مجلة جامعة الأزهر – غزة، عدد خاص بمؤتمر كلية الحقوق الخامس المحكَّم، المجلد 19 ص 43-82

المواجهة التشريعية للجريمة المعلوماتية بيـن الواقـع والمأمـول

أحمد محمد بـراك بن حمد

النائب العام – فلسطين

تاريخ الاستلام 2016/8/9 تاريخ القبول 2017/2/9

ملخص:

تطرق الباحث في هذا البحث إلى ماهية الجريمة المعلوماتية، وتحدث عن صور وأشكال هذه الجريمة حيث اتضح عدم كفاية النصوص القانونية التقليدية في قانون العقوبات وقانون الإجراءات الجزائية لمكافحة الجريمة المعلوماتية، وقصور التشريعات الفلسطينية المختلفة في معالجة هذه الجريمة لردع مرتكبيها، كما تناول المواجهة الدولية لمكافحة الجريمة المعلوماتية والتطرق إلى المشاريع المتعلقة بمكافحة الجريمة المعلوماتية والمواجهة الوطنية في التشريع الفلسطيني ومشاريع القوانين.

وخلص الباحث إلى ضرورة العمل على صياغة مشروع قانون خاص بالجرائم المعلوماتية أسوة بالاتجاه الغالب في الدول المقارنة والتوصية بضرورة وضع تشريع فلسطيني خاص بمكافحة الجرائم المعلوماتية يتفق مع الأحكام القانونية الدولية في مجال مواجهة هذه الجرائم.

Abstract:

The researcher tackled the informative crime and its forms, concluding that there is an inadequacy in the traditional legal provisions, the Penal Code, and the Criminal Procedure Code in combating cybercrimes. In addition, there is a failure in various Palestinian legislations in addressing this crime and deterring its perpetrators. The researcher also addressed the International confrontation to combat cybercrimes and the projects relating to combating a cyber crime and the national confrontation in the Palestinian legislation and draft laws.

The researcher concluded that there is a need for issuing a special draft law on crimes of informatics and recommended developing special Palestinian law for IT crimes in line with the international legal provisions.

مقدمة:

من المعلوم أن الفضاء الالكتروني يشكل بيئة خصبة لارتكاب الجريمة، وكلما كان تطور الوسائل التكنولوجية الجديدة متسارعاً كلما أخذت الوسائل الإجرامية أبعادا متطورة مواكبة في ذلك هذا التطور ومتلازمة معه في السياق نفسه، وفي ظل الثورة المعلوماتية الهائلة التي يشهدها العالم ظهرت هناك العديد من الإشكالات القانونية في المعاملات التي يقوم بها الأفراد باستخدام الانظمة المحوسبة، مما حدا بالتشريعات الجنائية السعي لتطوير تشريعاتها لمواكبة هذا التطور في سبيل الحد من الجرائم وانتشارها، وبذلك أصبحت التشريعات التي تحارب الجرائم المعلوماتية (الإلكترونية) ضرورة وتحظى باهتمام كافة الدول، لما لها من تأثير كبير وظاهر على حياة الفرد والدولة على حد سواء.

كل هذا جعل المشرع الجنائي المقارن مضطراً لمتابعة هذه المستجدات والتعامل معها من خلال التدخل التشريعي لمكافحة هذا النوع الخطير من الجرائم من أجل الحفاظ على مصالح الفرد والدولة.

ولقد ظهرت فكرة شبكة المعلومات العالمية أو الانترنت عندما أطلقت وزارة الدفاع الأمريكية مشروع أربانت عام 1969، وقد تم انشاء هذه الشبكة لمساعدة الجيش الأمريكي ، ثم استبدلت الوزارة البرتوكول NCP المعمول به في الشبكة ببروتوكلات الانترنت مما أسهم في نمو الشبكة هو ربط " المؤسسة الوطنية للعلوم " جامعات الولايات المتحدة الأمريكية بعضها ببعض مما سهل عملية الاتصال بين طلبة الجامعات وتبادل الرسائل الالكترونية والمعلومات بدخول الجامعات إلى الشبكة.

ثم بدأت الشبكة في التوسع والتقدم وأخذ طلبة الجامعات يسهمون بمعلوماتهم حيث كان أهم إنجاز لهذه المؤسسة هو عمل شبكة جديدة وبمميزات أكثر أسمتها NSFNET ثم ظهرت فكرت الـ www من المخبر الأوربي لفيزياء الجسيمات The CERN European Laboratory for Particale Pgysics والذي كان بحاجة إلى وسيلة سهلة لمتابعة الوثائق والمعلومات المتوفرة لديهم حتى يمكن الوصول إليها وتحديثها. ويُعتبر السيد Tim Berner Lee الذي كانت لديه خبرة سابقة بالنصوص المتشعبة hypertext هو مخترع Web وتم تطبيق المشروع عام 1992 .

وتم تطوير العديد من الطرائق لاستعراض وثائق www كان أنجها برنامج Mosaic الذي طوره السيد Marc Andersen من (NCSA) National Center for Supercomputing Applications والذي كان الخطوة التي أوصلت شبكة الانترنت على النحو الذي نراه الآن .

وتميزت هذه الشبكة حالياً بتقديم العديد من الخدمات لمستخدميها من الاتصال والحصول على معلومات وإتمام المعاملات، الحصول على البرامج ، وإجراء الدراسات [1].

ولا يخفى على أحد وجود فراغ تشريعي في التشريعات الفلسطينية لمعالجة الجرائم المعلوماتية سواء بطبيعتها أم التي ترتكب بواسطتها، والتي تقف التشريعات التقليدية عاجزة عن التصدي لهذا النوع من الجرائم، وهذا ما حدا بنا إلى معالجة هذا البحث عن طريق الدراسة التأصيلية التحليلة المقارنة بين ما هو قائم من التشريعات الوطنية وما هو مطبق في التشريعات الدولية المقارنة؛ وكذلك ما هو مقترح في مشروع قانون الجرائم المعلوماتية الفلسطيني لسنة 2016 المقدم لمجلس الوزراء الفلسطيني والذي تم قراءته بالقراءة الأولى وما هو مرتبط به من قوانين مقترحة.

وعلى ذلك سوف تكون خطة البحث على الوجه التالي:

المبحث الاول: ماهية الجريمة المعلوماتية.

المبحث الثاني : صور وأشكال الجريمة المعلوماتية.

المبحث الثالث : المواجهة الدولية للجريمة المعلوماتية.

المبحث الرابع : المواجهة الوطنية للجريمة المعلوماتية في التشريع الفلسطيني.

المبحث الخامس : المواجهة الوطنية للجريمة المعلوماتية في مشاريع القوانين.

المبحث الأول
ماهية الجريمة المعلوماتية

تمهيد وتقسيم:-

ينصرف مصطلح الجريمة المعلوماتية للدلالة على الجرائم التي ترتكب من خلال استخدام الحاسب الآلي (الكمبيوتر) وشبكة الانترنت[2]، فمفهوم الجريمة المعلوماتية يشمل أي استخدام غير قانوني للكمبيوتر والانترنت بقصد إلحاق الأذى بالغير من خلال وسائل غير مشروعة، مما يستدعي معه ملاحقة الفاعل ومعاقبته وفقاً للقانون، وتعتبر الجريمة المعلوماتية من الجرائم المستحدثة والتي لا تزال خاضعة للدراسة المستفيضة نظراً للمستجدات المواكبة لتطور هذه الجريمة ووسائل ارتكابها[3].

---

[1] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، 2014، ص 13-16 وما بعدها

[2] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، مصر 2013 ص 11.

[3] نهلا عبدالقادر المومني، الجرائم المعلوماتية، ،منشورات دار الثقافة للنشر والتوزيع، عمان-الأردن المرجع السابق، ص 46.

وللوقوف على ماهية الجريمة المعلوماتية لا بد من التعرف إلى المعنى المقصود بهذه الجريمة وفقا لما توصل إليه الفقه والقانون، وبيان خصائص هذا النوع من الجرائم، وتحليل الأركان القانونية المكونة لهذه الجريمة وهو ما سنتناوله بالدراسة من خلال ثلاثة مطالب على الوجه التالي، حيث سنتناول – بمشيئة الله – في المطلب الأول تعريف الجريمة المعلوماتية، وفي المطلب الثاني خصائص الجريمة المعلوماتية وفي المطلب الثالث أركان الجريمة المعلوماتية.

المطلب الاول

تعريف الجريمة المعلوماتية

لا يوجد تعريف فقهي محدد للجريمة المعلوماتية [1] حيث أورد الفقهاء الكثير من التعريفات لهذه الجريمة والتي تنطلق من العناصر التي يتضمنها كل تعريف على حدة [2].

وأكثر التعريفات شيوعا للجريمة المعلوماتية هي تعريفها بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى[3].

كما عرفها البعض " هي جرائم الأموال وجرائم الأشخاص وجرائم المصلحة العامة التي تقع باستعمال الكمبيوتر أو شبكة الانترنت سواء داخل البلاد أو خارجها[4].

ويرى البعض أن المقصود بالجريمة المعلوماتية هو "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، ويهدف إلى الاعتداء على الأموال المادية أو المعنوية [5].

كما عرفها آخرون بأنها "كل فعل أو امتناع يؤتيه شخص طبيعي أم معنوي عن طريق ممثليه، باستعمال نظام معلوماتي معين يتمثل في الحاسبات أم ما يقوم مقامها من نظم متطورة، وشبكات الاتصال، إضرارا بمصلحة أو حق يحميه القانون من خلال جزاء جنائي، سواء أكانت هذه المصالح أو الحقوق المحمية تمثل نماذج معلوماتية مستحدثة، أم كانت تدخل في نطاق المصالح أم الحقوق التي كان يحميها مسبقا قانون العقوبات بالطرق التقليدية، وسواء أكان الاعتداء واقعا داخل حدود الدولة أو كان يمس أقاليم عدة دول[6].

---

(1) نهلا عبدالقادر المومني، الجرائم المعلوماتية، ،منشورات دار الثقافة للنشر والتوزيع، عمان-الأردن المرجع السابق، ص 47.

(2) علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري للنشر والتوزيع، عمان - الأردن، 2009، ص 33. وانظر في تفاصيل هذه الاتجاهات هلالي عبد الله أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، مصر، 2011، ص 109- 110.

(3) ورد هذا التعريف للدكتورة نائلة قورة المشار إليه في كتاب نهلا المومني، الجرائم المعلوماتية، المرجع السابق، ص 48.

(4) غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص 11.

(5) محمد أمين الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان - الأردن، 2011، ص 9.

(6) هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية

وبذلك يتضح أن الجريمة المعلوماتية محل بحثنا قوامها أن تكون أحد سببين فقد تكون المعلوماتية وسيلة للغش والتحايل والاعتداء ، أو أن تكون المعلوماتية نفسها محلاً للاعتداء، فارتكاب الجريمة المعلوماتية يستدعي من الجاني استخدام وسيلة إلكترونية ليرتكب الجريمة من خلالها، وحتى عصرنا الحاضر تعددت هذه الوسائط التي تعمل على قراءة رموز وشفرات الشبكة المعلوماتية لتجعلها لغة واضحة لمستخدمي هذه الأجهزة [1].

وأخيرا فقد عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين. الجريمة المعلوماتية بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية[2].

ونحن نؤيد هذا التعريف فهو أكثر التعريفات انسجاما مع مفهوم الجريمة المعلوماتية من حيث إنه يشمل جميع الجرائم التي يكون فضائها العالم الالكتروني، كما أنه لم يقتصر على التركيز على فاعل الجريمة أو الجريمة ذاتها أو الوسيلة المرتكبة بها الجريمة بشكل ضيق، وإنما شمل كل هذه العناصر في التعريف لكي يضمن عدم إفلات المجرمين من دائرة العقاب[3].

المطلب الثاني

خصائص الجريمة المعلوماتية

نظرا للطبيعة الخاصة للجريمة المعلوماتية باعتبارها من الجرائم المستحدثة، وكونها تتصل وترتبط بالعالم الالكتروني سواء عن طريق الحاسوب أم الانترنت، تفردت هذه الجريمة عن غيرها من الجرائم بعدة خصائص يمكن تفصيلها على النحو الآتي:

1. الجريمة المعلوماتية من الجرائم العابرة للحدود:

بالنظر لكون الشبكات المعلوماتية غير مقيدة بفواصل جغرافية أو زمنية محددة، الأمر الذي يجعل من الجريمة المعلوماتية تتجاوز حدود الدول، وهذا الأمر مرتبط بالتطور الهائل الذي تمتاز به هذه الشبكات، فأصبح يتم تداول المعلومات والبيان والمعاملات من دولة إلى أخرى خلال وقت يسير جدا، وأصبح مفهوم السرعة هو المعيار لقياس مدى التطور في هذه الشبكات، وهذا أدى بالنتيجة إلى سهولة إمكانية تأثر عدة دول من الجريمة المعلوماتية المرتكبة في دولة ما عبر جهاز الكتروني من خلال التقنيات الموجودة فيه[4].

بودابست، المرجع السابق ص 110- 111

(1) حنان ريحان مبارك المضحكي، المرجع السابق ، ص 13-31

(2) مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد في فيينا عام 2000، مشار إليه في كتاب نهلا المومني، الجريمة المعلوماتية، المرجع السابق، ص 50.

(3) نهلا عبدالقادر المومني، الجرائم المعلوماتية، المرجع السابق، ص 50.

(4) نهلا عبدالقادر المومني، الجريمة المعلوماتية، المرجع السابق، ص 51.

وقد أدى هذا التطور في ارتكاب الجرائم المعلوماتية عبر الدول إلى تداعي العديد من دول العالم إلى التعاون وعقد الاتفاقيات المشتركة لمكافحة هذا النوع من الجرائم[1]، وبخاصة في ظل الإشكاليات المتعلقة بالملاحقة القضائية والتنازع القضائي.

2. صعوبة إثبات واكتشاف الجريمة المعلوماتية:

في الكثير من الجرائم المعلوماتية المرتكبة يصعب إثبات محلها نظرا لكون هذا النوع من الجرائم لا يترك أثرا ماديا ظاهرا، ناهيك عن التباعد الجغرافي بين الدول[2] ، مما يغدو معه صعوبة البحث والتحري في الأدلة الجنائية . والجرائم المعلوماتية في أكثر صورها هي جرائم غير مرئية، لا يمكن ملاحظتها من قبل المجني عليه، بحكم توافر المعرفة والخبرة لدى مرتكبها عادة[3].

3. خصوصية مرتكب الجريمة المعلوماتية:

يختلف فاعل الجريمة المعلوماتية عن غيره من المجرمين من حيث المستوى التعليمي له ، حيث إنه يكون ذا اختصاص ومعرفة في مجال تكنولوجيا المعلومات، فالمجرم العادي لا يستخدم عادة وسائل علمية ومعرفية لارتكاب جريمته على النقيض من مرتكب الجريمة المعلوماتية ، فالقيام بعملية اختراق أو استخدام بيانات أشخاص آخرين يتطلب مهارة وقدرة فنية عالية من قبل من يقوم بها، وهذا ما يظهر عادة في الجرائم الاقتصادية المرتكبة من خلال الشبكات المعلوماتية[4].

4. أسلوب ارتكاب الجريمة المعلوماتية:

الجريمة المعلوماتية ليست بحاجة إلى إعداد وتخطيط وبذل جهد كما هو الحال في سائر الجرائم التقليدية، حيث إن الجرائم المعلوماتية تحتاج إلى هدوء ذهني والقدرة الفنية على التعامل مع الشبكات المعلوماتية، وتتعدد الأجهزة المعلوماتية المستخدمة في الجرائم المعلوماتية فقد يستخدم جهاز الحاسب الآلي، أو الهواتف النقالة الذكية ، وكذلك الأقمار الصناعية تصنف كوسيط إلكتروني.

5. تعدد الأوصاف القانونية لمحل الجريمة المعلوماتية:

قد يظهر محل الجريمة المعلوماتية بمظهر مادي أو معنوي كما هو الحال بالنسبة للمعلومات التي قد تكون موجودة في الذاكرة الالكترونية ، أي يمكن وصفها بأنها حالة غير مادية أو أن تكون في صورة مادية من خلال تخزينها على الدعامة الالكترونية[5].

---

(1) هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، المرجع السابق ص 240.

(2) عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، 2014، ص 21.

(3) نهلا عبدالقادر المومني، الجريمة المعلوماتية، المرجع السابق، 54.

(4) نهلا عبدالقادر المومني (المرجع السابق) ص 59

(5) عبدالله دغش العجمي (المرجع السابق) ص 25

6. اشتراك أكثر من شخص في ارتكاب الجريمة المعلوماتية:

عادة ما يتم ارتكاب الجريمة المعلوماتية من خلال عدة أشخاص بحيث يكون أحدهم متخصصاً في التقنيات الالكترونية، حيث يتم إخراجها إلى حيز الوجود وهو ما قد يأخذ أشكالاً سلبية من خلال عدم قيام من يعلم بوقوع الجريمة بالتبليغ عنها حيث يتم إتمامها، وقد يكون الاشتراك إيجابيا من خلال تقديم المساعدة الفنية والمادية[1].

المطلب الثالث

أركان الجريمة المعلوماتية

الجريمة المعلوماتية كغيرها من الجرائم لابد من توافر أركانها القانونية من حيث الركن المادي والمعنوي حتى يمكن إطلاق صفة الجريمة عليها، سنتطرق إلى الركن المفترض في الجرائم المعلوماتية والذي يتحقق بوجود الشبكة المعلوماتية ، والجهاز المعلوماتي، وبالإضافة إلى الركن الشرعي أو القانوني ونقصد به النص القانوني وهو السند القانوني لتجريم الفعل تطبيقاً لمبدأ الشرعية (لا جريمة ولا عقوبة إلا بنص بالقانون). ولكون الجرائم المعلوماتية من المواضيع الحديثة وذات تقنيه عالية ومتطورة فمن غير الممكن للقاضي الجزائي الاجتهاد ولا القياس في التجريم، وذلك ما سوف نتناوله بالتفصيل في البندين التاليين.

أولاً:- الركن المادي:

يتمثل الركن المادي للجريمة بارتكاب فعل مادي أو الامتناع عن إتيان فعل يعاقب عليه القانون، فوجود النية لارتكاب الجريمة لا يكفي للقول بتوافر العناصر اللازمة للفعل الإجرامي[2].

حيث إن الركن المادي للجريمة يتكون من ثلاث عناصر وهي:

1- **السلوك الإجرامي** : أن الرغبة في ارتكاب اي فعل إجرامي يستتبع قيام الفاعل بسلوك مخالف للقانون، وهذا السلوك يفترض فيه نية إتيان فعل إيجابي كأن يقوم الفاعل باستخدام أداة معينة تساعده في تحقيق الفعل المنوي ارتكابه. وهذا السلوك يحتاج إلى توافر تقنيات وشبكات خاصه للقيام بالجريمة وهو ما يدخل في باب الإعداد والتحضير لارتكاب الجريمة ، فالجاني يقوم بتوفير الأجهزة الخاصة كجهاز الحاسوب مثلاً وإعداد البرامج اللازمة لارتكاب الجريمة وقد يتعدى ذلك قيام المجرم بتوفير كل ما يلزم من أدوات تستخدم بنية الإضرار بالغير، فالسلوك الإجرامي في الجريمة المعلوماتية عادة ما يبدأ بضغطة زر أو لمسة على شاشة الهاتف أو الحاسب الآلي على اختلاف أنواعه، فعلى سبيل المثال عندما يقوم المجرم المعلوماتي بالدخول

---

(1) نهلا عبدالقادر المومني (المرجع السابق) ص 58

(2) اسامة أحمد المناعسة وجلال محمد الزعبي ، جرائم تقنية نظم المعلومات الالكترونية ، دراسة مقارنة ، دار الثقافة للنشر والتوزيع عمان الاردن ، 2016 ، ص53

إلى الشبكة والتعارف إلى الاشخاص بعد انتحال شخصية أو صفة تتناسب مع ما يدعيه ككونه مستثمراً أو تاجراً للحصول على مبالغ نقدية دون وجه حق من الأشخاص الذين تعاملوا معه من خلال الشبكة المعلوماتية، أو عندما يقوم المجرم المعلوماتي ببرمجة فايروس كان قد حفظه في قرص مضغوط أو ممغنط وقام بارساله بضغطة زر أو لمسة شاشة إلى أحدهم مما أحدث ضرراً في الجهاز الآخر، وذلك متصور أيضاً في الهواتف النقالة، فالفعل هنا يتحدد بالإرسال وحدوث الضرر من جراء ما تم إرساله.

2- **النتيجة الجرمية:** يقصد بالنتيجة الجرمية الأثر الذي يحدثه السلوك الجرمي والذي يرتب عليه المشرع أحكاما قانونية وتقسم الجرائم بحسب نتيجتها الجرمية بالنظر إلى مدى تطلب حدوث نتيجة ما من عدمه إلى جرائم قانونية وجرائم مادية حيث لا يشترط في الجرائم القانونية تحقق نتيجة جرمية بل إن مجرد الإقدام عليها يوجب المسؤولية اما الجرائم المادية فلا بد من تحقق نتيجة جرمية ضارة تلحق بالمصلحة العامة أو الخاصة او كليهما[1]، وبالنظر إلى طبيعة الضرر في هذا الجانب في الجرائم المعلوماتية تختلف عن الضرر في الجرائم التقليدية بوصفه ذات طبيعة غير محددة لأنه متصل بتقنية المعلومات، والأغلب فإنه يتخذ طابعاً معنوياً في صورة معلومات لها طابع معنوي أو مادي[2]. وأكثر الأضرار المادية شيوعاً في الوسط المعلوماتي هي تدمير البيانات والمعلومات المخزنة على الشبكة المعلوماتية وفي الأجهزة المعلوماتية مما يترتب عليه خسائر فادحة للجهات التي ترتبط بها هذه المعلومات والبيانات وقد تنشأ أضرار مادية جراء التلاعب ببيانات ومعلومات الأجهزة المعلوماتية أو تدميرها كالحواسيب والبرامج المنظمة لعمل الطائرات والسيارات وغيرها من الوسائل الحيوية التي تنظم عملية نقل الأرواح مما يسبب عطلاً في هذه الوسائل وتدمرها وينجم عن ذلك خسائر فادحة في الأرواح. أما الأضرار المعنوية فتترتب بناء على المساس بحرمة الحياة الخاصة من خلال التجسس الإلكتروني. أو اختراق الأجهزة المعلوماتية والتحصل على بيانات أو صور خاصة، وما في حكمها.

3- **العلاقة السببية:** حتى يكتمل الركن المادي فلا بد من توافر علاقة سببيه بين السلوك والنتيجة، ففي حال انقضت العلاقة السببية لا يكون هناك مجال لملاحقة ومساءلة الجاني ولكن في الجانب المعلوماتي فإنه تثور إشكالية كبيرة عند محاولة ربط السلوك الإجرامي بالنتيجة الضارة

---

[1] اسامة أحمد المناعسة وجلال محمد الزعبي (المرجع السابق) ص 56

[2] حنان ريحان مبارك المضحكي ، المرجع السابق ، ص 89-90

التي تترتب بسببه، بسبب طبيعة هذه الجرائم المعقدة، ومن المتصور أن ينشأ أكثر من ضرر جراء السلوك الإجرامي الواحد.

ثانياً- الركن المعنوي للجريمة المعلوماتية :

يمثل الركن المعنوي الحالة النفسية للجاني والعلاقة بين ماديات الجريمة والسيطرة النفسية عليها من قبل شخصية الجاني . فالركن المعنوي هو سلوك ذهني أو نفسي، وهذا الركن هو محور المسؤولية الجنائية والذي يقوم على عنصرين وهما: العلم والإرادة الآثمة .

1- العلم : يقصد بالعلم الذي ينصب على جميع عناصر الجريمة أي ماديات الجريمة، وهذا العلم مفترض ولا يعتد الجهل بالقانون ويشمل العلم بالوقائع التي تعد من عناصر الجريمة والعلم بموضوع الجريمة وماهية الفعل أو الامتناع عنه والجهل والغلط بالوقائع والغلط بالشخص[1].

2- الإرادة: الإرادة هي عبارة عن قوة نفسية او نشاط نفسي توجه نحو تحقيق هدف معين غير مشروع وعلى ذلك عرفت المادة 63 من قانون العقوبات رقم16 لسنة 1960 "النية بأنها ارادة ارتكاب الجريمة على ما عرفها القانون"، والإرادة تتجه للسلوك والنتيجة في آن واحد، فإرادة الفعل تقوم على إتيان الفاعل بفعل يشكل خطراً على الحق الذي يحميه القانون، وهذا يتطلب علم الجاني بماهية الفعل وخطورته و أن تتوجه أعضاء جسمه للقيام بهذا الفعل أو الامتناع عنه. كما أن إرادة الفعل لا تكفي لوحدها إذ يستلزم الأمر توجه الإرادة نحو النتيجة المقصود من الفعل.

اما الدافع : فيقصد به النشاط النفسي الذي يحرك إرادة الجاني بارتكاب الفعل وتحقيق النتيجة الجرمية وقد عرفت المادة 76 من قانون العقوبات بأنها: العلة التي تحمل الفاعل على الفعل أو الغاية القصوى التي يتوخاها الفاعل والدافع بهذا المعنى ينصرف إلى الباعث الذي يحرك الإرادة ويدفعها إلى ارتكاب الفعل او إلى الغاية القصوى التي توخاها الفاعل .

والدافع في الجرائم المعلوماتية يجد أساسه في المبادئ العامة الواردة في التشريعات الجنائية بالتالي فلا بد من توافره لغيره من الأركان المشكلة لعناصر الجريمة حتى تستتبع المسؤولية الجزائية[2] ، وذلك حينما ينص المشرع على ذلك صراحة لكون الباعث أو الدافع لا يدخل في أركان الجريمة.

---

[1] اسامة أحمد المناعسة وجلال محمد الزعبي (المرجع السابق) ص 61

[2] اسامة أحمد المناعسة وجلال محمد الزعبي (المرجع السابق) ص 63

المبحث الثاني

صور وأشكال الجريمة المعلوماتية

تمهيد وتقسيم :-

يصنف الفقهاء والدارسون جرائم الكمبيوتر والانترنت (الجرائم المعلوماتية) ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته، وهناك من الفقه يقسمها بحسب أسلوب ارتكاب الجريمة، ومنهم من ذهب لتقسيمها حسب الباعث من ارتكاب الجريمة، والجانب الأخير منهم من يرى تقسيمها بناء على محل الجريمة . وفي هذا المبحث سيتم اعتماد التقسيم بناء على الجرائم التي ترتكب بواسطة الحاسوب، وسنتناول في المطلب الأول الجرائم الواقعة على البيانات، وفي المطلب الثاني الجرائم الواقعة على الأموال وفي المطلب الثالث الجرائم الواقعة على الأشخاص، وذلك على الوجه التالي:

المطلب الاول

الجرائم الواقعة على البيانات

يمكن تقسيم صور الجرائم الواقعة على البيانات إلى الأشكال التالية:

1) **جريمة الدخول غير المشروع:** ويقصد بالدخول غير المشروع هو دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع الكتروني أو نظام معلوماتي غير مصرح له بالدخول اليها[1] وفي هذه الحالة يكون محل الجريمة حاسباً آلياً أو موقعاً الكترونياً وكذلك يجب توفر القصد الجرمي أي أن يكون الدخول بطريقة متعمدة.
2) **جريمة تعطيل أو افساد نظام التشغيل:** وهو ما يتعلق بالإضرار بأنظمة المعلومات التي تتم عن طريق تعطيل نظام المعالجة الالية للبيانات.
3) **جريمة اتلاف المعلومات:** ويمكن تقسيمها إلى: جريمة تدمير البيانات والمعلومات وجريمة إدخال البيانات غير المشروع والتعديل عليها.
4) **التزوير المرتبط بالحاسب الآلي:** ويشمل هذه النوع من الجرائم تزوير البريد الإلكتروني وتزوير الرقائق والسجلات وتزوير الهوية، أو تزوير بطاقات الائتمان والمستندات العادية المعدة بواسطة الحاسب الآلي، أو الأجهزة المساعدة له مثل أجهزة التصوير الإلكتروني. أو تزوير التوقيع الإلكتروني والبصمة الإلكترونية وتزوير بطاقات الائتمان وبطاقات الدفع

---

[1] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة والمواثيق الدولية، دار النهضة العربية، القاهرة، 2011 ص 40 وما بعدها

الإلكتروني، ويعتبر هذا النوع من الجرائم المعلوماتية من أشدها خطورة وأكثرها حدوثا وتحقيقاً للخسائر للإفراد والمؤسسات. ويشمل كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل المعلومات وقواعد البيانات الموجودة بصورة الكترونية على الحواسب الآلية المتصلة أو غير المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة عليها.

وأبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي عليها. ويقوم بذلك النوع من الأنشطة ما يطلق عليهم المخترقون الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الانترنت مستغلين بعض الثغرات في تلك النظم وإجراءات أمن المعلومات التي يقوم بها مديرو تلك الأنظمة والشبكات بمعنى أخر وصول شخص غير مصرح له و إمكانية دخوله إلى حجرة الحواسب المركزية بالمؤسسة ثم خروجه دون إحداث أي أضرار فإنه يعتبر خرق السياسة وإجراءات أمن المعلومات بتلك المؤسسة. أما بالنسبة إلى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل لنظم المعلومات فإن تلك الأنشطة تتم بواسطة أفراد أو محترفون يطلق عليهم المخترقون الذين قد يقومون بهذه الأعمال بغرض الاستفادة المادية أو المعنوية من البيانات والمعلومات التي يقومون بالاستيلاء عليها بغرض الإضرار بالجهة صاحبة تلك البيانات.

المطلب الثاني

الجرائم الواقعة على الاشخاص

أصبحت ظاهرة الاعتداء على الأشخاص من الجرائم اليومية والواسعة الانتشار، وارتبط تطور هذه الجرائم بتطور الوسائل التكنولوجية بحيث أصبح من السهل التواصل بين الأفراد من خلال مواقع التواصل الاجتماعي، وقد أدى ذلك التطور إلى ازدياد ملحوظ في الجرائم التي تقع على الأشخاص واتخذت هذه الجرائم صورا متعددة أهمها ما يتعلق بالاعتداء على حرمة الحياة الخاصة.

يعد الاعتداء على حرمة الحياة الخاصة أبزر مظاهر الجرائم المعلوماتية الواقعة على الأشخاص، وتتعدد عناصر الحق في الحياة الخاصة إلى عدة أشكال، فهي تشمل حرمة جسم الإنسان، وحرمة المسكن، وحرمة الصورة، والمحادثات والمراسلات، والحياة المهنية.

وتظهر أهمية العلاقة بين حرمة الحياة الخاصة والتكنولوجيا، بتوافر التقنيات التي يملكها الإنسان، وما تحققه من أهداف متعددة في المجالات العلمية والثقافية والعسكرية، حيث أصبحت الشبكات المعلوماتية مستودعا للكثير من أسرار الأشخاص، والتي يمكن الوصول إليها بسهولة ويسر، وأصبح ما يطلق عليه بنك المعلومات من أهم وأخطر عناصر الحياة الخاصة للأفراد، ونظرا لخطورة الأفعال التي تقع على حرمة الحياة الخاصة فقد سعت التشريعات الجنائية إلى إحاطتها

بأهمية بالغة من خلال النص على حماية البيانات الخاصة بالأفراد ووسائل الحصول عليها من قبل السلطات العامة في الدولة، وجرّمت عمليات التعدي على هذه البيانات الشخصية المتعلقة بالحياة الخاصة.

والمقصود بالاعتداء هنا هو السب والقذف والتشهير وبث أفكار وأخبار من شانها الإضرار الأدبي أو المعنوي بالشخص أو الجهة المقصود هذا و تتنوع طرائق الاعتداء بداية من الدخول على الموقع الشخصي للشخص المشهر به وتغيير محتوياته والذي يندرج تحت الجرائم التى تتم ضد الحواسب و الشبكات أو عمل موقع أخر يتم نشر أخبار ومعلومات غير صحيحة و الذي يندرج تحت الجرائم باستخدام الحواسب الآلية و الشبكات والذى غالبا ما يتم من خلال إحدى مواقع الاستضافة المجانية لصفحات الانترنت.

وجرائم الاعتداء على الأشخاص والتي تتم باستخدام الحواسب الآلية و الشبكات الخاصة التي تتم ضد الحواسب الآلية، أما ما يندرج منها تحت بند الجرائم التي تتم باستخدام الحواسب الآلية هو ما يشابه التشهير بالأشخاص المعنويين أو الحقيقيين من بث أفكار ومعلومات وأحيانا أخبار و فضائح ملفقة من خلال بناء مواقع على شبكة الانترنت محتويا على كافة البيانات الشخصية مع العديد من الأخبار والموضوعات التي من شأنها الإضرار الأدبي والمعنوي و أحيانا المادي بالشخص أو الجهة المقصودة.

المطلب الثالث

الجرائم الواقعة على الأموال

يمكن تقسيم الجرائم الواقعة على الأموال إلى قسمين هما: الجرائم الواقعة باستخدام الحاسب الالي كجرائم تزييف عملة أو تزوير في سند رسمي أو اختلاس[1]، وجرائم واقعة على الحاسب الالي المتعلقة بالجانب المادي أو المعنوي كجرائم تدمير المعلومات والبيانات المالية المخزنة في الحاسب الآلي.

ويمكن تقسيم أنواع الجرائم إلى الأنواع التالية:

1- **جريمة السرقة : -**

تعرف السرقة بأنها اعتداء على ملكية منقول وحيازته بنية تملكه، وعرفتها المادة 1/399 من قانون العقوبات الأردني رقم (16) لسنة 1960م وتعديلاته بأنها "أخذ مال الغير المنقول دون رضاه" أما المقصود بأخذ المال فهو إزالة تصرف المالك فيه برفعه من مكانه ونقله، وإذا كان متصلا بغير منقول فبفصله عنه فصلا تاما ونقله، وأما إن كان غير ذلك فيشمل كل القوى المحرزة.

---

[1] اسامة أحمد المناعسة وجلال محمد الزعبي ، المرجع السابق ص 89

وجريمة السرقة هي اعتداء على حق الملكية ولذلك تعد الملكية هي محل الجريمة الرئيس، كما أن جريمة السرقة تمثل اعتداء على الملكية وأما موضوع الجريمة فهو المال المنقول.

وتتطلب جريمة السرقة توافر الركن المادي المتمثل بفعل أخذ دون رضى المالك والنتيجة الجرمية المتمثلة لخروج الشيء محل السرقة من حيازة المجني عليه إلى حيازة الجاني، وعلاقة السببية التي تربط الفعل بالنتيجة.

2- **جريمة الاحتيال :-**

الغش أو الاحتيال أو النصب تعبيرات يجري استخدامها بمعان مترادفة وإن كانت تتمايز في الحقيقة من الوجهة اللغوية أو الدلالات الاصطلاحية ، ويستخدم قانون العقوبات الأردني تعبير الاحتيال أما القانون المصري ، فيستخدم تعبير النصب ، وكلا القانونين لم يوردا تعريفا للاحتيال أو النصب، وإنما أوردا الأفعال المكونة للجريمة في كل منها .

أما غش (الكمبيوتر)/ الحاسوب، أو كما يسميه البعض، الاحتيال المعلوماتي أو الاحتيال باستخدام الحاسوب ، فقد تباينت بشأنه التعريفات وتعددت، وأساس تباينها تحديد الأفعال المنطوية تحت هذا الوصف وصور احتيال (الكمبيوتر)/ الحاسوب عديدة بل ويصعب في أحيان كثيرة حصرها لتباينها من حيث وسائل الاعتداء التقني نفسه أو تباينها من حيث البيانات محل الاعتداء ، ويمكن القول بإيجاز إنها كافة الوسائل التقنية للتوصل إلى البيانات المالية أو التي تتصل بحقوق مالية[1].

لقد كانت أكثر الوسائل التقنية رعبا فيما سبق من أنشطة في بداية ظاهرة جرائم الكمبيوتر الوصول إلى نظام أحد المصارف عن بعد عبر الاتصال المباشر بشبكة البنك أو عبر خطوط الهاتف التي تتيح مدخلا لشبكة نظام البنك فيقوم الجاني بالعبث بالبيانات المالية إما بإجراء التحويلات أو بتغيير البيانات لكسب حقوق او الخلاص من التزامات ، أو بزرع البرامج التي تحول آليا بعض المبالغ إلى حسابات خاصة به أو بشركائه، أو لإخفاء عملية اختلاس حصلت أو غير ذلك من أنشطة وأغراض الدخول هذه ، وجامع هذه الأنشطة أن الجاني يقوم بأعمال احتيالية موجهة لنظام الكمبيوتر فيجني المنافع المادية عن طريق العبث بالبيانات أو البرامج أو حتى عمليات النظام ذاته. أما في الوقت الحاضر ، فإن احتيال الانترنت المتمثل باستغلال مواقع الانترنت لجني مبالغ الآخرين عبر مشاريع وهمية لمنتجات أو خدمات أو من خلال الوصول إلى أرقام بطاقات ائتمان الزبائن سواء بجمعها عند تلقي الموقع الوهمي لها او التوسل للوصول اليها من مواقع اخرى ومن ثم استغلالها في عمليات شراء غير مشروعة أو الوفاء بمبالغ مقابل خدمات للجاني ، وانشطة التلاعب بالأسهم المالية وادارة المحافظ الالكترونية ومزادات البضائع على الانترنت، تمثل الأنشطة الأكثر

[1] محمد أمين الشوابكة ، المرجع السابق ص 185

رعباً لانتشارها الواسع، ولما تلحقه بمواقع الانترنت والشركات القائمة عليها من مخاطر كبيرة وخسائر فادحة.

3- التزوير المعلوماتي :

التزوير بشكل عام هو تغيير الحقيقة أياً كانت وسيلته، وأياً كان موضوعه، وهو يتسع للعديد من الجرائم التي نصت عليها قوانين العقوبات[1]. أما التزوير في المحررات ، فهو حسب تعريفه المستقر في الفقهين الفرنسي والمصري " تغيير الحقيقة في محرر بإحدى الطرائق التي نص عليها القانون ، تغييراً من شأنه إحداث ضرر مقترن بنية استعمال المحرر المزور فيما أعد له. وقد عرّف قانون العقوبات الأردني التزوير بأنه "تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي او اجتماعي" (مادة 260) .

وبالرجوع إلى قوانين العقوبات العربية ، نجدها في معرض تجريم التزوير عموما ، وتزوير المحررات على وجه الخصوص قد نصت على تجرم العديد من الصور، فقد نص قانون العقوبات الأردني –على سبيل المثال– على هذه الجرائم في الفصل الثاني من الباب الخامس تحت عنوان الجرائم المخلة بالثقة العامة (المواد 260 – 272) ، وساوى في العقوبة بين مرتكب التزوير ومستعمل المحرر المزور

وتتشابه جرائم التزوير مع جرائم الاحتيال من حيث قيامهما على تغيير الحقيقة ، غير أنهما تختلفان من زوايا متعددة ، أهمها أن جريمة تزوير المحررات لا بد أن تقع على محرر، ولا يشترط ذلك في جريمة الاحتيال . وغالبا ما تجتمع جريمتا التزوير والاحتيال ، ونكون بذلك أمام حالة التعدد المادي للجرائم .

وتقوم جريمة التزوير على ركنين ، مادي ومعنوي ، وإن كان جانب من الفقه يجعل من بعض عناصر الركن المادي ، كالضرر ، ركنا مستقلا بذاته . أما الركن المادي فيقوم على ثلاثة عناصر: تغيير الحقيقة ، وأن يكون التغيير قد تم بإحدى الطرق المحددة حصراً في القانون ، وأخيراً ، أن يترتب على تغيير الحقيقة ضرر. وهذا العنصر الأخير هو ما ثار بشأنه الخلاف حول موقعه ، إلا أن السائد في الفقه اعتباره عنصرا من عناصر الركن المادي ، وتغيير الحقيقة يمثل السلوك الإجرامي الذي يقوم به التزوير، فإذا انتفى انتفت الجريمة . ولا يشترط ان يكون التغير كليا ، أي إبدال كل البيانات بما يخالف الحقيقة ، ويكفي أن يكون تغيير الحقيقة جزئياً أو نسبياً ، والمستقر في الفقه ان المقصود في التزوير ، ليس تغيير الحقيقة الواقعية المطلقة ، وإنما تغيير الحقيقة النسبية .

---

[1] علي جبار الحسيناوي ، المرجع السابق ص 72

وتغيير الحقيقة وحده غير كاف في القانون ، وانما يلزم أن يتم بإحدى الطرائق المحددة حصراً في القانون ، والتي تقسم عموما إلى طرائق مادية تنال مادة المحرر وشكله ، وطرائق معنوية، تنال مضمون المحرر أو ظروفه أو ملابساته دون المساس بمادته او شكله ، ويكتمل الركن المادي بتحقق الضرر الناتج عن تغيير.

وموضوع جريمة التزوير ومحلها ، المحرر ، ولا وجود للتزوير إذا لم ينصب على تغيير الحقيقة في محرر، ويعرف المحرر بانه مجموعة من العلامات والرموز تعبر اصطلاحا عن مجموعة مترابطة من الافكار والمعاني الصادرة عن شخص أو اشخاص معينين وهو في جوهره كتابة مركبة من حروف وعلامات تعبر عن معنى أو فكرة معينة ، وحسب الاتجاه التشريعي والفقهي الراجح ، يفترض إمكان ادراك مادة المحرر بالقراءة البصرية وأن ينتقل معنى الرموز والعلامات عن طريق المطالعة والنظر ، ومن المسائل الهامة المفترض الاشارة اليها ، والمتصل بموضوع وهدف.

أما الركن المعنوي لجريمة التزوير ، فيتخذ صورة القصد الجنائي . ولا يكفي فيه القصد العام الذي يقوم على علم المتهم بأركان الجريمة ، واتجاه إرادته إلى الفعل المكون لها وتحقيق نتيجته ، بل تتطلب هذه الجريمة توافر قصد جنائي خاص ، يتمثل بنية استعمال المحرر المزور فيما زور من أجله، وعلى هذا فان القصد الجنائي في جريمة التزوير يعرف على نحو غالب لدى الفقه والقضاء بانه تعمد تغيير الحقيقة في محرر تغييراً من شأنه أن يسبب ضرراً وبنية استعمال المحرر فيما غيرت من أجله الحقيقة .

وعموما فإن نصوص التجريم التقليدية المنظمة لجرائم التزوير غير قابلة للانطباق على جرائم تزوير معطيات الحاسوب بدلالتها الواسعة ، مما يستدعي تدخلا تشريعيا لمواجهة هذه الجرائم، صيانة لاسس ومباديء النظام القانوني وكفالة للحقوق التي تهددها هذه الانشطة الجرمية المستجدة.

المبحث الثالث

المواجهة الدولية للجريمة المعلوماتية

تمهيد وتقسيم :-

نظرا لكون الجريمة المعلوماتية غير محددة في دولة معينة، وتتسم بأنها ذات طابع دولي فقد كان هناك العديد من الجهود الدولية لتوقيع إتفاقيات دولية لمكافحة والحد من هذه الجريمة العالمية عبر الوطنية. وفي هذا المبحث سيتم تناول أهم الاتفاقيات الدولية التي تناولت هذا الموضوع لمواجهة خطر الجريمة المعلوماتية لكونها جريمة عبر الوطنية مما يلزم التعاون الدولي لمواجهتها في ثلاثة مطالب ، حيث نتناول في المطلب الاول معاهدة بودابست لسنة 2001 المتعلقة بمكافحة الجرائم المعلوماتية، وفي المطلب الثاني الاتفاقية العربية لمكافحة تقنية المعلومات، وفي مطلب ثالث موقف التشريعات المقارنة من مكافحة الجرائم المعلوماتية وذلك الوجه التالي :

المطلب الأول

معاهدة بودابست لمكافحة جرائم تقنية المعلومات

لقد وقعت على تلك المعاهدة (26) دولة اوروبية بالإضافة إلى كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية ، ورغم أن هذه المعاهدة هي بالأصل أوروبية المنشأ ، إلا أنها اتفاقية ذات طابع دولي، وهي مفتوحة للدول الاخرى لطلب الانضمام إليها، وقد استغرقت المباحثات والمفاوضات بين الدول الموقعة على المعاهدة أربعة اعوام حتى تم التوصل إلى الصيغة النهائية المناسبة، كما تم الاتفاق على أهمية التعاون والتضامن الدولي في مجال مكافحة جرائم الانترنت، وبدون هذا التعاون لن يكون هناك أي أثر لأي مجهود تقوم به أي من الدول بمفردها، حيث إن تلك الجرائم تكون في الأغلب الأعم من الحالات جرائم عابرة للحدود [1].

وقد تضمنت الاتفاقية ثلاثة أقسام :

الاول : يتناول مجموعة الجرائم التي يمكن أن تتعرض لها الانترنت والكمبيوتر .

الثاني : يتناول مجموعة الإجراءات الجنائية التي يمكن أن تتخذ في مواجهة هذه النوعية من الجرائم.

الثالث: يتضمن موضوع التعاون الدولي بين الدول الأعضاء الموقعين على الاتفاقية .

نظرا لانتشار الجريمة المعلوماتية بشكل كبير فقد جاءت معاهدة بودابست لسنة 2001 وهي أول معاهدة دولية لمكافحة الجرائم المعلوماتية التي تهدف إلى توحيد الجهود الدولية لمكافحة الجرائم المعلوماتية، وتبلور التعاون الدولي في محاربتها ومحاولة الحد منها بعد أن وصلت تلك الجرائم إلى حد خطير بحيث يهدد الأشخاص والممتلكات[2] حيث تضمنت العديد من التعريفات للأفعال المجرمة تاركة لكل دولة تحديد العقوبة التي تراها مناسبة للفعل .

حيث تتكون هذه المعاهدة من مقدمة وأربعة فصول، ففي المقدمة تم استعراض الأهداف العامة للاتفاقية ومرجعياتها ومجموعة من التوجيهات العامة المحلية والاقليمية والدولية. أما الفصل الأول من المعاهدة فقد تناول المصطلحات الأساسية. أما الفصل الثاني فقد تناول الإجراءات الواجب اتخاذها على المستوى الوطني. أما الفصل الثالث والأخير فقد تطرق إلى التعاون الدولي.

واشتملت الاتفاقية على خمسة عناوين يمكن تقسيمها كما يلي:

1. الجرائم التي تمس سرية وأمن وسلامة وتوفير بيانات الحاسب ومنظوماته وهي تضم:
   أ. الدخول غير المشروع (مادة 2).
   ب. الاعتراض غير المشروع (مادة 3).

---

[1] رامي متولي القاضي ، المرجع السابق ، ص 66

[2] اسامة أحمد المناعسه وجلال محمد الزعبي ، المرجع السابق ص 91

ت. التدخل في البيانات (مادة 4).
ث. التدخل غير المشروع في المنظومة (مادة 5).
ج. إساءة استخدام الأجهزة (مادة 6).

2. الجرائم المتصلة بالحاسب الآلي وتتكون من:
   أ. جريمة التزوير المتعلقة بالحاسب (مادة 7).
   ب. جريمة الاحتيال المتعلقة بالحاسب (مادة 8).
3. الجرائم المرتبطة بالمحتوى وتشمل الجرائم الإباحية للأطفال (مادة 9).
4. الجرائم المرتبطة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المرتبطة بها (مادة 10).
5. المساهمة الجرمية والعقوبة، ويشتمل على بنود إضافية يشان الشروع و الاشتراك ، وأيضا الجزاءات أو التدبير وذلك طبقا للاتفاقيات أو المعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية (مادة 13).

المطلب الثاني

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

اهتمت الجامعة العربية من خلال الأمانة العامة لمجلس وراء الداخلية العرب بموضوع مكافحة الجرائم المعلوماتية من خلال تخصيص الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة لجرائم الانترنت فضلاً عن عقد اجتماع لفريق عمل يهتم بدراسة الجرائم المرتكبة بواسطة الحاسبات الإلكترونية وشبكات الانترنت (تونس 23-2000/3/24 م) .

وكذلك تخصيص الاجتماع الثامن للجنة المتخصصة بالجرائم المستجدة (تونس 15-16 / 2000/5 م) لموضوع جرائم نظم المعلومات وسبل مكافحتها .

فضلاً عن إعداد دراسة حول الإجراءات والتدابير التي تساعد على منع ومكافحة الجرائم المرتكبة بواسطة الحاسبات الإلكترونية وشبكات الانترنت عرضت على الدورة العشرين لمجلس وزراء الداخلية العرب (تونس 13-14 ت/2003/1) وتم تعميمها على الدول الأعضاء للاستفادة منها.

بعد هذه الجهود الحثيثة التي بذلتها الجامعة العربية في مجال مكافحة الجرائم المعلوماتية تم التوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بنهاية عام 2010م، وتتكون هذه الاتفاقية من (43) مادة وتشمل أحكاما موضوعية وأخرى إجرائية وتهدف جميعها إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات. وتجدر الإشارة إلى قيام دولة فلسطين بالتوقيع والتصديق على هذه الاتفاقية بموجب مرسوم من فخامة الرئيس الفلسطيني محمود عباس بتاريخ 2010/12/21 وهو ما يجعل الاتفاقية العربية محل التزام على كافة سلطات الدولة الفلسطينية ومواءمة التشريعات الوطنية الفلسطينية بموجب ذلك.

وتضمنت الاتفاقية العربية مجموعة من الأحكام الموضوعية والتي تمثلت في تجريم الأفعال المكونة لجرائم تقنية المعلومات[1] من أفعال الاختراق والاعتداء على سلامة البيانات والاعتراض غير المشروع، والاعتداء على حرمة الحياة الخاصة، والاعتداء على حقوق الملكية الفكرية وإساءة استخدام تقنية المعلومات، التزوير والاحتيال والإباحية، جرائم تقنية المعلومات المتعلقة بالإرهاب وغسل الأموال والمخدرات والاتجار في الجنس البشري والاستخدام غير المشروع لأدوات الائتمان والوثائق الإلكترونية. وشددت العقوبات على الجرائم التقليدية التي ترتكب بواسطة تقنية المعلومات، وأقرت المسؤولية الجنائية للأشخاص المعنوية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها. كما تضمنت تجريم أفعال اختراق الانظمة المعلوماتية وأي تغيير للحقيقة في البيانات. بالإضافة إلى العديد من الجرائم الإلكترونية الأخرى[2]، كما تناول الفصل الرابع من الاتفاقية التعاون القضائي بين الدول العربية من حيث الإنابات القضائية وتسليم المجرمين وتبادل المعلومات وغيرها.

المطلب الثالث

موقف التشريعات المقارنة من مكافحة الجريمة المعلوماتية

لقد عقدت الأمم المتحدة العديد من المؤتمرات لمواجهة الجرائم المعلوماتية وإصدار الكثير من التوصيات ، ففي السابع للأمم المتحدة الخاص بمكافحة الجريمة ومعاملة المجرمين أشار المؤتمر إلى جرائم الحاسب الآلي والصعوبات المتعلقة بها باعتبارها من الجرائم المتعدية الحدود ذات الطابع الاقتصادي ، وفي أغسطس عقد عام 1995 عقد المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين في هافانا، وكانت الجريمة الإلكترونية والاهتمام بمكافحتها وملاحقتها أحد الموضوعات التي تم بحثها، كما دعت الوكالات والمؤسسات ذات الطابع الدولي إلى التدخل لحماية المعلومات وعدم الاعتداء عليها وفي مقدمة هذه الوكالات منظمة التنمية والتعاون الاقتصادي [3].

ومن إمعان النظر في موقف التشريعات المقارنة من المواجهة التشريعية لتجريم الجرائم المعلوماتية نجدها ذات اتجاهين : اتجاه أول يدخل الجرائم المعلوماتية في متن قانون العقوبات واتجاه ثانٍ يفرد تشريعات مشتملة لمكافحة الجرائم المعلوماتية.

أما بخصوص الاتجاه الأول: فذهب بعض التشريعات المقارنة إلى إدراج نصوص خاصة بتجريم الجرائم المعلوماتية في تشريعاتها العقابية ، ومنها قانون العقوبات الفرنسي رقم (19-88) الذي أضاف إلى قانون العقوبات جرائم الحاسب (العقوبات المقررة لها في الأرقام 462 وما بعدها

---

(1) علي جبار الحسيناوي ، المرجع السابق ص 72

(2) اسامة أحمد المناعسه وجلال محمد الزعبي، مرجع سابق ص 95

(3) حنان ريحان مبارك المضحكي ، المرجع السابق ، ص 381

وكذلك التعديل في عام 1994 في المواد (232-1 إلى 323-7) تحت عنوان " الاعتداءات على نظام المعالجة الألية للمعطيات".

وكذلك في التشريع النرويجي والفلندي الذي أورد تعديلين على قانون العقوبات الفلندي عامي 1990 ، 1995 تضمنت غالبية الصور الجرائم المعلوماتية وكذلك مشروع قانون العقوبات الفلسطيني الباب الأخير منه.

ومن التشريعات العربية القانون العماني حيث أورد نصوص التجريم للجرائم المعلوماتية بموجب المرسوم السلطاني رقم (2001/72) والمعدّل لبعض أحكام قانون الجزاء العماني رقم (7) لعام 1974 والذي تضمن إضافة الفصل الثاني مكرر على الباب السابع تحت عنوان جرائم الحاسب الآلي (المواد 276 مكرر 1 و 276 مكرر 1 و 276 مكرر 2 و 276 مكرر 3 و 276 مكرر 4) وكذلك قانون العقوبات الجزائري (المادة 394 مكرر وما بعدها ، والمضافة بالقانون رقم (4-15) الصادر في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم (66-156) الصادر في 8 يونيو 1966م والمتضمن قانون العقوبات.

أما الاتجاه الثاني: وهو مذهب أفرد تشريعات خاصة بتجريم الجرائم المعلوماتية، وهو مذهب واتجاه المشرع الفلسطيني الجديد لأفراد قانون خاص لمكافحة الجرائم المعلوماتية، وكذلك أيضاً قانون جرائم الحاسب الألي والإنترنت الدنماركي لعام 1985م حيث شمل تجريم صور الجرائم المعلوماتية وتحديد عقوبات لها ، وكذلك وفي الحال ذاته في كلٍ من اليابان وألمانيا الاتحادية وبريطانيا وسويسرا والمجر وبولندا حيث توجد قوانين خاصة بمكافحة الجرائم المعلوماتية، وفي كندا هناك قانون خاصة للتعامل مع جرائم الحاسب الآلي والإنترنت حيث عدلت في عام 1985م قانونها الجنائي بحث شمل قوانين خاصة بجرائم الحاسب الألي والإنترنت.

وكذلك في السويد التي أصدرت قانون البيانات السويدي لعام 1973م الذي عالج الجرائم المعلوماتية وفي الولايات المتحدة الأمريكية أصدرت عدة قوانين خاصة في مجال حماية أنظمة الحاسب الألي لعام 1976م، وقانون الاحتيال وإساءة الحاسب الآلي لعام 1984م ، وقانون أمن الحاسب الالي لعام 1987م ، فضلاً عن إقرار قوانين في غالبية الولايات الأمريكية قوانين خاصة لجرائم الحاسب الألي[1].

[1] رامي متولي القاضي، المرجع السابق، ص 92

المبحث الرابع

المواجهة الوطنية للجريمة المعلوماتية في التشريع الفلسطيني

تمهيد وتقسيم :

على الرغم من أن القانون الفلسطيني حتى تاريخه لم يصدر قانوناً خاصاً لمكافحة الجرائم المعلوماتية، الا أن هناك جهوداً مبذولة لإصدار قانوناً خاصاً بمكافحة الجرائم المعلوماتية و نود أن نشير إلى أن التعديلات التشريعية الأخيرة في بعض المواضع كقانون الاتصالات السلكية واللاسلكية، وقانون الأوراق المالية، وقانون حماية المستهلك، وقانون مكافحة المخدرات والمؤثرات العقلية، كانت قد أشارت إلى تجريم بعض صور الجرائم المعلوماتية وهذا ما يقتضي منا بحث مدى انطباق نصوص قانون العقوبات التقليدي على مفهوم الجريمة المعلوماتية ومدى ملاءمة تطبيق القواعد الاجرائية على الجرائم المعلوماتية وذلك في ثلاثة مطالب على الوجه الآتي:

المطلب الأول :

الجريمة المعلوماتية في قانون العقوبات التقليدي

لا شك أن الجريمة المعلوماتية فرضت نفسها على الساحة القضائية الفلسطينية وبالرغم من المحاولات التشريعة لوجود قانون خاص ناظم للجرائم المعلوماتية إلا أنها لم ترى النور حتى تاريخه بالرغم من حالة الضرورة المجتمعية لمواجهة هذا النوع الخطر من الجرائم على أمن المجتمع.

ولذلك لا بد من أجهزة إنفاذ القانون مواجهة تلك الجرائم بما يتفق مع قانون العقوبات التقليدي، حينما يصبح ذلك صالحاً من الوجهة القانونية وان كانت في حالات كثيرة تقف تلك السلطات عاجزة عن المواجهة القانونية لبعض الوقائع لعدم انطباقها وبخاصة اننا نتكلم عن مال معنوي وليس كياناً مادياً ملموساً كمال منقول او عقار تقع عليه الجريمة حيث إن محل الجرائم المعلوماتية هو دائماً المعطيات إما بذاتها أو بما تمثله، وقد تكون هذه المعطيات مخزنة داخل النظام أو على أحد وسائط التخزين او تكون في طور النقل والتبادل ضمن وسائل الاتصال المدمجة مع نظام الحوسبة ، فالمصلحة محل الحماية في ميدان الجرائم المعلوماتية هو الحق في المعلومات ككيان معنوي ذو قيمة اقتصادية عالية فالإشكالية تكمن في ضرورة تخلي المشرع الفلسطيني بشكل خاص والعربي بشكل عام عن حرفية النص الجنائي التقليدي وتبنيه مفهوما أشمل للمال المنقول بحيث تشمل الأموال المعلوماتية المعنوية وذلك بإصدار نصوص قانونية خاصة تشمل هذه الطائفة الأخيرة من الأموال غير المحمية والتي أصبحت تشكل نواة المجتمع الإلكتروني الحديث.

وبذلك نجد انه يتم ملاحقة بعض الجرائم التي ترتكب بواسطة الكومبيوتر والانترنت عن طريق اسقاط نصوص قوانين العقوبات السارية في فلسطين[1].

مثل نصوص الابتزاز والاحتيال والسرقة والإتلاف والتزييف وتقليد الأختام والتزوير وخيانة الامانة والذم والقدح والتحقير وإفشاء الأسرار والحض على الفجور والجرائم الماسة بأمن الدولة الداخلي والخارجي عندما يتم عن طريق وسال تقنية المعلومات بحيث يتم تطبيق هذه النصوص عندما ترتكب هذه الجرائم بواسطة الكومبيوتر أو شبكة الانترنت وغنية عن البيان بأن هذه النصوص قاصرة عن الوفاء بالغرض وبالتالي يتضح مدى الحاجة إلى التجريم الإلكتروني الخاص بهذه الجرائم، وذلك ان نصوص هذه الجرائم تنطبق عندما يكون الكمبيوتر أو الانترنت أو المحمول (تقنية المعلومات) وسيلة لارتكاب السلوك وفي بعض الأحيان عندما تقع على الكمبيوتر ذاته إلا أن المجرم في كثير من الاحيان يفلت من العقاب بسبب عدم وجود النص التشريعي المناسب للتجريم[2].

وبامعان النظر في المادة 73 من قانون العقوبات الأردني رقم 16 لسنة 1960 الساري في الضفة الغربية والواردة في الأحكام العامة لقانون العقوبات نجدها عرفت العلنية بأنها تعد وسائل للعلنية :

1. الأعمال والحركات إذا حصلت في مكان عام أو مكان مباح للجمهور أو معرض للأنظار أو حصلت في مكان ليس من المحال المذكورة غير أنها جرت على صورة يستطيع معها أن يشاهدها أي شخص موجود في المحال المذكورة .

2. الكلام أو الصراخ سواء جهر بهما أو نقل بالوسائل الآلية بحيث يسمعها في كلا الحالين من لا دخل له في الفعل .

3. الكتابة والرسوم والصور اليدوية والشمسية والأفلام والشارات والتصاوير على اختلافها إذا عرضت في محل عام أو مكان مباح للجمهور أو معرض للأنظار أو بيعت أو عُرضت للبيع أو وزعت على أكثر من شخص.

وبلا أدنى شك بأن الحاسوب والانترنت تتوافر بهما العلنية ويتم فيها النقل بالوسائل الآلية سواء أكانت عن طريق الكلام أم الصراخ أم الكتابة أم الرسوم والصور اليدوية والشمسية والأفلام والشارات والتصاوير على اختلافها، فهي تعرض في مكان مباح للجمهور بحيث يسمعها أو يراها من لا دخل

---

(1) بنظر قانون العقوبات الاردني رقم 16 لسنة 1960 المطبق في الضفة الغربية وقانون العقوبات الفلسطيني والانتدابي 1936 المطبق في قطاع غزة

(2) عبد اللطيف محمود ربايعة، الجرائم الالكترونية التجريم والملاحقة والاثبات ، ورقة عمل مقدمة إلى المؤتمر الاول للجرائم االالكترونية في فلسطين، جامعة النجاح الوطنية، نابلس فلسطين، 2016 ص 11

له في الفعل وأكثر من شخص وبذلك تتحقق العلنية في الوسائل المعلوماتية مما يجعل من بعض الجرائم التقليدية التي تتم عبر الشبكة المعلوماتية جائزة قانونا ومحلا للتجريم ونذكر منها ما يلي:

1. جرائم الذم والقدح والتحقير الواقعة عبر الانترنت :

تعد جرائم الذم والقدح والتحقير من أكثر الجرائم شيوعاً في نطاق شبكة الانترنت، إذ يساء استخدامها للنيل من شرف الغير وكرامته أو اعتباره أو تعرضه إلى بغض الناس واحتقارهم بما يتم اسناده للمجني عليه في شكل رسالة بيانات عن طريق وسائل إلكترونية أو ضوئية أو بوسائل مشابهة سواء تم ذلك عن طريق البريد الالكتروني أم شبكة الويب العالمية أو مجموعات الأخبار أو غرف المحادثات والدردشة .

وبإمعان النظر سواء في المادة 73 من قانون العقوبات الاردني رقم 16 لسنة 1960 الساري في الضفة الغربية والتي تتطرق للطرائق العلنية أو المادة 189 من ذات القانون والتي حددت العقاب على جرائم الذم والقدح شريطة ان يقع عن طريق الصور التالية :

1. الذم والقدح الوجاهي ويشترط ان يقع :

أ. في مجلس بمواجهة المعتدى عليه .

ب. في مكان يُمكِّن أشخاصاً آخرين أن يسمعوه قل عددهم أو كثر .

2. الذم والقدح الغيابي وشرطه أن يقع أثناء الاجتماع بأشخاص كثيرين مجتمعين أو منفردين.

3. الذم والقدح الخطي وشرطه أن يقع :

أ. بما ينشر ويذاع بين الناس أو بما يوزع على فئة منهم من الكتابات أو الرسوم أو الصور الاستهزائية أو مسودات الرسوم (الرسوم قبل أن تزين و تصنع) .

ب. بما يرسل إلى المعتدى عليه من المكاتيب المفتوحة (غير المغلقة) و بطاقات البريد.

4. الذم أو القدح بواسطة المطبوعات وشرطه أن يقع :

أ. بواسطة الجرائد والصحف اليومية أو الموقوتة .

ب. بأي نوع كان من المطبوعات ووسائط النشر .

وهو بالفعل ما يتحقق في جميع الوسائل الإلكترونية (تقنية المعلومات) بتوافر العلنية مما يجعل النص قابلا للتطبيق حيث عرفت المادة 189 من قانون العقوبات لسنة 1960 الذم بأنه (هو اسناد مادة معينة إلى شخص ولو في معرض الشك والاستفهام من شأنها ان تنال من شرفه وكرامته أو تعرضه إلى بعض الناس واحتقارهم سواء أكانت تلك المادة جريمة تستلزم العقاب ام لا .

كما عرف القانون القدح في المادة 189 بأنه (هو الاعتداء على كرامة الغير أو شرفه أو اعتباره ولو في معرض الشك والاستفهام).

كما عرفت المادة 190 من ذات القانون التحقير بأنه (كل تحقير أو سباب – غير الذم والقدح – يوجه إلى المعتدى عليه وجهاً لوجه بالكلام أو الحركات أو بكتابة أو رسم لم يجعلا علنيين أو بمخابرة برقية أو هاتفية أو بمعاملة غليظة) .

ومما سبق يتبين أن جرائم الذم والقدح والتحقير يمكن ان تقع بواسطة الانترنت أو أي وسيلة الكترونية أخرى المشار اليها أعلاه من الوسائل الحديثة كشف عنها العلم لكونها جريمة تقع عبر هذه الوسائل المعلوماتية .

2. الجرائم المخلة بالآداب والاخلاق العامه في التشريع العقابي التقليدي :

جرم المشرع في قانون العقوبات الأردني رقم 16 لسنه 1960 التعرض للآداب والأخلاق العامة بصورتها التقليدية في المادة 319 حيث نصت على أن :

يعاقب بالحبس مده لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على خمسين ديناراً كل من:

1- باع أو أحرز بقصد البيع أو التوزيع أية مادة بذيئة مطبوعة أو مخطوطة أو أية صورة شمسية أو رسم أو نموذج أو أي شيء آخر، يؤدي إلى إفساد الأخلاق أو إعادة طبع مثل هذه الأشياء والمواد بأية طريقة أخرى بقصد بيعها أو توزيعها .
2- عرض في محل عام أي تصوير أو صورة شمسية أو رسم أو نموذج بذيء أو أي شيء آخر قد يؤدي إلى افساد الأخلاق، أو زرع مثل هذه الاشياء لعرضها في محل عام.
3- أدار أو اشترك في ادارة محل يتعاطى بيع أو نشر أو عرض أشياء بذيئة مطبوعة كانت أم مخطوطة أم صورة شمسية أم رسوم أم نماذج أو أية أشياء أخرى قد تؤدي إلى إفساد الأخلاق.
4- أعلن أو أذاع بأية وسيلة من الوسائل أن شخصاً يتعاطى بيع هذه المواد والأشياء البذيئة أو طبعها أو أعاد طبعها أو عرضها أو توزيعها.

وكذلك في المادة 320 من قانون العقوبات ذاته على أن " كل من فعل فعلا منافيا للحياء أو أبدى إشارة منافية للحياء في مكان عام أو في مجتمع عام أو بصورة يمكن معها لمن كان في مكان عام أن يرى يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تزيد عن خمسين ديناراً ".

وباستقراء المواد 319 و 320 من قانون العقوبات الأردني المشار إليها سابقاً نجد أن المشرع حرص على تجريم أي مادة بذيئة، تؤدي إلى إفساد الأخلاق وذلك إذا ما تم بيعها أو إحرازها بقصد البيع أو التوزيع، وبذلك فإن المشرِّع لا يعاقب على إحراز مواد بذيئة إلا إذا اتجهت النية إلى بيعها، فمن حاز مواداً بذيئة في بريده الالكتروني الخاص دون أن تتجه نيته إلى بيعها فإنه لا يعد

مرتكباً لجريمة الاخلال بالآداب أو الأخلاق العامة، فحتى يستلزم العقاب لا بدَّ له من بيع هذه المواد أو احرازها بقصد البيع أو توزيعها، وهذه الافعال يمكن تصورها في نطاق شبكة الانترنت أو البريد الإلكتروني أو مجموعات الأخبار وكذلك غرف الدردشة وكذلك اذا ما تم ذلك الفعل في مكان خاص بصورة يمكن معها لمن كان في مكان عام أن يراه كمقاهي الانترنت على سبيل المثال[1] ولكن بدون التوسع بها لتنطبق على التعرض للأخلاق والآداب العامة عبر الانترنت حيث لا يرد القول على القياس في النصوص الجزائية أو التوسع بها وعلى المشرع الفلسطيني أن يعنى بتعديل هذه النصوص بحيث تشتمل على تجريم التعرض للأخلاق والآداب العامة عبر الانترنت بما يتفق ومبدأ الشرعية الجنائية.

3. الجرائم الواقعة على أمن الدولة

وتقسم الجرائم من هذا النوع إلى قسمين هما :

1. **الجرائم الماسة بأمن الدولة الخارجي،** ومن أهم صور هذه الجرائم :

- التجسس والدخول على البيانات الخاصة بالدولة وسرقة أو إفشاء هذه البيانات كما نصت عليها كل من المواد 124 و 125 و 126 من قانون العقوبات رقم 16 لسنة 1960 وهي كما يلي:
- المادة 124 والتي تنص على " كل من دخل أو حاول الدخول إلى مكان محظور قصد الحصول على أشياء أو وثائق أو معلومات يجب أن تبقى مكتومة حرصاً على سلامة الدولة عوقب بالأشغال الشاقة المؤقتة، وإذا حصلت هذه المحاولة لمنفعة دولة أجنبية، عوقب بالأشغال الشاقة المؤبدة ".
- المادة 125 والتي تنص على " 1- من سرق أشياء أو وثائق أو معلومات كالتي ذكرت في المادة السابقة أو استحصل عليها عوقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات 2- إذا اقترفت الجناية لمنفعة دولة أجنبية كانت العقوبة الأشغال الشاقة المؤبدة ".
- المادة 126 والتي تنص على " من كان في حيازته بعض الوثائق أو المعلومات كالتي ذكرت في المادة 124 فأبلغها أو أفشاها دون سبب مشروع عوقب بالأشغال المؤقتة مدة لا تقل عن عشر سنوات ويعاقب بالأشغال الشاقة المؤبدة إذا أبلغ ذلك لمنفعة دولة أجنبية ".
- المادة 107 المؤامرة مع دولة اخرى كما نصت عليها المادة 107 من قانون العقوبات رقم 16 لسنة 1960 والتي تنص على " المؤامرة هي كل اتفاق تم بين شخصين أو اكثر على ارتكاب جريمة بوسائل معينة "

[1] محمد أمين الشوابكي، المرجع السابق ص 109- ص 110

- المادة 112 الاتصال مع العدو لأغراض غير مشروعة كما نصت عليها المادة 112 من قانون العقوبات رقم 16 لسنة 1960 والتي تنص " على كل أردني دس الدسائس لدى العدو أو اتصل به ليعاونه بأي وجه كان على فوز قواته على الدولة عوقب بالإعدام والركن المادي لهذه الجرائم قد يعتمد على استخدام الحاسب الالي المعتمد على شبكات الاتصال الدولية، وبذلك تتحقق الجريمة باستخدام وسائل تقنية المعلومات كوسيلة لارتكاب تلك الجرائم الخطرة.

2. **الجرائم الماسة بأمن الدولة الداخلي،** ومن أهم صور هذه الجرائم:

- إثارة الفتن والحض عليها مثل استخدام وسائل التواصل الاجتماعي للعصيان كما نصت عليها المادة رقم 137 من قانون العقوبات رقم 16 لسنة 1960 والتي تنص على 1- كل فعل يقترف بقصد إثارة عصيان مسلح ضد السلطات القائمة بموجب الدستور يعاقب عليه بالإعدام .
2- إذا نشب العصيان، عوقب المحرض وسائر العصاة بالإعدام .
- الجرائم التي تمس بالوحدة الوطنية أو تعكير صفو الأمة وغيرها. وقد تستخدم من خلال استعمال الوسائل الالكترونية كما نصت المادة رقم 150 من قانون العقوبات لسنة 1960 والتي تنص على " كل كتابة وكل خطاب أو عمل يقصد منه أو ينتج عنه إثارة النعرات المذهبية أو العنصرية أو الحض على النزاع بين الطوائف ومختلف عناصر الأمة يعاقب عليه بالحبس مدة ستة أشهر إلى ثلاث سنوات وبغرامة لا تزيد على خمسين دينار.

المطلب الثاني:

الجريمة المعلوماتية في التشريعات الخاصة

نتناول في هذا المطلب الجرائم المعلوماتية الواردة في التشريعات الخاصة في قانون الاتصالات السلكية واللاسلكية الفلسطيني رقم 3 لسنة 1996 وقانون مكافحة المخدرات والمؤثرات العقلية رقم 18 لسنة 2015 وقانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2015 وقانون الطفل رقم 7 لسنة 2004 وقانون حماية الأحداث رقم 4 لسنة 2016 وذلك في أربعة بنود على الوجه التالي:

1- قانون الاتصالات السلكية واللاسلكية :-

ينظم هذا القانون عملية الاتصالات وإنشاء وتشغيل الشبكات ومحطات البث واستخدام الموجات ، ويشتمل على الحماية الجنائية لتكنولوجيا الاتصالات في فلسطين وذلك من خلال عرض الجرائم والعقوبات المقررة لها في المواد (86-100) من مواد القانون.

فنجد أن القانون عرف الاتصالات بأنها نقل أو إرسال أو بث أو استقبال الإشارات أو الأصوات أو الصور أو البيانات سواء كانت شفوية أم كتابية بالوسائل السلكية أم الراديوية أم البصرية أم الكهرومغناطيسية أم أي وسيلة أخرى للاتصالات وبذلك فان كافة المحادثات التي تتم

بواسطة وعبر شبكة الانترنت أو الصور أو المراسلات سواء كانت شفوية أم كتابية فهي تخضع لأحكام هذا القانون وباستعراض صور الجرائم التي ترتكب في إطار الإساءة لتقنية الاتصالات التي تعرض لهذا القانون نجدها كالاتي :

جريمة التجسس على محادثات الغير:

لقد جرم القانون كل من قام بالتجسس على محادثات الغير وعمد على نشرها حيث نصت المادة 68 من قانون الاتصالات(على أن كل من نشر أو أشاع مضمون أي اتصال بواسطة شبكة اتصالات عامة أو رسالة هاتفية اطلع عليها بحكم وظيفته أو قام بتسجيلها دون سند قانوني يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تزيد على 300 دينار أو بكلتا العقوبتين) وكل من حرض بطريق الخداع شخصا مؤتمنا على سر المخابرات على خرق هذا السر يعاقب بغرامة لا تقل عن 100 دينار ولا تزيد عن 300 دينار والحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بإحدى هاتين العقوبتين.

جريمة التهديد والإهانة عبر وسائل الاتصالات السلكية واللاسلكية:

وهو ما نصت عليه المادة 91 من القانون حينما نصت على ان كل من قام بتهديد أي شخص أو إهانته أو نقل خبراً مختلقاً بأي وسيلة من وسائل الاتصالات بقصد إثارة الفزع يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن سنة أو بغرامة لا تقل عن 50 ديناراً ولا تزيد عن 200 دينار أو بكلتا العقوبتين.

الجرائم الماسة بالنظام العام والآداب العامة.

وهو ما نصت عليها المادة 91 من قانون الاتصالات السلكية واللاسلكية، فإن أي محادثة أو مراسلة أو مكالمة أو أي صورة مخلة بالآداب العامة يتم ارسالها أو إجرائها عبر أي وسيلة إلكترونية تعد جريمة معاقب عليها بمقتضى ذلك القانون حيث نصت تلك المادة على انه كل من قام او ساهم بتقديم خدمات اتصالات مخالفة للنظام العام أو الآداب العامة يعاقب بالعقوبات المنصوص عليها في الفقرة (أ) من هذه المادة بالإضافة إلى تطبيق الاحكام المنصوص عليها في المادة (31) من هذا القانون.

جريمة الاعتداء على مراسلات الاخرين عبر الوسائل الالكترونية:

نصت على هذه الجريمة المادة 92 من القانون المذكور كل من اعترض أو أعاق أو حور أو شطب محتوياته رساله بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تقل عن 50 ديناراً ولا تزيد عن 200 دينار أو بكلتا العقوبتين.

جريمة العبث بالبيانات المتعلقة بالمشتركين:

وهو ما نصت عليه المادة 96 من القانون بنصها كل من قام متعمدا باعتراض موجات مخصصة للغير أو التشويش عليها أو باستخدام موجات كهرومغناطيسية بدون ترخيص يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة اشهر او بغرامة مالية لا تقل عن 50 ديناراً ولا تزيد عن 200 دينار أو بكلتا العقوبتين. وبذلك فإن 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. إلا أنه في نهاية المطاف ومع وجود بعض النصوص التي تجرم سلوكيات تدخل في إطار الجرائم المعلوماتية إلا أنه بالمجمل لا يشتمل على الحماية الجنائية الكافية التي يمكن أن تستوعب كافة الأفعال التي ترتكب في إطار الجرائم المعلوماتية.

قانون مكافحة المخدرات والمؤثرات العقلية رقم 18 لسنة 2015 :

لقد تناول القانون المذكور في متن المادة 28 منه جرائم من المتصور ارتكابها إلكترونياً حيث نصت المادة المذكورة على أن "يعاقب بالاشغال الشاقة المؤقتة لمدة لا تزيد على 10 سنوات وبغرامة لا تقل عن 1000 دينار أردني كل من:

1- انشأ او نشر موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسوب بقصد الاتجار أو الترويج أو التعاطي بالمواد المخدرة أو المؤثرات العقلية أو تسهيل التعامل بها.
2- شفر أي من المواقع المعلوماتية التي يستخدمها تجار المخدرات لكي لا تقع تحت رقابة السلطات، أو تولى تجهيز الحاسوب بوسائل فك الشيفرة المرسلة إلى أحد طرفي الاتجار بالمواد المخدرة.
3- عرض معلومات على موقع الكتروني عن كيفية تصنيع المواد المخدرة أو المؤثرات العقلية أو السلائف الكيميائية أو عن كيفية إنتاجها وأساليب تسويقها وترويجها وطرائق تعاطيها.

وبذلك تناولت المادة المذكورة كل من أنشأ أو نشر أو عرض معلومات أو تشفير موقع على الشبكة المعلوماتية فيما يتعلق بالإتجار أو الترويج أو بتعاطي أو تصنيع المواد المخدرة أو المؤثرات العقلية أو السلائف الكيميائية وهي من جرائم المعلوماتية المنصوص عليها حديثاً.

قانون مكافحة غسل الاموال وتمويل الارهاب رقم 20 لسنة 2015 :

لقد تناول هذا القرار بقانون وبخاصة في التعديل القائم عليه بالقرار بقانون رقم 13 لسنة 2016 في المادة الثالثة منه ما يعد مالا غير مشروع ومحل لجريمة غسل الأموال كل مال متحصل من القرصنة المعلوماتية بشتى أنواعها.

هذا بالاضافة إلى أنه وبإمعان النظر في نص المادة الثالثة المذكورة التي عددت المال غير المشروع محل جريمة غسل الأموال نجدها بأنه من الجائز ارتكابها عبر الشبكة المعلوماتية أو الحاسوب، ولا خلاف في النص على وسيلة ارتكاب الجريمة.

وكذلك وبإمعان النظر في المادة الثانية المعدلة من القانون ذاته والتي حددت الأفعال المجرمة التي تعتبر جريمة غسل أموال جاء النص كالتالي:

1 – " يعد مرتكباً لجريمة غسل الأموال وتمويل الإرهاب كل من قام بأي فعل من الأفعال الآتية:

أ .استبدالاً وتحويلاً ونقلا لأموال من قبل أي شخص،وهو يعلم بأن هذه الأموال تشكل متحصلات جريمة لغرض إخفاءأو تمويه الأصل غير المشروع لهذه الأموال، أو لمساعدة شخص متورط في ارتكاب الجريمة الأصلية على الإفلات من التبعات القانونية المترتبة على أفعاله.

ب . إخفاء أو تمويه الطبيعة الحقيقية أو المصدر أو الموقع أو التصرف أو الحركة أو الملكية أوالحقوق المتعلقة بالأموال من قبل أي شخص يعلم أن هذه الأموال تشكل متحصلات جريمة.

ج . تملك الأموال أو حيازتها أو استخدامها من قبل أي شخص وهو يعلم في وقت الاستلام أن هذه الأموال هي متحصلات جريمة لغرض إخفاءأو تمويه الأصل غير المشروع لهذه الأموال.

د . الاشتراك أو المساعدة أو التحريض أو التآمر أو تقديم المشورة أو النصح أو التسهيل أو التواطؤ أو التستر أو الشروع في ارتكاب أي من الأفعال المنصوص عليها في هذه المادة.

2– يستخلص العلم أو النية أو الهدف باعتباره عناصر أساسية لازمة للجريمة من الظروف الواقعية والموضوعية، من أجل إثبات المصدر المستتر للمتحصلات، والذي لا يشترط الحصول على إدانة الجريمة الأصلية.

3– تعد جريمة غسل الأموال المتحصلة من أي من الجرائم الأصلية، سواء وقعت هذه الجرائم داخل دولة فلسطين أو خارجها، شريطة أن يكون الفعل مجرماً بموجب القانون الساري في البلد الذي وقعت فيه الجريمة ،كما تسري جريمة غسل الأموال على الأشخاص الذين اقترفوا أياً من تلك الجرائم.

4– يعد مرتكب الًجريمة تمويل الإرهاب كل شخص يقوم عمدا أو يشرع بأية وسيلة بصورة مباشرة أو غير مباشرة بتقديم أو جمع أموال من مصدر مشروع أو غير مشروع بقصد استخدامها أو مع علمه بأنها سوف تستخدم كلياً أو جزئيا لصالح شخص إرهابي أو منظمة إرهابية أو جمعية أو جماعة إرهابية أو في ارتكاب أي من الأعمال الإرهابية.

5– تعتبر أي من الأعمال المنصوص عليها في الفقرة 4 من هذه المادة، جريمة تمويل الإرهاب حتى لو لم يقع العمل الارهابي أو لم تستخدم الاموال فعليا لتنفيذ أو محاولة القيام به أو ترتبط الاموال بعمل إرهابي معين وأياً كان البلد الذي وقع فيه العمل الإرهابي أو محاولة ارتكابه.

يحظر على اي شخص القيام بأي من الأفعال الآتية:

أ . تجنيد أو تنظيم أونقل أو إمداد أو تجهيز المقاتلين الإرهابيين الأجانب وتمويل تنقلاتهم ونشاطاتهم.

ب . السفر أو محاولة السفر من فلسطين إلى أي دولة خارج فلسطين بغرض ارتكاب أو تدبير أو المشاركة أو الإعداد لأعمال إرهابية أو التدريب أوتلقي التدريب على الأعمال الإرهابية.

ج . توفير أو جمع أموال بقصد أو بمعرفة بأنها ستُستخدم لتمويل سفر أو تنقل المقاتلين الأجانب أو تنظيم أو تسهيل سفرهم.

د . الدخول أو العبور إلى دولة فلسطين لأغراض متصلة بالأعمال الإرهابية".

وبذلك نجد أنه بموجب هذا النص لم يحدد وسيلة ارتكاب الجريمة مما يعني ارتكابه سواء بوسيلة تقليدية أم إلكترونية مهما كانت وسيلة تقنية المعلومات مما يجعلها من الجرائم الجائز ارتكابها عبر وسائل تقنية المعلومات.

4- قانون الطفل رقم 7 لسنة 2004 المعدل وقانون حماية الاحداث رقم 4 لسنة 2016 :

تناول العدالة الجنائية للأطفال في فلسطين قانون حماية الاحداث لسنة 2016 وقانون الطفل المشار اليه أعلاه، حيث نجد أنه في المادة 59 من قانون حماية الأحداث نصت على أن "يعاقب بالحبس مده لا تزيد على سنة وبغرامة لا تتجاوز 1000 دينار أردني او بإحدى هاتين العقوبتين كل من نال أو حاول النيل من الحياة الخاصة للحدث ، سواء كان ذلك بنشر أو ترويج ملخص الجلسات والقرارات الصادرة عن الهيئات القضائية أو اخبار تتعلق بما يدور بالجلسات التي تعالج فيها قضايا الأحداث، وذلك بواسطة أي كتب أو الصحافة أو الاذاعة أو التلفزة أو السينما أو باي وسيلة اخرى، أو بنشر أو ترويج صور من شأنها أن تطلع العامة على هوية طفل متهما كان أو متضرراً مع مصادرة المطبوعات او المصنفات الفنية المخالفة.

ولا شك أنه من الجائز ارتكاب هذه الجريمة سواء بوسيلة تقليدية أو الكترونية بالنشر والترويج فيما يخص بالحياة الخاصة للحدث حيث أطلق المشرع الفلسطيني العنان حينما نص على وسيلة ارتكاب الجريمة بعبارة "بأي وسيلة أخرى". وكذلك نجد في قانون الطفل لسنة 2004 في الماد 2/27 حيث نص المشرع الفلسطيني على أنه تعد أعمالا محظورة إنتاج أو ترويج أو استيراد الالعاب أو المواد غير المطابقة للمواصفات والمعايير الصحية أو البيئية المحددة من قبل الجهات المختصة أو التي تضر بالقيم المجتمعية" ولا شك بأن هذا النص يعطي إمكانية المعاقبة على الجريمة إذا تمت بوسيلة إلكترونية عن طريق الترويج.

وبإمعان النظر كذلك في المادة 36 من قانون الطفل المذكور ذاته نجدها تنص على أن "يحذر نشر أو عرض أو تداول أو حيازة أية مصنفات مطبوعة أو مرئية أو مسموعة تخاطب غرائز الطفل الدنيا أو تزين له السلوكيات المخالفة للنظام العام والآداب العامة أو يكون من شأنها تشجيعه على

الانحراف" ولا شك بإنطباق ارتكاب هذه الجريمة عن طريق الوسائل الالكترونية بل هي مجالها الاوسع انتشارا يحتم على السلطات انفاذ القانون مواجهتها لما لها من أثار مدمرة على أطفالنا.

المطلب الثالث

المواجهة الإجرائية للجريمة المعلوماتية

ما يميز الجريمة المعلوماتية هو أنها ترتكب في مجال مفرغ يختلف كلياً عن المسرح التقليدي الذي ترتكب فيه الجريمة حيث تتم اجراءات الاستدلال عليها وضبطها وإثباتها بالوسائل التقليدية المتمثلة في إجراءات الاستدلال و التحقيق. هذه الإجراءات وضعت لضبط و اثبات جرائم ترتكب في عالم مادي ملموس، يلعب فيه السلوك المادي الدور الأبرز والأهم، فما مدى انطباق القواعد الإجرائية لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس؟ وهو ما يتطلب منا الحديث عن مشكلات ضبط الجريمة المعلوماتية و إثباتها .

1 - ضبط الجريمة المعلوماتية و اثباتها:

يعتمد ضبط واثبات الجريمة على جمع الأدلة التي حدد المشرع وسائل إثباتها والتي تتمثل في وسائل الإثبات الرئيسة في المعاينة و الخبرة و التفتيش و ضبط الأشياء المتعلقة بالجريمة ، أما غيرها من وسائل الإثبات كالاستجواب والمواجهة وسماع الشهود فهي مرحلة تالية من إجراءات التحقيق و جمع الأدلة. ولما كنا بصدد تناول الجريمة المعلوماتية وما تثيره من مشكلات إجرائية ، فسنتعرض للمشكلات القانونية التي يثيرها اثبات هذه الجرائم دون غيرها من الاجراءات كالاستجواب و المواجهة وسماع الشهود ، لأن هذه الأخيرة تتم في مواجهة البشر ، أما المعاينة و الخبرة و التفتيش ،فهي إجراءات فنية محلها الأشياء لا الافراد.

2- حجية المخرجات الالكترونية في الاثبات الجنائي :

المخرجات الإلكترونية متعددة ومتنوعة ، فهي تتنوع بين مخرجات ورقية ، و مخرجات لا ورقية. المعلومات تكون مسجلة على الأوعية الممغنطة كالأشرطة والأقراص المرنة والقرص الصلب وغيرها من الأوعية. التي أصبحت في تطور مستمر وأصبح تواجهنا مشكلة أساسية تتعلق بصعوبة التمييز بين الأصل و الصورة ، ذلك لأننا نتعامل مع بيئة إليكترونية وهو ما يستحيل معه تطبيق القواعد الخاصة بالمحررات العرفية.

فمواجهة الجرائم المعلوماتية لا تتأتى إلا عن طريق نظام قانوني متكامل أهم عناصره التدخل لضبط المعاملات و التجارة الإليكترونية وإضفاء الحجة القانونية على المستندات الإليكترونية كما هو الحال في المستندات الورقية ، حتى يتاح للقاضي الجنائي الاعتماد عليها و اتخاذها دليلاً جنائياً ، كغيره من الأدلة.

3- الخبرة و المعاينة في الجرائم المعلوماتية:

تعتبر كل من الخبرة و المعاينة من أكبر العقبات التي تواجه الإثبات في الجرائم المعلوماتية، فالمعاينة تتطلب انتقال المحقق إلى مسرح الجريمة ليشاهد آثارها بنفسه ، فيقوم بجمعها وجمع أي دليل يفيد في كشف الحقيقة ، وتقتضي المعاينة اثبات حالة الأشخاص و الأشياء الموجودة بمكان الجريمة ورفع الآثار المتعلقة بها بما يفيد التحقيق. والمعاينة تكون شخصية أو عينية. المعاينة الشخصية إذا تعلقت بشخص المجني عليه ، أو مكانية إذا تعلقت بالمكان الذي تمت فيه الجريمة. أما المعاينة العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة، وقد يقتضي الأمر الاستعانة بخبير للتعرف إلى طبيعة المادة أو نوعها إذا كان ذلك يحتاج لرأي المتخصص ، وفي هذه الحالة يتم إرسال هذه الاشياء إلى الخبير لنكون أمام إجراء آخر من إجراءات التحقيق و هو الخبرة ، فالخبرة هي أحد أهم وسائل جمع الأدلة ، يلجأ اليها المحقق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات. يثور التساؤل هنا عن مدى امكانية معاينة الجريمة المعلوماتية من حيث الوجود المادي وكيفية معاينته.

فالمحقق في هذه الحالة يتعامل مع بيئة الاليكترونية والبيانات المخزنة داخل نظام معلوماتية شديدة الحساسية ولا يتعامل مع أوراق وهو ما يؤكد القواعد الإجرائية التقليدية سنت لتواجه سلوكاً مادياً يرتكب بواسطة آلات وأدوات قابلة للربط. أما السلوك الاجرامي في الجريمة المعلوماتية فهو عبارة عن بيانات مخزنة في نظام معلوماتي يتطلب إثباته انتقال شخص متخصص حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الإسطوانة الصلبة الخاصة بالجهاز، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة. وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الانترنت. كما يقتضي ذلك ايضاً ان يعمل المحقق على الوصول إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات. من أين صدرت؟ ومن الذي يحتمل إجراؤها ، بالإضافة إلى ضرورة المام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الإسطوانة الصلبة للحاسب ، والأوقات التي يستخدم فيها برامج استعادة المعلومات التي تم إلغاؤه.

4- الصعوبات التي تعترض مواجهة الجريمة المعلوماتية :

لا خلاف في أن الجرائم المعلوماتية تتسم بسمات خاصه من حيث طبيعتها وسمات مرتكبيها، وهو ما انعكس على طبيعة الإجراءات الخاصة بملاحقة هؤلاء الجناة ، حيث أفرزت الطبيعة الخاصة بالجرائم المعلوماتية بعضا من الصعوبات العملية في تحقيقها وبخاصة في عملية الضبط والتفتيش والانتقال والمعاينة وتتبع مرتكبيها وهذه الصعوبات تتمثل في الآتي :

1- إخفاء الجريمة ، فهي تقع مستتره خفية لا يلحظها المجني عليه غالباً أو يدري بوقوعها .

2- غياب الدليل المرئي الممكن فهمه بالقراءة .

3- افتقار أكثر الآثار التقليدية دون أن يتخلف ما يشير إلى حدوث إدخال أو تعديل برامجه أو البيانات المخزنة داخله.

4- إعاقة الوصول إلى الدليل أو تدميره في زمن قصير .

5- الضخامة البالغة لكم البيانات المتعين فحصها.

6- الإحجام عن الإبلاغ في مجتمع الاعمال.

أما بخصوص التفتيش في الجرائم المعلوماتية فقد عرف المجلس الأوربي إجراء التفتيش في الجرائم المعلوماتية بأنه " الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الالكتروني " وهو الإجراء الذي يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات والادلة المطلوبة وبإمعان النظر في المشكلات الإجرائية الخاصة بالتفتيش في الجرائم المعلوماتية نجدها في مشكلة امتداد الإذن بالتفتيش في شبكات الحاسب حيث يتم التفتيش عن الأدلة في مكان آخر في نظام معلوماتي آخر، ويمكن التغلب على ذلك كما في بعض الأنظمة القانونية كالقانون الهولندي في المادة 25 منه بالنص في اذن التفتيش على الاذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث شريطة أن تفيد بشكل معقول في كشف الحقيقة وإذا ما وجدت هذه البيانات يجب تسليمها. وكذلك هناك إشكالية أخرى تتعلق بمشكلة التفتيش في الجرائم المعلوماتية العابرة للحدود وذلك عندما يتم إجراء التفتيش على جهاز حاسب آلي خارج النطاق الجغرافي للدولة التي أصدرت الإذن بالتفتيش، وبالتالي تثور مشكلة شرعية هذا الإجراء ومساسه بسيادة الدولة الاخرى.

وهذه المشكلة يجب تجاوزها من خلال تعزيز التعاون الدولي في مكافحة الجرائم المعلوماتية من خلال إبرام اتفاقيات ثنائية وجماعية تنظم مباشرة هذا الإجراء، ومثال ذلك الاتفاقية العربية لمكافحة تقنية المعلومات واتفاقية بودابست المشار إليهما آنفاً.

تناول قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 إجراء جمع الاستدلالات واجراءات جمع الادلة سواءً من قبل مأموري الضبط القضائي والنيابة العامة في المواد من 19 - 148 من القانون، وعليه يثور التساؤل هل تنطبق القواعد الإجرائية لوارده في قانون الإجراءات المذكور أم يجب إعداد قواعد إجرائية جديده تتفق مع طبيعة الجرائم المعلوماتية والإجابة بعد ما تناوله في هذا المطلب هو يجب وضع قواعد إجرائية تتفق مع الجرائم المعلوماتية .

المبحث الخامس

المواجهة الوطنية للجريمة المعلوماتية في مشاريع القوانين

سوف نتناول في هذا المبحث مشروع قانون العقوبات الفلسطيني، ومشروع قانون المعاملات الإلكترونية المقدم إلى مجلس الوزراء ومشروع قانون الجرائم الالكترونية المقدم أيضاً لمجلس الوزراء والذي تم قراءته بالقراءة الأولى، وذلك في ثلاثة مطالب على النحو التالي.

المطلب الأول:

مشروع قانون العقوبات.

لقد تناول مشروع قانون العقوبات في الفصل الأخير الجرائم المعلوماتية، وجاء هذا المشروع بأحكام محددة ومقننة للأفعال المجرمة في كافة الجرائم التقليدية ،حيث تضمن فصلاً خاصاً بجرائم الحاسوب والانترنت والعقوبات المقررة لها، ولكن مع وجود المعيقات والتحديات أمام إقرار قانون العقوبات والمصادقة عليه، والتي تنبع من كونه قانون مجتمعي يمس الحقوق ويقيد الحريات ويتعلق بحقوق كافة فئات المجتمع، وأنه يشكل المظلة لكافة الجرائم ، الأمر الذي يجعل من إجراءات تعديله اجراءات معقده تحتاج إلى فتره زمنية طويله ومراحل متعددة، الأمر الذي لا يحقق الانسجام والتناغم مع الجريمة المعلوماتية مما استوجب وضع هذه الجرائم في قانون خاص بذلك لمكافحة الجرائم المعلوماتية منفصلاً عن قانون العقوبات، مما يجعل إجراءات تعديله سهلة تتناسب مع سرعة التطور التكنولوجي وعداك عن صعوبة اقرار قانون العقوبات في هذه المرحلة التي يمر بها الشعب الفلسطيني من خلال الانقسام فإنه بالنظر إلى أحكام هذا القانون فإننا نجد أنه لم ينص على قواعد اجرائية خاصة لملاحقة الجريمة المعلوماتية لما لها من أهمية قصوى في متابعة ومعالجة هذا النوع من الجرائم وكذلك قواعد التعاون الدولي ووضع تعاريف خاصة لهذا النوع من الجرائم حيث يقف مشروع قانون العقوبات المذكور عائقاً أمام ذلك لكون القانون هو قانون موضوعي وليس إجرائي مما يعني حتمية وجود قانون خاص يتناول كافة القواعد الموضوعية والإجرائية بالإضافة إلى قواعد التعاون الدولي في مكافحة الجريمة، ووضع تعاريف خاصة لهذا القانون للأهمية .

المطلب الثاني:

مشروع قانون المعاملات الالكترونية

حيث جاء مشروع قانون المعاملات الإلكترونية والمقدم إلى مجلس الوزراء بأحكام ونصوص ناظمه للمعاملات الإلكترونية المدنية والتجارية ، حيث تضمن أحكاما خاصا بالعقوبات ، الا أن هذه الاحكام جاءت لتعاقب على مخالفة أحكام القانون ذاته، حيث يصعب تطبيقها في حالة ارتكاب جريمة الترويج للمخدرات بوسائل الكترونية أو في حالة غسل الأموال أو التشهير أو الاتجار بالبشر أو أي من الجرائم الإلكترونية المعروفة هذا من ناحية ، ومن ناحية أخرى يمكن لنا تطبيق العقوبات

الواردة في مشروع قانون المعاملات الالكترونية في حالة وقوع جريمة تزوير يكون محلها أداة التوقيع أو أنظمة التوقيع الإلكترونية، وهذا كله يدخل ضمن إطار المخالفة للأحكام الواردة في ذات المشروع، ومما يجدر التنويه اليه هو ضرورة مراجعة مشروع قانون الجرائم الإلكترونية ومشروع قانون المعاملات الإلكترونية بحيث لا يوجد تعارض بينهما وتحقيق الانسجام التشريعي، ويلاحظ على مشروع قانون المعاملات الإلكترونية وبعد مراجعته مع مشروع قانون الجرائم الإلكترونية المقدم لمجلس الوزراء ما يلي :

1- ضرورة اعادة ضبط وتوحيد التعريفات بين مشروعي القانون.
2- قانون المعاملات الإلكترونية تضمن نصوص عقوبات، وهذا التوجه غير صائب حيث إن هذا القانون هو قانون إجرائي شأنه شأن قانون البينات في المواد المدنية – والتجارية الذي لا يفترض أن يتضمن عقوبات وانما دوره أن يحيل على قانون جرائم تقنية المعلومات .
3- وعليه لابد من ازالة نصوص العقوبات من هذا المشروع كون قانون جرائم تقنية المعلومات هو القانون الاساسي بالنسبة له والاحالة في كل الجرائم العقوبات إلى قانون جرائم تقنية المعلومات.
4- يجب أن يتضمن قانون مكافحة تقنية المعلومات كل الأوصاف التي يمكن أن تعد جرم في نظر قانون المعاملات الإلكترونية ليتم تجريمها بموجبه.

المطلب الثالث:

مشروع قانون الجرائم الالكترونية

جاء هذا المشروع بأحكام ونصوص لتحديد الافعال المجرمة والعقوبات المقررة لها، حيث تضمن عدة جرائم الكترونية تم تصنيفها إلى عدة أقسام، وبالرجوع إلى القواعد العامة المتعلقة بأركان الجريمة والمتمثلة بالركن المادي أي الفعل والسلوك الإجرامي والنتيجة والعلاقة السببية ومن الركن المعنوي اي العلم والإرادة ، ولكن مدى توافر هذه الأركان يختلف من جريمة إلى أخرى حيث سنقوم ومن خلال بندين الأول قراءة في مشروع القانون من حيث تصنيف الجرائم الواردة منه، وفي البند الثاني قراءة نقدية لمشروع القانون، وهذا ما سنوضحه وفقا لما يلي:

أولاً: قراءة في الجرائم الإلكترونية الواردة في المشروع :

1- الجرائم الواقعة على البيانات :

لقد اشتمل مشروع القانون على الجرائم المتعلقة بالبيانات والمعلومات الإلكترونية التالية :

1. جريمة التوصل بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام(م1/3).

2. جريمة إلغاء أو حذف أو تدمير أو إفشاء أو اتلاف أو تغيير أو إعادة نشر البيانات أو المعلومات(م2/3).
3. جريمة تزوير مستند من مستندات الحكومة أو الهيئات أو المؤسسات العامة (م5).
4. تعطيل البرامج أو حذفها أو تعديلها أو إتلافها أو إيقافها عن العمل (م6).
5. جريمة فك مفاتيح التشفير الإلكترونية أو استخدام كلمة سر بقصد الدخول إلى نظام معلوماتي معين لارتكاب جريمة معينه (م1/25).
6. جريمة تعديل أو إتلاف الفحوصات الطبية أو التشخيص الطبي أو العلاج الطبي أو الرعاية الطبية (م8).
7. جريمة التنصت والتقاط أو اعتراض ما هو مرسل عن طريق الشبكة المعلوماتية (م9).
8. جريمة دخول موقع الكتروني لغايات تغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله (م15).

وتشمل أركان الجريمة في الجرائم المعلوماتية المذكورة أعلاه بما يلي:

أ. الركن المادي : يتمثل في تغيير الحقيقة في البيانات التي تتضمنها المستندات والمحررات الإلكترونية فإن تغيير وتعديل تلك البيانات يعتبر جريمة حتى لو لم تتحقق الغاية من التعديل والتحريف أو التزوير.

ب. الركن المعنوي : يتمثل باتجاه إرادة الجاني إلى الحاق الضرر بالمجني عليه مع علمه أن هذا الفعل يشكل جريمة.

2- الجرائم الواقعة على الأشخاص :

حيث تناول المشروع الجرائم الالكترونية الواقعة على الأشخاص على الوجه التالي:

1. جريمة انشاء موقع لغايات التشهير بالأشخاص (م17) من المشروع :

وتتكون الجريمة من ركنين على الوجه التالي :

أ. الركن المادي لهذه الجريمة يتمثل بإنشاء موقع خاص للتشهير بشخص معين فان عدم تحقق النتيجة لا يعتد به حيث أنه لا يحول دون معاقبة الجاني أي أن مجرد انشاء الموقع يشكل جريمة.

ب. الركن المعنوي لهذه الجريمة يتمثل باتجاه ارادة الجاني إلى إنشاء الموقع لغايات التشهير بشخص معين أي التحقيق الفوري للجريمة.

2. جريمة إنشاء موقع لغايات الاتجار بالأشخاص وتسهيل التعامل به(م18) من المشروع :

وتتكون الجريمة من ركنين على الوجه التالي :

أ. الركن المادي يتمثل بإنشاء الموقع لغايات الاتجار بالبشر فإن عدم تحقق النتيجة لأسباب عارضه لا يحول دون معاقبة الجاني.

ب. الركن المعنوي يتمثل باتجاه ارادة الجاني للإتجار بالأشخاص والحاق الضرر بهم.

3. **جريمة تهديد شخص أو ابتزازه للقيام بفعل معين أو الامتناع عن من خلال استعمال وسائل تقنية المعلومات(م10) من المشروع.**

أ. الركن المادي لهذه الجريمة يتمثل بوقوع فعل الابتزاز أو التهديد أي لا يكفي استعمال تقنية المعلومات بل لا بد من قيام المجرم بفعل التهديد أو الابتزاز فإن عدم تحقق النتيجة المرجوة من الجاني لا تحول دون معاقبته.

ب. الركن المعنوي : يتمثل باتجاه ارادة الجاني لاستخدام تقنية المعلومات لأجل ارتكاب جريمة الابتزاز او التهديد مع علمه بان هذا الفعل يشكل جريمة ويلحق الضرر بالآخرين.

4. **جريمة تحريض أنثى أو ذكر لارتكاب الدعارة والفجور وذلك من خلال استخدام وسائل تقنية المعلومات (م 14) من المشروع.**

أ. الركن المادي يتمثل بالقيام بفعل التحريض والاغواء باستخدام تقنية المعلومات فان وقوع فعل التحريض على ارتكاب فعل لا أخلاقي يشكل جريمة حتى لو لم تتحقق نتيجة التحريض.

ب. الركن المعنوي : اتجاه إرادة الجاني إلى تحقيق النتيجة مع علمه بذلك.

5. **جريمة انشاء المواقع الاباحية واللاأخلاقية والمخالفة للنظام العام. وذلك وفقا لأحكام المواد (19،21) من المشروع.**

أ. الركن المادي يتمثل: بإنشاء الموقع الإلكتروني ونشر الصور الاباحية عليه ونشر افكار تتناقض مع الأخلاق والدين وتحرض على نشر الرذيلة في المجتمع فان عدم تحقق النتيجة المرجوة من الجاني وهو ارتياد الأشخاص على هذه المواقع والتأثير عليها لا يحول دون معاقبة الجاني.

ب. الركن المعنوي يتمثل باتجاه ارادة الجاني وعلمه لتحقيق النتيجة.

6. **جريمة انشاء المواقع الإلكترونية للجماعات الإرهابية (م 22) من المشروع.**

أ. الركن المادي يتمثل بإطلاق الموقع الإلكتروني لغايات نشر الأفكار الإرهابية والترويج للجماعات الإرهابية والانضمام لها فإن عدم نشر تلك الأفكار لا يحول

دون معاقبة الجاني فان النتيجة المتمثلة بتشوية الأفكار وانحراف أخلاق المجتمع يكون تحقيقها نسبي أي أن هذه النتيجة غير حتمية.

ب. الركن المعنوي يتمثل باتجاه إرادة الجاني إلى إلحاق الضرر وإطلاق المواقع الإلكترونية مع علمه بذلك.

3- الجرائم الواقعة على الاموال :

وتشتمل على الجرائم الماسة بالأموال وذلك على الوجه التالي:

1. جريمة الاستيلاء على مال منقول أو على سند أو توقيع من خلال وسائل تقنية المعلومات.(م11) من المشروع.
2. جريمة الوصول دون وجه حق إلى ارقام او بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية للحصول على أموال غيره أو ما تتيحه من خدمات.(م12) من المشروع .
3. جريمة تحويل الاموال غير المشروعة أو نقلها او تمويه المصدر غير المشروع لها أو إخفائه أو قام باستخدام الأموال أو اكتسابها أو حيازتها .(م20) من المشروع .

وتتكون الجريمة من ركنين على الوجه التالي:

أ. الركن المادي لهذه الجرائم يتمثل :الحصول على أرقام بطاقات الائتمان ومعرفة البيانات المالية الخاصة بذلك فان سرقة هذه البطاقات والاطلاع على البيانات الخاصة بذلك يشكل جريمة إضافة إلى قيامه بتحويل تلك الأموال.

ب. الركن المعنوي : يتمثل باتجاه إرادة الجاني إلى الحصول على أموال معينه مع علمه بأن ذلك يشكل جريمة.

ثانياً- قراءة نقدية لمشروع القانون:

1- عدم تضمين المشروع للمذكرة إيضاحية وكذلك مذكرة السياسة التشريعية .

2- عدم الإشارة في ديباجة المشروع إلى قرار بقانون رقم 15 لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات.

3 - الأفضل أن يتم تقسيم بنود مواد القانون إلى عناوين وكل عنوان يشرح ويبين الاحكام الخاصة بهذا الموضوع وتصنيف الجرائم إلى أقسام و فصول أو أبواب تجمعها قاسم مشترك مثل جرائم المحتوى والبيانات او الاعتداء على الأموال وهكذا.

4- ضرورة وضع فصل خاص بالتعاون والمساعدة القضائية الدولية وتنظيم قواعد الاختصاص القضائي والتعاون الدولي بوجه خاص.

5- ضرورة وضع فصل خاص للقواعد الإجرائية لمباشرة التحقيق واعمال الاستدلال في الجرائم المعلوماتية .

6- عدم تنظيم المشروع لأحكام خاصة بالعقوبات التكميلية كمصادرة العائد والأصول من الأنشطة غير المشروعة، ومصادرة الأجهزة والبرامج والوسائل المستخدمة .

7- ضرورة تشديد عقوبة الغرامة بحق الشخص المعنوي على نحو يعادل إضعاف الحد الأقصى للغرامة المحددة للشخص الطبيعي.

8- عدم الاهتمام بالقواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات التي تتم عبر وسائل تقنية المعلومات.

9- ضرورة تشديد العقوبة المتعلقة ببعض الجرائم نظراً لخطورة التهديدات المحتملة وأهمية المصالح المحمية كحالة الجرائم التي تمس بأمن الدولة وحالات استهداف الجريمة للبينات والمؤسسات العامة والرسمية للدولة.

الخاتمة

النتائـــــج:

بعد التطرق من خلال هذا البحث إلى الجريمة المعلوماتية من حيث ماهية الجريمة المعلوماتية، ثم الحديث عن صور وأشكال هذه الجريمة المعلوماتية حيث اتضح عدم كفاية النصوص القانونية التقليدية في قانون العقوبات وقانون الإجراءات الجزائية لمكافحة الجريمة المعلوماتية، وقصور التشريعات الفلسطينية المختلفة في معالجة هذه الجريمة لردع مرتكبيها، كما تم تناول المواجهة الدولية لمكافحة الجريمة المعلوماتية، والتطرق إلى المشاريع المتعلقة بمكافحة الجريمة المعلوماتية

فإن الباحث يقترح التوصيات التالية :

التوصيات :

1. العمل على صياغة مشروع قانون خاص بالجرائم المعلوماتية أسوةً بالاتجاه الغالب في الدول المقارنة و التوصية بضرورة وضع تشريع فلسطيني خاص لمكافحة الجرائم المعلوماتية يتفق مع الأحكام القانونية الدولية في مجال مواجهة هذه الجرائم أو من ناحية أخرى ضرورة إجراء تعديلات تشريعية على نصوص القانون الجنائي الفلسطيني (قانون العقوبات وقانون الإجراءات الجزائية) بالشكل الذي يجرم صور الجرائم المعلوماتية المختلفة سواءً أكان بشكلها التقليدي أو المستحدث، وكذلك تنظيم الأحكام الإجرائية الخاصة بمواجهة هذه الجرائم وكذلك تنظيم قواعد التعاون القضائي الدولي في هذا الخصوص.
2. أن يشمل القانون على الشروط والضمانات التي توفر الحماية الكافية لحقوق الإنسان والحريات الأساسية الأخرى، وصون حياته الخاصة حين ملاحقة الجرائم المعلوماتية.

3- شمول قانون مكافحة الجرائم المعلوماتية آلية التعامل مع الجرائم المعلوماتية من حيث ضبطها وتفتيشها والمعاينة وجمع الأدلة. وكذلك وضع قواعد إجرائية جزائية خاصة .

4- توعية الكوادر القضائية بنوعية هذه الجرائم وآلية التعامل معها في الجلسات وتحري الدليل وتحليله.

5- عقد اتفاقيات دولية تساعد في التعاون القضائي والأمني لضبط المجرمين والجرائم المعلوماتية.

6- استغلال المجرمين النوابغ في العلوم المعلوماتية في مجال مكافحة الجرائم المعلوماتية.

7- إقامة المؤتمرات وورش العمل للمتخصصين على المستوى الإقليمي والعالمي لتبادل الخبرات في هذا المجال والتوصية بضرورة وضع تشريع فلسطيني خاص لمكافحة الجرائم المعلوماتية يتفق مع الأحكام القانونية الدولية في مجال مواجهة هذه الجرائم أو من ناحية أخرى ضرورة إجراء تعديلات تشريعية على نصوص القانون الجنائي الفلسطيني (قانون العقوبات وقانون الإجراءات الجزائية) بالشكل الذي يجرم صور الجرائم المعلوماتية المختلفة سواء بشكلها التقليدي أو المستحدث وكذلك تنظيم الأحكام الإجرائية الخاصة بمواجهة هذه الجرائم، وكذلك تنظيم قواعد التعاون القضائي الدولي في هذا الخصوص.

8- التوصية بضرورة النص على اعتبار استخدام وسائل تقنية المعلومات من الظروف المشددة في ارتكاب الجرائم التقليدية الواردة في قانون العقوبات.

9- التوصية بضرورة تدخل المشرع ببسط الحماية في مجال الخصوصية في جميع الجهات، وعدم اقتصارها على الجهات التي نص عليها المشرع صراحة مثل قطاع الأحوال المدنية والبنوك، وكذلك مد تلك الحماية على المستوى الشخصي من خلال نص عام ينص على كفالة حماية كافة المعلومات والبيانات المتعلقة بالأشخاص في مختلف الجهات .

10- ضرورة اتباع وسائل التأمين الحديثة ضد المخاطر التي تتعرض لها وسائل تقنية المعلومات، وتطبيق إجراءات التأمين الفني لتأمين عملية الاتصالات واتباع القواعد التي تحكم أمن المعلومات وإعداد برامج أمن المعلومات من خلال تحديد المعلومات المهمة وتحليل المخاطر والتهديدات وتحليل القابلية للعدوان، وتطبيق الإجراءات المضادة ومرحلة التقييم وإيجاد نوع من التنسيق بين الجهات المختلفة في هذا المجال.

11- تسمية القانون "قانون مكافحة تقنية المعلومات" وليس قانون مكافحة الجرائم الإلكترونية لكونه أكثر شمولاً واتفاقاً مع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

المراجع:

1- أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع عمان الأردن، 2016.

2- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، 2014.

3- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة والمواثيق الدولية، دار النهضة العربية، القاهرة، 2011.

4- عبد اللطيف محمود ربايعة، الجرائم الالكترونية التجريم والملاحقة والإثبات، ورقة عمل مقدمة إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، جامعة النجاح الوطنية، نابلس فلسطين، 2016.

5- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، 2014.

6- علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري للنشر والتوزيع، عمان – الأردن، 2009.

7- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، مصر 2013.

8- محمد أمين الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان – الأردن، 2011.

9- نهلا عبد القادر المومني، الجرائم المعلوماتية، ،منشورات دار الثقافة للنشر والتوزيع، عمان–الأردن.

10-هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، مصر، 2011.