جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني**

*المستشار د. عبد الكريم الشامي

تمهيد:

أدى التطور التكنولوجي الكبير إلى ازدياد أهمية الكمبيوتر(الحاسوب) في شتى مجالات الحياة المعاصرة، فلم يعد يوجد فرع من أي نشاط إلا ويستخدم في معاملاته الكمبيوتر ومن اكثر الأنشطة التي تستخدم الكمبيوتر البنوك والشركات والهيئات والمطارات وغيرها، بل هناك من يرى بان المجتمعات المعاصرة ستصوت قريبا من خلال جهاز الكمبيوتر مباشرة.

إن هذا التطور المذهل للكمبيوتر أدى إلى نشوء جرائم ناتجة عن ذلك الاستخدام، وهذه الجرائم إما أن تقع على الكمبيوتر ذاته، وإما أن تقع بواسطة الكمبيوتر حيث يصبح أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية.

ونظرا لازدياد الجرائم المتعلقة بالكمبيوتر شرعت الدول المتمدينة بوضع تشريعات جنائية خاصة لمكافحة جرائم الكمبيوتر التي تعتبر ظاهرة مستحدثة في علم الإجرام ومن هذه الدول الولايات المتحدة الأمريكية وفرنسا وكذلك الاتحاد الأوروبي الذي وضع اتفاقية حوّل جرائم الكمبيوتر سنة ٢٠٠١م، والتي أوصت فيها الدول الأعضاء باتخاذ كافة الإجراءات التشريعية أو غيرها حسب الضرورة لجعل الدخول إلى جميع نظم الكمبيوتر أو أي من أجزائه بدون وجه حق جريمة جنائية بحسب القانون المحلي، كما أوصت هذه الاتفاقية على مجموعة من المبادئ

** ورقة عمل مقدمة للأمانة العامة لمجلس وزراء الداخلية العرب (سبتمبر ٢٠٠٤).

* مستشار بديوان الفتوى والتشريع – مجلس الوزراء

العامة المتعلقة بالتعاون الدولي في مجال الشؤون الجنائية، وحددت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول الأعضاء في غياب الاتفاقيات الدولية.

أما في الدول العربية ومن ضمنها فلسطين فقليلا ما نجد تشريعات خاصة بمكافحة جرائم الكمبيوتر ويستثنى من هذه القاعدة سلطنة عمان التي أصدرت المرسوم السلطاني رقم ٢٠٠١/٧٢ الذي تضمن جرائم الحاسب الآلي وحدد فيه الجرائم التالية:

- الالتقاط غير المشروع للمعلومات أو البيانات.
- الدخول غير المشروع على أنظمة الحاسب الآلي.
- التجسس والتنصت على البيانات والمعلومات.
- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير البيانات أو وثائق مبرمجة أيا كان شكلها.
- إتلاف ومحو البيانات والمعلومات.
- جمع المعلومات والبيانات وإعادة استخدامها.
- تسريب البيانات والمعلومات.
- نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكا لقوانين حقوق الملكية والأسرار التجارية[1].

أما في فلسطين لا يوجد تشريع خاص يتعلق بجرائم الكمبيوتر والإنترنت إلا أنه يمكن ملاحقة هذه الجرائم عن طريق تطويع نصوص قانون العقوبات

[1] محمد أمين الرومي (جرائم الكمبيوتر والإنترنت) دار المطبوعات الجامعية – إسكندرية سنة ٢٠٠٣ – ص٨،٩.

الفلسطيني بحيث ينطوي تحت لوائها بعض الجرائم المتعلقة بالكمبيوتر كنصوص جرائم السرقة والنصب وخيانة الأمانة والإتلاف وغيرها. ولكن يهمنا أن نشير إلى أهمية التطور التشريعي لتحديد ماهية السياسة الجنائية الواجب اتباعها وفقا للقانون الأساسي المعدل ٢٠٠٣م، والذي اشتمل على الضمانات الدستورية الخاصة بمكافحة الجريمة ومن بينها أنه لا جريمة ولا عقوبة إلا بنص قانوني، ولا توقع عقوبة إلا بحكم قضائي، ولذلك فقد استطاعت السلطة الوطنية في فترة وجيزة من الزمن من إصدار رزمة من التشريعات القضائية المتطورة منها قانون السلطة القضائية، وقانون الإجراءات الجزائية،وقانون الإجراءات المدنية والتجارية، وما زال هناك مجموعة من التشريعات الجنائية الهامة تحت الإجراء في المجلس التشريعي من بينها مشروع قانون العقوبات والذي تعرض وبشكل مباشر في المواد (٣٩٣-٣٩٧) من الفصل السادس منه لجرائم الحاسب الآلي وهناك مشروع قانون الإنترنت والمعلوماتية، والذي مازال تحت الإعداد في ديوان الفتوى والتشريع بوزارة العدل والذي تضمن العديد من القواعد والأحكام والجرائم والعقوبات المستحدثة فيما يتعلق بالإنترنت والمعلوماتية.

ولا بد من التعرض في هذا البحث لأهم جرائم الكمبيوتر والإنترنت بشكل عام، وكذلك لأهم التشريعات الجنائية في فلسطين وحقيقة جدواها في مكافحة جرائم الكمبيوتر والإنترنت.

خطة العمل :

على ضوء ما تقدم نرى أنه من المفيد تقسيم هذا البحث إلى العناصر التالية :

أولا : جرائم الكمبيوتر.

ثانيا : جرائم الإنترنت.

ثالثا : مشروع قانون العقوبات الفلسطيني.
رابعا : مشروع قانون الإنترنت والمعلوماتية الفلسطيني.
خامسا : النتائج والتوصيات.

أولا : جرائم الكمبيوتر:

لقد كان السبب الرئيس الذي من أجله اخترع الكمبيوتر وتطور عبر أجياله المختلفة يهدف إلى تحقيق خصائص متعددة على سبيل المثال السرعة والدقة والمرونة والطاقة التخزينية وذلك من أجل إثراء الحضارة وتزويدها بوسائل التطور السريعة وما زال هذا السبب قائما حتى وقتنا الراهن. وبالرغم من كثرة هذه الخصائص والقدرات ومالها من مردود إيجابي إلا أن بعضها سيكون محط أنظار واستغلال الكثير من المجرمين وذلك بإساءة استخدام التقنية لأغراضهم الخاصة. وذلك لأن هذه التقنية لديها الاستعداد التام للفساد من قبل هؤلاء المجرمين وغيرهم الذين يستخدمونها لنهب المجتمع والسيطرة عليه دون مراعاة للنظم والقوانين[٢]، ولذلك سنتعرض لجرائم الكمبيوتر على النحو التالي:

١- جريمة سرقة المعلومات والبرامج :

تنشأ جريمة سرقة المعلومات والبرامج بكل فعل من شأنه الاستيلاء على برامج أو معلومات مملوكة للغير من داخل جهاز الكمبيوتر. سواء تم ذلك الاستيلاء على الديسك أو السي دي المحتوي على البيانات والمعلومات، أو عن طريق إدخال فيروس من شأنه نسخ هذه البرامج والمعلومات، أو عن طريق تشغيل جهاز الكمبيوتر والاطلاع على البرامج أو المعلومات المخزنة بداخله.

---

[٢] د. ذياب موسى البداينه (جرائم الحاسب والإنترنت) أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والأبحاث، الرياض، ١٩٩٩ ، ص٩٣-٩٥.

وقد عالج قانون العقوبات الفلسطيني لسنة ١٩٣٦ جريمة السرقة في القسم الخامس منه تحت عنوان الجرائم المتعلقة بالأموال. وبما أن قانون العقوبات المعمول به في قطاع غزة هو من زمن الانتداب البريطاني فقد أولى المشرع الجنائي الفلسطيني أهمية لهذا الموضوع في مشروع قانون العقوبات فيما يتعلق بجرائم الاعتداء على الأموال (السرقة والجرائم الملحقة بها).

٢- جريمة الاستعمال غير المشروع للكمبيوتر:

يطلق على هذه الجريمة سرقة وقت الكمبيوتر. وتتحقق هذه الجريمة بأن يقوم شخص باستعمال أو استخدام أو استغلال الكمبيوتر بدون تصريح بذلك من صاحب الشأن مثال ذلك أن يقوم موظف باستخدام كمبيوتر الشركة التي يعمل بها في إنجاز مصالحه الشخصية، فهذا الشخص يعد قد انتفع بالجهاز دون أن يدفع مقابل مادي لذلك الاستغلال.

التكييف القانوني لجريمة سرقة وقت الكمبيوتر :

جرى العمل في فلسطين والدول العربية وفقا لقوانين العقوبات على اعتبار سرقة المنفعة غير معاقب عليها ولكن الفقه اختلف على اعتبار هذا الفعل يشكل جريمة سرقة أو نصب أو خيانة أمانة.

أما في فرنسا فلا القانون الفرنسي ولا القضاء الفرنسي يعاقب على جريمة سرقة وقت الكمبيوتر وكذلك القضاء في الولايات المتحدة الأمريكية[٣].

٣- جريمة إتلاف البرامج والمعلومات :

الإتلاف أو التعييب أو التخريب هو التأثير على مادة الشيء بحيث يذهب أو يقلل من قيمته الاقتصادية والإتلاف لا يشترط فيه إفناء مادة الشيء ولكنه يتحقق بكل

[٣] محمد أمين الرومي، مرجع سابق ص٤٩-٥١.

فعل من شأنه أن يجعل الشيء غير صالح للاستخدام المعد له.

الإتلاف إما أن يكون عن عمد وقصد. وإما أن يكون بغير قصد كما أن الإتلاف قد يكون كليا ويتمثل في محو البرامج والمعلومات المخزنة داخل الجهاز كله.أو جزئيا ويطلق عليه (تشويه أو تعييب) ويتمثل ذلك في إدخال فيروس داخل الجهاز بحيث يعمل على التقليل من كفاءته أو بطء حركة الجهاز.

أما بالنسبة لطرق إتلاف البرامج والمعلومات الموجودة على جهاز الكمبيوتر فهي عديدة نذكر منها[٤]:

أ. استخدام برنامج القنبلة المنطقية.

ب. استخدام برنامج القنبلة الزمنية.

ج. استخدام برنامج الدودة.

كما يوجد العديد من الوسائل التي تساعد على انتقال العدوى بالفيروس عن طريق شبكة الإنترنت ومن أهمها انتقال العدوى عن :

أ. البريد الإلكتروني.

ب. الإرهاب.

ج. نسخ البرامج.

د. تحميل برامج من الشبكات.

ه. التخريب بواسطة الموظفين.

و. الجاسوسية.

ويتضمن قانون العقوبات الفلسطيني لسنة ١٩٣٦ والمعمول به في قطاع غزة في

[٤] لمزيد من المعلومات عن الفيروسات أنظر د. اللواء. د. محمد فتحي عيد (جرائم الحاسب الآلي) الفصل السادس، أكاديمية نايف العربية للعلوم الأمنية – مركز الدراسات والبحوث – الرياض ١٩٩٩.

القسم السادس منه مجموعة من الجرائم والعقوبات المتعلقة بإتلاف أو إضرار الأموال بسوء نية وقد أجملها في المواد من ٣١٧ إلى ٣٣٢ منه.

إضافة إلى ذلك فإن مشروع قانون العقوبات الفلسطيني قد خصص الفصل الخامس منه وبشكل أكثر دقة ووضوحا فيما يتعلق بجرائم التخريب والتعطيل والإتلاف حيث نص في المادة ٣٨٣ منه على أن (كل من خرب أو أتلف عمدا مالا مملوكا للغير أو جعله غير صالح للاستعمال يعاقب بالحبس وبغرامة لا تتجاوز ألف دينار أو بإحدى هاتين العقوبتين).

٤- جريمة التحويل الإلكتروني غير المشروع للأموال :

أدى انتشار استخدام الكمبيوتر في كافة القطاعات والمجالات ومنها البنوك والشركات إلى ظهور جريمة التحويل الإلكتروني غير المشروع للأموال عن طريق استخدام جهاز الكمبيوتر. وفيها يقوم الجاني بتحويل كل أو جزء من أرصدة الغير أو فوائدها إلى حسابه الخاص. ويتم ذلك عن طريق إدخال بيانات غير صحيحة ومغلوطة إلى جهاز الكمبيوتر. كالادعاء كذبا بوجود فواتير مستحقة الدفع. وتتأرجح جريمة التحويل الإلكتروني غير المشروع للأموال بين جريمتين فأحيانا تكيف هذه الجريمة على أنها جريمة نصب. وأحيانا أخرى تكيف على أساس أنها جريمة خيانة أمانة. ونشير هنا إلى أن قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ قد عالج جريمة النصب وكذلك جريمة خيانة الأمانة في المواد ٣٠٠، ٣٠١، ٣٠٢، ٣٠٣، ٣٠٤، ٣٠٥، ٣١٢، ٣١٣، ٣١٤، ٣١٥، ٣١٦.

خصائص الجرائم المتصلة بالكمبيوتر :

تتميز الجرائم المرتكبة بواسطة الكمبيوتر كأداة أو كهدف للجريمة بالخصائص التالية:

١. سرعة التنفيذ: لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكبير،وبضغطة

واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

٢. التنفيذ عن بعد: لا تتطلب جرائم الكمبيوتر في أغلبها (إلا جرائم سرقة معدات الكمبيوتر) وجود الفاعل في مكان الجريمة. بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب...الخ.

٣. إخفاء الجريمة : إن الجرائم التي تقع على الكمبيوتر أو بواسطته كجرائم (الإنترنت) جرائم مخفية، إلا أنه يمكن أن تلاحظ آثارها، والتخمين بوقوعها.

٤. الجاذبية : نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات...الخ.

٥. عابرة للدول : إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا، لا يعترف بالحدود الإقليمية للدول،ولا بالمكان، ولا بالزمان، وأصبحت ساحتها العالم أجمع[٥]. ففي مجتمع المعلومات تذوب

[٥] د. ذياب موسى البداينة (التقنية والإجرام المنظم) ورقة عمل قدمت في الندوة العلمية السابعة والأربعون (الجريمة المنظمة وأساليب مواجهتها في الوطن العربي) الإسكندرية ١٨ – ٢٠/٥/١٩٩٨.

الحدود الجغرافية بين الدول، لارتباط العالم بشبكة واحدة،حيث أن أغلب الجرائم المرتكبة عبر شبكة الإنترنت، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى، وقد يكون الضرر المترتب عن الجريمة ليس واقعا على المجني عليه داخل إقليم دولة الجاني، وتعارض المواد المعروضة مع الثقافات المتلقية لها خاصة إذا كانت تتعارض في الدين والعرف الاجتماعي والنظام الأخلاقي والسياسي للدولة[٦].

٦. جرائم ناعمة: تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح.إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا،فنقل بيانات من كمبيوتر إلى أخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن[٧].

٧. صعوبة إثباتها : تتميز جرائم الإنترنت عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناهي القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة[٨].

---

[٦] د. ذياب البداينة (التطبيقات الاجتماعية للإنترنت) بحث مقدم للحلقة العلمية حول شبكة الإنترنت من منظور أمني، أكاديمية نايف للعلوم الأمنية، بيروت، لبنان.

[٧] طارق عبد الوهاب سليم (الجرائم المرتكبة بواسطة الإنترنت وسبل مكافحتها) بحث مقدم للاجتماع الخامس للجنة المختصة بالجرائم المستجدة، مجلس وزراء الداخلية العرب، تونس، ٧ – ٩ يوليو ١٩٩٧.

[٨] عبد الرحمن البحر (معوقات التحقيق في جرائم الإنترنت في البحرين) رسالة ماجستير غير منشورة – الرياض، أكاديمية نايف العربية للعلوم الأمنية، ١٩٩٩.

٨. التلوث الثقافي : لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة.

٩. عالمية الجريمة والنظام العدلي:نظرا لارتباط المجتمع الدولي إلكترونيا،فقد أصبح مجتمعنا تخيليا مما أدى إلى أن تكون ساحة المجتمع الدولي بكافة دوله ومجتمعاته مكانا لارتكاب الجريمة من كل مكان، مما تطلب أن تمارس الدول المتطورة وخاصة الصناعية على الدول النامية من أجل سن تشريعات جديدة لمكافحة الجرائم المتصلة بالكمبيوتر مما استدعى أن تكون القوانين ذات صبغة عالمية.

الإجراءات الوطنية والدولية لمواجهة جرائم الكمبيوتر:

أ- المستوى الوطني :

نظرا لظهور مشكلة جرائم الكمبيوتر كمشكلة أمنية، وقانونية واجتماعية، فإن خبراء الأمن المعلوماتي وصانعي السياسات الحكومية ومسوقي الكمبيوتر، والأفراد المهتمين في هذا الموضوع بحاجة إلى تغيير نظرتهم تجاه جرائم الكمبيوتر، لا لأنها مشكلة وطنية فقط، وإنما كمشكلة عالمية،وتتطلب الإجراءات الوطنية تعاونا في مجال القطاعين العام والخاص،فعلى القطاع الخاص الالتزام بإجراءات الوقاية، وعلى القطاع العام تنفيذ الإجراءات اللازمة لمكافحة الجريمة،وبوجه عام هناك حاجة إلى تحقيق ما يلي:

١. وجود التشريعات اللازمة لحماية ملكية الكمبيوتر، وللبيانات، والمعلومات والمعدات اللازمة للتشغيل والتوصيل.

٢. زيادة الوعي الوطني لجرائم الكمبيوتر وللعقوبات المترتبة عليها.

٣. إنشاء وحدات مختصة في التحقيق في جرائم الكمبيوتر في المحاكم والشرطة.

٤. إيجاد نوع من التعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

ب- المستوى العربي:

عقدت الجمعية المصرية للقانون الجنائي مؤتمرها السادس في القاهرة في الفترة من ٢٥ إلى ٢٨ أكتوبر ١٩٩٣م وناقشت موضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات من خلال الأبحاث والدراسات المقدمة من الباحثين والتي دارت حول تحديد أنواع الجرائم المختلفة المتعلقة بنظم المعلومات من اعتداء مادي على الأجهزة وأدوات الكمبيوتر بالسرقة أو التخريب أو الإتلاف إلى اعتداء على البيانات والمعلومات المختزنة في قواعد المعلومات بالغش أو التزوير أو السرقة، والحصول على تلك البيانات والمعلومات دون إذن أو الاتجار فيها، والتحايل على الأجهزة للحصول على الأموال، وتحويل ونقل الأموال المتحصلة من الجرائم لغسلها[٩].

وأوضحت البحوث والمناقشات أن الاعتداء قد يحدث أثناء إدخال البيانات والمعلومات أو إخراجها أو من خلال المعالجة الآلية لها، وذلك بالحذف أو المحو أو الإضافة أو التعديل دون حق، وأن هذه المعلومات قد تكون ثقافية أو سياسية أو عسكرية أو اقتصادية أو علمية أو اجتماعية.

وقد بينت الأبحاث والدراسات والمناقشات صعوبة اكتشاف جرائم نظم المعلومات واثباتها، وأكدت على ضرورة تدريب رجال الشرطة القضائية ورجال التحقيق ورجال القضاء، كما حذرت من تزايد احتمالات انتهاك حرمة الحياة الخاصة عن طريق التجسس والتنصت على الكابلات الرابطة بين القواعد الأساسية والوحدات الفرعية.

وفي ختام المؤتمر قد تمكن المؤتمرون من تجريم الأفعال المتعلقة بالكمبيوتر

[٩] لمزيد من المعلومات أنظر اللواء د. محمد فتحي عيد، مرجع سابق (جرائم الحاسب الآلي).

والتوصية باتخاذ التدابير والإجراءات اللازمة والتي تكون على النحو التالي:

- **تجريم الأفعال المتعلقة بالكمبيوتر:**

١. حصول الشخص لنفسه أو لغيره على أموال عن طريق اختراق نظم المعلومات للاستيلاء عليها دون وجه حق.

٢. حصول الشخص لنفسه أو لغيره على بيانات أو معلومات أو مستندات عن طريق اختراق نظم المعلومات دون إذن.

٣. حصول الشخص لنفسه أو لغيره على أموال دون وجه حق عن طريق التحايل على الأجهزة.

٤. تحويل أموال دون حق عن طريق لختراق الأجهزة.

٥. تحويل أموال مستمدة بطريق غير مشروع عن طريق الأجهزة بقصد غسلها وتمويه مصدرها.

٦. إتلاف أو تشويه البيانات أو المعلومات أو المستندات المختزنة في قاعدة المعلومات.

٧. استخدام المعلومات المختزنة في قاعدة نظم المعلومات بقصد المساس بحرمة الحياة الخاصة للغير أو حقوقهم.

٨. تغيير الحقيقة في البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات عن طريق الإضافة أو الحذف أو المحو الكلي أو الجزئي أو التعديل.

٩. حصول الشخص على نسخة من البرامج المختزنة في قاعدة نظم المعلومات دون إذن.

١٠. حصول الشخص على البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات بقصد إفشائها أو قيامه بإفشائها فعلا أو الانتفاع بها بأي طريق.

١١. الاطلاع بأي طريق على المعلومات أو البيانات أو المستندات التي تحويها

قاعدة نظم المعلومات دون إذن بقصد معرفتها.

١٢. التسبب خطأ في حصول الغير على أموال أو بيانات أو معدات أو معلومات أو مستندات أو في ارتكاب فعل من الأفعال المذكورة أعلاه.

- **الإجراءات والتدابير الواجب اتباعها :**

١. مساءلة الأشخاص الطبيعيين والأشخاص المعنويين والمؤسسات الفردية إذا اقترنت الجريمة لصالح الأشخاص والمؤسسات أو بأسمائها بالإضافة إلى مساءلة الأشخاص الطبيعيين من مقترفيها وشركائهم.

٢. إدماج نصوص جرائم نظم المعلومات في قانون العقوبات الوطني على أن يفرد لها فصل خاص.

٣. تدريب رجال الشرطة القضائية ورجال التحقيق والقضاء على كيفية استخدام أجهزة المعلومات وأدواتها وأشرطتها وآلات الطباعة الخاصة بها والإحاطة بكيفية إساءة استخدامها.

٤. تدريب رجال الشرطة القضائية والتحقيق والقضاء على كيفية الكشف عن هذه الجرائم وإثباتها.

٥. حث الدول على التعاون فيما بينها خاصة في مجال المساعدات والإنابة القضائية للكشف عن هذه الجرائم، وجمع الأدلة لإثباتها، وتسليم المجرمين المقترفين لها، وتنفيذ الأحكام الأجنبية الصادرة بالإدانة والعقوبة على رعايا الدولة المقترفين لها بالخارج.

ومن جانب آخر تعكف جامعة الدول العربية ممثلة في الأمانة العامة لمجلس وزراء الداخلية العرب على إعداد مشروع اتفاقية عربية لجرائم الكمبيوتر وكذلك إنشاء لجنة تتألف من ممثلي عدد من الدول الأعضاء لمتابعة كافة المستجدات التقنية والاتفاقيات الدولية المتعلقة بجرائم الكمبيوتر والعمل على توحيد التشريعات

العربية بهذا الشأن،لذلك فقد شاركت السلطة الوطنية الفلسطينية ممثلة بديوان الفتوى والتشريع بتاريخ ٢٠٠٤/٠٩/١٥ بتقديم ورقة عمل حول جرائم الكمبيوتر والإنترنت بالتعاون مع وزارة الداخلية (الإدارة العامة للعلاقات العربية والشرطة الجنائية الدولية الانتربول) (انظر التوصيات).

ج- المستوى الدولي :

الجرائم المتعلقة بالكمبيوتر تتضمن موقفا متحولا أو متنقلا، أو متحركا وذلك بسبب طبيعة الكمبيوتر. فإن إمكانية التخزين متزايدة وكذلك التحريك،وانتقاء البيانات من خلال الاتصال من مسافة بعيدة،والقدرة على الاتصال ونقل البيانات وتحويلها بين الكمبيوتر من مسافات كبيرة. وكنتيجة لذلك فإن عدد الأمكنة والدول التي يمكن أن تكون متورطة في حالات جرائم الكمبيوتر في تزايد.وقد ترتكب الجريمة في نظام عدلي معين وجزئي في نظام ثان وثالث ومن أي مكان في العالم[١٠].

ومع خاصة الحد المتحرك فإنه لا بد من تحديد مكان وقوع الجريمة حيث أن أي نظام قضائي يجب أن يتعامل معها (التحقيق والمحاكمة). أما إذا كانت الجريمة تتطلب تدخل دولتين فإن تصارع الأنظمة القضائية أمر وارد، إذا لم يكن هناك اتفاقيات ثنائية أو قانون دولي تلتزم به الأطراف المعنية.

ويرتبط مع مشكلة الحد المتحرك، مشكلة تتعلق بسيادة الدولة في سن التشريعات للأفعال التي تحصل على أراضيها،والسؤال هنا كيف يتحدد مكان الجريمة، فبعض الدول ترى أن مكان ارتكاب الجريمة يمكن تحديده على مبدأ الوجود في الوقت ذاته حيث يمكن تحديد مكان جريمة بناء على حدوثها في مكان ما أو جزء منها.

أما المبدأ الثاني في تحديد الجريمة فيعتمد على مكان الأثر،فالمكان الذي يظهر فيه أثر الجريمة يعد مكان ارتكابها، وهذا المبدأ مقبول في دول كثيرة، خاصة

[١٠] أنظر د. البداينة – مرجع سابق (جرائم الحاسب والإنترنت) ص ١١٨ – ١٢١.

الأوروبية. وهنا تصبح جرائم الكمبيوتر ذات صلة. (فالفرد الذي يضغط على لوحة مفاتيح الكمبيوتر في بلد (أ) يمكن أن يدخل على بيانات في بلد (ب) ويمكن أن يحولها إلى بلد (ج)، مثل تحويل العملات أو الحوالات المالية.

وتظهر مشكلة أخرى وهي تتعلق بالسلوكيات المنحرفة في الجرائم ذات الصلة بالكمبيوتر وهي تتعلق باستخدام فيروسات الكمبيوتر، فإذا تمكن شخص ما من دخول قاعدة البيانات لأحد البنوك، وغذاها بأحد الفيروسات، وكان هذا الفيروس مبرمجا بحيث ينقل نفسه إلى بلاد أخرى، أو مدن أخرى. وعندما يدمر الفيروس يدمر برنامج البنك، فإن الأثر الناجم عن ذلك يظهر في أكثر من دولة، فأي من هذه الدول لها حق التحقيق والحكم في هذه الجريمة. إن مكان الجريمة هو مكان استخدام الكمبيوتر في تنفيذ العملية (بلد أ) أم البلد الذي تحولت إليه البيانات (بلد ب). والمبدأ الأكثر تطبيقا فيما يتعلق بالجرائم المتصلة بالكمبيوتر يقود إلى نتيجة مفادها أن مكان جريمة الكمبيوتر يتحدد في المكان الذي حصل فيه أحد أجزاء هذه الجريمة، وهذا يتطلب تنسيقا دوليا بين أنظمة العدالة المختلفة فيما يتعلق بالمحاكمة، والعقوبة...[11].

والأساس الآخر يكمن في تطبيق القانون في حالات العناصر الموجودة خارج حدود الدولة، فيما يتعلق بالاحتيال، والتخريب، والاستخدام غير المشروع... بواسطة الكمبيوتر أو للمعلومات الموجودة فيه. والموضوع المشار إليه هنا هو الحماية لبعض أنواع التعديات والجرائم المتصلة بالكمبيوتر في مواضيع الاقتصاد، أو البيانات الحكومية... الحكومات توسع نطاق نظامها العدلي إلى خارج حدودها لحماية أمنها الداخلي.

أما مشكلة الدخول المباشر حيث أن التقنيات الحديثة جعلت من الممكن أن تكون

[11] عبد الرحمن البحر – مرجع سابق.

البيانات متوافرة في بلد ما بينما هي مخزنة في بلد آخر، وهذا الموقف أصبح منتشرا خاصة في شبكات المعلومات الدولية. وهناك من ينظر إلى أن الدخول لقواعد المعلومات الوطنية من خارج الحدود الجغرافية يعد تدخلا في استقلالية الدولة وسيادتها[١٢].

وبما أن العالم مترابط إلكترونيا، فيجب الاهتمام على المستوى الدولي بمشكلة جرائم الكمبيوتر وخاصة في مجال التشريعات والتعاون المتبادل، ويعتقد مركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من جرائم الكمبيوتر تعتمد على الأمن في إجراءات معالجة المعلومات، والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر، ومنفذي القانون، والتدريب القانوني، وتطور أخلاقيات استخدام الكمبيوتر. والأمن الدولي لأنظمة المعلومات. ففي المجال الدولي هناك حاجة للتعاون الدولي المتبادل، والبحث الجنائي والقانوني عن بنوك المعلومات، ففي أوروبا قدمت لجنة جرائم الكمبيوتر توصيات تتعلق بجرائم الكمبيوتر تمحورت في النقاط التالية:

- المشكلات القانونية في استخدام بيانات الكمبيوتر والمعلومات المخزنة فيه في التحقيق الجنائي.
- الطبيعة العالمية لبعض جرائم الكمبيوتر.
- تحديد معايير لوسائل الأمن المعلوماتي وللوقاية من جرائم الكمبيوتر.
- مشكلة الخصوصية وخرقها في جرائم الكمبيوتر.
- موقف ضحايا جرائم الكمبيوتر، هذا وقد لخص التقرير الصادر عن اللجنة الأوروبية جرائم الكمبيوتر في التالي:

١. الاحتيال.

[١٢] د. البداينة – مرجع سابق (جرائم الحاسب والإنترنت) ص ١٢٠.

٢. حذف وتدمير البيانات أو المعلومات أو البرمجيات في الكمبيوتر.
٣. الدخول غير القانوني.
٤. الاعتراض غير القانوني للاتصال بين الكمبيوتر وخاصة في مجال التحويل المالي.
٥. الإنتاج غير القانوني لبيانات، أو معلومات أو برمجيات الكمبيوتر.
٦. وقد أقر الوزراء الأوروبيون في اجتماعهم بتاريخ ١٩٨٩/٠٩/١٣ التوصيات التالية:
١. إدراك أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالكمبيوتر.
٢. أن يؤخذ بالحسبان أن الجرائم المتصلة بالكمبيوتر ذات خاصية تحويلية.
٣. الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني.

الاتفاقية الأوروبية بشأن جرائم الكمبيوتر:

اقتناعا بالحاجة إلى تحقيق سياسة جنائية مشتركة رأت الدول الأعضاء في المجلس الأوروبي وبعد التوصيات التي تقدمت بها اللجنة الأوروبية حول مشكلات الجريمة في مجال جرائم الكمبيوتر تم توقيع هذه الاتفاقية بتاريخ ٢٣/١١/ ٢٠٠١م بغرض حماية المجتمع الأوروبي من جرائم الكمبيوتر وذلك من خلال التقريب بين التشريعات القانونية الجزائية ولتمكين وسائل التحقيق الفعالة فيما يتعلق بهذه الجرائم، وفتح الباب أمام أكبر عدد ممكن من الدول لكي تصبح أطرافا في الاتفاقية لحاجة المجتمع إلى نظام سريع وفعال للتعاون الدولي، والذي يأخذ بعين الاعتبار المتطلبات المحددة لمكافحة جرائم الكمبيوتر.

وتتكون هذه الاتفاقية من ٤٨ مادة مقسمة إلى أربعة فصول تكون على النحو التالي:

الفصل الأول يتضمن تعريفا للمصطلحات الواردة في الاتفاقية ومنها تعريف بنظام الحاسوب والذي يعني أي جهاز أو مجموعة من الأجهزة المتصلة فيما بينها، أو أي أجهزة أخرى ذات علاقة، والتي يقوم واحد أو أكثر منها، بحسب برنامج ما بالمعالجة الأوتوماتيكية للبيانات، كما بين هذا الفصل ما المقصود ببيانات الحاسوب وهو أي عرض أو تمثيل للحقائق أو المعلومات أو الأفكار بشكل ملائم لمعالجتها في نظام الحاسوب،بما في ذلك أي برنامج ملائم يؤدي لقيام نظام الحاسوب بالعمل وأداء وظيفة ما، وكذلك عرف مزود الخدمة بأي جهة عامة أو خاصة توفر لمستخدمي خدماتها القدرة على الاتصال بطريق نظام الحاسوب أو أي جهة أخرى تعالج أو تخزن بيانات الحاسوب بالنيابة عن جهة الاتصال أو مستخدمي تلك الخدمة، كما عرف مرور البيانات بمعنى أي بيانات حاسوب متعلقة بأي اتصال بطريق نظام الحاسوب، ينشئها نظام الحاسوب يشكل جزءا من سلسة اتصال، تشير إلى منشأ الاتصال أو اتجاهه أو طريقه أو وقته أو بياناته أو حجمه أو مدته أو نوع الخدمة أساسا.

أما الفصل الثاني من هذه الاتفاقية فيقع تحت عنوان الإجراءات الواجب اتخاذها على المستوى الوطني والمتمثلة في أن تتبنى التشريعات الجنائية الوطنية (قانون العقوبات العام) للدول الأعضاء في الاتفاقية جرائم ضد سرية وسلامة وتوفر بيانات وأنظمة الحاسوب، كالدخول غير المشروع والتدخل غير المشروع وتشويش البيانات وتشويش النظام وإساءة استخدام الأجهزة والتزييف المرتبط بالحاسوب والاحتيال والجرائم المرتبطة بالصور الإباحية للأطفال والجرائم المرتبطة بالتعدي على حقوق الطبع والحقوق الأخرى ذات العلاقة والمسؤولية والعقوبات

الإضافية[١٣]. ومن جانب آخر أن تتبنى الدول الأعضاء في قانون الإجراءات الجنائية تحديد السلطات والإجراءات الواردة في الاتفاقية بغرض إجراء التحقيقات والإجراءات الجنائية المحددة[١٤]. وكذلك تبيان الشروط واحتياطات الأمان المتمثلة في توفير الحماية الكافية للحقوق وحريات الإنسان، بما في ذلك الحقوق الناشئة عن أي التزامات أخذتها الدول الأعضاء على عاتقها بموجب اتفاقية المجلس الأوروبي لعام ١٩٥٠م، حول حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦م وأي أدوات دولية حول حقوق الإنسان[١٥].

وكذلك أكدت الاتفاقية على ضرورة تحديد الاختصاص بشأن أي جريمة وردت وفقا لأحكام هذه الاتفاقية، عندما ترتكب الجريمة على إقليم الدولة الطرف في الاتفاقية أو على متن سفينة ترفع علمها أو على متن طائرة مسجلة بموجب قوانينها أو من قبل أي من مواطنيها، إذا كانت الجريمة معاقب عليها بموجب قانونها الجنائي أو إذا ارتكبت الجريمة خارج الاختصاص الإقليمي لأي دولة[١٦].

كما حددت الاتفاقية في الفصل الثالث منها المبادئ العامة المتعلقة بالتعاون الدولي والمتمثل في تطبيق الأدوات الدولية ذات العلاقة حول التعاون الدولي في الشؤون الجنائية والإجراءات المتفق عليها على أساس التشريع الموحد أو المتبادل والقوانين المحلية، إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المرتبطة بأنظمة وبيانات الحاسوب أو لجمع الأدلة بشكلها الإلكتروني في

---

١٣ أنظر المادة رقم (٢) من الاتفاقية الأوروبية لجرائم الحاسوب.

١٤ أنظر المادة رقم (١٤) من الاتفاقية.

١٥ أنظر المادة رقم (١٥) من الاتفاقية.

١٦ أنظر المادة رقم (٢٢) من الاتفاقية.

جريمة جنائية[١٧] إضافة إلى ذلك الإشارة إلى المبادئ المتعلقة بالتسليم في الجرائم الجنائية الواردة في الاتفاقية بشرط أن تكون معاقب عليها بموجب قوانين كلا الطرفين المعنيين بسلب الحرية لمدة أقصاها سنة واحدة على الأقل أو بعقوبة أشد. وكذلك الجرائم الجنائية التي يجب أن يتم اعتبارها قابلة للتسليم، أو إذا كان هناك طرف يجعل التسليم مشروطا بوجود اتفاقية تسليم، ثم تلقى طلب تسليم من طرف آخر ليس لديه اتفاقية تسليم معه، فيجوز له أن يعتبر هذه الاتفاقية أساسا قانونيا للتسليم فيما يتعلق بأي جريمة جنائية مشارا إليها في الاتفاقية[١٨]. كما وضعت الاتفاقية مجموعة من المبادئ العامة المتعلقة بالمساعدة المتبادلة لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المرتبطة بأنظمة وبيانات الحاسوب، أو لجمع الأدلة بشكلها الإلكتروني في أي جريمة جنائية[١٩]، كما بينت الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقيات الدولية القابلة للتطبيق[٢٠]. كما استخدمت الاتفاقية مصطلح الشبكة بمعنى أن على كل طرف أن يعين نقطة اتصال متاحة بواقع (٢٤) ساعة في اليوم سبعة أيام في الأسبوع، لضمان توفير المساعدة الفورية لأغراض التحقيقات أو الإجراءات في الجرائم الجنائية المرتبطة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة بشكلها الإلكتروني في جريمة جنائية، مثل هذه المساعدة ستشمل، إذا سمح بذلك القانون المحلي والممارسة، تسهيل أو القيام مباشرة بما يلي:

أ. توفير المساعدة الفنية.

---

[١٧] أنظر المادة رقم (٢٣) من الاتفاقية.

[١٨] أنظر المادة رقم (٢٤) من الاتفاقية.

[١٩] أنظر المادة رقم (٢٥) من الاتفاقية.

[٢٠] أنظر المادة رقم (٢٧) من الاتفاقية.

ب. حفظ البيانات وفقا لما نصت عليه الاتفاقية.

ج. جمع الأدلة وإعطاء المعلومات القانونية، وتحديد المشتبه بهم[٢١].

واختتمت الاتفاقية الفصل الرابع بأحكام نهائية والتي تتضمن العديد من الأحكام والتي من ضمنها إجراء مشاورات بين الأطراف بشكل دوري من أجل تسهيل الأمور التالية:

أ. الاستخدام والتطبيق الفعال لهذه الاتفاقية بما في ذلك تحديد أي مشكلات تعترض سبيلها، وكذلك تأثيرات أي تصريح أو تحفظ تم وفقا لها.

ب. تبادل المعلومات حول التطورات القانونية أو التكنولوجية الهامة أو حول السياسة المتعلقة بجرائم الحاسوب وجمع الأدلة بشكلها الإلكتروني.

ج. دراسة إمكانية استكمال أو تعديل الاتفاقية[٢٢].

بهذا نرى أن هذه الاتفاقية تعد أول وثيقة قانونية دولية (أوروبية) تعتمد تدابير وأحكام حول جرائم الحاسوب والتي جسدت القلق البالغ الذي يساور الدول الأطراف، إزاء جسامة وخطورة جرائم الحاسوب، ومؤمنة بأن العمل الفعال ضد جرائم الحاسوب يتطلب تعاونا دوليا متزايدا وسريعا وفعالا في الأمور الجنائية وكذلك الحاجة لحماية المصالح المشروعة في استخدام وتطوير تكنولوجيا المعلومات.

ثانيا: جرائم الإنترنت:

إن الجرائم التي ترتكب على شبكة الإنترنت أو بوساطتها متنوعة وكثيرة، وهي دائما في ازدياد نتيجة التطور التكنولوجي المتواصل، وقد يكون محل الاعتداء فيها: المال، أو الأشخاص، أو الحقوق الذهنية كالاعتداء على حقوق المؤلف.

---

[٢١] أنظر المادة رقم (٣٥) من الاتفاقية.

[٢٢] أنظر المادة رقم (٤٦) من الاتفاقية.

ويمكن إجمال جرائم الإنترنت[٢٣] على النحو التالي:

١- جرائم الجنس عبر الإنترنت :

إذا كان لشبكة الإنترنت وجه إيجابي فإن لها وجه سلبي أيضا، ومن هذه الأوجه وجود مواقع على شبكة الإنترنت تحرض على ممارسة الجنس للكبار والصغار على حد سواء، وتقوم هذه المواقع بنشر صور جنسية فاضحة للبالغين والأطفال. وإذا كانت الدعوى لممارسة الجنس الموجه للبالغين يمكن أن تلاقى الرفض لتوافر تمام العقل لديهم ، فإن الوضع بالنسبة للطفل يختلف لصغر وعدم اكتمال نضجه العقلي.. لذلك فالطفل اكثر عرضه للانخداع بهذه المشاهد والصور الجنسية الساخنة. ولقد أدى انتشار هذه الصور الفاضحة على شبكة الإنترنت إلى دعوة أعضاء المجتمع الدولي بمكافحة عرض وتوزيع الصور الجنسية للأطفال عبر الإنترنت والعمل على توعية الجمهور لمواجهة الاستغلال الجنسي للأطفال عبر شبكة الإنترنت وكذلك دعوة المشرع الوطني لمحاربة التجارة الجنسية عبر الإنترنت وإلى تجريم كافة صور المعاملات التي تجرى على الصور الجنسية للأطفال سواء عن طريق إنتاجها أو توزيعها أو استيرادها أو حيازتها أو تخزينها داخل جهاز الكمبيوتر أو التعامل فيها بأي طريق من الطرق.

ويلاحظ أن قانون العقوبات الفلسطيني لسنة ١٩٣٦به من النصوص ما تكفي لمعالجة هذه الحالة الإجرامية وإخضاعها للعقاب الجنائي خاصة في الفصل السابع عشر منه المتعلق بالجرائم التي تقع على الآداب العامة، وذلك وفقا لأحكام المواد من ١٥١ إلى ١٦٩ من القانون، كما أولى المشرع الجنائي الفلسطيني عناية وأهمية

---

[٢٣] لمزيد من المعلومات أنظر طارق عبد الوهاب سليم (الجرائم المرتكبة بواسطة الإنترنت وسبل مكافحتها) بحث مقدم إلى الاجتماع الخامس للجنة المختصة بالجرائم المستجدة، مجلس وزراء الداخلية العرب، تونس، ٧ – ٩ يوليو ١٩٩٧.

لهذه الجرائم في مشروع قانون العقوبات، والذي خصص له الفصل الثامن بعنوان (البغاء وإفساد الأخلاق).

٢- جريمة السب والقذف عبر الإنترنت :

بالرجوع إلى قانون العقوبات الفلسطيني لسنة ١٩٣٦ فإنه يمكن تعريف القدح وفقا للمادة ٢٠١ منه على النحو التالي (كل من نشر بواسطة الطبع أو الكتابة أو الرسم أو التصوير أو بأية واسطة أخرى غير مجر د الإيماء أو اللفظ أو الصوت وبوجه غير مشروع مادة تكون قذفا بحق شخص، بقصد القذف بحق ذلك الشخص، يعتبر أنه ارتكب جنحة وتعرف تلك الجنحة بالقدح. كما يعرف القانون الذم في المادة ٢٠٢ منه على النحو التالي (كل من نشر شفويا وبوجه غير مشروع أمرا يكون قذفا بحق شخص آخر قاصدا بذلك القذف في حق ذلك الشخص، يعتبر انه ارتكب جنحة ويعاقب بالحبس مدة سنة واحدة وتعرف هذه الجنحة بالذم. وتعرف المادة ٢٠٣ من القانون القذف على النحو التالي (تعتبر المادة مكونة قذفا إذا اسند فيها إلى شخص ارتكاب جريمة أو سوء تصرف في وظيفة عامة أو أي أمر من شأنه أن يسئ إلى سمعته في مهنته أو صناعته أو وظيفته أو يعرضه إلى بغض الناس أو احتقارهم أو سخريتهم.

إضافة إلى المواد المذكورة أعلاه فإن مشروع قانون العقوبات قد تضمن بين أحكامه هذه الجرائم حيث خصص لها الفصل الرابع عشر منه بعنوان (الاعتداء على الشرف والاعتبار)) وفقا لأحكام المواد ٣٢٣، ٣٢٤، ٣٢٥، ٣٢٦، ٣٢٧، ٣٢٨، ٣٢٩، ٣٣٠، ٣٣١.

ومن جماع هذه النصوص العقابية يمكن توقيع عقوبة القذف والسب العلني أو غير العلني أو القذف بطريق الهاتف على من يقوم بإرسال شتائم إلى الغير بواسطة شبكة الإنترنت وسواء تم ذلك عن طريق إنشاء موقع خاص على شبكة الإنترنت

لسب أو قذف شخص معين، أو سواء كان السب أو القذف عن طريق إرسال بريد إلكتروني للشخص المجني عليه.

٣- جريمة التجسس عبر الإنترنت :

من الجرائم التي انتشرت عبر الإنترنت جرائم التجسس على الآخرين ويتم ذلك عن طريق إدخال ملف تجسس إلى المجني عليه ويسمى هذا الملف حصان طروادة. وفي حالة إصابة الجهاز بملف التجسس يقوم على الفور بفتح أحد المنافذ في جهاز الشخص المجني عليه وهذا المنفذ هو الباب الخلفي لحدوث اتصال بين جهاز الشخص المجني عليه وجهاز الشخص المخترق والملف الذي يكون لدى المجني عليه يسمى الخادم، بينما الجزء الأخر منه يسمى العميل وهو يكون لدى المخترق، والذي من خلاله يمكن للمخترق أن يسيطر على جهاز المجني عليه دون أن يشعر فبإمكان المخترق فتح القرص الصلب لجهاز المجني عليه والعبث به كيفما يشاء سواء بحذف أو بإضافة ملفات جديدة..الخ.

ويتم إدخال ملف التجسس إلى جهاز المجني عليه بإحدى الطرق التالية:

ا- برامج المحادثة.

ب- البريد الإلكتروني.

ج - زيارة الشخص لمواقع مجهولة تغريه بتنزيل بعض البرامج والملفات المجانية ومن ضمنها ملف التجسس.

وبالنسبة للتشريع الفلسطيني نجد أن القانون الأساسي المعدل لسنة ٢٠٠٣ وقانون العقوبات يحميان الحياة الشخصية للمواطن من أي اعتداء عليها. فالمادة ٣٢ من القانون الأساسي المعدل تنص على (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 تعويضا عادلا لمن وقع عليه الضرر.

هذا وقد عالج قانون العقوبات لسنة ١٩٣٦ هذه الجرائم في الفصل الثامن والعشرين منه والذي جاء بعنوان الجرائم التي تقع على الحرية الشخصية.

إضافة إلى ذلك فان مشروع قانون العقوبات الذي مازال تحت الإجراء خصص الفصل الحادي عشر منه إلى جرائم الاعتداء على الحرية الشخصية والحياة الخاصة، وذلك وفقا لأحكام المواد ٣٠٠، ٣٠١، ٣٠٢، ٣٠٣، ٣٠٤، ٣٠٥، ٣٠٦، ٣٠٧، ٣٠٨، ٣٠٩، ٣١٠، ٣١١، ٣١٢، ٣١٣، ٣١٤

ونشير هنا إلى المادة ٣٠٩ منه التي تنص على (يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة لأحد الأشخاص، بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه:

أولا : استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه حديثا خاصا جرى في أحد الأماكن أو عن طريق الهاتف.

ثانيا: التقط أو نقل أو نسخ أو أرسل بأي جهاز من الأجهزة صورة شخص في مكان خاص، وإذا صدرت الأفعال المشار إليها أثناء اجتماع على مسمع ومرأى الأشخاص الذين يهمهم الأمر الحاضرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضا ما لم يبدوا اعتراضهم على الفعل.

ثالثا: أساء عمدا استعمال أجهزة الخطوط الهاتفية، بأن أزعج الغير أو وجه إليهم ألفاظا بذيئة أو مخلة بالحياء أو تضمن حديثه معهم تحريضا على الفسق والفجور.

المشكلات العملية والإجرائية في جرائم الإنترنت:

يوجد العديد من المشكلات والصعوبات العملية والإجرائية التي تظهر عند ارتكاب إحدى جرائم الإنترنت ومن هذه المشكلات:

١- صعوبة إثبات هذه الجريمة.

٢- صعوبة التوصل إلى الجاني.
٣- صعوبة إلحاق العقوبة بالجاني المقيم في الخارج.
٤- تنازع القوانين الجنائية من حيث المكان.
٥- القصور في القوانين الجنائية القائمة.
٦- افتراض العلم بقانون جميع دول العالم.
٧- صعوبة السيطرة على أدلة ثبوت الجريمة.
٨- صعوبة تحديد المسئول جنائيا في الفعل الإجرامي.
٩- صعوبة المطالبة بالتعويض المدني.

ثالثا: مشروع قانون العقوبات الفلسطيني :

لم يتضمن قانون العقوبات الحالي أية إشارة إلى جرائم الكمبيوتر والإنترنت باعتبار أنها جرائم مستحدثة، وإنما جاءت نصوص قانون العقوبات لتعالج الجرائم بشكل تقليدي كجرائم النصب والسرقة وخيانة الأمانة والإتلاف وغيرها، هذه النصوص لم تعد كافية لمواجهة ظاهرة جرائم الكمبيوتر والإنترنت لهذا كله شرع المشرع الجنائي الفلسطيني بوضع سياسة جنائية متطورة تلبي احتياجات المجتمع الفلسطيني وتغطي العجز الجنائي في التشريعات الجنائية الحالية فقامت السلطة التنفيذية ممثلة في ديوان الفتوى والتشريع بوزارة العدل بإعداد مشروع قانون العقوبات الذي عالج فيه جرائم الحاسب الآلي بشكل يتماشى مع الأحداث المتلاحقة والسريعة لمواجهة هذا النوع الجديد من صور الإجرام.

كما بين مشروع قانون العقوبات جرائم الحاسب الآلي على النحو التالي:

قد نصت المادة ٣٩٣ على أن :

أ- كل من اقتحم بطريق الغش نظاما لمعلومات حاسب آلي خاص بالغير أو بقي فيه يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تجاوز ألف دينار أو بإحدى

هاتين العقوبتين.

ب- وإذا نتج عن ذلك تعطيل تشغيل النظام أو محو المعلومات التي يحتوي عليها أو تعديلها تكون العقوبة الحبس وغرامة لا تجاوز ثلاثة آلاف دينار أو إحدى هاتين العقوبتين.

كما أوضحت المادة ٣٩٤ من مشروع القانون جريمة إفساد أو عرقلة الحاسب الآلي فنصت على (كل من عرقل أو أفسد عمدا تشغيل نظام حاسب إلى خاص بالغير أو أدخل أو عدل بطريق الغش معلومات تخالف المعلومات التي تحتوي عليها يعاقب بالحبس وبغرامة لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين).

وكذلك جرم مشروع القانون وبشكل واضح جريمة التزوير والإضرار بالغير فنص في المادة ٣٩٥ منه على (كل من زور إضرارا بالغير وثائق حاسب آلي أو أستعمل وثائق مزورة مع علمه بتزويرها يعاقب بالحبس وبغرامة لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين).

كما استطاع المشرع الجنائي الخروج عن النظام العقابي التقليدي وجرم جريمة السرقة بشكل يتماشى مع التطور الهائل الذي لحق بالجريمة فنص في المادة ٣٩٦منه على أن (كل من سرق معلومات من نظام حاسب آلي خاص بالغير يعاقب بالحبس وبغرامة لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين، وكذلك يعاقب نفس العقوبة كل من حصل على معلومات خاصة بالغير أثناء تسجيلها أو إرسالها بأية وسيلة من وسائل المعالجة المعلوماتية التي من شأن إفشائها المساس بسمعة صاحبها أو بحياته الشخصية مما يمكن اطلاع الغير على تلك المعلومات دون إذنه.

وأخيرا وضع المشرع الجنائي حكما بمعاملة الشروع بجرائم الحاسب الآلي

بالعقوبة المقررة للجريمة التامة فنص في المادة ٣٩٧ على ما يلي (يعاقب على الشروع في الجرائم المنصوص عليها في هذا الفصل بذات العقوبة المقررة للجريمة التامة).

رابعا: مشروع قانون الإنترنت والمعلوماتية الفلسطيني:

انطلاقا من الدور الرئيس الذي يقوم به ديوان الفتوى والتشريع بوزارة العدل في تجسيد الوجود الفلسطيني في قضاء الإنترنت والمعلوماتية والحاسب الآلي واللحاق بالتطورات الهائلة التي لحقت بالمجتمع الدولي ومواكبة التقدم في هذا المجال من أجل حماية المجتمع الفلسطيني وصيانة حقوقه أفرادا ومؤسسات فقد شرع بالتعاون مع وزارة الاتصالات وتكنولوجيا المعلومات بإعداد مشروع قانون الإنترنت والمعلوماتية والذي يتكون من ٨٦ مادة عالج فيها الموضوعات ذات الصلة بالإنترنت والمعلوماتية ووضع أحكاما وقواعد وقام بتجريمها حماية لحقوق الأشخاص، كما حدد مهام مركز الحاسوب ودور الحاسوب الحكومي ودور وزارة الاتصالات وتكنولوجيا المعلومات مع وزارة التربية والتعليم في وضع الخطط اللازمة للاستفادة من تقنية المعلومات والاتصالات في خدمة التعليم، كما حدد مشروع القانون عناصر البنية التحتية لتكنولوجيا المعلومات، ووضع المشروع أحكاما لتنظيم الإنترنت وتطبيقاته كما وضع مجموعة من الإجراءات فيما يتعلق بمنح التراخيص والأذونات المتعلقة بإنشاء أو تشغيل خدمات الإنترنت والمعلوماتية عامة وخاصة، أما فيما يتعلق بأمن الشبكات والبيانات فقد منح مشروع القانون وزارة الاتصالات وتكنولوجيا المعلومات مع الجهات المختصة العمل على التكامل الواسع والشامل بين المعلومات وأجهزة الحاسب الآلي وذلك لمواجهة مخاطر التعدي على الخصوصية والسرقة والتهديد والجريمة وغيرها من مظاهر الهجمات عبر الإنترنت.

وأخيرا وضع المشرع مجموعة من العقوبات على الجرائم التي تتعلق بالحاسب الآلي والإنترنت الخ ...

خامسا :

أ- النتائج :

بعد أن انتهينا من جرائم الكمبيوتر والإنترنت نجد لزاما أن نبين دور المشرع الجنائي الفلسطيني في تدارك الوقت وأن يصدر تلك التشريعات، حيث شرعت السلطة الوطنية ممثلة في ديوان الفتوى والتشريع بإعداد مجموعة من التشريعات الجنائية الحديثة والمتطورة وذلك لتلبية احتياجات المجتمع الفلسطيني وتطوير النظام القانوني في فلسطين وكان من بين هذه المشاريع مشروع قانون العقوبات ومشروع قانون الإنترنت والمعلوماتية حيث أن هذه المشاريع ستغطي العديد من الثغرات القانونية التي يواجهها القضاء الفلسطيني في ذلك المجال.

ب- التوصيات :

١- الإسراع في إقرار وإصدار مشروعات القوانين المتعلقة بجرائم الكمبيوتر والإنترنت والمعلوماتية.

٢- عدم إجراء القياس في مجال الجرائم والعقوبات.

٣- تشكيل لجنة استشارية علمية تقوم بإعداد الأبحاث والدراسات والاطلاع على التشريعات المتعلقة بمثل هذه المواضيع وتزويد الجهات المعنية بها.

٤- إيجاد نوع من التنسيق بين فلسطين وجامعة الدول العربية لتبادل المعلومات في هذا المجال.

٥- تشكيل طاقم فني قانوني يكون على قدر كبير من الدراية والخبرة في مجال الكمبيوتر والإنترنت والمعلوماتية لصياغة قواعد وأحكام مشاريع القوانين المتعلقة بهذه المواضيع.

٦- العمل على إيجاد تعاون فلسطيني عربي حيث يعتبر الركيزة الأساسية في إستراتيجية عربية لمواجهة كافة المستجدات التقنية والاتفاقيات الدولية المتعلقة بجرائم الكمبيوتر والإنترنت.

٧- العمل على إيجاد تعاون فلسطيني إقليمي (ثنائي) ودولي في مجال الكمبيوتر والإنترنت.

٨- العمل إلي أقصى حد ممكن من الاستفادة من الخبراء المتخصصين في مجال الكمبيوتر والإنترنت وكذلك أساتذة القانون الجنائي غير التقليديين.

٩- إن إيجاد تشريع عربي نموذجي موحد بشأن جرائم الكمبيوتر يعتبر خطوة في الاتجاه الصحيح تساعد كافة الدول العربية في تطوير تشريعاتها الخاصة بهذه الجرائم واللحاق بالتطورات التي وصلت إليها المجتمعات الصناعية المتطورة.

١٠- الاستفادة من التجربة الأوروبية قدر الإمكان في مجال معالجة جرائم الكمبيوتر لا سيما الاتفاقية التي وضعها المجلس الأوروبي حول هذه الجرائم.