وزارة التعليم العالي والبحث العلمي
جامعة عباس لغرور
- خنشلـــــــة -

كليـــــة الحقوق و العلوم السياسية

قسم: الحقوق

نيابة العمادة في الدراسات للتدرج

مكافحة الجريمة المعلوماتية

مذكرة مكملة لنيل شهادة الماستر في الحقوق
تخصص: قانون جنائي و علوم جنائية

إعداد الطالب:

- أحمد الأقطش

تحت إشراف الدكتور:

الهاشمي تافرونت

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة الأصلية	الصفة
داود زمورة	أستاذ محاضر - ب -	جامعة خنشلة	رئيساً
الهاشمي تافرونت	أستاذ محاضر - أ -	جامعة خنشلة	مشرفاً و مقرراً
خديجة عمراوي	أستاذ محاضر- ب -	جامعة خنشلة	عضوا ممتحناً

السنة الجامعية : 2018-2019

"بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ"

الخاتمة

إهـــــــداء

إلى الذي أفنى عمره محترقاً لكي يريني النور

إلى من علمني النجاح والصبر

إلى من علمني أن أعتلي سلم الحياة بحكمةٍ و صبر..... إليك يا أبي

إلى من علمتني الصمود مهما تبدلت الظروف

لأجمل من رأت عيني

إلى ذلك النبع الصافي والشجرة التي لا تذبل التي كانت ولا زالت تقطع سكون الليل بدعواتها المخلصة والصادقة

إلى التي الجنة تحت أقدامها

إلى التي سهرت الليالي من أجل راحتي ... إلى الشمعة التي تنير أحلامي ومستقبلي.... إلى النجمة التي تتلألأ في قلبي ومسكني...

إليكي يا أمي

إلى من أشد بهم أزري وسندي في الدنيا ويلهجُ بذكرهم فؤادي أخواني وأخواتي

إلى الصخرة الشماء التي تعانق عنان السماء رفيقة دربي ... إليكِ يا كرنسي

إلى الغالي على قلبي عبد الله أسعد

إلى رمز البراءةِ والصدق عمرو، تالا، أية

إلى عزوتي وقدوتي في الحياة الدكتور نشأت الأقطش، سعد الأقطش

إلى روح المرحوم عمي الحاج محمد عبد العزيز الأقطش

إلى أبناء عمي و أبناء خالي وأبناء خالاتي وعماتي و إلى كل العائلة و الأصدقاء رفقاء الدرب في هذه الحياة.

إلى الأصدقاء الذين أنجبتهم الغربة لي وكانوا لي عوناً وسنداً.

إلى الذي علمونا كلماتٍ من درر وحروفٍ من ذهب دكاترتي و أساتذتي الكرام في مختلف المراحل الدراسية.

ولا أنسى أن أهديه إلى من هو أعز من نفسي علي وطني الجريح فلسطين وبلدي الثاني الجزائر.

الشكر والتقدير

عانينا الكثير من الصعاب وها نحن اليوم نطوي جهد عملٍ متواضع وحصاد سنوات الدراسة بين طيات هذه المذكرة.

فالشكر الأول و الأخير لله الواحد القهار مكورُ الليلِ على النهار.

أتقدم بجزيل الشكرِ والعرفان إلى الدكتور الفاضل " الهاشمي تافرونت" لقبوله الإشراف على هذه المذكرة وما أسداه لي من نصائح وتوجيهات كان لها الأثر البالغ بتتويج هذه المذكرة بالنجاح.

ولا أنسى في هذا المقام أن أتوجه بالشكر لأعضاء لجنة المناقشة

الدكتور زمورة داوود ، الدكتورة عمراوي خديجة لقبولهم مناقشة المذكرة.

كما أتوجه بالشكر لكل من أمد لي يد العون في إنجاز هذه المذكرة بنصيحة أو توجيه أو ترجمة.

مـقدمـة

تعد تقنية المعلومات الحديثة أو تكنولوجيا المعلومات والإتصالات وما نتج عنها من شبكات ووسائط إلكترونية قفزة حضارية نوعية في حياة الأفراد والدول، إلا أن هذا الجانب الايجابي المشرق لهذه التكنولوجيا لم ينفي الإنعكاسات السلبية التي أفرزتها إساءة إستخدام هذا التطور وما صاحبه من ظهور أنماط مستحدثة من السلوكيات الإجرامية بواسطة توظيف تقنيات المعلومة الحديثة في إرتكاب الجرائم وبواسطة شبكة المعلومات(الإنترنت) أو الأجهزة الأخرى كالهواتف النقالة، فقد تحول الإنسان إلى هدف من أهداف مجرمي التقنية الحديثة، وقد كشفت السنوات الأخيرة النقاب عن تكنولوجيا متطورة، لم تكشفها عقود من الزمن.

وإزاء التطورات السريعة والمذهلة في هذه التكنولوجيا التي جاءت لخدمة الإنسان، إلا أنه لم يرقى للبعض أن يحسن إستخدامها فأساء إستخدامها وألحق الضرر بأخيه الإنسان، فأتلف محتويات وأنظمة حاسوبه وكذلك قتله، لنجد أنفسنا أمام أصناف شتى من الجرائم المعلوماتية.

ولعل أهم القضايا التي تقلق رجال الفقه القانوني في الوقت الحاضر تلك هي الجريمة المعلوماتية، فلقد إنتشر الكمبيوتر في حياتنا اليومية فمعظم المجالات الحيوية أصبحت تعتمد عليه، وأدى هذا التطور لظهور مفاهيم جديدة من بينها الشبكة المعلوماتية التي أصبحت العصب الرئيسي للثورة المعلوماتية، وأصبح كل بعيد قريب فأضحى العالم قرية صغيرة.

وقد أدى التطور في إستخدام الحاسب الآلي إلى أن صار إستخدامه عنصراً فعالاً في تحقق تقدم الأمم والشعوب، كذلك معياراً لتطور وتقدم تلك الشعوب، ولقد رافق ذلك التقدم تزايد مستمر في الإعتماد على نظم المعلومات الآلية والتقنية القائمه على

الحاسب الآلي كوسائل رئيسية لحفظ ومعالجة وتشغيل البيانات داخل معظم المؤسسات الحكومية وغير الحكومية.

وهذا أدى الى ظهور جملة من الجرائم المعلوماتية التي قصرت التشريعات العقابية عن تجريمها لتعددها ولغياب نص التجريم إضافة إلى تعقيدات التحقيق فيها وضبط أدلتها ومرتكبيها وكل ذلك يجعل دراستها ومواجهتها أمراً صعباً لا ينفصل عن التعرف بشكلٍ عام عن مفهومها وتطورها وخصائصها ودوافعها وإجراءات التحقيق والمحاكمةِ فيها والجهود الدولية والوطنية للحد منها والعقوبات المقررة لملاحقة مرتكبيها، وتعدُ الطفرة المعلوماتية الرهيبة التي غزت القارات الخمس وفي خضام هذه التطورات نتيجة مجموعة من الجرائم ذات الطابع المعلوماتي ما عهدها الناس من قبل سميت بالجرائم المعلوماتية.

إن تعريف الجريمة المعلوماتية هو عبارة عن مصطلح قانوني وفني وتقني صعب الإمساك بكافة جوانبة القانونية، وإن المشرعين الجزائري والفلسطيني حذيا حذو التشريعات المقارنة الأخرى في تعريف الجريمة المعلوماتية من خلال سن قانون خاص في الجزائر يتعلق بالجريمة المعلوماتية، ألا وهو قانون رقم 04/09 المتضمن القواعد المتعلقة بالوقاية من الجرائم المتصلة بتكنولجيا الإعلام والإتصال ومكافحتها في التشريع الجزائري، أما المشرع الفلسطيني فقد إستحدث قانون خاص جديد بالجرائم المعلوماتية يعالج هذا الموضوع من كافة جوانبه وهو قانون رقم 10 سنة 2018 بشأن الجرائم المعلوماتية ومكافحتها وإجراءات التحقيق وملاحقة مرتكبي الجرائم المعلوماتية.

وهذا إن دل على شيءٍ فإنما يدل على إهتمام الدول في مكافحة الجريمة المعلوماتية التي إستحدثتها الوسائل الإلكترونية العصرية، وكيف سارت وتعاونت الدول فيما بينها في التعاون الدولي في مكافحة هذا النوع من الإجرام من خلال عقد الإتفاقيات الدولية والإقليمية، والتي تلزم الدول بإنشاء قوانين خاصة تتعلق بالجرائم المعلوماتية وإنشاء

أجهزة خاصة تتكفل بمواجهة هذه الجريمة، وبروز دور الإنتربول(منظمة الشرطة الجنائية الدولية) في المساعدة في مكافحة الجريمة المعلوماتية، وإن تسارع إيقاع التقدم التكنولوجي والتقني الهائل وظهور الفضاء الإلكتروني أستغله مرتكبوا الجرائم المعلوماتية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحده بل يشمل عدة دول مختلفه.

أهمية الموضوع:

يكتسي موضوع البحث أهمية متزايدة بسبب إستغلال وسائل الإتصالات الحديثة وسائر صور الإتصال الإلكتروني عبر الأقمار الصناعية التي إستغلها مرتكبوا الجرائم لتسهيل إرتكابهم لجرائمهم، فموضوع الدراسة المتمثل في دراسة القواعد الموضوعية والإجرائية الخاصة بالجرائم المعلوماتية، حيث يتناول الصور المتعلقة بهذه الجوانب في محاولة لتقديم الأساليب القانونية الممكنة لمكافحة هذه الجريمة في ظل النصوص التشريعية، والتعرف على الجرائم المُرتكبة ضد الحاسوب وشبكات الإنترنت، وإلقاء المسؤولية على الدولة بوضع التشريعات اللازمة لحماية المجتمع منها، وتبرز أيضاً أهميته من خلال إرتباطه الوثيق بظاهرة جديدة ظهرت مع التطور التكنولوجي، وهي الجرائم المعلوماتية التي تعتبر من الجرائم التي أثارت الكثير من المشاكل، فالطبيعة القانونية والفنية والتقنية الناجمة عن هذه الجرائم نتج عنها نوع جديد من الأدلة في الإثبات الجنائي، والمتمثل في الدليل الإلكتروني، كما وعالج هذا البحث واقع الجرائم الإلكترونية وملاحقتها في فلسطين، نظراً لحداثة الجريمة المعلوماتية في المجتمع الفلسطيني، وأنه يعتبر حالة مختلفة عن واقع هذه الجرائم في مختلف الدول بسبب وقوعها تحت الإحتلال الإسرائيلي الذي يسيطر على سماء وفضاء فلسطين الإلكتروني سيطرة تامة، مما يضفي لونا خاصا عند ملاحقته هذه الجرائم.

إشكالية البحث:

نظراً لحداثة الجرائم المعلوماتية وظهورها مع كل تقنية جديدة يتم إكتشافها وتوفيرها لأفراد المجتمع نقع في سوءِ إستخدامها، ما يستوجب على المشرع مواكبة التطور الحاصل على الصعيد التقني، من خلال إستحداث نصوص تشريعية لمكافحة الجرائم الناتجة عن هذه التقنيات ووضع حدٍ لها، وبالتالي العمل على تقليلها، إن لم يكن بالإمكان القضاء عليها.

وتتلخص مشكلة البحث في أن المشرع بالرغم من أنه سن نصوص قانونية خاصة بالجرائم المعلوماتية إلا أنه لم ينص على كافة أشكال الجرائم المعلوماتية وكذلك قانون الإجراءات الجزائية في كلا التشريعين لم يعالج الإجراءات التي تتعلق بالتحقيق والمحاكمة والمعاينة والتفتيش والضبط، وخاصة إذا كانت هذه الإجراءات تنصب على المعطيات المعنوية للجهاز الإلكتروني، ولم ينص على الضمانات التي يجب أن يحاط بها المتهم إذا ما تم ضبط وتفتيش الجهاز الإلكتروني الخاص به، وبما أن حوصلة الموضوع حول مكافحة الجرائم المعلوماتية، وحتى يتم الوقوف السليم على موضوع البحث ولنكون في بر الأمان وجب علينا معالجة هذا البحث بكافة صوره من خلال طرح **الإشكالية التالية:** هل وفق المشرع في سن آليات قانونية من شأنها وقاية ومكافحة الجرائم الناتجة التي إستحدثتها الوسائل الإلكترونية في عصر التكنولوجيا عبر القارات بهدف حماية الحقوق والحريات العامة للأفراد أم أن هذا الأخير هو ضحية هذا التطور؟

هل قانون الجرائم الإلكترونية قادرٌ على التصدي لجريمةٍ عصرية إستحدثتها الوسائل المعلوماتية في عصر العولمة، وهل هذا القانون قادر على تكييف الجرائم التي ترتكب عبر الوسائل الإلكترونية لحماية الحقوق المنتهكة؟

وللإجابه على هذه الإشكالية يستلزم طرح بعض التساؤولات الفرعية والتي نوردها على النحو التالي:

1-ما المقصود بالجريمة المعلوماتية؟

2-ما هي خصائص الجريمة المعلوماتية والمجرم المعلوماتي؟

3-ما هي طرق إثبات الجريمة الإلكترونية وكيفية إثبات هذه الجرائم؟

4-ما هي العقوبة التي حددها المشرع لمرتكبي الجرائم المعلوماتية؟

5-ما هي الآليات الوطنية والدولية لمكافحة ومواجهة الجريمة المعلوماتية وما هي طرق الوقاية من هذا النوع من الإجرام؟

منهج الدراسة:

بما أن هذا الموضوع يتطرق لأحدث الوسائل العلمية في إرتكاب الجريمة المعلوماتية من خلال إرتباطه الوثيق بالأجهزة المعلوماتية التي صاحبت التطور التكنولوجي، والتي لاقت إهتماماً كبيراً من رجال الفقه والقانون، وبخصوص المنهجية المتبعة لهذا البحث فقد إعتمدنا على المناهج التي نرى أنها تتماشى مع طبيعة الموضوع المطروح:

-**المنهج الوصفي:** لأن دراستنا تعتمد على تحليل النصوص القانونية المنظمة للجرائم المعلوماتية، وكذا وصف هذه الجرائم وفقاً لما نص عليه المشرع الجزائري والفلسطيني، وذلك من خلال الرجوع للدراسات السابقة والأبحاث والرسائل الأكاديمية العلمية والإتفاقيات الدولية والإقليمية ذات الصلة.

-**المنهج التاريخي:** من خلال التطرق لنشأة الجريمة المعلوماتية التي حصلت في القرن الماضي وصولاً إلى يومنا هذا، وذلك من شيوع إستخدام الكمبيوتر إلى ما وصل

عليه هذا النوع من الإجرام، وكذا من خلال التتبع لأهم القضايا المعلوماتية التي حصلت سابقاً وما جرى في الألفية الثالثة.

أهداف الدراسة:

1-تقديم صورة قانونية متكاملة حول الجرائم المعلوماتية وأنواعها وأركانها وماهيتها وطرق مكافحتها والوقاية منها.

2-تقديم دراسات قانونية وموضوعية تكشف الملامح والجوانب المختلفة لهذه الظاهرة.

3-التوصل للإختلافات (إن وجدت) المتعلقة بالنصوص القانونية للجرائم المعلوماتية.

4-بيان مدى نجاعة وحيوية وفعالية المكافحة الدولية والإقليمية من خلال الإتفاقيات الدولية المبرمة بين الدول في مواجهة الجريمة المعلوماتية.

أسباب إختيار الموضوع:

-أسباب ذاتية:

لأنها تكمن في مجال إهتمام الباحث في الجريمة المعلوماتية، ومن باب إثراء الحقل العلمي بمثل تلك الدراسات لأنها تجمع بين الدراسة الفنية والقانونية والتقنية.

-الأسباب الموضوعية:

تكمن فيما يطرحه موضوع الجريمة المعلوماتية من إشكاليات قانونية نظراً لحداثة الموضوع من الجانب الموضوعي لتجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات ونظراً لأهمية المكافحة في مجال الجريمة المعلوماتية وما فرضته من تحديات خاصه في عصرنا الحالي، وكذلك إستكمالاً للحصول على متطلبات شهادة الماستر في العلوم الجنائية والقانون الجنائي.

الدراسات السابقة:

1–بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دوكتوراة–تخصص قانون عام، جامعة الجزائر 1–كلية الحقوق–بن يوسف بن خدة، بن عكنون الجزائر،2018، وقد توصل الباحث من خلال هذه الأطروحة إلى عدة نتائج لعل من أهمها:أنه في مجال الجهود الدولية المبذولة لمجابهة ظاهرة الإجرام المعلوماتي، يمكن القول بأن بعض الإتفاقيات الدولية لا تزال تتخذ كمرجع لصياغة النصوص المتعلقة بوضع الإطار القانوني لحماية النظام المعلوماتي بشكل عام ومنها إتفاقية تريبس، ونتيجة أخرى ضرورة تعزيز الجهود الدولية الرامية إلى مكافحة الجريمة المعلوماتية بغرض صوغ صك شامل متعدد الأطراف يضع معالم نهج دولي في مجالات التجريم، وكنتيجة نهائية توصل إليها الباحث هي سد الفراغ التشريعي في مجالات البيئة الرقمية بتشعباتها كافة مع إصدار المذكرات التوضيحية للتشريعات، ورسم إستراتيجية متكاملة للأمن الإلكتروني ومكافحة الجرائم الإلكترونية.

2–أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم 04/09 ، رسالة ماجستير–تخصص قانون جنائي– كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر،2013، وقد توصل الباحث من خلال هذه الرسالة إلى عدة نتائج لعل من أهمها: أن مقدموا الخدمات يلعبون دوراً مهماً بما لديهم من تقنيات متماشية مع تطور التكنولوجيات الحديثة للإعلام والإتصال في مكافحة هذا النوع من الإجرام، وتقديم المساعدة التقنية للسلطات المكلفة بالبحث والتحري عن هذه الجرائم، ونتيجة أخرى أن القانون 04/09 يعد تحدياً فعلياً للسلطات القضائية وأعوانها من أجل تطبيقه نظراً لخصوصية الإجرائات التي جاء بها، وكنتيجة نهائية بالنسبة لتنسيق القوانين الجزائية العالمية سيؤدي بالتأكيد لإحكام قبضة العدالة على المجرمين في أي دولة يكونون فيها.

صعوبات الدراسة:

وأنا بصدد الدراسة والبحث في موضوع الجريمة المعلوماتية لم أواجه صعوبات كبيرة، إلا أني واجهتُ قلة المراجع والدراسات في مجال الجريمة المعلوماتية، لأنه لا يوجد دراسات سابقة كثيرة عن الموضوع وخاصة في فلسطين، أما بالنسبة للتشريع الجزائري واجهتني صعوبة في موضوع إثبات الجريمة المعلوماتية و خاصة ما يسمى بالدليل الإلكتروني، وواجهةُ صعوبة أيضاً في كيفية تكييف الصعوبات المقررة لملاحقة مرتكبي الجرائم المعلوماتية وخاصة في فلسطين كونه قانون جديد سنه المشرع الفلسطيني في الأونةِ الأخيرة.

خطة االبحث :

مقدمة.

الفصل الأول: الأحكام الموضوعية للجريمة المعلوماتية.

المبحث الأول: مفهوم الجريمة المعلوماتية.

المبحث الثاني: أركان الجريمة المعلوماتية.

الفصل الثاني: الأحكام الإجرائية للجريمة المعلوماتية وطرق مكافحتها محليا ودوليا.

المبحث الأول: الجرائم الموجهة ضد نظم المعلوماتية عن طريق الانترنت وطرق إثباتها.

المبحث الثاني: مكافحة الجريمة المعلوماتية.

الخاتمة.

الفصل الأول: ..... الأحكام الموضوعية للجريمة المعلوماتية.

تعتبر الجريمة المعلوماتية من الجرائم حديثة الظهور والنشأة، ذات توسع وتطور سريع وكبير، لذلك يصعب علينا أن نجد تعريفاً لها إلا في إجتهاد القضاء الحديث أو في شروحات الفقه، حتى أن هذا النوع من الجرائم يتمتع بطابع خاص به ولذلك سنتطرق إليه وسنوضحه من خلال ما يلي:

المطلب الأول: مفهوم الجريمة المعلوماتية.

المطلب الثاني: نشأة وتطور الجريمة المعلوماتية.

المطلب الثالث: خصائص الجريمة المعلوماتية.

المبحث الأول: مفهوم الجريمة المعلوماتية، نشأتها، خصائصها

المطلب الأول: مفهوم الجريمة المعلوماتية.

نظرا لكون هذا النوع من الجرائم في تطورٍ كبير وسريع، فلم يقم الفقه الحديث بوضع تعريفٍ محددٍ و واضحٍ له، بل لجأت التشريعات إلى إطلاق العديد من التعريفات عليها، وقد أطلقت على مثل هذه الجرائم عدة أسماء منها: الجريمة الإلكترونية، أو الجريمة المعلوماتية، أو الجريمة المرتبطة بالكمبيوتر والإنترنت، أو جرائم التقنية العالية، أو جرائم شبكة العنكبوت. ولمعرفة ما المقصود بالجريمة المعلوماتية يجب اولاً أن نتعرف على مصطلح الجريمة.

الفرع الأول: التعريف اللغوي والإصطلاحي.

أولاً: تعريف الجريمة لغةً و إصطلاحاً.

1-الجريمة لغةً: من فعل جرم جرماً جريمة، ويأتي بمعاني عديدة منها: الجرم :هو التعدي، أو الذنب والذي يجرم أهله شراً.[1]

2-الجريمة اصطلاحاً: تعددت آراء الفقهاء في تعريف الجريمة، وسنتطرق للبعض منها: هي كل فعل يضر بمصلحة إجتماعية أو يشكل خطراً عليها، ويسند الى فاعله لتحديد الجزاء الجنائي المحدد لها، وأيضاً تعتبر فعل معارض للقانون فهي فعل إرادي يحظره القانون ويقرر لفاعله جزائاً جنائياً.[2]

وقد عرفها الدكتور نجيب حسني "كل فعل غير مشروع صادر عن إرادة جنائية ويقرر له القانون عقوبة أو تدابير أين "هناك تعريف يقول" أنها كل فعل امتناع يمكن تعبّرُ عن ظاهرة إجتماعية محددة تعكس .إسناده لمرتكبه ويقرر له عقوبة جنائية السلوك غير السوي للإنسان، وتظهر على شكل ممارسات داخل المجتمعات سواء

[1] إبن منظور جمال الدين بن مكرم: **لسان العرب** ، ط1 ، دار صادر ، لبنان ،م3 ، ص. 129 -130.

[2] عبد الله سليمان : **شرح قانون العقوبات الجزائري (القسم العام)** ، ديوان المطبوعات الجامعية 2002 ، الجزائر ،ص.59.

كانت على شكل فردي أو جماعي، فيما يعرف بالإجرام الجماعي، أو الإجرام المنظم.[1]

أيضاَ عرفها الفقهاء بأنها:"سلوك إجتماعي يثير في ضمير الرأي العام شعوراً بضرورة توقيعِ عقوبة، لأنه يهدر مصلحة من المصالح التي يقوم عليها كيان المجتمع.[2]

وقد تطرق البعض الأخر من الفقهاء إلى تعريفها على أنها:" سلوك إنساني يرتكب إخلالا بقواعد القانون الجزائي يترتب عليه المساس بمصلحة يحميها المشرع، ويوقع القضاء على مرتكبه الجزاء الجنائي المناسب."[3]

ثانياً: تعريف المعلوماتية لغةً و إصطلاحاً.

1-المعلوماتية لغةً :علم الشئ وإدراكهُ، والعلم بالشيء أي اليقين والمعرفة.

ويطلق العلم على مجموعة من المسائل المتنوعة و الأصول الكلية المتكون منها الهيكل العام لكل مادة أو فن.[4]

كما تعني المعلومات: كل ما يعرفه الإنسان عن الشيء.[5]

2-المعلوماتية اصطلاحا: هو ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها، واختزانها، واسترجاعها، وتفسيرها، وبثها، وتحويلها، واستخدامها، كما يتضمن البحث عن تمثيل المعلومات في النظم الطبيعية والصناعية وإستخدام الرموز في نقل الرسالة والتعبير عنها.[6]

---

[1] weziwezi.com تاريخ الإطلاع على الموقع 2019/05/03

[2] ثروت جلال : **قانون العقوبات**، القسم العام، الدار الجامعية، بيروت، ص .89.

[3] جرادة عبد القادر : **مبادئ قانون العقوبات الفلسطيني ، (الجريمة والمجرم)** ، المجلد الأول، مكتبة الأفاق، غزة، 2010، ص .75.

[4] المسعدي محمود : **القاموس الجديد للطلاب ، معجم مدرسي ألفبائي** ، ط7 ، المؤسسة الوطنية للكتاب ، 1991 ، الجزائر ،ص .696 .

[5] المرجع نفسه، ص. 1107.

[6] الملط أحمد خليفة : **الجرائم المعلوماتية** ، ط2 ، دار الفكر الجامعي ،2006 ، مصر، ص.78 .

ويمكن الإستخلاص بأنها: عنصر من عناصر المعرفة والتي تسجل أو تنقل وتعالج من مكان ل أخر بوسيلة معينة، وتصل للطرف الأخر على شكل الرسالة.

الفرع الثاني: التعريف القانوني والقضائي للجريمة المعلوماتية

حداثة هذا النوع من الجرائم جعلت منها محلا للإختلاف بين الباحثين، فلم يتوصلوا الى مصطلحٍ واحد.

فالفريق الأول أطلق عليها لقب الغش المعلوماتي، و فريقٌ أخر أطلق عليها مصطلح جرائم الحاسوب، وآخر يذهب الى مصطلح الجرائم المعلوماتية، وهذا المصطلح هو المعتمد في متنِ هذه المذكرة، لأنه الأكثر تحديداً للمقصود، فهي ليست محصورة في جرائم الحاسوب فهي ترتكب عن طريق الإنترنت على وجه التحديد، وليست محصورة في الغش المعلوماتي، فقد تتجاوز ذلك لتصل الى فئة الجرائم ضد الأشخاص كالقتل والتحريض عليه.[1]

أولاً: التعريف القضائي للجريمة المعلوماتية :

عرفها التشريع الأمريكي بأنها:" الإستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات، أو الإستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات، وتتراوح خطورة تلك الجريمة ما بين جنحة من درجة الثانية الى جناية من الدرجة الثالثة."[2]

وتطرق مكتب التقييم بالولابات المتحدة الأمريكية الى تعريفها بقوله :" هي الجريمة التي تلعب البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيآ فيها."[3]

---

[1] العادلي صالح : **الجرائم المعلوماتية ماهيتها وصورها** ، ورقة عمل مقدمة لورشة العمل الأقليمية حول تطوير الشتريعات في مجال مكافحة الجرائم الإلكترونية، مسقط ، 2-4 ابريل 2006 ،الموقع الإلكتروني :www.iasj.net ، تاريخ الولوج إليه 05/04/

[2] القاضي رامي متولي : **مكافحة الجرائم المعلوماتية**، ط1، دار النهضة العربية، القاهرة، 2011م ، ص.23.

[3] عياد سامي علي حامد : **الجريمة المعلوماتية و إجرام الإنترنت**، دار الفكر الجامعي،2007 ، مصر، ص.38.

كما عرفها الفقيه Rosenblatt بأنها :" كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه."[1]

وعرفتها الدكتورة "هدى قشقوش" بأنها مجموعة الجرائم التي تتصل بالمعلوماتية.

ووفقآ لرأيها فأن هذه الجرائم هي جرائم الإعتداء على الأموال المعلوماتية: " وهي مجموعة الأدوات المكونة للحاسب الإلكتروني، وبرامجه ومعداته."[2]

-ثانياً: التعريف القانوني للجريمة المعلوماتية:

نظرا لحداثة هذا النوع من الجرائم، سارعت الدول لإيجاد قانون خاص يعالج الأفعال الناتجة عن التصرفات غير المشروعة، ولهذا نجد في الكثير من التشريعات أن المواد الاولى تتعلق بتعريف الجريمة المعلوماتية من نوع القانون المختص بهذه الجرائم.

ولحداثة هذا النوع من الجرائم، فلم يحدد تعريفا لها في بعض التشريعات مثل التشريع الفلسطيني، الذي أعتبر هذا النوع من الجرائم جديد ومستحدث.

هذا على عكس التشريعات الأخرى مثل التشريع السعودي الذي عرف الجريمة المعلوماتية بأنها:" أي فعل يرتكب متضمناً إستخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام."[3]

عرفها التشريع الأردني بأنها :" الجرائم التي يكون فيها الحاسوب وسيلة لإرتكاب فعل غير مشروع، أو محلاً لوقوع الفعل غير المشروع، وذلك للقيام بعمل أو الإمتناع عن أدائه، من شأنه الإعتداء على الأموال المادية والمعنوية، شريطة أن يكون صاحبها عن دراية ومعرفة تقنية كبيرة في التعامل مع الحاسوب والتعامل مع معطياته."[4]

---

[1] **المرجع نفسه**، ص.40.

[2] قشقوش هدى حامد : **جرائم الحاسب الإلكتروني**، دار النهضة العربية، مصر، ص5-6.

[3] المادة 01، من نظام مكافحة الجرائم المعلوماتية السعودي، 1428 هـ.

[4] الحلبي خالد عياد : **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت** ، ط1 ، دار الثقافة للنشر والتوزيع ، عمان ، 2011م، ص 31.

أما المشرع البحريني في قانون جرائم تقنية المعلومات رقم (60) لسنة 2014، لم يعرف الجرائم المعلوماتية في المادة الأولى منه، بل اكتفى بتعريف بعض المصطلحات[1]، كذلك فعل المشرع الأردني في قانون الجرائم الإلكترونية رقم (27) سنه 2015[2]، والمشرع الإمارتي في قانون مكافحة تقنية المعلومات الإماراتي رقم (5) لسنة 2012.[3]

ومن خلال ما سبق يمكن أن نجانب الصواب بتعريف الجريمة المعلوماتية على أنها:" الأفعال غير المشروعة والمجرمة التي يُستخدم الحاسوب الآلي أو الشبكات العنكبوتية للقيام بها، والتي تمس المعلومات والبيانات بهدف التغيير أو التعديل، أو التدمير أو المحو لتلك المعلومات والتي تشكل خطراً وآثاراً ضارة على المجتمع، ويقع على عاتق مرتكبها الجزاء الجنائي".

[1] قانون جرائم تقنية المعلومات رقم 60 لسنة 2014 لدولة البحرين، المنشور في الجريدة الرسمية البحرينية العدد 3178 بتاريخ 2014/10/09، و الصادر في قصر الرفاع بتاريخ 2014/09/20 عن ملك مملكة البحرين حمد بن عيسى آل خليفة.

[2] قانون الجرائم الإلكترونية رقم 27 لسنة 2015 لدولة الأردن، والمنشور في الجريدة الرسمية الأردنية العدد 5631، بتاريخ 2015/05/04، والصادر في المملكة الأردنية الهاشمية عن ملك الأردن عبد الله الثاني ابن الحسين.

[3] قانون مكافحة تقنية المعلومات رقم 5 لسنة 2012 لدولة الإمارات، والمنشور في الجريدة الرسمية الإماراتية المرسوم رقم 05 بتاريخ 2012، والصادر عن سمو الشيخ خليفة بن زايد آل نهيان.

المطلب الثاني: نشأة وتطور الجريمة المعلوماتية.

مرت الجرائم المعلوماتية بعدة مراحل تطورت من خلالها، نتيجة لتطور وسائل الإتصال والتقدم التقني الهائل الذي يمر به العالم الحالي، وقد قسمنا هذه المراحل الى:

الفرع الأول: المرحلة الأولى لنشأة الجريمة المعلوماتية

بدأت هذه المرحلة من شيوع إستخدام الكمبيوتر في الستينيات، حيث تم في هذه المرحلة ظهور أول معالج لما يسمى بجرائم الكمبيوتر، حيث كانت تقتصر المعالجة على مقالات ومواد صحفية تناقش التلاعب الذي يحصل بالبيانات والتجسس والدمار الذي يحصل في نظم الكمبيوتر، ويعد ذلك وتحديدا خلال فترة السبعينات بدأت بعض النقاشات يصاحبها التساؤل التالي: هل هذه الجرائم مجرد موجة عابرة أم أنها مستجدة؟ هل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في البيئة ومهنة الحوسبة؟ بقي بعد ذلك التعامل معها أقرب إلى النطاق الأخلاقي منه إلى النطاق القانوني، ومع تزايد الإستخدام لأجهزة الحاسوب تزايد معها عدد هذه الجرائم، وبالتالي ظهرت دراسة مسحية إهتمت بالجرائم المعلوماتية، وأيضاً دراسات قانونية قد عالجت بعض الجرائم الواقعة منها فعلياً، ومن خلال ما تم التعامل معه خلال هذه الفترة أصبح الحديث عنها كظاهرة إجرامية لا مجرد سلوكيات فرضية غير أخلاقية.[1]

الفرع الثاني: المرحلة الثانية لنشأة الجريمة المعلوماتية

شهدت فترة الثمانينات تضاعفاً كبيراً لجرائم الكمبيوتر، و زاد إرتباطها بعمليات إقتحام نظم الكمبيوتر عن بعد وتدمير الملفات أو البرامج، وهذا ما أدى إلى إشاعة مصطلح (الهاكرز) الذي يحمل معنى مقتحمي النظم ،حيث إنحصر الحديث عنهم بصغار

[1] عبد الفتاح مراد: **شرح جرائم الكمبيوتر والأنترنت** ، طبعة 1 ، دار الكتب والوثائق المصرية،مصر ، 2005، ص. 38-39.

السن ممن يتمتعون بذكاء عالي و الرغبة في المغامرة والتحدي وإظهار قدراتهم التقنية المتفوقة، وقد أدى هذا الحديث الى ظهور منظمات الهاكرز التي طالبت بدورها بأن يتوقف التشويه لحقيقتهم و صورتهم، بل وأصرت على أنهم يقومون بنوع من خدمات التوعية لإظهار ما لمعايير الأمن للنظم والمعلومات من أهمية، ولكن المشكلة أن مغامري الماضي أصبحوا عتاة إجرام فيما بعد، فهنا بدء المعلوماتي المتفوق بإظهار أهدافٍ إجرامية من إستيلاء على الأموال والتجسس والإستيلاء على بيانات مهمة وفي غاية السرية، أو الحصول على بيانات إقتصادية وإجتماعية وسياسية وعسكرية، وهذه الأسباب المدفوعة بأهداف إجرامية أظهرت تخوف عالمي كبير، لأن العالم أصبح كتاباً مقروءاً خالي من السرية أمام الهاكرز، يجولون فيه كما يريدون، يتحصل منها المغامر المعلوماتي على ما يخدم مصلحته الشخصية، ولا يأبه لأضرار عالمية قد تحدث.[1]

الفرع الثالث: المرحلة الثالثة لنشأة الجريمة المعلوماتية

جاءت هذه المرحلة في فترة التسعينات بتغير كبير فمفهوم هذه الجرائم ونطاقها، وذلك نتيجة التوسع الهائل لشبكات الأنترنت وما قدمته من تسهيلات للولوج الى الأنظمة والمعلومات، فأدى ذلك الى ظهور أشكال جديدة مثل تعطيل نظام معين والعمل على منعه من القيام بعمله المعتاد وهذا ما يطلق عليه نظام إنكار العمل أو الخدمة، كانت تمارس هذه الجرائم بشكلٍ أكبر على المواقع العنكبوتية المتعلقة بالأنشطة التسويقية، التي إذا توقفت عن العمل لأوقات معينة قد تكون بضع ساعات يعني خسارات مالية ضخمة تصل الى الملايين، ومما تتميز به هذه المرحلة هو الإنتشار الكبير للفايروسات عبر شبكات الإنترنت، عن طريق المواقع الإلكترونية التي أستغلها مجرموا المعلومات لتسهيل إنتشار الفيروسات الى ملايين المستخدمين، وفي ذات الوقت بدأت بالظهور

[1] عبد الفتاح مراد: **المرجع السابق** .39.

أنشطة الرسائل والمواد الكتابية المنشورة على الإنترنت أو المراسله عبر البريد الإلكتروني، المنطوية على إثارة الأحقاد، أو المساس بكرامة و إعتبار الأشخاص أو المُستهدِفة ترويج مواد او أفعال غير قانونية وغير مشروعة (جرائم المحتوى الضار).[1]

المطلب الثالث: خصائص الجريمة المعلوماتية.

نظراً لكون الجريمة المعلوماتية جريمة مستحدثة، ظهرت نتيجة التقدم والتطور في وسائل الإتصال والتكنولوجيا و إعتمادها على وسائل وطرق معينة لإرتكابها، فهذا ما جعل منها جريمة تتمتع بخصائص مختلفة عن الجرائم التقليدية، وسنتطرق في هذا المطلب الى الخصائص المتعلقة بالجريمة و أخرى متعلقة بالمجرم علي النحو الأتي:

الفرع الأول: خصائص الجريمة المعلوماتية: وهي الخصائص المتعلقة بموضوع الجريمة نفسها ومنها :

أولاً: عالمية الجريمة المعلوماتية (عابرة للحدود): كون الجريمة المعلوماتية جريمة تعتمد على الشبكات والمواقع الإلكترونية، وكونها ترتكب بواسطة أجهزة الحاسوب، فهي بالتالي غير مقيدة بحدود جغرافية معينة، وتباعد وقرب المسافات ليس له تأثير، فإن إرتكاب الجريمة المعلوماتية غير محدد بمكان أو منطقة معينة أو بوقتٍ ما.

ونظراً لتباعد المسافات بين المجرم والنتيجة الجرمية، أدى هذا الى ظهور إختلافات في كيفية تحديد الإختصاص في النظر في مثل هذه الجريمة، لهذا كانت الدول مجبرة على التكاثف والتعاون فيما بينها لمواجهة هذا النوع من الجرائم، فعلى المستوى العربي جاءت الإتفاقية العربية الموقعة سنة 2010 في المادة (30) منها على ما يلي: تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمدة إختصاصها على أي من الجرائم

[1] عبد الفتاح مراد : **المرجع السابق** ، ص.40.

المنصوص عليها في الفصل الثاني من هذه الإتفاقية وذلك إذا إرتكبت الجريمة كلياً أو جزئياً أو تحققت:

- في إقيلم دولة طرف.
- على متن سفينة تحمل علم دولة طرف .
- على متن طائرة تحمل قوانين دولة الطرف .
- إذا كانت الجريمة تمس أحد مصالح الدولة العليا.[1]

ثانياً: صعوبة إثبات الجرائم المعلوماتية : نظراً لكون الجريمة المعلوماتية تعتمد على الكمبيوتر والوسائل التقنية، بالتالي يصعب إثباتها من حيث عدم وجود دليل يدين المجرم.

فتوجه قسم من الفقهاء الى القول بأن سهولة محو الدليل، والتلاعب به خصوصا مع عدم توافر دليل مادي ملموس للجريمة المعلوماتية ، وأيضاً غياب القدرة الفنية لدى رجال الشرطة والمتعلقة بالأمور التفصيلية بالجريمة الإلكترونية، هي من الأمور التي تجعل إثبات الجريمة المعلوماتية صعبة المنال.[2]

وأكد إتجاه ثانٍ من الفقه على صعوبة إكتشاف الجرائم المعلوماتية، وإقامة الحد على مرتكبيها؛ ويعود هذا الى تعلق هذه الجرائم بالطابع التقني، والذي يضفي عليها الكثير من الصعوبة والتعقيد في الإثبات، وتعد سهولة التخلص من المعلومات وإخفائها وتدميرها من سمات هذة الجريمة التي تشكل صعوبة كبيرة في إثباتها.[3]

وكون هذا النوع من الجرائم يعتمد علي المعرفة التقنية الواسعة والكبيرة للتعامل والتعاطي مع الكمبيوتر وبياناته، فهي جريمة تحتاج الى قمة الذكاء لإرتكابها .

---

[1] لورنس سعيد الحوامدة : **الجرائم المعلوماتية أركانها وآلية مكافحتها** ، مجلة الميزان للدراسات الإسلامية و القانونية ، المجلد الرابع، العدد 1، جامعة العلوم الإسلامية العالمية، ماليزيا، 2017/2016، ص.9.

[2] لورنس سعيد الحوامده: المرجع نفسه، ص.11.

[3] أحمد محمود مصطفى : **جرائم الحاسبات الآلية في التشريع المصري**، ط1 ، دار النهضة العربية، القاهرة، 2010م، ص.18 .

ثالثاً:الجريمة المعلوماتية جرائم الأذكياء : توصف الجريمة المعلوماتية بأنها جريمة ناعمة، يعود ذلك لسهولة إرتكابها دون أي مجهود عضلي يذكر، وهذا على خلاف الجرائم الأخرى التي تتطلب مجهود بدني سواء للسرقة أو القتل أو الإغتصاب، فالجرائم المعلوماتية لا تتطلب سوى علم كافي بالجوانب الفنية والتقنية للجهاز الإلكتروني، فليس على المجرم التواجد في مسرح الجريمة، بل يكتفي فقط بضغطة زر لتنفيذها، وما يضفي الإغراء على الجرائم المعلوماتية هي سرعة القيام بها وسهولة محو أدلة الإدانة بعد إرتكابها، ومن المغريات الأخرى هي المبالغ المالية الضخمة التي يتحصل عليها في وقتٍ قصير، خاصة الموظفين الذين يعملون في الشركات التي تعتمد على النظام الإلكتروني في عملها فيسهل إختراقها من قبلها وتحقيق مبتغاهم.[1]

ولأن مثل هذا النوع من الجرائم يحتاج إلى ممارسة ومعرفة في التقنيات، فهي تحتاج إلى ساعات طويلة للتمرس لتعلم التعامل والتعاطي مع بيانات الإنترنت والكمبيوتر، ولهذا نجد أن أغلب مرتكبي الجرائم المعلوماتية هم من صغار السن والمراهقين، يعود هذا لكثرة الوقت الذي يقضونه في التعامل مع التقنيات ، التي كانت وما زالت تنتشر لتصبح أساساً لا يمكن التخلي عنه في وقتنا الحاضر.

الفرع الثاني: خصائص الجريمة المعلوماتية من حيث مرتكبها:

أولاً:المجرم المعلوماتي هو إنسان إجتماعي : المجرم المعلوماتي بكونه إنسان غير عنيف وهذا ما يميزه عن المجرمين الآخرين، فهو في لحظة ما يكون إنساناً طبيعياً قادر على التكيف والتعايش مع فئات مختلفة في المجتمع دون حيرة ولا ترددٍ ولا قلق، وهذا يعود إلى ذكائه الحاد، وفي لحظة أخرى يكون ذلك المجرم المحترف الذي يقوم بجريمته بكل هدوء وتروي ويقوم بمسح آثارها بسهولة ويسر.

[1] أسامة أحمد المناعسة، وأخرون : **جرائم الحاسوب الآلي والإنترنت**، ط1، دار وائل للنشر، عمان ، 2001 ، ص.107.

وتتنوع دوافع قيام المجرم المعلوماتي بفعلته، فقد يكون بدافع اللهو والتحدي، وقد يكون إنتقاماً من رب عمله الذي طرده، وقد يكون بدافع إظهار قدرته على إختراق الأجهزة أو بدافع مادي والنصب.[1]

كون المجرم المعلوماتي متكيف إجتماعياً، هناك من يرى أنه كلما زادة خطورته الإجرامية زادت قدرته على التكيف مع الناس والمجتمع.[2]

وفي أغلب الأحيان يعود المجرم المعلوماتي لتكرار جريمته، فيصبح عائدٍ للإجرام، وذلك برغبةٍ ملحةٍ منه في التعرف على الثغرات التي أطاحت به في المرة الأولى والعمل على سدها، وحتى لو عرضه ذلك للمحاكمة مرةٍ ثانيه فهو إنسان لحوح يحب التحدي والإكتشاف، وفي أغلب الأحيان المجرم المعلوماتي ليس له علاقة بالجرائم التقليدية الأخرى، فهو يكتفي بإرتكاب الجرائم المعلوماتية وحدها.[3]

ثانياً: المجرم المعلوماتي هو إنسان ذكي ومتخصص : المجرم المعلوماتي يتمتع بذكاء وقدرة ذهنية كبيرة في مجال التكنولوجيا، التي إكتسبها إما من خلال دراسات متخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة من خلال الممارسة العملية مع الحاسوب و الإنترنت، فهو من خلال قدرته يستطيع القيام بإختراق ودخول أصعب المواقع و البرامج، والتي تكون غالباً محمية ببرنامج حماية أو شيفرة معينة.[4]

وهذا النوع من الذكاء هو ما نفقده عند المجرميين التقليديين، الذين في غالب حالاتهم يتركون أثار خلفهُم لتدل عليهم، على عكس المجرم التقني الذي يكون قد ألم بجميع

---

[1] العريان محمد علي: **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2011، ص77.

[2] القاضي رامي المتولي: **المرجع السابق**، ص55.

[3] الديربي عبد العال ، محمد صادق إسماعيل : **الجرائم الإلكترونية**، ط1، المركز القومي للإصدارات القانونية، القاهرة ، 2012 ، ص58-59.

[4] المومني نهلا عبد القادر : **الجرائم المعلوماتية**، دار الثقافة، عمان، 2010، ص.77.

الجوانب الفنية والتقنية لجريمته ، فيكون من السهل عليه إخفاء ومحو الأدلة التي قد تُدينُه.

وهذا الحال لدى المجرمين المعلوماتيين الذين لا يتجاوزون حدود إلمامهم في الجريمة، فإذا كانت معلومات المجرم المعلوماتي قليلة، فإن جريمته لا تتعدى الإتلاف أو نسخ البيانات و البرامج، أما إذا كان المجرم المعلوماتي ذو خبرةٍ عالية تكون طبيعة جرائمه من إختراق الأجهزة أو جريمة التجسس الإلكتروني أو زرع الفايروسات أو سرقة الأموال.[1]

ومما يؤكد قدرة المجرم الذهنية والتقنية والعقلية هو قيام الهاكرز بإختراق مواقع دولة الإحتلال ومواقعها الحكومية، ومواقع البورصة والجامعات والمصارف، والتي تسببت في توقف بعض المرافق الحيوية مثل إشارات المرور والبنوك، وتم استخدام هذا النوع كأسلوب جديد للمقاومة في وجه الأحتلال[2].

وقد تبين من خلال العديد من القضايا أن المجرم المعلوماتي هو مجرم متخصص، اي يكتفي بنوع الجرائم المختصة بالكمبيوتر والإنترنت، ولكن قد يتمادى البعض في جرائمه ليصل إلى جرائم خطيرة.[3]

فالمجرم المعلوماتي يسعى دائماً لإكتشاف المزيد من الثغرات و فتح كل الطرق أمامه، وذلك سعياً للظهور والتميز بين آقارنه من المعلوماتيين .

---

[1] خالد محمود إبراهيم : **الجرائم المعلوماتية** ، ط1 ، دار الفكر الجامعي ، الإسكندرية ، 2009 ، ص .134-135.

[2] تقرير بعنوان " **الحرب الإلكترونية تقلق إسرائيل** "، مشار إليه عبر الموقع الرسمي لقناة الجزيرة الفضائية ، 2013/06/13 ، www.aljazeera.net

[3] الحلبي خالد عياد : **المرجع السابق** ،ص.32-33.

المبحث الثاني: أركان الجريمة المعلوماتية

اشترط المشرع لقيام الجريمة وجود ثلاث أركان أساسية، هي الركن المادي والركن المعنوي والركن الشرعي، وبدون توافر هذة الأركان ينتفي وجود الجريمة، وهذا هو الحال بالنسبة للجريمة المعلوماتية، إذا توافرت هذه الشروط وجدت الجريمة وإذا إنتفت نفى ذلك وجود الجريمة، والركن المادي الذي يمثل الفعل والنشاط الذي يرتكبه الجاني والسبب والعلاقة السببية بين الفعل والنتيجة، والركن المعنوي الذي يشكل العلم و الإرادة الخاطئة للجاني لمباشرة سلوكه، فالركن المادي له مظهر خارجي على عكس الركن المعنوي.[1]

وسنتطرق ونوضح كل ركن كالأتي:

المطلب الأول: الركن المادي للجريمة المعلوماتية.

المطلب الثاني: الركن المعنوي للجريمة المعلوماتية.

المطلب الثالث: الركن الشرعي للجريمة المعلوماتية.

المطلب الاول: الركن المادي للجريمة المعلوماتية.

يشكل السلوك العامل المشترك بين جميع الجرائم، وهو العنصر الأول من عناصر الركن المادي ، ولأن السلوك يعتبر أساس قيام الجريمة يجب أن يكون الفعل مخالفاً لنص قانوني مُشرَّع ، وقيام الفعل يجب أن يترتب عليه نتيجة جرمية وهي العنصر الثاني من عناصر الركن المادي التي تكون سواء بقيام الفعل أو تركاً لعمل ما وهذا طبقاً للإتجاه المادي، أما بالنسبة للإتجاه القانوني فهو الضرر الذي يصيب المصلحة التي يحميها الشارع.

والعنصر الثالث وهو العلاقة السببية بين الفعل وبين النتيجة الجرمية، وأنه لولا السلوك لما كانت النتيجة الإجرامية.[2]

---

[1] سرور احمد فتحي: **الوسيط في قانون العقوبات**، الجزء 1، القسم العام ، دار النهضة العربية، القاهرة، 1981، ص256.

[2] جرادة عبد القادر: **المرجع السابق** ، ص.138 .

ومن خلال ما سبق سنتطرق بالتفصيل لعناصر الركن المادي:

الفرع الأول: السلوك في الجريمة المعلوماتية

الجريمة المعلوماتية تقوم من خلال الحاسب الآلي والذي من دونه لا يمكن تصور قيام الجريمة، و تعتبر حيازة الشخص للحاسب الآلي والإنترنت أمراً مشروعاً، وكذلك استخدامه أمراً مشروعاً كأصل عام، ولكن الخلاف عندما تستخدم هذه الوسائل في غرضٍ غير مشروع، ولذلك تعد الوسيلة الإلكترونية من أهم مقومات السلوك الإجرامي في الجريمة المعلوماتية، فالسلوك هنا يتطلب وجود بيئة رقمية من حيث جهاز الحاسب الآلي للجرائم المعلوماتية بشكل عام، والإنترنت لجرائم الإنترنت بشكل خاص، كما يتطلب هذا الأمر معرفة كيفية إستخدام هذه التقنية مثل تنزيل برامج إختراق أو عمل برنامج بنفسه أو تحميل الصور المخلة والفايروسات تجهيزاً لنشرها على الإنترنت.[1]

ويتخذ السلوك المادي في الجريمة المعلوماتية صورتين الأولى إيجابية والأخرى سلبية.

أولاً: الصورة الإيجابية المتمثلة في المجهود البدني الذي يبذله في العالم الخارجي من أفعال ملموسة، يقوم من خلالها بالإعتداء على المصلحة التي يحميها المشرع، ومثال ذلك ما يقوم به الجاني في الجرائم المعلوماتية بالتعدي على الحاسب الآلي لإفساد ما به من برامج و وإفسادها أو نسخها، أو أن يقوم بإجراء اتصالات محلية ودولية بطريقة غير مشروعة، أي دون دفع المستحقات اللازمة عليه، أو أن يقوم الجاني بإختراق بيانات شبكات الإتصال ويحصل على بيانات الشركة نفسها ويقوم بنشرها أو تهديد أصحابها بإستخدامها بشكل غير مشروع.[2]

---

[1] خالد ممدوح إبراهيم :**حوكمة الإنترنت** ، ط1 ، دار الفكري الجامعي ، الإسكندرية ، 2011 ، ص.ص382 -383..

[2] عبد الفتاح بيومي حجازي : **الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة** ، المركز القومي للإصدارات القانونية ، القاهرة ، 2011 ، ص266.

ثانياً: الصورة السلبية المتمثلة في الإمتناع عن الإتيان بعملٍ أوجبه القانون [1].

فيمكن أن تقام الجريمة من خلال الكف عن عملٍ معين كان من الواجب مباشرته، مثل إمتناع رجل الإطفاء من القيام بواجبه رغم قدرته على ذلك، لكن لصور الإمتناع في الجريمة المعلوماتية شكلٍ أخر، فهي رغم إختلاف الفقهاء لكنها موجودةً ومن الممكن حدوثها، مثل إمتناع موظف الأمن عن حماية البيانات والمعلومات في الشركة التي يعمل بها، أو عدم الإبلاغ عن جريمة لحماية خصوصية الناس، أو عدم التدخل للحفاظ على أسرار الدولة في الجرائم التي تمس أمن الدولة.[2]

ويمكن تلخيص ما سبق بالقول بأن السلوك في الجريمة المعلوماتية الذي يتم من خلال جهاز إلكتروني أياً كان نوعه، والإتصال بالشبكة العنكبوتية في الجرائم المتعلقه بالإنترنت، حيث لا يمكن مباشرة الجريمة دون هذه الوسائل، ويكون السلوك إما إيجابي وذلك بقيام الجاني بفعل مادي بإستخدام إحدى الوسائل الإلكترونية وهي الصورة الغالبة والشائعه في هذه الجرائم، وقد يكون سلبي بالإمتناع عن قيام بعملٍ من الواجب الإتيان به، وهذا النوع نادر الحدوث.

الفرع الثاني: النتيجة الإجرامية في الجريمة المعلوماتية

هي العنصر الثاني من عناصر الركن المادي، وتعرف بأنها :" الضرر الذي نتج عن الفعل الإجرامي سواءاً كان بالإمتناع عن عمل أو الإتيان به، وهي الأثر الخارجي الذي يتولد عن السلوك، ويحدث تغيراً يعتد به القانون، حسب التصور المادي للنتيجة، أما التصور الشرعي والقانوني فهو الإعتداء على مصلحة يحميها القانون"[3].

ومثال على ذلك قيام طبيب بفتحِ ملفات المرضى لديه في المشفى من المنزل بواسطة الإنترنت، والقيام بتغيير مقدار الدواء ونوعه لدى المريض بهدف قتله، فإذا

---

[1] أسامة احمد المناعسة ، جلال محمد الزعبي ، **جرائم تقنية نظم المعلومات الإلكترونية** ، ط1 ، دار الثقافة للنشر والتوزيع ، 2010 ، ص50.

[2] إبراهيم محمد اللبيدي : **السلوك الإجرامي في جرائم الإنترنت** ، مركز الإعلام الأمني ، القاهرة ، ص25.

[3] ثروت جلال : **قانون العقوبات ، االقسم العام** ، الدار الجامعية ، بيروت ، 2007ص122.

مات المريض تحقق الهدف الإجرامي لسلوك الطبيب، والذي يكون لديه العلم الكامل بالعمل الذي قام به، فضلا عن امتلاكه لكلمات سر قاعدة البيانات التي سهلت عليه جريمته.[1]

وأيضاً يعتبر الإتلاف للبيانات والمعلومات من خلال نشر فايروس أو عن طريق الإختراق للأجهزة ، هو من الأثار المترتبة على الفعل الإجرامي، وهذه الآثار التقنية من السهل تقديرها واكتشافها، وقد يأتي الضرر معنوياً مثل السب والقذف والشتم ونشر صورٍ مسمومه بين أفراد المجتمع، وقد يصل الأمر لإختراق مواقع المؤسسات الحكومية، فهذه الآثار المعنوية يخضع تقديرها للسلطة التقديرية للقاضي المختص.

الفرع الثالث: العلاقة السببية في الجريمة المعلوماتية

وهي العلاقة بين السلوك الإجرامي سواء كان فعلاً أم تركاً وبين النتيجة الإجرامية، بمعنى أن السلوك الإجرامي هو سبب حدوث النتيجة الإجرامية، فلولا السلوك لما حدثت الجريمة.[2]

تبرز أهميت العلاقة السببية كونها عنصراً أساسياً لتحقق الركن المادي، وتحققها من أهم الشروط الجوهرية لإقامة المسؤولية الجزائية، فإذا أسندنا النتيجة الإجرامية إلى السلوك، وكانت هناك إرادة حرة وواعية، توافرت فيها أسباب إقامة المسؤولية الجزائية، وعلى عكس ذلك إذا لم توجد علاقة بين النتيجة والسبب انتفى سبب إقامة المسؤولية الجزائية.[3]

وتثبت أيضاً العلاقة السببية من خلال حيازة صور إباحية لأطفال في حاسوب بمجرد ثبوت الضرر، وذلك من خلال بث هذه الصور، فتظهر علاقة السببية بين حيازة هذه الصور وبين ترويجها أو عرضها أو تداولها.[4]

---

[1] خالد ممدوح إبراهيم :**حوكمة الإنترنت** ، ط1 ، دار الفكري الجامعي ، الإسكندرية ، 2011 ، ص388 .

[2] أسامة أحمد المناعسة و آخرين : **المرجع السابق**، ص48.

[3] جرادة عبد القادر : **المرجع السابق**، ص147 -148.

[4] الحسيناوي علي جبار : **جرائم الحاسوب والإنترنت** ، دار اليازوري للنشر والتوزيع ، عمان ،2009 ، ص39.

الفرع الرابع: أمثلة على الركن المادي في بعض الجرائم المعلوماتية :

أولاً: جريمة السرقة المعلوماتية :

هي من الجرائم غالبة الوقوع والتي تتم من خلال إختراق بيانات البنوك ومواقعها، أو الحصول على بيانات العملاء في الشركات، وكل ما يشمل الحصول على البيانات والمعلومات دون إذن صاحب المحل الإلكتروني، فهذا يكفي لقيام الركن المادي للجريمة المعلوماتية، وايضاً جريمة الإتلاف للبيانات التي قد يلجأ الجاني فيها لعدة طرق للقيام بجريمته، إما أن يتواصل عن بعد ويقوم بالدخول لبرنامج الحاسب الآلي وإتلاف البرامج والبيانات، أو أن يقوم بإرسال برامج فايروس لتدمير المعلومات، أو أن يتلف القاعدة الأساسية لبيانات المحل الإلكتروني.[1]

ثانياً: جريمة القذف والذم :

ومن الجرائم المعلوماتية المنتشرة بكثرة هي جريمة القذف والذم، ويتكون الركن المادي فيها من النشاط الخادش للشرف و الإعتبار، الذي يرتكبه الجاني عن طريق الحاسب الآلي أو الهاتف المحمول، مثل إرسال رسالة نصية تحمل عبارة نابية أو تلصق صفة سيئة بالمجني عليه، أو بإرسال صورة أو ملف صوتي أو غيرها من الوسائل الإلكترونية الحديثة.[2]

وقيام الركن المادي في جريمة سرقة البرامج الإكترونية لإستعمالها، في قيام الجاني بالإستيلاء على هذه البرامج قبل إستعمالها، فلا يمكن تصور الإستعمال قبل حدوث الإستيلاء، فللقول أن الركن المادي موجود في جريمة السرقة المعلوماتية، لا بد أن يستولي السارق على حيازة الشيء المسروق حتى يتمكن من إستعماله.[3]

---

[1] ناير نبيل عمر : **الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية** ، دار الجامعة الجديدة ، الإسكندرية ، 2012 ، ص71.

[2] يوسف حسن يوسف : **الجرائم الدولية للإنترنت** ،المركز القومي للإصدارات القانونية ، ط1 ، القاهرة ،2011 ، ص206.

[3] الهيتي محمد حماد : **التكنولوجيا الحديثة والقانون الجنائي** ، ط2 ، دار الثقافة للنشر والتوزيع ، عمان ،2010 ، ص224.

ثالثاً: جريمة الولوج والبقاء في نظام المعالجه الآلية للبيانات :

لثبوت هذا النوع من الجرائم يسلتزم المجرم أن يقوم بنشاطٍ مادي بإستخدام جهازٍ إلكتروني يؤدي إلى إنتهاك نظم الحماية الأمنية التي تضعها المؤسسة والشركات لحماية نظامها الإلكتروني من محاولات تعديلها أو العبث بها أو إتلافها، و يعبر عن إرادته في البقاء داخل هذا النظام.[1]

المطلب الثاني: الركن المعنوي في الجريمة المعلوماتية

يعتبر الركن المعنوي النصف الآخر للجريمة، ويمكن تعريفه بالحالة النفسية للمجرم أثناء إرتكابه للجريمة حيث لا تقوم الجريمة من دونه، فلا بد من توافر الإرادة الأثمة للمجرم عند إقدامه على السلوك الإجرامي، كما يجب أن تكون ألأفعال إرادية وإلا انتفى الركن المعنوي للجريمة، وأن تكون هذه الأفعال متجهة نحو مخالفة القواعد القانونية، ليترتب على مخالفتها الجزاء الجنائي المناسب.[2]

ويجب على الجاني أن يكون وقت إرتكابه للجريمة متمتعاً بالوعي والإرادة الحرّه، وهو متمتع بحرية الإختيار والتمييز، بمعنى أن لا يكون مجبراً ولا مكرهاً من أحد، وهذه الإرادة يتبعها تحمل المجرم للمسؤولية الجزائية والقانونية نتيجه أفعاله المخالفه للقانون.[3]

و يعتبر الركن المعنوي من العناصر الأساسية المكونة للجريمة ، وبناءاً عليه تترتب المسؤولية الجنائية، فالجريمة إما أن تأتي قصدية وعليها تتخذ صورة القصد الجنائي، وإما أن تكون بصورةٍ أخرى تتخذ صورة الخطأ غير المقصود.

وسنتطرق إلى كلا الصورتين كما يأتي :

---

[1] بلال أمين زين الدين : **جرائم نظم المعالجة الآلية للبيانات** ، ط1 ، دار الفكر الجامعي ، الإسكندرية ، 2008 ، ص271.

[2] عبد القادر جرادة :المرجع السابق، ص201.

[3] أمين محمد نوفل : **قانون العقوبات العام** ، كلية الشرطة الفلسطينية ، غزة ، ص8..

الفرع الأول: القصد الإجرامي في الجرائم المعلوماتية

ترتكب الجرائم الجزائية في أغلب حالاتها بصورةٍ قصدية، لذا فإن القصد الجنائي هو من أكثر صور الركن المعنوي تصوراً، وهو متمم للركن المادي بشكل خاص وللجريمة بشكلٍ عام، ويعتبر العنصر الفاصل في تحديد العقوبة، وذلك لكون عقوبة الجريمة القصدية تختلف عن الآخرى غير قصدية.[1]

ويتوفر القصد الجنائي عندما يريد الجاني الفعل الإجرامي والنتيجة، ويأتي مخالفآ لنظرية العلم التي يريد بها السلوك فقط دون نتيجة.

والحقيقة أن نظرية الإرادة أكثر واقعية من نظرية العلم، فعند إرتكاب أي مجرم للسلوك الإجرامي فهو يسعى لنيل النتيجة، ومن هنا يمكننا التمييز بين الخطأ غير المقصود والقصد الجنائي.[2]

وقد عرف المشرع الأردني النية في قانون العقوبات رقم (16) لسنه (1960) حيث نص على أن : " النية: هي إرادة إرتكاب جريمة على ما عرفها القانون."[3]

والقصد الجنائي له دور كبير في تحديد طبيعة السلوك المرتكب وماهيته والهدف منه، وذلك لتحديد النص القانوني الواجب تطبيقه، والذي يتناسب مع الجريمة المعلوماتية الواقعة، فأغلب الجرائم المعلوماتية تبدأ بخطوة واحده ألا وهي الدخول للنظام والولوج إليه، ثم ينفذ المجرم هدفه من هذا الإختراق، إما أن يكون لإتلاف المعلومات، أو سرقتها، أو تزويرها، أو نسخها، أو أي من الجرائم الإلكترونية الأخرى، فإذا لم يثبت الهدف من وراء الإختراق والولوج هنا نكن بصدد دخولٍ غير مشروع.[4]

---

[1] العفيفي يوسف خليل يوسف: **الجرائم الإلكترونية في التشريع الفلسطيني** ، رسالة ماجستير في القانون العام ، كلية الشريعة والقانون ،الجامعة الإسلامية ، غزة ، 2013 ، ص57.

[2] سرور أحمد فتحي : **المرجع السابق**، ص 530 ،531.

[3] مادة63 ، **قانون العقوبات الأردني** ، رقم 16 سنة 1960 ، مشار إليه في الموقع الرسمي للتشريعات الأردنية ، ديوان التشريع والرأي ، http://www.lob.gov.jol. تاريخ الإطلاع 2019/05/09

[4] الحسيناوي علي جبار : المرجع السابق ، ص39.

وتبرز أهمية القصد الجنائي في الجرائم المعلوماتية في تحديد جريمة الدخول غير المشروع، وجريمة تجاوز الصلاحيات المسموح بها، فالأولى القصد الجنائي فيها واضحاً وهو الدخول للأنظمة وهذا في حد ذاته جريمة يعاقب عليها القانون، فالقصد فيها الدخول والإختراق والولوج، أما بالنسبة للثانية فيكون للمخترق صلاحية الدخول للنظام لكنه تجاوز حدوده وصلاحيته والأماكن التي سمح له بالدخول إليها.[1]

واكتفى القضاء الأمريكي بالأخذ بالقصد العام في جرائم التهديد مثل التهديد عبر البريد الإلكتروني مع عدم الممانعة بالأخذ بالقصد الخاص، وهذا على خلاف المشرع الفرنسي الذي إفترض وجود قصد خاص في الجرائم الإلكترونية، فقد إشترط الإعتداء على الحياة الخاصه في الجرائم التي تتعلق بسرية الإتصالات، ومن ذلك البريد الإلكتروني كونه يعد من وسائل الإتصال الحديثة الخاصة.[2]

ومما سبق يمكن القول بأن الجرائم المعلوماتية لطبيعتها فإن أغلبها يرتكب بشكل قصدي، لأنها تتطلب معرفة كبيرة من الجاني بالحاسوب والإنترنت والتعاطي مع المعلومات والبيانات، فهي غالباً لا ترتكب إلا من قبل خبير أو من لديه علم كافي بالجريمة أو شخص متخصص، فهذا الخبير أو المتخصص من بداية جلوسه أمام الحاسب الآلي يسعى لتحقيق هدفه أو غايته المنشودة.

في بعض الأحيان قد يدخل الشخص موقعاً محظوراً الدخول والبقاء فيه، وهو على علم وتفكير منه بأن الدخول إليه مشروع ومسموح البقاء فيه، ففي هذه الحالة فإن الشخص لم يرد النتيجة فينتفي عنصر القصد الإجرامي .

[1] خالد ممدوح إبراهيم : **المرجع السابق**، ص393.

[2] الحسيناوي علي جبار: **المرجع السابق** ، ص39

الفرع الثاني: الخطأ غير المقصود في الجرائم المعلوماتية:

أفترض المشرع الفلسطيني حسن نية للشخص مرتكب السلوك بأنه لم يرد النتيجة، وأن لا يتحمل أي مسؤولية جنائية عن ما أقترفه من خطأ، إلا إذا جاء نص صريح يلغي هذه القاعدة.

فقد ذهب المشرع الفلسطيني إلى أنه تقرر المسؤولية جزائية عن الخطأ الإ بنص صريح على خلاف ذلك، وأن يتمتع الجاني بكامل القوى العقلية والإرادة، لأن الجاني أراد السلوك و لما يرد النتيجة.

وأيضاً فإن المشرع الأردني نص على صور الخطأ غير المقصود في المادة 64 من قانون العقوبات على أن: "يكون الخطأ إذا نجم الفعل الضار عن الإهمال أو قلة الإحتراز أو عدم مراعاة قوانين وأنظمة"[1].

وما يمكن إستنباطه من النصوص العقابية للجرائم المعلوماتية ،هو إحتمالية وقوع الخطأ أو الجهل في الجرائم المعلوماتية، فعلى سبيل المثال الدخول غير المشروع لموقع إلكتروني، فإنه يمكن الإحتجاج بالجهل والخطأ فقد يكون المستخدم ما زال جديداً، أو لم يملك العلم بعدم مشروعية الدخول والبقاء بهذا الموقع، أو ظناً منه أن الدخول إليه مباح.[2]

وتعد جريمة عدم الإبلاغ عن أنشطة غسيل الأموال أو التقصير في الكشف عنها، وجريمة الإخلال بالإبلاغ عن الأنشطة المصرفية أو البنكية المشبوهة، والتي كان من المفترض التبليغ عنها، فهذه جرائم إرتكبت بسبب إهمال أو تقصير ولا تعد من الجرائم

---

[1] المادة 63 ، **قانون العقوبات الأردني** ، رقم 16 سنة 1960 ، مشار إليه في الموقع الرسمي للتشريعات الأردنية ، ديوان التشريع والرأي ، http://www.lob.gov.jol. تاريخ الإطلاع 2019/05/09

[2] الروقي مروان مرزوق : **القصد الجنائي في الجرائم المعلوماتية** ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، السعودية ، 2011 ، ص121.

العمدية، لكنها رغم ذلك توقع مسؤولية جزائية وتأديبية ومدنية على من أهمل في واجبه، وخاصه من كان في عمل رسمي.[1]

الفرع الثالث: أمثلة على الركن المعنوي في الجرائم المعلوماتية

أولاً: جريمة تزوير بطاقات الإئتمان: إن توافر الركن المعنوي من خلال قيام الجاني في هذه الجريمة باللجوء الإ تغيير الحقيقة في البطاقات الإئتمانية، وهو على علم تام بكافة أركان التزوير، ويلحق الضرر بشخص أو بكافة الأفراد في المجتمع، وهذا هو القصد العام، والقصد الخاص للجاني هو إستعمال البطاقة المزورة، لإجراء عمليات سحبٍ غير مشروعة .[2]

ثانياً: جريمة الإتلاف الإلكتروني: يتكون القصد الجنائي في هذه الجريمة من عنصرين العلم والإرادة، فإذا قام شخص بإتلاف بيانات بشكل عمدي، واتجهت إرادته لهذا الفعل وهو على علم كامل بأن عمله غير مشروع توافر هنا في حقه القصد الجنائي، وعلى عكس ذلك إذا أتلف شخص بيانات طلب منه ذلك وكان من الواجب عليه إتلافها، فلا نكن هنا بصدد جريمة الإتلاف الإلكتروني[3].

ثالثاً: جريمة الذم: يكفي لإثبات هذه الجريمة يكفي علم الجاني بالألفاظ التي خرجت منه وأن القانون يعاقب عليها، فيكفي لإثباتها القصد العام لأنها تعتبر من الجرائم العمدية، وأن إرادته توجهت لذلك عن طريق خروج هذه الألفاظ منه بغض النظر عن الوسيلة، سمعية كانت أو كتابية أو أي وسيلة من وسائل التواصل الإلكتروني.[4]

---

[1] يونس عرب : **صور الجرائم الإلكترونية** ، مقدمة لورشة عمل بعنوان "تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية " ، مسقط ، سلطنة عمان ، 2-4 أبريل ، 2006 ، ص32.

[2] البغدادي كميت طالب: **الإستخدام غير المشروع لبطاقات الإئتمان** ، ط1 ، دار الثقافة للنشر والتوزيع ، عمان ، 2008 ، ص196.

[3] نايير نبيل عمر : **الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية** ، دار الجامعة الجديدة ، الإسكندرية ، 2012 ، ص102.

[4] يوسف حسن يوسف : **الجرائم الدولية للإنترنت** ، ط1 ، المركز القومي للإصدارات القانونية ،القاهرة ،2011 ، ص208.

رابعاً: جريمة السرقة الإلكترونية: تعد جريمة السرقة من الجرائم القصدية والتي تعتمد على العلم والإرادة ، وأجمع الفقهاء على توافر قصد خاص بجانب القصد العام، والمتمثل في قيام نية الجاني على تملك البيانات أو المعلومات المسروقة، فإذا قام شخص بسرقة قرص ممغنط أطلع على محتواه ثم أرجعه، انتفى عنه القصد في تملك المال الإلكتروني ، وأصبحت الجريمة هنا جريمة حيازة، بمعنى يجب توافر القصد الخاص في نية الجاني بتملك المال الإلكتروني المسروق.[1]

ومما سبق يمكن القول بأن أهمية الركن المعنوي تنبع من إمكانية تحديد نوع الجريمة والجزاء الجنائي المترتب عليها.

المطلب الثالث: الركن الشرعي في الجريمة المعلوماتية

إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان، وتختلف هذه الأفعال حسب إختلاف نشاطات الإنسان ، وهذا ما دفع المشرع للتدخل و تجريم هذه الأفعال وتحديد الفعل الضار من غيره، وتحديد المجرم والعقوبة المقرره لإرتكابه.[2]

"لا جريمة ولا عقوبة أو تدبير أمني بغير نصٍ قانوني"[3]،هذه القاعدة هي الأساس في مبدأ الشرعيه، والتي تعني عدم رجعية القانون الجنائي، أي لا يمكن معاقبة ومحاسبة الشخص على فعلٍ إرتكبه طالما لم يوجد نص يجرم فعله.

وأهم ما يميز هذا المبدأ عن غيره، هو أن القاضي عند تفسيره للنصوص القانونية فإنه يلجأ للتفسير الضيق، فيلجأ القاضي إلى الإبتعاد عن القياس، بمعنى عدم اللجوء لقياس فعلٍ لم يجرمه القانون على فعلٍ وردت نصوص تجرمه وتعاقب عليه.

---

[1] العريان محمد علي : **المرجع السابق** ، ص140.

[2] أحسن بوسقيعة : **الوجيزفي القانون الجزائي العام** ، ط10 ،دار هومه ، الجزائر ،2011 ، ص27.

[3] المادة 1 ، الأمر رقم 66-155 المؤرخ في 18/صفر عام 1386 الموافق 08/يونيو/1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم، والقانون رقم 2015/19 المؤرخ في 18/ربيع الأول/1437 الموافق 30/ديسمبر/2015.

وبعد ظهور الإنترنت إزداد التطور في ظاهرة الإجرام وخاصه التطور الملحوظ في الجرائم الإلكترونية، وقد إختلفت الدول في تحديد التقنية التشريعية، فأنشأ لها قانون جنائي للمعلوماتية مستقل بذاته، وآخرون أدمجوا النصوص العقابية للجرائم المعلوماتية في قانون العقوبات التقليدي.

وقد رأى بعض الفقهاء الإخلال بالأساس القانوني بحيث أن المشرع طلب في الجرائم العاديه الركن المادي بالسلوك المعين، وهذا يختلف عن السلوكيات في الجرائم المعلوماتية.

والإتجاه الأخر يرى أن الجرائم المعلوماتية ما هي الإ جرائم عاديه تقام عن طريق الحاسب الإلي أو الإنترنت، فيطلب من المشرع تطبيق العقوبة العاديه عليه بتكييف النصوص القانونية.

وتركز إختلاف الفقهاء على نقطتين أساسيتين هما: المصطلحات والموقع والتي يمكن تلخيصهما بالتالي:

1-المصطلحات: بسبب ما يميز الجريمة المعلوماتية من طابعٍ تقني، فأوجدت مشكلة المصطلحات التقنية التي تعتبر لغة غامضة بعيدة عن لغة القانون.

وبالنسبة لهذه الإشكالية التي طرحها الركن الشرعي للجريمة المعلوماتية فيختلف موقف التشريعات في تحديد تعريف المصطلحات التقنية، ففي الدول الأنجلوساكسونية التي تعتمد على طريقة إعطاء تعريفات في صلب الموضوع، أما الطريقة الفرنسية توكل مهمة تحديد المصطلحات للقضاء، وهي الطريقة المفضلة نتيجة لسرعة التطور في تقنيات الإعلام الآلي وإمكانية مواكبة القانون الجنائي لهذا التطور.[1]

وبدأت المحاولة في فرنسا عام 1985 حين تقدم وزير العدل بمشروع قانون العقوبات الجديد أضاف الى الكتاب الثالث منه باب رابع بعنوان "الجرائم المعلوماتية" والذي

[1] القهوجي علي عبد القادر: **الحماية الجنائية لبرامج الحاسب الإلي**، الدار الجامعية للطباعة والنشر، بيروت، 1999، ص24.

تكون من ثمانية مواد، يتضمن تجريم كل من ألتقط برامج أو معطيات أو أي عنصر أخر من النظام المعلوماتي عمداً واستخدم برامج أو عناصر ومعطيات دون إذن من اصحابها، وتخريب كل أو جزء من المعطيات الآلية وعرقلة لأدائه كوظيفة والحصول أو السماح بالحصول على فائده غير مشروعه عن طريق الإستخدام غير المشروع للمعطيات الآلية، ولكن بقي هذا المشروع حبرآ على ورق ولم يرى النور أبدا.[1]

وبعد ذلك تقدم الى الجمعية الوطنية الفرنسية النائب (Jacque) مع بعض النواب بمشروع قانون في الغش المعلوماتي، وكان هذا الإقتراح مجرد تعديل وتطويع بعض الجرائم التقليدية مثل السرقة والنصب وخيانة الأمانة والإخفاء والتخريب والإتلاف والتزوير وإستعمال المحررات المزورة، ولكن بعد نظر البرلمان الفرنسي لهذا الإقتراح، دارت حوله مناقشات طويلة ومعمقة ،وأدخلوا عليه تعديلات جوهرية وتم إقراره في شكل جديد.[2]

2-الموقع: ثار الإتجاه الأول الى إمكانية إدماج النصوص القانونية المتعلقة بالجرائم المعلوماتية في قانون العقوبات التقليدي، فإمكانه إدماجها إلى جرائم الأموال بإعتبار إمكانية إضفاء صفة المال على الكيانات المادية للحاسوب.

ويرى البعض الأخر بما أن مكونات الحاسوب هي مكونات مادية يمكن تملكها، والكيان المعنوي يدخل في إطار الملكية الفكرية، فيرى أنه من الأفضل دمجهما في إطار الجرائم ضد الملكية.

والإتجاه الثالث يرى أنه من الأفضل وضع قوانين مستقلة متتعلقة بالجرائم المعلوماتية، كونها تتعلق بقيمة خاصه.

---

[1] القهوجي علي عبد القادر : **المرجع السابق**، ص35.

[2] القهوجي علي عبد القادر: **المرجع نفسه** ، ص35.

المبحث الأول: الجرائم الموجهة ضد نظم المعلوماتية عن طريق الانترنت وطرق إثباتها

المطلب الأول: أنواع الجرائم المعلوماتية

أدى التطور الكبير في تكنولوجيا المعلومات الى تطور ظاهرة الجريمة المعلوماتية في المجتماعات الإنسانية، فقد أصبحت جرائم المعلومات تمثل مجموعة من الأنماط الإجرامية التي تتم عبر أنواع تكنولوجيا المعلومات المختلفة، سواء تلك التي تتمثل بتكنولوجيا التخزين و الإسترجاع أو المتجسدة بتكنولوجيا الإتصالات الحديثة وخاصة الإنترنت، ولكشف النقاب عن الجرائم المعلوماتية وإمتدادها من خلال تسليط الضوء على أهم أنواعها[1]، ومنها ما يلي:

– الجرائم التي ترتكب بوساطة وسائل إلكترونية كأداة لإرتكاب الجريمة مثل جرائم القدح والسب وكما هوالحال بالتهديد.

– جرائم التي تستهدف الوسائل الإلكترونية أو محتوياتها كما هو الحال في تدمير نظام المعلومات أو سرقة المعلومات أو التعدي على الخصوصية والسرية.

الفرع الأول: أنواع الجريمة المعلوماتية

أولاً: جريمة الإرهاب الإلكتروني: هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية.[2]

وفي وقتنا الحالي أصبح الإرهاب الإلكتروني هو السائد حالياً، فأصبح إقتحام المواقع وتدميرها وتغيير محتواها والدخول على الشبكات أو العبث بمحتوياتها والإستيلاء عليها

---

[1] جاسم جغفر حسن : **جرائم تكنولوجيا المعلومات** ، ط1 ، دار البداية ، الأردن ، 2012 ، ص172 .

[2] https://ar.wikipedia.org تاريخ الإطلاع 2019/05/12.

وتعطيلها أو الدخول على شبكات الطاقة وتعطيلها لأكثر فترة ممكنة هو أحد أساليب الإرهاب للوصول إلى غرضهم.[1]

وتتجسد جريمة الإرهاب المعلوماتي في ثلاث صور:

1-الإرهاب المعلوماتي ضد الأفراد: ويقصد به أن كل ما يقوم به الفرد في تعاملاته على الإنترنت فهو مسجل في ذاكرة الجهاز الحاسب الآلي، وشهدت مجتمعاتنا العديد من حالات الإبتزاز المعلوماتي من قبل أشخاص تمكنوا بطريقة أو بأخرى من الوصول إلى هذه الذاكره التي تحمل كل صغيرة وكبيرة تتعلق بمحادثات وأفعال وبيانات تتعلق بالضحية، وكونها تتم عن بعد فهذا يساعد في الإبتزاز، سواء تقمص الرجال للنساء أو العكس للوصول للمبتغى، وهو الوصول للأسرار التي تستغل ضد الفرد.[2]

وحتى هذه اللحظه لا توجد طريقة لحماية البيانات الشخصية، فقط يكتفي الفرد بأساليب المحافظة على سرية البيانات، ولكن تبقى مشكلة أن لكل شيفرة وسيلة معينة لكسرها.

2-الإرهاب المعلوماتي ضد المؤسسات: في ظل المنافسة الكبيرة والشرسة في الأسواق التي تشهدها مجتمعاتنا، أصبح التجسس على أنشطة الشركات من قبل المنافسين مصدراً حقيقياً للقلق، فيعتبر إختراق شبكات الإتصالات والنفاذ الى قواعد البيانات التي تتضمن المعلومات الحيوية عن أنشطتها من أخطر مصادر التهديد الإلكتروني، ومن المظاهر الأخرى للإرهاب المعلوماتي ضد المؤسسات هو إسقاط مواقع تابعة للمؤسسة من خلال بعث كمية كبيرة من الرسائل التلقائية للموقع حتى

---

[1] جاسم جعفر حسن : **المرجع السابق** ، ص173 .

[2] **المرجع نفسه**، ص 176 .

يعجز عن ملاحقتها فتسقط الرسائل ويسقط معها الموقع الإلكتروني، وأيضاً فك الشيفرة السرية للبيانات التي تتبادلها المؤسسة مع المؤسسات الآخرى والأشخاص.[1]

3-الإرهاب المعلوماتي ضد الدول: يتمثل الإرهاب المعلوماتي ضد الدول بإمكانية الولوج للمرافق العامة وتعطيلها مما يسبب شلل كامل في البنية التحتية الأساسية، وأصبحت الدول متخوفة من جيوش الفايروسات التي يمكنها إختراق حدود الدول لتشييع الخراب في كافة أرجاء البنية المعلوماتية الأساسية، ويزداد تخوف الدول من هذا النوع من الإرهاب طردياً مع نسبة إعتماد الدولة على الشبكات المعلوماتية في تسيير أمورها.

ثانياً: جريمة السرقة والإحتيال الإلكتروني:

السرقة هي:" هي أخذ ممتلكات شخص آخر دون إذن هذا الشخص أو موافقته بقصد حرمانه من مُلكه والانتفاع به بغرض التمليك".[2]

ويتكون الركن المادي لجريمة السرقة من فعل الإختلاس : ويقصد به كل نشاط مادي يهدف الى نقل الشيء المسروق من الذمة المالية للمجني عليه إلى الذمة المالية للسارق".[3]

ويأتي معنى الإختلاس في الجرائم المعلوماتية في التصور بأن سلوك الجاني للإستحواذ على معلومة من حاسب الغير، بطريقةٍ آلية تخلو من العنف المادي المعروف في السرقات المادية، على أن يتوافر بين فعل الجاني والنتيجة الجرمية عنصر السبب وذلك لتكملة شروط جريمة السرقة.

---

[1] جاسم جعفر حسن: **المرجع السابق**، ص176 .

[2] https://ar.wikipedia.org تاريخ الإطلاع 2019/05/13.

[3] مراد عبد الفتاح : **شرح جرائم الكمبيوتر والإنترنت** ، الإسكندرية، د ت، ص443 .

أما الركن المعنوي ومعناه الذي يدور حول نية الجاني في حيازة الشيء، وفي الجرائم المعلوماتيه تتمثل الركن المعنوي في نية الجاني في الإستحواذ على معلومة أو برنامج أو ملف مخزن على الحاسب.[1]

ثالثاً: جرائم أمن الدولة والتجسس وجرائم الكمبيوتر والإنترنت:

تقوم حكومات بعض الدول التي تسعى من خلال الحروب الجاسوسية إلى الحصول على معلومات إستراتيجية وعسكرية وإقتصادية أخرى، إلى التجسس من خلال الكمبيوتر على تلك المعلومات لدى الدول الآخرى، ومن أشهر تلك الحروب الجاسوسية تاريخياً تلك التي وقعت بين الولايات المتحدة والإتحاد السوفييتي خلال الحرب الباردة.

ويعد مواجهة هذه الجرائم في إطار النصوص القانونية قائماً بالفعل سواء ما هو مقرر في قانون العقوبات وقوانين أمن الدولة، فإنه وبذات إطار الحماية يمكن التصدي لما يرتكب من جرائم أمن دولة والتجسس بواسطة الكمبيوتر والإنترنت.[2]

رابعاً: جريمة تضليل العقول: تكنولوجيا الإعلام المزيف.

لقد لعبت تكنولوجيا المعلومات، وتحديدا تكنولوجيا الإتصالات أكثر من دور فعال في المجتمع، فرغم لعبها دورا إيجابيآ في المجتمع الإنساني، إلا أنها فعلت كئلك سلباً في المجتمع، حيث أنها لعبت بالعقول من خلال قلب وتزييف الحقائق على أشياء غير موجودة، ومن ثم العمل على إظهارها بشكلٍ آخر، والوعود التي لا يتم تنفيذها في النهاية، والتي تجعل من المواطن يعيش حالة من التأمل والترغيب لتنفيذ هذا الوعد، ويبقى المواطن يعيش في دوامة من الوعود الكاذبة التي تضييع عليه حقائق الأمور،

[1] مراد عبد الفتاح : **المرجع السابق**، ص459 .

[2] مراد عبد الفتاح: **المرجع نفسه**، ص486 .

وكل ذلك يأتي من أجل تحقيق فئة معينة من الناس أو طبقة محددة مكاسب على حساب المواطن العام.[1]

وهذا التضليل وحده يعتبر جريمة يجب أن يحاسب عليها القانون، أو الأعراف والتقاليد، فيعمدُ مديروا الإعلام إلى نشر أفكار وتوجهات لا تتطابق مع حقائق الوجود الإجتماعي، فإنهم يخلقون وعي غير قادر على الإستيعاب بإرادته الشروط الفعلية للحياة القائمة أو يرفضها.

فالنخبة الحاكمة لا تلجأ للتضليل دائماً للحفاظ على السيطرة الإجتماعية، فالحكام يلجأون للتضليل الإعلامي عندما يبدأ الشعب في الظهور ولأول مرة كإرادة إجتماعية في مسار العملية التاريخية، أما قبل ذلك فلا وجود للتضليل بالمعنى الدقيق للكلمة، بل بالغالب ما تجد قمعاً شاملاً إذ لا ضرورة لتضليل من يكونوا غارقين في بؤس الحياة.[2]

عندما يكون التضليل الإعلامي هو الأداة الأساسية للهيمنة الإجتماعية، كما هو الحال في الولايات المتحدة، تكون الأولوية لتنسيق وتنقيح الوسائل التقنية للتضليل على الأنشطة الثقافية الأخرى .

ولتحقيق جريمة التضليل الإعلامي في المجتمع التي تمارس على هذه العملية، تعمل وسائل الإعلام والقابعة خلف التكنولوجيا على توجيه العقول نحو الخارج لمواجهة الخطر القادم من الخارج، وذلك للسعي لإهدار طاقات الناس وقدراتهم ومبالغ طائلة على مشاريع وهمية كاذبة.[3]

---

[1] جاسم جعفر حسن : **المرجع السابق**، ص177 .

[2]: **المرجع نفسه** ، ص178 .

[3] المرجع نفسه، ص179 .

خامساً: جريمة التزييف والتزوير:

نظرا لتطور ملحقات الحاسب الآلي من طابعات وماسح ضوئي وأجهزة ملونة، أدخلت هذه الأمور الحاسب الآلي لعالم التزوير والتزييف، حيث أصبح من خلاله يمكن نقل توقيع على شيك أو ايصال أو عقد، وكذلك يمكن إستخدامه في تزييف العملات الورقية والتي لا يمكن التعرف عليها الإ بخبرة فنية ومهارة عالية.

والمشكلة الحقيقية التي تواجه الأمن أن المجرمين الجدد الذين يقومون بهذا النوع من الجرائم هم من الطبقات المرموقه، سواء كانوا رجال أعمال أو مهندسي كمبيوتر أو أمناء شرطة، وإتساع دائرة التزييف والتزوير حتى أصبح من الصعب حصر القائمين بها في ظل إنتشار ملحقات الحاسوب في كل مكان وسهولة الحصول عليها، لذلك فبعض الدول تمنع دخول الطابعات الملونه والماسح الضوئي حتى تحصل على المعلومات الكافيه عن الجهة التي ستذهب إليها.[1]

سادساً: جريمة العبث بالبرامج وتعمد الأذى والتدمير:

تختلف أشكال وأنواع الجريمة المعلوماتية وهذا نظراً للإختلاف في غاية وهدف الجاني، وجريمة العبث العمد، للتدمير وتسبيب الأذى ما هي إلا عبارة عن إستخدام فايروس محدد لتدير برامج أخرى في حواسيب أخرى، والفايروس ما هو إلا برنامج تم تصميمه بهدف الدخول إلى الأجهزة وإحداث الضرر، ويَّزداد خطورة الفايروس في ظل تواجد الإنترنت، لأن الشبكة العنكبوتية تجمع الأجهزة وتربطها فيما بينها وهذا يجعل من إنتشار الفايروس أمراً يسيراً وسريعاً.[2]

---

[1] جاسم جعفر حسن، **المرجع السابق**، ص182 .

[2] **المرجع نفسه**، ص183-184 .

سابعاً: جريمة السطو على بطاقات الإئتمان:

يمكن التلاعب بها من خلال الإنترنت ويأخذ عده صور منها:

– الحصول على بطاقات إئتمانية صحيحة بناء على مستندات مزورة .

– قيام حامل البطاقة بإستعمالها بعد إنتهاء مدة صلاحيتها أو بعد تنبيه البنك عليه بعدم إستخدامها.

– عثور البعض على بطاقة مفقودة وإساءة إستعمالها.

– وقد يتلاعب موظف البنك بمعلومات البطاقة مع الإتفاق المسبق مع العميل صاحب البطاقة، أو مع عصابة إجرامية تتعامل بسرقة الأموال من البنوك عبر الإنترنت.[1]

ثامناً: جريمة الإنتحال:

جريمة الإنتحال ليست بجريمةٍ جديدة، بدليل تواجد العديد من النصوص القانونية لمعالجة هذا النوع من الجرائم، ولكن ما استجد عليها أنها أخذت منحدراً جديداً بعد تطور التكنولوجيا.

ويمكن القول بأن الإنتحال هو قيام شخص معين بنسب نتائج و معلومات وتفسيرات كان قد توصل إليها شخص آخر إلى نفسه .

تاسعاً: جريمة السب والقذف:

السب علناً هو كل سب لا يشمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشاً للشرف والإعتبار، ويمكن توقيع عقوبة على جريمة السب والقذف سواء كان علني أم غير علني بطريقة الهاتف أو عن طريق الإنترنت سواء كان بإنشاء موقع على شبكة الإنترنت لسب وقذف الشخص المعني، أو ببعث رسائل خاصة عن طريق البريد الإلكتروني.

[1] جعفر حسن جاسم : **المرجع السابق** ، ص 193.

وهنا يجب التمييز بين ثلاث حالات:

1- في حال إسناد أمور لشخص ما حتى ولو كانت صادقة لأوجبت العقاب سواء كان ذلك عن طريق رسائل شخصية عبر غرف الحوار أو بإنشاء صفحة، فهنا تعتبر جريمة قذف لتوافر عنصرين هما القذف والعلانية، وعنصر العلانية حتى ولو لم يتم إستعمال الميكروفون ،فالجهر متوقف على الكتابة على الشبكة.[1]

2- في حالة القذف التي تتم عبر البريد الإلكتروني للشخص المعني، فيفتقد عنصر العلانية هنا نظراً لخصوصية الرسائل الشخصية، ولكن تعتبر جريمة قذف معاقب عليها عن طريق التيليفون، وذلك لأن غالباً44 ما يكون الإتصال بالشبكة عن طريق إستخدام التيليفون.

- أما بالنسبة للسب عن طريق إستخدام شبكة الإنترنت فيتحقق في حالة إذا ما تم فعل السب أثناء تواجد الشخص داخل غرف الحوار أو تم إنشاء الموقع على الإنترنت تتضمن أقوالاً بحق شخص معين.

عاشراً: جريمة المساعدة على الإنتحار:

يلقي القانون مصطلح مجرم على كل من إرتكب فعل إجرامي أو ساعد على إرتكابه، ويمكن الملاحظة خلال التطور التكنولوجي الكبير الذي نمر به، وأنه قد قدمت لنا الإنترنت العديد من الخدمات الإيجابية، وذلك لا يتنافى مع وجود العديد من السلبيات لديها، ولكن من أبرز هذه السلبيات، تقديم اليابان لخدمات عن طريق الإنترنت لتسهيل قتل النفس(الإنتحار) لكل من يرغب بذلك، مقابل مبلغ من المال،

[1] جاسم جعفر حسن: **المرجع السابق** ، ص196 .

وقد ساعدت إمراة على قتل نفسها والعديد من الاشخاص الذين يطلبون مواد قاتلة عن طريق الإنترنت.[1]

وقام أحد الأشخاص بالدخول للبيانات الخاصه بقاعدة المستشفى الذي يعتني بزوجته به، وقام بتغيير كميات الجرعات العلاجية ونوع الدواء وعندما أقدمت الممرضه على إعطائها الدواء أودى ذلك بحياتها، و تعد الممرضة وسيلة مادية لا قصد لها.

إحدى عشر: جرائم الجنس و العِرض عبر الإنترنت :

ومن الأثار السلبية للإنترنت وجود مواقع ومنشوارات تحض على ممارسة الجنس مع البالغين أو مع صغار السن، سواء على شكل صور أو مقاطع فيديو إباحية ساخنة، فهي لا تشكل مشكلة أمام البالغين الذين يتمتعون بالعقل التام والتفكير السليم، ولكن الخوف على من هم دون سن الرشد والذين يفتقرون للتفكير الكامل السليم وتحديد الأبعاد الخطيرة لهذه الأفعال، فقد يعملون على إغرائهم بصورة ساخنه لممثلين تم وضع صور وجوههم على أجساد أخرى، وقد يصل الأمر لتبادل الحديث وينتحل المجرم شخصية فتاة صغيره وذلك لخداع الفتى وجره الى طريق السوء أو لطلب مقابلتة حتى يمكنه القيام بفعلته.[2]

ويمكن للقاصر الإنحراف من خلال إشتراكه في غرف للدردشة الجماعية، أو المحادثة عبر البريد الإلكتروني مع حسابات وهمية تشجع على إرتكاب الجريمة الجنسية.

---

[1] جاسم جعفر حسن: **المرجع السابق**، ص202 .

[2] **المرجع نفسه** ،ص ص202 -203.

المطلب الثاني

الإثبات في الجرائم المعلوماتية

يقصد بالإثبات" إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية، وذلك بالطرق التي حددها القانون ووفق القواعد التي أخضعها لها"[1].

ويتضح أن فكرة الإثبات هي فكرة مركبة، إذ هي قابلة لأن تتحمل أكثر من وجه، ولكل وجهٍ منها معناه المتميز ومشاكله الخاصه، وتعتبر مهمة قواعد الإثبات هي تحديد ما هو لازم وما هو جائز وما هو محظور في ذلك كله.[2]

وللإثبات أكثر من وجه للنظر إليه فالنتيجة التي يسفر عنها الدليل أو البرهان، وهذه النتيجة إما الإدانة أو البراءة، ويثير هذا الوجه مسألة تحديد مناهج الإستدلال القضائي المؤدية لهذه النتيجة، ومن ناحية ثانية يمكن النظر إليه من ناحية "طرق الإثبات" أو الوسائل التي يتوسل بها أطراف الدعوى للتدليل على حقيقة واقعة، وهو وجه يثير مسألتين رئيسيتين: الأولى تحديد طرق الإثبات المقبولة في المواد الجنائية، والمسألة الثانية هي تحديد القيمة القانونية لكل دليل من تلك الألة[3].

ويمكن النظر إلا الإثبات من ناحية إقامة الأدلة، أي البحث عنها وتقديمها أمام سلطات التحقيق وقضاء الحكم، بل وأمام سلطة الإستدلال أيضاً، أي وضع العناصر

---

[1] .محمود نجيب حسنى : **شرح قانون الإجراءات الجنائية** ،دار النهضة العربية ، القاهرة، ط2 ،1988 ، ص405.

[2] محمد زكي أبو عامر : **الإثبات في المواد الجنائية** ،الفنية للطباعة والنشر ، الإسكندرية ،1985 ، ص 19 .

[3] سعيد عبد اللطيف حسن : **الحكم الصادر بالإدانه ،دراسة قانونية لنظم الحكم الجنائي وفلسفته والعوامل المؤثرة في إصداره في ضوء إتجاهات السياسة الجنائية المعاصرة** ، ط1، دار النهضة العربية ،االقاهرة،1989 ،ص47.

التي تتأسس عليها الواقعة من حيث وقوعها ونسبتها إلى مرتكبها تحت نظر القضاء، وهو ما يتضمن إجراءات البحث عن الأدلة، وهو معنى يثير مسألة التعرف على الإجراءات اللازمة أو الجائزة أوالمحظورة التي تحكم عملية البحث عن الأدلة وتقديمها إلى القضاء[1].

رغم إعطاء المشرع السلطة الواسعة للقاضي الجنائي بقبول الدليل وتقديمه، فقد قيده من حيث القواعد التي تبين كيفية الحصول عليه والشروط المتطلبة فيه، وتعتبر مخالفة هذه الشروط إهدار لقيمته و مستحيل على القاضي الأخد به، وإن كان مقتنعاً بما يستخلص منه، ويعني ذلك أن المخالفة لهذه القواعد تصيب عمل القاضي بالخلل وتصف قضائه بالبطلان.[2]

تتسم جرائم الإنترنت بصعوبة إثباتها وإكتشافها ،وترجع صعوبة إثبات تلك الجرائم إلى خصائص تقنية المعلومات ذاتها، وخاصة السرعة العالية التي ترتكب بها، وهو ما يسهل إرتكابها وطمسُ آثارها ومحو الأدلة التي تدين مرتكبها، إذ يستطيع أن يرتكب الجريمة دون أن يترك وراءه أي أثر ملموس، واذا كان دليل يدل على إدانته فإنه يستطيع تدميره ومحوه في ثواني معدوده، وخاصه أن المجرم المعلوماتي يتميز بالذكاء والدهاء والمهارة التقنية العالية، ومعارف فنية في مجال المعلوماتية وأنظمة الحاسب الآلي، وهو على دراية بلغة التخزين والأسلوب والتشغيل وقدرته على إستدعاء المعلومات، بل وقد يكون من الاختصاصيين في مجال تقنية المعلومات.[3]

---

[1] محمد زكي أبو عامر : **المرجع السابق** ،ص17-18.

[2] سليمان أحمد فضل : **المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية** ، دار النهضة العربية ، القاهرة ، 2013 ،ص353

[3] محمد محي الدين عوض : **مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات**، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي في القاهرة ،25-1993/10/28 ، دار النهضة العربية ،القاهرة ،1993 ،ص476 .

وفي هذه الجرائم تصطدم أجهزة العدالة الجنائية بتكتيك معلوماتي غيرمسبوق، سواء كمحل للجريمة أو كوسيلة مستحدثة لإرتكابها، وهو قدرة المجرمين على إستحداث وسائل مبتكرة على الدوام مثل برامج الإختراق وبرامج الفايروسات، حيث يغلب أن تكون السلطات القائمة على جمع الأدلة والتحقيق والإدعاء والقضاة أنفسهم لا تتوفر لديهم معرفة فنية وتقنية للتعامل مع مثل هذا النوع المعقدِ من الجرائم، ومن الأدلة على ذلك قيام المحلفين في قضية روبرت موريس الخاصة بإختراق شبكات الكمبيوتر في الولايات المتحدة الأمريكية 1988 أقروا بأنهم لا يعرفون شيئآ عن الكمبيوتر.[1]

ويمكن تقسيم ضوابط وعناصر الإثبات في الجرائم المعلوماتية آلى:

الفرع الأول: ضوابط إثبات الجريمة المعلوماتية بالأدلة الرقمية والعلمية :

يحتاج إثبات جريمة معلوماتية إلى دليل رقمي لإثبات الإختراق والتعدي على البيانات سواء بتزويرها أو إتلافها أو سرقتها، والدليل العلمي يتطلب إستخدام طرقٍ غير تقليدية في الإثبات، والدليل العلمي يقصتر على إجراء تجارب علمية ومعملية على جهاز الحاسب الآلي الذي أُستخدم في الإختراق والتعدي، وذلك لدعم دليلٍ قدم سابقآ سواء لإثبات الجريمة أو نفيها.[2]

ولإجراء هذه التجارب يحتاج إلى محقق جنائي وفني متخصص لديه مهارات فنية وتقنية لإستخلاص الأدلة الرقمية، لأن في هذه الحالة الفصل في الدعوى الجزائية، يتوقف على الرأي الفني الذي يثبت أو ينفي حدوث الواقعة [3].

---

[1] سليمان أحمد فضل : **المرجع السابق** ،ص357 .

[2] عبد الفتاح بيومي حجازي :**الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، دراسة معمقة في جرائم الحاسب الآلي والإنترنت** ، دار الكتب القانونية ، القاهرة ،2005 ، ص49-50 .

[3] محمود نجيب حسني : **المرجع السابق** ، ص474.

والدليل العلمي هو نتيجة التي تسفر عنها التجارب العملية والمعملية، والتي تثبت أو تنفي واقعة ثارت الشكوك حولها، وهو لا يعدو كونه رأيآ فنيآ يعتمد على خبرة ومهارة فني تقني يحدد ما إذا كان الإختراق قد تم من جهاز المشتبة به أم لا.[1]

إن واقع التقدم العلمي يدفعنا للإستعانه بخبراء وفنيين ومختصيين تقنيين، لدراسة الوقائع المختصه ومتعلقة بالجريمة ونسبتها للمتهم، وهي في تعد قرائن لا تصل مكانة الدليل، لكنها تعتبر كإحدى طرق الإثبات كالقرائن.[2]

والقول بإن الخبرة ورأي المختصيين ما هي الإ قرائن، ولا يعتد بها كوسائل للإثبات الجريمة المعلوماتية، تضفي صعوبة أخرى لصعوبات إكتشاف المجرم وتحديده في ضوء عدم التسليم بالأمورالتي تحكم الدليل الرقمي في الفكر الجنائي خارج نطاق تلك الجرائم.[3]

وأدت الصعوبات في كشف الجرائم المعلوماتية وصعوبة تحديد مرتكبها إلى الإستعانة بوسائل وأدوات يعمل الخبراء على تطويرها ل تجاري التطور السريع للجريمة المعلوماتية، ويمكن القول بأن الأدوات العلمية لإثبات الجريمة هي "أدوات تقوم بضبط الجريمة كباقي برامج الحماية، وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، والتصنت على الشبكات، وتقارير تنتجها نظم أمن البيانات، ويمكن إستخدام الأدوات المستخدمة في الجريمة، كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين للموقع".[4]

---

[1] محمد حماد الهيتي : **جرائم الحاسوب وماهيتها وموضعها واهم صورها** ،دار المناهج للنشر والتوزيع ،عمان ،2005 ،ص232 .

[2] عبد الفتاح بيومي حجازي : **المرجع السابق** ،ص51 .

[3] محمد حماد الهيتي : **المرجع السابق** ،ص233-234 .

[4] محمد علي العريان : **الجرائم المعلوماتية** ،الدار الجامعية الجديد للنشر ، الإسكندرية ،2004 ، ص44-45 .

وتكون هذه البرامج والتقنيات التي تستخدم في إثبات الجريمة المعلوماتية بالأدلة العلمية نتئجها محكومة بقواعد معينة حسب طبيعتها ومنها:

1-برامج الحاسب الآلي:

من خلال عمليات التحري الإلكتروني يمكن إستخدام برامج إسترجاع البيانات من الأقراص التالفة، وبرامج كسر كلمة المرور، وبرامج الضغط وفك الضغط، وبرامج البحث عن الملفات المخفية والعادية، وبرامج منع الكتابه على القرص الصلب التي تحمي مسرح الجريمة، وكذلك يمكن إسترجاع البيانات التي يلجأ المجرم إلى مسحها لإخفاء الأدلة، وتظهر دورها عند إتباع الإجراءات العلميه والفنية للتحري، حيث تمنع من تغيير المواد والبرامج المستخدمة في الإختراق والتعدي وإرتكاب الجريمة.

2- برامج فحص ومراقبة الشبكات:

وهي البرامج التي تستخدم لفحص البروتوكول لمعرفة المشاكل المتعلقة بالشبكات والعمليات التي تعرضت لها، وترجع فاعليتها على قدرتها الهائلة في الدخول للشبكات، وتلمس برامج السرقة والتلصص، وكذلك الفايروسات التي تستخدم في عملية الإختراق والتعدي والتزوير، وتحديد مصدرها بدقة.[1]

3- برامج تتبع الإختراق الموجود على شبكة الإنترنت:

تستخدم هذه البرامج برتوكولات معينة للتعرف على البرامج التي إستخدمت للإختراق والتعدي من خلال تحديد موقع الإختراق، وترجع قدرتها الفعالة على إمكانيتها الفائقة في إكتشاف الـ (IP) الخاص بالجاني داخل الشبكة، فهي ذات قدرة أعلى على التوغل في الشبكات الخارجية.[2]

---

[1] ثنيان ناصرآل ثنيان : **إثبات الجريمة الإلكترونية** ، رسالة ماجستير تخصص السياسة الجنائية ،بإشراف د.جلال الدين محمود صالح، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية ، 2012 ،ص77 .

[2] ممدوح عبد الحميد عبد المطلب : **جرائم إستخدام الحاسب الإلي وشبكة المعلومات العالمية:الجريمة عبر الإنترنت** ، مكتبة دار الحقوق، الشارقة ،2001 ،ص220 .

4-برامج فك الشيفرات:

من أهم فوائد الشفير أنه يقي من كشف التنصت على حزم المعلومات الخاصة بالمنظمات، فالتشفير هو الحصول على معلومات وبيانات مبهمة وغير مفهومة،إلا أن هناك برامجها يمكنها فك الشيفرات، وبصفة خاصة للبرامج والمواقع التي تقوم بعملية الإختراق والتعدي والتزوير، وهذه البرامج تحتوي على مليارات من الشيفرات، وتقوم بأستغلال الحاسب الآلي لتجربة هذه الشيفرات في ثواني معدودة، حتى تقوم بفتح هذا الموقع المشفر ومتابعته ومعرفة إذا ما تم إستخدام هذا الموقع في الإختراق أو التعدي.[1]

الفرع الثاني: ضوابط إثبات الجريمة المعلوماتية بالأدلة الإجرائية:

هي الأساليب التي تستخدم لإثبات وقوع جريمة وتحديد شخصية مرتكبها، وتعتبر من الأساليب ذات الفعالية في التحقيق الفني، حيث تسهم في إثبات الجريمة وبيان الغموض وإيجاد العلاقة بين الجاني والمجني عليه من قبل المحقق الفني، بإستخدام تقنيات وبرامج التتبع والتفتيش والضبط الإلكتروني، التي تتمتع بقدرة فائقة على التتبع والإسترجاع للبرامج والأدوات التي إستخدمت في التعدي أو الإختراق و إرتكاب الجريمة[2]، ويمكن تحديد هذه الضوابط بالشرح المختصر من خلال:

أولاً: الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته:

يجب على المحقق الفني الإطلاع على قاعدة البيانات والنظام المعلوماتي ومكوناته، ومعرفة الوقت المخصص لكل مستفيد في حال وجود اكتر من مستخدم، واسلوب

---

[1] ممدوح عبد الحميد عبد المطلب : **المرجع السابق**،ص220 .

[2] ثنيان ناصرآل ثنيان : **إثبات الجريمة الإلكترونية** ، رسالة ماجستير تخصص السياسة الجنائية ،إشراف د.جلال الدين محمود صالح، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية ، 2012 ،ص78-79 .

النسخ الاحتياطي و برامج الحماية المتوافرة [1]، وتتم عملية الإطلاع على عملية النظام المعلوماتي من خلال:

1-الإستعانه بالبرامج التحليلية الحديثة:

يمكن الإستعانة من هذه البرامج في حصر الحقائق والإحتمالات و الأسباب والفرضيات، وإستنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي، وفق برامج لتغطية كافة الإحتمالات وتقديم الإحتمال الأقوى.[2]

2-التوقيف خلال فترة التحقيق:

هو سلب المتهم الذي تدور حوله شبهات قوية لإرتكابه جريمة إلكترونية حريته، خلال فترة التحقيق حسب مقتضيات التحقيق ومصلحته، وهو إجراء من إجرائات التحقيق يطلق عليه مسمى الحبس الإحتياطي، ينتهي إما ببراءة المتهم أو إصدار عقوبة موقعة عليه، والهدف من تقييد حريته هو الخوف من إستغلال مهارته العالية في طمس أثار الجريمة المادية والإلكترونية[3].

ثانياً: إظهار الحقائق المتعلقة بالجريمة:

يتوجب على المحقق إظهار الحقائق خلال مرحلة جمع الإستدلالات الإلكترونية، والعمل على إثباتها في محضره نظرا لأهميتها في إثبات الجريمة، ويتوجب عليه رسم خطوات للبحث، من خلال إظهاره و تحديده لأركان الجريمة من خلال التطرق والبحث وإكتشاف وتحديد مكان وقوع الجريمة ووصفه، تحديد وقت وقوع الجريمة، الأسلوب

---

[1] محمد علي العريان : **الجرائم المعلوماتية** ،الدار الجامعية الجديد للنشر ، الإسكندرية ،2004 ، ص81 .

[2] محمد الأمين البشري : **التحقيق في جرائم الحاسب والإنترنت** ، المجلة العربية للدراسات العربية والتدريب ،العدد30 ،الرياض، 2001، ص186 .

[3] ثنيان ناصرآل ثنيان: **المرجع السابق**، ص79 .

المستخدم لإرتكاب الجريمة، الأداة المستخدمة في الجريمة، إبضاح الظروف المحيطة بالجريمة و تحديد دوافع الجريمة [1].

الفرع الثالث: عناصر إثبات الجريمة المعلوماتية:

أولاً: إظهار الركن المادي للجريمة المعلوماتية:

إن النشاط والفعل المادي في الجرائم المعلوماتية يحتاج الى الإتصال بالإنترنت ووجود بيئةٍ رقمية، ويتطلب أيضآ معرفة بداية هذا النشاط والشروع فيه والنتيجة، فيقوم مثلآ المجرم بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، و يلزمه القيام ببعض الأعمال التحضيرية مثل تحميل برامج للإختراق أو القيام بتجهيز موقع أو صفحات تحمل في طياتها ما هو مخل بالآداب، لكن ليس كل جريمة تحتاج إلى الأعمال التحضيرية، ويصعب الفصل في الجرائم المعلوماتية بين الأعمال التحضيرية وبين البدء بالفعل، رغم أن القانون لا يعاقب على الأعمال التحضيرية، إلا أنه يختلف في الجرائم المعلوماتية، فشراء برنامج للإختراق أو برامج فايروسات أوبرامج لفك الشيفرات أو الحيازة على صور مخلة للآطفال، فهذه الجرائم في حد ذاتها تعتبر جريمة.[2]

ثانياً: إظهار الركن المعنوي:

الركن المعنوي المتمثل في الحالة النفسية للجاني وعلاقة ماديات الجريمة بشخصية الجاني، ويتحدد الركن المعنوي من خلال مبدأ الإرادة ومبدأ العلم، فالمجرم المعلوماتي يستخدم الإرادة للتخطيط للجريمة، وتارةً أخرى يستخدم العلم للقيام بجريمته.[3]

---

[1] ثنيان ناصرآل ثنيان : **المرجع السابق**، ص80-83

[2] ممدوح عبد الحميد عبد المطلب، **المرجع السابق**، ص226 .

[3] محمد علي العريان : **المرجع السابق**، ص157 .

ثالثاً: تحديد مكان ووقت إرتكاب الجريمة:

لو قام مجرم من بريطانيا بإختراق جهاز خادم لأحد البنوك في السعودية، وكان هذا الخادم موجود في فرنسا فكيف يمكن تحديد وقت إرتكابها، هل هو بتوقيت السعودية أم فرنسا أم بريطانيا؟ وهنا أيضاً يثار جدل حول تحديد مكان إرتكاب الجريمة، وبالتالي ينشأ هنا الخلاف على القانون الواجب تطبيقه، حيث تعتبر ذات بعد دولي في هذا الشأن بحيث أن الجريمة المعلوماتية هي جريمة عابرة للحدود.[1]

الفرع الرابع: طرق إثبات الجريمة المعلوماتية:

أولاً: إثبات الجريمة المعلوماتية بالشهادة:

الشهادة هي إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص لحادثة قد شاهدها أو سمعها أو أدركها بأحد حواسه بطريقة مباشرة، وهي دليلٌ شفوي يدلي به الشخص أمام السلطات المعنية.[2]

وتقسم الشهادة لإثبات الجريمة المعلوماتية إلى ثلاث انواع، الشهادة المباشرة والسماعية والشهادة بالتسامع وسنوضحها كما يلي:

1-الشهادة المباشرة:

هي قيام الشاهد بالإدلاء بشهادته أمام القضاء المختص، أو الإكتفاء بتلاوة شهادته المكتوبة، تأتي الشهادة المباشرة في الجريمة المعلوماتية بإدلاء الشاهد بما رآه من ترتيبات المجرم البرمجية التي تتعلق بإرتكاب الجريمة، أو من خلال ما شاهده من

---

[1] محمد محمد شتا : **فكرة الحماية الجنائية لبرامج الحاسب الآلي** ، دار الجامعة الجديدة للنشر ، القاهرة، سنة2000 ،ص192.

[2] فتحي بن الطيب الخماسي : **الفقه الجنائي الإسلامي** ،دار قتيبة ،دمشق، 2004 ،ص97.

المجرم بقيامه بعملية التعدي أو الإختراق للملفات الإلكترونية أو أي نوع من أنواع التزوير الإلكتروني، في هذه الحالة تعتبر الشهادة مباشرة.[1]

2-الشهادة السماعية (غيرالمباشرة):

تختلف الشهادة السمعية عن الشهادة المباشرة كونها تعتبر شهادة من شخص آخر له العلم بالأمر موضوع الجريمة، أي يشهد أنه سمع من شخص آخر واقعة إرتكاب الجريمة المعلوماتية، مثل إرتكاب أي نوع من الجرائم المستحدثة أو جرائم الإنترنت، وتعتبر هذه الشهادة من حيث قيمتها أقل درجة من الشهادة المباشرة، ولكن عند وفاة الشخص الشاهد الأصلي يأخذ بها القاضي، ويجوز للقاضي الأخذ بها أو لا ولكن لا يعتمد عليها وحدها لأنه في هذه الحالة يصبح الحكم مشوباً، فالأخذ بها هو حسب قرار وما يراه قاضي التحقيق.[2]

3-الشهادة بالتسامع :

يختلف هذا النوع من الشهادة حيث أن الشاهد يقول سمعت الناس أو سمعتهم يقولون ولكن لا يستطيع إنساب القول لأشخاص معينين، ومن ناحية قيمتها فهي ضئيلة جداً، ولا يأخذ بها في الجرائم الجنائية سواء المعلوماتية أو التقليدية ولكن يقبل بها القضاء في بعض المسائل المتعلقة بالأمور التجارية.[3]

والشهادة في الجرائم المعلوماتية يمكن الأخد بها من خلال الإستعانة بالخبراء والفنيين المختصيين في مجال الحاسب الآلي، ففي حالة عدم إلمام قاضي التحقيق بالأمور التقنية ومجال الحاسب الآلي، يتحتم عليه الإستعانه بالخبراء بهدف تأمين الحاسوب والحفاظ على الأدلة الموجودة فيه من التلف أو تعطيلها من قبل مرتكب

---

[1] ثنيان ناصرآل ثنيان : **المرجع السابق** ، ص90 .

[2] ثنيان ناصر آل ثنيان: **المرجع نفسه**، ص.90.

[3] فتحي بن طيب الخماسي: **مرجع سابق** ،ص102-103 .

الجريمة المعلوماتية، ففي هذه الحالة يتم الأخذ بشهادة الخبراء والفنيين فيما تم إرتكابه من جرائم معلوماتية معتمداً على الحاسب الآلي.[1]

ثانياً: إثبات الجريمة المعلوماتية بالإقرار:

" هو إقرار المتهم على نفسه بإرتكاب الوقائع المكونة للجريمة كلها، من خلال إقرار المتهم بكل أو بعض الوقائع المنسوبة إليه".[2]

يقسم الإقرار إلى :

1-الإقرار الشفوي:

يعتبر الإقرار الشفوي أقل قيمة من الإقرار المكتوب، فكثير من المعترفين ينكرون إعترافاتهم ويدعون أنهم قالوا ذلك تحت التعنيف والضغط، ويمكن أن يثبت بوساطة كاتب التحقيق أو كاتب الجلسة، ولا يلزم أن يكون موقعاً عليه من المتهم بل يكفي توقيع المحقق أو الكاتب.[3]

2-الإقرار المكتوب :

لا يتطلب أن يكون له شكل معين فقد يكون مكتوب بواسطة آلة كاتبة أو بخط اليد أو على شكل حديث مسترسل، ولكي يكون الإقرار مقبولاً في الإثبات، يجب أن يكون مكتوباً وموقعاً عليه من المتهم، والإقرار بشكل عام سواء كان مكتوباً أو شفوياً فأمره متروك لتقدير القاضي وإقناعه به.[4]

---

[1] ثنيان ناصرآل ثنيان: **المرجع السابق**، ص92 .

[2] جميل عبد الباقي الصغير : **القانون الجنائي والتكنولوجيا الحديثة** ، دار النهضة العربية ،القاهرة ،1992 ،ص91 .

[3] جميل عبد الباقي الصغير: **المرجع السابق**،ص.91.

[4] **المرجع نفسه**، ص92.

ثالثاً: إثبات الجريمة المعلوماتية بالخبرة الفنية:

الخبرة الفنية هي إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكان إستخلاص الدليل الرقمي منه، أو هي الإستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدة فنية أو إدارية لا تتوفر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته.[1]

المطلب الثالث: العقوبات المقررة لمرتكب الجريدة المعلوماتية :

وبإستمرار المواد والنصوص التي تتعلق بالجرائم الماسة بالأنظمة المعلوماتية في قانون العقوبات الجزائري، من المادة 394 الى 394 مكرر 7،[2] حيث نجد أن المشرع قد تبنى هذا المبدأ وسن عقوبات تطبق على الشخص الطبيعي وعقوبات تطبق على الشخص المعنوي، وسنتناولها كما يلي :

الفرع الأول: العقوبات المطبقة على مرتكب الجريمة المعلوماتية في التشريع الجزائري

أولاً: العقوبات المطبقة على الشخص الطبيعي :

1- العقوبات الأصلية للجريمة المعلوماتية :

أ- جريمة الدخول والبقاء بالغش:

[1] سلامة مأمون محمد: **الإجراءات الجنائية في التشريع المصري**، دار النهضة العربية، القاهرة، 2001، ص645

[2] الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 والموافق 8 يونيو 1966، الذي يتضمن قانون العقوبات، المعدل والمتمم.

إذا كانت جريمة الدخول والبقاء بالغش بسيطة فإن العقوبة المقررة لها هي الحبس من 03 أشهر إلى سنة ، وغرامة مالية من 50.000 إلى 200.000 كما أشارت إليها المادة 394 مكرر من قانون العقوبات الجزائري.[1]

ب-جريمة الدخول وبالبقاء بالغش:

إذا كانت جريمة الدخول والبقاء بالغش مشددة فإن العقوبة تضاعف إذا ترتب على هذه الأفعال حذف أو تغيير لمعطيات العقوبة وتصبح الحبس من06 أشهر إلى سنتين، وغرامة مالية من 50.000 إلى 150.000دج، كما أشارت المادة 394 مكرر02 و 03 من قانون العقوبات الجزائري.[2]

ج-جريمة التلاعب بالمعطيات:

نصت عليها الماده 394 مكرر 01 ق.ع.ج ، وعقوبتها الحبس من 06 أشهر إلى 03سنوات، وغرامة مالية من500.000 إلى 2.000.000 دج[3]

والملاحظ أن التلاعب بالمعطيات تفوق بعقوبتها الدخول والبقاء بالغش، سواء كانت الأخيرة بصورتها البسطية أو المشددة، وتبقى عقوبة جريمة التلاعب أكبر لانه يتوافر فيها القصد الجنائي ،على عكس الدخول غير المصرح الذي قد يفتقر لعنصر القصد.[4]

---

[1] المادة 394 منم قانون العقوبات الجزائري نصت على أنه : يعاقب بالحبس من 03 أشهر إلى سنة ، وغرامة مالية من 50.000 إلى 200.000 ، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

[1] االمادة 394 مكرر الفقرة (2.3) من قانون االعقوبات االجزائري نصت على : تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة .وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة من 06 أشهر – سنتين وغرامة من 50.000 إلى 150.000.

[3] نص المادة 394 مكرر 01 من قانون العقوبات الجزائري نصت على أنه يعاقب بالحبس من 06أشهر إلى 3 سنوات وبغرامة من 500.000دج -2000.000 كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال وعدل بطريق الغش المعطيات التي يتضمنها.

[4] .نائلة قورة : **جرائم الحاسب الآلي الإقتصادية**، منشورات الحلبي الحقوقية،2005، ص228 .

د-جريمة التعامل مع المعطيات غير المشروعة:

تعاقب الماده394 مكرر02 بالحبس من شهرين إلى 03 سنوات، وبالغرامة المالية من 1000.000 دج إلى 5000.000 دج.[1]

ثانياً: العقوبات التكميلية :

نصت الماده394 مكرر 06 على عقوبات تكملية إلى جانب الأصلية وهي :

- مصادرة الأجهزة والبرامج والوسائل المستخدمة .

- غلاق المواقع التي تكون محلا للجريمة من جرائم الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.[2]

- إغلاق المحل أو مكان الإستغلال إذا ارتكبت الجريمة بعلم مالكها،واشترط المشرع علم المالك بالافعال الخطيرة التي يقوم بها زبونه.

ثالثاً: العقوبات المطبقة على الشخص المعنوي في الجريمة المعلوماتية:

يسأل الشخص المعنوي عن الجريمة المعلوماتية سواء بصفته فاعل أصلي أو شريك بها، كما يسأل عن الجريمة التامة أو الشروع فيها، وذلك بشرط أن الجريمة ارتكبت لحساب الشخص المعنوي سواء من ممثليه أو أحد أعضائه، وتتمثل العقوبة بالغرامة

---

[1] نصت المادة 394 مكرر02 من قانون العقوبات الجزائري على أنه يعاقب بالحبس من شهرين إلى 03 سنوات وبغرامة من 1000.000دج إلى 5000.000 دج كل من يقوم عمداً أو عن طريق الغش بما يأتي:

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتثية يمكن أن ترتكب بها الجرائم المنصوص عليها بهذا القسم.

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

[2] نصت المادة 394 مكرر 06 من قانون العقوبات الجزائري على أنه مع الإحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقاً لهذا القسم علاوةً على إغلاق المحل أو مكان الإستغلال إذا كامنت الجريمة قد أرتكبت بعلم مالكها.

المالية التي تعادل خمسة أضعاف الحد الأقصى للغرامة المالية المقدرة للشخص الطبيعي.[1]

رابعاً: عقوبة الإتفاق و الشروع الجنائي للجريمة المعلوماتية:

1-عقوبة الإتفاق في التشريع الجزائري :

بالرجوع الى الماده394 مكرر 05 التي جاء في نصها أن "كل من شارك في مجموعة أو في الإتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم التي نص عليها في هذا القسم، فإنه يعاقب بالعقوبات المقررة للجريمة نفسها، أيّ إذا إنعقدت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد".[2]

2-عقوبة الشروع في التشريع الجزائري :

نصت عليه الماده 11 من الإتفاقية الدولية للإجرام المعلوماتي، وتبناه المشرع الجزائري في الماده394 مكرر 07، فالجرائم المعلوماتية لها وصف جنحي، بمعنى لا عقاب على الشروع فيها إلا بنص.[3]

الفرع الثاني : العقوبات المقررة لمرتكبي الجريمة المعلوماتية في التشريع الفلسطيني:

أولاً: العقوبات الأصلية المقررة للشخص الطبيعي:

1-جريمة الدخول غير المشروع :

عاقب المشرع الفلسطيني على هذه الجريمة في المادة 4 من قانون الجرائم الإلكترونية على كل من دخل دون وجه حق بأي وسيلة، موقعاً إلكترونياً أو نظاماً أو شبكة

---

[1] إبتسام موهوب: **جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري**، رسالة ماجستير ،إشراف أ.كوثر شريط، جامعة العربي بن مهيدي، كلية الحقوق، 2014،ص43 .

[2] إبتسام موهوب: **المرجع نفسه**، ص45 .

[3] نصت المادة 394 مكرر07 من قانون العقوبات الجزائري على أن يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.

إلكترونية أو وسيلة تكنولوجيا المعلومات..." بالحبس والغرامة لا تقل عن200دينار أردني ولا تزيد عن 1000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين، وقد شدد المشرع أنه إذا ارتكبت هذه الأعمال على بيانات حكومية يعاقب بالحبس مدة لا تقل عن 06 أشهر وغرامة من 500 دينار أردني ولا تزيد عن 2000 دينار أردني، واذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو حذفها أو إتلافها أو نقلها أو تغييرها ..." ، فإنه يعاقب بالحبس بمدة لا تقل عن سنة وبغرامة لا تقل عن 1000 دينار أردني.[1]

2-جريمة التعطيل أو إعاقة الوصول والإعتراض والتنصت بغير حق:

عاقب عليها المشرع الفلسطيني بالحبس والغرامة لا تقل عن 200 دينار أردني ولا تزيد عن 1000 دينار، وذلك بحسب نص المادة 5 من قانون الجرائم الإلكترونية، وأما من عمل على إيقافها وتعطيلها عن العمل وإتلاف البرامج وحذفها فإنه يعاقب

---

[1] نصت المادة 04 من قانون الجرائم الإلكترونية الفلسطيني على أنه: **1-** كل من دخل عمداً دون وجه حق بأن وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا المعلومات أوجزء منها أو تجاوز الدخول المصرح به أو إسستمر بالتواجد بها بعد علمه بذلك يعاقب بالحبس أو بغرامة لا تقل عن 200 دينار أردني ولا تزيد على 1000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين.

2- إذا إرتكب الفعل المذكور في الفقرة 1 من هذه المادة على البيانات الحكومية يعاقب بالحبس لمدة لا تقل عن 06 أشهر أو بغرامة لا تقل عن 500 دينار أردني ولا تزيد عن 2000 دينار أردني أو ما يعادلها من العملة المتداولة قانوناً أو بكلتا العقوبتين.

3-إذا ترتب على الدخول إللقاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو حذفها أو إضافتها أو إفشائها أو إتلافها أو تغييرها أو نقلها أو إلتقاطها أو نسخها أو نشهر أو إعادة نشرها أو ألحق ضرراً بالمستخدمين أو المستفيدين أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو شغل عنوانه أو تصميماته أو طريقة إستخدامه، أو إنتحال شخصية مالكه

أو القائم على إدارته يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين.

4-إذا أرتكب الفعل المذكور في الفقرة 03 من هذه المادة على البيانات الحكومية يعاقب بسجن لمدة لا تزيد عن **5** سنوات وبغرامة لا تقل عن 3000 دينار أردني ولا تزيد عن 5000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

بالسجن مدة لا تزيد عن 5 سنوات ومن 3000-5000 دينار اردني غرامة او ما يعادلها بالعملة المتداولة.[1]

بينما التنصت والإعتراض يعاقب بالحبس مدة لا تقل عن سنة وغرامة من 1000-3000 دينار أردني.[2]

3-جريمة فك التشفير:

يعاقب عليها بالحبس او غرامة من 200-1000 دينار اردني، ومن إستعمل بصفة غير مشروعة عناصر تشفير شخصية أو أداة إنشاء التوقيع الإلكتروني، يعاقب بالحبس مدة لا تقل عن سنة وبغرامة من 1000-3000 دينار أردني.[3]

---

[1] نصت المادة 06 من قانون الجرائم الإلكترونية الفلسطينية كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات ما من شأنه إيقافها عن العمل أو تعطيلها أو إتلاف البرامج أو حذفها أو تعديلها يعاقب بالسجن مدة لا تزيد عن 5 سنوات و بغرامة لا تقل عن 3000 دينار أردني ولا تزيد عن 5000 دينار أردني أو ما يعادلها بالعملة المتداولة قانونياً.

[2] نصت المادة 07 من قانون الجرائم الإلكترونية الفلسطيني كل من إلتقط ما هو مرسل عن طريق الشبكة أو إحدى وسائل تكنولوجيا المعلومات أو سجله أو إعترضه أو تنسط عمداً دون وجه حق يعاقب بالحبس لمدة لا تقل عن سنة وبغرامة لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين.

[3] نصت المادة 08 من قانون الجرائم الإلكترونية الفلسطيني على أنه: **1-** كل من قام عمداً بفك بيانات مشفرة..... يعاقب بالحبس أو بغرامة لا تقل عن 200 دينار أردني ولا تزيد عن 1000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

2-كل من إستعمل بصفة غير مشروعة عناصر تشفير شخصية ..... يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 دينار أردني.

3- كل من أرتكب جريمة بإستخدام الوسائل المذكورة في الفقرة 02 يعاقب بالسجن وبغرامة لا تقل عن 3000 دينار أردني ولا تزيد عن 5000 دينار أردني.

4-جريمة الإنتفاع غير المشروع من خدمات الإتصالات:

يعاقب بالحبس لمدة لا تقل عن 06 أشهر وغرامة مالية من 500-1000 دينار أردني، وإذا كان الإنتفاع قصد تحقيق الربح فشدد في ذلك بالحبس مدة لا تقل عن سنة وغرامة من 1000-3000 دينار اردني.[1]

5-جريمة عدم تقديم بيانات صحيحة للجهات المختصة عن هويته :

يعاقب بالحبس وغرامة من200-1000 دينار.[2]

6-جريمة التزوير الإلكتروني :

عاقب عليه المشرع بكل صورة واشكاله سواء كان على مستندات أو التوقيع أو غيره، بالحبس مده لا تقل عن 05سنوات وذلك حسب التزوير، وغرامة مالية تتراوح ما بين 200-5000 دينار أردني في جميع الحالات، طبقاً لنص المادة 11،12 من نفس القانون.[3]

7-جريمة السرقة الإلكترونية:

عاقب عليها بالحبس لمدة لا تقل عن سنة أو غرامة مالية من 1000-5000 دينار أردني.[4]

---

[1] نصت المادة 09 من قانون الجرائم الإلكترونية الفلسطيني على أنه كل من ينتفع دون وجه حق بخدمات الإتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها يعاقب بالحبس لمدة لا تقل عن 06 أشهر وغرامة لا تقل عن 500 دينار أردني.

[2] نصت المادة 10 من قانون الجرائم الإلكترونية الفلسطينية كل من قام عمداً عبر إستخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بنشر أو إنشاء شهادة غير صحيحة أو قدم بيانات غير صحيحة عن هويته ..... يعاقب بالحبس وبغرامة لا تقل عن 200 دينار أردني و لا تزيد عن 1000 دينار أردني.

[3] عاقب عليه المشرع بكل صورة واشكاله سواء كان على مستندات أو التوقيع أو غيره، بالحبس مده لا تقل عن 05سنوات وذلك حسب التزوير، وغرامة مالية تتراوح ما بين 200-5000 دينار أردني في جميع الحالات.

[4] كل من إستعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة الأموال أو إختلاسها يعاقب بالسجن أو بغرامة لا تقل عن 3000 دينار أردني ولا تزيد عن 5000 دينار أردني.

8-جريمة التهديد والإبتزاز عن طريق الشبكة الإلكترونية:

يعاقب عليها بالحبس لمدة لا تقل عن سنة و غرامة من 200-3000 دينار أردني[1].

9-جريمة نشر وترويج للأعمال الإباحية والإستغلال الجنسي:

عاقب عليها المشرع لمن هم فوق ال18 سنة بالحبس لمدة لا تقل عن 03 أشهر وبغرامة من 200-1000 دينار أردني، وشدد المشرع في ذلك إذا إرتكبت لمن هم دون سن ال18 بالحبس مدة لا تقل عن سنتين وبغرامه من 1000-3000 دينار أردني.[2]

ثانياً: العقوبات التكميلية

وضع المشرع الفلسطيني في قانون الجرائم الإلكترونية مثل المشرع الجزائري هذه العقوبات التكميلية وذلك بهدف المزيد من الردع، ومن أجل أن يكسي العقوبة طبيعة مزدوجة، فهي عقوبات وتدابير بنفس الوقت، وذلك بحسب نص المادة 50 من نفس القانون، دون الإخلال بالعقوبات المنصوص عليها في هذا القانون وحقوق الغير حسن النية، ويتوجب على المحكمة إصدار قرار يتضمن الأتي:

أ-مدة إغلاق المحل،(وتترك هذه المدة للسلطة التقديرية للقاضي) وحجب الموقع الإلكتروني الذي إرتكبت فيه أو بوساطته تلك الجرائم.

ب-مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في إرتكاب أي من الجرائم المنصوص عليها.[3]

---

[1] كل من إستعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص أو أخر أو إبتزازه..... يعاقب بالحبس أو بغرامة لا تقل عن 200 دينار ولا تزيد عن 1000 دينار أردني.

[2] عاقب عليها المشرع لمن هم فوق ال18 سنة بالحبس لمدة لا تقل عن 03 أشهر وبغرامة من 200-1000 دينار أردني، وشدد المشرع في ذلك إذا إرتكبت لمن هم دون سن ال18 بالحبس مدة لا تقل عن سنتين وبغرامه من 1000-3000 دينار أردني.

[3] نصت المادة 50 من قانون الجرائم الإلكترونية الفلسطيني على أنه دون الإخلال بالعقوبات المنصوص عليها في هذا القانون وحقوق الغير حسن النية، ويتوجب على المحكمة إصدار قرار يتضمن الأتي:

الفرع الثاني: العقوبات المطبقة على الشخص المعنوي:

إذا إرتكب شخص معنوي لإسمه أو لحسابه إحدى الجرائم المنصوص عليها في هذا القرار يعاقب بغرامة من 5000- 10000دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات أو أن تقضي بحله في حال الطبيعي التابع له، وذلك حسب نص الماده 29 من نفس القانون.[1]

الفرع الثالث: العقوبة في جريمة الإتفاق والإشتراك والتحريض والشروع:

يعاقب المشرع بالعقوبة نفسها على الشخص سواء كان مشتركاً فيها أو تدخل فيها أو حرص على إرتكابها وذلك حسب مادة45 من قانون الجرائم الإلكترونية،[2] وإذا ساعد فيها أو تدخل أو إتفق في إرتكاب جناية أو جنحة فيعاقب عليها بالعقوبات المقررة ذاتها للفاعل الأصلي، وإن لم تقع الجريمة يعاقب بنصف العقوبة وذلك حسب المادة48 من نفس القانون.[3]

أ-مدة إغلاق المحل،(وتترك هذه المدة للسلطة التقديرية للقاضي) وحجب الموقع الإلكتروني الذي إرتكبت فيه أو بوساطته تلك الجرائم.

ب-مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في إرتكاب أي من الجرائم المنصوص عليها.[3]

[1] نصت المادة 29 من قانون الجرائم الإلكترونية الفلسطينية أنه إذا إرتكب بأسم الشخص المعنوي أو لحسابه إحدى الجرائم المنصوص عليها في هذا القرار بالقانون يعاقب بغرامة لا تقل عن 5000 ولا تزيد عن 10000 ينار أردني وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها 05 سنوات أو أن تقضي بحله إذا كانت الجريمة معاقب عليها بالحبس لمدة لا تقل عن سنة وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له.

[2] نصت المادة 45 من قانون الجرائم الإلكترونية الفلسطيني على أنه كل من إرتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ بإستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات أو إشترك فيها أو تدخل فيها أو حرض على إرتكابها ولم ينص عليها في هذا القرار بقانون، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع.

[3] نصت المادة 48 من نفس القانون على أنه يعاقب من يشترك بطريق الإتفاق أو التحريض أو المساعدة ..... بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب بنصف العقوبة المقررة لها.

أما بالنسبة **للشروع في الجريمة المعلوماتية** بوجهة نظر المشرع الفلسطيني، ف نص عليها بالمادة 49 من نفس القانون، والتي جاء فيها "يعد مرتكباً جريمة الشروع كل من شرع في إرتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها".[1]

المبحث الثاني: مكافحة الجريمة المعلوماتية :

إن الإنتشار الكبير والواسع لأجهزة الحاسوب وشبكات الإتصال المتعلقه بها، ساعد على توسع كبير للمجال الذي ترتكب فيه الجرائم المعلوماتية وتتمدد لتصل أضرارها الى العديد من المجتمعات، وهذا نتيجة للتطور الكبير في وسائل الإتصال وترابط الشبكات بعضها ببعض، فالضرر لا يقف عند حدود دولة معينة، ولا يكون متركزاً على مجتمعٍ بعينه، ولهذا كان لا بد من الدول أن توحد شملها لبناء قاعدة قانونية تعمل على دعم كفاح الدول في مواجهة الجريمة المعلوماتية، من خلال طرح المشاكل وايجاد حلول وتسخير التعاون الدولي للحد من أضرارها وإيقاف إنتشارها.

المطلب الأول: الطرق المنتهجة لمكافحة الجريمة المعلوماتية:

تعتبر الجرائم المعلوماتية من الظواهر التي تدق أجراس الخطر لتثير إنتباه المجتمعات للمخاطر والأضرار والخسائر التي تلحقها بالمجتمع، ولأن الجرائم المعلوماتية جرائم مستحدثة وترتكب من أشخاص فائقي الذكاء، فتسعى الدول للإتحاد مع بعضها لمكافحة هذا النوع من الجرائم، ورغم إختلاف السبل في المكافحة ولكن يبقى الهدف واحداً مشتركاً وهو وقف إنتشار هذه الجرائم والحد من أضرارها ومحاسبة كل من يجرأ للقيام بها.[2]

---

[1] نصت المادو 49 من نفس القانون على أنه يعد مرتكباً جريمة الشروع كل من شرع في إرتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها.

[2] مصطفى محمد موسى: **الجهاز الإلكتروني لمكافحة الجريمة**، دار الكتب القانونية، مصر ،2006، ص115.

وعلى هذا الأساس قمنا بدراسة بعض الآليات لمكافحة الجريمة المعلوماتية وسنتعرض لها من خلال ما يلي:

الفرع الأول: مواجهة الجريمة المعلوماتية على المستوى الدولي :

إن التزايد الكبير في نسبة الجريمة، وإستغلال المنظمات الإجرامية المناخ الدولي الذي يتسم بالمرونة لتوسيع مجال جرائمها وعملياتها عبر الحدود، إما بطريق مباشر من خلال مد نشاطها الدولي، أو طريق غير مباشر عن طريق إنتشار الشبكات الدولية للمنظات الإجرامية لتتعاون فيما بينها، كان لا بد من خلق أجهزة نوعية متخصصة ورفع كفائتها لملاحقة الجريمة.[1]

وقد أولت الأمم المتحدة وأغلب المنظمات الدولية إهتماماً بموضوع الجريمة المعلوماتية إهتماماً خاصاً، وهو الأمر الذي أدى لظهور العديد من الإتفاقيات والتي تتناول هذا النوع من الجرائم ومنها:

أولاً: إتفاقية برن :

وقعت إتفاقية برن سنة 1971 في سويسرا، والتي تعتبر حجر الأساس للحماية الدولية لحق المؤلف، وقد وقعت على هذه الإتفاقية نحو 120 دولة، وتعد المادة التاسعة من هذه الإتفاقية هي الأساس لأنها تنص على منح أصحاب حقوق المؤلف حق إستئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة و بأي شكلٍ كان، وتم التعديل هذه الإتفاقيه سنة1979 ووقعت عليها 140 دولة في سنة 1999.[2]

---

[1] بدري فيصل: **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، أطروحة دكتوراه، قانون عام، إشراف أ.د.البقيرات عبد القادر، جامعة الجزائر بن يوسف بن خده، كلية الحقوق، 2018، ص10 .

[2] يزن الأخضر محمد: **جرائم الكمبيوتر والإنترنت**، مذكرة لنيل رتبة ضابط، المدرسة العليا للشرطة، بن عكنون، 2007، 2008، ص49 .

وفضلاً على ذلك تمنح إتفاقية برن صاحب حق المؤلف الحق في أن يرخص أو يترجم أو يمنح أي ترجمةً أو إقتباساً لمصنفه للجمهور، وكذلك تلتزم الإتفاقية على توقيع الجزاءات سواء كان المؤلف المعتدى عليه وطنياً أو أجنبياً.[1]

وبموجب هذه الإتفاقية تتمتع برامج الحاسب الآلي سواء كانت بلغة المصدر أو بلغة الآلة بالحماية بإعتبارها أعمالاً أدبية وفقا لما جاء بها، ومما ميز هذه الإتفاقية هي أنها منحت دول العالم الثالث العديد من الحقوق، من بينها الحق في الترجمة المجانية للجامعات والإستفادة العلمية منها، والهدف الأساسي من إبرام هذه الإتفاقية هو حماية حقوق المؤلفين على مصنفاتهم الأدبية و الفنية.[2]

وإتفاقية برن كباقي الإتفاقيات تقوم على مبادىء أساسية التي تحدد نطاق الحماية الواجبة وأسلوب تطبيقها، وهذه المبادئ لاتتغير مع البرتوكولات ولا التغييرات، التي قد تدخل على الإتفاقية بعد ذلك، بل لا بد من التعديلات أن تتوافق من المبادئ الأساسية للإتفاقية.

ويمكن حصر مبادئها بإختصار فيما يلي:

1- مبدأ المعاملة الوطنية:

ويقصد به أن تتمتع كافه المصنفات الخاضعة لحماية الإتفاقية في إقليم دولة عضو، لنفس الحماية التي تتمتع بها المصنفات الوطنية لهذه الأخيرة لدى الدولة الأخرى الطرف من هذه الإتفاقية، فهذا المبدأ يجعل جميع الدول الأعضاء إقليماً واحداً، يتمتع المصنف الذي يتم نشره لأول مره في أي مكان من هذا الإقيلم بنفس درجة الحماية

---

[1] منير محمد الجنبيهي، ممدوح محمد الجنبيهي: **جرائم الإنترنت والحاسب الآلي و وسائل مكافحتها**،دار الفكر الجامعي ، الإسكندرية،2005، ص201 .

[2] شرابشة ليندة: **السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية**، ألقيت في الملتقى الدولي حول التنظيم القانون للإنترنت والجريمة الإلكترونية، جامعة زيان عاشور، الجلفة، 28/27 أفريل، 2009،ص7

التي يتمتع بها أي مصنف أخر بأي جزء من هذا الإقليم،فالتسوية تتم بين المصنف الذي ينشر في دولة متعاقدة، وذلك الذي ينشر في دولة متعاقدة أخرى.[1]

2- مبدأ الحد الأدنى للحماية :

هذا المبدأ يعتبر محاولة من واضعي الإتفاقية لمواجهة التفاوت التشريعي، بين مستويات الحماية في الأنظمة القانونية المختلفة.

وقد ثار خلاف على حماية هذه البرامج في ظل إتفاقية برن الذي حسمت في إتفاقية تريبس هذا الخلاف مقررة إعتبار البرمجييات مصنفات أدبية، تخضع للحماية وفقاً لقواعد إتفاقية برن للمصنفات الأدبية والفنية، وهذه الحماية تكون على أساسين[2]:

أ-المعيار الشخصي :

تستند إلى شخصية مؤلف البرنامج من حيث جنسيته أو موطنه فإتفاقية برن تقرر إشتمال الحماية للمصنفات التي تعد مؤلفوها من رعايا إحدى دول إتحاد برن سواء كانت هذه المصنفات منشورة أم لا.

ب-المعيار الإقليمي:

يقوم على أساس مكان أول نشر للمصنف، وفقا لهذا المعيار تتمتع البرمجيات بالحماية إذا ما نشرت في إحدى دول الأعضاء ولا عبرة هنا بجنسية المؤلف أو محل إقامته المعتاد.

وقد قامت إتفاقية برن على دعامة هامة مؤداها المساواة بين الوطني والأجنبي بالإضافة لوضع حد أدنى يتعين أن لا تقل عنه الحماية التي تلقاها أي من المصنفات المتمتعه

---

[1] رشا علي الدين: **النظام القانوني لحماية البرمجيات**، دار الجامعة الجديدة، الإسكندرية، 2007، ص241.

[2] بدري فيصل: **المرجع السابق**، ص17 .

بالحماية، ويتطبق هذين المبدأين في أقاليم كافة الدول الأعضاء في معاهدة برن، بإستثناء دول أصل المصنف، فالإتفاقية تستبعد أحكامها الخاصة بالحماية في دول الأصل.[1]

ويمكن القول بأن إتفاقية برن هي تقتصر على تقديم حلول للمشكلات القانونية الناتجة عن المصنفات المنشورة على شبكات الإنترنت، فهي لا تعالج النشر الإلكتروني عبر شبكات الإنترنت، ويعود السبب في ذلك أنها وقعت سنة 1971، اي قبل حدوث ثورة الإتصالات والمعلومات وظهور الإنترنت.[2]

ثانياً: معاهدة الويبو

الحقوق الملكية الفكرية هي أكثر ما يتم التعدي عليه، وخاصة عبر شبكات الإنترنت، كان لا بد من إيجاد منظمة تعمل على حماية الحقوق الفكرية، وكانت أول فكرة تجسدت على أرض الواقع، تشكيل المنظمة العالمية للملكية الفكرية "ويبو"، حيث تعتبر منظمة دولية غير حكومية، وإحدى الوكالات المتخصصة التابعة لمنظمة الأمم المتحدة مقرها الجنيف وقد تأسست بموجب إتفاقية ستوكهولم سنة 1967، وبلغ أعضاء هذه المنظمة 177دولة،[3] وتتركز أعمال ونشاطات هذة المنظمة على دعم حماية للملكية الفكرية بفرعيها الملكية الصناعية والملكية الأدبية في جميع أنحاء العالم، وهذا بفضل تعاون الدول مع بعضها البعض في هذا المجال، وتقسم معاهدة اليبو إلى ثلاث معاهدات:

1-معاهدة الويبو بشأن حق المؤلف :

تم التوقيع عليها سنة 1996 وتتكون من 18 مادة تقوم على أسس ومبادئ ثابتة.[4]

---

[1] بدري فيصل: المرجع السابق، ص17 .

[2] رشا علي الدين: المرجع السابق،ص244 .

[3] محمود أحمد عبابنة: **جرائم الحاسوب وأبعدها الدولية**، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص160

[4] منير محمد الجنبيهي، ممدوح محمد الجنبيهي: **المرجع السابق** ،ص202.

تبدأ بديباجة ثم تتناول علاقة تلك المعاهده بمعاهدة برن، ثم تتعرض لنطاق تطبيق حماية حق المؤلف كحق التوزيع والتأجير ونقل المصنف الى الجمهور والإلتزامات المتعلقة بالتدابير التكنولوجية والتقييدات على تلك الحقوق، وكذلك الإلتزامات المترتبه على المعاهدة ودخول المعاهدة حيز التنفيذ الفعلي.[1]

2- معاهدة الويبو بشأن الأداء والتسجيل الصوتي :

تم التوقيع عليها في 1996/12/20 وتتكون من أربعة فصول، يتناول الفصل الأول منها الأحكام العامة وعلاقة المعاهدة بالإتفاقيات الدولية الأخرى والتعريف والمستفيدون من الحماية بناء على تلك المعاهدة، أما الفصل الثاني فيتضمن حقوق فني الأداء معنوياً ومالياً، وحقوق الإستنساخ والتوزيع والتأجير، وحق إتاحة الأداء المثبت، أما بالنسبة للفصل الثالث فهو يتناول حقوق المنتجون من الإستنساخ والتأجير والتوزيع وحق إتاحة التسجيلات الصوتية، والفصل الرابع يتضمن الأحكام المشتركة كحق في مكافأة مقابل الإذاعة، أو النقل للجمهور والإستثناءات على هذا الحق ومدة الحماية والإلتزامات المتعلقة بالتدابير التكنولوجية وتم أيضا التعرض للإجراءات الشكلية.[2]

3- معاهدة الويبو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة:

تبدأ هذه الإتفاقية بمقدمة تتناول الطابع القانوني للمعاهدتين الجديدتين، وعلاقتهما بالمعاهدات الدولية الأخرى، ثم تتناول هذه الإتفاقية جدول الأعمال الرقمي والمعاهدات الجديدة، ثم تتعرض الإتفاقية إلى أحكام أخرى عامة عن المعاهدتين الجديدتين.[3]

وتهدف المنظمة العالمية للملكية الفكرية "الويبو" إلى:

---

[1] بدري فيصل: **المرجع السابق**، ص19 .

[2] منير محمد الجنبيهي، ممدوح محمد الجنبيهي: **المرجع السابق** ،ص204.

[3] منير محمد الجنبيهي، ممدوح محمد الجنبيهي: **المرجع نفسه**،ص205 .

– تدعيم الأخذ بالإجراءات التي تهدف الى تسيير الحماية الفعالة للملكية الفكرية في جميع انحاء العالم.

– تنسيق التشريعات الوطنية للدول الأعضاء في إطار الحماية الفاعلة للملكية الفكرية على مستوى العالم.

– تقديم الخدمات الفنية والقانونية والتدريبية في مجال العمل على حماية الملكية الفكرية.

– النهوض بأعباء التسجيل في مجال الحماية الدولية للملكية الفكرية، وأن تنشر البيانات الخاصة بالتسجيلات حيثما كان ذلك ملائماً.[1]

ثالثاً: إتفاقية تريبس

هي أيضاً من الإتفاقيات التي أُنشئت لحماية حقوق المؤلف، تم التوقيع عليها من قبل دول الأعضاء عام1994، وقد عالج موقعو الإتفاقية العامة للتعريفات والتجارة حقوق الملكية الفكرية بتوقيع إتفاق الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، فربطوا بذلك بين المعايير الدولية والمعايير المحلية.[2]

وجاءت إتفاقية تريبس كنتاج لمفاوضات إستمرت سنوات عديدة لتكون واحدة من أهم أدوات تحرير التجارة العالمية، والتي أثارت جدلاً ونقاشاً طويلاً أثناء المفاوضات بين الدول النامية والدول الصناعية.[3]

وقد تضمنت إتفاقية تريبس العديد من الإجراءات الهامة والفعالة لردع الإعتداءات على حقوق الملكية الفكرية، كما أنها ومن جهةٍ أخرى تفرض على الدول إتخاذ إجراءات والعديد من التدابير لمعالجة الوضع من تلك التدابير، مثل إعطاء الحق للسلطات في

---

[1] رشا علي الدين: **المرجع السابق**، ص262 .

[2] منير محمد الجنبيهي، ممدوح محمد الجنبيهي: **المرجع السابق** ،ص201 .

[3] رشا علي الدين : **المرجع السابق**،ص 173 .

إصدار أوامر بشن حملات مُفاجِئة لضبط الأدلة، والتي تكون بالعادة سريعة التخلص منها، والتحفظ على أدوات إرتكاب الجريمة، وفرض عقوبات جنائية رادعة، وفي حالة تراخي أحد الدول عن إتخاذ مثل تلك الإجراءات أو أن تمتنع عن تطبيق قوانينها الوطنية فإن المنظمة العالمية تعلن أن تلك الدولة تمتنع عن القيام بما عليها من واجبات، وبالتالي تصبح عرضةً لأن تتخذ باقي الدول ضدها إجراءات عقابية، وتتحد جميع أحكام إتفاقية تريبس في هدفٍ واحد وهو تحرير التجارة العالمية[1]، مع الأخذ بعين الإعتبار أمريين هاميين:

– ضرورة توفير إجراءات وتدابير لإنفاذ حقوق الملكية الفكرية دون أن تقف عائقآ أمام التجارة الدولية المشروعة.

– العمل على تشجيع الحماية الفاعلة في مجال حقوق الملكية الفكرية بكافة فروعها.وكأي إتفاقيةٍ أخرى تقوم تريبس على مجموعة من المبادئ سنتطرق إليها بإختصار وهي كالأتي :

1– مبدأ المعاملة الوطنية:

وتعني المساواة في الدولة العضو بين المواطنيين والأجانب المنتمين لإحدى دول الأعضاء، وقد ألزمت المادة الثالثة من الإتفاقية كل الدول الأعضاء بأن تمنح للمواطن الأجنبي المنتمي لدولة أخرى من دول الأعضاء نفس الحماية التي تمنح للمواطن الأصلي في شأن حماية الملكية الفكرية.[2]

---

[1] بدري فيصل: **المرجع السابق**، ص23

[2] كنعان نواف: **النماذج المعاصرة لحق المؤلف ووسائل حمايتها**، ط1، دار الثقافة للنشر والتوزيع، عمان،2009، ص362 .

2- مبدأ الدولة الأولى بالرعاية:

مفاد هذا المبدأ أن كل دولة عضو في منظمة التجارة العالمية تمنح دولة أخرى عضو ميزة تفضيلية أخرى، يتعين عليها أن تمنح نفس الميزة لجميع الدول الأعضاء، مع العلم أن هذا المبدأ لا يمنع الدول الأعضاء من فرض قيود تنظيمية للتجارة الدولية.

3- وضع حد أدنى من الحماية القانونية:

ومفاد هذا المبدأ أن الدول قد تقدم الحماية القانونية التي تفوق تلك التي طلبت منها في الإتفاقية، فليس هناك ما يمنع تقديم دولة من الدول الأعضاء الأخرى إمتيازات وحماية تفوق تلك المقررة في الإتفاقية، ولكن لا يجوز لها تقدير حماية أدنى من تلك التي حددتها إتفاقية تريبس.

4- وقت إنفاذ إفاقية تريبس :

تعد الدول المتقدمة والصناعية هي المتضررة الأولى من قرصنة الملكية الفكرية، ولهذا حاولت جاهدة جعل الدول النامية تنصاع للإتفاقيات والحد من القرصنة والتزوير والتقليد، ولكن هذا الدول الصناعية لم تتوصل لعقد إتفاقية تريبس ما لم يكن لديها قدر من المرونه التي من مظاهرها الرضا بالفترات الإنتقالية التي تم إقرارها وهي فترات سماح لا تلتزم بها الدول بالإلتزامات التي فرضتها الإتفاقية.[1]

5- المعاملة التفضيلية للدول النامية:

من أهم مقاصد إتفاقية تريبس هي مساعدة وتلبيةُ الإحتياجات الخاصة لأقل الدول الأعضاء نمواً، فهي تراعي المرونه في تنفيذ أحكامها خاصة على الصعيد الداخلي لهذه الدول الأعضاء، فإتفاقية تريبس أرادت مساعدة الدول النامية لإنشاء قاعدة

[1] بدري فيصل: **المرجع السابق**، ص26 .

تكنولوجية متطورة تخدم مصالحها الإقتصادية، وتساعدها للحاق بعجلة التجارة الدولية.[1]

وخلاصة ما تطرقنا إليهِ سابقاً برأينا يمكن القول بأن الإتفاقيات والمعاهدات الدولية، بالإضافة إلى المنظمات الدولية وما ينتج عنها من تقارير والجهود المبذولة للإحاطة بالجريمة المعلوماتية، تعد هي حجر الأساس الذي يرتكز عليه التعاون الدولي لمكافحة الجريمة المعلوماتية.

الفرع الثاني : مساعي بعض الأجهزة الدولية في مواجهة الجريمة المعلوماتية.

أولاً: دور الأمم المتحدة في مواجهة الجريمة المعلوماتية:

نظرا لما تتسبب به الجرائم المعلوماتية من أضرار وخسائر محلية ودولية، فقامت الأمم المتحدة بوضع هذه الجرائم من أولوياتها وعلى قائمة إهتماماتها، وتؤكد على أن منع هذه الجرائم يتطلب إستجابة دولية مشتركة بين أعضاء هذه المنظمة بغية التعاون من أجل الحد من إنتشارها وتخفيف أضرارها، من خلال إشرافها على المؤتمرات الدولية الخاصة لردع الجريمة ومعاقبة المجرمين وإبرامها للإتفاقيات الدولية.[2]

– ونجد من أهم المؤتمرات المبرمة في مجال مكافحة الجريمة الإلكترونية المؤتمر الثامن المنعقد سنة 1990، والذي توصل الى عده توصيات بعد دراسته التقرير الذي أعدته لجنة الخبراء العشرين.

– الإتفاقية المنشئة للمنظمة العالمية للملكية الفكرية في ستوكهولم سنة 1967، والتي تعتبر هذه المنظمة إحدى الوكالات المتخصصة للإمم المتحدة، حيث قامت هذه المنظمة من خلال العديد من الخبرات بالمساهمات العديدة بهدف حماية برامج الحاسب

---

[1] رشا علي الدين: **المرجع السابق**، ص182 .

[2] بوشعرة أمينه، موساوي سهام: **الإطار القانوني للجريمة الإلكترونية دراسة مقارنة**، مذكرة لنيل شهادة الماستر تخصص قانون خاص وعلوم جنائية ، بإشراف أ.د.دموش حكيمة، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، 2018، ص50 .

الآلي، وهو أغلب ما ذهبت إلية الدول الصناعية ودول العالم الثالث، إلى إخضاع برامج الحاسب الألي لقوانين حماية حق المؤلف، وأضافت برامج الحاسب الآلي للمصنفات الأدبية المجمعة وفقا للقانون وذلك وفق إطار إتفاقية التجارة العالمية "الغات"، وبذلك لعبت المنظمة العالمية للملكية الفكرية دوراً في حماية حق المؤلف وبرامج الحاسب الآلي.[1]

– الإتفاقية الخاصة لمكافحة جريمة إساءة إستعمال التكنولوجيا لإغراض إجرامية، والتي ركزت على المساهمات التي يمكن أن تقدمها الأمم المتحدة ولا سيما لجنة منع الجريمة وتحقيق العدالة الجنائية، والترويج لمزيد من الفعالية والكفاءة في تنفيذ القوانين وإقامة العدل، وكما أكدت على ضرورة منع إساءة إستعمال التكنولوجيا لإغراض إجرامية وتعزيز التنسيق بين الدول والقطاع الخاص لمكافحة وردع هذه الجريمة.[2]

ثانياً: دور المجلس الأوروبي في مواجهة الجريمة المعلوماتية:

للمجلس الأوروبي دور فعال في الحد من الجرائم المعلوماتية، وذلك من خلال إقراره العديد من التوصيات الخاصه بالبيانات ذات الصبغة الشخصية من سوء الإستخدام، وحماية الدفق المعلوماتي، وتتمثل مجهودات المجلس الأوروبي في مكافحة الجريمة المعلوماتية فيما يلي:

– التوقيع على الإتفاقية الخاصة لحماية الأشخاص من مخاطر المعالجة الآلية للبيانات والتي وقعت بين المجلس الأوروبي والسوق الإشتراكي سنه 1980، وبدأ التطبيق الفعلي لهذه الاتفاقية سنه 1985 والتي تخص الأشخاص الطبيعين في

[1] بوشعرة أمينه، موساوي سهام: **المرجع السابق**، ص51.

[2] بوشعرة أمينه، موساوي سهام: **المرجع نفسه**، ص.51.

القطاعين العام والخاص بشأن الملفات المعدة آلياً، بحيث تفضى بإلزامية إحكامها لتحقيق حماية البيانات الشخصية المعالجة آلياً.[1]

– إضافة إلى ما صدر عن المجلس الأوروبي من توصيات لتوسيع نطاق الحماية لتشمل قطاعات الأنشطة الخاصة مثل البيانات الطبية والإحصائية، وفي عام 1989 قام المجلس الأوروبي بنشر دراسة تتضمن أهمية تفعيل دور القانون في مواجهة الجرائم المرتكبة عبر الحاسب الآلي، كما تبعت هذه التوصية دراسة أخرى سنة 1995 تتمحور حول الإجرائات الجنائية للجريمة المعلوماتية، حيث قام المجلس الأوروبي بتشكيل لجنة خبراء الجريمة في العالم الإفتراضي سنة 1997.[2]

– توقيع إتفاقية بودابست لمكافحة الجرائم المعلوماتية والتي وقعت سنة 2001 ولم تدخل حيز التنفيذ حتى عام 2004، والتي تعاونت فيها كندا واليابان وجنوب أفريقيا و أمريكيا، وعلى الرغم من أنها أوروبية المنشأ إلا أنها ذات طابع دولي، فهي تعتبر إتفاقية جنائية دولية وأداة لمكافحة الجريمة السيبرانية.[3]

ثالثاً: دور المنظمة الدولية للشرطة الجنائية في مواجهة الجريمة المعلوماتية:

تهدف المنظمة الدولية للشرطة الجنائية(الإنتربول) إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة، وكذلك مساهمتها في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، حيث

---

[1] الحسيناوي علي جبار: **جرائم الحاسوب والإنترنت**، دار اليازوري العلمية للنشر والتوزيع ، عمان ،2009، ص151 .

[2] الحسيناوي علي جبار: **المرجع نفسه**، ص152.

[3] بوشعرة أمينه، موساوي سهام: **المرجع السابق**، ص53 .

تركزت إهتمامات الإنتربول في الفترة الأخيرة على الجريمة المنظمة، والأنشطة ذات الصلة بها.[1]

إختتمت أعمال إجتماع الجمعية العامة ال26 للشرطة الجنائية الدولية بالعاصمة الصينية بكين سنة 2017/09/29 بمشاركة نحو1000 من كبار قادة الشرطة والسياسيين في 156دولة، فأنه وبعد عام 2017 كانت هناك مؤتمرات لمواجهة الجريمة المعلوماتية في عدة قضايا، ومن أهم القضايا التي تم مناقشتها ضمن الإجتماع نجد جرائم الإنترنت والقرصنة الإلكترونية، والمخاطر الناجمة عنها، وآلية التصدي لهذا النوع من الجرائم على المستوى الدولي، حيث يؤدي الإنتربول الدور الرائد في مواجهة الجريمة المعلوماتية، من خلال تشجيع التعاون بين أجهزة الشرطة للدول، وتزويدها بالبيانات والمعلومات حول المجرم والجريمة وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في إقليم الدول المنظمة إليها، وهذا بالإضافه للتعاون في القبض على المجرمين عن طريق تعقب الأدلة الرقمية، وضبطها والقيام بعملية التفتيش العابر للحدود للأنظمة المعلوماتية وشبكات الإتصالات للبحث عن دليل وبراهين لإرتكاب الجريمة.[2]

وقد تستدعي الأمور للقيام بعمليات شرطية وأمنية مشتركة والتي من شأنها متابعة المجرمين الذين يستغلون التكنولوجيا الجديدة لتحقيق أغراضهم الغير شرعية.[3]

---

[1] بنعمر الحاج عيسى: **الآنتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود** ،مجلة الدراسات القانونية السياسية، كلية الحقوق، جامعة الأغواط، العدد 03 ،2006، ص252 .

[2] شبيلي مختار: **الجهاز العالمي لمكافحة الجريمة المنطمة**، ط2 ، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2016، ص266-267 .

[3] شبيلي مختار: **المرجع نفسه** ،ص274

بالتالي فإن نجاحها في تحقيق التعاون بين الدول الأطراف كونها تركز إهتمامها على الجريمة المنظمة والجريمة الإلكترونية، فهي تعتبر الجهاز الرئيس في تحقيق التعاون الدولي في مكافحة الجريمة المنظمة.[1]

وتهدف الأنتربول الى:

أ- تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان، للإعلان العالمي لحقوق الإنسان.

ب- إنشاء وتنمية كافة المؤسسات القدرة على المساهمة الفعالة في الوقاية من جرائم القانون العام ومكافحتها.

وكمثال على دور الإنتربول في مواجهة الجرائم المتعلقة بالأنظمة المعلوماتية ما حصل في لبنان عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة سنوات من موقعه على شبكة الإنترنت وذلك إثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الخصوص.[2]

رابعاً: دور الجامعة العربية في مواجهة الجريمة المعلوماتية:

سعت الدول العربية لإيجاد طرق تشريعية ناجعة لمواجهة الجرائم المعلوماتية، ومن بين هذه الجهود القانون العربي الإسترشادي، وقد تم إعداد هذا القانون العربي الإسترشادي (قانون الإمارات العربية)، بين وزراء العدل العرب و وزراء الخارجية أين تم التوقيع على هذا القانون في مواجهة الجريمة المعلوماتية في الدول العربية، و قامت جامعة الدول العربية من خلال الأمانة العامة لمجلس وزراء العدل العرب قي دورته

---

[1] شحاده يوسف: **الضابطة العدلية علاقتها بالقضاء ودورها في سير العدالة الجزائية**، ط1، مؤسسة يحسون للنشر والتوزيع ،بيروت ،ص456- 458.

[2] بدري فيصل: مرجع سابق، ص12 .

التاسعة عشر بإعتماد هذا القانون النموذجي في سنة 2003 والذي يعتبر أهم ما بذل من جهود عربية في مجال الحماية التشريعية من الجرائم المعلوماتية .

وقد تناول هذا القانون 27 ماده مقسمة على 4 فصول، يتناول الفصل الأول الحديث عن الجرائم المعلوماتية، أما الفصل الثاني فتحدث عن التجارة والمعاملات الإلكترونية، والفصل الثالث تناول الحديث عن حماية حقوق المؤلف عبر الوسائل الإلكترونية، والفصل الرابع تطرق فيه للحديث عن الإجراءات المتعلقة بالجريمة المعلوماتية .

وهنا يمكن إستخلاص أن الجامعة العربية والمجلس الأوروبي و والأمم المتحدة والإنتربول قد ساهموا في مكافحة الجريمة المعلوماتية، وبالرغم من إختلاف الأساليب المتبعة، إلا أنها كانت وما زالت تسعى وتهدف إلى تحقيق شيء واحد وهو التصدي للجريمة المعلوماتية.[1]

المطلب الثاني: دور التشريع الجزائري والفلسطيني في مكافحة الجريمة المعلوماتية:

الفرع الأول: آليات مكافحة الجريمة المعلوماتية في الجزائر:

إن إستعمال تكنولجيات الإتصال والإعلام في تنفيذ الجرائم المستحدثة تزيد من خطورة إستعمال هذه التقنيات، ولكن في ذات الوقت لا غنى للناس عنها، وأيضاً نتيجة للتطور المستمر للتكنولوجيا والتقنيات المستخدمة في الإتصال، التي تستدعي إمكانيات وخبرات لا يمكن مواكبتها إلا من خلال إنشاء هيئات و مراكز متخصصة، للتعامل مع مثل هذا النوع من الجرائم وحماية مستخدمي التقنيات من الأضرار التي تنشأ عنها، والعمل على تجنيد العاملين في قطاع العدالة عن طريق التكوين المتخصص والذي

[1] إيمان مسعود سالم: **الجريمة المعلوماتية**، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة محمد لمين دباغين، سطيف ، 2015،ص32 .

يهدف إلى توسيع معارفهم بتلك التكنولوجيا، ومعرفة كيفية إستخلاص الأدلة الرقمية وكيفية الحكم بواسطتها.[1]

وسنتطرق لبعض الهيئات المختصة بمكافحة الجرائم المعلوماتية في الجزائر :

أولاً: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته (الجريمة المعلوماتية) :

جاء نص المادة 13 من القانون04/09[2] على إنشاء هيئة للوقاية من من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وقد أوردت مهامها في المادة 14 من نفس القانون، وتتحدد تشكيلتها وكيفية سيرها عن طريق التنظيم .

وتتشكل هذه الهيئة من مجموعة من ضباط الشرطة القضائية التي ستسمح لهم هذه الصفه بالقيام بالمهام التي أوكلها لهم المشرع، وتقوم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإتصال والإعلام بهدفين أساسيين :

1-الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

وتكون هذه الإجراءات عن طريق توعية مستخدمي تكنولوجيات الإتصال بخطورة الجرائم التي يمكن أن يكونوا ضحايا لها وهم يتصفحون أو يستعملون هذه التكنولوجيا، ومن أهم هذه الجرائم التجسس على الإتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء.

---

[1] مريم مسعود أحمد: **آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون 04/09**، مذكرة ماجستير-قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، 2013، ص44 .

[2] **قانون رقم 04/09** المؤرخ في 5/ غشت/ 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمنشور في الجريدة الرسمية بتاريخ 16/ غشت /2009 ، العدد 47.

2-مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

وبحسب ما نصت عليه المادة 14 من قانون04/09[1]، فهنالك نوعين من المكافحة تقوم بهما الهيئة :

أ-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته.

ب-مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

ج-تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة للتعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وتحديد مكان تواجدهم.

وتقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تقوم بمشاركتها مع الهيئات المماثلة لها على المستوى الخارجي، وبدون المساس بمبدأ المعاملة بالمثل وتطبيق الإتفاقيات الدولية، وتقوم بدراسة والبحث مع الهيئات الدولية الأخرى عن كافة المعلومات المتعلقة بالجرائم المعلوماتية ومرتكبيها وأماكن تواجدهم.[2]

ثانياً: دور الضبطية القضائية في مواجهة الجريمة المعلوماتية

إن الجرائم المستحدثة تلقي المزيد من الأعباء على عاتق الضبطية القضائية، ومن المتصور أن يجد ضباط الشرطة القضائية أنفسهم غير قادرين على التعامل مع الوسائل الإستدلالية و الإجراءات التقليدية في مثل هذا النوع من الجرائم، وقد يفشل

---

[1] **قانون رقم 04/09** المؤرخ في 5/ غشت/ 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمنشور في الجريدة الرسمية بتاريخ 16/ غشت /2009 ، العدد 47.

[2] مريم مسعود أحمد:**المرجع السابق**، ص46.

جهاز الضبطية في تقدير أهمية الجريمة بسبب نقص الخبرة الكافية والتدريب، ولنفس السبب سيفشل في التحقيق في جمع أدلة الجرائم التكنولوجية، ونظرا لهذا السبب كان من أولويات السياسة الوطنية لمكافحة الجرائم المعلوماتية إنشاء سلك ضباط الشرطة القضائية وأعوانهم.[1]

فعلى مستوى الدرك الوطني الذي باشر سنة 2004 في عمليات تكوين مستخدمين من أجل إنشاء مركز وطني لمكافحة الجرائم المعلوماتية، وبموجب هذا العمل فالكثير من إطارات الدرك الوطني إستفادوا من تكوين خاص بجامعات سويسرا وأمريكيا وكندا، سواء في المجال التقني والفني أو في المجال القانوني، وكذلك تم التكوين في مؤسسات وطنية مثل مركز الدراسات والبحوث في الإعلام العلمي والتقني (cerise) الذي عرض تكويناً في الأمن المعلوماتي في إطار التكوين كل سنة، وهذا البرنامج التكويني يهدف إلى تطوير كفاءات سلك الدرك الوطني حتى تكون أكثر عملية في مجال مكافحة الجرائم المعلوماتية، بالإضافة إلى أن إطارات الدرك الوطني تساهم في عدة ملتقيات وطنية ودولية تنصب موضوعاتها في إطار الجرائم المعلوماتية، بينما مصالح الأمن الوطني هي غائبة عن مجارات تكريس مكافحة هذه الجرائم ما عدا ما يتم تنظيمية من ملتقيات ومعارض تتعلق بالموضوع، وكذلك المساهمة والمشاركة في ملتقيات ومؤتمرات وطنية ودولية تتناول بالخصوص حقوق المؤلف في البيئة الرقمية.[2]

---

[1] عبد الفتاح بيومي حجازي: **الإثبات الجنائي في جرائم الكمبيوتر والإنترنت**، دار الكتب القانونية، مصر، 2007، ص232 .

[2] Hadjira BOUDER: Orientations de la politique pénale de prévention et de lutte contre la criminalité liée aux TIC en Algérie, centre de recherche sue l'information scientifique et technique, CERIST, 03 Rue des frères Assiout, Benaknoun, Alger, Algérie, www.alexalaw.com [2011/02/28]. تاريخ الإطلاع 2019/05/27 .

ثالثاً: السلطة القضائية في مواجهة الجريمة المعلوماتية :

إن اللجوء الواسع والمتزايد للمواطنين في إستخدام شبكات الإنترنت فيتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي، ومنذ سنة 2003 وفي إطار إصلاح العدالة قامت وزارة العدل بإطلاق برنامج جديد لتطوير القضاة هدفه رفع مستوى أداء القضاة، ليواكب التطور القانوني الجاري الخاص بجرائم المعلوماتية، ولأجل هذا تم دمج مادة " الجريمة المعلوماتية " في برنامج تكوين طلبة المدرسة الوطنية للقضاء، على شكل ملتقيات ينشطها الخبراء.[1]

ولا شك أن تخصيص جهات القضاء وتخصص القضاة هما من السمات الحديثة البارزة للتنظيم القضائي الجزائري، وقد جاء في إتفاقية التمويل الجزائرية الأوروبية لمشروع دعم إصلاح العدالة في الجزائر أن " هذا المشروع يهدف إلى دعم التخصيص وتكوين القضاة داخل وخارج الوطن للإستجابة للمتطلبات المستجدة الناتجة عن التزايد المستمر للمنازعات التي يجب عليهم القصل فيها، ونظراً لأهمية التخصيص القضائي فقد عقد له عدة مؤتمرات دولية مثل مؤتمر روما1958 ومؤتمر نيس 1972، والتي أكدت بدورها على أهمية التخصص القضائي ودوره المهم في رفع مستوى العمل القضائي، ولنظام التخصص جانبين الجانب الأول هو تخصص القضاة، والجانب الثاني تخصيص جهات القضاء[2]

واذا كان للقضاء المتخصص جانبين هما تخصص القضاة والأجهزة القضائية المتخصصة، فإن هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة، وهو الأمر الذي نعتقد أنه جعل المشرع الجزائري يختار أسلوب الأقطاب القضائية وذلك

---

[1] مريم مسعود أحمد: **المرجع السابق**، ص49 .

[2] عمار بوضياف: **النظام القضائي الجزائري**، دار ريحانه، الجزائر، 2003، ص ص229-230 .

لتلافي العقبات التي تواجه القضاء المتخصص،[1] فيتجنب إنشاء هيئات قضائية جديدة، لكنه يوسع من دائرة الإختصاص الإقليمي للمحاكم لتشكل أقطاب قضائية ويمنحها إختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن إختصاصها العادي، وهذا ما يجعلنا نعتقد أنه من جانبٍ أخر، أن التخصص الذي سيسود التنظيم القضائي الجزائري سيرتكز أكثر على الجانب البشري أي تخصص القضاة، ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية.[2]

الفرع الثاني: آليات مكافحة الجريمة المعلوماتية في فلسطين

أولاً: نيابة الجرائم الإلكترونية :

وبحسب ما جاء بالمقابلة مع الأستاذة نسرين الريشماوي رئيسة نيابة الجرائم الإلكترونية، تعرف الريشماوي نيابة الجرائم الإلكترونية بأنها "نيابة خاصة بمتابعة الجرائم الإلكترونية المبينة على تقنية المعلومات والوسائل الإلكترونية ويعمل فيها أشخاص مختصين، تضم نحو 26 وكيل نيابة مختص، ومختبر مجهز بطاقم تقني يضم 9 أشخاص مدربين على أحدث النظم الإلكترونية "، تتركز مهمتهم في تحليل المعلومات التقنية وجمع الدلائل، ومن ثم بناء ملف تحقيقي مبني على الدليل الرقمي ومن ثم تنظيم لائحة الإتهام وتقديمها للمحكمة، ويقوم مبدأ عملهم على تتبع المتهم عبر التقنيات الإلكترونية يمكن أن يكون قد إستخدمها ومحاصرته وإدانته قضائياً.

وقد صرحت الريشماوي بأن فلسطين لا تعاني من عصابات داخلية منظمة، كل ما تتعرض له هو جريمة فردية عشوائية، ولكن تعرضت فلسطين لعدة هجمات منظمة من الخارج، ويتم التعامل مع الهجمات الخارجية من خلال الطرق الدبلوماسية حيث

---

[1] **عمار بوضياف: المرجع السابق،** ص229 .

[2] مريم مسعود أحمد: **المرجع السابق،** ص49 .

قام وكيل النيابه المخصص للتعاون القضائي ومساعدة قضائية دولية، وعبر النائب العام بطلب المساعدة عبر القنوات الدبلوماسية لوزارة العدل والخارجية لملاحقة هذه العصابة، وتم الإستجابة لطلبه، وتنتشر الجريمة المعلوماتية في كافة انحاء الوطن ولكنها تتمركز في مدينة الخليل حيث يكثر فيها الإبتزاز الإلكتروني، نظرا لطبيعة العلاقات التجارية فيها وعدد السكان وغيره من أسباب .

وقد عانت نيابة الجرائم الإلكترونية من قيام بعض الجرائم المعلوماتية بعناوين وخطوط إسرائيلية، وتقوم النيابة بتحليلها ومتابعتها حتى تصل لمرتكبها وتقوم بعد ذلك بالتواصل مع النائب العام للتنسيق مع الطرق الأخر، وأيضآ وجود خطابات تتم عبر الإرتباط المدني في حالة كون الجريمة خطيرة.

وكون المعلومات تقتصر على شخصٍ واحد وهو النائب العام فبالتالي تحافظ على خصوصيتها، حيث لا يستطيع أي شخص بالنيابة العامة أن يطلب معلومات من شركات الإتصالات دون موافقة النائب العام الجهة المخولة للإطلاع على الخصوصية، والذي يقوم بدوره بدرسة الطلب وعليه يجري المقارنه بين الطلب ومجرى التحقيق وبين المس بالخصوصية، وتجري العملية بسرية تامة للحفاظ على خصوصية المواطنين، حيث تقوم الشركات بتسجيل كافة بيانات المستخدمين مجبرة بقوة القانون وليس النيابة من تجبرهم .

ولكن تواجه نيابة الجرائم الإلكترونية بعض الصعوبات منها عدم وجود قانون رادع حيث تعمل النيابة تحت القانون الأردني وقانون الإتصالات، وتوجد بعض القضايا التي لا يوجد لها عقوبة مثل نشر الفايروس أو الإختراق.

ونظراً للصعوبة التي تقع على عاتق القاضي لفهم القضية المتعلقة بالبيانات والأنظمة الآلية لعدم الدراية والخبرة والمعرفة الكافية بالتقنيات، تقوم نيابة الجرائم الإلكترونية بموائمة ملف القضية وتسهيله ليصبح يسيراً على القاضي لفهمه، ويلاحظ وجود وعي

كبير لدي الشركات والمؤسسات والتي توفر وحدة وقسم خاص (TT) لحماية بياناتها، ويقومون بالتصدي لكل الهجمات الإلكترونية من أي جهةٍ كانت، وفي نفس الوقت يغيب هذا الوعي عند المواطنين الذين لا يدركون أهمية الحفاظ على سرية بيناتهم وخطورة وقْعها في المكان غير مناسب.[1]

المطلب الثالث: آليات الوقاية من الجريمة المعلوماتية.

الفرع الأول: دور المؤسسات الرسمية ومؤسسات المجتمع المدني في الوقاية من الجرائم المعلوماتية :

يختلف دور المؤسسات في الدولة بين المؤسسة التي تلعب دوراً وقائياً مثل الإعلام والأسرة والتعليم والثقافة، وبين المؤسسات التي تعمل على مكافحتها كالمؤسسة الأمنية والنيابة العامة والقضاء، وسنتطرق إلى دور المجلس التشريعي والمؤسسات الأمنية والإعلامية والأسرية والثقافية والعلمية للوقاية منها.[2]

1-المجلس التشريعي :

نظراً لغياب دور المجلس التشريعي الفلسطيني في إصدار التشريعات منذ أكثر من 10 سنوات، جاء القرار بقانون بشأن الجرائم الإلكترونية لسد الفراغ التشريعي التي عانت منه السلطة التنفيذية والقضائية، حيث تكفل التشريعات أمن و إستقرار المجتمعات وتشكل الضمانات الأساسية لحقوق الأفراد وهذا يتطلب سن تشريعات أو إستحداث القوانين الجزائية التقليدية لتتلائم مع التطور التكنولوجي والتقني والإقتصادي والإجتماعي، ولملاحقة مرتكبي تلك الجرائم من أجل تحقيق الردع العام والخاص من

---

[1] http://samanews.ps تاريخ الإطلاع 2019/05/28

[2] الردايدة عبد الكريم: **الجرائم المستحدثة وإستراتيجية مواجهتها**، ط1، دار ومكتبة الحامد للنشر والتوزيع، الأردن، 2013، ص 100 .

خلال فرض عقوبات صارمة تساهم في الحد من آثارها السلبية على الأفراد والمؤسسات.[1]

2- المؤسسة الأمنية :

تقوم المؤسسة الأمنية بمواجهة الجرائم الإلكترونية من خلال تأهيل كوادر أمنية متخصصة بإستخدام التقنيات الحديثة والفضاء الإلكتروني في عمليات التحري والبحث والمراقبة لمنعها وضبطها، والتوعية الثقافية الأمنية حول مخاطر إنتشارها.[2]

حيث تعمل على تحفيز الأفراد والمؤسسات على إبلاغ الجهات المختصة عنها[3]، بالإضافة إلى تعزيز الأبحاث العلمية الشرطية والأمنية حولها وتحليلها مع مواكبة التطور العلمي والتكنولوجي، وتعزيز التعاون الأمني إقليمياً و دولياً من خلال تبادل الخبرات القانونية والإجراءات الفنية والتقنية.[4]

3- المؤسسة الإعلامية :

يساعد الإعلام كسلطة رابعة على ترسيخ أمن المجتمع والتأثير فيه من خلال إثارة الرأي العام لمواجهة الجرائم بكافة أشكالها، من خلال تسليط الضوء على الأفعال والتصرفات السلبية وتوعية المجتمع بهذه الجرائم وللوقاية منها، بواسطة الصحافة الإلكترونية وإصدار الصحف والمجلات التوعوية ونشرها في أروقة المجتمع، ولإنجاح ذلك يتطلب وضع خطة إعلامية من أجل التعرف على ظاهرة الجرائم المعلوماتية في المجتمع لمواجهتها وتنمية الوعي المجتمعي بمخاطرها،وحث المواطنين على إبلاغ

---

[1] الردايدة عبد الكريم: **المرجع السابق**، ص263 .

[2] حمدان هاني: **دور العلاقات العامة لدى الأجهزة الأمنية في التوعية الأمنية**، مجلة الدراسات الأمنية، أكاديمية الشرطة الملكية، عمان، الأردن، 2004، العدد1، ص37 .

[3] مرسي محمد محمود السيد: **تفعيل دور الشرطة في تحقيق الإستقرار الأمني**، أطروحة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2004، ص55 .

[4] الجمال محمد علي: **دور الشرطة الوقائي في إنحسار جرائم العنف**، مجلة الأمن العام المصرية، عدد 163، ص65 .

الجهات المختصة حال تعرضه لهذه الجرائم والتعاون معهم، ونشر وتركيز الجهود على أداء المؤسسات الأمنية والقضائية في مجال مكافحة هذه الجرائم[1].

4- المؤسسة الدينية :

تلعب المؤسسات الدينية دوراً كبيراً في الوقاية من هذه الجرائم من خلال التربية الأخلاقية وتقوية الإيمان بين أفراد المجتمع والتنشئة السليمة للأفراد عبر وسائل التوعية الدينية المختلفة، ومن خلال وضع مؤلفات وكتب ذات بعد ديني عن مخاطرها، وتنظيم محاضرات إرشادية حول هذه الجرائم في أماكن العبادة والمدارس والجامعات وغيرها من المؤسسات، وتعزيز دور خطباء المساجد بالتعاون مع وزارة الأوقاف بتوعية الناس حول هذه الظواهر،

وبيان المخاطر التي تنشأ عن السلوكيات التي تتعارض مع الدين الإسلامي ومبادئ الشريعة الإسلامية، والمساهمة في تعزيز الوازع الديني والأخلاقي.[2]

5- الأسرة:

تساهم الأسرة في مواجهة هذه الجرائم كونها أكثر تأثيراً بوصفها المؤسسة الأولى التي تؤثر في تحديد شخصية الطفل وسلوكه، من خلال تنشأة وتوعية الأفراد وتوجيههم نحو السلوكيات الإيجابية وإبعادهم عن الجريمة، وتقديم لهم النصائح حول مخاطر هذه الجرائم، وتساهم أيضآ الأسرة في مكافحة ومواجهة الجرائم المعلوماتية من خلال معاقبة مرتكبها من أفراد الأسرة.[3]

---

[1] نبيل محمود فريد أبو الرب: **الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين**، مكتبة الشروق،جامعة النجاح الوطنية، فلسطين،2018،ص82 .

[2] نبيل محمود فريد أبو الرب: **المرجع نفسه**، ص82-83 .

[3] الردايدة عبد الكريم: **المرجع السابق**،ص212-215 .

6 – المؤسسات التعليمية والثقافية :

تلعب المؤسسات التعليمية والثقافية دوراً رئيسياً في مواجهة الجرائم المعلوماتية، وتحد من إنتشار السلوك غير المرغوب فيه في المجتمع، وتمنع إنحراف الأشخاص نحو إرتكاب الجرائم وتوجيهها إلى السلوك الإجتماعي الصحيح وتعزيز القيم والأخلاق من خلال التربية والإخلاص بالعمل وحسن التوجيه، وفرض الرقابة والمتابعة على أفرادها لرصدها ومعرفة أسباب إرتكابها من أجل الوصول إلى طرق ووسائل علاجها، والتركيز في المناهج الدراسية الإبتدائية على الأخلاق الحميدة كون الطفل في هذه المرحلة أكثر إستجابة.

وتعمل هذه المؤسسات من خلال إيجاد مقررات تعليمية تعمل على توعية أفراد المجتمع ونشر الكتب والمجلات التي تظهر المخاطر التابعة لهذه الجرائم[1].

الفرع الثاني : دور التربية والتوجيه في الوقاية من الجريمة المعلوماتية

أولاً: الجانب التربوي:

إن للجانب التربوي الأهمية الكبرى للتعامل بكل مصداقية ونزاهة مع هذه التطورات التكنولوجية الهائلة والحاصلة في عالم الإتصالات اليوم، لا سيما في مجال الشبكة العنكبوتية التي غزت كل نقاط العالم وهي في تزايد مستمر، ونظراً لقلة الوعي لدى فئات المجتمع وظهور المرحلة الإنبهارية بالمنجز الإلكتروني، يشاهد الجميع مدى الإندفاع الجماهيري الحاصل في التعامل مع هذه الوسائل الإلكترونية الحديثة، فبنظرةٍ بسيطة إستنتج الباحث محمد سيد محمد مجموعة من الخصائص ومن أبرزها سيطرة الرأي الشخصي على سير الموضوع ومحتوياته المعلوماتية، وإعتماد المدونات على

[1] . نبيل محمود فريد أبو الرب:**المرجع السابق**، ص83 .

مصطلحات مثل "سمعت" و " قيل لي" و"جاءني إتصال من صديق"، حيث يطغى الجهل العام بمجريات الأمور والشعور السلبي الحاد ضد كل شيء.[1]

ثانياً: الجانب التوجيهي:

هذا الجانب ينبغي أن تساهم فيه كل الوسائل الإعلامية من صحافة، التلفزة، الإذاعات والمسرح والسينما، على اعتبار مدى التصاقها بالجمهور العريض والواسع من أبناء المجتمع، ولهذا فالمسؤولية كبيرة على عواتقها، وهو أمر ينبغي أن يعيه المسئولون عن هذه القطاعات، وأن يدركوا تمام الإدراك ضرواة المعركة التي تنتظرهم، لأن القضية ليست مجرد عملية ترفيهية، كلا فالجهاد هنا لا يقل أهمية عن الجهاد في ساحات المعركة.

ولأن الوقاية خير من العلاج كان لا بد من إتخاذ تدابير وقائية تجنبنا من الوقوع ف المشكلة وتنقسم هذه التدابير إلى فرعين:

1- الحماية التقنية :

فعلى سبيل المثال الوقاية من الإصابة بفايروسات الحاسوب لابد من الأخذ بالإجراءات التالية :

- عدم إستخدام برامج مجهولة المصدر.
- عدم إستخدام إسطوانات تتضمن برامج متغيرة وقابلة للتغييرالأمر الذي يشك في أنها حاملة للعدوى الإلكترونية .
- مراقبة إستخدام الحاسوب للذاكرة للتأكد من عدم وجود فايروسات مختبئة فيها، و أنه يجب إنشاء مركز قومي لأمن الحاسبات والمعلومات كإجراء أمني وقائي[2].

---

[1] محمد سيد محمد: **وسائل الإعلام من المنادي إلى الإنترنت**، ط1، دار الفكر العربي، القاهرة، 2008،ص273-274 .

[2] .سليمان قوراري: **دور التربية والتوجيه في الحماية والوقاية من الجرائم الإلكترونية**، اعمال المؤتمر الدولي الرابع عشر، طرابلس، 24-25 مارس 2017، تاريخ الإطلاع 2019/05/28،ص7 ..

وبسبب الأخطار والأضرار والتحديات التي نواجهها قدمت الباحثة إسراء جبريل رشاد مرعي بعض الأساليب الوقائية في بحثها المنشور إلكترونيآ ومنها :

-إستعمال ما يطلق عليه جدار الحماية ويكون بمثابة الدور الذي تقوم به جمارك الحدود وذلك للحيلولة دون دخول الأجسام الغريبة والضارة.

- إستخدام تقنية التشفير لمنع إنتشار المعلومات.

- إستعمال تقنية التوقيع الإلكتروني لتجنب تزوير الرسائل الإلكترونية.

- ضرورة إمتلاك نسخ إحتياطية لمختلف الملفات الهامة والحساسة ووضعها في أماكن أمنة.

- التعامل بحذر شديد عند فتح البريد الإلكتروني وذلك بالتأكد من هوية باعث الرسالة.[1]

2-الحماية القانونية

في هذا الإطار لا بد من تفعيل الحماية القانونية الصارمة لحماية حق خصوصية المواطنين، والتي تعرف بأنها حق الشخص في حياة معزولة وخاصة، فالشخص له الحق بالعيش بعيداً عن أنظار الناس وعن القيود الإجتماعية.

ولأجل ضمان هذه الحماية وتفعيلها، يوضح الباحث (محمد سعيد مجذوب) أنه قد قامت حركة تشريعية واسعة لحماية الحق بالخصوصية من خلال منع إستخدام وحفظ ومقارنة وتوزيع المعلومات الشخصية بواسطة الكمبيوتر دون ترخيص.[2]

ومن هذا المنطلق وكما ذهبت إليه التطورات الحاصلة في حقوق الإنسان، فعلى السلطات العامة داخل الدولة الحفاظ على حرمة الحياة الشخصية الخاصه، إن تسجيل المعلومات الشخصية التي يقصد بها حفظها بالسجلات، فإن هذا السلوك ينطوي على

---

[1] .سليمان قوراري: **المرجع نفسه**، ص8 .

[2] محمد سعيد مجذوب: **النظرية العامة لحقوق الإنسان تطور الحقوق والحريات العامة والآليات القانونية لحمايتها**، ط1، المؤسسة الحديثة للكتاب، بيروت، لبنان، 2014، ص200 .

خرق جسيم وواضح لحرمة الحياة الخاصة، فإذا قام رجال الشرطة بالإحتفاظ بسجلٍ سري لديهم بغية إستخادمه في حال ترشيح الأشخاص لتولي عمل أو وظيفة ما من الوظائف المهمة في مجال الأمن أو السلك الدبلوماسي، فإن هذا التصرف يعتبر خرقاً فاضحاً لحق الإنسان بالخصوصية في حياته الخاصة، وحرمة المعلومات الشخصية الخاصة به.[1]

[1] محمد يوسف علوان، محمد خليل موسى: **القانون الدولي لحقوق الإنسان الحقوق المحمية**، ط1، دار الثقافة، عمان، الأردن، 2006، ص291 .

الخاتمة

لقد تم بحمد الله وفضله في ثنايا هذه الدراسة التعرف على الجريمة المعلوماتية وواقعها في فلسطين والجزائر وكيف عالجها المشرعين من خلال النصوص القانونية، التي تخص هذا النوع من الجرائم كونها من الجرائم العصرية المستهدفه، وتعد الجريمة المعلوماتية من أبرز وأخطر التحديات الأمنية التي تواجه كافة المجتمعات في العالم، في مجال إستخدام تقنيات المعلومات والإتصالات على مؤسسات القطاع العام والخاص.

ومما سبق يمكن أن نصل إلى نتيجة مفادها أن الجريمة المعلوماتية هي آفة العصر، وهي تحديات ناجمة عن الثورة المعلوماتية التي تواجه العالم وأن لها آثار ونتائج سلبية وإيجابية على الفرد والمجتمع، وبعد أن تطرقنا إلى الجرائم المعلوماتية، نجد أن هذا النوع من الإجرام شكل خطورة على المحيط المعلوماتي وذلك بسبب إتخاذها لأبعاد كبيرة من حيث الأضرار التي تتسبب بها، والتي تؤثر بشكل مباشر على أمن وسلامة الأنظمة المعلوماتية التي تهدف أيضاً بشكل أساسي إلى الغش والإضرار بالمستخدمين.

توصلنا بعد ذلك إلى فكرة أن هذا النوع من الأفعال غير المشروعة يتميز بعدة خصائص تختلف عن الجرائم التقليدية، فلهذا أصبحت الدول تواجه هذا الأخطبوط الذي أنتجته الحضارة التقنية والثورة التكنولوجية التي تمتد أذرعه في جميع أنحاء العالم ولم تفلت من قبضته لا الدول الضعيفة ولا المتطورة، وأستشرى خطره المدمر على مختلف القطاعات في الحياة، وبعد الإنتهاء من هذا البحث توصلنا إلى وجود مشكلة حقيقة في واقع الجرائم المعلوماتية في فلسطين والجزائر، وبناءاً على ذلك توصلنا إلى النتائج والمقترحات التالية:

النتائج:

1-الجريمة المعلوماتية هي الجريمة التي تتكون من فعل أو إمتناع عن فعل بإستخدام إحدى الوسائل المعلوماتية بشكل غير مشروع، بحيث يوقع ضرراً يلحق بالغير يعاقب عليه المشرع الجزائي.

2-تتميز الجريمة المعلوماتية بعدة خصائص لا نجدها في الجرائم التقليدية مثل الطابع التقني لهذه الجريمة، وكونها عابرة للحدود.

3-من أسباب إنتشار الجريمة الإلكترونية وجعلها عابرة للحدود الإنترنت الذي جعل من العالم قرية صغيرة، فقد ترتكب الجريمة المعلوماتية في دولة وتقع نتيجتها في دولة أخرى.

4-محل الجريمة المعلوماتية وموضوعها هو المعطيات والمعلومات الكمبيوترية والذي تستهدفه إعتداءات الجناة بشكل عام، إذ أن هذه الجرائم إما أن تقع على الكمبيوتر ذاته أو بواسطته، وذلك بإعتباره محل الجريمة تارةً ووسيلة لإرتكابها تارةً أخرى.

5-تتسم الجريمة المعلوماتية بصعوبة إكتشافها لأنها لا تترك أي دليل مرئي كما أن الجاني ذكي يخفي آثار جريمته، بحيث لا يترك أثر ملموس خلفه، وأن فقدان هذا الآثر من أهم المعوقات التي تواجه إثبات الجريمة المعلوماتية.

6-يتم ملاحقة مرتكبي الجرائم المعلوماتية عن طريق تطبيق القوانين سارية المفعول، التي أقرها المشرع من خلال قانون رقم 10 لسنة 2018 في فلسطين وقانون المساس بأنظمة المعالجة الآلية للمعطيات ومكافحتها 04/09.

7-تم إنشاء وحدة نيابة الجرائم المعلوماتية في فلسطين التابعة للمباحث العامة في الشرطة الفلسطينية سنة 2013 بهدف مواجهة التحديات القائمة في هذا المجال لمكافحة الجرائم المعلوماتية.

8-لا يوجد سيادة كاملة للفضاء المعلوماتي في فلسطين بسبب سيطرة الإحتلال الصهيوني على النسبة الكبرى من أراضينا مما أدى إلى صعوبة في ملاحقة المجرمين المعلوماتيين.

9-تكاتف وتعاون الجهود الإقليمية والدولية في مكافحة الجرائم المعلوماتية كونها جرام عابرة للقارات وأن هناك تعاون دولي قضائي بخصوص هذا النوع من الإجرام.

10-هناك جهود دولية مبذولة في مجابهة ظاهرة الإجرام المعلوماتي منها الإتفاقيات الدولية التي تعتبر كمرجع لصياغة النصوص المتعلقة بوضع الإطار القانوني لحماية النظام القانوني بشكل عام.

المقترحات:

1-لابد من وضع تعريف شامل للجريمة المعلوماتية حتى يتسنى لذوي الإختصاص التعامل مع هذه الجرائم لأنه من الصعب حصر مصطلحاتها كونها جرائم تجمع بين القانون والتقنية والفنية.

2-لابد من تأهيل أفراد الضبطية القضائية العاملين في الضبط العام (النيابة) والقضاء على كيفية التعامل مع هذا النوع من الإجرام، وأيضاً تأهيل وتدريب العاملين في وحدة نيابة الجرائم المعلوماتية في فلسطين بالشكل المطلوب.

3-إستحداث تشريعات نموذجية لمكافحة الجريمة المعلوماتية يمكن تطبيقها عالمياً وقابلة للإستخدام مع مراعاة التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي.

4- ضرورة مجانسة التشريعات الخاصة للفضاء المعلوماتي والإستخدام الآمن للإنترنت في المنطقة العربية.

5- الدعوة إلى توسيع آليات التعاون العربي في مجال مكافحة الجريمة المعلوماتية، وفتح القنوات العاجلة لطلب المساعدة القانونية المتبادلة.

6-رسم إستراتيجية متكاملة للأمن المعلوماتي ومكافحة الجريمة المعلوماتية بإشراك جميع القطاعات الحكومية والخاصة المعنية بذلك.

7-نشر الوعي والثقافة بين المواطنين بخطورة الجرائم المعلوماتية وكيفية التصدي لها حالة وقوعها وإحاطتهم بإرشادات خاصة للتبليغ عن مثل هذه الجرائم كون الفرد في المجتمع هو الضحية الأولى لمثل هذا النوع من الإجرام.

8-إنتهاج سياسة جنائية واضحة وكفيلة بمواجهة الجرائم المعلوماتية، حيث يتوافر لهذه السياسة مقومات النجاح من المناقشة المستقيضة والتخطيط الشامل والجهات التنفيذية القارة والناشطة والأدوات التشريعية والقضائية المتخصصة والفاعلة لِتتكلل الجهود المبذولة للنجاح في الإطار العام لهذه السياسة في مواجهة الجرائم المعلوماتية.

9-لابد من زيادة قدرة الخبير على نقل الأدلة غير المرئية وتحويلها بشكل غير صحيح إلى أدلة مقروءة أو المحافظة على دعائمها إلى حين القيام بأعمال الخبرة.

10-التوصية بالإستفادة من المجرمين المعلوماتيين بعد معاقبتهم أو تخفيف الحكم عنهم وذلك لأن لهم قدرات خاصة ومميزة بحيث يمكن الإستفادة منها لتعزيز الحماية الإلكترونية للمؤسسات المختلفة وذلك بإشاركهم في الدفاع عن الفضاء المعلوماتي للدولة.

فهرس المصادر والمراجع

أولاً: الإتفاقيات والمعاهدات الدولية:

1-الإتفاقية المنشأة للمنظمة العالمية للملكية الفكرية في ستوكهولم سنة 1967.

2-إتفاقية برن لحماية المصنفات الأدبية والفنية والتي عقدت في برن في سويسرا عام 1886، وتم التعديل عليها في مؤتمرات مختلفة أخرها في باريس عام 1979.

3-الإتفاقية الخاصة لحماية الأشخاص من مخاطر المعالجة الآلية للبيانات والتي وقعت بين المجلس الأوروبي والسوق الإشتراكي لسنة 1980 وبدء التطبيق الفعلي لها بسنة 1985.

4-مؤتمر الأمم المتحدة في مجال مكافحة الجريمة الإلكترونية الثامن والمنعقد سنة 1990.

5-إتفاقية تريبس حول الجوانب التجارية لحقوق الملكية الفكرية لعام 1994.

6-إتفاقية التجارة العالمية (الجات) والصادرة بتاريخ 1995/01/01.

7-معاهدات الويبو لعام 1996 وتنقسم إلى ثلاثة أقسام:

-معاهدة الويبو بشأن حقوق المؤلف.

-معاهدة الويبو بشأن الأداء والتسجيل والصوتي.

-معاهدة الويبو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة.

8-الإتفاقية الخاصة لمكافحة إساءة إستعمال التكنولوجيا لأغراضٍ إجرامية الصادرة بسنة 2001.

9-إتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام 2001.

10-القانون العربي النموذجي الإسترشادي لمكافحة جرائم تقنية المعلومات لسنة 2003.

ثانياً: النصوص التشريعية الدولية والوطنية (القوانين):

1-قانون جرائم تقنية المعلومات رقم 60 لسنة 2014 لدولة البحرين، المنشور في الجريدة الرسمية البحرينية العدد 3178 بتاريخ 2014/10/09، و الصادر في قصر الرفاع بتاريخ 2014/09/20 عن ملك مملكة البحرين حمد بن عيسى آل خليفة.

2-قانون الجرائم الإلكترونية رقم 27 لسنة 2015 لدولة الأردن، والمنشور في الجريدة الرسمية الأردنية العدد 5631، بتاريخ 2015/05/04، والصادر في المملكة الأردنية الهاشمية عن ملك الأردن عبد الله الثاني ابن الحسين.

3-قانون مكافحة تقنية المعلومات رقم 5 لسنة 2012 لدولة الإمارات، والمنشور في الجريدة الرسمية الإماراتية المرسوم رقم 05 بتاريخ 2012، والصادر عن سمو الشيخ خليفة بن زايد آل نهيان.

4-الإتفاقية العربية لمكافحة الجريمة الإلكترونية الصادرة في القاهرة، (قانون الإمارات العربية المتحدة لمكافحة الجريمة المعلوماتية)، بتاريخ 2003/12/21، والتي وقع عليها وزراء الداخلية والعدل العرب نيابةً عن دولهم.

5-قانون العقوبات الفلسطيني رقم 74 لسنة 1936 والمنشور في الوقائع الفلسطينية في العدد 652 المؤرخ في 1936/12/12، المعدل بقانون رقم 16 لسنة 1960 المعمول به حالياً وساري التطبيق في الأراضي الفلسطينية والصادر بتاريخ 1960/04/10.

6-لأمر 66/156المتضمن قانون العقوبات الجزائري المؤرخ في 8 جوان 1966 المعدل والمتمم بالجريدة الرسمية عدد 49

7-القانون رقم 04/09 المؤرخ في 14/شعبان/1430 الموافق 05/غشت/2009، والمنشور في الجريدة الرسمية الجزائرية العدد 47، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمنشور في الجريدة الرسمية الجزائرية العدد 47 المؤرخة في 25/شعبان/1430 الموافق 16/غشت/2009.

8-قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية الصادر في رام الله عن رئيس دولة فلسطين بتاريخ 2018/04/29، والمنشور في الجريدة الرسمية الفلسطينية ممتاز عدد 16 بتاريخ 2018/05/03.

9-قانون نظام مكافحة الجرائم المعلوماتية السعودي لعام 1428هـ.

10-الأمر 156/66 المتضمن قانون العقوبات الجزائري المؤرخ في 8 جوان 1966 المعدل والمتمم في الجريدة الرسمية الجزائرية عدد 49.

ثالثاً: قائمة الكتب باللغة العربية:

1-أحمد محمود مصطفى،جرائم الحاسبات الآلية في التشريع المصري، ط1، دار النهضة العربية، القاهرة، 2010.

2-أمين محمد نوفل، قانون العقوبات العام، كلية الشرطة الفلسطينية، غزة.

3-بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، ط1، دار الفكر الجامعي، الإسكندرية، 2008.

4-البغدادي كميت طالب، الإستخدام غير المشروع لبطاقات الإئتمان، ط1، دار الثقافة للنشر والتوزيع، عمان، 2008.

5-بنعمر الحاج عيسى: الآنتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود ،مجلة الدراسات القانونية السياسية، كلية الحقوق، جامعة الأغواط، العدد 03 ،2006.

6- بوسقيعة أحسن، الوجيز في القانون الجزائي العام، ط10، دار هومة، الجزائر، 2011.

7- بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، ط1، ج1، دار هومة، الجزائر، 2008.

8-بوضياف عمار، النظام القضائي الجزائري، دار ريحانة، الجزائر، 2003.

9-ثروت جلال، قانون العقوبات (القسم العام)، الدار الجامعية، بيروت، 2007.

10-جرادة عبد القادر، مبادئ قانون العقوبات الفلسطيني (الجريمة والمجرم)، م1، مكتبة الآفاق، غزة، 2010.

11-جاسم جعفر حسن، جرائم تكنولوجيا المعلومات، ط1، دار البداية، الأردن، 2012.

12-الحلبي خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2011.

13-حجازي عبد الفتاح بيومي، الجرائم المستحدثة في نطاق تكنولوجيا الإتصال الحديثة، المركز القومي للإصدارات القانونية، القاهرة، 2011.

14-الحسيناوي علي جبار، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، عمان، 2009.

15-حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت(دراسة معمقة في جرائم الحاسب الآلي والإنترنت)، دار الكتب القانونية، القاهرة، 2005.

16-حجازي عبد الفتاح بيومي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2007.

17-خالد محمود إبراهيم، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2009.

18-خالد محمود إبراهيم، حوكمة الإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2011.

19-الخماسي فتحي بن الطيب، الفقه الجنائي الإسلامي، دار قتيبة، دمشق، 2004.

20-الدربي عبد العال، محمد صادق إسماعيل، الجرائم الإلكترونية، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012

21-رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الإسكندرية، 2007.

22-الردايدة عبد الكريم، الجرائم المستحدثة وإستراتيجية مواجهتها، ط1، دار ومكتبة الحامد للنشر والتوزيع، الأردن، 2013.

23-سرور أحمد فتحي، الوسيط في قانون العقوبات، ج1، القسم العام، دار النهضة العربية، القاهرة، 1981.

24-السعيد عبد اللطيف حسن، الحكم الصادر بالإدانة(دراسة قانونية لنظم الحكم الجنائي وفلسفته والعوامل المؤثرة في إصداره في ضوء إتجاهات السياسة الجنائية المعاصرة)، ط1، دار النهضة العربية، القاهرة، 1989.

25-سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الداخلية، دار النهضة العربية، القاهرة، 2013.

26-سلامة مأمون محمد: الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، 2001، ص645

27-شتا محمد محمد، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعية الجديدة للنشر، القاهرة، 2000.

28-شبيلي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، ط2، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2016.

29-شحادي يوسف، الضابطة العدلية علاقتها بالقضاء ودورها في سير العدالة الجزائية، ط1، مؤسسة يحسون للنشر والتوزيع، بيروت.

30-الصغير جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 1992.

31-عبد الله سليمان، شارح قانون العقوبات الجزائري (القسم العام)، ديوان المطبوعات الجامعية، الجزائر، 2002.

32-عياد سامي علي حامد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، مصر، 2007.

33-عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، ط1، دار الكتب والوثائق المصرية، مصر، 2005.

34-العريان محمد علي، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011.

35-العريان محمد علي، الجرائم المعلوماتية، الدار الجامعية الجديد للنشر، الإسكندرية، 2004.

36-عبابنة محمود أحمد، جرام الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2009.

37-علوان محمد يوسف، محمد خليل موسى، القانون الدولي لحقوق الإنسان المحمية، ط1، دار الثقافة عمان،الأردن، 2006.

38-القاضي رامي المتولي، مكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2011.

39-قشقوش هدى حامد، جرائم الحاسب الإلكتروني، دار النهضة العربية، مصر.

40-القهوجي علي عبد القادر، الحماية الجنائي لبرامج الحاسب الآلي، دار الجامعية للطباعة والنشر، بيروت، 1999.

41-قورة نائلة، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي الحقوقية، بيروت، 2005.للنشر والتوزيع، عمان، 2009.

42-اللبيدي إبراهيم محمد، السلوك الإجرامي في جرائم الإنترنت، مركز الإعلام الأمني القاهرة.

43-إبن منظور مسعود (أبو الفضل جمال الدين محمد بن مكرم)، لسان العرب، ط1، دار صابر، لبنان، م3.

44-المسعدي محمود، القاموس الجديد للطلاب، معجم مدرسي ألفبائي، ط7، المؤسسة الوطنية للكتاب، الجزائر، 1991.

45-الملط أحمد خليفة، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، مصر، 2006.

46-المناعسة أسامة أحمد، جلال محمد الزعبي، صايل فاضل الهواوشة، جرائم الحاسوب الآلي والإنترنت، ط1، دار وائل للنشر، عمان، 2001.

47-المناعسة إسامة أحمد، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2010.

48-مراد عبد الفتاح، شرح جرائم الكمبيوتر، الإسكندرية.

49-محمود نجيب حسني، شرح قانون الإجراءات الجزائية، ط2، دار النهضة العربية، القاهرة، 1988.

50-محمد زكي أبو عامر، الإثبات في المواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، 1985.

51-ممدوح عبد الحميد عبد المطلب، جرائم إستخدام الحاسب الآلي وشبكة المعلومات العالمية(الجريمة عبر الإنترنت)، مكتبة دار الحقوق، الشارقة، 2001.

52-مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، دار الكتب القانونية، مصر، 2006.

53-منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.

54-محمد سيد محمد، وسائل الإعلام من المنادي إلى الإنترنت، ط1، دار الفكر العربي، القاهرة، 2008.

55–محمد سعيد مجذوب، النظرية العامة لحقوق الإنسان تطور الحقوق والحريات العامة والآليات القانونية لحمايتها، ط1، المؤسسة الحديثة للكتاب، بيروت، لبنان، 2014.

56–ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012.

57–الهيتي محمد حماد، تكنولوجيا الحديثة والقانون الجنائي، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2004.

58–الهيتي محمد حماد، تكنولوجيا الحديثة والقانون الجنائي، ط2، دار الثقافة للنشر والتوزيع، عمان، 2010.

59–الهيتي محمد حماد، جرائم الحاسوب وماهيتها وموضعها وأهم صورها، دار المناهج للنشر والتوزيع، عمان، 2005.

60–يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، ط1، القاهرة، 2011.

رابعاً: الرسائل الجامعية (الأطروحات، الرسائل، المذكرات) :

أ–أطروحات الدكتوراة:

1–بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه–قانون عام، إشراف البروفيسور البقيرات عبد القادر، بن يوسف بن خده–كلية الحقوق، جامعة الجزائر، 2018.

2–مرسي محمد محمود السيد، تفعيل دور الشرطة في تحقيق الإستقرار الأمني، رسالة دكتوراه، كليه الدراسات العليا، أكاديمية الشرطة، القاهرة، 2014.

ب-مذكرات الماجستير:

1-المومني نهلا عبد القادر، جرائم معلوماتية، رسالة ماجستير، دار الثقافة، عمان، 2010.

2-العفيفي يوسف خليل يوسف، جرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير- تخصص قانون عام، بإشراف الدكتور أيمن عبد العال، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2013.

3-الروقي مروان مرزوق، القصد الجنائي في الجرائم المعلوماتية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، السعودية، 2011.

4-ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، رسالة ماجستير- تخصص سياسة جنائية، إشراف الدكتور جلال الدين محمود صالح، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2012.

5-إبتسام موهوب، جرائم مساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، رسالة ماجستير بإشراف الأستاذة كوثر شريط، جامعة العربي بن مهيدي، كلية الحقوق، 2014.

6-أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون 04/09، رسالة ماجستير-قانون جنائي، بإشراف الدكتور قريشي محمد، كلية الحقوق والعلوم السياسية، جامعة قاصدي برباح، 2013.

7-نبيل محمود فريد أبو الرب، جرائم المعلوماتية والتحديات التشريعية في فلسطين، رسالة ماجستير-تخصص قانون عام، بإشراف الدكتور أنور جانم، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين،2018.

ج-مذكرات الماستر:

1-محمد يزن الأخضر، جرائم الكمبيوتر والإنترنت، مذكرة لنيل رتبة ضابط، المدرسة العليا للشرطة، بن عكنون، 2008.

2-بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية، دراسة مقارنة، مذكرة لنيل شهادة الماستر- تخصص قانون خاص وعلوم جنائية، بإشراف البروفيسوره دموش حكيمة، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، 2018.

3-إيمان مسعود سالم، الجريمة المعلوماتية مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة محمد أمين دباغين، سطيف، 2015.

خامساً: المجلات العلمية:

1-لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها، مجلة الميزان للدراسات الإسلامية والقانونية،م4، ع1، جامعة العلوم الإسلامية العالمية، الأردن، 2017.

2-محمد الأمين البشري، تحقيق في جرائم الحاسب والإنترنت، المجلة العربية للدراسات العربية والتدريب، ع30، الرياض، 2001.

3-بن عمر الحاج عيسى، الإنتربول كألية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود، مجلة الدراسات القانونية السياسية، كلية الحقوق، جامعة الأغواط، ع3، 2006.

4-حمدان هاني، دور العلاقات العامة لدى الأجهزة الأمنية في التوعية الأمنية، مجلة الدراسات الأمنية أكاديمية الشرطة الملكية، عمان الأردن،ع1، 2004.

5-الجمال محمد علي، دور الشرطة الوقائي في إنحسار جرائم العنف، مجلة الأمن العام المصرية، ع163.

سادساً: المؤتمرات الدولية والوطنية (المقالات والأبحاث والأعمال):

1-العادلي صالح، الجرائم المعلوماتية ماهيتها وصورها، ورقة عمل مقدمة لورشة العمل الإقليمية، حول التشريعات حول مكافحة الجرائم الإلكترونية، مسقط، 2-4 أبريل 2006.

2-تقرير بعنوان الحرب الإلكترونية تقلق إسرائيل، مشار إليه عبر الموقع الرسمي لقناة الجزيرة الفضائية، 2013/06/13، WWW.aljazeera.net.

3-محمد محيي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي) في القاهرة 25-1993/10/28، دار النهضة العربية، القاهرة،1993.

4-شرابشة ليندة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية ألقيت في الملتقى الدولي حول التنظيم القانوني للإنترنت والجريمة الإلكتروني، جامعة زيان عاشور، الجلفة، 27-28/أفريل/2009.

5-سليمان قوراري، دور التربية والتوجيه في الحماية والوقاية من الجرائم الإلكترونية، أعمال المؤتمر الدولي الرابع عشر، طرابلس، 24-25/مارس/2017.

6-Hadjira BOUDER: Orientations de la politique pénale de prévention et de lutte contre la criminalité liée aux TIC en Algérie, centre de recherche sue l'information scientifique et technique, CERIST, 03 Rue des frères Assiout, Benaknoun, Alger, Algérie, www.alexalaw.com .

ثامناً: المواقع الإلكترونية:

1- http://samanews.ps

2. https://ar.wikipedia.org

فهرس الموضوعات

المـــــــحتـويــات	رقم الصفحة
مقدمـة	1
الفصل الأول: الأحكام الموضوعية للجريمة المعلوماتية	10
المبحث الأول: مفهوم الجريمة المعلوماتية، نشأتها وخصائصها	11
المطلب الأول: مفهوم الجريمة المعلوماتية	11
الفرع الأول: التعريف اللغوي والإصطلاحي	11
أولاً: تعريف الجريمة لغةً وإصطلاحاً	11
ثانياً: تعريف المعلوماتية لغةً وإصطلاحاً	12
الفرع الثاني: التعريف القانوني والقضائي	13
أولاً: التعريف القضائي للجريمة المعلوماتية	13
ثانياً: التعريف القانوني للجريمة المعلوماتية	14
المطلب الثاني: نشأة وتطور الجريمة المعلوماتية	16
الفرع الأول: المرحلة الأولى لنشأة الجريمة المعلوماتية	16
الفرع الثاني: المرحلة الثانية لنشأة الجريمة المعلوماتية	16
الفرع الثالث: المرحلة الثالثة لنشأة الجريمة المعلوماتية	17
المطلب الثالث: خصائص الجريمة المعلوماتية	18
الفرع الأول: خصائص الجريمة المعلوماتية	18
أولاً: عالمية الجريمة المعلوماتية	18
ثانياً: صعوبة إثبات الجرائم المعلوماتية	19

ثالثاً: الجريمة المعلوماتية جرائم الأذكياء	20
الفرع الثاني: خصائص الجرائم المعلوماتية من حيث مرتكبها	20
أولاً: المجرم المعلوماتي هو إنسان إجتماعي	20
ثانياً: المجرم المعلوماتي هو إنسان ذكي ومتخصص	21
المبحث الثاني: أركان الجريمة المعلوماتية	23
المطلب الأول: الركن المادي للجريمة المعلوماتية	23
الفرع الأول: السلوك	24
أولاً: الصورة الإيجابية	24
ثانياً: الصورة السلبية	25
الفرع الثاني: النتيجة الإجرامية	25
الفرع الثالث: العلاقة السببية	26
الفرع الرابع: أمثلة على الركن المادي في بعض الجرائم المعلوماتية	27
أولاً: جريمة السرقة المعلوماتية	27
ثانياً: جريمة القذف والذم	27
ثالثاً: جريمة الولوج والبقاء في نظام المعالجة الآلية للبيانات	28
المطلب الثاني: الركن المعنوي للجريمة المعلوماتية	28
الفرع الأول: القصد الإجرامي في الجرائم المعلوماتية	29
الفرع الثاني: الخطأ غير المقصود في الجرائم المعلوماتية	31

الفرع الثالث: أمثلة على الركن المعنوي في الجرائم المعلوماتية	32
أولاً: جريمة تزوير بطاقات الإئتمان	32
ثانياً: جريمة الإتلاف الإلكتروني	32
ثالثاً: جريمة الذم	32
رابعاً: جريمة السرقة الإلكترونية	33
المطلب الثالث: الركن الشرعي للجريمة المعلوماتية	33
الفصل الثاني: الأحكام الإجرائية للجريمة المعلوماتية وطرق مكافحتها محلياً و دولياً	37
المبحث الأول: الجرائم الموجهة ضد نظم المعلوماتية عن طريق الإنترنت وطرق إثباتها	37
المطلب الأول: أنواع الجرائم المعلوماتية	37
الفرع الأول: أنواع الجرائم المعلوماتية	37
أولاً: جريمة الإرهاب التكنولوجي	37
ثانياً: جريمة السرقة و الإحتيال الإلكتروني	39
ثالثاً: جرائم أمن الدولة والتجسس وجرائم الكمبيوتر والإنترنت	40
رابعاً: جريمة تضليل العقول (تكنولوجيا الإعلام المزيف)	40
خامساً: جريمة التزييف والتزوير	42
سادساً: جريمة العبث بالبرامج و تعمد الأذى والتدمير	42
سابعاً: جريمة السطو على بطاقة الإئتمان	43
ثامناً: جريمة الإنتحال	43

تاسعاً: جريمة السب و القذف	43
عاشراً: جريمة المساعدة على الإنتحار	44
إحدى عشر: جرائم الجنس والعرض عبر الإنترنت	45
المطلب الثاني: الإثبات في الجرائم المعلوماتية	46
الفرع الأول: ضوابط إثبات الجريمة المعلوماتية بالأدلة الرقمية والعلمية	48
الفرع الثاني: ضوابط إثبات الجريمة المعلوماتية بالأدلة الإجرائية	51
أولاً: الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته	51
ثانياً: إظهار الحقائق المتعلقة بالجريمة	52
الفرع الثالث: عناصر إثبات الجريمة المعلوماتية	53
أولاً: إظهار الركن المادي للجريمة المعلوماتية	53
ثانياً: إظهار الركن المعنوي	53
ثالثاً: تحديد مكان ووقت إرتكاب الجريمة	54
الفرع الرابع: طرق إثبات الجريمة المعلوماتية	54

أولاً: إثبات الجريمة المعلوماتية بالشهادة	54
ثانياً: إثبات الجريمة المعلوماتية بالإقرار	56
ثالثاً: إثبات الجريمة المعلوماتية بالخبرة الفنية	57

المطلب الثالث: العقوبات المقررة لمرتكب الجريمة المعلوماتية	57
الفرع الأول: العقوبات المطبقة على مرتكب الجريمة المعلوماتية في التشريع الجزائري	57
أولاً: العقوبات المطبقة على الشخص الطبيعي	57
ثانياً: العقوبات التكميلية	59
ثالثاً: العقوبات المطبقة على الشخص المعنوي في الجرائم المعلوماتية	59
رابعاً: عقوبة الإتفاق والشروع الجنائي في الجريمة المعلوماتية	60
الفرع الثاني: العقوبات المقررة لمرتكبي الجريمة المعلوماتية في التشريع الفلسطيني	60
أولاً: العقوبات الأصلية المقررة للشخص الطبيعي	60
ثانياً: العقوبات التكميلية	64
الفرع الثاني: العقوبات المطبقة على الشخص المعنوي	65
الفرع الثالث: العقوبة في جريمة الإتفاق والإشتراك والتحريض و الشروع	65
المبحث الثاني: مكافحة الجريمة المعلوماتية	66
المطلب الأول: الطرق المنتهجة في مكافحة الجريمة المعلوماتية	66
الفرع الأول: مواجهة الجريمة المعلوماتية على المستوى الدولي	67
أولاً: إتفاقية برن	67
ثانياً: معاهدة الويبو	70

ثالثاً: إتفاقية تريبس	72
الفرع الثاني: مساعي بعض الأجهزة الدولية في مواجهة الجريمة المعلوماتية	75
أولاً: دور الأمم المتحدة في مواجهة الجريمة المعلوماتية	75
ثانياً: دور المجلس الأوروبي في مواجهة الجريمة المعلوماتة	76
ثالثاً: دور المنظمة الدولية (الإنتربول)	77
رابعاً: دور الجامعة العربية في مواجهة الجريمة المعلوماتية	79
المطلب الثاني: دور التشريع الجزائري والفلسطيني في مكافحة الجريمة المعلوماتية	80
الفرع الأول: آليات مكافحة الجريمة المعلوماتية في الجزائر	80
أولاً: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحته	81
ثانياً: دور الضبطية القضائية في مواجهة الجريمة المعلوماتية	82
ثالثاً: السلطة القضائية في مواجهة الجريمة المعلوماتية	84
الفرع الثاني: آليات مكافحة الجريمة المعلوماتية في فلسطين	85
أولاً: نيابة الجرائم الإلكترونية	85
المطلب الثالث: آليات الوقاية من الجريمة المعلوماتية	87
الفرع الأول: دور المؤسسات الرسمية ومؤسسات المجتمع المدني في الوقاية من الجرائم المعلوماتية	87

الفرع الثاني: دور التربية والتوجيه في الوقاية من الجريمة المعلوماتية	**90**
أولاً: الجانب التربوي	**90**
ثانياً: الجانب التوجيهي	**91**
الخاتمة	**95**
المصادر والمراجع	**100**
فهرس الموضوعات	**114**

فهرس المصادر والمراجع

الفصل الأول

الأحكام الموضوعية للجريمة المعلوماتية

الفصل الثاني :

الأحكام الإجرائية للجريمة المعلوماتية

وطرق مكافحتها محلياً و دولياً

مقدمة

الخاتمة

فهرس الموضوعات

ملخص :

الجريمة المعلوماتية من الجرائم المستحدثة التي بدأت في الإنتشار بشكل واسع في الآونة الأخيرة وقد إختلف الفقهاء في تعريفها، فهناك من عرفها على أنها كل فعل إجرامي يستخدم الكمبيوتر في إرتكابه كأداة رئيسية كما وقع إختلاف في تسميتها لأنها مصطلح زئبقي صعب الإمساك والإحاطة به بتعريف خاص، كما يتسم مجرم الجريمة المعلوماتية بأنه متخصص وله القدرة الفائقة والمهارة التقنية، ويعد الدليل الإلكتروني كدليل إثبات جنائي وله قوته الثبوتية فيها، وقد تضمنت هذه الدارسة معطيات قانونية وأخر فنية وتقنية نظراً لطبيعة الموضوع الذي يعتبر نقطة تقاطع بين علوم الحاسوب والنظم المعلوماتية والعلوم القانونية، كما أن كافة الدول تسعى إلى تحقيق التعاون الدولي من أجل التصدي لهذه الجريمة ، كما أن هناك محاولات لتطوير المنظومة القانونية وتكييفها مع المعطيات الدولية من خلال إستحداث تشريعات نموذجية لمكافحة الجريمة المعلوماتية حتى لايبقى الأفراد تحت مقصلة الجريمة المعلوماتية.

Abstract :

spread widely in recent times. The scholars have differed in their definition. There are those who define it as any criminal act used by the computer as a main tool and it has a different name because it is a mercurial term, The crime of cybercrime is specialized and has the ability and technical skill, and the electronic guide as evidence of criminal evidence and its strength, which included the study of legal and other technical because of the nature of the subject, which is a point of intersection between computer science and As well as attempts to develop the legal system and adapt it to international standards through the introduction of model legislation to combat cyber crime so that individuals remain under .the guillotine of information crime.