر ملائمة. كما افرزت الاتفاقية بندا خاصا لضرورة التعاون بين الدول.

و لم ينص القانون العربي النموذجي بشأن الجرائم المعلوماتية على اي قواعد لتحديد الاختصاص بنظر هذه الجرائم. فان كان الفقه الجنائي اليوم قبل فكرة تطبيق القانون الأجنبي لمواجهة الجريمة عبر الوطنية ما أظهر ضرورة تجاوز فكرة تلازم الاختصاص الجنائي والقضائي و التشريعي فيلزم من باب أولى قبول هذه الفكرة و التوسع فيها بالنسبة لجرائم ترتكب في القضاء السيبراني الذي يبتجاوز الحدود و القارات، و بذلك نصل الى ضرورة التفكير في وضع ضوابط اسناد جنائية لتحديد الاختصاص الموضوعي و الاجرامي بعد ان تصنف الى فئات مختلفة تشكل كل فئة فكرة مسندة تتضمن المصالح الواجب حمايتها جنائيا على المستوى العالمي لوضع ضوابط اسناد تشير الى القانون الواجب التطبيق[1].

إلا أن هذه القواعد يجب ان تتم صياغتها في اطار اتفاقات دولية لأن الجريمة الدولية لا يمكن مواجهتها إلا بالتعاون الدولي ، و هو اهم ما جاء في اتفاقية بودابست

[1] محمد سامي الشوا ثورة المعلومات وبعكسها على قانون العقوبات دار النهضة العربية القاهرة 1994–ص22

بشكل يسمح بتبادل التعاون سواء كان ذلك على مستوى جمع الأدلة أو تسليم المجرمين وهو ما يعني ان المجتمع الدولي مقبل على توسع في مجال التعاون القضائي الذي يتوقع أن يتم بين الاجهزة القضائية و الامنية بشكل مباشر نظراً لأن عامل الوقت في حفظ الادلة المعلوماتية سوف يكون حرجاً ومتطلباً لسرعة الانجاز[1].

[1] محمد عبد الطاهر حسين – المسئولية القانونية في مجال شبكات الانترنت – 2002 – دار النهضة العربية – القاهرة –ص58

الخاتمة

تعرضت الدراسة إلى أهم صور الجريمة الالكترونية عبر شبكة الانترنت الفصل الأول الاحكام الموضوعية للحماية الجزائية للمعلومات عبر شبكة الانترنت و الفصل الثاني الاحكام الاجرائية للجريمة الإلكترونية ، حيث افرزت لنا هذه التقنية الحديثة عناصر جديدة للحياة الخاصة لم تعرفها القوانين التي حصرت حمايتها الجنائية فيما تصورت انه يغطي حميع عناصر الحياة الخاصة للإنسان ، فقصرت هذه الحماية على المسكن و الصورة و المحادثات الهاتفية ، دون ان تشمل تلك البيانات المتدفقة عبر الشبكة العنكبوتية الدولية ، من جهة وتلك المخزنة في النظم المعلوماتية للمؤسسات العامة و الخاصة التي تتعامل مع الجمهور من جهة اخرى. أما جرائم الاعتداء على الأموال فقد أظهرت الحاجة الماسة للمواجهة التشريعية لنوع مستحدث من جرائم الاعتداء على الأموال ،لأن الأموال لم تعد تلك العملات المعدنية و الورقية التي عرفناها منذ زمن بعيد ،فقد أصبحت الأموال عبارة عن قيمة مالية مخزنة في بطاقات تقرأها الآلة تارة ، و تخزن على القرص الصلب للحاسب تارة اخرى ، أما طرق الاعتداء فلم تعد بالاختلاس الذي يتمثل في انهاء مادي لحيازة المجني عليه سواء تم ذلك بوسائل احتيالية أو خلسة دون رضائه ، بل أصبح الاعتداء يتم بطرق مستحدثة مثل الاختراق و فك الشفرات المختلفة للوصول إلى أرقام بطاقات الصرف و الإتمان، أو عن طريق اعداد برامج خاصة لتنفيذ عملية الاختلاس أو انهاء الحيازة ، الذي كثيراً ما يتم في وقت يكون فيه المتهم بعيداً عن موقع الجريمة أو مكانها. حيث ان المشكلة التي تثيرها الجريمة هذه المرة لاتكمن في السلوك الإجرامي المرتكب ، والفراغ التشريعي لمواجهة الجريمة، لكن النص حدد محل الجريمة ، لكنه لم يعرفها تاركاُ للفقه و القضاء هذه المهمة ، وهو ما يثور معه التساؤل حول مدى امكانية اعتبار الدعائم الممغنطة من قبيل الوثائق التي يمكن أن تكون محلاً لجريمة التزوير .

انتقل البحث بعد ذلك لتناول المشكلات القانونية التي تثيرها الجرائم المعلوماتية من حيث المسؤولية الجنائية ، بالنسبة لوسطاء تشغيل الشبكة التي ترتكب عن طريقها الجريمة الالكترونية ، فهذه الأخيرة يتدخل لتشغيلها العديد من الأفراد أو الجهات العامة منها و الخاصة فالشبكة لا تعمل الا عن طريق مزود الخدمة الذي يمد العميل بالوسيلة الفنية التي توصله بالشبكة ، أما متعهد الوصول فهو من يوفر لمالك الموقع المساحة للفضاء الإكتروني لكي يمكنه من استخدامها و تحميلها بالمضمون أو بالبيانات التي تتضمن الاعتداء أو المضمون المجرم ، وهنا تثور اشكالية حول امكانية تطبيق الأحكام العامة للمسؤولية الجنائية مما يستدعى التدخل التشريعيى لحسم هذه المشكلة ، اذا ما ارتكبت عن طريق الشبكة أي من جرائم السب أو التشهير. انتقل البحث بعد ذلك لمناقشة البعد الدولي للجرائم المعلوماتية موضحاً أن الجانب الدولي لهذه الجرائم يشكل نطاقها المكاني، وليس عنصراً فيها كما هو الحال بالنسبة للجريمة الدولية، لأن الجريمة المعلوماتية شأنها شأن الجرائم المنظمة عبر الوطنية التي يمكن ارتكابها داخل حدود دولة واحدة ، إلا أن عناصرها المادية تمتد لأكثر من دولة واحدة، مما يدرجها في قائمة الجرائم التي يجب دراستها ضمن موضوعات القانون الجنائي الدولي ، فالجريمة المعلوماتية ليست جريمة دولية لأن هذه الأخيرة يشكل العنصر الدولي فيها عنصراً من عناصرها ، لذلك فإن دراسة الجانب الدولي في هذه الجرائم يجب أن يكون في محاولة لتجاوز القواعد التقليدية لتحديد مبدأ الاقليمية الذي تتأسس عليه قواعد الاختصاص القضائي و القانوني لملاحقة الجرائم التي ترتكب عبر أكثر من دولة .

النتائج:

1- غياب نصوص دولية موحدة تواجه جرائم العالم الافتراضي،غياب نصوص دولية موحدة تكفل الحماية الجنائية للجرائم الالكترونية على شبكة الانترنت .

2- وجود قصور في قوانيننا في مجال الجرائم المعلوماتية ،اذ أنه لا تزال الكثير منها تخضع للنصوص التقليدية و هو الشيء الذي يعد مساسا مباشرا لمبدأ الشرعية من جهة و الذي ينعكس سلبا في مجال المتابعة اذ انه يؤدي الى افلات الكثير من الجناة من العقاب. و نظرا لنسبية الحماية من خلال النصوص التقليدية للجرائم الالكترونية نتيجة للطبيعة المتميزة للمال المعلوماتي استقر الفكر القانوني.

3- نظرا لخصوصية الجرائم التي ترتكب في البيئة الإلكترونية فقد خصها المشرع بقانون مستقل هو القانون رقم 04 /09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، تضمن مجموعة إجراءات جد استثنائية تتلائم مع البيئة الإلكترونية.

4- قد لا تقتصر الجرائم الإلكترونية على الإعتداء على الافراد أو المجموعات و إنما قد تكون على الصعيد الدولي لتشمل مجموعة من الجرائم كالتجسس الإلكتروني و السرقة المالية و غيرها من الجرائم العابرة للحدود و تكون أكثر خطورة عندما تستهدف الأمن الوطني.

5- ان المشرع الجزائري أحسن باستحداثه الهيئة الوطنية للجرائم الالكترونية المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها و لكن كان عليه إعداد و تجهيز قوات خاصة تعمل تحت هذه الهيئة حتى يمكن لها أن تقدم ولو جزء قليل من الخبرة و المساعدة في التحقيق لكافة المحاكم الوطنية وذلك نظرا لكثافة إنتشار هذا النوع من الجرائم و سرعة زوال الدليل الإلكتروني.

6- يعد الإرهاب الإلكتروني من أخطر أنواع الإرهاب على الدول في العصر الحاضر كيف لا و قد أصبح أكثر ضرورة لاعتماده على التكنولوجيا المتطورة مما زاد في اتساع مسرح عملياته الإرهابية ، وبالتالي أصبح من الصعب القضاء على المجرم الإلكتروني

الجديد و لم تقتصر إساءة استخدام الشبكة المعلوماتية على الأشخاص فحسب بل تعدى الأمر ليصل إلى الذمة المالية للغير مما شكل اعتداء على أموالهم المادية.

وهو ما نصل معه إلى **التوصيات** التالية :

1- ضرورة اعادة النظر في قواعد الاختصاص القضائي لأن الفضاء السيبراني أو cyber space عبارة عن مسرح لارتكاب جرائم مستحدثة ، ترتكب في عالم افتراضي غير ملموس ماديا لكن له وجودا حقيقياً، أهم خصائصه هي انه يتجاوز حدود الزمان و المكان ، وينذر بضرورة اعادة النظر في الكثير من القواعد و المسلمات القانونية مثل قواعد الاختصاص و مبدأ السيادة وغيره من المبادئ القانونية القائمة على المفهوم المادي للسلوك.

2- على المشرع الجزائري أن يتدخل لمواجهة الجريمة المعلوماتية التي ترتكب للاعتداء على الأموال ، وهو ما يتطلب ضرورة التنظيم القانوني للنقود الإلكترونية بتعريفها و رسم الاطار القانوني الخاص بها وتحديد الجهات الوطنية المختصة باصدارها و طرحها للجمهور حتى يتسنى مواجهة الاحتيال و التلاعب بهذه الأموال

3- على الدولة أن تعمل على تبني جهازاً خاصاً للخبرة الجنائية للجريمة الالكتونية التي ترتكب عبر شبكة الأنترنت ، يتكون اعضاؤه من فريق متخصص فنياً في التقنية المعلوماتية ، على أن يتم اعادة النظر في القواعد التقليدية للخبرة ، لأن اثبات الجريمة المعلوماتية يتطلب قواعد خاصة للتعامل مع الأدلة في هذه الجرائم ، لأن البحث عنها يتم داخل نظام الكتروني معقد ، يسهل فيه محو الادلة إذا ما تم التعامل الأولي مع الجهاز بشكل خاطئ .

4- العمل على اعادة النظر في المناهج الدراسية في كليات القانون، وضرورة تضمينها مادة عامة عن الحاسب الآلي و الشبكات المعلوماتية، بالاضافة إلى ضرورة ادراج

الجانب المعلوماتي لكل مادة قانونية فيجب أن تتضمن مادة القانون المدني قسما خاصاً بالمعاملات المالية الإلكترونية و التجارة الالكترونية، ودراسة الجرائم المعلوماتية مع القسم الخاص لمادة قانون العقوبات ، وتدريس المحاكم الإلكترونية في مادة المرافعات و تدريس الحكومة الكترونية ضمن مادة القانون الإداري وإضافة موضوع النظام القانوني إلى مادة الحقوق العينية.

5- العمل على عقد المزيد من الندوات العلمية و المؤتمرات حول العلاقة بين المعلوماتية و القانون ، وتبني خطة واسعة للتدريب و رفع مستوى الكفاءة المعلوماتية في القطاع الوظيفي للدولة ، وتخصيص دورات تدريبية مكثفة ، للقضاة و رجال النيابة العامة لرفع مستوى الكفاءة لديهم في استخدام التقنية المعلوماتية.

6- على الدول العربية المضي في عقد اتفاقات دولية اقليمية و عربية للتعاون على مكافحة الجرائم المعلوماتية على المستوى التشريعي و التنسيق فيما بينها لتعاون أجهزة الشرطة لتبادل البيانات و المعلومات ، بل و المهارات اللازمة لملاحقة المتهمين بارتكاب الجريمة المعلوماتية.

ومن هنا نصل إلى نهاية البحث كي نسجل أن الآلة في مواجهة الانسان فإما **أن يفرض عليها إرادته، أو تطغى عليه صنيعته، و تفلت من سيطرته،**

قائمة المصادر

والمراجع.

قائمة المصادر:

*** القران الكريم**

القوانين:

1- القانون رقم 04/15 المؤرخ في العاشر من نوفمبر عام 2004 الموافق للسابع والعشرين من رمضان لسنة 1425 هجرية المعدل والمتمم للأمر رقم 156 - 66 المتضمن قانون العقوبات، جريدة اسمية مؤرخة في 10 نوفمبر 2004،

2- المادة الثانية من القانون رقم 04/09 المؤرخ في 2009/08/05 ،الجريدة الرسمية العدد 07 لـ 2009

3- القانون رقم 04 / 09 المؤرخ في 14 شعبان عام 1430 هـ الموافق ل 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها والذي أدخل حيز التنفيذ بموجب الجريدة الرسمية الصادرة بتاريخ 16 أوت 2009

المراسيم الرئاسية:

1- المرسوم الرئاسي رقم 07-375 المؤرخ في أول ديسمبر 2007 المتضمن التصديق على الاتفاق بين الحكومة الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، الموقع في الجزائر في 25 أكتوبر 2003 ، جريدة رسمية عدد 77 المؤرخة في 9 ديسمبر 2007، ففي المادة الأولى منه أشارت في الفقرة 10 منها على التعاون في مجال مكافحة الاحتيالات المرتبطة بتكنولوجيات الإعلام والاتصال الجديدة .

2- مرسوم رئاسي رقم 288 / 15 المؤرخ في 22 غشت 2015، جريدة رسمية عدد 45 مؤرخة في 23 غشت 2015

قائمةالمراجع:

_1- الجنيهي، منير محمد، و الجنيهي، ممدوح (2006) ، جرائم الإنترنت و الحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي ،الإسكندرية.

2- رستم، هشام محمد (1999)، جرائم الحاسب المستحدثة، دار الكتب القانونية ،

3- قشقوش، هدى حامد (1992)، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية ، القاهرة

4-العريان، محمد علي (2009)، الجرائم المعلوماتية، دار الجامعة الجديدة ، الإسكندرية

5-الشوا، سامي، (1993)، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية للقانون الجنائي ، القاهرة

6-عبد الله عبد الكريم (2011)، جرائم المعلوماتية و الإنترنت – الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت

7- د.احمد السيد عفيفي – الاحكام العامة للعلانية في قانون العقوبات - دراسة مقارنة - - 2001 – 2002– دار النهضة العربية، القاهرة .

8- أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة 1994.

9- د.جميل عبد الباقي الصغير – الانترنت و القانون الجنائي – دار النهضة العربية - 2001 .

10 - حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الاسكندرية مصر 1991 .

11- عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – القاهرة 2007 .

12-عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والانترنت – دار الكتب القانونية – القاهرة 2005.

13- فهد بن عبدالله اللحيدان، – الإنترنت، شبكة المعلومات العالمية - الطبعة الأولى- الناشر غير معروف - .1996

14- فتوح الشاذلي – القانون الدولي الجنائي – دار المطبوعات الجامعية – الاسكندرية – 2001 .

1-قادة امال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط 2، دار هومه، الجزائر، 2007.

15- مبدر سليمان لويس – أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية ، رسالة الدكتوراة – حقوق القاهرة.

16- محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004.

17- محمد سامي الشوا ثورة المعلومات وبعكسها على قانون العقوبات دار النهضة العربية القاهرة 1994.

18- محمد عبد الطاهر حسين – المسئولية القانونية في مجال شبكات الانترنت - 2002 – دار النهضة العربية – القاهرة .

19- محمد حسن منصور – المسؤولون الالكترونين – دار الجامعة – للنشر – الاسكندرية 2003 .

20- محمود نجيب حسني – شرح قانون العقوبات – القسم الخاص – الجرائم المضرة بالمصلحة العامة – دار النهضة العربية - القاهرة.

21- مدحت رمضان – جرائم الاعتداء على الاشخاص و الانترنت – دار النهضة العربية – القاهرة – 2000 .

22- ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية القاهرة 1983 .

23- منير الجنبيهي – ممدوح الجنبيهي – البنوك الالكترونية ط 2 – 2006 دار الفكر الجامعي – الإسكندرية .

24- د.هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة،أسيوط،1992.

25- صليحة علي صداقة، الأبعاد القانوني والأخلاقي للمعلوماتية . الصحية، دار المطبوعات الجامعية الإسكندرية

26-1 غادة نصار، الارهاب والجريمة الالكترونية، ط 1، العربي للنشر والتوزيع، د ب ن، 2017، ص163.

المقالات:

1. إبراهيم رمضان إبراهيم عطايا ، الجريمة الإلكترونية وسبل مواجهتها فـــي الشريعة الإسلامية والأنظمة الدولية كلية الشريعة و القانون بطنطا، الاردن، 2014.
2. ذياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدوليية، ورقة علمية بعنوان الجرائم الالكترونية: المفهوم والاسباب، الملتقى العلمي في الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، خلال الفترة من 02 الى 0 سبتمبر 201، الاردن

3. عبد الحميد ابراهيم، العلاقة بين الإرهاب المعلوماتي و الجرائم المنظمة، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية خلال الفترة. من 24 9 مارس 1222 بالقنطيرة بالمغرب.

4. محمد لمين دباغين سطيف 2 الجزائر. كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017.

5. مقالات ذات صلة الإصدارات الـ 9كلها (COHEN AND FELDON)

المواقع الالكترونية:

1. https://www.nw3c.org/
2. https://drive.google.com/file/d/0B7Xzn6q9WBfsbGxHXzNBb080Umc/view?usp=sharing
3. WWW.UNODC.COM

المراجع الاجنبية:

1- David Bainbridge- Introduction to computer law-third edition- Pit Man publishing1996

2- Chriss Reed, Internet Law- 2004 - CAMPRIDGE UNIVERCITY PRESS

ملحق رقم (01):جدول فيديوهات الشبكة المظلمة

نوع الفيديو	عدد الفيديوهات	الحجم(BM)	مدة التشغيل(hh:mm:ss)
وثائقي	291	2376.91	35:15:31
هجوم إنتحاري	22	122.85	02:09:13
قطع رأس(beheading)	70	294.95	04:44:03
أخذ الرهائن	26	172.8	02:24:13
جزية(tribute)	13	128.69	02:49:40
رسالة	126	1293.91	44:60:48
دعاية	143	1566:98	23:42:19
تعليمات	1	16.72	00:08:24
تدريب	9	196.49	03:20:12
نشرة إخبارية	5	533.54	02:36:30
المجموع	7006	6723.83	122:06:53
المتوسم	حجم الملف	مدة التشغيل	معدل البث
	9.5MB	10.23	247.3KBPS

المصدر : (salem, reid, and chen, 2008, **p.611**) (موثق في البداية ، 2013.)

جدول الاشكال:

الرقم	الشكل	الصفحة
01	أسباب الجريمة الإلكترونية وفق مستوى التحليل	18
02	نظرية الفرصة	22
03	تصور لبعض أسباب الجريمة الإلكترونية في الفضاء التخيلي	26

فهرس

المحتويات

المحتويات

المبحث الأول: تعريف الجريمة الإلكترونية: 9

المطلب الأول : المعنى الإصطلاحي واللغوي للجريمة الإلكترونية: 9

المطلب الثاني : الطبيعة القانونية للجريمة الإلكترونية: 12

المطلب الثالث: أسباب الجريمة الإلكترونية: 18

المبحث الثاني : الإطار القانوني للجريمة الإلكترونية. 35

المطلب الأول: أركان الجريمة المعلوماتية: 36

الفرع الأول: تعريف نظام المعالجة الآلية للمعطيات : 36

الفرع الثاني: الحماية الفنية لأنظمة المعالجة الآلية للمعطيات: 37

المطلب الثاني: الأركان الأساسية للجريمة المعلوماتية: 40

الفرع الأول: الركن المادي: 40

الفرع الثاني: الركن المعنوي: 46

المطلب الثالث: خصائص الجريمة الإلكترونية: 50

الفصل الثاني: الاحكام الاجرائية للجريمة الإلكترونية: 57

المبحث الأول: ضبط الجريمة المعلوماتية و اثباتها:.....59

المطلب الأول: حجية المخرجات الاليكترونية في الاثبات: 60

المطلب الثاني : الخبرة و المعاينة في الجرائم المعلوماتية 63

المبحث الثاني: الاختصاص بنظر الجريمة الالكترونية 69

المطلب الأول: لامركزية الفضاء و عالمية الجريمة الالكترونية. 69

المطلب الثاني: التعاون الدولي لملاحقة الجرائم المعلوماتية: 71

خاتمة الموضوع:.....76

قائمة المصادر و المراجع: 83

فهرس المحتويات: 90

ملخص:

يشكل موضوع الحماية الجزائية للمعلومات عبر شبكة الانترنت هاجسا أمنيا حقيقيا على مستوى الأفراد والجماعات، الأمر الذي يحتم اعادة النظر في صياغة مفهوم ملم بجميع جوانب هده الظاهرة، انطلاقا من الأنماط المستحدثة عبر الشبكة العنكبوتية التي تهدف بالأساس الى الاضرار بالممتلكات والأشخاص متجاوزة الحدود الجغرافية للدولة، مما يستدعي داسة معمقة ومواكبة لسرعة انتشار الجريمة الالكترونية ومجالات تطبيقها في شقيها القانوني والاجرائي، وكذا توحيد جهود الحكومات والمنظمات الدولية لحل المشاكل القانونية التي تثيرها هذه الجرائم من حيث المسؤولية الجنائية خاصة ما تعلق بإنشاء هيكلة ادارية، وضبطية قضائية تربط كافة المؤسسات القضائية بقواعد بيانات قانونية لتوفير امكانية رفع مستويات الكفاءة عند رجال القانون، الأمر الدي يتزامن مع انتقال الجريمة الالكترونية من طابعها التقليدي الى طابع يهدد أمن و سيادة واستقرار الدول.

Abstract:

The issue of penal protection of information via the Internet is a real security concern at the level of individuals and COMMUNITIES, which necessitates reviewing the formulation of a concept familiar with all aspects of this phenomenon, starting from the patterns developed through the web that mainly aim to harm property and people beyond the geographical borders of the state, which it calls for an in-depth pedagogy and keeping pace with the rapid spread of electronic crime and its areas of application in its legal and procedural aspects, as well as uniting the efforts of governments and international organizations to solve the legal problems raised by these crimes in terms of criminal responsibility, especially those related to establishing an administrative structure, and judicial seizure linking all judicial institutions with legal databases to provide the possibility Raising the levels of competence of lawmen , which coincides with the transmission of electronic crime from its tradition al nature to one that threatens the security, sovereignty, and stability of states.