واقع الحماية الجزائية في المجال الإلكتروني وفقاً للقانون الفلسطيني

The reality of criminal protection in the electronic field according to Palestinian law

د. جهاد نزار دغمش: دكتوراه في الدراسات القانونية المقارنة، غزة

Dr. Jihad Nizar Doghmosh : PhD in Comparative Legal Studies، Gaza

Email: jehad19950597787026@gmail.com

الملخص:

تتناولت هذه الدراسة واقع الحماية الجزائية في المجال الإلكتروني وفقاً للقانون الفلسطيني، حيث تطرق إلى واقع مواجهة القانون الجنائي الفلسطيني للجرائم الإلكترونية، وأفق مواجهة الجرائم الالكترونية في المنظومة الجزائية الفلسطينية من خلال الاستشراف لسياسة جنائية فاعلة على الصعيد الوطني من أجل مواجهة حقيقية لنوع خطير من جرائم العصر، وهدفت الدراسة إلى إلقاء الضوء على الواقع الفلسطيني في هذا النوع من التجريم والمواجهة، ولتحقيق أهداف الدراسة فقد استخدام الباحث المنهج تحليلي مقارن، وتوصلت هذه الدراسة إلى مجموعة من التوصيات أهمها العمل على اقرار قانون العقوبات الفلسطيني بما يحويه من التجريم الالكتروني مع التوصية بتشديد العقوبات وعدم ايراد عقوبة بعض الجرائم على سبيل التخيير بين الحبس والغرامة، بالإضافة إلى إيجاد نوع من الجزاءات على مقترفي هذه الجرائم بحيث تكون من نفس نوع العمل، بحيث تتضمن بعض الاجراءات التي تحد من استخدامهم للتقنيات الحديثة، والعمل على اقرار قانون اجرائي يتضمن القواعد الخاصة بالتحري والتفتيش والضبط في المجال الالكتروني وكذلك النص من خلاله على الأدلة الإلكترونية وحجيتها في الإثبات.

الكلمات المفتاحية: الحماية الجزائية، القانون الفلسطيني، الجرائم الالكترونية،، الملاحقة، الإثبات.

ABSTRACT:

This study deals with the reality of criminal protection in the electronic field according to the Palestinian law، as it touches on the reality of confronting the Palestinian criminal law against cybercrime، and the second topic deals with the horizons of confronting electronic crimes in the Palestinian penal system by anticipating an effective criminal policy at the national level in order to confront a real type of dangerous One of the crimes of the age، and the study aimed to shed light on the Palestinian reality in this type of criminalization and confrontation، and to achieve the objectives of the study، the researcher used the comparative analytical method، and this study reached a set of recommendations، the most important of which is working on approving the Palestinian Penal Code

with its contents of electronic criminalization with the recommendation Tougher penalties Not mentioning the penalty for some crimes as a way of choosing between imprisonment and a fine، in addition to finding a kind of penalties for the perpetrators of these crimes so that they are of the same type of work، including some measures that limit their use of modern technologies، and work on approving a procedural law that includes rules for investigation and inspection. And control in the electronic field، as well as the text through which the electronic evidence and its authority in the proof.

Keywords: Criminal protection، Palestinian law، electronic crimes، prosecution، proof.

الإطار المنهجي للدراسة:

المقدمة:

مع التطور الهائل في عالم تكنولوجيا المعلومات ودخول وسائلها إلى شتى مجالات الحياة والذي أدى إلى تعاظم دورها بشكل غير محدود، فقد باتت الحواسيب الآلية والتقنيات الالكترونية وشبكة الانترنت لغة العصر التي لا يمكن الاستغناء عنها، وأصبح الاعتماد عليها كبيرا في أدق التفاصيل التي تتعلق بتسيير المرافق الاقتصادية والاجتماعية والعسكرية والطبية وغيرها، وقد أصبحت هذه الوسائل من الأهمية بمكان بحيث تعاظمت الضرورة في توفير أقصى درجات الحماية لما يحيط بها وذلك تجنبا لتعطيل سير تلك المرافق والمصالح الحيوية أو الاعتداء عليها بما يؤثر على المصالح الجوهرية في حياة الجماعة.

ومع انتشار هذه الوسائل الحديثة للتكنولوجيا بين أفراد المجتمعات وشيوع استخدامها والتوسع في التعامل من خلالها، أضحى لدى كل فرد القدرة على التفاعل والتواصل دون مانع من حدود أو جغرافيا، وذلك مع توافر القدرة على نقل وتلقي المعلومات والتقنيات والاضطلاع على البيانات والبرامج بكل سهولة و يُسر، ومع وجود الحسنات والفوائد الجمة التي رافقت ظهور هذه الحقول الجديدة والمتطورة من العلوم والمعرفة، إلا ان ذلك قد ترافق مع بروز العديد من المشكلات

والسلبيات التي ظهرت على شكل جرائم يقترفها بعض مستخدمي التكنولوجيا والتي تتصف بخطورتها وسهولة ارتكابها ومعضلة عبورها للحدود الوطنية، والتي يمكن أن يطلق عليها الجرائم الإلكترونية.

ويعتبر المجتمع الفلسطيني كغيره من المجتمعات من المتضررين من شيوع الجرائم الإلكترونية بصورة سريعة وعلى مستوى واسع، فلا بد من التصدي لهذه الجرائم من خلال وسائل الدفاع الاجتماعي المتعددة والتي من ضمنها الحماية القانونية الجزائية والتي تعتبر أهم وسائل المجتمع في الحفاظ على كينونته وحماية مصالحه.

ولكن مع حداثة هذه الجرائم وحداثة التشريعات الناظمة للحماية الجزائية في كافة الحقول والمجالات في فلسطين، لا زال هنالك قصور في رسم حدود هذه الحماية من الناحية الجزائية، والذي يتطلب معه إلى التنبه والإسراع إلى توفير الأطر القانونية السليمة والمرجعيات الإجرائية الواضحة لمكافحة هذا النوع الخطير من الجرائم.

مشكلة الدراسة:

من المشاهدات اليومية والتي تلفت الانتباه التوسع الكبير في استخدام الحاسب الآلي والانترنت من قبل جميع شرائح المجتمع، بل والاعتماد عليها في كثير من مجالات الحياة سواء الاقتصادية أو الاجتماعية أو التواصل والاتصال والتي تجعلها تكتسب أهمية كبرى بالنسبة إلى أفراد المجتمع بكل فئاته بحيث أصبحت تشكل مصلحة من مصالح المجتمع والتي تستأهل بناء عليها أن تكون جديرة بالحماية لمساسها بالعديد من المصالح الجوهرية في حياة أفراد المجتمع، وذلك من خلال إسدال ستار الحماية الجنائية على ما يمس أو يتعلق بالحقول الإلكترونية والحاسوب والإنترنت، وعليه يمكن طرح مشكلة البحث في التساؤل الرئيس التالي: ما هو واقع وأفق الحماية الجزائية في المجال الإلكتروني والإنترنت في فلسطين؟

أهمية الدراسة:

ولعل هذه الدراسة من الأهمية بمكان لإلقاء الضوء على الواقع الفلسطيني في هذا النوع من التجريم مع إبداء الرأي والمقترحات بشأن المفاصل المهمة في إرساء قواعد موضوعية وإجرائية تتكامل فيما بينها لتشكل حلقات الحماية للمصالح الاجتماعية المتعاظمة في مجال الحاسوب وتكنولوجيا المعلومات.

هيكل الدراسة:

لا بد من تشخيص الواقع ومن ثم التخطيط لاستشراف مستقبل مواجهة هذا النوع الخطير من الجرائم على أمن واستقرار المجتمعات، وعليه فقد تم تقسيم هذه الدراسة إلى مبحثين، يتناول المبحث الأول واقع مواجهة القانون الجنائي الفلسطيني للجرائم الإلكترونية، ويتناول المبحث الثاني أفق مواجهة الجرائم الالكترونية في المنظومة الجزائية الفلسطينية من خلال الاستشراف لسياسة جنائية فاعلة على الصعيد الوطني من أجل مواجهة حقيقية لنوع خطير من جرائم العصر، بحيث يشتمل على عرض لوضع هذه المواجهة من خلال بيان جوانب الحماية الموضوعية ومن ثم بيان جوانب الحماية الإجرائية.

المبحث الاول: واقع مواجهة القانون الجنائي الفلسطيني للجرائم الالكترونية

المطلب الأول: من حيث التجريم:

حيث أن شرعية التجريم والعقاب من أهم الأسس التي يقوم عليها القانون الجنائي في إطار العمل على حماية المصالح الجوهرية للمجتمع، وكذلك إن التجريم هو الخاصية التي يتمتع بها القانون الجنائي لحماية تلك المصالح إذ انه بهذه الخاصية يتمايز عن غيره من القوانين التي تقوم بتأثيم الفعل أو السلوك ليأتي القانون الجنائي من خلال التجريم ويعزز الحماية القانونية التي تضفيها تلك القوانين من أجل إظهار القوة الجبرية التي تتمترس خلفها القاعدة القانونية لتكون ملزمة وبالتالي ليصبح لديها القدرة على تنظيم حياة الجماعة.

الفرع الأول: التعريف بالجرائم الإلكترونية:

يمكن تعريف الجريمة بشكل عام بأنها " فعل محظور جنائيا، صادر عن إرادة خاطئة، يقرر له المشرع جزاء"[1] أو أنها " عمل أو امتناع يرتب القانون على ارتكابه عقوبة جنائية "[2] وعليه فإن الجريمة إنما هي العصيان الذي يسعى إلى التمرد على إرادة الجماعة مما يجعله متنافيا مع إرادة القانون الذي يحدد الفعل المخالف والعقاب المترتب بناء على الإرادة الجمعية.

[1]- محمود نجيب حسني، شرح قانون العقوبات القسم العام، دار النهضة العربية، القاهرة، ط6، 1989م، ص40.

[2]- محمود محمود مصطفى، شرح قانون العقوبات القسم العام، دار نشر الثقافة، القاهرة، ط10، 1983م، ص140.

ومن هنا ينشأ التمييز بين التأثيم القانوني وبين التجريم الذي يمثل اقصى درجات التاثيم، فالجريمة تمثل إخلالاً بالتزام مهم في حياة الناس والمجتمع مما يجعلها مستأهلة للعقاب.[1]

ويمكن تعريف الجريمة الالكترونية بأنها عبارة عن اعتداء يطال معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت، فهي جريمة تقنية تنشأ في الخفاء يقارفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات.[2]

وللوقوف على الجرائم الالكترونية وبيان ماهيتها لا بد من الإحاطة بالمعنى العام للوسائل التي تقع بها هذه الجرائم ومن ثم محلها وكذلك المصالح القانونية الجديرة بالحماية الجنائية، ولذلك نقف اولا على التعريف بالوسائل الإلكترونية، ومن ثم على المحل الذي يقع عليه الاعتداء في ثانيا، وبعد ذلك نبين المصلحة الجديرة بالحماية الجنائية في ثالثا.

أولا: التعريف بالوسائل الإلكترونية:

إن الوسائل الالكترونية هي ما يرتبط باستخدام التقنيات الحديثة والتي تعتبر كتطبيق للحاسب الآلي بشكل عام وترتبط بتقنيات الاتصالات الحديثة وتكنولوجيا المعلومات[3]، والتي بالتالي ترتبط بشكل أو بآخر بنظام الحاسب الآلي أو الإلكتروني (الكمبيوتر) بحيث يعتبر الكمبيوتر كنظام معلوماتي هو محور التعامل الإلكتروني بغض النظر عن الصورة التي يظهر من خلالها، وأيضا هنالك ما وراء ذلك والذي يربط بين عوالم الاتصال الحاسوبي والذي يعرف بشبكة الإنترنت وعليه فلا بد من الوقوف على معنى الحاسب الآلي أو الالكتروني لبيان الوسيلة الأساسية في الجرائم الإلكترونية، وكذلك توضيح المقصود بشبكة الإنترنت.

التعريف بالحاسب الآلي (الكمبيوتر): يعرف المتخصصون الحاسب الآلي على أنه " جهاز الكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة معينة، من خلال تنفيذ ثلاث عمليات أساسية وهي: استقبال البيانات المدخلة (الحصول على الحقائق المجردة)، ومعالجة البيانات الى معلومات (إجراء الحسابات والمقارنات ومعالجة المدخلات)، وإظهار المعلومات المخرجة (الحصول على النتائج) "[4] وقد عرفه البعض

[1]- رمسيس بهنام، نظرية التجريم في القانون الجنائي، دار النهضة، مصر، 1999م، ص9.

[2]- يونس عرب، جرائم الكمبيوتر والانترنت، اتحاد المصارف،2001، ص19.

[3]- عبد الفتاح بيومي حجازي، الجرائم المستحدثة، ط1، منشأة المعارف، الاسكندرية، 2009م، ص1.

[4] محمد الزعبي وآخرون، الحاسوب والبرمجيات الجاهزة، ط1، دار وائل للنشر، عمان 2002، ص5.

من خلال آلية أو نظام عمله على أنه " عبارة عن مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة طبقا لبرنامج تم وضعه مسبقا للحصول على نتائج معينة "[1] أو هو " آلة حاسبة الكترونية تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرامج معينة بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة "[2]، وبمعنى بسيط يمكن القول بأنه جهاز يهتم بمعالجة البيانات بطريقة آلية مسبقة الضبط بحيث يتم الحصول على نتاج هذه العملية عند الطلب.

هذا وقد عرف مشروع قانون العقوبات الفلسطيني في المادة (379) منه نظام الحاسوب على أنه " جهاز أو مجموعة من أجهزة متصلة أو متواصلة ببعضها البعض أو بواسطة برمجيات، وتقوم بمعالجة المعلومات بشكل آلي.

وبالتالي فإن الحاسوب كنظام متكامل إنما يعمل في إطار معادلة ثلاثية الأطراف، بحيث يتكون من مجموعة من الأجهزة التي تشكل الكيان المادي الملموس لنظام الحاسوب والتي يطلق عيها لفظ (Hard ware) أي المعدات كطرف أول، وكذلك من مجموعة من المعلومات والأوامر أو التعليمات والتي يطلق عليها لفظ (Soft ware) أي البرمجيات، أما الطرف الثالث بالمعادلة والذي يحقق القيمة الفعلية للمعدات والبرمجيات هو وجود الأشخاص الذين يتعاملون مع البرمجيات ويستخدمونها كل حسب هدفه[3].

التعريف بالأنترنت: يمكن تعريف الإنترنت بأنها عبارة عن شبكة الكترونية ضخمة تضم الملايين من الشبكات الداخلية وأجهزة الحاسوب المرتبطة مع بعضها البعض عن طريق الاتصال السلكي واللاسلكي والمنتشرة في أرجاء العالم وتزود المستخدمين على مدار الساعة بمجموعة كبيرة من الخدمات المعلوماتية المتنوعة.[4] وبالتالي فإن هذه الشبكة إنما هي بيئة خصبة لارتكاب الجرائم الإلكترونية والاعتداء ألمعلوماتي.

ثانيا: محل الجريمة الإلكترونية:

يمكن القول بأن الحاسب الآلي إنما هو أساس التعامل الإلكتروني والمعلوماتي، وبالتالي فهو المحور الأساسي الذي تدور حوله وعليه الجرائم الإلكترونية، بحيث يعتبر من أبرز الأخطار التي

[1]- هدى حامد قشوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة 1992، ص6.

[2]- عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، بدون دار او سنة نشر، ص19.

[3]- نهلة عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة، عمان 2008، ص21.

[4]- يوسف ابو فارة، الأعمال الالكترونية، جامعة القدس المفتوحة، رام الله 2012، ص17.

تتهدد الأنظمة المعلوماتية والكمبيوتر هو: التعدي على الكيان المادي للكمبيوتر من خلال الإتلاف أو السرقة أو الاستيلاء، وكذلك التعدي الذي يقع على الإطار المعلوماتي والذي يمكن ان يحدث من خلال:[1] تغيير البرامج، أو إدخال برامج مغلوطة مثل الفيروسات، أو الاطلاع غير المشروع على المعلومات أو الدخول غير المصرح به إلى الشبكات أو قواعد البيانات بصفة مقصودة أو غير مقصودة، وكذلك إدخال المعلومات بقصد التزييف والتزوير سواء بسوء نية أو حسن نية، وأيضا مسح المعلومات أو إخفائها أو عدم إدخالها أو تغييرها، وكذلك مفاتيح التشفير والكلمات السرية.

وخلاصة القول؛ إن محل هذه الجريمة وموضوعها هو المعطيات والمعلومات الكمبيوترية والتي تستهدفها اعتداءات الجناة بشكل عام، إذ ان هذه الجرائم إما أن تقع على الكمبيوتر ذاته وإما بواسطته، وذلك باعتباره محل للجريمة تارة ووسيلة لارتكابها تارة أخرى على محل آخر وهو المعلومات والمعطيات الالكترونية.

ثالثا: المصلحة الجديرة بالحماية الجنائية من خلال التجريم الإلكتروني

إن نقطة الانطلاق في تحديد هذه المصالح هي حماية الحواسيب والأجهزة الالكترونية والاضطلاع بأمن المعلومات التي ترفع على شبكة الانترنت وعلى الحواسيب المرتبطة بها. ويمكن رد مكونات أمن هذه المعلومات والأجهزة إلى العديد من الجوانب على درجة من الأهمية وهي:[2]

- سرية المعلومات: والذي يشمل ما يلزم من تدابير لمنع الاطلاع غير المصرح به على المعلومات السرية أو الخاصة.
- سلامة المعلومات: والذي يشمل التدابير اللازمة لحماية المعلومات من التغيير.
- ضمان الوصول الى المعلومات والموارد الحاسوبية: والذي يشمل حماية إمكانية الوصول إلى المعلومات لمن له الحق بالاطلاع عليها.
- سلامة الأجهزة الحاسوبية والمعدات الالكترونية وما عليها من برامج ومعلومات ومعطيات خاصة.

ولما كان الحاسوب والانترنت من المواضيع التي تهتم بالدرجة الأولى بالمعلومات وتخزينها وتداولها فقد أصبح من الضروري بمكان الاضطلاع بأمن هذه المعلومات وحمايتها، وفي سبيل ذلك قام المتخصصون بالتقنيات وتكنولوجيا المعلومات بصناعة تقنيات وبرامج تقوم بهذه المهمة

[1]- خالد الغثبر ومحمد القحطاني، أمن المعلومات بلغة ميسرة، ط1، جامعة الملك سعود، الرياض، 2009، ص7.

[2]- المرجع السابق، ص23.

من الناحية التقنية والتي تجعل من الحواسيب والشبكات مجالا افتراضيا يحوز كمًّا من المعلومات الخاصة بكل شخص على حدة لتكون ما يقابل الذمة المالية للشخص والتي يمكن ان نطلق عليها مصطلح **"الذمة المعلوماتية او التكنولوجية"**، والتي في نهاية الأمر لا يمكن أن تبقى بهذه الصورة إلا من خلال إضفاء الحماية القانونية والتي تبلغ أقصى درجاتها من خلال إسدال القانون الجنائي حمايته عليها.

وعليه يمكن استخلاص المصالح المستأهلة للحماية الجنائية كما يلي:

- حماية حق السرية، وحرمة الحياة الخاصة
- حماية حق الملكية المعلوماتية والفكرية والذي يمكن أن نطلق عليه الذمة المعلوماتية أو التكنولوجية، وذلك مع اقرار القوانين الخاصة والتي تقرر هذه الحقوق وحمايتها.
- حماية حقوق الملكية المادية على الأجهزة والمعدات وعلى كل الماديات التي يمكن ان يقع عليها أي اعتداء بواسطة الوسائل الإلكترونية.
- حماية النظام العام الالكتروني كجزء من النظام العام الإداري والاقتصادي في الدولة، وذلك مع التوجهات الحديثة للدول باتجاه ما يسمى بالحكومة الالكترونية والتي تذهب باتجاه الإدارة الالكترونية وتقديم العديد من الخدمات والمعاملات من خلال منظومة الكترونية شاملة.

الفرع الثاني: واقع التجريم الإلكتروني في القانون الجنائي الفلسطيني:

أولا: انطباق نصوص قانون العقوبات التقليدي:

إن واقع الجرائم الالكترونية في العصر الحديث فرض نفسه على الساحة التشريعية والقضائية في معظم دول العالم، بحيث أصبح هاجسا لكل المهتمين بالشأن العام، وفي فلسطين ومع انه لا يوجد تشريع خاص بالجرائم الإلكترونية إلا أن هذا الموضوع ونتيجة ضغط الواقع أصبح حائزا على اهتمامات كل القطاعات الناظمة للشأن التشريعي والإداري والاقتصادي في فلسطين.

إلا أن هذا الاهتمام مازال يبارح مرحلة المحاولات التي تهدف للوصول إلى صياغة أطر قانونية حديثة تقوم بتحقيق المواجهة الفاعلة للجرائم الإلكترونية، فبالنسبة للتجريم المطبق في فلسطين فإن المواجهة تقتصر على قواعد قانون العقوبات التقليدي بحيث يتم تطويع هذه النصوص والمفاضلة فيما بينها لتنطبق على السلوك المخالف لتخدم قطاع العدالة في معاقبة مرتكبي هذه الجرائم، والتي في كثير من الأحيان لا تؤدي الغرض المرجو منها في مواجه هذا السلوك سواء

كان ذلك بسبب عدم التكييف القانوني السليم لهذا السلوك وبالتالي افلات المجرم من العقاب أو بسبب عدم كفاية العقوبة المقررة وعدم تناسبها مع حجم الفعل والضرر اللذَين تحققا.

حيث انه يتم ملاحقة بعض الجرائم التي ترتكب بواسطة الكمبيوتر والانترنت عن طريق إسقاط نصوص قوانين العقوبات السارية في فلسطين[1]، مثل نصوص الابتزاز والنصب ونصوص السرقة والإتلاف والتزييف وتقليد الأختام والتزوير وخيانة الأمانة والسب والقذف والتشهير وإفشاء الأسرار والحض على الفجور، بحيث يتم تطبيق هذه النصوص عندما ترتكب هذه الجرائم بواسطة الكمبيوتر أو شبكة الإنترنت، وغني عن البيان بأن هذه النصوص تعتبر قاصرة عن الوفاء بالغرض وبالتالي تدق الحاجة إلى التجريم الإلكتروني الخاص بهذه الجرائم، ذلك أن نصوص هذه الجرائم تنطبق عندما يكون الكمبيوتر وسيلة لارتكاب السلوك وفي بعض الأحيان عندما تقع على الكمبيوتر ذاته إلا أن المجرم في كثير من الأحيان يفلت من العقاب بسبب عدم وجود النص التشريعي المناسب للتجريم.

ثانيا: قانون الاتصالات السلكية واللاسلكية الفلسطيني رقم 3 لسنة 1996م.

حيث ان جهات الملاحقة قد تجد ضالتها التجريمية في نصوص هذا القانون عندما يتعلق السلوك المرتكب بوسائل الاتصال، حيث أن هذا القانون يتعلق بعملية تنظيم الاتصالات وإنشاء وتشغيل الشبكات ومحطات البث واستخدام الموجات، وكذلك يشتمل على الحماية الجنائية لتكنولوجيا الاتصالات في فلسطين وذلك من خلال عرض الجرائم والعقوبات المقررة لها في المواد (86-100)، فمن ضمن ما نص عليه هذا القانون جريمة إجراء الاتصال بشكل غير مشروع (90/أ) وجريمة استخدام وسائل الاتصالات في تحقيق اغراض غير مشروعة (91/أ)، وجريمة تقديم اتصالات مخالفة للنظام العام والآداب العامة (91/ب)، وجريمة اعتراض أو تعويق أو تحوير محتويات رسائل اتصالات (3/92)، وجريمة إخفاء الرسائل أو رفض نقلها أو انشائها والعبث في مضمونها (3/93)، وغيرها من الجرائم المتعلقة بالاتصالات والشبكات.

علما أن هذا القانون يعتبر من القوانين الحديثة نسبيا في مجال تكنولوجيا الاتصالات كونه يتعلق بمعالجة الجوانب الفنية لعملية الاتصالات ذاتها وكذلك معالجة الإطار الرقابي وضبط المخالفات والجرائم التي ترتكب في إطار الإساءة لتقنية الاتصالات [2]. إلا أنه في نهاية المطاف ومع

[1]- ينطبق قانون العقوبات الأردني رقم 16 لسنة 1960م مع تعديلاته لسنة 1967م في الضفة الغربية، وينطبق قانون العقوبات الفلسطيني الانتدابي رقم 74 لسنة 1936م في قطاع غزة.

[2]- عبد الفتاح بيومي حجازي، الجرائم المستحدثة، مرجع سابق، ص315.

وجود بعض النصوص التي تجرم سلوكيات تدخل في إطار الجرائم الإلكترونية إلا انه بالمجمل لا يشتمل على الحماية الجنائية الكافية التي يمكن أن تستوعب الأفعال التي ترتكب في إطار الجرائم الإلكترونية.

ثالثا: مشاريع القوانين ذات العلاقة بالجرائم الإلكترونية:

في إطار إدراك المؤسسات لأهمية الجرائم الالكترونية فقد تبين ذلك من خلال إدراج بعض مشاريع القوانين التي تختص في الشأن الإلكتروني، ومن هذه المحاولات هو مشروع قانون العقوبات الفلسطيني[1]، والذي يتعرض وبشكل مباشر لجرائم الحاسوب والانترنت في الباب الخامس منه في المواد (379-396)، هذا وقد جاءت هذه النصوص بمجملها لتلبي الحد الأدنى من متطلبات التجريم في مواجهة الجرائم الإلكترونية، ذلك أن الأمر لا يخلو من النقد في إطار عدم اشتمال هذا المشروع على بعض صور الجرائم الالكترونية مثل الاطلاع غير المشروع على المعلومات، وكذلك جسامة العقوبات وإيرادها على سبيل التخيير بين الحبس والغرامة والذي يوسع حدود السلطة التقديرية للقاضي وخصوصا في الحد الأدنى الذي يمكنه معه إقرار عقوبات بسيطة جدا لا ترقى إلى مستوى مواجهة هذه الجرائم الخطيرة.

وكذلك من محاولات المشرع الفلسطيني لمواجهة الجرائم الالكترونية مشروع قانون الإنترنت والمعلوماتية رقم (8) لسنة 2002، والذي يتكون من تسعة فصول ويضم (35) مادة، بحيث يمكن اعتبار هذا المشروع امتدادا وتكميلا لما بدأه المشرع في قانون الاتصالات السلكية واللاسلكية لسنة 1996، ذلك أنه يعطي هذه الصورة كونه جاء على ذكر هذا القانون في مقدمة المشروع، وكذلك نص في المادة (25) منه على استكمال ما لسلطات الضبط في القانون المذكور تضاف سلطات جديدة، علما أن هذا لا يمكن عده انتقادا للمشروع بقدر ما هو بيان للوجهة القانونية التي يسير في نطاقها هذا المشروع. وقد نص هذا المشروع على الجرائم والعقوبات المتعلقة **بالأنترنت** والمعلوماتية في المواد (26-31) منه، وعلما أنه يتبنى وزارة الاتصالات كمرجعية إدارية وضبطية في إطار الإجراءات التي ينص عليها، وهو الذي يلاحظ من خلاله إغفاله لصلاحيات سلطات الضبط القضائي التي تختص بملاحقة الجرائم **الإلكترونية** والتي تحتاج إلى نصوص قانونية لإضفاء المشروعية الإجرائية في إطار الضبط والملاحقة، فهناك ضعف عام في تناول الجوانب الإجرائية والإثبات بحيث تؤسس لمشروعية الدليل **الإلكتروني**، أما في الجانب

[1]- مشروع قانون العقوبات الفلسطيني رقم 2001/93م.و، المقر بالقراءة الأولى من المجلس التشريعي الفلسطيني بتاريخ 2003/4/14م.

الموضوعي فيمكن القول بحق هذا المشروع ما قيل بحق مشروع قانون العقوبات من نقد في سبيل إبرازها كملاحظات لأخذها بعين الاعتبار عند إتمام المعالجة التشريعية لهذه المشاريع.

المطلب الثاني: على سبيل الملاحقة والإثبات:

إن الاعتماد على نظم المعلومات والكمبيوتر والشبكات في الاعمال في ازدياد مستمر ولا تزال تثار مشكلة امن هذه النظم والشبكات، إذ أن المشكلة الحقيقية تكمن في حمايتها وحماية محتواها من انشطة الاعتداء عليها.

وإن المواجهة الحقيقة لأي نوع من الجرائم إنما تظهر للعيان عندما يكون هناك أجهزة مختصة وإجراءات مقننة تظهر من خلالها القدرة على الملاحقة والكشف وإحراز الأدلة وصولا إلى إثبات الجريمة او السلوك المخالف للقانون امام الجهات القضائية المختصة تمهيدا لمحاكمته وإقرار العقوبات الرادعة بحق مقترف السلوك.

أولا: إنشاء وحدة الجرائم الالكترونية في جهاز الشرطة الفلسطيني:

وفي فلسطين فقد تم إنشاء وحدة الجرائم الالكترونية التابعة لإدارة المباحث العامة في الشرطة الفلسطينية في سنة 2011م، وذلك بمبادرة من مدير عام الشرطة بهدف مواجهة التحديات القائمة في هذا المجال لمكافحة الجرائم الالكترونية كظاهرة من الظواهر الإجرامية المستحدثة والتي تتطلب طواقم وإجراءات ومعدات خاصة والتي ترتكب إما عن طريق وسائل الاتصال المختلفة أو باستخدام الحاسوب والإنترنت، وتعمل هذه الوحدة جاهدة وباستخدام الطرق التكنولوجية الحديثة للكشف عن الجرائم، وكذلك التعرف على الجناة بهدف تقديمهم إلى العدالة.

هذا وتسعى هذه الوحدة إلى توفير الأدلة اللازمة لإثبات الجرائم الإلكترونية، وتسعى وبالعمل مع النيابة العامة للخروج بآليات قانونية سليمة للتحصل على الأدلة الإلكترونية التي يمكن استخدامها لإدانة المتهمين، وكذلك تعمل على صياغة دليل إرشادي للعاملين يبين إجراءات البحث والتحري في الجرائم الالكترونية وذلك بهدف توضيح الإجراءات الواجبة الإتباع وتسهيل مهمات جمع الأدلة.

ثانيا: التحري والتفتيش والضبط

يقصد بالتحري بالاصطلاح القانوني بحث واستقصاء الحقائق، وهو عمل أمني وقانوني يقوم به المتحري للحصول على معلومات وبيانات تعريفية او توضيحية عن الاشخاص او الأشياء او

الأماكن، وذلك للحد من الجرائم أو ضبطها لتحقيق الامن والحفاظ على النظام العام[1]، وقد نص قانون الاجراءات الجزائية الفلسطيني على أن يتولى مأمورو الضبط القضائي البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى [2]، وهو الذي يذهب معه المشرع في إقرار التحري كصلاحية لمأموري الضبط القضائي يقومون بها بهدف استقصاء الجرائم وضبطها.

ويمكن القول بان التحري الالكتروني إنما يتم عبر الحواسيب ونظم المعلومات وشبكة الانترنت وهو عمل أمنى وقانوني يقوم به مأموري الضبط القضائي بواسطة بواسطة التقنيات الإلكترونية والرقمية للحصول على المعلومات عن الأشخاص أو الأماكن أو الأشياء وذلك للحد من الجرائم أو ضبطها[3].

وقد نظم القانون قواعد التفتيش ودخول المنازل والانتقال إلى مسرح الجريمة وإجراء الكشف والمعاينة، فقد نص القانون الأساسي الفلسطيني في المادة 2/11 منه على عدم جواز تفتيش الشخص أو حبسه أو الاعتداء على حريته إلا بأمر قضائي وفق أحكام القانون، وكذلك نص قانون الاجراءات الجزائية الفلسطيني على اجراءات الكشف والمعاينة والانتقال الى مسرح الجريمة وأقر كذلك قواعد دخول وتفيش المساكن واقر لها حرمة خاصة بحيث لا يجوز دخولها او تفتيشها إلا بأمة من جهات الاختصاص[4].

ولكن ما يثور حول هذا الموضوع هو مدى انطباق هذه القواعد التقليدية الخاصة بالتفتيش والكشف والمعاينة على حالة تفتيش نظم الكمبيوتر وقواعد البيانات وتثور أيضا أهمية الاستعانة بالخبرة في هذه المجالات حيث أن الخطأ القانوني في تفتيش وضبط الدليل قد يفوت الفرصة في كشف الجريمة أو إدانة الجاني، حيث ان تفتيش الحواسيب ونظم المعلومات هو تفتيش لما يحفظه الجهاز أو الشبكة عندما يكون مزودا بحافظات الكترونية للعمليات التي تتم عبره، وهو في نهاية الامر تفتيش للفضاء الافتراضي غير الملموس في كثير من الاحيان وبما يصعب معه تحريز الدليل الا من خلال تجميده على شكل مادي ملموس، وكل هذا انما يتعلق بالقدرة على تحديد المطلوب مسبقا من أجل استحضار جميع الاجراءات القانونية اللازمة للنفاذ الى هذه الفضاءات الافتراضية

[1]- مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، مصر (المحلة الكبرى) 2005م، ص23.

[2]- هذا ما نصت عليه المادة 2/19 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[3]- مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، مرجع سابق، ص22.

[4]- وقد جاء ذلك في المواد (21، 27، 39) من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م.

بناء على امر مقنن من السلطات المختصة ذلك ان هذه الاجراءات قد تنطوي على كشف خصوصية البيانات المخزنة في النظام، فإذا لم تكن ضمن الاطار المبين في أوامر التفتيش والضبط فإنها تذهب باتجاه الصيرورة الى بطلان الإجراء وبالتالي بطلان الدليل الذي استمد منه.

ولا بد من الإشارة إلى الهدف الاساسي من إجراءات التفتيش والضبط وهو كشف الاعتداءات والجرائم التي تقع على الافراد والمصالح العامة، حيث أن البيانات المخزنة داخل الحواسيب والنظم ليس جميعها تتصل بجريمة الاعتداء موضوع التفتيش، لهذا فلا بد من المحافظة على الخصوصية وحرمة الحياة الخاصة في معرض الكشف عن الدليل، أو في معرض الإقرار باستخدام دليل ذي طبيعة الكرتونية ذلك أنه حق دستوري قد نص عليه القانون الأساسي الفلسطيني [1]. وهذا عوضا عن أنه من ضمن الأهداف الأساسية للتجريم الالكتروني هو حماية الخصوصية وحرمة الحياة الخاصة بالإضافة إلى الأهداف الأخرى في حماية المصالح الاستراتيجية للجماعة والنظام العام أو المتعلقة بالحقوق الأساسية للأفراد.

ثالثا: أدلة الإثبات في الجرائم الإلكترونية:

وحيث أن التعامل مع هذا النوع من الجرائم إنما يثير العديد من المشكلات الموضوعية الخاصة بالتجريم وكذلك المشكلات الإجرائية المتعلقة بالبحث والتحري وتقديم الدليل في ظل إقامة الدعوى الجزائية على المتهمين، والذي يتطلب معه التعرض لأدلة الإثبات في إطار عملية الملاحقة.

لقد انتهج المشرع الفلسطيني في مجال الإثبات الجنائي مبدأ الإثبات الحر، فقد نص قانون الإجراءات الجزائية الفلسطيني على جواز الإثبات في الدعاوى بجميع طرق الإثبات القانونية وان الحكم الجزائي يخضع لمبدأ الاقتناع الذاتي للقاضي[2]. وهذا ما أكدته أحكام محكمة النقض الفلسطينية[1].

[1]- فقد نص القانون الاساسي الفلسطيني المعدل لسنة 2003م في المادة (32) من على انه " كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع عليه الضرر."

[2]- هذا فقد نص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م في المادة (206) منه على انه "1- تقام البينة في الدعاوى الجزائية بجميع طرق الاثبات إلا إذا نص القانون على طريقة معينة للإثبات.2- إذا لم تقم البينة على المتهم قضت المحكمة ببراءته. " وكذلك نص في المادة (208) على انه " للمحكمة بناءً على طلب الخصوم،

وعليه فإنه المهم في هذا الإطار ان يكون الدليل المتحصل من الادلة التي يقبلها ويعترف بها القانون الفلسطيني، وبالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الإلكترونية، خاصة مع احتمال ظهور أنشطة الجرائم الالكترونية في العديد من مجالات الحياة العامة.

هذا وقد اقر المشرع الفلسطيني بعض الوسائل الحديثة في الإثبات والتي تدخل في إطار الدليل الالكتروني حيث نص في قانون 1البينات رقم 4 لسنة 2001م في المادة (19) من على أنه " 1- تكون للرسائل الموقع عليها قيمة السند العرفي من حيث الإثبات ما لم يثبت موقعها أنه لم يرسلها، ولم يكلف أحداً بإرسالها. 2- تكون للبرقيات ومكاتبات التلكس والفاكس والبريد الإلكتروني هذه القوة أيضاً إذا كان أصلها المودع في مكتب التصدير موقعاً عليها من مرسلها، وتعتبر البرقيات مطابقة لأصلها حتى يقوم الدليل على عكس ذلك."،

ويقصد بالتلكس: جهاز يستعمل للاتصال بين شخصين من خلال امتلاك كل منهما لنفس نوع الجهاز ليشكل وسيلة اتصال من خلال تبادل الرموز والأحرف والأرقام التي تصل إليهما بسرعة فائقة، أما الفاكس: فهو عبارة عن جهاز يقوم بنقل المعلومات الموجودة في سند او وثيقة ما طبقا للأصل وهو مقترن بالهاتف، أما البريد الإلكتروني: فهو وسيلة اتصال عصرية يتم من خلالها تبادل الرسائل بين طرفين يحجزان عنوانين لكل منهما على شبكة الانترنت[2].

أو من تلقاء نفسها أثناء سير الدعوى أن تأمر بتقديم أي دليل تراه لازماً لظهور الحقيقة، ولها أن تسمع شهادة من يحضر من تلقاء نفسه لإبداء معلوماته في الدعوى." وفي تأكيد لهذا النهج ما ذهب اليه حكم لمحكمة النقض الفلسطينية المنعقدة في عزة في الدعوى الجزائية رقم (205) لسنة 2003م " من المقرر قانونا في المواد الجزائية جواز اثباتها بكافة طرق الاثبات ما لم ينص القانون على خلاف ذلك... وإن من ضمن هذه الطرق حسبما نصت عليه المواد (108،106، 109) من قانون البيانات رقم 4 لسنة 2001م القرائن القضائية، كما ان ما استقر عليه قضاء هذه المحكمة ان البينة الظرفية كافية لإثبات التهمة قبل فاعلها "، وكلك نصت الفقرة الاولى من المادة (273) على انه " 1- تحكم المحكمة في الدعوى حسب قناعتها التي تكونت لديها بكامل حريتها ولا يجوز لها أن تبني حكمها على أي دليل لم يطرح أمامها في الجلسة أو تم التوصل إليه بطريق غير مشروع."

[1]- وفي تأكيد لهذا النهج ما ذهب اليه حكم لمحكمة النقض الفلسطينية المنعقدة في عزة في الدعوى الجزائية رقم (205) لسنة 2003م " من المقرر قانونا في المواد الجزائية جواز اثباتها بكافة طرق الاثبات ما لم ينص القانون على خلاف ذلك... وإن من ضمن هذه الطرق حسبما نصت عليه المواد (108،106، 109) من قانون البيانات رقم 4 لسنة 2001م القرائن القضائية، كما ان ما استقر عليه قضاء هذه المحكمة ان البينة الظرفية كافية لإثبات التهمة قبل فاعلها "

[2]- أحمد الحلو وآخرون، الأدلة الإلكترونية (الجوانب القانونية والتقنية)، معهد الحقوق، جامعة بيرزيت، رام الله 2015م، ص35.

المبحث الثاني: أفق مواجهة القانون الجنائي الفلسطيني للجرائم الالكترونية

يمكن تعريف السياسة التشريعية بأنها الأفكار والأهداف الرئيسية المراد تحقيقها والتي توجه القانون في مراحل إنشائه وتطبيقه، وأما السياسة الجنائية فهي مجموعة القواعد والمبادئ التي تتحدد على ضوئها صياغة نصوص القانون الجنائي سواء فيما يتعلق بالتجريم أو الملاحقة او الوقاية والمعالجة[1].

إن تحقيق مبادئ السياسة الجنائية لظاهرة معينة إنما تقتضي في بداية الامر رصد هذه الظاهرة ودراستها بصورة مستفيضة بحيث تتوافر جميع المعلومات المحيطة بها. ومن ثم تحديد ملامح الحماية القانونية لهذه الظاهرة، بحيث يتم استظهار المصالح التي تدور في فلك تقنينها، وذلك كله وصولا الى تحديد النقص في نصوص التجريم التي يمكن من خلالها إسدال ستار الحماية الجنائية على تلك المصالح المعتبرة والجديرة بالحماية، وذلك كله مع الاخذ بعين الاعتبار أسباب الوقاية والمنع.

واستطرادا في استكمال بيان ملامح هذه السياسة فإن الأدوات التشريعية التي تحقق مبادئ السياسة الجنائية إنما تتمثل بالقانون الجنائي بمعناه الواسع والذي يشتمل على ما يتعلق بالتجريم من قواعد موضوعية تتحدد بها الأفعال التي تشكل الاعتداءات على هذه المصالح وتشمل كذلك على ما يتعلق بالإجراءات الجنائية والتي لا سبيل إلى تطبيق القواعد الموضوعية الا من خلالها سواء ما تعلق منها بالإثبات أو ما تعلق منها بالملاحقة [2].

وعليه فإن من الاهمية بمكان تجريم وملاحقة هذه الظاهرة المستحدثة وذلك بغرض مكافحتها وتقليل الاضرار الناجمة عنها من خلال استشراف الإجراءات الضرورية التي يجب العمل على اتخذها من اجل الوصول الى مكافحة والتصدي لهذا النوع من الاجرام المستحدث والذي يتطلب الجهد الكبير والمتنوع من جهات عدة، فنحن بحاجة الى التجريم القانوني و الى الحماية المعلوماتية من خلال اقرار بروتوكولات وانشاء هيئات متخصصة لهذا الغرض وكذلك التثقيف المجتمعي والمؤسساتي بوسائل الحماية المعلوماتية.

[1]- أحمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة 1972م، ص10.

[2]- أحمد فتحي سرور، أصول السياسة الجنائية، المرجع السابق، ص17.

المطلب الأول: جوانب الحماية الجنائية الموضوعية:

أولا: إقرار القوانين المتعلقة بتبادل المعلومات وتداول البيانات والحقوق المتعلقة بالحاسوب والذمة المعلوماتية من أجل ايجاد القاعدة التي يستند اليها التجريم في حمايته للحقوق.

إذ انه وفي هذا الاطار لا بد من ايجاد مجموعة من القواعد التي تشتمل على الآليات التي تنظم أعمال جمع البيانات وتخزينها ومعالجتها ونقلها، وكذلك وضع القواعد التي تنشئ للأفراد الحقوق المعلوماتية المتعلقة بالكمبيوتر ونظم المعلومات وشبكة الانترنت والتي يتم من خلالها تنظيم الدخول الى المواقع الخاصة بهم وحقوق أصحابها بسلامتها وصحتها وقدرتهم على تغييرها وتعديلها، وأيضا إقرار الحماية الإدارية والتنظيمية والمدنية، بحيث يشكل من مجموعها القانون الذي يقرر الحقوق ويرتب الالتزامات على كل افراد المجتمع بما يتعلق بالبيانات والمعلومات الخاصة بالحواسيب والشبكات ووسائل الاتصال الحديثة.

ويمكن القول بأن التشريعات التي قطعت شوطا في حماية الخصوصية إنما ذهبت إلى توفير الإطار التشريعي الذي يكفل الحق في المعلومات وحرية تدفقها وانسيابها والحق في الحياة الخاصة ومبدأ عدم الاعتداء على البيانات الشخصية، وقد اشتملت قواعدها حماية الحياة الخاصة للأفراد من مخاطر جمع وتخزين ومعالجة واستخدام هذه البيانات والتي يمكن أن يتم جمعها من قبل الهيئات ومراكز المعلومات، وقد تضمن بعضها قيودا على نقل البيانات خارج الحدود وغير ذلك من القواعد التي يتلخص مضمنها في حماية امتلاك الشخص وتحكمه في معلوماته وبياناته الشخصية.[1]

ثانيا: إقرار القواعد الجزائية الموضوعية والتي تتضمن تحديد الافعال التي يمكن اعتبارها اعتداء على الحقوق المعلوماتية وتجريم هذه الافعال مع اقرار العقوبات المناسبة والتي يمكن أن يتحقق من خلالها الردع العام والخاص بحق مرتكبيها.

بالإضافة إلى إيجاد نوع من الجزاءات على مقترفي هذه الجرائم بحيث تكون من نفس نوع العمل بحيث تتضمن بعض الإجراءات التي تحد من استخدامهم للتقنيات الحديثة.

هذا وتتعدد صور الاعتداءات والجرائم وتتعدد وسائل وأهداف ارتكابها والتي من ضمنها الاطلاع غير المشروع، والتخريب المعلوماتي، ومنع الوصول إلى المعلومات الحاسوبية والاستيلاء على المواد أو المعلومات الحاسوبية. فهناك اعتداءات تقع على الحواسيب نفسها كجسم

[1]- بولين أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، ط1، منشورات الحلبي الحقوقية، بيروت 2009م، ص450.

مادي وهناك اعتداءات تقع عليها كجسم معلوماتي، وأيضا هناك من الاعتداءات ما يقع بواسطة الكمبيوتر وشبكة الانترنت والانظمة المعلوماتية، وبالتالي تتعدد اشكال وصور هذه الاعتداءات بتعدد الافعال التي تصلح لأن تتم من خلال استخدام الحاسوب والانترنت، مثل السرقة والنصب وغسل الأموال والسب والقذف والتشهير والتزوير... وغيرها.

ويمكن القول بأن تقسيم الجرائم الالكترونية الى جرائم هدف ووسيلة ومحتوى هو الاتجاه الذي تتبعه التدابير التشريعية في اوروبا، حيث أن افضل ما يظهر هذا التقسيم هو الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت لعام 2001 – ذلك ان العمل منذ مطلع عام 2000 يتجه إلى وضع اطار عام لتصنيف جرائم الكمبيوتر والانترنت، ويسعى إلى وضع قائمة الحد الأدنى محل التعاون الدولي في حقل مكافحة الجرائم الالكترونية، وهو جهد تقوده دول اوروبا لكن وبنفس الوقت بتدخل ومساهمة من قبل امريكا وأستراليا وكندا،، حيث أوجدت الاتفاقية الأوروبية تقسيما تضمن اربع طوائف رئيسة لجرائم الكمبيوتر والانترنت وهي على النحو التالي:[1]

الطائفة الأولى: - الجرائم المرتكبة ضد (السرية والسلامة والمصداقية) الخاصة بكينونة بيانات ونظم الحاسوب وتضم:

- الدخول غير المشروع أو غير المصرح به.
- المراقبة أو الاعتراض غير المشروع.
- التداخل والتشويش على البيانات.
- التاخل والتشويش على النظم.
- إساءة استخدام الأدوات والأجهزة.

الطائفة الثانية: الجرائم المرتبطة بالحاسوب وتضم: -

- التزوير بواسطة الحاسوب.
- الاحتيال بواسطة الحاسوب

الطائف الثالثة: الجرائم المرتبطة بالمحتوى وتضم طائفة الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية ودعارة الأطفال.

الطائفة الرابعة: الجرائم المرتبطة بالعدوان على حق المؤلف والحقوق المجاورة – قرصنة البرمجيات.

[1]- المذكرة التفسيرية للاتفاقية الأوروبية حول الجريمة الافتراضية، ترجمة وتحقيق عمر محمد يونس، بدون دار نشر، 2005م، ص15

ويمكن الإشارة هنا إلى أن نصوص مشروع قانون العقوبات الفلسطيني تتبنى نفس هذا التقسيم، حيث يلاحظ أن مشروع القانون الفلسطيني لم ينص على طائفة الجرائم المتعلقة بالخصوصية وحماية البيانات حيث ان الاتفاقية الأوروبية قد غفلتها كونها مدرجة في اتفاقية مستقلة لحماية البيانات الاسمية من المخاطر المعالجة الآلية للبيانات، وذلك ان إرهاصات إعداد المشروع كانت في نفس مرحلة المصادقة على الاتفاقية الأوروبية المشار اليها والذي يفهم من خلاله ان المشرع إنما تبنى تقسيما حديثا لهذه الجرائم وبما يتفق مع التوجهات الدولية بهذا الخصوص.

إلا انه ما زال لم يتم استكمال الخطوات القانونية لإقرار هذا المشروع وإخراجه الى حيز التنفيذ، والذي يبقي الغموض مكتنفا الجوانب الموضوعية للجرائم الالكترونية.

المطلب الثاني: الحماية الإجرائية

أولا: الضبط الإداري:

من خلال المنع والوقاية من هذه الجرائم، من خلال جهات متخصصة وفرض برامج الحماية وإمكانيات الوصول والذي تنتهجه بعض الدول، وكذلك مراكز الرصد والبحث الاستقصائي والتحليل المعلوماتي المتخصص في مجال تكنولوجيا المعلومات لتحديد مواطن الخلل ودراسة الظواهر الإجرامية المستحدثة والمتعلقة بشبكة الحاسوب والانترنت واقتراح انسب السبل للمواجه المبكرة.

وقد أعطى قانون الاتصالات الفلسطيني رقم 3 لسن 1996م سلطات الضبط الإداري لموظفي وزارة الاتصالات وقد فوض بعضهم صلاحيات الضبط القضائي وقد فوضهم العديد من الصلاحيات في هذا المجال.[1] ولكن هذا لا ينفي عن بعض الاجهزة المختصة في حفظ الامن والنظام العام صلاحياتها في الضبط الإداري.

ثانيا: الضبط الجنائي:

والذي يتضمن الملاحقة الإجرائية من قبل سلطات الضبط القضائي لمرتكبي هذه الجرائم، وذلك من خلال اقرار قواعد اجرائية خاصة بمتابعة وملاحقة هذه الجرائم ومرتكبيها، بحيث تعطي مأموري الضبط القضائي وسلطات التحقيق الإمكانيات القانونية الإجرائية والقدرة على التحرك

[1]- فقد نصت المواد (82-85) على سلطات الضبط وصلاحياتها وما يتعين عليها القام به، من قانون الاتصالات السلكية واللاسلكية الفلسطيني رم 3لسنة 1996م.

السريع والمواجهة من خلال تمكينهم قانونيا من خلال إقرار الإجراءات التي تمكنهم ممن ضبط هذه الجرائم.

ولعل بعض القواعد الاجرائية تذهب باتجاه الاستفادة من هذه التطورات التكنولوجية الحديثة بحيث تستخدم هذه النظم في التواصل فيما بين السلطات المختصة لتحقق السرعة في المواجهة، بحيث يتم استخدام التقنيات الحديثة في التواصل وإقرار الإجراءات والذي يتطلب معه إيجاد الكوادر المتخصص في جميع مراحل هذه الإجراءات ابتداء من مأموري الضبط القضائي مرورا بجهات التحقيق وانتهاء بسلطة المحاكمة والعقاب.

وهناك الكثير من التحديات الاجرائية لجرائم الكمبيوتر والانترنت والتي تواجه سلطات الضبط القضائي، وذلك كونها تتمتع بطبيعة افتراضية تجعلها متمايزة عن غيرها من الجرائم التقليدية، حيث أن هذه الجرائم لا تترك أثرا ماديا في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما ان مرتكبيها يملكون القدرة على إتلاف او تشويه او إضاعة الدليل في فترة قصيرة. وأهم الصعوبات التي تواجه الملاحقة الإجرائية هو ما يتعلق بإجراءات التفتيش ومحله، إذ أن التفتيش في هذا النمط من الجرائم عادة ما يتم على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، وقد تتجاوز هذه الجرائم من النظام المشتبه به إلى أنظمة أخرى مرتبطة به وفي ظل الوضع الحالي على مستوى العالم من شيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية، فإن امتداد التفتيش الى النظم غير النظام المشبه به يخلق التحديات الكبيرة في مدى قانونية الإجراء في الاصل وكذلك مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش[1].

ثالثا: في الإثبات وضبط الدليل:

وكذلك عملية الضبط لا تتوقف على تحريز جهاز الكمبيوتر فقد يمتد من ناحية ضبط المكونات المادية الى مختلف اجزاء النظام التي تزداد يوما بعد يوم، والاهم ان الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام او النظم المرتبطة بالنظام محل الاشتباه، اي على اشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف، وهذه الحقائق تثير مشكلات متعددة، منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز إضافة الى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه[2].

[1]- هلالي احمد، تفتيش نظم الحاسب الآلي، ط1، دار النهضة العربية، القاهرة 1997م،ص137

[2] يونس عرب، جرائم الكمبيوتر والانترنت، اصدار اتحاد المصارف العربية، 2001م، ص126.

وهذا هو ايضا حال الأدلة المتحصلة من التفتيش والضبط في الجرائم الإلكترونية ذلك أن الدليل الجنائي اما يجب أن يتصف بالوضوح والعقلانية والإقناعية والمشروعية وذلك بجانب موضوعيته وقضائيته[1].

وكذلك هنالك ما يثار حول قواعد الاختصاص القضائي وذلك كون هذه الجرائم في كثير من الاحيان انما هي بطبيعتها عابر للحدود ولا ترتبط بجنسيات ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود وما يحتاجه ذلك الى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية[2].

وعليه فان البعد الاجرائي لجرائم الكمبيوتر والانترنت ينطوي على تحديات ومشكلات جمة، عناوينها الرئيسة، الحاجة الى سرعة الكشف خشية ضياع الدليل، وخصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم، وقانونية وحجية أدلة جرائم الكمبيوتر والإنترنت، ومشكلات الاختصاص القضائي والقانون الواجب التطبيق. والحاجة الى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود والذي يجعل هذه الجرائم محل اهتمام الصعيدين الوطني والدولي [3]. وهذا كله إنما يذهب بنا الى ضرورة مواكبة التطورات الإجرائية والحاجة الى الخصوصية بالإجراء وهذا كله مرتبط بشكل عام بالمشروعية الإجرائية التي يجب توافرها وذلك كاستثناء سلبي على حرية القاضي في الاقتناع بالدليل ذلك أن الحرية في تكوين القانعة مقيدة بالمشروعية فلا يجوز للقاضي الحكم إلا بناء على أدلة مشروعة.[4] بحيث يتطلب اقرار قواعد اجرائية خاصة وتشكيل اجهزة الضبط القضائي المختصة قانونيا وتقنيا بحيث تواكب القدرات المتعاظمة للإجرام الالكتروني مع توفير كامل الإمكانات المادية والتدريبية.

ولعله من المناسب في اقرار القوانين ذات الصلة التأكيد على وجود بعض الوسائل والأدلة الالكترونية الحديثة مثل بطاقات الصراف الآلي وبطاقات الائتمان والكمبيالة الإلكترونية، وأيضا النص بما يقنن التوقيعات الالكترونية والسجل الالكتروني والبصمة الالكترونية[5]، وكل ما يمكن الإفادة منه في إطار تسهيل المواجهة من أجل الوصول الى حماية النظام العام الالكتروني، ولعل

[1]- أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، دار النهضة العربية، القاهرة 2010م، ص382.

[2]- يونس عرب، مرجع سابق، ص130.

[3]- يونس عرب جرائم الكمبوتر والانترنت، المرجع السابق، ص133.

[4]- أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، المرجع السابق، ص401.

[5]- أحمد الحلو وآخرون، الأدلة الإلكترونية (الجوانب القانونية والتقنية)، مرجع سابق، ص38.

مشاريع القوانين والتي ما زالت قيد الدراسة والإقرار [1]، يمكن أن تشكل المحاور الأساسية في توفير الغطاء التشريعي القانوني لهذا الفضاء الإلكتروني الافتراضي ولكن يجب ان يتم ذلك في إطار تكاملي بحيث يضمن شمولية المواجه.

الخاتمة:

لقد تم بحمد الله وفضله في ثنايا هذه الدراسة التعرف على واقع الحماية الجزائية في المجال الإلكتروني وفقاً للقانون الفلسطيني، وذلك من خلال عرض التعريف بالجرائم الالكترونية وبيان محلها والمصلحة المحمية جنائيا من خلال التجريم الالكتروني وتم أيضا التعرف على واقع التجريم الالكتروني في القانون الجنائي الفلسطيني وبيان جهات الملاحقة الإجرائية ابتداء مع عرض لمشروعية التحري والتفتيش والضبط، ومن ثم أدلة الإثبات الالكتروني في التشريعات الالكترونية، وبعد ذلك تم عرض الآفاق التي يمكن من خلالها تخطيط سياسة جنائية فاعلة في مواجهة هذه الجرائم وذلك من خلال بيان القواعد الموضوعية واجبة الإقرار وكذلك بيان القواعد الإجرائية الخاصة بالملاحقة وكذلك توفير اطار المشروعية الإجرائية للأدلة المتحصلة أثناء التفتيش واستقصاء الجرائم الالكترونية.

النتائج:

1- تعرف الجريمة الالكترونية بأنها عبارة عن اعتداء يطال معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت.
2- يعتبر الكمبيوتر كنظام معلوماتي هو محور التعامل الالكتروني بغض النظر عن الصورة التي يظهر من خلالها، ويعرف على أنه جهاز يهتم بمعالجة البيانات بطريقة آلية مسبقة الضبط بحيث يتم الحصول على نتاج هذه العملية عند الطلب.
3- يتم ملاحقة بعض الجرائم التي ترتكب بواسطة الكمبيوتر والانترنت عن طريق إسقاط نصوص قوانين العقوبات السارية في فلسطين، وتعتبر هذه النصوص قاصرة عن الوفاء بالغرض وبالتالي تدق الحاجة إلى التجريم الالكتروني الخاص بهذه الجرائم.

[1]- مشروع قانون العقوبات، ومشروع قانون المعاملات الالكترونية ومشروع قانون الانترنت والمعلوماتية، ومشروع قانون المبادلات والتجارة الإلكترونية، واخيرا مشروع قانون حماية البيانات والخصوصية الذي قرر مجلس الوزراء تشكيل لجنة لعداده.

4- تظهر المواجهة الحقيقة لأي نوع من الجرائم عندما يكون هناك أجهزة مختصة وإجراءات مقننة تظهر من خلالها القدرة على الملاحقة والكشف وإحراز الأدلة وصولا إلى إثبات الجريمة او السلوك المخالف للقانون امام الجهات القضائية المختصة تمهيدا لمحاكمته وإقرار العقوبات الرادعة بحق مقترف السلوك.

5- تواجه وحدة الجرائم الالكترونية العديد من المعيقات سواء منها المتعلقة بالإمكانات أو ما هو متعلق بالمعيقات الاجرائية من الناحية القانونية ومشروعية الاجراءات والادلة المستخلصة، وهو الذي يستأهل معه الوقوف على اقرار القوانين سواء المتعلق بالتجريم أو الملاحقة والاثبات.

التوصيات:

1- العمل على اقرار قانون العقوبات الفلسطيني بما يحويه من التجريم الالكتروني مع التوصية بتشديد العقوبات وعدم ايراد عقوبة بعض الجرائم على سبيل التخيير بين الحبس والغرامة، بالإضافة إلى إيجاد نوع من الجزاءات على مقترفي هذه الجرائم بحيث تكون من نفس نوع العمل، بحيث تتضمن بعض الاجراءات التي تحد من استخدامهم للتقنيات الحديثة.

2- العمل على اقرار قانون اجرائي يتضمن القواعد الخاصة بالتحري والتفتيش والضبط في المجال الالكتروني وكذلك النص من خلاله على الأدلة الإلكترونية وحجيتها في الإثبات.

3- التوجه نحو التخصص في الأعمال الإجرائية الخاصة بالجرائم الإلكترونية، وذلك من خلال العمل على تعزيز دور وحدة مكافحة الجرائم الإلكترونية في الشرطة، والعمل على تشكيل وحدة خاصة بالتحقيق في هذه الجرائم في النيابة العامة، مع إيجاد قضاء متخصص ويمتلك التدريب اللازم للنظر في الجرائم الإلكترونية.

4- الانضمام الى المؤسسات والاتفاقيات الدولية التي تُعنى بمكافحة الجرائم الإلكترونية.

5- تعزيز التعاون الدولي الشرطي والقضائي بهدف تبادل المعلومات والخبرات والتدريب فضلا عن المساعدة المتبادلة في كشف هذه الجرائم.

قائمة المراجع

1. أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، دار النهضة العربية، القاهرة 2010م.
2. أحمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة 1972م.
3. أحمد الحلو وآخرون، الأدلة الإلكترونية (الجوانب القانونية والتقنية)، معهد الحقوق، جامعة بيرزيت، رام الله 2015م.
4. بولين أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، ط1، منشورات الحلبي الحقوقية، بيروت 2009م.
5. خالد الغثبر ومحمد القحطاني، أمن المعلومات بلغة ميسرة، ط1، جامعة الملك سعود، الرياض، 2009م.
6. رمسيس بهنام، نظرية التجريم في القانون الجنائي، دار النهضة، مصر، 1999م.
7. عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، بدون دار او سنة نشر.
8. مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، مصر (المحلة الكبرى) 2005م.
9. محمود نجيب حسني، شرح قانون العقوبات القسم العام، دار النهضة العربية، القاهرة، ط6، 1989م.
10. محمود محمود مصطفى، شرح قانون العقوبات القسم العام، دار نشر الثقافة، القاهرة، ط10، 1983م.
11. عبد الفتاح بيومي حجازي، الجرائم المستحدثة، ط1،منشأة المعارف، الاسكندرية، 2009م.
12. محمد الزعبي وآخرون، الحاسوب والبرمجيات الجاهزة، ط1، دار وائل للنشر، عمان 2002م.
13. نهلة عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة، عمان 2008م.

14. هدى حامد قشوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة 1992م.

15. هلالي احمد، تفتيش نظم الحاسب الآلي، ط1، دار النهضة العربية، القاهرة 1997م.

16. يوسف ابو فارة، الأعمال الالكترونية، جامعة القدس المفتوحة، رام الله 2012م.

17. يونس عرب، جرائم الكمبيوتر والانترنت، اتحاد المصارف،2001.

18. يونس عرب، جرائم الكمبيوتر والانترنت، اصدار اتحاد المصارف العربية، 2001م.