الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة الدكتور مولاي الطاهر

كلية الحقوق و العلوم السياسية

مذكرة تخرج لنيل شهادة ماستر

بعنوان:

جريمة الانترنت في ظل التشريع المقارن

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر في علم الإجرام

من إعداد الطالب:

معزوز محمد مهدي

تحت إشراف الدكتور:

بن صغير عبد المومن

أعضاء لجنة المناقشة

الدكتور: خنفوسي عبد العزيز ..... رئيسا

الأستاذ: مكي لريبي .....عضوا مناقشا

الأستاذ : قميدي فوزي .....عضوا مناقشا

الدكتور: بن صغير عبد المومن ..... مشرفا و مقررا

السنة الجامعية

2014 -2015

كلمة شكر

إلى الشموع التي ذابت في كبرياء أساتذتنا الكرام لتنير كل خطوة في دربنا

لتذل كل عائق أمامنا

فكانوا رسلا للعلم و الأخلاق

كن عالما، فإن لم تستطع فكن متعلما، فإن لم تستطع فأحب العلماء فإن لم تستطع فلا تبغضهم

و نخص بالتقدير و الشكر الأستاذ بن صغير عبد المؤمن أقول له بشكر الرسول ﷺ

﴿إن الحوت في البحر و الطير في السماء ليذلون على معلم الناس الخير﴾

إلى من زرعوا التفاؤل في دربي و قدموا لي المساعدة و التسهيلات و الأفكار و المعلومات ربما دون أن يشعروا بدورهم بذلك فلهم منا كامل الشكر كما أتوجه بالشكر إلى كل من يقف إلى جانبي و من وقف بطريقي و عرقل مسيرة بحثي وزرع الشوك في طريق بحثي فلولا وجودهم لما أحسست بمتعة البحث

إلى من هم أكرم منا مكانة .... شهدائنا الأبرار إلى كل محبي العلم و المعرفة إلى بلدي الحبيبة " الجزائر "" التي غطتنا سمائها و احتضنتنا بترابها وروت عطشنا بمائها العذب.

شكرا لكم جميعا.

إهداء

بسم الله الرحمن الرحيم :(قل اعملو فسيرى الله عملكم و رسوله و المؤمنين) صدق الله العظيم .

الهي لا يطيب الليل إلا بشكرك و لا يطيب النهار إلا بطاعتك و لا تطيب اللحظات إلا بذكرك و لا تطيب الآخرة إلا بعفوك و لا تطيب الجنة إلا برؤيتك.

إلى من بلغ الرسالة و أدى الأمانة و نصح الأمة إلى نبي الرحمة و نور العالمين ... سيدنا محمد صلى الله عليه وسلم .

إلى من جرع الكأس فارغا ليسقيني قطرة حب إلى من حصد الأشواك عن دربي ليمهد لنا طريق العلم.

إلى القلب الكبير إلى من كلله الله بالهيبة و الوقار إلى علمني العطاء دون انتظار

إلى" والدي العزيز "

إلى من أرضعتني الحب و الحنان إلى رمز الحب و بلسم الشفاء إلى القلب الناصع بالبياض

" والدتي الحبيبة "

إلى من ساهم في إنجاح هذا العمل

عقد ابن القيم رحمه الله مقارنة بين العلم و المال يحسن إيرادها في هذا المقام فقد فضل العلم عن المال من عدة وجوه أهمها إن العلم ميراث الأنبياء و المال ميراث الملوك و الأغنياء.

إن العلم يحرس صاحبه و صاحب المال يحرس صاحبه

إن العلم يزداد بالبذل و العطاء و المال تذهبه النفقات ما دا الصدقات.

إن العلم يرافق صاحبه حتى في قبره و المال يفارقه بعد موته إلا ما كان بصدقة جارية

إن العلم يحكم على المال فالعلم حاكم و المال محكوما عليه يقول الله تعالى:

بسم الله الرحمن الرحيم

﴿ شهد الله أنه لا اله إلا هو و الملائكة و ألو العلم قائما بالقسط ﴾

صدق الله العظيم


مقدمة عامة

المقدمة:

عرف الإنسان الجريمة منذ أول وجود له على وجه الارض،وخير دليل على ذلك جريمة القتل التي وقعت بين ولدي ادم عليه السلام.فالجريمة هي نتاج طبيعي للحياة الجماعية للإنسان،فالاختلاف والتباين بين مصالح الافراد داخل الجماعة أو المجتمع على العموم، يؤدي بطبيعة الحال إلى ظهور منازعات فيما بينهم تتطور في الغالب إلى ارتكاب جرائم مختلفة.

مرت الجريمة عبر مختلف المراحل التي عرفها الإنسان،حيث تطورت بتطوره في مختلف مجالات الحياة،وتغيرت حسب دوافعه وظروفه الاجتماعية،وذلك باختلاف الزمان والمكان،فالجرائم التي كانت ترتكب في وقت مضى لم يعد لها وجود في الوقت الحاضر والعكس صحيح، بالإضافة إلى ذلك فالجرائم التي ترتكب في مكان ما لا ترتكب في مكان آخر وذلك راجع للاختلاف الموجود بين أفراد المجتمع من حيث المستوى الثقافي والعلمي والمادي وفي بعض الاحيان الديني.

تطورت الجريمة بتطور نمط حياة الإنسان، ولقد بلغ هذا التطور أوجه بظهور المجتمعات بمفهومها المعاصر،حيث أن هذه المجتمعات أصبحت تعيش الكثير من المشاكل نتج عنها وقوع الكثير من الجرائم،وذلك جراء الضغوط النفسية وتميز حياة الأفراد بطبيعة براغبات مادية،حيث أصبح الفرد داخل هذه المجتمعات يسعى بشتى الطرق للوصول إلى إشباع رغباته الشخصية،حتى ولو وصل به الأمر إلى إرتكاب العديد من الجرائم تكون نتائجها وخيمة على الافراد بصفة خاصة وعلى المجتمع بصفة عامة.

لم يقتصر تطور نمط حياة الفرد داخل المجتمع فحسب،بل تعداه إلى أكثر من ذلك، خاصة بظهور مفهوم الدولة بصورتها الحديثة،حيث نتج عنه ظهور مجتمع دولي تربط بينه الكثير من المعاملات تجارية كانت أو سياسية أو حتى عسكرية،هذا التطور على المستوى الدولي لم يمر هو الاخر بسلام على الإنسانية جمعاء،فالجريمة ومن ورائها المجرمين استغلوا هذا الوضع ليجعلوا للجريمة طابع تعدى الحدود.

أدى إكساب الجريمة للبعد عبر الوطني إلى عتبارها من الاعمال التي أضحت تهدد

ستقرار والامن العالميين،ذ ي جةلتشبعها عبر الحدود ا لوطنية،وذ لك نظرا لظور أنماط جد يدة أومستحدثة لم يعرفها العالم من قبل، ح يث طَ بح المجرمون يستغلون مختلف ا لوسا ئل التي أ نجتها هذا العصر في تطوير وتوسيع نشاطاتهم الإجرامية.

يقف وراء هذا التوسع العديد من العوامل،ولعل في مقدمتها التقدم العلمي في مجال عق ات بين الدول ع وجه الخصوص،فلقد ألغى التطور في هذ ا المج ل الفواصل بين الدول، و أوجد إحساسا واعيا لدى الشعوب بوهمية الحد ودالموضوعية،وبانها جزء من عالم واحد.

صاحب التطور الذي عرفه المجتمع الدولي في مجال تكنولوجيا الاتصالات،تطور كبير في مجال شبكات الاتصال،حيث أصبحت هذه الشبكات من بين أهم الوسائل التي تتم بها المعاملات على المستوى الدولي،مما أضحى من الصعوبة بما كان أن يستغنى عليها، ولعل من أهم الشبكات الاتصالية التي ت أخذ حيزا كبيرا في الحياة اليومية لمعاملات الافراد والدول على حد سواء شبكة نت.

شملت استعمالات الإ نت في الاونة الاخيرة مختلف نشاطات الإنسان التجارية بالإضافة إلى مجالات التعليم والترفيه، و لق د أخ ذت أثارها في البروز بشكل جلي في مجال الاتصالات،ونبادل الافكار والمعلومات،بشكل جعل الحدود الجغرافية تن عدم وتتلاشى، و من خلال هذا النشاط الإنساني عبر شبكة الإنترنت ظهرت الأنشطة الإجرا مية عبرها.

في بداية استخدام الانترنت لم يكن أحد من مخترعها يعلم أنه في يوم من الايام سوف ستعمل هذه الوسيلة الاتصالية في الإجرام. حيث كان الغرض من اختراعها في بادئ الامر هو استعمالها في مجالات عسكرية أو بحثية ، لكن مع مرور الوقت أصبح يعتمد عليها في مختلف مناحي الحياة، حيث ان نزايد عدد المشركين من خلالها عبر العالم، يعتبر من بين أكثر الاسباب التي أ ت إلى ظهور ذا النوع من الإجرام. وذلك راجع إلى التباين الموجود بين مستويات ونوايا هؤلاء المشتركين.

تطورت الجريمة المرتكبة عبر الإن نت بشكل رهيب في المدة خ رة، وذ لك بالنظ ر إلى التطور المستمر والمتسارع لشبكة الإنترنت،مما جعل هذه الشبكة وسيلة مثالية لتنف يذ العد يد من الجرائم بعيدا عن أعين الجهات الامنية. حيث مكنت الإنترنت العديد من المجرمين والجماعات الإجرامية من القيام بعدة أفع ل غير مشروعة مستغلي ن مختلف التسهيلات التي

ت قمـلذه الشبكة وذلك بدون أدنى مجهود وبدون الخوف من العقاب.وهو ما دفع ا العـ يد منالدول والهيئات والمنظمات إلى التحذير من خطورة هذه ا لظـارة التي تهدد كل مستخدمي ن تحيث.أصبحت من أسهل الوسائل التي يعتمد عليها مرتكبي الجريمة.سعت المجتمعات إلى الحد من الجريمة المرتكبة عبر الإنترنت، و ذلكلماتشكله هذه الظاهرة من إشكالات قانونية واقتصادية واجتماعية معقدة. فكماواكبت المجتمعات تطور الجريمة التقليدية بالتصدي لها وردعها عن طرق سن القوانين والتشريعات، دأبت كذلك على فعل نفس الشيء مع الجريمة المرتكبة عبر الإنترنت، وذ لكبالطنى إليها بالدراسة والتحليل من أجل وضعها في إطار ق انوي يمكن منخلاله وضع الط قالسليمة لمكافحتها.

تجسدت بداية مكافحة الجرائم المرتكبة عبر الإ ن تبالتطبيق عليها النصوص القانونية القائمة بمختلف فروعها. وذلك تفاديا لإفلات الجاني من جهة. وعدم وجود قوا نن خاصة بهذا النوع من الإجرام من جهة أ خىغأن حداثة الجريمة والسرعة في ارتكابها وتطورها جعل هذه القوانين غير مواكبة لها. وبالتالي أضحت غير مجدية في ما يخص مكافحة الجريمة المرتكبة عبر الإنترنت، مر الذي أدى بالدول وخاصة المتقدمة منها إلى المحاولة لإيجاد صيغقانونية يمكن من خلالها الحد من هذه الجرائم المستحدثة.

غير أن شكال الذي تاتى من هذه الوضعية هو في أي فرع من فروعالقانون يمكن إد ماجذه النصوص. حيث ذ بتتشريعات إلى إدماجها في نطاق قوانين العقوبات بما أن الجريمة تدخل في صلب هذه الاخية ، و أخرىاعتبرتها قوانين خاصة ليس لها علاقة بالعالم التقليدي، بلهي قوانين موضوعة خصيصا لمواجهة ظاهرة إجرامية مستحدثة لم يعرفها القانون من قبل.

ظهرت في خضم هذا التباين في الرؤى بين الت شرعات.اختلافات في دراسات الفقهاء للظا رة جرامية عبر الشبكة العالمية للإ نت.فهناك جانب من هؤلاء الفقهاء من اعتبر الجريمة المرتكبة عبر الإنترنت هي امتدا دللجرائم التقليديةو ذلك بـ لمـتملامـ مـظور تطور ا ريمة من حيث الـ ملن.فـا ريمة في نظرهم مواكبة لتطور الإنسان في مختلف مناحي الحياة.وبالتالي أ يظـا رة إجرامية مستحدثة تعـ ـت امـتـ اد لذا التطور.

ذهب جانب أخر من الفقه إلى اعتبار الجريمةالمرتكبة عبر الإنترنت أنها جريمةمستقلة بذاتها، وذلكبانفرادها بمجموعة من الخصائص والسمات ،بالإضافة إلى أنالمجرم الذي يقوم بهذه الجرائم يختلف عن نظيره في الجرائم التقليدية. فبالرغم من إمكانية إرتكاب جرائم تقليدية مختلفة مثل السرقة عبر الإنترنت،إلا أنها تنفردبجرائم لم تعرفها الشرعيات من قبل،وبالتالي تعتبر الجريمة المرتكبة عبر الإنترنت في نظر أصحاب هذا الرأي أنها جرائم لا علاقة لها بالعالم التقليدي، لأنها جرائم ترتكب في عالم مختلف ألا وهو العالم الافتراضي.

أدى هذا التباين في الرؤى بين القانونيين والفقهاء فيما يخص طبيعة هذه الجريمة إلى التساؤل عن:

خصوصية الجريمة المرتكبةعبر الانترنت والطرق الفعالة لمكافحتها في التشريع الجزائري والمقارن؟

ومن أجل الإجابة عن هذه الإشكالية ارتأينا تقسيم بحثنا إلى فصلين تطرقنا إلى الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت(الفصل الأول)،ثم إلى مكافحة الجريمة المرتكبة عبر الإنترنت (الفصل الثاني)،معتمدين عند معالجتنا لها على منهج يجمع بين المقارنة والتحليل.


الفصل الأول

تمهيد:

ظهر الحاسب الآلي كنتاج للتطور العلمي والتقدم التقني، الذي أدى إلى تدخل أنظمة المعالجة الآلية للمعلومات في كافة مجالات الحياة اليومية، نظرا لما يتمتع به الحاسب من قدر فائقة على تخزين أكبر قدر من البيانات و المعلومات، كما أوجدت الشبكات المعلوماتية وخاصة شبكة الإنترنت واستخدامها في نقل ونبادل المعلومات فجرا جديدا تمثل في بروز ما اصطلح على تسميته بالمجتمع المعلوماتي[1]

عرف رواج الإنترنت كوسيلة للاتصالات واستعمالاها في جل المعاملات اليومية ظهور سلبيات عديدة، خاصة بعد استغلال الكثير من المجرمين هذا التغير في نمط المعاملات مما أسفر على ظهور جرائم لم يكن يعرفها القانون من قبل انفراد الجريمة المرتكبة عبر الإنترنت بطبيعة خاصة بها، والتي استمدتها من الوسيلة التي ترتكب بها الا وهي الشبكة العالمية للإنترنت، وضع المشرع في مختلف أنحاء المعمورة في موضع المتفرج رغم المحاولات التي جاء بها، فإذا كانت الجرائم التقليدية قد نالت جانبا من الاعتناء، وذلك بتحديد مختلف المفاهيم والتعاريف الخاصة بها، إضافة إلى طرق مكافحتها، فإن الجريمة المرتكبة عبر الإنترنت مازالت قيد البحث من طرف الفقهاء والقانونيين.

بدورنا وفي خضم هذه البحوث التي تحاول وضع إطار يتم من خلاله تحديد الجريمة المرتكبة عبر الإنترنت ضمن قالب قانوني، سوف نعمد إلى تبيان ماهية الجريمة المرتكبة عبر الإنترنت (المبحث الأول)، ثم الطبيعة القانونية لهذه الجريمة (المبحث الثاني)

1: غازي عبد الرحمن هيان رشيد، الحماية القانونية من جرائم المعلوماتية(الحاسب و الإنترنت)، أطروحة لنيل شهادة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص92.

المبحث الاول : ماهية الجريمة المرتكبة عبر الانترنت

تعتبر الجريمة المرتكبة عبر الإنترنت من الآثار السلبية التي خلفتها التقنية العالية.حيث أخذت هذه الظاهر الإجرامية حيزا كبيرا من الدراسات من أجل تحديد مفهومها، مما انجر عنه وضع عدة مصطلحات للدلالة عليها، من بينها جرائم الحاسب، جرائم التقنية العالية، جرائم المعلوماتية، جرائم الغش المعلوماتي. وصولا إلى جرائم الإنترنت[1] . و يعتبر عدم الاستقرار على مصطلح واحد للدلالة على الجريمة المرتكبة عبر الإنترنت، من الصعوبات الواردة عليها، مما استوجب وضع مفهوم موحد لها (المطلب الأول).

أدى تطور العلوم الجنائية في ظهور عدةنظريات في علم الإجرام، و من بين أهمها تلك المتعلقة بطبيعةالمجرم. فعلى سبيل المثال التطور الذي عرفته الجريمة الاقتصادية نتج عنها ظهور أفراد الجريمة المنظمة، و بالتالي أصبح من الطبيعي ظهور نظريات جديدة تواكب التطور في مجال الاتصالات وخاصة شبكة الإنترنت، و التي أظهرت فئات جديدة تختلف عنالفئات الإجرامية التقليدية و المتمثلة في فئة مجرمي الإنترنت (المطلب الثاني).

المطلب الاول : مفهوم الجريمة المرتكبة عبر الإنترنت

عرفت الجريمة بصفة عامة على أنها كل فعل غير مشروع صادر عنإرادة اثمة يقرر له القانون عقوبة أو تدبيرا احترازيا، و تعتمد الجرائم الناشئة عنالاستخدام غير المشروع لشبكة الإنترنت على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم[2] .

1: DEBRAY Stéphane. Internet face aux substances ilicites : complice de Ia cybercriminalité ou outil de prévention? , DESS média électronique & internet, Université de Paris 8,2002-2003,p08

2 محمد عبيد الكعبي. الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت. دار النهضة العربية. القاهرة.ص.32

الفرع ول: التعريف بالجريمة المرتكبة عبر الانترنت

أ ت لدا ثةالتي تتميز بها الجريمة المرتكبة عالإنترنت. و اخ تلاف النظم القانونية والثقافية بين الدول، إ عد مإتفاق على مصطلح موحد للدلالة عليها. وعدم نفاق هذا انجر عنه عدم وضع تعريف موحد لهذه الظاهر الإجرامية و ذ لكخشية حرافي مجـ لضيق[1]، و لذلك نجد الفقه قد انقسم إلى أربعة اتجاهات توم على أسس مختلفة في تعريف الجريمة المرتكبة عالإنترنت وهي[2]:

ألا: اساس وسيلة ارتكاب الجريمة

تعتمد هذه التعريفات على وسيلة ارتكاب الجريمة، فطالما أنوسيلة ارتكاب الجريمة هو الحاسوب أو إحدى وسائل التقنية الحديثة المرتبطة به فتصير من جرائم الإنترنت و من ذلك تعريف مكتب تقييم التقنية في الولايات المتحدة الامريكية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا

عرف بعض الفقه [3] الجريمة المرتكبة عبر الانترنت بأنها:

« هي نشاط إجرامي تستخدم فيه التقنية الالكترونية (ا لمسوبالآلي الرقمي و شبكة الانترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل جرامي لمدف»[4]

بصياغة أخرى عرفها البعض الاخر[5] بأنها:

«جرائم الانترنت تعني جرائم الشبكة العالمية ا ليستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة مثل استخدامه في النصب و الاحتيال و غسل الاموال وتشويه السمعة و السب.»

1: محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004 .ص43.

2 غازي عبد الرحمن هيان الرشيد، المرجع السابق، ص106

3: مصطفى محمد موسى، أساليب الجريمة بالتقنية الرقمية(ماهيتها، مكافحتها)، دار الكتب القانونية، مصر، 2005 .ص56

4: كحلوش علي ،« جرائم الحاسوب وأساليب مواجهتها»، مجلة الشلالة، تصدر عن المديرية العامة للأمن الوطني، العدد 84، جويلية 2007 .ص51.

5: مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة، 2009 .ص112

تعرف جرائم الإنترنت أنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالكمبيوتر و الإنترنت في أعمال و أنشطة إجرامية بهدف أن تحقق عوائد مالية ضخمة يعاد ضخها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الإلكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الإنترنت أو تداول الأسهم وممارسة الانشطة التجارية عبر هذه الشبكة، و قد عبر خبراء المنظمة الاوروبية للتعاون الاقتصادي عنجريمة الإنترنت بأنها كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يربط بالمعالجة الالية للبيانات أو بنقلها[1].

تعتبر جرائم الإنترنت من هذا المطلق أي فعليرتكب متضمنا استخدام الحاسب الالي او الشبكة المعلوماتية، أو بمعنى خر هي كل فعلىغير مشروع يكون علم تكنولوجيا الحاسبات لية بقدر كبير لازما لارتكابه[2]، و يعتبر هذا التعريف بالغ العمومية والاتساع، لأنه يدخل فيه كل سلوك ضار بالمجتمع يستخدم فيه الحاسب الالي[3].

لقيتعريف الجريمة المرتكبة عبر الإنترنت المعتمد على الوسيلة المستخدمة في ارتكابها، عدة انتقادات مفادها أنتعريف الجريمة يستوجب الرجوع إلى الفعل و الاساس المكون لها وليس إلى الوسائل المستخدمة لتحقيقها فحسب، أو لمجرد ن الحاسب استخدم في جمة يتعين أنعتبرها من جرائم الإنترنت.[4]

يردفي ذ الإطار الأستاذ Fanderson_R على واضعي هذا التعريف بقوله:

"ليس لمجرد أنالحاسب قد استخدم في الجريمة أنعتبرها من اجرائم المعلوماتية"

والحجة التي اعتمد عليها منتقدي هذ االتعريف مفادها انه لا يمكن وضع تعريف لهذا النوع من الجرائم دون الرجوع إلى العمل الاساسي المكون لا[5]،أي بمعنى اخر لكي

1: عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية) ، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2007 ،ص15

2: عبد الفتاح بيومي حجازي، جرائم الإنترنت (دراسة متعمقة) >>، مجلة الشارقة للعلوم الشرعية و القانونية، المجلد 5، العدد 3، الإمارات العربية المتحدة، أكتوبر 2008 ،ص82

3: عمر بن محمد العتيبي، الأمن المعلوماتي في الواقع الإلكتروني ومدى توافقه مع معايير المحلية والدولية، أطروحة لنيل شهادة الدكتوراه الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010 ،ص21

4: محمد عبيد الكعبي، المرجع سابق، ص34

5: فارة أمال،الجريمة المعلوماتية، رسالة لنيل شهادة ماجستير القانون ، كلية الحقوق جامعةالجزائر ،2002 ،ص19.

تعرف الجريمة يجب الرجوع إلى العمل الاساسي المكون لها، و ليس فقط إلى الوسائل المستخدمة لتحقيقها. و يترتب على ذلك انه لا يكفي أن نعتبر مجرد استخدام الحاسب الآلي في الجريمة. أمن جرائم الإنترنت[1]

ثانيا: المعيار القائم على المعرفة بتقنية المعلومات

يستند أنصار هذا الاتجاه إلى معيار شخصي الذي يستوجب أن يكون فاعل هذه الجرائم ملما بتقنية المعلومات[2]، و من بين هذه التعريفات نجد تعريف وزارة العدل في الولايات المتحدة الامريكية التي عرفت الجريمة المرتكبة عالإنترنت بأنها:

" أية جريمة لفاعلها فنية بتقنية الحاسبات يمكنه من ارتكابها[3]" و من قبيل هذا التعريف جاء تعريف الأستاذ ThomsonDavid لجريمة الإنترنت بأنها: <<أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب>>[4]

عرفها كذلك بعض من الفقه على أنها: << ذلك النوع من الجرائم التي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعلها >>

فمن منظور أصحاب هذه التعاريف استلزموا لتعريف الجريمة المرتكبة عبر الإنترنت توافر سمات شخصية لدى مرتكبها، ولقد حصروا هذه السمات أساسا في الدراية والمعرفة التقنية.

اقتصار تعريف الجريمة المرتكبة عبر الإنترنت على شخصية الفاعل الذي لا بد أن يكون لديه إلمام بالتعامل مع تقنية أجهزة الحاسب الآلي يعتبر قاصرا، إذ لا بد خذ بالاعتبارات أخرى والمتعلقة بموضوع الجريمة[5]، حيث أن قصور هذا التعريف واضح إذ

1: غازي عبد الرحمن هيان الرشيد، المرجع السابق، ص107

2: محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005 ص16

3: محمد عبيد الكعبي ، المرجع سابق، ص34

4: هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني ،جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة 2004 ،ص407

5: منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، رسالة ماجستير العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، الرياض، 2010 ،ص63

أن مجردتوافر المعرفة التقنية بعلم ما لا يكفي في ضوء عدمتوافر العناصر الاخرى لتصنيف الجريمة ضمنالجرائم المتعلقة بذلك العلم[1]

ثالثا: على اساس موضوع الجريمة

يرى واضعو هذا التعريفأن الجريمة المرتكبة عبر الإنترنت ليست هي التي يكون النظام المعلوماتي أداةارتكابها، بل هي التي تقع عليه أوفي نطاقه[2]. ومن أشهر فقهاء هذا الاتجاه الفقيه rosenblatt الذي عرف جريمة الإنترنت بأنها:

[نشاط غير مشروع موجه لنسخ، أو تغيير أو حذف، أو للوصول إلى المعلومات المخزنة داخل الحاسب، أو التي يتحول عن طريقه.[3]

كما عرفت الجريمة المرتكبة عالإنترنت كذلك على النحو التالي :

<< الجريمة المرتكبة عالانترنت هي الجريمة الناجمة عن إدخال بيانات مزورة في نظمةوإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر[4]

سار يتم نظمة مم المتحدة هذا الاتجاه حيث وصفت الجريمة المرتكبة عبر الانترنت بأنها:

«كل تصرف غير مشروع من أجل القيام عملي لتإلكترونية تمس بأمن الانظمة المعلوماتيةو المعطياتالتي تعالجها »[5]

رابعا: اتجاه يأخذ بدمج عدة تعاريف

نظرا لعدم نجاح الاتجاهات السابقة بوضعتعريف شامل للجريمة المرتكبة عبر

---

1 : محمدعلي الكعبي، المرجع السابق، ص34

2 : أحمد خليفة الملط، الجرائم المعلوماتية، دارالفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006 ،ص85 86.

3 : غازي عبد الرحمن هيان ارشيد، المرجع السابق، ص106

4: يونس عرب، جرائم الكمبيوتر و الانترنت، أبو ظبي، 2002 ،ص8

5 :Chawki Mohamed, Essai Sur la Notion De Cyber criminalité 2006,p 7.

الإنترنت يتضمن كافة أركانها. عمد أصحاب هذا الاتجاه إلى تعريفها عن طريق دمج أكثر من تعريف،واعتبروا أن الجريمة المرتكبة عبر الإنترنت هي:

« الجريمة التي يستخدم فيها الحاسب الالي وسيلة أو أداة لارتكابها أو يمثل إغواء بذلك، أو جريمة يكون فيها الحاسب نفسه ضحيتها »[1].

أجرت منظمة التعاون الاقتصادي والتنمية استبيان حول تعريف الجريمة المرتكبة عالإنترنت، الذي تم توزيعه على دول الاعضاء، ولقد ورد في اجابة البلجيكية، بأنها هي:

" كل فعل أو امتناع، من شأنه اعتداء على الاموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة، أو غير مباشرة عن تدخل التقنية المعلوماتية."[2]

وفي تعريف اخر لمنظمة التعاون الاقتصادي للجريمة المرتكبة عالإنترنت بأنها:

« كل سلوك غير مشروع، أوغير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الالية للبيانات أو بنقلها»[3]

تعرضت هذه التعاريف لعدة انتقادات بسبب عدم دقتها في تحديد تعريف الجريمة المرتكبة عبر الإنترنت، إذيكفي وفقا لهذه التعاريف أن يكون السلوك غير اجتماعي أو غير أخلاقي أو ضد المجتمع حيمكن اعتباره من قبيل جرائم الإنترنت، كما أن هذه التعاريف تعتمد وصف الجريمة لا تحديد ماهيتها، ولا تتسع للعديد من الصور الجرمية الممكن اقترافها، و وصف الجريمة لا يعد من المعايير المنضبطة الكافية، لاعتمادها أساسا لتحديد ماهية الفعل الجرمي.[4]

بالرغم من الانتقاد الذي وجه لهذا التعريف إلا أنه يبقى الأنجع من الناحية العملية،

حيث في حين اعتمدت التعاريف الأخرى في تعريفها للجريمة المرتكبة عبر الإنترنت على

1 : غازي عبد الرحمن هيان ارشيد.المرجع لسابق، ص108 ،109.

2 : يونس عرب، جرائم الكمبيوتر و الانترنت، أبو ظبي، 2002 ،ص7

3 : يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها،سلطنة عمان، 2006 ،ص7

4 : محمود أحمد عبابنة،المرجع السابق، ص19

معيارو احد، إذ ـب و لضعوذ االتعريف إلى الاعتماد على دمج كل هذه المعايير، مما يعطيه صفة الكمال ولو نسبيا، في اذ ظلا لأياتي الفقه بتعريف كشمولا.

الفرع الثاني :خصائص الجريمة المرتكبة عبر الانترنت

تعتبر الجريمة المرتكبة عبر الإنترنت من نالجرائم المستحدثة، التي أتى بها التطور في مجال الاتصالات، فهي تختلف عن الجرائم التقليدية والتي ترتكب في العالم المادي، ولذلك فهي تتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يعرفها ا لعا لممن قبل، وسـ ف ذ بنهذه الخصائص التي ميزت الجريمة المرتكبة عبر الإنترنت على النحو التالي:

أولا: خفاءالجريمة و سرعة التطور في ارتكابها

تتسم الجرائم الذ شئة عناستخدام الإنترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة، مثلا عند إرسال الفيروسات المدمرة و سرقة الاموال والبيانات الخاصة وإتلافها، والتجسس وسرعة المكالمات وغيرها من الجرائم.[1]

فجرائم الإنترنت في أكـ صورها خفية لا يلاحظها المجني عليه أو لا يـي ـح بوقوعها والإمعان في حجب السلوك المكون لها وإخفائه طريق التلاعب غير المرئي في الذ ضـ ـكأو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أو سلفي الكثير من الاحوال بحكم توافر المعرفة و الخبرة في مجال الحاسبات غالبا لدى مرتكبها[2].

يستفيد المجرمين في مختلف من الشبكة في تبادل الافكار و الخبرات الإجرامية في مابينهم، و يظهر لنا ذلك جليا في مختلف المواقع الإلكترونية ومنتديات القراصنة (الاكرز) ، التضمن لهم الاتصال فيما بينهم من أجلتبادل المعارف والخبرات في مجال القرصنة وذلك من أجلارتكابهم لجرائمهم بعيدا عـن أعـ من.

1: محمدعبيد لكعبي، المرجع سابق، ص32

2: تي نعبد لرحمن الموشر، ا لمرجعالسابق ،ص20

تجدرشارةفي هذا الصدد أن الجريمة المرتكبة عبر الإنترنت أسرع تطورا من التشريعات، وذلك راجع إلى التطور التكنولوجي الهائل و المتسارع و الذي تجسده شبكة الإنترنت ،بالإضافةإلى مختلف المؤتمرات التي يعقدها القراصنة و التي تسمح لهم بابتكار وسائل و طرق غاية في التعقيد لم تعرفها التشريعات من قبل وذلك من أجل ارتكابهم لجرائمهم.

ثانيا: اعتبارا أقل عنفا في التنفيذ.

لا تتطلب جرائم الإنترنت عنفا لتنفيذا أومجهودا كبيرا، ف تنفذبأقل جد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صور ممارسة العنف والإيذاء كما هو الحال في جرمةالقتل أو خ ط ف، أوفي صورةالخلع أو الكسر و تقليد المفاتيح كما هو الحال في جرمةالسرقة.[1]

تتميز جرائم الإنترنت بأنها جرائم هادئة بطبيعتها لا تحتاج إلى العنف[2]، بل كل ما تحتاج إليه هو القدرة على التعامل معجهاز الحاسوب بمستوى تق يو ظفي ارتبط فع ل غالمشروعة، و تحتاج كذلك إلى وجود شبكة المعلومات الدولية(نترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكةللقيامجر ائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين، فمن هذا المنطلق تعد الجريمة المرتكبة عالإنترنت من ارائم النظيفة فلا اثار فيها لأية عنف أو دماء و إنما مجردأرقام و بيانات يتم تغييرها منالسجلات المخزونة في ذاكرة الحاسبات الالية و ليس لها أثرخارجي مادي[3]

ثالثا: جريمة عابرة لدود

1 : ذيبلموسى البداينة .دورالأجهزة الأمنية في مكافحة جرائالإرهاب المعلوماتي . المملكة المغربية، 2006 .ص20.

2 : عبدالفتاح بيومي حجازي .عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، ا الر ض، 2007 .ص ص 52

3:سيناء عبد الله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات ا لدولية والوطنية، ا لدار البيضاء،المملكة المغربية، 2007. ص52

عدظهور شبكات المعلومات لم عدهناك حدود مرئية أو ملموسة : ت قفأمام نقل المعلومات عالدول المختلفة. فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أ نظمةيفصل بينها الاف الاميال قد أ تإلى نتيجة مؤداها أنأماكن متعددة في دول مختلفة قد تتأثر بالصدمة المعلوماتية الواحدة في ان واحد. فالسهولة في حركة المعلومات عأنظمة التقنية الحديثة جعل بالإمكان ارت بك عنطريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في د ولة أخرى[1]، وذلك راجع إلى إمجتمع المعلومات لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عشبكات تخترق الزمان والمكان دون أنتخضع لحرس الحدود.

ذ اوقد لا يقتصر الضرر المترتب عنالجريمة على المجني عليه وحده ،وإنما قد يتعداه إ مضرر ن آخرين في دولعدة،و ذا هو الملاحظ من خلال جرائم نشر المواد ذات الخطر الديني أوالاخلاقي أوالامني أوالسياسي أو ا لاجتماعي أو الثقا أوالاقتصادي. لذلك فإنه يجب إيجاد تعاون دولي لمكافحة هذه الجرائم عنطريق المعاهدات والاتفاقيات الدولية[2]

راعا: امتناع المجني عليهم عن التبليغ

لا يتم في الغالب الاعم الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير. لذا نجد أنمعظم جرائم الإنترنت تم اكتشافها بالمصادفة، بل وبعد ، و قطويل من ارتكابها، زد على ذلك أنالجرائم التي لم تكتشف هي أكبكثير من تلك التي كشف ا لمتلرعنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة. والعدد الذي تم اكشافه. هو رقم خطير. وبعبارة أخرى. الفجوة بين عدد هذه الجرائم الحقيقي و ما تم اكتشافه فجوة كبيرة[3].

1 : نهلا عبد القادر المومني. الجرائم المعلوماتية. دار الثقافة للنشر والتوزيع. الطبعة الأولى. عمان. 2008. ص51

2 : محمد عبيد الكعبي . المرجع السابق.ص37.

3 : Grave-Raulin Laurent, Règles De Conflits De Juridictions Et Règles De Conflits De Lois Appliquées Aux Cybers Délit, Mémoire De Master 2 Professionnel Droit De L'internet Publique, Université Paris 2_Pantheon Sorbonne, 2008, P6

تبدى هذه الظاهرة على نحو أكثر حدة في المؤسسات المالية كالبنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة، حيث تخشى مجالس إدارتها عادة من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إتضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها[1].

خامسا: سرعة محو الدليل و توفر وسائل تقنية تعرقل الوصول إليه

تكون البيانات والمعلومات المتداولة عبر شبكة الإنترنت عبارة عن رموز مخزنة على وسائط تخزين ممغنطة، لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا لا سيما و أن الجاني يتعمد إلى عدم ترك أثر لجريمته[2]، ضف إلى ذلك ما يتطلبه من فحص دقيق لموقع الجريمة من قبل مختصين في هذا المجال للوقوف على إمكانية وجود دليل ضد الجاني، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة.[3]

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

يعيق المجرم في جرائم الإنترنت سلطات التحقيق الوصول إلى الدليل بشتى الوسائل، كمسح برامج أو وضع كلمات سرية ورموز وقد يلجأ لشفر التعليمات لمنع إيجاد أي دليل يدينه.[4]

---

1 : تركي بن عبد الرحمن الموشير ، المرجع السابق،ص19

2 : El Azzouzi Ali, Op-Cit, P 20

3 : محمد عبيد الكعبي، المرجع السابق، ص38

4 : محمد عبد الرحيم سلطان العلماء،جرائم الإنترنت والاحتساب عليها، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، الطبعة الثالثة،2004 ص877.

يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم ذلك عادة في لمح البصر و بمجرد لمسة خاطفة ع لوحة المفاتيح بجهاز الحاسوب، عاعتبار أن الجريمة تتم في صور أوامر تصدر إلى الجهاز، وما أن يحس الجاني بأي أمره سينكشف حتى يبادر بإلغاء هذه الاوامر، الامر الذي يجعل كشف الجريمة وتحديد مرتكبها أمرا في غاية الصعوبة.[1]

سادسا: نقص الخبر لدى الاجهزة الامنية والقضائية وعدم كفاية القوانين السارية

تتميز جرائم الإنترنت الكمبيوتر من السمات التي جعلتها تختلف عن غيرها من الجرائم، الامر الذي أدى إلى تغيير شامل في الية التحقيق وطرق جمع الادلة المتبعة من الجهات التي تقوم بعملية التحقيق، و ظهافةأعباء تتعلق بكيفية الكشف عنهذه الجريمة وأدلتها، وكذا القضاء من خلال تعديل الكثير من مفاهيمه التقليدية سواء فيما يتعلق بالأدلة أو تطبيقاتها أو لقوتها في ثبات.[2].

ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فتتطلبه لاكتشافها والبحث عنها، و تستلزم أسلوب خاص في التحقيق والتعامل، الامر الذي لم يتحقق في الجهات الامنية والقضائية لدينا، نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي ضدهذه الظاهرة.

لم تعد قادرة القوانين التقليدية على مواكبة هذه السرعة الهائلة في التكنولوجيا، والتي أ هتإلى تطور الجريمة من خلالها، وظهور جرائم لم تكن موجودة في ا لما ق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها[3]، مما تطلب ندخل المشع لسن قوانن حديثة لمواجهة هذه الجرائم حفاظا على مبدأ الشرعية الجنائية، مع تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوما تيةقادة على التعاون

1 : موسى مسعود ا أرحومة، شاليات جرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، . أكاديمية الدراسات العليا، طراباس، 2009 ،ص3

2 : عبد لرحمن جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة، رسالة ماجستير في القانون ،جامعة النجاح الوطنية، فلسطين، 2008 ،ص58

3 : محمد عبيد لكعبي، المرجع ا لما ق،ص40.

الدولي لمكافحتها[1].

الفرع الثالث: القطاعات التي تستهدفها الجريمة المرتكبة عبر الانترنت

دخلت مختلف القطاعات إعالم المعلوماتية خاصة عدظهور الإنترنت، نظرا للخدمات الكبيرة التي تقدمها، وخاصة باعتبارها تضمن السرعة وتقليص الوقت والتكاليف، إلا أنه بالمقابل أصبحت عرضة لكي تكون ضحية من ضحايا الجريمة المرتكبة عبر الإنترنت، ونذكر من بين هذه القطاعات، القطاع المالي والمؤسسات العسكرية إ جا ،بالاشخاص ا لطبيعين.

أولا: المؤسسات المالية ، وقتصادية

بدأ مفهوم التجار الإلكترونية لسهولة الاتصال بين المط فنولإمكانية اختزال العمليات الوردية والبشرية فضلا عن السرعة في إرسال البيانات وتخفيض تكلفة التشغيل والاهم هو يجاد أسواق أكثر اتساعا، ونتيجة لذلك فقد تحولت العديد من شر لتعمال إاستخدام الإنترنت ، وستفادة من مزايا التجار الإلكترونية، كما تحولتبعا لذلك الخطر الذي كان يهدد التجار السابقة ل يصبح خطرا متوافقا. معال تجار الإلكترونية، ف الاسيلاء على بطاقات الائتمان عبر الإنترنت أمرا ليس بالصعوبة بما كان في سابقه.

اتجهت كثير منالشر ا تالكبير والصغيرة على حد سواء وخصوصا في الدول المتق دمةإلى إنشاء مواقع لها على شبكة الإن نت بغرض الدعاية والإعلان وعرض منتجاتها وخدماتها، أمام لا ينالبشر متعدية بذلك حواجز الحدود الإقليمية ونفتح أبواب معارضها للزائرين طوال الأرع والعشرين ساعة وفي كل أيام الاسبوع، ويوفر استخدام الإنترنت في المعاملات التجارة والنقدية إضافة إ سعة نشار خفض العمالة والتكلفة، حيث تصل تكلفة إنجاز العمليات التجارة عبر الإنترنت في بعض

1: محمدعبد الرحيم ، سلطان العلماء، المرجع السا ق،ص878.

الاحيان إلى خمسة بالمائة فتظمن تكلفة إجازهـ ابا لطق التقليدية.[1]

طبيج الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال والاعمال، مما يجعل هذه الشبكات نظرا لطبيعتها المترابطة، وانفتاحها على العالم، هدفا مغريا للمجرمين، ومما يزيد من إغراء الاهداف الاقتصادية والمالية هو أنها تتأثر بشكل ملموس بالاظبا عدا لما ئدةوالتوقعات، والتشكيك في ةهذه المعلومات أو تخزينها بشكل بسيط يمكن أيؤدي إلى نتائج مدمر،وإضعاف الثقة في النظام الاقتصادي.

يشمل هذا الوضع إحداث خلل واسع في نظم الشبكات التي تتحكم بسريان أشطة المصارف وأسواق المال العالمية، ونشر الفوضى في الصفقات التجارية الدولية، إضافة إلى ذلك يمكن إحداث توقف جزئي أو كلي في م نظوم تكالتجارة والاعمال، بحيث تتعطل الانشطة الاقتصادية وتتوقف عن العمل.[2]

ثانيا: الاشخاص الطبيعيون

طبيج الاشخاص الطبيعيون يعبرون اكثر ضحايا الجرائم الم تكبةعبر الإنترنت، وذلك راجع إلى التزايد المستمر والكبير في أعداد المشتركين من خلال الشبكة العالمية للانترنت، فلمتعد الجرائم المركبة عبر الإنترنت مقتصرة على القطاعات المالية والعسكرية، وبالتالي فإنكثيرا من الاشخاص يتعرضون لجرائم النصب والسرقة والإتلاف ومن الطبيعي أتكون شبكة الإنترنت المجال الخصب لارتكاب تلك الجرائم، حيث أصبحت ملاين الاسرار المتعلقة بالناس سواء كانوا أفو ادعاديين او في مر كزمعينة في متناول كل من يستطيع اختراق شبكة المعلومات التي تنطوي على كل هذه الاسرار[3].

عتبر جرائم الإتلاف عن طرقالفيروسات منأكثر الجرائم التي يتعرض لها الاشخاص الطبيعيون عالبريد الإلكتروني الذي يعتبر من لمالبوابات التي يقفز منها

---

1 : صالح بن محمد ا المسد عبدالرحمن بن ر لشدالمهيني،جرائم الحاسب الآلي الخطر الحقيقي في .صو المعلومة، المجلة العربية للدراسات الأمنية و التدريب، المجلد 15 ، العدد29 ، الرياض، دونسنة ،ص172

2 : علي عدنان الفيل، الإجرام الإلكتروني، منشورات زين الحقوقية، دون بلدونسنة ، الطبعة الأو ،2011 ،ص92_93

3 : محمد محمدشتا ،فكرة الحماية الجنائية لبرامج الحاسب الآلي ، دارالجامعة الجديدة للنشر، الإسكندرية، 2001 ،ص94

القرصنة إلى أجنبي. الاشخاص وتعتبر من اكثر الجرائم التي يتعرض لها الاشخاص أيضا سرقة أرقام بطاقات الائتمان.

تشكل المعالجة الآلية للبيانات الشخصية خطورة اكثر على الحياة الخاصة إذا كانت هذه البيانات منظمه ومرتبطة بشبكة الإنترنت أين يمكن لكل مستعملي الانترنت الإطلاع عليها وحتى بوجه غير مشروع.

تعد جريمة انتهاك الحياة الخاصة من بين الجرائم الاكثر شيوعا عبر الإنترنت والتي يتعرض لها الاشخاص الطبيعيون، ومن أخطر صور هذه الجرائم تلك التي تنطوي على المعلومات المخزنة في الحاسب الآلي بعد استغلالها لأمور شتى بخلاف الهدف الذي جمعت من أجله. حيث تتمثل هذه الجريمة في قيام الجاني بالمعالجة الإلكترونية للبيانات الشخصية قاصدا استغلالها في شأن غير الذي تم جمعها من أجله كأن يتم استخدام المعلومات الإحصائية لخدمة مصلحة الضرائب مثلا، كذلك فإن نقل أو تسجيل المحادثات الخاصة تعد من الجرائم التي تمس الحياة الخاصة، فبعد ظهور الإنترنت بات من المتيسر اختراق هذه الوسائط والتقصت عليها وتسجيلها[1]

ثالثا:المؤسسات العسكرية

لم تقتصر حدود ثورة المعلومات على القطاع المدني بل كان لها أكبر الاهمية في تطوير انظمة الحرب الحديثة و أدت إلى ظهور ما يسمى بحرب المعلومات، حيث يستهدف هذا النوع من الإجرام الاهداف العسكرية والسياسية، فبالرغم من ندرة حدوثه عادة إلا أنه موجود على أرض الواقع، وأحسن مثال عن ذلك منها نجاح الإنجليزي (ديونالد أندرسون) في اختراق موقع البحرية الامريكية وسرقت كلمات السر الخاصة المستخدمة في الهجوم النووي، وأيضا نجاح الالماني (هيس لأندر) في اختراق قاعدة بيانات شبكة البنتاجون واستطاع الحصول على 29 وثيقة متعلقة بالأسلحة النووية([2]).

1 : محمود أحمد عبابنة،المرجع السابق، ص 72

2 : ، محمدسيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، ، دناشري للنشر الالكتروني،2012، ص 35

أضحت الدولة التي تملك المعلومات هي الدولة الأقوى، ولذلك بدأ الاهتمام ينصب على الجاسوسية العسكرية وأصبح بإطلاق الأقمار الصناعية من الجهات العسكرية هو المحور الذي يقوم عليه الاتجاه في تطوير الأجهزة. والمعدات العسكرية. مما استتبع ظهور حروب جديدة تسمى بحرب المعلومات بين الدول.

طبيعة المعلومات من خلال هذه الحروب هي السلاح الرئيسي، وبالتالي أدى ذلك إلى تطوير صياغة التنظيمات الهجومية والدفاعية لحرب المعلومات مما يجعل منظومة القوات المسلحة في الحروب المستقبلية والدفاعية لحرب المعلومات سوف تتكون من قسمين رئيسيين هما:

أ التواجد الفعلي للقوات المسلحة في مسرح العمليات.

ب ظهور حرب اتجاه اخر حرب المعلومات المعنية بتجميع المعلومات و تسيير سبل الحصول عليها و توزيعها بالإضافة إلى احتكارها بشكل مطلق و السيطرة على تدفق المعلومات لقوات الخصم.

تعتمد آليات هذه الحرب على شبكات الحاسب الآلي في نقل المعلومات عن طريق الشبكات ومن خلال الاقمار الصناعية، حيث يؤدي ذلك بدوره إلى تعاظم دور القوات المسلحة ونظم المعلومات في انظمة التسليح نظرا لحتمية وأهمية تخزين البيانات وسرعة معالجتها وعرضها بصورة مناسبة أمام القادة لاتخاذ القرار على أساس أهمية تلك المعلومات[1]

المطلب الثاني: مجرمي الانترنت

ينظر إشبكة الإنترنت دائما بوصفها أداة محايدة، وان مصدر ضعفها وانتهاكها هو الإنسان ذاته، والذي غالبا ما يهيئ الفرصة المناسبة لاستغلال الوسيلة المعلوماتية التي أعدها سواء عن حسن نية أو لا، فجوهر المشكلة مرتبط بذات الإنسان وشخصيته

1 : أيمن عبد الحفيظ، المرجع السابق، ص 42.

ودوافعه التي تحفزه القيام بسلوك إجرامي عشبكة الإنترنت من أجلتحقيق نتيجة إجرامية[1]

ا لفرع ول : اصناف مجرمي الانترنت

أ دى الـ تطورفي مجال استعمال الإنترنت إلى ظهور عدة أصناف من المجرمين يصعب حصرهم تحت طوائف محددة،لكن هذا لا يعني انه لا توجد محاولات في تحد يد مختلفأصناف المجرمين عالإنترنت، بل عالعكس هناك عدة دراسات وأبحاث حاولت وضع قواعد يصنف بها المجرمون كل حسب خطورته الإجرامية، وسوف نحاول بدورنا حصرهم عالنحو التالي:

أولا: طا ئفةالقراصنة.

1) القراصنة الهواة hackers

تضم هذه الطائفة الاشخاص الذين يستهدفون من الدخول إلى أنظمة الحاسبات لية غير المصرح لهم بالدخول إليها، كسر الحواجز الامنية الموضوعة لهذا الغرض. وذلك بهدف اكتساب الخبر ة أو بدافع الفضول أو لمجرد إثبات القدرة على اختراق هذه نظمة[2]

تباينت الآراء حول تصنيف هذه الطائفة، حيث يرى البعض أنه لا يبدو من المناسب أن نصنف هؤلاء ا لشب لبفي الطوائف الإجرامية لأن لديهم ببساطة ميلا للمغامرة والرغبة في الاكتشاف ونادرا ما تكون اهداف افعالهم المحظورة غير شريفة وهم لا يدركون ولا يقدرون مطلقا النتائج ا لمحتملةالتي يمكن أن تؤ ي إليها افعالهم غ المشروعة بالنسبة لنشاط منشآة أو شركة تجارية.[3]

1 : غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص 149.

2 : .طاق إو ليم الدسوقي عطية، الأمن لمعلوماتي، النظام القانوني لحماية المعلوماتي، .دراالجامعة الجديدة للنشر، الإسكندرية، 2009 ،ص180

3 : نهلا عبد القادرالمومني .المرجع السابق، ص81_82

أماالفريق الاخير فذهب إلى أنأفعال هذه الطائفة هي من الافعال المحظورة التي يعاقبها القانون، وذ لكي يستطيع مكافحة هذه الطائفة التي قد ينزلق أفرادها ل لمدخول في طوائف محترفي جرائم الإنترنت، طبافة إحتمالية انضمامهم إ لأضلنم نظم ك، أو أفراد غير شرفاء[1]

2) ا لقو طبةالمحترفين

تعرف هذه الطائفة بالمجرمين البالغين، أو المنضمين المهنيين، أو (crackers)، ومن أبرز سمات وخصائص أفراد هذه الطائفة، بأنهم ذوي مكانة في المجتمع، وأنهم دائما ما يكونوا من المتخصصين في مجال التقنية الإلكترونية، أي أنهم يتمتعون بمهارات، ومع افـفنيةفي مجال الانظمة الإلكترونية، والمعلوماتية تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات[2]

تعكس هذه الفئةاعتداءاتهم ميولا إجرامية خطرة تنبئ عنرغبتها في إحد ث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة، وخبراتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الاول، فقد يحدثون أضرا اكبير، وعادة ما يعود المجرم المحترف بالجريمة عالإنترنت إلى إركاب الجريمة مرة أخرى، حيث تزد د سوابقه القضائية وهو يعيش لسنوات طويلة من عائدات جرائمه، وهذا المجرم لا يـ فضلالافكار المـ تطرفةوإنما الافكار التي تدر عليه الارباح الشخصية[3] والتالي هم أكـ خطورة من ا طـ فن ول لأنهم قد يحدثون

ثانيا: طا ئفةالحاقدين

1 : محمود أحمدعبابنة، المرجع السابق، ص42

2 : محمددباس لحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات ،دار الحامد للنشر والتوزيع، عمان،الطبعة الأولى، 2007 ص73

3 : تركي بن عبد الرحمن المويشر، المرجع السابق،ص32

غالبا ما يطلق عهذه الطائفة المنتق مون، لأن صفة نتق لمو الثار هي ما تتميز به عن بقية الطوائف، وهي الباعث لتصرفاتهم، لأنها تنطلق ضد أصحاب العمل، والمنشات التي كانوا يعملون بها، انتقاما من رب العمل عسوء تقديره لهم.

يرى الباحثون أن لد فلواغراض الجريمة غير متوفرة لدى هذه الطائفة، فهم لا يهدفون إ إثب لدقدراتهم التقنية ومهاراتهم الفنية، ولا يبغون تحقيق مكاسب مادية أو سياسية ولا يفاخرون او يجاهرون انشطتهم، بل يعمدون إإخفاء وإنكار أفعالم ، لا يوجد تحديد فئةعمرية لهم، و لد لبانشطتهم تتم باستخدام تقنيات ،زر اعة الفيروسات، والبرامج الضارة لتخريب الانظمة المعلوماتية، أو إ تلاف كل أو ض معطياته، وألمواقع المستهدفة من الانترنت.[1]

تصنف هذه الطائفة من حيث الترتيب في الخطورة الإجرامية، من ضمن الطوائف الاقل خطورة نمجرمي التقنية المعلوماتية، ولكن ذلك لا يمنع أن ينجمعن بعض انشطتهم، خسائر جسيمة للمؤسسة التي يعملون بها[2]

ثالثا: طائفة المتطرفين الفكريين

ساهم الاختلاف الموجود بين ا لشرق وا لغربأو بن ا لشم الوالجنوب، أو بين الاشتراكيين والرأسماليين، أوحتى بين الأديان أو المذاهب المختلفة لذات الدين في إبرا هذه الطائفة، بمعنى أن تعمد كل طائفة إتاجج الافكار، و ُراء حول مواضيع الخلاف مع الطوائف الاخرى بصرف النظر عنطبيعة هذه الخلافات سواء كانت دينية أو سـ يلمية أواقتصادية[3].

يعرف التطرف في هذا المجال بانه عبارة عن أنشطةتوظف شبكة الإنترنت في نشر وتواستقبال وإنشاء المواقع والخدمات التي تسهل انتقال بتر وجالمواد الفكرية المغذ يةللتطر ف الفكري وخاصة المحرض على العنف أيا ن التيار أو الشخص أو

1 : أيمن عبد الحفيظ، المرجع السابق، ص 34

2 : أحمد خليفة الملط، المرجع السابق، ص 62.

3 : نهلا عبد القادر المومني، المرجع السابق ص85.

الجماعة التي تتبنى أو شجع أو تمول كل ما من شأنه توسيع دائرة ترويج مثل هذه الأنشطة

تجري حاليا حوارات مختلفة بين الاتجاهات الايديولوجية ، أوالدينية أو المذهبية تحت سماء مختلفة منها، حوار الاديان أوصراع الحضارات أوالتقريب بين الثقافات وغيرها، وقد تعمالجدل والنقاش بهذه الامور عبر مواقع الإنترنت، وقد وجدت بعض الافكار أوالآراء المتطرفة صدى لدى أتباعهذه الاتجاهات أو المذاهب أو المذاهب،مما دفع بعض المتشددين إلى سلوكالطريق الإجرامي، وأصبح هناك ما يعرف بالمجرم المعلوماتي المتطرف.

يستعمل المتطرفون كافة المواقع الإلكترونية التي تسعى لتحقيقأغراض دعائية لصالحهم، بما في ذلك الشبكات الإعلامية الإخبارية التي تتبع وترصد نشاطات الجماعة وتنشر بيانات وتصريحات قادتها ، والمنتديات والمدونات التي تقوم بتنشيط الحوار حول موضوعات مختلفة تطرحها الجماعة، و إصدارات إعلامية الالكترونية مثل المجلات التي تصدرها الجماعة على الانترنت حتى و لو بلغات أجنبية.

يستخدم المتطرفون خدمات البريد الإلكتروني المجانية للاتصال بأيمكان في العالم وعادة ما يقوم هؤلاء بالاتصال من مقاهي ومكاتب الإنترنت، والسبب في استخدام خدمة البريد الإلكتروني أنها مجانية ولا يتطلب الحصول عليها سوى إدخال بعض البيانات الشخصية البسيطة والتي تكون دائما على شكل بيانات غير صحيحة.

برزت سمات وخصائص هذه الطائفة، أن المجرم المتطرف لا يسعى لتحقيقهدف شخصي، أو الحصول على نفع مادي له، بل يعمل لتغيير المجتمع ليتماشى و يتوافق معمعتقداتصحته من الافكار و المعتقدات.[1]

1 : أحمد خليفة الملط، المرجع السابق، ص 90.

راعا: طائفة المتجسن

لقد تحولت وسائل التجسس من الطرق التقليدية إلى طرق حديثة استخدمت فيها التقنية الحديثة خاصة مع وجود الإنترنت، وذلك بسبب ضعف الوسائل الامنية المستخدمةفي حماية الشبكات سواء كانت هيئات حكومية أو مؤسسات خاصة. وذلك من خلال اختراق هذه الشبكات والمواقع من قبل الهاكرز،فيقوم هؤلاء في العبث أو إتلافمحتويات تلك الشبكة. هذا من جانب، ومن جانب آخر و هو الاهم. والذي يشكل الخطر الحقيقي على تلك المواقع. فيكمن في عمليات التجسس التي تقوم بها الاجهزة الاستخباراتية للحصول على أسرارومعلومات الدولة ومن ثم إفشائها إ دول أخرى معادية أو استغلالالما يضرالمصلحة الوطنية لتلك الدولة.

خامسا: طائفةمخترقي نظمة

يتبادل أفراد هذه الطائفة المعلومات فيما بينهم، بغية اطلاع بعضهم على مواطن الضعف في الانظمة المعلوماتية، وتجري عملية التبادل للمعلومات بينهم بوساطة النشرات الإعلامية الإلكترونية، مثل مجموعات الاخبار، بل أن أفراد هذه الطائفة يتولون عقد المؤتمرات لكافة مخترقي الانظمة المعلوماتية بحيث يدعى إليها الخبراء من بينهم للتشاور حول وسائل الاختراق واليات نجاحها، وكيفية تنظيم العمل فيما بينهم، ويتبع المخترقون أساليب عدة في عمليات تشويه صفحات المواقع، وتختلف هذه ساليب من موقع لآخر حسب نوع نظام الشغيل الذي يعتمد عليه الموقع[1].

الفرع الثاني: سمات مجرمي الانترنت

يتميز المجرم في الجرائم المرتكبة عبر الإنترنت بسمات وخصائص تميزه عن المجرم في الجرائم التقليدية، فهو مجرم ذو كفاءة عالية في مجال التقنية، فإذا كان المجرم التقليدي يلجا إلى استعمال العنف في غالب الاحيان، بالإضافة إلى عدم احتياجه إلى

1 : أحمد خليفة الملط، المرجع السابق، ص 92

مستوى علمي من أجل القيام بأفعاله. فمجرم الانترنت عكس ذلك، حيث أنه يحتاج فقط إلى جهاز حاسوب موصول بشبكة الإنترنت إلى جانب معرفة ودراية بمختلف الأنظمة المستعملة في هذا المجال، ويمكن حصر هذه السمات على النحو التالي:

أولا: السمات المشتركة بين جميع فئات مرتكبي جرائم الإنترنت.

1) مجرم الإنترنت يتمتع بالمعرفة والمهارة والذكاء.

تعني المعرفة التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها، وإمكانيات نجاحها واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على كافة الظروف المحيطة، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم، وتميز المعرفة بمفهومها السابق مجرمي الإنترنت، حيث يستطيع مجرم الانترنت أن يكون تصورا كاملا لجريمته.[1]

يتمتع مجرمي الإنترنت بقدر لا يستهان به من المهارة بتقنيات الحاسوب والإنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ جريمة الإنترنت يتطلب قدر من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات.

يعتبر كذلك الذكاء من أهم صفات مرتكب الجرائم عبر الإنترنت، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرنامج وارتكاب الجرائم السرعة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبير من الذكاء لكي يتمكن من ارتكاب تلك الجرائم.

إجرام الإنترنت هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف فمجرم الإنترنت يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها أحد

1: طاق إبراهيم الدسوقي عطية، المرجع السابق، ص476-177

سواه وذلك من أجل اخاق الحواجز الأمنية في البيئة الإلكترونية ومن ثم نيل مبتغاه.

2) مجرم الإنترنت يبرر ارتكاب جريمته

يوجد شعور لدى مرتكب فعل إجرام الإنترنت أن ما يقوم به لا يدخل في عداد الجرائم أو بمعنى اخر لا يمكن لهذا الفعل أن يتصف بعدم الاخلاقية وخاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله. حيث يفنى مرتكبو هذه الجرائم بين الاضرار بالأشخاص، الامر الذي يعدونه غاية في اللأ خلاقية و بين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحملنتائج الاعم

فهؤلاء الاشخاص لا يدركون أن سلوكهم يستحق العقاب ويبدو أن الاستخدام المتزايد للأنظمة المعلوماتية قد أنشأ مناخا نفسيا موائما لتصور استبعاد فكر الخير والشر وقد ساعد على عدم وجود احتكاك مباشر بالأشخاص ومما لا شك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل و المجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.

يقوم في كثير من الاحيان العاملون بالمؤسسات المختلفة باستخدام تلك لأغراض شخصية بوصفه سلوكا شاعا بين الجميع لالا ينظر إليه بوصفه فعلا إجراميا، إلا أن ذلك لا يعني أن عدم الشعور بعدم أخلاقية هذه الافعال الإجرامية لدى فئة كبير من مرتكبيها ينفي وجودمجرمين يرتكبون إجرامالإنترنت ومعلى علم وإدراك عدم مشروعية وأخلاقية هذا الفعل، فهناك فئة لديها اتجاه إجرامي خطير وسوء نية واضح ومعلى إدراك بخطورة أفعالهم[1]

1 تركي بن عبدالرحمن المويشير، المرجع السابق، ص28

3 الخوف من كشف الجريمة

يخشى المجرمون عبر الإنترنت بالخوف من كشف جرائمهم وافتضاح أمرهم، وبالرغم من هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي الانترنت بصفة خاصة لما يترتب عن كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الحيان.

تساعد طبيعة الانظمة المعلوماتية نفسها مجرمي الإنترنت على الحفاظ على سرية أفعالهم، ذلك أن الكثير ما يعرض المجرم إلى اكتشاف أمره هو أن يطرأ في أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها في حين أن أهم الاسباب التي تساعد على نجاح الجريمة المرتكبة عبر الإنترنت هي أن الحواسيب إنما تؤدي عملها غالبا بطريقة الية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى، وهو ما يساعد على عدم كشف الجريمة ما دامت جميع خطوات التنفيذ معروفة مسبقا حيث لا يحتمل أن تتدخل عوامل غير متوقعة يكون من شأنها الكشف عن الجريمة[1]

4 الميل إلى التقليد

يبلغ الميل إلى التقليد أقصاه حينما يوجد الفرد وسط جماعة، إذ يكون عندئذ أسرع انسياقا لتاثير الغير عليه، ويظهر ذلك في مجال الجريمة المرتكبة عبر الإنترنت لأن اغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمارات الفنية التي لديه مما يؤدي به الامر إلى ارتكاب الجرائم.

ولاشك أن ذلك نتيجة لعدم الاستواء في شخصية الفرد الذي يتأثر بخطية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط، وينتهي به الامر إلى التقليد وارتكاب الجريمة.

1: تركي بن عبد الرحمن الموشي ، المرجع السابق ،ص29

ثانيا: السمات التي تتميز بها الجماعات عن الفرد المستقل في ارتكاب جرائم الإنترنت

1. التنظيم والتخطيط:

في عالم الشبكات الإلكترونية وخاصة الشبكة العالمية للانترنت، كما هو الحال في العالم الحقيقي يقوم بمعظم الاعمال جرامية أفراد أو مجموعات صغ ة، حيث ترتكب أغلبالجرائم من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معن ،ويتم العمل بينهم وفقا لتخطيط و تنظيم سابق على ارتكاب الجريمة. فغالبا ما يكون م ضمنا فيها متخصص في الحاسبات يقوم بالجانب الفني من المشروع جرامي وشخص اخر من المحيط أو من خارج لمؤسسة المجني عليها لتغطية الت لا عبوتحول الماسب إليه، كما أن من عادة من يمارس ون الت لص والقرصنة على الحاسبات وشبكات المعلومات بصفة منتظمة حول أنشطتهم عقد المؤتمرات.[1]

تحتاج مثلا جريمة زرع الفيروسات إلى مجموعة من الاشخاص منهم المبر مجالذي يقوم بكتابة البرنامج ومنهم المستخدم الذي يقوم بعملية زرع الفيروسات داخل الاجهزة الاخرى، ونتج عن هذا التنظيم صعوبة كشف تلك الجريمة وإمكانية تنفيذها بدقة نيجة للتخصص داخل تلك الجماعة في كل جزء من أجزاء الجرمة.

يعتبر التخطيط مي ة هامة تتعلق بصفة مباشرة بالجماعة الإجرامية المنظمة. ويعني الدراسة المسبقة لأي عملية إجرامية تقدم المنظمة على ارتكا، ويتطلب الت خط يطقدر عاليا من الذكاء و الخبرة بهدف ضمان ستمرار أنشطتها عيدا عن رق ا بة ومتابعة السلطات المعنيةبقمع الجريمة. فالمنظمات جرامية تحتاج إلى عدد من محترفي الإجرا مالذين يملكون مؤهلات وخب ات عالية تمكنهم من سد جميع الثغرا ت قتصادية وجتماعية والقانونية التي قد تؤ ي إلى فشل أو اكتشاف الجريمة.

1: تركي بن عبدالرحمن الموشد، المرجع السابق ص34

2. التكيف الاجتماعي

عتبر هذه الخاصية امتدادا لسمة التخطيط ، والتنظيم. حيث إن التكيف الاجتماعي ينشأ بين مجموعة لها صفات مشتركة. لأنمجرمي الإنترنت هم عادةأذ سلى اجتماعيين قادرين على التكيف في بيئتهم الاجتماعية، ولا يضعون انفسهم في حالةعداء مع المجتمع الذي يحيط م ، لىقادران على التوافق ،والتصالح مع مجتمعهم باعتبا ر م أذ سلمرتفعو الذاء،بل لىخطو لهم جرامية قدتزدا د إذاز اد تكيفهم الاجتماعي مع توافر الشخصية جرامية.

3. التطور في السلوك جرامي

تتميز جرائم الإنترنت بأنها جرائم ر تبطة بالتطور السريع الذي نشهده اليوم في تكنولوجيا الاتصالات، والذي انعكس بدور على تطور مرتكب جريمة الانترنت وأسلوب ارتكابه من خلال ما ينهله من أفكار وتبا لىالخبرات مع ا لعديد ن المجر نحول العالم عبر الشبكة، وتطور التقنيات المستخدمة في ذلك[1]

يساهم وجود مجرم الإنترنت في جماعة إجرامية إلى التاثير في قدرته العقلية وسر عة إكتسابه المارة التقنية التي تؤدي به إلى التمر دا لداي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدراته على القيام بالدور الرئيسي في تنفيذ الجر م ة

ا لفرع الثالث :دوافع مجر يالإنترنت

تخت فالجريمة المرتكبة عبر الإنترنت عن الجريمة التقليدية من حيث الدوافع. حيث أن مجرمي الإنترنت يسعون من خلال ارتكابهم للجريمة بالإضافة إلى تحقيق المكسبالمادي إلى تحقيق أغراض معنوةمثل التعلم أو اللعب والمزا ح، أولمجرد الانتقام، ويمكن حصر هذه الدوافع في:

1: أيمن عبد الحفيظ،المرجع ا لسا ق،ص46 17

أولا: الدوافع الرئيسية لارتكاب المجرمين الجريمة عبر الإنترنت

1 تحقيق الكسب المادي

تعد الرغبة في تحقيق الثرا عوامل الرئيسية لارتكاب الجريمة عالانترنت، وهو من أهم الدوافع و أكثرها تحريكا للمجرم. نظرا للربح الكبير الذي يمكن أن يحققه هذا النوع من الانشطة الجرامية. وغالبا ما يكون الدافع لارتكاب هذه الجرائم وقوع الجاني بمشاكل مادية تعجز عن سداد ديونه المستحقة. أو لوجود مشاكل عائلية تعود إلى عدم توفر الاموال، أو الحاجة لها للعب القمار، أو شراء المخدرات، أو القيام بأعمال المرا نة إلى غير ذلك. حيث يسعى الجاني للخروج من هذه المازق إلى عمليات التلاعب بالأنظمة المعلوماتية للبنوك والمؤسسات المالية، وذلك بواسطة اختراق الانظمة المعلوماتية لها، واكتشافه لفجواتها الامنية.

2 الرغبة في التعلم

هناك من يرتكب جرائم الإنترنت بغية الحصول على الجديد من المعلومات وسبر أغوار هذه التقنية المسارعة النمو والتطور، و هؤلاء الاشخاص يقومون بالبحث و اكشاف الانظمة والعمل من خلال الجماعة وتعليم بعضهم، ويفضل هؤلاء القرصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الانظمة وكر س البعض منهم كل وقته في تعلم كيفية اخ اق المواقع الممنوعة والتقنيات الامنية للأنظمة الحاسوبية.

3 دوافع ذهنية او نمطية

غالبا ما يكون الدافع لدى مرتكب ارائم عبر الإنترنت هو الرغبة في إثبات الذات و تحقيق انتصار على تقنية الانظمة المعلوماتية دون أن يكون لهم نوايا اثمة. ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمبرمجي برا مج النظام المعلومي لارتكاب تلك ارائم.

ثانيا: الدوافع الشخصية و المؤثرات الخارجية.

1. ارتكاب الجرائم من اجل التسلية

يعتبر دافع المرح والتسلية من الدوافع التي تجعل الشخص يقوم بتصرفات ون كان لا يقصد من ورائها إحد ثجرائم وإ نماغرض المرح فقط ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة الجريمة

2. و افعسياسية

انشرت الكثير من المواقع غير المرغوب فيها على شبكة الانترنت ومن هذه المواقع ما يكون موجها ضد سياسة دولة محددة أوضد عقيدة أومذهب معين، وهي تهدف في المقام الاول إلى تشويه صورة الدولة أوالمعتقد المستهدف.

يتم غالبا في المواقع السياسية المعادية تلفيق الاخبار و المعلو ملتو لزور اأو حتى الاستناد إلى جزئي بسيط جدا من الحقيقة ومن ثم نسج الاخبار الملفقة حولها، وغالبا ما يعمد أصحاب تلك المواقع إلى إنشاء قاعدة بيانات بعناوين أشخاص يحصلون عليها من الشركات التي تبيع قواعد البيانات تلك أو بطرق أخرى ومن ثم يضيفون تلك العناوين إلى قائمتهم البريدية ويبدؤون في إغراق تلك العناوين بمنشوراتهم، وهم عادة يلجئون إلى هذه الطر قة رغبة في تجاوز الحجب الذي قد يتعرضون له ولإيصال أصواتهم إلى أكبر قدرممكن.

تعد الدوافع السياسية من أبرز المحاولات الدولية لاختر ق شبكات حكومية في مختلف دول العالم، كما أن الافراد قد يتمكنون من اختراق الاجهزة الامنية الحكومية، كذلك أصبحت شبكة الإنترنت مجالا خصبا لنشر أفكار العديد من الافرا دوالمجموعات، و وسيلة لترويج لأخبار وامور أخرى قد تحمل في طياتها مساسا بأمن الدولة أو بنظام الحكم أو قدحا في رموز دولية أو سياسية والإساءة لها بالذم و التشهير().

ا لم جث الثاني: تكييف الجريمة المرتكبة عبر الإنترنت

نقتضي تحديد الطبيعة القانونية للجريمة المرتكبة عبر الإنترنت، العمل على تصنيفها وتحديد الاركان التي نقوم علىها، فمع النمو السريع لاستخدام شبكة الإنترنت في شتى المجالات، وتنوع أشالها وصورها بصورة مطردة، مما جعل مهمة حصرها وتصنيفها تتميز بالصعوبة، وتجدر الإشـ لرةأن تحليل صور الجريمة المرتكب عبر الإنترنت وبيان أصنافها ليس بالأمر البسيط ، وذ لكيرجع إلى التباين والاختلاف لدى الفقه في معرض تصنيفهم لهذه الجرائم، وسبب ذ لك يرجع إعدم تبنيهم لمعايير واحدة ثابتة و لضوابط مشتركة.

ا لمط لب ول :انواع جرائم الانترنت

ل لتحدث عنأنواع جرائم الانترنت ، يمكن القول أن الركن الاساسي والمفترض بالنسبة لكل نوع هو ارتكاب الجريمة عبر شبكة الانترنت لكن لتحديد الركن المادي والمعنوي، يجب الحديث عن كل فعل على حدى بالتالي يجب أولا تحديد أنواع جرائم الانترنت ومن خلالها سأتطرق لأ رلىل نوع.[1]

وقد تضاربت الأراء لتحديد أنواع جرائم الانترنت وتعددت التصنيفات،فهناك من عددها بحسب موضوع الجريمة ، وأخر قسمها بحسب طريقة ارتكابها ، وقد صنفها معهد العدالة القومي بالولايات المتحدة الامريكية عام 1985 بحسب علاقتها بالجرائم التقليدية ، فاعتبر أن الصنف الأول يتمثل في الجرائم المنصوص علىها في قانون العقوبات متى ارتكبت باستعمال الشبكة ، والصنف الثاني تضمن دعم الانشطة الإجرامية ويتعلق الامر بما تلعبه الشبكة من دور في دعم جرائم غسيل الاموال،المخدرات ،الاتجار بالأسلحة ،واستعمال الشبكة كسوق للترويج غير المشروع في هذه المجالات ،بينما يتعلق الصنف الثالث بجرائم الدخول في نظام المعالجة الالية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى

1 : أحسن بوسقيعة، الوجيز الجزائي الخاص، الجزء ا ول ، دار هومة،2014، ص 262.

عمل الحاسوب ، بينما الصنف الرابع فتضمن جرائم الاتصال وتشمل كل ما يرتبط شبكات الهاتف .وما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الانترنت، وأخيرا صنف الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها بأي صورة طبقا لقانون حماية الملكية الفكرية

في حين عددت وزارة العدل الامريكية عام 2000 في معرض تجديدها للمكاتب المحلية لإنفاذ القانون الفيدرالي المتعلق بجرائم الكمبيوتر دون أن تقوم بتصنيفها وهي: السطو على بيانات الكمبيوتر ، الاتجار بكلمات السر ، حقوق الطبع ، سرقة الاسرار التجارية ، تزوير الماركات، تزوير العملة ، الصور الفاضحة الجنسية ، واستغلال الاطفال ،الاحتيال، الإزعاج عن طريق شبكة الانترنت ، التهديد ، الاتجار بالمتفجرات أو الاسلحة النارية أو المخدرات وغسيل الاموال عبر الشبكة.

بينما يذهب الاتجاه العالمي الجديد خاصة ما ورد بالاتفاقية الأوربية لعام2001 لجرائم الكمبيوتر والانترنت فقد قسمت هذه الجرائم إلى:[1]

- ☑ الجرائم التي تستهدف عناصر المعطيات والنظم
- ☑ الجرائم المرتبطة بالمحتوى بالكمبيوتر "التزوير والاحتيال."
- ☑ الجرائم المرتبطة بالمحتوى " فعال الإباحية و الاخلاقية."
- ☑ الجرائم المرتبطة بحقوق المؤلف والحقوق المجـــاورة.

وأمام هذا الاختلاف في تقسيم الجرائم المرتكبة باستخدام الشبكة، ارتأيت وضع هذه الجرائم ضمن صنفين إتباعا للتصنيف التقليدي للجرائم الذي يتضمن الجرائم الواقعة على المال و الجرائم الواقعة على الاشخاص، و ذلك أن الهدف من الجريمة في حد ذاتها هو إما الحصول على أموال أو الاعتداء على الاشخاص و يرى ستاذ أمين محمد

1 : أحسن بوسقيعة، المرجع نفسه ص262.

ا لثوا بكةأن هذا التصنيف يعود للدور الذي يلعبه الانترنت في ارتكاب هذه الجرائم ، فإماأن تكون الشبكة أداة ايجابية لارتكاب الجريمة فتسهل للمجرم المعلوماتي تحقيق غايته الجرمية ، و يلاحظ أن اغلب صورها في هذه الحالة تشكل جرائم الواقعة على الاشخاص في حين عندما تكون الشبكة عنصر سلبي في الجريمة أي محل للجريمة فان هدف المجرم ينصب حول البيانات و المعلومات المخزنة و المنقولة عبر قنوات الانترنت الخاصة ٌو العامة و باختراق الحواجز منية إن وجدت و تتعلق عموما بصور جرائم الاعتداء على موال. سأتطرق لهذه الانواع في فرعين الاول يتعلق بالجرائم الواقعة على الاموال مع التركيز اكثر على المعطيات، والثاني يخص الجرائم الواقعة على الأشخاص ،و إبراز أركان كل جريمة على حدى.[1]

الفرع الاول : جرائم الانترنت الواقعة على الاموال

تختلف الاموال من مادية إلى معنوية ، و استقر الرأي إلى أن المعلومات التي تعالج اليا و تأخذ حكمها البيانات المخزنة سواء في برامج الحاسوب ٌو في ذاكرته،تدخل ضمن الاموال و بالتالي تتمتع بالحماية الجنائية المقررة وقد سايرت هذا الرأي محكمة النقض الفرنسية في العديد من أحكامها منها قضائها بسرية المحتوى المعلوماتي للشرائط خلال المدة اللازمة لنسخ و إعادة إنتاج المعلومات أضرارا بالمطبعة المالكه لها.

ومن أجل ذلك ارتأيت البدأ بالجرائم الواقعة على البيانات و المعلومات المشكلة للنظام المعلوماتي للحاسب الآلي ٌو للشبكة أولا، باعتبارها حتى لو شكلت نوع قائم بذاته فإنها تعتبر الوسيلة الأساسية لارتكاب باقي جرائم الانترنت بمختلف اشكالها ثم التطرق لبعض الجرائم خرى.

أولا: الجرائم الماسة بنظام المعالجة لية للمعطيات

أن الصورة الغالبة لتحقيق غاية المجرم المعلوماتي في نطاق الشبكة تتمثل في فعل

1 : أحسن بوسقيعة، المرجع نفسه ص263.

الدخول غير ا لمشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن، ومن ثم قيام الجاني بارتكاب فعله الذي قد يكون مجرم فيشكل احد أنواع جرائم الانترنت،أولا يكون كذلك .وتنصب هذه الجرائم على المعلومة .باعتبارها العنصر الاساسي المكون للبرامج والبيانات والمعلومات الموجودة بالحاسب الالي ، ويشترط أن تكون المعلومة خاصة قاصرة على فرد أوأفراد دون غيرهم ، تبلغ حد من الاهمية به يستاثرون بها و تشكل لديهم عامل مهم، في أدائهم يميزهم عن غيرهم .وتحمل ابتكارا أو اضافه يكونوا هم مصدرها.

ولقد تضمن قانون الاحتيال وإساءة استخدام الكمبيوتر"CFAA" لعام1996 الصادر عن المشرع الامريكي ، تجريم الدخول الغير المشروع الى انظمة المعلوماتية ، معددا صور هذه الجريمة من خلال المادة 1030 من هذا القانون وهي:

1) الدخول العمدي إلى جهاز الحاسوب بدون تصريح أو تجاوزا للتصريح الممنوح له ، ويحصل بأية وسيلة على معلومات تقررت من قبل حكومة الولايات المتحدة بناء على أمر تنفيذي وتصريح برلماني يتطلب الحماية ، ضد فشاء غير المخول به لأسباب تتعلق بالدفاع الوطني أو العلاقات الاجنبية.

2) الوصول عمدا الى الحاسوب بدون ترخيص ، أو تجاوز الترخيص الممنوح بقصد الحصول على معلومات واردة في سجل مالي بمؤسسة مالية،أوان تشمل هذه المعلومات المتضمنة في ملف وكالة أو معلومات من أي حاسب محمي إذا تعلق بمحتوى اتصالات خارجية او بين الولايات.

3) الوصول العمدي بدون ترخيص لأي حاسوب غير عام يخص إحدى إدارات أو وكالات الولايات المتحدة مخصص لاستعمال حكومة الولايات المتحدة،أو لم يكن مخصص لها ولكن استعمل من قبل أو لأجل حكومة الولايات المتحدة الامريكية و كان ذلك التصرف مؤثرا على ذلك الاستعمال من قبل او لأجل حكومة الولايات المتحدة. [1]

4) الوصول لمعرفة وبقصد الغ ش إلى الحاسوب محمي ، بدون ترخيص أو بتجاوز

1 : أحسن بوسقيعة، المرجع نفسه، ص 263.

الترخيص الممنوح له ،وبأيه وسيلة تسهل نية الغش ويتحصل على أي ء ذي قيمة ، ما لم يكن موضوع الغش والشيء المتحصل عليه يتوقف فقط على استخدام الحاسوب وان قيمة هذا الاستخدام لا تزيد عن5000 دولار خلال فترة سنة.

5) كل من:

- سبب عن معرفة بث برنامج و معلومات أو شفرة أو أمر وسبب ضرر عن قصد كنتيجة لهذا التصرف ، وبدون ترخيص لكمبيوتر محمى.
- يتصل متعمدا لكمبيوتر محمي بدون ترخيص وكنتيجة لهذا السلوك سبب ضررا نتيجة إهمال.
- يصل متعمدا لكمبيوتر – محمي – بدون تفويض وكنتيجة لهذا السلوك يـ سبب ضررا.

كل من سبب باحتيال عن قصد ومعرفة ، تجاره أو مقايضة في أي كلمة سر أو معلومات مشابهة يمكن من خلالها الوصول للكمبيوتر بدون تفويض

و انتقد هذا القانون، لانطوائه على الكثير من الغموض والقصور ، يمكن للمجرمين تفادي تطبيق القانون عليهم،باستخدام حاسبات وشبكات من خارج الولايات المتحدة والدخول إ أنظمة الحاسبات داخل الولايات المتحدة الامريكية والاعتداء عليها أو استخدام هذه الانظمة ذاتها عن بعد للاعتداء على حاسبات تقع في دول أخرى.[1]

بينما نجد أن المشرع الانجليزي قد كفل حماية البيانات المخزنة في الحواسب من الاعتداء عليها ، أو إساءة استخدامها بإصداره لقانون إساءة استخدام الكمبيوتر عام 1990 COMPUTER MISUSEACT فجرم من خلال المادة الاولى منه فعل الدخول غير ا لمشروعإلى أي برنامج أو بيانات موضوعة في أي كمبيوتر ،مع جعله يؤدي أية ، وظيفة لتحقيق الدخول ، كما عاقب على أي دخول يقصد به تدبير غير مشروع ، إذا ، توافو للجاني العلم بعدم مشروعية الدخول ، وقت تغييره لوظيفة الكمبيوتر ، أو إذا اتجهت

1 : أحسن بوسقيعة، المرجع نفسه، ص 263.

نيته للاعتداء على تفاصيل أي برامج أو بيانات في أي كمبيوتر محدد أو غير محدد وتعلقت المادة الثانية من ذات القانون بتجريم فعل الدخول غير المشروع لارتكاب أية جريمة يعاقب عليها النص ، ألتسهيل ارتكاب الجريمة ، سواء للجاني نفسه ألشخص آخر ،وقد جرم في المادة الثالثة فعل الدخول إذا كانت الغاية منه تعمد تعديل modificationمحتوى أي كمبيوتر ، فيعاقب على إتلاف عمل الكمبيوتر أو إعاقة الدخول لأي برنامج أو بيانات موضوعة في أي كمبيوتر أو إتلاف عمل أي برنامج او صحة أي بيانات،و يعاقب الجاني متى اتجهت نيته بصورة مباشرة إلى أي كمبيوتر للشخص أو برنامج خاص أو بيانات من نوع خاص أو تعديل من نوع خاص ،من توافرت لديه المعرفة السابقة ، والمتمثلة باي تعديل يقصده الجاني كي يتسبب بفعله غير مشروع.

في حين نجد أن المشرع الفرنسي قد تناول جريمة الدخول غير المشروع أو البقاء بدون صلاحية داخل نظام معلوماتي من خلال المواد 1/323 إ 3/323 مجرما فعل الدخول أو البقاء بطريق الغش في نظام المعالجة الالية للمعطيات أو جزء منه ، و فرق بين مجرد الدخول أو البقاء ،و بين ما يترتب عن هذا الدخول أو البقاء من محو أو تعديل في المعطيات المخزنة أو إتلاف تشغيل هذا النظام[1]

و بالرجوع للمشرع الجزائري نجد انه، عاقب على جرائم أدرجها في القسم السابع مكرر من قانون العقوبات المعدل بالقانون 23/06 المؤرخ في 06/12/20 المتعلق بالمساس بأنظمة المعالجة الالية للمعطيات بالمواد 394مكررالى 394 مكرر7 مجرما من خلاله

أ. فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الالية للمعلومات أو محاولة ذلك ، أو متى ترتب عنه تغيير معطيات المنظومة أو حذف نظام التشغيل أو تخريبه.

ب. الإدخال أو الإزالة بطريقة الغش لمعطيات في نظام المعالجة لية للمعلومات.

1 : أحسن بوسقيعة، المرجع نفسه، ص 263.

ج. القيام عمدا وعن طريق الغش بتصميم أو بحث أو بتوفير ، نشر ، أو تجارة بمعطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم الماسة بأنظمة المعالجة الالية للمعطيات.

د. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الخاصة بأنظمة المعالجة الالية للمعطيات.

هـ. المشاركة في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم المنصوص عليها الخاصة بأنظمة المعالجة الالية للمعطيات. و رغم ذلك أشارت إحصائيات إلى وقوع بن200 الى 250 اعتداء يوميا على نظمة المعلوماتية بالجزائر وهو ما يستدعى التطبيق الفعلي لهذه النصوص.

و نلاحظ بالقراءة لما سبق أن الجريمة تتحقق بتوفر الركن المادي الذي تمثل في احد أشال الاعتداء على نظام المعالجة لية للمعطيات و الذي يكمن في احدا لصور التالية:

1- فعل الدخول أو البقاء غير المشروع في نظام المعالجة لية للمعطيات[1]

2- الاعتداءات العمدية على نظام المعالجة لية للمعطيات و التي تشترط وجود نظام معالجة للمعطيات كشرط مسبق

3- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام: خرب ،إتلاف ،تجار...

بينما تمثل الركن المعنوي في صورة القصد الجنائي: العلم و الإرادة، إضافة إ نية الغش. فيجب أن تتجه إرادة الجاني إلى فعل الدخول أو البقاء وهو يعلم أن ىلى له الحق في ذلك حتى لو كان بهدف الفضول و إثبات القدرة على المهارة و تبد نية ا لـشى من خلال سلوب الذي تم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام وبالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام. و نجد أن كل

1 : أحسن بوسقيعة، المرجع نفسه، ص 263.

التشريعات السالف ذكرها: أمري ، انجليزي ، فرنسي ، جزائري قد فرقت بين فعل ا لدخولوالبقاء فقد يكون فعل البقاء المجرم نتيجة دخول مشروع ،بينما الدخول المجرم هنا هو فعل غير مشروع ، و يعد من الجرائم المؤقتة و الشكلية. ال تكتمل بمجرد تحقيق السلوك جرامي دون تطلب ركن مادي للجريمة ، في حين يعتبر البقاء من الجرائم المستمرة فمجرد التواجد المعنوي للجاني داخل نظام للمعالجة لية للمعلومات و استغراقه لحيز وق بداخله تحقق الجريمة [1].

و تتحقق الجريمة متى كان الدخول و البقاء مسموح و مشروع ولكن تجاوز الفاعل الوقت المحدد و المسموح به و الغرض المصرح له بالدخول خلافا لإرادة صاحب الشأن المسيطر على النظام ، وينتفي القصد الجنائي إذا دخل المستخدم إلى النظام بطريق الخطا، لان ذلك يعد جهلا بالوقائع ولكن يسال جنائيا إذا دخل بطريق الخطا إ ظلم معلوماتي ، و ظل متجولا فيه مع علمه بذلك.

وما يلاحظ على التشريعات السابقة أا لم تورد تعريف لنظام المعالجة لية للمعطيات مكتفية بوضعه محلا للحماية، رغم انه الشرط و اللازم تحققه للبحث عن توفر أركان الجريمة من عدمه.

بينما عرفه الفقه الفرنسي أنه : " كل مركب يتكون من وحدة أو وحدات معالجة تتون كل منها من الذاكرة و البرامج و المعطيات و أجزة دخال و خراج و أجزة الربط و التي يربط بينها مجموعة العلاقات التي عن طريقها تتحقق نتيجة معينة و هي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية" ،فهو يتكون من عنصرين:

1. **مر كب:** يتكون من عناصر مادية و معنوية مختلفة تربط بينها نتيجة علاقات توحدها نحو تحقيق هدف محدد. [2]

2. **ضرورة خضوع النظام لحماية فنية :** حفاظا على خصوصية البيانات المتناقلة

1 : عبد الفتاح مراد، شرح جرائم الكمبيوتر و الانترنت، ط 1 ،2006 ص204.

2 : عبد الفتاح مراد، المرجع السابق، ص 204.

عبر الشبكات ، يوجد ثلاث أنواع من نظمة : أنظمة مفتوحة للجمهور ، أنظمة قاصرة على أصحاب الحق و بدون حماية فنية ، أنظمة قاصرة على أصحاب الحق و تتمتع بالحماية الفنية ، و النوع الثالث فقط هو المتمتع بالحماية الجنائية ، و لكن التشريعات لم تشرط وجوده،تماشيا مع الرأي الراجح من الفقه ذلك أن الحماية الجنائية تمتد لتغطي أنظمة المعالجة لية للمعطيات سواء كانت محمية و غير محمية.

ثانيا. جريمة إتلاف نظام المعلوماتية عبر الانترنت:

تقع جريمة تلاف في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الالي ، وذلك بالتعدي على البرامج و البيانات المخزنة و المتبادلة بين الحواسب و شبكاته، و تدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي، و يكون تلاف العمدي للبرامج و البيانات كمحوها ٍو تدميرها الكترونيا ، ٍو تشويهها على نحو يجعلها غير صالحة للاستعمال و يتم ذلك نتيجة لدخول ٍو البقاء غير المشروع داخل نظام المعالجة لية للمعلومات كما سبق ذكره، ويتحقق تلاف في إحدى ا لصورتن:

✍ **اعاقة سير العمل في نظام المعالجة لية للبيانات:** وهو فعل يسبب تباطؤ عمل نظام المعالجة لية للبيان ٍأو إرباكه مما يؤدي إ تغير في حالة عمل النظام على نحو يصيبه بالشال المؤقت و ذلك من خلال تعديل البرامج في نظام المعالجة او عمل برنامج احتيالي،ٍو من خلال التحويلات الالكترونية كإغراق موقع (site) على الشبكة بالرسائل الالكترونية إلى غاية شله.

و قد تناول المشرع الفرنسي جرائم تلاف و التخريب والتهديد ء من ذلك في الم واد 322/1إلى 4/322 قانون عقوبات 1994 .و تختلف هذه الجريمة عن جريمة ا لدخولأو البقاء في النظام، كون أن مجرد الدخول الاحتيالي يعد جريمة قائمة بذاتها سواء كان الدخول إلى كل ٍو جزءمن النظام المعلوماتي[1] ،كماأن الاعتداء على النظام المعلوماتي قد يقع دون المرور إلى النظام نفسه، كحالة بث برامج من شأنها أن تؤثر على

1 : عبد الفتاح مراد، المرجع السابق، ص 205.

سير النظام أوعلى الشبكات المربوط بها، و قد جرم المشرع الامريكي ذ سفى فعال ضمن قانو (CFAA) وهو ما فعله المشرع الاردني ضمنقا نون تصالا ت ر قم13 لسنة1995

✍ **الاعتداء عل البيانات داخل نظام المعالجة لية للبيانات :**

ويتم ذلك بإحدى الطريقتين :

أ. محو البيانات و المعلومات كلية و تدميرها الكترونيا.

ب. أن يتم تشويه المعلومة أو البرامج بتعديل البيانات أو تعديل طرق معالجتها أو وما لى ذا نتقالا.

و يترتب على ذلك تلاف بالمعنى القانوني متى كانت المعلومات و البرامج محل تلاف هي هدف الجاني ، بقصد ضرار بالغير أي دون اتجاه إرادة الجاني إلى ارت بل جرمةأخرى ومن التطبيقات القضائية ما ذهبت إليه محكمة الاستئناف الفرنسية بإدانة متهم بالجنحة الواردة ضمن المادة 3/323 من قانون العقوبات الفرنسي ، لقيامه بتعديل المعطيات التي سبق وان سجلها بطريقة نهائية على نظام الي للمحاسبة ، وقد أيدت محكمة النقض الفرنسية في قرارها في 8 ديسمبر1999 .واقعة التعديل أو لغاء العمدي لمعطيات يحتوي عليها نظام معالجة آلية بالمخالفة للوائح المطبقة و التي استخلصتها محكمة الاستئناف وقد يستهدف من هذا تلاف ارتكاب أفعال أخرى إضافة لجريمة تلاف .كتكييف واقعة قيام محاسب بمحو بيانات و معلومات معالجة أليا ت ضىإحدى الشركات على أا تشكل نصب معلوماتي ، إذ اعتبر المحو وقع بهدف النصب ،رغم انه ركن مادي للإتلاف ، كما قد يأخذ تلاف صورة التزوير ، اختلاس أموال مثل الطلبات المزورة المقدمة عبر الانترنت إلى شركات بطلب البضائع بالتلاعب بتغ لى المعلومات.

و تتنوع صور إتلاف البيانات و البرامج بحسب ما إذا اتخذت صورة التدخل في المعطي كأو إذا اتخذت صورة التدخل في الكيان المنطقي :[1]

1 :عبد الفتاح مراد، المرجع نفسه، ص 205.

التدخل في المعطيات:

المعطيات و البيانات تمثل المعلومات المدخلة في النظام الآلي للحاسب بغرض معالجتها ويتم التدخل فيها أما بإدخال معلومات ومية في النظام المعلوماتي أوبتزوير المعطيات الموجودة فيه ،و التغيير و التبديل الذي يقع على المعطيات و وامر المخزنة والمنقولة عبر شبكة الانترنت لا ينطبق عليه نصوص التزوير التقليدية إلا إذا أخرجت في صورة محرر مكتوب، و من أجل ذلك ظهر تيار قوي ينادي بالمساواة بين مستند ورقي ومستخرجات الحاسب الآلي، اسطوانات ممغنطة و شرائط وما يسجل في ذاكرة الحاسب الآلي.ويتم تغيير الحقيقة عن طريق الحذف بإزالة كلمة أو رمز معين أو عن طريق ضافة بزيادة عبارات أو بيانات غير صحيحة أو بتغيير محتوى الرسائل المنقولة كان يحتجز الفاعل أمر دفع موجه من بنك لأخر و يزيف الرسالة ، فيتم الدفع لحسابه.

وقد استوعب المشرع الفرنسي الفرق بين مختلف فعال التقنية بشكل دقيق فنص في المادة 441 المتعلقة بتجريم التزوير في محرر رسمي ، على تزوير الوثيقة المعلوماتية و استخدامها ، بالنص على لفظ أي سند أو دعامةوبأي وسيلة ،و يكون بذلك فرق بين تغيير الحقيقة في البيانات المسجلة في ذاكره النظام الآلي، و بين تغييرها في محررات النظام الآلي لمعالجة المعطيات فافرد نصا خاصا للمسالة و بينما احتوى الثانية في النص العام للتزوير.

التدخل في الكيان المنطقي:

يمثل الكيان المنطقي logiciel مجموعة البرامج المخصصة للقيام بالمعالجة عن طريق الحاسب الآلي ،و يتمثل إما بتعديل البرنامج أو خلق برنامج جديد [1]

تعديل البرنامج :

يعد البرنامج كيانا ماديا ، له أصل و مولد صادر عنه ، يمكن رؤيته على شاشة الحاسب كترجمة إلى أفار كما يمكن الاستحواذ عليه عن طريق تشغيله في الحاسب و

1 : هدى قشقوش، جرائم الكمبيوتر و الجرائم ا خرى في مجال التكنولوجيا المعلومات، ملتقى الفكر، 2006 ص302.

يتجسد في إحدى ا لصور الثلاث:

› **التلاعب في البرنامج** :يتم ذلك ببرمجة الجهاز الآلي و النظام بشكل يؤدي إلى اختفاء البيانات كليا ً و جزئيا كما هو الحال في برنامج. salami

› **اختلاس نتائج الحاسب أو دارة** : و يتم ذلك بإعادة نسخ المعطيات عن بعد ٍ و عن طريق النقل الالكتروني للبيانات ، وذلك بإتباع أسلوب التجسس المعلوماتي) عن طريق بث برامج خاصة بالتقاط البيانات المتبادلة عبر الشبكة).

› **تغيير نظام التشغيل** : و يكون ذلك بتزوير برنامج نظام التشغيل بمجموعة تعليمات إضافية على ا لوصول إليها بواسطة كلمة السر «pass word » أو مفتاح الشفرة و أداة الربط، بحيث تتيح الوصول الى جميع المعطيات الموجودة بالجهاز الآلي.

كيفية إتلاف البرنامج :

و تتم عملية تلاف بطريقة فنية و تقنية متنوعة من فيروسات programmes) (virus مرورا ببرامج الدودة worn software و أخيرا القنبلة المنطقية أو الزمنية-logic) (bomb،و يتفق الفقهاء في انجلترا و الولايات المتحدة على ن المشكلات القانونية التي تنشأ عن جميع الفيروسات تكون غالبا واحدة ، فلا وجه للتفرقة بين الفيروس و الدودة و حصان طروادة لأنها ترتب نفس ثار.

› **فيروسات الحاسب الالي** : هي برامج خبيثة تتسلل إ البرمجيات فتدخل إليها ،و تنسخ نفسها على برامج أخرى، عبر كامل الحاسب الآلي.و قد تستعمل لحماية البيانات والبرامج.من خطر النسخ غير المشروع، و لها هدف تخريبي عندما تستعمل للدعاية ٍ و الابتزاز، و تنشط هذه الفيروسات عند نسخ البرنامج من حاسب لأخر أو نقل المعلومات عبر شبكة الانترنت أين تكون مخبأة داخل الرسائل الالكترونية و الوثائق و المعلومات التجارية و المالية .و تنقسم الفيروسات إلى:[1]

أ **فيروس عام العدوى**: ينتقل من برنامج ٍخر و يهدف لتعطيل النظام بأكمله.

1 : هدى قشقوش، المرجع السابق، ص 302.

ت **فيروس محدد العدوى** : يستهدف نظام معين يتميز بالبطيء في الانتشار و صعوبة الاكتشاف.

ج **فيروس عام الهدف** : سل عداد ، يتسع مجال تدميره ، يضم العدد الاكبر الفيروسات.

د **فيروس محدد الهدف** : يستهدف عنصر معين من البرنامج ، و يتطلب مهارة في التطبيق كالتلاعب المالي او التغيير في التطبيق العسكري، كفيروس حصان طراودة trjan horse الذي ينتشر بكثرة على صفحات شبكة الانترنت و يلحق ذى بكمبيوتر المتصفح.

- **و ا ج الدودة** : **worn softwars** يشغل الفراغ الموجود في نظام التشغيل ليتنقل من حاسب أخر و شبكة لأخرى عبر الوصلات التي تربط بينها ،و تتكاثر إثناء الانتقال، وتعمل على خفض كفاءة الشبكة ، و التخريب الفعلي للملفات و البرامج من خلال ملإها لأي حيز من الشبكة ،و اطلقت دودة الانترنت من قبل طالب لمري " روبرت موريس " بجامعة علوم الكمبيوتر – ورنيل لإثبات عدم لا ئمةأساليب مان ا لمستعملة، فتسبب في تدمير ألاف من شبكات علام الالي المنتشرة في الولايات المتحدة و خسائر مالية معتبرة لمواجهة دودة الانترنت، و قد أدين من اجل ذلك بانتهاك قانون الاحتيال و إساءة استخدام الكمبيوتر و عوقب بثلاث سنوات حبس و العمل لأعمائة ساعة في الخدمة الاجتماعية و غرامة قدرها 10.500 دولا
- **ا لقنبلة المعلوماتية** : و التي تنقسم إ[1]:
- **ا لقنبلة المنطقية** :هي برامج مخفية تدخل بطرق غير مشروعة ، صغيرة ، تهدف لتدمير المعلومات في لحظة محددة ومدة زمنية منتظمة مثل: ما حدث في الولايات ا لمتحدة مكية بولاية لوس انجلوس تمكن احد العاملين بإدارة المياه و الطاقة من وضع هذه القنبلة في نظام الحاسب الالي للإدارة فا ىلتخريبه عدة مرات.

1 : هدى قشقوش، المرجع السابق، ص 303.

- **القنبلةالزمنية** : و تقوم بعمل تخريبي في زمن محدد سلفا بالثانية وساعة واليوم والشهر.مثل قيام خبير معلوماتى ، بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة و ذلك للانتقام بسبب فصله عن العمل ، و التي انفجرت بعد ستة أشهر من رحيله عنها. فترتب عن ذلك إتلاف كل البيانات. و يثار بشأن تلاف الذي يقع على نظم شبكة الانترنت و يضر بمستخدمها مسألة مسؤوليةالشبكة. التي تنحصر في توفير الاتصال مثل للمتعاقد معها، و لا يمكنمسالتها إلا إذا كانت مكلفة رسميا بمراقبة الاتصال و لا بقيت مسؤولية مرسل الفيروس هي القائمة وحدها.

ثالثا: جرمةالسرقة:

لتحقق جريمة السرقة يجب توفر ركن الاختلاس لشيء ،والذي يكون مملوك للغير طبقا لنص المادة 2/311 من قانون العقوبات الفرنسي والتي يقابلها المادة 350 قا نون عقوبات جزائري ، لكن هذا النص يشترط أن يقع الفعل على الشيء (chose) و التي يقابلها في القانون المصري و الاردني لفظ المال المنقول وان كانت القواعد العامة لا تدخل موال المعنوية ضمن هذه شياء ،إلا انه ما دام يمكن تأطير هذه موال المعنوية ووضعها في حيز يمكن الاستئثار به ،و تبديل حيازته فانه يمكن القول انه ينطبق عليها وصف المال و يتوسع مفهوم الاختلاس ليشملها ، الذي برز في شانه اتجاه اخذ بـ لاعتبار شياء غير الملموسة بالمعنى التقليدي ، وهو ما أكدته المحاكم الفرنسية ، فيما يخص بعض القوى كالكهرباء التي تصلح أن تكون محلا للسرقة ، ويؤكد هذا القول أن البيانا تأو المعلومات تأخذ شكل نبضات الكترونية تمثل رقم الصفر وواحد فهي تشبه التيار الكهربائي و بالتالي فالبرنامج في الكمبيوتر يشغل حيزا ماديا يمكن قياسه بمقياس معين " البايت، الكيلوبايت، الميجابايت"[1]

وقد استند الفقه الفرنسي على صلاحية خضوع المعلومات المخزنة لان تكون محل

1 : هدى قشقوش، المرجع السابق، ص 304.

للسرقة عند مبادلتها عبر الشبكات على أن :

1) لمة شيء الواردة في المادة 311 القا نونفرنسي الجديد تشمل شياء المادية و غير المادية.

2) إن الاستيلاء على المعلومة يمكن أن يتم عن طريق السمع و المشاهدة و بالتالي تغيير حيازتها و حرمان صاحبها من الانتفاع بها.

3) المعلومة قابلة للقياس و التحديد مثل الطاقة الكهروبائية

4) إن سرقة المعلومات و ليس الدعامة التي تحملها هي السبب في إدانة شخص من قبل محكمة النقض الفرنسية لنسخ مستندات سرية بدون علم ورضا المالك الشرعي.

5) المعلومة منفصلة عن دعامتها المادية هي مال يمكن تملكه لماله من قيمة اقتصادية إذ يمكن للجاني استغلال المعلومات بإبرام عقود مع الغير،وتأكد القول بان المعلومات هي شيء منقول وفقا للقانون 652/82 الصادر عام 1982المعرف للمعلومات أا أصوات ، صور ووثائق و معطيات و ما لىأيا كانت طبيعتها ،إذا و بعيدا عن الجدل الفقهي القائم حول مدى اعتبار المعلومات كشيء مادي يقع عليه وصف المال و بتسليمنا أا منقولات معنوية و نظرا للقيمة المالية التي تكسبها خاصة لولا هذه المعلومات فما الفائدة التي تحققها سرقة الدعامة المادية وهي فارغة.

و تتحقق سرقة المعلومات باعتبارها مال مملوك للغير و اختلاس بدون رضا صاحبها جـ يثأخرجت من حيازته إلى حيازة الجاني، و تكييف واقعة اخذ المعلومات باستنساخها عبر شبكة الانترنت و تخريب النسخة صلية لحرمان صاحبها منها كجريمة سرقة و ذلك لان الجاني باستيلائه على المعلومات المخزنة في الجهاز و إتلاف صل يؤ ي إلى تحقيق فعل الاختلاس بتبديل الحيازة فالمعلومات قد أخرجت من حيازة مالكها ووضعت تحت السلطة الفعلية للجاني،وكل ذلك يتوقف على توفر القصد الجنائي باعتباره يشكل الركن المعنوي للجريمة ،و الذي يتمثل في القصد الجنائي العام بانصراف إرادة الجاني إ ارتكاب العناصر المكونة للجريمة مع علمه بذلك،والقصد الجنائي

لها بتوفرنية التملك للمعلومات محل الاعتداء، و يمكن استخلاصه من مجرد الدخول غير المشروع للنظام خاصة بتجاوز أنظمة الحماية ،و ترتكب سرقة المال المعلوماتي المعنوي بأسلوبين أو في شكلين[1].

1) **الالتقاط غير المشروع للبيانات:**

يتم التقاط المعلومات بشكل غير مشروع من خلال الشبكة بإحدى الطرق التالية:

أ **اسلوب التجسس المعلوماتي** : يقوم قراصنة الانترنت باستخدام البرامج التي تتيح لهم الاطلاع على البيانات و المعلومات الخاصة بالمتعاملين على شبكة الانترنت ، و تختلف خطورة التجسس بخطورة و قيمة المعلومة : تجارية ، عسكرية... ، و يعتمد القراصنة على تعقب و قرصنة كلمات المرور،مثل التلميذ البريطاني الذي تمكن من الوصول لمعلومات سرية خاصة بإحدى الشركات الكبرى بعد تمكنه من الوصول إلى الكلمات السرية ،ولقد أدين متهمين في الولايات المتحدة في طار قانون الاحتيال و إساءة استخدام الكمبيوتر CFAA و تحت القانون الفدرالي لاحتيال التجسس و تشريعات نقل موال بين الولايات ، وقد قام المتهمون بطريقة غير شرعية بسرقة نصوص ملفات كمبيوتر بشركة تلفون بيل ساوث Bell sauth و التي تحتوي على معلومات خاصة افتراضيه تقدر ب 800.000دولار ، موضوعة في 911 نظام ، فنقلت المعلومات على شكل رسائل إخبارية للمتهمين.

كماأن اعتراض بريد الكتروني (e- mail) يتضمن بيانات متعلقة بأرقام حساب أو بطاقات ائتمان و استعملت في تحويلات الكترونية للأموال ، يعد فعل معاقب عليه ضمن قانون الاتصالات الاردني ،رقم 13 سنة1995 ، ولا يشترط تحقيق المنفعة لتجريم الفعل.

ب **أسلوب الخداع** : يعتمده قراصنة الانترنت بإنشاء مواقع وهمية،مشابهة لمواقع صلية للشركات و المؤسسات التجارية المتعاملة بالتسويق عبر الانترنت ومواقع

1 : هدى قشقوش، المرجع السابق، ص 304.

الويب web و التي تستغلها لاستقبال المعاملات التجارية و المالية الخاصة و السرية كالبيانات المتعلقة ببطاقة الدفع الالكتروني ،ويقبل هذا السلوب وصف تحديد لاكثر من أي وصف آخر ، فيوهم المستخدم للشبكة بوجود مشروع " كاذب " من خلال الموقع الوهمي بغرض الحصول على البيانات و المعلومات و استغلالها بصورة غير مشروعة كالتعاقد و التحويل الالكترونيين للأرصدة خاصة في مجال بطاقات الائتمان.

ج **تقنية تفجير الموقع المستهدف** :و يتم بضخ كميات كبيرة من الرسائل الالكترونية من جهاز حاسب الجاني نحو الجهاز المستهدف عبر الشبكة ، بقصد الضغط على السعة التخزينية ، بملاها بالرسائل الالكترونية المرسلة ، وفي النهاية تفجير الموقع العامل على الشبكة لتتشتت المعلومات ا ل يستحوذ عليها الجاني أو يمكن له التجول في النظام بسهولة والتقاط ما يروق له من معلومات و بيانات الغير.[1]

2) سرقة منفعة الحاسب الالي:

يقصد بسرقة منفعة الحاسب الالي ، استخدامه لأغراض شخصية أو تجارة بدون علم مالكه أو حائزه القانوني ،و الصورة الغالبة هنا لا تهدف إلى تحقيق غرض إجرامي بل قد يلجا إليها على سبيل المثال لتحرير بطاقات مخصصة لأعمال الخير أو نسخ العاب الفيديو للاستعمال الشخصي.و تتم سرقة منفعة الحاسب الالي ، بالاستخدام غير المشروع لأنظمة المعلوماتية. data processing systems (DP) .أو سرقة الخدمة المعلوماتية أو سرقة الوقت ، فهي تقتصر على وقت وجهد له دون نية اختلاس البيانات و المعلومات وهي تشبه فعل استعمال أشياء الغير بدون وجه حق المجرمة في بعض التشريعات مثل الاردني . المادة 412عقوبات . ولقد تضاربت أراء الفقهاء حول الوصف الذي ينطبق على هذا الفعل بين السرقة.الاحتيال، خيانة الامانة، وقد استبعد القضاء الفرنسي وصف السرقة في حالة منفعة الحاسب الالي إعمالا لمبدا التفسير الضيق لنص القانوني، ففي حكم صادر عن محكمة جنح lille في قضية تتخلص وقائعها

1 : هدى قشقوش، المرجع السابق، ص 304..

في قيام اثنين من المختلسين (laurent.c) (Arnaudl) اللذان كان لهما شغف بالمعلوماتية قاما بانتحال اسم شركة و إشاء خط بريدي في النظام المعلوماتي الخاص بشركة cafés grandes mère عن طريق حاسب الي وجهاز إرسال معلوماتي مرئي. فتمكن من توفير قدر كبير من النفقات التليفونية ، وتحميل الشركة المدعية تكلفة تشغيله وقد قام قاضي التحقيق بإحالتهما على أساس جنحة السرقة باعتبارهما استعملا بدون وجه حق حـ اسبإلي خاص بالغير ، وقضت محكمة الجنح ببراءة المتهمين كونه لم يوجد استيلاء مادي على الحاسب الالي بالمعنى الوارد في قانون ا لعق ولتوإنما ما حصل هو استخدام جهاز علام الالي عن بعد باستخدام شبكة الانترنت ، و بدون إذن الشركةوذا الاستعمال لم يعطل عمل الجهاز ٍو يعرقل انتفاع زبائن الشركة. [1]

و نجدأن بعض الدول تعاقب في نصوصها الجنائية على استخدام ملكية الغير بدون وجه حق و سرقة الخدمات مثل الدانمارك ، فلنندا ، انجلترا. وهو ما يمكن تطبيقه على هذه الممارسات في انتظار وجود نصوص خاصة بها وأمثلتها كثيرة من خلال استخدام كلمة مرور خاصة بمقهى الانترنت أو بأي شخص أخر ، للدخول النظام شبكة الانترنت،وإجراء اتصالات مختلفة و مطولة دون دفع الرسوم فاستفاد من خدمات الشبكة دون دفع المقابل .وقد جاء توضيح نيومكسيكو new mescico لبيان خدمة و منفعة الكمبيوتر بانها تشمل : وقت الكمبيوتر، استخدام أنظمة الكمبيوتر و شبكاته، برامج الكمبيوتر ، تحضير و تجهيز البيانات لاستخدام الكمبيوتر، وكذلك محتويات الكمبيوتر من بيانات ٍو أيأداء أخر للنظام المعلوماتي ٍو جزء منه[2] .وتبقى ظاهرة سرقة المعلومات ٍو منفعة جهاز الحاسب موجودة على شبكة الانترنت بقوة، من خلال الممارسات اليومية سواء لمرتادي مقاهي الانترنت خصوصا ٍو مستخدمي الشبكةعموما.

1 : هدى قشقوش، المرجع السابق، ص 304.

2 : أحسن بوسقيعة، المرجع السابق، ص 268.

ر لعا: التحويل الالكتروني الغير المشروع للأموال:

يتم ولوج مخترقي الشبكات إلى بيا نات هد بالآخرين، من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه ، مما يسمح للجاني بالتوغل في النظام المعلوماتي وعادة ما يكون هؤلاء من العاملين على إدخال البيانات في ذاكرة الجهاز أو من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات ، و تتمعملية التحويل الإلكتروني للأموال بأحد ا لطق الموالية:

4 الاحتيال " النصب:"

يتم ذلك بطرق احتيالية يوهم من اجلها المجني عليه بوجود مشروع كاذب أو يحدث الامل لديه بحصول ربح، فيسلم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال، وهو يعلم أن ليس له صفة التصرف فيه، و قد يتخذ إسم أو صفة كاذبة ، تمكنه من الإستيلاء على مال المجني عليه فيتم التحويل الإلكتروني للأموال ،و ذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة أو يتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في إيهام الحاسب و حتيال عليه فيسلمه النظام المال.

ويرى الدكتور محمد سامي شوا: انه لا يوجد أي إثال عندما يكون الاستيلاء على موال ناشئ عن التلاعب في البيانات المدخلة ٌو المختزنة في النظام ٌو برامجه من قبل شخص، ليستخرج باسمه أو إسم شركائه شكات ٌو فواتير بمبالغ غير مستحقة، لكي يثورالإشكال عندما يكون محل الاستيلاء نقود كتابية ٌو بنكية عن طريق القيد الكتابي ،بلعتبارأن رصدة أو فوائدها لا تعد منقولات فكيف يتم الاستلاء عليها وتحويلها نتيجة تلاعب ببيانات الحاسب الالي و بالتالي الاستيلاء المادي على المال.

ومن اجل ذلك ذهب معظم التشريعات التي اعتبار هذه رصدة بمثابة ديون لا يمكن أن تكون محلا للاختلاس،رغم أن بعض الدول اعتبرتها أموال وتصلح أن تكون محلا للتحويل، خاصة أمام ما يحققه ذلك من ربح للجاني وخسارة فادحة للمجني عليه،منها

الولايات المتحدة التي أصدرت عدة قوانين اعتبرت من خلالها الاموال الكتابية و البنكية عبارة عن أموال ،كذلك في الجزائر فان المستندات و الاوراق المالية تعد من الاموال ، بنما في التشريع الفرنسي ، فقد ابتكر نظرية التسليم العادل la théorie remise par équivalentو التي أقرتها محكمة النقض الفرنسية و بموجب أصبح نص المعاقب على الاحتيال و النصب التقليدي " المادة313 قانون فرنسي جديد " تنطبق على جميع افعال التلاعب في البيانات المنقولة عبر شبكة الانترنت و التي تؤدي إ إلغاء ، رصيد دأو خ في رصيد دائن بمبالغ غير مستحقه من خلال تزييف أمر التحويل و تغيير مساره أو بياناته ، مما ينتج عه تحويل رصيد و فوائد ، شخص لحساب الفاعل و عن طريق انتحال شخصية الغير للقيام بالتحويل الالكتروني للنقود[1]

2 **الاحتيال باستخدام بطاقات الدفع الالكتروني عبر الانترنت:**

يعتمد نظام بطاقة الدفع الالكتروني على عمليات التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى ، رصيدالتاجر أو الدائن الذي يوجد به حسابه و ذلك من خلال شبكة التسوية الالكترونية للهيئات الدولية " هيئة الفيزا ارد visa card،هيئة الماستر كارد " master و تعطي بطاقة الدفع الالكتروني الحق للعميل بالحصول على السلع و الخدمات عبر الشبكة عن طريق تصريح كتابي اوتليفوني، بخصم القيمة على حساب بطاقة الدفع الالكتروني الخاصة به ،وتتم العملية بدخول العميل أوالزبون إلى موقع التاجر على الشبكة و يختار السلع المراد شراءها و يتم التعاقد بملأ النموذج الالكتروني ببيانات بطاقة الائتمان الخاصة بالمشترى وعنوانه فيقوم محاسب المتجر بخصم قيمه السلع من بطاقة الدفع الالكتروني و إرسالها إلى المشترى و أمام التطور التكنولوجي أصبحت إمكانية خلق مفاتيح البطاقات و الحسابات البنكية بالطرق الغير المشروعة ممكنة عبر قنوات شبكة الانترنت.

ويمكن الاحتيال باستخدام بطاقات ئتمان من قبل صاحب البطاقة الشرعي و

1 : آمال قارة، الحماية الجزائية المعلوماتية في التشريع الجزائري، ط2، دار هومة،2007 ص350.

ذلك باسائته لاستخدام بيانات البطاقة الائتمانية أثناء مدة صلاحيتها ، بدفع ثمن السلع و الخدمات عن طريق الشبكة بملأ الاستمارة رغم علمه أن رصيده غير كافي لتغطية هذه المبا لغأو أن يقوم بتحويل رصيده من بنك لآخر وهو يعلم انه تجاوز رصيده الحقيقي .وفي صورة أخرى يتم الغش باستخدام بيانات البطاقة الائتمانية بعد مدة صلاحيتها أو إلغاؤها ، فقد يكون البنك مصدر البطاقة قد أ لغاأثناء مدة صلاحيتها بسبب سوء استخدامها من العميل الذي يتعين عليه إعادتها للبنك ، و الذي قد يمتنع عن ذلك ويستمر في استعمالها باستخدام بياناتها في تعاملاته عبر الشبكة، وهو ما يشكل جريمة النصب بمجرد ملا البيانات لإقناع الغير بوجود ائتمان وهمي. لان البطاقة قد خلعت عنها قيمتها كاداة ائتمان خاصة بتحقق تسليم البضاعة و السلع المشترات و تمكينه من الاستفادة بالخدمات[1]

ويرى الفقيه jeandidier أن قيام الحامل القانوني باستعمال بطاقة ملغاة في سحب النقود أو التحويلات الالكترونية لأوراق البنوك .لا يشكل جريمة ، لأنه يفترض في أجهزة السحب الالكتروني المرتبطة مباشرة (on-line) بحسابات العملاء في البنك أن تر فضإجراء أي تسليم أو تحويل للنقود التي يطلبها الحامل إذا كانت تزيد عن رصيده في البنك .أما إذا كانت البطاقة منتهية الصلاحية تعين على الحامل إعدا للبنك ا لصلو لكنه إذا استعملها للوفاء فلا نكون أمام جريمة النصب إنما مجرد الكذب لصلاحية البطاقة، وهو الامر الذي يتعين على التاجر المتعامل معه التحقق من الامر ، في إطار الالتزامات التعاقدية وإلا تحمل جانب من المسؤولية بتحميله الضرر وحده.

وقد يكون الغش في إستخدام البطاقة من قبل الغير، في حالة التقاطها عبر الشبكة و إستعمالها بطريقة غير مشروعة في سحب النقود الرقمية أو الوفاء بها. وبذلك تكون بياناتها محلا للسرقة من خلال تداولها عبر شبكة الانترنت بين العميل والتاجر بواسطة التجسس او الخداع أو الحصول عليها بإستخدام تقنية التفجير" إحرق الموقع

1 : أحسن بوسقيعة، المرجع السابق، ص 269..

"،وقد ذهبت المحاكم الفرنسية إلىان سرقة بيانات بطاقة الائتمان و استخدامها بصورة غير شرعية، يشكل جريمة النصب على أساس إنتحال الغير إسم كاذب في حين يرى جانب من الفقه أن هذا الفعل شكل جريمة السرقة باستعمال مفتاح مصطنع باعتبار أن البطاقة الائتمان تعد مفتاح مصطنع لأن النصوص القانونية لم تحدد بدقة ما هي المفاتيح المصطنعة

ومن الامثلة الواقعية لاحتيال " بطاقات الائتمان واقعة المتطفل hacher كيفن ميتلك الذي أسندت إليه تهمة استخدام دخول احتيالي للكمبيوتر للحصول على 20.000 بطاقة ائتمانية من شركة (netcom) للاتصالات في سان جوس بكاليفورنيا وقد تكون بطاقات الائتمان محلا للتزوير و ذلك بتخليق أرقام بطاقات ائتما نخطة بنك معين من خلال تزويد الحاسب بالرقم الخاص للبنك مصدر البطاقة بواسطة برامج تشغيل خاصة وقد اكتشفت بعض البنوك تكرار اعتراض بعض حاملي بطاقات الدفع الالكتروني على عمليات لم يقوموا بإجرائها و تبين للبنوك أنها عمليات تمت عن طريق شبكة الانترنت من قبل بعض الهواة و المخربين

و من مثلة زعمهابة من" الاكرز" بمدينة الإسكندرية المصرية تضم خمسة أشخاص الاستيلاء على حسابات بطاقات "في "الخاصة بعملاء البنوك، لكن الشاب الفرنسي جان كلود كان اكثر نبلا من أفراد العصابة المصرية، فقد استطاع تصميم بطاقة صرف الي وسحب بها مبالغ من أحد البنوك ثم ذهب إلى البنك وأعاد إليه المبالغ وأخبرهم أنه فعل ذلك ليؤكد لهم أن نظام الحماية في بطاقات الصرف الخاصة با لبنك ضعيف ويمكن اختراقه، إلا أن ذلك لم يمنع الشرطة الفرنسية من إلقاء القبض عليه ومحاكمته، و لهذه حداث اثر بالغ على المواطن الجزائري الذي أجده م تخوفجدا من بطاقات الدفع الالكتروني التي بدأت توزع عبر نقاط البريد وطنيا و يحبذ بقاء التعامل بالشيك، لان هذه البطاقات ستكون محلا للاحتيال أو السرقة الالكترونية، أو مهما كان المصطلح المناسب فالأصح هو أن المبلغ المالي الذي تحمله لن يكون بمأمن و الكثير ممن

وصلته لا يستعملها[1]

و أن مجال الجرائم المرتكبة على أموال عبر الشبكة جد واسع ولا يمكن حصره سواء لان الاختلاف في التكييف للوقائع لم يستقر فيه على رأي، خاصة أمام الفراغ القانوني الحاصل .ومن جهة أخرى أمام تزايد رقعة مجال هذه الجرائم وما يخلق يوميا من أساليب جديدة في الاحتيال و التخريب و الاستحواذ على المال و الأفكار ، فلا يسعني حصر كل أنواع الجرائم الواقعة على المال عبر الشبكة من مخدرات ،تجارة الاسلحة ،انتهاكات حقوق الملكية الفكرية الذي يعد لوحده موضوع الساعة ويتطلب بحث خاص به . ،القمار،غسيل موال،و التي عادةما تأخذ شكل الجريمة المنظمة، لتبقى ضرورة صدور نصوص قانونية تحصر الافعال و الممارسات اليومية خاصة أمام الإحصائيات المسجلة و المتنامية.

الفرع الثاني: بعض جرائم الانترنت الماسة بالأشخاص

سأحاول في هذا الفرع التعرض لبعض الجرائم التي تقع على الاشخاص بواسطة الانترنت منها جرائم التهديد ، السب و القذف ، الجرائم الخلاقية .....، و ذلك للانتشار الواسع لهذا النوع من الاعتداءات فقد أكدت شركة جارليك المتخصصة في مجال التامين الإلكتروني أن أكثر من ستين في المائة من الجرائم الإلكترونية تستهدف الافراد.

أولا:جريمة التهديد:

وهو الوعيد بشر و يقصد به زرع الخوف في النفس، بالضغط على إرادة الإنسان ، وتخويفه من ضرار ما سيلحقه أو سوف يلحق أشياء أو اشخاص له بها صلة، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق أذى ضد نفس المجني عليه أو ماله أو ضد شرف أو مال الغير ، ولا يشترط أن يتم إلحاق أذى فعلا أي تنفيذ الوعيد لأنا تشكل جريمة أخرى قائمة بذاتها ،تخرج من طار التهديد إلى التنفيذ الفعلي ، وقد يكون التهديد مصحوبا بالأمر أو طلب لقيام المهدد بفعل أو الامتناع عن الفعل ، أو

1 : آمال قارة، المرجع السابق، ص 351.

لمجرد الانتقام ويقصد الجاني من كل ذلك إيقاع الذعر والقلق والخوف في نفس المجني عليه مع علمه إنما يقوم به مجرم قانونا ,و لقدأصبحت الانترنت الوسيلة الحديثة لارتكاب جرائم التهديد ، والتي في حد ذاتها تحتوي عدة وسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة و للأسف استعملت لجريمة وهي:

4 **البريد الالكتروني:** [1]

البريد الالكتروني عبارة عن خط مفتوح على كل أنحاء العالم يستطيع الفرد من خلاله إرسال و استقبال كل ما يريده من رسائل سواء كتابه ً و صوتا و صورة و تعد الخدمة الاكثر استعمالا من قبل مستخدمي الشبكة ، فتسمح لتبادل الرسائل بين مستخدمي الشبكة ، سواء بين طرفين أو أكثر في نفس الوقت . القوائم البريدية . أين توزع رسالة الكترونية على ألاف الاشخاص في وقت واحد ، كل على عنوانه البريدي. وكثيرة هي رسائل المرسلة عن طريق البريد الالكتروني إلى المجني عليهم. المتضمنة تهديد بارتكاب جناية ضد نفسه ً و ماله ً و ضد الغير في نفسه ً و ماله .و بإسناد إليه أمور م ل،ة با لشرف أو إفشاء سرار الخاصة به سواء كان مصحوبا بأمر أو ط لبأو لج ردتنقلم أو التسلية بمشاعر الآخرين ، وكثيرا ما يقع التهديد بتدمير أو إغراق الموقع الالكتروني ً و جهاز المرسل إليه .و ينطبق النص التقليدي لجريمة التهديد في اغلب التشريعات على التهديد المرتكب عبر الشبكة .نظرا لعدم اهتمام المشرع بوسيلة التهديد بقدر اهتمامه بمحتوى التهديد و جسامته .ولقد أدانت محكمة (nanterre) بفرنسا احد الجناة بالحبس لمدة شهرين مع يقاف .لأنه بعث رسالة تهديد بالقتل عن طريق البريد الالكتروني إلى أحد رجال السياسة.

2 **منتديات المناقشة و المجموعات الإخبارية وغرف المحادثات و الدردشة:**

هي ساحات افتراضية للقاء و التحدث بين مستخدمي شبكة الانترنت، من ذوي الاهتمامات المشتركة الذين يؤلفون فيما بينهم مجموعات نقاش و تبادل البيانات

1 : لهالي فارة، المرجع السابق، ص 351.

و المعلو ملتو فار حول م وضوعأو قضية معينة ، و ذلك من خلال الرسائل المكتوبة عبر لوحة المفاتيح ،و التي يراها الآخرين على الشاشة ليتم الرد عليها بنفس الشكل و تم اختيار الموضوع بكل حرية مهما كان نوعه في حدود ما توفره الانترنت من تقنية، ويمكن لآي شخص خلالها أن يقدم على تهديد الغير أو أن يكون هو محلا للتهديد على اعتبار أن المشرع لم يحصر وسيلة التهديد

3. صفحات الويب:

وهي النظام الاكثر شهرة في شبكة الانترنت، الل بحثعن المعلومات و الاتصال والتبادل عبر الشبكة فهو أساس نمو الشبكة الهائل ، منذ توزيعه عبرها عام 1991 الذي اعتمد كمرحلة أولية على برنامج التصفح ثم انتقل إلى مرحلة التعميم من قبل نت وكية.فتتم جريمة التهديد هنا بقيام شخص بإشاء موقع ويب خاص به و ينشر عليه تهديد لشخص آخرأو يتوعد بإتلاف موقعآخر خاص بشخص و شركة.

وفي إحدى ا لدول وروية تم ضبط احدالاشخاص أثناء قيامه بتهديد إحدى شركات المياه الغازية، طالبا منها مبلغ من المال حتى لا يقوم بوضع صورة ، زج اجةالمياه المنتجة من الشركة و بداخلها حشرة على موقع الانترنت ، بينما قام احد ابرز مبرمجي الحواسب بمصر بابتزاز شركة تجارية للخدمات بتهديدها بتدمير موقعها على الشبكة و التشهير بها إذا لم تدفع له مبلغ ألفي دولار و الذي تمت محاكمته وعقابه بالحبس لمدة ستة أشهر نافذة ،و يطلق على الشخص الذ ي يقوم بإرسال عشرات الرسائل دفعة واحدة عبر الانترنت إلى اشخاص لا يعرفهم ولم يطلبوا منه هذه الرسائل والتي تكون في الغالب بياذ ئأو إعلانات أو شتائم و تهديدات بمجرمSPAM ،ومع أن المئات يرتكبون هذه الجريمة يوميا ومنهم من لا يرى فيها جرما إلا أن العديدين لا يعرفون أن هذا العمل غير قانوني وكانت شركات الخدمة م لى لمرا أ ونلاين تقوم على الفور بإلغاء اشتراك أي زبون يستخدم بريدها لإرسال كمية من الرسائل دفعة واحدة إلى قوائم بريدية يتم تجميعها عشوائيا ولكن إن تتدخل المباحث الأمريكية وتلاحق احد الاشـ اص وتقدمه إلى

المحكمة التي تحكم عليه بالسجن يعني أن مرتكب جريمة الـ SPAM لم يعد يواجه خطر إلغاء اشتراكاته مع شركات الانترنت وإنما يواجه أيضا السجن والغرامة

وإذا كانت جريمة الـ SPAM غير مقبولة وتلاحقها المباحث فان الجرائم ك أمية وخطورة قطعا ستتعر ض إ الملاحقة مثل جرائم إرسال تهديدات إلى الاخرين عبر البريد الالكتروني وهذا ما تم عندما ألقت ا لشرطةالامريكية في نيويورك القبض على شابين أرسلا تهديدا عبر البريد الالكتروني لجمعية إسلامية في ولاية متشغن وقامت الجمعية بتحويل التهديد إلى المباحث التي لاحقت الرسالة الالكترونية وتوصلت إلى عنوان مرسلها وقامت باعتقاله وتم تحويل الشابين إلى المحكمة.

وقد قدمت وزارة العدل الاميركية اتهاما رسميا إلى مواطنين أمكين من ولاية نيويورك بتوجيه تهديدات بالقتل لمواطنين مسلمين مقيمين في ولاية ديترويت ويفيد محضر الاتهام أن مايكل براتيساكس وجون بارنيت وجها رسائل إلكترونية إلى المركز سلامي الاميركي عدة مرات من منزلهما في ولاية نيويورك وهددا بقتل مسلمين يمارسون شعائرهم الدينية سلامية بحرية في الولايات المتحدة انتقاما لما يجري في منطقة الشرق وسط وأوضحت الوزارة في بيانها انه يجب على هيئة الاتهام إثبات خطورة هذه الرسائل الإلكترونية . وفي الممكن أن تصل عقوبة براتيساكس للسجن اثنتي عشرعاما، بينما قد يحكم على بارنيت بالسجن ستة أعوام، وجاء الاتهام بعد تحقيق أجراه مكتب المباحث الفيدرالي الذي تشرف عليه وزارة العدل ، لقد حول المركز سلامي ا لرسالة التي وصلته عبر البريد الالكتروني للمباحث وقامت وحدة خاصة من شرطة الانترنيت في المباحث بملاحقة مصدر الرسالة ومعرفة الكومبيوتر الذي صدرت منه وبالتالي مكان هذا الكومبيوتر ومن هم أصحابه وقامت على ضوء ذلك باعتقال المذكورين ، وهذا يعني بالخصوص أن كاتب أية رسالة عبر الانترنيت حتى لو كتبها من بريد الكتروني وهمي أو مزور لا يمكنه الهروب من الملاحقة القانونية ، وهذا ما حصل مؤخرا في السعودية فقد اعتقلت الاجهزة منية المعودية مجموعة من الاشخاص يكتبون ويبثون رسائل بذيئة

عبر الانترنيت حيث لاحقت الجهات منية هذه الرسائل وعرفت مصادرها وهو مر الذي دفع مسئولا في وزارة الداخلية السعودية إلى التصريح قبل مدة بأن الوزارة ستلاحق الذين يسيئون للآخرين عبر الانترنت.

من المعروف أن إبداء الرأي شيء وإرسال بريد الكتروني يتضمن تهديدات شيء آخر وهذه ليست المرة و التي يتم فيها اعتقال أشخاص بعد تهديدات عبر الهاتف أو البريد الالكتروني والطريف أن الكثيرين من عرب أمريكا يتبادلون تهديدات بالقتل عبر البريد أو بالهاتف كلما اختلفوا ويظن البعض أن تستره وراء جهاز كومبيوتر في غرفته في مكان ما من العالم يعني أن أحدا لن يعرف علاقته بجريمة يرتكبها عبر الانترنت . ربما كان هذا صحيحا قبل سنوات، ولكن بعد تطور خدمة الانترنت وسن قوانين دولية لضبطها وتشكيل شرطة انترنيت لملاحقة المجرمين اختلفت الصورة تماما وأصبح بإمانك سوق من يرسل إليك بتهديد أو حتى بشتائم بذيئة إلى القضاء ، إذ يكفي أن تحول رسالته إلى المباحث سواء في قطر أو خارجها حتى يتم التعامل معها من قبل محترفين في أجزة الشرطة.

ثانيا : الطبيعة الملاحقة:

تتم جرائم الملاحقة على شبكة الإنترنت غالبا باستخدام البريد الإلكتروني أو وسائل الحوارات الانية المختلفة على الشبكة، تشمل الملاحقة رسائل تخويف ومضايقة.تتفق جرائم الملاحقة على شبكة الإنترنت مع مثيلاتها خارج الشبكة في الاهداف والتي تتمثل في الرغبة في التحكم في الضحية ،و تتميز عنها بسهولة إمكانية إخفاء هوية المجرم علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة ، الامر الذي ساعد في تفشي هذه الجريمة، من المهم الإشارة إلى أن كون طبيعة جريمة الملاحقة على شبكة الإنترنت لا تتطلب اتصال مادي بين المجرم والضحية، لا يعني بأي حال من الاحوال قلة خطورتها،فقدرة المجرم على إخفاء هويته تساعده على التمادي في جريمته والتي قد تفضي به إلى تصرفات عنف مادية علاوة على الآثار السلبية النفسية على

الضحية.فالقصد من المضايقة هو خلق نوع من التذمر و الملل في نفس المجني عليه مما يؤدي به للانصياع لطلبات الجاني او لمجرد المضايقة فقط.

ثالثا: انتحال صفة

هي جريمة الالفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظرا لسرعة انتشار ارتكابها خاصة في الاوساط التجارية. تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية ، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية شخص المجرم، لتسهيل ارتكابه جرائم أخرى، إن ارتكاب هذه الجريمة على شبكة الإنترنت أمر سهل وهذه من اكبر سلبيات الإنترنت الامنية .وللتغلب على هذه المشكلة ، فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت .كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة.

رابعا: التغرير والاستدراج:

غالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة. حيث يقوم المجرمون بإلمام ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت .والتي قد تتطور إلى اللقاء المادي بين الطرفين، و القصد من ذلك هو ربط علاقات غير مشروعة أو استخدام طفال في أغراض أخرى لا أخلاقية.إن مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد اخر، وكون معظم الضحايا هم من صغار السن ، فإن كثير من الحوادث لا يتم الإبلاغ عنها ، حيث لا يدرك كثير من الضحايا أنهم قد غرر بهم.

خامسا: التشهير وتشويه السمعة:

يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فردا أو مجتمع أو دين أو مؤسسة تجارية أو سياسية. تتعدد الوسائل

المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين و يضم لهذه الجرائم كذلك تشويه السمعة،الشائعات و الاخبار الكاذبة لمحاربة الرموز السياسية و الفكرية و حتى الدينية من اجل تشكيك الناس في مصداقية هؤلاء فراد،و قد يكون الهدف من ذلك هو الابتزاز،و مثالها ضبط المحاكم المصرية لمهندس كمبيوتر بتهمة نشر معلومات كاذبة على الانترنيت للتشهير بعائلة مسؤول مصري و تصميم موقع على الانترنيت لذلك الهدف و قد كانت ابنة المسؤول أكثر عرضة للقذف و التشهير و بعد التحري عرفت هوية الجاني و تحفظت الاجهزة بعد توقيفه على جهاز الكمبيوتر الذي اعتبر كدليل مادي على ارتكاب الجريمة.

سادسا: صناعة ونشر الإباحية

لقد وفرت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية وقد شجعتها بشتى وسائل عرضها من صور وفيديو و حوارات بوضعها في متناول الجميع ، ولعل هذا يعد أكبر الجوانب السلبية للإنترنت خاصة في مجتمع محافظ على دينه وتقاليده كمجتمعنا الإسلامي، وركز المهندس حمد بن عبد العزيز السليم – مدير مركز أمن المعلومات بوحدة خدمات الإنترنت في مدينة الملك عبد العزيز للعلوم والتقنية على صناعة ونشر الإباحية عند تقسيمه لجرائم الانترنت مما يحرض القاصرين على أنشطة جنسية غير مشروعة، وصناعة الإباحية من أشهر الصناعات الحالية وأكثرها رواجًا خاصة في الدول الغربية والآسيوية كما ان صناعة ونشر الإباحية مجرمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم الأطفال.

لقد تمت إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الامريكية خلال أربع سنوات السابقة ل: 1998م ، تتعلق هذه الجرائم بتغرير الاطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية لأطفال،و أن هذه الجرائم تشكل طائفة .

Sexuel Crimes شمل: تحريض القاصرين على أنشطة جنسية غير مشروعة وإفساد القاصرين بأنشطة جسية عبر الوسائل الالكترونية، وإغواءأو محاولةإغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة Luring or Attempted Luring of a Minor by Computer for Unlawful Sexual Purposes وتلقيأو نشر المعلومات عن القاصرين عبر الكمبيوتر من اجل أنشطة جنسية غير مشروعة ، والتحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية،نشر وتسهيل نشر واستضافة المواد الفاحشة عبر الانترنت بوجه عام وللقاصرين تحديدا ،ونشر الفحش والمساس بالحياء (هتك العرض بالنظر) عبر الانترنت، وتصوير أو إظار ا لقصر ىضمن أنشطة جنسية ،واستخدام الانترنت لترويج الدعارة بصورة قسرية أو للإغواء أو لنشر المواد الفاحشة ،التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم، و الحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية ، ،وإمعان النظر في هذه وصاف نجد أا تجتمع جميعا تحت صورة واحدة هي استغلال الانترنت والكمبيوتر لترويج ا لدعارةأو إثارة الفحش واستغلال طفال والقصر في أنشطة جنسية غير مشروعة و لعل الكثير منا تفاجئوا بصور خليعة تظهر على شاشة الكمبيوتر، و هي نوع من الدعاية المجانية لهذه المواقع التي تبيع الرذيلة و تحقق ملايين الدولارات من الارباح و تستهدف نشر البغاء في المجتمعات.

وفي اعتراف القاتل السفاح الذي ذاع صيته في كل أنحاء أمريكا والمعروف باسم تيدباندي (Ted Bundy) عند مقابلته مع الدكتور جايمز دوبسون في دراسة تعالج تأثير باحية المعروضة على شبكات الانترنت . يوم قبل إعدامه . قال: "اشد أنواع المواد الإباحية فتكا تلك المقترنة بعنف أو بالعنف الجنسي. لأن تزاوج هذين العاملين – كما تيقنت جيدا – تورث ما لا يمكن وصفه من التصرفات التي هي في منتهى الشناعة والشاعة" ،وقال أيضا: "[أ ناو لمثا] لم و لدوحوشا، نحن أبنا ؤكموأزواجكم، تربينا في بيوتمحافظة، ولكن المواد الإباحية يمكنها اليوم أن تمد يديها داخل أي منزل فتخطف

أطفالم"وقال قبل ساعات من إعدامه" :لقد عشت الآن فترة طويلة في السجون وصاحبت رجالا كثيرين قد اعتادوا العنف مثلي، وبدون استثناء فإن كلهم كان شديد غماس في الصور الإباحية وشديد التأثر بتلك المواد ومدمنا لها".

ـ لثا:جرائم القذف و السب

تعد جرائم السب و القذف الاكثر شيوعا في نطاق الشبكة.فتستعمل للمساس بشرف الغير أوكرامته و اعتباره.و يتم السب و القذف وجاهيا عبر خطوط الاتصال المباشر او يكون كتابيا.أو عن طريق المطبوعات و ذلك عبر المبادلات الالكترونية بريد الكتروني،صفحات الويب،غرف المحادثة فحسب القواعد العامة لجرائم القذف و السب يستعمل الجاني عبارات بذيئة تمس و تخدش شرف المجني عليه. و مهما كانت الوسيلة المعتمدة، مع علمه أن ما يقوم به يعد مساسا بسمعة الغيربل أن إرادته اتجه لذلك بالذات ، و بالتطور أصبحت الانترنت إحدى هذه الوسائل أن لم نقل اكثرها رواجا.فعادة ما ترسل عبارات السب أو القذف عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب مما يؤدي بكل من يدخل هذا الموقع لمشاهدتها أو ستماع إلا و يتحقق بذلك ركن العلنية الذي تتطلبه الكثير من التشريعات في السب العلني.و إذا لم يطلع عليها احد فانه يمكن تطبيق مواد السب أو القذف غير العلني و يرى جانب من الفقه انطباق النصوص التقليدية على جرائم السب و القذف الانترنتية. وذلك باعتبار صفحات الانترنت كنشرة إعلامية فتأخذ حكم السب و القذف عبر الإعلام. لتوفر فيه عناصر: الكتابة شر فار التي توضع تحت تصرف الجمهور، طبقا للحكم الصادر بفرنسا في 03 أوت 1999 .و من التطبيقات في الدول العربية هو ما تفاجأت به إحدى ملكات الجمال إثر تواجدها بدبي بخبر على موقع للانترنت مفاده وفاة ثري عربي خلال ممارسته الجنس مع ملكة الجمال المعنية بذكر اسمها .و تقدمت ببلاغ للنيابة العامة و بعد التحقيق توبع صاحب الموقع بتهمة المساس بعرض المعنية بطريق النشر عبر صفحات الانترنت طبقا لقانون العقوبات تحادي ر قم03 لسنة1987 .رغم أن

المحكمة قضت بعدم إختصاصها باعتبار موقع الانترنت مصدره لندن ، و بعد الاستئناف و رجوع الدعوى من جديد إلى محكمةأول درجة تمت إدانة المتهم و عقابه بثلاث أشر حبس ، و إحالة الشق المدني على المحكمة المدنية المختصة .

الفرع الثا ث:جرام واقعة على أمن الدول

لستغ ث الكث من الجماعات المتطرفة الطبيعة الاتصالية الا نت من أجل بث معتقداتها ،و أفا راء بل تعداه الامر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذ ا ملآخر في استعمال الإنترنت، التي سمحت لهم في ارتكاب جرائم غاية في الفتك في حق المجتمعات والدول، بل الاخطر من ذ لك أ ت ا حتالإنترنت لكث من الدول ممارسة التجسس على دول أخرى، و ذلك بالاطلاع على مختلف الأسرار العسكرة والاقتصادية لهذه الاخير، خاصة فيما يتعلق بالدول التي يكون بينها نزاعات، و.يبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الإنترنت، حيث تعطي الإنترنت فر صاللتأ ثر على معتقد ثو تقاليد مجتمعات بأكملها مما يسهل خلق الفوضى.

أولا: الإرهاب

أ صبح راب في الوقت الراهن ظاهر عالمية، تربط بعوامل اجتماعية وث قافية وس يلسيةو تكنو لوجيةأفرزها التطورات السريعة والمتلاحقة في العصر الحديث، فقد شهدت العقود الاخيرة فالقرون ا لعشرين بروز العديد من التنظيمات المسلحة والعمليات الإرهابية في مختلف أنحاء العالم[1].

يتم بث ث قافة راب عبر نت عن طرق تأسيس مواقع افتراضية تم ل المنظم ت ر ابية، وهي مواقع آخذة في الازدياد مع ازدياد المنظم ت ر ابية حيث عل لعب رذه المواقع تحملها مسؤولية إحدىالهجمات التي ارتكبت، أو بيانات تنفي أو

1:عبد الله بن عبد العزيز الموسف، أساليب تطور ا لامج والمناهج ا لتربية ، لمواجة ارائه المستحدثة، جامعة نايف العربية للعلوم ا منية، الرياض، ا لطبعة و ،2004، ص 25.

عـلى ء أخبار صادرة عن منظمات أو جهات دولية أخرى.

تجند الجماعات ا لإرهابية من خلال الانترنت عند طورل ابية جديدة تساعدهم عتنفيذ أعمالهم جرامية، وهم في ذلك يعتمدون على فئة الشباب، خصوصا ضعاف العقل والفكر، فتعلن لجماعات ر ابية عبر مواقعها على الانترنت عن حاجتها لى عناصر انتحارية ،كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب الديني، فدائما ما تصف الاهداف التي تستهدفها عملياتهم بالكافرة، وتقوم بدعوى الشباب إلى الجهاد وحثهم على الاستشهاد في سبيل الله والفوز بالجنة[1].

الجدير با لذكرأنه إذا كانت ال جماعات ر ابية تسعى إلى الدعاية والترويج لنفسها عن طرق اليات مختلفة منها جذب انتباه وسائل الإعلام المعروفةلتغطية أخبار اجماعة وانشطتها، إلا أن السياسات تحريرية لهذه الوسائل، و المعايير الخاصة بها في نشر وسائل معينةو إ سقاطأخرى كل ذلك يمثل قيودا على استفادة اجماعات من نشر وسائل الإعلام عنها، بنما في المقابل تتيح المواقع الإلكترونية للجماعات ر ابية قدرا كبير من التحكم في المعلومات و الرسائل الإعلامية التي ترد توجيهها، بل ايضا تتيح لاالمرونة في توجيه الرسائل لفئات مختلفة من الجمهور المستهدف، ورسم صور ذهنية عن الجماعة وعن اعدائها أحيانا تستخدم الجماعات ا لإرهابية الإنترنت إلى جانب أغر اض الدعاية والترويج في نشر معلومات بهدف شن حرب نفسية ضد أعدائها، وهو ما يتحقق من خلال نشر معلومات مضللة أو مغلوطة، نشر تهديدات وصور ولقطات فيديو مرعبة(مثل مواد الفيديو التي تصور احتجاز الرهائن المختطفين من قبل الجماعة)[2]

ثانيا: الجريمة المنظمة.

عرف الجرعة المنظمة بأنها تعبير عن مجتمع إجرامي يعمل خارج إطار الشعب والحكومة ويضم بين طياته ألاف المجرمن الدين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطور وتقدما، كما يخضع أفردها

1: محمد سيد سلطان، المرجع السابق، ص 13.

2: مها عبد المجيد صلاح، المرجع السابق، ص 12.

لقواعد قانونية سنوها لأنفسهم وترفض أحكاما بالغة القسوة على من يخرج عن نظام الجماعة ويلتزمون في أداء أنشطتهم جرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من ورائها الأموال الطائلة.[1]

الجريمة المنظمة ليست وليدة التقدم ون كانت استفادت منه. فالمة المنظمة وبسبب تقدم وسائل الاتصال والتكنولوجيا أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، بل أصبح انتشارها على نطاق واسع وكبير و أصبحت لا تحدها الحدود اغرافية. كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الانترنت في تخطيط وتمرير وتوجيه المخططات جرامية وتنفيذ وتوجيه العمليات جرامية بسر و سهولة.[2]

اكتشفت جماعات الجريمة المنظمة استخدام التكنولوجيات بصفتها فص للاستغلال و تحقيقأرباح غير مشروعة، وفطن المجرمون أيضا أن شبكة الإنترنت تستطيع أن تؤمن فرصا جديدة وفوائد جمة للأعمال غير المشروعة.

عد ا لابط نالجريمة المنظمة وشبكة الإنة نت ليس طبيعيا فقط، ولكنه ترا ط من المرجح أن يتطور إلى حد أبعد في المستقبل. فشبكة الإنترنت تؤ م نالاهداف في نفس الوقت للجريمة، وتمكن من استغلال هذه الاهداف لتحقيق أرباح كبيرة باقل قدر ممكن من المخاطر، وجماعات الجر مةالمنظمة لا تريد اكثر من ذلك. ولهذا السبب من الاهمية بمكان تحديد بعض الطرق التي تتداخل فيها الجريمة المنظمة حاليا مع الجريمة التي ترتكب من خلال الشبكات الإلكترونية[3]

ثالثا: جرمةالتجسس.

ينتج عن الاستخدام المتزايد للحاسبات الالية في العديد من المجلات، تجميع المعلومات بدرجة كبير في موضع واحد، ويؤدي هذا التخزين في الحاسبات المركة إ

1: نهلا عبد القادر المومني، المرجع السابق، ص 87.

2: سامي علي حامد عياد، المرجع السابق، ص 83.

3: عبد الله عبد الكريم عبد الله، المرجع السابق، ص 42

سهولة التجسس عليها، وعلى المعلومات المخزنة فيها بمختلف درجات سريتها.

يقصد بالتجسس في هذا الموضع هو الاطلاع على معلومات خاصة بالغير مؤمنة في جهاز اخر، وليس مسموحا لغير المخولين بالاطلاع عليها سهلت شبكة الإنترنت الاعمال التجسسية بشكل كبير، حيث يقوم المجرم بالتجسس على ا لأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاث أهداف أساسية، وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي.

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

راعا : الجرائم الماسة بالأمن الفكري.

ينطوي الخوف من عواقب ثورة المعلومات والاتصال على تيار عاطفي خفي وقوي، يتمسك بثقافة وقيم ومفاهيم أخذت قاعدتها الاجتماعية والمادية والتربوية تتزعزع، وغدا باديا للعيان أنها اليوم تترنح تحت وطأة قوى التكنولوجيا والمعلوماتية والاتصالية التي تلح علينا بالانفتاح بالمعرفة والصوت والصور، وإذا كنا قد تغي نا عن ابائنا دون ضجة كبيرة كالحاصلة اليوم، فهل يمكن أن نتوقع غير ذلك بصدد أولادنا؟

تتجسد الإجابة في أن الاحتمال الأكبر هو أن التغيير سيحصل، كما تنبئ وقائع تكنولوجيا المعلومات اليوم، وكما دهشنا بالتلفزيون وتخوفنا من اثر ه على حياتنا لأول مر ة، وتغي نارغم النقد و التردد، فليس هنالك ما يدعونا لاعتقاد غير ذلك بصدد ثورة المعلومات اليوم وخاصة الإنترنت.

بناءا على خصائص الشبكة العالمية ا لإ نت، التي منحت المستخدم الكثير من الخيارات، من خلال عدم خضوعها لأي رقابة ،وعبو رها لحدود الجغ رافية بين الدول، و نمو االسر يع المتواصل، وإمكانية مشاركة الجميع من مختلف دول العالم، مع ما

تمنحه من القدر على التخفي وعدم المواجهة نتيجة الافاضية التي تعد من أهم خصائص هذه الشبكة، إضافة إلى الكم الهائل من المعلومات التي يمكن الحصول عليها من عدة مصادر لا يمكن التحكم فيها ومتابعتها أو شراف عليها، كل ذلك جعل هذه الشبكة من أهم مقومات المجتمع المعلوماتي التي تؤدي إلى نحراف الفكري، من خلال عرض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العالمية الا نت ، وتهدد الامن بأبعاده كافة.

تتولى عبر الانترنت الهجمات الثقافية، والحضارية التي قد تزعزع الامن الفكر ي والعقدي للشعوب المغلوبة على أمرها،و تنشر عبرها الغالبة فكرها، ولغتها، وقيمها، وقد ظهر في أدبيات بعض الباحثن من بدا ياتشبكةالانترنت أشارت التحذير من الغزو الفكر يالمركز الذي يستقبله الجيل العربي المسلم مما قد يجعله عرضة للهز مة الفكرة.

المطلب الثاني: اركان الجريمة المرتكبة عبر الانترنت

تتخذ الجريمة المركبة عبر الإنترنت من الفضاء الافتراضي سر حا لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المر تكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع،ومجر م يقوم بهذا الفعل، ومن خلال هذا التشابه سوف نتطرق إلى تبيان ا لأركان التي تقوم عليها هذه الجريمة، حيث نسلك سبيل المقارنة بينها وبين الجريمة التقليدية، وبالتالي نعمد إلى تبيان مدى انطباق مبدأ الشرعية على الجريمة لمر تكبة عبر الانترنت (ا لفرع ول)، ثم نوضح الركن المادي (ا لفرعالثاني)، لتنتهي إلى تحديد الركن المعنوي فيها (ا لفرعالثالث).

ا لفر ع ول : الركن الشرعي.

ي قصدبالركن الشرعي للجرمة وجود نص يجرم الفعل ويوضح العقاب المرتكب

عليه وقت وقع هذا الفعل[1]، فمبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم تتوفر النص القانوني، فلا جريمة ولا عقوبة إلا بنص، ومتى ما انتفى النص على تجريم مثل هذه الافعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصير في مافحةك اجرائم غير أن السؤال المطروح هو مدى تطبيق مبدأ الشرعية على الجرائم التي ترتكب عبر الإنترنت؟

أولا : مدى انطباق النصوص القائمة على جرائم الانترنت.

تشعب الإشكالات الناجمة عن استخدام الحواسيب الالية وشبكاتها جعل مهمة القضاء صعبة نظر لعدم وجود نصوص كفيلة بمعالجة هذه المشكلات، والتي من بينها الاستخدام غير المشروع لشبكة الإ ت

حاولت قوانين العقوبات مواجهة تحديات ارائم المركبة عبر الإنترنت بطق تقليدية كتلك المقرر في جرائم الاموال، إلا أنه تبين قصور هذه الوسائل التقليدية عن مواجهة العديد من الافعال التي تهدد مصالح اجتماعية والتي ارتب ط بظور وانتشار أجهز الكمبيوتر.

تبين في بعض الاحوال أن ثمة أفعالا جديدة ترتبط باستعمال الكمبيوتر لا تكفي النصوص القائمة لمكافحتها، من ذلك الاعتداء على حرمة الحياة الخاصة، هذا النوع ن الاعتداء لا يعاقب عليه قانون العقوبات لا إذا كان مرتبطا بمكان خاص، أما تجميع معلو ملت عن فراد وتسجيلها في الكمبيوتر، فإنه لا يخضع للتجرم وفقا للقواعد العامة، كما أن التداخل في النظام نظام الحاسب الالي وتغيير البيانات، فهي صور جديدة لا يعرفها قانون العقوبات قبل ظهور الكمبيوتر وشبكة الإنترنت، كل ذلك يؤكد قصورا لقو اعدالتقليدية في القانون الجنائي على مكافحة هذا النوع الجديد من

1: عبد المحسن بدوي محمد أحمد، استراتيجيات و نظريات معالجة قضايا الجريمة و الانحراف في وسائل ا علام الجماهيري، جامعة نايف العربية، الخرطوم، 2005، ص5.

ارائم.[1]

لا يتطور القانون الجنائي دائما بنفس السرعة التي تتطور بها التكنولوجيا ولا بـ ـفى المارة التي يأتي بها الذهن البشري لتسخير هذه المبتكرات لاستخدامه السيئ. لـ لكو كإستنتاج أولي و منطقي نعتقد أن القانون الجنائي لا يكفي من حيث المبدأ في مواجهة هذا النمط من جرام خاصة أن النصوص قد وضعت للتطبيق وفق معايير معينة كانت سائدة أيام وضعها .

ثانيا: الحاجة لتدخل المشرع لمواجهة جرائم الانترنت.

تعتبر الجريمة الواقعة من نتاج التطور التكنولوجي أنها من المستحدثات التي عجزت مواد القوانين العقابية التقليدية مواجهتها، لذلك سعت معظم دول العالم ولا سيما تلك المتقدمة قانونيا إلى سن التشريعات والقوانين لمواجهة هذه ارائم

تعتبر الولايات المتحدة الا وكية من بين الدول السباقة التي جسدت تشريع مستقل بشأن جرائم الكمبيوتر بصفة عامة و جرائم ذ نت بصفة خاصة كما تتميز الولايات المتحدة ا لأمريكية بوجود اكبر قدر من التشريعات تغطي مسائل جرائم الكمبيوتر

وضـ عت الولايات المتحدة الامريكية قانونا خاصا بحماية الحاسوب والشبكات ا لمحسوبة، وذلك عام 1976، وفي عام 1985 حدد معهد العدالة القومي فيها خمسة أنواع رئيسية لهذا النوع من الجرائم و هي:

1) جرائم الحاسوب الداخلية.
2) جرائم الاستخدام غير المشروع عن بعد، شبكات المعلومات المحسوبة
3) جرائم التلاعب بالحاسوب، أي التلاعب غير المخول و غير المشروع في الشبكات ا لمحسوبة.
4) دعم التعاملات الإجرامية للنظم و الشبكات المحسوبة، و إسنادها من قبل

1: عبد الجبار الحنيص، المرجع السابق، ص 195.

الآخرين.

5) سرقة البرامج الجاهزة و المكونات المادية.

صدر في عام 1986 قانون آخر يعرف فيه جميع المصطلحات الضرورة لتطبيق جرائم النظم المعلوماتية والشبكات المحوسبة، وعلى أثر ذلك قامت الولايات المتحدة الأمريكية الداخليةبدورها بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم، والتي تتماشى مع التشريعات الاتحادية المذكورة.

قام كذلك المشرع الفرنسي بسن تشريع خاص فيما يخص جرائم المعلومات وذلك في أغسطس عام 1986، حيث تقدم النائب " جاك جودفرن" باقتراح قانون تم اعتماده من البرلمان الفرنسي وصدر في 5 يناير 1988 برقم 19 تحت عنوان" الجرائم في المواد المعلوماتية"، وتم إدماجه في الفصل الثاني من قانون العقوبات وخصصت له المواد من 2/432 إلى 9/462.

الجدير بالذكر أن الفصل المخصص لهذه الجرائم الحق بالباب المخصص بالجنايات والجنح ضد الاشخاص، أي بعد الفصل الثاني من الجرائم المخصصة بالجنايات والجنح ضد الملكية، وقد ركزت اللجنة التشريعية على الهدف الذي توخاه اقترح "جودفرن" حماية النظام المعلوماتي ضد أي اعتداء خارجي، فقرر أن الهدف من النصوص الجديدة تجريم وردع الدخول غير المشروع على برامج المعلوماتية[1]

يعتبر تدخل المشرع لوضع نصوص قانونية لتجريم الافعال غير مشروعة الناتجة عن استعمال الإنترنت أكثر من ضروري، خاصة في ظل التطور السريع الذي يعرفه هذا النوع من الجرائم، ولقد اتخذنا المشرعين الامريكي و الفرنسي كمثال نظرا للتطور الكبير ولقوة القانونية التي يتمتعان بها.

غير أن الملاحظ على المستوى الدولي وجود فجوة رقمية رهيبة بين الدول، فبالنسبة للدول التي تعاني من التخلف في المجال المعلوماتي، لم تسن بعد قوانين تجرم بها

1: أحمد خليفة الملط، المرجع السابق، ص 126.

الافعال غير المشروعة عبر الإنترنت ،و اكتفائها بتطبيق قواعد قانون العقوبات الخاصة بها، غير أن هذه القوانين اثبتت قصورا في هذا المجال كما أسلفنا الذكر، الامر الذي يستوجب منها التوسع في تفسير هذه النصوص لتطبيقها على الجرائم المرتكبة عبر نت.

ثالثا: التوسع في تفسير النصوص القائمة لتطبيقها على جرائم الانترنت.

لس أمام الدول التي لم تسن بعد قوانين خاصة لتجرم مختلف ارائم الن شئة عن الاستخدام غير المشرح لشبكة الإنترنت سوى تطبيق القوانين الجنائية القائمة بموادها التقليدية على هذه الوقائع خوفا من إفلات الجناة من قبضة العدالة، وذلك مع بعض التفسير الموسع لهذه النصوص.

فعلى الرغم من أن القصور التشريعي قدأصبح واقعا ملموسا، إلا أن هذا لا يحول دون الاجتهاد في تفسير النصوص العقابية التقليدية التي تعاقب على صور الاعتداءات المختلفة على المال، بحيث يمكن تطبيقها على الجرائم المستحدثة التي أوجدتها ثور الاتصالات عن بعد، فلا محالة أن التطور قد يوسع من دائر المجالات التي تحما ضوص الـ تجم والعقاب بحيث يمكن أن ندخل في إطارها عنصر أخرى طالما أمكن اعتبارها من جنسها وأن المشرع يحميها بذات هذه النصوص.

يكون اتخاذ سبيل التفسير الموسع للنصوص التقليدية من أجل تطبيقها على ارائم لمرتكبة عبر انترنت، بمنح السلطات القضائية حرية تفسير هذه النصوص حيث أن القاضي يمكنه أن يعطي تفسيرا أكثر مرونة للنصوص القانونية يسمح من وضع هذه الجرا ئم تحطائلة الـ تجم والمتابعة، وذلك في ظل السلطة التقديرية التي يتمتع بها القاضي.

فعندما عرض قضيةجز ائية على القاضي فإن أول عملية يقوم بها هي تكييف الو اقعةلمعرف ةمدى ظا بقا معالنص الذي يجرمها، و لـلوصولإلى هذه الغاية يقوم القاضي باستخلاص عناصر الواقعة من النص ،وقديصادف القاضي أثناء ذلك صعوبة

أو غموضا فيقوم عندئذ بتفسير النص الجنائي.[1]

لكن تطبيق هذه النصوص التقليدية بمفهومها الموسع والخاصة ببعض ارائم السرقة على سبيل المثال على الجرائم الواقعة بطرق الانترنت من شأنه المساس بمبدأ الشرعية الجنائية، إذا ترك الامر بيد القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله.

الفرع الثاني : الركن المادي

يطلق مبدأ تحديد الفعل غير المشرح وعطائه صفة الجريمة ،بتحديد الركن المادي فيه، فلا جريمة دون ركن مادي، الذي يتمثل في السلوك الذي يقوم به الجاني من أجل تحقيق غاية ما ويحدد له القانون العقاب اللازم، وهو يتباين بتباين ارائم المركبة من قبل الجاني، شرطة أن يكون له مظهر خارجي ملموس، غير أن تحديد الركن المادي الجرائم الواقعة عبر شبكة العالمية الانترنت تكتفيه العديد من الصعوبات خاصة فيما يتعلق بتحديد النتيجة جرامية والربطة السببية، وسوف نبين الركن المادي في هذا النطاق كالآتي:

أولا: القواعد العامة في الركن المادي للجريمة

1) السلوك الإجرامي:

عدالسلوك جرامي أمعناصر الركن المادي لأي جريمة، لأنه يكشف عن سلوك مخالف لإرادة المشرع، ويبدو بمظاهر مادية ملموسة في العالم الخارجي، ويعني ذلك أن الافكار داخل النفس لا عقاب عليها، و يعرف السلوك جرامي في ارائم التقليدية على أنه فعل الجاني الذي يحدث أثر في العالم الخارجي ، و يغير هذا السلوك لا يمكن محاسبة الشخص مهما بلغت خطورة أفاره وهواجسه الداخلية، والسلوك هو الذي يخرج النية و التفكير في جرام إلى حيز الوجود واعتبار القانون، ولا يكاد يفرق ن

1: محمد عبيد الكعبي، المرجع السابق، ص 53.

السلوك الإيجابي (الفعل) والسلوك السلبي (الامتناع عن فعل)، مادام أن لهما نفس النيجة.

2) النتيجة جرامية:

يقصد بالنتيجة جرامية، ثر المادي الذي يحدث في العالم الخارجي كأثر لسلوك جرامي. فالسلوك قد أحدث تغير ا حسيا ملموسا في الواقع الخارجي. ومفهوم النتيجة كعنصر في الركن المادي المادي للجرمة يقوم على أساس ما يعتد به المشرع ويرتب عليه نتائج،غض النظر عما يمكن أن يحدثه السلوك جرامي من نتائج أخرى[1]

3) الرابطة السببية

تتمثل الرابطة السببية هي الصلة التي تربط بين الفعل والنتيجة وتثبت أن ارتكاب الفعل هو الذي أدى على حدوث النتيجة. وأهمية رابطة السببية ترجع إلى أن إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة. وتحقق رابطة السببيةتلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حدالشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت الجرمة غير عمدية، فإن نفي رابطة السببية يؤدي إلى انتفاء المسئولية كلية عنها، ذلك انه لا شرع في ارائم غالعمدية.[2]

ثانيا: تحديد الركن المادي في الجريمة المرتكبة عبر الانترنت.

تحديد الركن المادي في ارائم المركبةعبر الإنترنت ينير جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة والمتمثل في الجانب التقني، وهذا ما يميز ركنها المادي، الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو الشبكة العالمية للإنترنت، ومن هنا تبدأ التساؤلات التي تتعلق ببداية النشاط التقني أو الشروع فيه.

1: عبد الله سليمان ، المرجع السابق، ص 149.

2: م ضوربن صالح السلمي، المرجع السابق، ص 75

ومكان البداية واكتمال الـ كي الما ي ،و أجزا ءالـ سلوك جرامي لمرتكب في العالم المادي، أو العالم الافتراضي، وغيرها من التساؤلات التي تتعلق بطبيعة الجرمة.

يتطلب النشاط و السلوك المادي في جرائم الانترنت وجود بيئة رقمية ،وا تصال بالإ نت ،وتتطلب أيضا معرفة بداية هذا النشاط و الشروع فيه ونتيجته، ليس كل جريمة تستلزم وجود أعمال تحضيرية، لا أنه يصعب الفصل بين العمل ا لـ قضي والبدء في النشاط جرامي في جرائم نترنت حتى ولو كان القانون لا يعاقب على الاعمال التحضيرية ففي مجال تكنولوجيا المعلومات الامر يختلف عض الشيء، فشراء بر امج اخترق، ومعدات لفك الشفرات و كلمات المرور، وحيازة صو ردعارة للأطف ل فمثل هذه الاشياء تمثل جريمة في حد ذاتها.

مجمل القول أن السلوك الإجرامي في الجريمة المرتكبة عبر الانترنت يربط بالمعلومة المخزنة داخل الحاسب الالي أو ا نلكحرمةالاشخاص، والسلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب الآلي فيتم تدمير النظام المعلوماتي أو حصول التزوير أوالسرقة عن طريق الشلل إلى نظام أ رصدةالعملاء في البنوك[1]

تثير مسالة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة، فهل تق صرعلى العالم الافتراضي، أم أن لها جزءا في العالم المادي، وهل تق صرالنيجة على مكان واحد أو تمتد لشمل دولا ،و أقاليمعدة،فعلى سبيل المثال إذ قام أحدالمجرمين في أ مكا ا الاتيية باخ إق جهاز خادم أحدالبنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البلدالمسروق أم توقيت الجهاز الخادم في الصين.

تحديد رابطة السببية في مجال أضرار الإنترنت يعد من المسائل الصعبة والمعقدة بالنظر إلى تعقيدات صناعة الحاسوب والإنترنت،تطور إمكانياتها و سارع هذا التطور، إضافة إلى تعدد و تنوع أساليب الاتصال بين الاجهزةالإلكترونية وتعدد المراحل التي تمر

1: منصور بن صالح السلمي، المرجع السابق، ص 76

بها الاوامر المدخلة حتى تخرج و تنفذ النتيجة المراد الحصول عليها، كل ذلك سيؤدي حتما إلى صعوبة تحديد السبب أو الاسباب الحقيقية للإماءات المرتكبة في هذه لمسؤولية[1]

الفرع الثالث : الركن المعنوي

عتبر اركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تعد بين ماديات اجريمة وشخصية الجاني، ويطلق عليها الركن الادبي أو الشخصي وهو يعني في الحقيقة الجاني أو المجرم تحديدا، فالركن المعنوي هو المسلك الذهني أو النفسي للجاني اعتباره محور القانون الجنائي، من إسناد وإذناب مع إقرار حق الدولة في العقاب الذي يبني عـ المقومات[2]، هذا عالعموم في جميع الجرائم، غير أن التساؤل يثور في مجال الجرائم المرتكبة عبر الإنترنت.

1: منصور بن صالح السلمي، المرجع السابق، ص 76

2: منصور بن صالح السلمي، المرجع نفسه، ص 68


الفصل الثاني

تمهيد:

صاحب ظهور شبكة الإنترنت بروز تحديات جديدة للمنظومة القانونية الموضوعية والإجرائية عل 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 والمنهج، وألقت بضلالها على العالم بأسره، فكانت الاضرار والخسائر التي انجرت عنها فادحة على المستويين الدولي و المحلي، الامر الذي أدى بمختلف الدول إلى الإسراع من أجل المحاولة للتصدي لهذه الظاهرة، فتضافرت الجهود من أجل إيجاد سبل مكافحة الجريمة المرتكبة عبر الإنترنت بنجاعة وفعالية أكثر.

يتضح لنا جليا خطورة الجرائم المرتكبة عبر نترنت الامر الذي يوجب الكثير من الجهد لمكافحتها، لكنها تبقى بعيدة كل البعد عن الأسس السليمة والخاصة بها، حيث أن جراءات التقليدية المطبقة على هذا النوع من الجرائم لم تعد مجدية نظرا لاختلاف الجرائم التقليدية وجراءم الإنترنت فعدم كفاية التشريعات الخاصة بها و تباينها، وصعوبة التكييف القانوني لها بالإضافة إلى الطبيعة اللامادية للجريمة من أهم الصعوبات التي تعتري سبل مكافحة هذه الجريمة. فقصور التشريعات يعرقل جهود التحقيق في هذه الجرائم، وقصور إحدى الدول أو بعضها في مواجهة هذه الجريمة يؤدي إلى إحباط الجهود المبذولة في دول أخرى، ذلك لأننا بصدد الحديث عن جريمةعابرة الحدود.

المبحث الاول : مكافحة و قمع جرائم الانترنت

بعد العرض لعدد من جرائم الانترنت،أجد نفسي أمام سؤال ملح يطرح نفسه بقوة، وهو هل هناك ضرورة لإيجاد انظمة تعطي السلطات الامنية والقضائية الحق في تجريمها و تطبيق عقوبات على مرتكبيها،أو يمكن استخدام الانظمة المقررة لتجريم ومعاقبة المماارسك التقليدية كالسرقة و التزوير.. ؟

في الحقيقة لا يوجد إجماع بين المختصين على رأي واحد،لكن نظرا لأن الانظمة الخاصة بالجرائم التقليدية قد لا تغطي جميع جوانب جرائم الانترنت لذا فإن من المهم في رأيي وجود نظام يجرم الاعمال غير المشروعة على الانترنت ويعاقب مرتكبيها،والاهم من ذلك هو توعية أفراد السلطات الامنية والقضائية المعنية بهذه الانواع من الجرائم من حيث كيفية التعامل معها وتدريبهم على دراسة و تحليل الادلة.[1]

فلاشك أن طبيعة هذه الجرائم تختلف عن الجرائم التقليدية ولذلك فإنه يتعين على من يتعامل معها أن يمتلك قدرات تقنية لا ئمة خ هةوأنه في الاونة الاخيرة قد زادت عمليات القرصنةوالهجوم على أجهزة الحاسب الالي،ووصل الامر إلى اختراق الاجهزة ذات الطابع السري كتلك الموجودة في المجال العسكري ومجال البورصة و البنوك، للتعرف على حسابات العملاء والوقوف على المهم من المعلومات،مما ينذر باندلاع حرب من نوع جديد بين الدول قد نطلق عليها مجازا الحرب الباردة الإلكترونية فقد أشار تقرير سنوي كشفت عنه شركة " مكافي" الرائدة في مجال الحماية الرقمية،إلى أن هذه الحرب التي تشن على أجهزة الكمبيوتر في العالم،تنذر بالتحول إلى أحد اكبر التهديدات الامنية خلال العقد المقبل.

ونوه التقرير إلى أن ما يقرب من 120 دولة تقوم بتطوير طرق لاستخدام الإنترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر والخدمات التابعة للحكومات، هيفا إلى أجزة المخابرات تقوم بالفعل باختبار شبكات الدول الاخرى بصورة روتينية بحثا عن ثغرات،وأن

1: إلياس بن سمير الهاجري "جرائم الإنترنت" الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية،المملكة المغربية،9 13 أفل2006 ص58.

أساليبها تزداد تطورا كل سنة.وحذر التقرير من أن الهجمات على مواقع الكترونية خاصة وحكومية في استونيا العام الماضي لم تكن سوى "قمة جبل الجليد"، حيث قالت استونيا أن الاف المواقع تأثرت بالهجمات التي أدت إلى شل البنية التحتية في البلد الذي يعتمد بشدة على شبكات الانترنت وتنبأ بأن الهجمات المستقبلية ستكون أكثر تطورا من مجرد عمليات بحث بدافع الفضول،إلى عمليات جيدة التمويل والتنظيم من التجسس السياسي والعسكري والاقتصادي والتقني،وفي نفس السياق أظهر تقرير أعدته شركة " سيمانتك" أن مجرمي شبكة الانترنت في منطقة المحيط الهادي،أصبحوا أكثر حرفية على نحو متزايد في تطوير وتوزيع الشفرات والبرامج الخبيثة.مشيرا أن الصين تشهد نسبة 42% من جرائم الانترنت في المنطقة،تاتي بعدها كوريا الجنوبية في المرتبة الثانية بنسبة 14% من تلك الجرائم، واحتلت اليابان المركز الثالث بنسبة 12. %

ونقلت صحيفة "بيزنس تايمز" السنغافورية عن "داريك هور" المدير العام لشركة سيمانتك في سنغافورة قوله أن "تهديدات الانترنت والقرصنة الماكرة المتبعة حاليا، تظ أن القرصنة يجعلون من جرائم الانترنت مهنتهم الفعلية.ويستخدمون أساليب شبيهة بالممارسات الخبيثة من أجل النجاح في تحقيق هدفهم"، وأضاف "هذه المواقع يمكن أن تكشف الكثير من المعلومات السرية الخاصة بالمستخدمين.ويمكن أن تستخدم هذه المعلومات بعد ذلك في محاولات لسرقة الهوية والاحتيال عبر الإنترنت أو السماح بالدخول على مواقع أخرى، حتى المهاجمون من خلالها مزيدا من الهجمات."

بدأت الصين الحرب الباردة على الانترنت بتوجيه ضربة لأكبر خمس دول متقدمة تكنولوجيا على مستوى العالم.وهي الولايات المتحدة الامريكية وفرنسا وانجلترا والمانيا وأخيرا روسيا.الامر الذي أكدته التقارير الصحفية بأن الصين تضع خطة لفرض " هيمنة إلكونية" على خصومها العالميين بحلول عام 2050.وذكرت صحيفة "التايمز "البريطانية عن مصادر في البنتاجون أن الصين تجهز لضربات معلوماتية تحسبا لهجوم عسكري أمريكي.وأن قراصنة

الكمبيوتر من الجيش الصيني وضعوا خطة لتعطيل أسطول حاملات طائرات أمريكية عن طريق هجوم معلوماتي.

وعلى عكس ما كان معروف قديما من أن الضربة الجوية تعد هي عنصر المبادرة في أي حرب،إلا أن اليوم ووفقا لما جاء في تقرير البنتاجون فإن الجيش الصيني يعتبر " الهجمات المعلوماتية" هي "وسيلة كسب المبادرة" في المراحل الاولى من أي حرب،حيث ترغب الصين في شل قدرات العدو المالية والعسكرية والاتصالية في المراحل المبكرة من النزاع.وأظهرت الصحيفة أن البنتاجون سجل أكثر من 79 الف محاولة قرصنة خلال عام 2005 نجح منها نحو1300 محاولة.يأتي ذلك بعد أن وجهت كل من المانيا والولايات المتحدة وبريطانيا أصابع الاتهام إلى الصين،بشن هجوم قراصنة على شبكاتهم الالكترونية لتحقيق أغراض عسكرية.فمنذ شهور قليلة تعرضت وزارة الدفاع الأمريكية" البتاجون" لهجوم كاسح للقراصنة"،حيث قام قراصنة بشن هجوم على ثلاثة عشر جهازا مركزيا يتحكم بتدفق المعلومات على شبكة الانترنت على مستوى العالم،وتمكنوا من تعطيل ثلاثة أجهزة والسيطرة عليها بشكل كامل طوال اثنتي عشر ساعة.في أكبر عملية تشهدها الشبكة منذ عام 2002.

القراصنة نجحوا في الشهور الماضية في اختراق شبكة وزارة الدفاع الأمريكية و البريطانية. وقد تركز الهجوم الذي تمكن الخبراء من مواكبته بشكل عاجل دون أن يشعر به معظم مستخدمي الانترنت على أجهزة شركة**Ultra DNS**،وهي الشركة التي تدير وتنظم جميع خطوط الشبكة التي تنتهي بالرمز"org." ووصف المراقبون الهجمة بأنها كانت "قوية بصورة غير اعتيادية"، غير أن خبراء المعلوماتية حول العالم نجحوا في احتواءها، بعدما بذلوا مجهودا كبيرا ليحافظوا على كفاءة بعض خطوط الشبكة الحيوية، التي أتخمت بفيض هائل من المعلومات،ونجح القراصنة في اختراق نظام البريد الإلكتروني غير السري لوزارة الدفاع مركزية" البتاجون"

وعشية زيارة المستشارة الالمانية "انجيلا ميركل" لبكين نهاية العام الماضي، قالت مجلة "دير شبيجل" الالمانية أن كمبيوترات مكتب المستشارة وثلاث وزارات أصيبت بـ"دودة" من نوع

" هـ ن طروادة" أو"تروجان".ولم يحدد المقال الجهة المسئولة أو مصدر الدودة.لكنها أشارت إلى أن الاستخبارات المحلية الالمانية تعتقد أن مجموعة مرتبطة بالجيش الصيني ربما تكون وراء الاختراق المزعوم.واكتمل الضلع الثالث في مثلث ضحايا حرب القرصنة بعد انضمام بريطانيا هي الاخرى إلى الولايات المتحدة وألمانيا بعد تعرض شبكات الكمبيوتر الخاصة بالحكومة البريطانية هي الاخرى لمثل هذه الهجمات.فقد نقلت صحيفة الجارديان البريطانية عن مسئولين بريطانيين قولهم أن القراصنة اخترقوا شبكة وزارة الخارجية وغيرها من الوزارات الكبرى.وأضاف المسئولون أن حادثا وقع العام الماضي وأدى إلى إغلاق جزء من نظام الحاسوب في مجلس العموم البريطاني.وتبين انه من عمل عصابة صينية منظمة من قراصنة الكمبيوتر.[1]

وبذلك يظهر أن جرائم الانترنت قد خرجت من يد الهواة و أصبحت تشكل خطة حرب تستلزم المواجهة الحقيقية بموجب قوانين صارمة و إجراءات محكمة و متطورة،و من أ جل ذلك سأتطرق في هذا المبحث للقوانين الداخلية التي سنت لمكافحة هذه الممارسات في المطلب ول،ثم سأعرج في المطلب الثاني لأتحدث عن إجراءات متابعة هذه الجرائم

المطلب الاول : القوانين المعاقبة على جرائم الانترنت.

لم تواكب التشريعات الداخلية تطور التقنية عموما.ولو كانت هناك بوادر لوضع بعض النصوص إلا أنها بقيت في الغالب محصورة في مجرد حماية لنظام المعالجة الآلية للمعطيات كمفهوم عام ولم تعالج الافعال المقترفة بشكل مفصل.و التي تتطور بشكل مذهل في الثانية الواحدة و كأنها مسابقة عالمية بين المخترقين و القراصنة حول من يبتكر أكثر جريمة انترنت تطورا و سرعة.وما ألحقته من خسائر حتى بالدول المتقدمة.ففي تقرير صادر من مكتب التحقيقات الفيدرالي "FBI" أن جرائم الكمبيوتر تكلف الاقتصاد الامريكي 67.2 مليار دولار

1: علي عبد القادر قهوجي.الحماية الجنائية لبرامج الحاسوب الآلي.الدار الجامعية للطباعة والنشر .بيروت. 2000 ص407.

سنويا وأيضا أن حوالي 64% من الشركات تعرضت لخسائر مالية بسبب حوادث اختراق أنظمة الكمبيوتر خلال العام الماضي.

و من أبرز الحوادث ما قام به " كيفن ميتيك" مع بداية ظهور الانترنت.فهو ما أن يضع يديه على لوحة المفاتيح الخاصة بالكمبيوتر حتى يجد نفسه مشدودا لتحطيم أي شبكة معلومات تقع في طريقه.أكثر من ثمانية عشر عاما وهو يصول ويجول.حيث اخترق شركة الهاتف البريطانية والشركات العالمية مثل موتورلا وأبل وغيرها.بل إنه أختر ق وزارة الدفاع الامريكية " البتاجون" وبرع في اقتحام المقاسم والحصول على مكالمات هاتفية مجانية، رغم القبض عليه وإيداعه السجن مرات عديدة.وهذا لدليل على عدم وجود قواعد ردعية تحكم اندفاعه هذا فبخروج جرائم الانترنت من عالم الهواة إلى عالم الجريمة المنظمة و الحرب البار دة لكرونية مازالت الدول و خاصة النامية منها في خطواتها الاولى لتعريف هذا النوع من الجرائم.وسن بعض القوانين المعاقبة رغم إدراكها لضرورة التصدي لهؤلاء المجرمين.و هو ماأدى بتكافل الجهود لسن قواعد عالمية ،تبعالدول خطاها لتجريم الممارسات اللاأ خلاقية عبر الانترنت و الماسة بأمن الافراد و الدول و بذلك سأتناول في الفرع الاول التشريعات الداخلية و في فرع ثاني سأتطرق للتعاون الدولي في مجال جرائم الانترنت.[1]

الفرع الاول: تشريعات لمكافحة جرائم الانترنت

تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الالي والانترنت، حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الالي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها.

[1]: أمال قادة ،المرجع السابق،ص 480.

وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصا بحماية أنظمة الحاسب الآلي (1976 م– 1985م).وفي عام (1985م)حدّد معهد العدالة القومي خمسة أنواع رئيسية للجرائم المعلوماتية وهي :جرائم الحاسب الآلي الداخلية،جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي،دعم التعاملات جرامية،وسرقة البرامج الجاهزة والمكونات المادية للحاسب.وفي عام (1986م) صدر تشريع يحمل الرقم (1213)،عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه،وعلى أثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي، فأقرتقانون مكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى.وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت،حيث عدلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت.كما شمل القانون الجديد تحديدعوبات المخالفات الحاسوبية،وجرائم التدمير،أو الدخول غير المشروع لأنظمة الحاسب الآلي.

وفي عام (1985م) سنت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت،والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها.[1]

1: أمال قادة ،المرجع السابق،ص 482

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم(88-19) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها.

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانة.

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها.وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الاكواد الخاصة بالبرامج.

و ينتظر أن يبدأ الكونجرس الاميركي قريبا في مناقشة تشريع جديد تقدم به النائب الجمهوري "جيمس سينسنبرينر"،من شأنه إدخال تغييرات جذرية على قواعد الخصوصية على الإنترنت. ويتيح القانون الجديد للحكومة الاميركية فرصة الحصول من موفري خدمات الإنترنت على سجلات كاملة بالأنشطة التي يقوم بها الاميركيون على الشركة الدولية.ويأتي المقترح الجديد بعد أسابيع قليلة من تصريح لوزير العدل الاميركي" البرتو جونزاليس "بأنه :يتعين على الشركات التي تقدم خدمات الانترنت داخل الولايات المتحدة البدء في تخزين سجلات بالأعمال التي يقوم بها مستخدمي الانترنت الأميركيين لفترات زمنية سماها "معقولة"،وهو تصريح اعتبره المراقبون تحولا جذريا من إدارة الرئيس "بوش" عن رؤيتها المعلنة سابقا عن قضية الخصوصية.و سيتم بمقتضى التشريع تخزين سجلات كاملة للأنشطة التي يقوم بها المستخدمون الاميركيون على الإنترنت وبموجبه، ستخضع اليوميات التي يكتبها المستخدمون على الإنترنت وأنشطتهم على محركات البحث على الشبكة الدولية ورسائل البريد الإلكتروني الخاص بهم لرقابة السلطات الاميركية.فتعتبر مخالفة جنائية كل " سيلاء" لأعمال غير مشروعة كالدعارة.

ويقترح النائب "سينسنبرينر"، وهو رئيس للجنة التشريع بمجلس النواب،أن يفرض على موفري خدمات الإنترنت في الولايات المتحدة تقديم سجلات تشتمل على معلومات خاصة بالأنشطة التي يقوم بها الاميركيون على الانترنت،بحيث تساعد الشرطة في "إجراء التحقيقات الجنائية"،ويقترح أيضا فرض غرامات على الشركات التي لا تلتزم بالتشريع الجديد وعقوبات بالسجن تصل إلى عشر سنوات وبالإضافة إلى هذا،سوف يعتبر تشريع "سينسنبرينر" الجديد،الذي ينتظر أن يكشف عنه قريبا،أية مخالفات تتم من خلال اليوميات التي تتم كتابتها على الإنترنت أو نشاط المستخدمين على محركات البحث ورسائل البريد الإلكتروني مخالفات جنائية يعاقب عليها القانون،بما فيها استخدام الاطفال في تجارة الدعارة غير المشروعة.

وكان الوزير الاميركي " جوزالس" قد حذر خلال خطاب له أمام المركز الوطني للأطفال المفقودين والمستغلين، من خطورة ترك الانترنت مفتوحة دون رقابة،داعيا إلى استحداث تشريع جديد من الكونجرس وقال:"تستخدم الانترنت على نطاق واسع في إرسال واستقبال أعداد هائلة من رسائل البريد الإلكتروني التي تحتوي على صور لأطفال يجري استغلالهم في الدعارة" وقد عارضت الإدارة الاميركية الحالية بشدة فرض أية قواعد على الشركات التي توفرخدمات الانترنت على الشبكة الدولية، معلنة"تحفظاتها الشديدة" على مثل هذه الاقتراحات،لكن إقرار البرلمان الاوروبي ،لتشريع مماثل يفرض على موفري الانترنت الأوروبيين تقديم سجلات بأنشطة المستخدمين على الانترنت،دفع أقطاب الإدارة الاميركية للحديث بحرية أكبر عن مثل هذا التشريع،ويأتي التشريع الجديد كجزء من محاولات الجمهوريين المستميتة لإرضاء مؤيديهم من المتشددين

وفي السعودية، أعلنت السلطات المختصة أنها ستفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال فيما يعادل 133ألف دولار لجرائم القرصنة المرتبطة بالانترنت و إساءة استخدام كاميرات الهواتف المحمولة ،مثل التقاط صور دون تصريح ،وأكد

بيان صادر عن الحكومة السعودية موافقتها على مشروع قانون بخصوص الجرائم المعلوماتية كان مجلس الشورى السعودي قد اقترحه العام الماضي،وبموجب مشروع القانون ،توقع العقوبة على الدخول غير المشروع إلى موقع الكتروني أو الدخول إلى موقع الكتروني لتغيير تصميم هذا الموقع أوإلغائه أوإتلافه أو تعديله .كما يجرم مشروعالقانون " المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف المحمولة المزودة بكاميرا أو ما في حكمها بقصد التشهير بالآخرين و إلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة."[1]

و قد صدر عن مجلس الوزراء السعودي مؤخرا القرار ذو الرقم (79) بتاريخ7 3 1428 هـ بالموافقة على نظام مكافحة جرائم المعلوماتية،ويعتبر هذا النظام دليلا على مواكبة المملكة للتطورات التقنية الحديثة ووضع أطر تنظيمية لمكافحة الاستخدامات السلبية والحد منها، حيث يعوّل على هذا النظام في سد الفراغ النظامي في هذا الجانب ،كما يعوّل عليه في نشر الاستخدامات الإيجابية التي أوجدت التقنية لأجلها،وقد استهل النظام بتعريف الالفاظ والعبارات الواردة والتي من أهمها معنى الجريمة المعلوماتية (وهي كل فعل يرتكب متضمنا استخدام الحاسب الالي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام)، و تتخذه الافعال أو الجرائم عدة أشكال منها:التشهير بالآخرين وإلحاق الضرر بهم،النصب والاحتيال نشر الإباحية و الرذيلة ،نشر الفيروسات ، المساس بالقيم الدينية ،وكذلك من الالفاظ المهمة التي عرفها النظام معنى الدخول غير المشروع (وهو دخول شخص بطريقة متعمدة إلى حاسب الي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات الية غير مصرح لذلك الشخص بالدخول إليها)،ويهدف النظام إلى الحد من وقوع جرائم المعلوماتية من خلال تحديد الجرائم والعقوبات المقرّرة لكل منها والتي يتحقق من خلالها :المساعدة على تحقيق الأمن المعلوملي،حفظ الحقوق المترتبة على الاستخدام للحاسبات الالية والشبكات المعلوماتية،حماية المصلحة العامة والاخلاق والاداب العامة،حماية الاقتصاد الوطني.

1: علي عبد القادر قهوجي،المرجع السابق،ص 349.

كما بيّن النظام في مواده من الثالثة وحتى المادة العاشرة العقوبات المقرّرة للجرائم المعلوماتية،حيث حدّد لكل جريمة عقوبة معينة بداية من العقوبة بسجن لمدة لا تزيد على سنة وغرامة لا تزيد على خمسمائة الف ريال أو بإحدى هاتين العقوبتين،وانتهاء بعقوبة بالسجن لمدة لا تزيد على عشر سنوات وغرامة لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين .علما بأن قرار سمو وزير الداخلية رقم (1900) الصادر مؤخرا بتاريخ 9 7 1428هـ والذي حدّد الجرائم الكبيرة الموجبة للتوقيف جعل من ضمن الجرائم الكبيرة (انتهاك الاعراض بالتصوير والنشر والتهديد بالنشر) وهي تعد من الجرائم المعلوماتية الواردة بالمادة الثالثة من النظام فقرة (4 5) ومانصها: (4- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقّالة المزوّدة بالكاميرا،أو ما في حكمها. 5- التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة).والمعاقب على ارتكاب هذه الجرائم بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة الف ريال أو بإحدى هاتين العقوبتين.

كما أسند النظام لهيئة الاتصالات وتقنية المعلومات وفقا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الامنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناءالمحاكمة،وكذلك أسند التحقيق والادعاء العام في هذه الجرائم لهيئة التحقيق والادعاء العام.إلا أنه وجه لهذا النظام بعض الانتقادات من قِبل بعض المختصين منها أنه نظام عقوبات فقط ولم يتطرق إلى مكافحة جرائم المعلومات كما هو واضح بعنوانه، وكذلكانتقد بانه لم يفرّق بين كبار السن والاحداث الذين يعدون شريحة كبيرة من المستخدمين لهذه التقنية،كما انتقد بانه لم يحدد مرجعية واضحة لهذا النظام.[1]

ويرى بعض الفقه انه لا بد من أمرين:

1) ضرورة إصدار لائحة تنفيذية لهذا النظام تبيّن الية تطبيق هذا النظام للجهات المختصة والية تعاون هيئة الاتصالات وتقنية المعلومات مع الجهات الأمنية وهيئة التحقيق والادعاء العام نظرا لأن الجرائم المعلوماتية جديدة على المجتمع وكذلك تحديد الجهة القضائية في

1: عبد القادر قهوجي،المرجع السابق،ص350.

نظر هذه الجرائم.فالنظام لم يحدّد المحكمة المختصة في ذلك وأما بالنسبة لعدم تطرق النظام للتفرقة بين كبار السن والاحداث فيفسر ذلك بأن القاعدة العامة أن الاحداث لا يخضعون للنظام ولا يطبق عليهم أنظمة العقوبات بشكل عام وفقا للمادة (13) من نظام جزائية والتي تنص على أنه (يتم التحقيق مع الأحداث والفتيات ومحاكمتهم وفقا للأنظمة واللوائح المنظمة لذلك) وإنما يتم تعزيرهم من قِبل قاضي محكمة الأحداث حسب ما يراه ويقدّره ولذلك لم يتطرق النظام للأحداث.

2) ضرورة إنشاء وحدة لمكافحة جرائم المعلومات مدعمة بالإمكانيات المادية والبشرية المؤهلة ،دورها الآتي:

أ. توعية المواطنين وتبصيرهم على هذه الجرائم وبيان أضرارها الدينية والامنية والاجتماعية والاقتصادية وغيرها والعقوبات المقرّرة عليها والحث على الاستخدامات الإيجابية للتقنية.

ب.القيام باستقبال الشكاوى من داخل المملكة وخارجها حول هذه الجرائم ودراستها ومن ثم إرسالها لجهة التحقيق المختصة لإكمال ما يلزم حيالها.

ج.تكون حلقة الوصل بين الجهات الامنية المختصة بداخل المملكة وخارجها فيما يتعلق بهذه الجرائم وكذلك صلاحية الاتصال بالشرطة الدولية.

و كما سبق ذكره فان المشرع الجزائري قد جرم الافعال الماسة بنظام المعالجة الالية للمعطيات وأما سميت بالغش المعلوماتي.بموجب القسم السابع مكرر من قانون العقوبات المعدل بالقانون 23/06 المؤرخ في 06/12/20 في المواد من 394 مكرر الى 394 مكرر7،فقد عاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 دج إلى 200000 دج وتطبق العقوبات ذاتها على المحاولة.و تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة،أما إذا ترتب عنها تخريب نظام إشتغال المنظومة تكون العقوبة من ستة أشهر إلى سنتين حبس و الغرامة من 50000 دج إلى 300000دج.[1] .و تعاقب المادة 394مكرر 1 على

1: أحسن بوسقيعة، المرجع السابق ص270.

ا ـلمـ ـان بمنظومة معلوماتية بالحبس من ستة أ شرإلى ثلاث سنوات و بغرامة من 500000دج إلى 4000000 دج

في حين نصت المادة 394مكرر 2 على عقوبة الحبس من شهرين إلى ثلاثة سنوات وبغرامة من مليون إلى عشرة ملايين دج لىمن يقوم عمدا و بطريق الغش بتصميم أ وبحث أ و تجميعأو توفير .نشر ، تجار في معطيات مخزنة أو معالجة أ ومرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى الجرائم المذكورة أعلاه،و قد عاقب المشرع الجزائري الشخص المعنوى بموجب المادة394 مكرر4 بغرامة تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي عند ارتكابه للأفعال المجرمة بهذا القانون.و قد تضمنت المادة 394مكرر3 مضاعفة العقوبة المقررة لجرائم الغش المعلوماتي،إذا ـلـدفت الجريمة الدفاع الوطني أ واليـ ئلتوالمؤسسات الخاضعة للقانون العام.أ ماإ ذاتمت الجريمة في شكل تجمع غرض ٌعداد للجريمة المعلوماتية و تجسد ذلك في فعل مادي أ وأكثر معاقب عليه بعقوبة الجريمة ذاتها.و أقر في المادة 394مكرر6 بـمـلـدر ةٌجهزة و البرامج و الوسائل المستخدمةمع إغلاق المواقع التي تكون محلا لجريمة من جرائم الغش المعلوماتي،علاوة على إغلاق المحل أو مكان ـ ستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها و رغم وجود هذه النصوص فإنها لم تضع حد للأفعال المجرمة.(1)

كماأن رجال العدالة نفسهم مازالوا لم يتعوّدوا على تطبيق مثل هذه النصوص رغم أنهم أ ـل المطالبين بتفعيلها إلى جانب رجال الا منلإ ـطاأكثر صدى و فاعلية.و رغم ندرة القضايا المعروضة على قضاتنا في هذا المجال فإنهم يتعاملون معها من زاوية الجريمة التقليدية و لا يسقطون عليها النصوص المستجدة ولا يعطونها تكييف الجريمة المعلوماتية و مثـ الـذلك:ما جرى بجلسة لمحكمة الجنايات المنعقدة بمجلس قضاء بجاية التي تعلقت بقضية تزوير عملة وطنية،أ ين استعمل الجاني عدة أجهزة إ علامألي و سكنار و ـ لات ـلـتساخ و التي وضعت أمام هيئة المحكمة كـدٔلـ ةإقناع،و الغريب في الا مرأ نالرئيس لم يـ ركز

1: أ حسن بوسقيعة،المرجع السابق،ص 271

بشكل أساسي على هذه الاجهزة في مواجهة المتهم و لم يتم تشغيلها لتحليل ما تضمنته من بيانات ورسومات،و البرنامج المعتمد لصنع الأوراق النقدية المزورة ذات السعر ألف دينار و خمسمائة دينارجزائري،و في المقابل نجد أن النيابة قد ركزت في دفاعها على هذ الامر و استندت إلى محاضر الدرك الذين كانوا أكثر دقة و يبدوا أنهم أكثر استوعابا لدور المعالجة لية للبيانات،في اقتراف مثل هذه الجرائم.فقد بينوا أ ولاأن هذه الا جزة وجدت في غرفة نوم المتهم الرئيسي بي البالغ من العمر الثالثة و العشرون سنة.الميسور الحال و المتفوق جدا في استعمال الإ علام الالي ،وإنهم قاموا بتفتيش محتويات الا ربعأجهزة كمبيوتر المحجوزة و وجدو أن من بينها واحد مخزن فيه نماذج لأوراق نقدية ذات السعر القانوني ألف دينار جزائري،و التي تبين أنها مطابقة للأوراق المزورة التي ضبطت لدى باقي المتهمين ولقد أوضح ا لمحضرأن الجهاز المعني هو الجهاز الشخصي المحمول للمتهم الرئيسي.الذي انتهت محكمة الجنايات بإدانته بالجرم المنسوب إليه و عقابه بثلاثة سنوات سجن موقوفة النفاذ .[1]

و حرصا من المشرع الجزائري على محاصرة هذه ارائم،قد أعلن البرلمان الجزائري يوم 14 نوفم من ا لسنةالماضية،وضع قانون لمكافحة الجريمة السايبرية،ويهدف الإجراء إلى التصدي لهجمات كهذه من خلال استراتيجيات الرصد والمنع حسبما قاله وزير البريد وتقنيات الاتصال حميد بصلاح .فقد شكل وزير العدل الجزائري يوم الاربعاء 29 مارس من نفس ا لسنةمجموعة عمل مكلفة بصياغة قانون "منسجم"، بخصوص جرائم الانترنت،و تدخل الخطوة في إطار إصلاح القطاع الذي بدأ قبل ست سنوات.

وحسب الكاتب العام لوزارة العدل "عبد السلام الديب" فإن المجموعة مكلفة بوضع آليةمن شأنها تعزيز الإطار القانوني للجرائم المتصلة بتكنولوجيا المعلومات،وتتكون المجموعة من خبراء عن وزارة البريد وتكنولوجيا الإعلام والاتصال ووزارة العدل ووزارة الداخلية و المديرةالعامة للأمن الوطني والدرك الوطني،والذي سيكشف عن مسودته قريبا حسب تصريح بلابد يوم 10 أفريل في منتدى بالجزائر العاصمة وما أفادت به صحيفة ا لشرق يوم

1: أ حسنبوسقيعة،المرجع السابق،ص 271.

الست16 فاير من السنة الجارية.ونقلت الصحيفة عن " نوا رحزالله" المدير العام لشركات الانترنت الخاصة (إيباد) قوله إن ممثلي عدد من الوزارات وخبراء خدمات الامن قد قامت بوضع القانون بغية خلق الادوات المخصصة لمحاربة جرائم الانترنت بما فيها اختراق احواسيب والتحويل غير القانوني للأموال وترويج الإباحية والفساد وسرقة الملكية الفكرية.مقترح القانون الجديد سيفرض جزاءات تتراوح بين الغرامات المالية والسجن مدى الحياة .

وترى ا لمحامية"فاطمة بن إبراهيم" بأن القانون لا يكفي "إن لم يكن عديم الجدوى" و أن "مجرمي الحواسيب يستغلون الفراغ القانوني القائم في هذا ا لمجال ليعملوا بالا على حريتهم،"مو ـ ة: "على الجزائر سن قانون خاص بجميع أشكال جرائم الحاسوب [لكن] اعتماد قانون كهذا سيكون عديم الفائدة في غياب حملة وطنية في زمن العولمة. فمكافحة الجرائم الحاسوبية تستدعي التنسيق الإقليمي فليس بمقدور أي بلد مهما كانت قوانينه.معالجة هذه الجريمة بالقدرات الذاتية.[1]

وذكرت جريدة " الخبر "الجزائرية على موقعها في شبكة الإنترنت يوم الثلاثاء 30 نوفمبر 2008،أن مشروع القانون يعاقب على اختراق وتخريب المواقع الإلكترونية والحواسيب وسرقة المعلومات المحمية وأرقام البطاقات الائتمانية وإنشاء وارتياد المواقع التي تروج لإرهاب .مشيرة إلى أن مشروع القانون سيعرض قبل نهاية العام الجاري.وأوضحت مصادر صحفية جزائرية أن المشروع يأخذ بتجارب وتشريعات دول غربية أخرى وسترافقه حملة توعية واسعة للتعريف به.مؤكدة أن التفكير في وضع القانون الجديد جاء بعد تزايد عدد الجرائم الإلكترونية في الآونة الاخيرة وخاصة ضدّ مؤسسات حكومية ". و أضافت المصدرقائلة: " إن العقوبات التي يتضمنها مشروع القانون الجديد تتراوح بين الحبس أو الغرامة المالية أو كلهما معا مع مصادرة الوسائل المستخدمة في الجريمة".

1: مدحت رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهظة العربية، ص 504.

وحتى في غياب سياسة إقليمية يرى العديد من الجزائريين في مشروع القانون خطوة محمودة.م لا"مراد" يهو صاحب مقهى بمنطقة برج البحري،كند مخاوفه من إ زد يا شعبية مواقع الإسلاميين الداعية للجهاد المسلح بين الشباب خاصة اليافعين.قال موضحا " ا لشب ل اليافعون يدخلون هذه المواقع بدافع الفضول وليس بمقدورنا منعهم والبعض منهم ينزّل محتوياتها على أقراص مضغوطة ثم يطالعونها مع أصدقائهم".ويعتقد أن قانون الجرائم الحاسوبية سيساعد في الحدّ من المشكلة التي يراها يو ميا وأ ملأن ينجح الفريق العامل لصياغة القانون الجديد في القضاء على مرتكبي الجرائم الحاسوبية بمن فيهم الإرهابيين الذين ستغل ون للو اق عالكترونية لإغراء الشباب.في حين أ ن" م وان عزي" رئيس الفريق المسؤول عن تطبيق القوانين المتعلقة بمبادرة المصالحة الوطنية يتفق على أن ثمّة فراغا قانونيا في الجزائر حول مسألة الجريمة الحاسوبية.إذ يرى أن صعود ظاهرة الإرهاب هي التي دفعت السلطات الجزائرية إلى الانتباه لهذه الجرائم.[1]

الفرع الثاني :الاتفاقيات الدولية.

نظرا لتميز جرائم الانترنت بالعالمية باعتبارها جرائم عابرة لقارات.فلابد من صدور قوانين دولية وتكاتف الجهود لإتخاذ تدابير فعّالة للحدّ و القضاء عليها ومعاقبة مرتكبها .فرغم وجود بعض الاتفاقيات المقررة لمكافحة الجريمة بصورة عامة خاصة المنظمة و العابرة للحدود و التي تنطبق تماما و مواصفات جرائم الانترنت .فقد وجدت معاهدات سنت خصيصا لمكافحة جرائم الكمبيوتر و الانترنت.

أولا: معاهدات لمكافحة الجريمة عموما

حددت جملة من تدابير مكافحة الجرائم المتصلة بالحواسيب في إطار مؤتمر الا مم الحادي عشر لمنع الجريمة والعدالة الجنائية المنعقد في بانكوك في الفترة 18 25 / 2005/4 و

[1]: حسن بوسقيعة.المرجع السابق.ص 271.

الذي جاء من بين صفحاته ضرورة التعاون الدولي على المستوى القضائي لتخطي حدود الدولة الواحدة للتحقيق في الجريمة ،و يمكن الاعتماد في مجال جرائم الانترنت على اختصاصات المنظمة الدولية للشرطة الجزائية (interpol) ،المنشأة بموجب المؤتمر الدولي المنعقد في بروكسل في الفترة من 6 1946/6/9 و الذي يقوم على مبادئ التعاون مي الدولي،بالنسبة ل 182 دولة عضو،لتقفي أ ثرالمجرمين ومتابعة الجريمة .ومن الامثلة على دور انتربول في جرائم الانترنت ما حصل في لبنان عندما تم توقيف أحد الطلبة الجامعيين ، من قبل القضاء اللبناني بتهمة إرسال صور إ باحية لفتيات قصر دون العاشرة من عمرها من موقعه على الشبكة. وذ لك أثر تلقي برقية من الانتربول في ألمانيا بهذا الخصوص و للمنظمة عدة مكاتب مركزية إقليمية في كل من: طوكيو ، نيوزيلندا، نيروبي ، اذربجان ، بيونس ايرس، لتسهيل مرور الرسائل.[1]

و بانعقاد المجلس الاروبي في لكسمبورج عام1991،أنشات الشرطة الاوروبية لملاحقة جناة الجرائم العابرة للحدود و في نفس السياق أقام مجلس الوزراء العرب مكتب عربي للشرطة الجنائية يهدف لتنمية التعاون بين الشرطة العربية ،و بعد إجراء تسليم المجرمين من أهم الإجراءات يدخل من جهة ضمن التعاون الدولي ومن جهة ساهم كثيرا في متابعة جناة جرائم المعلوماتية، والذي كان موضوع اتفاقيات دولية و إقليمية مثل اتفاقية الرياض لتعاون دول الخليج 1994 ،اتفاقية التعاون الامني و تسليم المجرمين للمملكة العربية السعودية 1982 ، اتفاقية بين الجزائر و بلجيكا سنة1970 و تفاقية اوروبية لتسليم المجرمين 1957.

ثانيا:الاتفاقيات الخاصة بمكافحة جرائم الانترنت

و لقد جاء في الاتفاقية اوربية للجرائم المعلوماتية الموقعة بتكليف من المجلس الاوربي،و التي أ برمت لمساعدة الدول في مكافحة جرائم الانترنت.في مادتها 24 جملة من

1: مدحت رمضان، المرجع السابق ص504

فعال التي يمكن أن يطبق بشأنها أسلوب تسليم المجرمين منها : الدخول غير المشروع،الاعتراض غير المشروع،جرائم الإباحية و صور الا طفال الـ ـاة.

كما تضمنت الاتفاقية جانب أخر من التعاون انصب هذه المرة حول تدريب أ عـ ل من،لإكسابهم خبرات عملية مثل ما ورد في التوصية الصادرة عن اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم المعلوماتية بدول مجلس التعاون الخليجي .وما نص عليه البند "د" من القرار الصادر بشأن الجرائم ذات الصلة بالحاسب الآلي نمؤتمر ٔمم المتحدة لمنع الجريمة و معاملة السجناء هافا نا1990،و قد اشترط في المتدرب خبرة لا تقل عن خمس سنوات في مجال تكنولوجيا المعلومات و إدارة ا لشبات حتى يتمكن من تلقي تدريب متخصص، وهي عملية شملت الكثير من الاجهزة الامنية عبر العالم مثل كندا ،و الجزائر التي أعدت برنامج لمدارس الأمن و الدرك الوطني و أرسلت قضاة للتدريب في الولايات المتحدة الامريكية.

و تعد الولايات المتحدة الأمريكية ،من الدول المتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية و الشبكات،وهي تساعد على تدريب أجهزة الشرطة و قضاة الدول الاخرى،بتمكينها من تعزيز قدراتها على ضـ ـطمشاكل الجرائم الإلكترونية قبل أن تفلت منها زمام الامور فقد أوجدت وزارة العدل الامريكية مكتب للمساعدة و التدريب لتطوير أجهزة الإدعاء العام في الدول الا خرى،وعـمل إلى جانبه البرنامج الدولي للمساعدة و التدريب (ICITAP) لتوفير ا لمـ اعـ ك لأجزة ا لشرطةبالـ ل النامية.

ورغم وجود بعض العقبات التي تعرقل التعاون الدولي ،مثل عدم وجود نموذج موحد للنشاط جرامي فـ يجبإ يجـ لتشريعات داخلية تقرب وجهات النظر، حيأخذ التعاون مجراه مثل قانون حماية الملكية الفكريـة .و الإجراءات الجزائية ،التشفير...و تساهم تفاقيات و الصكوك الصادرة عن منظمة الامم المتحدة كثيرا في استخدام تقنيات خاصة للتخفيف من شدة اختلاف النظر القانونية مثل التسليم المراقب ،المراقبة الالكترونية ،غيرها نأشكال المراقبة وهو ما أخذت به الجزائر في تعديلها لقانون جراءات الجزائية.

و قدتناولت الاتفاقية الاوروبية للإجرام المعلوماتي في مادتها 29 على سرية حفظ البيانات المعلوماتية المخزنة.و حق كل طرف أن يطلب من الا خرالحفظ السريع للمعلومات المخزنة، عن طريق إحدى الوسائل الالكترونية الموجودة داخل النطاق المكاني للطرف الخر و التي ستكون محلالطلب المساعدة من الطرف الاول بغرض التفتيش أو الدخول ،ضبط أو الكشف على البيانات المشار إليها.وهو الطلب الذي يجب الاستجابة إليه طبقا للمادة 30 من تفاقية.وعلى المعني تقديم المساعدة للطالب على وجه السرعة للكشف عن هوية مؤدي الخدمة و مصدر الاتصال و قد أجازتاتفاقية المساعدة للدخول للبيانات المحفوظة طبقا للمادة31 منها ،و سمحت المادة 32 من الاتفاقية بالدخول للبيانات المخزنة خارج نطاق الحدود بشرط وجود اتفاقيات أوأنها بيانات متاحة للجمهور.

وأقرت المادة 33 وجوب تعاون الدول الاطراف في حالة التجارة غير المشروعة ،و ركزت الاتفاقية في المادة 34 على البيانات المتداولة بالاتصالات عبر الشبكة و قد دعت الاتفاقية الدول عضاء لإنشاء نقطة اتصال تعمل لمدة 24 ساعةلتأمين المساعدة المباشرة للتحقيقات و استقبال الادلة ذات الشكل الالكتروني. و تثور مسألة الاختصاص في جرائم نترنت و التي تبقى رهينة إبرام اتفاقيات توحد نظريات الاختصاص و تتبنى نفس جراءات لحل هذا مشكل ،و مواكبة الجريمة التي تسابق الريح.ولقد سمحت الاتفاقية للطرف في الحالات الطارئة طلب المساعدة القضائية الدولية عملا بالمادة 25 منها.عن طريق وسائل الاتصال السريعة " فاكس ، بريد الكتروني..." و الذي يتلقى الرد بنفس الطريقة

ثالثا:اتفاقية بودابست لمكافحة جرائم الانترنت2001

ومواكبةلتطورفقدأبرمالمجلس وربي اتفاقية ببوداست في 2001/11/8 و وضعت للمصادقة في 2001/11/23 ،و التي تضمنت التعريف بأهدافها و وضعت قائمة للجرائم التي يجب على الدول المصادقة عليها أن تجرمها في قوانينها الداخلية ،و التي وقعت عليها 30 دولة. و تعد الاولى في مجال مكافحة جرائم الانترنت و شملت العديد من جرائم الانترنت منها:الإرهاب

، تزوير بطاقات الائتمان ، دعارة طفال و تعمد الاتفا قيةإلى تنسيق القوانين الجديدة في دول عديدة .وجاءت نتيجة مشاورات طويلة بين الحكومات و أجزة الشرطة و قطاع الكمبيوتر، و صاغ نصها عدد من الخبراء في مجلس أوربا بمساعدة عدة دول منها الولايات المتحدة.

وتحدد الاتفاقية أفضل الطرق الواجب اتباعها للتحقيق في جرائم الانترنت .التي تعهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها.و تحاول الاتفاقية الموازنة بين جهات المتابعة و صلاحياتها و بين احترام حقوق الإنسان و مصلحة مستخدمي ومزودي الخدمة، و تغشى البنوكمن تطبيق الاتفاقية الذي ستؤدي لإ ذ اعةعيوبها منية على الملأ، بينما يخشى مزودي الخدمة على أنيحملهم ذلك تكاليف باظة في سبيل تخزين البيانات لاستعمالها مستقبلا في جمع ثباتات في حالة المتابعة.

المطلب الثاني: متابعة جرائم الانترنت

على الرغم من وجود تشابه كبير بين التحقيق في جرائم الانترنت وبين التحقيق في الجرائم الاخرى فهي جميعا تحتاج إلى إجراءات تتشابه في عمومها ،مثل المعاينة والتفتيش والمراقبة والتحريات والاستجواب بالإضافة إلى جمع الادلة، كما أنها تشترك في كونها تسعى إلى الإجابة على الاسئلة المشهورة لدى المحقق،ماذا حدث ؟وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟. تظل الجرائم المتعلقة بشبكة الانترنت تمتاز عن غيرها من الجرائم ببعض الخصائص،وهذا بالطبع يستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية،وتمكن المحقق من كشف الجريمة والتعرف على مرتكبها بالسرعة والدقة اللازمين، فالتحقيق في هذا النوع من الجرائم يستدعي الرجوع إلى عدد كبير من السجلات التي يجب الإطلاع عليها مثل الكتيبات الخاصة بأجهزة الحاسب الآلي،ملفات تسجيل العمليات الحاسوبية،بالإضافة إلى الإطلاع على كم كبير من السجلات عن خلفية المنظمة وموظفيها، كما يتم في الكثير من مراحله في بيئة رقمية، منخلال التعامل مع الحواسيب والشبكات ووسا ط

التخزين ووسائل الاتصال.وسوف أتناول في هذا المطلب بعض جراءات المتبعة و المستجدة لمتابعة جرائم الانترنت.

الفرع ول:إجراءات متابعة جرائم الانترنت

يجب الحديث عن المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المتعلقة بشبكة الانترنت ، الذي ينصب على تلك المهارات التي تتسم بالجدة والحداثة وتعتبر إفرازا للتطور الإنساني في مجال تقنية الاتصالات والحوسبة وأمرا مطلوب في من يتعامل مع هذه الجرائم المستحدثة و:

1. **التعرف على المكونات المادية للحاسب الالي والتعامل المبدئي معها:** المهم هنا أن يتمكن المحقق من معرفة الشكل المميز للحواسيب وملحقاتها ومسميات كل منها، والهدف من استخدامه وما هي احتمالات توظيفه لارتكاب أي من الجرائم الانترنتية.خاصة وسائط التخزين بصفتها أدلة محتملة. واكتساب هذه المهارة يعد أحد الاهداف المرجوة من البرامج التدريبية الخاصة بالتحقيق في الجرائم الحاسوبية لدى العديد من الدول كالولايات المتحدة وكندا واستراليا .وما تسعى الجزائر لتحقيقه في مدارس الأمن و الدفاع الوطني.

2. **معرفة اساسيات عمل شبكات الحاسب الالي واهم مصطلحاتها :** إن المحقق بحاجة إلى معرفة مبادئ الاتصال الشبكي وأنواعه المختلفة. وكيفية انتقال البيانات من جهاز إلى اخر على شكل حزم، ومبادئ البرتوكولات الرئيسية الخاصة بالاتصال بالشبكة .مما يسمح له تصور كيفية ارتكاب الفعل الإجرامي في الفضاء السيبراني و مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات الفنية التي تحول دون ذلك.

3. **تمييز انظمة تشغيل الحاسوب المختلفة والتعامل المبدئي معها:** يجب أن يكون لدى المحقق على الاقل فهم مبدئي بانواع الانظمة التشغيلية لأجهزة الحاسب الالي ،وخصائص ومميزات كل نظام وأبجديات أنظمة الملفات التي يعتمد عليها .و ذلك لمشاركته في متابعة

وفحص وتفتيش مسرح الجريمة.و حتى يتخذ القرار المناسب مع الخبير بشان أي مسالة فنية،وبدون توافر الحد الادنى من المعرفة فان القرار على الارجح سوف يكون للخبير وحده

4. التعرف على الصيغ المختلفة للملفات وتطبيقات الحاسوب الرئيسية التي نتعامل معها: كالملفات الوعاء الحقيقي لأدلة الإدانة في الكثير من القضايا،المتعلقة بشبكة الانترنت ،بما تحويه من معلومات.

5. **إجادة التعامل مع خدمات الإنترنت:** يدور في مجتمع الانترنت الكثير من الحديث الذي قد يفيد المحقق،في توضيح غموض بعض الجرائم،و الذي يستخدم كأداة تعليمية للإطلاع على مستجدات الجرائم وطرق ارتكابها،وكوسيلة اتصال وتبادل المعلومات فيما بين رجال القانون.

6. **معرفة الادوات والاساليب المستخدمة في ارتكاب جرائم الإنترنت:** معرفة رجال العدالة باستخدام هذه الادوات أمر في غاية الاهمية، خاصة عند مناقشة الشهود واستجواب المتهمين فبدونه لن يستطيعوا طرح الأسئلة التي تتصل مباشرة بالفعل الإجرامي وأسلوب ارتكابه، كما انها تساعد المحقق على التواصل مع خبير الحاسوب الجنائي عند شرح تقريره.

7. **معرفة اهم تقنيات امن الحاسوب والانترنت وادواتها وطريقة عملها:** لمجرد استيعابها وليس التخصص فيها،فيكفي أن يتمكن المحقق من فهم أسلوب الأمن ومنه كيفية اختراقه.

8. **الإطلاع على بعض الجوانب المتعلقة بجرائم الانترنت:** يغلب عليها الطابع النظري فيمكن اكتسابها بالإطلاع على المطبوعات أو الانترنت، ومن أهمها :الواقع الحالي والاتجاهات المستقبلية لجرائم الإنترنت،الفئات المختلفة لمرتكبي هذه الجرائم ،والخصائص المشتركة بينها، معرفة وفهم التشريعات المختلفة لهذه الجرائم والإلمام باتجاهات القوانين والتشريعات في البلدان المختلفة،تحليل بعض القضايا المشهورة للاستفادة من تجارب رجال العدالة في مواجهة هذه الجرائم،الوقوف على الابعاد الدولية لهذه الجرائم واليات التعاون المشترك بين الدول والتعرف على الاتفاقيات والمعاهدات الموجودة بهذا الخصوص ، معرفة مصادر

المعلومات المتوفرة على الشبكة حول هذه الجرائم عبر المواقع المتخصصة ذات المحتوى الجيد و الموثوقية ومستفادة ما.

9. معرفة جرائم الانترنت وخصائصها:يعتبر هذا بمثابة حجر الاساس في نجاح المحقق أو القاضي في مواجهة هذه الجرائم: و عند تقديم بلاغ أو شكوى بالجريمة لابد أن يوجد قل تواصل بين الشاكي و المتلقي بشان المعلومات محل التبليغ.و التي تتباين بتباين فئات جرائم الحاسب الآلي والانترنت والطبيعة الفنية التي تتميز بها كل فئة .ويمكن الحصول عليها عن طريق طرح أسئلة حول : المعلومات الخاصة بالمبلغ .طبيعة ونوع جريمة الحاسب الالي محل البلاغ،الاسئلة الستة المشهورة والمتعلقة بالجريمة ماذا؟ وأين؟ ومتى؟ وكيف؟ومن؟ ولماذا؟المعلومات ذات العلاقة بالأنظمة الحاسوبية،مثل طبيعة العتاد ونوعية المجيات، والمسئولين عن الانظمة وطريقة الاتصال بهم وغيرها،لأن دقة وتكامل المعلومات على البلاغ على درجة كبيرة فهي تساهم في مساعدة المحقق على تحديد ما إذا كان السلوك محل البلاغ مجرم يندرج ضمن جرائم الإنترنت .ووضع تصور مبدئي عن خطة العمل المناسبة للتحقيق في الحادث بالإضافة لتحديد نوع الخبرة الفنية التي يحتاجها في المعاينة ورفع وتحريز الادلة من موقع الحادث،و سرعة استدعاء الخبراء القادرين على إنجاز ذلك.

وقبل إنهاء البلاغ يجب التاكيد على المبلغ بضرورة القيام بتجهيز قائمة بأسماء العاملين في المؤسسة،ممن لهم علاقة بالأجهزة المتضررة،تجهيز النسخ الاحتياطية من بيانات الاجهزة المتضررة لفحصها من قبل فريق التحقيق فور وصوله الموقع.و التاكيد على عدم الإعلام بالحادث إلا لمن لزم الامر.

بعد الانتهاء من جمع المعلومات اللازمة عن الحادث، يبدأ المحقق تحديد خطة العمل المناسبة وفريق العمل اللازم للتحري،وهذا بمجرد انتهائه من معاينة موقع الحادث ورسمه الصورة الاولية للواقعة فيقوم بالتخطيط على ثلاث مستويات مختلفة .يبنى كل مستوى منها على الاخر:

1. **تخطيط استراتيجي:** وهو تخطيط بعيد المدى يهتم بحماية البنية التحتية لشبكات الحاسوب الوطنية.من خلال تحديد مصادر الخطر المحتملة التي قد تمثل تهديدا لها ،ويضع تصورات على درجة من المرونة تكون كفيلة بالتصدي لهذا النوع من الجرائم قبل وقوعها وضبطها والحد من اثارها ، ويتم هذا التخطيط على مستوى واضعي السياسات الامنية، حيث يهدف بشكل عام إلى منع وقوع هذه الجريمة داخل إقليم الدولة، والحد من قابلية الشبكات الوطنية للتعرض لها، ومن ثم السيطرة على الحوادث إن وقعت وضبطها والحد من اثارها، ما يميز هذا التخطيط انه يضع الخطوط الاسترشادية للجهات المكافحة لهذا النوع من الجرائم، كما يحدد الاليات اللازمة لتنفيذ الخطة.
2. **تخطيط تكتيي:** ينبثق من الخطة الإستراتجية و يدعمها ويتم على مستوى الجهات الرسمية والغير رسمية التي لها علاقة بتقنية المعلومات للتعامل مع جرائم الحاسوب والانترنت، ويمتاز بطابع تفصيلي.وخطط تكتيكية خاصة بالتعامل مع جرائم الانترنت، تتضمن إجراءات مسبقة التحديد على درجة عالية من التفصيل والوضوح للتحقيق في هذه الجرائم.
3. **خطة عمل:** هو التخطيط الذي يقوم به المحقق لتحديد الاسلوب الامثل في التعامل مع حادث بعينه، في الإطار العام لإجراءات الخطة التكتيكية،وبما يتناسب مع خصوصية ظروف وملابسات الحادث.

على المحقق اخذ بالاعتبار حجم ونوع الحادث لتعيين فريق التحقيق و كفائته ، الظروف المحيطة بالحادث، لتعلقها بقرارات على درجة كبيرة من الاهمية في التحقيق، ومنها : أمية الاجهزة الحاسوبية والشبكات المتضررة لعمل المنظمة أو المؤسسة.حساسية البيانات التي قد تكون محل الجريمة الحاسوبية،المتهمون المحتملون،اطلاع الرأي العام على الجريمة أم لا.مستوى الاختراق الامني الذي تسبب فيه الجاني .ومستوى المهارة الفنية التي يتمتع بها.

هناك محققون جنائيون ذوو خبرة طويلة، وهناك أخصائيون في الحاسب الآلي و الشبكات ذو معرفة واسعة، ولكنه من النادر أن يوجد شخص واحد يمتلك مهارات عالية في الاثنين معا، ولذلك يستعين المحقق بخبراء في هذا المجال بحسب كل قضية وملابساتها، كما يمكن الاستعانة ببعض خبراء مسرح الجريمة التقليدية.مثل خبير البصمات وخبير التصوير وعلى هذا الاساس يمكن تقسيم فريق التحقيق في هذا النوع من الجرائم إلى فئتين هما:

الفئة الاولى تضم:

1) **قائد الفريق**: صاحب خبرة طويلة في مجال التحقيق الجنائي، و معرفة خاصة بجرائم الحاسب الآلي والانترنت يتولى السيطرة الكاملة على مسرح الجريمة، وتوزيع المهام على الفريق والإشراف على قيامهم بأعمالهم، والتنسيق مع الجهات ذات العلاقة، واتخاذ كافة القرارات المتصلة بالتحقيق.

2) **محققجنائي**: و احداً وأكثر،لديه خبرة بالتحقيق وإجراءاته،مع إلمامه بطبيعة الجريمة وكيفية التعامل مع الادلة الرقمية فيتولى البحث عن الأدلة وتلقي التصريحات.

3) **خبير حاسوب الي وشبكات**: شخص أو أكثر، يجمع بين المعرفة بعلوم الحاسوب والشبكات وإجراءات التحقيق ويكون مسئولا عن رفع وتحريز الادلة الجنائية الرقمية بالطريقة الفنية المناسبة ،التي لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوى والعرض على المحكمة.

4) **خبير تدقيق حسابات**: متخصص في المراجعة المحاسبية و خبير في التعامل مع نظمة البرمجية المستخدمة في المؤسسات المصرفية واليات تبادل النقد الالكتروني، ويعمل مع خبير الحاسب الآلي والشبكات لتحديد أسلوب الجريمة ،و مركز الضرر مع تقدير الخسائر المادية الناتجة عن الجريمة.

5) **خبير تصوير**: الفوتوغرافي والفيديو، لتصوير مسرح الجريمة.

6) **خبيصمات:** لرفع البصمات خاصة من المكونات المادية للحواسيب والشبكات المتضررة،بالخصوص لوحة المفاتيح والفأرة، وذلكعداتخاذ الاحتياطات الفنية اللازمة من قبل خبير الحاسوب.

7) **خبير رسم تخطيطي:** يقوم برسم تخطيطي (كروي) لمسرح الجريمة ،بطريقة فنية دقيقة مستخدما مقياسا مناسبا، بما يوضح تقسيماته وأماكن تواجد الادلة والاشخاص فيه.

الفئة الثانية:

وهم أفراد حماية وتأمين مسرح الجريمة وأفراد القبض وأفراد التحريات وغيرهم، وتحديدهم نوعا وكما متروك لتقدير المحقق، حسبما تفرضه طبيعة الجريمة وحجمها وظروفا.

عند الشروع في جمع الادلة من مسرح جريمة من الجرائم المتعلقة بشبكة الانترنت ينبغي التعامل معه على أنه مسرحين هما:

1) **مسرحتقليدي:** ويقع خارج بيئة الحاسب الآلي والانترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية، قد يترك فيها الجاني اثار عدة، كالبصمات وغيرها، وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الادلة الموجودة فيه كل بحسب اختصاصه.

2) **مسرحسيبراني" افتراضي":** ويقع داخل بيئة الحاسب الآلي وشبكة الانترنت، ويتكون من البيانات الرقمية التي تتواجد وتنقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الاقراص الصلبة الموجودة بداخله، والتعامل مع الادلة الموجودة في هذا المسرح يجب أن يتم على يد خبير متخصص في التعامل مع الادلة الرقمية.

أ. معاينة مسرح الجريمة المتعلقة بشبكة الإنترنت:

مع التسليم بأهمية المعاينة في كشف غموض الكثير من الجرائم التقليدية وجدارتها بتبوء مكان الصدارة والأولوية فيما عدا حالات استثنائية على ما عداها من الإجراءات الاستقصائية

خرى،إلا أن دورها في مجال كشف غموض الجرائم المعلوماتية وضبط الاشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها لا ترقى إلى نفس الدرجة من الاهمية، ومرد ذلك اعتبارين ما:

الاول أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يخلف عن ارتكابها اثارا مادية، والثاني هو أن عددا كبيرا من الاشخاص قد يتردد على المكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا والتي تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها ،مما يفسح المجال لحدوث تغير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقي ظلالا من الشك على الدليل المستمد من المعاينة، وحتى يكون للمعانية في الجرائم المتعلقة بشبكة الانترنت فائدة في كشف الحقيقة عنها وعن مرتكبها ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي:

- تصوير الحاسب الالي والاجهزة الطرفية المتصلة به والمحتويات العامة بمكانه،مع التركيز خاصة على تصوير الاجزاء الخلفية للحاسب وملحقاته ومراعاة تسجيل وقت وتاريخ ومكان إلتقاط كل صورة.
- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية الخاصة بالتسجيلات الإلكترونية التي تتزود بها شبكات المعلومات،بموافقة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع.
- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الامر فيما بعد على القضاء.
- وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي بالمسئولين بها ودور كل واحد منهم.
- فصل الكهرباء عن موقع المعاينة لشل فاعلية الجاني في القيام بأي فعل من شأنه التاثير على أثار الجريمة.

- إعادالموظفين عن أجهزة الحاسب الالي.و كذلك عن الاماكن الاخرى التي توجد بها أجهزة للحاسب الالي.
- عدم نقل أي معلومة من مسرح الجريمة إلا بعد التاكد من خلو المحيط الخارجي لموقع الحاسب الالي من أي مجال مغناطيسي يمكن أن يتسبب في محو البيانات المسجلة.
- الـتحـفظعما قد يوجد بسلة المهملات من الاوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة والاشرطة والاقراص الممغنطة غير السليمةوفحصها ورفع البصمات المحتمل اتصالها بالجريمة.
- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع البصمات.
- قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسب الالي والشبكات ونظم المعلومات.واسترجاع المعلومات، والذين تلقوا تدريبا كافيا على التعامل مع نوعية الاثار والادلة التي يحويها مسرح الجريمة المعلوماتية. ففي فرنسا مثلا يقوم فريق مكون من 13 شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إليه وكلاء النيابة والمحققين وجمعهم تلقوا تدريب متخصص إلى جانب اختصاصهم الاساسي في مجال التكنولوجيا الحديثة. وهم يقومون بمرافقة المحققين أثناء التفتيش حيث يقومون بفحص كل جهاز وينقلون نسخة من الاسطوانة الصلبة وبيانات البريد الإلكتروني ثم يقومون بتحرير تقرير يرسل إلى القاضي الذي يتولى التحقيق.

أما عن المعدات والبرامج فهم يستخدمون برامج تستطيع استعادة المعلومات من على سطوانة الصلبة .كما يمكنها قراءة الاسطوانات المرنة والصلبة التالفة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة.ومن المهم هنا أن يتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد.مع توثيق كل دليل على حدى بما فيها الادلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها ومن قام برفعه وتحريزه

وكيف ومتى تم ذلك.و البعض يرى أن التوثيق يجب أن يشمل المصادر المتاحة على الشبكة التي ترتبط بها الاجهزة محل التحقيق.

ولعل من أبرز الاماكن التي يحتمل وجود الادلة الجنائية المتعلقة بجرائم الانترنت فيها ما يلي:

☑ **الورق:** على الرغم من أن وجود أجهزة الحاسب الآلي، قلل من حجم الاوراق و الملفات التقليدية المستخدمة حيث يتم حفظ المعلومات والبيانات على أجهزة الحاسب الآلي، نجد الكثيرين ممن يقوموا بطابعة المعلومات لأغراض المراجعة أو التاكد من الشكل العام للمستند أو الرسالة أو الرسومات.وبالتالي فهي تعتبر من الادلة التي ينبغي الإهتمام بها في البحث عن الحقيقة.

☑ **جاز الحاسب الالي وملحقاته:** وجود جهاز الحاسب الآلي هام جدا للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو جريمة حاسوبية،إنها مرتبطة بالمكان أو الشخص الحائز على الجهاز،ولأجهزة الحاسب الالي أشكال وأحكام وألوان مختلفة وخبير الحاسب الآلي وحده الذي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة.

☑ **البرمجياتSoftware :** إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص أو ليس و لسعالانتشار فإن أخذ الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الاهمية عند فحص الدليل.

☑ **وسائط التخزين المتحركة:** كالأقراص المدمجة "أقراص الليزر" والاقراص المرنة والأشرطة المغناطيسية والفلاش ديسك –ميموري وغيرها. وتعد هذه الوسائط جزاء من الجريمة الانترنتية متى كانت محتوياتها عنصر من عناصر الجريمة.

☑ **المراشد Manuals :**الخاصة بالمكونات المادية والمنطقية للحاسب الآلي والتي تفيد في معرفة التفاصيل الدقيقة لكيفية عملها.

☑ **المودمModem** :وهو الوسيلة التي تمكن أجهزة الحاسب الالي من الاتصال ببعضها البعض،عبر خطوط الهاتف.وفي الوقت الحالي تطورت المودم لتكون أجهزة إرسال واستقبال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.

☑ **ا لطابعات:** والتي قد تحتوي على ذاكرة تحتفظ ببعض الصفحات التي سبق طباعتها.

ب. التفتيش:

ويعرّف التفتيش بوجه عام بأنه عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص،وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة، وفي الجرائم المتعلقة بشبكة الانترنت نجد أن الدخول غير المشروع إلى الانظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة و ق ع، إجراء يفيد في كشف الحقيقة عنها وعن مرتكبها، وتقتضيه مصلحة وظروف التحقيق في ا لا ئم المعلوماتية،وهو إجراء جائز قانونا ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني واللغوى.

قابلية مكونات وشبكات الحاسب الالي للتفتيش:

للحاسب الالي مو ن ت مادية Hardware ، وأخرى منطقية Software ، كما أن له شبكات اتصال بعدية Networks Telecommunication سلكية ولا سلكية محلية ودولية.فما مدى قابلية تلك المكونات للتفتيش؟

المكونات المادية للحاسب الالي:

لا يختلف اثنان في أن الولوج إلى المكونات المادية للحاسب الالي بحثا عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هو من الاماكن العامة أو من الاماكن الخاصة، حيث

أن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش. فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانونا في التشريعات المختلفة مع مراعاة التمييز بين ما إذا كانت مكونات الحاسب المراد تفتيشها منعزلة عن غيرها من الحاسبات الاخرى أم أنها متصلة بحاسب الي أخر أو بنهاية طرفية Terminal في مكان أخر كمسكن غير المتهم مثلا.فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الاخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن أما 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 والميادين والشوارع، أو كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة. فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الاشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.

المكونات المنطقية للحاسب الالي ومدي قابليتها للتفتيش:

تفتيش المكونات المنطقية للحاسب الآلي أثار خلافا كبيرا في الفقه بشأن جواز تفتيشها. فذهب رأي إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط "أي شيء" فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسب المحسوسة وغير المحسوسة بينما ذهب رأي اخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة. ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسب الآلي لابد أن يشمل "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي".بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب .وفي مقابل هذين الرأيين يوجد

رئي آخر رأى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الحاسب الالي أم لا،فذهب إلى أن النظر في ذلك يجب أن يستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على بيانات الحاسب الالي إذا اتخذت شكلا ماديا،

ويذهب رأي فقهي إلى انه في تحديد مدلول الشيء بالنسبة لمكونات الحاسب الالي يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية وبين طبيعة هذه البرامج والكيانات، وإنما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرف بأنها كل ما يشغل حيزا ماديا في فراغ معين وأن الحيز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزا ماديا في ذاكرة الحاسب الالي ويمكن قياسها بمقياس معين، وإنها أيضا تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها تعد طبقا لذلك ذات كيان مادي وتتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الاشياء المادية.

شبكات الحاسب الالي ومدى خضوعها للتفتيش "التفتيش عن بعد":

إن طبيعة التكنولوجيا الرقمية قد عقدت من التحدي أمام اعمال التفتيش والضبط،فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، لكن من الممكن الوصول إليها من خلال حواسيب تقع في الابنية الجاري تفتيشها، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي اخر أو حتى في بلد اخر، وفي حين أن السلطات في بعض البلدان قد لا تنزعج من أن تقوم تحقيقاتها إلكترونيا إلى اختصاص قضائي سيادي اخر، إلا أن السلطات في ذلك الاختصاص السيادي قد تشعر ببالغ انزعاج، وهذا يزيد من تعقيد مشاكل الجريمة السيبرانية العابرة للحدود ويزيد من أهمية تبادل المساعدة القانونية، ونستطيع أن نميز في هذه الصورة بين ثلاثة احتمالات على النحو التالي:

أ **الاحتمال الاول:** اتصال حاسب المتهم بحاسب اخر أو نهاية طرفية موجودة في مكان اخر داخل الدولة، يُثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن

الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان اخر مملوك لشخص غير المتهم؟

يرى الفقه الالماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع اخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجزائية الالماني ،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 اخر يوجد في مكان اخر غير مكان البحث الاصلي، ويتم هذا الامتداد وفقا لضابطين: "أ" إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث. "ب" إذا وجدت مخاطر تتعلق بضياع بعض الادلة نظرا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث وذات الشيء نجده في القانون الاتحادي الاسترالي حيث لم تعد صلاحيات التفتيش المتصلة بالأدلة الحاسوبية تقتصر على مواقع محددة، فقد توخى قانون الجرائم السيبرنية لعام 2001 إمكانية أن تتوزع بيانات الأدلة على شبكة حواسيب، ويسمح هذا القانون بعمليات تفتيش البيانات خارج المواقع التي يمكن اختراقها من خلال حواسيب توجد في الابنية الجاري تفتيشها ، ويشير مصطلح "البيانات المختجزة في حاسوب ما " إلى " أية بيانات محتجزة في جهاز تخزين على شبكة حواسيب يشكِل الحاسوب جزءا منها". فلا توجد حدود جغرافية محددة، ولا أي اشتراط بالحصول على موافقة طرف ثالث ، غير أن المادة 3 LBبقانون الجرائم لعام 1914، والتي أدرجها قانون الجرائم السيبرنية، تشترط إخطار شاغل المبنى قدر الإمكان عمليا، وهذا قد يكون أكثر تعقيدا مما يبدو عليه، إذ انه في مسار إجراء عملية بحث من خلال بيئة مرتبطة شبكيا، فإن المرء لا يكون متاكدا دائما من مكان وجوده.

ب **الاحتمال الثاني:** اتصال حاسب المتهم بحاسب اخر أو نهاية طرفية موجودة في مكان اخر خارج الدولة من المشاكل التي تواجه سلطة الادعاء في جمع الادلة قيام مرتكبي الجرائم بتخزين بياناتهم في انظمة تقنية خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية مستهدفين عرقلة الادعاء في جمع الادلة والتحقيقات وفي هذه الحالة فإن امتداد الإذن

بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن ودخوله في المجال الجغرافي للدولة أخرى وهو ما يسمي بالولوج أو التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها،لذا فإن جانب من الفقه يرى بأن التفتيش الإلكتروني العابر للحدود لا بد وأن يتم في إطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد تعقد بين الدول المعنية، وبالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في غياب تلك الاتفاقية، أو على الاقل الحصول على إذن الدولة الاخرى، وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم السيبيرية كما سبق ذكره أعلاه.

وكتطبيق لهذا الإجراء الاخير: فقد حدث في ألمانيا أثناء جمع إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب الي، فقد تبين وجود اتصال بين الحاسب الالي المتواجد في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها، وعندما أرادت سلطات التحقيق الالمانية ضبط هذه البيانات، فلم تتمكن من ذلك إلا عن طريق التماس المساعدة، الذي تم بالتبادل بين الدولتين ومع ذلك أجازت المادة 32 من الاتفاقية الاوربية بشأن الجرائم المعلوماتية السالف ذكرها ، إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين: الاولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتش

ج **احتمال الثالث:** التنصت والمراقبة الإلكترونية لشبكات الحاسب الالي التي نصت والاشكال الاخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريبا، فالقانون الفرنسي الصادر في 1991/7/10م ،يجيز اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات ، وفي هولندا أجاز المشرع لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة ضالع فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات ، وفي اليابان أقرت محكمة مقاطعة KOFU سنة1991م شرعية التنصت على شبكات الحاسب للبحث عن دليل

وتفتيش نظم الحاسب الآلي يمكن أن يتم بطرق عدة. فمثلا المرشد الفيدرالي الامريكي جاء بأربع طرق أساسية للتفتيش ممكنة التحقق هي:

1. تفتيش الحاسب الآلي وطبع نسخة ورقية من ملفات معينة في ذات الوقت.
2. تفتيش الحاسب الآلي وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت.
3. عمل نسخة إلكترونية طبق الاصل من جهاز التخزين بالكامل في الموقع. وبعد ذلك يتم إعادة عمل نسخةمن جهاز التخزين خارج الموقع للمراجعة
4. .ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.

الوسائل والبرمجيات المساعدة في التحقيق في الجرائم المتعلقة بالإنترنت: عند القيام بالتحقيق في الجريمة.يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة، وقواعد فنية تحقق الشرعية، وسهولة الوصول إلى الجاني.و يتم ذلك بالاعتماد على مجموعةوسائل، وفي هذا المجال هي:

ا لوسا ئلالمادية:

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

أ. عنوانIP ، والبريد الإلكتروني، وبرامج المحادثة:

عنوان الإنترنت هو المسئول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للموجهات والشبكات المعنية نقل الرسالة، وهو يوجد بكل جهاز مرتبط بالإنترنت، ويتكون من أربعة أجزاء، كل جزء يتكون من أربع خانات، فيكون المجموع اثنا عشر خانة كحد أقصى، حيث يشير الجزء الاول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الحاسب الآلي الذي تم الاتصال منه.وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز لتحديد

موقعه لمعرفة الجاني الذي قام بتلك الاعمال غير القانونية، ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك.

هذا وتوجد أكثر من طريقة يمكن من خلالها معرفة هذا العنوان الخاص بجهاز الحاسب الآلي في حالة الاتصال المباشر، منها على سبيل المثال ما يستخدم في حالة العمل على نظامشغيل WINDOWS حيث يتم كتابة WINPCFG في أمر التشغيل ليظهر مربع حوار يبين فيه عنوانIP ، مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل اتصال بشبكة الإنترنت،أما في حالة استخدام أحد البرامج التحادثية كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى ولو لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة.

ب. البروكسيPROXY :

يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الامن وتوفير خدمات الذاكرة الجاهزة . Cache Memory وتقوم فكرة البروكسي على تلقى مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية،أم إنه لم يتم تنزيلها من قبل فيتم إرسال الطلب إلي الشبكة العالمية، وفي هذه الاخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عنلون IP ومن أهم مزايا مزود البروكسي أن ذاكرة Cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوى في الإثبات عن طريق فحص تلك ا لعمليا تالمحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.

ج. برامج التتبع:

تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم ،وتقدم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوى هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP التي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى د. نظام كشف الاختراق :Intrusion Detection System ويرمز له اختصارا بالأحرف IDS وهذه الفئة من البرامج تتولي مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب أو الشبكة ، ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الاحداث فور وقوعها في جهاز الحاسب الآلي أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عده ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة ، والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها.

.. نظام جرة العسل Honey Pot :

وهو نظام حاسوبي مصمم خصيصا لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعا خاطئا بسهولة الاعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز اخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الاساليب التي يتبعها المهاجم في محاولة اعتداء، وتحليلها وبالتالي اتخاذ إجراء

وقائي فعال وهذه المعلومات التي تم جمعها تفيد في تحليل أبعاد الجريمة في حال وقوعها ويهتم فريق التحقيق بالعديد من البيانات التي توضح معالم الجريمة.

و. ادوات تدقيق ومراجعة العمليات الحاسوبيةAuditing Tools :

وهي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسوب معين .وتسجيلها في ملفات خاصة يطلق عليها Logs هذه الادوات تأتي مضمنة في أ نظمةالتشغيل المختلفة، وبعضها يأتي كبرامج مستقلة يتم تركيبها على انظمة التشغيل بعد إعدادها للعمل. كل ما يلزم هو قيام مدير الشبكة او النظام بإعدادها للعمل في وقت سابق لارتكاب الجريمة حتى تقوم بتسجيل المعلومات التي لها علاقة بالحادثة وربما ساعدت في كشف أسلوب الجريمة و مرتكبها ومن أمثلة هذه الادوات أداة Event Viewer لبيئة النوافذ،وأداة Syslogd لبيئةيونيكس.

ح. أدوات الضبط:

هي أدوات تعتبر من الوسائل المادية التي تساعد في ضبط الجريمة المعلوماتية، منها على سبيل المثال برامج الحماية وأدوات المراجعة. وأدوات مراقبة المستخدمين للشبكة، وبرامج التنصت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي ، والتسجيل وغيرها من الادوات مثلIDS,MNM4, MANGEMEN]

ط. الوسائل المساعدةللتحقيق:

من هذه الوسائل الادوات المستخدمة في استرجاع المعلومات من الاقراص التالفة، وبرامج كسر كلمات المرور، وبرامج الضغط وفك الضغط، وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسب، وبرامج نسخ البيانات، أيضا من الأدوات المهمة والتي تساعد جدا في عملية التحقيق في برامج منع الكتابة على القرص الصلب وذلك بعد ارتكاب الجريمة مما يساعد في المحافظة على مسرح الجريمة، وهناك البرامج التي تساعد على استرجاع الملفات والمعلومات التي قد يلجا الجاني إلى حذفها نهائيا من الحاسب الالي وهناك

أيضا برمجيات تحرير الملفات الست عشرية Hexadecimal Editors وهي برامج تمكن المحقق من الإطلاع على محتوى كل ملف حاسوبي بشكله الثنائي، متيحة له المزيد من القدرة على تحليل الملف والتعرف على طبيعة البيانات التي يحتويها، خاصة وأن بعض الانظمة قد لا تستطيع تحديد إلى أية فئة من الملفات ينتمي هذا الملف، وقد يتطلب الامر استخدام هذا النوع من برامج التحرير التي تعتمد على أن الكثير من الملفات تحتوى على مجموعة من الرموز ذات الدلالة تتواجد في بداية الملف، ويستطيع الخبير الحاسوبي من خلالها تحديد نوع الملف بدقة ، وهناك برمجيات البحث عن المفردات النصية والتي تستخدم في البحث عبر البيانات عن تلك الملفات التي تحتوى على مفردات معينة عادة ما تكون لها علاقة بالقضية ،كذلك توجد برمجيات استعراض الصور والتي تستخدم في عرض الصور الرقمية على شاشة الجهاز وبالتالي فهي تقدم خدمة جيدة للمحقق من خلال تمكينه من مشاهدة واستعراض الصور الرقمية المخزنة داخل أجهزة الحاسب الالي أو وسائط التخزين الخارجية، حيث تبرز الحاجة لهذه البرمجيات في الجرائم الإباحية "نشر مواد ذات طابع إباحي."

ي. ادوات فحص ومراقبة الشبكات:

هذه الادوات تستخدم في فحص بروتوكول TCP/IP وذلك لمعرفة ما قد يصيب الشبكة من مشاكل، ومعرفة العمليات التي تتعرض لها، ومن هذه دوات:

- **ARP** : ووظيفتها تحديد مكان الحاسب الالي فيزيائيا على الشبكة.
- **برنامج Visual Route 5.2a** :وهو عبارة عن برنامج يلتقط أي عملية فحص عملت ¬ ضد الشبكة، فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها مسح، والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان IP أو اسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.
- **أداة TRACER** : تقوم هذه الاداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها والوقت والفترات التي قضاها، وهي تسمح

برؤية المسار الذي اتخذه IP من مضيف إلى اخر، وتستخدم هذه الاداة الخيار Time To Live TTLالتي تكون ضمن IP لكي تستقبل من كل موجه رسالة وبذلك يكون هو العدد الحقيقي للوثبات،ويتم بذلك تحديد وبشكل دقيق المسار التي تسلكه الرزمة.وهذه الاداة تستخدم في الاساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف. ولكن يمكن أيضا من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها.

أداةNET STAT : هي أداة لفحص حالة الاتصال الحالي للبرتوكولTCP/IP ، ولها عدد من المهام من أهمها عرض جميع الاتصالات الحالية، ومنافذ التنصت، وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول التوجيه

الوسائل الإجرائية:

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

1. اقتفاء اثر:

من أخطر ما يخشاه مجرم نظم المعلومات تقصي أثره أثناء ارتكابه للجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح أولاها نصيحة هي قم بمسح اثارك Cover Your Tracks ، فلو لم يقم المخترق بمسح اثاره فمؤكد أنه سوف يتم القبض عليه حتى وإن كانت عملية الاختراق قد تمت بشكل سليم.ويمكن تقصي الاثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

2. الإطلاع على عمليات النظام المعلوماتي واسلوب حمايته:

ينبغي على المحقق وهو بصدد التحقيق في إحدى جرائم الانترنت أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء،وعليه الإطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين و الملف تواالإجراءات وتصنيف الموارد العامة، ومدى مزامنة الاجهزة، ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور، توزيع الصلاحيات للمستفيدين،إجراءات أمن العاملين،أسلوب النسخ الاحتياطي، والاستعانة ببرامج الحماية، كمراقبة المستفيدين والموارد والبرامج التي تعالج البيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام، و معرفة نوعية برامج الحماية وأسلوب عملها، والاستفادة من التقارير التي تنتجها نظم أمن البيانات وتقارير جدران الحماية.

3. الاستعانة بالذكاء الصناعي :

أثبتت تقنيات الحاسب الالي نجاحها في جمع الادلة الجنائية وتحليلها واستنتاج الحقائق منها،فيمكن الاستعانة به في حصر الحقائق والاحتمالات والاسباب والفرضيات و استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الالي، وفق برامج صممت خصيصا لذاالغرض.

ا لفرع الثاني:الصعوبات جرائية و بعض الهيئات المساعدة

أولا:الصعوبات جرائية:

أ نأنشطة مكافحة جرائم الكمبيوتر و الانترنت أبرزت تحديات و مشاكل كثيرة ،تغاير في جوانب متعددة التحديات و المشكلات التي تربط بالجرائم التقليدية خرى،فهذه الجرائم لا تترك أثرا ماديا في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية ،كان مرتكبها يملكون القدرة على إتلافأو تشويه أو إضاعة الدليل في فترة قصيرة.

فالتفتيش : في هذا النمط من الجرائم يتم عادة على نظام الكمبيوتر و قواعد البيانات و شبكات المعلومات و قد تجاوزت النظام المشتبه به إلى أ نظمةأخرى مرتبطة ، وهذا هو الوضع الغالب في ظل شيوع الربط بين الحواسيب و انتشار الشبكات الداخلية على مستوى المنشات و الشبكات المحلية و قليمية و الدولية ، و امتداد التفتيش إلى نظم غير النظام محل الاشتباه ، يخ لق تحدي ت كبيرة حول مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتيةلأصحاب النظم التي يمتد إليها التفتيش.

و الضبط : لا يتوقف على حجز جهاز الكمبيوتر فقد يمتد من ناحية ضبط المكونات المادية إلى مختلف اجزاء النظام التي تزداد يوما بعد يوم ،و الأهم أن الضبط ينصب على المعطيات و البيانات و البرامج المخزنة في النظام أ والنظم المرتبطة بالنظام محل الاشتباه، أي على أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير و الإ تلاف،و هذه الحقائق تثير مشكلات متعددة،منها المعايير المقبولة للضبط المعلوماتي و معايير التحرير إ ضافة إ لى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه ، وإن كان المشتبه به ، عندما تتعدى أنشطة الضبط إلى كل محتويات النظام التي تضم عادة معلومات و بيانات قد يحرص على سريتها أ وأن تكون محل حماية بحكم القانون أو لطبيعتها.

وأد ة ثبات : ذات نوعية مختلفة ، فهي معنوية الطبيعة كسجلات الكمبيوتر ومعلومات الدخول و الاشتراك و النفاذ و البرمجيات ، وقد أثارت و تثير أمام القضاء مشكلات من حيث مدى قبولها و حجيتها و المعايير المتطلبة لتكون كذلك خاصة في ظل قواعد ثبات التقليدية.

كماأن إ خ ضـ ص القضاء بنظر خطر الكمبيوتر و القانون المعين تطبيقه على الفعل لا يخلد ائما با لـ وضوح أو القبول أمام حقيقة أن غالبية هذه الافعال ترتكب من قبل أشخاص من خارج الحدود ، أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها وهو ما يبرز أهمية امتحان قواعد ختصاص و القانون الواجب التطبيق وما إذا كانت النظريات و القواعـد القائمة في هذا

الحقل تطال هذه الجرائم أ م يتعنأفراد قواعد خاصة بها في ضوء خصوصيتها ، وما يثيره من مشكلات في مجال الاختصاص القضائي ، و يرتبط بمشكلات الاختصاص القانوني مشكلات امتداد أشطة الملاحقة و التحري و الضبط و التفتيش خارج الحدود وما يحتاجه ذ لكإلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية.

إذن فان البعد الإجرائي لجرائم الكمبيوتر و الانترنت ي نطويعلى تحديات و مشكلات كثة،عناوينها الرئيسة ، الحاجة إلى سرعة الكشف خشية ضياع الدليل ، و خصوصية قواعد التفتيش و الضبط الملائمة لهذه الجرائم ،و قانونية و حجية أ دلةجرائم الكمبيوتر و الانترنت و مشكلات خ صة صلالقضائي و القانون الواجب التطبيق ،و الحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق و الملاحقة خارج الحدود ،وهذه المشكلات محل اهتمام كبير وطنيا و دوليا ،و التي يجب أن تفعل من أجلها الاتفاقيات الموجودة و أن توجد أ خرىأكثر حداثة ،دقة و تقنية.

ا لمستجدات جرائية في القانون الجزائري:

وتجاوزا للعراقيل التي يمكن أن تثور حال متابعة الجريمة و في ظل سرعةإتلاف الدليل وحفاظاعلى ما يثبت الجريمة ذاتها من الأدلة،و في ظل الحاجة للتدخل السريع لضبط الجريمة ،ولارتباط مادة الجريمة أو وسيلتها بأ نظمةأ طو فلأخرى لا صلة لهم بها أو بشبكات و نظممعلومات خارج الحدود أ شا تإليها الاحكام المستحدثة في قانون جراءات الجزائية و التي يمكن تلخيصها في:

- جواز التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني طبقا للمادة 47 ق ا ج.
- جواز ذلك في كل وقت ليلا أو نهارا بإذن مسبق من وكيل الجمهورية المختص.
- جواز ذلك لقاضي التحقيق وعبر التراب الوطني ، و يمكنه أمر ضابط الشرطة بذلك . نفس المادةالسابقة.

- جواز خلال بقو اعدالتفتيش في الجريمة المتلبس بها إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا أو محبوسا حالة عدم لمكان نقله لمخاطر تتعلق بالنظام العام أو احتمال الفرارأو الخوف من اختفاء دلة .و يتم التفتيش بإذن وكيل الجمهوريةأو قاضي التحقيق و بحضور شاهدين أو ممثل يعينه صاحب المسكن حسبالمادة47 مكرر قانون إجراءات جزائية.
- جوازتمديد الوقف تحت النظر لمدة 48 ساعةأخرى وفقا للمادة 51من ق ا ج.
- جوزإتباع طرق اعتراض المرسلات عن طريق إذن منوكيل الجمهورية بالكيفيات المحددة في المواد 65 مكرر5 حتى 65 مكرر10 ق ا ج.
- جوزإتباع طريقة التسريب وفقا للمواد 65 مكرر11 حتى65 مكرر18 ق ا ج.

ثانيا: بعض الهيئات المساعدة لمتابعة جرائم الانترنت

نظالنوع و خصوصية جرائم الانترنت ،فقد أوجدت بعض الدول أجهزة مختصة تتولى تطبيق قوانين مكافحة الجريمة المعلوماتية و تتبع الجناة و من أ ما:

1. مركز الشكاوى الخاصة بجرائم الانترنت:

قد طوّرت وكالات تطبيق القوانين أساليب جديدة وعلاقات جديدة للقبض على المجرمين في الفضاء السيبرني، أو الانترنت ،فظهر كنتيجة لذلك مركز الشكاوى الخاصة بجرائم الانترنت (IC3) هو كناية عن نظام تبليغ وإحالة لشكاوى الناس في الولايات المتحدة والعالم أجمع ضد جرائم الانترنت،ويخدم المركز، بواسطة استمارة للشكاوى مرسلة على الإنترنت وبواسطة فريق من الموظفين والمحللين، الجمهور ووكالات فرض تطبيق القوانين الاميركية والدولية التي تحقق في جرائم الانترنت.

نشأ مركز الشكاوى الخاصة بجرائم الانترنت كمفهوم سنة 1998بعد إدراك بأن الجريمة بدأت تدخل الانترنت لأن الاعمال التجارية والمالية كانت قد بدأت تتم عبر الانترنت، ولأن مكتب التحقيقات الفدرالي أراد أن يكون قادرا على تعقب هذه النشاطات وعلى تطوير تقنيات تحقيق خاصة بجرائم الانترنت.

ولم يكن انذاك أي مكان واحد معين يمكن للناس التبليغ فيه عن جرائم الإنترنت، وأراد مكتب التحقيقات الفدرالي التمييز بين جرائم الانترنت والنشاطات الإجرامية الاخرى التي تَبلغ عنها عادة الشرطة المحلية ومكتب التحقيقات الفدرالي والوكالات الاخرى التي تطبق القوانين الفدرالية وهيئة التجارة الفدرالية (FTC) و المكتب الاميركي للتفتيش البريدي(USPIS) ، وهو الشعبة التي تطبق القوانين المتعلقة بمصلحة البريد الاميركية، وغيرها من الوكالات.

وقد تم تأسيس أول مكتب للمركز سنة 1999 في مورغانتاون بولاية وست فرجينيا، وسمّي مركز شكاوى الاحتيال على الانترنت، وكان المكتب عبارة عن شراكة بين مكتب التحقيقات الفدرالي والمركز القومي لجرائم موظفي المكاتب، وهذا الاخير مؤسسة لا تبغي الربح متعاقدة مع وزارة العدل الاميركية مهمتها الاساسية تحسين قدرات موظفي أجهزة تطبيق القانون، على صعيد الولاية والصعيد المحلي، على اكتشاف جرائم الانترنت أو الجرائم الاقتصادية ومعالجة أمرها.

وفي عام 2002، وبغية توضيح نطاق جرائم الانترنت التي يجري تحليلها، بدءا من الاحتيال البسيط إلى تشكيلة من النشاطات الإجرامية التي أخذت تظهر على الانترنت، أعيدت تسمية المركز وأطلق عليه اسم مركز الشكاوى الخاصة بجرائم الانترنت، ودعا مكتب التحقيقات الفدرالي وكالات فدرالية أخرى، مثل مكتب التفتيش البريدي وهيئة التجارة الفدرالية والشرطة السرية وغيرها، للمساعدة في تزويد المركز بالموظفين وللمساهمة في العمل ضد جرائم الانترنت.

وقد أصبح هناك اليوم في مركز الشكاوى القائم بفيرمونت، بولاية وست فرجينيا، ستة موظفين فدراليين و حوالى أربعين محللا من القطاع الاكاديمي وقطاع صناعة الكمبيوتر وخدمات الانترنت يتلقون الشكاوى المتعلقة بجرائم الإنترنت من الجمهور، ثم يقومون بالبحث في الشكاوى وتوضيب ملفها وإحالتها إلى وكالات تطبيق القانون الفدرالية والمحلية والتابعة للولايات وإلى أجهزة تطبيق القانون الدولية أو الوكالات التنظيمية وفرق العمل التي تشارك فيها عدة وكالات، للقيام بالتحقيق فيها.

وبإمكان الناس من كافة انحاء العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بالجرائم الواقعة على الانترنت(http://www.ic3.gov) ، ويطلب الموقع اسم الشخص وعنوانه البريدي ورقم هاتفه؛ إضافة إلى اسم وعنوان ورقم هاتف والعنوان الإلكتروني، إذا

كانت متوفرة. للشخص.أو المنظمة.المشتبه بقيامه بنشاط إجرامي؛ علاوة على تفاصيل تتعلق بكيفية وقوع الجريمة حسب اعتقاد مقدم الشكوى ووقت وقوعها وسبب اعتقاده بوقوعها؛ بالإضافة إلى أي معلومات أخرى تدعم الشكوى.

يعمل مركز الشكاوى الخاصة بجرائم الانترنت ووكالات أميركية أخرى مع المنظمات الدولية مثل لجنة الجرائم الاقتصادية والمالية في نيجيريا (EFCC) ومع المسؤولين عن تطبيق القانون في بلدان أخرى لمحاربة الاحتيال على الانترنت.وإعداد ملفات القضايا وإحالتها على المركز.هدف عمليات المركز الرئيسي هو أخذ شكوى المواطن الفرد التي قد تتعلق بجريمة تنجم عنها أضرار بحدود 100 دولار مثلا. وضمها إلى المعلومات المبلغ عنها من جانب 100 أو 1000 ضحية أخرى من مختلف أنحاء العالم، فقدت أموالا نتيجة نفس السيناريو.وثم إعداد ملف قضية مهمة بأسرع وقت ممكن و إحالا على الجهات المختصة بالمتابعة.

والحقيقة هي أنه لا يسمح لمعظم الوكالات فرض تطبيق القانون، معالجة أمر القضايا التي تمثل مبالغ ضئيلة نسبيا، ومبلغ مئة دولار أقل على الارجح من المبلغ المسموح بالتحقيق في أمره، غير أن معظم المجرمين يعملون على الانترنت لكي يوسعوا نطاق فرصهم في إيذاء الضحايا وكسب المال؛ وجرائم الانترنت لا تقتصر أبدا على ضحية واحدة، وهكذا، إذا تمكن محققوم كتبا لشاوى من ربط عدة شكاوى ببعضها البعض.وحولوها إلى قضية واحدة قيمتها عشرة الاف أو مئة ألف دولار، أضرت بمائة أو ألف ضحية.تصبح الجريمة عندئذ قضية مهمة، ويصبح بإمكان وكالات تطبيق القانون التحقيق فيها.

وساعدمركوا لشاوى الخاصة بجرائم الانترنت أحيانا وكالات تطبيق القانون من خلال إجراء الابحاث وإعداد ملف القضية الاولي، وقد وجد محققو المركز، خلال السنتين والنصف الاولتين من عمر المشروع، وعلى الرغم من جهود إعداد القضايا وإحالتها بسرعة إلى وكالات تطبيق القوانين، أن فرق العمل الخاصة بمكافحة جرائم الانترنت لم تكن جميعا مجهزة لمتابعة هذه الجرائم أو ىالتحقيق فيها بسرعة، وقد لا تملك بعض فرق العمل هذه القدرة على القيام بعمليات سرية، أو قد لا تملك التجهيزات اللازمة لاقتفاء الآثار الرقمية للأدلة

الجرمية التي يحولها إليها مركز الشكاوى. لذلك، أصبح من المهم جدا بالنسبة لمركز الشكاوى أن يطور ويتعقب اثار الجرائم ثم يتوصل إلى إعداد ملف القضية الاولي،مثلا. قد يتعرف مركز الشكاوى الخاصة بجرائم الانترنت على هوية100 ضحية، ويقرر انه يبدو أن النشاط الإجرامي صادر عن جهاز مقدم خدمات كمبيوتر في كندا، مثلا. لكن ذلك الجهاز قد يكون مجرد كمبيوتر تم التسلل إليه، وقد يكون ما حدث هو أن المجرمين يستخدمون هذه الالة " كنقطة انطلاق وهمية" لإخفاء مكان تواجدهم الحقيقي. لذا فإنه من المفيد بالنسبة لمحالي مركز الشكاوى أن يعرفوا المزيد عن "نقطة الانطلاق الوهمية"؛ فقد تكون هناك مجموعة في تكساس، أو أفريقيا الغربية، أو رومانيا، تستخدم جهاز مقدم خدمات الانترنت في كندا لجمع المعلومات عن الضحايا المحتملين.

2. وحدة مبادرات جرائم الانترنت ودمج موارد ها:

نظرا لتوصل مركز الشكاوى الخاصة بجرائم الانترنت IC3 إلى أنه من الافضل في بعض القضايا التقنية المعقدة تعقب أثر التحقيقات المبكرة، قام بإنشاء مكتب فرعي لهذا الغرض في بيترسبرغ، بولاية بنسلفينيا، أطلق عليه اسم "وحدة مبادرات جرائم الانترنت ودمج مواردها " (CIRFU). وتقوم محللو هذه الوحدة بإلغاء مسارات التحقيق الخاطئة ويغربلون أدلة القضية وينقحونها قبل إحالتها إلى وكالات تطبيق القوانين أو فرق العمل الخاصة المحلية أو الدولية.

تحظى وحدة مبادرات جرائم الإنترنت (CIRFU) بالدعم من بعض أكبر الشركات التي يستهدفها مجرمو الفضاء السبراني،أي المنظمات والتجار الذين يعملون في مجال الانترنت مثل ما يكروسوفت و بايباي/ باي بال،وأميركا أونلاين،وجمعيات هذه الصناعة التجارية مثل اتحاد برامج كمبيوتر الاعمال، وجمعية التسويق المباشر، ومجلس مخاطر التجار، وصناعة الخدمات المالية،وغيرها ،وقد انضم محققون ومحللون من هذه المنظمات،يعمل الكثير منهم على قضايا جرائم تت،إلى وحدة المبادرات المذكورة لتحديد اتجاهات وتكنولوجيات جرائم الانترنت، ولجمع المعلومات لإعداد ملفات قضايا قانونية ذات شأن،ولمساعدة وكالات تطبيق القانون في جميع أنحاء العالم على اكتشاف جرائم الإنترنت ومحاربتها.

المبحث الثاني :الجهود الدولية في مواجهة جرائم الإنترنت

لم يكن هناك قلق مع بدايات شبكة الإنترنت من جرائم يمكن أن ترتكب عليها أو بواسطتها لا لأنها امنة في تصميمها وبناءها ،بل نظرا لمحدودية مستخدميها ،علاوة على كونها كانت مقصورة على فئة معينة من المستخدمين – الباحثين ومنتسبي الجامعات إلا أنه ومع توسع استخدامها ودخول جميع فئات المجتمع إلى قائمة مستخدميها بدأت تظهر على الوجود ما يسمى بالجرائم المعلوماتية على الشبكة[1] أو بواسطتها ،جرائم تتميز بحداثة الاسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو اثارها وتعدد صورها وأشكالها. ليس هذا فحسب بل اتصفت بالعالمية وبانها عابرة للحدود ، وهذا أمر طبيعي خاصة إذا ما علمنا أن شبكة الإنترنت ذاتها لا تعرف الحدود أي أنها ذات طبيعة عالمية.

وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات و المواصلات . وتعزيز التعاون بينها واتخاذ تدابير فعّالة للحد منها والقضاء عليها ولمعاقبة مرتكبيها.

وعلى هدي ما تقدم سوف نتناول بالدراسة التعاون الدولي وأهميته في مجال مكافحة الجرائم المتعلقة بالإنترنت " فصل أول" مع بيان للصعوبات التي قد تواجه هذا التعاون " فصل ثان ".

المطلب الاول :التعاون الدولي في مواجهة جرائم الإنترنت

يمكن ارتكاب الجريمة السيبرنية من أقصى بقاع الارض بنفس سهولة ارتكابها من أقرب مان. كما أن رسالة واحدة تعزز ارتكاب جريمة سيبرنية يمكن تمريرها من خلال الكثيرين من مقدمي الخدمات في بلدان مختلفة لها نظم قانونية مختلفة. كما أن الآثار الرقمية التي يمكن

---

1 :جرائم الحاسب الالي – ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية " الإنترنت" الأول والذي أنعقد بمقر الأمانة العامة بالرياض خلال الفترة من 4 2004/4/5م

تتبعها تكون ضعيفة أو سر عةالزوال،ولذا تستلزم اتخاذ إجراء سريع. وهذا هو الحال تحديدا حين يسعى المرء إلى منع ارتكاب جريمة في مرحلة التنفيذ، مثل شن هجوم إلكتروني على بنية تحتية حرجة. وهذا هو الحال أيضا حين يسعى المرء إلى جمع أدلة تتصل بجر عةل تكنت مؤخرا. وتصبح المهمة بالغة الصعوبة حين تعبر الهجمة اختصاصات قضائية متعددة ذات نظم مختلفة في حفظ الادلة. وهكذا لم تعد تكفي الوسائل التقليدية لإنفاذ القانون.

إن بطء الإجراءات الرسمية يجازف بفقدان الادلة،وقد تكون بلدان متعددة متورطة في مر. ولذا تشكل متابعة وحفظ سلسلة الادلة تحديا كبيرا. بل حتى الجرائم "المحلية" قد يكون لها بعد دولي، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان التي مرت الهجمة من خلالها.

وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل،فقد تكون هناك حاجة إلى مساعدة من السلطات في البلد الذي كان منشأ الجريمة،أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرَّم وهو في طريقه إلى الهدف،أو حيث قد توجد أدلة الجريمة. وهناك عنصران أساسيان للتعاون: المساعدة غير الرسمية من محقق لآخر، والمساعدة الرسمية المتبادلة.

وقد تكون المساعدة غير الرسمية أسرع إنجازا،وهي الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أي أوامر تفتيش أو طلب تسليم المجرم). وهي تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتولد نتيجة الاتصالات التي جرت مع الوقت في مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

ومن ناحية أخرى فإن المساعدة الرسمية المتبادلة هي عملية أكثر إرهاقا يتم اللجوء إليها عادة عملا بترتيبات معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية. وهي تشترط في الغالب الاعم أن تكون الجريمة المعنية على درجة معينة من القسوة وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب. ويشار إلى هذا الامر الاخير باعتباره " جرما مزدوجا."

وسوف نبحث فيما يلي التعاون القضائي " م بحث أول" والتعاون الدولي في مجال تسليم المجرمين" م بحث ثان" ،والتعاون الدولي في مجال التدريب" م بحث ثالث"

الفرع الأول: التعاون القضائي

فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالإنترنت غالبا ما تقتضي تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمةلتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالإنترنت ،وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة .ولتحديد مصدر الجريمة غالبا ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها .وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه. وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى . بمعنى الحاجة إلى ما يسمي التعاون القضائي.

أولا: التعاون الامني على المستوى الدولي

1) أولا:ضرورة التعاون الامني الدولي

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدرٍ من الأمن والنظام. وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والافراد على حد سواء. ولقد أثبت الواقع العملي أن الدولة– أي دولة– لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة . فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وانماط جديدة من الجرائم منها

را ئم المتعلقة بشبكة الإنترنت وهي نوعٌ من الجرائم المعلوماتية ،التي باتت تشكل خطرا لا على سرية النظم الحاسوبية او سلامتها او توافرها فحسب ، بل تعدت إلى أمن البنى الاساسية ارجة[1]

ومع تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دو على المستوى الإجرائي الجنائي ،بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول ا لمختلفة،وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها[2]

فمثلا في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما ،ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى ،وتقع الآثار المدمرة لهذا الهجوم في دو لةثالثة. فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكشاف هذه الجرائم ومعاقبة مرتكبيها .لذا فإن التحقيقات في الجرائم المتصلة بالحاسب الآلي وملاحقتها قضائيا تؤكد على أهمية المساعدة القانونية المتبادلة بين الدول ، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود ،لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها بمعنى اخر أنه متى ما فرّ المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزا.

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة،خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العادلة.

1: تدابير مكافحة الجرائم المتصلة بالحواسيب – مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة 18 2005/4/25 م- وثيقةرقم. A/CONF.203/14

2 :د/جميل عبد الباقي الصغير. الجوانب الإجرائية للجرائم المتعلقة بالإنترنت. دار النهضة العربية. القاهرة 1998م ص 75

2) جهود المنظمة الدولية للشرطة الجنائية" الإنتربول"

البدايات الاولية للتعاون الدولي الشرطي ترجع إلى عام 1904م عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الابيض بتاريخ 1904/5/18 موالتي نصت في مادتها الاولى ع"" تتعهد كل الحكومات المتعاقدة بإنشاء أو تعين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج ، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الاطراف المتعاقدة. ""

ولم تمر سنة على إبرام هذه الاتفاقية إلا وكانت سبع دول من الدول المتعاقدة تنشي مثل تلك الاجهزة وتتبادل من خلالها المعلومات والبيانات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج من أجل القضاء على هذه الجريمة في أقاليمها[1]

ثانيا:المساعدة القضائية الدولية

الإنترنت ما هي إلا شبكة عالمية تمتاز بأنها دولية وأنها عابرة للحدود ولا تعرف للحدود الجغرافية مع وبالتالي فإن الجرائم المتصلة بها تعتبر هي الاخرى عالمية وذات طابع دولي واثرها يمتد لأكثر من دول ة.ففي واقعة تتلخص وقائعها في قيام شخصين مقيمين في ملبورن بأستراليا بإرسال ما بين ستة إلى سبعة لاين رسالة إلكترونية على عناوين في أستراليا والولايات المتحدة الامريكية بالإضافة إلى قيامهما بوضع عدة رسائل على لوحات الرسائل لدى الشركات الرئيسية المقدمة لخدمات الإنترنت . وذلك كله بهدف التشجيع على شراء أسهم إحدى الشركات الامريكية التي كانت تباع أسهما في الولايات المتحدة الامريكية في الرابطة الوطنية للأسعار المؤتمتة للمتاجرة بالأوراق المالية " بورصة " NASDAQ . وكانت هذه الرسائل تبشر على غير الحقيقة بزيادة سعر أسهم الشركة بنسبة 900 %. ونتيجة لذلك وبعد فترة قصيرة حدثت زيادة في حجم تداول أسهم تلك الشركة لتصل إلى عشرةأمثالها وبالتالي تضاعف سعر السهم .ولقد اعترف أحد المتهمين وهو مساهم في الشركة أنه قدم معلومات

1: H . Feraud , E.Schlanilz , la cooperatation policiere international , R.I.D.P,1974 ,p477-478

زائفة وغير صحيحة وعندما ارتفعت الاسعار باع أسهمه في الشركة محققا بذلك ربحا كبيرا[1].

والملاحظ هنا أن الشخصين قد انتهكا القانون الاسترالي والامريكي بالإضافة إلى التلاعب في الاسواق المالية ناهيك عن تعطل أجهزة الحاسب الآلي في كلا البلدين بسبب الكم الهائل من الرسائل الإلكترونية.

ومن خلال المثال السابق نلاحظ أن ملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة من أجل توقيع العقاب عليهم يستلزم القيام بإجراءات إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها . ومن هذه الإجراءات معاينة مواقع الإنترنت في الخارج أو ضبط الاقراص الصلبة أو تفتيش نظم الحاسب الآلي وهذا كله قد يصطدم بمشاكل الحدود والولايات الـقضائية. ولأن كان كذلك فلا مناص من تقديم المساعدة القانونية المتبادلـة. وهذا ذاته ما حصل في الواقعة السابقة حيث كان هناك تعاون بن السلطات الاسترالية و السلطات الامريكية.

وتعّرف المساعدة القضائية الدولية بأنها"" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخري بصدد جريمة من الجرائم" [2].

وتتخذ المساعدة القضائية في المجال الجنائي صور عدة منها:

1. **تبادل المعلومات:**

وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما ، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم ، وقد يشمل التبادل السوابق القضائية للجناة[3].

ولهذه الصورة من صور المساعدة القضائية الدولية صدى كبيرا في كثير من الاتفاقيات كالبند

1 :تدابير مكافحة الجرائم المتصلة بالحواسيب – مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة 18 2005/4/25 م– وثيقةرقم. A/CONF.203/14 ص5

2:د/ سالم محمد سليمان الأوجلي : أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية ، رسالة دكتوراه ، كلية الحقوق جامعة عين شمس 1997 م ص425

3 : المادة5 من اتفاقية الرياض العربية للتعاون القضائي 1983

"و" والبند "ز" من الفقرة الثانية من المادة الاولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية. وهناك البند أولا من المادة الرابعة من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي.

وذات الصورة نجدها في المادة الاولى من اتفاقية الرياض العربية للتعاون القضائي[1] ، والمادة الاولى والثانية من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي[2].ويوجد لها تطبيق كذلك في اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية2000 في البنود الثالث والرابع والخامس من المادة الثامنة منها.

2. **تدابير الإجراءات:**

ويقصد به قيام دولة ما بناء على اتفاقية او معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة[3] من أهمها التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات . بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة. وأيضا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الاهمية بمكان بحيث تؤدى دورا مهما في الوصول إلى الحقيقة.

ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الامم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية[4] ، واتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م في المادة21 منها ، وذات الشيء نجده في معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999م في المادة 9 منها ، وأيضا المادة 16 من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م.

---

1 صدرت هذه الاتفاقية في 1993/4/6م بمدينة الرياض بالمملكة العربية السعودية

2 :اعتمد هذا النموذج من المجلس الأعلى لمجلس التعاون الخليجي في دورته الرابعة والتي انعقدت بدولة الكويت في الفترة من 21- 2003/12/22م

3 :د/ سالم محمد سليمان الأوجلي- المرجع السابق ص 427

4 :اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/118 ، بتاريخ1990/12/14

3. **الإنابة القضائية الدولية:**

ويقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها ، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها[1].

الفرع الثاني :تسليم المجرمين

استقر فقه القانون الدولي على اعتبار تسليم المجرمين شكلا من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها واستقرارها وحتى لا يبقى أولئك العابثين بمنأى عن العقاب يعيثون في الأرض فسادا.

وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافات المجالات ومنها مجال الاتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل أمتد إلى أكثر من إقليم ، بحيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في بلد معين ويقبل على التنفيذ في بلد اخر ويرتكب الفرار إلى بلد ثالث للابتعاد عن أيدي أجهزة ا لعدا لة. فالجريمة إذا أصبح لها طابع دولي والمجرم ذاته أصبح مجرما دوليا ، وهذا بالفعل ما ينطبق على الجرائم المتعلقة بالإنترنت.

وحيث أن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الاعمال القضائية على المجرمين الفارين ، كان لا بد من إيجاد الية معينه للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها ، ولكي يتم ذلك ويكون هناك تعاون دولي ناجح في مجال تحقيق العدالة كان لزاما تنظيم هذا النوع من التعاون الدولي تشريعيا وقضائيا وتنفيذيا. فالدولة ما دامت عضوا في المجتمع الدولي لا بد لها من الإيفاء بالالتزامات المترتبة على هذه العضوية ومن ضمنها الارتباط بعلاقات دولية وثنائية تتعلق باستلام وتسليم ا لمجرمن.

1: د/جميل عبد الباقي الصغير- الجوانب الإجرائية – المرجع السابق ص83

ولو أمعناالنظر في نظام تسليم المجرمين لوجدناه يقوم على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب أحد الجرائم العابرة للحدود ومنها الجرائم المتعلقة بالإنترنت عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك ، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة . فهو إذا يحقق مصالح الدولتين الاطراف في عملية التسليم ، فهو يحقق مصلحة الدولة الاولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وتشريعاتها ، ويحقق في ذات الوقت مصلحة للدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون ومن شأن بقائه فيها تهديد أمنها و لستقرارا .

ا لمطلبالثاني : التعاون الدولي في مجال التدريب على مواجهة الجرائم المتعلقة بالإنترنت

التقدم المتواصل في تكنولوجيا الحاسب الآلي والإنترنت يفرض على جهات إنفاذ القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات ، والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومواجهتها هذا من ناحية ، ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية ، لما تتسم به هذه الجرائم من حداثة في الاسلوب وسرعة في التنفيذ وسهولة في إخفائها والقدرة على محو اثارها. حيث أثبتت الوقائع العملية ان هناك جرائم متعلقة بالحاسب الآلي وشبكة الإنترنت قد ارتكبت على مرأى ومسمع من رجال الشرطة ، بل قام بعض ، رجالا لشرطة بتقديم يد المساعدة لمرتكبي هذه الجرائم دون قصد وعن جهل ، أو على سبيل واجبات المهنة التي يلزمهم بها هذا القانون. مثلما حدث عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الامريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة ، ونتيجة لذلك أتلف ما كان قد سلم من الملفات

وا لامج[1]. وإتلاف الأدلة قد يقع كذلك عن خطأ مشترك بين الخبراء وبين الجهة المجني عليها ، فمثلا في تحقيق إحدى الجرائم المعلوماتية والتي تدور وقائعها حول طلب أحد الاشخاص منإحدى الشركات زعم انه وضع قنبلة منطقية بنظام حاسبها الآلي. تبين أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيرا للتحقق من صحة ذلك وإبطال مفعول القنبلة إن وجدت ، وبالفعل نجح الخبير في اكتشاف القنبلة وإزالتها من البرنامج الموضوعة فيه ، وعندما تولت الشرطة التحقيق اتضح انه بإزالة القنبلة أتلفت كل الادلة على وجودها[2] وبالتالي فإن ظهور هذه الانماط الجديدة من الجرائم أصبح وهذا ما أثبته الواقع العملي يشكل عبئا ثقيلا على عاتق جميع أجهزة العدالة الجنائية سواء رجال الضبط القضائي أو رجال التحقيق أو المحاكم على مختلف درجاتها. سيما وأن متطلبات العدالة وكما أسلفنا تقتضي أن تتحمل الاجهزة الامنية الحكومية كامل المسؤولية تجاه اكتشاف كافة الجرائم المعلوماتية وضبط الجناة فيها وتحقيق العدالة في حقهم.

لأجل ذلك كان لا بد أن تكون تلك الاجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة.

مركز الشكاوى الخاصة بجرائم الإنترنت(IC3) ووه ةم بطر لت جرائم نتودج موا ردا(CIRFU)، هما بمثابة عمل متطور ومتقدم باستمرار، وأثناء هذا التقدم، يراجع موظفو ومحللو مركز الشكاوى ما أثبت نجاحه وما ثبت فشله من إجراءات، ويسعون باستمرار لتأمين مساعدة الخبراء والمصادر التي تزودهم بمعلومات استخباراتية ليصبحوا أكثر فطنة بخصوص جرائم الإنترنت، ولكي يتعلموا كيف يمكنهم محاربتها بصورة أكثر فعالية، فهذه هي مهمة مركز الشكاوى الدائمة التي لا تتغير

1: د/محمد أبو العلا عقيدة ،مرجع سابق ص 24

ا لفر ع ول: التدريب واهميته في مجال مكافحة الجرائم المتعلقة بشبكة الإنترنت

التدريب يعد جزءا من عملية التنمية الإدارية وهو يهتم بالدرجة الأولي بالكفاءة والفعالية في إنجاز العمل . من هنا فقد حرصت الكثير من المنظمات العامة والخاصة على العناية به ، باعتباره أحد الادوات الاساسية لرفع مستوى الاداء وزيادة الكفاية الإنتاجية وإعداد العاملين على اختلاف مستوياتهم للقيام بواجبات أعمالهم والمهام الموكلة إليهم على خير وجه. إضافة إلى تهيئتهم لتحمل المزيد من المسؤوليات من خلال زيادة قدراتهم على مواجهة المهام المعقدة في الحاضر والمستقبل .

ولهذا أصبح ينظر إلى التدريب على أنه وسيلة للاستثمار الذي تلجأ إليه المنظمات الإدارية لتحقيق أهدافها باعتباره عنصرا حيويا لا بد منه لبناء الخبرات والمهارات المتجددة .

والواقع أن التدريب أصبح يلعب دورا هاما في حياة الإنسان في عصرنا الحاضر ، حتى يمكننا القول بأننا نعيش اليوم عصر التدريب ، فقد زاد الاهتمام بالتدريب بمختلف جوانبه الفنية والتكتيكية فقد أضحي ضرورة للفرد المتدرب وللمنظمة التي ينتسب إليها في ان واحد ، سواء أكانت منظمة مدنية أو عسكرية ، حكومية أو خاصة ، تعمل في قطاع العدالة أم في غيره ، فهو أحد العناصر الاساسية لزيادة كفاءة العنصر البشري ويرفع إنتاجيته ويحقق التنمية بمفهومها الشامل . والهدف من عملية التدريب إدخال وإحداث تعديلات جوهرية على سلوك المتدربين ، تبدو اثارها واضحة في سلوكهم لأداء الاعمال التي يكفلون بها كل في مجال تخصصه ، بشكل أفضل بعد عملية التدريب لا قبلها.[1]

وتبدوا أهمية التدريب وضرورته في أنه من ناحية يعد الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الاخرين من خلال أشخاص أكفاء مؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة ، كما أنه يعد من ناحية أخرى الوسيلة الملائمة والفعالة لوضع المعارف العلمية موضع التطبيق الفعلي والتعرف

1: صالح محمد النويجم : تقويم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض من وجهة نظر العاملين فيها رسالة ماجستير في العلوم الإدارية ، جامعة نايف العربية للعلوم الأمنية الرياض 2005 م ص1

على الاخطاء والسلبيات التي يمكن أن يكشف التطبيق العملي للقوانين والانظمة واللوائح ، ووضع الحلول الكفيلة بتجنبها . وتزداد أهمية التدريب في الوقت الحاضر نظرا للتطور التكنولوجي الكبير الذي يشهده العالم اليوم.[1]

والتدريب المقصود هنا ليس التدريب التقليدي فحسب فلا يكفي أن تتوافر لدي رجال العدالة الجزائية الخلفية القانونية أو أركان العمل الشرطي وإنما لا بد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية. وهذه الخبرة الفنية لا تتأتى دون تدريب تخصصي يراعي فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب ، ويلاحظ هنا أنه من الاسهل تدريب متخصص في تكنولوجيا المعلومات وشبكات الاتصال بدلا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلي دعاء العام . ويذهب بعض الخبراء إلى أنه يجب أن تتوافر لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي[2].

وبالنسبة للمنهج التدريبي فيجب أن يشتمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلي مع ذكر لمفاهيم معالجة البيانات وتحديد نوعية و أنماط الجرائم المعلوماتية ، و بيان لأهم الصفات التي يتميز بها المجرم المعلوماتى ، والدوافع وراء ارتكاب الجرائم المعلوماتية.

وفيما يتعلق بمنهج التحقيق فإنه لا بد وأن يشتمل على:

1. إجراءات التحقيق.
2. الخطط للتحقيق
3. تجميع المعلومات وتحليلها
4. أساليب المواجهة والاستجواب

1: محمد السيد عرفة. تدريب رجال العدالة وأثره في تحقيق العدالة ، جامعة نايف العربية للعلوم الأمنية،الرياض 2005 ،ص2

2 هشام محمد فريد رستم – الجرائم المعلوماتية " أصول التحقيق الجنائي الفني "- بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون بجامعة مارات العربية المتحدة في الفترة 3-2000/5/3م المجلد الثاني الطبعة الثالثة - 2004 م ص 496

5. مراجعة النظم الفنية للبيانات
6. أساليب المعمل الجنائي.

بالإضافة إلى ذلك لا بد وإن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على أدلة الاتهام وما يخص الملاحقة الدولية والتعاون المشترك[1]

وفيما يخص التدريب فإنه لا بد وأن يراعى في البرنامج التدريبي نوعه وصفته و ما إذا كان رسميا من خلال حلقات دراسية أو حلقات نقاش – ورش العمل – حول النوع المستحدث من الجرائم ، وحلقات النقاش التي يمكن أن تثمر أفضل تدريب رسمي هي تلك التي تكفل تفاعل المشاركين ، وتتضمن تحليلا لحالات دراسية وإكساب خبرة عملية في كيفية التعامل مع الحاسب الآلي وكيفية استخدام تقنيات الاتصال بين شبكات الحاسب الآلي ، وما يرتبط بها من قواعد بيانات ومعلومات . وقد يكون البرنامج التدريبي غير رسمي من خلال تكليف المتدرب بالعمل مع شخص لدية خبرة في تحقيق الجرائم المعلوماتية ، أو التدريب باستخدام أسلوب الفريق والذي تقوم فلسفته على تدريب الفريق أو مجموعة متخصصة في جرائم الحاسب الآلي مرة واحدة بحيث يكون لكل فريق من الفرق مهمة محددة فضلا عن إلمامه بمهام زملائه الآخرين ، فطبقا لهذا الاسلوب يتم التركيز على تدريب مجموعة من المتخصصين في مجالات معينة بحيث يلم كل منهم بتخصص الآخرين ، ويزداد في نفس الوقت فهما لتخصصه الاصلي. ويتعين هنا على الفريق أن يخوض تجارب عملية بحيث تعرض عليه عينة من الجرائم المعلوماتية التي تم التحقيق فيها ، على أن يراعى في هذه العينة التنويع لكي تؤدي دورها في إكساب المشاركين في البرنامج التدريبي الخبرة المطلوبة . وهذا الامر يتطلب أن يعهد بالتدريب إلى جهات متخصصة تعنى باختيار المدربين ممن تتوافر لديهم الصلاحية العلمية والفنية والصفات الشخصية ليتولوا التدريب في هذا المجال ، والذي من شأنه تحقيق نتائج طيبة في

1 هشام محمد فريد رستم ، مرجع سابق ص 497

عملية التدريب. والعلمية التدريبية لا بد وأن تكون مستمرة ولا تتوقف عند حد معين ، سيما وان الجرائم المعلوماتية ومنها الجرائم المتعلقة بالإنترنت في تطور مستمر وبشكل سريع جدا.

ليس هذا فحسب بل لا بد وأن تسعى الاجهزة الامنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات في المجال المعلوماتى وضمهم إليها ليكونوا ضمن كوادرها والاستفادة منهم ، ومن أجل ذلك ينبغي على كليات الشرطة من جهة أن تعمل جاهدة لقبول دفعات من الجامعين من خريجي كليات الحاسبات الآلية لتخرجهم ضباطا مؤهلين قانونيا وتقنيا ، كذلك يتعين على الكليات المعينة بتدريس القانون أن تسعى جاهدة إلى تدريس الحاسبات الالية وكل ما يتعلق به إلى الطلبة .وأن تكون مادة الحاسب الآلي وتقنية المعلومات إحدى المواد الاساسية. لأن من شأن ذلك أن تتكون لدي خريجي هذه الكليات ثقافة قانونية وثقافة حاسوبية[1].

الفرع الثاني: مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجزائية

أجهزة العدالة في الكثير من الدول سيما الدول النامية ليست لديها تلك الجاهزية لمواجهة الجرائم المتعلقة بشبكة الإنترنت ومثيلاتها من الجرائم المستحدثة ذات التطور المستمر لعدة أسباب منها الافتقار إلى الموارد الكافية مادية كانت أو بشرية ، أو لأن سلطات التحقيق لديها محدودة أو لأنه لديها قوانين ونظم سبقها الزمن أو قد تفتقر لأي قوانين لتتصدى بها لهذه النوعية من الجرائم .

من هنا و لأننا نعلم أنه ما من دولة يمكنها النجاح في مواجهة هذه الانماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول كانت الدعوة إلى ضرورة وجود تعاون دولي ليس فقط في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين فحسب ، وإنما أيضا في مجال تدريب رجال العدالة ، فتدريب الكوادر البشرية القائمة على إنفاذ القانون ليس بذات المستوى في جميع الدول وإنما يختلف من دولة لأخرى بحسب تقدم

1. هشام محمد فريد رستم ، مرجع سابق ص 499

الدولة ورقيها ،ولو أمعنا النظر في بعض الصكوك الدولية والإقليمية لوجدنا أنها دعت وبصريح النص إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينها .

كما هو الحال في المادة 29 من اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر ا لوطنية2000 م و المادة9 من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر ادود.

والتعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المتعلقة بشبكة الإنترنت قد يكون بين الدول وأجهزة العدالة الجزائية لديها. فعلي الصعيد العربي نجد مثلا أنه هناك اجتماعات تم عقدها في إطار التنسيق بين المعاهد القضائية العربية لتوفير التدريب والتأهيل المناسبين لأعضاء الهيئات القضائية العربية . وقد تمخضت الاجتماعات عن الاتفاق على إعداد مشروع اتفاقية للتعاون بين المعاهد القضائية العربية تسمي اتفاقية عمّان للتعاون العلمي بين المعاهد القضائية العربية والتي وقعت في 9 إبرل1997 م. وفي جمهورية صرالعربية نجد أن النيابة العامة تعقد الكثير من الندوات والمؤتمرات وحلقات النقاش وتشارك فيها سواء عقدت داخل مصر أو خارجها ، بالإضافة انه يتم إرسال أعضاء النيابة من مختلف الدرجات في برامج خارجية وذلك بالتعاون مع أجهزة النيابة العامة في الدول الاخرى والهيئات الدولية بهدف الإطلاع على أحدث النظم المقارنة ، وذات الشيء نجده في سلطنة عمـان. و قد يتم من خلال عقد ندوات ومؤتمرات أو ورش العمل الجماعي متخصصة في مواجهة تلك الجرائم تعقد على المستوى الدولي أو على المستوى الإقليمي ، حيث تقدم هذه الفعاليات العلمية من أبحاثها ودراستها وموضوعات محاورها الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال تحليل ومناقشة أبعادها بعقلية ناجحة مما يمكن المعنيين بالوقاية ومكافحة هذه الجرائم من التعرف على أساليب ارتكابها وأخطارها ووسائل الوقاية والمكافحة بأساليب تتناسب وتفوق أساليب ووسائل مرتكبيها. وعلى هامش هذه المؤتمرات أو

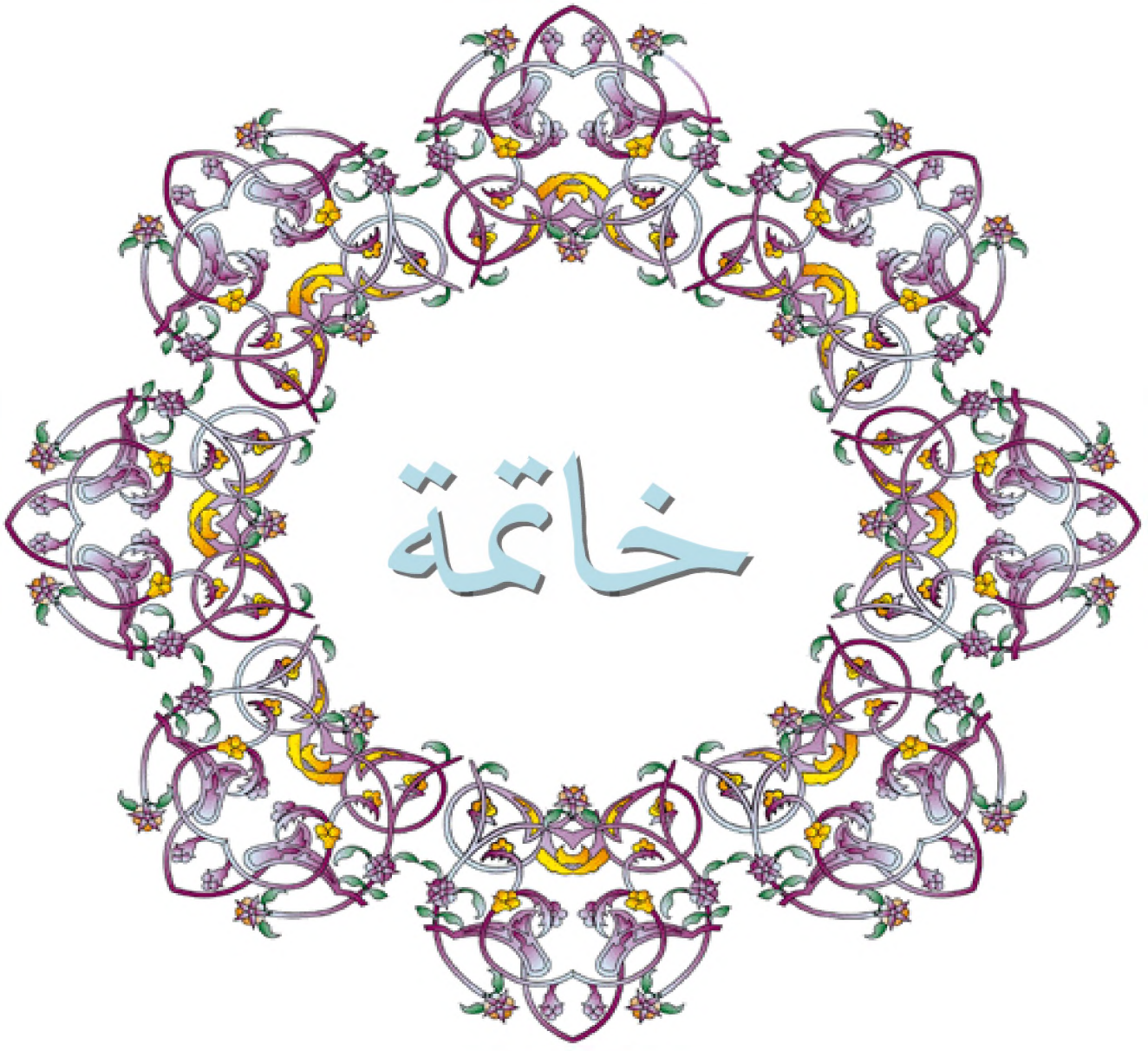
الندوات أو ورش العمل الجماعي تعقد اللقاءات وتبادل الآراء والخبرات. [1]

وقد يتحقق من عقد اللقاءات وحلقات المناقشة المصغرة بين مسؤلي الاتصال بالسفارات أو المكاتب الجغرافية الإقليمية للمنظمات والاجهزة المعنية مع جهات أو أطراف يقعون في دائرة عملهم أو بالقرب منها بناء على رغبة الجهة التي يمثلونها ، يتم خلالها تبادل الآراء والخبرات بين المشاركين . وتمثل كافة هذه اللقاءات وحلقات المناقشة وسيلة طيبة للحوار والمناقشة والتشاور للتعارف وتبادل الرأي والخبرة وطرح الافكار والتصورات وتدارس سبل تنمية وتشجيع التعاون فيما بين الاطراف.

وقد يتحقق عن طريق تنظيم الدورات التدريبية للعاملين في أجهزة العدالة الجزائية والمعنيين بمكافحة الجريمة على المستوى الدولي ، وتعد هذه الصورة اكثر تطورا للتعاون الدولي الذي يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة من خلال تبادل الخبرة ، وطرح موضوعات ومشكلات للتدارس المشترك ، والتعرف على أحدث التطورات في مجال الجريمة سيما المعلوماتية وأساليب مكافحتها ، وغالبا ما يجري تنظيم مثل هذا التدريب من خلال المنظمات أو الدول أو الاجهزة الكبرى ذات مستوى أكثر تقدما يمكن أن يشجع الاطراف الاخرى على المشاركة في هذه البرامج التدريبية ، كما يمكنها تحمل نفقات وأعباء مثل هذه الدورات

وتحقق مثل هذه الدورات والبرامج العديد من الفوائد للجهات المنظمة وللمشاركين فيها ، فالجهة المنظمة يمكنها من خلال عقد مثل هذه البرامج أن تطرح ما تريد من موضوعات حيوية ، كما أنها تعلن عن دورها الرائد لتزيد من ثقة الاطراف الأخرى في أدائها ، بما يشجع على إجراء المزيد من التعاون معها ، وبما يضعها في مكانه خاصة لدى المتدربون والجهات التي يتبعونها. وعلى الجانب الأخر فإن هذه البرامج يمكن أن تفيد متلقي التدريب عن طريق زيادة مهاراته وخبراته ومعلوماته وقدراته على التعامل مع الاجهزة الدولية الاخرى ، الامر الذي ينعكس على الجهة التي ينتمي إليها بالفائدة.

1: محمد السيد عرفة، المرجع السابق، ص5


خاتمة

يتجلى لنا من خلال دراستنا للجريمة المرتكبة عبر الإنترنت أنها من أكثر الجرائم التي عرفها العالم الحديث خطورة، وذ لكلما تتسم به هذه الجريمة من اختلاف عن الجرائم المعروفة في العالم التقليدي،بالإضافة إلى التحديات التي فرضتها على الجهات الخاصة بوضع القوانين وإنفاذها،فإذا كنا قد تناولنا في هذه الدراسة موضوع الجريمة المرتكبة عبر نترنت.فإننا بذلك قد تناولنا مشكلة من مشكلات التي أفرزتها ثورة تصالات،فهذه الثورة كما نعلم على قدر ما قدمته من تسهيلات للأفراد والمجتمعات على حد سواء فقد زعزعت سكينتهم بهذا النوع الجديد من الجرائم التي تتميز بطبيعة فنية وعلم يةمعقدة.

غيرت الجريمة المرتكبة عبر نترنت النظ رةالتقليدية التي كان ينظر بها إ الجر مةعلى العموم. فهذا النوع من الإجرام ظهر معه مفهوم جديد لهذه الظاهرة لم يكن يعرفه ا لقا نون من قبل. فإذا كانت الجرير مةالتقليدية قد حضيت بمختلف الاطر القانونية من أجل تحد يد مفهومها وطبيعتها.فإن الجريمة المرتكبة عبر الإنترن ت لم تنل هذا القدر نالتقنيين، ح يث أن هذه الجريمة اتسمت بخصوصية ميزتها عن الجرائم التقليدية.

تجلت أول خصوصية تمي تبها الجريمة المرتكبة عبر الإنترنت عن الجريمة التقليدية، في صعوبة وضع تعريف موحد لها، فلقد تعددت التعريفات واختلفت في وصف هذه الظاهرة الإجرامية المستحدثة فمنها من ارتكز في تعريفها عل موضوع الجريمة، ومنها من ذهب إلى اعتب ار ضرورة معرفة المجرم بمختلف الطرق التي يتم ارتكاب الجريمة من خلالها أساس لتعري فها،في حين ذهب جانب خر إلى تعريفها على أساس الوسيلة المرتكبة بواسطتها، غير أنهذه التعاريف كلها لـ م تف بالغرض نظرا لعدم إلمامها بمختلف جوانب الجريمة. لهذا ذهب فريق نالفقه إلى دمج كل هذه التعاريف من أجل الوصول إلى تعريف مانع لها، وفي نظرنا يعتبر هذا الرأي الاخير الاقرب إلى الإحاطة بمقتضيات تحديد مفهوم الجريمة.

عتبر كذلك الخصائص التي انفرد تبها الجريمة المرتكبة عبر الإنترنت، من بين ا لعوا مل التي مهدت لها التميز بالخصوصية عن الجريمة التقليدية، حيث تعلقت هذه الخصائص بجميع جوانب الج رمة،مثل طابعها العابر للحدود،وارتكابها في العالم الافتراضي وانعدام ثار

التقليدية لها، بالإضافة إلى ضعف مستوى القائمين على مكافحتها بالنظر إلى التطور المذ سارع في ارتكابها فإن هذه الخصائص تكرس الاختلاف الجوري عن الخصائص العادية للجرائم التقليدية، وكان لها الدور الاكبر في إبرا هذا النشاط الإجرامي كظاهرة إج امية مستحدثة.

أضافت السمات التي يتميز بها المجرم الذي يرتكب جرائمه عبر الإنتر نت الكثير من التميز للجريمة المرتكبة عبر الإنترنت، حيث يعتبر هذا المجر م من الأشخاص اللذين يتمتعون بنسبة عالية من المهار ة والمعرفة والذكاء، فإذا كان المجرم التقليدي يسعى إلى ارتكاب جرائمه في الغالب عن ط ق استعمال العنف، فإن مجرم الإنترنت عتبر مجرم غير عنيف، بل يرتكب جرائمه في هدوء دون أن يلفت النظر إلى الافعال التي يقوم بها، ولقد ساهمت كث ة الا قط ك المستخدمة للانترنت من انتشار هذا النوع من الإجرام وأعطت فرصا للمجرمين من أجل عتداء على أكثر من قطاع في آن واحد، فإن كان المجرم التقليدي ليس بإمكانه الاعتداء على مصالح مختلفة غير موجودة في مكان واحد، فإن مجرم الإنترنت يمكنه الاعتداء على أك ن قطاع عبر مختلف أنحاء العالم وذلك بمجرد انضغط ع زر واحد.

تجلت خصوصية الجرائم المرتكبة عبر الإنترنت أكثر في عدم إمكانية تطبيق احكام الجرائم الت قليد يةعليها، وذلك نظرا للطابع المستحدث لهذه الجريمة ،فإذا كان مثلا تصنيف الجرائم التقليدية لم يتميز بالصعوبة،فإن تصنيف الجرا ئم المرتكبة عبر الإنترنت سـ م بالتشعب وذلك راجع لعدم إمكانية حصر هذه الجرائم في قالب واحد الامر الذي أ ى إلى تعدد التصنيفات والاسس التي بنى عليها.

لم تتو قف إشالات تطبيق أحكام ارائم التقليدية على الجرائم المرتكبة عبر الإنترنت عند هذا الحدّ، بل تعدته إلى تحديد أر ان هذه الجريمة، فإذا كان تحديد أركان الجريمة الت قليد يةواضحا والمتمثلة في الركن المادي والمعنوي والركن الشرعي، فإن تطبيق هذا التحديد عا ر ائم المرتكبة عبر الإنترنت يتسم بصعوبة كبيرة، وذلك في ظل خصوصية هذه الجريمة،حيث يعتبر تحديد القصد الجنائي فيها بالإضافة إلى تحديد السلوك الإجرامي والنتيجة الإجرامية والعلاقة السببية بينهما بالغ الصعوبة، في ظل الطابع العالمي للجرعة

المرتكبةالإنترنت.

ظرتكذلك خصوصية الجريمة المرتكبة عبر الإنترنت أكـ من خلال النصوص القانونية المطبقة عليها. فبروز هذه الظاهر الإجرامية المستحدثة قد أظهر أنهناك قصورا كبيرا في النصوص الجنائية الموضوعية والإجرائية. بحيث أصبحت هذه النصوص عاجزة عن ضمان الحماية اللازمة والفعالة المصالح التي أفرزتها ثورة الاتصالات. فمبدأ شرعية القوانين والعقـ طـ جغير مواكب لهذه الجريمة. لذلك فقد حاولت الشريعات العقابية المختلفة أن تواجه هذه الظاهر الإجرامية الجديدة لمواجهتها. وقام البعض الاخر بإجراء تعديلات على النصوص القائمة لمواكبة هذه الجرا ئمالمتطورة.وهناك تشريعات مازالت تطبق نصوصها التقليدية مع إعطاء القضاء السلطة التقديرية للتوسع في تفسير هذه النصوص لكي تطبق على الجرائم المرتكبة عبر الإنترنت.

جعلت الخصوصية التي نتميز بها الجريمة المرتكبة عبر الإنترنت هـ قلا لدول واليئـ ك والمنظمات الدولية والإقليمية تدرك مىخطورة هذه الظاهر الإجرامية ومدى التحديات التي تفرضها عليها. مما أ ىبها إلى المسارعة من أجل وضعها في إطار قانوني يمكن من خلاله وضع طرق ناجعة وفعالة لمكافحتها. ولقد تمثلت الجهود الدولية في تلك التي بذلها منظمه م المتحدة بمختلف الهيئات التابعة لها. وذلك بعقد المؤتمرات وإبرام المعاهدات بين الدول الاعضاء فيها. والتحسين من مخاطر هذه الظاهر بالإضافة إلى إرشاد ا لدولالمختلفة عن الركب التكنولوجي لكيفية سن قوانينها الداخلية في هذا المجال. دون إغفال الجهود التي تبذلها المنظمة العالمية للملكية للف كرة ا لـ دابت على وضع المناهج لحماية مختل ف المنتجـ ك الف كرة عبر العالم وكذلك جهود مجموع ةالثمانية.

أما فيما يخص الجهود الإقليمية فتمثلت في جهود الاتحاد **الاوربي** الذي يعبر الإطار الانجع لمكافحة الجريمة المرتكبة عبر الإنترنت خاصة بعدإبر ام اتفاقية بودابست سنة2001 والتي وضعت الاسس السليمة التي ينبغي ع دولتحـ ا دوربي الاخذ بها في هذا المجال.بالإضافة إلى جهود الاتحاد وربيهناك جهود تبذل عالمستوى العربي. فبا لرغم من

قلتها إلا أنها تبقى محاولات رائدة في الوطن العر ي خ هةالجهود التي بذل في إطار الجامعة العربية، في انتظار المزيد من الجهود للحد من هذه ا لظ اهرة ولحماية مكـ سبات العالم العربي.

و ا كبالمشرع ازائري ولو بقدر قليل الحركي ةالتشريعية التي فرضت نف سا عالميا،خاصة مع دخول الإنترنت في مختلف مناحي حياة المواطن ازائري، فبعد الفراغ التشريعي الذي كانت تعاني منه الجزائر في هذا المجال سعت لسده في بادئ الامر بتعديل قانون العقوبات وذلك بالقانون رق م04 15، غير محدودية هذا القانون دفع المشرع ا زائر ي إلى إصدار قانو نخ صوالمتمثل في القانون رق م09 04 والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ولم يكن هذين القانونين الوحيدين في هذا المجال بل كانت هناك محاولات أخرى خاصة في قوانين الملكية الفكرية مثل قانون حماية حق المؤلف والحقوق المجاورة، غير أنبالرغم من هذه المحاولات يبقى المشرع الجزائري بعيدا كل البعد عن التطور القانوني على المستوى العالمي من جهة، وعن تطور أساليب ارتكاب الجريمة عبر الإنترنت من جهة أخرى، مما يستلزم مراجعة وتطوير القوانين القائمة وإصدار المزيد من القوانين لتقوية الترسانة القانونية في هذا المجال.

اصطدمت محاولات التصدي للجريمة المرتكبة عبر الإنترنت بعدة صعوبات، فخصوصية الجريمة والسرعةتطورها ا أدىباغلب هذه المحاولات إلى الفشل والدليل على ذلك ما نسمعه عبر وسائل الإعلام المختلفة عن الجرائم الكثة التي مازالتترتكب عبر الشبكة العالمية لـ لإ نت ، حيثعتبر اكتشاف واثبات الجريمة المرتكبة عبر الانترنت من اكثر الصعوبات التي تعترض سلطات إنفاذ القانون، ففي الغالب تكون هذه الجرائم مستترة، وكذلك الامر بالنسبة لإثباتها في ظل الطابع اللامادي للجريمة حيثافتقار هذه الجرائم للدليل المادي يجعل أمر إثباتها غاية في الصعوبة.

تميزت شبكة الإنترنت بتعدي الحدود الوطنية، فهي شبكة عالمية الوجود، وبالتالي كل المعاملات التي تتم عبرها تتصف بهذه الصفة، وحتى الافعال غير المشروعة التي ترتكب عبرها تكتسب هذه الصفة هي الاخرى، ففي ظل هذه الخصوصية ا نثقت عدة إشكالات فيما يخص

التعاون القضائي الدولي وتحديد قواعد الاختصاص، حيث أن التباين الموجود بين قوانين الدول المختلفة جعل من بعض الافعال مجرمة في دولة وغير مجرمة في دولة أخرى، بالإضافة إلى تعدد المعايير واختلافها من دولة إلى أخرى فيما يخص تحديد القانون الواجب التطبيق والمحكمةالمختصة الامر الذي يمنح الفرصة للجاني للإفلات من المتابعة والعقاب.

أخيرا يتجلى لنا أن الخصوصية التي ميزت الجريمة المرتكبة عبر الإنترنت قد استمدتها من الوسيلة التي ترتكب من خلالها ألاوهي الإنترنت حيث أن عالميةالشبكةوافتراضية المعاملات عبرها بالإضافة إلى عدم امتلاك أي جهة لهذه الشبكة أو التحكم بضلالها على الافعال التي ترتكب من خلالها، الأمر الذي يستوجب استحداث قوانين موضوعية وإجرائية تكون خاصة بها سواء على المستوى الوطني أو الدولي تتماشى مع العالم الافتراضي للشبكة الذي يختلف كل الاختلاف عن العالم التقليدي.

وكنتيجة للموضوع يمكن تقديم بعض التوصيات المتمثلة في:

- ضرورة نمو الجهود الدولية لمكافحة جرائم الانترنت من خلال مجموعة تشريعات وطنية واتفاقيات دولية وإقليمية وثنائية.
- الدعوة إلى النظر في التفاوض على اتفاقية دولية تحت مظلة الامم المتحدة وجامعة الدول العربية لمكافحة جرائم الانترنت مع الاخذ في الاعتبار بالجهود الدولية السابقة في هذا المجال ومن أهمها اتفاقية بودابست ودليل الامم المتحدة لمنع الجريمة المتصلة بالحواسب ومكافحتها.
- تنمية وعي الثقافة المعلوماتية للعاملين في مجالات العدالة الجنائية من خلال عقد الندوات المتخصصة والدورات التدريبية لهم في هذا المجال.
- دعوة الدول المتقدمة في المجال المعلوماتي إلى تقديم المساعدات للبلدان التي تحتاجها خاصة البلدان الاقل نموا، لتمكينها من مكافحة هذه النوعية من الجرائم ومن خلال توفير المزيد من برامج التدريب والمساعدة الفنية الاهتمام بعقد الدورات التدريبية التي تعتني بفحص سبل مكافحة جرائم المعلومات وعقد المؤتمرات الدولية

سنويا بصفة دورية.

- العمل على وضع أو إيجاد ضوابط لإلزام مقاهي الانترنت، ومقدمي هذه الخدمة لتسجيل بيانات مستخدمي الشبكة العالمية للمعلومات (انترنت)، وكذا إلزام مسئولي المواقع التي تستخدم البروكسيات بالاحتفاظ بالبيانات الأساسية والحقيقية لمستخدمي مواقعهم على الشبكة.


قائمة المراجع

قائمة المراجع:

أولا: قائمة المراجع باللغة العربية

4 قائمة الكتب :

أ: قائمة الكتب باللغة العربية

1. احمد خليفة الملط، الجرائم المعلوماتية، درلفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006
2. إلياس بن سمير الهاجري "جرائم الإنترنت" الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية ، المملكة المغربية،9 13 افريل 2006
3. جميل عبد الباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة
4. ذياب موسى البداينة،دور الاجهزة الامنية في مكافحة جرائم الإرهاب المعلوماتي ، المملكة المغربية، 2006
5. سالم محمد سليمان الاوجلي : احكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية ، رسالة دكتوراه ، كلية الحقوق جامعة عين شمس 1997م
6. سيناء عبد الله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، الدار البيضاء، المملكة المغربية، 2007
7. صالح بن محمد المسند، عبد الرحمن بن راشد المهيني،جرائم الحاسب للالي الخطر الحقيقي في عصر المعلومات، المجلة العربية للدارسات الامنية و التدريب، المجلد 15، العدد 29،الرياض ، دون سنة
8. طارق إبراهيم ا لدسوقي عطية، الامن لمعلوماتي، النظام القانوني لحماية المعلوماتي، ار الجامعة الجديدة للنشر، الإسكندرية، 2009
9. عباس ابو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الامنية، الرياض، 2007
10. عبد الرحمن جميل محمود حسين، الحماية القانونية لبرامج الحاسب الالي دراسة مقارنة، رسالة ماجستير في القانون ،جامعة النجاح الوطنية، فلسطين، 2008
11. عبد الله بن عبد العزيز اليوسف، اساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الامنية، الرياض، الطبعة الاولى، 2004
12. عبد الله عبد لكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، بيروت، الطبعة الاولى، 2007

13.عبد المحسن بدوي محمد احمد، استراتيجيات و نظريات معالجة قضايا الجريمة و الانحراف في وسائل الإعلام الجماهيري، جامعة نايف العربية، الخرطوم، 2005

14.علي عبد القادر قهوجي،الحماية الجنائية لبرامج الحاسوب الالي،الدار الجامعية للطباعة والنشر ،بيروت، 2000

15.علي عدنان الفيل، الإجرام الإلكتروني، منشورات زين الحقوقية، دون بلد وسنة ، الطبعة الاولى، 2011

16.محمد السيد عرفة، تدريب رجال العدالة واثره في تحقيق العدالة ، جامعة نايف العربية للعلوم الامنية،الرياض 2005

17.محمد دباس لحميد، ماركو إبراهيم نينو، حماية انظمة المعلومات، دار الحامد للنشر وللتوزيع، عمان، الطبعة الاولى، 2007

18.محمد سيد سلطان، قضايا قانونية في امن المعلومات وحماية البيئة الإلكترونية، در ناشري للنشر الالكتروني،2012

19.محمد عبد الرحيم سلطان العلماء،جرائم الإنترنت والاحتساب عليها، جامعة الإمارات العربية المتحدة، كلية الشرعة والقانون، المجلد الثالث، الطبعة الثالثة،2004

20. محمد عبيد الكعيبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة،

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

22. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الالي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001

23.محمود احمد عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، الاردن، 2005

24.مدحت رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهظة العربية

25.مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الاولى، مطابع الشرطة، 2009.

26. مصطفى محمد موسى، اساليب الجريمة بالتقنية الرقمية(ماهيتها، مكافحتها)، دار الكتب القانونية، مصر، 2005

27.موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ،اكاديمية الدراسات العليا، طرابلس.

28.نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الاولى، عمان، 2008

29.هدى قشقوش، جرائم الكمبيوتر و الجرائم الاخرى في مجال التكنولوجيا المعلومات، ملتقى الفكر، 2006

30.يونس عرب،جرائم الكمبيوتر و الانترنت، أبو ظبي، 2002

31.يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها،سلطنة عمان، 2006،

2 قائمة الاطروحات و الرسائل

أ الاطروحات :

1. هشام محمد فريد رستم – الجرائم المعلوماتية " اصول التحقيق الجنائي الفني "- بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة 1 3/5/2000م المجلد الثاني الطبعة الثالثة 2004 م ص 496
2. غازي عبد الرحمن هيان لرشيد، الحماية القانونية من جرائم المعلوماتية(الحاسب و الإنترنت)، اطروحة لنيل شهادة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.
3. عمر بن محمد العتيبي، الامن المعلوماتي في الواقع الإلكترونية ومدى توافقه مع معايير المحلية والدولية، اطروحة لنيل شهادة الدكتوراه الفلسفة في العلوم الامنية، جامعة نايف العربية للعلوم الامنية، الرياض، 2010
4. هدى قشقوش، جرائم الكمبيوتر و الجرائم الاخرى في مجال التكنولوجيا المعلومات، ملتقى الفكر، 2006

ب الرسائل

1. امال قارة ، الجريمة المعلوماتية، رسالة لنيل شهادة ماجستر في القانون ، كلية الحقوق، جامعة الجزائر، 2002،
2. صالح محمد النويجم : تقويم كفاءة العملية التدريبية في معاهد التدريب الامنية بمدينة الرياض من وجهة نظر العاملين فيها رسالة ماجستير في العلوم الإدارية ، جامعة نايف العربية للعلوم الامنية الرياض 2005م

ج المجلات :

1. عارف خليل أبو عيد، << جرائم الإنترنت (دراسة مقارنة) >>، مجلة الشارقة للعلوم الشرعية والقانونية، المجلد 5، العدد 3، الإمارات العربية المتحدة، اكتوبر 2008، ص82
2. كحلوش علي، « جرائم الحاسوب واساليب مواجهتها»، مجلة الشلالة، تصدر عن المديرية العامة للامن الوطني، العدد 84، جويلية 2007.

ثانيا: المراجع باللغة الأجنبية.

المراجع باللغة الانجليزية

1. DEBRAY Stéphane. Internet Face Aux Substances Ilicites : Complice De Ia Cybercriminalité Ou Outil De Prévention? , DESS Média Electronique & Internet, Université De Paris

المراجع باللغة الفرنسية

1. H . Feraud , E.Schlanilz , La Cooperatation Policiere International , R.I.D.P,1974 ,P477-478
2. Chawki Mohamed, *Essai Sur Ia Notion De Cybercnminalité* 2006,P 7.
3. Grave-Raulin Laurent, Règles De Conflits De Juridictions Et Règles De Conflits De Lois Appliquées Aux Cybers Délit, Mémoire De Master 2 Professionnel Droit De L'internet Publique, Université Paris 2_Pantheon Sorbonne, 2008, P6

الفهرس

الفهرس

الإهداء.....
الشكر.....
المقدمة..... 01

الفصل الأول: الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري و المقارن

تمهيد 06
المبحث الأول : ماهية الجريمة المرتكبة عبر الانترنت 07
المطلب الأول : مفهوم الجريمة المرتكبة عبر الإنترنت..... 07
الفرع الأول: التعريف بالجريمة المرتكبة عبر الانترنت..... 08
الفرع الثاني :خصائص الجريمة المرتكبة عبر الانترنت 13
الفرع الثالث: القطاعات التي تستهدفها الجريمة المرتكبة عبر الانترنت..... 18
المطلب الثاني: مجرمي الانترنت..... 22
الفرع الأول : أصناف مجرمي الانترنت 22
الفرع الثاني: سمات مجرمي الانترنت..... 26
الفرع الثالث :دوافع مجرمي الإنترنت 31
المبحث الثاني:تكييف الجريمة المرتكبة عبر الإنترنت..... 34
الفرع الأول : جرائم الانترنت الواقعة على الأموال 36
الفرع الثاني: بعض جرائم الانترنت الماسة بالأشخاص..... 56
الفرع الثالث:جرام واقعة على أمن الدول..... 65
المطلب الثاني: أركان الجريمة المرتكبة عبر الانترنت..... 69
الفرع الأول: الركن الشرعي..... 70
الفرع الثاني: الركن المادي..... 74
الفرع الثالث الركن المعنوي 77

الفصل الثاني : مكافحة الجريمة المرتكبة عبر الانترنت في القانون الجزائري و تشريع المقارن

تمهيد : 79

المبحث الأول: مكافحة و قمع جرائم الانترنت..... 80

المطلب الأول: القوانين المعاقبة على جرائم الانترنت..... 83

الفرع الأول: تشريعات لمكافحة جرائم الانترنت..... 84

الفرع الثاني :الاتفاقيات الدولية..... 94

المطلب الثاني: متابعة جرائم الانترنت..... 98

الفرع الأول:إجراءات متابعة جرائم الانترنت 99

الفرع الثاني:الصعوبات الإجرائية و بعض الهيئات المساعدة..... 119

المبحث الثاني:الجهود الدولية في مواجهة جرائم الإنترنت..... 126

المطلب الأول :التعاون الدولي في مواجهة جرائم الإنترنت..... 126

الفرع الأول : التعاون القضائي..... 128

الفرع الثاني :تسليم المجرمين 133

المطلب الثاني : التعاون الدولي في مجال التدريب على مواجهة الجرائم المتعلقة بالإنترنت 134

الفرع الأول: التدريب وأهميته في مجال مكافحة الجرائم المتعلقة بشبكة الإنترنت 136

الفرع الثاني: مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجزائية 139

خاتمة : 143

قائمة المراجع: 150

الفهرس: 155