وزارة التعليم العالي والبحث العلمي

جامعة مولود معمري – تيزي وزو

كلية الحقوق والعلوم السياسية

مدرسة الدكتوراه " القانون الأساسي والعلوم السياسية "

الجريمة المرتكبة عبر الإنترنت

مذكرة لنيل شهادة الماجستير في القانون

تخصص: القانون الدولي للأعمال

من إعداد الطالب :

صغير يوسف

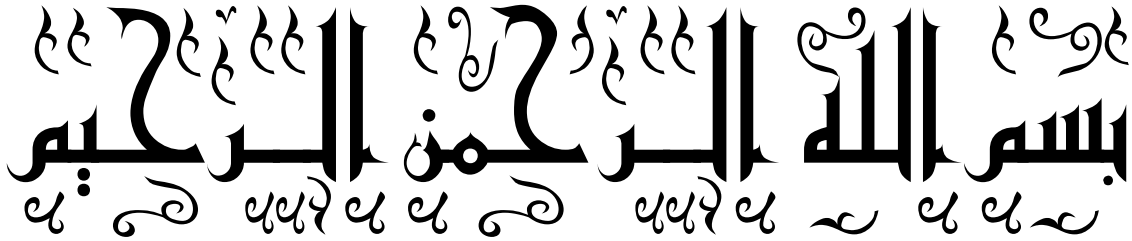
تحت إشراف:

الأستاذ الدكتور: إقلولي محمد

أعضاء لجنة المناقشة:

- د/ جبالي واعمر، أستاذ ، كلية الحقوق، جامعة مولود معمري، تيزي وزو.....رئيسا
- د /إ قلولي محمد، أستاذ ، كلية الحقوق، جامعة مولود معمري، تيزي وزو.....مشرفا ومقررا
- د/ مباركي علي، أستاذ محاضر قسم أ، كلية الحقوق، جامعة مولود معمري، تيزي وزو.....ممتحنا

تاريخ المناقشة : 06 / 03 / 2013


بسم الله الرحمن الرحيم

إهداء

أهدي ثمرة جهدي

إلى روح أمي الطاهرة راجيا من الله أن يسكنها الجنة

إلى من تنحني هامتي له خجلا أبي

إلى من أشد بهم أزري أخي وأخواتي

إلى كل أساتذتي في معهد الحقوق

إلى كل موظفي مكتبة الحقوق والعلوم السياسية

إلى جميع الأصدقاء

يوسف

كلمة شكر وعرفان

يسرني أن أتقدم بجزيل الشكر والعرفان إلى اللجنة الموقرة التي قبلت
مناقشة هذا البحث المتواضع

كما أتقدم بالشكر الجزيل إلى الذي ، شجعني ووقف وراء هذا العمل
المتواضع بمجهوداته ونصائحه القيمة التي أنارت طريقي وقومت مساري
، إلى رمز العلم، العمل والالتزام
أستاذي المشرف الدكتور

"إقلولي محمد"

يوسف

مقدمة:

عرف الإنسان الجريمة منذ أول وجود له على وجه الأرض، وخير دليل عل ذلك جريمة القتل التي وقعت بين ولدي آدم عليه السلام، فالجريمة هي نتاج طبيعي للحياة الجماعية للإنسان، فالتضارب والتباين بين مصالح الأفراد داخل الجماعة أو المجتمع على العموم، يؤدي بطبيعة الحال إلى ظهور منازعات فيما بينهم تنتهي 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 الإجتماعية، وذلك باختلاف الزمان والمكان، فالجرائم التي كانت ترتكب في وقت مضى لم يعد لها وجود في الوقت الحاضر والعكس صحيح، بالإضافة إلى ذلك أن الجرائم 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 الأحيان الديني.

تطورت الجريمة بتطور نمط حياة الإنسان، ولقد بلغ هذا التطور أوجه بظهور المجتمعات بمفهومها المعاصر، حيث أن هذه المجتمعات أصبحت تعيش الكثير من التراكمات ما نتج عنها وقوع الكثير من الجرائم، وذلك جراء الضغوط النفسية وتميز حياة الأفراد بطبيعة براغماتية مادية، حيث أصبح الفرد داخل هذه المجتمعات يسعى بشتى الطرق للوصول إلى إشباع رغباته الشخصية، حتى ولو وصل به الأمر إلى ارتكاب العديد من الجرائم تكون نتائجها وخيمة على الأفراد 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 الآخر بسلام على الإنسانية جمعاء، فالجريمة ومن ورائها المجرمين استغلوا هذا الوضع ليجعلوا للجريمة طابع متعد للحدود.

أدى اكتساب الجريمة للبعد عبر الوطني إلى اعتبارها من الأعمال التي أضحت تهدد الاستقرار والأمن العالميين، نتيجة لتشعبها عبر الحدود الوطنية، وذلك نظراً لظهور أنماط جديدة أو مستحدثة لم يعرفها العالم من قبل، حيث أصبح المجرمون يستغلون مختلف الوسائل التي أنتجها هذا العصر في تطوير وتوسيع نشاطاتهم الإجرامية.

يقف وراء هذا التوسع العديد من العوامل، ولعل في مقدمتها التقدم العلمي في مجال الاتصالات بين الدول على وجه الخصوص، فلقد ألغى التطور في هذا المجال الفواصل بين الدول، وأوجد إحساسا واعيا لدى الشعوب بوهمية الحدود الموضوعية، وبأنها جزء من عالم واحد[1].

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 تأخذ حيزا كبيرا في الحياة اليومية لمعاملات الأفراد والدول على حد سواء شبكة الإنترنت[2].

شملت استعمالات الإنترنت في الآونة الأخيرة مختلف نشاطات الإنسان التجارية بالإضافة إلى مجالات التعليم والترفيه، ولقد أخذت آثارها في البروز بشكل جلي في مجال

---

[1]– **جعفر عبد السلام**، دور التنظيم الدولي في مكافحة الجريمة، مؤتمر الوقاية من الجريمة في عصر العولمة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 6–8 ماي 2001، ص10.

[2]– المراد بالإنترنت هو وجود اتصال بين مجموعة من الحاسبات الإلكترونية (الكمبيوتر)، من خلال شبكة اتصال يطلق عليها Network أي وسيط لنقل المعلومات التي تشارك فيها المنظمات والمؤسسات الحكومية، وغير الحكومية، والأفراد الذين قرروا السماح لآخرين بالاتصال بحواسيبهم، ومشاركتهم المعلومات، وفي المقابل لذلك إمكان استعمال معلومات الآخرين، مع العلم بأنه لا يوجد مالك حصري للإنترنت، وأقرب ما يوصف بالهيئة الحاكمة للإنترنت هو العديد من المنظمات التي تهدف الربح. **عطا عبد العاطي محمد السنباطي**، موقف الشريعة الإسلامية من الإجرام الدولي "**جرائم الحاسب الآلي والإنترنت**"، مؤتمر الوقاية من الجريمة في عصر العولمة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 6–8 ماي 2001، ص287.

الاتصالات، وتبادل الأفكار والمعلومات، بشكل جعل الحدود الجغرافية تنعدم وتتلاشى، ومن خلال هذا النشاط الإنساني عبر شبكة الإنترنت ظهرت الأنشطة الإجرامية عبرها.

في بداية استخدام الانترنت لم يكن أحد من مخترعيها يعلم أنه في يوم من الأيام سوف تستعمل هذه الوسيلة الاتصالية في الإجرام، حيث كان الغرض من اختراعها في بادئ الأمر هو استعمالها في مجالات عسكرية أو بحثية[3]، لكن مع مرور الوقت أصبح يعتمد عليها في مختلف مناحي الحياة، حيث أن تزايد عدد المشتركين من خلالها عبر العالم، يعتبر من بين أكثر الأسباب التي أدّت إلى ظهور هذا النوع من الإجرام، وذلك راجع إلى التباين الموجود بين مستويات ونوايا هؤلاء المشتركين[4].

تطورت الجريمة المرتكبة عبر الإنترنت بشكل رهيب في المدة الأخيرة، وذلك بالنظر إلى التطور المستمر والمتسارع لشبكة الإنترنت، مما جعل هذه الشبكة وسيلة مثالية لتنفيذ العديد من الجرائم بعيدا عن أعين الجهات الأمنية، حيث مكنت الإنترنت العديد من المجرمين والجماعات الإجرامية من القيام بعدة أفعال غير مشروعة مستغلين مختلف التسهيلات التي تقدمها هذه الشبكة وذلك بدون أدنى مجهود وبدون الخوف من العقاب،

---

[3]– شرعت وزارة الدفاع الأمريكية في عام 1969 في بناء أول شبكة معلومات بواسطة الحواسيب الآلية وهو ما يعرف بشبكة ARPANET التي كانت معدة للاستخدام العسكري، ثم تطورت واتسع نطاقها الجغرافي والتطبيقي بدخول الجامعات والمعاهد البحثية، ثم القطاع الخاص، ثم الاستخدام في أغراض التسويق، حتى وصلت الشبكة إلى وضعها الحالي، وتخطى عدد مستخدميها أكثر من 851 مليون مستخدم بنهاية عام 2003 وبزيادة سنوية بحدود 30% وبتغطية لكل دول العالم، **تركي بن عبد الرحمن المويشر**، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة الأمنية، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص3

[4]– سجلت أول حالة اعتداء أمني على شبكة الإنترنت في عام 1988، أي بعد مضي ما يقارب من عشرين عاما على إنشائها، حيث قام روبرت موريس الطالب في جامعة كورنل بتطوير فيروس (عرف لاحقا باسم فيروس موريس) استغل هذا الفيروس ثغرة في نظام البريد الإلكتروني المستخدم آنذاك مكنته من استنساخ نفسه ونقل نسخة إلى عدد كبير من أجهزة الحاسب الآلي المرتبطة بالشبكة، أحدث هذا الفيروس شللا مؤقتا في جميع الأجهزة التي أصابها، وكانت ما يقرب من 10% من مجموع الأجهزة المرتبطة بالشبكة آنذاك، **إياس بن سمير الهاجري**، « **أمن المعلومات على شبكة الإنترنت**»، ندوة حقوق الملكية الفكرية، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص137_138

وهو ما دفع العديد من الدول والهيئات والمنظمات إلى التحذير من خطورة هذه الظاهرة التي تهدد كل مستخدمي الإنترنت حيث، أصبحت من أسهل الوسائل التي يعتمد عليها مرتكبي الجريمة.

سعت المجتمعات إلى الحد من الجريمة المرتكبة عبر الإنترنت، وذلك لما تشكله هذه الظاهرة من إشكالات قانونية واقتصادية واجتماعية معقدة، فكما واكبت المجتمعات تطور الجريمة التقليدية بالتصدي لها وردعها عن طريق سن القوانين والتشريعات، دأبت كذلك على فعل نفس الشيء مع الجريمة المرتكبة عبر الإنترنت، وذلك بالتطرق إليها بالدراسة والتحليل من أجل وضعها في إطار قانوني يمكن من خلاله وضع الطرق السليمة لمكافحتها.

تجسدت بداية مكافحة الجرائم المرتكبة عبر الإنترنت بالتطبيق عليها النصوص القانونية القائمة بمختلف فروعها، وذلك تفاديا لإفلات الجاني من جهة، وعدم وجود قوانين خاصة بهذا النوع من الإجرام من جهة أخرى، غير أن حداثة الجريمة والسرعة في ارتكابها وتطورها جعل هذه القوانين غير مواكبة لها، وبالتالي أضحت غير مجدية في ما يخص مكافحة الجريمة المرتكبة عبر الإنترنت، الأمر الذي أدى بالدول وخاصة المتقدمة منها إلى المحاولة لإيجاد صيغ قانونية يمكن من خلالها الحد من هذه الجرائم المستحدثة.

غير أن الإشكال الذي تأتى من هذه الوضعية هو في أي فرع من فروع القانون يمكن إدماج هذه النصوص، حيث ذهبت تشريعات إلى إدماجها في نطاق قوانين العقوبات بما أن الجريمة تدخل في صلب هذه الأخيرة، وأخرى اعتبرتها قوانين خاصة ليس لها علاقة بالعالم التقليدي، بل هي قوانين موضوعة خصيصا لمواجهة ظاهرة إجرامية مستحدثة لم يعرفها القانون من قبل.

ظهرت في خضم هذا التباين في الرؤى بين التشريعات، اختلافات في دراسات الفقهاء للظاهرة الإجرامية عبر الشبكة العالمية للإنترنت، فهناك جانب من هؤلاء الفقهاء من اعتبر الجريمة المرتكبة عبر الإنترنت هي امتداد للجرائم التقليدية، وذلك باعتمادهم على منظور تطور الجريمة من حيث الزمان، فالجريمة في نظرهم مواكبة لتطور الإنسان

في مختلف مناحي الحياة، وبالتالي أي ظاهرة إجرامية مستحدثة تعتبر امتداد لهذا التطور.

ذهب جانب آخر من الفقه إلى اعتبار الجريمة المرتكبة عبر الإنترنت أنها جريمة مستقلة بذاتها، وذلك بانفرادها بمجموعة من الخصائص والسمات، بالإضافة إلى أن المجرم الذي يقوم بهذه الجرائم يختلف عن نظيره في الجرائم التقليدية، فبالرغم من إمكانية ارتكاب جرائم تقليدية مختلفة مثل السرقة عبر الإنترنت، إلاّ أنها تنفرد بجرائم لم تعرفها التشريعات من قبل، وبالتالي تعتبر الجريمة المرتكبة عبر الإنترنت في نظر أصحاب هذا الرأي أنها جرائم لا علاقة لها بالعالم التقليدي، بل هي 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 المرتكبة عبر الإنترنت مقارنة بالجرائم التقليدية والطرق الفعالة لمكافحتها؟**

ومن أجل الإجابة على 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 لذلك على منهج يجمع بين المقارنة والتحليل.

الفصل الأول

الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت

ظهر الحاسب الآلي كنتاج للتطور العلمي والتقدم التقني، الذي أدى إلى تدخل أنظمة المعالجة الآلية للمعلومات في كافة مجالات الحياة اليومية، نظراً لما يتمتع به الحاسب من قدرة فائقة على تخزين أكبر قدر من البيانات والمعلومات، كما أوجدت الشبكات المعلوماتية وخاصة شبكة الإنترنت واستخدامها في نقل وتبادل المعلومات فجرا جديدا تمثل في بروز ما اصطلح على تسميته بالمجتمع المعلوماتي[5].

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[6].

انفراد الجريمة المرتكبة عبر الإنترنت بطبيعة خاصة بها، والتي استمدتها من الوسيلة التي ترتكب بها ألا 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)**.

---

[5]– **غازي عبد الرحمن هيان الرشيد**، ، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص92.

[6]– *La technologie est mise au point pour pouvoir être utilisée mais il est aussi très fréquent qu'elle soit mal employée voire employée abusivement. En général, la cybercriminalité porte sur l'usage illicite des technologies de l'information et des communications.* Voir : **KURBALIJA Jovan, GELBSTEIN Eduardo,** Gouvernance de l'internet **–** enjeux, acteurs et fractures, publié par diplofoundation et global knowledge partnership, Suisse, 2005, p 98.

المبحث الأول
ماهية الجريمة المرتكبة عبر الإنترنت

تعتبر الجريمة المرتكبة عبر الإنترنت من الآثار السلبية التي خلفتها التقنية العالية، حيث أخذت هذه الظاهرة 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[7]، ويعتبر 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 إلى ظهور عدة نظريات في علم الإجرام، ومن بين أهمها تلك المتعلقة بطبيعة المجرم، فعلى سبيل المثال التطور الذي عرفته الجريمة الاقتصادية نتج عنها ظهور أفراد الجريمة المنظمة، وبالتالي أصبح من الطبيعي ظهور نظريات جديدة تواكب التطور في مجال الاتصالات وخاصة شبكة الإنترنت، والتي أظهرت فئات جديدة تختلف عن الفئات الإجرامية التقليدية والمتمثلة في فئة مجرمي الإنترنت **(المطلب الثاني)**.

المطلب الأول
مفهوم الجريمة المرتكبة عبر الإنترنت

عرفت الجريمة بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدبيراً احترازياً، وتعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت على المعلومة بشكل رئيسي، وهذا الذي أدّى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم[(8)]، والتي كانت هناك اتجاهات مختلفة في تعريفها **(الفرع الأول)**، كما اتسمت بمجموعة من الخصائص والسمات التي

---

[7]– **DEBRAY Stéphane**, Internet face aux substances illicites : complice de la cybercriminalité ou outil de prévention ?, DESS média électronique & Internet, Université de Paris 8, 2002-2003, p 08.

[8]– **محمد عبيد الكعبي**، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ص32.

ميزتها عن غيرها من الجرائم **(الفرع الثاني)**، خاصة من ناحية تباين القطاعات المستهدفة من خلالها **(الفرع الثالث)**.

الفرع الأول

التعريف بالجريمة بالمرتكبة عبر الإنترنت

أدت الحداثة التي تتميز بها الجريمة المرتكبة عبر الإنترنت، واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحّد للدلالة عليها، وعدم الاتفاق هذا انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية وذلك خشية حصرها في مجال ضيق[9]،ولذلك نجد الفقه قد انقسم إلى أربعة اتجاهات تقوم على أسس مختلفة في تعريف الجريمة المرتكبة عبر الإنترنت وهي[10]:

أولاً: على أساس وسيلة ارتكاب الجريمة

تعتمد هذه التعريفات على وسيلة ارتكاب الجريمة، فطالما أن وسيلة ارتكاب الجريمة هو الحاسوب أو إحدى وسائل التقنية الحديثة المرتبطة به فتعتبر من جرائم الإنترنت[11]، ومن ذلك تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً[12].

---

[9]– **محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص43.

- il n'existe pas de définition universelle pour le terme cybercriminalité. Celui-ci est utilisé généralement pour décrire l'activité criminelle dans laquelle le système ou le réseau informatique est une partie essentielle du crime. Il est également employé pour décrire des activités criminelles traditionnelles dans lesquelles les ordinateurs ou les réseaux sont utilisés pour réaliser une activité illicite. Dans le premier cas, les technologies sont la cible de l'attaque. Dans le second, elles en sont le vecteur. Voir : **EL AZZOUZI Ali,** La cybercriminalité au Maroc, Bishops solution, Casablanca, 2010, p 17.

[10]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص106.

[11]– *la définition de la cybercriminalité met l'accent sur la méthode - par exemple l'accès non autorisé à des systèmes informatiques sécurisés - on court le risque de confondre la cybercriminalité avec l'hacktivisme (désobéissance civile numérique).*Voir : **KURBALIJA Jovan, GELBSTEIN Eduardo,** op-cit, p 99, voir aussi :

- **CHERNAOUTI-HELI Slange**, « Comment lutter contre la cybercriminalité ? » ; revue la Science, n° 391, Mais 2010, p 24

[12]– **محمد عبيد الكعبي**، المرجع السابق، ص33.

عرّف بعض الفقه [13] الجريمة المرتكبة عبر الإنترنت بأنّها:

« ***هي نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسوب الآلي الرقمي وشبكة الانترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف*** ». [14]

بصياغة أخرى عرفها البعض الآخر [15] بأنها:

« ***جرائم الانترنت تعني جرائم الشبكة العالمية التي يستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة مثل استخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب***».

تعرف جرائم الإنترنت أنّها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالكمبيوتر والإنترنت في أعمال وأنشطة إجرامية بهدف أن تحقق عوائد مالية ضخمة يعاد ضخّها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الإلكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الإنترنت أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة، وقد عبر خبراء المنظمة الأوروبية للتعاون الاقتصادي عن جريمة الإنترنت بأنّها كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها[16].

---

[13]– **مصطفى محمد موسى**، أساليب إجرامية بالتقنية الرقمية(ماهيتها، مكافحتها)، دار الكتب القانونية، مصر، 2005، ص56.

[14]– **كحلوش علي**، « **جرائم الحاسوب وأساليب مواجهتها** »، مجلة الشرطة، تصدر عن المديرية العامة للأمن الوطني، العدد 84، جويلية 2007، ص51. أنظر كذلك:

- **EL AZZOUZI Ali,** op-cit, p 43.

[15]– **مصطفى محمد موسى**، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009، ص112، *أنظر كذلك*: **عبد الجبار الحنيص**، « **الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي- دراسة مقارنة-**»، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27، العدد الأول، 2011، ص190.

[16]– **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2007، ص15.

تعتبر جرائم الإنترنت من هذا المطلق أيّ فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية، أو بمعنى آخر هي كل فعل غير مشروع يكون علم تكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه[17]، ويعتبر هذا التعريف بالغ العمومية والاتساع، لأنه يدخل فيه كل سلوك ضار بالمجتمع يستخدم فيه الحاسب الآلي[18].

لقي تعريف الجريمة المرتكبة عبر الإنترنت المعتمد على الوسيلة المستخدمة في ارتكابها، عدة انتقادات مفادها أن تعريف الجريمة يستوجب الرجوع إلى الفعل والأساس المكون لها وليس إلى الوسائل المستخدمة لتحقيقها فحسب، أو لمجرد أن الحاسب استخدم في جريمة يتعين أن نعتبرها من جرائم الإنترنت[19].

يرُد في هذا الإطار الأستاذ R_Fanderson على واضعي هذا التعريف بقوله: "**ليس لمجرد أن الحاسب قد استخدم في الجريمة أن نعتبرها من الجرائم المعلوماتية**"، والحجة التي اعتمد عليها منتقدي هذا التعريف مفادها أنّه لا يمكن وضع تعريف لهذا النوع من الجرائم دون الرجوع إلى العمل الأساسي المكون لها[20]، أي بمعنى آخر لكي تعرف الجريمة يجب الرجوع إلى العمل الأساسي المكون لها، وليس فقط إلى الوسائل المستخدمة لتحقيقها، ويترتب على ذلك أنّه لا يكفي أن نعتبر مجرد استخدام الحاسب الآلي في الجريمة، أنّها من جرائم الإنترنت[21].

---

[17]– **عارف خليل أبو عيد**، « **جرائم الإنترنت (دراسة مقارنة)** »، مجلة الشارقة للعلوم الشرعية والقانونية، المجلد 5، العدد 3، الإمارات العربية المتحدة، أكتوبر 2008، ص82.

[18]– **عمر بن محمد العتيبي**، الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة مقدمة استكمالاً لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، الرياض، 2010، ص21

[19]– **محمد عبيد الكعبي**، المرجع السابق، ص34

[20]– **قارة آمال**، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2002، ص19.

[21]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص107

ثانياً: على أساس توافر المعرفة بتقنية المعلومات

يستند أنصار هذا الاتجاه إلى معيار شخصي الذي يستوجب أن يكون فاعل هذه الجرائم ملما بتقنية المعلومات[22]، ومن بين هذه التعريفات نجد تعريف وزارة العدل في الولايات المتحدة الأمريكية التي عرفت الجريمة المرتكبة عبر الإنترنت بأنّها:

« ***أية جريمة لفاعلها معرفة فنية بتقنية الحاسبات يمكنه من ارتكابها*** » [23]،ومن قبيل هذا التعريف جاء تعريف الأستاذ "David Thomson" لجريمة الإنترنت بأنّها:

«أيّة جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب» [24].

عرّفها كذلك بعض من الفقه على أنها: « **ذلك النوع من الجرائم التي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها** » [25]

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.[26]

اقتصار تعريف الجريمة المرتكبة عبر الإنترنت على شخصية الفاعل الذي لابد أن يكون لديه إلمام بالتعامل مع تقنية أجهزة الحاسب لآلي يعتبر قاصرا، إذ لابد الأخذ

22– **محمود أحمد عبابنة**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005، ص 16.

23– **محمد عبيد الكعبي**، المرجع السابق، ص34.

24– **هشام محمد فريد رستم**، « **الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي** »، بحوث مؤتمر القانون والكمبيوتر والإنترنت، من 1–3 ماي 2000،جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة 2004، ص407

25– المخاطر الأمنية للإنترنت، مقال متوفر على الموقع التالي www.minchawi.com

– عرّفها البعض كذلك على النحو التالي: « **جريمة الإنترنت هي الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني** » أنظر في هذا التعريف: **محمد عادل ريان**، « **جرائم الحاسب الآلي وأمن البيانات** »، متوفر على الموقع التالي www.anaharonline.com

26– أنظر في ذلك المحاضرة التي ألقيت من طرف **بورزام أحمد**، وكيل الجمهورية لدى محكمة باتنة، تحت عنوان (جرائم المعلوماتية)، بالمجلس القضائي بباتنة، يوم 20 جوان 2006، ص7.

بالاعتبارات أخرى والمتعلقة بموضوع الجريمة[27]، حيث أن قصور هذا التعريف واضح إذ أن مجرد توافر المعرفة التقنية بعلم ما لا يكفي في ضوء عدم توافر العناصر الأخرى لتصنيف الجريمة ضمن الجرائم المتعلقة بذلك العلم[28].

ثالثا: على أساس موضوع الجريمة

يرى واضعو هذا التعريف أن الجريمة المرتكبة عبر الإنترنت ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه[29]، ومن أشهر فقهاء هذا الاتجاه الفقيه "rosenblatt" الذي عرف جريمة الإنترنت بأنّها:

« ***نشاط غير مشروع موجه لنسخ، أو تغيير أو حذف، أو للوصول إلى المعلومات المخزّنة داخل الحاسب، أو التي تحول عن طريقه*** » [30].

كما عرفت الجريمة المرتكبة عبر الإنترنت كذلك على النحو التالي:

« ***الجريمة المرتكبة عبر الإنترنت هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيداً من الناحية التقنية مثل تعديل الكمبيوتر*** ». [31]

---

[27]– **منصور بن صالح السلمي**، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2010، ص63

[28]– **محمد عبي الكعبي**، المرجع السابق، ص34

[29]– **أحمد خليفة الملط**، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006، ص85–86، *أنظر كذلك*: **محمد علي العريان**، المرجع السابق، ص45، *أنظر كذلك*: **محمد حماد مرهج الهيتي**، جرائم الحاسوب ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، دار المناهج للنشر والتوزيع، الأردن، الطبعة الأولى 2006، ص78

[30]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص106

[31]– **يونس عرب**، « **جرائم الكمبيوتر والأنترنت(إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات)**»، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10–12 فيفري، 2002، ص8.

– من أنصار هذا المذهب لدى الفقه العربي الدكتورة "هدى قشقوش" التي عرّفت بدورها الجريمة المرتكبة عبر الإنترنت على النحو التالي: « **كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه=**

سايرت منظمة الأمم المتحدة هذا الاتجاه، حيث وصفت الجريمة المرتكبة عبر الإنترنت بأنّها:

« كل تصرف غير مشروع من أجل القيام بعمليات إلكترونية تمس بأمن الأنظمة المعلوماتية والمواضيع التي تعالجها ». [32]

رابعا: اتجاه يأخذ بدمج عدة تعاريف

نظرا لعدم نجاح الاتجاهات السابقة بوضع تعريف شامل للجريمة المرتكبة عبر 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 الآلي كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيتها » [33].

أجرت منظمة التعاون الاقتصادي والتنمية استبيان حول تعريف الجريمة المرتكبة عبر الإنترنت، الذي تم توزيعه على دول الأعضاء، ولقد ورد في الإجابة البلجيكية، بأنها هي:

« كل فعل أو امتناع، من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة، أو غير مباشرة عن تدخل التقنية المعلوماتية » [34].

وفي تعريف آخر لمنظمة التعاون الاقتصادي للجريمة المرتكبة عبر الإنترنت بأنها:

« كل سلوك غير مشروع، أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها » [35].

=**البيانات** » أنظر في ذلك: **محمود أحمد عبابنة**، المرجع السابق، ص16. *وكذلك:* **دويب حسين صابر**، « **القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع**»، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، الرياض، أيام 6 و7 أفريل 2010، ص2.

[32] - **CHAWKI Mohamed,** « *Essai sur la notion de cybercriminalité* », juillet 2006, p7, Disponible sur le site : http://www.iehei.org

[33] – **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص108-109

[34] – **هشام محمد فريد رستم**، المرجع السابق، ص409

تعرضت هذه التعاريف لعدة انتقادات بسبب عدم دقتها في تحديد تعريف الجريمة المرتكبة عبر الإنترنت، إذ يكفي وفقا لهذه التعاريف أن يكون السلوك غير اجتماعي أو غير أخلاقي أو ضد المجتمع حتى يمكن اعتباره من قبيل جرائم الإنترنت، كما أن هذه التعاريف تعتمد وصف الجريمة لا تحديد ماهيتها، ولا تتسع للعديد من الصورة الجرمية الممكن اقترافها، ووصف الجريمة لا يعد من المعايير المنضبطة الكافية، لاعتمادها أساسا لتحديد ماهية الفعل الجرمي[36].

بالرغم من الانتقاد الذي وجه لهذا التعريف إلاّ أنه يبقى الأنجع من الناحية العملية، حيث في حين اعتمدت التعاريف الأخرى في تعريفها للجريمة المرتكبة عبر الإنترنت على معيار واحد، إذ ذهب واضعو هذا التعريف إلى الاعتماد على دمج كل هذه المعايير، مما يعطيه صفة الكمال ولو نسبيا، في انتظار أن يأتي الفقه بتعريف أكثر شمولاً.

الفرع الثاني

خصائص الجريمة المرتكبة عبر الإنترنت

تعتبر الجريمة المرتكبة عبر الإنترنت من بين الجرائم 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 العالم من قبل، وسوف نبين هذه الخصائص التي ميزت الجريمة المرتكبة عبر الإنترنت على النحو التالي:

أولا: خفاء الجريمة وسرعة التطور في ارتكابها

تتسم الجرائم الناشئة عن استخدام الإنترنت بأنها خفية ومستترة في أغلبها، لأنّ الضحية لا يلاحظها رغم أنّها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات

---

[35]– **يونس عرب**، صور الجرائم الإلكترونية واتجاهات تبويبها، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، 2–4 أفريل 2006، ص7

[36]– **محمود أحمد عبابنة**، المرجع السابق، ص19

فنية تمكنه من جريمته بدقة، مثلا عند إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم[37].

فجرائم الإنترنت في أكثر صورها خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أمر ليس في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبيها[38].

يستفيد المجرمين في مختلف من الشبكة في تبادل الأفكار والخبرات الإجرامية في ما بينهم، ويظهر لنا ذلك جليا في مختلف المواقع الإلكترونية ومنتديات القراصنة (الهاكرز)[39] ، التي تضمن لهم الاتصال فيما بينهم من أجل تبادل المعارف والخبرات في مجال القرصنة وذلك من أجل ارتكابهم لجرائمهم بعيدا عن أعين الأمن[40].

تجدر الإشارة في هذا الصدد أن الجريمة المرتكبة عبر الإنترنت أسرع تطورا من التشريعات، وذلك راجع إلى التطور التكنولوجي الهائل والمتسارع والذي تجسده شبكة الإنترنت، بالإضافة إلى مختلف المؤتمرات التي يعقدها القراصنة والتي تسمح لهم بابتكار وسائل وطرق غاية في التعقيد لم تعرفها التشريعات من قبل وذلك من أجل ارتكابهم لجرائمهم.

---

[37]– **محمد عبيد الكعبي**، المرجع السابق، ص32

[38]– **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص20

[39]– لمزيد من المعلومات أنظر ص26 من هذا بحثنا

[40]– يقوم صغار نوابغ المعلوماتية بإقامة مؤتمرات يتبادلون فيها المعلومات والمهارات وكان أول مؤتمر قد حدث سنة 1990 بأوروبا، حيث اجتمع في هذا المؤتمر مراهقون من كل أنحاء العالم ليشاركوا في أفكارهم ويعلموا بعضهم البعض كيف يقتحمون أنظمة الحواسيب في الدول الأخرى، وتنمية مهاراتهم واكتساب الخبرة، ومنذ ذلك الحين تكررت اقامة مؤتمرات أخرى خاصة في الولايات المتحدة الأمريكية وبالتحديد في مدينة لاس فيجاس الأمريكية، حيث ينعقد سنوياً مؤتمر يسمىDEF CON الذي يجمع المراهقين من أنحاء العالم سنوياً ضمن أكبر التجمعات التي تقلق خبراء أمن المعلومات والحكومات على حد سواء أو يسمح هذا التجمع المريب للقراصنة بتبادل المعلومات والشفرات الخبيثة مما يؤدي إلى تكوين شبكات من القراصنة تمتد في جميع أنحاء العالم. *أنظر في هذا:* **أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار نشر، 2005، ص26

ثانيا: اعتبارها أقل عنفا في التنفيذ

لا تتطلب جرائم الإنترنت عنفا لتنفيذها أو مجهودا كبيرا، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة[41].

تتميز جرائم الإنترنت بأنها جرائم هادئة بطبيعتها لا تحتاج إلى العنف[42]، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية(الإنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين، فمن هذا المنطلق تعد الجريمة المرتكبة عبر الإنترنت من الجرائم النظيفة فلا آثار فيها لأية عنف أو دماء وإنما مجرد أرقام وبيانات يتم تغييرها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي[43]

ثالثا: جريمة عابرة للحدود

بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدّت إلى نتيجة مؤدّاها أنّ أماكن متعددة في دول مختلفة قد تتأثّر بالجريمة المعلوماتية الواحدة في

41– **ذياب موسى البداينة**،« **دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي** »، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية، المنعقدة بكلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية، أيام 9-13 أفريل 2006، ص20.

42– **عباس أبو شامة عبد المحمود**، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص52.

43– **سيناء عبد الله محسن**، « **المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية** »، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، الدار البيضاء، المملكة المغربية، 10-20 يونيو 2007، ص52.

آن واحد[44]، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى[45]، وذلك راجع إلى أنّ مجتمع المعلومات لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود.[46]

هذا وقد لا يقتصر الضرر المترتب عن الجريمة على المجني عليه وحده وإنّما قد يتعداه إلى متضررين آخرين في دول عدّة، وهذا هو الملاحظ من خلال جرائم نشر المواد ذات الخطر الديني أو الأخلاقي أو الأمني أو السياسي أو التربوي أو الثقافي أو الاقتصادي، لذلك فإنّه يجب إيجاد تعاون دولي لمكافحة هذه الجرائم عن طريق المعاهدات والاتفاقيات الدولية[47]

نتج عن الطبيعة التي تتميز بها الجريمة المرتكبة عبر الإنترنت بأنها جريمة لا حدود لها العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه[48]، بالإضافة إلى إشكاليات تتعلق

---

[44] –**MASCALA Corinne**, « *criminalité et contrat électronique* », IN : Le contrat électronique, Travaux de l'association CAPITANT Henri, journées national, Paris, 2000, p 119.

[45]– **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2008، ص51.

[46]– **المرجع نفسه**، ص50.

[47]– **محمد عبيد الكعبي**، المرجع السابق،ص37.

[48]– كانت القضية المعروفة باسم مرض نقص المناعة المكتسبة (الإيدز) من القضايا التي لفتت النظر إلى بعدها الدولي للجرائم المعلوماتية، وتتلخص وقائع هذه القضية التي حدثت عام 1989 في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة) إذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس، وفي الثالث من فبراير من عام1990 تم إلقاء القبض على المتهم "جوزيف بوب" في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي حيث إن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه إحدى عشر تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلاّ أنّ إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية. ومهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين:

بإجراءات الملاحقة القضائية [49]وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.[50]

رابعا: امتناع المجني عليهم عن التبليغ

لا يتم في الغالب الأعم الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، لذا نجد أنّ معظم جرائم الإنترنت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة، والعدد الذي تم اكتشافه، هو رقم خطير، وبعبارة أخرى، الفجوة بين عدد هذه الجرائم الحقيقي وما تم اكتشافه فجوة كبيرة[51].

تتبدى 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 إلى تضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها[52].

خامسا: سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه

تكون البيانات والمعلومات المتداولة عبر شبكة الإنترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تقرأ إلاّ بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا لا سيما وأن الجاني

الأولى: أنّها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية.

الثانية: أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة برنامج خبيث(فيروس)، أنظر ***نهلا عبد القادر المومني***، مرجع سابق، ص51-52

[49]- **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

[50]- **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص19

[51]- **محمد صالح العادلي**، « **الجرائم المعلوماتية(ماهيتها وصورها)** »، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، 2-4 أفريل 2006، ص7.

[52]- **هشام محمد فريد رستم**، المرجع السابق، ص432

يتعمد إلى عدم ترك أثر لجريمته[53]، 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.(54)

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

يعيق المجرم في جرائم الإنترنت سلطات التحقيق الوصول إلى الدليل بشتى الوسائل، كمسح برامج أو وضع كلمات سرية ورموز وقد يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه(55).

يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم ذلك عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب، على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما إن يحس الجاني بانّ أمره سينكشف حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبها أمراً في غاية الصعوبة(56).

سادسا: نقص الخبرة لدى الأجهزة الأمنية والقضائية وعدم كفاية القوانين السارية

تتميز جرائم الإنترنت بالكثير من السمات التي جعلتها تختلف عن غيرها من الجرائم، الأمر الذي أدّى إلى تغيير شامل في آلية التحقيق وطرق جمع الأدلّة المتبعة

53- **EL AZZOUZI Ali,** op-cit, p 20.

54- **محمد عبيد الكعبي**، المرجع السابق، ص38

55- **محمد عبد الرحيم سلطان العلماء، « جرائم الإنترنت والاحتساب عليها »**، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 1-3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، الطبعة الثالثة، 2004، ص877

56- **موسى مسعود أرحومة، « الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية »**، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص3

من الجهات التي تقوم بعملية التحقيق، وإضافة أعباء تتعلق بكيفية الكشف عن هذه الجريمة وأدلتها، وكذا القضاء من خلال تعديل الكثير من مفاهيمه التقليدية سواءً فيما يتعلق بالأدلة أو تطبيقاتها أو لقوتها في الإثبات.[57].

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

لم تعد قادرة القوانين التقليدية على مواكبة هذه السرعة الهائلة في التكنولوجيا، والتي أدّت إلى تطور الجريمة من خلالها، وظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها[58]، مما تطلب تدخل المشرّع لسن قوانين حديثة لمواجهة هذه الجرائم حفاضا على مبدأ الشرعية الجنائية، مع تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها[59].

الفرع الثالث

القطاعات التي تستهدفها الجريمة المرتكبة عبر الإنترنت

دخلت مختلف القطاعات إلى عالم المعلوماتية خاصة بعد ظهور الإنترنت، نظرا للخدمات الكبيرة التي تقدمها، وخاصة باعتبارها تضمن السرعة وتقليص الوقت والتكاليف، إلا انه بالمقابل أصبحت عرضة لكي تكون ضحية من ضحايا الجريمة المرتكبة عبر الإنترنت، ونذكر من بين هذه القطاعات، القطاع المالي والمؤسسات العسكرية إلى جانب الأشخاص الطبيعيين.

---

[57]– **عبد الرحمن جميل محمود حسين**، الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة، رسالة قدمت استكمالاً لمتطلبات درجة الماجستير في القانون الخاص بكلية الدراسات العليا في جامعة النجاح الوطنية، فلسطين، 2008، ص58

[58]– **محمد عبيد الكعبي**، المرجع السابق، ص40.

[59]– **محمد عبد الرحيم سلطان العلماء**، المرجع السابق، ص878.

أولا: المؤسسات المالية والاقتصادية

بدأ مفهوم التجارة الإلكترونية لسهولة الاتصال بين الطرفين ولإمكانية اختزال العمليات الورقية والبشرية فضلا عن السرعة في إرسال البيانات وتخفيض تكلفة التشغيل والأهم هو إيجاد أسواق أكثر اتساعا، ونتيجة لذلك فقد تحولت العديد من شركات الأعمال إلى استخدام الإنترنت والاستفادة من مزايا التجارة الإلكترونية، كما تحول تبعا لذلك الخطر الذي كان يهدد التجارة السابقة ليصبح خطراً متوافقاً مع التجارة الإلكترونية، فالاستيلاء على بطاقات الائتمان عبر الإنترنت أمرا ليس بالصعوبة بما كان في سابقه[60].

اتجهت كثير من الشركات الكبيرة والصغيرة على حد سواء وخصوصا في الدول المتقدمة إلى إنشاء مواقع لها على شبكة الإنترنت بغرض الدعاية والإعلان وعرض منتجاتها وخدماتها، أمام ملايين البشر متعدية بذلك حواجز الحدود الإقليمية وتفتح أبواب معارضها للزائرين طوال الأربع والعشرين ساعة وفي كل أيام الأسبوع، ويوفر استخدام الإنترنت في المعاملات التجارية والنقدية إضافة إلى سعة الانتشار خفض العمالة والتكلفة، حيث تصل تكلفة إنجاز العمليات التجارية عبر الإنترنت في بعض الأحيان إلى خمسة بالمائة فقط من تكلفة إنجازها بالطرق التقليدية.[61]

أصبح الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال والأعمال، مما يجعل هذه الشبكات نظراً لطبيعتها المترابطة، وانفتاحها على العالم، هدفا مغريا للمجرمين، ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل ملموس بالانطباعات السائدة والتوقعات، والتشكيك في صحة هذه المعلومات أو تخزينها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة، وإضعاف الثقة في النظام الاقتصادي.

---

[60]- **صالح بن سعد الصالح، « مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي، الدورة التدريبية مكافحة الجرائم الاقتصادية »** ، كلية التدريب، قسم البرامج لتدريبية، الرياض، 10-2007/3/14، ص17.

[61]- **صالح بن محمد المسند، عبد الرحمن بن راشد المهيني، « جرائم الحاسب للآلي الخطر الحقيقي في عصر المعلومات »**، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 29، الرياض، دون سنة نشر، ص172

يشمل هذا الوضع إحداث خلل واسع في نظم الشبكات التي تتحكم بسريان أنشطة المصارف وأسواق المال العالمية، ونشر الفوضى في الصفقات التجارية الدولية، إضافة إلى ذلك يمكن إحداث توقف جزئي أو كلي في منظومات التجارة والأعمال، بحيث تتعطل الأنشطة الاقتصادية وتتوقف عن العمل.[62]

ثانيا: الأشخاص الطبيعيون

أصبح الأشخاص الطبيعيون يعتبرون أكثر ضحايا الجرائم المرتكبة عبر الإنترنت، وذلك راجع إلى التزايد المستمر والكبير في أعداد المشتركين من خلال الشبكة العالمية للإنترنت، فلم تعد الجرائم المرتكبة عبر الإنترنت مقتصرة على القطاعات المالية والعسكرية، وبالتالي فإن كثيرا من الأشخاص يتعرضون لجرائم النصب والسرقة والإتلاف ومن الطبيعي أن تكون شبكة الإنترنت المجال الخصب لارتكاب تلك الجرائم، حيث أصبحت ملايين الأسرار المتعلقة بالناس سواء كانوا أفراد عاديين أو في مراكز معينة في متناول كل من يستطيع اختراق شبكة المعلومات التي تنطوي على كل هذه الأسرار[63].

تعتبر جرائم الإتلاف عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر البريد الإلكتروني الذي يعتبر من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الأشخاص وتعتبر من أكثر الجرائم التي يتعرض لها الأشخاص أيضا سرقة أرقام بطاقات الائتمان.

يتعرض كذلك الأشخاص لجرائم النصب على شبكة الإنترنت وخير مثال على ذلك وقوع الكثير من الشعب الأمريكي ضحية لجريمة النصب من قبل أشخاص مستغلين الحادث الإرهابي الذي حدث في الولايات الأمريكية المتحدة في الحادي عشر من سبتمبر سنة 2001، حيث قامت العديد من الجهات بإنشاء عدة مواقع على شبكة الإنترنت

---

[62]- **علي عدنان الفيل**، الإجرام الإلكتروني، منشورات زين الحقوقية، دون بلد وسنة نشر، الطبعة الأولى، 2011، ص92-93

[63]- **محمد محمد شتا**، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001، ص94

بغرض جمع التبرعات للضحايا، وعلى هذا الأساس قامت حكومة الولايات المتحدة الأمريكية بتحذير رعاياها من الوقوع ضحايا لتلك العمليات الإجرامية[64].

تشكل المعالجة الآلية للبيانات الشخصية خطورة أكثر على الحياة الخاصة إذا كانت هذه البيانات منظمة ومرتبطة بشبكة الإنترنت أين يمكن لكل مستعمل للإنترنت الإطّلاع عليها وحتى بوجه غير مشروع.[65]

تعد جريمة انتهاك الحياة الخاصة من بين الجرائم الأكثر شيوعا عبر الإنترنت والتي يتعرض لها الأشخاص 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 مثلاً، كذلك فإن نقل أو تسجيل المحادثات الخاصة تعد من الجرائم التي تمس الحياة الخاصة، فبعد ظهور الإنترنت بات من المتيسر اختراق هذه الوسائط والتنصت عليها وتسجيلها[66].

ثالثا: المؤسسات العسكرية

لم تقتصر حدود ثورة المعلومات على القطاع المدني بل كان لها أكبر الأهمية في تطوير أنظمة الحرب الحديثة وأدت إلى ظهور ما يسمى بحرب المعلومات، حيث يستهدف هذا النوع من الإجرام الأهداف العسكرية والسياسية، فبالرغم من ندرة حدوثه عادة إلاّ أنه موجود على أرض الواقع، وأحسن مثال عن ذلك منها نجاح الإنجليزي (نيكولاس أندرسون) في اختراق موقع البحرية الأمريكية وسرقت كلمات السر الخاصة المستخدمة

---

[64]– **أيمن عبد الحفيظ**، المرجع السابق، ص43–44.

[65]– **كريم كريمة**، « **حماية الحق في الخصوصية من التعدي في ظل مجتمع المعلومات** »، مجلة العلوم القانونية ولإدارية، كلية الحقوق، جامعة جيلالي اليابس، سيدي بلعباس، العدد الثاني، 2005، ص148. *أنظر كذلك*:
- **FAUCHOUX Vincent- DEPREZ Pierre**, Le droit de l'Internet (loi, contrat et usages), édition Litec, Paris, 2008, p211.

[66]– **محمود أحمد عبابنة**، المرجع السابق، ص72.

في الهجوم النووي، وأيضا نجاح الألماني (هيس لأندر) في اختراق قاعدة بيانات شبكة البنتاجون واستطاع الحصول على 29 وثيقة متعلقة بالأسلحة النووية[67].

أضحت الدولة التي تملك المعلومات هي الدولة الأقوى، ولذلك بدأ الاهتمام ينصب على الجاسوسية العسكرية وأصبح إطلاق 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.

أصبحت 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 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 آخر حرب المعلومات المعنية بتجميع المعلومات وتيسير سبل الحصول عليها وتوزيعها بالإضافة إلى احتكارها بشكل مطلق والسيطرة على تدفق المعلومات لقوات الخصم.

تعتمد آليات هذه الحرب على شبكات الحاسب الآلي في نقل المعلومات عن طريق الشبكات ومن خلال الأقمار الصناعية، حيث يؤدي ذلك بدوره إلى تعاظم دور القوات المسلحة ونظم المعلومات في أنظمة التسليح نظرا لحتمية وأهمية تخزين البيانات وسرعة معالجتها وعرضها بصورة مناسبة أمام القادة لاتخاذ القرار على أساس أهمية تلك المعلومات[68].

بادرت الدول إلى القيام التجسس على الدول الأخرى للحصول منها على المعلومات التي تجعلها قادرة على مواجهتها في أي وقت، وذلك باقتحام المواقع العسكرية الهامة

---

[67]– **محمد سيد سلطان**، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، 2012، ص35، متوفر على الموقع التالي: www.Nashiri.Net

[68]– **أيمن عبد الحفيظ**، المرجع السابق، ص42.

والاطلاع على بياناتها، وفي بعض الأحيان نشر هذه البيانات على شبكة المعلومات الدولية كما حدث في اختراق شبكة وكالة "ناسا" الأمريكية للفضاء والطيران، اختراق الموقع الإعلامي لمختبري "سانيا وادك ديبج" الأمريكي الذي يعمل في إطار الأسلحة النووية، وأيضا اختراق الحاسب الآلي الرئيسي لوزارة الدفاع الأمريكية ونشر أبحاث الصواريخ البالستية[69].

المطلب الثاني

مجرمي الإنترنت

ينظر إلى شبكة الإنترنت دائما بوصفها أداة محايدة، وأن مصدر ضعفها وانتهاكها هو الإنسان ذاته، والذي غالبا ما يهيئ الفرصة المناسبة لاستغلال الوسيلة المعلوماتية التي أعدّها سواء عن حسن نية أو لا، فجوهر المشكلة مرتبط بذات الإنسان وشخصيته ودوافعه التي تحفزه القيام بسلوك إجرامي عبر شبكة الإنترنت من أجل تحقيق نتيجة إجرامية. [70].

سوف نستعرض في هذا النطاق مختلف أصناف مجرمي الإنترنت **(الفرع الأول)**، كذلك سنبين السمات التي يتميز بها مجرم الإنترنت **(الفرع الثاني)**، بالإضافة إلى الدوافع التي تؤدي إلى ارتكاب الجريمة عبر الإنترنت **(الفرع الثالث)**.

الفرع الأول

أصناف مجرمي الإنترنت

أدى التطور في مجال استعمال الإنترنت إلى ظهور عدة أصناف من المجرمين يصعب حصرهم تحت طوائف محددة، لكن هذا لا يعني أنه لا توجد محاولات في تحديد مختلف أصناف المجرمين عبر الإنترنت، بل على العكس هناك عدة دراسات وأبحاث حاولت وضع قواعد يصنف بها المجرمون كل حسب خطورته الإجرامية، وسوف نحاول بدورنا حصرهم على النحو التالي:

---

[69]– **أحمد صلاح الدين إبراهيم**،« **ومضات في جرائم الإنترنت- الأنماط، المسؤولية الجنائية، إستراتيجية المواجهة** »، ص7، مقال متوفر على الموقع التالي: http://www.eastlaws.com

[70]– **غازي عبد الرحمن هيان الرشيد**، الرجع لسابق، ص149

أولاً: طائفة القراصنة

1-القراصنة الهواة Hackers:[71]

يقصد بهم الشباب البالغ المفتون بالمعلوماتية، والحاسبات الآلية وبعضهم يطلق عليهم صغار نوابغ المعلوماتية، وأغلب هذه الطائفة هم من الطلبة، أو الشباب الحاصلين على معرفة في مجال التقنية المعلوماتية، والباعث الأساسي لهذه الطائفة هو الاستمتاع باللعب والمزاح باستخدام هذه التقنية، لإثبات مهاراتهم، وقدراتهم باكتشاف، وإظهار مواطن الضعف في الأنظمة المعلوماتية، دون إلحاق أي ضرر بها، فهم لديهم الرغبة في المغامرة والتحدي والرغبة في الاكتشاف[72].

تضم هذه الطائفة الأشخاص الذين يستهدفون من الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها، كسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة أو بدافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة[73].

تباينت الآراء حول تصنيف هذه الطائفة، حيث يرى البعض أنه لا يبدو من المناسب أن نصنف هؤلاء الشباب في الطوائف الإجرامية لأن لديهم ببساطة ميلا للمغامرة والرغبة في الاكتشاف ونادرا ما تكون أهداف أفعالهم المحظورة غير شريفة وهم لا يدركون

---

[71] -« ***Un hacker est une personne qui s'introduit sans autorisation dans un système informatique par l'intermédiaire d'un réseau en vue d'accéder à des information ou par simple défi, pour leurs actes d'intrusion illégale, les hackers sont appelés les pirates de l'informatique*** » Voir : **Les Officiers de l'équipe de lutte contre la cybercriminalité de la Gendarmerie Nationale**, « *Criminologie : Une menace émergente* », Revue de la gendarmerie, N° 15, novembre, 2005, p 11.

[72] – **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص46. *أنظر كذلك*:

- *pour plus d'information sur les motivation des Hacker voir* : **AGSOUS Naima, « *cybercriminalité :les réseaux informatiques* »,** Revue de la gendarmerie, N° 29, novembre, 2008, p

[73] – **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي، (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص180

ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية[74].

ذهب فريق آخر إلى اعتبار هؤلاء في مرتبة أقل من المجرمين، وذلك لأن سلوكهم بسيط وبدافع المغامرة والتحدي، قليلاً ما يقومون بأعمال تخريبية غير شريفة ولا خوف منهم على الإطلاق، ولا يهدفون إلا إلى الحصول على المعلومات بخلاف المحترفون الذين يهدفون إلى الاستيلاء على البيانات، وبخلاف مؤلفي الفيروسات الذين يهدفون إلى تخريب المعلومات الموجودة في أجهزة الكمبيوتر.

أما الفريق الأخير فذهب إلى أن أفعال هذه الطائفة هي من الأفعال المحظورة التي يعاقبها القانون، وذلك كي يستطيع مكافحة هذه الطائفة التي قد ينزلق أفرادها للدخول في طوائف محترفي جرائم الإنترنت، إضافة إلى احتمالية انضمامهم إلى أحضان منظمات أو أفراد غير شرفاء[75]

2-القراصنة المحترفين Crackers:

تعرف هذه الطائفة بالمجرمين البالغين، أو المخربين المهنيين، أو (crackers)، وأعمارهم تتراوح بين 25-45 عاماً، 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، ومعارف فنية في مجال الأنظمة الإلكترونية، والمعلوماتية تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات[76].

تعكس هذه الفئة اعتداءاتهم ميولا إجرامية خطرة تنبئ عن رغبتها في إحداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة، وخبراتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول، فقد يحدثون أضرارا كبيرة، وعادة ما يعود المجرم المحترف بالجريمة عبر الإنترنت إلى ارتكاب الجريمة مرة أخرى، حيث تزداد

---

[74]- **نهلا عبد القادر المومني**، المرجع السابق، ص81_82

[75]- **محمود أحمد عبابنة**، المرجع السابق، ص42

[76]- **محمد دباس الحميد، ماركو إبراهيم نينو**، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان، الطبعة الأولى، 2007 ص73

سوابقه القضائية وهو يعيش لسنوات طويلة من عائدات جرائمه، وهذا المجرم لا يفضل الأفكار المتطرفة وإنما الأفكار التي تدر عليه الأرباح الشخصية[77]، وبالتالي هم أكثر خطورة من الصنف الأول لأنهم قد يحدثون أضرارا كبيرة على المجني عليه[78].

ثانيا: طائفة الحاقدين

غالبا ما يطلق على هذه الطائفة المنتقمون، لأن صفة الانتقام والثأر هي ما تتميز به عن بقية الطوائف، وهي الباعث لتصرفاتهم، لأنها تنطلق ضد أصحاب العمل، والمنشآت التي كانوا يعملون بها، انتقاما من رب العمل على سوء تقديره لهم.[79]

يرى الباحثون أن أهداف وأغراض الجريمة غير متوفرة لدى هذه الطائفة، فهم لا يهدفون إلى إثبات قدراتهم التقنية ومهاراتهم الفنية، ولا يبغون تحقيق مكاسب مادية أو سياسية ولا يفاخرون أو يجاهرون بأنشطتهم، بل يعمدون إلى إخفاء وإنكار أفعالهم ولا يوجد تحديد فئة عمرية لهم، وأغلب أنشطتهم تتم باستخدام تقنيات زراعة الفيروسات، والبرامج الضارة لتخريب الأنظمة المعلوماتية، أو إتلاف كل أو بعض معطياته، أو المواقع المستهدفة من الإنترنت[80].

تصنف هذه الطائفة من حيث الترتيب في الخطورة الإجرامية، من ضمن الطوائف الأقل خطورة بين مجرمي التقنية المعلوماتية، ولكن ذلك لا يمنع أن ينجم عن بعض أنشطتهم، خسائر جسيمة للمؤسسة التي يعملون بها[81].

77- **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص32

78- **وليد عاكوم**، « **مفهوم وظاهرة الإجرام المعلوماتي**»، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية الممتحنة، 1-3 مايو 2000، المجلد الأول، الطبعة الثالثة 2004، ص 12.

79- **محمد بن عبد الله بن علي المنشاوي**، جرائم الإنترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص38.

80- **أيمن عبد الحفيظ**، المرجع السابق، ص34

81- **أحمد خليفة الملط**، المرجع السابق، ص62

ثالثا: طائفة المتطرفين الفكريين

ساهم الاختلاف الموجود بين الشرق والغرب أو بين الشمال والجنوب، أو بين الاشتراكيين والرأسماليين، أو حتى بين الأديان أو المذاهب المختلفة لذات الدين في إبراز هذه الطائفة، بمعنى أن تعمد كل طائفة إلى تأجج الأفكار، والآراء حول مواضيع الخلاف مع الطوائف الأخرى بصرف النظر عن طبيعة هذه الخلافات سواء كانت دينية أو سياسية أو اقتصادية[82].

يعرف التطرف في هذا المجال بأنه عبارة عن أنشطة توظف شبكة الإنترنت في نشر وبث واستقبال وإنشاء المواقع والخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري وخاصة المحرض على العنف أياً كان التيار أو الشخص أو الجماعة التي تتبنى أو تشجع أو تمول كل ما من شأنه توسيع دائرة ترويج مثل هذه الأنشطة[83].

تجري حاليا حوارات مختلفة بين الاتجاهات الإيديولوجية، أو الدينية أو المذهبية تحت سماء مختلفة منها، حوار الأديان أو صراع الحضارات أو التقريب بين الثقافات وغيرها، وقد عم الجدل والنقاش بهذه الأمور عبر مواقع الإنترنت، وقد وجدت بعض الأفكار أو الآراء المتطرفة صدى لدى أتباع هذه الاتجاهات أو الديانات أو المذاهب، مما دفع بعض المتشددين إلى سلوك الطريق الإجرامي، وأصبح هناك ما يعرف بالمجرم المعلوماتي المتطرف.

يستعمل المتطرفون كافة المواقع الإلكترونية التي تسعى لتحقيق أغراض دعائية لصالحهم، بما في ذلك الشبكات الإعلامية الإخبارية التي تتبع وترصد نشاطات الجماعة وتنشر بيانات وتصريحات قادتها ، والمنتديات والمدونات التي تقوم على تنشيط الحوار

---

[82]– **نهلا عبد القادر المومني**، المرجع السابق، ص85–86.

[83]– **فايز بن عبد الله الشهري**، « **ثقافة التطرف على شبكة الإنترنت الملامح والاتجاهات** »، الندوة العلمية استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 25_2010/10/27، ص5

حول موضوعات مختلفة تطرحها الجماعة، والإصدارات الإعلامية الإلكترونية مثل المجلات التي تصدرها الجماعة على الإنترنت حتى ولو بلغات أجنبية[84].

يستخدم المتطرفون خدمات البريد الإلكتروني المجانية للاتصال بأي مكان 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[85].

برزت سمات وخصائص هذه الطائفة، أن المجرم المتطرف لا يسعى لتحقيق هدف شخصي، أو الحصول على نفع مادي له، بل يعمل على تغيير المجتمع ليتماشى ويتوافق مع ما يعتقد صحته من الأفكار و المعتقدات.

رابعا: طائفة المتجسسين

لقد تحولت وسائل التجسس من الطرق التقليدية إلى طرق حديثة استخدمت فيها التقنية الحديثة خاصة مع وجود الإنترنت، وذلك بسبب ضعف الوسائل الأمنية المستخدمة في حماية الشبكات سواء كانت هيئات حكومية أو مؤسسات خاصة، وذلك من خلال اختراق هذه الشبكات والمواقع من قبل الهاكرز، فيقوم هؤلاء في العبث أو إتلاف محتويات تلك الشبكة، هذا من جانب، ومن جانب آخر وهو الأهم، والذي يشكل الخطر الحقيقي على تلك المواقع، فيكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على أسرار ومعلومات الدولة ومن ثم إفشائها إلى دول أخرى معادية أو استغلالها لما يضر المصلحة الوطنية لتلك الدولة[86].

---

[84]– **مها عبد المجيد صلاح، «استراتيجيات الاتصال في مواقع الجماعات المتطرفة على شبكة الإنترنت دراسة تحليلية»**، الندوة العلمية استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 25_2010/10/27، ص8

[85]– **مصطفى محمد موسى، « التنظيمات الإرهابية وشبكة الإنترنت»**، الندوة العلمية استشراف التهديدات الإرهابية، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 20-2007/8/22، ص37

[86]– **دشن بن محمد القحطاني،« الاستخدامات غير المشروعة لتقنية المعلومات عبر الإنترنت»**، ص15، مقال متوفر على الموقع التالي: http://www.minshawi.com

من أهم أهداف هذه الطائفة في استخدام الأنظمة المعلوماتية، هي الحصول على معلومات الأعداء، والأصدقاء على حد سواء، بغية تفادي شرها أو التفوق عليها، ولم تعد المعلومات العسكرية هي الهدف الرئيس، بل أصبحت تشمل المعلومات الاقتصادية، والتقنية والصناعية[87].

من سمات هذه الطائفة أنها غير مرتبطة بغرض محدد، إذ أن أغلب من يقومون بهذا العمل هم موظفون لدى الدول أو الشركات والمؤسسات التي يعملون بها، فليس لهذه الطائفة أهداف شخصية، ومن أبرز الأمثلة على حالة التجسس المعلوماتي، محاولة المخابرات الروسية عبر استئجار بعض المختصين في مختلف مجالات المعلوماتية، لاختراق الأنظمة المعلوماتية العسكرية للغرب، وكذلك قيام شركتي هيتاشي، وميتسوبيشي اليابانيتين، بالتجسس على شركة IBM الأمريكية[88].

بالإضافة إلى ذلك قد تكون الإنترنت أداة جيدة للغاية في عملية التجسس الصناعي، على سبيل المثال، قد يتم تنزيل الأسرار الصناعية من كمبيوتر في إحدى الشركات وإرسالها بالبريد الإلكتروني مباشرة إلى منافستها[89].

خامسا: طائفة مخترقي الأنظمة

يتبادل أفراد هذه الطائفة المعلومات فيما بينهم، بغية اطلاع بعضهم على مواطن الضعف في الأنظمة المعلوماتية، وتجري عملية التبادل للمعلومات بينهم بوساطة النشرات الإعلامية الإلكترونية، مثل مجموعات الأخبار، بل إن أفراد هذه الطائفة يتولون عقد المؤتمرات لكافة مخترقي الأنظمة المعلوماتية بحيث يدعى إليها الخبراء من بينهم للتشاور حول وسائل الاختراق وآليات نجاحها، وكيفية تنظيم العمل فيما بينهم، ويتبع المخترقون

---

[87]– **محمد حماد مرهج الهيتي**، جرائم الحاسوب...، المرجع السابق، ص137.

[88]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص154.

[89]– **إيهاب ماهر السنباطي**، « **الجرائم الإلكترونية (الجرائم السيبيرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد** »، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، يونيو 2007، ص21.

أساليب عدة في عمليات تشويه صفحات المواقع، وتختلف هذه الأساليب من موقع لآخر حسب نوع نظام التشغيل الذي يعتمد عليه الموقع[90].

تبرز سمات هذه الطائفة أيضا، في أنهم ينطلقون من دوافع التحدي واثبات المقدرة على اختراق الأنظمة المعلوماتية، فنشاطهم ليس تخريبيا، بل إن العديد من الجهات تستعين بهم، في عمليات فحص وتدقيق مستوى أمن الأنظمة المعلوماتية فيها[91]، وأفراد هذه الطائفة ليس لهم فئة عمرية محددة أيضا فمنهم الصغار والكبار وهم في الغالب لا ينتمون إلى طائفة مجرمي التقنية، والكسب المادي ليس من أولوياتهم وإنما مجرد تحقيق المتعة والإشباع الشخصي في إثبات قدراتهم وكفاءتهم على اختراق الأنظمة المعلوماتية، إلى درجة أنهم ينصبون من أنفسهم أوصياء على أمن الأنظمة المعلوماتية في المؤسسات المختلفة[92].

---

[90]– تتمثل هذه الأساليب في:

أ–الدخول بهوية مخفية: تمكن هذه الطريقة في بعض الحالات، المخترق من الحصول على ملف كلمة الدخول المشفرة، الخاصة بأحد المشرفين على الشبكة، أو من يملكون حق تعديل محتويات الموقع، العمل على فك تشفيرها، حيث يتم إرسال كلمة السر مشفرة في مختلف المزودات لكن هذه الشفرة تظهر في بعض المزودات ضمن ملف كلمة السر.

ب–استغلال الثغرات الأمنية في مزودات الويب وأنظمة التشغيل: لا يخلو أي نظام تشغيل أو مزود ويب من ثغرات أمنية تعرض مستخدميه لخطر الاختراق، يستغل المخترقون الثغرات الأمنية في عمليات الاختراق على أن تجد الشركة المصممة للنظام الحل المناسب لها، وتبقى بعض الثغرات متاحة لفترة طويلة حتى يتم اكتشافها، وذلك لأن أغلب الثغرات التي يكتشفها المخترقون لا يعلنون عنها بسرعة ليتمكنوا من استغلالها لفترة أطول.

ج–استخدام بروتوكول Telnet: تسمح كثير من الثغرات الأمنية في الأنظمة المختلفة سواء كانت يونيكس، أو ويندوز، أو غيرها، باستخدام تطبيقات تعتمد على بروتوكول Telnet، الذي يسمح بالوصول إلى أجهزة الكمبيوتر عن بعد، وتنفيذ الأوامر إليها، ويمكن استخدام هذا البروتوكول للدخول إلى مزودات ويب وتغيير الصفحات فيها. *أنظر في هذا*: **عمر بن محمد العتيبي**، المرجع السابق، ص49–50

[91]– **DEBRAY Stéphane,** op-cit, p 12.

[92]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص156.

الفرع الثاني

سمات مجرمي الإنترنت

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 يلجأ إلى استعمال العنف في غالب الأحيان، بالإضافة إلى عدم احتياجه إلى مستوى علمي من أجل القيام بأفعاله، فمجرم الإنترنت 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:

أولاً: 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 الإنترنت أن يكوّن تصورا كاملا لجريمته[93].

يتمتع مجرمو 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 قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات[94].

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

---

[93]- **طارق إبراهيم الدسوقي عطية**، المرجع السابق، ص176-177.

[94] -**MASCALA Corinne**, « *criminalité et contrat électronique* », Op-cit, p 118.

في البرامج وارتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من الذكاء لكي يتمكن من ارتكاب تلك الجرائم[95].

إجرام الإنترنت هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فمجرم الإنترنت يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها أحد سواه وذلك من أجل اختراق 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 آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الأضرار بالأشخاص، الأمر الذي يعدونه غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصادياً تحمل نتائج تلاعبهم[96].

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

يقوم في كثير من الأحيان العاملون بالمؤسسات المختلفة باستخدام الإنترنت لأغراض شخصية بوصفه سلوكاً شائعاً بين الجميع ولا ينظر إليه بوصفه فعلاً إجرامياً، إلاّ أن ذلك لا يعني أن عدم الشعور بعدم أخلاقية هذه الأفعال الإجرامية لدى فئة كبيرة من مرتكبيها ينفي وجود مجرمين يرتكبون إجرام الإنترنت وهم على علم وإدراك بعدم

---

[95]- **أيمن عبد الحفيظ**، المرجع السابق، ص13

[96]- **نهلا عبد القدر المومني**، المرجع السابق، ص78

مشروعية وأخلاقية هذا الفعل، فهناك فئة لديها اتجاه إجرامي خطير وسوء نية واضح وهم على إدراك بخطورة أفعالهم[97].

3- الخوف من كشف الجريمة

يتصف المجرمون عبر الإنترنت بالخوف من كشف جرائمهم وافتضاح أمرهم، وبالرغم من هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي الإنترنت بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان[98].

تساعد طبيعة الأنظمة 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 الأسباب التي تساعد على نجاح الجريمة المرتكبة عبر الإنترنت هي أن الحواسيب إنما تؤدي عملها غالبا بطريقة آلية 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[99]

4- الميل إلى التقليد

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

---

[97]- **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص28

[98]- **نهلا عبد القادر المومني**، المرجع السابق، 79

[99]- **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص29

ولا شك أن ذلك نتيجة لعدم الاستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط، وينتهي به الأمر إلى التقليد وارتكاب الجريمة[100].

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

1- التنظيم والتخطيط :

في عالم الشبكات الإلكترونية وخاصة الشبكة العالمية للإنترنت، كما هو الحال في العالم الحقيقي يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة[101]، حيث ترتكب أغلب الجرائم من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معين ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمنا فيها متخصص في الحاسبات يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب وتحويل المكاسب إليه، كما أن من عادة من يمارسون التلصص والقرصنة على الحاسبات وشبكات المعلومات بصفة منتظمة حول أنشطتهم عقد المؤتمرات.[102]

تحتاج مثلا جريمة زرع الفيروسات إلى مجموعة من الأشخاص منهم المبرمج الذي يقوم بكتابة البرنامج ومنهم المستخدم الذي يقوم بعملية زرع الفيروسات داخل الأجهزة الأخرى، وينتج عن هذا التنظيم صعوبة كشف تلك الجريمة وإمكانية تنفيذها بدقة نتيجة للتخصص داخل تلك الجماعة في كل جزء من أجزاء الجريمة.

يعتبر التخطيط ميزة هامة تتعلق بصفة مباشرة بالجماعة الإجرامية المنظمة، ويعني الدراسة المسبقة لأي عملية إجرامية تقدم المنظمة على ارتكابها، ويتطلب التخطيط قدراً عالياً من الذكاء والخبرة بهدف ضمان استمرار أنشطتها بعيداً عن رقابة ومتابعة السلطات المعنية بقمع الجريمة، فالمنظمات الإجرامية تحتاج إلى عدد من محترفي الإجرام الذين

---

[100]- **أيمن عبد الحفيظ**، المرجع السابق، ص15

[101]- **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص 34

[102]- **هشام محمد فريد رستم**، المرجع السابق، ص436-437

يملكون مؤهلات وخبرات عالية تمكنهم من سد جميع الثغرات الاقتصادية والاجتماعية والقانونية التي قد تؤدي إلى فشل أو اكتشاف الجريمة[103].

2- التكيف الاجتماعي

تعتبر هذه الخاصية امتدادا لسمة التخطيط والتنظيم، حيث إن التكيف الاجتماعي ينشأ بين مجموعة لها صفات مشتركة فمثلا جماعة صغار نوابغ المعلوماتية لا شك أنهم يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم صلات وروابط تساعدهم على ارتكاب جرائمهم وتتعدى تلك الروابط والصلات النطاق المحلي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي، ولا شك أن إقامة المؤتمرات الدولية بين هؤلاء المجموعات خير دليل على وجود تلك الصلات والروابط الدولية بينها[104].

بالإضافة إلى ذلك أن مجرمي الإنترنت هم عادة أناس اجتماعيين قادرين على التكيف في بيئتهم الاجتماعية، ولا يضعون أنفسهم في حالة عداء مع المجتمع الذي يحيط بهم، بل قادرين على التوافق والتصالح مع مجتمعهم باعتبارهم أناس مرتفعوا الذكاء، بل إن خطورتهم الإجرامية قد تزداد إذا زاد تكيفهم الاجتماعي مع توافر الشخصية الإجرامية لديهم[105].

تمنح هذه الخاصية المنظمات الإجرامية القدرة على تحويل أنشطتها من دولة إلى دولة أخرى تكون قوانينها أكثر مرونة، وهي خاصية تجعلها قادرة على الإفلات من إجراءات مكافحة غير فعالة بسبب الحدود الإقليمية، وغير متناسقة بين الدول، وبالتالي تبين هذه الخاصية مدى خطورة قوة الجماعات الإجرامية المنظمة عبر الإنترنت. [106]

---

[103]- **قرايش سامية**، التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية، مذكرة لنيل درجة الماجستير في القانون فرع تحولات الدولة، كلية الحقوق، جامعة مولود معمري، تيزي وزو، دون تاريخ مناقشة، ص28

[104]- **أيمن عبد الحفيظ**، المرجع السابق، ص16-17

[105]- **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص28.

[106]- **قرايش سامية**، المرجع السابق، ص30.

3- التطور في السلوك الإجرامي

تتميز جرائم الإنترنت بأنها جرائم مرتبطة بالتطور السريع الذي نشهده اليوم في تكنولوجيا الاتصالات، والذي انعكس بدوره على تطور مرتكب جريمة الإنترنت وأسلوب ارتكابه من خلال ما ينهله من أفكار وتبادل الخبرات مع العديد من المجرمين حول العالم عبر الشبكة، وتطور التقنيات المستخدمة في ذلك.[107]

يساهم وجود مجرم الإنترنت في جماعة إجرامية إلى التأثير في قدرته العقلية وسرعة إكسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة [108].

الفرع الثالث

دوافع مجرمي الإنترنت

تختلف الجريمة المرتكبة عبر الإنترنت عن الجريمة التقليدية من حيث الدوافع، حيث أن مجرمي الإنترنت يسعون من خلال ارتكابهم للجريمة -بالإضافة إلى تحقيق المكسب المادي- إلى تحقيق أغراض معنوية مثل التعلم أو اللعب والمزاح، أو لمجرد الانتقام، ويمكن حصر هذه الدوافع في:

أولا: الدوافع الرئيسية لارتكاب المجرمين للجريمة عبر الإنترنت

1- تحقيق الكسب المادي

تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الإنترنت، وهو من أهم الدوافع وأكثرها تحريكا للمجرم، نظراً للربح الكبير الذي يمكن أن يحققه هذا النوع من الأنشطة الإجرامية، وغالبا ما يكون الدافع لارتكاب هذه الجرائم وقوع الجاني

---

[107]- **عبد الرحمن محمد بحر**، معوقات التحقيق في جرائم الإنترنت دراسة مسحية على ضباط الشرطة في البحرين، رسالة مقدمة إلى معهد الدراسات العليا استكمالاً لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، معهد الدراسات العليا قسم العلوم الشرطية، الرياض، 1999، ص26.

[108]- **أيمن عبد الحفيظ**، المرجع السابق، ص17.

بمشاكل مادية تعجزه عن سداد ديونه المستحقة، أو لوجود مشاكل عائلية تعود إلى عدم توفر الأموال، أو الحاجة لها للعب القمار، أو شراء المخدرات، أو القيام بأعمال المراهنة إلى غير ذلك، حيث يسعى الجاني للخروج من هذه المآزق إلى عمليات التلاعب بالأنظمة المعلوماتية للبنوك والمؤسسات المالية، وذلك بواسطة اختراق الأنظمة المعلوماتية لها، واكتشافه لفجواتها الأمنية[109].

يقوم مرتكبوا الجريمة عبر الإنترنت ذوي الكفاءة الفنية العالية، بما لديهم من خبرة ومهارة في المجال التكنولوجي بتوجيه هذه الإمكانات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك، يستطيع المجرمون بمجرد دخولهم إلى أنظمة البنوك معرفة أرقام الحاسب وسرقتها أو تحويلها، ويكون المكسب المادي أيضا هدفا لمن هم أقل في المعرفة التقنية وقد يكونون غير مؤهلين على الإطلاق في المجال المعلوماتي لذلك يكون أسلوب ارتكابهم للجريمة مختلفا، لأن الجريمة تكون متعلقة بالحاسب الآلي أو المعلومات ولكن دون الدخول إلى أنظمة تلك الحواسب ويكون أسلوب ارتكابهم للجرائم أسلوبا محدوداً في مجال معين لا يحتاج إلى خبرة ومهارة[110].

تجدر الإشارة إلى أنه في حال نجاح المجرم في ارتكاب جريمته عبر الإنترنت، فإن ذلك قد يدر عليه أرباحاً هائلة في زمن قياسي، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة لاقترافه هذا النوع من الإجرام من خلال ما يرويه أحد هؤلاء المجرمين المحترفين في سجن كاليفورنيا بقوله: « لقد سرقت أكثر من نصف مليار دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكاني أن أكرر ذلك في أي وقت، لقد كان شيئا سهلاً فأنا أعرف أسلوب عمل جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة ولو لم يكن سوء الحظ قد صادفني »[111].

---

[109]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص157–158

[110]– مشار إليه لدى: **أيمن عبد الحفيظ**، المرجع السابق، ص18.

[111]– **نهلا عبد القادر المومني**، المرجع السابق، ص91.

2- الرغبة في التعلم

هناك من يرتكب جرائم الإنترنت بغية الحصول على الجديد من المعلومات وسبر أغوار هذه التقنية المتسارعة النمو والتطور، وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية[112].

3- دوافع ذهنية أو نمطية

غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الإنترنت هو الرغبة في إثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا آثمة، ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم.[113]

ففي الوقت الذي يزداد فيه الاهتمام بأمن الحاسب الآلي وشبكاته، عن طريق تطوير طرق جديدة وصعبة لاختراقه، كبرمجيات التشفير التي تمكن مستقبلها وحده من فهمه، من الأمثلة على ذلك وزارة الدفاع الأمريكية التي تقوم بتغيير أنظمة الترميز للبيانات المستحدثة يوميا، حتى أن بعض المعلومات الحساسة تغير كل ساعة أنظمة ترميزها، وهذا مما لا شك فيه يدل على قدر عال من التقنية ولنظام المتطور، فعن الجانب الآخر الذي يقف على الضفة الأخرى، أصحاب الشغف الإلكتروني يتسابقون لخرق هذه الأنظمة وإظهار تفوقهم عليها، والدليل على ذلك قيام أحد الهواة في أوربا بحل شفرة احد مراكز المعلومات في وزارة الدفاع الأمريكية وتمكنه من العبث في بيانات هذا المركز[114].

---

[112]- **تركي عبد الرحمن المويشر**، المرجع السابق، ص32.

[113]- **أحمد خليفة الملط**، المرجع السابق، ص90.

[114]- **محمود أحمد عبابنة**، المرجع السابق، ص25.

ثانيا: الدوافع الشخصية والمؤثرات الخارجية

1-ارتكاب الجرائم من أجل التسلية

يعتبر دافع المزاح والتسلية من الدوافع التي تجعل الشخص يقوم بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض المزاح فقط ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة الجريمة[115].

2- دوافع سياسية

انتشرت الكثير من المواقع غير المرغوب فيها على شبكة الإنترنت ومن هذه المواقع ما يكون موجها ضد سياسة دولة محددة أو ضد عقيدة أو مذهب معين، وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد المستهدف.

يتم غالبا في المواقع السياسية المعادية تلفيق الأخبار والمعلومات ولو زوراً أو حتى الاستناد إلى جزئي بسيط جدا من الحقيقة ومن ثم نسج الأخبار 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 قسراً إلى قائمتهم البريدية ويبدؤون في إغراق تلك العناوين بمنشوراتهم، وهم عادة يلجئون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له ولإيصال أصواتهم إلى أكبر قدر ممكن[116].

تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم، كما أن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية، كذلك أصبحت شبكة الإنترنت مجالاً خصبا لنشر أفكار العديد من الأفراد والمجموعات، ووسيلة لترويج لأخبار وأمور أخرى قد تحمل في طياتها مساسا بأمن الدولة أو بنظام الحكم أو قدحا في رموز دولية أو سياسية والإساءة لها بالذم والتشهير[117].

---

[115]- **أيمن عبد الحفيظ**، المرجع السابق، ص20.

[116]- **صالح بن سعد صالح**، المرجع السابق، ص12.

[117]- **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص39.

3-دافع الانتقام

يكون دافع الانتقام مؤثراً في ارتكاب هذه الجرائم[118]، حيث يعد من أخطر الدوافع التي يمكن أن تدفع شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها لأنه غالبا ما يكون أحد موظفيها، ويقوم بهذا الدافع نتيجة إما لفصله من العمل أو تخطيه في الحوافز أو الترقية فهذه الأمور تجعله يقدم على ارتكاب جريمته[119].

تشير التقديرات إلى أن نسبة كبيرة من الجرائم المرتكبة عبر الإنترنت ترتكب من قبل موظفي الجهة نفسها، ومن الوقائع التي حدثت في الولايات المتحدة الأمريكية أنه حكم على أحد الموظفين في إحدى شركات التأمين بالسجن لمدة سبع سنوات وغرامة مقدارها 150 ألف دولار لأنه أدخل فيروسا في أجهزة الشركة التي كان يعمل فيها مما أدى إلى ضياع 160 سجلاً من سجلات العملاء، وذلك انتقاما من الشركة لأنها قامت بفصله من العمل[120].

المبحث الثاني

التكييف الجريمة المرتكبة عبر الإنترنت

تقتضي تحديد الطبيعة القانونية للجريمة المرتكبة عبر الإنترنت، العمل على تصنيفها وتحديد الأركان التي تقوم عليها، فمع النمو السريع لاستخدام شبكة الانترنت في شتى المجالات، وتنوع أشكالها وصورها بصورة مطردة، مما جعل مهمة حصرها وتصنيفها تتميز بالصعوبة، وتجدر الإشارة أن تحليل صور الجريمة المرتكب عبر الإنترنت وبيان أصنافها ليس بالأمر البسيط وذلك يرجع إلى التباين والاختلاف لدى الفقه في معرض تصنيفهم لهذه الجرائم، وسبب ذلك يرجع إلى عدم تبنيهم لمعايير واحدة ثابتة

---

[118]- **أحمد خليفة الملط**، المرجع السابق، ص90.

[119]- **أيمن عبد الحفيظ**، المرجع السابق، ص19.

[120]- **صالح بن محمد المسند، عبد الرحمن بن راشد المهيني**، المرجع السابق، ص182.

-« *La criminalité informatique est essentiellement orientée vers le profit Toutefois, les criminels informatique n'ont pas tous des motivations identique, de plus, il semble évident que le criminel informatique n'a pas une motivation unique et que ses objectifs sont souvent variés et complémenter* », voir : **AGSOUS Naima,** op-cit, p 21.

ولضوابط مشتركة[121]، ومن هذا المنطلق دأب الفقهاء في وضع عدة أسس من أجل تصنيف الجرائم المرتكبة عبر الإنترنت **(المطلب الأول)**.

تعتبر أركان الجريمة جزء لا يتجزأ من طبيعتها وتخلف أحدها يؤدي إلى انتفاء الجريمة، فهذه، حيث يتطلب القانون كأصل عام وجود ركن مادي وركن معنوي، وركن شرعي بموجبه يتم التجريم والعقاب، وهو الأمر المعمول به في كل الجرائم تقليدية كانت أو مستحدثة، فبالرغم من أن في الجرائم التقليدية هناك رأي يلغي الركن الشرعي واكتفائه بالركن المادي والمعنوي بحجة أن الركن الشرعي هو الذي يحدد هذه الأركان، غير أن في الجريمة المرتكبة عبر الإنترنت، يجب الاعتماد على الأركان الثلاثة لتحديد الجريمة، نظراً لعدم كفاية القوانين السارية أو التقليدية **(المطلب الثاني)**.

المطلب الأول

تصنيف الجرائم المرتكبة عبر الإنترنت

تعتبر الجرائم المرتكبة عبر الإنترنت من الجرائم المستحدثة، وهي تستهدف الكثير من القطاعات-كما أسلفنا الذكر- مما جعل من مأمورية الفقهاء فيما يخص تحديدها وتصنيفها يتميز بالصعوبة، على عكس الجرائم التقليدية التي يمكن تصنيفها بسهولة فائقة.

لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم المرتكبة عبر الإنترنت وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة، وعلى هذا الأساس سوف نعتمد في تقسيم هذا المطلب على مختلف معايير التصنيف وهي على أساس الجرائم الواقعة على الأموال **(الفرع الأول)**، ثم الجرائم الواقعة على الأشخاص **(الفرع الثاني)**، وأخيرا إلى أساس الجرائم الواقعة على أمن الدول **(الفرع الثالث)**.

---

[121]– **محمود أحمد عبابنة**، المرجع السابق، ص47

الفرع الأول
جرائم واقعة على الأموال

صاحب ظهور شبكة الإنترنت تطورات كبيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما إنجر عنه تطور وسائل الدفع والوفاء وأضحت جزء لا يتجزأ من هذه المعاملات، وفي خضم هذا التداول المالي عبر الإنترنت انتهز بعض المجرمين من أجل السطو عليها، حيث ابتكرت عدة طرق من أجل ذلك، على غرار السطو والسرقة، والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة.

أولا: جرائم السطو على أرقام بطاقات الائتمان والتحويل الإلكتروني غير المشروع للأموال

واكب استخدام البطاقات الائتمانية[122] من خلال شبكة الإنترنت واكبه ظهور الكثير من المتسللين للسطو عليها، باعتبارها نقودا إلكترونية ، خاصة من جهة أن الاستيلاء على بطاقات الائتمان أمرا ليس بالصعوبة بما كان، فلصوص بطاقات الائتمان مثلا يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الإنترنت ومن ثم بيع هذه المعلومات للآخرين[123].

تتم عملية التحويل الإلكتروني غير المشروع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه، مما يسمح للجاني

---

[122]– البطاقة الائتمانية عبارة عن بطاقة بلاستيكية تصدر من قبل بنك أو مؤسسة لتقديم خدمات أو تسهيلات معينة، على أن يقوم حامل البطاقة بسداد المبالغ المستحقة كليا أو جزئيا وفق نصوص العقد بين العميل(حامل البطاقة)، والمصرف أو المؤسسة المصدرة للبطاقة، **هشام مفيد محمود**،« **الآثار السلبية الناجمة عن تزوير البطاقات الائتمانية**»، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص107، *أنظر كذلك*: **الصديق محمد الأمين الضرير**،« **بطاقات الائتمان**»، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، أيام 10–12 ماي 2003 المجلد الثاني، ص637

[123]– **حسن طاهر داود**، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2000، ص73

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[124]، وتتم عملية التحويل الإلكتروني غير المشروع للأموال بأحد الطرق الموالية:

أ_الاحتيال: يتم ذلك بطرق احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح، فيسلم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال وهو يعلم أن ليس له صفة التصرف فيه[125]، وقد يتخذ اسم أو صفة كاذبة، تمكنه من الاستيلاء على مال المجني عليه فيتم التحويل الإلكتروني للأموال وذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة أو يتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في إيهام الحاسب والاحتيال عليه فيسلمه النظام المال[126].

ب_الاحتيال باستخدام بطاقات الدفع الإلكتروني: يعتمد نظام بطاقة الدفع الإلكتروني على عمليات التحويل الإلكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر أو الدائن الذي يوجد به حسابه وذلك من خلال شبكة التسوية الإلكترونية للهيئات الدولية "هيئة الفيزا كارد"، هيئة الماستر كارد"[127]، وتعطي بطاقة الدفع الإلكتروني الحق للعميل بالحصول على السلع والخدمات على الشبكة عن طريق تصريح كتابي أو تلفوني، بخصم القيمة على حساب بطاقة الدفع الإلكتروني الخاصة به، وتتم العملية بدخول العميل أو الزبون إلى موقع التاجر ويختار السلع المراد شرائها ويتم التعاقد بملأ النموذج الإلكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري[128]، وأمام

---

[124]– **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2010، ص76

[125]– **يونس عرب، « قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان»**، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، المنعقدة بمسقط، سلطنة عمان، 2-4 أفريل 2006، ص16

[126]– **عباس أبو شامة عبد المحمود**، المرجع السابق، ص54

[127]– **عمر الشيخ الأصم، « البطاقات الائتمانية المستخدمة الأكثر انتشارا في البلاد العربية »**، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص12

[128]– **محمد عبد الرسول خياط، « عمليات تزوير البطاقات الائتمانية »**، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص41، *أنظر كذلك*: **أحمد شوقي أبو خطوة**،=

التطور التكنولوجي أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريق غير المشروع ممكنة عبر قنوات شبكة الإنترنت.[129]

2- القمار وغسيل الأموال عبر الإنترنت

يعد الفضاء السيبراني من أكثر الأسباب التي تشجع على ممارسة القمار عبر الإنترنت مقارنة بممارستها على الكازينوهات في الواقع المادي، إذ يمنح الراغب في ممارسة القمار من خلال الكازينوهات الافتراضية، الخصوصية وخفاء الشخصية التي يبحث عنها الكثيرون، حيث يستطيع الشخص ممارسة القمار دون حتى أن يغادر غرفة نومه.(130)

وكثيرا ما تتداخل عملية غسيل الأموال(131) مع ممارسة القمار عبر شبكة الإنترنت، مما زاد من انتشار أندية القمار الإفتراضية، الأمر الذي جعل مواقع الكازينوهات

=« **جريمة الاحتيال ماهيتها وخصائصها**»، دورة عمل حول جرائم الاحتيال والإجرام المنظم، جامعة نايف العربية للعلوم الأمنية، أيام 18-20 جوان 2007،الرياض، الطبعة الأولى، 2008، ص39

129- SEDALIAN Valérie, Droit de l'internet- Réglementation- Responsabilités- contrat, Edition Net Press, Paris, 1997, p 149.

130- **محمد بن نصير محمد السرحاني**، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت-دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، تخصص القيادة الأمنية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية، الرياض، 2004، ص53-54

131- يعتبر مصطلح غسيل الأموال حديث نسبيا، وكان يبدو ولوقت قريب، غريبا جدا في لغة الشرطة، ومبهما بالنسبة للكثير من الناس وبدأ استخدام هذا المصطلح في الولايات المتحدة الأمريكية نسبة إلى مؤسسات الغسل التي تمتلكها المافيا، وهي مؤسسات نقدية كان يتاح فيها مزج الإيرادات المشروعة والإيرادات غير المشروعة إلى حد تظهر عنده كافة الإيرادات كأنها متحصلة من مصدر مشروع، وكان أول استخدام لتعبير غسيل الأموال في سياق قانوني أو قضائي حصل في قضية ضبطت في الولايات المتحدة الأمريكية اشتملت على مصادرة أموال قيل أنها مغسولة ومتأتية من الاتجار غير المشروع الكولومبي، وقد تطورت عمليات غسل الأموال بعد ذلك وأصبحت أكثر تعقيدا واستخدمت أحدث التكنولوجيات لإخفاء طابع الأموال أو مصدرها أو استخدامها الحقيقي. *أنظر في هذا كل من:*

- **محمد فتحي عيد**، الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 1999، ص298، **دليلة مباركي**، غسيل لأموال، أطروحة مقدمة لنيل شهادة الدكتوراه علوم، تخصص قانون جنائي، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم القانونية، باتنة، 2008، ص8. **بسام أحمد الزلمي**، « **دور النقود الإلكترونية في عمليات غسيل الأموال** »، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، 2010، ص523، *و كذلك*: **محمد عبد السلام سلامة**، « **جرائم غسيل الأموال إلكترونيا في ظل النظام**=

الافتراضية على الإنترنت محل اشتباه ومراقبة، ومن البديهي أن يأخذ المجرمون بأحدث ما توصلت إليه التقنية لخدمة أنشطتهم الإجرامية ويشمل ذلك بالطبع طرق غسيل الأموال التي استفادت من عصر التقنية فلجأت إلى الإنترنت لتوسعة وتسريع أعمالها في غسيل أموالها غير المشروعة[132].

ساعدت شبكة الإنترنت القائمون بعمليات غسيل الأموال بتوفير عدة مميزات منها السرعة الشديدة وتخطي الحواجز الحدودية بين الدول وتفادي القوانين التي قد تضعها الدول من أجل إعاقة هذا النشاط، وكذا تشفير عملياتهم مما يعطيها قدر كبير من السرية، وخاصة في تسهيل على مرتكبي جرائم غسيل الأموال نقلها إلى أي مكان في العالم[133]، من أجل استثمارها في إقليم أي دولة من العالم، وإعطاء هذه الأموال الصبغة المشروعة[134].

3- جريمة السرقة والسطو على أموال البنوك

تعرف السرقة[135] بأنها اختلاس شيء منقول مملوك للغير بدون رضاه بنية امتلاكه[136]، وتتم سرقة المال المعلوماتي [137]- إن أمكن الوصف- عن طريق اختلاس

=**العالمي الجديد**»، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 10-12ماي 2003، المجلد الرابع، ص1507

[132]- **محمد زيدان، محمد حمو**،« **متطلبات أمن المعلومات المصرفية في بيئة الإنترنت**»، المؤتمر السادس لجمعيات المكتبات والمعلومات السعودية، بيئة المعلومات الآمنة المفاهيم والتشريعات والتطبيقات، 6-7 أفريل 2010، الرياض، ص 8-9. أنظر كذلك:

-EL AZZOUZI Ali, op-cit , p 71.

[133]- **خالد بن عبد الله بن معيض العبيدي**، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2009، ص50

[134]- **صالحة العمري**، « **جريمة غسيل الأموال وطرق مكافحتها** »، مجلة الاجتهاد القضائي، العدد الخامس، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، دون سنة نشر، ص179

[135]- « *Le vol consiste en un détournement, à son propre usage ou à l'usage de quelqu'un d'autre, de biens animés ou inanimés de façon temporaire ou permanente. Le vol n'est consommé que lorsque la chose volée est déplacée ou devient amovible* », Voir : **KElCi Sevgi** « ***Vol, fraude et autres infractions semblables et Internet*** », Revu Lex Electronica, vol.12 n°1 ,2007, p 07, disponible sur le site : http://www.lex-electronica.org/articles/v12-1/kelci.pdf

البيانات والمعلومات، والإفادة منها باستخدام السارق للمعلومات الشخصية- مثل الاسم، العنوان، الأرقام السرية- الخاصة بالمجني عليهم، والاستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الإنترنت بحيث تؤدي بالغير إلى تقديم الأموال- الإلكترونية أو المادية- إلى الجاني عن طريق التحويل البنكي[138].

تتجسد جريمة السطو على أموال البنوك عن طريق استخدام الشخص الحاسب الآلي للدخول إلى شبكة الإنترنت والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية، وتحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى[139]، وذلك بإدخال بيانات غير حقيقية أو تعديل أو مسح البيانات الموجودة بقصد اختلاس الأموال أو نقلها أو إتلافها[140]، وتقوم هذه التقنية على الاستيلاء على الأموال بكميات صغيرة جدا من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الأموال[141].

---

[136]- **نايف بن محمد المرواني**، جريمة السرقة (دراسة نفسية اجتماعية)، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2011، ص59.

[137]- ثمة مشكلة في معظم الأنظمة القانونية، تتمثل في أن السرقة لا تكون إلا ضد ممتلكات ملموسة، وإذا كان محل الجريمة معلومات أو بيانات، عندئذ قد تعتبر الممتلكات محل البحث غير ملموسة، وفي مجال الكمبيوتر للمواد والممتلكات معاني مختلفة، ورغم الشكل التقليدي للممتلكات الملموسة، هناك ممتلكات عديدة غير مادية في مجال الإنترنت، وفي هذا الوضع، لدينا أصول ينبغي حمايتها بيد أنها قد لا تندرج تحت التصنيف المعتاد لقوانين التقليدية، **إيهاب ماهر السنباطي**، المرجع السابق، ص20-21

[138]- **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والإنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004، ص138، *أنظر كذلك*: **عمر الفاروق الحسيني« لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات »**، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 1-3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول، الطبعة الثالثة، 2004، ص343. وكذلك:

- **KElCi Sevgi,** op-cit , p 08.

[139]- **عباس أبو شامة، « التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، ونشاطها في الدول العربية»**، الندوة العلمية الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، أيام 28-30جوان 1999، ص 20

[140]- **عارف خليل أبو عيد**، المرجع السابق، ص88، *أنظر كذلك*: **نعيم دهمش، ظاهر شاهر القشي، «مخاطر العمليات المصرفية التي تتم من خلال القنوات الالكترونية»** ،مجلة البنوك، العدد الثاني، المجلد الثالث والعشرون، آذار 2004، الأردن، ص2.

[141]- **وليد عاكوم**، المرجع سابق، ص15.

5- تجارة المخدرات عبر الإنترنت

ظهرت عصر الإنترنت مخاوف من مواقع السوء – إن صح التعبير– وهو تعبير مقارب لصديق السوء، ومن تلك المواقع طبعا المواقع المنتشرة عبر الإنترنت والتي لا تتعلق بالترويج للمخدرات وتشويق النشئ لاستخدامها بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة[142].

والأمر هنا لا يحتاج إلى رفاق سوء بل يمكن للمراهق الانزواء في غرفته والدخول إلى أي من هذه المواقع ومن ثم تطبيق ما يقرأه ويؤكد هذه المخاوف أحد الخبراء التربويين في بتسبيرج بالولايات المتحدة الأمريكية والذي أكد أنه ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات والإنترنت[143].

الفرع الثاني
جرائم واقعة على الأشخاص

يعد الهدف الأول والأسمى لوضع القوانين وسن التشريعات، حماية سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرضون لها، سواء في أبدانهم أو في حياتهم الخاصة، أو في سمعتهم وشرفهم.

تطور الأمر بعد ذلك مع ظهور شبكة الإنترنت، فرغم الفوائد التي أتت بها، والتسهيلات التي قدمتها في الحياة اليومية للفرد والمجتمع على حد سواء، إلاّ أنها أصبحت سلاح فتاك في يد المجرمين ، بالإضافة إلى ذلك فإن المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما يجعلها عرضة للانتهاك والاستعمال من طرف هؤلاء المجرمين، وجعلت سمعة وشرف الأفراد مستباحة.

---

[142]–**محمد محمد صالح الألفي، «أنماط جرائم الإنترنت»**، ص11، متوفر على الموقع التالي: http://www.eastlaws.com

[143]– مشار إليه لدى : **صالح بن سعد الصالح، « مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي»**، الدورة التدريبية مكافحة الجرائم الاقتصادية، جامعة نايف العربية للعلوم الأمنية، كلية التدريب، قسم البرامج التدريبية، الرياض، 10–14 مارس 2007، ص 17.

1- جريمة التهديد والمضايقة والملاحقة

يقصد بالتهديد الوعيد بشر، وهو زرع الخوف في النفس بالضغط على إرادة الإنسان، وتخويفه من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له بها صلة [144]، ويعد تهديد الغير من خلال البريد الإلكتروني واحدا من أهم الاستخدامات غير المشروع للإنترنت، حيث يقوم الفاعل بإرسال رسالة إلكترونية للمجني عليه تنطوي على عبارات تسبب خوفا أو ترويعا لمتلقيها.[145]

تتم في هذا النطاق جرائم الملاحقة عبر شبكة الإنترنت باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة، وتشمل الملاحقة رسائل تخويف ومضايقة، وتتفق مع مثيلاتها خارج الشبكة في الأهداف المجسدة في رغبة التحكم في الضحية، وتتميز عنها بسهولة إمكانية إخفاء هوية المجرم علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة[146].

تجدر الإشارة إلى أن طبيعة جريمة الملاحقة عبر شبكة الإنترنت لا تتطلب اتصال مادي بين المجرم والضحية، ولا يعني بأي حال من الأحوال 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[147].

2- انتحال الشخصية والتغرير والاستدراج

يقصد بانتحال الشخصية ما يعمد إليه المجرم من استخدام شخصية شخص آخر للاستفادة من سمعته مثلاً أو ماله أو صلاحياته، ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين على شبكة الإنترنت، وتتخذ جريمة

144- **محمد عبيد الكعبي**، المرجع السابق، ص88

145- **خالد بن عبد الله بن معيض العبيدي**، المرجع السابق، ص52

146- **إلياس بن سمير الهاجري**، « **جرائم الإنترنت** »، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية المنعقدة بكلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية، 9-13 أفريل 2006، ص58

147- **إلياس بن سمير الهاجري**، المرجع السابق، ص144-145

انتحال الشخصية عبر الإنترنت أحد الوجهين التاليين: انتحال شخصية الفرد وانتحال شخصية المواقع[148].

ولقد سماها بعض المختصين في أمن المعلومات جريمة الألفية الجديدة، وذلك نظرا لسرعة انتشار ارتكابها خاصة في الأوساط التجارية[149].

أما فيما يخص التغرير والاستدراج فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين، إن مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر، وكون معظم الضحايا هم من صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها، حيث لا يدرك كثير من الضحايا أنهم قد غُرر بهم.

---

[148]– **انتحال شخصية الفرد**، عن التنامي المتزايد لشبكة الإنترنت أعطى للمجرمين قدرة أكبر على جمع المعلومات لشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم، فتنتشر في شبكة الإنترنت الكثير من الإعلانات المشبوهة والتي تداعب عادة غريزة الطمع الإنساني في محاولة الاستيلاء على معلوما اختيارية من الضحية، فهناك مثلا إعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية، وهذا يتطلب بطبيعة الحال الإفصاح عن بعض لمعلومات الشخصية كالاسم والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، الأمر الذي يؤدي إلى الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو حتى الإساءة إلى سمعة الضحية.

–**انتحال شخصية المواقع**: مع أن هذا الأسلوب حديثاً نسبيا، إلاّ أنه أشد خطورة، وأكثر صعوبة في اكتشافه، من انتحال شخصية الأفراد، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التي يتم الاتصال بها من خلال نظم الاتصال الآمن، حيث يمكن وبسهولة اختراق مثل هذا الحاجز الأمني، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني، أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين، ثم يقوم بتركيب البرنامج الخاص به هناك، مما يؤدي إلى توجه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور، ويتوقع أن يكثر استخدام أسلوب انتحال شخصية المواقع في المستقبل، نظراً لصعوبة اكتشافها، **محمد بن عبد الله بن علي المنشاوي**، المرجع السابق، ص54–55.

[149]– **عمرو عيسى الفقي**، الجرائم المعلوماتية– جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، 2006، ص102.

3- صناعة ونشر الإباحة

إذا كان لشبكة الإنترنت وجه إيجابي فإن لها وجه سلبي أيضا، ومن هذه الأوجه وجود مواقع على شبكة الإنترنت تحرض على ممارسة الجنس للكبار والصغار على حد سواء، وتقوم هذه المواقع بنشر صور جنسية فاضحة للبالغين والأطفال[150]، وإذا كانت الدعوى لممارسة الجنس الموجه للبالغين يمكن أن تلاقي الرفض لتوافر تمام العقل لديهم، فإن الوضع بالنسبة للطفل يختلف لصغر وعدم اكتمال نضجه العقلي[151].

تعد صناعة ونشر الإباحة جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم الأطفال[152]، حيث يضر استغلال الأطفال المستخدمين في إنتاج هذه المواد ويمثل اعتداءا عليهم في كل مرة يتم فيها عرض هذه الصور، وبهذه الطريقة يظهر كل الأطفال كأهداف للاستغلال الجنسي[153]، ويتخذ الاستغلال الجنسي للأطفال على الإنترنت أشكالا متعددة انطلاقا من الصور ووصولا إلى التسجيلات المرئية للجرائم الجنسية العنيفة، وتستمر معاناة الضحايا حتى بعد انتهاء الاعتداء الفعلي الذي تعرضوا له بسبب إمكان تناقل الصور على الإنترنت إلى ما لا نهاية.

ينتمي معظم منتجي هذه المواد إلى فئتين واسعتين: هم المتربصون جنسيا بالأطفال، وكذلك مجموعات الإجرام المنظم التي تجذبها الأرباح الطائلة المتأتية من

150- **FAUCHOUX Vincent- DEPREZ Pierre**, Op-cit, p 215.

151- **عبد الكريم خالد الشامي، « جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني»**، ص19، مقال متوفر على موقع بوابة فلسطين القانونية، http://www.pal-ip.org . أنظر كذلك:

- **DEBRAY Stéphane,** op-cit, p 13.

152- **خالد محيي الدين أحمد، « الجرائم المتعلقة بالرغبة الإشباعية باستخدام الكمبيوتر »**، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، أيام 19-20 يونيو 2007، ص37، *أنظر كذلك*، **علوي مصطفى، «الضحية المنسية أمام لغة الكبار»**، مجلة الشرطة، تصدر عن المديرية العامة للأمن الوطني، العدد 87، جوان 2008، ص30

153- **كريستينا سكولمان، « عن جرائم الإنترنت: طبيعتها وخصائصها »**، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، أيام 19 و20 يونيو 2007، ص40

الترويج التجاري لمثل هذه الصور[154] ، ولقد عرفت سنوات التسعينات انفجارا في إنشاء المواقع الإلكترونية التي شهدت اتساعا في الجرائم المخلة بالحياء، وذلك بنشر وتوزيع الرسائل والصور والأفلام الإباحية التي تستعمل في عروضها أطفالا ونساء، فأكثر من 470000 موقع إباحي موجود تم التعرف عليها مابين 2004\2006، وأكثر من 600000 صورة لأطفال في وضعيات غير مشروعة[155].

4- جرائم القذف والسّب وتشويه السمعة

تعد جرائم السب والقذف الأكثر شيوعا في نطاق الشبكة، فتستعمل للمساس بشرف الغير أو كرامتهم واعتبارهم، ويتم السب والقذف وجاهيا عبر خطوط الاتصال المباشر أو يكون كتابيا، أو عن طريق المطبوعات، وذلك عبر المبادلات الإلكترونية (بريد إلكتروني، صفحات الويب، غرف المحادثة)[156].

يستعمل الجاني حسب القواعد العامة لجرائم القذف والسب عبارات بذيئة تمس وتخدش شرف المجني عليه، ومهما كانت الوسيلة المعتمدة، مع علمه أن ما يقوم به يعد مساسا بسمعة الغير، بل أن إرادته اتجهت لذلك بالذات، وبالتطور أصبحت الإنترنت إحدى هذه الوسائل إن لم نقل أكثرها رواجا، فعادة ترسل عبارات السب والقذف عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب ما يؤدي بكل من يدخل هذا الموقع لمشاهدتها أو الاستماع إليها، ويتحقق بذلك ركن العلنية الذي تطلبه الكثير من التشريعات

154- **الأنتربول**، الجرائم ضد الأطفال، مقال متوفر على الموقع التالي http://www.interpol.int ، *أنظر كذلك*: **ذياب البداينة**،« **سوء معاملة الأطفال- الضحية المنسية** »، مجلة الفكر الشرطي، المجلد 11، العدد 11، أكاديمية نايف العربية للعلوم الأمنية، الرياض، دون سنة نشر، ص174

155- **أخام بن عودة زواوي مليكة**، «تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية»، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 27-30 أكتوبر 2009، ص18

156- **عبد الرحمن بن عبد الله السند**، الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات (الإنترنت)، دار الوراقين للنشر والتوزيع، بيروت، الطبعة الأولى، 2004، ص312

في السب العلني، وإذا لم يطلع عليها أحد فإنه يمكن تطبيق مواد السب أو القذف غير العلني [157].

تعتبر شبكة الإنترنت مسرحاً غير محدود، فهي تتلقى كل ما يدرج عليها دون قيد أو رقابة، لذلك تشكّل بعض حالات سوء استخدامها حالات سلبية شاذة تؤذي البعض خاصة إذا تمّ التشهير بهم عبر إيراد معلومات مغلوطة[158]، حيث يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن الضحية، والذي قد يكون فرداً أو مجتمع 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[159].

الفرع الثالث

جرائم واقعة على أمن الدول

استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للإنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا منحى آخر في استعمال الإنترنت، التي سمحت لهم في ارتكاب جرائم غاية في الفتك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت الإنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية والاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون بينها نزاعات، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الإنترنت، حيث تعطي الإنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يسهل خلق الفوضى.

---

[157] – **محمد عبيد الكعبي**، المرجع السابق، ص114، *أنظر كذلك*: **سامي علي حامد عياد**، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص77

[158] – **محمد دباس الحميد، ماركو إبراهيم نينو**، المرجع السابق، ص68

[159] – **محمد أمين أحمد الشوابكة**، المرجع السابق، ص31–32

أولاً:الإرهاب

أصبح الإرهاب في الوقت الراهن ظاهرة عالمية، ترتبط بعوامل اجتماعية وثقافية وسياسية وتكنولوجية أفرزتها التطورات السريعة والمتلاحقة في العصر الحديث، فقد شهدت العقود الأخيرة من القرن العشرين بروز العديد من التنظيمات المسلحة والعمليات الإرهابية في مختلف أنحاء العالم[160].

يتم بث ثقافة الإرهاب عبر الإنترنت عن طريق تأسيس مواقع إفتراضية تمثل المنظمات الإرهابية، وهي مواقع آخذة في الازدياد مع ازدياد المنظمات الإرهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى الهجمات التي ارتكبت، أو بيانات تنفي أو تعلق على أخبار صادرة عن منظمات أو جهات دولية أخرى.

تجند الجماعات الإرهابية من خلال الإنترنت عناصر إرهابية جديدة تساعدهم على تنفيذ أعمالهم الإجرامية، وهم في ذلك يعتمدون على فئة الشباب، خصوصا ضعاف العقل والفكر، فتعلن الجماعات الإرهابية عبر مواقعها على الإنترنت عن حاجتها إلى عناصر انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب الديني، فدائما ما تصف الأهداف التي تستهدفها عملياتهم بالكافرة، وتقوم بدعوى الشباب إلى الجهاد وحثهم على الاستشهاد في سبيل الله والفوز بالجنة[161].

الجدير بالذكر أنه إذا كانت الجماعات الإرهابية تسعى إلى الدعاية والترويج لنفسها عن طريق آليات مختلفة منها جذب انتباه وسائل الإعلام المعروفة لتغطية أخبار الجماعة وأنشطتها، إلاّ أن السياسات التحريرية لهذه الوسائل، والمعايير الخاصة بها في نشر أخبار معينة وإسقاط أخرى كل ذلك يمثل قيوداً على استفادة الجماعات من نشر وسائل الإعلام عنها، بينما في المقابل تتيح المواقع الإلكترونية للجماعات الإرهابية قدراً كبيرا من التحكم في المعلومات والرسائل الإعلامية التي تريد توجيهها، بل أيضا تتيح لها المرونة

---

[160]– **عبد الله بن عبد العزيز اليوسف**، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص25.

[161]– **محمد سيد سلطان**، المرجع السابق، ص13.

في توجيه الرسائل لفئات مختلفة من الجمهور المستهدف، ورسم صورة ذهنية عن الجماعة وعن أعدائها أيضاً.[162]

تستخدم الجماعات الإرهابية الإنترنت إلى جانب أغراض 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) [(163)].

ثانياً:الجريمة المنظمة

تعرف الجريمة المنظمة بأنها تعبير عن مجتمع إجرامي يعمل خارج إطار الشعب والحكومة ويضم بين طياته آلاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطوراً وتقدماً، كما يخضع أفرادها لقواعد قانونية سنّوها لأنفسهم وترفض أحكاما بالغة القسوة على من يخرج عن نظام الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من ورائها الأموال الطائلة[(164)].

الجريمة المنظمة ليست وليدة التقدم وإن كانت استفادت منه، فالجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنولوجيا أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، بل أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية، كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة[(165)].

---

[162]– **DEBRAY Stéphane,** op-cit, p 13.

[163]– **مها عبد المجيد صلاح**، المرجع السابق، ص12.

[164]– **نهلا عبد القادر المومني**، المرجع السابق، ص87.

[165]– **سامي علي حامد عياد**، المرجع السابق، ص83.

اكتشفت جماعات الجريمة المنظمة استخدام التكنولوجيات بصفتها فرص للاستغلال وتحقيق أرباح غير مشروعة، وفطن المجرمون أيضاً أن شبكة الإنترنت تستطيع أن تؤمن فرصاً جديدة وفوائد جمة للأعمال غير المشروعة.

يعد الترابط بين الجريمة المنظمة وشبكة الإنترنت ليس طبيعيا فقط، ولكنه ترابط من المرجح أن يتطور إلى حد أبعد في المستقبل، فشبكة الإنترنت تؤمّن الأقنية والأهداف في نفس الوقت للجريمة، وتمكن من استغلال هذه الأقنية والأهداف لتحقيق أرباح كبيرة بأقل قدر ممكن من المخاطر، وجماعات الجريمة المنظمة لا تريد أكثر من ذلك، ولهذا السبب من الأهمية بمكان تحديد بعض الطرق التي تتداخل فيها الجريمة المنظمة حاليا مع الجريمة التي ترتكب من خلال الشبكات الإلكترونية[166].

ثالثا: جريمة التجسس

ينتج عن الاستخدام المتزايد للحاسبات الآلية في العديد من المجلات، تجميع المعلومات بدرجة كبيرة في موضع واحد، ويؤدي هذا التخزين في الحاسبات المركزية إلى سهولة التجسس عليها، وعلى المعلومات المخزنة فيها بمختلف درجات سريتها.

يقصد بالتجسس في هذا الموضع هو الاطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر، وليس مسموحا لغير المخولين بالاطلاع عليها[167].

سهّلت شبكة الإنترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاث أهداف رئيسية، وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي.[168]

كما تمارس العديد من الدول التجسس باستخدام التقنية المعلوماتية، وهذه الأنشطة تمارس من قبل دولة على دولة أو دول أخرى، أو من قبل الدولة على مواطنيها، أو من قبل شركة على شركات أخرى منافسة[169].

---

[166]– **عبد الله عبد الكريم عبد الله**، المرجع السابق، ص42–43

[167]– **محمد عبد الرحيم سلطان العلماء**، المرجع السابق، ص880

[168]– **علي عدنان الفيل**، المرجع السابق، ص96–97

[169]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص154

رابعاً: 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 والصورة، وإذا كنا قد تغيرنا عن آبائنا 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 آثاره على حياتنا لأول مرة، وتغيرنا رغم النقد والتردد، فليس هنالك ما يدعونا لاعتقاد غير ذلك بصدد ثورة المعلومات اليوم وخاصة الإنترنت[170].

بناءا على خصائص الشبكة العالمية للإنترنت، التي منحت المستخدم الكثير من الخيارات، من خلال عدم خضوعها لأي رقابة، وعبورها للحدود الجغرافية بين الدول، ونموها السريع المتواصل، وإمكانية مشاركة الجميع من مختلف دول العالم، مع ما تمنحه من القدرة على التخفي وعدم المواجهة نتيجة للافتراضية 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 الإشراف عليها، كل ذلك جعل هذه الشبكة من أهم مقومات المجتمع المعلوماتي التي تؤدي إلى الانحراف الفكري، من خلال تعرض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العالمية للإنترنت، وتهدد الأمن بأبعاده كافة[171].

---

[170]– **سمير إبراهيم حسن**، « **الثورة المعلوماتية عواقبها وآفاقها** »، مجلة جامعة دمشق، المجلد 18، العدد الأول، 2002، ص213.

[171]– **ناصر بن محمد البقمي**، «**أثر التحول إلى مجتمع معلوماتي على الأمن الفكري**»، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن الفكري بجامعة الملك سعود، المملكة السعودية، 22–25 جمادى الأول 1430هـ، ص18

تتوالى عبر الإنترنت الهجمات الثقافية، والحضارية التي قد تزعزع الأمن الفكري والعقدي للشعوب المغلوبة على أمرها، وتنشر عبرها القوى الغالبة فكرها، ولغتها، وقيمها، وقد ظهر في أدبيات بعض الباحثين مذ بدايات شبكة الإنترنت إشارات التحذير من الغزو الفكري المركز الذي يستقبله الجيل العربي المسلم مما قد يجعله عرضة للهزيمة الفكرية[172].

المطلب الثاني
أركان الجريمة المرتكبة عبر الإنترنت

تتخذ الجريمة المرتكبة عبر الإنترنت من الفضاء الافتراضي مسرحاً لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع، ومجرم يقوم بهذا الفعل، ومن خلال هذا التشابه سوف نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة، حيث نسلك سبيل المقارنة بينها وبين الجريمة التقليدية، وبالتالي نعمد إلى تبيان مدى انطباق مبدأ الشرعية على الجريمة المرتكبة عبر الإنترنت **(الفرع الأول)**، ثم نوضح الركن المادي **(الفرع الثاني)**، لننتهي إلى تحديد الركن المعنوي فيها **(الفرع الثالث)**.

الفرع الأول
الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضح العقاب المترتب عليه وقت وقوع هذا الفعل[173]، فمبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوفر النص القانوني، فلا جريمة ولا عقوبة إلا بنص ، ومتى ما انتفى النص على تجريم مثل

---

[172]– **فايز بن عبد الله الشهري، « التحديات الأمنية المصاحبة لوسائل الاتصال الحديثة دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنت »**، المرجع السابق، ص10

[173]– **عبد المحسن بدوي محمد أحمد، « إستراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيري »**، الندوة العلمية حول الإعلام والأمن، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، الخرطوم 11–13 سنة 2005، ص5

هذه الأفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصور في مكافحة هكذا جرائم[174]، غير أن السؤال المطروح هو مدى تطبيق مبدأ الشرعية على الجرائم التي ترتكب عبر الإنترنت؟

أولاً: مدى انطباق النصوص القائمة على جرائم الإنترنت

تشعب الإشكالات الناجمة عن استخدام الحواسيب الآلية وشبكاتها جعل مهمة القضاء صعبة نظرا لعدم وجود نصوص كفيلة بمعالجة هذه المشكلات، والتي من بينها الاستخدام غير المشروع لشبكة الإنترنت[175].

حاولت قوانين العقوبات مواجهة تحديات الجرائم المرتكبة عبر الإنترنت بطرق تقليدية كتلك المقررة في جرائم الأموال، إلا أنه تبين قصور هذه الوسائل التقليدية عن مواجهة العديد من الأفعال التي تهدد مصالح اجتماعية والتي ارتبطت بظهور وانتشار أجهزة الكمبيوتر.

تبين في بعض الأحوال أن ثمة أفعالا جديدة ترتبط باستعمال الكمبيوتر لا تكفي النصوص القائمة لمكافحتها، من ذلك الاعتداء على حرمة الحياة الخاصة، هذا النوع من الاعتداء لا يعاقب عليه قانون العقوبات إلاّ إذا كان مرتبطا بمكان خاص، أما تجميع معلومات عن الأفراد وتسجيلها في الكمبيوتر، فإنه لا يخضع للتجريم وفقا للقواعد العامة، كما أن التداخل في النظام نظام الحاسب الآلي وتغيير البيانات، فهي صور جديدة لا يعرفها قانون العقوبات قبل ظهور الكمبيوتر وشبكة الإنترنت، كل ذلك يؤكد قصور القواعد التقليدية في القانون الجنائي على مكافحة هذا النوع الجديد من الجرائم[176].

---

[174]- **يونس عرب، « قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان»**، المرجع السابق، ص43.

[175]- **عبد الجبار الحنيص**، المرجع السابق، ص195

[176]- **غنام محمد غنام، « عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر »**، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1-3 ماي 2003، المجلد الثاني، ص625-626.

لا يتطور القانون الجنائي دائما بنفس السرعة التي تتطور بها التكنولوجيا ولا بنفس المهارة التي يأتي بها الذهن البشري لتسخير هذه المبتكرات لاستخدامه السيئ، لذلك وكاستنتاج أولي ومنطقي نعتقد أن القانون الجنائي لا يكفي من حيث المبدأ في مواجهة هذا النمط من الإجرام خاصة أن النصوص قد وضعت للتطبيق وفق معايير معينة كانت سائدة أيام وضعها[177]

ثانيا: الحاجة لتدخل المشرع لمواجهة جرائم الإنترنت

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 الجرائم[178].

تعتبر الولايات المتحدة الأمريكية من بين الدول السباقة التي جسدت تشريع مستقل بشأن جرائم الكمبيوتر بصفة عامة وجرائم الإنترنت بصفة خاصة كما تتميز الولايات المتحدة الأمريكية بوجود أكبر قدر من التشريعات تغطي مسائل جرائم الكمبيوتر والإنترنت والاتصالات[179]

وضعت الولايات المتحدة الأمريكية قانونا خاصا بحماية الحاسوب والشبكات المحوسبة، وذلك عام 1976، وفي عام 1985 حدد معهد العدالة القومي فيها خمسة أنواع رئيسية لهذا النوع من الجرائم وهي:

1-جرائم الحاسوب الداخلية.

2-جرائم الاستخدام غير المشروع عن بعد، شبكات المعلومات المحوسبة.

3-جرائم التلاعب بالحاسوب، أي التلاعب غير المخول وغير المشروع في الشبكات المحوسبة.

---

[177]- **محمد حماد مرهج الهيتي**، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، 2004، ص176.

[178]- **محمد عبيد الكعبي**، المرجع السابق، ص58.

[179]- **يونس عرب**، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، المرجع السابق، ص3.

4-دعم التعاملات الإجرامية للنظم والشبكات المحوسبة، وإسنادها من قبل الآخرين.

5-سرقة البرامج الجاهزة والمكونات المادية.

صدر في عام 1986 قانون آخر يعرف فيه جميع المصطلحات الضرورية لتطبيق جرائم النظم المعلوماتية والشبكات المحوسبة، وعلى أثر ذلك قامت الولايات الأمريكية الداخلية بدورها بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم، والتي تتماشى مع التشريعات الاتحادية المذكورة[180].

قام كذلك المشرع الفرنسي قام بسن تشريع خاص فيما يخص الإجرام المعلوماتي وذلك في أغسطس عام 1986، حيث تقدم النائب "جاك جودفران" 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 ألحق بالباب المخصص بالجنايات والجنح ضد الأشخاص، أي بعد الفصل الثاني من الجرائم المخصصة بالجنايات والجنح ضد الملكية، وقد ركزت اللجنة التشريعية على الهدف الذي توخاه اقتراح "جودفران" حماية النظام المعلوماتي ضد أي اعتداء خارجي، فقررت أن الهدف من النصوص الجديدة تجريم وردع الدخول غير المشروع على برامج المعلوماتية[181].

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

---

[180]- **أحمد بن محمد اليماني**، الحماية الجنائية للبريد الإلكتروني دراسة تأصيلية مقارنة، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في قسم العدالة الجنائية، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات، قسم العدالة الجنائية، الرياض، 2010، ص99.

[181]- **أحمد خليفة الملط**، المرجع السابق، ص126

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 الأفعال غير المشروعة عبر الإنترنت، واكتفائها بتطبيق قواعد قانون العقوبات الخاصة بها، غير أن هذه القوانين أثبتت قصورها في هذا المجال كما أسلفنا الذكر، الأمر الذي يستوجب منها التوسع في تفسير هذه النصوص لتطبيقها على الجرائم المرتكبة عبر الإنترنت.

ثالثا: التوسع في تفسير النصوص القائمة لتطبيقها على جرائم الإنترنت

ليس أمام الدول التي لم تسن بعد قوانين خاصة لتجريم مختلف الجرائم الناشئة عن الاستخدام غير المشروع 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[182].

فعلى الرغم من أن القصور التشريعي قد أصبح 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 ثورة الاتصالات عن بعد، فلا محالة أن التطور قد يوسع من دائرة المجالات التي تحميها نصوص التجريم والعقاب بحيث يمكن أن ندخل في إطارها عناصر أخرى طالما أمكن اعتبارها من جنسها وأن المشرع يحميها بذات هذه النصوص.

يكون اتخاذ سبيل التفسير الموسع للنصوص التقليدية من أجل تطبيقها على الجرائم المرتكبة عبر الإنترنت، بمنح السلطات القضائية حرية تفسير هذه النصوص حيث أن القاضي يمكنه أن يعطي تفسيراً أكثر مرونة للنصوص القانونية يسمح من وضع هذه الجرائم تحت طائلة التجريم والمتابعة، وذلك في ظل السلطة التقديرية التي يتمتع بها القاضي.

---

[182] – **محمد عبيد الكعبي**، المرجع السابق، ص52.

فعندما تعرض قضية جزائية على القاضي فإن أول عملية يقوم بها هي تكييف الواقعة لمعرفة مدى تطابقها مع النص الذي يجرمها، وللوصول إلى هذه الغاية يقوم القاضي باستخلاص عناصر الواقعة من النص، وقد يصادف القاضي أثناء ذلك صعوبة أو غموضا فيقوم عندئذ بتفسير النص الجنائي[183].

لكن تطبيق هذه النصوص التقليدية بمفهومها الموسع والخاصة ببعض الجرائم كالسرقة على سبيل المثال على الجرائم الواقعة بطريق الإنترنت من شأنه المساس بمبدأ الشرعية الجنائية، إذا ترك الأمر بيد القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله[184].

الفرع الثاني

الركن المادي

ينطلق مبدأ تحديد الفعل غير المشروع وإعطائه 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 الجرائم المرتكبة من قبل الجاني، شريطة أن يكون له مظهر خارجي ملموس، غير أن تحديد الركن المادي في الجرائم الواقعة عبر الشبكة العالمية للإنترنت تكتنفه العديد من الصعوبات خاصة فيما يتعلق بتحديد النتيجة الإجرامية والرابطة السببية، وسوف نبيّن الركن المادي في هذا النطاق كالآتي:

أولا: القواعد العامة في الركن المادي للجريمة

1-السلوك الإجرامي

يعد السلوك الإجرامي أهم عناصر الركن المادي لأي جريمة، لأنه يكشف عن سلوك مخالف لإرادة المشرع، ويبدو بمظاهر مادية ملموسة في العالم الخارجي، ويعني ذلك أن الأفكار داخل النفس لا عقاب عليها.

---

[183]- **بارش سليمان**، مبدأ الشرعية في قانون العقوبات الجزائري، دار الهدى، عين مليلة، 2006، ص18.

[184]- **محمد عبيد الكعبي**، المرجع السابق، ص53.

يعرف السلوك الإجرامي في الجرائم التقليدية على أنه فعل الجاني الذي يحدث أثر في العالم الخارجي، وبغير هذا السلوك لا يمكن محاسبة الشخص مهما بلغت خطورة أفكاره وهواجسه الداخلية، والسلوك هو الذي يخرج النية والتفكير في الإجرام إلى حيز الوجود واعتبار القانون، ولا يكاد يفرق بين السلوك الإيجابي (الفعل) والسلوك السلبي (الامتناع عن فعل)، مادام أن لهما نفس النتيجة.

أ-السلوك الإيجابي:

يكون في صورة فعل أو قول يجرمه القانون يصدر عن الجاني ويؤدي إلى إحداث نتيجة في الجرائم ذات النتيجة وكذلك يعتبر سلوكا إجراميا في ذاته في الجرائم الشكلية، ولا يهتم القانون بالوسيلة سواء كانت مادية أو معنوية، فإذا كان السلوك محظوراً قانوناً فهو يشكل جريمة، وكذلك إذا أدّى إلى نتيجة منعها القانون ويدخل ضمن السلوك الإيجابي فعل السرقة، والقتل والضرب والنصب، وشهادة الزور، والبلاغ الكاذب والتحريض على الجريمة، والغش والتدليس وغيرها من السلوكيات[185].

ب- السلوك السلبي:

يتمثل هذا الفعل بسلوك أو موقف يتخذه المكلّف بقاعدة قانونية تفرض عليه أن يعمل فلا يعمل، ففي هذه الحالة يقوم المكلف بالحيلولة دون جسمه كله أو بعضه وبين الحركة التي يتطلبها القانون، أو قد يتحرك باتجاه مضاد لما أمره به.

يقوم الفعل السلبي على الامتناع أو إحجام شخص عن القيام بعمل يوجبه عليه القانون إذا كان باستطاعته القيام به، وعليه فلا يجوز للقاضي أن يمتنع عن الحكم بالدعوى ولا للشاهد أن يمتنع عن الإدلاء بشهادته أمام المحكمة بواقعة يعلمها ولا للموظف أن يمتنع عن أداء مهام وظيفته[186].

---

[185]- **منصور رحماني**، الوجيز في القانون الجنائي العام، دار العلوم للنشر والتوزيع، عنابة، 2006، ص94.

[186]- **عبد الله سليمان**، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول(الجريمة)، ديوان المطبوعات الجامعية، الجزائر، 1995، ص148.

2- النتيجة الإجرامية:

يقصد بالنتيجة الإجرامية، الأثر المادي الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي، فالسلوك قد أحدث تغييرا حسيا ملموسا في الواقع الخارجي، ومفهوم النتيجة كعنصر في الركن المادي للجريمة يقوم على أساس ما يعتد به المشرع ويرتب عليه نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى[187].

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 السببية تلازماً مادياً بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولاً عن النتيجة التي تحققت، أما إذا كانت الجريمة غير عمدية، فإن نفي رابطة السببية يؤدي إلى انتفاء المسئولية كلية عنها، ذلك أنه لا شروع في الجرائم غير العمدية[188].

ثانيا: تحديد الركن المادي في الجريمة المرتكبة عبر الإنترنت

تحديد الركن المادي في الجرائم المرتكبة عبر الإنترنت يثير 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، ومكان البداية واكتمال الركن المادي، وأجزاء السلوك الإجرامي المرتكب في العالم المادي، أو العالم الافتراضي، وغيرها من التساؤلات التي تتعلق بطبيعة الجريمة.[189]

---

[187]- **عبد الله سليمان**، المرجع السابق، ص149.

[188]- **أشرف توفيق شمس الدين**، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، طبعة خاصة لطلاب التعليم المفتوح بكلية لحقوق بجامعة بنها، دون دار نشر، 2009، ص82.

[189]- **منصور بن صالح السلمي**، المرجع السابق، ص76

يتطلب النشاط أو السلوك المادي في جرائم الإنترنت وجود بيئة رقمية واتصال بالإنترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها أشياء أو صور مخلة بالآداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات[190] تمهيدا لبثها.

ليس كل جريمة تستلزم وجود أعمال تحضيرية، إلاّ أنه يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الإنترنت- حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية- ففي مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

يتمثل النشاط المادي في الجريمة المرتكبة عبر الإنترنت في الدخول غير المشروع في نظم وقواعد معالجة البيانات، سواء ترتب عن هذا الدخول غير المشروع تلاعب بهذه البيانات أم لا، إذ أن مجرد الدخول غير المشروع لمواقع المعلومات والبرامج جريمة مرتكبة عبر الإنترنت، وقد يتخذ هذا النشاط الإجرامي عدة صور كانتهاك السرية خصوصية للبيانات الشخصية والإضرار بصاحبها والاطلاع على المراسلات الإلكترونية، والإدلاء بالبيانات الكاذبة في إطار المعاملات والعمليات الإلكترونية يعد كذلك من أهم صور الركن المادي للجريمة المرتكبة عبر الإنترنت[191].

---

[190]- يتصف برنامج الفيروس بأن له تأثير كبيرا على برامج الحاسب الآلي لما له من قدرة على إحداث تغيير في البرامج والبيانات المتداولة على الحاسب تصل إلى حد الإتلاف الكلي للبرامج، ويلاحظ أن مصطلح الفيروس نشأ مع الأيام الأولى لاختراع الحاسب وكان رائد علم الحواسيب وهو يدعى "جون فاننيومان" هو الذي قام بوضع أسس هذا الفيروس سنة 1949 عندما نشر مقالا أطلق عليه (نظرية وأنظم الأوتوماتا المعقدة) والتي كانت أساسا لوضع فكرة الحاسبات التجارية والتي بدأت تظهر بعد ذلك بسنوات، وتبنى بعد ذلك مجموعة من العلماء النظرية وطوروا أبحاثهم في هذا الاتجاه مما أدى إلى بداية ظهور الفيروسات سنة 1959 على هيئة كود غريب يظهر في حواسيب بعض الشركات بعد عدة ساعات من العمل، **أيمن عبد الحفيظ**، المرجع السابق، ص58

[191]- **عبد الرزاق السندالي**، « **التشريع المغربي في الجرائم المعلوماتية** »، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، 19_20 يونيو 2007، ص69

مجمل القول أن السلوك الإجرامي في الجريمة المرتكبة عبر الإنترنت يرتبط بالمعلومة المخزنة داخل الحاسب الآلي أو انتهاك حرمة الأشخاص، والسلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب الآلي فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك مثلاً[192].

تثير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة، فهل تقتصر على العالم الافتراضي، أم أن لها جزءا في العالم المادي، وهل تقتصر النتيجة على مكان واحد أو تمتد لتشمل دولا وأقاليم عدة[193]، فعلى سبيل المثال إذ قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم أحد البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين

تحديد رابطة السببية في مجال أضرار الإنترنت يعد من المسائل الصعبة والمعقدة بالنظر إلى تعقيدات صناعة الحاسوب والإنترنت، وتطور إمكانياتها وتسارع هذا التطور، إضافة إلى تعدد وتنوع أساليب الاتصال بين الأجهزة الإلكترونية وتعدد المراحل التي تمر بها الأوامر المدخلة حتى تخرج وتنفذ النتيجة المراد الحصول عليها، كل ذلك سيؤدي حتما إلى صعوبة تحديد السبب أو الأسباب الحقيقية للإساءات المرتكبة في هذه المسؤولية[194].

الفرع الثالث

الركن المعنوي

يعتبر الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويطلق عليه الركن الأدبي أو الشخصي وهو يعني في الحقيقة الجاني أو المجرم تحديداً، فالركن المعنوي هو المسلك الذهني أو النفسي للجاني باعتباره

---

[192]– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، مصر،2009، ص113–114.

[193]– **منصور بن صالح السلمي**، المرجع السابق، ص76

[194]– **منصور بن صالح السلمي**، المرجع السابق، ص75–76.

محور القانون الجنائي، من إسناد وإذناب مع إقرار حق الدولة في العقاب الذي يبني على المقومات[195]، هذا على العموم في جميع الجرائم، غير أن التساؤل يثور في مجال الجرائم المرتكبة عبر الإنترنت، فهل المقومات التي تحكم الركن المعنوي في الجرائم التقليدية هي نفسها في الجرائم المرتكبة عبر الإنترنت؟

أولا: الركن المعنوي في نطاق الجريمة التقليدية

يتمثل الركن المعنوي في ظل الجرائم التقليدية في:

1-عناصر القصد الجنائي

أ-العلم

لا يتحقق القصد الجنائي إلاّ إذا كان الجاني يعلم بالعناصر الأساسية لقيام الجريمة سواء تعلق ذلك بسلوكه الإجرامي أم بموضوع الاعتداء، فإذا كان الجاني جاهلاً بشيء من ذلك فلا يتحقق القصد الجنائي، ففي جريمة السرقة لا يتحقق القصد الجنائي إلاّ إذا كان الجاني يعلم أن المال المسروق ملك لغيره، ولا يتوافر القصد في جريمة التسميم إلاّ إذا كان الجاني يعرف أن الطعام الذي قدمه إلى المجني عليه يحتوي على السم، فالذي يأخذ مال غيره معتقداً أنه ماله، أو الذي يطعم غيره طعاما مسموما وهو يجهل ذلك، ففي كلاهما لا يتوفر القصد الجنائي، وليس كل جهل ينتفي معه القصد الجنائي، بل هناك وقائع يؤثر الجهل بها في القصد، وأخرى لا يتأثر بها القصد[196].

ب-الإرادة

الإرادة هي نشاط نفسي يهدف إلى تحقيق غرض معين، فإذا كان غرض الجاني تحقيق نتيجة إجرامية، كانت الإرادة المتجهة إلى الفعل المنطوي على إحداث النتيجة هي "القصد الجنائي"، والغرض هو الهدف القريب الذي تتجه إليه الإرادة، أما الباعث فهو عبارة عن الدافع إلى إشباع حاجة معينة، وهذا الدافع له طبيعة نفسية، بخلاف الغاية التي لها طبيعة موضوعية، فإذا أراد الجاني أن يسرق المجني عليه لضائقة مالية مر بها،

---

[195]- **منصور بن صالح السلمي**، المرجع السابق ، ص68.

[196]- **منصور رحماني**، المرجع السابق، ص108.

كانت الغاية التي يسعى لها هو الحصول على المال، وأما الغرض فهو قتل المجني عليه لسرقته، فهذا الغرض يتصور الجاني تحقيقه بطعن المجني عليه لقتله والاستيلاء على ماله، فيوجه إرادته لهذا الغرض، أما الباعث على فعله فهو التخلص من الديون التي تثقل كاهله[197].

2-صور القصد الجنائي

أ-القصد الجنائي العام

يهدف الجاني عند ارتكابه الواقعة الإجرامية مع العلم بعناصرها إلى تحقيق غرض معين، بتحقيقه قد تتم الجريمة ويتوافر لها القصد الجنائي العام، ففي جريمة القتل يكون غرض الجاني إزهاق روح المجني عليه، وفي جريمة السرقة غرض الجاني حيازة المال المسروق، وفي جريمة الرشوة يكون غرض الجاني الحصول على منفعة من الراشي، وعليه فالقصد العام أمر ضروري ومطلوب في كل الجرائم العمدية[198].

ب-القصد الجنائي الخاص:

يلتقي القصد الخاص مع القصد العام في جميع عناصره، ويزيد عنه في تحديد الإرادة الإجرامية لدى الجاني إما بباعث معين قد يدفعه إلى الجريمة، وإما بنتيجة محددة يريدها، وحكمة هذا التحديد هي الرغبة في توضيح هذه الجريمة وتمييزها عن غيرها من الجرائم التي تشترك معها في بعض العناصر[199]

ثانيا: تحديد الركن المعنوي في الجريمة المرتكبة عبر الإنترنت

يكتسي تحديد الركن المعنوي بالغ الأهمية في الجريمة المرتكبة عبر الإنترت، كما هو الحال بالنسبة للجريمة المرتكبة في العالم المادي، حيث بموجبه يمكن تحديد مناط مسائلة الجاني، وذلك بتحديد القصد الجنائي لديه، الذي بدونه لا يمكن أن يعاقب الشخص المرتكب للفعل.

---

[197]- **أشرف توفيق شمس الدين**، المرجع السابق، ص155.

[198]- **عبد الله سليمان**، المرجع السابق، ص261

[199]- **منصور رحماني**، المرجع السابق، ص112.

يتلاقى القصد الجنائي بصورتيه العام والخاص في الجرائم المرتكبة عبر الإنترنت مع مثيله في الجرائم التقليدية في عدة نقاط، منها العلم والإرادة، فالمجرم يجب أن يكون عالم بأن الفعل الذي يقوم به يعتبر فعل غير مشروع، وذلك بإرادة صريحة من أجل إحداث الضرر للمجني عليه.

أما القصد الخاص فيلتقي مع القصد العام في الكثير من عناصره، ويزيد عنه في تحديد الإرادة الإجرامية لدى الجاني إما بباعث معين قد يدفعه إلى الجريمة، وإما بنتيجة محددة يريدها، وحكمة هذا التحديد هي الرغبة في توضيح هذه الجريمة وتمييزها عن غيرها من الجرائم التي تشترك معها في بعض العناصر[200].

ولتبيان الفرق بين القصد الجنائي العام والقصد الجنائي الخاص، فإن القصد الجنائي العام يقوم على العلم والإرادة، كما يقوم القصد الجنائي الخاص على العلم والإرادة، غير أنه يمتاز عنه بأن العلم والإرادة فيه لا يقتصران على أركان الجريمة وعناصرها، وإنما يمتدان بالإضافة إلى ذلك إلى وقائع ليست في ذاتها من أركان الجريمة، وإذا تطلب القانون في جريمة توافر القصد الخاص فمعنى ذلك أنه يتطلب أولا انصراف العلم والإرادة إلى أركان الجريمة، وبذلك يتوافر القصد العام، ثم يتطلب بعد ذلك انصراف العلم والإرادة إلى وقائع لا تعد طبقا للقانون من أركان الجريمة، وبهذا الاتجاه الخاص للعلم والإرادة يقوم القصد الخاص، ولقيام الركن المعنوي في الجرائم المرتكبة عبر الإنترنت، لابد أن يعلم الجاني أنه يرتكب من خلال شبكة الإنترنت أحد الأفعال التي يتضمنها نص التجريم، وأن تتجه إرادته إلى القيام بذلك الفعل[201].

يقوم الركن المعنوي للجريمة المرتكبة عبر الإنترنت على أساس مجسد في توافر الإرادة الآثمة لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرّمه القانون، كانتحال شخصية المزود عبر الإنترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجرمية المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة الجرمية

---

[200]– **منصور رحماني**، المرجع السابق، ص112.

[201]– **منصور بن صالح السلمي**، المرجع السابق، ص78.

من العمل غير المشروع الذي بيت النية على ارتكابه، وهو عالم بالآثار الضارة الناشئة عنه[202].

يعد تبيان مفهوم الركن المعنوي في الجرائم المرتكبة عبر الإنترنت من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص المادية التي يلزم تطبيقها، إذ بدون الركن المعنوي لن يكون هناك سوى جريمة الدخول غير المشروع، لذلك فإن اتجاه القضاء المقارن في تطلب العمد بالنسبة لجريمة الدخول فقط يعد من الموضوعات المنفذة هنا[203].

نستنتج أنه لقيام أي جريمة يجب أن يتوافر الركن المعنوي بكل عناصره وصوره إلى جانب الأركان الأخرى، لأن الحالة النفسية للجاني بصفة عامة أو القصد بصفة خاصة هو الذي يحدد لنا مسؤولية الفاعل من عدمها، فمثلا لا يمكن أن نحاسب شخص مسلوب الإرادة الذي استكره على فعل أشياء معتبرة غير مشروعة في نظر القانون، بل يجب أن يكون ذا إرادة واضحة لكي تتم مسائلته.

غير أنه ورغم هذا التوافق بين جميع الجرائم في وجوب توافر الركن المعنوي فيها، إلاّ أن هناك استثناءات فيما يخص الجريمة المرتكبة عبر الإنترنت، وذلك في ظل الطبيعة اللامادية للجريمة، والسرعة في ارتكابها، حيث لا تدع المجال لتحديد الفعل من عدمه فما بالك بتحديد القصد الجنائي فيها، بالإضافة إلى اختلاف طبيعة المجرمين، حيث ينفرد المجرمون الذين يقومون بأفعالهم غير المشروعة عبر الإنترنت عن نظرائهم في الجريمة التقليدية فيما يخص الباعث.

يتباين الركن المعنوي في الجريمة المرتكبة عبر الإنترنت بتباين الباعث الذي يدفع الجاني لارتكاب أفعاله، فكما أسلفنا الذكر، ليس كل المجرمين عبر الإنترنت لهم نية في الإجرام، فبالرغم من أن هناك من المجرمين من يسعى لتحقيق أغراض مادية أو سياسية

---

[202]– **عبد الله ذيب عبد الله محمود**، حماية المستهلك في التعاقد الإلكتروني دراسة مقارنة، رسالة قدمت استكمالا لمتطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، سنة 2009، ص96.

[203]– **منصور بن صالح السلمي**، المرجع السابق، ص68

أو إيديولوجية، إلاّ أنه هناك من الأفراد من يقوم بأفعاله من أجل التعلم أو لمجرّد التسلية في بعض الأحيان، مما يجعل في هذه الحالة تحقق شرط القصد الجنائي منعدم، ومنه لا يتوافر الركن المعنوي في كذا جرائم.

يعتبر الباعث الدافع النفسي لتحقيق سلوك معين بالنظر إلى غاية محددة يريدها الجاني[204]، فالباعث في الجرائم المرتكبة عبر الإنترنت يعد من الصعوبات التي تعوق الوصول إلى تحديد العقوبة لمقترف الفعل المجرم، وذلك لانعدام القصد الجنائي، فمثلا إذا اخترق أحد القراصنة الهواة قاعدة بيانات لشركة معينة من أجل التعلم أو من أجل التسلية دون علمه أن هذا الفعل مجرم ينتفي هنا الركن المعنوي للجريمة.

غير أن الملاحظ على هذه الأفعال، وبالرغم من عدم توافر القصد الجنائي فيها، إلاّ أنها تسبب أضرارا وخسائر فادحة لدى الجهة المجني عليها تفوق أضرار الجريمة التقليدية، غير أن انتفاء القصد الجنائي يعفي الجاني من المسائلة، وبالتالي يتم ضياع حقوق الجهة المجني عليها، ومنه يستحسن إيجاد سبيل للحد من هذه الصعوبة، وذلك بمسائلة الجاني على أساس الضرر الذي ألحقه بالمجني عليه أو الاكتفاء بتوفر الركن المادي والشرعي للجريمة.

[204]– **منصور رحماني**، المرجع السابق، ص113

الفصل الثاني

مكافحة الجريمة المرتكبة عبر الإنترنت

صاحب ظهور شبكة الإنترنت بروز تحديات جديدة للمنظومة القانونية الموضوعية والإجرائية عل المستوى الدولي والمحلي، 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 الأضرار والخسائر التي انجرت عنها فادحة على المستويين الدولي والمحلي، الأمر الذي أدّى بمختلف الدول إلى الإسراع من أجل المحاولة للتصدي لهذه الظاهرة [205]، فتضافرت الجهود من أجل إيجاد سبل مكافحة الجريمة المرتكبة عبر الإنترنت بنجاعة وفعالية أكثر **(المبحث الأول)**

يتضح لنا جليا خطورة الجرائم المرتكبة عبر الإنترنت الأمر الذي يوجب الكثير من الجهد لمكافحتها، لكنها تبقى بعيدة كل البعد عن الأسس السليمة والخاصة بها، حيث أن الإجراءات التقليدية المطبقة على هذا النوع من الجرائم لم تعد مجدية نظرا لاختلاف الجرائم التقليدية وجرائم الإنترنت، فعدم كفاية التشريعات الخاصة بها وتباينها، 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 جريمة عابرة للحدود **(المبحث الثاني)**

المبحث الأول

طرق مكافحة الجريمة المرتكبة عبر الإنترنت

تتجسد أول طرق مكافحة الجرائم المرتكبة عبر الإنترنت في الاستدلال الذي يتضمن كل من التفتيش والمعاينة والخبرة، والتي تثير إشكالات إجرائية تعود إلى خصوصية

[205]– *Une coopération internationale est indispensable, car les pays qui ne se pas dotés de lois contre la cybercriminalité sont des paradis numérique* .Voir : **CHERNAOUTI-HELI Slange,** op-cit , p 26.

الجريمة المرتكبة عبر الإنترنت[206]، أما غيرها كالاستجواب والمواجهة وسماع الشهود فإننا نستبعدها في هذه الدراسة نظرا لعدم وجود أي صعوبات في اتخاذها. **(المطلب الأول)**

أما ثاني سبل مكافحة الجريمة المرتكبة عبر الإنترنت هي تلك الجهود الدولية والداخلية لتجسيد منظومة قانونية للوقاية من هذه الجريمة المستحدثة، فأما الدولية تتمثل في جهود الهيئات والمنظمات الدولية والإقليمية، وأما فيما يخص التشريعات الداخلية فسنتطرق إلى التجربة الجزائرية **(المطلب الثاني)**.

المطلب الأول

الاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت

يعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حدد المشرع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية، وتتمثل في وسائل الإثبات الرئيسية في التفتيش **(الفرع الأول)**، والمعاينة **(الفرع الثاني)** والخبرة **(الفرع الثالث)**.

الفرع الأول

التفتيش

يمكن تعريف التفتيش بأنه إجراء من إجراءات التحقيق يقوم به موظف مختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم[207]، هذا في الجرائم التقليدية،

---

[206]– *L'un des principaux défis que représente la lutte contre la cybercriminalité concerne la collecte de preuves destinées aux procès. De nos jours, la rapidité des communications exige une réaction fulgurante de la part des organismes chargés de faire appliquer la loi. Une possibilité pour la sauvegarde de la preuve se trouve dans les journaux du réseau qui fournissent des informations sur les personnes ayant accédé à telle ou telle ressource de l'Internet et à quel moment elles l'ont fait.* Voir : **KURBALIJA Jovan, GELBSTEIN Eduardo,** op-cit, p100.

[207]– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص192، أنظر كذلك: **أحمد عيد بن حرب العطوي**، التفتيش ودوره في الإثبات الجنائي، مشروع مقدم كمطلب تكميلي ضمن

لكن التساؤل يثور عندما نكون بصدد تفتيش عن حيثيات جريمة مرتكبة عبر الإنترنت حول مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش؟

أولا: المكونات المادية للحاسب

لا يختلف اثنان في أن الولوج إلى المكونات المادية للحاسب الآلي بحثا عن شيء ما يتصل بجريمة من جرائم الإنترنت، 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 وهل هو من الأماكن العامة أو من الأماكن الخاصة، حيث أن صفة المكان وطبيعته أهمية قصوى، 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 الأخرى أو متصلة بحاسب آلي آخر أو بنهاية طرفية في مكان آخر كمسكن غير المتهم مثلاً[208].

فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير 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، أوكانت من الأماكن العامة بالتخصيص كالمقاهي المطاعم والسيارات العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[209].

متطلبات برنامج التخصص المتقدم في مكافحة الجريمة "القسم الخاص" لحصول على درجة الماجستير في مكافحة الجريمة، المركز العالي للدراسات الأمنية، المعهد العالي للعلوم الأمنية، قسم العلوم الشرطية، الرياض، 1987، ص12

[208]– **حسين بن سعيد الغافري، «التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت»**، ص11، مقال متوفر على الموقع التالي: http://www.eastlaws.com

[209]– **طارق إبراهيم الدسوقي عطية**، المرجع السابق، ص379_380

ثانيا: المكونات المنطقية للحاسب الآلي

أثار تفتيش المكونات المنطقية للحاسب الآلي 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 بالضبط "أي شيء"، فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسب المحسوسة وغير المحسوسة.[210]

ذهب رأي آخر 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.

يوجد في مقابل هذين الرأيين يوجد رأي آخر نأى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الحاسب الآلي أم لا، فذهب إلى أن النظر في ذلك يجب أن يستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلا ماديا[211].

ثالثا: شبكات الحاسب الآلي

عَقّدت طبيعة التكنولوجيا الرقمية التحدي أمام أعمال التفتيش، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة وبعيدة تماما عن الموقع المادي للتفتيش، وإن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية

---

[210]– **أمير فرج يوسف**، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2008، ص224

[211]– **علي محمود علي حمودة، «الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي»**، ص22_23، مقال متوفر على الموقع التالي http://www.arablawinfo.com

الجاري تفتيشها[212]، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، إلا أن السلطات في ذلك الاختصاص السيادي قد تشعر ببالغ الانزعاج وهذا يزيد من تعقيد مشاكل الجريمة المرتكبة عبر الإنترنت العابرة للحدود ويزيد من أهمية تبادل المساعدة القانونية، ونستطيع أن نميز في هذه الصورة بين ثلاثة احتمالات على النحو التالي[213]:

أ-الاحتمال الأول: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر 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 آخر مملوك لشخص غير المتهم؟

يرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استناداً إلى مقتضيات القسم 103 من قانون الإجراءات الجزائية الألماني[214]"، ونجد انعكاسات هذا الرأي في المادة 88 من قانون تحقيق الجنايات البلجيكي التي تنص على:

« إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقا لضابطين :

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

ب- إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث » [215]

---

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

[213]- **حسين بن سعيد الغافري**، «**التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت**»، المرجع السابق، ص12

[214]- المرجع نفسه، ص13

[215]- **محمد أبو العلا عقيدة**، المرجع السابق، ص10

ب . الاحتمال الثاني: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة.

تواجه سلطة الادعاء في جمع الأدلة عدة مشاكل، كقيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية مستهدفين عرقلة الادعاء في جمع الأدلة والتحقيقات وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة المختصة التي صدر من جهتها الإذن ودخوله في المجال الجغرافي للدولة أخرى وهو ما يسمي بالولوج أو التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها.[216]

يرى أن جانب من الفقه أن التفتيش الإلكتروني العابر للحدود لا بد أن 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 الأقل الحصول على إذن الدولة الأخرى وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم المرتكبة عبر الإنترنت.

وكتطبيق لهذا الإجراء الأخير: ما حدث في ألمانيا أثناء جمع إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب آلي، حيث تبين وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها، وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، فلم تتمكن من ذلك إلا عن طريق التماس المساعدة، الذي تم بالتبادل بين الدولتين[217]، ومع ذلك أجازت المادة 32 من الاتفاقية الأوربية بشأن جرائم الإنترنت، إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين: الأولى إذا تعلق التفتيش

---

[216]– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص381_382

[217]– **طارق إبراهيم الدسوقي عطية**، المرجع السابق، ص389

بمعلومات أو بيانات مباحة للجمهور، والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش[218].

ج. الاحتمال الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي

عرفت لجنة الخبراء للبرلمان الأوروبي في اجتماعها بستراسبورغ بتاريخ 2006/10/06 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية اعتراض المراسلات بأنها، عملية مراقبة للمراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجرائم[219].

سمحت جميع الدول تقريبا بالتنصت والأشكال الأخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنها أقرت بها تحت ظروف معينة، فالقانون الفرنسي الصادر في 1991/7/10، 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.[220]

أخذ المشرع الجزائري بقابلية إجراء التنصت من خلال قانون الإجراءات الجزائية حيث نصت المادة 65 مكرر 5 منه على:

« إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة

---

[218]– **محمد أبو العلا عقيدة**، المرجع السابق، ص10

[219]– **لوجاني نور الدين، «أساليب البحث والتحري الخاصة وإجراءاتها وفقا للقانون رقم 22/06 المؤرخ في 2006/12/20»**، يوم دراسي حول: علاقة النيابة العامة بالشرطة القضائية–احترام حقوق الإنسان ومكافحة الجريمة– يوم 12 ديسمبر 2007، بمقر أمن ولاية إيليزي، ص8.

[220]– **حسين بن سعيد الغافري، « التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت »**، المرجع السابق، ص14.

بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يلي:

-اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

-وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.... » [221]

نستخلص من نص المادة 65 مكرر5 من قانون الإجراءات الجزائية الجزائري، أن المقصود باعتراض المراسلات، اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهاته المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض[222].

الفرع الثاني
المعاينة

تعد المعاينة من المراحل الأولى للاستدلال حول ملابسات الجريمة، ومن أهم المراحل على الإطلاق، نظراً لما يمكن أن توفره من أدلة إثبات الجريمة، وتزداد أهميتها في الجرائم المرتكبة عبر الإنترنت، وذلك راجع إلى الطبيعة الخاصة للسلوك الإجرامي فيها، بالإضافة إلى اعتبارها من الجرائم المستحدثة، مما استوجب ابتكار إجراءات خاصة بالمعاينة في هذا المجال.

أولا: مفهوم المعاينة

تأتي المعاينة لغةً بمعنى النظر، وعاين الشيئ رآه بعينه، ودلالتها في اللغة تشير بمعناه الواسع إلى الرؤية والمشاهدة، ودلالتها القانونية وخاصة في المجال الجنائي، هي التي تعتمد على حاسة البصر، وتبعا لذلك تعني المعاينة رؤية أماكن ارتكاب الوقائع

---

[221]- المادة 65 مكرر5 من قانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية رقم 84

[222]- **لوجاني نور الدين**، المرجع السابق، ص8

الجنائية، كما تنصرف إلى فحص جسم المجني عليه، والمتهم واثبات ما يوجد بها من آثار، وعرفها جانب من الفقه، بأنها مشاهدة واثبات الحالة في مكان الجريمة.

وفي محاولة لتجاوز جوهر المعاينة لمجرد الرؤية والمشاهدة، وعدم انحسارها أو اعتمادها على حاسة النظر، عرّف بعض الفقه المعاينة بأنها:

"***إثبات مباشر ومادي لحالة الأشخاص والأمكنة ذات الصلة بالحادث، عن طريق رؤيتها أو فحصها فحصا حسيا مباشراً***"، وبعض الفقه عرفها بأنها:

"***إثبات لحالة الأماكن والأشخاص، وكل ما يفيد في كشف الحقيقة عن الجريمة ومرتكبه***"[223].

يتبين لنا من خلال المفاهيم والدلالات السابقة، أن جوهر المعاينة هو ملاحظة وفحص حسي مباشرة لمكان أو شخص أو شخص أو شيئ له علاقة بالجريمة، لإثبات حالته، والكشف والتحفظ على كل ما قد يفيد من الأشياء، في كشف الحقيقة[224].

يجوز الإلتجاء إلى المعاينة في كافة الجرائم، وهي إجراء هادف غايته كشف وصيانة العناصر المادية التي تتعلق بالجريمة، وتفيد في التحقيق الجاري بشأنها، فإذا انعدمت بالنسبة للتحقيق جدواها وفائدتها لم تكن ثمة مجال أو مقتضى لإجرائها، ولا تجدي في كشف الحقيقة بشأنه المعاينة، مثل جريمة التزوير المعنوي وجريمة القذف والسب التي تقع بالقول في غير العلانية وغيرها[225]. والسؤال الذي يطرح نفسه الآن هو ما إمكانية معاينة مسرح الجريمة المرتكبة عبر الإنترنت؟

ثانيا: مسرح الجريمة المرتكبة عبر الإنترنت

ينبغي عند الشروع في جمع الأدلة من مسرح جريمة الحاسوب والإنترنت، التعامل معه على أنه مسرحين.

223– **محمد علي أحمد الكواري**، مسرح الجريمة ودوره في كشف غموض الجريمة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص44

224– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص529

225– **هشام محمد فريد رستم**، المرجع السابق، ص483

– مسرح تقليدي: ويقع خارج بيئة الحاسوب، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى المسرح أية جريمة تقليدية قد يترك فيها الجاني آثار عدة، كالبصمات وغيرها، وربما تركك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.

–مسرح سيبراني: ويقع داخل بيئة الحاسوب، ويتكون من البيانات الرقمية التي تتواجد وتنقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الأقراص الصلبة الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع[226].

ثالثا: أهمية المعاينة في الجريمة المرتكبة عبر الإنترنت

تكمن أهمية وجدارة المعاينة عقب وقوع جريمة من الجرائم التقليدية في أنها تتبوأ مكانة الصدارة على ما عداها من الإجراءات الاستقصائية الأخرى، بحكم مركز المحورية لدورها في تصور كيفية وقوع الجريمة، وظروف وملابسات ارتكابها وتوفير الأدلة المادية من المادة التي تجمع عن طريقها وتمحيص وتقييم الأدلة الأخرى والتنسيق بينها في ضوء المعلومات التي منها، بما يكفل في ذات الوقت التخطيط السليم لعمليات البحث، والتحقيق الجنائي وتطويرها.

إلا أن دورها في مجال كشف غموض جرائم الإنترنت، وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها، إلى نفس الدرجة من الأهمية، ويمكن رد ذلك إلى أن هناك على الدوام تقريبا، مسرحا للجريمة التقليدية جرت عليه الأحداث، وتركت آثارها المادية التي تنبثق منه الأدلة، والمعاينة في مسرح الجريمة تتيح المجال أمام الباحث والمحقق الجنائي للكشف عن طريق معاينة الآثار المادية التي خلفها ارتكاب الجريمة، والتحفظ على الأشياء التي تفيد في التحقيق الجاري بشأنها، بينما لا يوجد عادة مسرح مماثل للجريمة المرتكبة عبر الإنترنت وأقرب تشبيه لمسرحها، قد يكون الموقع أو

[226]– **محمد بن نصير محمد السرحاني**، المرجع السابق، ص77

المكتب الذي توجد فيه المعدات والأنظمة المعلوماتية، التي كانت محلا للجريمة أو أداتها[227].

يقلل مثل هذا المسرح إلى حد كبير من فرص إفصاحه عن الحقائق المراد التوصل إليها من وراء معاينته لسببين رئيسيين:

أولهما: أن الجرائم التي تقع بواسطة الأنظمة المعلوماتية قلما يتخلف عن ارتكابها آثار مادية.

ثانيهما: أن عددا كبيرا من الأشخاص يكون قد تردد على مكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا، التي تنقضي عادة بين ارتكاب الجريمة واكتشافها، مما يفسح المجال لحدوث تغيير أو تلف أو عبث بالآثار المادية أو زوال بعضها، وهو ما يلقي ضلالا من الشك على الدليل المستقى من المعاينة[228].

ينبغي لتفادي كل هذا وحتى يكون للمعاينة في الجرائم المتعلقة بشبكة الإنترنت فائدة في كشف الحقيقة عنها وعن مرتكبيها مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي[229]:

1-تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2-العناية بملاحظة الطريقة التي تم بها إعداد النظام.

3-ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.

---

[227]- **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص101

[228]- **أمير فرج يوسف**، الرجع السابق، ص220

[229]- **عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، «الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة مقارنة»**، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، 12_14 نوفمبر 2007، الرياض، ص17

4-عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

5- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، ويرفع عليها البصمات ذات الصلة بالجريمة.

6- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

7- قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوفر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات[230].

يتم التوثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد مع توثيق كل دليل على حدة بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها ومن قام برفعه وتحريزه وكيف ومتى تم ذلك، بل إن البعض يرى أن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي ترتبط بها الأجهزة محل التحقيق ولعل أبرز الأماكن التي يحتمل وجود الأدلة الجنائية المتعلقة بجرائم الإنترنت فيها ما يلي[231]:

-*الورق:* على الرغم من وجود أجهزة الحاسب الآلي قلل من حجم الأوراق الملفات التقليدية المستخدمة حيث يتم حفظ المعلومات والبيانات على أجهزة الحاسب الآلي، نجد الكثيرين ممن يقوموا بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات، وبالتالي فهي تعتبر من الأدلة التي ينبغي الاهتمام بها في البحث عن الحقيقة.

-*جهاز الحاسب الآلي وملحقاته:* وجود جهاز الحاسب الآلي هام جدا للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو جريمة حاسوبية، وإنها مرتبطة بالمكان أو

---

[230]- **محمد أبو العلا عقيدة**، المرجع السابق، ص7-8.

[231]- **محمد الأمين البشري**، «**التحقيق في جرائم الحاسب الآلي**»، مؤتمر القانون و الكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1_3 مايو 2000، المجلد الثالث، ص1058

الشخص الحائز على الجهاز، ولأجهزة الحاسب الآلي أشكال وأحكام وألوان مختلفة وخبير لحاسب الآلي وحده الذي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة.

-*البرمجيات:* إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص أو ليس واسع الانتشار، فإن أخذ الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

-*وسائط التخزين المتحركة*: كالأقراص المدمجة "أقراص الليزر" والأقراص المرنة والأشرطة المغناطيسية وغيرها، وتعد هذه الوسائط جزء من الجريمة المرتكبة عبر الإنترنت متى كانت محتوياتها عنصر من عناصر الجريمة.

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

-*المودم:* وهو الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال ببعضها البعض عبر خطوط الهاتف، وفي الوقت الحالي تطور المودم ليكون جهاز إرسال واستقبال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها[232].

الفرع الثالث

الخبرة

يعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجأ إليها القضاة أو سلطات الاستدلال على حد سواء، وذلك كل ما استعصى عليهم فهم موضوع معين يتميز بالتقنية، ومن بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد الجريمة المرتكبة عبر الإنترنت، حيث أنه لا يستطيع التعامل مع هذه الجريمة إلاّ شخص ذو دراية وخبرة في مجال الشبكات.

---

[232]- **حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت**، المرجع السابق، ص10_11

أولا: تعريف الخبرة

يقصد بالخبرة: "***مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة فنية أو دراية علمية لا تتوافر لديه***"[233].

يطلق لفظ الخبير على كل شخص توافرت لديه معرفة عملية وفنية لتخصصه في مادة معينة وتستعين به السلطة القضائية وجهات التحقيق في تقدير المسائل الفنية استكمالا لنقص معلومات القاضي في هذه النواحي[234]، ومساعدة له في اكتشاف الحقيقة لهذا الغرض يجب أن يتوفر لديه القدرة على تطبيق تلك القواعد النظرية على الحالات الواقعية ولا يتحقق ذلك إلا بالممارسة العملية[235].

يستنبط من خلال هذه التعاريف أن الخبرة هي بحث في المسائل المادية أو الفنية التي يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات، كفحص بصمات عثر عليها بمكان الحادث، أو مدى نسبة توقيع معين إلى شخص بعينه، أو تحديد سبب الوفاة في جريمة قتل عمد.

ثانيا: أهمية الاستعانة بالخبراء

تحتل الخبرة مكانا مهما في العمل القضائي والاستدلالي، باعتبارها طريقا مهما من طرق إثبات الحقوق في المنازعات التي تنظر أمام القضاء، لاسيما في مواجهة التطور التقني في شتى المجالات، وإذا كان المبدأ القانوني يقضي أنه على القاضي الإلمام بالتشريع والفقه، وأن يواكب مسيرتهما على الصعيد الوطني، فإنه ليس بالضرورة أن يكون ملما بالفيزياء والهندسة والرياضة والميكانيكا وعلم الفلك والطب، فالقاضي قد يصف أو يعاين هيكل الحقيقة، دون أن يكون لديه إمكانية الدخول إلى مضمونها، ومعرفة ذلك

---

[233]– **عبد الله بن سعود بن محمد السراني**، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، المرجع السابق، ص80

[234]– **محمد فاروق عبد الحميد كامل**، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 1999، ص286

[235]– **محمد علي أحمد الكواري**، المرجع السابق، ص40

المضمون، لأن المسألة تستلزم معارف فنية اختصاصية لا يدركها إلا أهل الفن والاختصاص.

وجدت الخبرة لتكون وسيلة أو طريقا من طرق البينات يلتمسها الخصوم لإثبات بعض الحقوق ذات الطبيعة المركبة من جهة، ولتكون وسيلة مساعدة للقاضي في إنارة طريق الوصول إلى الحقيقة تمهيدا لإقرار الحق لصاحبه في النزاع المعروض عليه للحكم فيه، وفصل الخصومات المستحكمة القائمة بين الأفراد[236].

إذا كان للخبرة تلك الأهمية في الجرائم التقليدية، فإن أهميتها ازدادت وأصبحت حتمية في إثبات الجرائم المرتكبة عبر الإنترنت، فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أوتحديد مدلولها بالاستعانة بالمعلومات العلمية، وهي بحث لمسائل مادية أو فنية يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات.

تستعين الشرطة وسلطات التحقيق أو المحاكمة منذ ظهور الجرائم المرتكبة من خلال شبكة الإنترنت بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، وذلك بغرض كشف غموض الجريمة، أو تجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق، ويلاحظ أن نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء[237].

وبالنظر إلى الطبيعة الخاصة بالجرائم المرتكبة عبر الإنترنت فإن إماطة اللثام عنها قد يحتاج إلى خبرة فنية منذ بدء مرحلة التحري عن هذه الجرائم، وتستمر الحاجة إليها في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص بأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء .

---

[236]– **محمد واصل، حسين بن علي الهلالي**، الخبرة الفنية أمام القضاء دراسة مقارنة، المكتب الفني، مسقط، سلطنة عمان، 2004، ص27_28

[237]– **عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري**، المرجع السابق، ص24_25

ثالثا: مجالات الخبرة بالنسبة للجرائم المرتكبة عبر الإنترنت

تتنوع العمليات الإلكترونية بتنوع المجالات التي تستخدم شبكة الإنترنت، فنجد أمثلة لها في الأعمال المصرفية، الإدارة الإلكترونية، والتجارة الإلكترونية، ولذلك فإنه يتصور تنوع الجرائم التي تقع على هذه العمليات وفقا لنوع العمليات الإلكترونية المستخدمة في ارتكابها.

تقتضي عمليات البحث الجنائي والتحقيق في جرائم الإنترنت الاستعانة بخبرات عديدة ومتنوعة، فإن اختيار خبير في نوعية الإجرام في مجال الإنترنت الذي تندرج الواقعة المرتكبة في اختصاصه يغدو أمرا بالغ الأهمية، ويمكن الاسترشاد في عملية الاختيار هذه بتصنيف لهذا الإجرام، يرتكز على نوعية الأساليب المستخدمة في الارتكاب إلى ما يلي:

أ- تزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة.

ب- التلاعب في البيانات.

ج- التلاعب في البرامج الأساسية أو برامج التطبيقات.

د- الغش أثناء نقل وبث البيانات[238].

رابعا: الشروط المتطلبة في الخبرة في مجال الجرائم المرتكبة عبر الإنترنت

تقتضي فاعلية الخبرة ضرورة الجمع بين التعمق في كل من الدراسة العلمية والنظرية والممارسة العملية للتخصص العلمي والنظري، وكذا متابعة مستمرة للتطورات التي تلحق بفروع التخصص، غير أن ذلك ليس شرطا لازما في بعض الأحيان فقد يقتصر الخبير على مجرد الخبرة العملية في فرع التخصص دون أن يكون هناك رصيد من الدراسة العلمية والنظرية وهو الأمر الذي نلاحظه في مجالات الخبرة في الفروع المهنية المختلفة[239]، منها مجال الحاسب الآلي، حيث يتعين في خبراء الحاسب الآلي المنتدبين للتحقيق أن تتوافر لديهم القدرة الفنية والإمكانات العلمية في المسألة موضوع

---

[238]- **هشام فريد رستم**، المرجع السابق، ص433

[239]- **محمد فاروق عبد الحميد كامل**، المرجع السابق، ص286

الخبرة، ولا يكفي في ذلك حصول الخبير على شهادة علمية، بل يجب مراعاة الخبرة العملية لأنها هي التي تحقق الكفاءة الفنية، ولذلك لا وجود لخبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرمجياتها وشبكاتها، أو لديه القدرة على التعامل مع كل أنواع الجريمة المرتكبة عبر الإنترنت[240].

تستوجب طبيعة هذه الجرائم توافر شروط خاصة في الخبير الذي ينتدب لبحث مسائل فنية وعلمية بالنسبة لها وهي:

1. الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسة والفرعية، والأجهزة الطرفية الملحقة به، وكلمات المرور أو السر وأكواد التشفير.

2. طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

3. قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك أعطاب أو تدمير الأدلة المحصلة من الوسائل الإلكترونية.

4. التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على الحاسب أو النظام أو الشبكة[241].

يتعين كذلك على الخبير في الجرائم المرتكبة عبر الإنترنت التنسيق مع المحقق الجنائي قبل محاكمة الجاني في هذه الجريمة، على أن يشمل اللقاء كافة الخبراء الذين ساهموا مع سلطات الضبط أو التحقيق في تلقي البلاغ أو إجراءات الضبط والتفتيش أو فحص البرامج وجمع الأدلة الجنائية، على أن يتم في هذا اللقاء حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بيئة أو قرينة، كما يجب على المحقق الجنائي أن يشرح

---

[240]– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص138

[241]– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص98

لهؤلاء الخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة المقام عنها الدعوى الجنائية ضد المتهم[242].

تجدر كذلك الإشارة إلى أنه وإن كان من المقرر أن المحكمة تملك سلطة تقديرية بالنسبة لتقدير الخبير الذي يرد إليها، إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز لها تفنيدها إلا بأسانيد فنية تخضع للتقدير المطلق لمحكمة الموضوع، ومن ثم فلا تستطيع المحكمة أن تفندها وترد عليها إلا بأسانيد فنية قد يصعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى[243].

المطلب الثاني

الجهود التشريعية للحد من الجريمة المرتكبة عبر الإنترنت

دأبت المجتمعات والدول عبر حقب زمنية مختلفة في سن تشريعات وقوانين من أجل مواجهة كل من تسوّل له نفسه خرق الآداب العامة بأعمال غير مشروعة، ومن ذلك الجرائم المرتكبة عبر الإنترنت، فبالرغم من قلّتها إلاّ أنها تعتبر محاولات هامة وملموسة في هذا المجال، وتتمثل هذه الجهود على المستوى الدولي في الجهود التي تبذلها مختلف الهيئات والمنظمات العالمية، بالإضافة إلى المنظمات الإقليمية، والتي تعتبر كإطار دولي يوازي عالمية الجريمة المرتكبة عبر الإنترنت **(الفرع الأول)**.

تعتبر الجهود الدولية داعمة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية، فهي بمثابة قوانين استرشادية تأخذ بها الدول لمواجهة الجرائم المستحدثة بما فيها تلك المرتكبة عبر شبكة الإنترنت، فهناك العديد من الدول التي اتخذت سبيل تطوير قوانين العقوبات، كما هناك دول ارتأت إفرادها بقوانين خاصة، وفي هذا الإطار سوف نستعرض تجربة المشرع الجزائري التي انتهجها للحد من هذه الظاهرة **(الفرع الثاني)**.

---

[242]– **المرجع نفسه**، ص99

[243]– **علي محمود عي حمودة**، المرجع السابق، ص53

الفرع الأول
على المستوى الدولي

تعددت الجهود الدولية والإقليمية في سبيل مكافحة الجريمة المرتكبة عبر الإنترنت، نظرا للتهديدات الكبيرة التي أتت بها الجريمة على هذين المستويين ، وفي هذا النطاق سنبين الجهود الدولية في مواجهة الجريمة المرتكبة عبر الإنترنت**(أولا)**، وكذا الجهود الإقليمية في هذا المجال**(ثانيا)**.

أولا: الجهود الدولية لمكافحة الجريمة المرتكبة عبر الإنترنت

تتمثل الجهود الدولية في إطار مكافحة الجريمة المرتكبة عبر الإنترنت في:

1-جهود منظمة الأمم المتحدة

بذلت منظمة الأمم المتحدة جهودا كبيرة في سبيل العمل على مكافحة جرائم الإنترنت، وذلك لما تسببه هذه الجرائم من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء، وإيمانا منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به[244].

توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب، وأشار القرار إلى أن الإجراء الدولي لمواجهة جرائم الإنترنت يتطلب من الدول الأعضاء اتخاذ عدة إجراءات تتلخص في[245]:

أ- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة (التحقيق، قبول الأدلة) على نحو ملائم وإدخال التعديلات إذا دعت الضرورة.

ب- مصادرة العائد والأصول من الأنشطة غير المشروعة.

---

[244]- **عواطف محمد عثمان عبد الحليم، « جرائم المعلوماتية، تعريفها، صورها، جهود مكافحتها دوليا، إقليميا، ووطنيا»**، مجلة العدل، العدد الرابع والعشرون، السنة العاشرة، دون سنة وبلد نشر، ص69

[245]- **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص186

ج- اتخاذ تدابير أمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان

د- رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة على مكافحة هذا النوع من الجرائم بأهمية مكافحة هذه الجرائم ومحاكمة مرتكبيها.

هـ- التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتبعة في استخدام الحاسوب ضمن المناهج المدرسية.

و- حماية مصالح الدولة وحقوق ضحايا جرائم الإنترنت[246].

تزايد الجرائم المرتكبة عبر الإنترنت وما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية سنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بالإضافة إلى الدور الذي يمكن أن تقوم به كل من منظمة الأمم المتحدة والمنظمات الإقليمية[247].

عقدت كذلك منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية وذلك بالبرازيل أيام 12_19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية، حيث احتل هذا النوع من الجرائم موقعا بارزا في جدول أعمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها[248].

دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية من أجل دراسة شاملة لمشكلة الجريمة السيبرانية وتدابير التصدي

---

[246]- **محمد فتحي عيد**، الإنترنت ودوره في انتشار المخدرات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص194

[247]- اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم (55/63)، الصادرة عن هيئة الأمم المتحدة، الجلسة العامة81، ديسمبر 2000

[248]- مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها لجرائم الحاسوبية، المنعقد بالبرازيل 12_19 أفريل 2010، رقم9/ A /conf.213

لها، ولقد ركز فريق الخبراء دراسته لهذا الموضوع على ظاهرة الجريمة السيبرانية بالتطرق إلى المواضيع التالية:

– تحليل ظاهرة الجريمة السيبرانية، جمع المعلومات والإحصائيات المتعلقة بالجريمة السيبرانية، تحديات الجريمة السيبرانية، مدى موائمة التشريعات للظاهرة الإجرامية السيبرانية، النص على الجرائم السيبرانية، إجراءات التحقيق، التعاون الدولي، الأدلة الإلكترونية، مسؤولية متعهدي خدمات الإنترنت، التصدي للجريمة خارج دائرة التدابير القانونية، المساعدة التقنية الدولية، دور القطاع الخاص في لحد من الجريمة [249].

دأبت منظمة الأمم المتحدة وذلك استمراراً لتلك الجهود المبذولة لمكافحة جرائم الإنترنت على عقد عدة مؤتمرات، فلم تكن المؤتمرات السالفة الذكر الأولى ولن تكون الأخيرة، حيث عمدت اللجنة الاقتصادية والاجتماعية لغربي آسيا التابعة للمجلس الاقتصادي والاجتماعي وذلك تحت غطاء منظمة الأمم المتحدة على عقد ورشة عمل حول التشريعات السيبرانية وتطبيقها في منطقة الإسكوا عام 2008[250].

بالإضافة إلى تلك المؤتمرات التي عقدتها أطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المنعقد بفيينا في أكتوبر 2010، حيث بيّن المؤتمر فهرس الأمثلة المعلقة بتسليم المجرمين وتبادل المساعدة القانونية وأشكال أخرى من التعاون الدولي في المسائل القانونية، استنادا إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[251]،

---

[249]– اجتماع فريق الخبراء المعني بالجريمة السيبرانية، مشروع المواضيع المطروحة لنظر في إطار دراسة شاملة بشأن الجريمة السيبرانية وتدابير التصدي لها، فيينا 17_21 يناير 2011، رقم UNODC/ccpcj/eg 4/2011/2

[250]– اللجنة الاقتصادية والاجتماعية لغربي آسيا(الإسكوا)، ورشة عمل حول التشريعات السيبرانية تطبيقها في منطقة الإسكوا، بيروت 15_16 ديسمبر 2008، المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة، رقم E /ESCWA/ICTD/2009 /1

[251]– مؤتمر هيئة الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة عبر الوطنية، المنعقد بفيينا في 18_22 أكتوبر 2010، رقم: CTOC/cop /2010/crp5

نجد في نفس المؤتمر مشاورات الخبراء بشأن استخدام الاتفاقية من أجل التصدي للأشكال المستجدة من الجريمة[252]، كما لا يمكننا إغفال مجهودات لجنة حقوق الطفل التابعة لمنظمة الأمم المتحدة التي عقدت اتفاقي خاصة بحقوق الطفل وذلك من أجل النظر في الجرائم التي ترتكب في حق الطفولة منها استغلالهم في المواد الإباحية عبر الإنترنت[253].

يعتبر ما قد سلف قطرة من بحر المجهودات التي بذلتها هيئة الأمم المتحدة في مجال التصدي لجرائم الإنترنت، فهناك مجهودات أخرى لا يتسع النطاق لذكرها كلها، ولكن تبقى الهيئة الإطار الأمثل لمكافحة هذا النوع من الإجرام، وسوف تبقى تبذل جهودا أكثر مادام هناك جريمة ومجرمين يجوبون الفضاء السيبيراني.

2- منظمة التعاون الاقتصادي والتنمية

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية، بدأت هذه المنظمة الاهتمام بالجرائم المرتكبة عبر الإنترنت منذ عام 1978، حيث وضعت مجموعة أدلة وقواعد إرشادية تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها[254].

أصدرت هذه المنظمة تقريرا عام 1983، بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى لأفعال سوء استخدام

---

[252]- أنشطة مكتب الأمم المتحدة المعني بالمخدرات والجريمة في مجال التصدي للأشكال المستجدة من الجريمة، مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، فيينا، 18_22 أكتوبر 2010، رقم: CTOC/cop /2010/3

[253]- اتفاقية حقوق الطفل، النظر في التقارير المقدمة من الدول بموجب الفقرة 1من المادة 12 من البروتوكول الاختياري لاتفاقية حقوق الطفل المتعلق ببيع وبغاء الأطفال في المواد الإباحية، لجنة حقوق الطفل، الدورة السابعة والخمسون، 30 ماي_17 جويلية 2011، الأمم المتحدة، رقم: CRC /c/opsc/egy/co/1

[254]- **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص179

الحاسوب التي يجب على الدول أن تجرمها وتفرض لها عقوبات في قوانينها، ومن أمثلة هذه الأفعال: الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به، ويشمل ذلك الحاسب والمعلومات المخزنة داخله، الإفشاء غير المصرح به للمعلومات المعالجة آليا والنسخ إتلاف أو تخريب ما يحويه من بيانات وبرامج والإعاقة غير المشروعة للوصول إلى مصادر الحاسب كمنع أو تعطيل استخدام الحاسب أو برامجه، أو البيانات المخزنة في قواعد الحاسب[255].

أوصت اللجنة المكلفة المصدرة للتقرير إلى وجوب أن تمتد الحماية إلى صورة أخرى لإساءة استخدام الحاسوب، منها الاتجار في الأسرار والاختراق غير المأذون فيه للحاسب أو لأنظمته، وفي عام 1992 وضعت المنظمة توصيات إرشادية خاصة بأمن أنظمة المعلومات، وقد تمخضت جهود المنظمة من أجل معالجة الجرائم المرتكبة عبر الإنترنت بالتوصية بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء الأفعال التالية:

1_ التلاعب في البيانات المعالجة آليا بما في ذلك محوها.

2_ التجسس المعلوماتي ويندرج تحته الحصول، أو الاقتناء، أو الاستعمال غير المشروع للمعطيات

3_ التخريب المعلوماتي ويندرج تحته الاستخدام غير المشروع، أو سرقة وقت الحاسب.

4_ قرصنة البرامج.

5_ الدخول غير المشروع على البيانات أو نقلها.

6_ اعتراض استخدام المعطيات أو نقلها[256].

---

[255]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص179_180

[256]– دليل للبلدان النامية: فهم الجريمة السيبرانية، شعبة تطبيقات تكنولوجيا المعلومات والاتصالات ولأمن السيبراني، دائرة السياسات والاستراتيجيات، قطاع تنمية الاتصالات، الصادر عن الاتحاد الدولي للاتصالات، أفريل 2009، ص94

تعقد المنظمة سنويا عددا من الملتقيات وورش العمل المعمقة للقطاعات ذات العلاقة بهذا المجال تركز فيها على معايير الأمن ومستوياته، إضافة إلى معايير تنفيذ وتطبيق القانون وذلك بهدف مواكبة التطورات في مجال جرائم الإنترنت.

3- المنظمة العالمية للملكية الفكرية

تعد المنظمة العالمية للملكية الفكرية، إحدى الوكالات التابعة للأمم المتحدة، وقد اهتمت هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم، بهدف تشجيع النشاط الابتكاري، وتطوير إدارة الاتحادات المنشأة في مجالات حماية الملكية الصناعية، وحماية المصنفات الأدبية والفنية[257].

اهتمت هذه المنظمة في المجال المعلوماتي بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، فبعد أن استقر الرأي لديها بعدم إمكانية توفير الحماية لهما في تشريعات براءات الاختراع، تم الاتفاق على توفيرها بواسطة الاتفاقيات العالمية وخاصة "التربس" و"برن" اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصة تشريعات حق المؤلف[258]، وكذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية والقرصنة المتعمدة والمرتكبة في إطار تجاري، وبالطبع يعتبر الإنترنت من الأماكن الخصبة لهذا النوع من التصرفات[259]، والتي وفرت بموجبها الحماية القانونية للبرامج وقواعد البيانات المعلوماتية.

تنص المادة الرابعة من معاهدة المنظمة العالمية للملكية الفكرية والمعتمدة في سنة 1996 على أنه:

« تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية في معنى المادة الثانية من اتفاقية برن، وتطبيق تلك الحماية على برامج الحاسوب أياً كانت طريقة

257- **عبد الرحمن جميل محمود حسين**، المرجع السابق، ص86_87

258- **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص181

259- **جون فرنسوا هنروت**،« **أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي**»، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة لمغربية، 19-20 يونيو 2007، ص98

التعبير عنها أو شكلها"، وتنص المادة الخامسة على أنه: "تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه أياً كان شكلها إذا كانت تعتبر ابتكارات بسبب اختيار محتوياتها أو ترتيبها » [260].

ساد الاتجاه لدى أغلب الدول الصناعية ودول العالم الثالث إلى الميل إلى خضوع برامج الحاسب الآلي لقوانين حماية حق المؤلف، حيث عدلت معظم الدول تشريعاتها الخاصة بحق المؤلف وأضافت برامج الحاسب إلى المصنفات الأدبية المحمية وفقا للقانون، وذلك نتيجة لاستمرار لجان الخبراء في دراسة الأسلوب المناسب لحماية برامج الحاسب الآلي ومسائلها الفنية عبر الاجتماعات المتكررة وبالتعاون ما بين الويبو واليونسكو [261].

ثانيا: دور الهيئات والمنظمات الإقليمية في مكافحة الجريمة المرتكبة عبر الإنترنت

تتمثل الجهود الإقليمية في مكافحة الجريمة المرتكبة عبر الإنترنت في:

1- الإتحاد الأوروبي

توجت الجهود التي يبذلها الإتحاد الأوروبي والمجلس الأوروبي بصدور اتفاقية بودابست لمكافحة جرائم المعلوماتية (الجرائم الإلكترونية) وتعرف بالاتفاقية الأوروبية لمكافحة جرائم المعلوماتية، وتتلخص أهم أهدافها في السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمّة للاتفاقية من غير الدول الأوروبية والتأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الإنترنت، وتحقيق التوازن بين حقوق الإنسان والإجراءات المتخذة لمواجهة جرائم الإنترنت، حيث تقدم هذه الاتفاقية الخاصة بجرائم الإنترنت دليلاً إرشاديا لتطوير مثل هذا التشريع[262].

---

[260]– **حسام الدين كامل الأهواني**، « **حماية حقوق الملكية الفكرية في مجال الإنترنت** »، ص3، مقال متوفر على الموقع التالي: http://www.osamabahar.com

[261]– **محمود أحمد عبابنة**، المرجع السابق، ص161

[262]– *Les rédacteurs de la Convention sur la cybercriminalité du Conseil de l'Europe se sont voulus plus proches de l'opinion du droit réel, estimant que le seul aspect spécifique de la cybercriminalité est l'utilisation des TIC comme moyen de commettre un délit. La Convention, qui est entrée en*

تقوم هذه الاتفاقية كذلك بتعريف وتحديد العقوبات من جرائم الإنترنت في إطار قوانينهم المحلية، وباستقراء هذه الاتفاقية نجد في ديباجتها الكثير من الجرائم المرتكبة عبر الإنترنت، منها المتعلقة بالبيانات الشخصية في مجال الخدمات المتعلقة بالاتصالات السلكية واللاسلكية[263].

وضعت تلك الاتفاقية من قبل مجلس أوربا بالتعاون مع كندا، واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية وعرضت للتوقيع في بودابست في عام 2001 ودخلت حيز التنفيذ في عام 2004[264]، وتعتبر الاتفاقية متاحة لأية دولة من أنحاء العالم تسعى للانضمام إليها، وهناك عدد من البلدان الأخرى من مختلف الأقاليم على وشك طلب الانضمام للاتفاقية، حيث أن في سبتمبر 2006، طلبت الفلبين الانضمام إليها، والجدير بالذكر أيضا أن الكثير من البلدان تعدّ حاليا تشريعا بشأن جرائم الإنترنت (مثل الأرجنتين، والبرازيل، وكولومبيا، والهند، وإندونيسيا وغيرها)، باستخدام الاتفاقية كنموذج[265].

لا تعتبر اتفاقية بودابست المجهود الأول الذي بذله المجلس الأوروبي في هذا المجال، بل بذل جهود عديدة من قبل، نذكر منها على سبيل المثال اتفاقية تتعلق بحماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات ذات الصبغة الشخصية وذلك في

---

vigueur le 1er juillet 2004, constitue le principal instrument international dans ce domaine. Voir : **KURBALIJA Jovan, GELBSTEIN Eduardo**, op-cit, p 98**.**

[263]– **واقد يوسف**، النظام القانوني للدفع الإلكتروني، مذكرة لنيل درجة الماجستير، تخصص قانون التعاون لدولي، جامعة مولود معمري، كلية الحقوق، تيزي وزو، ص185

[264]- *Le conseil de l'Europe a initié dés 1997un projet de convention international visant à lutté contre la cybercriminalité, cette convention à été signée le 23 novembre 2001 à Budapest, par trente pays dont douze d l'Union européenne et quatre non membres du conseil de l'Europe , le Canada, l'Afrique du sud, le Japon, USA.* Voir : **CAPRIOLI Eric A,,** Règlement des litiges internationaux et droit applicable dans le commerce électronique, édition du Juris-Classeur, Litec, Paris, 2002, p 78, et Voir aussi :

-كريستينا سكولمان، « الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية»، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19–20 يونيو 2007، المملكة المغربية، ص 119–120

[265]– **كريستينا سكولمان، «المعايير الدولية المتعلقة بجرائم الإنترنت (مجلس أوربا)»**، الندوة الإقليمية حول لجرائم المتصلة بالكمبيوتر، 19–20 يونيو 2007، المملكة المغربية، ص62

28 يناير سنة1981[266]، لكن تبقى اتفاقية بودابست الحيز الأمثل لمواجهة الجريمة المرتكبة عبر الإنترنت.

2- على المستوى العربي

أدى رواج المعلومات في كل الدول العربية إلى ظهور عدة ممارسات إجرامية في هذا النطاق مما حذا بهذه الدول إلى المحاولة لإيجاد سبل تشريعية وإجرائية ناجعة لمواجهة هذا النوع من الجرائم المستجدة.[267]

نجد من تلك الجهود القرار الصادر عن مجلس وزراء العدل العرب الخاص بإصدار القانون الجزائي الموحد، كقانون عربي نموذجي، أين نجد الباب السابع الخاص بالجرائم ضد الأشخاص، قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص، الناتج عن المعالجات المعلوماتية، وذلك في المواد 461-464 التي أشارت على وجوب حماية الحياة الخاصة، وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها و العقاب المطبق في حال ارتكاب هذه الجرائم[268].

تم في مجال الملكية الفكرية إبرام الاتفاقية العربية لحماية حقوق المؤلف حيث نصت في مجال المعلوماتية، على توفير الحماية القانونية للبرامج المعلوماتية(برام الحاسب الآلي)، بالإضافة إلى حث وتشجيع الدول الأعضاء على ضرورة تطوير تشريعاتها الجزائية لمواجهة الجرائم المرتكبة عبر الإنترنت[269].

غير أن الملاحظ في هذه المحاولات على المستوى العربي هو اعتمادها على علاج نقص التشريعات والأنظمة الخاصة بموضوع جرائم الإنترنت، وذلك بوضع أطر عامة حول ضوابط استخدام وأمن الإنترنت عن طريق تحديد بعض النشاطات الإجرامية التي يمكن أن توظف الشبكة والحاسبات عموما فيها، كما تشمل هذه المحاولات على العديد

---

[266]- **محمود أحمد عبابنة**، المرجع السابق، ص164

[267]- **عباس أبو شامة عبد المحمود**، المرجع السابق، ص50

[268]- **تركي بن عبد الرحمن المويشر**، المرجع السابق، ص 175

[269]- **محمود أحمد عبابنة**، المرجع السابق، ص 181

من تعليمات أمن المنشئات الحاسوبية، والأجهزة، والبرامج، وبعض القواعد العامة المنظمة لارتباط المنشئات الحكومية بالشبكة العالمية[270].

3-مجموعة الدول الثمانية:

تمثل هذه المجموعة إطارا ناضجا لإجراء الدراسات البحثية والتطبيقية في مختلف الموضوعات التي تهم المنظمة، وهي ليست إطار تشريعيا للدول الأعضاء، ولكنها تقوم على فكرة تبادل زعماء هذه الدول الرأي في المسائل ذات الاهتمام المشترك لبلورة خطط عملية كحصيلة لتوجيهات قادة هذه الدول، ومكافحة كل ما من شأنه التأثير أو تهديد أمن واستقرار الدول الأعضاء[271].

اعتمد وزراء العدل لدول مجموعة الثمانية خلال اجتماع عقد بواشنطن يومي التاسع والعاشر من ديسمبر 1997 المبادئ التي تشكل الأساس لشبكة نقاط اتصال وطنية وبجانب هذه المبادئ تم وضع خطة عمل لإنشاء شبكة متابعة لتقديم تقارير بشأن مدى التزام الدول الأعضاء في الشبكة، وقد أنشئت على غرار نموذج الإنتربول في الفترة ما بين 1998 و2000، وتتواصل الجهود من أجل زيادة الدول المشاركة[272].

تناولت مجموعة الثمانية في المؤتمر الذي عقدته في باريس في عام 2000، موضوع الجريمة السيبرانية وحثت إلى منع الملاذات الرقمية غير الخاضعة للقانون، وكانت مجموعة الثمانية قد ربطت منذ ذلك الوقت محاولاتها الرامية إلى إيجاد حلول دولية باتفاقية مجلس أوربا بشأن الجريمة السيبرانية، وفي عام 2001 ناقشت مجموعة الثمانية الأدوات الإجرائية لمكافحة الجريمة السيبرانية في ورشة عمل عقدت بطوكيو، ركزت على ما إذا كان ينبغي تنفيذ الالتزامات باحتجاز البيانات أو ما إذا كان حفظ البيانات يعد حلا بديلا[273].

---

[270]– **فايز بن عبد الله الشهري**، « **التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة (دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنت)**»، المرجع السابق، ص21.

[271]– **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص 184

[272]– **جون فرنسوا هنروت**، المرجع السابق، ص101

[273]– دليل فهم الجريمة السيبرانية للدول النامية، المرجع السابق، ص 84

نلاحظ أن ما جاءت به جهود هذه المجموعة من توجيهات لم تخرج في أحكامها عن مجال تعداد للجرائم المرتكبة عبر الإنترنت عما وضعه المجلس الأوروبي مما يتطلب من الدول الأعضاء في هذه المجموع المزيد من الجهود والتعاون من أجل الحد من ظاهرة الجرائم المرتكبة في الفضاء الافتراضي.[274]

الفرع الثاني
على المستوى الداخلي

واكب المشرع الجزائري مختلف التطورات التشريعية لتي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الإلكترونية بما فيها الإنترنت، خاصة التي تهدف إلى الحد من الاستخدام غير المشروع لها، وذلك مراعاة منه لما يشهده العالم من تطورات كبيرة في مجال الإعلام والاتصال خاصة الإنترنت، وكذلك إيمانا منه بأن الجزائر ليست بمعزل عن التطورات الإجرامية التي تحدث في العالم، خاصة في ظل التنامي المتسارع لاستعمال الإنترنت في الجزائر، فكانت محاولاته في الحد من هذه الظاهرة المستحدثة على النحو التالي:

أولا: مكافحة الجريمة المرتكبة عبر الإنترنت في قوانين الملكية الفكرية

نظرا للاعتداءات التي تتعرض لها مختلف المنتجات الفكرية عبر الإنترنت ارتأينا البحث في مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية، وسنفصل في ذلك من خلال نقطتين أساسيتين:

1-الحماية في إطار قانون الملكية الصناعية.

2-الحماية في إطار قانون الملكية الأدبية والفنية.

274- « *Il faudra probablement aller plus loin pour gagner la bataille contre la cybercriminalité, peut- on imaginer un droit pénal supranational pour se donner vraiment la possibilité de sanctionner ces comportement illicites ? Faut-il aller jusque a la création d'une cyberepolice international qui se jouirait comme les délinquant des frontières* ».Voir : MASCALA Corinne, « ***criminalité et contrat électronique*** », op-cit, p 118.

1- مكافحة الجريمة المرتكبة عبر الإنترنت من خلال قوانين الملكية الصناعية

أ- في الأمر 06-03 المتعلق بالعلامات التجارية

تطرق المشرع الجزائري إلى تنظيم أحام العلامات التجارية من خلال عدة قوانين آخرها الأمر رقم 06-03 المؤرخ في 19-07-2003 والمتعلق بالعلامات[275].

تعرف العلامات التجارية على أنها كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات، ويشترط في العلامة أن تكون مميزة وجديدة وغير مخالفة للنظام العام[276]، غير أن السؤال المطروح، هو هل تستفيد برامج الحاسب الآلي من الحماية الجنائية للعلامات التجارية؟

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجأ أصحاب البرامج إلى وضع الاسم مقترنا به، غير أن الحماية بأحكام العلامات التجارية قد تكون فعالة بالنسبة للنسخ البسيط، لكن ليس الأمر كذلك بالنسبة للنسخ المعقد.

ب- في الأمر رقم 03-07 يتعلق ببراءات الاختراع

عرّفت المادة 02 من الأمر 03-07 الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية، وبشأن الشروط التي يجب توافرها في الاختراع

---

[275]- تجسدت هذه القوانين في: أمر رقم 66-57 مؤرخ في 19-03-1966 المتعلق بعلامات المصنع والعلامات التجارية والمعدل والمتمم بـ أمر رقم 67-233 مؤرخ في 19-10-1967 المتضمن أحكام العلامات التجارية، والمعدل أمر رقم 03-06 مؤرخ 19 جويلية 2003 والمتعلق بالعلامات، ج ر عدد 44 صادر بـ 23 جويلية 2003.

[276]- **فشار عطاء الله، «مواجهة الجريمة المعلوماتية في التشريع الجزائري»**، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص6.

فتتمثل فيما يلي: (شرط الابتكار، شرط الجدة، القابلية لتطبيق الصناعي، المشروعية)[277].

يتحصل المخترع في حال توافر هذه الشروط على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية[278]، غير السؤال المطروح هو هل تستفيد برامج الحاسب من الحماية بواسطة براءات الاختراع؟

التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع لأحد السببين:

-إما تجرد البرامج من أي طابع صناعي.

-إما صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة فليس من الهين توافر شرط الجدة في البرمجيات وليس من الهين إثبات توافر هذا الشرط إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا الأمر يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال لتي تتولى بحثه[279].

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة الاختراع، ويتمثل هذا التحفظ في الإجراءات لمعقدة للحصول على البراءة والتكلفة العالية والمدد الطويلة التي يستغرقها هذا التسجيل، فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة

---

[277]- أنظر المادة 2 من قانون 03-07 المؤرخ في 19-07-2003 يتعلق ببراءات الاختراع، الجريدة الرسمية عدد 44 صادر في 2003/07/23.

[278]- **شبراك حياة**، حقوق صاحب براءة الاختراع في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون الأعمال، كلية الحقوق والعلوم الإدارية، الجزائر، 2002، ص17

[279]- **قارة أمال**، الجريمة المعلوماتية، المرجع السابق، ص112

سنوات بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر وعليه يمكن للغير الوصول إلى سر البرنامج واستغلاله قبل صدور البراءة.

تجدر الإشارة إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا للمادة 07 من الأمر 03-07 المتضمن براءة الاختراع التي نصت على أنه:

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

2-مكافحة الجريمة المرتكبة عبر الإنترنت من خلال قوانين الملكية الأدبية والفنية

شهد النصف الأخير من القرن العشرين تطورا ملحوظاً في مجال الاتصال رافقه تطور في وسائل نقل الإنتاج الفكري على اختلاف صوره من علوم وفنون وآداب، مما أوجد مصنفات جديدة جديرة بحماية حق المؤلف كانت محل اهتمام ودراسة من قبل المختصين في مجال الملكية الفكرية[280]، وقد كان من أهم هذه المصنفات، المصنفات الخاصة ببرامج الحاسبات الإلكترونية، وقواعد البيانات التي كانت طبيعتها التقنية تختلف عن المصنفات التقليدية، الأمر الذي تطلب متابعتها باستمرار ووضع قواعد قانونية محددة وثابتة لحمايتها[(281)].

اتجه المشرع الجزائري إلى الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي، وذلك ما من خلال تعديله للأمر 73-14 بموجب الأمر 97_10[(282)] والذي يتبين من خلال استقرائنا له ما يلي:

---

[280] – Les délits le plus souvent évoqués dans le cadre de l'internet sont très certainement ceux qui emportent atteinte au droit de la propriété intellectuelle. Voir : **FAUCHOUX Vincent- DEPREZ Pierre**, Op-cit, p 215

[281]– **عمر مشهور حديثة حجازي**، المبادئ الأساسية لقانون حق المؤلف، ندوة حق المؤلف في الأردن: بين النظرية والتطبيق، كلية الحقوق، الجامعة الأردنية، 12 كانون الثاني 2004، ص4

[282]– أمر رقم 97-10 مؤرخ في 06-03-1997 المتعلق بحق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 13 صادر في 1997/03/12، معدل ومتمم بـ أمر 03-05 مؤرخ في 19-07-2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 44 صادر في 2003/07/23.

1-أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية، والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي التي تمكن من القيام بنشاط علمي، أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وترجم باندفاعات إلكترونية بالحاسوب، أما قواعد البيانات فهي عبارة عن مجموعة المصنفات والأساليب والقواعد، كما يمكن أن تشمل الوثائق المتعلقة بسير المعطيات وقد أشارت المادة 05 إلى قواعد البيانات بنصها:

« ***تعتبر أيضا مصنفات محمية الأعمال الآتية: مجموعات المعلومات البسيطة التي تأتي أصالتها من انتقاء مواردها أو تنسيقها أو ترتيبها*** ».

2-أن الحماية تحدد من 25 سنة إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية برن التي حددت كمدة دنيا للحماية 50 سنة، وبالتالي هذه المدة تشمل حتى مصنفات الإعلام لآلي[283].

3- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية، إذ في السابق تجريم الاعتداءات على الملكية الفكرية تناولته المواد 390-394 من قانون العقوبات، لكنها أخرجت بموجب الأمر 97-10 من مظلة قانون العقوبات وأصبح لها تجريم خاص، حيث أن قانون العقوبات كان يقرر بموجب المادة 393 الغرامة كعقوبة للاعتداء على حق المؤلف، بينما الأمر 97-10 وكذا الأمر 03-05 يقرران عقوبتي الحبس والغرامة[284].

اتضح مما سبق أن المشرع الجزائري سواء بدافع توفير الحماية الجزائية للمعلوماتية أو بدوافع خارجية قد واكب التطورات الحاصلة في المجال المعلوماتي، بأن أخضع

---

[283]- **عبد القادر دوحة، محمد بن حاج الطاهر،« مدى مواكبة المشرع الجزائري لتطور الجريمة الإلكترونية »**، الملتقى الوطني الأول-النظام القانوني للمجتمع الإلكتروني، المركز الجامعي خميس مليانة، مهد العلوم القانونية والإدارية، 09_10_11 مارس 2008، ص10

[284]- **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، 2007، ص78-79.

المعلوماتية لقانون الملكية الفكرية موسعا بذلك من سلطة القاضي في تقرير العقوبة، وذلك ضمانا وحماية لحق المؤلف ومالك الحق المجاور.

ثانيا-مكافحة الجريمة المرتكبة عبر الإنترنت في قانون العقوبات

تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي عموما والإجرام عبر الإنترنت خصوصا بموجب القانون 04-15[285] المتضمن تعديل قانون العقوبات، الذي بموجبه جرم المشرع بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات وهي :

1- جريمة التوصل أو الدخول غير المصرح به: تقوم هذه الجريمة بمجرد ما يتم الدخول غير المرخص به وعن طريق الغش إلى المنظومة المعلوماتية، سواء مس ذلك الدخول أو البقاء كامل المنظومة أو جزء منها فقط[286]، وهو ما أشارت إليه المادة 394 مكرر من قانون العقوبات بنصها على:

« ***يعاقب بالحبس والغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة*** »

أورد المشرع ظرفين لتشدد عقوبة الدخول غير المشروع إلى المنظمات المعلوماتية، أوله حذف أو تغيير المعطيات، والظرف الثاني هو تخريب نظام اشتغال المنظومة، وقد أشار المشرع في المادة المذكورة أعلاه على تجريم فعل الشروع في جريمة الدخول غير المصرح به ، وذلك بقوله *"أو يحاول ذلك"*.

2- جريمة التزوير المعلوماتي: النشاط الإجرامي في هذه الجريمة ينحصر في أفعال الإدخال والمحو والتعديل، ولا يشترط اجتماعهما معا حتى يتوافر النشاط الإجرامي

---

[285]- قانون 04-15 مؤرخ في 10-11-2004 المتضمن قانون العقوبات، جريدة رسمية عدد 71 الصادر في 2004/11/10.

[286]- **بورزام أحمد**، المرجع السابق، ص14.

فيها، إذ يتوفر الركن المادي للجريمة بمجرد القيام بفعل واحد على حدى، لكن القاسم المشترك في هذه الأفعال جميعا هو انطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل آخر قائمة[287]، ولقد أكد المشرع على معاقبة هذه الجرائم في المادة 394 مكرر 1 بنصها:

« ***يعاقب بالحبس وبالغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها*** »

3- جريمة الاستيلاء على المعطيات: تعد هذه الجريمة من بين أكثر الجرائم وقوعا في العالم الافتراضي، وهي ما أقرته المادة 394 مكرر 2 بنصها على:

« ***كل من يقوم عمدا وبطريق الغش 1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية 2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم***».

4- جريمة إتلاف وتدمير المعطيات: تطرق إليها المشرع الجزائري بالمادة 394 مكرر 1 من قانون العقوبات والتي تنص على:

« ***يعاقب بالحبس والغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها*** »، وجريمة الإتلاف حسب نص المادة المذكورة تتمثل في إزالة معطيات نظام المعالجة الآلية عن طريق الفيروسات مثلا[288].

5- جريمة الاحتيال المعلوماتي تطرقت إليه فحوى المادة 394 مكرر2/1 من خلال نصها عل

---

[287]- **خثير مسعود**، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى، عين مليلة، الجزائر، 2010، ص123

[288]- **عبد القادر دوحة، محمد بن حاج الطاهر**، المرجع السابق، ص7.

« ***يعاقب بالحبس وبالغرامة كل من قام بطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية...*** » أي أن يهدف مرتكبها إلى جني فوائد مالية من جراء ذلك[289].

6- أنشطة الإنترنت المجسدة لجرائم المحتوى الضار والتصرف غير القانوني:

نصت مواد القسم السابع مكرر من قانون العقوبات وخاصة المادة 394 مكرر2/2 على تجريم أفعال الحيازة، الإفشاء والنشر التي ترد على المعطيات الآلية بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق، وجمع الأفعال غير المشروعة، وذلك بعقوبتي الحبس والغرامة إضافية إلى ما نصت عليه المادة 394 مكرر6 بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات[290].

تتمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي عقوبة الحبس والغرامة، وعقوبات تكميلية بموجب نص المادة 394 مكرر6 والمتمثلة في: مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع والمحل أو أماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الإنترنت الذي ترتكب فيه هذه الجرائم بشرط علم مالكه.

أورد المشرع ظروفا تشدد بها عقوبة الجريمة وهي:

- حالة الدخول والبقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام،

-إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

---

[289]- أنظر المواد 394 مكرر2 و394 مكرر1 و394 مكرر1/2 من قانون 04-15 المؤرخ في 2004/11/10 المتضمن تعديل قانون العقوبات، جريدة رسمية عدد 71 صادر 2004/11/10.

[290]- أنظر المواد 394 مكرر2 و394 مكرر 6 من قانون 04-15 المؤرخ في 2004/11/10 .

أكد المشرع الجزائري أيضا بموجب المادة 394 مكرر5[291] على تجريم الاشتراك (سواء شخص طبيعي أو معنوي) في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية–بعقوبة الجريمة–وكان التحضير لهذه الجرائم مجسدا بفعل أو بعدة أفعال مادية[292]، أي بمعنى آخر فإن المشرع استثنى من العقاب الأعمال التحضيرية للجرائم المعلوماتية المرتكبة من طرف شخص منفرد.

كما نصت المادة 394 مكرر4 على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع مكرر بغرامة تعادل 5 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي[293]، غير أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء في نفس الجريمة، والشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها وهو ما نصت عليه المادة 394 مكرر7 من قانون العقوبات.

نص المشرع الجزائري على حماية الأشخاص من التعدي على حياتهم الخاصة وذلك من خلال المادة 303 مكرر، حيث حددت هذه المادة الحالات التي يتم فيها المساس بحرمة الحياة الخاصة وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية أو صور في مكان خاص بغير إذن صاحبها أو رضاه.

كما جاءت المادة 303 مكرر1 مدعمة للمادة السالفة الذكر حيث يظهر من خلال نص وأسلوب صياغة هذه المادة، أن المشرع الجزائري لم يكتف بتجريم التقاط التسجيلات أو الصور أو الوثائق، بل جرم كذلك استخدامها أو عرضها على الجمهور، الأمر الذي يمكن من إسقاط هذه المادة على الصور والوثائق والتسجيلات في حال نشرها على شبكة الإنترنت مادام هذا الفعل يحقق العلنية[294].

---

[291]– تنص هذه المادة على أنه «***كل من شارك في مجموعة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها***».

[292]– **بورزام أحمد**، المرجع السابق، ص15

[293]– **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص130

[294]– **عبد القادر دوحة، محمد بن حاج الطاهر**، المرجع السابق، ص4.

نخلص إلى أن المشرع الجزائري رغم تداركه من خلال قانون 15-04 والمتضمن تعديل قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة، إلا أنه أغفل تجريم الاعتداءات الواردة على منتجات الإعلام الآلي، فلم يستحدث نصا خاصا بالتزوير المعلوماتي، ولم يتبنى الاتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

ثالثا: مكافحة الجريمة المرتكبة عبر الإنترنت في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

سنتطرق فيما يلي إلى أسباب صدور القانون رقم 09-04 مؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**(1)**، ثم إلى مضمون هذا القانون باختصار**(2)**[295].

1- أسباب صدور قانون مكافحة الجرائم المعلوماتية

دفع القصور الذي عرفه القانون رقم 04-15 والمعدل لقانون العقوبات الذي نص على حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، بالمشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام والاتصال وخاصة الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، خاصة في ظل الثورة التي تعرفها في مجال استخدام الإنترنت، وذلك بوضع هذا القانون من أجل تعزيز القواعد السابقة، من خلال وضع إطار قانوني أكثر ملائمة مع خصوصية الجريمة المرتكبة عبر الإنترنت.

كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها.

[295]- القانون رقم 09-04 المؤرخ في 5-2-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 لسنة 2009.

أخذ المشرع بعين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة، لذلك تم اختيار عنوان "*القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها*" حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا، كما أن التركيز على مجالي الإعلام والاتصال بين مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الإجرام والوقاية منه[296].

ثانيا: مضمون قانون مكافحة الجرائم المعلوماتية

يحتوي قانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على ستة فصول نلخصها فيما يلي:

الفصل الأول نص على الأحكام العامة التي تبين الأهداف المتوخاة من القانون وتحدد مفهوم مصطلح التقنية الواردة وكذا مجال تطبيق أحكامها[297].

الفصل الثاني حيث جسد أحكام خاصة بمراقبة الاتصالات الإلكترونية، وقد روعي في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية[298]، حيث نص القانون على أربع حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية، عندما يصعب الوصول إلى

---

[296]- **الأزرق بن عبد الله، أحمد عمراني، «نظام المعلوماتية في القانون الجزائري واقع وآفاق»**، المؤتمر السادس لجمعية المكتبات ولمعلومات السعودية، البيئة المعلوماتية الآمنة المفاهيم والتشريعات والتطبيقات، الرياض، 6_7 أفريل 2010، ص15_16

[297]- المواد 1_2_3 من قانون رقم 09-04 مؤرخ في 2009/2/5 المرجع السابق

[298]- المادة 4 من قانون 04/09 المؤرخ في 2009/2/5 مرجع نفسه

نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

الفصل الثالث تضمن القواعد الإجرائية، الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن ومع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة، وعلى هذا الأساس يجوز للجهات القضائية وضباط الشرطة القضائية الدخول والتفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها[299].

الفصل الرابع تطرق إلى التزامات المتعاملين في مجال الاتصالات الإلكترونية وذلك من خلال تحديد الالتزامات التي تقع على عاتق المتعاملين في الاتصالات الإلكترونية لاسيما إلزامية حفظ المعطيات المتعلقة بحركة السير والتي من شأنها المساعدة في الكشف عن الجرائم ومرتكبها، يهدف هذا القانون إلى إعطاء مقدمي الخدمات دور إيجابيا ومساعدا للسلطات العمومية في مواجهة الجرائم وكشف مرتكبها[300]، حيث ألزم هذا القانون مقدمي خدمات الإنترنت على التدخل الفوري لسحب المحتويات التي بإمكانهم الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الدخول إليها غير ممكن، إضافة إلى وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام والآداب العامة وإخطار المشتركين لديهم بوجودها.

الفصل الخامس أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته، إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية

---

[299]– **فشار عطاء الله**، المرجع السابق، ص35

[300]– المواد 10_11_12 من قانون رقم 09-04 المؤرخ في 2009/2/5 مرجع سابق

في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد تمت الإحالة على التنظيم فيما يخص تحديد كيفية تشكيل وتنظيم هذه الهيئة[301].

الفصل السادس: نص على التعاون والمساعدة القضائية الدولية، إذ تناول قواعد الاختصاص القضائي والتعاون الدولي بوجه عام:

فيما يخص الاختصاص القضائي فهو فضلا عن قواعد الاختصاص العادية فقد تم توسيع اختصاص المحاكم الجزائية للنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي ترتكب من طرف الرعايا الأجانب عندما تكون المصالح الإستراتيجية للجزائر مستهدفة.

أما فيما يتعلق بالتعاون الدولي يقوم على مجموعة من المبادئ العامة في مجال التعاون الدولي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خاصة ما يتعلق منها بالمساعدة وتبادل المعلومات، حيث تم اعتماد مبدأ التعاون على أساس المعاملة بالمثل[302].

يعتبر القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نطاقا شاملا في مجال مكافحة الجرائم المرتكبة عبر الإنترنت، حيث جاء تجريمه للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عاما، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا.

المبحث الثاني

صعوبات مكافحة الجريمة المرتكبة عبر الإنترنت

رغم الجهود المبذولة للحد من الجرائم المرتكبة عبر الإنترنت، سواء كانت من طرف المشرعين أو من طرف سلطات التحقيق والضبطية القضائية، دولية كانت أو داخلية، إلاّ أن هذه الجهود تصطدم بعدة عراقيل وصعوبات، والتي تتجلى في المقام الأول في

---

[301]- المواد 13 و14 من قانون 09-04 المؤرخ في 2009/2/5.

[302]- **الأزرق بن عبد الله، أحمد عمراني**، المرجع السابق، ص17

لامادية الجريمة المرتكبة عبر الإنترنت، وكذا السمات التي يتميز بها الدليل الذي يستخلص من هذه الجريمة **(المطلب الأول)**.

لا تعتبر صعوبات اكتشاف واثبات الجريمة المرتكبة عبر الإنترنت وحدها التي تحد من مكافحة الجريمة المرتكبة عبر الإنترنت، بل هناك صعوبات أخرى، خاصة تلك المتعلقة بالجانب القضائي، والمتعلقة بالقانون الواجب التطبيق وتحديد المحكمة المختصة بمتابعة مرتكبي هذه الجرائم، والذين في معظم الأحوال يكونون أشخاص من خارج حدود الدولة **(المطلب الثاني)**.

المطلب الأول

صعوبة اكتشاف واثبات الجريمة المرتكبة عبر الإنترنت

تتسم الجرائم التي ترتكب في نطاق شبكة الإنترنت بكون محلها معلومات أو برامج معالجة آليا عبر الحواسيب، أو جرائم تتعلق بالأشخاص عبر عالم افتراضي غير متناهي وغير محدود، مما يعطيها طابع خاص ليس فقط في طريقة ارتكابها، بل كذلك في الوسيلة التي ترتكب بها، الأمر الذي ينجم عنه صعوبات في اكتشاف الجريمة المرتكبة عبر الإنترنت.**(الفرع الأول)**.

تقودنا صعوبة اكتشاف الجريمة حتما إلى صعوبة إثباتها، فالمجرم يسعى بشتى الطرق لكي لا يترك وراءه آثارا تدل على ارتكابه للجريمة، وبالتالي تكون عملية إثبات الجريمة تتميز بالصعوبة، لكن الصعوبة تتجلى أكثر في نطاق الجرائم المرتكبة عبر الإنترنت في ظل لاماديتها، الأمر الذي يجعل إسناد الفعل غير المشروع إلى المجرم شبه مستحيل **(الفرع الثاني)**.

الفرع الأول

اكتشاف الجريمة المرتكبة عبر الإنترنت

يعترض اكتشاف الجرائم المرتكبة عبر الإنترنت العديد من الصعوبات، وذلك راجع إلى عدة اعتبارات منها ما هو متعلق بفقدان الآثار المادية للجريمة، حيث في الغالب تعد الجريمة المرتكبة عبر الإنترنت لا تترك آثار مادية خلفها، ومنها ما هو راجع إلى التكتم

الذي تنتهجه الجهات المجني عليها، كما تلعب نقص الخبرة التي يتميز بها أفراد سلطات الاستدلال دوراً هاما في عدم اكتشاف هذا النوع المستحدث من الجرائم.

أولا: فقدان الآثار التقليدية للجريمة

تظل الجريمة المرتكبة عبر الإنترنت مجهولة ما لم يبلغ عنها للجهات المعنية بالاستدلالات أو التحقيق الجنائي، وفي هذا الصدد تجدر الإشارة أن أهم الجرائم لا تصل إلى علم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية لا تخلف آثار مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة[303]، فالعديد من الجرائم المرتكبة عبر الإنترنت، تتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية، كجرائم التجسس التي تتم عن طريق اعتراض النبضات الإلكترونية، وجرائم الاختلاس التي تتم عبر تعديل البرامج والتلاعب بالأنظمة المعلوماتية[304].

يرجع السبب في افتقاد الآثار التقليدية للجريمة المرتكبة عبر الإنترنت إلى ما لاحظه جانب من الفقه من أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسب الآلي دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معدا ومخزنا على جهاز الحاسب[305].

تضع الوسيلة التي ترتكب بها الجريمة ضمن قالب غير تقليدي، نظرا أن ارتكابها يتم عادة عن طريق نقل المعلومات على شكل نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي، وشبكة الاتصالات العالمية (الإنترنت) بصورة آلية، كما تنساب الكهرباء عبر الأسلاك [306].

---

[303]– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص41

[304]– **غازي عبد الرحمان هيان الرشيد**، المرجع السابق، ص539

[305]– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص83

[306]– **محمد حماد مرهج الهيتي**، جرائم الحاسوب....، المرجع السابق، ص214

تستفيد الكيانات الإجرامية من لامادية الآثار والمعالم التي يمكن الاستدلال من خلالها على وقوع جريمة مادية ونسبتها لشخص أو أشخاص محددين، فالمعطيات المتداولة من صوت وصورة وكتابة ومواد فيديو، سواء اتخذت شكل تجميع لمعطيات أو برامج حاسوب، تتمثل كلها في أنظمة تشغيل في شكل إلكتروني يتجسد في وحدات حسابية تندثر بسهولة فائقة، ويكفي الضغط على زر في لوحة الاستخدام لزوال ملفات أو حتى قواعد بيانات وأنظمة بأكملها.

تأتي من هنا مشكلة ضبط هذه المعطيات وإحرازها في شكل إلكتروني وحجزها ووضعها في خاتم قانوني لاستغلالها في البحث، وإذا كانت بعض التجهيزات والتقنيات تسمح للباحثين بالوصول إلى هذه المعطيات التي تبقى في ذاكرة الحاسوب المستعمل، إلاّ أنّها تتطلب خبرة عالية وإمكانيات قد لا تتوافر عادة لدى مصالح الشرطة القضائية المكلفة بالبحث، وحتى في حالة حجز المعطيات الرقمية، فإن البيانات أو المعلومات التي تشتمل عليها لا تتضمن آثارا أو بصمات يمكن الاستدلال من خلالها على صاحبها، بل يحتاج الوصول إلى هذا الهدف إلى عمليات بحث وتحري أخرى للوصول على نسق من القرائن المادية الأخرى التي يمكن أن تعزز دلالتها وقيمتها في الإثبات[307].

ثانيا: فرض الجناة لتدابير أمنية

يعمد المجرمون عبر الإنترنت عادة إلى إخفاء جرائمهم، وإزالة آثارها عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الكمبيوتر والبرامج، ودون ترك أثر، ولا سيما أن التخزين الإلكتروني غير مرئي والبيانات مكتوبة بلغة رقمية لا يفهمها إلا الآلة ما لم تستعاد على شاشة الكمبيوتر ليتمكن الإنسان من قرائتها وفهمها، وهذا يشكل عقبة أمام إقامة الدليل على الجريمة المرتكبة عبر الإنترنت وإثباتها[308].

فلا مرية أن المجرمين الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة قبل ارتكابها لكي لا

---

[307]– **احمد آيت الطالب**، « **العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة** »، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية، كلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية، 9_2006/4/13، ص16

[308]– **فريد منعم جبور**، المرجع السبق، ص209

يقعوا تحت طائلة العقاب. فهم قد يزيدون من صعوبة إجراءات التفتيش التي يتوقع حدوثها للبحث عن الأدلة التي قد تدينهم باستخدام كلمات السر التي لا تمكن غيرهم من الوصول إلى البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال، وقد يلجأ هؤلاء المجرمون أيضا إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها بحيث قد يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات التحري والضبط الوصول إلى كشف أفعالهم غير المشروعة[309].

بالإضافة إلى ذلك يقوم المجرمون عبر الإنترنت بإخفاء هويتهم أو انتحال شخصية أخرى حتى لا يمكن التعرف عليهم في حالة اكتشاف الجريمة، وقيام المحققين بالتحري عنها، حيث توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيته، سواء أثناء إرسال البريد أو أثناء تصفح المواقع، فم يسعون من خلالها إلى إخفاء شخصيتهم وفا من مسائلة نظامية[310].

يعتبر انتحال الشخصية عبر البريد الالكتروني من بين أكثر الطرق استعمالا من طرف المجرمين عبر الإنترنت، حيث يقومون بتزييف رسائل البريد الإلكتروني لتبدو صادرة من شخص آخر، وبالرغم أن الكثير من هذه الرسائل ليست مؤذية وتمر على سبيل الفكاهة، إلا أن بعضها الآخر يكون شديد الأذى[311].

ثالثا: التكتم عليها من قبل الجهات المجني عليها

ما يزيد من صعوبة اكتشاف الجريمة المرتكبة عبر الإنترنت هو أن الجهات المجني عليها التي غالبا ما تكون مصرفا أو مؤسسة مالية، شركة أو مشروعا صناعيا ضخما، تلجأ إلى التكتم على مثل هذه الجرائم إن تعرضت لها[312]، ولا تبلغ السلطات المختصة في مكافحة هذه الجريمة.

---

[309]– **علي محمود علي حمودة**، المرجع السابق، ص20

[310]– **محمد بن عبد الله علي المنشاوي**، المرجع السابق، ص54

[311]– **حسن طاهر داود**، المرجع السابق، ص87

[312]– **محمد حماد مرهج الهيتي**، جرائم الحاسوب...، المرجع السابق، ص217

تحرص الجهات المجني على عدم الإبلاغ عن الجريمة التي راحت ضحيتها من أجل إخفاء أساليب ارتكابها للحيلولة دون تقليد الآخرين للجناة ومحاكاتهم في جرائمهم، كما قد يتوخى بعض المجني عليهم من وراء العزوف عن الإبلاغ عدم إتاحة الفرصة للأجهزة الأمنية من الاطلاع على معلومات لم يجر الإبلاغ عنها، وربما يتجلّى ذلك بصورة أكبر في نطاق جرائم الإنترنت التي تقع على شركات التأمين أو البنوك رغبة في توقي الخسائر التي يتوقع تحققها نتيجة هذا الإبلاغ بسبب نقص ثقة العملاء في هذه المؤسسات[313].

تظل الجريمة المرتكبة عبر الإنترنت مستترة ما لم يتم الإبلاغ عنها، ومن ثم عمل الاستدلالات أو تحريك الدعوى الجنائية حسب القانون السائد، والصعوبة التي تواجه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة العادية كما هو الحال في الجريمة التقليدية[314].

رابعا: نقص خبرة سلطات الاستدلال

تفرض متطلبات العدالة الجنائية على الأجهزة الحكومية بشكل عام، والأجهزة المسؤولة عن تتبع الجرائم وضبطها والتحقيق فيها بشكل خاص أن تتحمل مسؤولياتها نحو اكتشاف المجرمين وضبطهم ومحاكمتهم، ومثل هذا الأمر يقتضي توفير الإمكانات التقنية اللازمة، سواء في عملية التحقيق أو الكشف والاستدلال عن الجرائم، لاسيما بعد أن تطورت ليس فقط أساليب الكشف عن الجرائم، إنما أيضا تطور أساليب ارتكاب الجرائم وظهور أنماط جديدة من الجرائم ما كانت التشريعات لتعرفها من قبل، إلا بعد أن ظهرت وسائل متطورة تمكن المجرمين ارتكاب جرائمهم بأساليب وطرق غير معهودة[315].

---

[313]– **موسى مسعود أرحومة**، المرجع السابق، ص5

[314] - *La lutte contre la cybercriminalité n'est pas le monopole de l'état, elle concerne l'ensemble des acteurs publics et privés, les entreprises comme les particuliers qui doivent avoir une démarche citoyenne.* Voir: **Les Officiers de l'équipe de lutte contre la cybercriminalité de la Gendarmerie Nationale,** op-cit, p13.

[315]– **محمد حماد مرهج الهيتي**، جرائم الحاسوب...، المرجع السابق، ص215

تواجه عملية استخلاص الدليل في الجريمة المرتكبة عبر الإنترنت نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجرائم المرتكبة عبر الإنترنت وكيفية التعامل معها، وذلك على الأقل في البلدان العربية، نظرا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخرا عن أوربا وكندا والولايات المتحدة الأمريكية، وأن أجهزة العدالة المقاومة للجرائم المرتبطة بهذه التقنية تبدأ بالتكوين والتشكيل عقب ظهور هذه الجرائم، وهو أمر يستغرق وقتا أبطأ من وقت انتشار الجريمة، لأن الجريمة المرتكبة عبر الإنترنت تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن الحركة التشريعية، أو الثقافة الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التطور ينعكس سلبا على إجراءات الاستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة المرتكبة عبر الإنترنت، ومن هنا تأتي الدعوة إلى وجوب تأهيل سلطات الأمن وجهات التحقيق والإدعاء والحكم في شأن هذه الجرائم[316].

لاحظ جانب كبير من الفقه الجنائي أن البحث والتحقيق في جرائم الحاسب الآلي هي مسألة في غاية الأهمية والصعوبة، ولاسيما بالنظر لاعتبارات التكوين العلمي والتدريبي، والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي والحكم، ذلك أن حداثة الجرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق إلمام كاف بها، فلا يكفي أن يكون لهم الخلفية القانونية أو أركان العمل الشرطي فقط، ولكن لابد من الإلمام بخبرة فنية في مجال الجريمة المرتكبة عبر الإنترنت[317].

إلا أن المشكلة ليست في منح الموظفين ذوي العلاقة بجرائم الإنترنت صفة مأموري الضبط القضائي، ذلك أن مأموري الضبط القضائي القائمين بالفعل وسلطات التحقيق الجنائي تنقصها الثقافة في الجريمة المرتكبة عبر الإنترنت، حيث نقص الخبرة لدى رجال

316– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص81

317– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص122

الأمن والمحققين العاملين الآن في مجال مكافحة الجرائم المرتكبة عبر الإنترنت هو خير معين لمرتكبي جرائم الإنترنت.

أثبتت الوقائع أن هنالك جرائم متعلقة بالإنترنت ارتكبت على مرأى ومسمع من رجال الأمن، بل قام بعض رجال الأمن بتقديم يد المساعدة لمرتكبي جرائم الإنترنت دون قصد وعن جهل[318]، فإذا كان هذا هو حال الأشخاص المناط بهم إنفاذ القوانين وحماية المجتمع من الأشرار فإننا حسب أن الكثيرين من عامة الناس قد تقع في حقهم أو في حضورهم أو بتسهيلات منهم جرائم عبر الإنترنت[319].

يزيد من التحدي الذي يواجه أجهزة العدالة الجنائية في جرائم الإنترنت، أن الجناة في هذه الجرائم لهم المفردات والمصطلحات الخاصة بهم، لدرجة أنهم يطلقون على أنفسهم اسم النخبة بدعوى أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاته المتميزة، ويطلق على رجال الشرطة والنيابة والقضاة صفة الضعفاء أو القاصرين[320].

بدأت بعض الدول محاولات جادة في استيعاب رجال الأمن والقضاء ضمن المتخصصين في المعلوماتية أو علوم وتطبيقات الحاسب الآلي، فضلا عن قبول خبراء هذا المجال ضمن رجال الضبط والقضاء، ولكن هذه المحاولات لن تأتي ثمارها في القريب العاجل للآتي:

1- الميزانيات المالية لدى أجهزة الأمن والقضاء تكون ضعيفة بالنظر إلى خبرة المتخصصين في علوم الحاسب الآلي فضلا عن أنها لا تصل إلى ذات المبالغ التي تسددها مؤسسات وشركات القطاع الخاص[321].

---

[318]- كمثال عن ذلك طلب إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من الشركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، وقد حدث نتيجة لذلك أن تسببت دائرة البوليس بدون قصد في إتلاف ما كان قد سلم من الملفات والبرامج: **محمد أبو العلا عقيدة**، المرجع السابق، ص4

[319]- **محمد الأمين البشري**، « **التحقيق في الجرائم المستحدثة** »، المرجع السابق، ص107.

[320]- **حسين بن سعيد الغافري**، « **التحقيق وجمع الأدلة المتعلقة بشبكة الإنترنت** »، المرجع السابق، ص20

[321]- **محمد الأمين البشري**، « **تأهيل المحققين في جرائم الحاسوب والإنترنت** »، المرجع السابق، ص23

2- من المعروف أن الخبرة العملية لدى سلطات الضبط والتحقيق الجنائي تتأتى من ممارسة أعمال الضبط والتحقيق والاعتياد عليها وذلك يقتضي وقوع هذه الجرائم موضوع الضبط والتحقيق، ولذلك الجريمة المرتكبة عبر الإنترنت لم تقع حتى الآن بالعدد وبالشكل الذي يوازي جريمة التقليدية كالسرقة أو الضرب أو القتل، ولذلك فالخبرة الإجرائية في الضبط والتحقيق لدى أجهزة العدالة بشأن جريمة الإنترنت لازالت حديثة، إلا أنه مع انتشار الحاسب الآلي وتفشيه في الحياة الخاصة والعامة، ولدى الحكومة والقطاع الخاص، وما يستتبعه ن أفعال مخالفة-وليست مجرمة- نظرا لعدم وضوح الرؤية في نصوص التجريم فإن ذلك يثري عمل الضبط والتحقيق مستقبلا[322].

3- كذلك أدى انتشار الحاسب الآلي على نطاق واسع وتعدد أنظمته وبرامجه وتطورها بشكل سريع ومتلاحق، يجعل ملاحقتها من حيث إعداد وتدريب رجال الضبط والتحقيق الجنائي عليها أمر يتسم بالصعوبة، ومع ذلك فيجب ألا يكون ذلك مبررا للنقاش لأن التدريب في كل الأحوال لن يخلو من فائدة سيما وأن هذه الأجهزة عند تدريبها ستكون قابلة لتحديث وتطوير فنها أولا بأول كلما جد جديد، وذلك لأن الأسس أو القواعد العامة في فن الحاسب الآلي والجريمة المرتكبة عبر الإنترنت موجودة لديها بالفعل، وذلك بدلاً من عدم التدريب أساساً[323].

الفرع الثاني
إثبات الجريمة المرتكبة عبر الإنترنت

تتعلق عملية إثبات الجرائم بصفة عامة بإقامة الدليل، وذلك بالنظر إلى نوع الجريمة وإلى الإجراءات التي يتم إتباعها للحصول على الدليل، وهذه الخطوات هي المتبعة في كل الجرائم بما فيها الجرائم المرتكبة عبر الإنترنت، غير أن في هذه الأخيرة تكون عملية

---

[322]- **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع لسابق، ص85

[323]- **عبد الرحمن عبد العزيز الشنيفي**، مدى استفادة الأجهزة الأمنية من خدمات شبكة الإنترنت دراسة استطلاعية على إدارتي الشرطة والمرور بمدينة الرياض، دراسة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العلوم الإدارية، كلية الدراسات العليا، قسم العلوم الإدارية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص32

استخلاص الدليل صعبة للغاية نظراً لكون الأدلة في هذا النوع من الجرائم يتميز بخصوصيته المعنوية، بالإضافة إلى ذلك فالإجراءات المتبعة في إثبات هذه الأدلة أثبتت قصورها، فإذا كانت ذات فائدة في الجرائم التقليدية، فهي غير مجدية في جرائم الإنترنت في غالب الأحوال، خاصة في ظل الطابع العالمي لهذه الجريمة.

أولا:غياب دليل مرئي يمكن فهمه

يكون دليل الإثبات في الجريمة التقليدية مرئيا من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب، وكذلك المادة السامة التي تستعمل في القتل، أو المحرر ذاته الذي تم تزويره، أو النقود التي زيفت وأدوات تزييفها، وفي كل هذه الأمثلة يستطيع رجل الضبط أو التحقيق الجنائي رؤية الدليل المادي وملامسته بإحدى حواسه.[324]

لكن في الجرائم التي تقع على العمليات الإلكترونية المختلفة خاصة التي تقع عبر شبكة الإنترنت، كالتي تقع على عمليات التجارة الإلكترونية، أو على العمليات الإلكترونية للأعمال المصرفية، أو على أعمال الحكومة الإلكترونية، يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، فإذا وقعت جرائم معينة على هذه الجوانب المعنوية، كجرائم السرقة أو الاختلاس أو الاستيلاء أو الغش أو التزوير أو الإتلاف فإنه قد يصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة[325].

يوجد شك في أن إثبات الأمور المادية التي تترك آثارا ملحوظة يكون سهلا ميسورا، بعكس إثبات الأمور المعنوية فإنه يكون في منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي آثار قد تدل عليه أو تكشف عنه، بحسبان أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحاسبات الآلية فالجرائم التي ترتكب على العمليات الإلكترونية التي تعتمد في موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين

---

[324]– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص36

[325]– **علي محمود علي حمودة**، المرجع السابق، ص16.

الإلكتروني يصعب أن تخلف وراءها آثارا مرئية قد تكشف عنها أو يستدل من خلالها على الجناة[326].

تعد الطبيعة غير المرئية للأدلة المتحصل عليها من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع عبر الإنترنت حيث يعتبر كشف وتجميع من هذا النوع لإثبات وقوع الجريمة والتعرف على مرتكبها أحد أبرز المشكلات التي يمكن أن تواجه جهات التحري والملاحقة كضباط لشرطة[327].

اعتادت جهات التحري والتحقيق على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإنترنت الأمر مختلف، فالمتحري أو المحقق لا يستطيع أي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية

ثانيا: سهولة إخفاء الدليل

تعتبر سهولة إخفاء الدليل أو محوه تدميره من بين الصعوبات التي يمكن أن تعترض العملية الإثباتية في مجال جرائم الإنترنت، حيث يقوم الجاني بمحو أو تدمير أدلة الإدانة بسهولة متناهية، فضلا عن سهولة تنصله من مسؤولية هذا العمل بإرجاعه، حسبما تشهد بذلك وقائع عديدة، على خطأ في نظام الحاسب أو الشبكة أو في الأجهزة[328].

كما أن هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الإنترنت ويكون أمرها حكرا عليهم كالتجسس على ملفات البيانات المختزنة والوقوف على ما بها من أسرار، كما أنهم قد ينسخون هذه الملفات ويحصلون على نسخ منها بقصد استعمالها

326– **غازي عبد الرحمان هيان الرشيد**، المرجع السابق، ص539

327– **عبد الرحمن محمد بحر**، المرجع السابق، ص27

328– من الأمثلة الواقعية حالة شهدتها النمسا تتلخص وقائعها في قيام أحد مهربي الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر على الحاسب من خلال لوحة المفاتيح بالنسخ أو الطبع محو وتدمير البيانات كلها، **هشام فريد رستم**، المرجع السابق، ص 429_430

تحقيقا لمصالحهم الخاصة، كذلك فإنه قد يقومون باختراق قواعد البيانات والتغيير في محتوياتها تحقيقا لمآرب خاصة، وقد يخربون الأنظمة تخريبا منطقيا بحيث يمكن تمويهه، كما لو كان مصدره خطأ في البرنامج أو في الأجهزة أو في أنظمة التشغيل أو التصميم الكلي للنظام المعالج آليا للمعلومات، وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسب أو يعدلون برامجه أو يحرفون البيانات المخزنة بداخله دون أن يتخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل[329].

مما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصل من الوسائل الإلكترونية أنه يمكن محو الدليل في زمن قصير، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جدا ، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده[330].

ثالثا: إعاقة الوصول إلى الدليل

جناة الجرائم الإنترنت من المجرمين المحترفين الذين لا يرتكبون جرائمهم بسبب الاستفزاز أو الاستثارة وإنما هم يخططون لما يفعلون ويستخدمون قدراتهم الفنية والعقلية لنجاح هذا التخطيط، ولذلك نجد أنهم وهم يرتكبون الجرائم عبر الإنترنت يحيطون أنفسهم بتدابير أمنية واقية تزيد من صعوبة تحديد هويتهم [331].

---

[329]– **محمد حماد مرهج الهيتي**، جرائم الحاسوب...، المرجع السابق، ص212

[330]– **حسين بن سعيد الغافري**، « **التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت** »، المرجع السابق، ص19.

[331]- كمثال لذلك نجد أنهم قد يستخدمون التشفير وكلمات السر التي تمكنهم من إخفاء الأدلة التي قد تكون قائمة ضدهم، وقد يدسون تعليمات خفية بين الأدلة لتصبح كالرمز فلا يمكن لغيرهم أن يفهم مقصودها، وقد يقوم هؤلاء أيضا بتشفير التعليمات باستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها في منتهى الصعوبة، **محمد علي حمودة**، المرجع السابق، ص18

يستخدم هؤلاء الجناة مختلف الوسائل عبر الإنترنت لإعاقة الوصول إليهم، كاستخدام كلمات سر أو دس تعليمات خفية بينها أو ترميزها[332]، لإعاقة أو منع الإطلاع عليها أو ضبطها ويشكل استخدام تقنيات التشفير لهذا الغرض أحد أكبر العقبات التي تعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة، والتي تحد من قدرة جهات التحري والتحقيق والملاحقة على قرائتها، الأمر الذي يجعل صون حرمة البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والإلكترونية أو بتدابير الأمن والدفاع أمرا بالغ الصعوبة[333].

يكشف هذا الأمر عن أهمية التعاون القضائي الدولي في مجال الإنابة القضائية خاصة في مجال الجرائم العابرة للقارات والتي منها تلك الجرائم التي تقع الشبكة العالمية للإنترنت.

رابعا: جرائم الإنترنت متعدية الحدود

تعد شبكة الإنترنت بطبيعتها عالمية الهوية والانتشار، وتبعا لذلك فكل نشاط إجرامي يتم من خلالها يكتسب هذه الصفة بالضرورة، وبالنظر إلى الطبيعة الاتصالية لشبكة الإنترنت والممارسات التجارية وغير التجارية التي سمح بها، يمكن تخيل العديد من الفرص التي تساهم بوجود نشاط إجرامي في مجال غسيل الأموال، والتجارة في المخدرات، والأنشطة الإرهابية المنظمة، ونظرا لارتباط أنشطة الاقتصاد الخفي ببعضها خاصة في مجال القمار وتجارة المخدرات، فإنه يمكن أن يطور المجرمون عبر شبكة الإنترنت آليات معقدة لغسل الأموال يصعب معها تتبع مثل هذه العمليات على الشبكة من الناحية الفنية، إضافة إلى تعقد النواحي القانونية في مثل هذه الجرائم الممتدة.

---

[332]– يتم البحث عن الدليل الرقمي في وسط افتراضي يحتويه الجهاز الذي ارتكبت به أو ضده الجريمة محل البحث، وغالبا ما يكون هذا الجهاز مزودا بنظام حماية، بحيث لا يمكن تشغيله إلاّ باستعمال كلمة مرور معلومة لدى المجرم، وهو ما يحول دون الحصول على المعلومات من خلاله، **طارق محمد الجملي**، «**الدليل الرقمي في مجال الإثبات الجنائي**»، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28_2009/10/29، ص17

[333]– **هشام فريد رستم**، المرجع السابق، ص427

يثير البعد عبر الوطني في مجال الجرائم المرتكبة عبر الإنترنت مشكلات عديدة مثل تتبع الاتصالات الإلكترونية عن طرق سلطات التحقيق لأجل إقامة الدليل على الجرائم التي ترتكب في مجال الإنترنت، ولا شك في أن اختلاف التشريعات فيما بينها فيما يتعلق بشروط قبولها للأدلة وتنفيذ بعض الإجراءات مثل التفتيش والمعاينة عبر الحدود ليثير مشكلات عديدة قد تعوق اتخاذ الإجراءات اللازمة لضبط هذا النوع من الجرائم العابرة للحدود.

كذلك فإن هناك معوقات كثيرة قد تعترض الحصول على الأدلة بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية، ومثال ذلك أنه قد يتعذر اتخاذ إجراءات التفتيش لضبط هذه الجرائم عندما يكون الحاسب الآلي متصلا بحاسبات أخرى خارج الدولة، ويكون تفتيش هذه الحاسبات ضرورية لإماطة اللثام عما تشتمله من جرائم وليس بِخافٍ علينا أن الجرائم التي ترتكب في فضاء شبكة الإنترنت. كما أنها تقع على المستوى الوطني، فإنها قد ترتكب أيضا على المستوى الدولي، فالجريمة المرتكبة عبر الإنترنت تتميز اتساع النطاق أو البعد الجغرافي لها، حيث قد يتم تسجيل الإبلاغ عن الجريمة في مكان معين بينما توجد الأدلة الجنائية في دولة أخرى، مما يتطلب إخضاع إجراءات التحقيق للقوانين أو التشريعات الجنائية السارية في هذه الدولة[334].

خامسا: ضخامة البيانات المتعين فحصها

تعرف قواعد البيانات بأنها عبارة عن مجموع بطاقات تشمل على بيانات معدلة ومنظمة تسمح باقتطاع البيانات حسب مشيئة المستعمل، ومصطلح قادة البيانات أو بنك البيانات شاع استعماله، وربما يعني لمعظم الناس أن نوع من الكمبيوتر تجمع فيه كل أنواع المعطيات الخام على أمل أن يستطاع الرجوع إليها عند الحاجة.

تعتبر قاعدة البيانات بأنها نظام فعال يستعمل لترتيب الملفات التي تحتوي على معلومات محددة كما أن قاعدة بيانات واحدة يمكنها أن تشمل على عدد لا يحصى من الملفات، ويمكن استخراج هذه البطاقات بنظام أبجدي باختيار عناصر معينة وترتيبها

[334]– **سالم بن محمد السالم**، المرجع السابق، ص17

للاستفادة منها لاحقاً، وتعتبر قواعد البيانات كوسيط لتخزين المعلومات ومعالجتها أي ترتيبها وتنظيمها الذي غايته أن يجمع كل المعطيات أو المعلومات المتعلقة بحقل خاص[335]

يشكل الكم الهائل من البيانات التي يجري تداولها عبر الإنترنت أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها، آية ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التي قد لا تثبت كلها تقريبا شيئا على الإطلاق[336]،

قد تكون النتيجة سلبية بحيث لا يمكنها كشف الدليل المراد ضبطه أو تحصيله، وهذا مرده في المقام الأول عدم وجود آلية للفرز الذاتي للملفات المخزنة، حتى يمكن الوقوف على الملفات غير المشروعة وضبطها، ومن هنا فالأمر جدّ مرهق، بل وغير مجد في كثير من الأحيان، لما يستغرقه من وقت لا طائل منه، ما يجعل القضاء لا يكترث بالدليل الرقمي، ولا يعول عليه كثيرا لافتقاره إلى المصداقية التي تجعله جديرا بالثقة[337].

لذلك وفي ظل تواضع المستوى الفني لرجال الضبط والمحقق الجنائي–كما أسلفنا الذكر– فيما يتعلق بفنون الحاسب الآلي واستخداماته، فإنه يكون من الملائم وجوب ندب خبراء فنيين في مثل هذه الجرائم حتى يمكن فرز المعلومات التي يحتاجها التحقيق عن تلك التي لا حاجة لها، وإلاّ دخل رجل الضبط والمحقق في دائرة مغلقة من المعلومات لن يخرج منها، وهذا يتطلب أن يكون ندب هؤلاء الخبراء وجوبياً ومن ثم تعديل التشريعات الجنائية القائمة التي تجعل ندب خبير في الدعوى أمر جوازي للمحقق إن شاء أمر به أو رفضه، وذلك لأن طبيعة الجريمة تستلزم التعامل معها بطريقة حرفية أو فنية تفوق قدرات رجل الضبط أو المحقق إلاّ إذا كان مؤهلاً لذلك، فيمكنه الاعتماد على قدراته الشخصية

---

[335]– **بوعمرة آسيا**، النظام القانوني لقواعد البيانات، مذكرة لنيل شهادة الماجستير في القانون، فرع الملكية الفكرية، كلية الحقوق، جامعة الجزائر، 2005، ص11_12

[336]– **هشام محمد فريد رستم**، المرجع السابق، ص430

[337]– **موسى مسعود أرحومة**، المرجع السابق، ص6

في ضبط وتحقيق هذه الجرائم شرط ألاّ يخرج عمله عن الأصول الفنية المتعارف عليها[338].

سادسا: قصور إجراءات الحصول على الدليل الإلكتروني

يشترط في الدليل الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة، وذلك يقتضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن[339]، على عكس إثبات الجرائم المرتكبة عبر الإنترنت حيث لا تقف الصعوبة فيها عند التعذر للوصول إلى الأدلة التي تكفي لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة، فإذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة فإنه قد يصعب عليها القيام بهذا التحري وبهذه الطرق بالنسبة للجرائم التي ترتكب عن طريق الإنترنت.

فعلى الرغم من أن إرهاصات الثورة التكنولوجية في مجال الاتصالات عن بعد قد أفرزت العديد من الجرائم ذات الطبيعة الخاصة، فما زالت إجراءات البحث عن هذه الجرائم وضبطها تتم في إطار النصوص الإجرائية التقليدية التي وضعت لكي تطبق على الجرائم التقليدية التي تنص عليها القوانين العقابية، الأمر الذي ستترتب عليه الكثير من المشكلات بالنسبة لضبط هذه الجرائم المستجدة ذات الكيان المعنوي والتي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الإنترنت، فيتعذر تبعا لذلك اتخاذ إجراءات جمع الدليل بالنسبة لها، أو قد تلحق عدم المشروعية بهذه الإجراءات[340].

يلجأ بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة في الخارج، فيصعب إثباتها، ويثور التساؤل حول حرية تدفق المعلومات وهل يصلح لتدفق البيانات

---

[338]– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص110_111

[339]– **طارق محمد الجملي**، المرجع السابق، ص16

[340]– **علي محمود علي حمودة**، المرجع السابق، ص21.

الموجودة خارج الدولة المتعلقة بالجريمة محل البحث، حيث يواجه التفتيش وجمع الأدلة صعوبات كثيرة في هذا المجال، وقد يتعلقان بما أنهما يتعلقان ببيانات مخزنة وموجودة خارج حدود الدولة، وتثير مسألة الدخول إليها ومحاولة جمعها وتحويلها إلى الدولة التي يجري فيها التحقيق، مشكلات تتعلق بسيادة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات[341].

لا تفلح غالبا وسائل المعاينة وطرقها التقليدية في إثبات هذه الجريمة نظراً لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فلأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف آثاراً مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة.

لكن فكرة معاينة مسرح الجريمة في الجريمة المرتكبة عبر الإنترنت يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة، وذلك راجع إلى أنه كثير من الأشخاص يترددون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة حتى اكتشافها أو التحقيق فيها هي فترة طويلة نسبياً، الأمر الذي يعطي مجالاً للجاني أو الآخرين أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المرتكبة عبر الإنترنت[342].

أما بالنسبة لعمل الخبراء في مجال التحقيق في الجرائم المرتكبة عبر الإنترنت فهو مشوب بعيب أن معظم هؤلاء الخبراء ليس لهم صفة الضبطية القضائية، بل أكثر من ذلك أنّ أغلبهم عندهم سوابق في مجال الإجرام الإلكتروني، حيث تقوم سلطات الاستدلال بانتدابهم من أجل الخبرة التي يتمتعون بها.

تعتبر كذلك قضية انتهاك الخصوصية من بين أهم القضايا المطروحة في مجال التحقيق في الجرائم المتعلقة بالشبكة العالمية للإنترنت، خاصة فيما يتعلق بالتفتيش والمعاينة عبر الإنترنت، حيث يتطلب ذلك فحص مختلف المعاملات عبرها بما فيها

---

[341]– **محمد أبو العلا عقيدة**، الرجع السابق، ص2.

[342]– **نهلا عبد القادر المومني**، المرجع السابق، ص56–57.

تفتيش البريد الإلكتروني مثلاً، الأمر الذي يجعل خصوصيات الأفراد على المحك[343]، خاصة إذا كان التفتيش والمعاينة متعلقة بحاسبات متصلة بالحاسب محل التحقيق، فالحق في الخاصة بمثابة عائق يحول دون إجراء التحقيق على أكمل وجه فيما يخص الجرائم المرتكبة عبر الإنترنت.

يزداد الأمر تعقيدا إذا علمنا أن كافة التشريعات العقابية والإجرائية تقضي بإعفاء المتهم من تقديم ما من شأنه إثبات إدانته بطريقة مباشرة وبذلك لا يجوز إجبار المتهم على البوح لسلطة التحقيق بالرمز السري للمرور إلى ملفات البيانات أو أن يكشف عن كلمة السر وطبع البيانات المخزنة، بالنظام وغير ذلك من الأمور التي من شأنها أن تؤدي إلى إدانته[344].

المطلب الثاني
صعوبات متعلقة بالجانب القضائي

يفرض الطابع الدولي لجرائم الإنترنت تعاون أكثر من دولة بما أن الجريمة تخترق كل الحدود الإقليمية المعمول بها، غير أن الملاحظ في الواقع قصور هذا التعاون الدولي

---

[343]– يتخذ الحق في الخصوصية أربع صور هي:

1–خصوصية المعلومات: والتي تتضمن القواعد التي تحكم جمع وإرادة البيانات الخاصة كمعلومات بطاقة الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وهي المعبر عنها عادة اصطلاحا حماية البيانات.

2–الخصوصية الجسدية أو المادية: والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات وفحص المخدرات وشمل بالطبع جسد الفرد من أنشطة التفتيش وأنشطة الإيذاء غير القانونية.

3– خصوصية الاتصالات: والتي تغطي في تطورها الراهن سرية وخصوصية المراسلات الإلكترونية والبريد الإلكتروني وغيرها من وسائل الاتصال والتحادث في البيئة الرقمية إلى جانب ما تغطيه وفق مفهومها التقليدي من خصوصية كافة أنواع المراسلات والاتصالات العادية، كالبريد والهاتف وغيرها.

4–الخصوصية المكانية أو خصوصية المكان: والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الإلكترونية والتوثق من بطاقات الهوية، **يونس عرب**،« **دور الخصوصية في تشجيع الاندماج بالمجتمع الرقمي** »، ندوة أخلاق المعلومات، نادي المعلومات العربي، عمان، الأردن، 16–17 أكتوبر 2002، ص27.

[344]– **عفيفي كامل عفيفي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007، ص365

مقارنة بتطور الجريمة، وكذا الإجراءات التقليدية المطبقة في مجال التعاون الدولي للحد من الإجرام العابر للحدود لم تتطور بتطور التقنية، مما يولد فارق شاسع بين سرعة الجرائم المرتكبة عبر الإنترنت وبطئ الإجراءات المتبعة **(الفرع الأول)**.

انبثق عن الطابع العالمي للجريمة المرتكبة عبر الإنترنت صعوبات أخرى تتمثل في القانون الواجب التطبيق والمحكمة المختصة، حيث أن ميزة الجريمة المتعدية خلقت إشكالا حادا انجر عنه تنازع قوانين أكثر من دولة في هذا المجال، وكذلك صعوبة تحديد المحكمة المختصة تعتبر إشكالا عويصاً، حيث ترى كل دولة أن لها الحق في متابعة مرتكب هذه الجريمة لعدة اعتبارات **(الفرع الثاني)**.

الفرع الأول

قصور التعاون القضائي الدولي في مكافحة الجريمة المرتكبة عبر الإنترنت

يعتبر التعاون الدولي في مجال مكافحة الجريمة المرتكبة عبر الإنترنت من بين أصعب المواضيع المطروحة على هذا المستوى، وذلك راجع إلى الاختلافات القائمة في التشريعات والممارسات بين الدول وكذلك بسبب العدد المحدود نسبيا من المعاهدات والاتفاقيات المتاحة للدول بشأن التعاون الدولي[345]، ويعد التعاون الدولي بكافة صوره في مجال مكافحة الجرائم المتعلقة بشبكة الإنترنت، مطلبا تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها، إلا أنه ثمة معوقات تقف دون تحقيقه أهمها:

أولاً: عدم وجود نموذج موحد للنشاط الإجرامي

نظرا لعدم وجود مفهوم عام مشترك بين الدول حول نماذج النشاط المتعلق بالجرائم المرتكبة عبر الإنترنت، ونظرا لاختلاف المفاهيم الخاصة بها لاختلاف التقاليد والأعراف القانونية الدولية فإن هذا يضعف من منظومة القانون الدولي في مجال ضبط تلك الجرائم، وبالتالي يسهل على الجناة الإفلات من المسائلة الجنائية[346].

---

[345]– **فريق الخبراء المعني بالجريمة السيبرانية**، مشروع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدي لها، UNODC، فيينا، 17_21 يناير 2011

[346]– **إيهاب ماهر السنباطي**، المرجع السابق، ص68

يضفي عدم توفر تعريف موحّد للجريمة المرتكبة عبر الإنترنت إلى بقاء أفعالا جرمية دون تجريم، حيث تكون أفعال في تشريع ما معتبرة جرما، وتكون في تشريع آخر مباحة، لاختلاف تحديد عناصر الجرم المعلوماتي بين الدولتين المعنيتين.[347]

تثير الطبيعة الدولية للجريمة المرتكبة عبر الإنترنت مشاكل فيما يتعلق تحيدي القانون الواجب التطبيق، هل هو قانون الدولة التي ارتكب فيها الفعل أم قانون الدولة التي ظهرت فيهما الآثار الضارة، إضافة إلى تعارض القوانين من ناحية موضوعية وإجرائية الأمر الذي يستلزم ضرورة العمل على توحيد التشريعات فيما يتعلق بمكافحة الجرائم المرتكبة عبر الإنترنت إضافة إلى إبرام الاتفاقيات في هذا المجال[348].

ثانياً: تنوع واختلاف النظم القانونية الإجرائية

سبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع الأدلة أو التحقيق أنها قانونية في دولة معينة، فإنه قد تكون ذات الطريقة غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات تطبيق القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعّالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع[349].

تعتبر قضية الدودة الحاسوبية "لوف باغ love bug" التي أعدّت في الفلبين عام

---

[347]– **فريد منعم جبور**، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الإلكترونية (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2010، ص215

[348]– **عواطف محمد عثمان عبد الحليم**، المرجع السابق، ص68

[349]– **براء منذر كمال عبد اللطيف، ناظر أحمد منديل، « التعاون القضائي الدولي في مواجهة جرائم الإنترنت»**، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009، ص11.

2000 وقيل أنها عطّلت ملايين الحواسيب في جميع أنحاء العالم، أحسن مثال على اختلاف النهج القانونية بين الدول، حيث أعاقت هذه القضية التحقيقات بسبب أن ذلك العمل المؤذي والضار لم يكن آنذاك مجرما بشكل كاف في الفلبين[350]

ثالثاً:عدم وجود قنوات اتصال

يعد أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون[351].

يعتبر عدم وجود الاتصال والتنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة المرتكبة عبر الإنترنت بين الدول المختلفة، خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق، سيما وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة، عن طريق الضبط أو التفتيش في نظام معلوماتي معين هو أمر غاية في الصعوبة، فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته[352].

رابعاً: مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت :

أثارت الجرائم المرتكبة عبر الإنترنت مسألة الاختصاص على المستوى المحلي والدولي، بالرغم من أنه لا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير لمحددة قانوناً لذلك.

ينجم عن اختلاف التشريعات والنظم القانونية تنازع في الاختصاص بين الدول خاصة في إطار الجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود، فقد يحدث

---

[350]– مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، المرجع السابق، ص6

[351]– **براء منذر كمال عبد اللطيف، ناظر أحمد منديل**، المرجع السابق، ص12

[352]– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص104_105

أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استناداً إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة[353].

يلاحظ أن اختصاص القضاء بنظر الجرائم التي تتم عبر شبكة الإنترنت والقانون الواجب تطبيقه على الفعل لا يحضى بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال من قبل أشخاص من خارج حدود الدولة أو أنه تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق وما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات في حقل الاختصاص القضائي، ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود[354].

أدى هذا البعد عبر الوطني للجريمة المرتكبة عبر الإنترنت شتت الجهود وأعاق التعاون الدولي في مجال التصدي لهذا النوع من الإجرام، وذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق[355]

---

[353]– **حسين بن سعيد بن سيف الغافري**، « **الجهود الدولية في مواجهة جرائم الإنترنت** »، ص52_53، مقال متوفر على الموقع التالي:http://www.minshawi.com

[354]– **عبد الله عبد الكريم عبد الله**، المرجع السابق، ص47_48

[355]– **محمود أحمد عبابنة**، المرجع السابق، ص35

خامساً: التجريم المزدوج

يعتبر شرط التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية والاتفاقات الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته تلك ، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المرتكبة عبر الإنترنت، سيما وأن معظم الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت.

يجد شرط التجريم المزدوج أساسه في أن الدولة طالبة التسليم تبتغي من وراء طلبها محاكمة من نسب إليه ارتكاب السلوك الإجرامي أو تنفيذ العقوبة المحكوم بها عليه، وهذا يفترض بداهة أن السلوك مجرم في تشريعها، حيث أنه إذا لم يكن مجرماً فلا يتصور وجود دعوى عمومية أو ملاحقة جزائية ضد الشخص المتهم كما لا يتصور قيام حكم جزائي يقضي بعقوبة عليه هذا من ناحية، ومن ناحية أخرى لا يجوز مطالبة الدولة المطلوب إليها التسليم بإيقاع عقوبة على ارتكاب سلوك ما هو في الأساس غير مجرم وفقاً لقانونها[356].

يرجع هذا إلى عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم الحاسب وشبكة الإنترنت، ومن ثم تطور الجريمة المرتكبة عبر الإنترنت بذات السرعة، ومن ثم يظهر الأثر السلبي

---

[356]– من أشهر الحالات التي وقعت في التسعينات، الهجوم الذي شنه شاب روسي على مصرف سيتي بنك بالولايات المتحدة الأمريكية، فعن طريق استخدام حاسوبه الموجود في روسيا، نجح المتهم في أن يخترق دون إذن وحدات خدمة حواسيب لمصرف في الولايات المتحدة، وقام بتجنيد عدد من المتواطئين لفتح حسابات مصرفية في شتى أنحاء العالم، ثم أصدر تعليمات إلى حاسوب سيتي بنك بتحويل أموال إلى تلك الحسابات، وعند اكتشاف المخطط وتحديد هوية لمتهم، صدر في حقه أمر اعتقال من محكمة اتحادية بالولايات المتحدة، ولم تكن هناك معاهدة تسليم المجرمين في ذلك الوقت بين روسيا والولايات المتحدة الأمريكية. **حسين بن سعيد بن سيف الغافري**،« **الجهود الدولية في مواجهة جرائم الإنترنت** » ، المرجع السابق، ص26

في التعاون الدولي[357].

سادساً: الصعوبات الخاصة بالإنابة القضائية الدولية

نبعت الإنابة القضائية الدولية من الواجبات أو الالتزامات التي يفرضها القانون الدولي العام على الأمم المتحدة وبموجبها يعهد للسلطات القضائية – المطلوب منها اتخاذ إجراء – القيام بالتحقيق أو بالعديد من التحقيقات، لمصلحة السلطة القضائية المختصة في الدول الطالبة، مع مراعاة احترام حقوق وحريات الإنسان المعترف بها عالمياً، ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل، واحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية[358].

تهدف الإنابة القضائية إلى نقل الإجراءات في المسائل الجنائية، لمواجهة ما تشهده الظواهر الإجرامية من تطور، وتذليل العقبات التي تعرض سير الإجراءات الجنائية المتعلقة بقضايا ممتدة خارج الوطنية والإنابة القضائية تجد أساسها في القوانين الوطنية وفي الاتفاقيات الدولية وفي مبدأ المعاملة بالمثل.

يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية، فمثلاً طلب الحصول على دليل إثبات وهو عادة من شأن النيابة العامة تقوم بتوثيقه المحكمة الوطنية المختصة في الدولة الطالبة ثم يمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب[359].

تتسم أعمال الإنابة القضائي الدولية بالبطء والتعقيد، الأمر الذي قد يتعارض مع

---

[357]– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص105

[358]– تعرف الإنابة القضائية بأنها: طلب من السلطة القضائية المنيبة إلى السلطة المنابة قضائية كانت أم دبلوماسية أساسه التبادل باتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة في الخارج وكذا أي إجراء قضائي آخر يلزم اتخاذه للفصل في المسألة المثارة أو المحتمل إثارتها في المستقبل أمام القاضي المنيب ليس في مقدوره القيام به في نطاق دائرة اختصاصه، **شائف علي محمد الشيباني**، « **الإنابة القضائية الدولية في القانون اليمني دراسة مقارنة**»، مقال موجه لدائرة التدريب والتأهيل، النيابة العامة، الجمهورية اليمنية، 2006، ص10

[359]– **حسين بن سعيد بن سيف الغافري**، « **الجهود الدولية في مواجهة جرائم الإنترنت** »، المرجع لسابق، ص14

طبيعة أعمال الإنترنت وما تتميز به من سرعة، كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد ، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب.

أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق ، مثال ذلك الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال ، ونفس الشيء نجده في البند الثاني من المادة 30 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999م والمادة 15من اتفاقية الرياض العربية للتعاون القضائي 1983م ، والمادة 53 من اتفاقية شينغين1990 [360]والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف ، والفقرة 13 من المادة 46 من اتفاقية الأمم المتحدة لمكافحة الفساد.

يعتبر عامل السرعة من العوامل الرئيسية والهامة في مكافحة الجرائم المتعلقة بالإنترنت، ولكون غالبية هذه الاتفاقيات صدرت في وقت لم تكن شبكة الإنترنت قد ظهرت، أو كانت موجودة ولكنها محدودة، فإن تعديل هذه الاتفاقيات التقليدية للتعاون القضائي الدولي أصبح ضرورة ملحة خاصة مع التطور الكبير في تكنولوجيا المعلومات والاتصالات[361].

---

[360]- يتكون نظام معلومات شنغين من قسم مركزي مقره مدينة ستراسبورغ، وأقسام وطنية في كل دولة من الدول المنظمة، كذلك به بنك معلومات كبير تسجل فيه المعلومات التي ترسله إليه قوات الشرطة والسلطات القضائية في كل دولة، من بين هذه المعلومات عناوين الأفراد سواء أولئك المطلوب تسليمهم من قبل دول أخرى، أو الممنوعين من دخول أراض دولة ما، أو المعلن اختفاؤهم أو المطلوب تقديهم للعدالة بأمر قضائي لأي سبب كان، ولا يتم الرجوع إلى نظام= =المعلومات شنغين إلاّ في حالة القيام بإجراءات المراقبة على الحدود من طرف الشرطة والجمارك وكذلك تسليم تأشيرات الدخول وكذا الإقامات، **جان فرنسوا هنروت**، المرجع السابق، ص109

[361]– **براء منذر كمال عبد اللطيف، ناظر أحمد منديل**، المرجع السابق، ص12

الفرع الثاني

إشكالية تحديد القانون الواجب التطبيق والمحكمة المختصة بالجرائم المرتكبة عبر الإنترنت

تبرز أهمية تحديد القانون الواجب التطبيق والمحكمة المختصة في مجال الجرائم المرتكبة عبر الإنترنت جراء البعد العبر الوطني الذي تتميز به هذه الجريمة[362]، لأن غالبية الأفعال ترتكب من خارج الحدود أو أنها تمر عبر شبكة الإنترنت، وهو ما يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق، وما إذا كانت النظريات والقواعد القائمة في هذا المجال تطال هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات في حقل الاختصاص القضائي.

أولا: تحديد القانون الواجب التطبيق:

1-المبادئ التقليدية في تحديد القانون الواجب التطبيق

أ-مبدأ إقليمية النص الجنائي:

يرتبط قانون العقوبات في أية دولة ارتباطاً وثيقاً بسيادتها، بل أنّه في الحقيقة أهم مظاهر الدولة في سيادتها على إقليمها، ولذلك يعد مبدأ إقليمية النص الجنائي هو من المبادئ المستقرة في قوانين كل دول العالم، وقد تم اعتماده في التشريعات الجنائية لكل الدول[363].

ب-مبدأ عينية النص الجنائي:

يقصد بمبدأ العينية تتبع التشريع الجنائي الوطني للدولة، ليطبق على بعض الجرائم بعينها، والعقاب عليها رغم عدم وقوعها على الإقليم الوطني التي ترتكب في الخارج، بصرف النظر عن جنسية مرتكبيها، وهذا الامتداد يستند إلى ما للدولة من حق في الدفاع الذاتي، ضد كافة صور الاعتداء على مصالحها الأمنية، والمالية ولو ارتكبت خارج إقليمها، لاسيما وإن السلطات الأجنبية التي وقعت هذه الجرائم فوق إقليمها بالنسبة للجرائم التي لا تحفل بها التشريعات العقابية الأجنبية لعدم مساسها بمصالح مباشرة لبلادها،

---

[362]- **GRAVE-RAULIN Laurent**, op-cit, p 25

[363]- **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص499 وما يليها

وبالتالي تتقاعس عن ملاحقة الجاني، وتقديمه للعدالة لينال ما يستحقه من عقاب، والهدف من هذا المبدأ هو المساعدة في معالجة قصور وعجز مبدأ الإقليمية وهو من المبادئ المعتمدة في التشريعات الجنائية لدول العالم.

ج- مبدأ شخصية النص الجنائي

يرى الفقهاء أنّ لمبدأ شخصية النص الجنائي وجهان: أحدهما إيجابي وآخر سلبي، أما الوجه الإيجابي، فيعني بتطبيق النص الجنائي على كل من يحمل جنسية الدولة، ولو ارتكبت جريمته خارج إقليمها، أما الوجه السلبي للمبدأ، فيعني بتطبيق النص الجنائي، على كل جريمة يكون المجني عليه فيها، منتميا إلى جنسية الدولة ولو كان مرتكب هذه الجريمة أجنبيا وارتكبها خارج إقليم الدولة

2-انتفاء المبادئ التقليدية أمام خصوصية الجريمة المرتكبة عبر الإنترنت

يترتب على عدم تبعية شبكة الإنترنت لأي جهة أو شخص محدد ولعدم وجود مقر لها في دولة معينة، تخضع لرقابتها أو سيطرتها، ونظرا لعدم وجود قانون جنائي موحّد يحكم هذه الشبكة، فإن القوانين الجنائية التي تطبق عليها تتعدد بتعدد الدول المرتبطة بها، باعتبار أن القانون الجنائي يتعلق بسيادة الدولة.

الأصل في القوانين هو إقليمية القانون الجنائي، فإذا ما ارتكب شخص ما جريمة عن طريق الإنترنت بداخل الدولة، وتحققت نتيجتها بذات الدولة، فالقانون الواجب التطبيق بلا منازع هو قانون هذه الدولة بغض النظر عن جنسية الجاني أو المجني عليه، فقط يكفي أن تكون هذه الجريمة على إقليم الدولة سواء كان إقليما بريا، أو بحريا، أو جويا[364].

يترتب على تطبيق مبدأ إقليمية قانون العقوبات عدم اهتمام الدولة إلاّ بالجرائم التي تقع على إقليمها، فلا يمتد إلى ما يرتكب خارجه من جرائم ولو كان مرتكبوها من رعايا هذه الدولة، غير أن هذه النتيجة قد لا تتفق مع حماية مصالح الدولة[365]، خاصة فيما

---

[364]- **محمد عبيد الكعبي**، المرجع السابق، ص69

[365]- **أشرف توفيق شمس الدين**، الرجع السبق، ص58

يتعلق بالجرائم التي ترتكب عبر الإنترنت، وذلك راجع إلى البعد الدولي، بل العالمي لنشاط الشبكة، حيث يضع دول مختلفة في حالة اتصال دائم والبيانات والمعلومات التي يتم إدخالها وتحميلها على الشبكة تنتشر في ثوان معدودة في كل الدول المرتبطة بها، بحيث تكون متاحة لأي مستخدم في تلك الدول[366].

كذلك الأمر بالنسبة لمبدئي عينية وشخصية النص الجنائي اللذان لا يمكن تطبيقهما في هذا النطاق فإذا كان هذان المبدءان وضعا لكي يغطيا القصور الذي تميز به مبدأ إقليمية النص الجنائي في الجرائم التقليدية، فالأمر غير ذلك في الجرائم المرتكبة عبر الإنترنت، خاصة في ظل عالمية الشبكة، حيث أن السلوك في هذه الجريمة يمر عبر عدة دول الشيء الذي يخلق إشكالا كبيرا في تحديد القانون الواجب التطبيق نظرا لاختلاف تشريعات هذه الدول، وعدم وجود اتفاقات فيما بينها، فمثلاً دولة تأخذ بمبدأ الإقليمية والأخرى بمبدأ العينية، ودولة أخرى تأخذ بمبدأ الشخصية، الأمر الذي يثير نزاع فيما ينه على القانون الواجب تطبيقه، فكل دولة ترى نفسها الأحق بمتابعة الجاني.

ثانيا- تحديد المحكمة المختصة

تباينت المعايير الفقهية التي اعتمدت لتحديد المحكمة المختصة بنظر الجرائم المرتكبة عبر الإنترنت إلى ثلاث معايير هم:

1- معيار الاختصاص المكاني:

تعتمد أغلب التشريعات في تحديد الاختصاص المكاني، أتباع ثلاثة ضوابط هي، مكان وقوع الجريمة أو محل إقامة المتهم أو مكان ضبطه إلقاء القبض عليه، وفي حالة اجتماع أكثر من ضابط، تكون المحكمة التي ترفع إليها الدعوى أولاً، هي المختصة مكانيا بنظر الدعوى[367].

---

[366]- **أحمد عبد الكريم سلامة**، المرجع السابق، ص28

[367]- **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص518

يقصد بمكان ارتكاب الجريمة، المكان الذي ارتكب فيه السلوك ليس الذي تحققت فيه النتيجة، كون السلوك هو التعبير المادي عن إرادة مخالفة القانون، أما النتيجة فهي حدث خارجي يترتب عن السلوك.

ينعقد الاختصاص وفقا لهذا المعيار، للمحكمة التي يقع في نطاقها النشاط الإجرامي، وليس مكان حصول النتيجة أو الآثار المترتبة عليه، بدعوى أن اتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكنفه بعض الصعوبات، يمكن إجمالها في أنه معيار مرن وفضفاض، فضلا عن أن معيار حصول النشاط أدعى إلى تيسير عملية الإثبات وجمع أدلة الجريمة وأن المحكمة التي لها ولاية نظر الدعوى تكون قريبة من مسرح الجريمة، ناهيك أن الحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة[368].

تثير هذه القاعدة بعض الصعوبات عند التطبيق، فبالنسبة للجرائم الآنية (الوقتية)، لا صعوبة في الأمر لأنها ترتكب وتتم في لحظة واحدة، ولذلك تعتبر من اختصاص المحكمة التي وقع الفعل في دائرتها، أما بالنسبة للجرائم المستمرة والتي تظل قائمة ما بقي التدخل الإرادي من جانب الفاعل كجريمة حبس الأشخاص بغير حق أو إخفاء الأشياء المتحصلة من جريمة، يتحدد الإختصاص المكاني بالنسبة لهذه الجريمة بأي مكان قامت فيه حالة الاستمرار أما الجرائم الشبيهة بالجرائم المستمرة، بالنظر إلى ما يداخلها من عنصر زمني، ومثالها الاعتياد، والجرائم المتتابعة وجرائم الشروع حيث يعتبر مكانا للجريمة، كل محل يقع فيه فعل من أفعال الاعتياد أو التتابع، أو البدء في التنفيذ.

يقصد بمكان إقامة المتهم، المحل الذي يوجد فيه محل إقامته الفعلي أو الحكمي، وموطن الإقامة الفعلي، هو المكان الذي يقيم فيه المتهم ويسكنه، أما محل الإقامة الحكمي، فهو المكان القانوني الذي يقيم فيه الشخص عادة أو يتواجد به، أو تعرف به سيرته وشؤونه.

---

[368]– **موسى مسعود أرحومة**، المرجع السابق، ص15

أ مكان إلقاء القبض على المتهم، فهو غير المكان الذي يتم توقيفه(أو حبسه)، الحق أن مكان التوقيف، يعد بمثابة مكان حكمي للمتهم لكن الأمر لن تغدو له أهمية قانونية طالما إن القانون يسوي بين مكان الإقامة ومكان إلقاء القبض، ومكان ارتكاب الجريمة، في تحديد الإختصاص المكاني.

يمثل السلوك الإجرامي والنتيجة الإجرامية شطري الجريمة في إطار الجرائم المرتكبة عبر الإنترنت، ومن ثم فإن سلطات ومحاكم مكان النشاط الإجرامي، ومكان النتيجة تكون مختصة، وعلى ذلك فإذا تم بث الفيروس المعلوماتي(السلوك الإجرامي) في مكان، وتحققت النتيجة(تدمير المعلومات) في مكان آخر وألقي القبض على الجاني (أو المتهم) في مكان ثالث، فإن الإختصاص ينعقد لمحاكم إحدى هذه الأماكن[369].

ينتقد بعض الفقه فكرة المساواة بين هذه المحاكم، أو يجب أن ينظر إلى اختصاص محل ارتكاب الجريمة، كاختصاص رئيسي يقدم على غيره ويتبعه اختصاص محل الإقامة، ثم اختصاص مكان إلقاء القبض على المتهم.

2- معيار القانون الأكثر ملائمة

يرى أصحاب هذا الاتجاه، بأنه نظرا للطبيعة الخاصة لجرائم المعلوماتية والأضرار الناجمة عنها التي تمتد ليشمل أكثر من دولة واحدة، وأحيانا قد تتفاوت نسبة الضرر بين دولة وأخرى إلى القول بأنه يجب التوسع في تفسير قاعدة اختصاص محكمة وقوع الفعل (حصول الضرر)، ليجعل الإختصاص لمحكمة الدولة الأكثر تعرضا للضرر بشكل فعلي، مع التركيز على مبدأ التخلي أو التنازل عن الإختصاص بخلاف ذلك، وإن جعل الإختصاص لقانون دولة ما لمجرد إمكانية الوصول إلى المعلومة من هذه الدولة أو تلك، أصبح أمرا غير كافي من الناحية القانونية، لإعلان اختصاص هذه الدولة أو تلك.

من التطبيقات القضائية لذلك ما أعلنته إحدى محاكم ولاية نيويورك بعدم اختصاصاتها في قضية تزوير ماركات تجارية، أقدم عليها موقع ويب أحد وادي الجاز

[369]- **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم لكمبيوتر والإنترنت، المرجع السابق، ص51_52

في ولاية ميسوري، وعللت المحكمة قرارها بأن صلاحيتها لا تنشأ منه من داخل هذه الولاية، بل تنشأ فقط إذا ألحق هذا الموقع ضررا فعليا ضمن نطاقها[370].

بني هذا المعيار على الأخذ بعين الاعتبار نقطة الاتصال المميزة والسلطة الفعلية، أي باختصاص قضاء الدولة التي قانونها هو الأكثر تعرضا للانتهاك بسبب الفعل الجرمي، ومن أمثلة ذلك ما أصدرته إحدى المحاكم الأمريكية، التي أعتبت فيه أنه لا يمكن الارتكاز على مجرد النفاذ، أو الاتصال بهذا الموقع، أو المورد انطلاقا من الأراضي الأمريكية، حيث قضت باختصاص قضاء الدولة من منطلق وقوع الضرر الفعلي لا الاحتمالي[371].

3- معيار الضرر المرتقب

صاحب ظهور شبكة الإنترنت وجود عالم افتراضي، حيث تسري فيه مختلف المواد المعلوماتية دون إمكانية تحديد وجهتها، وهذا العالم الافتراضي لا يخضع لأي سلطة إقليمية، وبالتالي ترتب على هذه الحالة أن الضرر الذي تسببه الجريمة المرتكبة عبر الإنترنت يمكن أن يحدث في أي دولة تكون متصلة بالإنترنت، وهذا هو معيار الضرر المرتقب أو الافتراضي.

قدم المجلس الأوروبي العدلي تفسيرا خاصا بشأن مفهوم قاعدة اختصاص محل وقوع أو حدوث الفعل الضار، وذلك بالتأكيد على حق المتضرر، باللجوء حسب خياره إلى محكمة محل ارتكاب الفعل، أو إلى محل وقوع الضرر، ولكن مع إضافة قيد هام، أو أساسي في حالة لجوء المتضرر إلى محكمة محل وقوع الضرر، يقضي بحجب اختصاص هذه المحكمة، إذا أثبت المدعي عليه، أنه لم يكن قادرا على الارتقاب بصورة معقولة، وإن الفعل أو الامتناع كان من شأنه إحداث أو إنتاج ضرر مماثل في دولته.[372]

---

[370]- **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص523

[371]- **فريد منعم جبور**، المرجع السابق، ص207

[372]- **غازي عبد الرحمن هيان الرشيد**، المرجع السابق، ص524.

ورد في حيثيات هذا القرار أن المعلومات المنشورة في شبكة الإنترنت يمكن معاينتها من قبل جميع الدول الموصولة بها، ومن دون أن تكون موجهة بالضرورة محددة، لكن طبيعة هذه الوسيلة الإعلامية الجديدة لا يجب أن ينتج عنها تطبيق لجميع القوانين الموجودة بل يجب أن نطبق معيار (الارتقاب)، على المسؤول عن المعلومات الضارة فيها، وهذا المعيار لا يمكن إيجاده إلا من خلال إيجاد صلة أو علاقة للقانون المختص مع مبدأ موضوعي، وذلك بمعزل عن تذرع كل دولة باختصاصها المحتمل.

وأول المعالم الموضوعية في الاختصاص هي محل تمركز الموقع الذي نشرت الأقوال أو المعلومات بواسطته، وهو أكيد ويمكن التحكم بخلاف مكان تلقيها الذي يبقى احتماليا، وقد وجد هذا المعيار طريقة إلى التطبيق في بعض الدول، ومنها فرنسا حيث أصدرت محكمة استئناف باريس في عام 1999، قرارا أعتبر صراحة أن الطبيعة الكونية الخاصة لشبكة الإنترنت، لا يجب أن تؤدي إلى تطبيق محتمل لجميع القوانين الموجودة، بل إلى تطبيق القانون ذي الصلة مع مبدأ موضوعي، هو ارتقاب المسؤول للمحتوى الضار الذي ينشره[373].

[373]– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم لكمبيوتر والإنترنت، المرجع السابق ، ص52

خاتمة:

يتجلى لنا من خلال دراستنا للجريمة المرتكبة عبر الإنترنت أنها من أكثر الجرائم التي عرفها العالم الحديث خطورة، وذلك لما 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 الإنترنت، فإننا بذلك قد تناولنا مشكلة من مشكلات التي أفرزتها ثورة الاتصالات، 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 وعلمية معقدة.

غيرت الجريمة المرتكبة عبر الإنترنت النظرة التقليدية التي كان ينظر بها إلى الجريمة على العموم، فهذا النوع من الإجرام ظهر معه مفهوم جديد لهذه الظاهرة لم يكن يعرفه القانون من قبل، فإذا كانت الجريمة التقليدية قد حضيت بمختلف الأطر القانونية من أجل تحديد مفهومها وطبيعتها، فإن الجريمة المرتكبة عبر الإنترنت لم تنل هذا القدر من التقنين، حيث أن هذه الجريمة اتسمت بخصوصية ميزتها عن الجرائم التقليدية.

تجلت أول خصوصية تميزت بها 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 اعتبار ضرورة معرفة المجرم بمختلف الطرق التي يتم ارتكاب الجريمة من خلالها أساس لتعريفها، في حين ذهب جانب آخر إلى تعريفها على أساس الوسيلة المرتكبة بواسطتها، غير أن هذه التعاريف كلها لم تف بالغرض نظرا لعدم إلمامها بمختلف جوانب لجريمة، لهذا ذهب فريق من الفقه إلى دمج كل هذه التعاريف من أجل الوصول إلى تعريف مانع لها، وفي نظرنا يعتبر هذا الرأي الأخير الأقرب إلى الإحاطة بمقتضيات تحديد مفهوم الجريمة.

تعتبر كذلك الخصائص التي انفردت بها الجريمة المرتكبة عبر الإنترنت، من بين العوامل التي مهدت لها التميز بالخصوصية عن الجريمة التقليدية، حيث تعلقت هذه الخصائص بجميع جوانب الجريمة، مثل طابعها العابر للحدود، وارتكابها في العالم الافتراضي وانعدام الآثار التقليدية لها، بالإضافة إلى ضعف مستوى القائمين على مكافحتها بالنظر إلى التطور المتسارع في ارتكابها، فإن هذه الخصائص تكرس الاختلاف الجوهري عن الخصائص العادية للجرائم التقليدية، وكان لها الدور الأكبر في إبراز هذا النشاط الإجرامي كظاهرة إجرامية مستحدثة.

أضافت السمات التي يتميز بها المجرم الذي يرتكب جرائمه عبر الإنترنت الكثير من التميز للجريمة المرتكبة عبر الإنترنت، حيث يعتبر هذا المجرم من الأشخاص الذين يتمتعون بنسبة عالية من المهارة والمعرفة والذكاء، فإذا كان المجرم التقليدي يسعى إلى ارتكاب جرائمه في الغالب عن طريق استعمال العنف، فإن مجرم الإنترنت يعتبر مجرم غير عنيف، بل يرتكب جرائمه في هدوء دون أن يلفت النظر إلى الأفعال التي يقوم بها، ولقد ساهمت كثرة القطاعات المستخدمة للإنترنت من انتشار هذا النوع من الإجرام وأعطت فرصا للمجرمين من أجل الاعتداء 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 أكثر من قطاع عبر مختلف أنحاء العالم وذلك بمجرد الضغط على زر واحد.

تجلت خصوصية الجرائم المرتكبة عبر الإنترنت أكثر في عدم إمكانية تطبيق أحكام الجرائم التقليدية عليها، وذلك نظرا للطابع المستحدث لهذه الجريمة، فإذا كان مثلا تصنيف الجرائم التقليدية لم يتميز بالصعوبة، فإن تصنيف الجرائم المرتكبة عبر الإنترنت اتسم بالتشعب وذلك راجع لعدم إمكانية حصر هذه الجرائم في قالب واحد الأمر الذي أدى إلى تعدد التصنيفات والأسس التي تبنى عليها.

لم تتوقف إشكالات تطبيق أحكام الجرائم التقليدية على الجرائم المرتكبة عبر الإنترنت عند هذا الحد، بل تعدته إلى تحديد أركان هذه الجريمة، فإذا كان تحديد أركان الجريمة التقليدية واضحا والمتمثلة في الركن المادي والمعنوي والركن الشرعي، فإن تطبيق

هذا التحديد على الجرائم 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 للجريمة المرتكبة عبر الإنترنت.

ظهرت كذلك خصوصية الجريمة المرتكبة عبر الإنترنت أكثر من خلال النصوص القانونية المطبقة عليها، فبروز هذه الظاهرة الإجرامية المستحدثة قد أظهر أن هناك 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 والعقاب أصبح غير مواكب لهذه الجريمة، لذلك فقد حاولت التشريعات العقابية المختلفة أن تواجه هذه الظاهرة الإجرامية الجديدة لمواجهتها، وقام البعض الآخر بإجراء تعديلات على النصوص القائمة لمواكبة هذه الجرائم المتطورة، 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 تتميز بها الجريمة المرتكبة عبر الإنترنت مختلف الدول والهيئات والمنظمات الدولية والإقليمية تدرك مدى خطورة هذه الظاهرة الإجرامية ومدى التحديات التي تفرضها عليها، مما أدى بها إلى المسارعة من أجل وضعها في إطار قانوني يمكن من خلاله وضع طرق ناجعة وفعالة لمكافحتها، ولقد تمثلت الجهود الدولية في تلك التي تبذلها منظمة الأمم المتحدة بمختلف الهيئات التابعة لها، وذلك بعقد المؤتمرات وإبرام المعاهدات بين الدول الأعضاء فيها، والتحسين من مخاطر هذه الظاهرة بالإضافة إلى إرشاد الدول المتخلفة عن الركب التكنولوجي لكيفية سن قوانينها الداخلية في هذا المجال، دون إغفال الجهود التي تبذلها المنظمة العالمية للملكية الفكرية التي دأبت على وضع المناهج لحماية مختلف المنتجات الفكرية عبر العالم وكذلك جهود مجموعة الثمانية.

أما فيما يخص الجهود الإقليمية فتمثلت في جهود الاتحاد الأوربي الذي يعتبر الإطار الأنجع لمكافحة الجريمة المرتكبة عبر الإنترنت خاصة بعد إبرام اتفاقية بودابست

سنة 2001 والتي وضعت الأسس السليمة التي ينبغي على دول الاتحاد الأوربي الأخذ بها في هذا المجال، بالإضافة إلى جهود الاتحاد الأوربي هناك جهود تبذل على المستوى العربي، فبالرغم من قلتها إلاّ أنها تبقى محاولات رائدة في الوطن العربي، خاصة الجهود التي تبذل في إطار الجامعة العربية، في انتظار المزيد من الجهود للحد من هذه الظاهرة ولحماية مكتسبات العالم العربي.

واكب المشرع الجزائري ولو بقدر قليل الحركية التشريعية التي فرضت نفسها عالميا، خاصة مع دخول الإنترنت في مختلف مناحي حياة المواطن الجزائري، فبعد الفراغ التشريعي الذي كانت تعاني منه الجزائر في هذا المجال سعت لسده في بادئ الأمر بتعديل قانون العقوبات وذلك بالقانون رقم 04-15، غير محدودية هذا القانون دفع المشرع الجزائري إلى إصدار قانون خاص والمتمثل في القانون رقم 09-04 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 أن بالرغم 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 والسرعة في تطورها أدى بأغلب هذه المحاولات إلى الفشل والدليل على ذلك ما نسمعه عبر وسائل الإعلام المختلفة عن الجرائم الكثيرة التي مازالت ترتكب عبر الشبكة العالمية للإنترنت، حيث يعتبر اكتشاف واثبات الجريمة المرتكبة عبر الانترنت من أكثر الصعوبات التي تعترض سلطات إنفاذ القانون، ففي الغالب تكون هذه الجرائم مستترة، وكذلك الأمر بالنسبة لإثباتها في ظل الطابع اللامادي للجريمة، حيث افتقار هذه الجرائم للدليل المادي يجعل أمر إثباتها غاية في الصعوبة.

خاتمة:

تميزت شبكة الإنترنت بتعدي الحدود الوطنية، فهي شبكة عالمية الوجود، وبالتالي كل المعاملات التي تتم عبرها تتصف بهذه الصفة، وحتى الأفعال غير المشروعة التي ترتكب عبرها تكتسب هذه الصفة هي الأخرى، ففي ظل هذه الخصوصية انبثقت عدة إشكالات فيما يخص التعاون القضائي الدولي وتحديد قواعد الاختصاص، حيث أن التباين الموجود بين قوانين الدول المختلفة جعل من بعض الأفعال مجرمة في دولة وغير مجرمة في دولة أخرى، بالإضافة إلى تعدد المعايير واختلافها من دولة إلى أخرى فيما يخص تحديد القانون الواجب التطبيق والمحكمة المختصة الأمر 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 ألا وهي الإنترنت، حيث أن عالمية الشبكة وافتراضية المعاملات عبرها بالإضافة إلى عدم امتلاك أي جهة لهذه الشبكة ألقت بضلالها على الأفعال 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.

أولا: باللغة العربية:

I- الكتب:

1 – **أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار نشر، دون بلد النشر، 2005.

2 – **أحمد خليفة الملط**، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، ، 2006

3 - **أشرف توفيق شمس الدين**، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، طبعة خاصة لطلاب التعليم المفتوح بكلية لحقوق بجامعة بنها، 2009.

4 - **أمير فرج يوسف**، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، .2008.

5 - **بارش سليمان**، مبدأ الشرعية في قانون العقوبات الجزائري، دار الهدى، عين مليلة، الجزائر، 2006.

6 - **حسن طاهر داود**، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض ، 2000.

7 – **خثير مسعود**، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى، عين مليلة، الجزائر، 2010

8 – **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2010

9 – **سامي علي حامد عياد**، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007

10 – **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ، 2007

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

12 - **علي عدنان الفيل**، الإجرام الإلكتروني، الطبعة الأولى، منشورات زين الحقوقية، دمشق، 2011.

13 - **عمرو عيسى الفقي**، الجرائم المعلوماتية– جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، 2006

14 – **عبد الله بن عبد العزيز اليوسف**، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض ، 2004.

15 – **عبد الله سليمان**، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول(الجريمة)، ديوان المطبوعات الجامعية، الجزائر، 1995

16 – **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.

17 – **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، مصر،2009.

18 – **عبد الرحمن بن عبد الله السند**، الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات (الإنترنت)، الطبعة الأولى، دار الوراقين للنشر والتوزيع، بيروت، 2004.

19 – **فريد منعم جبور**، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الإلكترونية (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010.

20 – **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007.

21 – **محمد عبيد الكعبي**، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة،.دون سنة النشر.

22 – **محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004

23 – **مصطفى محمد موسى**، أساليب إجرامية بالتقنية الرقمية(ماهيتها، مكافحتها)، دار الكتب القانونية، مصر، 2005.

24 – ***مصطفى محمد موسى***، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009.

25 – **محمود أحمد عبابنة**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005.

26 – **محمد حماد مرهج الهيتي**، جرائم الحاسوب–ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان ، 2006.

27 – ــــــــــــــــــــــ، التكنولوجيا الحديثة وقانون الجنائي، دار الثقافة والتوزيع، عمان، 2004.

28 – **محمد محمد شتا**، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001.

29 – **محمد سيد سلطان**، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، 2012، متوفر على الموقع التالي: www.Nashiri.Net

30 – **محمد فتحي عيد**، الإجرام المعاصر، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض ، 1999.

31 – **محمد أمين أحمد الشوابكة،** جرائم الحاسوب والإنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004

32 – **.محمد دباس الحميد، ماركو إبراهيم نينو،** حماية أنظمة المعلومات، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2007.

33 – **محمد حماد مرهج الهيتي،** التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، 2004

34 – **منصور رحماني،** الوجيز في القانون الجنائي العام، دار العلوم للنشر والتوزيع، عنابة، 2006

35 – **محمد علي أحمد الكواري،** مسرح الجريمة ودوره في كشف غموض الجريمة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007

36 – **محمد فاروق عبد الحميد كامل،** القواعد الفنية الشرطية للتحقيق والبحث الجنائي، الطبعة الأولى،أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1999.

37 – **محمد واصل، حسين بن علي الهلالي،** الخبرة الفنية أمام القضاء دراسة مقارنة، المكتب الفني، مسقط، سلطنة عمان، 2004

38 – **محمد فتحي عيد،** الإنترنت ودوره في انتشار المخدرات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003

39 – **طارق إبراهيم الدسوقي عطية،** الأمن المعلوماتي، (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجيدة للنشر، 2009

40 – **محمد دباس الحميد، ماركو إبراهيم نينو،** حماية أنظمة المعلومات، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2007.

41 – صنفات الفنية ودور الشرطة والقانون دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007.

42 – **نايف بن محمد المرواني**، جريمة السرقة (دراسة نفسية اجتماعية)، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.

43 – **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2008

II- الرسائل والمذكرات الجامعية:

أولا: الرسائل الجامعية

1 – **تركي بن عبد الرحمن المويشر**، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة الأمنية، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية،الرياض، 2009

2 – **عمر بن محمد العتيبي**، الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة مقدمة استكمالاً لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، الرياض، 2010

3 – **غازي عبد الرحمن هيان الرشيد**، ، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004

4 – **مباركي دليلة** ، غسيل لأموال، أطروحة مقدمة لنيل شهادة الدكتوراه علوم، تخصص قانون جنائي، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم القانونية، باتنة، 2008

ثانيا: المذكرات الجامعية

1 – **أحمد عيد بن حرب العطوي**، التفتيش ودوره في الإثبات الجنائي، مشروع مقدم كمطلب تكميلي ضمن متطلبات برنامج التخصص المتقدم في مكافحة الجريمة "القسم الخاص" لحصول على درجة الماجستير في مكافحة الجريمة، المركز العالي للدراسات الأمنية، المعهد العالي للعلوم الأمنية، قسم العلوم الشرطية، الرياض، 1987

2 – **أحمد بن محمد اليماني**، الحماية الجنائية للبريد الإلكتروني دراسة تأصيلية مقارنة، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في قسم العدالة الجنائية، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات، قسم العدالة الجنائية، الرياض، 2010

3 – **بوعمرة آسيا**، النظام القانوني لقواعد البيانات، مذكرة لنيل شهادة الماجستير في القانون، فرع الملكية الفكرية، كلية الحقوق، جامعة الجزائر، 2005.

4 – **خالد بن عبد الله بن معيض العبيدي**، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2009

5 – **شبراك حياة**، حقوق صاحب براءة الاختراع في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون الأعمال، كلية الحقوق والعلوم الإدارية، الجزائر، دون سنة المناقشة.

6 – **عبد الرحمن محمد بحر**، معوقات التحقيق في جرائم الإنترنت دراسة مسحية على ضباط الشرطة في البحرين، رسالة مقدمة إلى معهد الدراسات العليا استكمالاً لمتطلبات الحصول على درجة الماجستير في

العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، معهد الدراسات العليا قسم العلوم الشرطية، الرياض، .1999

7 – **عبد الرحمن عبد العزيز الشنيفي**، مدى استفادة الأجهزة الأمنية من خدمات شبكة الإنترنت دراسة استطلاعية على إدارتي الشرطة والمرور بمدينة الرياض، دراسة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العلوم الإدارية، كلية الدراسات العليا، قسم العلوم الإدارية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003.

8 – **عبد الرحمن جميل محمود حسين**، الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة، رسالة قدمت استكمالاً لمتطلبات درجة الماجستير في القانون الخاص بكلية الدراسات العليا في جامعة النجاح الوطنية، فلسطين، 2008

9 – **عبد الله ذيب عبد الله محمود**، حماية المستهلك في التعاقد الإلكتروني دراسة مقارنة، رسالة قدمت استكمالا لمتطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، سنة 2009

10 – **عبد الله بن عبد العزيز بن عبد الله الخثعمي**، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011

11 – **قارة آمال**، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2002

12 – **قرايش سامية**، التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية، مذكرة لنيل درجة الماجستير في القانون فرع تحولات الدولة، كلية الحقوق، جامعة مولود معمري، تيزي وزو، دون تاريخ مناقشة

13 – **محمد بن نصير محمد السرحاني**، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت–دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، تخصص القيادة الأمنية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية، الرياض، 2004

14 – **محمد بن عبد الله بن علي المنشاوي**، جرائم الإنترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003

15 – **منصور بن صالح السلمي**،المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2010

16 – **واقد يوسف**، النظام القانوني للدفع الإلكتروني، مذكرة لنيل درجة الماجستير، تخصص قانون التعاون لدولي، جامعة مولود معمري، كلية الحقوق، تيزي وزو، 2011

III- المقالات:

1 – **الصديق محمد الأمين الضرير**،« **بطاقات الائتمان**»، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، أيام 10–12 ماي 2003 المجلد الثاني، ص ص 637–658.

2 – **أسامة أبو كحلوش علي، «جرائم الحاسوب وأساليب مواجهتها»**، مجلة الشرطة، تصدر عن المديرية العامة للأمن الوطني، العدد 84، جويلية 2007، ص ص51–51

3 – **أحمد صلاح الدين إبراهيم،« ومضات في جرائم الإنترنت- الأنماط، المسؤولية الجنائية، إستراتيجية المواجهة »**، ص ص1–62، مقال متوفر على الموقع التالي: http://www.eastlaws.com

4 – **أحمد شوقي أبو خطوة، «جريمة الاحتيال ماهيتها وخصائصها»**، دورة عمل حول جرائم الاحتيال والإجرام المنظم، جامعة نايف العربية للعلوم الأمنية، أيام 18–20 جوان 2007،الرياض، الطبعة الأولى، 2008، ص ص 7–50.

5 – **إيهاب ماهر السنباطي، « الجرائم الإلكترونية (الجرائم السيبيرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد »**، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، يونيو 2007، ص ص 15–36.

6 – **احمد آيت الطالب، «العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة»**، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية، كلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية، 9_2006/4/13، ص ص 2–27.

7 – **إلياس بن سمير الهاجري، «أمن المعلومات على شبكة الإنترنت»**، ندوة حقوق الملكية الفكرية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص ص135–149.

8 – **أخام بن عودة زواوي مليكة، «تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية»**، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 27–30 أكتوبر 2009، ص ص 1–25.

9 – الأزرق بن عبد الله، أحمد عمراني، «**نظام المعلوماتية في القانون الجزائري واقع وآفاق**»، المؤتمر السادس لجمعية المكتبات ولمعلومات السعودية، البيئة المعلوماتية الآمنة المفاهيم والتشريعات والتطبيقات، الرياض، 6_7 أفريل 2010، ص ص 1–25.

10 – **إلياس بن سمير الهاجري**، «**جرائم الإنترنت**»، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية المنعقدة بكلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية، 9–13 أفريل 2006، ص ص55–60

11 – **الأنتربول، الجرائم ضد الأطفال**، مقال متوفر على الموقع التالي http://www.interpol.int

12 – **بسام أحمد الزلمي**، « **دور النقود الإلكترونية في عمليات غسيل الأموال** »، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، 2010، ص ص 543–562.

13 – **براء منذر كمال عبد اللطيف، ناظر أحمد منديل، التعاون القضائي الدولي في مواجهة جرائم الإنترنت**، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة، كلية القانون،جامعة تكريت، العراق، 2009، ص ص 1–22.

14 - **جون فرنسوا هنروت**،« **أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي**»، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة لمغربية، 19–20 يونيو 2007، ص ص 95– 111.

15 - **حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت**، ص ص 1–61، مقال متوفر على الموقع التالي: http://www.minshawi.com

16 – **حسام الدين كامل الأهواني**، « **حماية حقوق الملكية الفكرية في مجال الإنترنت** »، ص ص1–16، مقال متوفر على الموقع التالي: http://www.osamabahar.com

17 – **حسين بن سعيد الغافري**، «التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت»، ص ص 1–27، مقال متوفر على الموقع التالي: http://www.eastlaws.com

18 – **خالد محيي الدين أحمد**، « **الجرائم المتعلقة بالرغبة الإشباعية باستخدام الكمبيوتر** »، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، أيام 19–20 يونيو 2007، ص ص37–39.

19 – **دشن بن محمد القحطاني**،« الاستخدامات غير المشروعة لتقنية المعلومات عبر الإنترنت»،ص ص 1–33، مقال متوفر على الموقع التالي: http://www.minshawi.com

20 – **دويب حسين صابر**، « **القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع**»، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، الرياض، أيام 6 و7 أفريل 2010، ص ص 1–22.

21 – **ذياب موسى البداينة**،« **دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي** »، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية، المنعقدة بكلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية، أيام 9–13 أفريل 2006، ص ص 1–29.

22 – **ذياب البداينة**،« **سوء معاملة الأطفال- الضحية المنسية** »، مجلة الفكر الشرطي، المجلد 11، العدد 11، أكاديمية نايف العربية للعلوم الأمنية، الرياض، دون سنة نشر، ص ص 167–219.

23 – **سيناء عبد الله محسن، «المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية»**، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، الدار البيضاء، المملكة المغربية، 10-20 يونيو 2007، ص ص 51-60.

24 – **سمير إبراهيم حسن، « الثورة المعلوماتية عواقبها وآفاقها »**، مجلة جامعة دمشق، المجلد 18، العدد الأول، 2002، ص ص 207-224.

25 – **شائف علي محمد الشيباني**، الإنابة القضائية الدولية في القانون اليمني دراسة مقارنة، مقال موجه لدائرة التدريب والتأهيل، النيابة العامة، الجمهورية اليمنية، 2006، ص ص 1-59.

26 – **صالح بن سعد الصالح، مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي**، الدورة التدريبية مكافحة الجرائم الاقتصادية، كلية التدريب، قسم البرامج لتدريبية، الرياض، 10-2007/3/14، ص ص 2-28

27 – **صالح بن سعد الصالح، « مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي»**، الدورة التدريبية مكافحة الجرائم الاقتصادية، جامعة نايف العربية للعلوم الأمنية، كلية التدريب، قسم البرامج التدريبية، الرياض، 10-14 مارس 2007، ص ص1-28

28 – **صالح بن محمد المسند، عبد الرحمن بن راشد المهيني، « جرائم الحاسب للآلي الخطر الحقيقي في عصر المعلومات»**، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 29، الرياض، دون سنة نشر، ص ص 137-207

29 – **صالحة العمري، « جريمة غسيل الأموال وطرق مكافحتها »**، مجلة الاجتهاد القضائي، العدد الخامس، مخبر أثر الاجتهاد القضائي على

حركة التشريع، جامعة محمد خيضر، بسكرة، دون سنة نشر، ص ص178-205.

30 - **طارق محمد الجملي، «الدليل الرقمي في مجال الإثبات الجنائي»**، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28_2009/10/29، ص ص 1-33.

31 - **عمر الشيخ الأصم،«البطاقات الائتمانية المستخدمة الأكثر انتشارا في البلاد العربية»**، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص ص 7-32.

32 - **عارف خليل أبو عيد، « جرائم الإنترنت-دراسة مقارنة »**، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد5، العدد3، ص ص 71-113

33 - **عمر الفاروق الحسيني« لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات »**، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 1-3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول، الطبعة الثالثة، 2004، ص ص 329-354.

34 - **عبد الكريم خالد الشامي، « جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني»**، ص ص 1-28، مقال متوفر على موقع بوابة فلسطين القانونية، http://www.pal-ip.org

35 - **علوي مصطفى، «الضحية المنسية أمام لغة الكبار»**، مجلة الشرطة، تصدر عن المديرية العامة للأمن الوطني، العدد 87، جوان 2008، ص ص 30-31.

36 - **عبد المحسن بدوي محمد أحمد، «إستراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيري»**، الندوة العلمية حول الإعلام والأمن، مركز الدراسات والبحوث، قسم الندوات

واللقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، الخرطوم 11-13 سنة 2005، ص ص 1-32.

37 - **عبد الرزاق السندالي، « التشريع المغربي في الجرائم المعلوماتية »**، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، 19_20 يونيو 2007، ص ص 67-76.

38 - **عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، «الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة مقارنة»**، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، 12_14 نوفمبر 2007، الرياض ص ص 1-45،.

39 - **عواطف محمد عثمان عبد الحليم، « جرائم المعلوماتية، تعريفها، صورها، جهود مكافحتها دوليا، إقليميا، ووطنيا»**، مجلة العدل، العدد الرابع والعشرون، السنة العاشرة، دون سنة وبلد نشر، ص ص57-77.

40 - **عمر مشهور حديثة حجازي، المبادئ الأساسية لقانون حق المؤلف، ندوة حق المؤلف في الأردن: بين النظرية والتطبيق**، كلية الحقوق، الجامعة الأردنية، 12 كانون الثاني 2004، ص ص 1-14.

41 - **عبد القادر دوحة، محمد بن حاج الطاهر، «مدى مواكبة المشرع الجزائري لتطور الجريمة الإلكترونية»**، الملتقى الوطني الأول_النظام القانوني لمجتمع الإلكتروني، المركز الجامعي خميس مليانة، مهد العلوم القانونية والإدارية، 09_10_11 مارس 2008، ص ص 1-17.

42 - **علي محمود علي حمودة، « الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي»**، ص ص 1-74، مقال متوفر على الموقع التالي: http://www.arablawinfo;com

43 – **عبد الجبار الحنيص، (الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي- دراسة مقارنة-)**، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27، العدد الأول، 2011،ص ص 185–211

44 – **عارف خليل أبو عيد، "جرائم الإنترنت (دراسة مقارنة)"**، مجلة الشارقة للعلوم الشرعية والقانونية، المجلد 5، العدد 3، الإمارات العربية المتحدة، أكتوبر 2008، ص ص71–113.

45 – **عباس أبو شامة، « التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، ونشاطها في الدول العربية»**، الندوة العلمية الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، أيام 28–30جوان 1999، ص ص 9–42.

46 – **غنام محمد غنام، « عدم ملائمة الواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر »**، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1–3.

47 – **فايز بن عبد الله الشهري، «ثقافة التطرف على شبكة الإنترنت الملامح والاتجاهات»**، الندوة العلمية استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 25_2010/10/27، ص ص 2–37.

48 - **فشار عطاء الله، «مواجهة الجريمة المعلوماتية في التشريع الجزائري»**، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص ص 1–42.

49 – **فايز بن عبد الله الشهري، « التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة (دراسة وصفية تأصيلية للظاهرة الإجرامية على**

شبكة الإنترنت)»، ص ص 1-28، مقال متوفر على الموقع التالي: http://www.osamabahar.com

50 - **كريستينا سكولمان، « عن جرائم الإنترنت: طبيعتها وخصائصها »**، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، أيام 19 و20 يونيو 2007، ص ص

51 - **كريستينا سكولمان، « الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية»**، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 يونيو 2007، المملكة المغربية،ص ص 119-127.

52 - **كريستينا سكولمان، «المعايير الدولية المتعلقة بجرائم الإنترنت (مجلس أوربا)»**، الندوة الإقليمية حول لجرائم المتصلة بالكمبيوتر، 19-20 يونيو 2007، المملكة المغربية، ص ص 61-66.

53 - **كريم كريمة، « حماية الحق في الخصوصية من التعدي في ظل مجتمع المعلومات »**، مجلة العلوم القانونية ولإدارية، كلية الحقوق، جامعة جيلالي اليابس، سيدي بلعباس، العدد الثاني، 2005، ص ص 129-159.

54 - **لوجاني نور الدين، «أساليب البحث والتحري الخاصة وإجراءاتها وفقا للقانون رقم 22/06 المؤرخ في 2006/12/20»**، يوم دراسي حول: علاقة النيابة العامة بالشرطة القضائية-احترام حقوق الإنسان ومكافحة الجريمة- يوم 12 ديسمبر 2007، بمقر أمن ولاية إيليزي، ص ص 2-21.

55 - **محمد صالح العادلي، «الجرائم المعلوماتية(ماهيتها وصورها)»**، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، 2-4 أفريل 2006، ص ص 1-14.

56 – **محمد عبد الرحيم سلطان العلماء، «جرائم الإنترنت والاحتساب عليها»**، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 1–3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، الطبعة الثالثة، 2004، ص ص 871–885.

57 – **موسى مسعود أرحومة، «الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية»**، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص ص 1–25

58 – **مها عبد المجيد صلاح، «استراتيجيات الاتصال في مواقع الجماعات المتطرفة على شبكة الإنترنت دراسة تحليلية»**، الندوة العلمية استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 25_2010/10/27، ص ص

59 – **مصطفى محمد موسى، التنظيمات الإرهابية وشبكة الإنترنت**، الندوة العلمية استشراف التهديدات الإرهابية، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 20_2007/8/22، ص ص 3–64.

60 – **محمد عبد السلام سلامة، « جرائم غسيل الأموال إلكترونيا في ظل النظام العالمي الجديد»**، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 10–12ماي 2003، المجلد الرابع، ص ص 1505–1528.

61 – **محمد محمد صالح الألفي، «أنماط جرائم الإنترنت»**، ص ص1–13، مقل متوفر على الموقع التالي: http://www.eastlaws.com

62 – **محمد عبد الرسول خياط، « عمليات تزوير البطاقات الائتمانية »**، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص ص 33–62.

63 - **محمد زيدان، محمد حمو،« متطلبات أمن المعلومات المصرفية في بيئة الإنترنت»**، المؤتمر السادس لجمعيات المكتبات والمعلومات السعودية، بيئة المعلومات الآمنة المفاهيم والتشريعات والتطبيقات، 6–7 أفريل 2010، الرياض، ص ص 1–18. 1430

64 – **محمد عادل ريان، «جرائم الحاسب الآلي وأمن البيانات»**، متوفر على الموقع التالي www.anaharonline.com

65 - **_____المخاطر الأمنية للإنترنت**، مقال متوفر على الموقع التالي www.minchawi.com

66 – **محمد أبو العلا عقيدة« التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية»**، ص ص1–16، مقال متوفر على الموقع التالي: http://arblawinfo.com

67 – **محمد الأمين البشري، «التحقيق في جرائم الحاسب الآلي»**، مؤتمر القانون و الكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1_3 مايو 2000، المجلد الثالث، ص ص 1033–1082.

68 - **ناصر بن محمد البقمي، أثر التحول إلى مجتمع معلوماتي على الأمن الفكري**، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن الفكري بجامعة الملك سعود، المملكة السعودية، 22–25 جمادى الأول، ص ص 1–56.

69 – **نعيم دهمش، ظاهر شاهر القشي، «مخاطر العمليات المصرفية التي تتم من خلال القنوات الالكترونية»** ،مجلة البنوك، العدد الثاني، المجلد الثالث والعشرون، آذار 2004، الأردن، ص ص 1–4.

70 - **هشام محمد فريد رستم، «أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي»**، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 1-3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004، ص ص 401-506.

71 - **هشام مفيد محمود،« الآثار السلبية الناجمة عن تزوير البطاقات الائتمانية»**، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص ص 105-124.

72 - **وليد عاكوم، «مفهوم وظاهرة الإجرام المعلوماتي»**، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 1-3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول، الطبعة الثالثة، 2004، ص ص 11-21.

73 - **يونس عرب، جرائم الكمبيوتر والإنترنت (إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات)**، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10-12 فيفري، 2002، ص ص 1-49.

74 - **يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها**، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، 2-4 أفريل 2006، ص ص 1-81.

75 - .**يونس عرب، «قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان»**، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية،

المنعقدة بمسقط، سلطنة عمان، 2-4 أفريل 2006، ص ص 1-55.

76 - **يونس عرب، دور الخصوصية في تشجيع الاندماج بالمجتمع الرقمي**، ندوة أخلاق المعلومات، نادي المعلومات العربي، عمان، الأردن، 16-17 أكتوبر 2002، ص ص 1-67.

IV-النصوص القانونية:

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

2- أمر رقم 05/03 مؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 44 صادر 2003/07/23.

3- أمر رقم 06/03 مؤرخ في 2003/07/19 المتعلق بالعلامات، الجريدة الرسمية عدد 44 صادر 2003/07/23.

4- قانون رقم 07/03 مؤرخ في 2003/07/19 يتعلق ببراءات الاختراع، الجريدة الرسمية عدد 44 صادر 2003/07/23

5- قانون رقم 15/04 مؤرخ في 2004/11/10 المتضمن تعديل قانون العقوبات، الجريدة الرسمية رقم 71 صادر 2004/11/10

6- قانون رقم 22/06 مؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية عدد 84 صادر 2006.

7- قانون رقم 04/09 مؤرخ في 2009/2/5 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 صادر 2009.

VI – وثائق الأمم المتحدة:

1 – –اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم (55/63)، الصادرة عن هيئة الأمم المتحدة، الجلسة العامة81، ديسمبر 2000

2 – مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها لجرائم الحاسوبية، المنعقد بالبرازيل 12_19 أفريل 2010، رقم9/ A /conf.213

3 – –اجتماع فريق الخبراء المعني بالجريمة السيبرانية، مشروع المواضيع المطروحة لنظر في إطار دراسة شاملة بشأن الجريمة السيبرانية وتدابير التصدي لها، فيينا 17_21 يناير 2011، رقم UNODC/ccpcj/eg 4/2011/2

4 – –اللجنة الاقتصادية والاجتماعية لغربي آسيا(الإسكوا)، ورشة عمل حول التشريعات السيبرانية تطبيقها في منطقة الإسكوا، ببيروت 15_16 ديسمبر 2008، المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة، رقم 1/ E /ESCWA/ICTD/2009

5 – –مؤتمر هيئة الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة عبر الوطنية، المنعقد بفيينا في 18_22 أكتوبر 2010، رقم: CTOC/cop /2010/crp5

6 – –أنشطة مكتب الأمم المتحدة المعني بالمخدرات والجريمة في مجال التصدي للأشكال المستجدة من الجريمة، مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، فيينا، 18_22 أكتوبر 2010، رقم: CTOC/cop /2010/3

7 – اتفاقية حقوق الطفل، النظر في التقارير المقدمة من الدول بموجب الفقرة 1من المادة 12 من البروتوكول الاختياري لاتفاقية حقوق الطفل

المتعلق ببيع وبغاء الأطفال في المواد الإباحية، لجنة حقوق الطفل، الدورة السابعة والخمسون، 30 ماي_17 جويلية 2011، الأمم المتحدة، رقم: CRC /c/opsc/egy/co/1

V- وثائق الاتحاد الدولي للاتصالات

دليل للبلدان النامية: فهم الجريمة السيبرانية، شعبة تطبيقات تكنولوجيا المعلومات والاتصالات ولأمن السيبراني، دائرة السياسات والاستراتيجيات، قطاع تنمية الاتصالات، الصادر عن الاتحاد الدولي للاتصالات، أفريل 2009، ص94.

ثانيا باللغة الفرنسية:

I- OUVRAGES :

1. **CAPRIOLI Eric A,** Règlement des litiges internationaux et droit applicable dans le commerce électronique, , Litec, Paris, 2002.
2. **EL AZZOUZI Ali,** La cybercriminalité au Maroc, Edition Bishops solution, Casablanca, 2010.
3. **FAUCHOUX Vincent- DEPREZ Pierre**, Le droit de l'Internet (loi, contrat et usages), édition Litec, Paris, 2008.
4. **KURBALIJA Jovan, GELBSTEIN Eduardo,** Gouvernance de l'internet – enjeux, acteurs et fractures, publié par diplofoundation et global knowledge partnership, Suisse, 2005.
5. **SEDALIAN Valérie**, Droit de l'internet- Réglementation- Responsabilités- contrat, Edition Net Press, Paris, 1997.

II- MEMOIRES :

1. **DEBRAY Stéphane**, Internet face aux substances illicites : complice de la cybercriminalité ou outil de prévention ?, DESS média électronique & Internet, Université de Paris 8, 2002-2003.
2. **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.

III- ARTICLES :

1. **AGSOUS Naima, « *cybercriminalité : les réseaux informatiques* »,** Revue de la gendarmerie, N° 29, novembre, 2008, p p 19-22.
2. **CHERNAOUTI-HELI Slange**, « Comment lutter contre la cybercriminalité ? » ; revue la Science, n° 391, Mais 2010, p p 24-27.
3. **KElCi Sevgi** « ***Vol, fraude et autres infractions semblables et Internet* »,** Revu Lex Electronica, vol.12 n°1 ,2007, p p 01-22, disponible su le site : http://www.lex-electronica.org/articles/v12-1/kelci.pdf
4. **Les Officiers de l'équipe de lutte contre la cybercriminalité de la Gendarmerie Nationale**, « ***Criminologie : Une menace émergente*** », Revue de la gendarmerie, N° 15, novembre, 2005, p p 10-13.
5. **MASCALA Corinne**, « ***criminalité et contrat électronique*** », IN : Le contrat électronique, Travaux de l'association CAPITANT Henri, journées national, Paris, 2000, p p 115-119.
6. **CHAWKI Mohamed,** « *Essai sur la notion de cybercriminalité* », juillet 2006, p7, Disponible sur le site : http://www.iehei.org

VI- SITES INTERNET :

1. http://www.eastlaws.com
2. http://www.interpol.int
3. http://www.minshawi.com
4. http://www.osamabahar.com
5. ://www.osamabahar.com
6. http://www.pal-ip.org

فهرس الموضوعات

تعددت العمليات الإلكترونية كأثر مترتب على الثورة المعلوماتية وسهولة وتقديم الخدمات العامة عن طريق الوسائل الإلكترونية، والتي تدور في فلك شبكة الإنترنت، إلا أن رواج العمليات الإلكترونية واكبها ظهور آثار سلبية مجسدة في الجرائم المستحدثة التي ترتكب عن طريق الوسائل التقنية الحديثة وهي ما يطلق عليها بالجرائم المرتكبة عبر الإنترنت.

يثير هذا الإجرام المعاصر الكثير من الإشكالات من نواحي عديدة أهمها صعوبة اكتشاف هذه الجرائم وإثباتها، ويعود ذلك إلى سهولة طمس معالمها ومحو آثارها قبل اكتشافها، إذ يستطيع المجرم الإلكتروني ارتكاب الجريمة عبر الإنترنت دون أن يترك وراءه أي أثر خارجي ملموس، خاصة أنه يتميز بذكاء ومهارات تقنية عالية وذو دراية تامة بمجال المعلومات وأنظمة برامج الحاسبات الآلية.

وأمام خطورة وخصوصيات هذه الجريمة المرتكبة عبر الإنترنت، كان لابد من تكاتف التشريعات الدولية والداخلية للدول من أجل محاولة ردعها وإيجاد إطار خاص بها يراعي خصوصية هذه الجريمة المستحدثة.

La société actuelle est de plus en plus dépendante de l'informatique. Les nouvelles technologies de l'information et de la communication (internet) contribuent à apporter des changements importants dans nos sociétés. Elles améliorent la productivité, révolutionnent les méthodes de travail et grâce à leur rapidité d'exécution modifient les modes de transfert de capitaux.

mais il est aussi très fréquent qu'elle soit mal employée voir employer abusivement. En général, qui à engendré la cybercriminalité, cette derniere porte sur l'usage illicite des technologies de l'information et des communications.

les cybercriminels ont su tirer avantage de la faible coopération internationale en matière de lutte contre cette nouvelle forme de criminalité. Ils peuvent ainsi lancer des attaques transfrontalières, car le risque personnel encouru est moindre et la difficulté de remonter jusqu'à la source des attaques est accrue.

Toutefois, le besoin d'un cadre juridique pour réglementer la cybercriminalité reste indispensable pour qu'internet ne restera pas une zone de non droit.