جامعة مولود معمري – تيزي وزو -
كلية الحقوق والعلوم السياسية
قسم القانون – نظام ل.م.د

الجريمة الإلكترونية واقع وتحدي

مذكرة لنيل شهادة المـــاستر في القانون

تخصص قانون جنائي وعلوم إجرامية

إعداد الطّالبتين:
رزيق ليلة
رمضاني حميدة

إشراف الأستاذ:
أ/ لملوم كريم

لجنة المناقشة:

** الدكتور " نسير رفيق"أستاذ بجامعة مولود معمري تيزي وزو.....رئيسا
** أستاذ "لملوم كريم" أستاذ مساعد(أ)،جامعة مولود معمري،تيزي وزو .....مشرفا ومقررا
** أستاذ "خريمش مصطفى"أستاذ مساعد (أ)،جامعة مولود معمري تيزي وزو.....ممتحنا

تاريخ المناقشة: 2018/07/ 09

بسم الله الرحمان الرحيم

﴿و ما أوتيتم من العلم إلا قليلا﴾

(سورة الإسراء ، الآية 85)

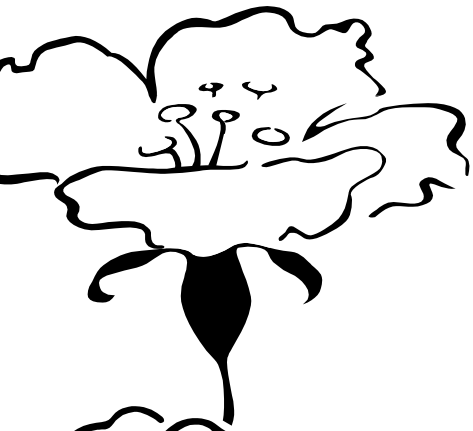
كلمة شكر

نشكر الله سبحانه وتعالى على فضله أن يسر لنا إتمام هذه المذكرة .

اعترافا بالفضل والجميل نتوجه بخالص الشكر والإمتنان مع كل احترامنا للأستاذ لملوم كريم الذي تفضل بالإشراف على هذا العمل وتابعه في جميع مراحل إنجازه

فجزاه الله عنا كل الخير

*ليلة حميدة



إهـداء

الى من تذرف الدموع لذكراه ويشتاق القلب الى رؤياه ،منبع الفخر والاعتزاز
الذي أنار لي دربي ووهب لي حياة الأمان والرفاهية والتي حرم منها وشجعني على الدراسة
صاحب البسمة والقلب الطاهر اغلى شخص في الوجود
والذي أتمنى ان تخلد روحه الطاهرة في جنان الرحمان أبي الحبيب رحمه الله
الى منبع الحنان والطيبة التي كانت مدرسة ومعلمة في ان واحد
التي أفادتني بتوجيهاتها ونصائحها القيمة أمي الغالية أطال الله في عمرها
الى كل عائلة أبي وأمي
الى كل إخوتي وأخواتي وعائلاتهم
إلى من كان صديقا وأخا وسندا لي في حياتي رفيق العمر نصر الدين وعائلته الكريمة
الى ياسمينة التي لطالما وقفت بجانبي في كل لحظات حياتي أختي العزيزة
الى زميلتي في اعداد هذا العمل المتواضع ليلة
الشكر الجزيل لله عز وجل الذي سهل لنا طريق العلم وبذكره تطمئن القلوب

حميدة

إهداء

الى أرواح جدي وجدتي رحمهما الله
الى من أنار دربي ووهب لي الامان وشجعني على الدراسة أبي العزيز
الى منبع الحنان وأطيب قلب واغلى كيان امي الغالية
إلى القلوب الطاهرة والرقيقة والنفوس البريئة إخوتي (كمال ، حكيمة جميلة،علجية،نورية)
الى جميع أفراد عائلة ابي وعائلة امي
الى أغلى شخص لدي والذي لطالما كان سندا لي منذ الصغرخالي صالح
الى اساتذتي الكرام فمنهم استقيت الحروف وتعلمت كيف انطق الكلمات واصوغ العبارات
الى صديقاتي ججيقة ، نورة،سلوى ،آنية،رشيدة،صبرينة،سامية،ليندة،لبنى،نعيمة
الى زميلاتي في العمل:الاساتذة حاج أعراب باهية ،علجية،ليلة،سعاد،حميدة
الى زميلتي في اعداد هذه المذكرة رمضاني حميدة
الى اعزشخص لدي رفيق دربي مزيان
اهدي هذا العمل المتواضع داعية المولى عز وجل ان تكلل بالنجاح والقبول من طرف اعضاء لجنة المناقشة المبجلين

ليلة

ليلة

قائمة المختصرات بالغة العربية:

ص: .....صفحة
ص.ص:..... من صفحة الى صفحة
د.ت.ن:..... دون تاريخ النشر
ج.ر: .....الجريدة رسمية للجمهورية الجزائرية الديمقراطية الشعبية
ع: .....عدد
ق.ع.ج:..... قانون العقوبات الجزائري
ق.إ.ج.ج:..... قانون الاجراءات الجزائية الجزائري

قائمة المختصرات باللغة الفرنسية

P :……page
OP.CIT……..……ouvrage précédemment cité
PP……..……du page à page

مقدمة:

تعتبر القوانين مرآة المجتمع و مقياس الحضارة و رقي الدولة، فبقدر ما تكون متطورة، بقدر ما تحقق الغايات التي وجدت لأجلها و قد رافق التطور الكبير الذي شهده العالم في الآونة الأخيرة، تطورات في مختلف جوانب الحياة في المجتمع لاسيما من الناحية التكنولوجية.

في ظل اتساع ثورة تقنية المعلومات والاتصالات وتأثيرها في كافة شؤون الحياة المختلفة، لما لها من فائدة وأهمية مادية ومعنوية في توفير الوقت والجهد وسرعة وسهولة نقل المعلومات وتبادلها وتخزينها ، والتي جعلت من العالم قرية صغيرة ،وانتشرت بشكل واسع في مختلف أنحاء العالم،لقد أثبت واقع الحال ان أهمية هذه الثورة ،ومنها شبكة المعلومات الدولية (World Wide Web) والاستخدام المتزايد لمواقع التواصل الاجتماعي مثل موقع (facebook) وموقع (Twitter) من الأمور المهمة في الحياة وأداة مساعدة وفاعلة في تطوير وتنمية استراتيجيات المؤسسات العامة و الخاصة والأفراد وتمكنهم من التقدم ،لذا كانت الدول المتقدمة أولى بالاستفادة منها وأصبح من الصعوبة الاستغناء عنها.

ورغم هذه الايجابيات التي وفرتها شبكة الانترنيت، إلا أنها أفرزت نوع جديد من الجرائم ألا وهي الجريمة الالكترونية والتي تعد تطور للجريمة التقليدية تدخل في ارتكابها وسائل تكنولوجية، فهي ظاهرة إجرامية مستجدة نسبيا ،بحيث تعاني المجتمعات في الآونة الأخيرة من انتهاك للحقوق والخصوصيات الالكترونية ، وجاء تطور 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 .

وبتنامي معدلات الجريمة وتطور أشكالها وتهديدها المباشر لحياة الأشخاص وأمن الدول قد دق ناقوس الخطر في مجتمعات العصر الراهن نظرا لحجم المخاطر وهول الخسائر الناجمة عن هذه الجرائم التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة.

فالجريمة الالكترونية جريمة تقنية تنشأ في الخفاء وتظهر مدى خطورتها في الاعتداءات التي تمس الحياة الخاصة للأفراد وتهدد الأمن والسيادة الوطنيين وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري.

أصبح 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 مليا للحد من هذه الجرائم من خلال التوعية والوسائل الوقائية الأمنية و غيرها، بحيث بات لزاما ان يواكب تطور الجريمة و أساليبها تطورا في مجال السياسة التشريعية عموما و الساسة الجنائية على وجه الخصوص.

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

تتجلى أهمية هذا البحث في كون هذا النوع المستجد من الإجرام مرتبط بالتقنية الحديثة المتمثلة في الحاسب الآلي وشبكة الانترنيت كما سبق ذكره والتي هي في تطور دائم مما يفرض على المشرعين لمختلف الدول مواكبة هذه الظاهرة مع إيجاد الحلول التشريعية لمكافحتها وعدم الاكتفاء بالنصوص التقليدية التي أضحت عاجزة سواء من الناحية الموضوعية باعتبار ان الجريمة الالكترونية تمس حقوقا غير مادية (المعلومات، البيانات ، التجارة الالكترونية....) أو من الناحية الإجرائية وما تثيره من صعوبات وتتمحور حول إثبات الجريمة أو القانون الواجب التطبيق أو المحكمة المختصة في نظر هذه الجريمة وكذا حتمية التعاون الدولي في هذا المجال.

من خلال ما سبق تبيانه من أهمية لموضوع الجريمة الالكترونية يمكن أن نتوصل إلى طرح الإشكالية التالية:

ما مدى فعالية النصوص القانونية في مكافحة الجريمة الالكترونية؟

ومن أجل الإجابة على هذه الإشكالية قمنا بتقسيم بحثنا إلى فصلين تطرقنا إلى الأحكام العامة للجريمة الالكترونية(الفصل الأول)،ثم مكافحة الجريمة الالكترونية (الفصل الثاني)

الفصل الأوّل
الأحكام العامة للجريمة الالكترونية

ظهر الحاسب الآلي نتيجة للتطور العلمي والتقدم التقني، الذي أدى إلى تدخل أنظمة المعالجة الآلية للمعلومات في كافة مجالات الحياة اليومية ، نظرا لما يتمتع به الحاسب من قدرة فائقة على تخزين أكبر قدر من البيانات والمعلومات .

عرفت الانترنيت رواجا كوسيلة للاتصالات واستعمالها في كل المعاملات اليومية ظهور سلبيات عديدة،خاصة بعد استغلال الكثير من المجرمين هذا التغير في نمط المعاملات مما أسفر إلى ظهور جرائم لم يكن يعرفها القانون من قبل.

فإذا كانت الجرائم التقليدية قد نالت جانبا من الاعتناء وذلك بتحديد مختلف المفاهيم والتعاريف الخاصة بها ، إضافة إلى طرق مكافحتها ، فإن الجريمة الالكترونية لا تزال محل البحث من طرف الفقهاء والقانونيين ، وذلك نظرا للطبيعة الخاصة التي تنفرد بها.

فقبل الدخول إلى مختلف الاشكالات التي أثيرت في خصوص هذا الموضوع، سنتطرق في هذا الفصل إلى مفهوم الجريمة الالكترونية (المبحث الأول) و صور الجريمة الالكترونية (المبحث الثاني).

المبحث الأول
مفهوم الجريمة الالكترونية

لقد ترتّب على الاستخدام المتزايد لوسائل التكنولوجيا ظهور ما يعرف بالجريمة الإلكترونية و استخدمت عدة مصطلحات للدلالة على هذه الظاهرة الإجرامية فهناك من يطلق عليها الغش المعلوماتي وهناك من يطلق عليها اسم جرائم الكمبيوتر أو الجريمة الالكترونية.

إن الجريمة الالكترونية جريمة مستحدثة يعتمد مرتكبها على وسائل تقنية و يكون ذا دراية كافية باستخدام الأنظمة المعلوماتية، لذلك فإن الإحاطة بمفهومها الدقيق لا يزال محل خلاف فقهي، فهي كما سبق الذكر ظاهرة إجرامية مستحدثة تتميز عن الجريمة التقليدية، و تختلف عنها من حيث المفهوم، و لإزالة اللبس سنتناول في هذا المبحث التعاريف الفقهية للجريمة الالكترونية (المطلب الأول) و خصائص و أركان الجريمة الالكترونية(المطلب الثاني).

المطلب الأوّل
تعاريف الجـريـــمة الالكترونيــة

لقد تعددت التعريفات التي تناولت الجريمة الإلكترونية و يرجع ذلك إلى الخلاف الذي أثير بشأن تعريفها، فالجريمة الالكترونية صنف جديد من الجرائم، بحيث مع ظهور ثورة المعلومات و الاتصالات ظهر معها نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى الصورة الالكترونية التي يصعب التعامل معها. فنجد التعاريف الفقهية (الفرع الأول) و تعريفها على ضوء الاتفاقيات الدولية (الفرع الثاني)، و تعريفها في نظر المشرع الجزائري (الفرع الثالث).

الفرع الأوّل
التعاريف الفقهية للجريمة الالكترونية

على الرغم من تنامي جهود التصدي لظاهرة الجريمة الالكترونية إلّا أنه لا يوجد تعريف محدد و متفق عليه بين الفقهاء، فقد ذهب جانب من الفقه إلى تعريفها على نحو ضيق و جانب آخر عرّفها على نحو موسّع.

أوّلا/ التعريف الضيق:

يعرف الفقيه الفرنسي ماس Masse[1] الجريمة الالكترونية بأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح." و الجرائم الالكترونية لدى هذا الفقيه جرائم ضد الأموال، استخدم لهذا التعريف معيارين هما: الوسيلة، و تحقيق الربح المستمد من معيار محل الجريمة المتمثل في المال.

و يعرفها الفقيهان الفرنسيان Vivantو Lestant[2] بأنها "مجموعة من الأفعال المرتبطة بالمعلوماتية و التي يمكن أن تكون جديرة بالعقاب". فهذا التعريف مستند من بين معيارية على احتمال جدارة الفعل بالعقاب و هو معيار غير منضبط و لا يستقيم مع تعريف قانوني و إن كان يصلح هذا التعريف في نطاق علوم الاجتماع و غيرها.

أما الفقيه Merwe ذهب إلى أن الجريمة الالكترونية هي "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي- أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية."

كما عرفها الفقيه Rosblat[3] بأنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب و إلى تحويل طريقه."

و عرفها (كلاوس تايدومان) بأنها "كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلي."

و يدخل في نطاق تعريفات الجريمة الالكترونية الضيقة تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرّف الجريمة الالكترونية من خلال تحديد مفهوم جريمة الحاسب بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج دورا رئيسيا.

[1]-محمد أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة ، الأردن، 2005، ص17.

[2]- لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة التخرج لنيل شهادة الماستر ،جامعة أكلي محند اولحاج، البويرة، 2016، ص 7.

[3] -محمد أحمد عبابنة، ، المرجع السابق، ص ص15-16.

ثانيا/ التعريف الموسع للجريمة المعلوماتية:

ذهب الفقيهان Michel وCredo[1] إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة، هذا بالإضافة إلى الحالات المتعلقة بالولوج[2] غير المصرح به لحاسب المجني عليه أو بياناته. كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، و انتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق الكترونية و تزييف المكونات المادية و المعنوية للحاسب، بل و سرقة الحاسب في حد ذاته و أي من مكوناته.

و ذهب رأي آخر من الفقه إلى تعريف الجريمة الالكترونية بأنها عمل أو امتناع يأتيه الإنسان، إضرارا بمكونات الحاسب و شبكات الاتصال الخاصة به التي يحميها قانون العقوبات و يفرض لها عقاب.

و يرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها "كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر."

و يعرفها Ticolement بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب."[3]

و يعرفها David Tompson بأنها جريمة يكون متطلبا لاقترافها أن يتوفر لدى فاعلها معرفة تقنية الحاسب.

و الدكتور هلالي عبد الله أحمد يرى أنها "عمل أو امتناع يأتيه إضرارا بمكونات الحاسب و شبكات الاتصال الخاصة به، التي يحميها قانون العقوبات و يفرض له عقابا."

الفرع الثاني

تعريف الجريمة الالكترونية على ضوء الاتفاقيات الدولية

يعرف خبراء منظمة التعاون الاقتصادي و التنمية جريمة الكمبيوتر بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات، أو نقلها[4]. و يتبنى هذا التعريف الفقيه الألمانيVirich Siehr يعتمد هذا التعريف على معيارين هما: وصف السلوك، و اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

[1]- لعاقل فريال، المرجع السابق، ص ص 9-10.

[2] -محمد أمين أحمد الشوابكة، جرائم الحاسوب و الانترنيت، الجريمة المعلوماتية، دار الثقافة، عمان، 2004، ص9.

[3]-مليكة عطوي، "الجريمة المعلوماتية"، حوليات جامعة الجزائر، عدد 21، 2012، ص13.

[4] - رابحي أحسن، "الجريمة الالكترونية: النقطة المظلمة"، بالنسبة للتكنولوجيا المعلوماتية"، المجلة الجزائرية للعلوم القانونية الاقتصادية السياسية، عدد 01، 2011، ص227.

كما عرّف جريمة الكمبيوتر خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي و التنمية OECD بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية."

قدمت المادة الأولى من الاتفاقية الدولية للإجرام المعلوماتي تعريف للنظام المعلوماتي على النحو التالي: "يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات صلة بذلك، 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".

عرف المؤتمر العاشر للأمم المتحدة لمنع الجريمة و معاقبة المجرمين الجريمة الالكترونية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب و تشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية.[1]

كذلك عرفتها اتفاقية بودابست في المادة الأولى منها بعنوان تعريف خاص بأغراض هذه الاتفاقية منظومة معلوماتية و معطيات معلوماتية.

أ- **منظومة معلوماتية**: أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها أو ذات صلة بذلك، و يقوم أحدها أو أكثر من واحد منها تتبعا للبرنامج بعمل معالج آلية للمعطيات.

ب- معطيات معلوماتية: أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل معين جاهز لعملية المعالجة داخل منظومة معلوماتية بما في ذلك البرامج الماسة لجعل منظومة معلوماتية تطبق[2] وظيفة

يذهب بعض الفقهاء إلى أنه عند وضع تعريف محدّد للجريمة الالكترونية يجب مراعاة عدة اعتبارات مهمة منها:

1- أن يكون هذا التعريف مقبول و مفهوم على المستوى العالمي.
2- أن يكون هذا التعريف التطور السريع و المتلاحق في تكنولوجيا المعلومات.
3- أن يحدّد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي.
4- أن يفرق هذا التعريف بين الجريمة العادية و الجريمة الالكترونية و ذلك عن طريق إيضاح الخصائص المميزة للجريمة الالكترونية.

الفرع الثالث

[1]-عقد هذا المؤتمر في الفترة ما بين (17-10) أفريل 2000.

[2]- الاتفاقية الدولية حول الإجرام السيبيري التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي و تم وضعها للتوقيع بتاريخ 2001/11/23. وقعت عليها 30 دولة و لأهمية هذه الاتفاقية، انضم إليها العديد من الدول من خارج المجلس الأوربي، و أبرزها الو م أ التي صادقت عليها في 22 سبتمبر 2006، و دخلت حيز النفاذ في 2007/01/01 و اشتملت على عدة جوانب من جرائم الانترنيت، بينها الإرهاب و عمليات تزوير بطاقات الائتمان و دعارة الأطفال.

تعريف الجريمة الالكترونية في نظر المشرع الجزائري

لقد تطرق المشرع الجزائري على غرار الدول الأخرى مثل فرنسا إلى تجريم أفعال المساس بأنظمة الحاسب الآلي و ذلك نتيجة تأثر الجزائر بما أفرزته الثورة الالكترونية من أشكال جديدة من الجرائم التي لم تشهدها البشرية من قبل، ممّا دفع بالمشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون 15/04 المؤرخ في 10-11-2004 المتضمن تعديل قانون العقوبات و لكن المشرع تناول في النصوص المستحدثة الاعتداءات الماسة بالأنظمة المعلوماتية و أغفل الاعتداءات الماسة بمنتجات الإعلام الآلي و سنبين بصفة موجزة الأفعال التي جرّمها المشرع الجزائري بموجب القانون السابق الذكر:[1]

1-جريمة التوصل أو الدخول غير المصرح به:

نصت عليها المادة 394[2] مكرر من قانون العقوبات بقولها "يعاقب بالحبس و الغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك. و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة". فلقد أورد المشرع ظرفي تشديد لعقوبة الدخول غير المشروع و هما: في حالة ما إذا ترتب عن الدخول غير المشروع حذف أو تغيير المعطيات، أو تخريب نظام اشتغال المنظومة، وقد نص المشرع في المادة المذكورة على تجريم فعل الشروع في جريمة الدخول غير المصرح به و ذلك بقوله "أو يحاول ذلك"

2-جريمة التزوير المعلوماتي:

نص عليها المشرع في نص المادة 394[3]مكرر1 من ق ع ج بقوله "يعاقب بالحبس و بالغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو زال أو عدل بطريق الغش المعطيات التي يتضمنها".

3- جريمة الاستيلاء على المعطيات:

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

4-جريمة إتلاف و تدمير المعطيات:

نص عليها المشرع الجزائري في المادة 394 مكرر1 من قانون العقوبات المذكورة سابقا و جريمة الإتلاف حسب المادة المذكورة تتمثل في إزالة معطيات نظام المعالجة الآلية عن طريق الفيروسات.

[1] - أشرف عبد القادر قنديل، الإثبات في الجريمة الالكترونية، دار الجامعة الجديدة ، الإسكندرية، 2015، ص ص 109-110.

[2]- القانون رقم 15/04 المؤرخ في 2004/11/10 المتضمن قانون العقوبات المعدّل و المتمم للأمر 156/66 المؤرخ في 08جوان 1966 المتضمن قانون العقوبات، عدد 71 بتاريخ 2004/11/10.

[3] - راجع المادة 394 مكرر 1 من القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدّل و المتمم للأمر 156/66 المؤرخ في 08جوان 1966 المتضمن قانون العقوبات، عدد 71 بتاريخ 2004/11/10.

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

المطلب الثاني

خصائص الجريمة الالكترونية و أركانها

تتسم الجريمة الالكترونية عن غيرها من الجرائم التقليدية بمجموعة خصائص ومميزات وتجعلها ذات بعد حديث يتطلب النظر فيها في العديد من الزوايا(الفرع الأول) والحديث عن الجريمة الالكترونية يقودنا إلى البحث في أركانها العامة وهي المنطوية على الركن الشرعي، المادي و المعنوي(الفرع الثاني).

الفرع الأول

خصائص الجريمة الالكتروني

تعد الجريمة الالكترونية من أبرز أنواع الجرائم الحديثة ، ناعمة التنفيذ ، صعبة الاكتشاف وصعبة الإثبات وهذا ما سنوضحه فيما يلي:

أولا : الجريمة الالكترونية جريمة حديثة:

تتسم الجريمة الالكترونية بأنها من أبرز أنواع الجرائم الحديثة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة سواء التي تتعرض أجهزة الكمبيوتر أو تلك التي تسخر تلك الأجهزة لارتكابها.

حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية، جعل العالم قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته و إمكانياته أجهزة الدولة الرقابية، بل أنه يضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها و أمن مواطنيها. بالإضافة إلى ظهور أنواع أخرى من الجرائم غير التقليدية، نتيجة للثورة المعلوماتية كسرقة الملكيات الفكرية، الاتجار غير المشروع في الأسلحة، غسيل الأموال...إلخ

ثانيا/ الجريمة الإلكترونية ناعمة التنفيذ:

تتميز الجريمة الإلكترونية بكونها هادئة بطبيعتها لا تحتاج إلى العنف، فكل ما [2] تحتاج إليه هو القدرة على التعامل مع الجهاز المستخدم بمستوى تقني و تحتاج إلى شبكة الانترنيت، مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة. و من هذا المنطلق تعتبر الجريمة الالكترونية من الجرائم النظيفة التي لا تترك أثرا و لا عنفا، و إنما مجرد أرقام و بيانات يتم تغييرها من السجلات المخزنة في ذاكرة الكمبيوتر و ليس لها أثر خارجي مادي ملموس.

1 أ/زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي، دار الهدى ، عين مليلة، الجزائر، 2011، ص56.

2- صغير يوسف ،الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون ، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو،كلية الحقوق والعلوم السياسية، 2013،ص16.

ثالثا/ الجريمة الإلكترونية صعبة الاكتشاف:

نتيجة للخاصية السابقة، تتميز الجريمة الإلكترونية بأنها صعبة الاكتشاف، و إن تحقق الاكتشاف فلا يكون إلّا صدفة. الأمر الذي يمكن رده إلى عدّة أسباب لعل أهمها عدم ترك هذه الجريمة لأي أثر مرئي، كما أن الجاني يمكنه ارتكابها في دول و قارات أخرى، كما أنها تتميز بسهولة تدمير دليل الإدانة في أقل من ثانية. و الجرائم الالكترونية خفية لا يلاحظها المجني عليه، بحيث يمكن إخفاء السلوك عن طريق التلاعب غير المرئي في الذبذبات الالكترونية التي تسجل البيانات.[1]

كما أن المجني عليه يلعب دورا رئيسيا في صعوبة اكتشاف الجريمة، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية لخسائر فادحة، على عدم الكشف حتى بين موظفيها عما تعرضت له، و عدم إبلاغ السلطات المختصة تجنبا للإضرار بسمعتها و مكانتها، بالإضافة إلى أن المجني عليه يتردد أحيانا في الإبلاغ عن هذه الجرائم، خوفا من الكشف عن أسلوب ارتكابها، الذي قد يؤدي إلى تكرار وقوعها بناءا على تقليدها من قبل الآخرين.

رابعا/ الجريمة الإلكترونية صعبة الإثبات:

إن صعوبة اكتشاف الجريمة الالكترونية يؤدي إلى صعوبة إثباتها[2]، حيث أن اكتشاف الجرائم الالكترونية أمر صعب، لكن حتى في حال اكتشافها و الإبلاغ عنها فإن إثباتها تحيطه الكثير من الصعوبات، خاصة و أن الجريمة الالكترونية تقع خارج الإطار المادي الملموس، و تقدم أركانها في بيئة افتراضية مما يعقّد الأمور على سلطات الأمن و الأجهزة القضائية.

تجدر الإشارة إلى أن الوسائل التقليدية لا تفلح غالبا في إثبات الجريمة الالكترونية نظرا لطبيعتها الخاصة، بالإضافة إلى نقص الخبرة الفنية و التقنية لدى أفراد الشرطة و جهات القضاء، ممّا يشكل عائقا أساسيا أمام إثبات هذه الجريمة. فهذه الأخيرة تتطلب تدريب و تأهيل هذه الجهات في مجال تقنية المعلومات و كيفية جمع الأدلة و التفتيش في بيئة الانترنيت، و نتيجة لنقص الخبرة كثيرا ما تخفق أجهزة الشرطة في البحث و التحري بخصوص هذا النوع من الجريمة، الأمر الذي يتطلب نوع من التخصص التقني لتحصين الجهاز الأمني و القضائي ضد هذه الجريمة.[3]

الفرع الثاني
أركان الجريمة الالكترونية

[1]- نهلا عبد القادر المومني، الجرائم المعلوماتية،الطبعة الثانية ، دار الثقافة، الأردن،2010،ص ص50-51.

[2] -محمد أحمد عبابنة، المرجع السابق، ص37.

[2] - مدونة الجرائم الالكترونية وأمن المعلومات،خصائص جرائم الانترنيت ، د ت ن، الرابط:
http://ecis-eg.blogspot.com/2015/04/internet-crimesproperties.html.

لقيام الجريمة الالكترونية لابد من توافر الركن الشرعي ، الركن المادي والركن المعنوي وهذا ما سنطرحه فيما يلي:

أولا/ الركن الشرعي:

فالركن الشرعي عامة يعرف على أنه: "عدم إمكانية متابعة أي شخص جزائيا إلّا إذا ما وجد نص صريح يجرم السلوك المرتكب قبل ارتكابه". الأمر الذي من خلاله تنتج مجموعة أحكام أساسية تحمل الصفة الإلزامية و لا مجال للتخلي عنها و المتمثلة في انفراد التشريع بالتجريم،حظر التفسير الواسع للنص الجنائي الموضوعي، حظر القياس في المسائل الجنائية، و عدم رجعية النص الجنائي إلا ما كان منه أقل شدة.[1]

فانطلاقا من نتائج مبدأ الشرعية الموضحة سابقا، يرى الفقه أن الانترنيت خلقت العديد من الإشكالات، فلا يمكن تطبيق نص جنائي تقليدي شرع في زمن لم تعرف فيه الانترنيت على سلوكات ارتكبت باستعمالها، مثل سب شخص على موقع شبكي، بالإضافة إلى التطور الرهيب و السريع للانترنيت الذي يقابله عادة البطء التشريعي...إلخ.

ثانيا/ الركن المادي:

ينطلق مبدأ تحديد الفعل غير المشروع و إعطائه صفة الجريمة بتحديد الركن المادي فيه. فلا جريمة دون ركن مادي، الذي يتمثل في السلوك الذي يقوم به الجاني من أجل تحقيق غاية ما و يحدّد له القانون العقاب اللازم و هو يتباين بتباين الجرائم المرتكبة من قبل الجاني، بشرط أن يكون له مظهر خارجي ملموس، غير أن تحديد الركن المادي في الجرائم الواقعة عبر الشبكة العالمية للانترنيت تكتنفه العديد من الصعوبات خاصة فيما يتعلق بتحديد النتيجة الإجرامية و الرابطة السببية و هذا ما نبينه فيما يلي:

النشاط أو السلوك المادي في الجريمة الإلكترونية يتطلب وجود بيئة رقمية و اتصال بالانترنيت و يتطلب أيضا معرفة بداية هذا النشاط و الشروع فيه و نتيجته. فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، و كذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها أشياء أو صور مخلة بالآداب العامة و تحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد فيروسات تمهيدا لبثها.

يتمثل النشاط المادي في الجريمة الالكترونية في الدخول غير المشروع في نظم و قواعد معالجة البيانات سواء ترتب عن هذا الدخول غير المشروع تلاعب بهذه البيانات أم لا. إذ أن مجرّد الدخول غير المشروع لمواقع المعلومات و البرامج جريمة مرتكبة عبر الانترنيت، و قد يتخذ هذا النشاط الإجرامي عدة صور كانتهاك السرية و خصوصية البيانات الشخصية و الإضرار بصاحبها و الإطلاع على المراسلات الالكترونية[2]، و الإدلاء بالبيانات الكاذبة في إطار المعاملات و العمليات الالكترونية.

[1] - راجع المادة 02 من القانون رقم 15/04 المؤرخ في 2004/11/10 المعدّل و المتمّم للأمر 156/66 المؤرخ في 08 جوان 1966 المتضمن: قانون العقوبات (ج ر عدد 71 بتاريخ 2004/11/10).

[2] - زبيحة زيدان ،المرجع السابق،ص73.

[2] - أحسن بوسقيعة،الوجيز في القانون الجزائي العام، الطبعة الثانية ، دار هومة ،الجزائر،2013،ص126 .

فخلاصة القول أن السلوك الإجرامي في الجريمة الالكترونية يرتبط بالمعلومة المخزنة داخل الحاسب الآلي أو انتهاك حرمة الأشخاص، و السلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب الآلي فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك مثلا.

أما مسألة النتيجة الإجرامية في الجريمة الالكترونية تثير عدّة مشاكل، فهل تقتصر على العالم الافتراضي، أم أن لها جزءا في العالم المادي، و هل تتحقق النتيجة في مكان واحد أو تمتد لتشمل دولا و أقاليم عدة، فعلى سبيل المثال إذا قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم أحد البنوك في الإمارات، و هذا الخادم موجود في الصين، فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين[1].

كما أن مسألة تحديد رابطة السببية في مجال أضرار الانترنيت تعدّ من المسائل الصعبة و المعقدة بالنظر إلى تعقيدات صناعة الحاسوب و الانترنيت، و تطور إمكانياتهاو تسارع هذا التطور، إضافة إلى تعدّد و تنوع أساليب الاتصال بين الأجهزة الالكترونية و تعدد المراحل التي تمر بها الأوامر المدخلة حتى تخرج و تنفذ النتيجة المراد الحصول عليها، كل ذلك سيؤدي حتما إلى صعوبة تحديد السبب أو الأسباب الحقيقية للإساءات المرتكبة في هذه المسؤولية.

ثالثا/ الركن المعنوي:

يعتبر الركن المعنوي الحالة النفسية للجاني، و العلاقة التي تربط بين ماديات الجريمة و شخصية الجاني و يطلق عليه الركن الأدبي .

أما الركن المعنوي في الجرائم التقليدية فيتمثل في عناصر القصد الجنائي العلم و الإرادة[2] أي أن يكون الجاني على علم بالعناصر الأساسية لقيام الجريمة، و أن يكون غرضه هو تحقيق النتيجة الإجرامية.

أمّا الركن المعنوي في الجريمة الالكترونية يقوم على أساس مجسد في توافر الإرادة الآثمة لدى الفاعل، و توجيه هذه الإرادة إلى القيام بعمل غير مشروع جرّمه القانون، كسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الإجرامية المترتبة على الأفعال السابقة، فتكسب إرادة الجاني الصفة الإجرامية من العمل غير المشروع الذي له النية على ارتكابه، و هو عالم بالآثار الضارة الناشئة عنه.

فالركن المعنوي في الجريمة الالكترونية يتباين بتباين الباعث الذي يدفع الجاني لارتكاب أفعاله، فليس كل المجرمين عبر الانترنيت لهم نية في الإجرام. فبالرغم من أن هناك من المجرمين من يسعى لتحقيق أغراض مادية أو سياسية أو إيديولوجية إلّا أنه هناك من الأفراد من يقوم بأفعاله من أجل التعلم أو لمجرد التسلية في بعض الأحيان،

مما يجعل في هذه الحالة تحقق شرط القصد الجنائي منعدم و منه لا يتوافر الركن المعنوي في بعض الجرائم.[2]

---

[2] - صغير يوسف، المرجع السابق، ص71.

[2] – نائلة عادل محمد فريد قورة،جرائم الحاسب الآلي الاقتصادية ،دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية، 2005،ص49.

و الملاحظ على هذه الأفعال الإجرامية الالكترونية، و بالرغم من عدم توافر القصد الجنائي فيها، إلّا أنها تسبب أضرارا و خسائر فادحة للجهة المجني عليها (الضحية) تفوق أضرار الجريمة التقليدية، غير أن انتفاء القصد الجنائي يعفي الجاني من المسائلة و بالتالي يتم ضياع حقوق الضحية، و بالتالي يستحسن إيجاد سبيل للحد من هذه الصعوبة، و ذلك بمساءلة الجاني على أساس الضرر الذي ألحقه بالمجني عليه أو الاكتفاء بتوافر الركن المادي و الشرعي للجريمة[1].

المبحث الثاني
صور الجريمة الالكترونية

تعتبر الجريمة الالكترونية من الجرائم المستحدثة و هي تستهدف العديد من القطاعات، ممّا جعل تصنيفها من قبل الفقهاء يتميّز بالصعوبة على عكس الجرائم التقليدية التي يمكن تصنيفها بسهولة فائقة.

لم يستقر الفقهاء على معيار واحد لتصنيف الجريمة الالكترونية و ذلك لتشعب هذه الجرائم و سرعة تطوّرها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة أو دافع المجرم، أو على أساس محل الجريمة.

و على هذا الأساس نعتمد في تقسيم هذا المبحث على مختلف معايير التصنيف و هي الجرائم الواقعة على الأموال و الجرائم الواقعة على الأشخاص (المطلب الأول) ثم الجرائم الواقعة على أمن الدول (المطلب الثاني).

[1] - نائلة عادل محمد فريد قورة، المرجع السابق،ص368.

المطلب الأول
جرائم واقعة على الأموال و جرائم واقعة على الأشخاص

أصبحت معظم المعاملات التجارية تتم من خلال شبكة الانترنيت مثل البيع و الشراء، مما انجر عنه وسائل الدفع و الوفاء.و في خضم هذا التداول المالي عبر الانترنيت،انتهز بعض المجرمين الفرصة من أجل السطو عليها مرتكبين بذلك جرائم ضد الأموال(الفرع الأول)

إنّ الهدف الأوّل و الأسمى من وضع القوانين هو حماية سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرّضون لها سواء في أبدانهم أو في حياتهم الخاصة، أو في سمعتهم و شرفهم. تطور الأمر بعد ذلك مع ظهور شبكة الانترنيت التي أصبحت سلاحا فتاكًا في يد المجرمين يقترفون جرائم ضد الأشخاص (الفرع الثاني).

الفرع الأول
جرائم واقعة على الأموال

تتمثل في مختلف الجرائم التالية :

أولا/ جرائم السطو على أرقام بطاقات الائتمان و التحويل الالكتروني غير المشروع للأموال:

أدّى استخدام البطاقات الائتمانية من خلال شبكة الانترنيت إلى ظهور الكثير من المتسللين للسطو عليها باعتبارها نقود الكترونية، خاصة أنّ الاستيلاء على هذه البطاقات ليس بالأمر الصعب، بحيث أنّ لصوص هذه البطاقات يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنيت و من ثمّ بيع هذه المعلومات للآخرين[1].

تتم عملية التحويل الالكتروني غير المشروع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجنى عليه، ممّا يسمح للجاني بالتوغل في النظام المعلوماتي[1] و الخدمات على الشبكة عن طريق تصريح كتابي أو تلفوني، بخصم القيمة على حساب بطاقة الدفع الالكتروني الخاصة به، و تتم العملية بدخول العميل أو الزبون إلى موقع التاجر و يختار السلع المراد شرائها و يتم التعاقد بملأ النموذج الالكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري.

ثانيا/ القمارو تبييض الأموال عبر الانترنيت:

إنّ الفضاء السيبيرياني من أكثر الأسباب المشجعة على ممارسة القمار عبر الانترنيت مقارنة بممارستها على الكازينوهات في الواقع المادي، إذ يمنح الراغب في

[1]- البطاقة الائتمانية عبارة عن بطاقة بلاستيكية تصدر من قبل بنك أو مؤسسة لتقديم خدمات أو تسهيلات معينة على أن يقوم حامل البطاقة بتسديد المبالغ المستحقّة كلّيا أو جزئيا وفق نصوص العقد بين العميل (حامل البطاقة) أو المصرف أو المؤسسة المصدّرة للبطاقة، أنظر: الصديق محمد الأمين الضرير،"بطاقات الائتمان"، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة و القانون، جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، أيام 10-12 ماي 2003، ص637.

ممارسة القمار من خلال الكازينوهات الافتراضية، الخصوصية و إخفاء الشخصية التي يبحث عنها الكثيرون، بحيث يستطيع الشخص ممارسة القمار دون حتى أن يغادر غرفة نومه.

و كثيرا ما تتداخل عملية تبييض [1] الأموال مع ممارسة القمار عبر شبكة الانترنيت، الأمر الذي جعل مواقع الكازينوهات الافتراضية على الانترنيت محل اشتباه و مراقبة.

و من البديهي أن يأخذ المجرمون بأحدث ما توصلت إليه التقنية لخدمة أنشطتهم الإجرامية و يشمل بذلك بالطبع تبييض الأموال التي استفادت من عصر التقنية فلجأت إلى الانترنيت لتوسعة و تسريع أعمالها في تبييض أموالها غير المشروعة.

ثالثا/ جريمة السرقة و السطو على أموال البنوك:

تعرف السرقة بالمفهوم العام بأنها اختلاس شيء منقول مملوك للغير بدون رضاه بنية امتلاكه[2]. أما سرقة المال المعلوماتي-إن أمكن الوصف- تتم عن طريق اختلاس البيانات و المعلومات و الإفادة منها، باستخدام السارق المعلومات الشخصية، مثل الاسم، العنوان، الأرقام السرية الخاصة بالمجني عليهم، ليبدأ بها عملية السرقة المتخفية عبر الانترنيت بحيث تؤدي بالغير إلى تقديم الأموال الالكترونية إلى الجاني عن طريق التحويل البنكي.

تتجسّد جريمة السطو على أموال البنوك عن طريق استخدام الشخص الحاسب الآلي للدخول إلى شبكة الانترنيت و الوصول غير المشروع إلى البنوك و المصارف و المؤسسات المالية، و تحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى، و ذلك عن طريق إدخال بيانات غير حقيقية أو تعديل أو مسح البيانات الموجودة بقصد اختلاس الأموال أو نقلها أو إتلافها. و تتم عملية التحويل الالكتروني غير المشروع للأموال بأحد الطرق الموالية:

أ- الاحتيال:

يتم بطرق احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح، فيسلّم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال و هو يعلم أنّ ليس له صفة التصرف فيه، و قد يتخذ اسم أو صفة كاذبة تمكّنه من الاستيلاء على مال المجني عن طريق الشبكة أو يتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في إيهام الحاسب و الاحتيال عليه فيسلمه النظام المالي.[3]

ب-الاحتيال باستخدام بطاقات الدفع الالكتروني:

يقوم نظام بطاقة الدفع الالكتروني على عمليات التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدّر للبطاقة إلى رصيد التاجر أو الدائن الذي يوجد به حسابه و

[1]- محمد فتحي عيد، الاجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية.1999، ص298.

[2] -KELCI Seugi « Vol.Fraude et autres infractions semblables et internet », disponible sur le site : http//www.lex-electronica.org/articles/v12-1/kelci.pchf.

[3] - سجلت مصالح المديرية العامة للأمن الوطني المختصة في مكافحة الجريمة الالكترونية خلال 8أشهر من السنة الماضية 25قضية متعلقة بجرائم الاحتيال عبر الانترنيت، و تمّت معالجة 17 قضية، أين تورّط فيها 32 متورط، لتصل النسبة المئوية للقضايا المعالجة إلى 68%.

ذلك من خلال شبكة التسوية الالكترونية للهيئات الدولية "هيئة الفيزاكارد"، "هيئة الماستركارد" و تعطي بطاقة الدفع الالكتروني الحق للعميل بالحصول على السلع.

الفرع الثاني
جرائم واقعة على الأشخاص

إنّ الهدف الأوّل و الأسمى من وضع القوانين هو حماية سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرّضون لها سواء في أبدانهم أو في حياتهم الخاصة، أو في سمعتهم و شرفهم. تطور الأمر بعد ذلك مع ظهور شبكة الانترنيت التي أصبحت سلاحا فتاكًا في يد المجرمين و هذا ما سنوضحه فيما يلي:

أولًا/ جريمة التهديد و المضايقة و الملاحقة:

التهديد هو الوعيد بالشر، الذي يقصد به زرع الخوف في النفس بالضغط على إرادة الإنسان و تخويفه من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له به صلة.[1]

يعتبر تهديد الغير من خلال البريد الالكتروني واحد من أهم الاستخدامات غير المشروعة للانترنيت، حيث يقوم الفاعل بإرسال رسالة إلكترونية إلى المجني عليه تنطوي على عبارات تسبّب خوفا له.

تتم جرائم الملاحقة على شبكة الانترنيت غالبا باستخدام البريد الالكتروني أو وسائل الحوارات الآلية المختلفة على الشبكة، و تشمل الملاحقة وسائل تخويف و مضايقة تتفق مع مثيلاتها خارج الشبكة في الأهداف المجسدة في رغبة التحكم في الضحية، و تتميّز عنها بسهولة إمكانية إخفاء هوية المجرم، علاوة على تعدّد و سهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة.

ثانيا/ انتحال الشخصية و التغرير و الاستدراج:

يقصد بانتحال الشخصية استخدام المجرم شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحيته و لذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية و سرية المعلومات الشخصية للمستفيدين على شبكة الانترنيت.

تتخذ جريمة انتحال الشخصية عبر الانترنيت أحد الوجهين التاليين: انتحال شخصية الفرد و انتحال شخصية المواقع[2]. و لقد سماها بعض المختصين في أمن المعلومات جريمة الألفية الجديدة، و ذلك نظرا لسرعة انتشار ارتكابها خاصة في الأوساط التجارية.[3]

أمّا عن التغرير و الاستدراج فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين صداقة على الانترنيت و التي قد تتطوّر إلى التقاء مادي بين الطرفين.

---

[1]- محمد عبيدالكعبي،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت، دار النهضة العربية، القاهرة، د.ت.ن، ص88.

[2]- انتحال شخصية الفرد: إنّ التطور المتزايد لشبكة الانترنيت أعطى للمجرمين قدرة أكبر على جمع المعلومات عن شخصية الضحية، و الاستفادة منها في ارتكاب جرائمهم، فتنتشر في شبكة الانترنيت الكثير من الإعلانات المشبوهة، فهناك مثلا إعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية، الذي يتطلب الإفصاح عن المعلومات الشخصية كالإسم و العنوان و رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، الأمر الذي يؤدي إلى الاستيلاء على رصيده البنكي أو حتى الإساءة إلى سمعة الضحية.

[3] - عمرو عيسى الفقي، الجرائم المعلوماتية. جرائم الحاسب الآلي و الانترنيت في مصر و الدول العربية، المكتب الجامعي الحديث، الاسكندرية،2006، ص102.

ثالثا/المساس بصور الأشخاص عن طريق الصناعة الإباحية:

إنّ شبكة الانترنيت ليس لها فقط وجه ايجابي، و إنّما لها وجه سلبي أيضا، منها وجود مواقع على شبكة الانترنيت تحرص على ممارسة الجنس للكبار و الصغار على حدّ سواء، و تقوم هذه المواقع بنشر صور و أفلام جنسية فاضحة للبالغين والقصر[1].

إنّ التشهير عن طريق صناعة و نشر المقاطع الإباحية تعدّ جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم [2] الأطفال، حيث يضم استغلال المستخدمين في إنتاج هذه المواد و يمثل اعتداءا عليهم في كل مرة يتم فيها عرض هذه الصور و يتخذ الاستغلال الجنسي للأطفال على الانترنيت أشكالا متعددة انطلاقا من الصور وصولا إلى التسجيلات المرئية للجرائم الجنسية العنيفة. و تستمر معاناة الضحايا حتى بعد انتهاء الاعتداء الفعلي الذي تعرّض له بسبب إمكان تناقل الصور على الانترنيت إلى ما لا نهاية[3].

رابعا/ جرائم القذف و السب و تشويه السمعة:

يستعمل الجاني حسب القواعد العامة لجرائم القذف و السب عبارات بدائية تمسّ شرف المجني عليه، مهما كانت الوسيلة المعتمدة. و بالتطور التكنولوجي أصبحت الانترنيت إحدى هذه الوسائل فأصبحت ترسل هذه العبارات عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب.[4]

تعتبر شبكة الانترنيت مسرحا غير محدود، فهي تتلقى كل ما يدرج عليها دون قيد أو رقابة، حيث يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن الضحية، التي قد تكون فردا أو مجتمعا أو مؤسسة تجارية أو سياسية.[5] حيث بلغ عدد القضايا المسجلة في مجال الجرائم الماسة بالأشخاص سنة 2017 إلى 430، أين تمت معالجة 200قضية، وبلغ عدد المتورطين فيها 365، لتصل نسبة القضايا المعالجة إلى 68%.

المطلب الثاني
جرائم واقعة على أمن الدولة و جرائم ماسة بالأمن الفكري

[1] - FAUCHOUX Vincent-DEPREZ pierre, le droit de l'internet (loi, contrat et usage), éditionLitec, paris. 2008, p215.

2 - خالد محي الدين أحمد، "الجرائم المتعلقة بالرغبة الاشباعية باستخدام الكمبيوتر"، الندوة الاقليمية حول الجرائم المتّصلة بالكمبيوتر، المملكة المغربية، أيام 19-20جوان 2007، ص37.

[3] -علوي مصطفى،"الضحية المنسية أمام لغة الكبار"، مجلة الشرطة، المديرية العامة للأمن الوطني، العدد87، جوان،2008، ص30.

[4] -عبد الرحمن بن عبد الله السند، الأحكام الفقهية للمعاملات الالكترونية، الحاسب الآلي و شبكة المعلومات (الانترنيت)، دار الوراقين للنشر و التوزيع، بيروت،2004، ص318.

[5] - محمد أمين أحمد الشوابكة، المرجع السابق، ص ص31-32.

استغلّت الكثير من الجماعات المتطرّفة، الطبيعة الاتصالية للانترنيت من أجل بثّ معتقداتها و أفكارها، بل تعدّاه الأمر إلى ممارسات تهدّد أمن الدولة المتعدّى عليها، خاصة المتمثلة في الإرهاب و الجريمة المنظمة و جريمة التجسس (الفرع الأول) وأخرى تهدد الأمن الفكري(الفرع الثاني)

الفرع الأوّل
جرائم واقعة على أمن الدولة

تشمل الإرهاب و الجريمة المنظمة و جريمة التجسس و هذا سنوضحه فيما يلي:

أولا/ الإرهاب:

أصبح الإرهاب في الوقت الراهن ظاهرة عالمية، ترتبط بعوامل اجتماعية و ثقافية و سياسية و تكنولوجية. يتمّ بث ثقافة الإرهاب عبر الانترنيت عن طريق تأسيس مواقع افتراضية تمثّل المنظمات الإرهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى الهجمات التي ارتكبت أو بيانات تنفي أو تعلّق على أخبار صادرة عن منظمات أو جهات دولية.[1] و الجدير بالذكر أنّه إذا كانت الجماعات الإرهابية تسعى إلى الدعاية و الترويج لنفسها عن طريق آليات مختلفة منها جذب انتباه وسائل الإعلام المعروفة لتغطية أخبار الجماعة و أنشطتها.

تستخدم الجماعات الإرهابية الانترنيت إلى جانب أغراض الدعاية و الترويج في نشر معلومات بهدف شنّ حرب نفسية ضدّ أعدائها، و هو ما يتحقق من خلال نشر معلومات مضللة أو مغلوطة، نشر تهديدات و صور و لقطات فيديو مرعبة.

ثانيا/ الجريمة المنظمة:

تعرف الجريمة المنظمة على أنّها الجريمة التي أوفرتها الحضارة لكي تمكّن الإنسان المجرم من تحقيق أهدافه الإجرامية بطريقة متقدمة، لا يتمكّن القانون من ملاحقته بفضل ما أحاط به نفسه من وسائل يخفي بها أغراضه الإجرامية. إنّ الجريمة المنظمة و بسبب تقدّم وسائل الاتصال و التكنولوجيا أصبحت غير محددة لا بقيود الزمان و لا المكان و لا تحدّها الحدود الجغرافية.[2]

اكتشفت جماعات الجريمة المنظمة استخدام التكنولوجيا بصفتها فرص الأشغال و تحقيق أرباح غير مشروعة و فطن المجرمون أيضا أنّ شبكة الانترنيت تستطيع أن تؤمن فرصا جديدة و فوائد غير مشروعة. و يعدّ الترابط بين الجريمة المنظمة و شبكة الانترنيت ليس طبيعيا فقط و لكنّه ترابط من الأرجح أن يتطوّر إلى حدّ أبعد في المستقبل، شبكة الانترنيت تؤمن الأهداف والأقنية في نفس الوقت و تمكن من استغلالهما لتحقيق أرباح و أهداف كبيرة بأقلّ قدر ممكن من المخاطر.

ثالثا/ جريمة التّجسّس:

يقصد بالتجسس الإطّلاع على معلومات خاصة بالغير مؤمنة بجهاز آخر و ليس مسموحا بغير المخوّلين بالإطّلاع عليها. سهّلت شبكة الانترنيت الأعمال التجسّسية بشكل كبير حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو

[1] -عبد الله بن عبد العزيز اليوسف، أساليب تطور البرامج و المناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض،2004، ص25.

[2] - سامي علي حامد عباد، الجريمة المعلوماتية و اجرام الانترنيت، دار الفكر الجامعي، الاسكندرية، 2004، ص83.

المؤسسات الدولية أو الوطنية، و تستهدف عملية التجسس في عصر المعلومات ثلاثة أهداف رئيسية.[1]التجسس العسكري و التجسس السياسي و التجسس الاقتصادي .

كما تمارس العديد من الدول التجسس باستخدام التقنية المعلوماتية، و تمارس من قبل دولة على دولة أو دول أخرى، أو من قبل دولة على مواطنيها، أو من قبل شركة على شركات أخرى منافسة.

الفرع الثاني

الجرائم الماسة بالأمن الفكري

بناءًا على خصائص الشبكة العالمية للانترنيت التي منحت المستخدم الكثير من الخيرات من خلال عدم خضوعها لأيّ رقابة، و عبورها بالحدود الجغرافية بين الدول و نموّها السريع المتواصل و إمكانية مشاركة الجميع من مختلف دول العالم، مع ما تمنحه من القدرة على التخفي و عدم المواجهة الافتراضية التي تعدّ من أهمّ خصائص هذه الشبكة، بالإضافة إلى الكمّ الهائل من المعلومات التي يمكن الحصول عليها من عدة مصادر لا يمكن التحكم فيها و متابعتها أو الإشراف عليها، كل ذلك جعل هذه الشبكة من أهمّ مقوّمات المجتمع المعلوماتي[2] التي تؤدّي إلى الانحراف الفكري من خلال تعرّض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العالمية للانترنيت و تهدّد الأمن بأبعاده كافة. فكما اندهشنا بالتلفزيون و تخوفنا من آثاره على حياتنا لأوّل مرة و تغيرنا رغم النقد و التردد، فليس هناك ما يدعونا لاعتقاد غير ذلك بسبب ثورة المعلومات اليوم و خاصة الانترنيت.

[2] - سمير إبراهيم حسن، "الثورة المعلوماتية عواقبها و آفاقها"، مجلة جامعة دمشق، العدد الأوّل،2002، ص213.

الفصل الثاني
آليات مكافحة الجريمة الالكترونية

صاحب ظهور شبكة الانترنيت بروز تحديات جديدة للمنظومة القانونية الموضوعية و الاجرائية على المستوى الدولي و المحلي خاصة بعد أن أصبحت هذه الوسيلة يعتمد عليها الجناة في ارتكاب طائفة من الجرائم المستحدثة التي تختلف عن الجرائم التقليدية في الطريقة و المناهج ، و ألقت بضلالها على العالم بأسره، فكانت الأضرار و الخسائر التي انجرت عنها فادحة على المستويين الدولي و المحلي، الأمر الذي أدّى بمختلف الدول إلى الإسراع من أجل المحاولة للتصدّي لهذه الظاهرة فتضافرت الجهود من أجل ايجاد سبل مكافحة الجريمة الالكترونية بنجاعة و فعالية أكثر (المبحث الأول).

يتضح لنا كليا خطورة الجريمة الالكترونية الأمر الذي يوجب الكثير من الجهد لمكافحتها، لكنها تبقى بعيدة كل البعد عن الأسس السليمة و الخاصة بها، حيث أنّ الإجراءات التقليدية المطبّقة على هذا النوع من الجرائم لم تعد مجدية نظرا لاختلاف الجرائم التقليدية عن الجريمة الالكترونية. فعدم كفاية التشريعات الخاصة بها و تباينها، و صعوبة التكييف القانوني لها بالإضافة إلى الطبيعة اللّامادية للجريمة من أهمّ الصعوبات التي تعتري سبل مكافحة هذه الجريمة. فقصور تشريعات إحدى الدول أو بعضها في مواجهة هذه الجريمة يؤدّي إلى احباط الجهود المبذولة في دول أخرى، ذلك لأننا بصدد الحديث عن جريمة عابرة الحدود الوطنية. (المبحث الثاني)

المبحث الأول
طرق مكافحة الجريمة الالكترونية

تتجسد أول طرق مكافحة الجريمة الالكترونية في الاستدلال الذي يتضمن كل من التفتيش، المعاينة و الخبرة، و التي تثير اشكالات اجرائية تعود إلى خصوصية الجريمة الالكترونية و هذا ما سنتطرّق إليه في (المطلب الأول).

أمّا ثاني سبل مكافحة الجريمة الالكترونية تتمثل في الجهود التشريعية سواءً على المستوى الدولي، و العربي لتنظيم منظومة قانونية للوقاية من هذه الجريمة المستحدثة، و هذا ما سنتناوله في (المطلب الثاني).

المطلب الأوّل
الاستدلال كوسيلة لإثبات الجريمة الالكترونية

يقوم ضبط الجريمة و اثباتها في المقام الأوّل على جمع الأدلّة التي حدّد المشرع وسائل اثباتها على سبل الحصر و ذلك لما فيها من مساس بحرية الأفراد و حقوقهم الأساسية. فلا يجوز أن تخرج الأدلّة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية و تتمثل في وسائل الاثبات الرئيسية في التفتيش (الفرع الأول)، المعاينة (الفرع الثاني)، و الخبرة (الفرع الثالث).

الفرع الأوّل
التفتيش

التفتيش في الجرائم التقليدية هو إجراء من إجراءات التحقيق يقوم به موظف مختص طبقا للإجراءات المقرّرة قانونا في محل يتمتع بالحرمة بهدف الوصول إلى أدلّة مادية لجناية أو جنحة تحقق وقوعها الاثبات ارتكابها أو نسبتها إلى المتّهم.[1]

و لكن التساؤل يثور عندما نكون بصدد تفتيش عن حيثيات الجريمة الالكترونية حول مدى قابلية مكونات و شبكات الحاسب الآلي للتفتيش؟.

أولا: المكونات المادية للحاسب:

تتكون نظم الحاسوب من مكونات مادية و مكونات منطقية، كما أنّه تربطه بغيره من الحاسبات شبكات اتصال بعدية على المستوى المحلي أو الدولي.[2]

و الواقع أنّ تفتيش المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة الكترونية وقعت و يفيد في كشف الحقيقة عنها و عن مرتكبيها. يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقرّرة. معناه أنّ حكم تفتيش المكونات المادية يتوقف على طبيعة المكان الموجودة فيه و هل هو من الأماكن العامة أو من الأماكن الخاصة، حيث أنّ صفة المكان و طبيعته أهمية، فإذا كانت موجودة في مكان خاص كمسكن المتّهم[3] أو أحد ملحقاته كان لها حكمة فلا يجوز تفتيشها إلّا في الحالات التي يجوز فيها تفتيش مسكنه و بنفس الضمانات و الإجراءات المقررة قانونا في التشريعات المختلفة، مع مراعاة التمييز بين ما إذا كانت مكونات الحاسب المراد تفتيشها منعزلة عن غيرها من الحاسبات أو متصلة بحاسب آلي آخر كمسكن غير المتهم مثلا.

أمّا لو وجد شخص يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة سواء أكانت عامة بطبيعتها كالطرق العامة الميادين و الشوارع أو كانت من الأماكن العامة بالتخصيص كالمقاهي، المطاعم، و السيارات العامة فإن تفتيشها لا يكون إلّا في الحالات التي يجوز فيها تفتيش الأشخاص و بنفس الضمانات و القيود المنصوص عليها في هذا المجال.[4]

ثانيا/ مدى خضوع مكونات الحاسوب المعنوية للتفتيش:

---

[1]-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنيت، دار الفكر الجامعي، الإسكندرية،2006، ص192.

[2] -زبيحة زيدان، المرجع السابق، ص20.

[3] - عبد القادر قنديل، المرجع السابق، ص140 .

[4] -حسين بن سعيد الغافري، التحقيق و جمع الأدلّة في الجرائم المتعلقة بشبكة الانترنيت، ص11، موقع:http://www.eastlaws.com

تفتيش المكونات المعنوية للحاسوب أثار خلافا كبيرا في الفقه بشأن مدى جواز تفتيشها، فذهب الرأي الأوّل إلى جواز ضبط البيانات الالكترونية بمختلف أشكالها، و يستند في ذلك إلى عمومية نصوص التفتيش لتشمل المكونات المادية و غير المادية.[1]

في حين ذهب الرأي الآخر إلى عدم انطباق إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة و لذلك فإنّه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أنّ تفتيش الحاسب الآلي لابدّ أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي، و هكذا تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حصل بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأدلّة المادية أو أيّ معالجة بواسطة الحاسب. و في مقابل هذين الرأيين يوجد رأي آخر نأى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية بمكونات الحاسب الآلي أم لا، فذهب إلى أن النظرة في ذلك يجب أن يستند إلى الواقع العملي و الذي يتطلّب أن يقع الضبط على بيانات الحاسب إذا اتخذت شكلا ماديا.[2]

و يذهب رأي فقهي آخر إلى أنه في تحديد مدلول الشيء بالنسبة لمكونات الحاسب الآلي يجب عدم الخلط بين الحق الذهني للشخص في البرامج والكيانات المنطقية وبين طبيعة هذه البرامج والكيانات، وإنما يتعيين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرف بأنها كل ما يشغل حيزًا ماديا في فراغ معين، وأن الحيز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزا ماديا في ذاكرة الحاسب الآلي، ويمكن قياسها بمقياس معين، وأنها أيضا تأخذ شكل نبضات الكترونية[3]تمثل الرقم 0و1، فإنها تعد طبقا لذلك ذات كيان مادي.[4]

ثالثا: شبكة الحاسب الآلي:

عقدت طبيعة التكنولوجيا الرقمية التحدي أمام أعمال التفتيش، فالبيانات التي تحتوي على أدلّة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة وبعيدة تماما عن الموقع المادي للتفتيش وإن ظل من الممكن الوصول إليها من خلال حواسب تقع في الأبنية الجاري تفتيشها، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، إلّا أنّ السلطات في ذلك الاختصاص السياسي قد تشعر ببالغ الانزعاج. وهذا ما يزيد من تعقيد مشاكل الجريمة الالكترونية ويزيد من أهمية تبادل المساعدة القانونية. وفي هذا الصدد يمكن أن نميّز في هذه الصورة بين ثلاثة احتمالات:

1- الاحتمال الأول: اتصال حاسب المتهم بحاسب آخر موجود في مكان آخر داخل الدولة:

ويثار التساؤل حول مدى امكانية امتداد الحق في التفتيش إذا تبيّن أنّ الحاسب موجود في منزل المتهم متصل بجهاز في مكان آخر سلوك لشخص لغير المتهم؟

---

[1] -أمير فرج يوسف، الجريمة المعلوماتية على شبكة الانترنيت، دار المطبوعات الجامعة، الإسكندرية، 2008 ، ص224.

[2] -علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي،ص ص22-23، مقال متوفر على الموقع:http://www.arablawinfo.com

[3]- علي محمود علي حمودة، المرجع نفسه، ص 25.

[4] -عبد الله بن عبد العزيز بن عبد الله الخثعمي، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص38.

يرى الفقه الألماني امكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم103[1] من قانون الاجراءات الجزائية الألمانية. ونجد انعكاسات هذا الرأي في المادة 88 من قانون تحقيق الجنايات البلجيكي التي تنص على "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي و يمتد هذا الامتداد وفقا لضابطين:

أ-إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث.

ب-إذا وجدت مخاطر تتعلق بضياع بعض الأدلّة نظرا لسهولة عملية محو أو اتلاف أو نقل البيانات محل البحث.

2- الاحتمال الثاني: اتصال حاسب المتهم بحاسب آخر موجود في مكان آخر خارج الدولة:

تواجه سلطة الادعاء في جمع الأدلّة عدة مشاكل كقيام مرتكبو الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية مستهدفين عرقلة الادعاء في جمع الأدلة و التحقيقات. و في هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة مختصة التي صدر من جهتها الإذن و دخوله في المجال الجغرافي لدولة أخرى و هو ما يسمى بالولوج أو التفتيش عبر الحدود، قد يتغير القيام به بسبب تمسك الدولة بسيادتها.[2]

يرى جاني من الفقه أنّ التفتيش الالكتروني العابر للحدود لابدّ أن يتم في اطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد بعقد بين الدول المعنية و بالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في غياب تلك الاتفاقية أو على الأقل الحصول على إذن دولة أخرى، و هذا ما يؤكد أهمية التعاون الدولي في مجال مكافحة الجريمة الالكترونية و كتطبيق لهذا الاجراء الأخير ما حدث في ألمانيا أثناء جمع اجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب آلي، حيث تبين وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا و بين شبكة الاتصالات في سويسرا[3]، حيث يتم تخزين بيانات من مشروعات فيها. و عندما أرادت سلطة التحقيق الألمانية ضبط هذه البيانات فلن تتمكن من ذلك إلّا عن طريق التماس المساعدة الذي تمّ بالتبادل بين الدولتين، و مع ذلك أجازت المادة 32 من الاتفاقية الأوربية بشأن جرائم الانترنيت امكانية الدخول بغرض التفتيش و الضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين:

الحالة الأولى: إذا تعلّق التفتيش بمعلومات أو بيانات مباحة للجمهور.

الحالة الثانية: إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

3-الإحتمال الثالث: التنصت و المراقبة الالكترونية لشبكات الحاسب الآلي:

عرفت لجنة الخبراء للبرلمان الأوربي في اجتماعها بستراسبورغ بتاريخ 2006.10.06 حول أساليب التحري التقنية و علاقتها بالأفعال الارهابية اعتراض المراسلات بأنها عملية مراقبة للمراسلات السلكية و اللاسلكية و ذلك في اطار البحث و

[1] -حسين بن سعيد الغافري، المرجع السابق،ص13.

[2]- عبد الفتاح بيومي حجازي، المرجع السابق، ص381-382.

[3]- فاطمة زهرة بوعناد، "مكافحة الجريمة الالكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية، كلية الحقوق و العلوم السياسية، جامعة سيدي بلعباس، الجزائر،ع2013،1،ص68.

التحري عن الجريمة و الأدلّة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجرائم.

سمحت جميع الدول تقريبا بالتنصت و الأشكال الأخرى للمراقبة الالكترونية، رغم أنها مثيرة للجدل إلّا أنها أقرّت بها تحت ظروف معينة، فالقانون الفرنسي الصادر في 1991.07.10 بحيز اعترافي الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات، و في هولندا أجاز المشرع لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة ضالع فيها المتهم و تشمل هذه الشبكة التليكس و الفاكس و نقل البيانات.[1]

الفرع الثاني
المعاينة

تعد المعاينة من المراحل الأولى للاستدلال حول ملابسات الجريمة و من أهم المراحل على الإطلاق، نظرا لما يمكن أن توفره من أدلّة لإثبات الجريمة و تزداد أهميتها في الجريمة الالكترونية و ذلك راجع إلى الطبيعة الخاصة للسلوك الإجرامي فيها، بالإضافة إلى اعتبارها من الجرائم المستحدثة، ما استوجب ابتكار اجراءات خاصة بالمعاينة في هذا المجال.

أولا/ مفهوم المعاينة:

هو اجراء غايته كشف و صيانة العناصر المادية التي تتعلق بالجريمة و تفيد في التحقيق الجاري بشأنها، فإذا انعدمت للتحقيق جداوها و فائدتها لم يكن ثمة مجال أو مقتضى لإجرائها و لا تجدي لكشف الحقيقة بشأنه المعاينة مثل جريمة التزوير المعنوي و جريمة القذف و السب و التي تقع بالقول في غير العلنية و غيرها.

و قد عرّفها بعض الفقهاء بأنها "اثبات مباشر و مادي لحالة الأشخاص و الأمكنة ذات الصلة بالحادث عن طريق رؤيتها أو فحصها فحصا حسيا مباشرا."[2] و عرّفها أيضا بعض الفقهاء بأنها "اثبات لحالة الأماكن الأشخاص و كل ما يفيد في كشف الحقيقة عن الجريمة و مرتكبيها."

يتضح لنا جليا أنّ جوهر المعاينة هو ملاحظة و فحص حسي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته و الكشف و التحفظ على ما قد يفيد من الأشياء في كشف الحقيقة. و هذا ما يجعلنا نتساءل عن مدى امكانية معاينة مسرح الجريمة الالكترونية.

ثانيا/ مسرح الجريمة الالكترونية:

ينبغي عند الشروع أو القيام بجمع الأدلّة من مسرح الجريمة الالكترونية (الحاسوب و الانترنيت) التعامل معه على أنه مسرحين:

- **مسرح تقليدي**: يقع خارج بيئة الحاسوب و يتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، و هو أقرب إلى مسرح الجريمة التقليدية، قد يترك فيها الجاني آثار عدّة كالبصمات و غيرها، و ربما أيضا يترك متعلقات شخصية أو وسائط تخزين رقمية و يتعامل أعضاء فريق التحقيق مع الأدلّة الموجودة فيه كل بحسب اختصاصه.

[1] -حسين بن سعيد الغافري، المرجع السابق، ص13-14.

[2] -محمد علي الكواري، مسرح الجريمة و دوره في كشف غموض الجريمة، جامعة نايف العربية للعلوم الأمنية، الرياض،2007،ص44.

- **مسرح سبيراني**[1]: و يقع داخل بيئة الحاسوب، و يتكون من البيانات الرقمية التي تتواجد و تنقل داخل بيئة الحاسوب و شبكاته في ذاكرته و في الأقراص الصلبة المتواجدة بداخله و التعامل مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلّا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع.

ثالثا/ أهمية المعاينة في الجريمة الالكترونية:

تكمن أهمية و جدارة المعاينة بعد وقوع جريمة من الجرائم التقليدية بحكم دورها في تصور كيفية وقوع الجريمة و ظروف ملابسات ارتكابها و توفير الأدلة المادية من المدى التي تجمع عن طريقها و تمحيص و تقييم الأدلّة الأخرى و التنسيق بينها في ضوء المعلومات التي منها، بما يكفل في ذات الوقت التخطيط لعمليات البحث، و التحقيق الجنائي و تطويرها، إلّا أنّ دورها في مجال كشف غموض الجريمة الالكترونية و ضبط الأشياء التي قد تفيد في اثبات وقوعها و نسبتها إلى مرتكبها، إلى نفس درجة من الأهمية يمكن ردّ ذلك إلى أنّ هناك على الدوام تقريبا مسرحا للجريمة الالكترونية جرت عليه الأحداث و تركت آثارها المادية التي تنبثق منها الأدلّة.[2]

و المعاينة في مسرح الجريمة تتيح المجال أمام الباحث و المحقق الجنائي للكشف عن طريق معاينة الآثار المادية التي خلفها ارتكاب الجريمة و التحفظ على الأشياء التي تفيد في الجاري بشأنها. بينما لا توجد فيه المعدات و الأنظمة المعلوماتية التي كانت محلا للجريمة أو أداتها.[3] يقلل مثل هذا المسرح إلى حدّ كبير من فرض إفصاحه عن الحقائق المراد التوصل إليها من وراء معاينته لسببين رئيسيين:

أولا: أن الجرائم التي تقع بواسطة الأنظمة المعلوماتية فلما يتخلف عن ارتكابها آثار مادية.

ثانيا: أن عددا كبيرا من الأشخاص يكون قد تردّد على مكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا التي تنقضي عادة بين ارتكاب الجريمة و اكتشافها مما يفسح المجال لحدوث تغيير أو تلف أو عبث بالآثار المادية أو زوال بعضها و هو ما يلقي ضلالا من الشك على الدليل المستقي من المعاينة.

ينبغي لتفادي كل هذا و حتى يكون للمعاينة في الجرائم الالكترونية فائدة في كشف الحقيقة عنها و عن مرتكبيها مراعاة عدة قواعد و ارشادات فنية أبرزها ما يلي:

- تصوير الحاسب و الأجهزة الطرفية المتصلة به على أن يتم تسجيل وقت و تاريخ و مكان التقاط كل صورة.
- العناية بملاحظة الطريقة التي تم بها إعداد النظام.
- ملاحظة و إثبات حالة التوصيلات و الكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة و التحليل عن عرض الأمر فيما بعد على المحكمة.[4]

---

[1]-محمد ناصر محمد السرحاني، مهارات التحقيق الجنائي القي في جرائم الحاسوب و الانترنيت، رسالة لمتطلبات الحصول على درجة الماجستيرفي العلوم الشرطية، جامعة نايف العربية للعلوم،، الرياض،2004،ص77.

[2]-عبد الفتاح بيومي حجازي، المرجع السابق،ص101.

[3]- عبد الفتاح بيومي حجازي، المرجع نفسه،ص103-104.

[4]- محمد أبو العلا عقيدة،"التحقيق و جمع الأدلة في مجال الجرائم الالكترونية،ص ص1-16، مقال متوفر على الموقع التالي: http://arablawinfo.com

عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل اجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوة مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

-التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة و أوراق الكربون و الشرائط و الأقراص الممغنطة غير السليمة و فحصها و يرفع عليها البصمات ذات الصلة بالجريمة.

-التحفظ على مستندات الإدخال و المخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع و مضاهاة ما قد يوجد عليها من بصمات.

الفرع الثالث

الخبرة

تعتبر الاستعانة بالخبراء من بين الاجراءات التي يلجأ اليها القضاة أو سلطات الاستقلال على حدّ سواء، و ذلك كلما استعصى عليهم فهم موضوع معين يتميّز بالتقنية، و الجريمة الالكترونية من بين الجرائم التي تستدعي اللجوء إلى الخبرة، ذلك أنّه لا يستطيع التعامل مع هذه الجريمة إلّا شخص ذو دراية و خبرة في مجال الشبكات.

أوّلا/ تعريف الخبرة:

الخبرة هي اجراء يتعلّق بموضوع يتطلّب الالمام بمعلومات فنّية لإمكان استخلاص الدليل منه. أو هي الاستشارة الفنية التي يستعين بها المحقّق أو القاضي في مجال الاثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدة فنية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله و ثقافته.

كما عرّفها البعض بأنّها الاستشارة الفنية[1] التي يستعين بها القاضي أو المحقّق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه، و الخبرة الفنية تعتبر اجراء من اجراءات التحقيق بحسب الأصل.

ثانيا/ أهمية الاستعانة بالخبراء:

تحتل الخبرة الفنية مكانا مهمّا في العمل القضائي و الاستدلالي باعتبارها تقدّم عونا ثمينا لجهة التحقيق و القضاء و لسائر السلطات المختصة بالدعوى الجنائية في أداء عملها، فبدونها يتعذّر الوصول إلى الرأي السديد بشأن المسائل الفنية التي يكون على ضوئها كشف الحقيقة المبنية على الأصول و الحقائق العلمية.[2]

إذا كان للخبرة أهمية في الجرائم التقليدية فإنّ أهميتها تزداد و تصبح ضرورية بل و حتمية في اشتقاق الأدلة الالكترونية لإثبات الجريمة الالكترونية، حيث تتعلق بمسائل فنية أية في التعقيد و محل الجريمة فيها غير مادي، و التطور في أساليب ارتكابها سريع و متلاحق و لا يكشف غموضها إلّا متخصص و على درجة كبيرة من التميز في مجال تخصصه.[3]

---

[1] -نعيم سعيداني، آليات البحث و التحرّي عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر،2013، ص165.

[2] -محمد علي أحمد الكواري، المرجع السابق، ص40.

[3] - محمد واصل حسين بن علي الهلالي،الخبرة الفنية أمام القضاء، دراسة مقارنة، المكتب الفني،عمان،2004، ص27-28.

ثالثا/ مجالات الخبرة بالنسبة للجريمة الالكترونية:

تتنوع العمليات الالكترونية بتنوع المجالات التي تستخدم فيها شبكة الانترنيت، فنجدها مثلا في الأعمال المصرفية، الإدارة الالكترونية و التجارة الالكترونية، و لذلك فإنه يتصور تنوّع الجرائم التي تقع على هذه العمليات وفقًا لنوع العمليات الالكترونية المستخدمة في ارتكابها. تقتضي عمليات البحث الجنائي و التحقيق في جرائمه الالكترونية الاستعانة بخبرات عديدة و متنوعة، فإنّ اختيار خبير في نوعية الإجرام في مجال الجريمة الالكترونية الذي تندرج الواقعة المرتكبة في اختصاصه يغدو أمرا بالغ الأهمية.[1]

المطلب الثاني

الجهود التشريعية لمكافحة الجريمة الالكترونية

دأبت المجتمعات و الدول عبر الزمن في سن تشريعات و قوانين من أجل مواجهة كل الجريمة الالكترونية، فبالرغم من قلّتها إلّا أنّها تعتبر محاولات هامة و ملموسة في هذا المجال و تتمثل هذه الجهود على المستوى الدولي في الجهود التي تبذلها مختلف الهيئات و المنظمات العالمية بالإضافة إلى المنظمات الإقليمية.(الفرع الأول)

تعتبر الجهود الدولية داعمة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية، فتعتبر بمثابة قوانين استرشادية تأخذ بها الدول لمواجهة الجرائم المستحدثة بما فيها الجريمة الالكترونية، فهناك العديد من الدول التي اتخذت سبيل تطوير قوانين العقوبات، و هناك دول ارتأت أفرادها بقوانين خاصة، و في هذا الاطار سوف نستعرض تجربة المشرع الجزائري التي انتهجها للحدّ من هذه الجريمة. (الفرع الثاني)

الفرع الأوّل

على المستوى الدولي

تعدّدت الجهود الدولية و الإقليمية في سبيل مكافحة الجريمة الالكترونية، نظرا للتهديدات الكبيرة التي أتت بها الجريمة على هذين المستويين، و في هذا المجال سنبين الجهود الدولية في مواجهة الجريمة الالكترونية (أولا) و كذا الجهود الاقليمية في هذا السياق (ثانيا).

أولا/ الجهود الدولية لمكافحة الجريمة الالكترونية:

تتمثل الجهود الدولية في إطار مكافحة الجريمة الالكترونية في:

1-جهود منظمة الأمم المتحدة:

بذلت منظمة الأمم المتحدة جهودا كبيرة في سبيل العمل على مكافحة جرائم الانترنيت، نظرا لما ينتج منها من أضرار بالغة و خسائر فادحة بالإنسانية جمعاء.

توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة الالكترونية و معاملة المجرمين[2] إلى اصدار قرار خاص بالجرائم المتعلقة بالحاسوب و أشار في مضمونه إلى أنّ الاجراء الدولي لمواجهة الجريمة الالكترونية يتطلب من الدول الأعضاء اتخاذ عدّة اجراءات أهمها:

[1] -طالع الموقع المجلس الأوربي: http://www.consiliem.europa.eu/fr/home.

[2] - نجاري بن حاج علي فايزة، الآليات القانونية لمكافحة الإرهاب الالكتروني، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، ص70.

- تحديث القوانين و أغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة (التخفيف قبول الأدلة) على نحو ملائم و ادخال التعديلات إذا دعت الضرورة.
- مصادرة العائد و الأصول من الأنشطة غير المشروعة.
- اتخاذ تدابير أمن و الوقاية مع مراعاة خصوصية الأفراد و احترام حقوق الإنسان.
- رفع الوعي لدى الجماهير و القضاة و الأجهزة العاملة على مكافحة هذه الجريمة بأهمية مكافحة هذه الجريمة و محاكمة مرتكبيها.
- التعاون مع المنظمات المهتمة بهذا الموضوع، و وضع و تدريس الآداب المتبعة في استخدام الحاسوب ضمّت المناهج المدرسية.
- حماية مصالح الدولة و حقوق ضحايا الجريمة الالكترونية.

عقدت منظمة الأمم المتحدة اتفاقية خاصة بمكافحة اساءة استعمال التكنولوجيا لأغراض اجرامية سنة 2000 أين أكّدت على الحاجة إلى تعزيز التنسيق و التعاون بين الدول في مكافحة اساءة استعمال تكنولوجيا المعلومات لأغراض اجرامية.

-كما عقدت كذلك المؤتمر الثاني عشر لمنع الجريمة و العدالة الجنائية و ذلك بالبرازيل أيام 12-19 أفريل 2010، بحيث ناقشت فيه الدول الأعضاء مختلف التطورات الأخيرة في استخدام العلم و التكنولوجيا من جانب المجرمين و السلطات المختصة في مكافحة الجريمة الالكترونية.

اضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات و ذلك تحت اشراف الأمم المتحدة عام 1944، الذي نتج عنه عدة توصيات و قرارات ذات صلة بالجريمة الالكترونية.[1]

2-منظمة التعاون الاقتصادي و التنمية[2]

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي و تباغم التطور الاقتصادي مع التنمية الاجتماعية. بدأت هذه المنظمة تهتم بالجريمة الالكترونية منذ عام 1978، ذلك بوضعها لمجموعة أدلّة و قواعد ارشادية تتصل بتقنية المعلومات.

يعدّ الدليل المتعلّق بحماية الخصوصية و قواعد نقل البيانات من أوّل الأدلّة التي تمّ تبنّيها من قبل مجلس المنظمة سنة 1980 مع التوصية للأعضاء بالالتزام بها.

في عام 1983 أصدرت هذه المنظمة تقريرا بعنوان الجرائم المرتبطة بالحاسوب و تحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة و المقترحات الخاصة في عدد من الدول الأعضاء، حيث تضمّن التقرير الحدّ الأدنى لأفعال سوء استخدام الحاسوب التي يجب على الدول أن تجرمها و تفرض لها عقوبات في قوانينها، و من أمثلة هذه الأفعال الاستخدام أو الدخول إلى نظام و مصادر الحاسوب على نحو غير مصرّح به، و يشمل ذلك الحاسب و المعلومات المخزّنة في قواعد الحاسب. كما أوصت

[1] - نجاري بن حاج علي فايزة، المرجع السابق، ص71.

[2] منظمة التعاون الاقتصادي و التنمية(OECD)، تضم مجموعة من الدول: استراليا، النمسا، بلجيكا، كندا، جمهورية التشيك، الدنمارك، فنلندا، فرنسا، اسبانيا، ايسلندا، اليونان، ألمانيا، ايرلندا، السويد، سويسرا، لكسمبورغ،المكسيك، هولندا،نيوزيلندا، النرويج، بولندا، البرتغال، تركيا، بريطانيا، الولايات المتحدة الأمريكية، تعمل هذه الدول متحدة في ايطار المنظمة على تنمية الاقتصاد العالمي و التنمية الاجتماعية.

اللجنة المصدّرة للتقرير إلى وجوب أن تمتدّ الحماية إلى صورة أخرى لإساءة استخدام الحاسوب، منها الاتجار في الأسرار و الاختراق غير المأذون فيه للحاسب أو لأنظمته.

و في عام 1992 وضعت المنظمة توصيات إرشادية خاصة بأمن أنظمة المعلومات، حيث تمخضت جهود المنظمة من أجل معالجة الجريمة الالكترونية بالتوصية بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء الأفعال التالية:[1]

- التلاعب في البيانات المعالجة آليا بما في ذلك محوها.
- التجسس المعلوماتي و يندرج تحته الحصول أو الاقتناء أو الاستعمال غير المشروع للمعطيات.
- التخريب المعلوماتي و يندرج تحته الاستخدام غير المشروع أو سرقة وقت الحاسب.
- قرصنة البرامج.
- الدخول غير المشروع على البيانات أو نقلها.
- اعتراض استخدام المعطيات أو نقلها.

تعقد المنظمة سنويا عدد من الملتقيات و ورش العمل المعقّمة للقطاعات ذات العلاقة بهذا المجال تركّز فيها على معايير الأمن و مستوياته، إضافة إلى معايير تنفيذ و تطبيق القانون و ذلك بهدف مواكبة التطورات في مجال جرائم الانترنيت.

3-المنظمة العالمية للملكية الفكرية:

تم توقيع المنظمة العالمية للملكية الفكرية في استوكهولم في السويد سنة 1967 [2]، و أصبحت إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتبارا من 17 ديسمبر 1974. اهتمت هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم بهدف تشجيع النشاط الابتكاري.

كما اهتمت هذه المنظمة في المجال المعلوماتي بتوفير الحماية القانونية للبرامج المعلوماتية و قواعد البيانات، فبعد أن يستقر الرأي لديها بعدم امكانية توفير الحماية لهما في تشريعات براءات الاختراع، تم الاتفاق على توفيرها بواسطة الاتفاقيات العالمية و خاصة التريس و برن اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصة تشريعات حق المؤلف، و كذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية و القرصنة المتعمدة و المرتكبة في إطار تجاري، و تعتبر الانترنيت من الأماكن الخصبة لهذا النوع من التصرفات و التي وفّرت بموجبها الحماية القانونية للبرامج و قواعد البيانات المعلوماتية.

حيث تنص المادة الرابعة من معاهدة المنظمات العالمية للملكية الفكرية و المعتمدة سنة 1996 على أنه: "تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية في معنى المادة الثانية من اتفاقية برن. و تطبيق تلك الحماية على برامج الحاسوب أيّا كانت طريقة التعبير عنها أو شكلها، و تنص المادة الخامسة على أنه: تتمتع مجموعات البيانات أو المواد الأخرى

---

[1] - www.oecd-ong.

[2] -محمد أحمد عبابنة، المرجع السابق، ص159.

-ويشار إليها باللغة الفرنسية Organisation mondiale de la propriété intellectuelle(OMPL) و تضمّ في عضويتها وفقا لما وردني احصاء منشور في عام 1999، قرابة 170 دولة بينها حوالي 18 دولة عربية، من ضمنها الأردن و ليبيا.

بالحماية بصفتها هذه أيّا كان شكلها إذا كانت تعتبر ابتكارات بسبب اختيار محتوياتها أو ترتيبها".[1]

ثانيا/ دور الهيئات و المنظمات الاقليمية في مكافحة الجريمة الالكترونية:

تتمثل الجهود الاقليمية في مكافحة الجريمة الالكترونية في:

1- الاتحاد الأوروبي:

توّجت الجهود التي يبذلها الاتحاد الاوربي و المجلس الاوربي بصدور اتفاقية بودابست لمكافحة الجريمة الالكترونية و تعرف بالاتفاقية الأوربية لمكافحة الجريمة الالكترونية. و تتخلص أهم أهدافها في السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوربية و الدول المنظمة للاتفاقية من غير الدول الاوربية. و التأكيد على أهمية التعاون الاقليمي و الدولي في ميدان مكافحة الجريمة الالكترونية، و تحقيق التوازن بين حقوق الإنسان و الاجراءات المتخذة لمواجهة هذه الجريمة.[2]

وضعت اتفاقية بودابست من قبل مجلس أوربا بالتعاون مع كندا، و اليابان و جنوب افريقيا و الولايات المتحدة الأمريكية، و عرضت للتوقيع في بودابست في عام 2001 و دخلت حيّز التنفيذ سنة 2004.

لا تعتبر اتفاقية بودابست المجهود الأوّل الذي بذله المجلس الأوربي في هذا المجال، بل بذل جهود عديدة من قبل لاسيما الاتفاقية المتعلقة بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية و ذلك في 28 جانفي 1981، لكن تبقى اتفاقية بودابست الحيّز الأمثل لمواجهة الجريمة الالكترونية.

2- **مجموعة الدول الثمانية**:[3]

تمثل هذه المجموعة إطارا ناضجا لإجراء الدراسات البحثية و التطبيقية في مختلف المواضيع التي تهم المنظمة، تقوم على فكرة تبادل زعماء هذه الدول الرأي في المسائل ذات الاهتمام المشترك. تناولت مجموعة الثمانية في المؤتمر الذي عقدته في باريس عام 2000 موضوع الجريمة الالكترونية و حثت إلى منع ملاذات الرقمية غير الخاضعة للقانون. و كانت مجموعة الثمانية قد ربطت منذ ذلك الوقت محاولاتها الرامية إلى ايجاد حلول دولية باتفاقية مجلس أوربا بشأن الجريمة الالكترونية. في عام 2001 ناقشت مجموعة الثمانية الأدوات الاجرامية لمكافحة الجريمة الالكترونية في ورشة عمل عقدت بطوكيو، ركزت على ما إذا كان ينبغي تنفيذ الالتزامات باحتجاز البيانات أو ما إذا كان حفظ البيانات يعدّ حلّا بديلا.

3- **على المستوى العربي**:

نجد من الجهود العربية في سبيل مواجهة الجريمة الالكترونية القرار الصادر عن مجلس وزراء العدل العرب الخاص بإصدار القانون الجزائي الموحّد كقانون عربي نموذجي، أين نجد الباب السابع الخاص بالجرائم ضد الأشخاص، قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص، الناتج عن المعالجة المعلوماتية و ذلك في المواد 461-464 التي أشارت على وجوب حماية الحياة الخاصة، و أسرار الأفراد من خطر

[1] - محمود أحمد عبابنة، المرجع نفسه، ص162.

[2] -KURBALIJA Jouan, GELBSTEIN Eduardo, Gouvernance de l'internet, actems et fractures, publie par diplo fondation et global knowledge partnership, Suisse 2005, p98.

[3] -مجموعة الثمانية G8نشأتها و مؤتمراتها السنوية، أجندتها عملها على الموقع.www.g8utoriontо.com

المعالجة الآلية و كيفية جمع المعلومات الاسمية و كيفية الاطلاع عليها و العقوبة المطبّقة في حال ارتكاب هذه الجرائم.[1]

كذلك فإنّ الجمعية المصرية للقانون الجنائي لها اتجاه موحّد في هذا المجال، و تمثل ذلك في مؤتمرها السادس المنعقد في القاهرة من 25-28 أكتوبر 1993، حول جرائم الكمبيوتر و الجرائم الأخرى في مجال تكنولوجيا المعلومات التي أكّد فيها المؤتمرون على عالمية الجرائم الالكترونية و وجوب تكاثف الجهود لمكافحتها، لأنّها تمثل وجها سلبيا، و وجوب تعديل نصوص قانون العقوبات التقليدية، و إضافة نصوص جديدة، لأن النصوص الحالية لا يحيط معظمها بالأنشطة المراد تجريمها.

و في بيروت انعقد مؤتمر في قانون الملكية الفكرية فيما بين الفترة 25-26 مارس 1997. تمثلت توصيات المؤتمر بضرورة انشاء محاكم متخصصة للبحث في الالتزامات المغلقة بالحماية الالكترونية و تشجيع التعاون بين الدول العربية.[2]

الفرع الثاني
في التشريع الجزائري

واكب المشرع الجزائري مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الالكترونية بما فيها الانترنيت، خاصة التي تهدف إلى الحد من الاستخدام غير المشروع لها، و ذلك مراعاة منه لما يشهده العالم من تطورات كبيرة في مجال الاعلام و الاتصال خاصة الانترنيت، و كذلك إيمانا منه بأن الجزائر ليست بمعزل عن التطورات الاجرامية التي تحدث في العالم، خاصة في ظلّ التنامي المتصارع لاستعمال الانترنيت في الجزائر، فكانت محاولاته في الحدّ من هذه الظاهرة المستحدثة على النحو التالي:

أوّلا/ مكافحة الجريمة الالكترونية في قوانين الملكية الفكرية:

نظرا للاعتداءات التي تتعرّض لها مختلف المفتحات الفكرية عبر الانترنيت تطرّقنا في بحثنا هذا إلى مدى امكانية الحماية من خلال نصوص قانون الملكية الفكرية، و سنتوصل في ذلك من خلال نقطتين أساسيتين:

1. الحماية في إطار قانون الملكية الصناعية.
2. الحماية في إطار قانون الملكية الأدبية و الفنية.

1) مكافحة الجريمة الالكترونية في اطار الملكية الصناعية:

أ- في الأمر03-06 المتعلق بالعلامات التجارية :

تطرّق المشرع الجزائري إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين، آخرها الأمر رقم 03-06 المؤرخ في 2003/07/19[3]، و المتعلق بالعلامات. و تعرف العلامات التجارية على أنها كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يضعها المنتج أو يقدم بإصلاحها أو تجهيزها، أو ختمها لتمييزها عن

---

[1] -عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض،2007،ص59.

[2] - تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فاعليته، أطروحة مقدمة للحصول على درجة دكتوراه الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص17.

[3] - الأمر رقم 03-06 المؤرخ في 19جويلية2003 المتعلق بالعلامات التجارية،ج ر عدد44، صادر في 23جويلية2003

بقية المبيعات أو المصنوعات[1] أو الخدمات، و من شروط العلامة التجارية:أن تكون مميّزة،أن تكون جديدة،أن تكون غير مخالفة للنظام العام.

ب- في الأمر رقم 03-07 المتعلق ببراءات الاختراع: عرفت المادة 02 من الأمر 03-07 الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال للتقنية ، وبشأن الشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي[2] :(شرط الابتكار ، شرط الجدة ، القابلية للتطبيق الصناعي ، المشروعية)

تجدر الاشارة الى ان المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا للمادة 07 من الأمر 03-07[2] المتضمن براءة الاختراع التي نصت على انه:

" لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب"

2) مكافحة الجريمة الالكترونية من خلال القوانين الأدبية و الفنية:

نظرا للتطور الذي واكب مجال الاتصال، و الذي رافقه تطور في وسائل نقل الإنتاج الفكري، على اختلاف صوره من علوم و فنون و آداب، ممّا أوجد مصنفات جديدة جديرة بحماية حق المؤلف، و قد كان من أهم هذه المصنفات التي حضها بالاهتمام من قبل المختصين في مجال الملكية الفكرية نجد: المصنفات الخاصة ببرامج الحاسبات الالكترونية، و قواعد البيانات التي كانت طبيعتها اتقنية تختلف عن المصنفات التقليدية الامر الذي تطلب متابعتها باستمرار ووضع قواعد قانونية محددة وثابتة لحمايتها.

-اتجه المشرع الجزائري إلى الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي، و ذلك من خلال تعديله للأمر 73-14 بموجب الأمر 97-10.[3] و الذي يتبين من خلال استقراءها ما يلي:

1- أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الاعلام الآلي ضمن المصنفات الأصلية و التي عبّر عنها بمصنفات قواعد البيانات و برامج الإعلام الآلي، التي تمكن من القيام بنشاط علمي أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة و تترجم بانتفاعات الكترونية بالحاسوب. أمّا قواعد البيانات فهي مجموعة المصنفات والأساليب و القواعد، و يمكن أن تشمل أيضا الوثائق المتعلقة بسير المعطيات.

2-أن الحماية تحدّد من 25 إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية برن التي حدّدت كمدة دنيا للحماية 50 سنة، و بالتالي هذه المدة تشمل حتى مصنفات الاعلام الآلي.

4- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لا سيما مؤلفي المصنفات المعلوماتية

---

[1]- الأمر رقم 03-07 المؤرخ في 2003/07/19، المتعلق ببراءات الاختراع،جر عدد44 صادر في23جويلية2003.

[3] -أمر رقم 97-10، مؤرخ في 06-03-1997 المتعلق بحق المؤلف و الحقوق المجاورة، الجريدة الرسمية، عدد13، الصادر في 1997/03/12 معدّل و متم بأمر 05/03/ مؤرخ في 2003/07/19، المتعلق بحقوق المؤلف، و الحقوق المجاورة، الجريدة الرسمية عدد 44، الصادر في 2003/07/23.

ثانيا:مكافحة الجريمة الالكترونية في ظل قانون العقوبات:

لما كانت الحاجة ملحّة و ضرورية لحماية أنظمة المعالجة الآلية فلقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لهذا الغرض. و لهذا نجد المشرع الجزائري قد تدارك مؤخرا و لو نسبيا الفراغ القانوني في مجال الاجرام الالكتروني و ذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 15/04[1] المتضمن تعديل قانون العقوبات، لكن تجدر الإشارة إلى أن المشروع الجزائري قد ركّز على الاعتداءات الماسة بالأنظمة المعلوماتية، و أغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي و المتمثلة في التزوير الالكتروني. و لذلك ارتأينا و حتى لا تكون دراستنا لموضوع الحماية الجزائية ناقصة أن تتعرّض للاعتداءات الواردة على المعلوماتية من خلال ما يلي:

أ/ جريمة المساس بأنظمة المعالجة الآلية للمعطيات:

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي و هو الفعل المنصوص و المعاقب عليه في المواد 394 مكرّر الى المادة 394 مكرر 07. و نجد أنّ المشرع الجزائري لم يعرّف لنا نظام المعالجة الآلية للمعطيات، بالرجوع إلى الاتفاقية الدولية الخاصة بالإجرام الالكتروني قدمت تعريفا للنظام المعلوماتي في مادتها الثانية. و كذلك عرّفها الفقه الفرنسي.[2]

و بالعودة إلى قانون العقوبات الجزائري نجد أنّ الغش المعلوماتي يأخذ صورتان أساسيتان:

- الدخول في منظومة معلوماتية.
- المساس بالمنظومة المعلوماتية.

1-الدخول في منظومة معلوماتية: و يشمل فعلين هما: الدخول و البقاء.

- **جريمة الدخول غير المشروع:**

تنص المادة 394 مكرر من قانون العقوبات الجزائري، و التي تقابلها المادة 323 فقرة 01 قانون عقوبات فرنسي على معاقبة كل من يدخل عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك. و تضاعف العقوبة إذا ترتّب على الدخول أو البقاء أو الحذف أو تغيير معطيات المنظومة أو تخريب النظام.

- **جريمة البقاء الغير مشروع:**

نصّ المشرع الجزائري على هذه الجريمة في المادة 394 مكرّر من قانون العقوبات الجزائري المقابلة لنص المادة 1/323 من قانون العقوبات الفرنسي. و يقصد بالبقاء الدخول الشرعي أكثر من الوقت المحدّد و ذلك بغية عدم أتاء إتاوة. و تقوم الجريمة مباشرة على الحاسوب أو سواء حصل الدخول مباشرة على الحاسوب أو حصل بعد كما يجرم القاء حتى و لو تمّ بصفة عرضية.[3]

---

[1] - القانون رقم رقم 15/04 المؤرخ في 10 نوفمبر 2004، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71، صادر في 2004/11/10.

[2]-الاتفاقية الدولية حول الإجرام المعلوماتي، التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوربي، و تم وضعها للتوقيع منذ تاريخ 2001/11/23.

[3] - أحسن بوسقيعة، الوجيز في القانون الجزئي، الطبعة السادسة، دار هومة، الجزائر، 2007،ص445.

2-المساس بمنظومة معلوماتية:

تنص المادة 394 مكرر 1 من قانون عقوبات جزائري و التي يقابلها في النص الفرنسي المادة 3/323 من قانون العقوبات الفرنسي: على ان " كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها."[1]

ب/جريمة التزوير المعلوماتي:

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي الذي يعتبر من أخطر صور الغش المعلوماتي نظرا للدور الهام و الخطير الذي أصبح يقوم به الحاسوب الآن. و نجد أن المشرع الجزائري نص على التزوير الخاص بالمحررات في القسم الثالث و الرابع و الخامس من الفصل السابع من الباب الأوّل من الكتاب الثالث من قانون العقوبات في المواد من 214الى229 التي تشترط المحرّر لتطبيق جريمة التزوير. و لم يتخذ أي موقف لتوسيع مفهوم المحرّر من أجل إدماج المستندات المعلوماتية ضمن المحرّرات محل جريمة التزوير.[2]

ثالثا:مكافحة الجريمة الالكترونية في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال:

يعتبر قانون04/09 المتعلق بالجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها نطاقا شاملا في مجال مكافحة الجرائم الالكترونية. حيث جاء تجريمه للأفعال المخالفة للقانون و التي ترتكب عبر وسائل الاتصال، و بالتالي فهو يطبّق على كل التكنولوجيات القديمة و الجديدة بما فيها شبكة الانترنيت على كلّ تقنية تظهر مستقبلا.

و لقد تبنى المشرع الجزائري بموجب هذا القانون، تعريفا موسعا للجرائم الالكترونية، بعدما كان النظام العقابي يقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، حيث أصبحت تشمل بالإضافة إلى هذه الأفعال أي جريمة أخرى أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية، و بذلك لم يعد مفهوم الجريمة الالكترونية في التشريع الجزائري، يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء بل توسع نطاقها إضافة لتلك الأفعال التي تكون المعلومة.

و قد عرّفت المادة 02 من القانون 04/09 [3] الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال أن جرائم المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات ، و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

رابعا: مكافحة الجريمة الالكترونية في قانون الاجراءات الجزائية الجزائري المعدل بموجب القانون 04-14 المؤرخ في 2004/11/10.

تناول قانون الاجراءات الجزائية موضوع الجرائم الافتراضية من خلال:

[1] -مرزوق نسيمة، جرائم الانترنيت، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006-2009، ص10.

[2] - أمال قارة، المرجع السابق، ص42.

[3] - القانون رقم 04/09، المؤرخ في 2009/02/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، الجريدة الرسمية عدد 47، سنة 2009.

- إحداث المحاكم الجزائية ذات الاختصاص الموسع التي أجازت لها تمديد اختصاصها للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و ذلك في المواد 37، 40، 329 من ق إ ج.
- نصت المادة 16 من هذا القانون على أن تمديد الإختصاص الإقليمي لضباط الشرطة القضائية لمعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كافة الاقليم الوطني.
- التنصيص على قواعد استثنائية للتفتيش في المواد 45-47.[1]
- إمكانية استعمال أساليب خاصة للتحري في هذه الجرائم,
- التنصيص على إمكانية تمديد فترة التوقيف للنظر

المبحث الثاني
صعوبات مكافحة الجريمة الالكترونية

رغم الجهود المبذولة للحدّ من الجرائم الالكترونية، سواء كانت من طرف المشرعين أو من طرف سلطات التحقيق و الضبطية القضائية دولية كانت أو داخلية إلّا أنّ هذه الجهود تصطدم بعدّة عراقيل و صعوبات و التي تتخلّى في المقام الأوّل في اللّامادية الجريمة الالكترونية. و كذا السمات التي يتميّز بها الدليل الذي يستخلص من هذه الجريمة (المطلب الأول).

لا تعتبر صعوبات اكتشاف و اثبات الجريمة الالكترونية و حدّها التي تحدّ من مكافحة الجريمة الالكترونية بل هناك صعوبات أخرى تلك المتعلقة بالجانب القضائي و المتعلقة بالقانون الواجب التطبيق و تحديد المحكمة المختصة بمتابعة مرتكبي هذه الجرائم، و الذين في معظم الأحوال يكونون أشخاص من خارج حدود الدولة (المطلب الثاني).

المطلب الأوّل:
صعوبة اكتشاف و إثبات الجريمة الالكترونية:

تتسم الجريمة الالكترونية بكون محلها معلومات أو برامج معالجة آليا عبر الحاسوب، أو جرائم تتعلق بالأشخاص عبر عالم افتراضي غير متناهي و غير محدود مما يعطيها طابع خاص ليس فقط في طريقة ارتكابها بل كذلك في الوسيلة التي ترتكب بها، الأمر الذي ينجم عنه صعوبات في اكتشاف الجريمة الالكترونية (الفرع الأوّل).

تؤدي صعوبة اكتشاف الجريمة حتما إلى صعوبة اثباتها. فالمجرم يسعى بشتى الطرق لكي لا يترك وراءه آثار تدلّ على ارتكابه للجريمة، و بالتالي تكون عملية الاثبات صعبة. لكن الصعوبة تتجلى أكثر في نطاق الجرائم الالكترونية في ظل لا ماديانها، الأمر الذي يجعل اسناد الفعل الغير مشروع إلى المجرم شبه مستحيل (الفرع الثاني).

الفرع الأوّل
اكتشاف الجريمة الالكترونية

يعترض اكتشاف الجريمة الالكترونية العديد من الصعوبات و ذلك راجع إلى ما هو متعلّق بفقدان الآثار المادية للجريمة، لأنه في غالب الأحيان الجريمة الالكترونية لا تترك

1- راجع المادتين 45و47 من القانون رقم 04-14 المؤرخ في 2004/11/10 المتضمن قانون الاجراءات الجزائية الجزائري المعدل.

آثار مادية خلفها، و منها ما هو راجع إلى التكتم الذي تنتهجه جهات المجنى عليها، كما يلعب نقص الخبرة التي يتميّز بها أفراد سلطات الاستدلال دورا هاما في عدم اكتشاف هذا النوع المستحدث من الجرائم.

أوّلا/ عدم ظهور الدليل المادي:

إنّ الجريمة الالكترونية تتم في بيئة لا علاقة لها بالورق أو المحررات، فعن طريق كليك بسيط يمكن تغيير الكثير من المعلومات في وقت قصير فيصعب استخلاص الدليل المادي لهذه الجريمة لأنه عالم غير واقعي.

فهناك الكثير من المواقع التي تحث على الإرهاب و الانتحار، ولا يعرف حتى مالكها الحقيقي لذا لا بدّ من وضع أجهزة مراقبة و برامج لتفادي اختراق القرصنة و تأهيل المحققين. و من مبررات عدم ظهور الدليل المادي هو أننا نتعامل مع معلومة، هذه المعلومة هي الوسيلة لاقتراف الجريمة، المعلومة التي كانت في الأصل فكرة جسدت في قالب فني، و لقد أكدت احصائيات أمريكية أنّ الموظفين العاملين بالمؤسسات التي تعتمد على نظام المعلوماتية هم الذين يقومون باختراق أجهزة المؤسسات و الاختلاس لدرايتهم بالثغرات الأمنية الموجودة و التعامل معها، و بالتالي عدم إمكانية ظهور الدليل المادي، و يعمل المجرم المعلوماتي على التخطيط الجيّد من أجل عدم ترك دليل مادي، حتى و إن تركه فإنّه بإمكانه العودة و محوه و طمس آثاره قبل وصول أيدي العدالة إليه.[1]

ثانيا/ فرض الجنّاة لتدابير أمنية:

يعمد المجرمون عبر الانترنيت عادة إلى اخفاء جرائمهم و ازالة آثارها عن طريق التلاعب بقواعد البيانات و القوائم بجهاز الكمبيوتر و البرامج، و على هذا الأساس ينطلق فقهاء القانون الجزائي على الشخص الذي يرتكب الجرائم الالكترونية مصطلح المجرم الالكتروني، تمييزا له عن المجرم التقليدي و هو الشخص الذي لديه مهارات، و يصنفون ضمن فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم الغير المشروعة قبل ارتكابها لكي لا يقعوا تحت طائلة العقاب. فهم حقيقة يزيدون من صعوبة اجراءات التفتيش التي نتوقع حدوثها للبحث عن الأدلّة التي تدينهم و ذلك عن طريق دس تعليمات بطريقة يستحيل على غيرهم الإطّلاع عليها.[2] و يتعذر على جهات التحري و الضبط إلى الوصول إلى كشف أعمالهم و أفعالهم الغير المشروعة و بالإضافة إلى ذلك فهم ينتحلون شخصيات و يخفون هويتهم الحقيقية حتى لا يتم التعرف عليهم في حالة اكتشاف الجريمة.

ثالثا/ التكتم عليها من قبل الجهات المجني عليها:

إنّ عدم الإبلاغ يزيد من صعوبة اكتشاف الجريمة الالكترونية، لأن الجهات المجني عليها غالبا ما تكون مصرفا أو مؤسسات مالية، شركة أو مشروعا صناعيا ضخما تلتجئ إلى التكتم على مثل هذه الجرائم إن تعرضت لها و لا تبلغ السلطات المختصة في مكافحة الجريمة و تحرص جهات المجني عليها على عدم الابلاغ من أجل اخفاء أساليب ارتكابها للحيلولة دون تقليد الآخرين للجناة محاكاتهم في جرائمهم.[3]

---

[1] -عبد الفتاح بيومي حجازي، المرجع السابق، ص34.

[2] - علي محمود علي حمودة، المرجع السابق، ص20.

[3] -موسى مسعود رحومة، "الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبرالوطنية"، المؤتمر المغاربي الأول حول المعلوماتية و القانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص3.

إنّ عدم الإبلاغ بعمليات الخرق التي يقوم بها المجرم الالكتروني خوفا على سمعة المؤسسة أو الشركة، و خصوصا التجارية و هروب الزبائن من التعامل معها. إنّ هذا الإبلاغ بعمليات يتسرّب إلى المجرم الالكتروني، و بالتالي تكشف الثغرات الأمنية في النظام المعلوماتي. و تظل الجريمة الالكترونية مستمرة ما لم يتم الإبلاغ عنها، و من ثم تحريك الدعوى الجنائية، و الصعوبة التي تواجه أجهزة الأمن و المحققين هي أنّ هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة العادية كما هو الحال في الجريمة التقليدية.[1]

رابعا/ نقص خبرات سلطات الاستدلال:

إنّ صعوبة اكتشاف الجريمة بالدرجة الأولى مرده إلى نقص خبرة المحققين مما يضعنا أمام معادلة غير متكافئة طرفها أجهزة التحقيق بنقص خبرتها في مجال الكمبيوتر و الانترنيت، و الطرف الآخر قراصنة محتلون و منحلون أخلاقيا يتمتعون بمهارات عالية يواكبون كل جديد في العالم الالكتروني.[2] و قد وصل بعض المجرمون المعلوماتيون الإطلاق على أنفسهم تسمية "النخبة"، أما رجال الشرطة فقد أطلقوا عليهم اسم "الضعفاء"، و نلاحظ أنّ عمليات سن التشريعات أبطأ من عملية الإجرام و هذا في العالم كله دون استثناء. و من العوامل المساعدة في نقص الخبرة في الجرائم الالكترونية:

- عدم تخصيص أموال من أجل التأهيل الجيّد للمحققين.
- حداثة الجريمة و خصوصيتها التي لم يعتد عليها رجال الشرطة مما جعلهم قاصرين في مواجهتها.
- ضخامة المعلومات الموجودة على الشبكة و انتشار أجهزة الكمبيوتر مما يصعب عملية التحقيق.
- الانترنيت بيئة خصبة للسلوك الإجرامي.
- التطور السريع للتقنية الحديثة.
- عدم وجود هيئات قضائية مختصة.
- وجود مواقع على الشبكة تسهل عملية ارسال البريد الالكتروني دون الحاجة إلى ذكر البيانات اللّازمة مثل معرفة المرسل.[3]

و يميل الفقه الجنائي إلى القول بضرورة تنمية الخبرة و المهارات للأشخاص المختصين لوضع مناهج مدروسة للتدريب على التحقيق مراعين بذلك خصوصية التطور الفني السريع دون اهمال التعاون الدولي في مثل هذه الحالات.

خامسا/ عدم وجود تعاون دولي:

في ظل الصراعات التي أصبحت شبحا يزعزع أمن و سلامة العالم يصعب إيجاد تعاون دولي حقيقي من أجل مكافحة الجريمة الالكترونية أو حتى التعاون من أجل كشف الجريمة. و لقد تطرقنا سابقا أنّ السلوك الإجرامي قد يرتكب في بلد معين و لكن النتيجة تحدث في بلد آخر، كأن تقوم مجموعة من المجرمين بتشويه معلومات معينة و ليس

[1]- La lutte contre la cybercriminalité n'est pas le monopole de l'état, elle concerne l'ensemble des acteurs publics et privés, les entreprises comme les particuliers qui doivent avoir une démarche citoyenne. Voir les officiers de l'équipe de lutte contre la cybercriminalité de la gendarmerie nationale, OP-cit. p13.

[2] -محمد حماد مرهج الهيتي، التكنولوجيا الحديثة و القانون الجنائي، دار الثقافة، عمان، 2004، ص215.

[3] -عبد الفتاح بيومي جحازي، المرجع السابق، ص122.

بالضرورة أن ينتج هذا السلوك آثاره في بلد المجرمين، و بالتالي فإن التعاون الدولي مهم عند التعامل مع هذه الجرائم لأنه يساعد على تطوير أساليب متماثلة للتحقيق و توحيد قانون جنائي و اجرامي لحماية شبكة المعلومات الدولية.[1]

الفرع الثاني

اثبات الجريمة المرتكبة عبر الانترنيت

تتعلق عملية اثبات الجرائم بصفة عامة بإقامة الدليل، و ذلك بالنظر إلى نوع الجريمة و إلى الاجراءات التي يتم اتباعها للحصول على الدليل. و هذه الخطوات هي المتبعة في كل الجرائم بما فيها الجرائم الالكترونية، غير أن هذه الأخيرة تكون عملية استخلاص الدليل صعبة للغاية نظرا لكون الأدلة في هذا النوع من الجرائم تتميز بخصوصيته المعنوية، بالإضافة إلى ذلك فالإجراءات المتبعة في اثبات هذه الأدلة أثبتت قصورها، فإذا كانت ذات فائدة في الجرائم التقليدية فهي غير موجودة في جرائم الانترنيت في غالب الأحوال خاصة في ظل الطابع العالمي لهذه الجريمة.

أولا/ إعاقة الوصول إلى الدليل:

جناة الجرائم الالكترونية من المجرمين المحترفين الذين لا يرتكبون جرائمهم بسبب الاستفزاز أو الاستثارة، و إنّما هم يخططون لما يفعلون و يستخدمون قدراتهم الفنية و العقلية لنجاح هذا التخطيط، و لذلك نجد أنهم و هم يرتكبون الجرائم الالكترونية يحيطون أنفسهم بتدابير أمنية واقية تزيد من صعوبة كشفهم، و كمثال كذلك نجدهم يستخدمون التشفير و كلمة السر التي تمكنهم من اخفاء الأدلة التي قد تكون ضدهم، و قد يدوسون تعليمات خفية بين الأدلة لتصبح كالرمز فلا يمكن لغيرهم أن يفهم مقصودها.[2]

و قد يقوم هؤلاء أيضا بتشفير التعليمات باستخدام طرق و برامج تشفير البيانات المتطورة مما يجعل الوصول إليها بمنتهى الصعوبة، و ليس يخاف كذلك أنّ هؤلاء الجناة قد يستخدمون الوسائل الالكترونية المختلفة لإعاقة الوصول إليهم، فقد يستخدمون البريد الالكتروني في اصدار تكليفاتهم بارتكاب جرائم القتل و الاغتيالات و التخريب دون أن يتمكن أحد من تحديد أماكنهم أو تسجيل[3] هذه التكليفات على النحو الذي كان يحدث في الاتصالات السلكية و اللاسلكية، كذلك فإن مرتكبي الجرائم الالكترونية يصعب ملاحقتهم لاستحالة تحديد هويتهم سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها لأنهم في الغالب يستخدمون أسماء مستعارة أو عند دخولهم إلى الشبكة ليس عن طريق مقاهي الانترنيت.

يلاحظ أن ملاحقة جرائم الانترنيت قد تتعلق ببيانات تكون مخزنة في داخل دولة أجنبية بواسطة شبكة الاتصال عن بعد و أنه قد يصعب ضبط مثل هذه الأدلة لأن هذا الإجراء يتعارض مع مبدأ السيادة التي تحرص عليه كل دولة، و لعل هذا الأمر يكشف لنا عن أهمية

---

[1] - محمود أحمد عبانية، المرجع السابق، ص120.

[2] - درقاوي عبد القادر، جريمة السرقة في عصر المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان، 2004، ص174.

[3] -علي محمود علي حمودة، المرجع السابق، ص16.

التعاون القضائي الدولي في مجال الإنابة القضائية خاصة في مجال الجرائم العابرة للقارات و التي منها التي تقع بسبب ثورة الاتصالات عن بعد.[1]

ثانيا/ سهولة إخفاء الدليل و محوه:

كما سبق القول فإنّ الجناة الذين يستخدمون الوسائل الالكترونية في ارتكاب جرائمهم يتميزون بالذكاء و الإتقان الفني للعمل الذي يقومون به و الذي يتميز بالطبيعة التي يقومون بها أثناء تشغيلهم لهذه الوسائل الالكترونية، و يستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي يتم تسجيل البيانات عن طريقها. كما أن هناك بعض الأفعال غير المشروعة يرتكبها جناة الوسائل الإلكترونية.[2]ويكون أمرها حكرا عليهم كالتجسس على ملفات البيانات المختزنة و الوقوف على ما بها من أسرار، كما قد ينسخون هذه الملفات و يتحصلون على نسخ منها بقصد استعمالها تحقيقا لمصالحهم الخاصة، كذلك فإنه قد يقومون باختراق قواعد البيانات و التغيير في محتوياتها تجفيفا لمآرب خاصة، و قد يخربون الأنظمة تخريبا منطقيا بحيث يمكن تمويهه كما لو كان مصدره خطأ في البرنامج للمعلومات، و قد يدخلون بيانات غير معتمدة في نظام[3] الحاسب أو يعدلون برامجه أو يحرقون البيانات المخزنة داخله دون أن يتخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل، و مما يزيد من خطورة إمكانية و سهولة إخفاء الأدلة المتحصلة من الوسائل الالكترونية، أنه يمكن محو الدليل في وقت أو زمن قصير، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة جيدة و يدمرها في وقت قصير جدا، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها و في الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده.

و يلاحظ أن المجني عليهم قد يساهمون بدورهم في عدم كشف هذه الجرائم فقد يحجمون عن تقديم الدليل الذي قد يكون بحوزتهم عن هذه الجرائم و قد يكون مقصدهم من ذلك استقرار حركة التعامل الاقتصادي بالنسبة لهم أو رعيتهم في اخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليدها من طرف الآخرين و لعل هذا الأمر تلجأ إليه المؤسسات المالية كالبنوك و المؤسسات الادخارية و شركات الإقراض و السمسرة حيث يخشى القائمون على ادارتها من شيوع أمر الجرائم التي تقع داخلها على زعزعة الثقة فيها.[4]

ثالثا/ غياب الدليل المرئي:

الجرائم الالكترونية التي تقع على العمليات الالكترونية المختلفة قد يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات. فإذا وقعت جرائم معينة على هذه الجوانب المعنوية كجرائم السرقة أو الاختلاس أو الاستيلاء أو الغش أو التزوير أو الإتلاف، فإنه قد يصعب

---

[1] -غازي عبد الرحمان هيان رشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب و الانترنيت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الاسلامية، كلية الحقوق، لبنان، 2004، ص539.

[2] -هشام فريد رستم، "أصول التحقيق الجنائي الفني و اقتراح انشاء آلية عربية موحدة للتدريب التخصصي"، مؤتمر القانون و الكمبيوتر و الانترنيت، المنعقد من 1 إلى 3 ماي 2000، جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، الطبعة الثالثة، 2004، ص429-430.

[3] -محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، و الصعوبات التي تواجهها، دراسة تحليلية لوقائع الاعتداءات التي يتعرض لها الحاسوب و موقف التشريعات الجنائية منها، دار المناهج للنشر و التوزيع، عمان، 2006، ص212.

[4] -حسين بن سعيد الغافري، المرجع السابق، ص19.

اقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة يوجد شك في اثبات الأمور المادية التي تترك آثارا ملحوظة يكون سهلا ميسورا يعكس اثبات الأمور المعنوية.[1]

فإنه يكون بمنتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي آثار قد تدل عليه أو تكشف عنه. بحسب أن أغلب المعلومات و البيانات التي تتداول عبر الحاسبات الآلية و التي من خلالها تتم العمليات الالكترونية تكون في هيئة رموز و نبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو ادراكها إلا من خلال هذه الحاسبات الآلية.

فالجرائم التي ترتكب على العمليات الالكترونية التي تعتمد في موضوعها على التشفير و الأكواد السرية و النبضات و الأرقام و التخزين الالكتروني يصعب \ان تخلف آثارا مادية قد تكشف عنها أو يستدل من خلالها على الجناة. و كمثال لذلك نجد أن التجسس المعلوماتي نسخ الملفات و سرقة وقت الآلة يصعب على الشركات التي تكون الضحية لمثل هذه الأفعال اكتشاف أمرها و ملاحقة الجناة عنها، و لعل هذه الطبيعة الغير المرئية للأدلة المتحصلة من الوسائل الالكترونية الحاسبات، و من ثم يستحيل عليهم الوصول إلى الجناة، فمن المعلوم أن جهات التحري و التحقيق اعتادت على الوسائل التقليدية للإثبات الجنائي الذي يعتمد على الإثبات المادي للجريمة و لكن في محيط الالكتروني الأمر مختلف، فالمتحري أو المحقق لا يستطيع أي متهما تطبيق اجراءات الجريمة و لكن في المحيط الالكتروني الأمر مختلف، فالمتحري أو المحقق لا يستطيع أي متهما تطبيق اجراءات الإثبات التقليدية على المعلومات المعنوية.[2]

رابعا/ صعوبة فهم الدليل المتحصل عليه من الوسائل الالكترونية:

لا شك في أن طبيعة الدليل تنعكس عليه، فالدليل الفني قد يكون مضمونه مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص بعكس الدليل القولي، فإن الكثير ممن يتصلون به يسهل عليهم فهم مضمونه و إدراك حقيقته، و إذا كان الدليل الناتج عن الجرائم التي تقع على العمليات الالكترونية قد يتحصل من عمليات فنية معقدة عن طريق التلاعب في نبضات و ذبذبات الكترونية و عمليات أخرى غير مرئية، فإن الوصول إليه و فهم مضمونه قد يكون في غاية الصعوبة. فالطبيعة غيرالمادية للبيانات المخزنة بالحاسب الآلي و الطبيعة المعنوية لوسائل نقل هذه البيانات تثير مشكلات عديدة في الإثبات الجنائي.[3]

مثال ذلك: إثبات التدليس والذي قد يقع على نظام المعالجة الآلية للمعلومات يتطلب تمكين مأمور الضبط القضائي أو سلطة التحقيق من جمع المعطيات الضرورية التي تساعد على اجراء التحريات و التحقيقات من صحتها للتأكد مما إذا كانت هناك جريمة قد وقعت أم لا.

و مثل هذا الأمر طلب إعادة عرض كافة العمليات الآلية التي تمت لأجل الكشف عن هذا التدليس، و قد يستعصي هذا الأمر فهما على مأمور الضبط القضائي لعدم قدرته على فك رموز الكثير من المسائل الفنية الدقيقة التي من خلال ثناياها قد يتولد الدليل المتحصل من

---

[1] -عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنيت، دراسة متعمقة في جرائم الحاسب الآلي و الانترنيت، بهجات للطباعة و التجلي، مصر، 2009، ص36.

[2] -عبد الرحمان محمد بحر، معوقات التحقيق في جرائم الانترنيت، دراسة مسحية على ضباط الشرطة في البحرين، رسالة مقدمة إلى معهد الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، معهد الدراسات العليا، قسم العلوم الشرطية، الرياض، 1999، ص27.

[3] -عفيفي كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2007، ص365.

الوسائل الالكترونية كذلك فإن الكثير من العمليات الآلية للبيانات التي قد يقوم بها الحاسبات الآلي بطريقة آلية دون الحاجة إليه، أو إجراء تعديلات في برامجه أو القيام بالتلاعب في البيانات المخزنة، و بالنظر إلى أن طبيعة هذه العمليات يصعب أن تخلف وراءها آثارا مادية ملموسة تكشف عنه و المخزنة في برنامج الحاسب قد يكون من السهل اعترافها و ارتكاب جرائم التزوير و استيلاء، تقع عليها عن طريق ادخال البيانات غير معتمدة في نظام الحاسب، فإن ذلك سيزيد من صعوبة عمل المحققين الذين يعملون في حقل الجرائم التي نتفحص عن هذه العمليات الالكترونية.

فقد تستعصي عليهم فهم الأدلة المتحصلة عليها بسبب تعقيدها و صعوبة الامتداد إلى مرتكبي الجرائم الواقعة في سياق مثل هذه العمليات الالكترونية بالوسائل الالكترونية قد تزداد صعوبة، في تلك الحالات التي يتصل فيها الحاسب الآلي شبكة الاتصالات العالمية.[1]

ففي مثل هذه الحالات فإن فهم هذا الدليل يحتاج إلى خبرة فنية و مقدرة على معالجة المعلومات و البيانات بصورة يمكن معها تحديد مكان وجوده و اختيار أفضل السبل لضبطه، و بالنظر إلى أهمية الخبرة في فك غموض الجرائم التي تقع بالوسائل الالكترونية فإن ذلك يكشف لنا عن الأهمية المتزايدة لتدريب الخبراء القضائيين على تقنيات الحاسبات الآلية لتمكينهم من القيام بمهامهم في المسائل الالكترونية الدقيقة و اعداد تقاريرهم الفنية فيها و التي تكون ذات أهمية بالنسبة لقضاء الحكم، لا يغيب عن الذهن فهم الأدلة الفنية التي نتحصل عليها من الوسائل الالكترونية نتطلب تدريب جهات الضبط القضائي و التحقيق.

خامسا/ الضخامة البالغة لكم البيانات فحصها:

يشكل الكم الهائل للبيانات التي يجري في الأنظمة[2] المعلوماتية تداولها أهم الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها، و أنّ طباعة كل ما يوجد على الدعامات الممغنطة يمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التي لا تثبت شيء على الإطلاق. و في مواجهة هذه الصعوبة يسلك المحقق غير المتدرب أحد الطريقين إما بحجز البيانات الالكترونية بقدر يفوق القدرة البشرية على مراجعتها أو التغاضي عن هذه البيانات كلية بأمل الحصول على اعتراف من المتهم و الواقع أننا يمكن مواجهة ذلك بطريقتين أخرتين أيسر في التطبيق و هما إما الاستعانة بالخبرة الفنية لتحديد ما يجب البحث عنه دون سواه للإطلاع عليه و ضبطه، أو الاستعانة بما تتيحه نظم المعالجة الآلية للبيانات بأساليب التدقيق و الفحص المنتظم أو المنهجي، و نظم وسائل الإختبار و المراجعة، بالإضافة إلى أساليب الفحص المنصب بوجه خاص على الحالة أو الواقعة محل البحث و بالإضافة إلى كل هذه العقبات نجد أن هناك عقبة أخيرة تتصل بنقص خبرة الشرطة و جهات الادعاء و القضاء حيث تتطلب كشف الجريمة الالكترونية و التوصل إلى مرتكبيها و ملاحقتهم قضائيا و وضع استراتجيات تحقيق و تدريب و مهارات خاصة يسمح بفهم و مواجهة تقنيات الحاسب الالكتروني المتطورة و أساليب التلاعب المعقدة التي تستخدم عادة في ارتكاب هذه الجرائم.

[1] -هشام محمد فريد رستم، المرجع السابق، ص19.

[2] - عبد الرحمان محمد بحر، المرجع السابق، ص46.

و لذلك وجدت سلطات البحث الجنائي و التحقيق بنفسها غير قادرة على التعامل بالوسائل التقليدية مع هذه النوعية من الجرائم و لنقص الخبرة و التدريب كثيرا ما تخفف أجهزة الشرطة في تقدير أهمية الجريمة الالكترونية لنقص الخبرة في مجال الحاسب الآلي.[1]

المطلب الثاني

صعوبات متعلقة بالجانب القضائي

يفرض الطابع الدولي للجريمة الالكترونية تعاون أكثر من دولة بما أن الجريمة تخترق كل الحدود الإقليمية المعمول بها، غير أنّ الملاحظ في الواقع تصور هذا التعاون الدولي مقارنة بتطور الجريمة، و كذلك الإجراءات التقليدية المطبقة في مجال التعاون الدولي للحد من الإجرام العابر للحدود لم تتطور بتطور التقنية، مما يولد فارق شاسع بين سرعة الجرائم الالكترونية و بطئ الإجراءات المتبعة (الفرع الأول).

انبثق عن الطابع العالمي للجريمة الالكترونية صعوبات أخرى تتمثل في القانون الواجب التطبيق و المحكمة المختصة، حيث أنّ ميزة الجريمة المتعدية خلقت اشكالا حادا انجر عنه تنازع قوانين أكثر من دولة في هذا المجال و كذلك صعوبة تحديد المحكمة المختصة تعتبر اشكالا عويصا حيث ترى كل دولة أن لها الحق في متابعة مرتكب هذه الجريمة لعدة اعتبارات (الفرع الثاني).

الفرع الأول

قصور التعاون القضائي الدولي في مكافحة الجريمة الالكترونية

يعتبر التعاون الدولي في مجال مكافحة الجريمة الالكترونية من بين أصعب المواضيع المطروحة على هذا المستوى و ذلك راجع إلى الاختلافات القائمة في التشريعات و الممارسات بين الدول، و كذلك بسبب العدد المحدود نسبيا من المعاهدات و الاتفاقيات المتاحة للدول بشأن التعاون الدولي، و يعدّ التعاون الدولي بكافة صوره في مجال مكافحة الجرائم الالكترونية، مطلبا نسبيا إلى تحقيقه أغلب الدول إن لم يكن كلها، إلّا أنه ثمة معوقات تقف دون تحقيقه أهمها:

أولا/ عدم وجود نموذج موحد للنشاط الاجرامي:

إن عدم وجود مفهوم عام مشترك بين الدول حول النماذج التي تتعلق بالجرائم الالكترونية يضعف من منظومة القانون الدولي في مجال ضبط هذه الجرائم، و ذلك راجع إلى اختلاف المفاهيم الخاصة بها، لاختلاف التقاليد و الأعراف القانونية الدولية و بالتالي يسهل على الجناة الإفلات من المساءلة الجنائية.[2]، حيث أنّ عدم توفر تعريف موحّد للجريمة الالكترونية يؤدي إلى بقاء أفعالا إجرامية دون تجريم، حيث تكون أفعال في تشريع ما يعتبره جرما، و تكون في تشريع آخر مباحة، بسبب اختلاف تحديد عناصر الجرم المعلوماتي بين الدولتين المعنيتين[3] تثير الطبيعة الدولية للجريمة الالكتروني، مشاكل فيما يخص تحديد القانون الواجب التطبيق، هل هو قانون الدولة التي ارتكب فيها الفعل، أم قانون الدولة التي

[1] - سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003، ص114.

[2] -ايهاب ماهر السنباطي، "الجرائم الالكترونية (الجرائم السيبرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد"، الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، جوان 2007، ص68.

[3] -فريد منعم جبور، حماية المستهلك عبر الانترنيت و مكافحة الجرائم الالكترونية (دراسة مقارنة) منشورات الحلبي الحقوقية، بيروت، 2010، ص215.

ظهرت فيها آثار الجريمة، إضافة إلى تعارض القوانين من الناحيتين الموضوعية و الاجرائية. الأمر الذي يستدعي ضرورة العمل على توحيد التشريعات في مجال مكافحة الجريمة الالكترونية.

ثانيا/ تنوع و اختلاف النظم القانونية الاجرائية:

إن اختلاف طرق التحري و التحقيق و المحاكمة من دولة إلى أخرى، إذ تثبت فائدتها و فعاليتها في دولة ما، و قد تكون عديمة الفائدة في دولة أخرى، أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الالكترونية، التسليم المراقب، و العمليات المستترة.[1]

تعتبر قضية الدودة الحاسوبية لوف باع love bugالتي أعدت في الفلبين عام 2000 و قيل أنها عطلت ملايين الحواسيب في جميع أنحاء العالم. أحسن مثال على اختلاف النهج القانونية بين الدول حيث أعاقت هذه القضية التحقيقات بسبب ان ذلك العمل المؤذي و الضار لم يكن آنذاك مجرما بشكل كاف في الفلبين.[2]

ثالثا/ عدم وجود قنوات اتصال:

إن من أهم الأهداف المرجوة من التعاون الدولي في مجال مكافحة الجريمة الالكترونية هو الحصول على المعلومات و البيانات المتعلقة بها و بالمجرمين. و لتحقيق هذا الهدف كان لزاما على أن يكون نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع الأدلة و المعلومات الهامة التي تفيد في التصدي لهذا النوع من الجرائم.[3]

رابعا/ مشكلة الاختصاص في الجرائم الالكترونية:

ينجم عن اختلاف التشريعات و النظم القانونية تنازع في الاختصاص بين الدول خاصة في اطار الجرائم الالكترونية التي تتميز بكونها عابرة للحدود. فقد يحدث أن ترتكب الجريمة في اقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة لاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الاقليمية.

و تخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي. و قد تكون هذه الجريمة من الجرائم التي تهدد أمن و سلامة دولة أخرى، فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية

كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من اقليم دولة معينة، و تم الاطلاع عليها في دولة أخرى. ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الاقليمية لكل دولة من الدول التي مستها الجريمة.[4]

إن اختصاص القضاء بنظر الجرائم الالكترونية و القانون الواجب تطبيقه على الفعل لا يحضى بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال تكون من قبل أشخاص من

---

[1] - براء منذر كمال عبد اللطيف، ناظر أحمد منديل "التعاون القضائي الدولي في مواجهة جرائم الانترنيت"، المؤتمر العلمي الأول، تحولات القانون العام في مطلع الألفية الثالثة، جامعة تكريت، كلية القانون، العراق، 2009، ص11.

[2] -مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة و العدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم و التكنولوجيا من جانب المجرمين و السلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل، 12 إلى 19 أفريل 2010، رقم A/conf213/9

[3] -براء منذركمال عبد اللطيف، ناظر أحمد منديل، المرجع نفسه، ص12.

[4] - حسين بن سعيد سيف الغافري،"الجهود الدولية في مواجهة جرائم الانترنيت"، ص52-53، مقال متوفر على الموقع التالي:http://www.minshawi.com

خارج حدود الدولة أو أنه تمر عبر شبكات معلومات و أنظمة خارج الحدود، حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها.

-أدى هذا البعد عبر الوطني للجريمة الالكترونية إلى تشتت الجهود و اعاقة التعاون الدولي في مجال التصدي لهذا النوع من الاجرام.[1]

خامسا/ التجريم المزدوج:

يعتبر شرط التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية و الاتفاقات الدولية المعنية بتسليم المجرمين. يجد شرط التجريم المزدوج أساسه في ان الدولة طالبة التسليم تبتغي من وراء طلبها محاكمة من نسب إليه السلوك الاجرامي أو تنفيذ العقوبة المحكوم بها عليه، و هذا يفترض أن السلوك مجرم في تشريعها.[2]

و في ظل التقدم السريع لنظم الحاسب و شبكة الانترنيت تبقى المعاهدات الثنائية و الجماعية بين الدول قاصرة عن تحقيق الحماية المطلوبة لكون أن تطور الجريمة الالكترونية يظهر الأثر السلبي في التعاون الدولي.[3]

سادسا/ الصعوبات الخاصة بالانابة القضائية:

أصبحت الانابة القضائية الدولية من الواجبات أو الالتزامات التي يفرضها القانون الدولي العام على الأمم المتحدة و بموجبها يعهد للسلطات القضائية المطلوب منها اتخاذ اجراء –القيام بالتحقيق أو بالعديد من التحقيقات- لمصلحة السلطة القضائية المختصة في الدول الطالبة، مع مراعاة احترام حقوق و حريات الانسان المعترف بها عالميا، و مقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل و احترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية.

تهدف الانابة القانونية إلى نقل الاجراءات في المسائل الجنائية لمواجهة ما تشهده الظواهر الاجرامية من تطوّر و تذليل العقبات التي تعرقل سير الاجراءات الجنائية المتعلقة بقضايا ممتدة خارج الوطنية. و الانابة الوطنية تجد أساسها في القوانين الوطنية و في الاتفاقيات الدولية و في مبدأ المعاملة بالمثل.

الفرع الثاني

اشكالية تحديد القانون الواجب التطبيق و المحكمة المختصة بالجريمة الالكترونية

تبرز أهمية تحديد القانون الواجب التطبيق و المحكمة المختصة في مجال الجرائم الالكترونية من خلال البعد العبر الوطني الذي تتميز به هذه الجريمة، لأن غالبية الأفعال ترتكب من خارج الحدود أو أنها تمر عبر شبكة الانترنيت، و هو ما يبرز أهمية اختيار مدى ملاءمة قواعد الاختصاص و القانون الواجب التطبيق و ما إذا كانت النظريات و القواعد القائمة على تطبيق على هذه الجرائم أم يتعين افراد قواعد خاصة بها في ضوء خصوصيتها و ما تشيره من مشكلات في حقل الاختصاص القضائي.

أولا/ تحديد القانون الواجب التطبيق:

1-المبادئ التقليدية في تحديد القانون الواجب التطبيق:

أ- مبدأ اقليمية النص الجنائي:

[1] - محمود أحمد عبانية، المرجع السابق، ص35.

[2] -حسن بن سعيد بن سيف الغافري،، المرجع نفسه، ص26.

[3] -عبد الفتاح ليومي حجازي، المرجع السابق، ص105.

يرتبط قانون العقوبات في أية دولة ارتباط وثيقا بسيادتها، بل أنه في الحقيقة أهم مظاهر الدولة في سيادتها على اقليمها، و لذلك يعدّ مبدأ اقليمية النص الجنائي هو من المبادئ المستقرة في قوانين كل دول العالم، و قد تم اعتماده في التشريعات الجنائية لكل الدول.[1]

ب- **مبدأ عينية النص الجنائي:**

يقصد بمبدأ العينية تتبع التشريع الجنائي الوطني للدولة ليطبّق على بعض الجرائم بعينها، و العقاب عليها رغم عدم وقوعها على الإقليم الوطني التي ترتكب في الخارج، بغضّ النظر عن جنسية مرتكبيها، و الهدف من هذا المبدأ هو المساعدة في معالجة قصور و عجز مبدأ الاقليمية.

أ- **مبدأ شخصية النص الجنائي:**

يرى الفقهاء أن لمبدأ شخصية النص الجنائي و

جهان: أحدهما ايجابي و آخر سلبي، أمّا الوجه الايجابي فيعني بتطبيق النص الجنائي على كل من يحمل جنسية الدولة، أو لو ارتكبت جريمته خارج اقليمها، أو الوجه السلبي المبدأ فيعني بتطبيق النص الجنائي، على كل جريمة يكون المجني عليه فيها، منتميا إلى جنسية الدولة و لو كان مرتكب هذه الجريمة أجنبيا و ارتكبها خارج اقليم الدولة.

2-انتفاء المبادئ التقليدية أمام خصوصية الجريمة الالكترونية:

يترتب على عدم تبعية شبكة الانترنيت لأي جهة أو شخص محدد و لعدم وجود مقر لها في دولة معينة، تخضع لرقابتها أو سيطرتها، و نظرا لعدم وجود قانون جنائي موحد يحكم هذه الشبكة، فإن القوانين الجنائية التي تطبّق عليها تتعدّد بتعدّد الدول المرتبطة بها، باعتبار أنّ القانون الجنائي يتعلق بسيادة الدولة.[2]

الأصل هو إقليمية القانون الجنائي، فإذا ما ارتكب شخص ما جريمة عن طريق الانترنيت بداخل الدولة، و تحققت نتيجتها بذات الدولة، فالقانون الواجب التطبيق بلا منازع هو قانون هذه الدولة بغض النظر عن جنسية الجاني أو المجني عليه، فقط، يكفي أن تكون هذه الجريمة على اقليم الدولة سواء كان اقليميا بريا أو بحريا أو جويا.

تطبيق مبدأ الاقليمية يترتب عليه عدم اهتمام الدولة إلا بالجرائم التي تقع على إقليمها، فلا يمتد إلى ما يرتكب خارجه من جرائم و لو كان مرتكبوها من رعايا هذه الدولة، غير أن هذه النتيجة قد لا تتفق مع حماية مصالح الدولة، خاصة فيما يتعلق بالجرائم التي ترتكب عبر الانترنيت[3]

ثانيا/ تحديد المحكمة المختصة:

اختلفت المعايير الفقهية التي اعتمدت لتحديد المحكمة المختصة بنظر الجرائم الالكترونية إلى ثلاث معايير هم:

---

[1] -غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص499.

[2] - محمد عبيد الكعبي، المرجع السابق، ص69.

2-أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة و العقوبة، كلية الحقوق، جامعة بنها، 2009، ص58.

1- معيار الاختصاص المكاني:

تعتمد أغلب التشريعات في تحديد الاختصاص المكاني على إتباع ثلاثة ضوابط هي: مكان وقوع الجريمة، أو محل إقامة المتهم أو مكان ضبطه بإلقاء القبض عليه. و في حالة اجتماع أكثر من ضابط تكون المحكمة التي ترفع إليها الدعوى أولا هي المختصة بنظر الدعوى اقليميا.[1]

ينعقد الاختصاص وفقا لهذا المعيار للمحكمة التي يقع في نطاقها النشاط الإجرامي، و ليس مكان حصول النتيجة بدعوى أن اتخاذ آثار الفعل الاجرامي كمعيار لتحديد مكان وقوع الجريمة، تواجهه بعض الصعوبات بدليل أن معيار وقوع النشاط الاجرامي أدى إلى تيسير عملية الإثبات و جمع أدلة الجريمة و أن المحكمة المختصة في النظر في الدعوى تكون هي القريبة من مسرح الجريمة بالإضافة أن الحكم الذي يصدر يكون أكثر فعالية و يسهل معه ملاحقة الجناة.[2]

هذه القاعدة تثير بعض الصعوبات عند التطبيق، فبالنسبة للجرائم الآنية (الوقتية) لا صعوبة فيها كونها ترتكب و تتم في لحظة واحدة ولذلك تعتبر من اختصاص المحكمة التي وقع الفعل في دائرتها، أما بالنسبة للجرائم المستمرة و التي تظل قائمة كجريمة حبس الأشخاص بغير حق أو اخفاء الأشياء المتحصلة من جريمة يتحدد الاختصاص المكاني (المحلي) بالنسبة لهذه الجريمة بأي مكان قامت فيه حالة الاستمرار أما الجريمة الشبيهة بالجرائم المستمرة، بالنظر إلى ما يداخلها من عنصر زمني، و مثالها الاعتياد، و جرائم الاعتياد و جرائم الشروع، حيث مكانا للجريمة، كل محل يقع فيه فعل من أفعال الاعتياد أو التتابع أو البدء في التنفيذ.[3]

يقصد بمكان اقامة المتهم المحل الذي يوجد فيه محل إقامته الفعلي أو الحكمي، و موطن الإقامة الفعلي هو المكان الذي يقيم فيه المتهم و يسكنه، أما محل الإقامة الحكمي، فهو المكان القانوني الذي يقيم فيه الشخص عادة أو يتواجد به أو يعرف به سيرته و شؤونه.

أما مكان القاء القبض على المتهم فهو غير المكان الذي يتم توقيفه، فمكان التوقيف يعد بمثابة مكان حكمي للمتهم لكن الأمر لن تغدو له أهمية قانونية طالما أن القانون يسوي بين مكان الإقامة و مكان إلقاء القبض، و مكان ارتكاب الجريمة في تحديد الاختصاص المكاني.

إن السلوك الاجرامي و النتيجة الاجرامية يمثلان شطري الجريمة في إطار الجرائم الالكترونية، و بالتالي فإن سلطات و محاكم مكان النشاط الاجرامي و مكان النتيجة تكون مختصة.

1- معيار القانون الأكثر ملائمة:

يرى أصحاب هذا الاتجاه بأنه نظرا للطبيعة الخاصة للجريمة الالكترونية و الأضرار الناجمة عنها التي تمتد لتشمل أكثر من دولة واحدة، فإنه يمكن القول بأنه يجب التوسع في تفسير قاعدة اختصاص محكمة وقوع الضرر، ليجعل الاختصاص لمحكمة الدولة الأكثر تعرضا للضرر بشكل فعلي.[4]

---

[1] -غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص518.

[2] -موسى مسعود أرحومة، المرجع السابق، ص15.

[3] -عبد الفتاح بيومي الحجازي، ص 51-52.

[4] -غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص523.

و من التطبيقات القضائية لذلك ما أعلنته إحدى محاكم ولاية نيويورك بعدم اختصاصها في قضية تزوير ماركات (علامات) تجارية، أقدم عليها موقع ويب أحد وادي الجاز في ولاية ميسوري، و سببت المحكمة قرارها بأن صلاحيتها لا تنشأ منه من داخل هذه الولاية، بل تنشأ فقط إذا ألحق هذا الموقع ضررا فعليا ضمن نطاقها.[1]

2- **معيار الضرر المرتقب: (الافتراضي)**

صاحب ظهور شبكة الانترنيت وجود عالم افتراضي، حيث تسري فيه مختلف المواد المعلوماتية دون إمكانية تحديد وجهتها، و هذا العالم الافتراضي لا يخضع لأي سلطة اقليمية و بالتالي ترتب على هذه الحالة أن الضرر الذي تسببه الجريمة الالكترونية يمكن أن يحدث في أي دولة تكون متصلة بالانترنيت، و هذا هو معيار الضرر المرتقب.

[1] - فريد منعم جبور، المرجع السابق، ص207.

الخاتمة:

تعتبر الجريمة الالكترونية من بين أحدث و أخطر الجرائم التي عرفها العالم و ذلك لما تتميز به من خصائص بخلاف الجريمة التقليدية،فهي نتيجة كل فعل يستهدف سوء استخدام التكنولوجيا الحديثة، ومع غزو الانترنيت دول العالم،أصبح من الصعوبة ضبط وكشف مكان هذه الجرائم كونها عابرة للحدود الوطنية وتتسم بسرعة فائقة دون رقابة من أي دولة .

تتفق كل النظريات والدراسات المنجزة حول نقطة أساسية تتمثل في الغاية المادية البحتة التي يسعى إليها المجرم الالكتروني من سطو على الأموال،إلى الاعتداء على البيانات السرية وتدمير البرامج المعلوماتية لأية دولة لتهديدها في أمنها القومي وكذلك ظهور ما يعرف بالإرهاب الالكتروني الذي أصبح هاجسا حقيقيا يهدد سلامة وامن المجتمع الدولي عن طريق التهديد بتدمير أساليب وإستراتيجية الدفاعات الأمنية والاقتصادية للدول وعوائدها المالية.

بالإضافة إلى جرائم الآداب العامة والمساس بالأخلاق من خلال الإباحية الالكترونية التي تجسدها المواقع الجنسية الإباحية خاصة منها الموجهة للأطفال ما دون سن البلوغ.

إن الخصوصية التي تتميز بها الجريمة الالكترونية أدت بمختلف الدول و الهيئات و المنظمات الدولية و الاقليمية إلى تدارك مدى خطورة هذه الظاهرة الاجرامية و مدى التحديات التي تفرضها عليها، الشيء الذي أدى بها إلى المسارعة من أجل وضعها في إطار قانوني وعقد مؤتمرات وإبرام عدة اتفاقيات من أجل مكافحة هذه الجريمة والحد منها.

اصطدمت محاولات التصدي للجريمة الالكترونية بعدة صعوبات، فخصوصية الجريمة و السرعة في تطورها، أدى بأغلب هذه المحاولات إلى الفشل بحيث من الصعب الكشف عنها وتحديد الدليل المادي الذي يدين مرتكبها.

لذلك من المتوقع أن هذا النوع من الجرائم يستمر ويطغى على ساحة الإجرام بقدر كبير وسيتطور مع مرور الوقت إلى ماهو اخطر وأعقد لذا فان وجود إستراتيجية فعالة لدى الدول تحارب هذه الجرائم هي الوسيلة الضامنة لتقليلها ومحاولة التحكم بها،وسن قوانين موضوعية وإجرائية أكثر فعالية سواء على المستوى الوطني أو الدولي كعقد الاتفاقيات ثنائية أو متعددة الأطراف لتفعيل التعاون الدولي لمكافحة هذه الجريمة وتضمين بنودها بموضوع التعاون الدولي والقضائي والأمني نظرا لطابع الجريمة الدولي ووجوب تطبيق وتنفيذ هذه القوانين بصفة مثالية .

وفي الاخير نستنتج أن القوانين التي وضعت من أجل مكافحة الجريمة الالكترونية لم تنل قدرا كافيا من الفعالية مما يتطلب مضاعفة الجهود لمواكبة تطور هذه الجريمة.

قائمة المراجع:

أولا: باللغة العربية:

1-الكتب:

أ- الكتب العامة:

1- أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة و العقوبة، كلية الحقوق، جامعة بنها، 2009.
2- أحسن بوسقيعة ،الوجيز في القانون الجزائي،الطبعة السادسة،دارهومة، الجزائر،2007.
3- أحسن بوسقيعة ،الوجيز في القانون الجزائي العام ، الطبعة الثانية ،دارهومة، الجزائر،2013.

ب-الكتب الخاصة:

1-أشرف عبد القادر قنديل ،الإثبات في الجريمة الالكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2015.

2-زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى للنشر و التوزيع، عين مليلة، الجزائر، 2011.

3-محمد أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر، الأردن، 2005.

4-محمد أمين الشوابكة، جرائم الحاسوب و الانترنيت، الجريمة المعلوماتية، دار الثقافة للنشر، عمان، 2004.

5-محمد واصل حسن بن علي الهلالي، الخبرة الفنية أمام القضاء، دراسة مقارنة، المكتب الفني، عمان، 2004.

6-محمد حماد مرهج الهيني، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، و الصعوبات التي تواجهها، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب و موقف التشريعات الجنائية منها، دار المناهج للنشر و التوزيع، عمان، 2006.

7-محمد عبيد الكعبي، الجرائم النائشة عن الاستخدام غير المشروع لشبكة الانترنيت، دار النهضة العربية، القاهرة،(د ت ن).

8-محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004.

9-محمد فتحي عيد، الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1999.

10-مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، القاهرة، 2008.

11-عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

12-عبد الله بن عبد العزيز اليوسف، أساليب تطور البرامج و المناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

13-عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الانترنيت (الجرائم الالكترونية)، منشورات الحلبي الحقوقية، بيروت، 2007.

14-عبد الرحمان بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية، الحاسب الآلي و شبكة المعلومات (الانترنيت)، دار الوراقين، بيروت، 2004.

15-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنيت، دار الفكر الجامعي، الإسكندرية، 2006.

16- عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنيت، دراسة متعمقة في جرائم الحاسب الآلي و الانترنيت، بهجات للطباعة و التجليد، مصر، 2009.

17-عمرو عيسى الفقي، جرائم المعلوماتية، جرائم الحاسب الآلي و الانترنيت في مصر و الدول العربية، المكتب الجامعي الحديث، الاسكندرية، 2006.

18-ساسي علي حامد عياد، الجريمة المعلوماتية و جرائم الانترنيت، دار الفكر الجامعي، الإسكندرية، 2004.

2-الرسائل و المذكرات الجامعية:

أ- الرسائل الجامعية:

1-تركي عبد الرحمان الموشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فعاليته، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة الأمنية، الرياض 2009.

2-غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب و الانترنيت)، أطروحة أعدّت لنيل درجة الدكتوراه في القانون، الجامعة الاسلامية، لبنان، كلية الحقوق، 2004.

ب-مذكرات الماجستير:

1-دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري و المقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منتوري، كلية الحقوق، قسنطينة، 2013.

2-لعاقل فريال،مذكرة التخرج لنيل شهادة الماستر،الجريمة المعلوماتية في ظل التشريع الجزائري،جامعة أكلي محند اولحاج،البويرة،2016 .

3-محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الانترنيت، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

4-مرزوق نسيمة،جرائم الانترنيت،مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء ،الجزائر،2006-2009.

5-نجاري بن حاج علي فايزة، الآليات القانونية لمكافحة الإرهاب القانوني، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال جامعة مولود معمري، كلية الحقوق و العلوم السياسية.

6-سوير سفيان، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، جامعة أبو بكر القايد، كلية الحقوق و العلوم السياسية، تلمسان، 2011.

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

8-عبد الرحمان محمد بحر، معوقات التحقيق في جرائم الانترنيت، دراسة مسحية على ضباط الشرطة في البحرين، رسالة مقدمة إلى معهد الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، معهد الدراسات العليا، قسم العلوم الشرطية، الرياض، 1999.

9-صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، كلية الحقوق و العلوم السياسية، تيزي وزو،2013/03/06.

10-قارة أمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي و العلوم الجنائية، جامعة الجزائر، كلية الحقوق، الجزائر، 2002.

11-شبراك حياة، حقوق صاحب براءة الاختراع في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية تخصص قانون الأعمال، كلية الحقوق و العلوم الإدارية، الجزائر، (د ت م).

3-المقالات

قائمة المراجع

1-ايهاب ماهر السنباطي، "الجرائم الالكترونية (الجرائم السيبيرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد"، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، يونيو 2007،ص68.

2-الصديق محمد الأمين الضرير، "بطاقات الائتمان"، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة و القانون، جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، أيام 10-12 ماي 2003، المجلد الثاني، ص ص637-658.

3-براء منذر كمال عبد اللطيف، التعاون القضائي الدولي في مواجهة جرائم الانترنيت، المؤتمر العلمي الأول، تحولات القانون العام في مطلع الألفية الثالثة، جامعة تكريت، كلية القانون، العراق، 2009، ص ص1-22.

4-حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنيت، ص ص1-61 مقال متوفر على الموقع التالي: http://www.minshawi.com

5-موسى مسعود أرحومة، "الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية"، المؤتمر المغاربي الأول حول المعلوماتية و القانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص ص 1-25.

6-محمد أبو العلا عقيدة، "التحقيق و جمع الأدلة في مجال الجرائم الالكترونية"، ص ص1-16، مقال متوفر على الموقع التالي:http://arblawinfo.com

7-مليكة عطوي، "الجريمة المعلوماتية"، حوليات جامعة الجزائر العدد 21، 2012،ص13.

8-نائلة عادل محمد فريد قورة – جرائم الحاسب الالي الاقتصادية دراسة نظرية وتطبيقية-منشورات الحاتي الحقوقية،2005.

9-سمير ابراهيم حسن، "الثورة المعلوماتية عواقبها و آفاقها"، مجلة جامعة دمشق، مجلد 18، العدد الأول، 2002.

10-علوي مصطفى، "الصحة المنسية أمام لغة الكبار"، مجلة الشرطة، المديرية العامة للأمن الوطني، العدد 87، جوان 2008.

11-علي محمود علي حمودة،"الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي،ص ص1-74،مقال متوفر على الموقع :http://www.arablawinfo.com

12-فاطمة الزهراء بوعناد، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، كلية الحقوق و العلوم السياسية، جامعة سيدي بلعباس، الجزائر، عدد01، 2013،ص68.

13-رابحي أحسن، "الجريمة الالكترونية: النقطة المظلمة بالنسبة للتكنولوجيا المعلوماتية"، المحكمة الجزائرية للعلوم القانونية، الاقتصادية و السياسية، العدد01، 2011،ص227.

14-خالد محي الدين أحمد، "الجرائم المتعلقة بالرغبة الإشباعية باستخدام الكمبيوتر"الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر،المملكة المغربية، أيام 19-20 جوان 2007، ص37.

4-النصوص القانونية:

1-أمر رقم 10/97 مؤرخ في 1997/03/06 المتعلق بحق المؤلف و الحقوق المجاورة، الجريدة الرسمية، عدد 13 صادر 1997/03/12.

5-قانون رقم 15/04 مؤرخ في 2004/11/10 المعدل والمتمم للامر 156/66 المؤرخ في08جوان1966 المتضمن قانون العقوبات، الجريدة الرسمية رقم 71 صادر 2004/11/10.

6-قانون رقم 22/06 مؤرخ في 20 ديسمبر 2006 المعدّل.

7-قانون رقم 04/09 مؤرخ في 2009/02/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، الجريدة الرسمية، عدد 47، صادر 2009.

8-قانون رقم 02/16 مؤرخ في 08 جوان 2016، المتضمن تعديل قانون العقوبات، الجريدة الرسمية عدد 37، مؤرخ في 22 جوان 2016.

5- المواقع الالكترونية:

1- مدونة الجرائم الالكترونية وأمن المعلومات،خصائص جرائم الانترنيت ، د ت ن، الرابط:
http://ecis-eg.blogspot.com/2015/04/internet-crimesproperties.html.
2- www.oecd- ong.

ثانيا: باللغة الفرنسية:

I-OUVRAGES :

1-FAUCHOUX Vincent-DEPREZ Pierre, le droit de l'internet (loi, contrat et usages), édition Litec, Paris, 2008.

2-KURBALIJA Jovan ,GELBSTEIN Eduardo ,Gouvernance de l internet

Enjeux,acteurs et fractures ,publié par diplofoundation et global knowledje partnership,suisse,2005.

II-ARTICLE :

KELCI Sevgi « vol, fraude et autres infractions semblables et Internet », Revue Lex Electronica, vol 12 n°1, 2007, pp 01-22, disponible sur le site :

http://www.lex-electronica.org/articles/v12-1/kelci.pdf

الفـــهرس.