الجامعة الإسلامية- غزة

عمادة الدراسات العليا

كلية الشريعة والقانون

قسم القانون العام

الجرائم الإلكترونية في التشريع الفلسطيني

{دراسة تحليلية مقارنة}

The Electronic Crimes in the Palestinian law

(A comparative analytical study)

الباحث

يوسف خليل يوسف العفيفي

إشراف

د. أيمن عبد العال

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام من كلية الشريعة والقانون، بالجامعة الإسلامية بغزة.

١٤٣٥ هـ / ٢٠١٣ م

بسم الله الرحمن الرحيم

{ وَمَن يَتَّقِ اللَّهَ يَجْعَل لَّهُ مَخْرَجًا وَيَرْزُقْهُ مِنْ حَيْثُ لَا يَحْتَسِبُ وَمَن يَتَوَكَّلْ عَلَى اللَّهِ فَهُوَ حَسْبُهُ إِنَّ اللَّهَ بَالِغُ أَمْرِهِ قَدْ جَعَلَ اللَّهُ لِكُلِّ شَيْءٍ قَدْرًا }

صدق الله العظيم

[الطلاق: ٢- ٣]

إهداء

إلي كل من أضاء بعلمه عقل غيره أو هدى بالجواب الصحيح حيرة سائليه

فأظهر بسماحته تواضع العلماء وبرحابته سماحة العارفين

أهدي عملي هذا إلى أبي رمز العطاء

وإلى أمي عنوان المحبة والحنان

وإلى رفيقة دربي زوجتي

وإلى أملي المتجدد . .أولادي خليل وإلياس

وإلى أخوتي وأسرتي الكريمة

وإلى كل من علمني حرفاً أصبح سنا برقه يضيء الطريق أمامي

شكر وتقدير

انطلاقاً من قول رسول الله صلي الله عليه وسلم «لَا يَشْكُرُ اللَّهَ مَنْ لَا يَشْكُرُ النَّاسَ»[1]

أتقدم بجزيل الشكر والعرفان من الدكتور الفاضل/ أيمن نصر عبد العال رئيس قسم الشريعة والقانون بالجامعة الإسلامية، الذي أشرف على هذه الرسالة ومنحني من فكره الرشيد، ورأيه السديد، وبذل من جهده الكثير مما كان له أكبر الأثر في إخراج هذه الرسالة إلى النور، والشكر موصول لعضوي لجنة المناقشة الدكتور الفاضل/ باسم صبحي بشناق نائب عميد شئون البحث العلمي والدراسات العليا بالجامعة الإسلامية ، والدكتور الفاضل/ ساهر إبراهيم الوليد رئيس قسم الحقوق بجامعة الأزهر لقبولهما مناقشة هذه الرسالة.

وإلى أساتذتي في كلية الشريعة والقانون .

وإلى الدكتور القاضي عبد القادر جرادة والذي لم يبخل علينا يوماً من استشاراته السديدة.

وأخيرا أتوجه بكل مشاعر الحب والعرفان لكل من ساعدني وقدم لي العون في إنجاز هذه الدراسة.

[1] [رَوَاهُ أَحْمَدُ (٧٧٥٥)، وَأَبُو دَاوُد (٤١٩٨)، وَالتِّرْمِذِيُّ- صحيح الجامع (١٩٢٦) وصححه الألباني]

الملخص

تناولت هذه الدراسة موضوع " الجرائم الإلكترونية في التشريع الفلسطيني" من خلال ثلاثة فصول متكاملة، حيث كان الفصل الأول بعنوان "الجريمة الإلكترونية تعريفها صورها طبيعتها"، ففي البداية تم تسليط الضوء على تحديد المقصود بالجريمة بشكل عام، ومن ثم التركيز على تعريف الجريمة الإلكترونية وذكر الاتجاهات الفقهية التي ذهبت في تعريفها، وتحدث الباحث عن خصائص الجريمة الإلكترونية، وخصائص المجرم الإلكتروني، وتعرض الباحث إلى صور الجرائم الإلكترونية الحديثة بشكل عام، ومن ثم بيان هذه الصور التي وردت في قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦م مع تعديلاته لسنة ٢٠١٠م، والجرائم الإلكترونية التي أوردها مشروع قانون العقوبات لسنة ٢٠١٠م، والجرائم الإلكترونية التي نص عليها المشرع الأردني في قانون جرائم أنظمة المعلومات رقم ٣٠ لسنة ٢٠١٠م، ثم تطرق الباحث في نهاية هذا الفصل إلى الطبيعة القانونية لمحل الجرائم الإلكترونية.

أما الفصل الثاني فكان بعنوان " القواعد الموضوعية للجرائم الإلكترونية" ، وتطرق الباحث في بدايته إلى ركني الجريمة الإلكترونية، الركن المادي والركن المعنوي، ثم تناول الباحث ركني المحاولة في الجرائم الإلكترونية، وأظهر الباحث أن المحاولة متصورة ومتوقع حدوثها في الجرائم الإلكترونية، وفي نهاية هذا الفصل ركز الباحث على الجزاء الجنائي للجرائم الإلكترونية في القانون الفلسطيني على فرعين الأول الجزاء الجنائي للجرائم الإلكترونية في قانون العقوبات رقم ٧٤ لسنة ١٩٣٦م مع تعديلاته لسنة ٢٠١٠م، والثاني الجزاء الجنائي للجرائم الإلكترونية في مشروع قانون العقوبات لسنة ٢٠١٠م، وفي نهاية هذا الفصل تناول الباحث الجزاء الجنائي للجرائم الإلكترونية في قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م، وأوضح الباحث النقص الحاصل في قانون العقوبات رقم ٧٤ لسنة ١٩٣٦م وتعديلاته لسنة ٢٠١٠م، ومشروع قانون العقوبات لسنة ٢٠١٠م وبيّن كيفية الخروج من ذلك، وهو بتشريع قانون مستقل يكافح الجرائم الإلكترونية.

أما الفصل الثالث فكان بعنوان " القواعد الإجرائية للجريمة الإلكترونية "، وفيه تناول الباحث ثلاث مراحل تمر بها الدعوى الجزائية في الجرائم الإلكترونية، وكان أول هذه المراحل مرحلة جمع الاستدلالات، فبيّن الباحث ماهية مرحلة جمع الاستدلالات، والجهة المخولة بمباشرتها وصلاحيات مأموري الضبط القضائي في الظروف العادية والاستثنائية، والاشكالات التي تواجه مأموري الضبط القضائي في هذه المرحلة، ثم بيّن بعدها الباحث مرحلة التحقيق الابتدائي والجهة المخولة بهذه المرحلة وهي النيابة العامة، وأوضح الباحث صلاحيات النيابة العامة في مرحلة

التحقيق الابتدائي، وركز الباحث على عملية التفتيش في الجرائم الإلكترونية وتناول صلاحيات النيابة العامة في التفتيش، وصلاحيات مأمور الضبط القضائي في التفتيش في حالة التلبس، وبيّن الباحث الإشكالات التي تواجه عملية التفتيش في الجرائم الإلكترونية، وختم هذا الفصل بشرح مرحلة المحاكمة في الجرائم الإلكترونية والجهة المختصة بها، مع بيان الصعوبات التي تواجه هذه المرحلة مثل مدى اقتناع القاضي بالأدلة الإلكترونية، وموضوع تسليم المجرمين.

Abstract

This study discusses the idea of "Electronic Crimes in Palestinian Legislation" through three integrated chapters. In first chapter, entitled "Electronic Crime: definition, from and nature," the light is shed on defining the notion of crime in general.

After that, it's been focused on defining Electronic Crimes and mentioning the religious trends that defined it. The researcher stated the properties of Electronic Crime and the characteristics of the criminal. The researcher also discusses the forms of modern electronic crimes in general and then traces them in the Palestinian penal code number 74 of 1936 and it's adjustments in 2010, electronic crimes in the penal code bill of 2010 and the electronic crimes in the Jordanian crime law of Information Technology number 30 of 2010.

After this the researcher talks about the legal nature of Electronic Crimes at the end of the chapter.

The second chapter is entitled "The procedural Rules of Electronic Crime". In the beginning of the chapter, the researcher discusses the divisions of the Electronic Crime; the physical division and the moral division. Then the researcher talks about the attempt in Electronic Crime, and he states that attempt is possible in Electronic Crime.

At the end of the chapter, the researcher focuses on the criminal penalty of the Electronic Crime in the Palestinian law through two sections. The first is the criminal penalty of Electronic Crime in the Palestinian penal code number 74 of 1936 and it's adjustments of 2010.

The second section is the criminal penalty of Electronic Crime in the penal code bill of 2010.

At the end the researcher discusses the criminal penalty of Electronic Crime in the Jordanian crime law of It number 30 of 2010. The researcher clarifies the deficiency in the penal code number 74 of 1936 and it's adjustments of 2010 and the penal code bill of 2010, and he

suggests how to overcome it using an independent code bill that fights Electronic Crime.

The third chapter is called "The practical rules in Electronic Crime" in which the researcher discusses the steps of a criminal case in Electronic Crime in three phases. The first phase is collecting evidence. The researcher explains the it and the entity authorized of it and the powers of the judicial officers in normal and exceptional cases and the obstacles that face the judicial officers in this phase. After that the researcher explains the phase of preliminary investigation and the entity authorized of it, which is the public prosecution. The researcher states the powers of the public prosecution in the preliminary investigation, And he also focuses on inspection in Electronic Crime, the role of public prosecution in inspection, and the powers of judicial officers in inspection in the case of flagrante. The researcher then discusses the obstacles that faces inspection in Electronic Crime. Finally the researcher concludes the chapter explaining the phase of trial in Electronic Crime and the entity authorized of it with the obstacles that faces trials such as convincing the handing the criminals.

Researcher:
Youssef Kh. Al Afifi

Translator:
Mohammed A. Eldada

بسم الله الرحمن الرحيم

مقدمة

الحمد لله رب العالمين علم بالقلم علم الإنسان ما لم يعلم، والصلاة والسلام على معلم الناس الخير سيدنا محمد وعلى آله وصحبه وسلم...أما بعد:

كشفت السنوات الأخيرة النقاب عن تكنولوجيا متطورة، لم تكشفها عقوداً من الزمن، وازاء التطورات السريعة والمذهلة في هذه التكنولوجيا التي جاءت لخدمة الإنسان، إلا أنه لم يرق للبعض أن يحسن استخدامها، فأساء استخدامها وألحق الضرر بأخيه الإنسان، فسبه وقذفه وسرق ماله وأتلف محتويات وأنظمة حاسوبه وكذلك قتله، لنجد أنفسنا أمام صنوف شتى من الجرائم الإلكترونية.

وإزاء ذلك يبرز دور كل منا في محاربة هذه الجريمة وصد مرتكبيها، ولاسيما رجال القانون حيث أنها تعتبر تحدياً كبيراً أمامهم وذلك لاختلافها النوعي عن الجريمة التقليدية، فالمجرم الإلكتروني يسب ويسرق ويخرب ويقتل وهو في بيته ولم يغادر مكانه ودون أن يبذل الكثير من الجهد.

وقد خلت كثير من التشريعات في بعض الدول من النصوص التي تعالج هذه الجرائم ومن بينها فلسطين إلى وقت قريب، حتى تم إدخال بعض التعديلات على قانون العقوبات المطبق، إلا أنه وبإمعان النظر فيه نجد أنه قاصر عن معالجة بعض الجرائم الإلكترونية، غير أن الباحث وجد أن مشروع قانون العقوبات الفلسطيني أفرد باباً خاصاً لهذه الجرائم.

ونظراً لحداثة الجرائم الإلكترونية، وظهورها مع كل تقنية حديثة يتم اكتشافها وتوفيرها لأفراد المجتمع، نجد إساءة في استخدامها، ما يستوجب على المشرع الفلسطيني مواكبة التطور الحاصل على الصعيد التقني، من خلال استحداث نصوص تشريعية لمكافحة الجرائم الناتجة عن هذه التقنيات ووضع حد لها، وبالتالي العمل على تقليلها إن لم يكن في الإمكان القضاء عليها.

وبالنظر إلى المجرم الإلكتروني، فإننا نواجه هنا نوع متميز من المجرمين وذلك لتمتعهم بذكاء حاد، ومعرفتهم كيفية الإفلات من العقاب، وصعوبة إثبات جرائمهم، وسهولة ارتكاب هذا النوع من الجرائم من قبلهم دون أن يبذلوا الكثير من الجهد، وكل ذلك يستلزم معالجته من خلال تعيين خبراء يستعان بهم في محاربة هذه الجرائم.

ويطلق بعض فقهاء القانون على هذا النوع من الجرائم " الجرائم الإلكترونية عابرة الحدود " نظراً لارتكاب بعض المجرمين جرائمهم بحيث يكون المجرم في دولة، والمجني عليه وموضوع الجريمة في دولة أخرى، مثل سرقة خطوط الاتصالات الدولية وخطوط الإنترنت والهاكرز وغيرها، ومثل هذه الحالات تحتاج لمعالجة من خلال وجود تعاون دولي، واتفاقيات دولية لمكافحة الجرائم الإلكترونية.

وبدأت دول العالم تفرد تشريعات خاصة لمكافحة الجرائم الإلكترونية، وكانت السويد لها السبق عالمياً، بينما كانت سلطنة عمُان لها السبق بين الدول العربية في تشريع قانون لمكافحة الجرائم الإلكترونية وتبعتها بعد ذلك السعودية والإمارات والسودان ودول عربية أخرى .

إن إفراد قانون خاص لمكافحة الجرائم الإلكترونية بات اليوم ضرورياً من أي وقت مضى، لانتشار نظام الحكومة الإلكترونية ، والتي تستند في أغلب معاملاتها الإدارية والمالية على الوسائل الإلكترونية الحديثة والإنترنت ، وذلك في مجال الاقتصاد والتجارة والأمن والصحة في المجتمع .

أولاً : موضوع البحث :

دراسة موضوع الجرائم الإلكترونية من حيث ماهيتها وخصائصها وأركانها وتمييزها عن غيرها من الجرائم، وبيان أنواعها، والحديث عن بعض قواعدها الموضوعية والإجرائية وصولاً إلى محاكمة مرتكبيها .

ثانياً : أهمية البحث وسبب اختياره :

تأتي أهمية إعداد هذا البحث وسبب اختياره لعدة أسباب، أهمها:

١- حداثة الجريمة الإلكترونية في المجتمع الفلسطيني، وتأثيرها بشكل كبير على الأطفال والمراهقين ، الأمر الذي يمثل تهديداً للأمن العام في المجتمع .

٢- إن المشرع الفلسطيني لم يقر قانون لمواجهة الجرائم الإلكترونية ، مع وجود مشروع قانون العقوبات الذي تحدث في فصل كامل عن هذه الجرائم.

٣-ندرة الدراسات القانونية الفلسطينية في هذا الموضوع، فنكاد لا نجد دراسة قانونية متكاملة عن الجرائم الإلكترونية في التشريع الفلسطيني.

٤- رغبة الباحث نفسه في دراسة هذا الموضوع، من خلال شرح الجرائم الإلكترونية بالتفصيل ، وبيان أحكامها.

ثالثاً: أهداف البحث:

١- تقديم رؤية قانونية متكاملة حول الجرائم الإلكترونية ، وأنواعها ، وأركانها ، والأحكام الموضوعية والإجرائية فيها .

٢- معرفة سلطات الضبط القضائي والنيابة العامة والتمييز بينهما في التحقيق في الجرائم الإلكترونية ، وكذلك المحكمة المختصة بالنظر فيها .

٣- بيان مدى فعالية نصوص التجريم للجرائم الإلكترونية في التشريع الفلسطيني مقارنة مع التشريع الأردني والقوانين العربية الأخرى.

رابعاً: مشكلة البحث :

تتلخص مشكلة البحث في أن القانون الفلسطيني لم ينص على كافة أشكال الجرائم الإلكترونية، وكذلك قانون الإجراءات لم يعالج الإجراءات التي تتعلق بالتحقيق فيها مثل الكشف والمعاينة والتفتيش والضبط خاصة إذا كانت هذه الإجراءات تنصب على المعطيات المعنوية

للجهاز الإلكتروني، ولم ينص المشرع على الضمانات التي يجب أن يحاط بها المتهم إذا ما تم تفتيش أو ضبط الجهاز الإلكتروني الخاص به خاصة إذا كان الجهاز يحتوي على بيانات ومعلومات تمس حياته الشخصية.

خامساً: أسئلة البحث :

تثير هذه الدراسة الكثير من التساؤلات ومنها ما هو تالي :

١- ما هي الجريمة الإلكترونية ؟

٢- ما هي خصائص الجريمة الإلكترونية ؟

٣- ما هي إجراءات التحقيق في الجريمة الإلكترونية ؟

٤- ما هو موقف المشرع والقضاء الفلسطيني من الجريمة الإلكترونية ؟

٥- هل يتناسب الجزاء الجنائي المقرر على مرتكب الجرائم الإلكترونية مع جسامة السلوك المرتكب ؟

سادساً : منهجية البحث :

أتبع الباحث المنهج المقارن بين القانون الفلسطيني والقانون الأردني في هذا البحث، مع الإشارة إلى موقف بعض التشريعات العربية كالتشريع العُماني والإماراتي والسعودي والسوداني، والأجنبية مثل الولايات المتحدة وفرنسا وانجلترا وكندا.

وكذلك أتبع الباحث المنهج الوصفي التحليلي لجملة من النصوص القانونية للوقوف على معرفة الجريمة الإلكترونية من حيث ماهيتها وخصائصها وأركانها ، والجزاء الجنائي المترتب على ارتكابها ، وبعض أحكامها الموضوعية والإجرائية ، للخروج منها برؤية قانونية مفادها مدى إمكانية مكافحة الجريمة الإلكترونية والمعاقبة عليها .

وسيستند الباحث في هذا البحث إلى العديد من المراجع مثل الدساتير والقوانين والأنظمة والمعاهدات والاتفاقيات الدولية، والكتب القانونية والصحف المحلية، والمقالات المنشورة على المواقع الإلكترونية.

سابعاً : هيكلية البحث :

الفصل الأول / الجريمة الإلكترونية تعريفها ، صورها ، طبيعتها .

المبحث الأول / تعريف الجريمة الإلكترونية وخصائصها .

المبحث الثاني / صور الجريمة الإلكترونية .

المبحث الثالث / الطبيعة القانونية لمحل الجريمة الإلكترونية .

الفصل الثاني / القواعد الموضوعية للجرائم الإلكترونية .

المبحث الأول / أركان الجريمة الإلكترونية .

المبحث الثاني / المحاولة في الجرائم الإلكترونية.

المبحث الثالث / الجزاء الجنائي للجرائم الإلكترونية .

الفصل الثالث / القواعد الإجرائية للجريمة الإلكترونية .

المبحث الأول / جمع الاستدلالات في الجرائم الإلكترونية .

المبحث الثاني / التحقيق الابتدائي في الجرائم الإلكترونية .

المبحث الثالث / المحاكمة في الجرائم الإلكترونية .

الفصل الأول

الجريمة الإلكترونية تعريفها ، صورها ، طبيعتها

تمهيد وتقسيم

يعتبر الإنترنت أكبر بوابة علمية تم اكتشافها حتى الآن، من خلاله يستطيع الفرد أن يقوم بالكثير من الاعمال والتصرفات التي كانت تحتاج سابقاً إلى مجهود بدني ، ولكن كلما ظهرت سبل التيسير على الأفراد من خلال استعمال الإنترنت ، ظهر من يفسد سهولة استخدام هذه التقنية في أمن وأمان ، وهذا ما يضعنا بين دفتين ظهور جرائم إلكترونية جديدة من جهة ، وقيام ثورة تقنية وتشريعية لمكافحة هذه الجرائم من جهة أخرى ، وعلى ذلك وقبل الخوض في غمار الحديث عن الجريمة الإلكترونية لابد لنا أن نقف أولاً على تعريف الجريمة الإلكترونية ، ومعرفة خصائصها وصورها وطبيعتها وذلك عبر المباحث التالية:

المبحث الأول : تعريف الجريمة الإلكترونية وخصائصها .

المبحث الثاني : صور الجريمة الإلكترونية .

المبحث الثالث : الطبيعة القانونية لمحل الجريمة الإلكترونية .

المبحث الأول

تعريف الجريمة الإلكترونية وخصائصها

تعد الجريمة الإلكترونية من الجرائم الحديثة ، ولذلك لن نجد تعريف لها إلا في شروحات الفقه واجتهاد القضاء الحديث ، وعليه فإن الجريمة الإلكترونية كظاهرة إجرامية لها طبيعة خاصة تختلف عن باقي الجرائم ، وذلك ما سنوضحه فيما هو تالٍ :

المطلب الأول : تعريف الجريمة الإلكترونية .

المطلب الثاني : خصائص الجريمة الإلكترونية والمجرم الإلكتروني .

المطلب الأول

تعريف الجريمة الإلكترونية

لم يعرف المشرع الفلسطيني الجريمة الإلكترونية كون هذه الجريمة حديثة على الساحة الفلسطينية كما لم يتطرق الفقه والقضاء الفلسطيني إلى تعريفها.

وعرف المشرع السعودي الجريمة الإلكترونية بأنها: " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام "[١].

وعرفها القانون الأمريكي بأنها: " الاستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة "[٢].

ونرى تميُز تعريف القانون الأمريكي للجريمة الإلكترونية عن التعريف السعودي ، حيث وضح مدى خطورة بعض أنواع هذه الجريمة عن طريق تصنيفها ما بين جنحة وجناية ، وهذا ما

---

[١] راجع المادة رقم ١/٨ من نظام مكافحة جرائم المعلوماتية السعودي رقم م/١٧ ، لسنة ١٤٢٨هـ، مشار إليه في الموقع الرسمي لمجلس الوزراء السعودي عبر الرابط التالي: http://www.boe.gov.sa/ .

[٢] أنظر القانون الأمريكي رقم ١٢١٣ لسنة ١٩٨٦ م الخاص بمواجهة جرائم الكمبيوتر ، مشار إليه في كتاب رامي متولي القاضي، **مكافحة الجرائم المعلوماتية** ، الطبعة الأولى ، دار النهضة العربية، القاهرة، ٢٠١١م، ص٢٣ .

نطالب به المشرع الفلسطيني بأن يضع قانون كامل يختص بالجرائم الإلكترونية ، ويصنف هذه الجرائم ما بين الجنحة والجناية.

لم يستقر الفقه الحديث في وضع تعريف محدد للجريمة الإلكترونية ، كون هذه الظاهرة المستحدثة تتطور من حين إلى آخر ، وهناك عدة أسماء أطلقت على هذه الجريمة منها : الجريمة المعلوماتية أو الجريمة الإلكترونية أو الجرائم المرتبطة بالكمبيوتر أو جرائم الكمبيوتر والإنترنت أو الجرائم التقنية العالية أو جرائم الشبكة العنكبوتية[١].

ولذلك وقبل الخوض في تعريف الجريمة الإلكترونية ، لا بد وأن نتطرق إلى معرفة ماهية الجريمة بحد ذاتها بشكل عام، فقد عرّف القانون التفسيري الفلسطيني الجريمة بـ" ....ونعني لفظة جرم كل فعل أو محاولة أو ترك يستوجب العقوبة بحكم القانون "[٢].

وتعددت التعريفات الفقهية لمصطلح الجريمة ، ولكن لا يوجد بينها اختلاف كبير، فقد عرفها أحد الفقهاء بأنها: "سلوكاً اجتماعياً يثير في ضمير الرأي العام شعوراً بضرورة توقيع عقوبة لأنه يهدر مصلحة من المصالح التي يقوم عليها كيان المجتمع"[٣]، وعرفها آخر بأنها: "سلوك إنساني يرتكب إخلالاً بقواعد القانون الجزائي يترتب عليه المساس بمصلحة يحميها الشارع ، ويوقع القضاء على مرتكبه الجزاء الجنائي المناسب "[٤]، وعرفها آخر بأنها: "سلوك انساني إرادي آثم، ينظم أحكامه المشرع ويحدد خصائصه ويرتب عليه نتائج قانونية"[٥].

من ذلك يتضح لنا أن جميع الجرائم لها سمات مشتركة ، في كون أن السلوك الإجرامي يجب أن يكون مخالفاً لأحكام القانون الذي يعمل على حماية مصالح الأفراد في المجتمع ، كما أن الإخلال بهذا القانون يوقع على مرتكبه الجزاء الجنائي المناسب من خلال محاكمة القضاء له.

---

[١] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، ٢٠١٠م، ص٦٢، ٦٣.

[٢] راجع المادة ٢ من القانون التفسيري الفلسطيني رقم ٩ لسنة ١٩٤٥ م ، والمادة رقم ٥ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ .

[٣] جلال ثروت، **قانون العقوبات**، القسم العام، الدار الجامعية، بيروت، غير متضمن سنة النشر، ص٨٩.

٤ عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، الجريمة والمجرم، المجلد الأول، مكتبة أفاق، غزة، ٢٠١٠م، ص١٠٧ .

[٥] يسر أنور علي، أمال عبد الرحيم عثمان، **أصول علمي الأجرام والعقاب**، الجزء الأول في علم الأجرام، غير متضمن دار النشر، ١٩٩٤م، ص٧٥.

ومن هنا يتجلى تطبيق مبدأ الشرعية في القانون الجنائي " لا جريمة ولا عقوبة إلا بنص قانوني"[١] فإن لم يكن هناك نص قانوني لم يكن بالتالي جريمة ولا عقوبة عليها .

وانقسم الفقه في تعريف الجريمة الإلكترونية إلى عدة اتجاهات والتي سنبينها عبر الفروع الأتية:

الفرع الأول

الجرائم التي تستهدف المعلومات أو البيانات الإلكترونية نفسها

هناك جانب من الفقه جعل موضوع الجريمة الإلكترونية المكونات المعنوية للحاسب الآلي مثل البرامج والبيانات والمعلومات المخزنة بأي واسطة إلكترونية، أو أنظمة المعلومات التي تشغل الأجهزة الإلكترونية.

فعرفها الفقيه (Rosenblatt) بأنها: " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه"[٢].

وعرفها الفقه الفرنسي بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية، والتي يمكن أن تكون جديرة بالعقاب"[٣].

وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: " الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيساً "[٤].

---

[١] راجع المادة ١٥ من القانون الأساسي الفلسطيني المعدل لسنة٢٠٠٥م، و المادة ١ في مشروع قانون العقوبات الفلسطيني.

[٢] مشار إليه لدى نهلا عبد القادر المومني، **الجرائم المعلوماتية**، رسالة ماجستير، الطبعة الثانية، دار الثقافة، عمان، ٢٠١٠م، ص٤٨.

[٣] مشار إليه لدى يوسف المصري، **الجرائم المعلوماتية والرقمية للحاسوب والإنترنت**، الطبعة الأولى، دار العدالة، القاهرة، ٢٠١١م، ص٩.

[٤] مشار إليه لدى أسامة أحمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة، **جرائم الحاسب الآلي والإنترنت**، الطبعة الأولى، دار وائل للنشر، عمان، ٢٠٠١م، ص٧٣ .

وعرفتها منظمة التعاون الاقتصادي والتنمية على أنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مُباشرة عن تدخل التقنية المعلوماتية"[١].

ويتضح لنا من خلال التعريفات السابقة أن الجريمة الإلكترونية طبقاً للاتجاه الموضوعي، هي الاعتداء سواء كان بالفعل أو الامتناع على المعلومات الإلكترونية مما يسبب ضرر للغير، موجباً الجزاء الجنائي عن هذا الاعتداء .

الفرع الثاني

الجرائم التي ترتكب بواسطة النظام الإلكتروني

وطبقاً لهذا الاتجاه فالجرائم الإلكترونية هي التي ترتكب بواسطة النظام الإلكتروني، أي أن هذا الاتجاه جعل الوسيلة الإلكترونية شرطاً في قيام الجريمة الإلكترونية:

فعرفها الأستاذ (جون فور ستر) وكذلك الأستاذ (Eslie D.Ball) أنها: " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية "، ويعرفها الفقيه (تاديمان Tiedemaun) بأنها: " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب "[٢].

وعرفها الفقيه (دول) بأنها: " كل فعل إجرامي يستخدم الحاسب الآلي لإتمامه"، وعرفها الفقيه (لميتو) بأنها: "الفعل غير المشروع الذي يستخدم فيه الحاسب الآلي كأداة رئيسية"[٣].

ومن هذه التعريفات يتضح أن هذا الجانب من الفقه نظر إلى الجريمة الإلكترونية من حيث الوسيلة التي يرتكب من خلالها ، وهو الحاسب الآلي بشتى أنواعه وأسمائه ، وهذه الوسيلة التي يرتكب من خلالها الجريمة الإلكترونية تعتبر ركناً أساسياً من أركان الجريمة الإلكترونية ، فلا يمكننا أن نتصور وجود جريمة إلكترونية بدون وجود الوسيلة وهي الحاسب الآلي .

---

[١] مشار إليه لدى رامي متولي القاضي ، المرجع السابق، ص٢٣ .

[٢] مشار إليه لدى يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، ٢٠١١م، ص١٣ .

[٣] مشار إليه لدى أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٦٥.

الفرع الثالث

التعريف الشامل للجريمة الإلكترونية

جمع بعض الفقهاء بين الاتجاهين، الاتجاه الموضوعي الذي ينظر إلى البيانات والمعلومات، وبين الاتجاه الذي يأخذ بالوسيلة التي ترتكب بها الجريمة الإلكترونية، ومن هذه التعريفات ما هو آت :

فعرفها جانب من الفقه بأنها: " ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعلها" ، كما عرفها آخر بأنها: " الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني"[١].

وعرفها جانب آخر بأنها: "كل جريمة تتم في محيط أجهزة الكمبيوتر "، أو " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها "[٢].

وسماها البعض بالإرهاب الإلكتروني وعرفه بأنه : " هو ذلك الذي ينتج عن التطور التكنولوجي والثورة المعلوماتية ، باستغلال شبكة الإنترنت للهدم والتخريب "، وعرفها آخر أيضاً بأنها: "العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه وصور الإفساد في الأرض " ، ويعرف أيضاً الإرهاب الإلكتروني بأنه: "هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين ، أو هو مهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية ، واستخدام التقنيات الرقمية لإخافة وإخضاع الآخرين بشتى صنوف العدوان وصور الإفساد"[٣].

---

[١] مشار إليه لدى علي جبار الحسيناوي، **جرائم الحاسوب والإنترنت**، دار اليازوري للنشر والتوزيع، عمان، ٢٠٠٩م، ص٣٣.

[٢] مشار إليه لدى خالد ممدوح إبراهيم، **حوكمة الإنترنت**، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، ٢٠١١م، ص٣٥٧، ٣٥٨.

[٣] مشار إليه لدى محمد محمد الألفي، **المواجهة الأمنية والتشريعية لجرائم الإرهاب عبر الإنترنت**، المكتبة المصرية الحديثة، القاهرة، ص ١٣ .

ومما سلف يتضح أن تسمية الجريمة الإلكترونية بالإرهاب الإلكتروني غير مناسب، إلا إذا كانت الجريمة منظمة ومدعومة من قبل فئات مأجورة، تستهدف الأمن والسلم الإقليمي أو العالمي، فعندئذ يمكننا تعريف الجريمة الإلكترونية بالإرهاب الإلكتروني.

وعرفها الفقه المصري بأنها: " كل فعل أو امتناع عمدي ، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية "، أو أنها " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة ، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[١].

وعرف الفقه الأردني الجريمة الإلكترونية :

حيث عرفها جانب منه بأن: " هي الجرائم التي يكون فيها الحاسوب وسيلة ارتكاب فعل غير مشروع، أو محل لوقوع الفعل غير المشروع، وذلك بالقيام بعمل أو الامتناع عن أدائه من شأنه الاعتداء على الأموال المادية أو المعنوية، شريطة أن يكون مرتكبها على معرفة تقنية في استخدام الحاسوب والتعامل مع معطياته "[٢].

وعرفها آخر بأنها: " كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها "[٣].

وعرفها آخر بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجاً بطريقة مباشرة وغير مباشرة لتدخل التقنية المعلوماتية"[٤].

وفي الواقع قد تؤدي بعض أنواع الجرائم الإلكترونية إلى إتلاف آلاف الأجهزة أو خسائر بالملايين، أو قد تؤدي إلى جرائم قتل مثل اختراق برامج المستشفيات والعبث في أجهزة الإنعاش عن طريق الإنترنت، وكذلك قد تؤدي إلى إفشاء أسرار الدولة، ولذلك تعتبر هذه الجرائم خطرة

---

[١] مشار إليه لدى محمد علي العريان ، **الجرائم المعلوماتية** ، دار الجامعة الجديدة ، الاسكندرية، ٢٠١١م، ص٥٦.

[٢] خالد عياد الحلبي ، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت** ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م ، ص ٣١ .

[٣] محمد أمين الشوابكة ، **جرائم الحاسوب والإنترنت / الجريمة المعلوماتية** ، الطبعة الرابعة ، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م ، ص ١٠ .

[٤] محمود أحمد عبابنة ، **جرائم الحاسوب وأبعادها الدولية** ، الطبعة الأولى / الإصدار الثاني ، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٩م، ص ١٩ .

وتهدد الأمن العام في المجتمع، ويجب معالجتها من خلال وضع التشريعات المناسبة للقضاء عليها.

وخلاصة القول يرى الباحث أن أغلب التعريفات السابقة لم تكن متكاملة في تعريف الجريمة الإلكترونية ولذلك يمكننا تعريفها بأنها: " كل فعل أو امتناع عن فعل بشكل عمدي مخالف لأحكام القانون ، يرتكبه شخص أو أكثر عبر جهاز إلكتروني، مما يتسبب هذا الفعل أو الامتناع ضرر للغير يستوجب إيقاع العقوبة المناسبة على الفاعل وتعويض مادي عادل".

المطلب الثاني

خصائص الجريمة الإلكترونية والمجرم الإلكتروني

تختلف الجريمة الإلكترونية عن الجريمة التقليدية من حيث خصائصها ، فالجريمة الإلكترونية لم تظهر إلا في عصر الحاسب الآلي والإنترنت ، وكون هذه الجرائم حديثة ومتطورة فإن لها خصائص منفردة تتميز بها عن غيرها من الجرائم التقليدية ، وهذه الخصائص يمكننا أن نستخرجها من خلال التعريف الذي انتهينا إليه في نهاية المطلب السابق، كما أن المجرم الإلكتروني له سمات منفردة به لا نجدها في المجرمين الآخرين[١]، وكل ذلك سنفصله عبر الفروع الأتية :

الفرع الأول

خصائص الجريمة الإلكترونية

للجريمة الإلكترونية مجموعة من الخصائص التي تنفرد بها عن الجرائم التقليدية، ومن أهم هذه الخصائص أن الجرائم الإلكترونية تتطلب وجود جهاز إلكتروني ومعرفة كيفية استخدامه، وإن الهدف من هذه الجرائم الكيانات المعنوية لهذا الجهاز، كما أن الجريمة الإلكترونية لا حدود لها، وهذه الجرائم صعبة الأثبات والاكتشاف، ولذلك فهي مغرية للمجرمين، وعلى ضوء ما سبق سنتناول هذه الخصائص بالتفصيل عبر ما هو تالٍ:

---

[١] عبد العال الديربي، محمد صادق إسماعيل، **الجرائم الإلكترونية**، الطبعة الاولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢م، ص٤٧.

أولاً : يتطلب لارتكابها وجود جهاز إلكتروني ومعرفة بتقنية استخدامه:

تتميز الجريمة الإلكترونية عن غيرها أن الجهاز الإلكتروني هو أداة الجريمة ووسيلة تنفيذها، أو هو موضوع الجريمة كإتلاف أو سرقة البيانات والمعلومات وهنا تثور المشكلة، أما لو كان موضوع الاعتداء هو الجهاز نفسه أو شاشته أو الكيانات المادية للحاسب الآلي فهنا تكفي نصوص التجريم التقليدية، ويطبق قانون العقوبات الفلسطيني على موضوع الجريمة، فبدون الجهاز الإلكتروني تنتفي الجريمة الإلكترونية، وتتطلب هذه الجريمة دراية كافية وخبرة فائقة بالكمبيوتر والإنترنت في بعض الجرائم، أو معرفة بسلوكيات الفعل المرتكب في الجرائم البسيطة منها، كما أنها لا تمتاز بالعنف، وأغلب الجرائم الإلكترونية ترتكب عبر الإنترنت[١].

ولذلك فإن ما يميز الجريمة الإلكترونية عن غيرها من الجرائم، أنها تتطلب وجود علم كافي بالجوانب الفنية والتقنية لاستخدام الحاسوب والإنترنت، وتعتبر العلاقة بين مدى الدراية بالجوانب الفنية والتقنية للحاسوب وبين الجريمة الإلكترونية علاقة طردية، فكلما زادت الخبرة لدى الأفراد بمعرفة تقنية الحاسوب، زاد احتمال استخدام خبرتهم بشكل غير مشروع[٢].

وأثبت الواقع العملي[٣] أن الجرائم الإلكترونية قد ترتكب من خلال الهواتف المحمولة، خاصة بعد ظهور أجهزة الهاتف الذكية والتي هي في الحقيقة عبارة عن أجهزة كمبيوتر صغيرة، والتي من خلالها يتم الاتصال بشبكة الإنترنت ، ويسهل تخزين ونقل المعلومات من خلالها، وليس كما ذكر بعض الباحثين بأن الحاسب الآلي هو الأداة الوحيدة في ارتكاب الجريمة الإلكترونية، ففي أيامنا هذه نرى أنه يمكن تصنيف هواتف المحمول الذكية ضمن أجهزة الكمبيوتر، وذلك لأنه لا يختلف عن الحاسوب سوى في الحجم – بل أن الهواتف الذكية يمكن من خلالها الاتصال المباشر بخلاف الحاسب الآلي – أما بالنسبة للوظائف الأخرى فتتم ممارسة جميع وظائف الحاسب الآلي من خلال الهاتف الذكي.

ويتمثل علاج المشكلة السابقة من خلال وجود برامج حماية على كل أجهزة الحاسوب سواء المنزلية أو المتوافرة في أماكن العمل، وذلك لضمان الحفاظ على الأسرار الشخصية والمهنية، وعدم جعل الجهاز متصل بالإنترنت والتيار الكهربائي خارج وقت الاستخدام له.

---

[١] رامي متولي القاضي، المرجع السابق ، ص ٥٢ – ٥٣ ، محمد محمد الألفي، المرجع السابق، ص ٨٢.

[٢] محمود أحمد عبابنة، المرجع السابق ، ص ٣٦ .

[٣] إن هذا الأمر قد اتضح لي أثناء عملي كمحقق في الشرطة الفلسطينية، وقد حققت في عدة جرائم إلكترونية، وكان الكثير من هذه الجرائم ترتكب عبر الهواتف المحمولة.

ثانياً : موضوع الاعتداء هو معطيات الجهاز الإلكتروني:

تعد البيانات والمعلومات المخزنة على الحاسب الآلي هي موضوع الجرائم الإلكترونية، فهذه البيانات يمكن تخزينها ونقلها من جهاز لآخر عبر الوسائط الصلبة أو المرنة أو عبر البريد الإلكتروني، ولذلك فهي تعتبر مكونات معنوية تقبل الحيازة والنقل، ويمكن سرقته وإتلافه، ولذلك يجب أن يكون هذا المال محل حماية من قبل القانون الجزائي[١].

وعليه فإذا كان موضوع الاعتداء هو الحاسب الآلي أو شاشته أو أحد مكوناته المادية فإنه في هذه الحالة يصلح تطبيق نصوص قانون العقوبات الفلسطيني، أما لو كان موضوع الاعتداء هو معطيات الحاسوب من البيانات والمعلومات، فنحن هنا بصدد جريمة إلكترونية وتحتاج إلى نصوص أكثر دقة في معالجتها.

ولذلك فإن البيانات والمعلومات الحاسوبية تعد مالاً قابل للحيازة والنقل، وله قيمة مادية، وقد نص المشرع الأردني في المادة ٥٤ من القانون المدني الأردني بأن " كل شيء يمكن حيازته مادياً أو معنوياً والانتفاع به انتفاعاً مشروعاً، ولا يخرج عن التعامل بطبيعته أو بحكم القانون، يصح أن يكون محلاً للحقوق المالية"[٢].

ثالثاً : الجريمة الإلكترونية لا حدود جغرافية لها :

أزالت الشبكة العنكبوتية – الإنترنت– كل الحدود الجغرافية بين الدول ، وجعلت العالم كله كقرية صغيرة يسهل التواصل بين الأفراد ليس في الدول وحسب بل أنه من السهل التواصل بين الأشخاص في القارات المختلفة ، وهذا ما جعل الجريمة الإلكترونية عابرة للحدود[٣].

ولأن أغلب الجرائم الإلكترونية ترتكب عبر الإنترنت فإنها تتسم بالطابع الدولي ، حيث تقع هذه الجرائم فيكون المجرم في دولة والمجني عليه في دولة أخرى، ويمكن أن يكون الضرر قد حدث في دولة ثالثة أو في عدة دول، مثل اختراق المواقع والأجهزة وإتلافها ، وسرقة البيانات والمعلومات والأموال، كل ذلك جعل من مكافحة الجريمة الإلكترونية أمراً عسيراً، وذلك لتعدد الأماكن التي تتعلق بالجريمة، و تنازع قوانين الدول الواجبة التطبيق ، واختلاف الإجراءات الجزائية

---

[١] خالد عياد الحلبي، المرجع السابق، ص ٥٥ .

[٢] المادة ٥٤ من القانون المدني الأردني رقم (٤٣) لسنة ١٩٧٦، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ui/main.html.

[٣] خالد ممدوح إبراهيم ، **حوكمة الإنترنت** ، المرجع السابق ، ص ٣٦٠ .

من دولة لأخرى ، وصعوبة ملاحقة الجناة، كل ذلك يتطلب وجود تعاون دولي للقبض على الجناة وتقديمهم للمحاكم المختصة بنظر النزاع [١].

فالتحقيق في الجرائم الإلكترونية يتطلب القيام بإجراءات وأعمال للتحقيق خارج حدود الدولة، مثل تفتيش المواقع الإلكترونية أو تفتيش الأجهزة الإلكترونية – المادية– للعثور على البيانات أو المعلومات ، أو إلقاء القبض على المطلوبين ، أو معاينة مسرح الجريمة ، وكل ذلك يحتاج إلى تعاون دولي ملموس على أرض الواقع[٢].

ويرى الباحث مما تقدم ضرورة التعاون الدولي لملاحقة المجرمين الإلكترونيين، مع أن يكون هناك دور أكبر وفعّال للإنتربول الدولي بشأن القبض على المجرمين الإلكترونيين وتسليمهم إلى الجهات القانونية المختصة، وتسهيل مهام مأموري الضبط القضائي بشأن إجراء الكشف والمعاينة والتفتيش وغيرها من الإجراءات المتعلقة بجمع الاستدلالات، والعمل على عقد المؤتمرات الدولية للخروج منها باتفاقيات دولية تعالج مشكلة مكافحة الجرائم الإلكترونية والقضاء عليها.

رابعاً : الجريمة الإلكترونية صعبة الاكتشاف والإثبات:

الجرائم الإلكترونية من الجرائم التي لا تترك آثار خارجية مادية، فهي لا تترك بقع دماء كما في جرائم الاعتداء والقتل، ولا إتلاف كما في جرائم السطو ، فالجريمة الإلكترونية جريمة نظيفة أي لا تترك آثار مادية ملموسة، ولذلك كانت هذه الجريمة صعبة الاكتشاف والإثبات.

ومما جعل الجرائم الإلكترونية صعبة الاكتشاف والإثبات البعد الجغرافي بين الجاني والمجني عليه كما ذكرنا، واستخدام الجاني وسائل فنية حديثة في جرمه، كما أن هذه الجرائم ترتكب في وقت سريع، ويتم محو أثرها في وقت أسرع لا يتعدى الثواني، ومما يزيد الأمر صعوبة عدم وجود خبرة لدى ضباط التحقيق في مثل هذه الجرائم من ناحية التحقيق والبحث على الأدلة والتحفظ عليها، ومن الصعوبات التي تواجه إثبات هذه الجرائم عدم اقتناع القضاة بكثير من الجرائم المستحدثة في هذا المجال[٣].

وتعد هذه الخاصية من السمات التي تتميز بها الجريمة الإلكترونية عن غيرها، فقد انتشرت مكاتب تقوم بأعمال السرقة والقرصنة، من خلالها يقوم بعض الأشخاص باستئجار قراصنة

---

[١] محمود أحمد عبابنة، المرجع السابق، ص ٣٥ .

[٢] رامي متولي القاضي ، المرجع السابق ، ص ٥٣ .

[٣] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت** ، المرجع السابق ، ص١٠٦ ، ١٠٧ .

محترفين لسرقة بيانات الشركات العالمية مقابل مبالغ من المال وبيعها لأشخاص مستفيدين، وكل هذه الأعمال غير مشروعة، وإن من الأسباب الكامنة في صعوبة اكتشاف واثبات هذه الجرائم عدم تقديم شكاوي من قبل أصحاب الشركات التي يتم اختراقها ، وذلك خوفاً على سمعة الشركة وعلى المستثمرين فيها[١].

ويؤكد لنا الواقع أننا بحاجة إلى توظيف خبراء تقنيين في هذا المجال، والعمل على تدريب ضباط التحقيق ليكون لديهم القدرة على معرفة الأدلة الإلكترونية والحفاظ عليها، وتوفير الأجهزة والبرامج الحديثة التي من خلالها يمكن استرجاع أي ملف أو معلومة تساعد في الكشف عن الحقائق، والأهم من ذلك أن يتم تطوير التشريع الفلسطيني ليستطيع مواكبة هذا التطور الإجرامي، وكذلك عقد دورات للقضاة في الدول الأكثر خبرة في هذا المجال ليلمسوا مدى خطورة هذه الجرائم على صعيد الفرد والمجتمع.

خامساً : الجرائم الإلكترونية جرائم الأذكياء:

الجريمة الإلكترونية جريمة ناعمة، وذلك لسهولة ارتكابها دون أي مجهود بدني يذكر، بخلاف الجريمة التقليدية التي تتطلب مجهود بدني مثل القتل والسرقة والاغتصاب، فالجرائم الإلكترونية لا تتطلب سوى علم كافي بالجوانب الفنية والتقنية للجهاز الإلكتروني، وتعتبر الجرائم الإلكترونية جرائم مغرية لسرعة تنفيذها وسهولة محو أدلة الإدانة فيها، فهي تنفذ عن بعد دون التواجد في مسرح الجريمة، ولا تتطلب سوى ضغط مفتاح معين في الجهاز لتنفيذها، ومن مغريات هذه الجرائم المكاسب المادية الضخمة التي تحققها في وقت قصير، خاصة الموظفين الذين يعملون في الشركات التي تعتمد على النظام الإلكتروني في عملها، فمن السهل لديهم اختراق الأجهزة والبرامج وتحقيق مأربهم[٢].

وفي الواقع إن كثير من المجرمين الإلكترونيين هم من صغار السن والمراهقين، نظراً لأن هاتين الفئتين من أكثر الفئات التي تقضي أوقات طويلة على الإنترنت، ومن كثرة ممارستهم للإنترنت تولدت لديهم الخبرة والقدرة على اختراق الأجهزة والقرصنة وارتكاب الجرائم.

---

[١] نهلا عبد القادر المومني، المرجع السابق ، ص٥٤.

[٢] أسامة أحمد المناعسة وآخرين ، **جرائم الحاسب الآلي والإنترنت** ، المرجع السابق ، ص١٠٧ .

الفرع الثاني

خصائص المجرم الإلكتروني

المجرم الإلكتروني شخص طبيعي، لديه قدرة على تشغيل الحاسب الآلي واستخدامه، وليس المقصود بالقدرة هنا هو الخبرة العالية، ولكن القدرة هنا تتمثل بمعرفة كيفية ارتكاب الجريمة من خلال الحاسب الآلي[١]، وهناك مجموعة من الخصائص التي يتميز بها المجرم الإلكتروني والتي سنبينها فيما هو آت:

أولاً: المجرم الإلكتروني إنسان اجتماعي:

المجرم الإلكتروني فئة فريدة من نوعها في عالم الإجرام، كون هذا المجرم إنسان غير عنيف خلافاً للمجرمين التقليديين، فهو يتمتع بذكاء حاد مما يساعده على التكيف مع أفراد المجتمع دون قلق أو حيرة، فهو يرتكب جريمته بكل هدوء وتروي ثم يمحو آثارها بسهولة ويسر، فيكون في لحظة إنسان طبيعي، وفي لحظة أخرى مجرم محترف.

وكثير مما يدفع المجرم الإلكتروني إلى ارتكاب جريمته هو الانتقام من رب العمل الذي طرده من عمله، أو بدافع إظهار قدرته على اختراق الأجهزة والمواقع أو بدافع اللهو أو النصب أو بدافع مادي.[٢]

وكون المجرم الإلكتروني متكيف اجتماعياً، فهناك من يرى بأنه كلما زاد خطورته الإجرامية زادت قدرته على التكيف مع أفراد المجتمع.[٣]

وفي كثير من الأحيان يعود المجرم الإلكتروني لارتكاب جريمته مرة أخرى، فهو مجرم عائد للإجرام، وذلك رغبةً منه في التحدي لسد الثغرات التي أدت إلى تقديمه للمحكمة في المرة الأولى، وقد يؤدي عودته للإجرام تقديمه للمحاكمة مرة أخرى، كما أن المجرم الإلكتروني لا علاقة له بالجرائم التقليدية في كثير من الأحيان، فهو يرتكب الجرائم الإلكترونية وحدها دون غيرها.[٤]

---

[١] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٧١.

[٢] محمد علي العريان، المرجع السابق ، ص ٧٧ .

[٣] رامي متولي القاضي، المرجع السابق ، ص ٥٥.

[٤] عبد العال الديربي، محمد صادق إسماعيل، المرجع السابق، ص٥٨، ٥٩.

ثانياً: المجرم الإلكتروني مجرم ذكي ومتخصص:

من أهم ما يميز المجرم الإلكتروني أنه مجرم يتمتع بذكاء حاد، لا نجد هذا الذكاء في المجرمين التقليديين الذين في الغالب ما يتركوا أثراً ليدُل عليهم، بخلاف المجرم الإلكتروني فقد ألم بجميع الجوانب الفنية والتقنية لجريمته، مما يساعده في التخلص من أدلة إدانته في وقت سريع وبدون جهد يذكر، وهذا هو حال أغلب هؤلاء المجرمين، ولكن قد تكون الخبرة لدى المجرم الإلكتروني محدودة فقط في نطاق إلمامه بظروف الجريمة، فإذا كانت خبرة المجرم قليلة فالجرائم التي يرتكبها لا تتعدى الإتلاف أو نسخ البيانات والبرامج، أما إذا كان المجرم على مستوى عالي من الخبرة فقد يرتكب جريمة اختراق الأجهزة أو جريمة التجسس الإلكتروني أو يزرع الفيروسات أو يسرق الأموال[١].

وتبين من خلال الكثير من القضايا أن المجرمين الإلكترونيين هم مجرمين متخصصين، أي أنهم متخصصين في جرائم الإنترنت والكمبيوتر، كما أن هؤلاء المجرمين قد يتمادوا في جرائمهم إلى حد ارتكابهم الجرائم الخطيرة[٢].

فالمجرم الإلكتروني يتمتع بذكاء وقدرة ذهنية كبيرة في مجال التكنولوجيا والتي كسبها أما عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة من الممارسة العملية للحاسوب والإنترنت، فهو من خلال قدرته يستطيع اختراق ودخول أصعب المواقع والبرامج، والتي تكون في العادة محمية من قبل برامج مكافحة، أو عن طريق شيفرة معينة [٣].

ومما يؤكد على قدرة بعض الأشخاص الذهنية والعقلية هو اختراق الهاكرز لمواقع دولة الاحتلال ومواقعها الحكومية، ومواقع البورصة والجامعات والمصارف، والتي تسببت في إيقاف بعض المرافق الحيوية مثل التيار الكهربائي والاشارات الضوئية والبنوك، واستخدم هذا الاسلوب الحديث كنوع من أنواع المقاومة في وجه الاحتلال[٤].

---

[١] خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩م، ص١٣٤، ١٣٥.

[٢] خالد عياد الحلبي، المرجع السابق، ص٣٢، ٣٣.

[٣] نهلا عبد القادر المومني، المرجع السابق ، ص٧٧.

[٤] تقرير بعنوان " الحرب الإلكترونية تقلق إسرائيل" ، مشار إليه عبر الموقع الرسمي لقناة الجزيرة الفضائية، بتاريخ ٢٠١٣/٦/١٣، عبر الرابط التالي، http://www.aljazeera.net .

المبحث الثاني

صور الجريمة الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة، والتي اختلف الفقه في تصنيفها إلى عدة مسميات، ولم تراع أغلب التقسيمات خصائص الجرائم الإلكترونية وموضوعها، وإن أهم ما يميز الجرائم الإلكترونية عن غيرها هو أن هذه الجرائم تستهدف الكيانات المعنوية للحاسب الآلي، وترتكب بواسطة جهاز إلكتروني، أما ما يستهدف الكيانات المادية للحاسب الآلي فيندرج تحت صور الجرائم التقليدية[1].

واختلاف الفقه في تقسيم الجرائم الإلكترونية هو نتيجة ظهور جرائم جديدة من حين لأخر، حيث أن الجرائم الإلكترونية لا حصر لها، ولا يمكننا أن نجملها بكل أصنافها وأشكالها، فهي متغيرة ومتجددة، فكلما ظهرت وسيلة جديدة لاستخدام الحاسب الآلي والإنترنت ظهرت معه جريمة جديدة، وعليه سنجمل أشكال الجريمة الإلكترونية عبر المطالب الأتية:

المطلب الأول: صور الجرائم الإلكترونية الحديثة.

المطلب الثاني: صور الجرائم الإلكترونية في قانون العقوبات الفلسطيني.

المطلب الثالث: صور الجرائم الإلكترونية في قانون أنظمة المعلومات الأردني.

المطلب الأول

صور الجرائم الإلكترونية الحديثة

صنف الفقهاء والباحثين الجرائم الإلكترونية إلى عدة تقسيمات، فمنهم من صنفها إلى جرائم ترتكب بواسطة الحاسب الآلي، ومنهم من قسمها إلى جرائم ترتكب على المعلومات والبيانات الحاسوبية، ومنهم من قسمها نسبة إلى الهدف من الجريمة، وهناك الكثير من التقسيمات والتصنيفات[2]، وسنبين فيما يلي أبرز هذه التصنيفات عبر الفروع الأتية:

---

[1] يوسف المصري، المرجع السابق، ص٢٦.

[2] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص٣٦ .

الفرع الأول

جرائم نظم ووسائل وشبكات المعلومات

يُقصد بجرائم نظم ووسائل وشبكات المعلومات الجرائم التي تقع على المكونات المعنوية للحاسب الآلي من بيانات ومعلومات، مثل اختراق الحاسب الآلي أو الشبكة إما مجرداً، أو بهدف ارتكاب جريمة أخرى مثل تخريب المعطيات والأنظمة، أو خلق البرامج الضارة التي تنقل عبر الحاسب الآلي والشبكات وغيرها من الجرائم الاخرى[١].

وأكثر الجرائم التي تتعلق بالأنظمة والمعلومات جريمة الدخول غير المصرح به، ويُقصد بها وجود هجمات على معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المحتوى، أو تعطيل قدرة وكفاءة الأنظمة للقيام بأعمالها، وتتطلب هذه الجريمة وجود ركن مادي ومعنوي، ويتمثل الركن المادي بفعل الدخول الذي يطلق عليه الدخول المنطقي، وذلك بغرض فتح باب يؤدي إلى نظام الكمبيوتر بمكوناته المنطقية، أما الركن المعنوي فيتمثل بالقصد الجنائي كون هذه الجريمة من الجرائم العمدية فيجب توافر العلم والإرادة للجاني عند دخوله الغير مصرح به للنظام[٢].

ومن الجرائم الإلكترونية التي تستهدف أنظمة المعلومات نفسها، تلك التي يكون الغاية منها الدخول إلى أنظمة المعلومات والمواقع على شبكة الإنترنت بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفتـه أو انتحال شخصية مالكه، فكل هذه التصرفات تعد من الجرائم الإلكترونية التي تضر بالغير[٣].

---

[١] جمال محمد غيطاس، **أمن المعلومات والأمن القومي**، الطبعة الاولى، نهضة مصر للطباعة والنشر، القاهرة، ٢٠٠٧م، ص٢١٢.

[٢] خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، المرجع السابق، ص٢٤٢ وما بعدها.

[٣] راجع المادة رقم ٣ فقرة ب من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي: http://www.lob.gov.jo/ ا.

ومن أمثلة جرائم الاختراق التي تتعلق بأنظمة المعلومات والشبكات جرائم تدمير المواقع واختراق المواقع الرسمية واختراق الأجهزة الشخصية، واختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه[١]. وجميع هذه الجرائم تبدأ بانتهاك خصوصية الشخص وهذا سبباً كافياً لتجريمها، فضلاً عن إلحاق الضرر المادي والمعنوي بالمجني عليه[٢].

وفي إطار ذلك نص قانون العقوبات الفرنسي على أن جرائم نظم المعلومات هي " إدخال البيانات بطريقة الغش في نظام المعالجة الآلية أو محوها أو التعديل بطريقة الغش للمعطيات التي يحتويها يعاقب بالحبس لمدة ثلاث سنوات وبغرامه مقدارها ٣٠٠٠٠٠ فرانك "[٣].

ونص مشروع القانون العربي لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات على تعريف إتلاف البرامج بأنها: "تدمير البرامج الإلكترونية، سواء أكان كلياً أو جزئياً، أو إتلافها على نحو يجعلها غير صالحة للاستعمال"[٤].

وخلاصة القول أن الجرائم المتعلقة بأنظمة المعلومات أو الشبكات تنصب بدخول المواقع أو الأجهزة بطريقة غير مشروعة أو بطريقة مشروعة– كما لو تمت الجريمة من قبل موظف مختص– وإتلاف البيانات أو سرقتها أو نسخها أو تبديلها أو نشر فيروس يؤدي إلى ما ذكر، وقد تتعدد أسماء وأشكال الجرائم التي تستهدف أنظمة المعلومات ولكن كلها تدور في حلقة واحدة، فهذه الجرائم قد تتغير أساليب وطرق ارتكابها مع التطور التكنولوجي، ولكن في النهاية فإنه يعاقب على ارتكابها بنص قانوني واحد إلا إذا ظهرت جريمة جديدة لم تكن متوقعة ولم تغطيها النصوص القانونية.

ومن الفيروسات الشهيرة التي انتشرت عبر شبكة الإنترنت، وتسببت في خسائر كبيرة لمستخدمي الإنترنت فيروس حصان طروادة، حيث أطلق اسم حصاد طروادة على أحد الفيروسات التي هاجمت أجهزة أربع دول وهي انجلترا والنرويج والسويد والدنمارك، ومن نماذج فيروس حصان

---

[١] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص١١٦.

[٢] علي جبار الحسيناوي، المرجع السابق، ص١٠٤.

[٣] راجع المادة رقم ٣٢٣–٣ من قانون العقوبات الفرنسي، مشار إليه في كتاب جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، دار النهضة العربية، القاهرة، ٢٠٠٢م، ص٤٧.

[٤] راجع المادة رقم ١/١٥ من مشروع القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات، مشار إليه في الملحق الأول في كتاب عادل عزام الحيط، **جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية**، الطبعة الأولى، دار الثقافة، عمان، ٢٠١١م، ص٤٣٤.

طروادة التي ظهرت في النصف الأول من عام ١٩٩٠م، وكان هذا الفيروس يصل الأجهزة عن طريق البريد الإلكتروني ويهدد صاحب الجهاز بأن يرسل الفيروس إلى أجهزة أخرى وأن يتم إرسال مبلغ ٣٧٨ دولار، وإلا يتم محو البيانات والملفات المخزنة على الهارديسك، وبالفعل كان يتم محو بيانات الجهاز الذي أصيب بالفيروس[١].

الفرع الثاني

الجرائم الواقعة على الأموال والاتصالات

بيّن الواقع أن الجرائم الواقعة على الأموال والاتصالات من أخطر الجرائم الإلكترونية الحديثة، كون هذه الجرائم توقع خسائر مادية ضخمة، فالجرائم المالية التقليدية لا تتم إلا بالسطو على البنوك أو الشركات، وهي تحتاج إلى تخطيط مسبق ومجهود جماعي، بخلاف الجرائم المالية الإلكترونية فهي تتم بطرق سهلة تحتاج فقط إلى شخص متخصص في برامج الحاسب الآلي، وهي لا تحتاج إلى مجهود جماعي بل يكفي شخص أو أثنين لارتكاب الجريمة، كما أن الجرائم الإلكترونية توقع خسائر أكبر بكثير من الجرائم التقليدية، وكذلك الأمر بالنسبة للجرائم المتعلقة بالاتصالات.

ومن الجرائم الواقعة على الأموال جرائم سرقة الأموال والبيانات والبرامج والخدمات الإلكترونية، وتتطلب هذه الجرائم توافر الركن المادي المتمثل في فعل الاختلاس لمال منقول مملوك للغير، وكذلك لا بد من توافر الركن المعنوي المتمثل في القصد الجنائي الخاص للجاني في نيته لتملك الأموال أو البيانات المسروقة[٢].

ومن أمثلة الجرائم المالية الإلكترونية السحب النقدي عن طريق بطاقة الصراف الآلي، فمن الممكن أن يقوم شخص بتزوير بطاقة صراف آلي والسحب عليه من خلال أحد البنوك، وتعد هذه الحالة من حالات السرقة والتي تتم عن طريق وسيلة إلكترونية وهي بطاقة الصراف الآلي[٣].

---

[١] محمد علي العريان، المرجع السابق، ص ١٠٩,١١٠ .

[٢] خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، المرجع السابق، ص٢٩٧.

[٣] هدى حامد قشقوش، **جرائم الحاسب الآلي في التشريع المقارن**، دار النهضة العربية، القاهرة، ص١١٤، ١١٥.

وفي فرنسا قضت محكمة الجنح حكماً يتعلق بموظف قام بنسخ برامج معلوماتية تتعلق بشركة بيجو على قرص إلكتروني، ومن ثم استخدم هذه البرامج لدى شركة أخرى عمل لديها بعد أن ترك عمله في شركة بيجو، وأدانته المحكمة بالسرقة على أساس سرقة البرامج الإلكترونية[١].

ومن الجرائم المالية الإلكترونية لعب القمار عبر الإنترنت، حيث يوجد أكثر من ألف موقع للقمار على شبكة الإنترنت، والذي يسمح لمرتاديه بلعب جميع أنواع القمار الموجودة في أندية القمار، و ينفق الأمريكيين ما يقارب مليار دولار سنوياً للعب القمار عبر الإنترنت[٢].

وفي التشريع الإماراتي نص المشرع في المادة رقم ١١ من القانون الاتحادي رقم٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات في الإمارات على أن "كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في الوصول من دون وجه حق، إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية يعاقب بالحبس والغرامة، فإن قصد من ذلك استخدامها في الحصول على أموال الغير، أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين، وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن ثلاثين ألف درهم أو إحدى هاتين العقوبتين إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال الغير"[٣].

ومن أخطر الجرائم الإلكترونية المالية جريمة غسل الأموال عبر الإنترنت، حيث بدأت عملية غسل الأموال من تجارة المخدرات والمقامرة والجنس وغيرها من الجرائم، ومن المجالات التي يتم من خلالها غسل الأموال عبر الإنترنت المضاربة على الأسهم في البورصة والتجارة في العقارات والأراضي والشقق ومجال المزايدات والمناقصات الحكومية وشراء التحف الثمينة والهدايا، والمجالات في هذا الشأن لا حصر لها[٤].

---

[١] علي عبد القادر القهوجي، **الحماية الجنائية لبرامج الحاسب**، دار الجامعة الجديدة للنشر، الاسكندرية، ١٩٩٧م، ص٦٣.

[٢] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص١١٦.

[٣] المادة رقم ١١ من القانون الاتحادي رقم٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات في الإمارات، مشار إليه في كتاب علي عدنان الفيل، **النظام القانوني للمعاملات الإلكترونية في الوطن العربي**، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١م، ص٣٠٥.

[٤] يوسف حسن يوسف، **جريمة غسل الأموال بالطرق التقليدية عبر شبكات الإنترنت وبنوك الويب**، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١م، ص٣٥.

وتنصب الجريمة الإلكترونية على الاتصالات سواء الخلوية أو خطوط الهاتف والإنترنت، فالمجرم الإلكتروني قد يقوم بتزوير بطاقات الهاتف أو قد يستخرج أرقام كروت الشحن التي لم تستخدم من خلال حسابات ومواقع الشركات الخلوية، وقد يصل إلى الحصول على خط انترنت دون علم الشركة، ففي الإمارات أدين مهندس فني كان يعمل في إحدى شركات الحاسب الآلي، حيث أمد شخص بالرقم السري للإنترنت الخاص بهذه الشركة والذي استخدم الإنترنت لمدة شهرين وأدانته المحكمة على هذا الفعل[١].

الفرع الثالث

جرائم الاعتداء على الأشخاص والجرائم الجنسية

إن جرائم الاعتداء على الأشخاص وحياتهم الخاصة من أكثر الجرائم الإلكترونية انتشاراً، وتتنوع الجرائم التي تمس بالأشخاص، فلها عدة صور وأشكال، ولكن أكثرها يدور حول الذم والتهديد والتشهير عبر الإنترنت، مثل أن يقوم شخص بنشر صور فاضحة لشخص آخر بهدف تشويه سمعته والإساءة له، ولكن قد يتخذ الاعتداء على الأشخاص صور أخطر من ذلك قد تؤدي إلى القتل، فمثلاً عند قيام شخص بالعبث بالنظام الإلكتروني لمستشفى حديث فقد يؤدي ذلك إلى وفاة أحد المرضى.

وتهدف الجرائم التي تمس بالأشخاص الحط من مكانتهم الاجتماعية والإساءة المباشرة أو غير المباشرة لهم، ويتمثل الركن المادي في هذه الجريمة بتصرف مادي يصدر عن الفاعل الأمر الذي يتطلب مشاهدة أو إدراك هذا التصرف من الغير وهو ما يشار إليه بمصطلح العلانية[٢].

وإن أكثر الجرائم التي تنتشر عبر الإنترنت هي جرائم الذم والتهديد والتشهير، حيث يعد الإنترنت أفضل بيئة لمثل هذه الجرائم نظراً لسرعة تنفيذها، والبعد المكاني بين الجاني والمجني عليه، ويفضل الكثير من المجرمين ارتكاب هذه الجريمة عبر الإنترنت لصعوبة الكشف عن هويتهم وإيقاعهم تحت طائلة المسئولية، وترتكب مثل هذه الجرائم للطعن في شرف الغير أو بدافع

---

[١] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٤٧.

[٢] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٢٨٥.

الانتقام أو لدفع الناس للحقد وبغض شخص معين، كما أن هذه الجرائم ترتكب على عدة أشكال كتابية أو سمعية أو مرئية[١].

ومن صور جرائم الاعتداء على الأشخاص، جريمة الاعتداء على حرمة الحياة الخاصة، فللحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، و مثل ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الخاصة بشخص ما أو تسجيل مكالمات أو فيديو أو مراقبته[٢].

وكفل القانون الأساسي الفلسطيني حماية الحياة الخاصة، حيث نص في المادة رقم٣٢ على أن: " كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع عليه الضرر"[٣].

ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسلوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، ويقوم بنشرها عبر الإنترنت، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإرادة على ذلك[٤].

والذي نراه أن المواقع الجنسية التي تنتشر على الإنترنت من أكثر المواقع زيارة من قبل مستخدمي الإنترنت والحاسب الآلي، وذلك يترك آثار سلبية على المجتمع، فقد أكدت الدراسات أن هناك ارتباط بين زيادة الجرائم الجنسية ومشاهدة الأفلام الإباحية والمقاطع الشاذة عبر الإنترنت، فكل الأعمال الإباحية التي تنشر عبر الإنترنت تؤدي إلى زيادة جرائم الاغتصاب والتحرش والزنا وغيرها من الجرائم الجنسية.

ومن أخطر الجرائم الجنسية الإلكترونية الاستغلال الجنسي للأطفال، فهناك العديد من المواقع التي تنشر صور للأطفال في أوضاع جنسية مخلة، أو تبث أفلام إباحية لأطفال، وهناك

---

[١] عادل عزام الحيط، المرجع السابق، ص١٩٨، ١٩٩.

[٢] خالد ممدوح إبراهيم، **حوكمة الإنترنت**، المرجع السابق، ص ٤١٠، ٤١١.

[٣] راجع المادة رقم ٣٢ من القانون الأساسي الفلسطيني المعدل لسنة ٢٠٠٥م.

[٤] خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، المرجع السابق، ص٢٩٧.

مواقع أخرى تجذب الأطفال لإيقاعهم في شبكات الدعارة والاستغلال الجنسي، وهذه الأفلام المخلة تؤدي إلى جذب المنحرفين ليوقعوا بالأطفال في الفاحشة من خلال محادثتهم عبر الدردشة وغرف المحادثات أو عبر مواقع التواصل الاجتماعي[١].

كما أن ارتياد هذه المواقع ومشاهدة الأفلام الإباحية يعد من الأمور التي نهى عنها الله عز وجل في أكثر من موضع، قال تعالى: " **قل للمؤمنين يغضوا من أبصارهم ويحفظوا فروجهم ذلك أزكى لهم إن الله خبير بما يصنعون** "[٢].

كما أن الإحصائيات أفادت بأن نسبة زوار المواقع الإباحية في الأسبوع الواحد حوالي ٤.٧مليون زائر في إحصائية سابقة فما بالك اليوم مع انتشار الإنترنت في كل بيت، كما ظهرت مع هذه المواقع ظاهرة إدمان مشاهدة الأفلام الإباحية خاصة للأشخاص الذين تابعوا المواقع الإباحية في سن مبكر، وكذلك انتشرت الرذيلة بين الذكور والعنف الجنسي بين الأزواج بسبب هذه المواقع التي تبث الأفلام الإباحية ليل نهار[٣].

وفي قطاع غزة قامت الحكومة الفلسطينية بحجب جميع المواقع الإباحية، حيث أصدر وزير الاتصالات وتكنولوجيا المعلومات قرار وزاري رقم ٢٠١٢/٣٣ والذي تضمن فيه الأمر بحجب كافة المواقع الإلكترونية المخلة بالآداب، مع إلزام مزودي الخدمة –الإنترنت– بتطبيق مواد هذا القرار، الأمر الذي يعمل على حماية المجتمع ومستخدمي الإنترنت من الدخول في مثل هذه المواقع المشبوهة[٤].

---

[١] محمد أمين الشوابكة، المرجع السابق، ص ١٠٥، ١٠٦ .

[٢] سورة النور الآية ٣٠ .

[٣] أمير فرج يوسف، **الجرائم المعلوماتية على شبكة الإنترنت**، دار المطبوعات الجامعية، الاسكندرية، ٢٠٠٨م، ص٦٢.

[٤] انظر القرار الوزاري رقم ٢٠١٢/٣٣ والصادر عن وزير الاتصالات وتكنولوجيا المعلومات اسامة العيساوي بتاريخ ٢٠١٢/٨/٢٢م، مشار إليه في الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات عبر الرابط التالي: http://www.mtit.gov.ps/

الفرع الرابع

جرائم الأمن العام وتجارة الرقيق والمخدرات

تعد حرب المعلومات من الحروب الجديدة التي ظهرت بظهور الحاسب الآلي والإنترنت، فتتنافس اليوم الدول العظمى فيما يعرف بالحرب الإلكترونية بشأن اختراق كل دولة أجهزة الدولة الأخرى للحصول على المعلومات التي تتعلق بالشؤون العسكرية والأمنية والاقتصادية، وكما نعلم أن الإنترنت قد خرج من رحم المؤسسة العسكرية، وظهر معه المحتوى المعلوماتي الرقمي العسكري والذي يتعلق بكل صغيرة وكبيرة داخل المؤسسة العسكرية والتي هي اليوم الهدف الأساسي في الحرب الإلكترونية[١]، ومن خلالها ظهرت صور التجسس الإلكتروني والذي يهدف إلى التجسس على الدول للحصول على المعلومات التي تتعلق بالأسلحة الجديدة والعملاء وغيرها من المعلومات الأمنية والعسكرية.

ومن الجرائم التي تهدد الأمن العام، جريمة التجسس الإلكتروني والذي يتخذ الركن المادي فيها صورة سلوك الجاني في استعمال نظام إلكتروني معين قادر من خلاله الدخول إلى حافظة السر الإلكتروني، وتمكنه من الاطلاع عليها أو نسخها، أما الركن المعنوي فيتمثل بالقصد العام وكذلك تتطلب هذه الجريمة وجود قصد خاص يرغب من خلالها الفاعل إيقاع ضرر بالدولة أو بالنظام العام فيها، والإساءة لها[٢].

ومن الجرائم التي تهدد الأمن العام، إنشاء مواقع على الإنترنت تعمل على نشر الفتنة والتفرقة بين أفراد المجتمع، من خلال بث الأفكار المكتوبة أو المسموعة أو المرئية، والتي تفرق بين أفراد المجتمع من الناحية السياسية أو العقائدية أو الدينية، وكذلك إنشاء المواقع التي تنشر الأفكار المعادية للدولة وتنظم الجماعات المأجورة و تروج لأفكارها وتدعو للانضمام معها وهي في الحقيقة لا تخدم إلا العدو[٣].

وأثبتت التجربة الفلسطينية أن الإنترنت ومواقع التواصل الاجتماعي هي أفضل بيئة للإسقاط في مستنقع العمالة مع العدو الإسرائيلي، فقد استخدم الاحتلال الإنترنت لإسقاط الشباب من خلال تجنيده لفتيات يعملن في الموساد الإسرائيلي، ليتواصلن مع الشباب في قطاع غزة عبر

---

[١] جمال محمد غيطاس، المرجع السابق، ص٦٣ وما بعدها.

[٢] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٢٦٥.

[٣] محمد محمد الألفي، المرجع السابق، ص ٩٤ .

الشات أو مواقع التواصل الاجتماعي لإغرائهم بالمال والجنس وفي النهاية يسقطن الشباب للعمالة مع الاحتلال، وجمع المعلومات التي تتعلق بأعمال المقاومة الفلسطينية[١]، ولذلك يجب العمل على نشر التوعية الأمنية والدينية بين أفراد المجتمع خاصة فئة الشباب لتحذيرهم من خطر الإنترنت، وعدم التواصل مع الأشخاص المشبوهين، والعمل على حماية الجبهة الداخلية في المجتمع الفلسطيني.

وكشف الباحثون عن استخدام بعض عصابات الإنترنت في تجارة الرقيق الأبيض، من خلال عقد صفقات لبيع فتيات من أربعين دولة نامية ومن أوروبا الشرقية في دول الغرب، لاستخدام هؤلاء الفتيات في المتعة والجنس، ويتم ذلك بإرسال كتالوجات متضمنة صور الفتيات ومواصفاتهن وأسعارهن، وقد يتم عقد لقاءات بين الفتيات والأشخاص الراغبين بالشراء، وتربح هذه العصابات الملايين من الدولارات التي يتم استخدامها فيما بعد في عمليات غسل الأموال[٢].

وفي إطار ذلك عُقد المؤتمر الدولي لمكافحة استغلال الأطفال في الجنس عبر الإنترنت، في الفترة من ٢٩ سبتمبر – الأول من أكتوبر ١٩٩٩م في مدينة فينا بالنمسا، وأكد المؤتمر على ضرورة التعاون الدولي لمكافحة هذا النوع من الجرائم، والعمل على ضبط شبكات الإنترنت من موردي الخدمة، مع توفير خطوط اتصال للإبلاغ عن مثل هذه الحالات[٣].

وفي التشريع السعودي نص المشرع في المادة رقم ٦ على أنه: "يعاقب بالسجن مدة لا تزيد عن خمس سنوات وبغرامة لا تزيد عن ثلاث ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: ..٢- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس البشري، أو تسهيل التعامل به"[٤].

---

[١] ندوة أمنية بعنوان "وسائل الإسقاط الامني وطرق مواجهتها"، عقدتها هيئة التوجيه السياسي والمعنوي في وزارة الداخلية بالتعاون مع وزارة التربية والتعليم، واستهدفت هذه الندوة طلاب الثانوية في محافظة خانيونس بتاريخ ٢٠١٣/٤/٢١م، مشار إليها في الموقع الرسمي لوزارة الداخلية،غزة، عبر الرابط التالي:/http://www.moi.gov.ps

[٢] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٣٣.

[٣] عبد الفتاح بيومي حجازي، **الجريمة في عصر العولمة**، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٠م، ص١٩٣.

[٤] راجع المادة رقم ٢/٦ من نظام مكافحة جرائم المعلوماتية السعودي رقم م/١٧ ، لسنة ١٤٢٨هـ مشار إليه في الموقع الرسمي لمجلس الوزراء السعودي عبر الرابط التالي: http://www.boe.gov.sa/ .

وفي العصر الحديث ظهرت طرق لم تكن في الحسبان تدفع الشخص لإدمان المخدرات، فقد ظهر على الإنترنت مواقع تختص للتحفيز على تعاطي المخدرات والترغيب إليها، ولم يصل الأمر إلى ذلك فقط بل تعدى إلى نشر طرق زرع المخدرات بكافة أنواعها، وكيفية تحضيرها بأبسط الطرق[١].

وفي التشريع السوداني نص المشرع في المادة رقم ٢١ على أنه: " كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية أو ما في حكمها أو يسهل التعامل فيها، يعاقب بالسجن مدة لا تتجاوز عشرين سنة أو بالغرامة أو بالعقوبتين معاً"[٢].

المطلب الثاني

صور الجرائم الإلكترونية في قانون العقوبات الفلسطيني

تعد الجرائم الإلكترونية من الجرائم المستحدثة على الساحة الفلسطينية، والتي لم يكن قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ يعاقب عليها، إلى أن عدل المشرع الفلسطيني واستحدث في مواده الجرائم الإلكترونية، وعليه سنتناول بالشرح الجرائم الإلكترونية في قانون العقوبات، ومشروع قانون العقوبات، وذلك عبر الفروع التالية:

الفرع الأول

قانون العقوبات رقم ٧٤ لسنة ١٩٣٦

لم يكن المشرع الفلسطيني يعاقب على الجرائم الإلكترونية، وكانت هذه الإشكالية واضحة في قانون العقوبات رقم ٧٤ لسنة ١٩٣٦، إلى أن أضيفت المادة رقم ٢٦٢ مكرر إلى قانون العقوبات، وتم نشرها في الوقائع الفلسطينية في العدد الخامس والسبعون بتاريخ ٢٠٠٩/٦/٢٥م، ولكن هذه المادة لم تتضمن جميع أشكال الجرائم الإلكترونية التي ذكرناها في المطلب السابق،

---

[١] يوسف المصري، المرجع السابق، ص٨٥.

[٢] راجع المادة رقم ٢١ من قانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧م، مشار إليه في الملحق رقم (٤) في كتاب محمد علي العريان، المرجع السابق ، ص ٣١٣ .

حيث جعل المشرع الفلسطيني كافة أشكال الجرائم الإلكترونية يعاقب عليها بهذه المادة، كما اعتبرت هذه الجرائم جنحة دون تصنيفها حسب درجة بعضها .

أولاً: الاعتداء على حرمة الحياة الخاصة:

وفرت البيئة الإلكترونية حياة خاصة للأفراد، وقد تتعرض هذه الحياة لاعتداء من قبل آخرين، ويظهر الركن المادي في هذه الجريمة من خلال سلوك الجاني بتمام ولوجه إلى النظام الإلكتروني وينتهي بتمام فعله، أما الركن المعنوي فيتمثل في قصد الجاني والذي قد يتعدد فقد يكون قصده الإطلاع المجرد أو الإطلاع بقصد الإفشاء أو الاطلاع بقصد التهديد والابتزاز[١].

وفي المادة ٢٦٢ مكرر البند (أ، ب، د/١) خصصها المشرع لجرائم الاعتداء على حرمة الحياة الخاصة، فكان الأول أ/١ لجريمة استراق السمع أو تسجيل الأحاديث الخاصة بين الأفراد، ولم يحدد المشرع في هذه الجريمة نوعاً معيناً من الأجهزة، فأي جهاز يستخدم في عملية التصنت يعتبر أنه أداة الجريمة، ونص المشرع على أن "كل من استرق السمع أو سجل أو نسخ أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه حديثاً خاصاً جرى في أحد الأماكن، أو عن طريق الهاتف بدون رضاء صاحب الشأن"[٢].

ويتمثل الركن المادي في الجريمة السابقة في قيام الجاني باستراق السمع أو التصنت على المحادثات الشخصية، فإذا توافرت للفعل صفة الخصوصية والسرية، وقصد الجاني بعلمه وإرادته ارتكاب فعل التصنت بدون رضا المجني عليه توافرت أركان الجريمة التامة[٣].

أما البند ب/١ كانت لجريمة التقاط أو نسخ أو إرسال صور لشخص في مكان خاص، وهذه الجريمة كثير ما تحدث بأن يتم نشر صور لفتيات على مواقع التواصل الاجتماعي بهدف التشهير بهن، ولكن أشترط المشرع أن تتم هذه الجريمة بدون رضا المتضرر، فنص المشرع في ذلك على أن "كل من التقط أو نقل أو نسخ أو أرسل بأي جهاز من الأجهزة صورة شخص في مكان خاص، فإذا صدرت الأفعال المذكورة أثناء اجتماع على مسمع ومرأى الأشخاص الذين

---

[١] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٢٢٨وما بعدها.

[٢] راجع المادة رقم (أ/١) ٢٦٢ مكرر من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٣] بلال أمين زين الدين، **جرائم نظم المعالجة الآلية للبيانات**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨م، ص٢٨٨، ٢٨٩.

يهمهم الأمر الحاضرين في ذلك الاجتماع فإن رضاءهم يكون مفترضاً ما لم يبدوا اعتراضهم على الفعل"[١]، وكان البند د/١ تأكيداً لما جاء فيما سبق على تجريم كافة أشكال الاعتداء على حرمة الحياة الخاصة حيث نص على أنه: " أذاع أو نشر أو طبع أو نسخ أو استعمل ولو في غير علانية، تسجيلاً أو صورة أو مستنداً متحصلاً عليه بإحدى الطرق المبينة في البنود (أ،ب،ج) من هذه المادة وكان ذلك بدون رضاء صاحب الشأن، يعتبر أنه اعتدى على حرمة الحياة الخاصة لأحد الأشخاص.."[٢].

ويقصد بالحياة الخاصة كل ما يحتفظ به الإنسان من أسرار بعيداً عن الأخرين، وهذه الأسرار تتعلق به أو بعائلته، وكان قصد المشرع من هذا النص هو صون حياة الإنسان وحرمتها، وحمايتها من تدخل وعبث الآخرين[٣].

ثانياً: الجرائم الجنسية وجرائم الذم:

تشمل الجرائم الجنسية جرائم ارتياد المواقع الإباحية للشراء منها أو للاشتراك بها، أو للانضمام للقوائم الإباحية لتبادل الأفلام والصور منها، وكل ما يندرج تحت أعمال الدعارة والاستغلال الجنسي للأطفال[٤].

ونص البند ج/١ فشمل الجرائم الجنسية وجريمة الذم، حيث ذكر المشرع الإنترنت وأجهزة الخطوط الهاتفية والوسائل التكنولوجية الأخرى من الأدوات التي تستعمل في هذه الجرائم مثل نشر وطباعة وعرض المواد الإباحية، أو ذم شخص ما عبر الإنترنت أو إرسال رسائل بها عبارات ذم وتحقير عبر الهاتف المحمول، وأشترط المشرع في هذه الجرائم أن يكون استخدام الجهاز في الجريمة عمداً حيث نص على أن "كل من أساء عمداً استعمال أجهزة الخطوط الهاتفية أو الإنترنت أو أية وسيلة تكنولوجية أخرى بأن روج أو نقل أو طبع أو نسخ أية مواد إباحية، أو أزعج الغير، أووجه إليهم ألفاظ بذيئة أو مخلة بالحياء أو تضمن حديثه معهم تحريضاً على الفسق والفجور"[٥].

---

[١] راجع المادة رقم (ب/١) ٢٦٢ مكرر من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٢] راجع المادة رقم (د/١) ٢٦٢ مكرر من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٣] عبد الفتاح بيومي حجازي، **الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة**، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١م، ص٢٦٦.

[٤] علي جبار الحسيناوي، المرجع السابق، ص١٠٤.

[٥] راجع المادة رقم (ج/١) ٢٦٢ مكرر من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

ولقد أجرى الباحث إحصائية حول الجرائم الإلكترونية التي سجلت ضمن دائرة اختصاص إحدى مراكز الشرطة، وقد تبين بأن عدد الجرائم التي ارتكبت عام ٢٠١١م (١٢) جريمة من ضمنها (١٠) جرائم ارتكبت عبر الهاتف المحمول منها خمسة معاكسات، وأربعة ذم وتهديد، وواحدة تغشيش لطلاب الثانوية العامة عبر الجوال.

وفي إطار ذلك تتابع وزارة الاتصالات وتكنولوجيا المعلومات قرار حظر المواقع المخلة بالآداب، حيث قامت الوزارة بحظر هذه المواقع قبل عام وهي تعمل في الوقت الحالي على متابعة تطبيق القرار، والذي يهدف إلى حماية النسيج المجتمعي والأطفال والمراهقين، خاصة حمايتهم من الاحتلال الإسرائيلي والذي يحاول استدراجهم إلى مستنقع الرذيلة[١].

ثالثاً: جرائم أنظمة المعلومات:

أما الجريمة الأخيرة التي نص عليها المشرع الفلسطيني في هذه المادة فهي جرائم أنظمة المعلومات، وما يتعلق بها من اختراق الأجهزة وإتلاف المعلومات أو محوها أو تعديلها، حيث نص المشرع الفلسطيني على أن "كل من اقتحم نظاماً لمعلومات حاسوب خاص بالغير أو بقي فيه دون وجه مشروع، .. وإذا نتج عن ذلك تعطيل تشغيل النظام أو محو المعلومات التي يحتوي عليها أو تعديلها"[٢].

وتفترض جريمة الدخول غير المشروع أن يكون النظام المخترق غير متاح للجمهور، أما إذا كان النظام متاح للجمهور فلا يمكننا القول بأن هناك جريمة، فيجب أن يكون النظام الذي تم اختراقه غير متاح للجمهور ولا يمكن الدخول فيه إلا لأشخاص معينين[٣].

ويتمثل الركن المادي في جريمة الإتلاف بالسلوك الذي يقع من الفاعل سواء إيجابي أو سلبي، ينتج عنه ضرر يلحق بالغير ، أما الركن المعنوي فيمثل القصد الجنائي الذي يتكون من

---

[١] تقرير بعنوان "قرار وزارة الاتصالات بفلترة المواقع المخلة بالآداب ينجح في حماية نسيج المجتمع" ، صحيف الرأي، المكتب الاعلامي الحكومي، وزارة الأعلام، غزة، العدد (٢٤٩)، ص٤، ٢٠١٣/٨/٢٩م.

[٢] راجع المادة رقم ٣/ ٢٦٢ مكرر من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٣] عبد الفتاح بيومي حجازي، **التجارة الإلكترونية**، الكتاب الثاني، دار الكتب القانونية، القاهرة، ٢٠٠٧م، ص٢٨.

عنصري العلم والإرادة، العلم بالفعل المرتكب ومحل الاعتداء وإرادة هذا الفعل والنتيجة المترتبة عنه[١].

وفي فرنسا قضت محكمة جنح باريس متهم بجريمة الدخول بدون وجه حق إلى نظام المعالجة الآلية للمعلومات، حيث قام المتهم بتقديم نفسه بأنه مندوب عن المجموعة الفيدرالية FBI لكي يحصل على توريد خدمات تليفونية من شركات الخدمة مقابل مبلغ ٢٥٠٠٠٠ دولار[٢].

وخلاصة القول أن ما ذكرناه هو مجموعة الجرائم التي يعاقب عليها المشرع الفلسطيني في الوقت الحالي، أما الجرائم الأخرى مثل الجرائم المالية عبر الإنترنت والمخدرات وغيرها، فلم ينص عليها قانون العقوبات، وهنا تثور بعض المشكلات التي تتعلق بفلتان بعض المجرمين من الحساب والعقاب، بحجة أن فعلتهم لم ينص عليها القانون، وهناك مشروع قانون العقوبات الذي توسع بعض الشيء في جمع الجرائم الإلكترونية، والتي سنبينها في الفرع التالي.

الفرع الثاني

مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠

لم يرَّ مشروع قانون العقوبات الفلسطيني النور بعد، فما زال بين المداولات والمناقشات في أروقة المجلس التشريعي، وقد تضمن هذا المشروع باباً خاصاً وهو الباب السابع ليعالج مسألة الجرائم الإلكترونية، ولكن هل تضمن هذا الباب كافة أشكال الجرائم الإلكترونية؟، هذا ما سنوضحه فيما هو آت:

أولاً: جرائم التصنت والاعتراض:

تحدثت المشرع في المادة رقم ٥٤٦ عن جريمة التصنت والاعتراض الغير مشروع، فتعتبر هذه الجريمة من جرائم الاعتداء على حرمة الحياة الخاصة، ومثالها تسجيل المكالمات الهاتفية، أو

---

[١] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص١٢٠ بعدها.

[٢] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٦٢.

المحادثات الإلكترونية، فكل ما من شأنه التصنت على الآخرين فهو عمل غير مشروع ويجرمه القانون[١].

وكان هدف المشرع من تجريم التصنت والاعتراض هو حماية الحق في حرية الاتصال واحترام نقل البيانات دون تدخل من أحد، ويتمثل الركن المادي في هذه الجريمة بقيام الجاني باستراق السمع أو اعتراض المعلومات باستعمال أي من الأجهزة المخصصة لذلك أما الركن المعنوي فيتمثل بقصد الجاني بعلمه وإرادته بارتكاب فعل التصنت أو الاعتراض[٢].

ثانياً: جرائم أنظمة المعلومات ونشر الفيروسات وإساءة استخدام الاجهزة:

يعرف الفيروس بأنه: " هو عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جداً وتصيب النظام المعلوماتي بشلل النظام"[٣]، كما أن الفيروسات يمكن أن تقوم بنسخ نفسها من جهاز لآخر وتتكاثر بأعداد كبيرة[٤].

نص المشرع الفلسطيني في المواد رقم ٥٤٥، ٥٤٧، ٥٤٨، ٥٤٩ على الجرائم التي تستهدف أنظمة المعلومات والبرامج ونظم التشغيل، من حيث اقتحام الأنظمة أو تعطيلها، أو محو أو تخريب أو حجب أو نسخ أو إتلاف البيانات، وكذلك نشر الفيروسات التي تتسبب فيما ذكر، أو إساءة استخدام الأجهزة الإلكترونية بشكل عام[٥].

---

[١] نصت المادة رقم ٥٤٦ من مشروع قانون العقوبات لسنة ٢٠١٠م على أنه: " كل من تنصت أو اعترض بدون حق باستعمال سبل تقنية، على أية معلومات غير معروضة للعموم، من وإلى أو داخل نظام حاسوب بما في ذلك الإصدارات الإلكترومغناطيسية لنظام حاسوب يحتوي على معلومات محوسبه، يعاقب بالحبس مدة لا تزيد على ستة أشهر، وبغرامة لا تجاوز مائتي دينار، أو بإحدى هاتين العقوبتين".

[٢] بلال أمين زين الدين، المرجع السابق، ص٢٨٨، ٢٨٩.

[٣] محمد علي العريان ، المرجع السابق، ص١٠٢.

[٤] يوسف المصري، المرجع السابق، ص٧٦.

[٥] نصت المادة رقم ٥٤٥ من مشروع قانون العقوبات لسنة ٢٠١٠م على أنه: " ١-كل من اقتحم نظاماً لمعلومات حاسوب خاص بالغير أو بقي فيه دون وجه مشروع، يعاقب بالحبس مدة لا تزيد على سنة، وبغرامة لا تجاوز ألف دينار أو بإحدى هاتين العقوبتين. ٢- وإذا نتج عن ذلك تعطيل تشغيل النظام أو محو المعلومات التي يحتوي عليها أو تعديلها، تكون العقوبة الحبس، وبغرامة لا تجاوز ثلاثة آلاف دينار، أو بإحدى هاتين العقوبتين."
ونصت المادة رقم ٥٤٧ على أنه: " كل من قام بتخريب أو محو أو إفساد أو تغيير أو حجب معلومات حاسب آلي خاص بالغير مما أدى إلى إلحاق ضرر جسيم بهم، يعاقب بالحبس، وبغرامة لا تجاوز ثلاثة آلاف دينار، أو بإحدى هاتين العقوبتين".=

ثالثاً: جرائم التزوير المعلوماتي:

أما المواد رقم ٥٥٠، ٥٥١، ٥٥٢ فنصت على جرائم التزوير المعلوماتية، واستغلال الحاسب الآلي في عملية التزوير المعلوماتي، أو تزوير أي نظام إلكتروني بشكل غير مشروع[١].

ويعرف التزوير المعلوماتي بأنه: " تغيير الحقيقة بقصد الغش في محرر تغييراً واقعاً على شيء مما عد هذا المحرر لإثباته ومن شأنه أن يسبب ضرر"، ويتمثل الركن المادي لهذه الجريمة من خلال النشاط الذي يمارسه الجاني لتغيير الحقيقة، ويستخدم وسائل إلكترونية في ذلك محدث ضرر يلحق بالغير، أما الركن المعنوي فيتكون من القصد العام بعلم الجاني بالأفعال التي ارتكبها واتجاه إرادته لارتكابها، أما القصد الخاص فهو أن يتم تغيير الحقيقة بقصد التزوير[٢]، والذي دفع

=ونصت المادة رقم ٥٤٨ على أنه: "١- كل من أعاق بشكل خطير عمل أنظمة حاسوب من خلال إدخال أو نقل أو تغيير أو حجب معلومات حاسوب دون وجه مشروع، يعاقب بالحبس، وبغرامة لا تجاوز ألفي دينار، أو بإحدى هاتين العقوبتين. ٢- كل من سجل أو زرع عمداً فيروساً على الأقراص أو الأسطوانات الخاصة بحساب مملوك للغير بقصد تدمير برامجه أو بياناته المسجلة أو المخزنة في داخله يعاقب بالحبس وبغرامة لا تجاوز ألفي دينار، أو بإحدى هاتين العقوبتين".

ونصت المادة رقم ٥٤٧ على أنه: " كل من قام بإنتاج أو بيع أو شراء بهدف الاستعمال أو استيراد أو توزيع أو إيجاد ما يلي:١- جهاز يحتوي على برامج حاسوب مصمم أو معُد للقيام بجريمة أو أكثر مما ذكر في المواد السابقة من هذا الفصل. ٢- استعمل بوجه غير مشروع كلمة سر أو رمز مرور أو معلومات مشابهة بقصد المرور إلى نظام حاسوب أو إلى جزء منه للقيام بجريمة أو أكثر مما ذكر في المواد السابقة من هذا الفصل، يعاقب بالحبس مدة لا تزيد على سنة، وبغرامة لا تجاوز ألف دينار، أو بإحدى هاتين العقوبتين. ٣- يستثنى من تطبيق أحكام هذه المادة إنتاج أية أجهزة أو برمجيات للقيام بحماية أو بفحص أي شيء مما تم ذكره في الفقرتين (١ ، ٢) أعلاه".

[١] نصت المادة رقم ٥٥٠ من مشروع قانون العقوبات لسنة ٢٠١٠م على أنه: " كل من قام بإدخال أو تغيير أو محو أو حجب معلومات حاسوب مما قد يؤدي إلى نشوء معلومات غير موثوق بها بهدف ترويج استعمالها أو تطبيقها على اعتبار أنها معلومات موثوق بها، يعاقب بالحبس مدة لا تزيد على سنة، وبغرامة لا تجاوز ألفي دينار، أو بإحدى هاتين العقوبتين".

ونصت المادة رقم ٥٥١ على أنه: " كل من زور وثائق حاسوب أو استعمل وثائق مزورة مع علمه بتزويرها للإضرار بالغير، يعاقب بالحبس، وبغرامة لا تجاوز ثلاثة آلاف دينار، أو بإحدى هاتين العقوبتين".

ونصت المادة رقم ٥٥٢ على أنه: " كل من عرقل أو أفسد عمداً تشغيل نظام حاسوب خاص بالغير أو أدخل أو عدّل بطريق الغش معلومات تخالف المعلومات التي يحتوي عليها، يعاقب بالحبس، وبغرامة لا تجاوز ثلاثة آلاف دينار، أو بإحدى هاتين العقوبتين".

[٢] محمد علي العريان ، المرجع السابق، ص١٦٢ وما بعدها.

فقهاء القانون الجنائي اعتبار التزوير المعلوماتي جريمة نظراً لزيادة التلاعب في الحواسيب العائدة للبنوك والمؤسسات المالية، والتي ينتج عنها خسائر مالية كبيرة[١].

فالتزوير المعلوماتي ينصب على تعديل البيانات أو المعلومات المخزنة على الحاسب الآلي، مما يسبب ذلك ضرر للغير، وقد يكون التزوير بإضافة أو محو بعض البيانات أو المعلومات الذي يؤدي إلى تغيير جوهري فيها.

رابعاً: الجرائم الجنسية:

إن أكثر أشكال الجرائم الجنسية انتشاراً هي ارتياد المواقع والقوائم الإباحية لشراء الأفلام والصور أو مشاهدتها، كما قد يستخدم الجاني أساليب الابتزاز الجنسي عن طريق تهديد الفتيات بنشر صور لهن عبر الإنترنت[٢]، وأخطر الجرائم الجنسية هي الاستغلال الجنسي للأطفال مثل تصوير الأطفال في أوضاع مخلة ونشرها عبر المواقع الإباحية[٣].

ونصت المادة رقم ٥٥٤ فقد تحدثت على الجرائم الجنسية، من حيث التعامل بالمواد الإباحية أو نشرها أو بيعها أو شرائها أو عرضها[٤].

خامساً: الجرائم المالية:

وفي المادة رقم ٥٥٣ فقد نصت على الجرائم المالية، من حيث الاعتداء على الحسابات البنكية أو المصرفية، أو الحصول على أرقام بطاقات الائتمان، وكل جريمة إلكترونية تهدف إلى عائد مادي أو اقتصادي للجاني[٥].

---

[١] علي جبار الحسيناوي، المرجع السابق، ص٦٩.

[٢] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص٩٠.

[٣] محمد أمين الشوابكة ، المرجع السابق ، ص ١٠٥ .

[٤] نصت المادة رقم ٥٥٤ من مشروع قانون العقوبات لسنة ٢٠١٠م على أنه: " كل من قام بإنتاج صور إباحية بهدف توزيعها من خلال نظام حاسوب، أو قام بعرضها أو توفيرها أو شرائها أو معالجتها من خلال نفس النظام، أو من خلال وسيط لتخزين معلومات حاسوب، يعاقب بالحبس مدة لا تزيد على سنتين، وبغرامة لا تجاوز خمسة آلاف دينار، أو بإحدى هاتين العقوبتين".

[٥] نصت المادة رقم ٥٥٣ من مشروع قانون العقوبات لسنة ٢٠١٠م على أنه: " ١-كل من قام بإحداث فقدان لحق ملكية الغير وذلك من خلال إدخال أو تغيير أو محو أو حجب معلومات حاسوب، أو التداخل في عمل نظام حاسوب بقصد الاحتيال، أو لأي غرض آخر غير مشروع، بهدف جلب منفعة اقتصادية له أو للغير، يعاقب=

ويتمثل الركن المادي في جرائم السرقة الإلكترونية بفعل الاختلاس لمال منقول مملوك للغير، أما الركن المعنوي فيتمثل في القصد الجنائي الخاص وهو نية التملك[1].

فتتيح شبكة الإنترنت المجال للمخترقين الاطلاع على الحسابات البنكية للعملاء، ومن ثم يستغل القراصنة ذلك للتلاعب في هذه الحسابات ونقل الأرصدة من حساب لآخر أو إضافة أرقام لحسابات أخرى، أو اختلاس الأموال من حسابات العملاء، وتزايدت هذه الجريمة بشكل ملحوظ مما دفع الحكومات إلى البحث عن طرق لمكافحة السرقة عبر الإنترنت، وذلك من خلال وضع أنظمة الحماية المختلفة لأجهزة البنوك، وعقد الاتفاقيات الدولية ومراقبة مقاهي الإنترنت[2].

سادساً: جرائم سرقة البيانات والمعلومات والحقوق الفكرية الإلكترونية:

نص المشروع في المواد رقم ٥٥٥، ٥٥٦ على جرائم سرقة الحقوق الفكرية مثل الكتابات والأعمال الفنية سواء الصوتية أو المرئية، وسرقة البيانات والمعلومات التي تتعلق بالآخرين سواء تم سرقتها أثناء تسجيلها أو أرسالها أو تخزينها[3].

=بالحبس مدة لا تزيد على سنة، وبغرامة لا تجاوز ألفي دينار، أو بإحدى هاتين العقوبتين. ٢- كل من استولى بغير حق على أموال البنوك أو العملاء لديها عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات يعاقب بالسجن المؤقت وبالغرامة بقدر ما استفاد من الجريمة مع رد ما استولى عليه بدون وجه حق. ٣- كل من استخدم الشبكة المعلوماتية في الوصول دون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية يعاقب بالحبس مدة لا تزيد على سنتين، وبغرامة لا تجاوز خمس آلاف دينار، أو بإحدى هاتين العقوبتين".

[1] خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، المرجع السابق، ص٢٩٧.

[2] محمد الشناوي، **جرائم النصب المستحدثة**، دار الكتب القانونية، القاهرة، ٢٠٠٨م، ص٨٧.

[3] نصت المادة رقم ٥٥٥ من مشروع قانون العقوبات لسنة ٢٠١٠م على أنه: " كل من انتهك حقاً من حقوق الملكية الفكرية للغير سواء فيما يتعلق بالأعمال الأدبية أو الفنية أو التصويرية أو ما هو في حكم ذلك، يعاقب بالحبس مدة لا تزيد على ستة أشهر، وبغرامة لا تجاوز خمسمائة دينار، أو بإحدى هاتين العقوبتين".
ونصت المادة رقم ٥٥٦ على أنه: " ١- كل من سرق معلومات من نظام حاسوب خاص بالغير، يعاقب بالحبس، وبغرامة لا تجاوز ثلاثة آلاف دينار، أو بإحدى هاتين العقوبتين. ٢- ويعاقب بذات العقوبة كل من حصل بوجه غير مشروع بأية وسيلة من وسائل المعالجة المعلوماتية، أو مكّن غيره من الحصول على معلومات خاصة بالغير أثناء تسجيلها، أو إرسالها، متى كان من شأن إفشائها المساس بسمعة صاحبها أو بحياته الشخصية".

ويمثل الركن المادي في جريمة سرقة الحقوق الفكرية الإلكترونية بالنشاط الإجرامي للجاني في قيامه بأي فعل من شأنه الاعتداء على الحق الأدبي للمؤلف، أما الركن المعنوي فيكفي بعلم الجاني بأن ما ينشره من برامج هو لشخص آخر وأن تتجه إرادته إلى هذا الفعل[١].

سابعاً: جرائم الإتلاف والتعدي على الاشخاص:

وفي أخر مواد ٥٥٨، ٥٥٩، ٥٦٠ نص المشروع على الجرائم التي تضر بالآخرين سواء في أجهزتهم أو سمعتهم أو شرفهم ، ومن أمثلة هذه الجرائم إنشاء الفيروسات بهدف إتلاف الأجهزة أو اختراقها، أو نشر صور فاضحة لأشخاص بهدف الاساءة لسمعتهم، أو مضايقة الاشخاص بأي طريقة من الطرق عبر مواقع الإنترنت[٢].

ومن الجرائم التي تستهدف الأشخاص جريمة التشهير ويمثل الركن المادي فيها بنشاط الجاني المتمثل في فعل التشهير الذي يشترط فيه العلانية ، أما الركن المعنوي فهو علم الجاني بالسلوك الذي اقترفه واتجاه إرادته نحو هذا الفعل كما يجب أن يكون فعل التشهير علني[٣].

ويمثل الركن المادي في جريمة القذف بالسلوك الآثم وهو الرمي بالزنا أو نفي النسب، أما الركن المعنوي فهو علم الجاني بمدلول عبارات القذف ويعلم بأن ما قذف به غير صحيح، واتجاه إرادته إلى هذا القول[٤].

---

[١] محمد علي العريان ، المرجع السابق، ص٢٢٢ وما بعدها.

[٢] نصت المادة رقم ٥٥٨ من مشروع قانون العقوبات لسنة ٢٠١٠م على أنه: " كل من قام بدون وجه مشروع بصناعة أو نشر الفيروسات عن طريق الشبكة الدولية (الإنترنت) بقصد إحداث إتلاف كلّي أو جزئي للمعلومات لدى الغير، يعاقب بالحبس وبغرامة لا تقل عن ألف دينار، أو بإحدى هاتين العقوبتين".

ونصت المادة رقم ٥٥٩ على أنه: " كل من قام بدون وجه مشروع بمضايقة أو ملاحقة شخص آخر عبر الشبكة الدولية (الإنترنت) سواء من خلال البريد الإلكتروني أو بواسطة أية وسيلة أخرى، يعاقب بالحبس مدة لا تزيد على سنة، وبغرامة لا تجاوز ألف دينار، أو بإحدى هاتين العقوبتين".

ونصت المادة رقم ٥٦٠ على أنه: " كل من قام بدون وجه مشروع بنشر معلومات أو بيانات تتعلق بالآخرين عبر الشبكة الدولية (الإنترنت) قاصداً الإساءة لهم أو تشويه سمعتهم، يعاقب بالحبس، وبغرامة لا تقل عن ألف دينار، أو بإحدى هاتين العقوبتين".

[٣] يوسف المصري، المرجع السابق، ص١٤٥ وما بعدها.

[٤] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص٢٠٠، ٢٠١.

إن الجرائم التي ذكرناها فيما أعلاه هي الجرائم الإلكترونية التي نص عليها المشرع الفلسطيني في مشروع قانون العقوبات لسنة ٢٠١٠م، وهذه المواد أجملت أغلب صور الجرائم الإلكترونية التي ظهرت على الساحة الفلسطينية، ولكنها لم تجمل جميع الجرائم الإلكترونية لأن هناك عدة جرائم ظهرت في دول مجاورة ولم تظهر بعد على الساحة الفلسطينية، ولكنها ليست ببعيدة، ولذلك كان الأجدر بالمشرع الفلسطيني أن يذكر كل الجرائم الإلكترونية حتى التي لم تظهر منها في الواقع الفلسطيني، حتى نتفادى الفراغ التشريعي الذي من الممكن أن يحدث في المستقبل، فمن هذه الجرائم إنشاء المواقع الإلكترونية التي تروج للمخدرات أو للعب القمار أو لغسيل الأموال، والجرائم الإلكترونية التي تتعلق بالإتجار بالجنس البشري.

وليت المشرع الفلسطيني يعمد إلى تشريع قانون خاص لمكافحة الجرائم الإلكترونية، على غرار المشرع الأردني والسوداني، وبذلك سيضمن المشرع نوع من الاستقرار على الصعيد الجزائي، وسيسد المشرع الثغرات الموجودة في قانون العقوبات، ومشروع قانون العقوبات الذي لم يختلف كثيراً عن الأول من حيث مكافحته للجريمة الإلكترونية، لعدم اشتماله على كافة أشكال الجرائم الإلكترونية التي ظهرت حديثاً مثل الجرائم التي تتعلق بغسيل الأموال والإتجار بالمخدرات والجنس البشري.

والمطالبة باستحداث قوانين تكافح الجرائم الإلكترونية ليس مطلباً فلسطينياً فقط، بل إنه مطلب عالمي، حيث شهدت السنوات الخمس الأولى من القرن الجديد تزايداً ملحوظاً في عدد الجرائم الإلكترونية في جمهورية مصر العربية، على المستوى الأمني والاقتصادي والاجتماعي[١].

المطلب الثالث

صور الجرائم الإلكترونية في قانون أنظمة المعلومات الأردني

تميز المشرع الأردني عن المشرع الفلسطيني بأن أقر قانون خاص يكافح الجرائم الإلكترونية، وهو قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م، ويعد هذا القانون من أحدث التشريعات العربية التي كافحت الجرائم الإلكترونية، وقد تضمنت المادة الاولى من هذا القانون على مجموعة من المصطلحات مثل تعريف البيانات والمعلومات والشبكة المعلوماتية

[١] جمال محمد غيطاس، المرجع السابق، ص٢١١.

وغيرها[1]، ويثار التساؤل عن مدى فعالية هذا القانون وعن مدى اشتماله على جميع صور الجرائم الإلكترونية؟، وهذا هو ما سنوضحه فيما هو آت:

أولاً: جرائم أنظمة المعلومات:

نص قانون أنظمة المعلومات الأردني في المواد ٣,٤,٥ على الجرائم التي تتعلق بالبرامج والمعلومات، مثل جرائم الاختراق والإتلاف والتصنت ومحو ونسخ البيانات الإلكترونية، وكافة أشكال الجرائم التي تتعلق بأنظمة المعلومات[2].

---

[1] رامي متولي القاضي، المرجع السابق، ص٢٣ .

[2] نصت المادة رقم ٣ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l. على أنه: " أ- كل من دخل قصداً الى موقعٍ الكترونيٍ أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلتا هاتين العقوبتين . ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (٢٠٠)مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار أو بكلتا هاتين العقوبتين".

ونصت المادة رقم ٤ على أنه: " كل من ادخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الاخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار أو بكلتا هاتين العقوبتين" .

ونصت المادة رقم ٥ على أنه: " كل من قام قصداً بالتقاط أو باعتراض أو بالتنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار أو بكلتا هاتين العقوبتين" .

ويمثل الركن المادي في جريمة الولوج والبقاء في النظام الإلكتروني في الفعل الذي يرتكبه الجاني والذي يهدف من خلاله انتهاك نظام الحماية الأمنية للمواقع والأنظمة الإلكترونية، أما الركن المعنوي فيمثل العلم بالجريمة واتجاه إرادة الجاني لارتكابها[١].

ثانياً: الجرائم المالية:

وفي المادة رقم ٦ فقد نص المشرع الأردني على الجرائم المالية، مثل التي تتعلق ببطاقات الائتمان و المعاملات المالية والمصرفية [٢].

ومن ضمن الجرائم المالية جرائم إساءة استخدام البطاقات المالية مثل استخدام البطاقات والسحب عليها على الرغم من عدم كفاية الرصيد، أو استخدام البطاقة بعد إلغائها أو انتهاء مدة صلاحيتها، أو إساءة استخدام البطاقة من قبل الغير[٣].

ويتمثل الركن المادي في جرائم السرقة الإلكترونية في فعل الاختلاس لمال منقول مملوك للغير، أما الركن المعنوي فيتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، وكذلك تتطلب هذه الجريمة توافر قصد خاص وهو نية تملك الشيء المختلس[٤].

---

[١] بلال أمين زين الدين، المرجع السابق، ص٢٧١ وما بعدها.

[٢] نصت المادة رقم ٦ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l http://www.lob.gov.jo/. على أنه: " أ- كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنتين أو بغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٢٠٠٠) ألفي دينار أو بكلتا هاتين العقوبتين. ب- كل من استخدم عن طريق الشبكة المعلوماتية أو أي نظام معلومات قصداً دون سبب مشروع بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية للحصول لنفسه أو لغيره على بيانات أو معلومات أو أموال أو خدمات تخص الاخرين يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار".

[٣] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٢٠١.

[٤] محمد علي العريان ، المرجع السابق، ص١٢٦ وما بعدها.

وخصص المشرع الأردني في المادة ٧ الجرائم التي يرتكبها الموظفين أثناء عملهم في المواد من٣ إلى٦ بأن تضاعف لهم العقوبة إذا ما اقترفوا هذه الجرائم أثناء أوقات عملهم[١].

ثالثاً: الجرائم الجنسية:

تتيح شبكة الإنترنت أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم على الجميع منازلهم ومكاتبهم[٢]، الأمر الذي أدى إلى زيادة جرائم الاغتصاب والتحرش بالأطفال والعنف الجنسي وفقد العائلة لقيمها[٣].

وفي المواد رقم ٩,٨ فقد نص المشرع الأردني على الجرائم الجنسية و على كافة أشكال التعامل بالمواد الإباحية من حيث الترويج لها و نشرها وعرضها، وركز المشرع الأردني على تأثير كافة الأعمال الإباحية على الأطفال الذين لم يكملوا سن الثامن عشر[٤].

---

[١] نصت المادة رقم ٧ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l. على أنه: " تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (٣) الى (٦) من هذا القانون بحق كل من قام بارتكاب أي منها أثناء تأديته وظيفته أو عمله أو باستغلال أيٍ منهما".

[٢] محمد علي العريان ، المرجع السابق، ص٩١ وما بعدها.

[٣] يوسف المصري، المرجع السابق، ص١٤٥ وما بعدها.

[٤] نصت المادة رقم ٨ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l. على أنه: " أ- كل من أرسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية يشارك فيها أو تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر وبغرامة لا تقل عن (٣٠٠) ثلاثمائة دينار ولا تزيد على (٥٠٠٠) خمسة ألاف دينار. ب-كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية في إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا او عقليا، أو توجيهه أو تحريضه على ارتكاب جريمة، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة الاف دينار. ج- كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا او عقليا، في الدعارة أو الأعمال الإباحية ، يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (٥٠٠٠) خمسة ألاف دينار ولا تزيد على (١٥٠٠٠) خمسة عشر ألف دينار".=

رابعاً: جرائم النظام والأمن العام:

تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية، خاصة مع استخدام الإنترنت وانتشاره عربياً وعالمياً[١]، حيث توقع هذه الجريمة ضررها على المجتمع ككل، ويمثل الركن المادي لهذه الجريمة السلوك الإجرامي وهو القائم على الدخول غير المشروع لأنظمة المعالجة الآلية للمعلومات والبيانات الإلكترونية للحصول على الوثائق والبيانات السرية، أما الركن المعنوي فهو القصد الخاص الذي يمثل قصد الجاني بإيقاع ضرر بالدولة والإساءة لها[٢].

وتحدثت المواد رقم ١١,١٠ عن الجرائم التي تمس النظام والأمن العام، من حيث ما يتعلق بإنشاء الجماعات التي تعمل على نشر الفتنة بين أفراد المجتمع، والجرائم التي تستهدف المعلومات التي تخص الدولة في الشؤون الداخلية والخارجية والاقتصادية[٣].

وانتشرت في العصر الحديث جريمة التجسس الإلكتروني، والتي تهدف إلى التجسس على الاعداء لمعرفة أخبارهم والخطط التي يعدوا لها، ومن صور التجسس الإلكتروني اختراق الأقمار

=ونصت المادة رقم ٩ على أنه: " كل من قام قصداً باستخدام الشبكة المعلوماتية أو أي نظام معلومات للترويج للدعارة يعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (٣٠٠) ثلاثمائة دينار ولا تزيد على (٥٠٠٠) خمسة الاف دينار".

[١] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص١٣٢.

[٢] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص ٢٦٥ وما بعدها.

[٣] نصت المادة رقم ١٠ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l. على أنه: " كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو انشأ موقعاً الكترونياً لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة".

ونصت المادة رقم ١١ على أنه: " أ- كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع الكتروني أو نظام معلومات باي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٥٠٠٠) خمسة ألاف دينار. ب- إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة ، بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها ، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار".

الصناعية التي يمكنها تصوير كل ما يتحرك على الأرض مثل الإنسان والآلات الحربية والمدنية والمنشآت العسكرية، وتكمن خطورة التجسس الإلكتروني في أن من يقوم به ليس القراصنة ولا العابثين بل هي أجهزة مخابرات بعض الدول التي تهدف إلى الحصول على المعلومات الأمنية والعسكرية والاقتصادية في تلك الدول[١].

ومن الجرائم التي تهدد الأمن العام الجرائم المنظمة مثل المافيا التي قد تنشأ مواقع عبر الإنترنت لمساعدتها في إدارة عملياتها وتلقي المراسلات واصطياد الضحايا، والجريمة المنظمة تهدد أمن المجتمع فهدفها هو إفشاء الرعب والخوف وتنفيذ عمليات إرهابية تستهدف الأمن والسلم في المجتمع[٢].

ومما سبق وبالمقارنة مع الواقع الفلسطيني يتبين أن المشرع الأردني قد انتهج خطوة في الاتجاه الصحيح من حيث أنه شرع قانون يختص في مكافحة الجرائم الإلكترونية، ولكن هذه الخطوة غير كافية، نظراً لوجود العديد من الجرائم التي لم ينص عليها المشرع الأردني في قانون جرائم أنظمة المعلومات، في حين أن هناك أكثر من دولة عربية شرعت قوانين تكافح الجرائم الإلكترونية، وكانت قوانين هذه الدول شاملة لأغلب الجرائم الإلكترونية التي ظهرت في العصر الحديث، ومثال ذلك قانون جرائم المعلومات السوداني لسنة ٢٠٠٧م، الصادر بتاريخ ٢٠٠٧/٦/٢٠م، فبعد اطلاعنا على مجموعة من قوانين الجرائم الإلكترونية في الدول العربية، ومن بينها عُمان والأمارات والسعودية[٣]، كان القانون السوداني هو الأعم بينها من حيث أنه جرم كل أشكال الجرائم الإلكترونية التي ظهرت في الوقت الحاضر، ومن هنا ندعو المشرع الفلسطيني أن يخطو خطو المشرع السوداني في تشريع قانون يغطي جميع الجرائم الإلكترونية التي من الممكن أن تقع في الوقت الحالي.

---

[١] منير محمد الجنيهي، ممدوح محمد الجنيهي، **جرائم الإنترنت والحاسب الآلي**، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص١٠٦، ١٠٧.

[٢] يوسف المصري، المرجع السابق، ص٨٤.

[٣] أنظر قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢ العُماني، مشار إليه في موقع تقنية المعلومات العُماني عبر الرابط التالي: http://www.ita.gov.om/، و أنظر النظام السعودي بشأن مكافحة جرائم المعلوماتية لعام ١٤٢٨هـ، مشار إليه في الموقع الرسمي لمجلس الوزراء السعودي عبر الرابط التالي: http://www.boe.gov.sa/ ، وأنظر القانون الاتحادي رقم٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات في الإمارات، مشار إليه في كتاب د . رامي متولي القاضي ، مكافحة الجرائم المعلوماتية ، ملحق رقم (١)، المرجع السابق، ص١٧٩.

المبحث الثالث

الطبيعة القانونية لمحل الجريمة الإلكترونية

أثبتت الإحصائيات[1] تزايد ظهور الجرائم الإلكترونية، وأخذت بالتطور من حين لأخر، وقد تسبب ذلك بحدوث إشكالات قانونية كثيرة، من بينها عدم قدرة نصوص قانون العقوبات مواجهة هذه الجرائم، واستحدث المشرع الفلسطيني المادة ٢٦٢مكرر في قانون العقوبات الفلسطيني لسنة ١٩٣٦م، ولكن هذه المادة غير كافية لعدم قدرتها مواكبة التطور السريع للجرائم الإلكترونية، فعلى سبيل المثال إن الواقع العملي للقضاء الفلسطيني يطبق نص المادة ٢٦٢ مكرر[2] على كافة الجرائم التي تتعلق بالحاسوب والإنترنت والهاتف المحمول، وهذا الخطأ قد يستفيد منه المحامون لإفلات الجناة من العقاب، وسيتسبب ذلك في عدم العدالة الجنائية في المجتمع الفلسطيني.

وكما يجري العمل إن الأجهزة الإلكترونية المادية يطبق عليها نصوص التجريم التقليدية، فهي تصلح لتطبيق هذه النصوص عليها مثل التي تتعلق بالسرقة والإتلاف ولا خلاف عليها، ولكن الاختلاف في الجريمة الإلكترونية هو حول المال الإلكتروني المعنوي مثل المعلومات والبيانات المخزنة، أو استخدام الجهاز الإلكتروني في تنفيذ الجرائم[3].

فالبيانات والمعلومات الإلكترونية تقبل حيازتها ونقلها عبر الأقراص الصلبة والمرنة، وكذلك يتم نقلها عبر البريد الإلكتروني، كما أن البيانات والبرامج لها قيمة مادية كبيرة، ولذلك فهي تعتبر مال منقول، ويقول الدكتور عبد الرزاق السنهوري أنه " إذا كان التطور قد زاد من عدد الأشياء المعنوية بحيث تفوق بعضها قيمة الأشياء المادية مما استدعى الأمر إلى إعادة النظر في حصر

---

[1] أجرى الباحث إحصائية للقضايا التي سجلت لدى نيابة شمال غزة في محافظة شمال غزة عام ٢٠١١م وكان عددها ٢٨ قضية، أما عام ٢٠١٢م فكان عدد الجرائم ٤١ قضية، فكان هناك زيادة ملحوظة في عدد القضايا بـ١٣ قضية، وكان عدد القضايا في النصف الاول من سنة ٢٠١٣م ٣٢ قضية الأمر الذي يؤكد زيادة عدد هذه الجرائم، فعددها في النصف الأول من هذه السنة أكثر بـ٤ قضايا عن سنة ٢٠١١م.

[2] درج القضاء الفلسطيني على تطبيق نص المادة رقم ٢٦٢ مكرر من قانون العقوبات رقم ٧٤ لسنة ١٩٣٦م على كافة أشكال الجرائم الإلكترونية، ونرى أن تطبيق القضاء لذلك النص لا يخالف مبدأ الشرعية حيث أن هذه المادة تنص على كافة الجرائم التي ترتكب عبر الأجهزة الإلكترونية، وفي الواقع إن الجرائم الإلكترونية ترتكب لإساءة استخدام الأجهزة الإلكترونية.

[3] هدى حامد قشقوش، المرجع السابق، ص٣١.

الأموال على الأشياء المادية وحدها، والبحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الحق المالي، حتى يمكن إسباغ صفة المال على الشيء المعنوي"[١].

كما ويرى جانب من الفقه أن المعلومات الإلكترونية، لها قيمة اقتصادية في ذاتها، كونها تقبل للحيازة المشروعة، ولها مظهر معنوي يقبل النقل والحيازة، ولذلك يجب على المشرع أن يضع الحماية القانونية للمعلومات الإلكترونية[٢].

وأكد المشرع الأردني على ما سبق في المادة رقم ٥٤ من القانون المدني على أن "كل شيء يمكن حيازته مادياً أو معنوياً والانتفاع به انتفاعاً مشروعاً، ولا يخرج عن التعامل بطبيعته أو بحكم القانون يصح أن يكون محلاً للحقوق المالية"[٣]، حيث عالج المشرع الأردني مسألة الطبيعة القانونية لمحل الجرائم الإلكترونية من خلال هذه المادة، وقطع الطريق على من حاول الإفلات من الجزاء الجنائي لمن ارتكاب جريمة إلكترونية، إذا أحتج بأن البيانات والمعلومات لا يمكن تقويمها بمال، أو أن المشرع لم يعتبرها مال له قيمة اقتصادية ويصلح أن يكون محلاً للحقوق المالية[٤].

ويعد توفير الحماية القانونية لبيانات وبرامج الحاسب الآلي، له عدة نتائج إيجابية أهمها إضفاء الحماية القانونية لهذه البيانات والبرامج مما يوفر الأمن المعلوماتي للمواطنين، الأمر الذي يرتب ردع لقراصنة الكمبيوتر والمخترقين، وكذلك ملاحقة كل من ارتكب جريمة إلكترونية، ومطالبة كل متضرر تعويض مناسب عما لحقه من ضرر[٥].

وخلاصة القول أن البيانات والمعلومات وبرامج الحاسب الآلي هي مال قابل للنقل والحيازة المشروعة ويكون محلاً للحقوق المالية، وهذا ما اتجه إليه الفقه الحديث، وإن القول خلاف ذلك

---

[١] مشار إليه لدى خالد عياد الحلبي، المرجع السابق، ص٥٥، ٥٨.

[٢] محمد علي العريان، المرجع السابق، ص ٦٤ .

[٣] راجع المادة رقم ٥٤ من القانون المدني الأردني رقم (٤٣) لسنة ١٩٧٦م ، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ui/main.html.

[٤] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت**، المرجع السابق، ص١١٦ .

[٥] عبد الرحمن جميل حسين، **الحماية القانونية لبرامج الحاسب الآلي**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، ٢٠٠٨م، ص١٦.

يتسبب لنا بالكثير من المشاكل القانونية على الصعيد الجزائي، ويحدث ارباكاً بين القانونيين لن يستفيد منه إلا المجرمين[1].

ومما سبق اتضح لنا ماهية الجرائم الإلكترونية وتعريفها وخصائصها وصورها، وقد أوضحنا ذلك تفصيلاً، مع بيان الطبيعة القانونية لمحلها، وسنوضح في الفصل التالي القواعد الموضوعية للجرائم الإلكترونية من حيث أركان الجريمة الإلكترونية والمحاولة فيها والجزاء الجنائي المترتب عليها في القانون الفلسطيني والقانون الأردني.

[1] من الجرائم الإلكترونية الجديدة التي كانت تواجه محققي الشرطة سرقة نقاط الجوال، حيث كان هناك إشكالية في التعامل مع الواقعة إن كانت جريمة أم لا، ولكن تم التعامل فيما بعد مع هذا النوع من الجرائم بعد انتشاره بشكل ملحوظ على اعتبار أن نقاط الجوال مال إلكتروني قابل للحيازة والنقل من جوال لأخر، ولذلك تم التعامل مع هذه الجريمة كجريمة إلكترونية، نظراً لانطباق نص المادة رقم ٢٦٢ مكرر من قانون العقوبات رقم ٧٤ لسنة ١٩٣٦م، على هذه الواقع، وتوافر أركان الجريمة المادي والمعنوي والشرعي، كما أن الفاعل استخدم جهاز إلكتروني –هاتف محمول– في تنفيذ جريمته.

الفصل الثاني

القواعد الموضوعية للجرائم الإلكترونية

تمهيد وتقسيم :

تعتبر الجرائم الإلكترونية من الجرائم الجديدة، التي لم يتناولها فقهاء القانون إلا في العصر الحديث، فقد ظهرت هذه الجرائم مع ظهور الوسائل التكنولوجية الحديثة ووسائل الاتصال السريعة، كل ذلك أثر سلباً في سرعة المعالجة التشريعية لهذه الجرائم، فكونها جرائم جديدة وسريعة التطور كان من الصعب على الفقهاء تحديد اركانها وشرحها وتفصيلها، إلا أن فقهاء القانون الحديث قد بدأوا في وضع الخطوط العريضة لمعالجة هذه الجرائم، من خلال البحث عن صور الجرائم الإلكترونية وشرح اركانها، وتصنيف هذه الجرائم حسب درجة خطورتها والخسائر التي تخلفها سواء مادية أو معنوية، للخروج من ذلك إلى وضع الجزاء الجنائي المناسب على كل جريمة، وعليه سوف نعرض القواعد الموضوعية للجرائم الإلكترونية من خلال المباحث التالية:

المبحث الأول : أركان الجريمة الإلكترونية .

المبحث الثاني : المحاولة في الجرائم الإلكترونية .

المبحث الثالث : الجزاء الجنائي للجرائم الإلكترونية .

المبحث الأول

أركان الجريمة الإلكترونية

اشترط المشرع الجزائي لقيام أي جريمة وجود ثلاث أركان أساسية، وهي الركن المادي والركن المعنوي والركن الشرعي، وبدون هذه الأركان تنتفي الجريمة، وهذا هو الحال بالنسبة للجرائم الإلكترونية، فلقيام الجريمة الإلكترونية لا بد من أن يتوفر فيها أركان الجريمة، وبدون هذه الأركان يصبح هناك خلل في موضوع الجريمة، ويتمثل الركن المادي في النشاط الذي يرتكبه الجاني، أما الركن المعنوي فيتمثل في الإرادة الخاطئة لمباشرة السلوك الإجرامي، فالركن المادي له مظهر خارجي أما الركن المعنوي فهو يكمن في نفس الجاني[١]، أما الركن الشرعي فنعني به وجود نص قانوني يحدد الجريمة والجزاء الجنائي على سلوكيات معينة والذي ينقلها من دائرة الإباحة إلى دائرة التأثيم[٢]، وسوف نوضح الركن المادي والركن المعنوي عبر ما هو تال:

المطلب الأول : الركن المادي في الجريمة الإلكترونية .

المطلب الثاني : الركن المعنوي في الجريمة الإلكترونية .

المطلب الأول

الركن المادي في الجريمة الإلكترونية

يعد السلوك هو القاسم المشترك بين جميع الجرائم، وهو العنصر الأول من عناصر الركن المادي للجريمة، ويجب أن يكون الموضوع الذي يقع عليه السلوك محل حماية من قبل المشرع، وأن يكون مجرم بنص القانون[٣]، ونص المشرع الفلسطيني على أن: "...ولا عقاب إلا على الأفعال اللاحقة لنفاذ القانون"[٤]، ويجب أن يترتب على هذا السلوك نتيجة إجرامية وهو العنصر الثاني للركن

---

[١] أحمد فتحي سرور، **الوسيط في قانون العقوبات**، الجزء الأول، القسم العام، دار النهضة العربية، القاهرة، ١٩٨١م، ص٢٥٦.

[٢] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، مرجع سابق، ص١١٩.

[٣] جلال ثروت، المرجع السابق، ص١١٩.

[٤] راجع المادة ١٥ من القانون الاساسي الفلسطيني المعدل لسنة ٢٠٠٥م.

المادي للجريمة، وهو الأثر الذي يتركه السلوك الإجرامي سواء كان فعلاً أم تركاً في العالم الخارجي وذلك طبقاً للاتجاه المادي، أما الاتجاه القانوني فهو الضرر الذي يصيب المصلحة التي يحميها الشارع، أما العنصر الثالث فهو علاقة السببية بين السلوك سواء كان فعل أم امتناع وبين النتيجة الإجرامية، وبمعنى أخر لولا السلوك فعلاً أم امتناعاً ما كانت لتحدث النتيجة الإجرامية[١].

أما المشرع الفلسطيني فقد اكتفى بالسلوك أو النشاط الإجرامي فقط ليتحقق الركن المادي للجريمة دون النظر إلى النتيجة الإجرامية وعلاقة السببية، فيكفي أن يباشر المجرم سلوكه الإجرامي للقول بأن الركن المادي للجريمة أكتمل، إلا إذا كانت هناك بعض الجرائم تتطلب تحقق النتيجة الإجرامية لاكتمال الركن المادي فيها، ونص المشرع الفلسطيني في ذلك على أن: " لا عبرة للنتيجة التي كان القصد أن يؤدي إليها ارتكاب فعل أو ترك إلا إذا ورد نص صريح على أن نية الوصول إلى تلك النتيجة تؤلف عنصراً من عناصر الجرم الذي يتكون كله أو بعضه من ذلك الفعل أو الترك"[٢].

وكذلك المشرع الأردني اكتفى لقيام الجريمة السلوك الجنائي، دون النظر إلى النتيجة الإجرامية التي كان يبتغيها الجاني، إلا إذا كانت الجريمة تتطلب تحقق نتيجة معينة، وهذا ما نص عليه المشرع الأردني في المادة رقم ٦٥ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠م حيث نص على أن: "لا عبرة للنتيجة إذا كان القصد أن يؤدي إليها ارتكاب فعل إلا إذا ورد نص صريح على أن نية الوصول الى تلك النتيجة تؤلف عنصراً من عناصر الجرم الذي يتكون كله أو بعضه من ذلك الفعل"[٣].

ونرى مما تقدم أنه لكي يتوفر الركن المادي في الجرائم الإلكترونية لا بد من وجود بيئة رقمية، تتمثل في جهاز إلكتروني مثل الحاسب الآلي أو هاتف محمول، وأن يكون الجهاز الإلكتروني متصل بالإنترنت في الجرائم المتصلة بالإنترنت، فبدون ما ذكر لا يمكننا مباشرة السلوك الإجرامي، ولا نكون بصدد جريمة إلكترونية فكما قلنا بأن الجهاز الإلكتروني من أهم عناصر الجريمة الإلكترونية.

---

[١] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص١٣٨ وما بعدها.

[٢] راجع المادة رقم ٢/١١ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٣] راجع المادة رقم ٦٥ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ui/main.html.

وفي ضوء ما سبق سنتناول بالتفصيل السلوك والنتيجة الإجرامية وعلاقة السببية في الجرائم الإلكترونية عبر الفروع الآتية:

الفرع الأول

السلوك في الجرائم الإلكترونية

من أهم ما يميز الجرائم الإلكترونية بشكل عام هو وجود حاسب آلي، فبدون الحاسب الآلي لا يمكننا تصور وجود جريمة إلكترونية، ويعد حيازة الحاسب الآلي والإنترنت مشروع، كما أن استخدامهما مشروع كأصل عام، ولكن الخلاف يثور حين تستخدم هذا الوسائل الحديثة لغايات غير مشروعة، ولذلك تعد الوسيلة الإلكترونية من أهم مقومات السلوك الإجرامي في الجرائم الإلكترونية، فالسلوك هنا يتطلب وجود بيئة رقمية من حيث الجهاز الإلكتروني للجرائم الإلكترونية بشكل عام، والاتصال بالإنترنت لجرائم الإنترنت بشكل خاص، كما ويتطلب الأمر معرفة بكيفية استخدام هذه التقنية مثل كيفية تحميل صور مخلة بالآداب على الجهاز، أو إعداد برنامج فايروس تجهيزاً لنشره عبر الإنترنت[1].

إن المنطق التقني الذي ذكرناه يمثل سلوكاً مادياً إيجابياً للجرائم الإلكترونية، فهذا يجعل الجرائم الإلكترونية ذات طابع موحد يتمثل في السلوك والنشاط المادي كعنصر اساسي للجرائم الإلكترونية، ونلمس ذلك عندما نص المشرع المقارن على الجرائم التي ترتكب عبر الحاسوب حيث قرر عبارة " إذا ارتكبت الجريمة باستخدام الحاسوب..."، وعبارة "باستخدام المعالجة الآلية للبيانات" وبهذه الحالات ادرك المشرع القيمة الموحدة للشروع في الجرائم الإلكترونية[2].

ويتخذ السلوك في الجرائم الإلكترونية صورتين: الأولى وهي السلوك الإيجابي والذي يتطلب مجهود بدني يتمثل في العالم الخارجي من حركات عضوية يأتيها الجاني بهدف الاعتداء على المصلحة التي يحميها الشارع، ومثال ذلك في الجرائم الإلكترونية كل الأفعال التي يرتكبها الجاني في التلاعب ببرامج وبيانات الحاسب الآلي بهدف إتلاف البيانات أو سرقتها أو نسخها.

---

[1] خالد ممدوح إبراهيم، **حوكمة الإنترنت**، المرجع السابق، ص ٣٨٢ وما بعدها.

[2] علي جبار الحسيناوي، المرجع السابق، ص٣٧، نقلاً عن عمر محمد يونس، **الجرائم الناشئة عن استخدام الإنترنت**، رسالة دكتوراه، جامعة عين شمس/كلية الحقوق، ٢٠٠٤م، ص٢٥٢.

ومثال السلوك الإجرامي الإيجابي استخدام الجاني وسائل الاتصال بشكل غير قانوني، كأن يقوم باختراق شبكات الاتصال أو يقوم بإجراء المكالمات المحلية أو الدولية بشكل غير مشروع، أي بدون دفعة الرسوم المستحقة، أو أن يقوم الجاني باختراق شبكات الاتصال ويحصل على بيانات الشركات الخاصة ويقوم بنشرها، أو يهدد أصحابها باستخدامها بشكل غير مشروع[١].

أما الصورة الثانية وهي السلوك السلبي، وهو الامتناع عن إتيان أمر يوجبه المشرع[٢]، فمن الممكن ارتكاب جريمة بالكف عن عمل معين كان من الواجب مباشرته، وهذا الامتناع عن قاعدة أمرة فرضها المشرع، مثل امتناع المنقذ البحري من إنقاذ غريق كان بإمكانه إنقاذه، أما صور الامتناع في الجرائم الإلكترونية فهي مع اختلاف الفقهاء متوافرة ومن الممكن حدوثها، مثل امتناع موظف أمن عن حماية بيانات ومعلومات الشركة التي يعمل بها، أو عدم الإبلاغ عن جريمة للحفاظ على حقوق الغير وخصوصيتهم، أو عدم التدخل للحفاظ على اسرار الدولة في الجرائم التي تمس أمن الدولة[٣].

وخلاصة القول أن السلوك في الجرائم الإلكترونية يتم عن طريق الوسيلة وهي الجهاز الإلكتروني أياً كان نوعه أو شكله، واتصال بشبكة الإنترنت للجرائم المرتبطة بالإنترنت، وبدون هذه الوسيلة لا يمكن مباشرة السلوك الإجرامي، وقد يكون السلوك ايجابي بمباشرة الفعل من الجاني وهو أغلب صور الجرائم الإلكترونية والذي يرتكب على هيئة فعل مادي باستخدام أحدى الوسائل الإلكترونية، وقد يكون السلوك سلبي بالامتناع عن فعل كان من الواجب اتيانه وهو نادر الحدوث وفي الغالب يرتكب من قبل موظفين مختصين.

الفرع الثاني

النتيجة الإجرامية في الجرائم الإلكترونية

النتيجة الإجرامية هي العنصر الثاني من عناصر الركن المادي للجريمة، وهي عبارة عن الضرر الذي نتج عن السلوك الإجرامي سواء كان فعلاً أم تركاً، وهو الأثر الخارجي الذي يتولد

---

[١] عبد الفتاح بيومي حجازي، **الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة**، المرجع السابق، ص٢٦٦.

[٢] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٥٠.

[٣] إبراهيم محمود اللبيدي، **السلوك الإجرامي في جرائم الإنترنت**، مركز الأعلام الأمني، القاهرة، نسخة إلكترونية، ص٢٥.

عن السلوك ويحدث تغييراً يعتد به القانون، وذلك طبقاً للتصور المادي للنتيجة، أما التصور القانوني أو الشرعي فهو الاعتداء على المصلحة التي يحميها القانون[١].

ومثال تحقق النتيجة الإجرامية في الجرائم الإلكترونية الطبيب المعالج الذي يدخل إلى قاعدة بيانات المشفى عن طريق الإنترنت من منزله أو مكان أخر، ثم يقوم بتغيير معدل دواء لأحد المرض بهدف قتله، فإذا مات المريض تحققت النتيجة الإجرامية لسلوك الطبيب، والذي يكون لديه العلم الكافي بالفعل الذي ارتكبه، فضلاً عن ذلك فهو يملك كلمات المرور الخاصة بقاعدة بيانات المستشفى الأمر الذي يسر له ارتكاب جريمته[٢].

كذلك يعتبر إتلاف البيانات والمعلومات بسبب نشر الفيروسات أو اختراق الأجهزة هو الأثر والنتيجة المترتبة على تلك الجرائم، وهذه الأضرار تقنية من السهل اكتشافها وتقديرها، كما قد يكون الضرر معنوي مثل ذم أو سب شخص عن طريق الإنترنت أو إنشاء مواقع تبث الأفكار المسمومة لأفراد المجتمع، أو اختراق مواقع المؤسسات الحكومية بهدف الاطلاع على الأسرار الأمنية والاقتصادية، فهذه الجرائم أثرها معنوي يخضع تقديرها للسلطة التقديرية للقاضي المختص.

الفرع الثالث

علاقة السببية في الجرائم الإلكترونية

يُقصد بعلاقة السببية هي العلاقة بين السلوك الإجرامي فعلاً أم تركاً وبين النتيجة الإجرامية، بمعنى أن السلوك الإجرامي هو السبب في إحداث النتيجة الإجرامية، ولولا هذا السلوك ما كانت لتحدث النتيجة الإجرامية[٣]، وتبرز الأهمية القانونية لعلاقة السببية من حيث أنها من العناصر الأساسية المكونة للركن المادي للجريمة، وتحققها شرطاً جوهرياً من شروط المسئولية الجزائية، فإذا اسندنا النتيجة الإجرامية إلى السلوك وكانت هناك إرادة حرة واعية توافرت أسباب قيام المسئولية الجزائية، أما إذا لم يكن هناك علاقة بين النتيجة الإجرامية والسلوك انتفت المسئولية الجزائية[٤].

---

[١] جلال ثروت، المرجع السابق، ص١٢٢.

[٢] خالد ممدوح إبراهيم، **حوكمة الإنترنت**، المرجع السابق، ص ٣٨٨.

[٣] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت** ، المرجع السابق ، ص٤٨.

[٤] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص١٤٧ وما بعدها.

ولكي تكتمل علاقة السببية في جريمة التعدي على الحق في الخصوصية، يجب أن يكون هناك اتصال بالإنترنت من خلال جهاز إلكتروني، ومن ثم اختراق جهاز ما أو موقع ما والوصول إلى بياناته الخاصة، وبعدها يتم نشر هذه البيانات من صور أو معلومات عبر موقع معد مسبقاً لذلك، أو عن طريق المواقع الإلكترونية مثل مواقع التواصل الاجتماعي، وتثبت كذلك علاقة السببية في جريمة حيازة صور إباحية لأطفال في حاسوب بمجرد ثبوت الضرر من خلال بث هذه الصور، فتظهر علاقة السببية بين حيازة هذه الصور وبين ترويجها أو عرضها أو تداولها[١].

أمثلة على الركن المادي في بعض الجرائم الإلكترونية:

إن أكثر الجرائم التي توقع خسائر مادية هي جرائم السرقة الإلكترونية، وأغلب هذه الجرائم ترتكب عبر اختراق مواقع البنوك لسرقة الحسابات البنكية، أو الحصول على بيانات العملاء في الشركات، وكل ما يشمل الحصول على بيانات أو معلومات دون الحصول على إذن من صاحب المحل الإلكتروني، فذلك يكفي لقيام الركن المادي لجريمة السرقة الإلكترونية، وفي جريمة الإتلاف الإلكترونية فهناك عدة طرق قد ينتهجها المجرم الإلكتروني في ارتكاب جريمته، إما عن طريق إتلاف قاعدة البيانات الأساسية للمحل الإلكتروني، أو عن طريق الاتصال عن بعد والدخول لبرامج الحاسب الآلي وإتلاف البرامج والبيانات والمعلومات، أو عن طريق إرسال برامج فايروس لتدمر البيانات والمعلومات تلقائياً[٢].

ومن الجرائم الإلكترونية المنتشرة بكثرة جرائم الذم والقذف، ويتكون الركن المادي في هذه الجرائم من النشاط الخادش للشرف والاعتبار، الذي يرتكبه الجاني عن طريق الحاسب الآلي أو الهاتف المحمول، مثل إرسال رسائل نصية بها عبارة تلصق صفة سيئة بالمجني عليه أو تشبيهه بحيوان، وقد ترتكب هذه الجريمة بإرسال ملف صوتي أو صورة أو غيرها من الوسائل الإلكترونية الحديثة[٣].

ويتمثل الركن المادي في جريمة سرقة البرامج الإلكترونية لاستعمالها، في قيام الجاني بالاستيلاء على هذه البرامج قبل استعمالها، فالاستعمال لا يمكن تصوره قبل حدوث استيلاء على

---

[١] علي جبار الحسيناوي، المرجع السابق، ص٣٩.

[٢] ناير نبيل عمر، **الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، ٢٠١٢م، ص٧١.

[٣] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص٢٠٦ .

البرنامج، فللقول بوجود الركن المادي لجريمة السرقة لا بد أن يستولي السارق على حيازة الشيء المسروق حتى يتمكن من استعماله[١].

وفي جريمة الولوج والبقاء في نظام المعالجة الآلية للبيانات، يلزم لقيام الركن المادي أن يقوم الجاني بنشاط مادي باستخدام جهاز إلكتروني يؤدي إلى انتهاك نظام الحماية الأمنية التي تضعها المؤسسات أو الإدارات أو الشركات لحماية نظامها الإلكتروني من محاولات العبث بها أو تعديلها أو اتلافها، ويعبر عن إرادته في البقاء داخل هذا النظام[٢].

المطلب الثاني

الركن المعنوي في الجريمة الإلكترونية

الركن المعنوي هو النصف الآخر للجريمة، ويمكن التعبير عنه بأنه الحالة النفسية للجاني وقت ارتكاب جريمته، حيث لا تقوم الجريمة قانوناً بدونه، فلا بد من توافر الإرادة الآثمة لدى الجاني عند إقدامه على السلوك الإجرامي، كما يجب أن تكون الأفعال إرادية، وإلا انتفى الركن المعنوي للجريمة، وأن تكون هذه الأفعال متجه نحو مخالفة القواعد القانونية، ليترتب على مخالفتها الجزاء الجنائي المناسب[٣].

وفي إطار ذلك نص المشرع القطري على الركن المعنوي صراحة في المادة رقم ٣٢ من قانون العقوبات على أن: "يتكون الركن المعنوي للجريمة من العمد أو الخطأ يتوفر الخطأ باتجاه إرادة الجاني إلى ارتكاب فعل أو امتناع عن فعل، بقصد إحداث النتيجة التي يعاقب عليها القانون بسبب خطأ الجاني، سواء كان هذا الخطأ بسبب الإهمال أو عدم الانتباه أو عدم الاحتياط أو الطيش أو الرعونة أو عدم مراعاة القوانين أو اللوائح، ويسأل الجاني عن الجريمة سواء ارتكبها عمداً أم خطأ، ما لم يشترط القانون توفر العمد صراحة"[٤].

---

[١] محمد حمّاد الهيتي، **التكنولوجيا الحديثة والقانون الجنائي**، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠م، ص٢٢٤.

[٢] بلال أمين زين الدين، **جرائم نظم المعالجة الآلية للبيانات**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨م، ص٢٧١.

[٣] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص٢٠١ وما بعدها.

[٤] راجع المادة رقم ٣٢ من قانون العقوبات القطري رقم (١١) لسنة ٢٠٠٤، مشار إليه في موقع الميزان، البوابة القانونية القطرية عبر الرابط التالي: http://www.almeezan.qa/ .

ويجب أن يكون الجاني متمتعاً بإرادة حرة واعية حال ارتكاب جرمه، دون إجبار أو إكراه من أحد، فيكون ارتكب جريمته وهو متمتعاً بحرية الاختيار والتمييز، فلا ينسب السلوك معنوياً لمن لم يكن لديه القدرة على الاختيار أو التمييز ساعة ارتكاب الجريمة، وهذه الإرادة يتبعها تحمل المسئولية القانونية والجزائية عن الأفعال المخالفة للقانون[١].

فالركن المعنوي من العناصر القانونية المكونة للجريمة، وعليها يترتب تكييف الجزاء الجنائي، فالجريمة تكون في أغلب الأحيان قصدية وتتخذ صورة القصد الجنائي، ولكن هناك صور أخرى تسمى الخطأ غير المقصود، وعليه سنبين ذلك عبر الفروع التالية:

الفرع الأول

القصد الإجرامي في الجرائم الإلكترونية

إن أغلب الجرائم الجزائية ترتكب بصورة قصدية، ولذلك فإن القصد الجنائي من أكثر صور الركن المعنوي تصوراً، وهو متمم للركن المعنوي بشكل خاص وللجريمة بشكل عام، ويعتبر القصد عنصر فاصل في تحديد العقوبة، لأن عقوبة الجريمة القصدية تختلف عن عقوبة الجريمة غير القصدية.

ولم يعرف المشرع الفلسطيني القصد الجنائي، وترك هذا الأمر للفقه والقضاء ليقوما بشرحه وتفصيله، حيث اعتبر الفقه أن القصد الجنائي يتكون من عنصرين أساسيين وهما العلم والإرادة، وانقسم الفقه الغربي إلى نظريتين نظرية العلم ونظرية الإرادة، فطبقاً لنظرية العلم يكفي أن تتجه إرادة الجاني إلى السلوك الإجرامي فقط لكي يقوم القصد قانوناً، دون النظر إلى النتيجة الإجرامية فهي من الطبيعي أن تتولد كأثر للسلوك لا دخل لإرادة الإنسان في وقوعها[٢].

أما طبقاً لنظرية الإرادة فالقصد الجنائي يتوفر عندما يريد الجاني السلوك الإجرامي بالإضافة للنتيجة، وهذا على خلاف نظرية العلم التي أراد فيها الجاني السلوك دون النتيجة، والحقيقة أن نظرية الإرادة هي أكثر واقعية من نظرية العلم، فكل المجرمين عند اقترافهم لسلوك

---

[١] أمين محمد نوفل، **قانون العقوبات العام**، كلية الشرطة الفلسطينية، غزة، غير متضمن مكان وسنة النشر،ص٨.

[٢] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص٢٠٤.

معين فهو لابتغاء النتيجة، وليس لمجرد السلوك، ومن خلال هذه النظرية يمكننا التمييز بين القصد الجنائي والخطأ غير المقصود[١].

أما المشرع الأردني فقد عرف النية في قانون العقوبات رقم ١٦ لسنة ١٩٦٠ حيث نص على أن: "النية: هي إرادة ارتكاب الجريمة على ما عرفها القانون"[٢]، وهذا ما أخذ به المشرع الفلسطيني في الضفة الغربية، وكذلك نص المشرع الأردني على أن: " تعد الجريمة مقصودة وإن تجاوزت النتيجة الجرمية الناشئة عن الفعل قصد الفاعل إذا كان قد توقع حصولها فقبل بالمخاطرة.."[٣].

إن القصد الجنائي له دور هام في معرفة طبيعة السلوك المرتكب وماهيته والهدف منه، وتحديد التكييف القانوني للجرائم الإلكترونية، وذلك لمعرفة النص القانوني الواجب تطبيقه، والذي يتناسب مع الجريمة الإلكترونية الواقعة، فأغلب الجرائم الإلكترونية تتم بخطوة أولى وهي الدخول للنظام أو الولوج إليه، ومن ثم ينفذ المجرم الإلكترونية هدفه من وراء الاختراق، فإما أن يكون هدفه سرقة معلومات أو إتلافها أو نسخها أو تزويرها أو أي من الجرائم الإلكترونية الأخرى، فإن لم يثبت الهدف من وراء الاختراق والولوج للنظام نكن بصدد جريمة الدخول الغير مشروع[٤].

وتبرز أهمية القصد الجنائي في التمييز بين جريمة الدخول غير المشروع للأنظمة، وبين جريمة تجاوز الصلاحيات المسموح بها، فالأولى القصد الجنائي فيها واضح وهو أن الدخول للأنظمة في حد ذاته جريمة يعاقب القانون عليها، والقصد فيها هو الدخول للنظام واختراقه والولوج إليه، أما الثانية فيكون المخترق له الصلاحية للدخول للنظام، ولكنه تجاوز صلاحيته وتعدى

---

[١] أحمد فتحي سرور، المرجع السابق، ص٥٣٠، ٥٣١.

[٢] راجع المادة رقم ٦٣ من قانون العقوبات الأردني، وقانون العقوبات المطبق في الضفة الغربية رقم ١٦ لسنة ١٩٦٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي : http://www.lob.gov.jo/ ا.

[٣] راجع المادة رقم ٦٤ من قانون العقوبات الأردني، وقانون العقوبات المطبق في الضفة الغربية رقم ١٦ لسنة ١٩٦٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي: http://www.lob.gov.jo/ ا.

[٤] علي جبار الحسيناوي، المرجع السابق، ص٣٩.

الأماكن المسموح له الدخول فيها[1]، فكلا الحالتين تعتبر جريمة ولكن كل منهما جريمة تختلف عن الأخرى، والقصد الجنائي فيها له دور في تحديد نوع الجريمة.

واكتفى القضاء الأمريكي بالقصد العام في جرائم التهديد مثل جرائم التهديد عبر البريد الإلكتروني، مع عدم ممانعته بالأخذ بالقصد الخاص في ذات الجرائم، وذلك على خلاف المشرع الفرنسي والذي افترض سوء النية واشترط وجود قصد خاص في الجرائم الإلكترونية، فقد اشترط الاعتداء على الحياة الخاصة في الجرائم التي تتعلق بسرية الاتصالات، ومن ذلك البريد الإلكتروني كونه يعد من وسائل الاتصال الحديثة الخاصة[2].

ونرى مما سلف أن أغلب الجرائم الإلكترونية ترتكب بشكل قصدي، وذلك بسبب طبيعة هذه الجرائم، والتي تتطلب علم كافي حول الجهاز الإلكتروني والبيئة الإلكترونية أو معرفة السلوك الإجرامي في حد ذاته، كما أنها غالباً لا ترتكب إلا من خبير أو متخصص أو من لديه علم كافي حول الجريمة التي ارتكبها، فيكون المجرم في أغلب الأحيان ملم بكافة الجوانب الفنية لجريمته، وهو يعمل لتحقيق غايته المنشودة والنتيجة التي ينشدها من بداية جلوسه أمام الحاسب الآلي والبدء في استخدامه، ولكن قد تكون هناك بعض الحلات التي لا يتوافر فيها النية الإجرامية لدى الجاني، كأن يدخل شخص إلى نظام إلكتروني محظور الدخول أو البقاء فيه، وهو يحسب أن الدخول والبقاء فيه مشروع، فهنا لا يتوافر القصد الإجرامي لدى الفاعل لأنه لم يرد النتيجة.

الفرع الثاني

الخطأ غير المقصود في الجرائم الإلكترونية

الخطأ[3] هو أحد صور الركن المعنوي، وهو يمثل الركن المعنوي في الجرائم الغير مقصودة، ونص المشرع الفلسطيني في المادة رقم ١٢ من قانون العقوبات على أن: "١/ كل من

---

[1] خالد ممدوح إبراهيم، **حوكمة الإنترنت**، المرجع السابق، ص ٣٩٣.

[2] علي جبار الحسيناوي، المرجع السابق، ص٣٩.

[3] نصت المادة رقم ٢٤٣ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦على أنه: "كل من أتى فعلاً من الأفعال الآتية بطيش أو إهمال من شأنه أن يعرض حياة إنسان للخطر أو بصورة يحتمل معها أن يلحق ضرراً بشخص آخر، أي: (أ) ساق مركبة أو ركب حيواناً على طريق عام، أو (ب) قاد أو اشترك في قيادة أو تسيير سفينة، أو (ج) ارتكب فعلاً بواسطة النار أو أية مادة أخرى سريعة الالتهاب أو اغفل اتخاذ الحيطة لتلافي كل خطر يحتمل وقوعه من النار أو المواد السريعة الالتهاب الموجودة في حوزته، أو (د) أغفل اتخاذ الحيطة لتلافي=

ارتكب فعلاً أو تركاً وهو يعتقد اعتقاداً صادقاً ومعقولاً بوجود أحوال خاصة وكان مخطئاً في اعتقاده ذلك، لا يكون مسؤولاً جزائياً عن الفعل او الترك الذي ارتكبه إلى درجة تفوق المسؤولية التي تترتب عليه فيما لو كان واقع الحال مطابقاً للأحوال التي اعتقد بوجودها، ٢/ يجوز أن لا يعمل بهذه القاعدة إذا ورد نص صريح أو ضمني يقضي بذلك في التشريع الذي يتعلق بالموضوع "[١].

نستنتج من النص السابق أن المشرع الفلسطيني نص على صورة الخطأ غير المقصود ووضع لها شروط وأحوال معينة، وافترض المشرع الفلسطيني ضمنياً حسن نية مرتكب السلوك بأنه لم يتوقع حدوث النتيجة التي افضى سلوكه إليها، ولذلك لا يتحمل الجاني أي مسئولية جزائية عن الخطأ الذي ارتكبه، إلا إذا اشترط نص صريح أو ضمني إلغاء هذه القاعدة، وأن يتحمل الجاني الجزاء الجنائي على الخطأ الذي ارتكبه.

فالمشرع الفلسطيني لا يقرر المسئولية الجزائية عن الخطأ إلا بنص خاص، وأن يكون الجاني متمتعاً بكامل قواه العقلية، فالجاني هنا أراد السلوك ولكنه لم يرد ولم يتوقع النتيجة.

وكذلك المشرع الأردني حيث نص على صور الخطأ غير المقصود في المادة رقم ٦٤ من قانون العقوبات على أن: " يكون الخطأ إذا نجم الفعل الضار عن الإهمال أو قلة الاحتراز أو عدم مراعاة القوانين والأنظمة"[٢].

إن الخطأ الغير مقصود متصور في الجرائم الإلكترونية، وذلك لما ذكرنا بأن المشرع الفلسطيني والأردني قد نصا صراحة على الخطأ[٣]، وذلك بالرغم من أن الجرائم الإلكترونية يرتكب

=ما قد يحتمل وقوعه من الخطر من حيوان موجود في حوزته، أو (هـ) عالج شخصاً أخذ على نفسه معالجته معالجة طبية أو جراحية، أو (و) صرف أو قدم أو باع أو ناول أي شخص علاجاً أو مادة سامة أو خطرة، أو (ز) ارتكب فعلاً يتعلق بآلات عهد بها إليه كلياً أو جزئياً أو أغفل اتخاذ الحيطة اللازمة لتلافي ما قد ينجم عنها من الأخطار، أو(ح) ارتكب فعلاً يتعلق بمواد مفرقعة موجودة في حيازته أو أغفل اتخاذ الحيطة اللازمة لتلافي ما قد ينجم عنها من الأخطار".

[١] راجع المادة رقم ١٢ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٢] راجع المادة رقم ٦٤ من قانون العقوبات الأردني، وقانون العقوبات المطبق في الضفة الغربية رقم ١٦ لسنة ١٩٦٠ ، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي: http://www.lob.gov.jo/ ا.

[٣] أنظر ما سبق ص ٤٦، ٤٧ .

أغلبها بشكل قصدي، وهذا ما نص عليه المشرعان الأردني والفلسطيني في المواد التي تعاقب على الجرائم الإلكترونية بأن ذكرا لفظ (عمداً أو قصداً).

فالخطأ أو الجهل من المتصور وقوعه في الجرائم الإلكترونية، وهذا يمكننا استنباطه من خلال النصوص العقابية للجرائم الإلكترونية، فعلى سبيل المثال ذكر المشرع الدخول غير المشروع، فإنه يمكن الاحتجاج بالخطأ أو الجهل، فربما يكون الجاني من المستخدمين الجدد للحاسب الآلي وقد دخل نظام وهو لا يعلم بأن الدخول في النظام أو البقاء فيه محظور، أو كان يعتقد بأن الدخول لهذا النظام مباح[١].

ولا تعد جريمة عدم الابلاغ عن انشطة غسيل الأموال المشبوهة أو التقصير في الكشف عنها، وجريمة الإخلال بالإبلاغ عن الأنشطة المصرفية أو البنكية المشبوهة والتي كان من المفترض الإبلاغ عنها، من صور الجرائم العمدية فهي ترتكب عن خطأ وإهمال، ولكنها توقع مسئولية جزائية ومدنية وتأديبية بحق من أهمل أو قصر في أداء واجباته، خاصة من كان في عمل رسمي وكان عليه تحري الحيطة والحظر[٢].

أمثلة على الركن المعنوي في الجرائم الإلكترونية:

يثبت الركن المعنوي في جرائم السرقة التي تقع على الأموال الإلكترونية المعنوية، وذلك من خلال توافر القصد العام، فجريمة السرقة تعد من الجرائم القصدية، والتي ترتكز على العلم والإرادة، بأن يكون الجاني على علم بالفعل الذي يرتكبه وإرادته تتجه نحو هذا الفعل لتحقيق النتيجة الإجرامية التي يبتغيها[٣]، وأجمع الفقهاء على وجود قصد خاص بجانب القصد العام في جريمة السرقة الإلكترونية، والمتمثلة بأن تكون نية الجاني تتجه نحو تملك البيانات أو المعلومات المسروقة، فلو قام شخص بسرقة قرص ممغنط ثم أطلع على محتواه وأرجعه ينتفي لديه القصد في

---

[١] مروان مرزوق الروقي، **القصد الجنائي في الجرائم المعلوماتية**، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، السعودية، ٢٠١١م، ص١٢١.

[٢] المحامي الدكتور يونس عرب، **ورقة عمل بعنوان** "**صور الجرائم الإلكترونية**" ، مقدمة لورشة عمل بعنوان "تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية" هيئة تنظيم الاتصالات / مسقط – سلطنة عمان، ٢-٤ ابريل ٢٠٠٦م ، ص٣٢، مشار إليه عبر موقع منتدى كلية الحقوق لجامعة المنصورة، مصر، عبر الرابط التالي: http://www.flaw.net

[٣] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت**، المرجع السابق، ص١٨٠ .

تملك المال الإلكتروني، وتصبح الجريمة هنا مجرد حيازة، فلا بد من توافر القصد الخاص في نية تملك المال الإلكتروني المسروق[١].

وجريمة الذم من الجرائم العمدية التي يكفي لإثباتها القصد العام، ويتخذ فيها الركن المعنوي صورة القصد الجنائي، بعنصريه العلم والإرادة فيكفي لإثبات ذلك أن يكون الجاني يعلم بالألفاظ التي خرجت منه وأن القانون يعاقب عليها، وإرادته هي من وجهت هذه الأقوال، ويترجم ذلك من خلال إخراج هذه الأقوال على أي شكلاً كانت كتابية أو سمعية أو غيرها عن طريق أي وسيلة من الوسائل الإلكترونية[٢].

وجريمة الإتلاف الإلكتروني من الجرائم القصدية، والتي يعتبر الركن المعنوي فيها هو القصد الجاني، فالقصد الجنائي في جريمة الإتلاف الإلكترونية يتكون من عنصرين العلم والإرادة، فلو قام شخص بإتلاف برامج أو معلومات بشكل عمدي، واتجهت إرادته لهذا الفعل وكان يعلم بأن عمله غير مشروع توافر في حقة القصد الجنائي، على خلاف إذا ما قام بإتلاف برامج أو معلومات كان مطالباً منه ومن الواجب عليه إتلافها، فلا نكن هنا بصدد جريمة الإتلاف الإلكتروني[٣].

ويتوافر الركن المعنوي فيمن يقوم بتزوير بطاقة الائتمان، ذلك لأنه يقوم بتغيير الحقيقة في البطاقة الممغنطة وهو يعلم بجميع اركان التزوير، ويترتب على هذا الفعل ضرراً يلحق بأحد الأفراد أو المجتمع ككل، وهذا هو القصد العام، أما القصد الخاص وهو نية المزور في استعمال بطاقة الائتمان في اغراض غير مشروعة وإجراء عمليات السحب الإلكتروني عن طريقها[٤].

ونرى مما تقدم أن القصد الجنائي مهم في تحديد الجريمة، فإذا لم يثبت وجود القصد في الإتلاف مثلاً، وكان هناك ولوج إلى داخل النظام تترتب جريمة أخرى وهي جريمة الدخول الغير مشروع، ولذلك فإن الركن المعنوي له أهمية بالغة في تحديد نوع الجريمة والتي يترتب عليها الجزاء الجنائي.

---

[١] محمد علي العريان، المرجع السابق، ص ١٤٠ .

[٢] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص٢٠٨ .

[٣] نايل نبيل عمر، المرجع السابق، ص١٠٢.

[٤] كميت طالب البغدادي، **الاستخدام غير المشروع لبطاقات الائتمان**، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨م، ص١٩٦.

المبحث الثاني

المحاولة في الجرائم الإلكترونية

المحاولة الإجرامية هي البدء الفعلي في الجريمة، وهي مرحلة تأتي بعد مرحلة التخطيط والتحضير وقبل تمام الجريمة، فلجاني بدأ في تنفيذ جريمته دون أن يكملها لأسباب خارجة عن إرادته[١]، ونص المشرع الفلسطيني على المحاولة في المادة رقم (١/٣٠) من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ على أنه: "يعتبر الشخص بأنه حاول ارتكاب الجرم إذا ما شرع في تنفيذ نيته على ارتكاب ذلك الجرم باستعمال وسائل تؤدي إلى وقوعه، واظهر نيته هذه بفعل من الأفعال الظاهرة، ولكنه لم يتمكن من تنفيذ نيته إلى حد إيقاع الجرم"[٢]، حيث اشترط المشرع الفلسطيني بدء الجاني في تنفيذ جريمته من خلال إظهار نيته على التصميم لارتكابها وتنفيذ بعض الأفعال المكونة لها دون إتمام النتيجة التي يصبوا إليها، ونص المشرع الفلسطيني على أن المحاولة لا تشمل المخالفات في نص المادة رقم ٢٨ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ على انه: " إن لفظة الجرم الواردة في هذا الفصل لا تشمل المخالفة"[٣] وقصد المشرع بهذا الفصل أي الفصل الذي نص فيه على المحاولة.

وكذلك فقد نص المشرع الأردني على المحاولة بأن عرفها في المادة ٦٨ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠ بأنها: " الشروع: هو البدء في تنفيذ فعل من الأفعال الظاهرة المؤدية الى ارتكاب جناية أو جنحة، فإذا لم يتمكن الفاعل من إتمام الأفعال اللازمة لحصول تلك الجناية أو الجنحة لحيلولة أسباب لا دخل لإرادته فيها..."[٤]، واشترط المشرع الأردني حدوث المحاولة أو الشروع في الجنايات أو الجنح، ونرى أن المشرع الأردني والفلسطيني قد أصابا في ذلك لأن المحاولة لا يمكننا تصور حدوثها في المخالفات، ولأن المخالفات كثير وهي إما أن تقع أو لا تقع، وعليه سنتناول دراسة المحاولة في الجرائم الإلكترونية عبر المطالب الآتية:

---

[١] جلال ثروت، المرجع السابق، ص وما بعدها ١٧٣.

[٢] راجع المادة رقم (١/٣٠) من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٣] راجع المادة رقم ٢٨ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٤] راجع المادة رقم ٦٨ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، وقانون العقوبات المطبق في الضفة الغربية رقم ١٦ لسنة ١٩٦٠ ، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

المطلب الأول : الركن المادي للمحاولة في الجريمة الإلكترونية .

المطلب الثاني : الركن المعنوي للمحاولة في الجريمة الإلكترونية .

المطلب الأول

الركن المادي للمحاولة في الجريمة الإلكترونية

يتمثل الركن المادي للمحاولة في الجريمة الإلكترونية بسلوك معين ينفذه الجاني في العالم الخارجي، فالمشرع لا يعاقب على الأعمال التحضيرية –إلا إذا كانت في حد ذاتها جريمة تامة– أو على الأفكار التي تدور في نفس الجاني، ما لم تتخذ هذه الأفكار سلوكاً يترجم في العالم الخارجي، فيجب أن يكون هناك بدء في تنفيذ الجريمة الإلكترونية للقول بأن هناك محاولة أو شروع، وأن يتم وقف هذا السلوك، وأن يكون الوقف لاإرادي أي لا دخل لإرادة الجاني في إيقاف تنفيذ الجريمة، فالمحاولة الإجرامية تعتبر جريمة ناقصة لعدم اكتمال الركن المادي فيها، والعنصر الذي يجعل الجريمة محاولة هو عدم تحقق النتيجة الإجرامية[1]، وعليه سنوضح ذلك عبر الفروع التالية:

الفرع الأول

البدء في تنفيذ الجريمة الإلكترونية

قبل أن نبدأ في بيان البدء في التنفيذ، هناك مرحلة تسبق ذلك ألا وهي مرحلة التخطيط والتحضير، فيجب علينا التعرف على هذه المرحلة وما لها من آثار تترتب على الجرائم الإلكترونية، وهل يعاقب المشرع عليها أم لا ؟

فالأعمال التحضيرية هي كل ما يسبق البدء في تنفيذ الجريمة الإلكترونية، فتجهيز البرامج أو تجهيز المكونات المادية للحاسب الآلي، أو إدخال شيفرة غير صحيحة فكل ذلك يعتبر أعمال تحضيرية تسبق البدء في التنفيذ، كما أن البدء في التنفيذ يجب أن يكون أحد مكونات السلوك الإجرامي للجريمة، فالدخول إلى نظام غير مصرح به يعد بحد ذاته جريمة تامة، حتى ولو كانت بدءً في تنفيذ جريمة أخرى، وهذا قد يحدث في كثير من الجرائم الإلكترونية، وعليه فإن البدء في

[1] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص١٦٣.

تنفيذ الجريمة الإلكترونية يجب أن يكون بالشروع في أحد سلوكيات الجريمة المرتكبة، أما الاعمال التحضيرية فلا تعد من ضمن سلوكيات الجريمة إلا إذا كانت في حد ذاتها تعد جريمة تامة[١].

وفي التشريع المصري نص المشرع على أنه: " ولا يعتبر شروعاً في الجناية أو الجنحة مجرد العزم على ارتكابها ولا الأعمال التحضيرية لذلك"[٢]، حيث أكد المشرع المصري على ما ذكرناه سابقاً بأن الأعمال التحضيرية لا تدخل ضمن أفعال المحاولة ولا يعاقب عليها القانون.

والبدء في تنفيذ جريمة هو الفاصل بين الأعمال التحضيرية – والتي لا يعاقب عليها القانون– وبين المحاولة في الجريمة، وهنا يتدخل المشرع للعقاب على المحاولة لحماية المصالح التي يحميها القانون، واختلف الفقهاء في وضع معيار واحد ينظم مرحلة البدء في تنفيذ أي جريمة بشكل عام على مذهبين، المذهب الأول وهو المذهب المادي الذي يعتبر أن المحاولة لا تتحقق إلا إذا أتى الجاني بعض الأفعال التي تدخل ضمن المكونات الأساسية للركن المادي للجريمة، أو ما يعرف بالأفعال الخطرة[٣].

أما المذهب الثاني وهو المذهب الشخصي، فلا يهتم بالفعل أو السلوك الذي يحدثه الجاني بل يركز على النية الإجرامية أو الخطورة الإجرامية لدى الجاني، وقد تعددت تعريفات الفقهاء لهذا المعيار، ولكن جميعها تدور حول وجود نية إجرامية لدى الجاني بدون رجعه عن ارتكاب جريمته[٤].

وأخذ المشرع الفلسطيني بالمذهب الشخصي[٥]، على خلاف المشرع الأردني الذي خلط بين المعيارين، بحيث لم يضيق من نطاق المحاولة الإجرامية على غرار المعيار المادي، وكذلك لم

---

[١] نائلة عادل قورة، المرجع السابق، ص٤٧٩ وما بعدها.

[٢] راجع المادة رقم ٤٥ من قانون العقوبات المصري رقم ٩٥ لسنة ٢٠٠٣م، مشار إليه في الموقع الرسمي لوزارة العدل المصرية عبر الرابط التالي:/http://www.arablegalportal.org .

[٣] نظام توفيق المجالي، **شرح قانون العقوبات القسم العام**، الكتاب الأول، مكتبة دار الثقافة للنشر والتوزيع، عمان، ١٩٩٨م، ص٣٠٩.

[٤] محمد صبحي نجم، **قانون العقوبات، القسم العام**، الطبعة الأولى، الإصدار الرابع، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٠م، ص٢٢٥.

[٥] نصت المادة رقم ١/٣٠ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ على أنه: "(١) يعتبر الشخص بأنه حاول ارتكاب الجرم إذا ما شرع في تنفيذ نيته على ارتكاب ذلك الجرم باستعمال وسائل تؤدي إلى وقوعه واظهر نيته هذه بفعل من الأفعال الظاهرة ولكنه لم يتمكن من تنفيذ نيته إلى حد إيقاع الجرم".

يوسع على غرار المعيار الشخصي، فلم يشترط المشرع الأردني أن تكون الأفعال قريبة جداً من الركن المادي للجريمة، ولم يشترط أن تكون الأفعال تؤدي حالاً إلى ارتكاب الجريمة[١].

كما أنه يوجد نوعين من المحاولة وهما المحاولة الناقصة وتسمى الجريمة الموقوفة، والمحاولة التامة وتسمى الجريمة الخائبة، فالمحاولة الناقصة هي التي يَشرع فيها الجاني للبدء في جريمته ولكنه يتوقف لسبب خارج عن إرادته، مثل من يقتحم نظام بنكي ليسرق بيانات أو معلومات تخص حسابات بنكيه، ولكنه يفشل بسبب وجود أنظمة حماية تمنع الجاني من نسخ مثل هذه الملفات والمعلومات، أما المحاولة التامة فهي عندما يشرع الجاني في جريمته ويكملها ولكن لم تتحقق النتيجة الإجرامية التي أرادها، مثل من يخترق نظام بنكي بهدف سرقة حسابات بنكية لعملاء ولكن بعد تمام الجريمة يكتشف الجاني أنه سرق بيانات لا علاقة لها بحسابات العملاء[٢].

ومن الأمثلة على المحاولة التامة كأن يقوم شخص بوضع بطاقة الصراف الآلي في الجهاز، ويقوم بوضع الأرقام الخاصة بالبطاقة، ولكن يصيب الجهاز عطل مفاجئ فنسمي هذه الحالة بالمحاولة التامة، أما المحاولة الناقصة فمثل أن يضع الشخص بطاقة الصراف الآلي في الجهاز وينقطع التيار الكهربائي فهنا تكون محاولة ناقصة[٣].

ونرى مما سلف أن البدء في التنفيذ متصور في الجرائم الإلكترونية، وذلك بإتيان الأعمال والسلوكيات التي تكّون الركن المادي للجريمة الإلكترونية، وقد يسبق هذه السلوكيات أعمال تحضيرية، مثل تجهيز الحاسب الآلي والبرامج وتوصيلة بالإنترنت، ولكن قد تكون بعض الأعمال التحضيرية جريمة تامة في حد ذاتها تمهد لارتكاب جريمة أخرى، مثل جريمة الدخول غير المشروع في جريمة محاولة سرقة الحسابات البنكية، ومن مظاهر البدء في التنفيذ إدخال بطاقة الائتمان داخل جهاز الصراف الآلي من قبل سارقها أو مزورها، ليقوم بعملية السحب ولكنه يفشل لعطل في الجهاز أو لخطأ في الكود السري أو لانقطاع التيار الكهربائي، فيعد إدخال البطاقة في الصراف الآلي أول مظاهر البدء في التنفيذ[٤].

---

[١] نظام توفيق المجالي، المرجع السابق، ص٣١٣.

[٢] جلال ثروت، المرجع السابق، ص١٧٥.

[٣] نائلة عادل قورة، المرجع السابق، ص٤٧٩، ٤٨٠.

[٤] جميل عبد الباقي الصغير، **الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة**، دار النهضة العربية، القاهرة، ٢٠٠٣م، ص١٠٥.

وأهتم المشرع الفرنسي بمسألة المحاولة في الجرائم الإلكترونية، فقد نص في القانون العقوبات رقم ١٩ لسنة ١٩٨٨ على المحاولة في الجرائم الإلكترونية، وعاقب على الشروع فيها بنفس عقوبة الجريمة التامة، فالمحاولة في جرائم الدخول إلى الأنظمة بطرق احتيالية أو جريمة محو أو نسخ أو اتلاف البيانات فكل ذلك يعاقب عليه المشرع الجزائي الفرنسي، وذلك رغبة منه في حماية المصالح المعتدى عليها[١].

ويتحقق الشروع في الجرائم الإلكترونية من خلال تحضير الأجهزة والبرامج تمهيداً لاختراق موقع معين، أو تحضير الرسائل وكتابتها على الإيميل أو على جهاز إلكتروني تمهيداً لإرسالها لأشخاص معينين بهدف ذمهم أو ابتزازهم أو تهديدهم، أو العمل على تجهيز موقع عبر الإنترنت ليروج للمخدرات أو للإتجار بالجنس البشري أو للعب القمار أو لغسيل الأموال، فكل ما ذكرناه يعد من الخطوات الأولى للبدء في تنفيذ الجرائم الإلكترونية[٢].

وخلاصة القول إن المحاولة في الجرائم الإلكترونية هو أمر واقعي ومن المحتمل أن يحدث، وقد نص المشرع الفلسطيني في مشروع قانون العقوبات على أن: "يعاقب على الشروع في الجرائم المنصوص عليها في هذا الفصل بنصف العقوبة المقررة للجريمة التامة "[٣]، فقد استدرك المشرع الفلسطيني خطورة الأمر، وحتى لا يدع مجالاً للجناة للإفلات من العقاب فنص على المحاولة في الجرائم الإلكترونية وقرر العقاب عليها بنصف عقوبة الجريمة التامة.

الفرع الثاني

الوقف اللاإرادي لتنفيذ الجريمة الإلكترونية

الوقف اللاإرادي لتنفيذ الجريمة هو أحد اركان المحاولة الإجرامية، فلكي يكتمل الركن المادي للمحاولة الإجرامية لا بد للجاني بالبدء في تنفيذ جريمته على النحو الذي ذكرناه في الفرع السابق، ومن ثم يجب أن يلي البدء في التنفيذ وقف لا إرادي، بمعنى أن يتم إيقاف تنفيذ الجريمة لأسباب لا دخل لإرادة الجاني فيها[٤].

---

[١] هدى حامد قشقوش، المرجع السابق، ص١٢٩.

[٢] مروان مرزوق الروقي، المرجع السابق، ص١٠٧، ١٠٨.

[٣] راجع المادة رقم ٥٧٧ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٤] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت**، المرجع السابق، ص٤٦ وما بعدها .

ولذلك يجب للقول بوجود محاولة إجرامية عدم تمام الجريمة التي كان الجاني يقصد ارتكابها، وأن يكون عدم تمامها لأسباب خارجة عن إرادة الجاني، فالجاني تتكشف مدى خطورته الإجرامية من خلال فشلة في إتمام جريمته، فهو بذل كل جهده لتمام جريمته ولولا وجود تدخل خارج عن إرادته لتحققت جريمته، وفي ذلك فقد شدد المشرع الاسباني في العقاب على المحاولة التامة وجعل عقوبتها اشد من عقوبة المحاولة الناقصة[١].

ولا يكفي للقول بوجود محاولة إجرامية أن يأتي الفاعل بعض الأفعال التي تؤدي إلى جريمته أو يظهر نيته من خلال هذه الأفعال، فلا بد أن تتوقف السلوكيات التي تؤدي إلي إتمام الجريمة، وأن يكون هذا الوقف لا دخل لإرادة الجاني فيه، ويتضح ذلك بعدم تحقق النتيجة الإجرامية للجاني جزئيه كانت أم كليه، وهذا الفصل ما بين الجريمة التامة والمحاولة الإجرامية[٢].

ومن صور الوقف اللاإرادي في الجرائم الإلكترونية محاولة دخول الجاني إلى نظام إلكتروني بهدف الوصول إلى البيانات والمعلومات المخزنة في النظام، ولكنه يفشل في ذلك بسبب وضع صاحب النظام برامج حماية ضد الاختراق والنسخ، أو أن يصاب الجاني بالأغماء بعد أن يبدأ في تنفيذ جريمته، وتتوافر المحاولة الإجرامية في حق من تحايل باستخدام بطاقة صراف آلي مزورة لسحب مبالغ مالية من حساب صديقة ولكنه أكتشف بعد دخوله للحساب أنه خالي من أي مبالغ نقدية، فتعتبر هذه الحالة محاولة إجرامية مكتملة الأركان وذلك لأن ما منعه من تحقيق نتيجته الإجرامية هو بسبب عدم وجود مال ليسرقه، وهذا السبب لا دخل لإرادة الجاني فيه، فلو وجد مال لسرقه دون تردد[٣].

ويجب التمييز بين المحاولة التي يعاقب عليها القانون والمحاولة التي لا يعاقب عليها القانون، فالمحاولة التي يعاقب عليها القانون هي التي ذكرناها فيما سلف، أما المحاولة التي لا يعاقب عليها القانون فهي عندما يبدأ الجاني في تنفيذ جريمته ثم يعدل عنها إرادياً، فمعنى ذلك أن

---

[١] مبارك عبد العزيز النوبيت، **نظرية الشروع في الجريمة**، العدد الثاني، الطبعة الأولى، مجلة الحقوق والشريعة، الكويت، ١٩٧٨م، ص٤٥ وما بعدها.

[٢] فخري عبد الرازق الحديثي، خالد حميدي الزعبي، **شرح قانون العقوبات، القسم العام**، الموسوعة الجنائية١، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠م، ص١١٦.

[٣] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص١٧٥ وما بعدها.

الجاني قد قطع شوطاً في أفعال جريمته، ولكنه عدل عنها اختيارياً، أي إنه كان قادراً على إتمام جريمته، ولكنه تراجع عن ذلك لأسباب تكمن في نفسه، دون أي تدخل خارجي[١].

ونص الأردني على أن: "وكل من شرع في فعل ورجع باختياره عن أفعال الجرم الإجرامية لا يعاقب إلا على الفعل أو الأفعال التي اقترفها إذا كانت تشكل في حد ذاتها جريمة"[٢] ومثال ذلك في محاولة سرقة بيانات أو معلومات من نظام معين، فقيام الجاني بالولوج لنظام بطريقة غير مشروعة للوصول إلى البيانات المراد سرقتها ومن ثم يعدل الجاني اختيارياً عن سرقة البيانات مع قدرته على سرقتها، فقد لا يعاقب الجاني على محاولة سرقة البيانات الإلكترونية ولكنه يعاقب على جريمة الدخول غير المشروع للنظام الإلكتروني وهي جريمة مستقلة في حد ذاتها..

وكذلك يجب التمييز بين العدول في المحاولة التامة والعدول في المحاولة الناقصة، فالعدول في المحاولة الناقصة لا يعاقب عليه المشرع الجزائي، والحكمة من ذلك هو تشجيع من يرتكب سلوكاً إجرامياً على التوبة والعدول عن جرمه، فلو كان هناك عقاب على المحاولة الناقصة لقام الجاني بفعلته دون تردد، ومع ذلك قد تكّون بعض السلوكيات المرتبطة بالمحاولة جريمة تامة ومستقلة في حد ذاتها، ومثال ذلك إذا توقف الجاني من محو البيانات والمعلومات من جهاز المجني عليه، أما العدول في المحاولة التامة فإن الجاني قد ارتكب جميع الافعال المكونة لجريمته، ولكنه عدل بعد ذلك مما حال دون تحقق النتيجة، ففي هذه الحالة لا يمكن للمشرع أن يعفي الجاني من أفعاله، خاصة وإنه قد ارتكبها تامة، ولكن عدول الجاني في هذه الحالة قد يعطيه ظرف مخفف عند إيقاع العقاب عليه، وهذا ما يتطابق مع روح القانون وما يرغبه المجتمع ويقدره القضاء، ومثال ذلك من يقوم بحذف صور إباحية من موقعة الإلكتروني بعد عرضها[٣].

ويكون عدول الجاني مختلطاً، عند وجود عوامل خارجية اضطرت الجاني للعدول عن جريمته، وكذلك عدل الجاني عن جرمه من تلقاء نفسه، ومثال ذلك عند قيام شخص بالسحب من بطاقة صراف آلي مزورة ولكنه يتوقف لمشاهدته شخص يحسبه شرطي، وأختلف الفقهاء في هذه الحالة، فمنهم من قال بأن العدول اختيارياً على اعتبار أنه لا عبرة بالبواعث قانوناً والتي أثرت في

---

[١] محمد صبحي نجم، **قانون العقوبات**، المرجع السابق، ص٢٣٢.

[٢] راجع المادة رقم ٩٥ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، وقانون العقوبات المطبق في الضفة الغربية رقم ١٦ لسنة ١٩٦٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ui/main.html.

[٣] نظام توفيق المجالي، المرجع السابق، ص٣٢٢ وما بعدها.

نفس الجاني، ويؤخذ على هذا الرأي أن الجاني لولا وجود أسباب خارجيه لما تراجع عن جريمته، أما الجانب الآخر من الفقه فقد رأى بوجوب الموازنة في هذه الحالة، بمعنى إذا كان الجانب الإرادي هو الغالب كان العدول إرادياً، أما إذا كانت الأسباب الخارجية هي الغالبة كان العدول اضطرارياً، ويؤخذ على هذا الرأي كذلك صعوبة تحديد معيار ليوازي بين الأسباب الإرادية والاضطرارية[١].

ونرى مما سلف أن العدول الاضطراري هو الأقرب، فلو نظرنا إلى نفس الجاني لعلمنا يقيناً أن الجاني لو لم تدخل عليه الظروف الخارجية لاستكمل أفعال جريمته دون تردد أو رجعه، فالجاني قد بدء في ارتكاب جريمته وأظهر النية على ذلك، ولكن دخل عليه أمر لم يكن بالحسبان جعله يتراجع عن جريمته، ومثال ذلك من قام بوضع بطاقة صراف آلي في جهاز الصراف بهدف سرقة أموال من حساب صاحب البطاقة، وبعد أن يدخل الحساب يكتشف أنه خالي من أي مبالغ نقدية، فعدولة هنا اضطرارياً لأنه لم يجد شيء يسرقه، بينما لو وجد مال وعدل عن السرقة، فيعتبر عدولة هنا اختيارياً[٢].

أما المشرع الفلسطيني فيعاقب على العدول الاختياري في كل الأحوال فقد نص على أنه: "(٢) لا عبرة، إلا فيما يتعلق بالعقوبة، سواء أقام ذلك الشخص بكل ما هو ضروري لإتمام ارتكاب الجرم أم لم يقم بذلك، وسواء أحالت دون تنفيذ نيته بتمامها ظروف لم يكن فيها مختاراً أم عدل من تلقاء نفسه عن متابعة تنفيذ نيته"[٣].

المطلب الثاني

الركن المعنوي للمحاولة في الجريمة الإلكترونية

يتمثل الركن المعنوي للمحاولة في الجريمة الإلكترونية في صورة القصد الجنائي، والتي لا تختلف البتة عن صورة القصد الجنائي في الجريمة التامة، فالاختلاف ما بين الجريمة التامة والمحاولة الإجرامية يكمن في الوقائع المادية فقط، دون اختلاف بين الحالتين في الركن المعنوي، فالجاني في كلا الحالتين تتجه إرادته نحو جميع العناصر المادية التي تتألف منها جريمته، أما إذا

---

[١] مبارك عبد العزيز النوبيت، المرجع السابق، ص٥١، ٥٢.

[٢] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص١٧٦.

[٣] راجع المادة رقم ٣٠/٢ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

كانت إرادة الجاني تتجه صوب المحاولة فقط فلا يعاقب على المحاولة في هذه الحالة، ولكنه يعاقب على الأفعال التي ارتكبها وهي تمثل جريمة في حد ذاتها[١].

فالواقع أن القصد الجنائي في الجريمة التامة لا يختلف عن القصد الجنائي في المحاولة الإجرامية، حيث أن الجاني في كلا الحالتين عقد العزم على ارتكاب جريمته، وتجاوز في ذلك مرحلة التفكير والتخطيط، وبدء بالفعل في السلوكيات التي يتكون منها الركن المادي للجريمة، إلا أن الجريمة لم تكتمل لوجود ظروف خارجيه لا دخل لإرادة الجاني فيها تسببت في عدم تحقق النتيجة الإجرامية، وهذا هو الفصل ما بين المحاولة الإجرامية والجريمة التامة[٢].

وفي إطار ذلك نص المشرع الكويتي في المادة رقم ٤٥ من قانون العقوبات على أن: " الشروع في جريمة هو ارتكاب فعل بقصد تنفيذها، إذا لم يستطع الفاعل لأسباب لا دخل لإرادته فيها إتمام الجريمة، ولا يعد شروعا في الجريمة مجرد التفكير فيها، أو التصميم على ارتكابها"[٣].

وتبرز أهمية القصد الجنائي للمحاولة في الجرائم الإلكترونية أن الجاني إذا دخل نظام إلكترونية معين لا يعني أنه حاول ارتكاب جريمة الاحتيال المعلوماتي أو شرع فيها، فلا بد أن تتجه إرادة الجاني إلى ارتكاب هذه الجريمة، ولكن يسأل في الوقت عينه عن جريمة دخول نظام غير مصرح به أو جريمة الإتلاف الإلكتروني متى توافرت أركان هذه الجرائم، كما أنه إذا ترتب على دخول الشخص إلى نظام إلكتروني تغيير في بعض البيانات أدى إلى عملاً احتيالياً فإنه لا يسأل عن الاحتيال المعلوماتي طالما لم تتجه إرادته إلى ارتكاب هذه الجريمة، ولكنه يسأل كذلك عن أي جريمة أخرى تتوافر اركانها[٤].

الجريمة الإلكترونية والجريمة المستحيلة:

الجريمة المستحيلة هي الجريمة التي استنفذ الجاني فيها كل سلوكه الإجرامي ليحقق نتيجته الإجرامية التي يعاقب عليها القانون دون وقوعها، وذلك لاستحالة وقوعها في الظروف التي حدثت

---

[١] جلال ثروت، المرجع السابق، ص١٨٣، فخري عبد الرازق الحديثي، خالد حميدي الزعبي، **شرح قانون العقوبات، العقوبات**، المرجع السابق، ص١١٥.

[٢] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص١٨١.

[٣] راجع المادة رقم ٤٥ من قانون الجزاء الكويتي رقم ١٦ لسنة ١٩٦٠م، مشار إليها في موقع منتدى كلية الحقوق لجامعة المنصورة، مصر، عبر الرابط التالي: http://www.f-law.net/law/ .

[٤] نائلة عادل قورة، المرجع السابق، ص٤٨٦، ٤٨٧.

فيها، فالجريمة المستحيلة تشبه المحاولة التامة في أن الجاني قد استنفذ كل أفعالة الإجرامية للوصول إلى النتيجة التي يهدف لها، ولكن الاختلاف بينهما في أن المحاولة التامة لم تحدث فيها النتيجة الإجرامية لتدخل اسباب خارجية حالت دون وقوعها، أما الجريمة المستحيلة فإن النتيجة الإجرامية من المستحيل أن تقع بأي شكل من الأشكال[١].

وأختلف الفقه في موضوع الجريمة المستحيلة على عدة نظريات، ولكن المشرع الفلسطيني عاقب على الجريمة المستحيلة وأعتبرها محاولة إجرامية حيث نص في المادة رقم ٣/٣٠ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ على أنه: " لا عبرة فيما إذا لم يكن في الإمكان ارتكاب الجرم بالفعل بسبب ظروف كان يجهلها المجرم"[٢]، وكذلك اعتبر المشرع الأردني الجريمة المستحيلة صورة من صور المحاولة[٣].

ومثال الجرائم الإلكترونية المستحيلة قيام شخص بوضع بطاقة الصرف الآلي المسروقة في جهاز الصراف الآلي، ولكن الجهاز يرفض سحب المال وذلك لعدم صلاحية البطاقة، فلولا عدم صلاحية البطاقة لقام الجاني بسحب الأموال من جهاز الصراف الآلي وحقق نتيجته الإجرامية، ومثال آخر وهو أن تكون بطاقة الصراف الآلي صالحة للسحب، ولكن لم يكن هناك مال في حساب صاحب البطاقة المسروقة، أو استخدام الجاني شيفرة خاطئة لاختراق نظام معين، فهذه الوقائع استحال تحقيق النتيجة الإجرامية لأسباب تتعلق بالوقائع المادية للجريمة، ترتب عليها توافر أركان المحاولة الإجرامية التي تستلزم العقاب عليها[٤].

وخلاصة القول إن الجريمة الإلكترونية تقبل المحاولة كما ذكرنا، وأن الجريمة المستحيلة ما هي إلا صورة من صور المحاولة الإجرامية، ولذلك فقد عاقب المشرع الفلسطيني والأردني عليها، وذلك لوصول الجاني إلى درجة التصميم على بلوغ الهدف، فلو لم يعاقب المشرع على المحاولة لعاد الجاني لارتكاب جريمته مرة أخرى، ولربما أخذ التدابير اللازم لكي لا تفشل جريمته في المرة الثانية، والجرائم الإلكترونية تعد من الجرائم التي تقبل المحاولة، ولكن في الواقع ربما الكثير من الأشخاص الذين يتعرضون لمحاولات اختراق أجهزتهم أو محاولات لسرقة معلوماتهم أو بياناتهم الشخصية، قد لا يتقدموا بشكاوي أو تبليغات ضد من حاول اختراق أجهزتهم أو سرقة بياناتهم،

---

[١] نظام توفيق المجالي، المرجع السابق، ص٣٣٤.

[٢] راجع المادة رقم (٣/٣٠) من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦.

[٣] فخري عبد الرازق الحديثي، خالد حميدي الزعبي، **شرح قانون العقوبات**، المرجع السابق، ص١٢٨.

[٤] نائلة عادل قورة، المرجع السابق، ص٤٨٦.

ولذلك يجب على كل من يتعرض لاعتداء إلكتروني سواء نجح الاعتداء عليه أو فشل، أن يتقدم بشكاوى إلى الجهات المختصة ضد من حاول الاعتداء على خصوصياتهم الإلكترونية، لكي يحاسب كل مجرم على ما يرتكبه من جرم ويأخذ الجزاء الجنائي المناسب.

المبحث الثالث

الجزاء الجنائي للجرائم الإلكترونية

إن الجزاء الجنائي من أقوى الوسائل التي تكافح الجرائم الجنائية، وقد تطورت أنواع الجزاء الجنائي على مر العصور، وأصبح المشرع الحديث يبحث عن التدابير الوقائية التي تمنع حدوث الجريمة قبل وقوعها، إلى أن تطور التشريع وأصبح يؤدي مهمته على الوجه الصحيح بجعل الجزاء الجنائي هو عملية إعادة تأهيل وإصلاح للمجرمين[١]، وفرض الجزاء الجنائي على الجناة لأهداف عديدة منها تحقيق العدالة والمساواة أمام القانون، وتعويض من لحقه ضرر جراء جرم معين، والردع العام والذي يعد من أهم أهداف الجزاء الجنائي والذي يعمل على الحفاظ على أمن المجتمع من زيادة عدد الجرائم، وكذلك الردع الخاص الذي يمنع الجاني من العودة إلى مستنقع الجريمة، مع العمل على إصلاح وتأهيل الجناة لإعادة دمجهم في المجتمع من جديد[٢].

ولا يترتب الجزاء الجنائي إلا على جريمة جزائية، وتعرف الجريمة الجزائية بأنها: "كل فعل أو امتناع يصدر عن شخص مسؤول قرر له القانون عقاباً"[٣]، ولكن في العصر الحديث ظهر نوع ثاني للجزاء الجنائي وهو ما يسمى التدابير الاحترازية أو الوقائية والعلاجية، وتعتبر التدابير الاحترازية هي مجموعة الإجراءات التي تتخذها السلطة القضائية وتطبقها على الجناة بهدف نزع الروح الإجرامية من داخلهم، وإعادة تأهيلهم للحيلولة بينهم وبين ارتكابهم الجرائم، والعمل على دمجهم من جديد في المجتمع، وتتخذ صور التدابير الاحترازية على عدة أشكال منها تدابير سالبة للحرية كعلاج الجناة في المستشفيات النفسية أو وضعهم في أماكن العلاج من الإدمان على

---

[١] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، الطبعة الثانية، عدد كفر كنا، مكتبة أفاق، غزة، ٢٠١٣م، ص٧٠٨ وما بعدها.

[٢] حسن محمد ربيع، **شرح قانون العقوبات الاتحادي**، القسم العام، الجزء الثاني، الطبعة الثانية، أكاديمية شرطة دبي، ١٩٩٣م، ص٣٣ وما بعدها.

[٣] نائل عبد الرحمن صالح، **محاضرات في قانون العقوبات القسم العام**، الجامعة الأردنية، الطبعة الأولى، دار الفكر للنشر والتوزيع، عمان، ١٩٩٥م، ص٣٥.

المخدرات، وهناك تدابير مقيدة للحرية مثل منع الجاني من التردد على أماكن معينة، وكذلك التدابير المانعة من الحقوق مثل المنع من سياقة السيارة، وهناك تدابير عينية مثل مصادرة الأجهزة الإلكترونية والهواتف الخلوية[١].

ومن المبادئ المستقرة في كافة التشريعات مبدأ شرعية العقوبة، حيث نص في ذلك القانون الفلسطيني بأنه: " لا جريمة ولا عقوبة إلا بنص قانوني"[٢]، وكذلك فقد نص المشرع الأردني على أن: "لا يقضى بأية عقوبة لم ينص القانون عليها حين اقتراف الجريمة"[٣]، وعليه فإن القانون الأساسي الفلسطيني وكذلك مشروع قانون العقوبات والقانون الأردني قد أكدا على حماية أفراد المجتمع من عدم إيقاع أي عقوبة عليهم لم ينص عليها القانون.

وعلى ضوء ما ذكرنا سنشرح الجزاء الجنائي للجرائم الإلكترونية في القانون الفلسطيني والقانون الأردني في مطلبين منفصلين على نحو ما هو تال:-

المطلب الأول : الجزاء الجنائي للجرائم الإلكترونية في القانون الفلسطيني.

المطلب الثاني : الجزاء الجنائي للجرائم الإلكترونية في القانون الأردني.

المطلب الأول

الجزاء الجنائي للجرائم الإلكترونية في القانون الفلسطيني

إن الجرائم الإلكترونية من الجرائم الحديثة التي دخلت على المجتمع الفلسطيني، والتي لم نكن نشهدها من قبل، فأصبحت هذه الجرائم تقلق أفراد المجتمع، لصعوبة محاسبة الجناة عليها وفرض الجزاء الجنائي المناسب لكل مجرم، وعليه سنشرح الجزاء الجنائي للجرائم الإلكترونية في ضوء قانون العقوبات رقم ٧٤ لسنة ١٩٣٦، ومشروع قانون العقوبات لسنة ٢٠١٠م، عبر الفرعين التاليين:

---

[١] محمد صبحي نجم، **المدخل إلى علم الإجرام وعلم العقاب**، الجامعة الأردنية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ١٩٩٨م، ص٩٧ وما بعدها.

[٢] راجع المادة ١٥ من القانون الأساسي الفلسطيني المعدل لسنة٢٠٠٥ م، و المادة١ في مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٣] راجع المادة رقم ٦٥ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ui/main.html.

الفرع الأول

الجزاء الجنائي للجرائم الإلكترونية في قانون العقوبات رقم ٧٤ لسنة ١٩٣٦م

لم يكن القانون الفلسطيني يعاقب على الجرائم الإلكترونية قبل تاريخ ٢٠٠٩/٦/٢٥م، وذلك لقصور من المشرع وفراغ تشريعي ولحداثة هذه الجرائم على الساحة الفلسطيني، وبعد ذلك التاريخ استحدث المشرع المادة ٢٦٢ مكرر وتم نشرها في الوقائع الفلسطينية بتاريخ ٢٠٠٩/٦/٢٥م، وكان إقرار هذه المادة اعتراف صريح من المشرع الفلسطيني بأن هذه الجرائم قد ظهرت بشكل ملحوظ على الساحة الفلسطينية، وأنها بدأت تشكل خطراً على المجتمع، وتناولت هذه المادة مجموعة من الجرائم وتضمنت العقوبات عليها، وكذلك التدابير الاحترازية التي تشملها[١].

أولاً: جرائم الاعتداء على الحياة الخاصة والجرائم الإباحية:

وفرت البيئة الإلكترونية حياة خاصة للأفراد، وقد تتعرض هذه الحياة لاعتداء من قبل آخرين، ويظهر الركن المادي في هذه الجريمة من خلال سلوك الجاني بتمام ولوجه إلى النظام الإلكتروني وينتهي بتمام فعله، أما الركن المعنوي فيتمثل في قصد الجاني والذي يأخذ عدة صور فقد يكون قصده الاطلاع المجرد أو الاطلاع بقصد الإفشاء أو الاطلاع بقصد التهديد والابتزاز[٢].

ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسلوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة الآداب العامة، ويقوم بنشرها عبر الإنترنت، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإرادة على ذلك[٣].

ونص المشرع الفلسطيني في الفقرة ١ من المادة ٢٦٢ مكرر على الجرائم التي تمس حرمة الحياة الخاصة، وعدد المشرع عدة أشكال لهذه الجرائم، ومنها جرائم التنصت على الأخرين كتسجيل صوت أو فيديو أو رسالة أو صورة أو التقاط أو نسخ أي معلومات إلكترونية، وكذلك يعتبر اعتداء على حرمة الحياة الخاصة إذا قام الجاني بنشر أو ترويج لما ذكر بدون علم أو رضا صاحب الشأن، ونص المشرع في هذه المادة على الجرائم الإباحية، والتي تتعلق بنشر أو ترويج أو

---

[١] راجع المادة ٢٦٢ مكرر، من المادة ٣ في الوقائع الفلسطينية، العدد الخامس والسبعون، ص٣١.

[٢] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٢٢٨وما بعدها.

[٣] خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، المرجع السابق، ص٢٩٧.

نسخ أو طباعة المواد الإباحية، وجرائم السب بالألفاظ البذيئة التي تخدش الحياة أو كان فيها تحريض على الفسق والفجور، فكل من يرتكب هذه الجرائم يعاقب بالحبس مدة لا تزيد عن سنة، أما التدابير الاحترازية الأخرى فقد نص المشرع في الفقرة رقم ٢على إعدام أو إتلاف كل المواد المضبوطة في الجرائم التي ذكرناها، ومصادرة الاجهزة المستخدمة في الجريمة مثل الحاسب الآلي أو اللاب توب أو الهاتف المحمول[١].

ثانياً: جرائم دخول الأنظمة بوجه غير مشروع:

تتطلب هذه الجريمة وجود ركن مادي ومعنوي، ويتمثل الركن المادي بفعل الدخول الذي يطلق عليه الدخول المنطقي، وذلك بغرض فتح باب يؤدي إلى نظام الكمبيوتر بمكوناته المنطقية، أما الركن المعنوي فيتمثل بالقصد الجنائي كون هذه الجريمة من الجرائم العمدية فيجب توافر العلم والإرادة للجاني عند دخوله الغير مصرح به للنظام[٢]. كما ويجب أن يكون النظام الذي تم اختراقه غير متاح للجمهور ولا يمكن الدخول فيه إلا لأشخاص معينين حتى تتوافر أركان الجريمة[٣].

---

[١] نصت المادة ٢٦٢ مكرر من قانون العقوبات رقم ٧٤ لسنة ١٩٣٦ المعدل لسنة ٢٠١٠م على أن: "١- كل من:
أ- استرق السمع أو سجل أو نسخ أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه حديثاً خاصاً جرى في أحد الأماكن، أو عن طريق الهاتف بدون رضاء صاحب الشأن.
ب- التقط أو نقل أو نسخ أو أرسل بأي جهاز من الأجهزة صورة شخص في مكان خاص، فإذا صدرت الأفعال المذكورة أثناء اجتماع على مسمع ومرأى الأشخاص الذين يهمهم الأمر الحاضرين في ذلك الاجتماع فان رضاءهم يكون مفترضاً ما لم يبدوا اعتراضهم على الفعل.
ج- أساء عمداً استعمال أجهزة الخطوط الهاتفية أو الإنترنت أو أية وسيلة تكنولوجية أخرى بأن روج أو نقل أو طبع أو نسخ أية مواد إباحية، أو أزعج الغير، أو وجه إليهم ألفاظاً بذيئة أو مخلة بالحياء، أو تضمن حديثه معهم تحريضاً على الفسق والفجور.
د- أذاع أو نشر أو طبع أو نسخ أو استعمل ولو في غير علانية، تسجيلاً أو صورة أو مستنداً متحصلاً عليه بإحدى الطرق المبينة في البنود (أ،ب،ج) من هذه المادة وكان ذلك بدون رضاء صاحب الشأن.
يعتبر أنه اعتدى على حرمة الحياة الخاصة لأحد الأشخاص يعاقب بالحبس مدة لا تزيد على سنة.
٢- يحكم في جميع الأحوال المنصوص عليها في الفقرة (١) من هذه المادة بما يلي:
أ- محو التسجيلات المتحصلة عن الجريمة أو إعدامها.
ب- مصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها."

[٢] خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، المرجع السابق، ص٢٤٢ وما بعدها.

[٣] عبد الفتاح بيومي حجازي، المرجع السابق، ص٢٨.

ونص المشرع في الفقرة الثالثة من نفس المادة على جرائم اختراق الأنظمة والبقاء فيها بوجه غير مشروع، وحدد العقوبة الخاصة بهذه الجريمة بالحبس لمدة لا تزيد عن سنة وغرامة لا تتجاوز ألف دينار أردني أو أحدى هاتين العقوبتين، حيث نص قانون العقوبات على أنه: "٣- كل من اقتحم نظاماً لمعلومات حاسوب خاص بالغير أو بقي فيه دون وجه مشروع، يعاقب بالحبس مدة لا تزيد على سنة، وبغرامة لا تتجاوز ألف دينار أو بإحدى هاتين العقوبتين..."[١].

ثالثاً: جرائم أنظمة المعلومات:

يُقصد بها هنا جرائم نظم ووسائل وشبكات المعلومات أي الجرائم التي تقع على المكونات المعنوية للحاسب الآلي من بيانات ومعلومات، مثل اختراق الحاسب الآلي أو الشبكات إما مجرداً، أو بهدف ارتكاب جريمة أخرى مثل تخريب المعطيات والأنظمة، أو خلق البرامج الضارة التي تنقل عبر الحاسب الآلي والشبكات وغيرها من الجرائم[٢].

ونص المشرع في الفقرة الثالثة على جرائم تعطيل الأنظمة أو محوها أو تعديلها، وحدد عقوبتها بالحبس وغرامة لا تتجاوز ثلاثة آلاف دينار أو أحدى هاتين العقوبتين، ونص المشرع في ذلك على أن: "....وإذا نتج عن ذلك تعطيل تشغيل النظام أو محو المعلومات التي يحتوي عليها أو تعديلها، تكون العقوبة الحبس، وبغرامة لا تتجاوز ثلاثة آلاف دينار، أو بإحدى هاتين العقوبتين"[٣].

وفي فرنسا حكم القضاء الفرنسي بإدانة متهم قام بإدخال فيروس على أسطوانات أعلانية، تحتوي على برنامج يريد الترويج له، مما أدى إلى نقل هذا الفيروس إلى بعض الأجهزة، الأمر الذي أدى إلى إتلاف المعلومات في هذه الأجهزة[٤].

رابعاً: عقوبة المحاولة في الجرائم الإلكترونية:

لم تنص المادة ٢٦٢مكرر على المحاولة في الجرائم الإلكترونية، ولذلك فعند وقوع محاولة في إحدى الجرائم التي ذكرناها نرجع إلى الأصل العام في قانون العقوبات، وذلك للمادة رقم ٢٩ حيث نصت على أن: "كل من حاول ارتكاب جرم يعاقب بالعقوبات التالية إلا في المواضع التي

---

[١] راجع المادة رقم ٢٦٢/٣ مكرر من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ المعدل لسنة ٢٠١٠م.

[٢] جمال محمد غيطاس، المرجع السابق، ص٢١٢.

[٣] راجع المادة رقم ٢٦٢/٣ مكرر من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ المعدل لسنة ٢٠١٠م.

[٤] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٦٢.

نص فيها هذا القانون على عقوبة خاصة:.....(د) بالحبس مدة لا تتجاوز نصف الحد الأقصى للعقوبة التي قد يعاقب بها الفاعل بعد إدانته، في أية حالة أخرى"[1]، ونفهم من نص المادة السابق أن كل من حاول ارتكاب جريمة إلكترونية مما نصت علية المادة رقم ٢٦٢ مكرر يعاقب بنصف العقوبة التي قررها القانون، والتي يدان بها الفاعل، ففي جرائم دخول الأنظمة بشكل غير مشروع فالعقوبة على الجريمة التامة هنا هو الحبس مدة سنة وغرامة ألف دينار أردني، فلو توافرت أركان المحاولة في هذه الجريمة كانت العقوبة المقررة هي الحبس ستة أشهر وغرامة خمسمائة دينار أو أحدى هاتين العقوبتين، وكذلك الحال بالنسبة إلى باقي الجرائم التي ذكرناها[2].

وفي الواقع العملي إن كل الجرائم الإلكترونية التي يعاقب عليها بهذه المادة تعتبر جنح، ولكن الحقيقة أن المشرع لم يكن موفقاً في تصنيف الجرائم الإلكترونية، وذلك لعدم النص على كافة الجرائم الإلكترونية، فالمشرع نص هنا على الجرائم الأكثر وقوعاً، ولم يتطرق إلى باقي الجرائم الإلكترونية مثل نشر الفيروسات، والسرقة من بطاقات الائتمان والحسابات البنكية، وجرائم غسيل الأموال والترويج للمخدرات عبر مواقع الإنترنت[3].

وخلاصة القول إن العقوبات التي قررها المشرع في هذه المادة لم تكن كافيه، لاعتبار الجرائم الإلكترونية جنح، ففي الحقيقة قد تصل الجرائم الإلكترونية إلى درجة الجناية، فقد يؤدي نشر فايروس على شبكة الإنترنت خسائر بالمليارات، أو قد يؤدي العبث في إحدى برامج المستشفيات إلى وفاة إحدى المرضى[4]، أو قد يؤدي اختراق أحد الأنظمة الأمنية إلى أفشاء أسرار عسكرية وأمنية للعدو، ولذلك يجب رفع سقف العقوبات في هذه الجرائم، وأن يتم إعادة النظر في تصنيفها، ووضع العقوبات المناسبة عليها لتتلاءم بشكل أكبر مع الواقع العملي والأضرار التي تخلفها.

---

[1] راجع المادة رقم د/٢٩ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ المعدل لسنة ٢٠١٠م.

[2] أنظر ما سبق ص٢٤.

[3] طبقاً لإحصائية أجراها الباحث سُجل لدى محكمة صلح جباليا سنة ٢٠١١م (٢٨) جريمة إلكترونية، وسنة ٢٠١٢م (٤١) جريمة إلكترونية، وسنة ٢٠١٣ حتى نهاية شهر ٨ (٣٢) جريمة إلكترونية، وكل هذه الجرائم التي سجلت جنح.

[4] خالد ممدوح إبراهيم ، **حوكمة الإنترنت** ، المرجع السابق ، ص ٣٩٩ .

يعتبر ما سلف ذكره هو مجموعة الجرائم التي نص عليها قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦م المعدل لسنة ٢٠١٠م، أما في الفرع التالي سنتناول بالشرح الجرائم التي نص عليها مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

الفرع الثاني

الجزاء الجنائي للجرائم الإلكترونية في مشروع قانون العقوبات لسنة ٢٠١٠م

عرضنا في الفرع السابق الجزاء الجنائي للجرائم الإلكترونية في قانون العقوبات رقم٧٤ لسنة ١٩٣٦ المعدل لسنة ٢٠١٠م، وعرفنا أن نصوص القانون لم تكن كافية لتجريم كافة أشكال الجرائم الإلكترونية، وفي هذا الفرع سنعرض الجزاء الجنائي على الجرائم الإلكترونية في مشروع قانون العقوبات لسنة٢٠١٠، مع أن هذا المشروع لم يتم إقراره بعد، وسنبحث عن أشكال الجرائم الإلكترونية التي جرمها المشروع والعقوبات التي فرضها عليها، وذلك على نحو ما هو تّال:

أولاً: جرائم الدخول غير المشروع:

من أمثلة جرائم الاختراق التي تتعلق بأنظمة المعلومات والشبكات جرائم تدمير المواقع واختراق المواقع الرسمية واختراق الأجهزة الشخصية، واختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه[١]. وجميع هذه الجرائم تبدأ بانتهاك خصوصية الشخص وهذا سبب كافاً لتجريمها، فضلاً عن إلحاق الضرر المادي والمعنوي بالمجني عليه[٢].

ونص مشروع قانون العقوبات في المادة رقم ٥٤٥ على جريمة الدخول إلى نظام إلكتروني أو البقاء فيه بوجه غير مشروع، وعاقب عليها بالحبس مدة سنة وغرامة لا تتجاوز ألف دينار أردني أو أحدى هاتين العقوبتين، وإذا ترتب على هذا الدخول إتلاف أو تعديل أو محو في بيانات ومعلومات النظام يعاقب الجاني **بالحبس**[٣]، وغرامة لا تتجاوز ثلاثة آلاف دينار أردني أو أحدى هاتين العقوبتين[١].

---

[١] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص١١٦.

[٢] علي جبار الحسيناوي، المرجع السابق، ص١٠٤.

[٣] نصت المادة رقم ٣٩ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦على عقوبة الحبس بأنها: "(١) تكون عقوبة الحبس مقرونة بالأشغال الشاقة إلا إذا أوعزت المحكمة بغير ذلك.(٢) إذا ثبت على شخص ارتكاب جرم يستوجب الحكم عليه بالحبس المؤبد أو الحبس لمدة أخرى فيجوز للمحكمة أن تحكم عليه بالحبس لمدة أقل من=

وفي التشريع البريطاني نص قانون إساءة استخدام الحاسوب لسنة ١٩٩٠ على أنه: "يعدّ الشخص مذنباً بارتكاب جرم إذا: أ- تسبب عن قصد في جعل جهاز الحاسوب يؤدي أي إجراء لتأمين الاختراق والدخول إلى أي برامج أو بيانات مخزّنة على أي حاسوب. ب- كان الاختراق الذي قصده ذلك الشخص اختراقاً غير مصرح به؛ و. ج- كان يعلم وقت تسببه في أن يؤدي الحاسوب هذا الإجراء حقيقة الوضع الذي يقوم به"[٢].

وفي فرنسا أدانت محكمة جنح باريس متهم بجريمة الدخول بدون وجه حق إلى نظام المعالجة الآلية للمعلومات، حيث قام المتهم بتقديم نفسه بأنه مندوب عن المجموعة الفيدرالية FBI لكي يحصل على توريد خدمات تليفونية من شركات الخدمة مقابل مبلغ ٢٥٠٠٠٠ دولار[٣].

ثانياً: جرائم التصنت والاعتراض غير المشروع:

إن هدف المشرع من تجريم التصنت والاعتراض هو حماية الحق في حرية الاتصال واحترام نقل البيانات دون تدخل من أحد، ويمثل الركن المادي في هذه الجريمة في قيام الجاني باستراق السمع أو اعتراض المعلومات باستعمال أي من الأجهزة المخصصة لذلك أما الركن المعنوي فيتمثل بقصد الجاني بعلمه وإرادته بارتكاب فعل التصنت أو الاعتراض[٤].

ونصت المادة رقم ٥٤٦ على جرائم التصنت الغير مشروع، أو جرائم الاعتراض لمعلومات أو بيانات غير معروضة للعامة، فيعاقب كل من يرتكب هذه الجرائم بالحبس مدة لا تزيد عن ستة أشهر، وبغرامة لا تزيد عن مئتين دينار أو أحدى هاتين العقوبتين[٥]، وتعتبر هذه الجريمة من

=ذلك"، أما مشروع قانون العقوبات لسنة ٢٠١٠م فقد نص على عقوبة الحبس في المادة رقم ٤٧ بأنها: " عقوبة السجن أو الحبس هي: إيداع المحكوم عليه في أحد مراكز الإصلاح والتأهيل المخصصة لذلك بموجب القانون المدة المحكوم بها عليه لهذا الغرض، ويكلف المحكوم عليه بالسجن أو الحبس بأداء الأعمال المقررة قانوناً في مراكز الإصلاح والتأهيل سواء داخل تلك المراكز أو خارجها في الأعمال التي تعينها الدولة، وإذا أطلق القانون لفظ السجن عدا ذلك سجناً مؤقتاً".

[١] راجع المادة رقم ٥٤٥ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٢] راجع المادة رقم ١ من قانون إساءة استخدام الحاسوب في بريطانيا لسنة ١٩٩٠م، مشار إليه في الملحق الثاني في كتاب د. عادل عزام الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، المرجع السابق، ص٤٣٩.

[٣] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٦٢.

[٤] بلال أمين زين الدين، المرجع السابق، ص٢٨٨، ٢٨٩.

[٥] راجع المادة رقم ٥٤٦ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

الجرائم التي تمس بالحياة الشخصية للأفراد، والتي كفلها أغلب الدساتير في التشريعات المقارنة بالحماية، وعملت على صونها من أي انتهاك.

ثالثاً: جرائم أنظمة المعلومات:

استبعد الفقه التقليدي المعلومات من طائفة الأموال بحجة أنها غير مادية، أما الفقه الحديث فقد أدرج المعلومات مع الأموال، وذلك نظراً لقيمتها الاقتصادية العالية، ويعتبر فقهاء القانون الحديث أن القانون الذي لا يعتبر المعلومات مال له قيمة اقتصادية إنه قانون بعيد عن الواقع[١].

ويُقصد بجرائم أنظمة المعلومات أي الجرائم التي تقع على المكونات المعنوية للحاسب الآلي من بيانات ومعلومات، مثل اختراق الحاسب الآلي أو الشبكة إما مجرداً، أو بهدف ارتكاب جريمة أخرى مثل تخريب المعطيات والأنظمة، أو خلق البرامج الضارة التي تنقل عبر الحاسب الآلي والشبكات وغيرها من الجرائم الاخرى[٢].

ونص المشروع على جرائم أنظمة المعلومات فكل من يقوم بإفساد أو محو أو تعديل معلومات تخص الغير مما يلحق به ضرراً جسيماً فيعاقب بالحبس، وغرامة لا تتجاوز ثلاثة آلاف دينار، أو بإحدى هاتين العقوبتين، أما لو قام الجاني بإعاقة تشغيل نظام للغير بشكل خطير عن طريق نقل أو تغيير أو حجب معلومات النظام، أو إذا قام الجاني بزرع فايروس بهدف تدمير أو تعطيل نظام معين ففي كلتا الحالتين يعاقب الجاني بالحبس و غرامة لا تتجاوز ألفي دينار أو أحدى هاتين العقوبتين[٣].

رابعاً: جرائم إساءة استخدام الأجهزة:

كل من يقوم بالحصول على جهاز إلكتروني وبه برامج معدة لارتكاب جريمة، أو قام باستخدام كلمات مرور أو معلومات بهدف الدخول إلى نظام إلكتروني لارتكاب إحدى الجرائم

---

[١] علي عبد القادر القهوجي، المرجع السابق، ص٥٠.

[٢] جمال محمد غيطاس، المرجع السابق، ص٢١٢.

[٣] راجع المادة رقم ٥٤٧ ، ٥٤٨ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

الإلكترونية، فقد نصت المادة رقم ٥٤٩ على أن الجاني في الحالات السابق يعاقب بالحبس مدة لا تزيد عن سنة، وبغرامة لا تتجاوز ألف دينا، أو بإحدى هاتين العقوبتين[١].

وأدان القضاء الفرنسي موظف بجرم إساءة الائتمان التقنية حيث كان يعمل في شركة إعلانات، وقام بتسليم إحدى الشركات المنافسة إعلانات الشركة التي يعمل بها لتقوم بنسخها وإرجاعها له[٢].

خامساً: جرائم التزوير بواسطة الحاسوب:

ليست المعلومات الورقية وحدها تقبل التزوير، فكذلك البيانات والمعلومات الإلكترونية تقبل التزوير، ونص المشروع في المادة رقم ٥٥٠ على أن كل من يقوم بتعديل أو إدخال معلومات حاسوبية بهدف الترويج لها واستعمالها بشكل غير مشروع، فيعاقب بالحبس مدة لا تزيد عن سنة، وبغرامة لا تتجاوز ألفي دينار، أو أحدى هاتين العقوبتين[٣].

وفي حادثة في أمريكا قام موظف بنك بتزوير حسابات أصدقائه في البنك الذي يعمل به، بحيث تزداد أرصدتهم، ومن ثم يقوم أصدقاءه بسحب هذه المبالغ، وقد نجح بالفعل وكان يرغب بالتوقف إلا أن أصدقاءه أجبروه على الاستمرار في عملية التزوير، إلى أن كشف أمره وقبض عليه[٤].

أما من يقوم بتزوير وثائق حاسوب واستخدمها مع علمه بتزويرها، أو قام بإفساد نظام تشغيل أو عطلة، أو قام بتعديل بيانات النظام بطريقة الغش مما أدى للضرر بالغير فيعاقب بالحبس، وبغرامة لا تتجاوز ثلاثة آلاف دينار، أو أحدى هاتين العقوبتين[٥].

---

[١] راجع المادة رقم ٥٤٩ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٢] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص١١٥.

[٣] راجع المادة رقم ٥٥٠ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٤] يوسف المصري، المرجع السابق، ص٨٣.

[٥] راجع المادة رقم ٥٥١، ٥٥٢ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

سادساً: جرائم الاحتيال والسرقة الإلكترونية:

لاقت فكرة تجريم سرقة البرامج والمعلومات الإلكترونية معاداة من قبل الكثيرين، ولكن الواقع المفروض علينا أنه لا يمكننا إنكار ملكية الشخص للبرنامج أو المعلومة، وبالتالي فالسارق يستحوذ على مال ليس ملكاً له، وهذا هو جوهر الاختلاس في السرقة[١].

فجرائم الاحتيال والسرقة من أكثر الجرائم التي توقع خسائر مادية فادحة، ونص المشروع على أن كل من قام بحجب أو التقاط أو نسخ أو نقل معلومات أو بيانات بهدف نقل الملكية وجلب مصلحة اقتصادية بشكل غير مشروع، يعاقب بالحبس مدة لا تزيد عن سنة، وبغرامة لا تتجاوز ألفي دينار، أو أحدى هاتين العقوبتين.

أما إذا استخدم الجاني إحدى الطرق التقنية بهدف الحصول على أموال البنوك أو أموال العملاء فيها فيعاقب بالسجن المؤقت، وبغرامة بقدر ما استفاد من الأموال التي تحصل عليها من جريمته، مع إعادة كل الأموال التي حصل عليها بدون وجه حق.

وإذا استخدمت الوسائل الإلكترونية بهدف الوصول إلى أرقام بطاقات الائتمان أو أي بطاقات مالية أخرى، للاستيلاء على أموال صاحب البطاقة، يعاقب الفاعل بالحبس مدة لا تزيد عن سنتين، وبغرامة لا تتجاوز خمسة آلاف دينار، أو بإحدى هاتين العقوبتين[٢].

ورأت محكمة النقض الفرنسية أنه إذا قام شخص بالصرف من بطاقة الائتمان الخاصة به متجاوزاً رصيده في حسابه البنكي، فذلك لا يندرج تحت أي وصف جنائي، ولكن يعتبر اخلال بالتزام تعاقدي بين حامل البطاقة والبنك[٣].

---

[١] هدى حامد قشقوش، المرجع السابق، ص٥٩.

[٢] راجع المادة رقم ٥٥٣ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٣] عبد الفتاح بيومي حجازي، **الحكومة الإليكترونية ونظامها القانوني**، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص٧٣٩.

سابعاً: جرائم التعامل بالمواد الإباحية:

إن الجرائم الجنسية والتي تتعلق بالتعامل بالمواد الإباحية من أخطر الجرائم الإلكترونية، وترتكب هذه الجرائم من خلال طباعة أو نشر أو نسخ المواد الإباحية، وقد عاقب المشروع عليها بالسجن مدة لا تزيد عن سنتين، وغرامه لا تتجاوز خمسة آلاف دينار، أو أحدى هاتين العقوبتين[١].

وإدين شخص في الصين بغرامة مقدارها ١٣٥٠ دولار، لأنه قام باختلاس اسم وكلمة سر أحد مستخدمي الإنترنت، واستخدمها في الاتصال بأحد اصدقائه، وتبادل معه صور إباحية[٢].

ثامناً: جرائم الاعتداء على الحقوق الفكرية، وسرقة البيانات الإلكترونية:

نص مشروع قانون العقوبات على الجرائم التي تمس بالحقوق الفكرية والأدبية مثل الأعمال الفنية أو الأدبية أو التصويرية، وترتكب هذه الجرائم من خلال سرقتها أو نسخها أو تعديلها، فيعاقب الجاني في هذه الحالة بالحبس مدة لا تزيد عن ستة أشهر، وبغرامة لا تتجاوز خمسمائة دينار، أو بإحدى هاتين العقوبتين[٣].

وإذا قام الجاني بسرقة بيانات أو معلومات تخص الغير بواسطة أي وسيلة إلكترونية، أو قام بالحصول عليها أثناء تسجيلها أو أرسالها عبر الوسائل الإلكترونية، أو مّكّن الغير من الحصول على هذه البيانات أو المعلومات، وكانت هذه البيانات مما يؤثر سلباً على سمة صاحبها أو حياته الشخصية، فإن مرتكب الأفعال السابقة يعاقب بالحبس، وبغرامه لا تتجاوز ثلاثة آلاف دينار، أو بإحدى هاتين العقوبتين[٤].

وقضت محكمة النقض الفرنسية بإدانة شخص قام بسرق ديسكات تحتوي على بيانات معلوماتية تخص منشأة، وقد أيد الفقه هذا الحكم، كون الكيانات الإلكترونية مال قابل للسرقة وله قيمة اقتصادية[٥].

---

[١] راجع المادة رقم ٥٥٤ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٢] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٤٨.

[٣] راجع المادة رقم ٥٥٥ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٤] راجع المادة رقم ٥٥٦ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٥] محمد أمين الشوابكة، المرجع السابق، ص ١٤٩ .

تاسعاً: الجرائم التي تتعلق بالإنترنت:

ولدت فكرة الإنترنت داخل وزارة الدفاع الأمريكية، وكانت تستخدم لأغراض عسكرية، وكان الهدف من الإنترنت هو وضع القوات الامريكية في حالة تأهب قصوى داخل مراكز إدارة الصواريخ، إذا ما قامت حرب نووية أو أي اعتداء عسكري عليها، وبزوال خطر الحروب تم استخدام هذه التقنية من الجانب العسكري إلى الجانب السلمي إلى ما وصلت عليه في الوقت الحالي[١].

وأكثر الجرائم التي تزعج رواد الإنترنت هي الفيروسات التي يتم صنعها ونشرها من حين لأخر عبر شبكة الإنترنت، ونص المشروع على جريمة صنع أو نشر الفيروسات، وعاقب عليها بالحبس، وبغرامه لا تقل عن ألف دينار، ويعاقب بذات العقوبة كل من ينشر عبر شبكة الإنترنت أي معلومات أو بيانات تهدف إلى تشويه سمعة الغير أو الإساءة له[٢].

وإذا قام شخص بملاحقة الغير أو مضايقته بأي وسيلة إلكترونية عبر الإنترنت فإنه يعاقب بالحبس مدة لا تزيد عن سنة، وبغرامه لا تتجاوز ألف دينار، أو بإحدى هاتين العقوبتين[٣].

ويمتلئ الإنترنت بالمخاطر التي تهدد الاطفال والمراهقين، ولذلك يجب أن تكون الشبكة أو الحاسب الذي يستخدمه، مزود ببرامج الحماية التي تمنع ظهور المواد غير المرغوب فيها، مثل الصور والمشاهد الإباحية ودعايات الجماعات العنصرية، والاعلانات التي تهدم القيم لدى الأطفال[٤].

كما وفرت البيئة الإلكترونية حياة خاصة للأفراد، وقد تتعرض هذه الحياة لاعتداء من قبل آخرين عبر الإنترنت، ويظهر الركن المادي في هذه الجريمة من خلال سلوك الجاني بتمام ولوجه إلى النظام الإلكتروني وينتهي بتمام فعله، أما الركن المعنوي فيتمثل في قصد الجاني والذي قد

---

[١] عبد الفتاح بيومي حجازي، **الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة**، المرجع السابق، ص٢٣، ٢٤.

[٢] راجع المادة رقم ٥٥٨، ٥٦٠ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٣] راجع المادة رقم ٥٥٩ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٤] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٤٥.

يتعدد فقد يكون قصده الاطلاع المجرد أو الاطلاع بقصد الإفشاء أو الاطلاع بقصد التهديد والابتزاز[١].

عاشراً: عقوبة المحاولة في الجرائم الإلكترونية:

نص مشروع قانون العقوبات الفلسطيني على المحاولة في مادة خاصة بالباب الذي يتعلق بالجرائم الإلكترونية حيث نص على انه: " يعاقب على الشروع في الجرائم المنصوص عليها في هذا الفصل بنصف العقوبة المقررة للجريمة التامة"، وعليه فعند وجود محاولة في إحدى الجرائم التي ذكرناها في هذا الفرع يعاقب عليها بنصف العقوبة التي قررها القانون للجريمة التامة[٢].

ونرى مما سبق أن مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م قد صنف أكثر الجرائم الإلكترونية، وتضمن جرائم لم ينص عليها قانون العقوبات رقم ٧٤ لسنة ١٩٣٦، ولكن هناك جرائم لم ينص عليها مشروع قانون العقوبات، وذلك ربما لأنها لم تظهر بعد على الساحة الفلسطينية، ولكنه كان الأجدر به أن ينص عليها، ومن هذه الجرائم ترويج المخدرات وغسيل الأموال والإتجار بالجنس البشري عبر مواقع الإنترنت.

كما أن العقوبات التي فرضها المشروع لا تختلف كثيراً عن العقوبات الموجودة في قانون العقوبات لسنة ١٩٣٦- لبعض الجرائم المتطابقة في القانونين- حيث أن العقوبات متدنية، ولا تتناسب مع حجم الضرر الذي تخلفه بعض الجرائم، فعلى سبيل المثال إن عقوبة جريمة الوصول لأرقام بطاقات الائتمان في مشروع قانون العقوبات الفلسطيني يعاقب الفاعل بالحبس مدة لا تزيد عن سنتين، وبغرامة لا تتجاوز خمسة آلاف دينار، أو بإحدى هاتين العقوبتين، أما عقوبة نفس الجريمة في قانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧م فهي السجن مدة لا تتجاوز خمس سنوات، أو بالغرامة، أو العقوبتين معاً[٣]، فلو نظرنا إلى القانونين لنجد فارق كبير في العقوبات مع أن الجرائم واحدة، ولذلك نطلب من المشرع الفلسطيني أن يحذوا حذوا المشرع السوداني في التشديد في العقوبات على الجرائم الإلكترونية.

---

[١] أسامة أحمد المناعسة، جلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية**، المرجع السابق، ص٢٢٨وما بعدها.

[٢] راجع المادة رقم ٥٦١ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

[٣] راجع المادة رقم ١٢ من قانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧، مشار إليه في الملحق رقم (٤) في كتاب محمد علي العريان، المرجع السابق ، ص ٣١٣، والمادة رقم ٥٥٣ من مشروع قانون العقوبات الفلسطيني لسنة٢٠١٠م.

المطلب الثاني

الجزاء الجنائي للجرائم الإلكترونية في القانون الأردني

أفرد المشرع الأردني قانوناً مستقلاً عالج فيه الجرائم الإلكترونية، وسمي هذا القانون بقانون جرائم أنظمة المعلومات الأردني لسنة ٢٠١٠، على خلاف المشرع الفلسطيني الذي ضمّن النصوص التي تعالج الجرائم الإلكترونية في قانون العقوبات، وعليه سنعرض الجزاء الجنائي للجرائم الإلكترونية في القانون الأردني على نحو ما هو تالٍ:

أولاً: جرائم الدخول غير المشروع:

نص المشرع الأردني في المادة الثالثة من قانون أنظمة المعلومات على جريمة الدخول إلى نظام إلكتروني بطريقة غير مشروعة، وعاقب عليها بالحبس مدة لا تقل عن أسبوع، ولا تزيد على ثلاثة أشهر، أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار، أو بكلتا هاتين العقوبتين، وإذا كان الدخول بهدف تعديل أو إتلاف أو نسخ أو انتحال شخصية صاحب النظام، فيعاقب الجاني بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار، أو بكلتا هاتين العقوبتين[١].

وقد يكون الدخول غير المشروع لنظام إلكتروني تم بطريقة الصدفة، مثل أن يقوم شخص بإدخال أرقام أو رموز فيكتشف أنه دخل إلى معلومات وبيانات أخرى، لا يستطيع الوصول لها بالطرق العادية[٢].

ثانياً: جرائم أنظمة المعلومات:

ونص القانون على الجرائم التي تتعلق بأنظمة المعلومات من حيث نسخ أو تعديل أو إتلاف أو حجب أو نشر بيانات أو معلومات تتعلق بالغير، أو إذا قام الجاني بتمّكين الآخرين من الاطلاع عليها، أو انتحل شخصية صاحبها، فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر

---

[١] راجع المادة رقم ٣ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jol.

[٢] هدى حامد قشقوش، المرجع السابق، ص٥٩.

ولا تزيد على سنة، أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار، أو بكلتا هاتين العقوبتين[١].

وقد تتم الجرائم التي تتعلق بأنظمة المعلومات من خلال نشر الفيروسات والتي تعمل على تدمير البرامج والبيانات المخزنة، وقد يمتد أثره ليشمل حذف أو تعديل أو إصابة البيانات والبرامج[٢].

ثالثاً: جرائم التنصت والاعتراض غير المشروع:

وإذا قام الجاني بالتنصت أو الاعتراض على ما هو مرسل عن طريق أي وسيلة إلكترونية بطريقة غير مشروعة، فيعاقب الجاني بالحبس مدة لا تقل عن شهر ولا تزيد على سنة، أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار، أو بكلتا هاتين العقوبتين[٣].

وجرم المشرع مسألة التنصت على الآخرين وذلك لحماية حرمة الحياة الخاصة وصوناً لها، وتشمل الحماية فيما يجريه الآخرين من أحاديث أو يتبادلونه من صور أو غيرها من الملفات والبيانات الشخصية[٤].

رابعاً: الجرائم المالية:

يتمثل الركن المادي في جرائم السرقة الإلكترونية في فعل الاختلاس لمال منقول مملوك للغير، أما الركن المعنوي فيتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، وكذلك تتطلب هذه الجريمة توافر قصد خاص وهو نية تملك الشيء المختلس[٥].

وكما ذكرنا بأن الجرائم المالية من أكثر الجرائم انتشاراً عبر الوسائل الإلكترونية، وذلك لسهولة ارتكابها بالنظر إلى جرائم السرقة التقليدية، وجرم المشرع الأردني كل من أستخدم الوسائل الإلكترونية بهدف الوصول إلى أرقام بطاقات الائتمان أو أي أرقام أخرى تستخدم في المعاملات

---

[١] راجع المادة رقم ٤ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٢] علي عبد القادر القهوجي، المرجع السابق، ص٥٠.

[٣] راجع المادة رقم ٥ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٤] عبد الفتاح بيومي حجازي، **الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة**، المرجع السابق، ص١٥١.

[٥] محمد علي العريان ، المرجع السابق، ص١٢٦ وما بعدها.

المالية الإلكترونية، وحدد عقوبة الجاني بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنتين، أو بغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٢٠٠٠) ألفي دينار، أو بكلتا هاتين العقوبتين، أما لو أستخدم الجاني هذه الأرقام أو البطاقات أو ساعد الغير في استخدامها للحصول على أموال الغير، فيعاقب الجاني بالحبس مدة لا تقل عن سنـة، وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار ،أما لو أرتكب الجاني أي جريمة من التي ذكرناها أعلاه، وهي جرائم دخول الأنظمة بطرق غير مشروعة وجرائم أنظمة المعلومات وجرائم التنصت والاعتراض والجرائم المالية، أثناء تأديته لمهام وظيفته، أو أستغل عمله في ارتكابها فتضاعف له العقوبة[١].

وعملت الدول على تغيير تشريعاتها لمواجهة الجرائم الإلكترونية، بحيث تعترف هذه التشريعات بالمال الإلكترونية مثل البيانات والمعلومات والخدمات المختلفة، والتي اصبحت في هذا العصر أكثر الأموال تعرضاً للجريمة، ومن أمثلة هذه الجرائم سرقة المعلومات والخدمات وتدمير البرامج عن طريق فيروسات الحاسب الآلي[٢].

وأدان القضاء الإنجليزي شخصاً كان يعمل مبرمجاً في إحدى البنوك في الكويت، حيث قام بعمل برنامج أو أمر لكمبيوتر بموجبه يتم تحويل أموال من أرصده في البنك الذي يعمل به والتي لم يجر عليها معاملات مالية منذ زمن، إلى حسابات قد فتحها في إنجلترا ، وقد علق تنفيذ هذا الأمر على تركه للعمل في البنك المحوّل منه، وبعد ان عاد إلى إنجلترا وتم فعّله، كشف أمره وتمت إدانته[٣].

وقام شخص يعمل اخصائياً للحسابات في أحد بنوك أمريكا، باكتشاف شفرة تحويل حسابات للعملاء بين البنوك، حيث قام بإصدار أمر إلكتروني بتحويل مبالغ مالية قدرت بأربعه ملايين دولار لحسابه في سويسرا ثم اشترى ألماس ووضعه في خزينة أحد البنوك هناك، ومضت الأشهر دون أن يكتشف احد أمره حتى أعترف على نفسه وهو مخمور[٤].

---

[١] راجع المادة رقم ٦، ٧ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ I.

[٢] محمد حسين منصور، **المسئولية الإلكترونية**، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٣م، ص١٧٩.

[٣] محمد أمين الشوابكة، المرجع السابق، ص ١٨٧ .

[٤] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٣٤، ٣٥.

خامساً: جرائم التعامل بالمواد الإباحية:

أثبتت دراسة أدست خطورة المواقع الإباحية على جميع المجتمعات، ويمكن لمس آثارها على ارتفاع عدد جرائم الاغتصاب بشكل عام، واغتصاب الأطفال بشكل خاص والعنف الجنسي، وكانت الدراسات في المجتمع السعودي قد أثبتت أن هناك علاقة ما بين مشاهدة المواد الإباحية والجرائم الجنسية[١].

ومن أخطر الجرائم الجنسية الإلكترونية الاستغلال الجنسي للأطفال، فهناك العديد من المواقع التي تنشر صور للأطفال في أوضاع جنسية مخلة، أو تبث أفلام إباحية للأطفال، وهناك مواقع أخرى تجذب الأطفال لإيقاعهم في شبكات الدعارة والاستغلال الجنسي، وهذه الأفلام المخلة تؤدي إلى جذب المنحرفين ليوقعوا بالأطفال في الفاحشة من خلال محادثتهم عبر الدردشة وغرف المحادثات وعبر مواقع التواصل الاجتماعي[٢].

وصنف المشرع الأردني عدة صور للجرائم الجنسية الإلكترونية، فمن يقوم بأرسال أو نشر أي مواد إباحية لمن لم يكمل ثمانية عشر من عمره، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن (٣٠٠) ثلاثمائة دينار ولا تزيد على (٥٠٠٠) خمسة ألاف دينار.

وإذا قام الجاني بنشر أو إعداد أو طباعة أو تجهيز أو عرض أي مواد إباحية، وذلك للتأثير على من لم يكمل ثمانية عشر من عمره، أو للتأثير على من هو معاق نفسياً أو عقلياً، أو للتحريض على ارتكاب جريمة، فيعاقب الفاعل بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة الاف دينار.

ويعاقب كل من يستخدم الوسائل الإلكترونية ونظم المعلومات في استغلال كل من لم يكمل ثامنة عشر من عمره، أو من هو معاق نفسياً أو عقلياً، لاستخدامه في أعمال الدعارة والأعمال الجنسية، بالأشغال الشاقة المؤقتة، وبغرامة لا تقل عن (٥٠٠٠) خمسة ألاف دينار ولا تزيد على (١٥٠٠٠) خمسة عشر ألف دينار.

---

[١] يوسف المصري، المرجع السابق، ص٦٥، ٦٦.

[٢] محمد أمين الشوابكة، المرجع السابق، ص ١٠٥، ١٠٦ .

وإذا استخدم الجاني الشبكة المعلوماتية أو أي نظام إلكتروني بهدف الترويج للدعارة، فيعاقب بالحبس مدة لا تقل عن ستة اشهر، وبغرامة لا تقل عن (٣٠٠) ثلاثمائة دينار ولا تزيد على (٥٠٠٠) خمسة الاف دينار[١].

وقد تم حصر عدد القوائم العربية الإباحية على شبكة الإنترنت ومنها موقع (yahoo) فكان عددها ١٧١ قائمة، في حين وصل أكثرها أعضاء نحو ٩ آلاف عضو[٢].

سادساً: الجرائم التي تمس الأمن العام:

يقصد بالجرائم التي تمس الأمن العام أو المصلحة العامة الجرائم التي لا يكون المعتدى عليه فرد بعينه أو مجموعة من الأفراد، بل أن الحق المعتدى عليه هو حق يصيب المجتمع ككل، ومثل هذه الجرائم الإخبار الخاطئ عن الجرائم الإلكترونية، وتهديد السلامة العامة، بث البيانات من مصادر مجهولة، جرائم تعطيل الأعمال الحكومية، الحصول على معلومات سرية[٣].

وجرائم أمن الدولة أو ما يسمى بالإرهاب من الجرائم الخطير التي تمس الأمن القومي للدولة، ونص المشرع الأردني على أنه من يقوم باستخدام الشبكة المعلوماتية أو أي وسيلة إلكترونية أو أنشأ موقعاً على شبكة الإنترنت لإنشاء جماعة إرهابية أو للترويج لأفكارها أو لتسهيل أعمال إرهابية، فيعاقب الفاعل بالأشغال الشاقة المؤقتة[٤].

وإذا قام شخص بالدخول إلى نظام إلكتروني خاص بالدولة بطريقة غير مشروعة، للاطلاع على بيانات ومعلومات غير معروضة للجمهور، تمس أمن الدولة أو علاقاته الخارجية أو الاقتصاد الوطني، فيعاقب الفاعل بالحبس مدة لا تقل عن أربعة أشهر، وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٥٠٠٠) خمسة ألاف دينار، أما إذا كان الجاني يهدف من وراء دخوله على النحو السابق إلى نسخ أو تعديل أو إتلاف أو إفشاء أو نشر البيانات والمعلومات

---

[١] راجع المادة رقم ٨، ٩ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٢] علي جبار الحسيناوي، المرجع السابق، ص٩٩.

[٣] يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المرجع السابق، ص٢٩١ .

[٤] راجع المادة رقم ١٠ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

التي تمس أمن الوطن، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار[١].

ومن الجرائم التي تمس الأمن العام جرائم التجسس الإلكترونية، ومثالها اختراق المواقع والصفحات الإلكترونية بهدف التجسس أو التنصت على ما تحتويه من بيانات ومعلومات سواء كانت هذه البيانات كتابية أو مرئية أو صوتية، وقد يكون الهدف من التجسس الحصول على معلومات أمنية أو عسكرية أو اقتصادية أو سياسية أو مالية أو تعليمية[٢].

سابعاً: عقوبة المحاولة في الجرائم الإلكترونية:

إن النقص الذي يصيب المحاولة الإجرامية هو النقص المادي، أي أن النقص يصيب العناصر المادية للجريمة دون عناصرها المعنوية، خاصة النقص الذي يصيب عنصر النتيجة لأسباب خارجة عن إرادة الجاني، فعند توافر ما ذكر نكون بصدد محاولة إجرامية[٣].

لم ينص المشرع الأردني على المحاولة للجرائم الإلكترونية في قانون جرائم أنظمة المعلومات لسنة ٢٠١٠، وبالعودة إلى الأصل وهو قانون العقوبات الأردني نجد أن المشرع الأردني قد نص في المادة رقم ٧٠ من قانون العقوبات على أنه: " ....فإذا لم يتمكن الفاعل من إتمام الأفعال اللازمة لحصول تلك الجناية أو الجنحة لحيلولة أسباب لا دخل لإرادته فيها عوقب على الوجه الآتي إلا إذا نص القانون على خلاف ذلك:.... وخمس سنوات من ذات العقوبة على الأقل إذا كانت العقوبة الأشغال الشاقة المؤبدة أو الاعتقال المؤبد،٢- أن يحط من أية عقوبة أخرى مؤقتة من النصف الى الثلثين"[٤].

---

[١] راجع المادة رقم ١١ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٢] محمد محمد الألفي، المرجع السابق، ص٩٢,٩٣.

[٣] جلال ثروت، المرجع السابق، ص ١٧٣.

[٤] راجع المادة رقم ٦٨ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

فالشخص الذي لم يتمكن من إتلاف حاسوب الغير بواسطة فيروس أعده ونشره، بسبب وضع صاحب الحاسوب برنامج حماية من الفيروسات، يعتبر الشخص الذي ارسل الفيروس إلى الحاسوب ولم يتمكن من تدميره أنه حاول ارتكاب جريمة[١].

وكذلك نص المشرع الأردني في المادة رقم ٧٠ على أن: " إذا كانت الأفعال اللازمة لإتمام الجريمة قد تمت ولكن لحيلولة أسباب مانعة لا دخل لإرادة فاعلها فيها لم تتم الجريمة المقصودة، عوقب على الوجه التالي:.... وسبع سنوات الى عشرين سنة من ذات العقوبة إذا كانت العقوبة الأشغال الشاقة المؤبدة أو الاعتقال المؤبد،٢- أن ينزل من أية عقوبة أخرى من الثلث الى النصف"[٢].

وفي المادة ٧١ نص المشرع الأردني على أنه: " لا يعاقب على الشروع في الجنحة إلا في الحالات التي ينص عليها القانون صراحة"[٣].

ونص المشرع العُماني على أنه: " يعاقب بنصف الحد الأعلى للعقوبة المقررة قانوناً للجريمة على الشروع في ارتكاب إحدى الجرائم المنصوص عليها في هذا القانون"[٤].

وخلاصة ما سبق من النصوص التي ذكرناها إن قانون جرائم أنظمة المعلومات لم ينص على المحاولة في الجرائم الإلكترونية، ولذلك ففي حالة وقوع جريمة إلكترونية مما نص عليها القانون نطبق أحكام قانون العقوبات الأردني، فالجنح لا يعاقب عليها إلا عندما ينص القانون عليها صراحة، كما أن يحط من أي عقوبة غير الإعدام والأشغال الشاقة المؤبدة من النصف الى الثلثين هذا في حالة لم تتم الأفعال المكونة للجريمة، أما في حالة تمام الأفعال المكونة للجريمة ولكن لم تتم الجريمة فتحط العقوبة من الثلث إلى النصف غير عقوبة الإعدام والأشغال المؤبدة[٥].

---

[١] عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المرجع السابق، ص ١٦٧.

[٢] راجع المادة رقم ٧٠ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٣] راجع المادة رقم ٧١ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٤] راجع المادة رقم ٣٠ من قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢ العُماني، مشار إليه في موقع تقنية المعلومات العُماني عبر الرابط التالي: http://www.ita.gov.om/.

[٥] فخري عبد الرازق الحديثي، خالد حميدي الزعبي، **شرح قانون العقوبات**، المرجع السابق، ص٣٢٤.

ثامناً: التدابير الاحترازية:

في حال ضبط أي أجهزة إلكترونية أو أي مواد لها صلة بجريمة إلكترونية، فللمحكمة أن تحكم بمصادرة الأجهزة التي استخدمت في الجريمة أو إتلاف أي مواد مضبوطة لها علاقة بالجريمة، وكذلك تعطيل أي أنظمة أو مواقع إلكترونية استخدم في الجريمة[1].

كما أن بعض التشريعات جعلت الحكم بمصادرة الأجهزة أو المعدات أو النسخ المقلدة في الجرائم الإلكترونية وجوبياً، وإلا كان الحكم معيباً مستوجباً نقضه للخطأ في تطبيق القانون[2].

تاسعاً: عقوبة المشترك والمحرض والعائد للجريمة الإلكترونية:

نص قانون جرائم أنظمة المعلومات الأردني على عقوبة المشترك والمحرض على الجرائم الإلكترونية وجعل عقوبة المشترك والمحرض نفس عقوبة الجاني، أما العائد[3] للجريمة الإلكترونية

---

[1] راجع المادة رقم ١٢ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

[2] محمد علي العريان ، المرجع السابق، ص ٢٤٨.

[3] نصت المادة رقم ٢٣ من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ على تعريف المشترك بأنه: " (١) لدى ارتكاب جرم يعتبر كل شخص من الأشخاص المشار إليهم أدناه بأنه قد اشترك في ارتكاب ذلك الجرم وأنه ارتكبه ويجوز اتهامه به: (أ) كل من ارتكب بنفسه الفعل المكون للجرم أو أحد الأفعال المكونة للجرم أو أغفل القيام أمر أو أمور يعتبر إغفالها مكوناً للجرم. (ب) كل من ارتكب فعلاً أو أغفل القيام بفعل بقصد تمكين أو مساعدة غيره على ارتكاب الجرم. (ج) كل من ساعد شخصاً آخر على ارتكاب الجرم، سواء أكان حاضراً حين ارتكابه أم لم يكن. ويعتبر الشخص بأنه ساعد غيره على ارتكاب الجرم إذا كان موجوداً في المكان الذي ارتكب فيه الجرم بقصد إرهاب المقاومين أو تقوية تصميم الفاعل الأصلي أو ضمان ارتكاب الجرم المقصود. (د) كل من حمل أو أغرى شخصاً آخر على ارتكاب الجرم، سواء أكان حاضراً حين ارتكابه أم لم يكن".

وعرفت المادة رقم ٣١ المحرض بأنه: " كل من حاول حمل غيره أو حاول تحريضه أو تشويقه على ارتكاب فعل أو ترك في فلسطين أو في الخارج، وكان ذلك الفعل أو الترك، فيما لو تم وقوعه، يعد جرماً بمقتضى شرائع فلسطين أو الشرائع المعمول بها إذ ذاك في البلاد التي كان في النية ارتكاب الفعل أو الترك فيها، يعتبر مجرماً بنفس الجرم ويعاقب بنفس العقوبة التي يعاقب بها فيما لو حاول بنفسه ارتكاب ذلك الفعل أو الترك في فلسطين، سواء أكان هو الذي حاول ارتكاب الفعل أو الترك أم الشخص الآخر الذي حمله أو حرضه أو شوقه".

أما العود فهو عندما يرتكب شخص جريمة معينة، ثم يعود بعد الحكم عليه بارتكاب هذه الجريمة مرة ثانية.

فتضاعف له العقوبة[1]، وشدد المشرع عقوبة العائد للجريمة لأن الدافع الأساسي لديه هو تحقيق الربح غير المشروع[2].

ونرى مما سبق أن المشرع الأردني قد أصاب حين أفرد تشريعاً خاصاً يكافح به الجرائم الإلكترونية، وهذا ما نفضله وندعو المشرع الفلسطيني للعمل به، مع أن قانون أنظمة المعلومات الإلكتروني لم يكن شاملاً لجميع الجرائم الإلكترونية مثل جرائم غسل الأموال والترويج للمخدرات، كما لم يتضمن الجزاء الجنائي للمحاولة الإجرامية، فكان من الأفضل لو تضمن ذلك، وعلى الرغم من القصور الموجودة في هذا القانون إلا أنه أفضل بكثير من قانون العقوبات الفلسطيني رقم٧٤ لسنة١٩٣٦، وعليه ندعو المشرع الفلسطيني أن ينظم قانون خاص يعالج فيه الجرائم الإلكترونية مثل المشرع الأردني، مع أن يراجع الجرائم الإلكترونية التي ظهرت في الدول الأخرى ليشملها بالعقاب.

[1] راجع المادة رقم ١٣، ١٥ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي: http://www.lob.gov.jo/ l.

[2] محمد علي العريان ، المرجع السابق، ص ٢٤٧.

الفصل الثالث

القواعد الإجرائية للجرائم الإلكترونية

تمهيد وتقسيم :

الجرائم الإلكترونية كغيرها من الجرائم تمر بثلاث إجراءات لا غنى عنها، وتتمثل هذه الإجراءات في إجراءات جمع الاستدلالات وإجراءات التحقيق الابتدائي وإجراءات التحقيق النهائي (المحاكمة)، إلا أن هذه الإجراءات تختلف بعض الشيء عن إجراءات الجرائم التقليدية، في أن الجرائم الإلكترونية طبيعتها وبيئتها تختلف عن الجرائم التقليدية، كما أنها تتطلب وجود خبراء تقنيين وأجهزة إلكترونية لكشف ملابسات الجريمة قد لا نجد هذه الأشياء في الجرائم التقليدية، وهناك صعوبات كثيرة تواجه إجراءات التحقيق والمحاكمة في الجرائم الإلكترونية، ومثل هذه الصعوبات صعوبة الحصول على الأدلة في الجرائم الإلكترونية وصعوبة إثباتها، ومن أكثر الصعوبات التي تواجه التحقيق في الجرائم الإلكترونية هو القبض على الجناة خاصة وأن الجرائم الإلكترونية لا حدود جغرافية لها، فمن الصعب البحث عن الجناة والقبض عليهم إذا كانوا خارج إقليم الدولة، كما أن الجهاز الشرطي والقضائي قليل الخبرة في مثل هذه الجرائم مما يؤدي إلى صعوبة التحقيق فيها.

وفي ذلك سنتناول دراسة القواعد الإجرائية للجرائم الإلكترونية، من خلال البحث في إجراءات جمع الاستدلالات والتي يختص بها مأمورو الضبط القضائي، وإجراءات التحقيق الابتدائي أمام النيابة العامة، وفي النهاية سنبحث إجراءات المحاكمة أمام المحكمة، وذلك عبر المباحث التالية:

المبحث الأول : جمع الاستدلالات في الجرائم الإلكترونية .

المبحث الثاني : التحقيق الابتدائي في الجرائم الإلكترونية .

المبحث الثالث : المحاكمة في الجرائم الإلكترونية .

المبحث الأول

جمع الاستدلالات في الجرائم الإلكترونية

إجراءات جمع الاستدلالات من الإجراءات التي تسبق التحقيق ورفع الدعوى الجزائية[١]، والتي يختص بها مأموري الضبط القضائي، والتي يكون عليهم النائب العام مشرف ومسئول عن أعمالهم، حيث يحق للنائب العامة الإشراف على أعمال الضبطية القضائية، كما يحق له مطالبة الجهات المختصة مسائلة مأموري الضبط القضائي تأديبياً عن تقصيرهم أو مخالفتهم لواجبات عملهم[٢]، وإجراءات جمع الاستدلالات ينطوي فيها عملية البحث والتحري حول الجريمة والتمهيد للتحقيق فيها، دون التوغل في عملية التحقيق التي تختص بها النيابة العامة دون غيرها[٣].

كما أن قواعد الإجراءات الجزائية تهم كل فرد في المجتمع سواء كان بريئاً أم مذنباً، فالمجتمع ينشد الحقيقة ولا يرغب في إفلات أي مذنب من العقاب، وذلك لا يتم إلا باتخاذ الإجراءات الجزائية المناسبة[٤].

ونص المشرع الفلسطيني على من يخول بصفة الضبطية القضائية حيث نص على أنه: "يكون من مأموري الضبط القضائي: ١-مدير الشرطة ونوابه ومساعدوه ومديرو شرطة المحافظات والإدارات العامة، ٢-ضباط وضباط صف الشرطة، كل في دائرة اختصاصه، ٣-رؤساء المراكب البحرية والجوية، ٤-الموظفون الذين خولوا صلاحيات الضبط القضائي بموجب القانون"[٥].

فبمقتضى هذه المرحلة تجمع الدلائل التي تفيد في كشف الحقيقة، والتي قد تصلح اساساً للمحاكمة في الجنح والمخالفات، أو أساساً للتحقيق الابتدائي في الجنايات والجنح[٦].

---

[١] ممدوح خليل البحر، **مبادئ قانون أصول المحاكمات الجزائية**، دار الثقافة، عمان، ١٩٩٨م، ص١٩٤.

[٢] راجع المادة رقم ١٩، ٢٠ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] عبد القادر جرادة، **موسوعة الإجراءات الجزائية في التشريع الفلسطيني**، المجلد الأول، مكتبة آفاق، غزة، عدد بئر السبع، ٢٠٠٩م، ص٢٧٧.

[٤] إدوارد غالي الدهبي، **الإجراءات الجنائية**، الطبعة الثانية، مكتبة غريب، القاهرة، ١٩٩٠م، ص٨.

[٥] راجع المادة رقم ٢١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٦] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، الطبعة الثامنة، دار النهضة العربية، القاهرة، ٢٠١٢م، ص٥٣٧.

ونص المشرع الأردني على الضبطية القضائية، والقائمين بها على أنه: "يساعد المدعي العام في إجراء وظائف الضابطة العدلية: الحكام الإداريون، مدير الأمن العام، مديرو الشرطة، رؤساء المراكز الأمنية، ضباط وأفراد الشرطة، الموظفون المكلفون بالتحري والمباحث الجنائية، المخاتير، رؤساء المراكب البحرية والجوية، وجميع الموظفين الذين خولوا صلاحيات الضابطة العدلية بموجب هذا القانون والقوانين والأنظمة ذات العلاقة"[١].

وعلى ضوء ذلك سنتناول إجراءات جمع الاستدلالات في الجرائم الإلكترونية عبر المطالب التالية:

المطلب الأول : جمع الاستدلالات في الظروف العادية.

المطلب الثاني : جمع الاستدلالات في الظروف الاستثنائية.

المطلب الأول

جمع الاستدلالات في الظروف العادية

لمأمور الضبط القضائي مهام من الواجب عليه مباشرتها في الظروف العادية، مثل أن يتلقى الشكاوي والبلاغات حول وقوع جريمة إلكترونية معينة، وإجراء الكشف والمعاينة والبحث والتحري حول الجرائم وسماع الأقوال وغيرها من الإجراءات التي تمهد للتحقيق في الجرائم الإلكترونية، ومع ذلك فإن الاستدلال لا يعتبر مرحلة من مراحل الدعوى الجزائية[٢]، وعليه سنتناول ذلك عبر الفروع الآتية:

---

[١] راجع المادة رقم ٩ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

[٢] عبد الرحمن توفيق أحمد، **شرح الإجراءات الجزائية**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م، ص٤٣.

الفرع الأول

تلقي البلاغات والشكاوي والتحري عنها

إن أول ما يحرك الضابطة القضائية هو وجود بلاغ أو شكوى من شخص أو جهة معينة تفيد بوقوع جريمة إلكترونية، أو أن هناك جريمة على وشك الوقوع، فمن اختصاصات الضابطة القضائية هو تلقي الشكاوي والبلاغات عن الجرائم[١]، سواء كانت الشكوى أو البلاغ جوازياً أم وجوبياً[٢].

ومن بعد أن يتلقى مأمور الضبط القضائي بلاغ أو شكوى حول وقوع جريمة إلكترونية، يبدأ بالتحري والاستقصاء لمعرفة ملابسات الجريمة، والبحث عن الركن الشرعي أي معرفة إذا كان الفعل المرتكب يشكل جريمة أم لا، وكذلك البحث عن المشتبه بهم وسماع أقوالهم، وندب الخبراء وسماع أقوال المتواجدين في مسرح الجريمة[٣]، وكل ذلك يجب أن يتم على وجه السرعة دون أي تباطؤ، لأن أي تأخير في عملية التحري قد يؤدي إلى ضياع الأدلة وتغيير في مسرح الجريمة. كما أن التبليغ عن الجرائم من قبل الأفراد قد يكون إلزامي في بعض الأحيان، لكل من وصل إليه العلم بوقوع جريمة[٤].

وفي إطار ذلك قامت وزارة الداخلية في غزة بإنشاء إدارة المصادر الفنية بالمباحث العامة، وذلك حرصاً منها على مكافحة الجريمة الإلكترونية، والعمل على توظيف خبراء في المجال الإلكتروني للتحري والتحقيق في هذه الجرائم، حيث قامت هذه الإدارة بالكشف عن ٣٦ رقم

---

[١] راجع المادة رقم ٢٢/١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م، والمواد رقم ٤٤، ٤٥، ٥٢ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ui/main.html .

[٢] إدوارد غالي الدهبي، المرجع السابق، ص٣٣٣.

[٣] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت**، المرجع السابق، ص٢٤٦، ٢٤٧ .

[٤] نائل عبد الرحمن صالح، **محاضرات في أصول المحاكمات الجزائية**، الطبعة الأولى، دار الفكر للنشر والتوزيع، عمان، ١٩٩٧م، ص٢٦٠.

جوال قام بعمليات معاكسة للمواطنين، كما استرجعت الإدارة ثلاث حسابات على الفيسبوك كانت مسروقة[1].

الفرع الثاني

معاينة مسرح الجريمة

يقصد بمعاينة مسرح الجريمة هو فحص مسرح الجريمة وكل ما يرتبط بمرتكبها، وإثباته على حالته[2]، ولا تتمتع معاينة مسرح الجريمة الإلكتروني بالأهمية التي تتمتع بها مسارح الجرائم التقليدية، وذلك لأن الجرائم الإلكترونية لا تترك آثار مادية في العالم الخارجي مثل التي تتركها الجرائم التقليدية، ومع ذلك فهناك خطوات على مأموري الضبط القضائي اتخاذها في معاينة مسرح الجريمة الإلكتروني، مثل تصوير الحاسوب والاجهزة المتصلة به في أوضاعها، مع تصوير الاجزاء الخلفية للحاسب الآلي وإثبات الأسلاك المتصلة بالجهاز وتسجيل تاريخ كل عملية تصوير، وإذا كان الحاسب الآلي قيد التشغيل يجب منع أي شخص من استخدامه، وعدم العبث من قبل طاقم المعاينة في البيانات والمعلومات المخزنة عليه مثل سجل المحادثات وسلة المحذوفات، والتحفظ على المستندات الورقية الموجودة في مسرح الجريمة[3].

ونص المشرع الفلسطيني على أنه: "وفقاً لأحكام القانون على مأموري الضبط القيام بما يلي:...٢- إجراء الكشف والمعاينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق..."[4]، أما المشرع الأردني فقد نص على أنه: "١- اذا وقع جرم مشهود يستوجب عقوبة جنائية يجب على المدعي العام ان ينتقل في الحال الى موقع الجريمة"[5]. وتلعب المعاينة دوراً هاماً في التحقيق إذ

---

[1] محمد الزرد، تقرير بعنوان "المصادر الفنية بالمباحث العامة تحارب الجريمة إلكترونياً"، جريدة وزارة الداخلية ملحق يصدر مع صحيفة الرأي، العدد ١٢٣، ٢٠١٣/٥/٢٣م، ص٣.

[2] ساهر إبراهيم الوليد، **الوجيز في شرح قانون الإجراءات الجزائية الفلسطيني**، الجزء الأول، الطبعة الثانية، ٢٠٠٨م، ص٢٠٩.

[3] أمير فرج يوسف، المرجع السابق، ص٢٣٠، ٢٣١.

[4] راجع المادة رقم ٢٢/٢ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م

[5] راجع المادة رقم ٢٩/١ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

يتمكن المحقق من رؤية أدلة الجريمة وإثباتها قبل العبث بها[١]. كما يستطيع مأمور الضبط القضائي الاستعانة بأهل الخبرة عند إجراء المعاينة إذا لزم الأمر، وذلك لإعطاء رأيهم الفني في ذلك[٢].

ونستنتج مما سبق أن المشرع الأردني جعل إجراء الكشف والمعاينة من اختصاص المدعي العام أو النيابة العامة، أما المشرع الفلسطيني جعل إجراء المعاينة من اختصاص مأمور الضبط القضائي والنيابة العامة، وهذا ما نفضله كون المعاينة تحتاج إلى سرعة التنفيذ للتحفظ على مسرح الجريمة على حالته، وبطبيعة الحال فإن مأمور الضبط القضائي هو أقرب من النيابة العامة لمسرح الجريمة.

والمعاينة في الجرائم الإلكترونية قد تتطلب معاينة العالم الافتراضي، ويستطيع عضو سلطة التحقيق أو مأمور الضبط القضائي الانتقال إلى العالم الافتراضي من خلال حاسوبه الشخصي أو أحدى مقاهي الإنترنت، أو من خلال جهاز الخبير، أو عن طريق اللجوء إلى مقر مزود الخدمة والذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة، وهناك خطوات يجب اتباعها في معاينة العالم الافتراضي، وهي تصوير شاشة الحاسب الآلي، وعدم نقل أي مواد معلوماتية من مسرح الجريمة قبل التأكد من عدم اختراق الجهاز الذي قد يتسبب في محو البيانات المسجلة، ويجب تعطيل حركة الاتصالات والتحفظ على سلة المهملات، وفي النهاية يجب الاستعانة بأهل الخبرة متى دعت الحاجة لذلك[٣].

الفرع الثالث

سماع أقوال الشهود والمشتبه بهم

لمأمور الضبط القضائي أن يستمع لأقوال الشهود والمشتبه بهم بشروط معينة، فقد خول القانون ذلك لمأموري الضبط القضائي لأن الشاهد مع مرور الوقت قد ينسى ما شاهده أو سمعه، أو قد يتأثر بالروايات التي يسمعها من شهود آخرين، وكذلك الحال بالنسبة للمشتبه بهم فإن تدوين

---

[١] عبد الرؤوف مهدي، **شرح القواعد العامة للإجراءات الجنائية**، دار النهضة العربية، القاهرة، ٢٠٠٦م، ص٤٥٢.

[٢] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٥٥٥.

[٣] نبيلة هبة هروال، **الجوانب الإجرائية لجرائم الإنترنت**، دار الفكر الجامعي، الإسكندرية، ٢٠١٣م، ص٢١٨ وما بعدها.

أقوالهم في حال ارتكاب الواقعة تمنع من تلقينهم الأقوال من قبل الآخرين في المستقبل. فالشهادة دليل من الأدلة الجنائية التي يسعى المحقق جمعها للوصول للحقيقة[١].

ويجب على مأموري الضبط القضائي عدم تحليف الشاهد اليمين عند سماع أقواله[٢]، فالجهة المخولة بتحليف اليمين هي النيابة العامة والمحكمة، ونص المشرع الفلسطيني على ذلك وجعل سماع أقوال الشهود أمام مأموري الضبط القضائي دون حلف اليمين[٣]، وكذلك المشرع الأردني جعل حلف اليمين للمدعي العام دون غيره[٤]، وبمفهوم المخالفة لا يجوز لمأمور الضبط القضائي أن يقوم بتحليف الشاهد اليمين إلا إذا فوضه وكيل النيابة بذلك.

وفي الواقع أنه نادراً ما نجد شاهداً على وقائع الجرائم الإلكترونية، وذلك لعدة أسباب أهمها أن الجرائم الإلكترونية تتطلب دراية كافية بالجوانب الفنية والتقنية للحاسوب، وهذا لا بد من أن يتوفر في شاهد الجرائم الإلكترونية، كما أن الجرائم الإلكترونية ترتكب في هدوء، أي أن الجاني في العادة يرتكبها وحده دون وجود أحد معه، والجرائم الإلكترونية كما نعلم لا تترك آثاراً خارجية يشهد بها أحد كما هو المعتاد في الجرائم التقليدية.

وليس لمأمور الضبط القضائي أن يأمر بإحضار متهم أو شاهد، بل له استدعاء من يشاء لسماع أقواله، وإذا رفض الحضور فلا سبيل إلى اكراهه وإحضاره بمذكرة قبض، ذلك لأن هذا الإجراء من اختصاص النيابة العامة[٥].

أما لو كان هناك شاهد من ذوي الخبرة في المجال الإلكتروني، وقد شاهد المجرم وهو يرتكب جريمة إلكترونية وعلم بها الشاهد وبملابساتها، فيجب على مأمور الضبط القضائي أن يسمع أقواله دون تحليفه اليمين، ولمأمور الضبط أن يقوم بتعيين خبير يساعده في سؤال الشاهد أو المشتبه فيهم في بعض الأمور الفنية أثناء التحقيق.

---

[١] عبد الرؤوف مهدي، المرجع السابق، ص٤٥٥.

[٢] ممدوح خليل البحر، المرجع السابق، ص٢٠٣.

[٣] راجع المادة رقم ٢٢/٢ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م

[٤] راجع المادة رقم ٧١ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

[٥] إدوارد غالي الدهبي، المرجع السابق، ص٣٣٤.

ويعد كذلك من إجراءات جمع الاستدلالات سماع أقوال المشتبه بهم، ويقتصر هذا الإجراء بإعلام المشتبه بهم بالتهم المنسوبة إليهم، ومجمل الأدلة الموجهة ضدهم دون مناقشتهم تفصيلياً في الواقعة، وسماع أقوالهم دون مواجهتهم، ويعد من المشتبه فيهم كل شخص كان متواجداً في مسرح الجريمة أو يحوم حولها أو هناك أدلة أخرى ضده، ويجب على مأمور الضبط القضائي سماع أقواله وتدوينها مع إرسالها لوكيل النيابة المختص خلال أربع وعشرين ساعة، إذا دعت الحاجة لذلك[١].

الفرع الرابع

الاستعانة بالخبراء

تعد الجرائم الإلكترونية من الجرائم التي تتطلب توافر خبراء متخصصين في مجال الحاسوب والإنترنت، كون هذه الجرائم ترتكب في بيئة رقمية لم تظهر من قبل في الجرائم التقليدية، فقلت الخبرة لدى المحققين وأعضاء النيابة العامة قد يضيع الأدلة المتوافر في هذه الجرائم، فوجود الخبراء المتخصصين في هذا المجال يساعد على كشف الأدلة والحفاظ عليها، خاصة وأن هذه الجرائم غاية في التعقيد، ففي أغلب الأحيان لن تكون هناك الخبرة الكافية لدي أفراد الشرطة وأعضاء النيابة العامة للكشف عن ملابسات الجرائم الإلكترونية[٢].

والاستعانة بالخبراء من مهام مأموري الضبط القضائي، حيث يعمل الخبير تحت إشراف مأمور الضبط القضائي دون تحليفه اليمين[٣] إلا إذا خاف مأمور الضبط ألا يستطيع استماع أقواله مرة ثانية إذا كان مريضاً مثلاً[٤] ويشرف على عمله بالكامل، ومن واجبات الخبير في مجال الجرائم الإلكترونية العمل على تجميع الحاسب الآلي وتشغيله، والبحث عن أدلة الإثبات والحفاظ عليها بالشكل والهيئة التي وجدت عليها، والحفاظ على الأنظمة الإلكترونية موضوع الجريمة ونقلها أو عزلها دون تغيير أو إتلاف فيها، ونقل أدلة الأثبات دون إحداث تغيير أو تلف فيها، وتحويل الأدلة

---

[١] عبد القادر جرادة، **دستور الاستدلال والتحقيق الجنائي**، الطبعة الأولى، مكتبة آفاق، غزة، عدد الطيبة، ٢٠١٢م، ص١٨، ١٩.

[٢] رامي متولي القاضي ، المرجع السابق ، ص١١٢.

[٣] ساهر إبراهيم الوليد، المرجع السابق، ص٢١٠.

[٤] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٥٦٢,٥٦٣.

الرقمية على هيئة صور كتابية –إن أمكن– ليقدر القاضي المختص من الاطلاع عليها وفهمها بسهولة ويسر[١].

ونص القانون البلجيكي في ذلك على أنه: "يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحمولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق"[٢].

وخلاصة القول إن تعيين الخبراء في مجال الجرائم الإلكترونية ضرورة ملحة، لأن الجرائم الإلكترونية جرائم معقدة ويصعب الكشف عن الأدلة فيها، كما أن أدلتها لا يستطيع استنباطها إلا خبير، فمحققين الشرطة وأعضاء النيابة العامة قليلو الخبرة في هذا المجال، وبدون خبراء في مجال الجرائم الإلكترونية ستضيع الأدلة المطلوبة إما مع مرور الوقت، أو بالخطأ من قبل المحقق.

الفرع الخامس

رفع البصمات وتحرير المحاضر

تعرف البصمة بأنها الخطوط التي تظهر على الأصابع وراحة اليد، وأثبت العلم أن بصمة اليدين لا تتغير مع مرور الوقت، كما أن البصمة تختلف من شخص لآخر، ولا توجد بصمات تتشابه بين الأشخاص، وتثبت البصمة على الأسطح الملساء، ونستفيد منها في مجال الجرائم الإلكترونية أنها قد تعرفنا على الجناة من خلال البحث عن بصماتهم في مسرح الجريمة، أو البحث عن صاحب البصمة من سجل السوابق[٣].

---

[١] عبد العال الديربي، محمد صادق إسماعيل، المرجع السابق، ص٣١٨-٣٢٠.

[٢] راجع المادة رقم ٨٨ من قانون تحقيق الجنايات البلجيكي لسنة ٢٠٠٠م، مشار إليه في كتاب رامي متولي القاضي ، المرجع السابق، هامش رقم ٢، ص١١٣.

[٣] خليل حسن الجريسي، **أساليب التحقيق والبحث الجنائي الفني**، الطبعة الثالثة، مطبعة دار المنارة، غزة، ٢٠٠٣م، ص١٠٩.

ومنح المشرع الفلسطيني رفع البصمات لمأمور الضبط القضائي حيث نص على أن: "يترتب على مأمور الضبط فور حضوره مكان الواقعة أن يبحث عن البصمات التي يمكن أن يكون الجاني قد تركها ؛ ليقوم برفعها بمعرفة خبير البصمات"[١].

وفي الواقع إن رفع البصمات من الإجراءات المهمة والتي تساعد في كشف هوية الجناة، خاصة وأن الاجهزة الإلكترونية عادة ما تكون ملساء مما يسمح بترك بصمات مستخدميها، فالذي يستخدم بطاقات الائتمان بشكل غير مشروع من الممكن أن يترك بصماته على هذه البطاقة أو على جهاز الصراف الآلي، ومن يستخدم الهاتف الذكي كذلك يترك بصماته.

وفي نهاية أي إجراء من إجراءات جمع الاستدلالات التي يقوم بها مأمور الضبط القضائي، يجب عليه أن يحرر هذا الإجراءات في محاضر رسمية[٢]، وأن تشمل المحاضر اسم محرر المحضر وتوقيعه ومكان وتاريخ تحريره، وتوقيع الشاهد أو المشتبه فيه أو الخبير المنتدب، ومثل هذه المحاضر الكشف والمعاينة وإفادات الشهود والمشتبه بهم وتقارير الخبراء، ويجب على مأمور الضبط القضائي أن يرسل هذه المحاضر للنيابة العامة لاستكمال التحقيق[٣].

الفرع السادس

مراقبة المحادثات وتسجيلها وضبط المرسلات

الاعتداء على حرمة الحياة الخاصة من الجرائم التي يعاقب عليها القانون، وكفلة القانون الأساسي ومعظم دساتير العالم[٤]، فلا يجوز أن يقوم أي شخص أو أي جهة بمراقبة المحادثات الشخصية سواء الهاتفية أو الإلكترونية، أو أن يقوم بتسجيلها إلا في الحدود وبالشروط التي فرضها القانون[٥].

---

[١] راجع المادة رقم ١٣٥ من التعليمات القضائية للنائب العام رقم ١ لسنة ٢٠٠٦م.

[٢] نائل عبد الرحمن صالح، **محاضرات في أصول المحاكمات الجزائية**، المرجع السابق، ص٢٦٢.

[٣] **دليل الإجراءات الجزائية**، كتيب صادر عن وزارة العدل ووزارة الداخلية، غزة، ٢٠٠٧م، ص٥، ٦.

[٤] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٧٩٧.

[٥] راجع المادة رقم ٣٢ من القانون الأساسي الفلسطيني المعدل لسنة ٢٠٠٣م، والمادة رقم ٤٣٠ من مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

وفي إطار ذلك فقد أجاز المشرع الفلسطيني للنائب العام أو أحد مساعديه أن يقوم بمراقبة المحادثات الشخصية وأن يسجلها، ولكن ذلك ضمن شروط[١]، ونص عليها المشرع الفلسطيني على أنه: "٢- كما يجوز له مراقبة المحادثات السلكية واللاسلكية، وإجراء تسجيلات لأحاديث في مكان خاص بناءً على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة في جناية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة، ٣- يجب أن يكون أمر الضبط أو إذن المراقبة أو التسجيل مسبباً، ولمدة لا تتجاوز خمسة عشر يوماً قابلة للتجديد لمرة واحدة"[٢]، وكذلك الحال في التشريع الأردني والذي منح النيابة العامة الحق في مراقبة المحادثات وتسجيلها إذا كان لهذا الإجراء أهمية في إظهار الحقيقة[٣].

وفي الواقع إن تسجيل المحادثات نوع من أنواع التفتيش لأن فيه كشف عن خصوصيات الأفراد وأسرارهم، ولذلك تسري عليه القواعد العامة للتفتيش وضماناته من حيث تحديد الأشخاص والأماكن المأذون التسجيل فيها[٤].

وأضاف المشرع الفلسطيني الحماية الجزائية على المرسلات الكتابية، مثل الخطابات والرسائل والمطبوعات، ولم يتناول المشرع المرسلات الإلكترونية إلا أنها في الوقت الحاضر هي الأكثر انتشاراً مع قلة استخدام المرسلات القديمة شيئاً فشيئا مع إمكانية القياس عليها[٥]، ومنح القانون الجزائي للنائب العام أو أحد مساعديه الحق في ضبط المرسلات مثل الرسائل والمطبوعات والجرائد والطرود والبرقيات، وذلك بشروط وهي أن يصدر الأمر من النائب العام أو أحد مساعديه، وأن يكون لهذا الإجراء فائدة في ظهور الحقيقة، وأن يكون الامر مسبباً ولا يتجاوز خمسة عشر يوماً قابلة للتجديد مرة واحدة، ونص المشرع الفلسطيني على أن: "١- للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق والبريد الخطابات والرسائل والجرائد والمطبوعات والطرود

---

[١] عبد القادر جرادة، **موسوعة الإجراءات الجزائية**، المجلد الأول، المرجع السابق، ص٣١٤.

[٢] راجع المادة رقم ٥١/٣,٢ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] نصت المادة رقم ٨٨ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م على أنه: " للمدعي العام أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق كافة الرسائل البرقية كما يجوز له مراقبة المحادثات الهاتفية متى كان لذلك فائدة في اظهار الحقيقة"، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي: http://www.lob.gov.jo/ l.

[٤] عبد الرؤوف مهدي، المرجع السابق، ص٤٥٥.

[٥] راجع المادة ١٨ من الدستور الأردني لسنة ١٩٥٢م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

والبرقيات المتعلقة بالجريمة وشخص مرتكبها"[1]، وكذلك نص المشرع الأردني على أن: "للمدعي العام أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق كافة الرسائل البرقية، كما يجوز له مراقبة المحادثات الهاتفية متى كان لذلك فائدة في إظهار الحقيقة"[2].

ومراقبة الهاتف الخاص فيه تقييد كبير للحرية الشخصية للفرد التي هي في الأصل مصونة من أي اعتداء يقع عليها[3]، وقضت محكمة النقض الفرنسية أنه يعد تنصتاً غير مشروع أن يطالب رجل الشرطة شخصاً بأن يتحدث تليفونياً أمامه مع آخر يتوقع تورطه في جريمة، ثم يسجل هذه المكالمة ويحررها في محضر[4].

وخلاصة ما سبق إن مراقبة المحادثات وتسجيلها وضبط المرسلات من الإجراءات التي تختص بها النيابة العامة دون غيرها، وذلك لخطورة هذه الإجراءات والتي تبيح للنيابة العامة اقتحام الحياة الشخصية للأفراد ومراقبتها، وقد ضمّنها المشرع الجزائي في مرحلة جمع الاستدلالات، وربما قد فعل ذلك لأن هذه الإجراءات قد تساعد في كشف الحقيقة، وهي تمهد فيما بعد في التحقيق[5].

الفرع السابع

التحفظ على أدوات الجريمة

يجب على مأمور الضبط القضائي عند الانتقال لمسرح الجريمة أن يقوم بضبط كل ما يتعلق بموضوع الجريمة ويفيد في كشف الحقيقة[6]، سواء كانت الأشياء المضبوطة تعود للمتهم أم

---

[1] راجع المادة رقم ٥١/١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[2] راجع المادة رقم ٨٨ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[3] نائل عبد الرحمن صالح، **محاضرات في أصول المحاكمات الجزائية**، المرجع السابق، ص٢٩٦.

[4] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٨٠٥.

[5] أنظر المادة رقم ٥١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م، والتي تنص على مسألة مراقبة المحادثات وتسجيلها وضبط المرسلات، والتي جعلها المشرع في الفصل الخاص بإجراءات مرحلة جمع الاستدلالات.

[6] ساهر إبراهيم الوليد، المرجع السابق، ص٢٨٧.

لغيره ولا يهم نوعها ولا طبيعتها[١]، ولكن في الجريمة الإلكترونية الوضع يختلف فيجب علينا أن نميز بين ضبط الكيانات المادية الإلكترونية، وضبط الكيانات المعنوية الإلكترونية، فالضبط الأول هو ما يقوم مأمور الضبط القضائي بضبطه في مسرح الجريمة مثل أجهزة النسخ والتسجيل وأجهزة الربط بالشبكات والطابعات والمحررات الإلكترونية، أما الضبط الثاني وهو من اختصاص النيابة العامة لأن اكتشافه يتم بعد تفتيش الكيان المنطقي للحاسب الآلي، ومثل هذه المضبوطات البرامج الإلكترونية والفايروسات والبيانات والمعلومات المسروقة والمواد الإباحية المخزنة وكل المواد المعنوية التي يمكن تخزينها على الحاسب الآلي وتتعلق بالجريمة[٢].

والضبط الثاني هو ما يشكل صعوبة لدى مأموري الضبط القضائي، وذلك لصعوبة ضبط الكيانات المعنوية للأجهزة الإلكترونية، وعدم وجود الخبرة الكافية لمأموري الضبط القضائي في مثل هذه الأمور[٣]، فيجب على مأموري الضبط القضائي والنيابة العامة الاستعانة بأصحاب الخبرة عند ضبط المواد الإلكترونية التي تصلح أن تكون دليلاً في الواقعة، وعلى مأمور الضبط القضائي إثبات الحالة التي عليها الواقعة دون تدخل منه أو تغيير أو عبث في الأجهزة الإلكترونية موضوع الجريمة[٤]، وقد يتطلب الأمر ضبط معلومات تكون مخزنة على الشبكة العنكبوتية والتي يكون مصدرها دولة أخرى، ولذلك نحن بحاجة إلى تعاون دولي لضبط مثل هذه المعلومات[٥].

وفي إطار ما ذكر نص المشرع الفلسطيني على أنه: " وفقاً لأحكام القانون على مأموري الضبط القيام بما يلي:... ٣- اتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة"[٦]، ونرى من النص السابق أن مأمور الضبط القضائي له استخدام أي وسيلة ولو كانت إلكترونية للمحافظة على أدلة الجريمة، مثل أن يقوم بنسخ البيانات والبرامج موضوع الجريمة من الحاسب الآلي إلى اسطوانة أو ذاكرة خارجية، فمثل هذا الإجراء لا يتعارض مع القانون بل إنه يحافظ على الأدلة ويساعد في الكشف عن الحقيقة.

---

[١] ممدوح خليل البحر، المرجع السابق، ص٢٣٧.

[٢] محمد محمد الألفي، المرجع السابق، ص٣٧٠، خالد عياد الحلبي، المرجع السابق، ص١٦٩ .

[٣] أمير فرج يوسف، المرجع السابق، ص٢٣٦.

[٤] علي جبار الحسيناوي، المرجع السابق، ص١٢٢.

[٥] رامي متولي القاضي، المرجع السابق ، ص٢٣ .

[٦] راجع المادة رقم ٢٢ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م

المطلب الثاني

جمع الاستدلالات في الظروف الاستثنائية

إن طبيعة العمل الشرطي تتطلب في بعض الأحيان اتخاذ إجراءات سريعة ومستعجلة، وقد تكون هذه الإجراءات لا يملكها مأمور الضبط القضائي، ولكن المشرع منحه بعض الإجراءات الضرورية والتي تساهم في كشف الحقيقة وضبط الجناة، وعليه سنتناول إجراءات جمع الاستدلالات في الظروف الاستثنائية والتي تتمثل في القبض بدون مذكرة، والإجراءات المتاحة في حالة التلبس، وهي ما سنتناوله في الفرعين الآتيين:

الفرع الأول

القبض بدون مذكرة

إن القبض على المجرمين أو المشتبه بهم يعد من أعمال التحقيق الابتدائي، إلا أن هناك بعض الحالات التي يجب فيها على مأمور الضبط القضائي أن يلقي القبض على المجرمين أو المشتبه فيهم بدون الحصول على مذكرة قبض من النيابة العامة، ومن أمثلة هذه الحالات إذا ارتكبت الجريمة أمام مأمور الضبط القضائي[1]، أو إذا خاف مأمور الضبط هروب أحد المشتبه فيهم وكانت هناك أدلة ضده على ارتكابه جرم معين، أو إذا ارتكبت الجريمة على مرأى ومسمع من الجمهور، فيجب على مأمور الضبط القضائي في الحالات السابق أن يقوم بالقبض على المجرمين والمشتبه فيهم دون الانتظار للحصور على مذكرة قبض من النيابة العامة[2].

ولا يجوز القبض على متهم في الجرائم التي يقيد القانون رفع الدعوى فيها بتقديم شكوى أو طلب أو صدور إذن، إلا إذا تحقق هذا الشرط[3].

ونص المشرع الفلسطيني على الحالات التي يجوز فيها لمأمور الضبط القضائي القبض بدون مذكرة وهي على النحو التالي: " لمأمور الضبط القضائي أن يقبض بلا مذكرة على أي

---

[1] ساهر إبراهيم الوليد، المرجع السابق، ص٢٢٨.

[2] فخري عبد الرازق الحديثي، شرح قانون أصول المحاكمات الجزائية، الموسوعة الجنائية (٤)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م، ص٢١٠ وما بعدها.

[3] إدوارد غالي الدهبي، المرجع السابق، ص٣٥١.

شخص حاضر توجد دلائل على اتهامه في الأحوال التالية: "١-حالة التلبس في الجنايات، أو الجنح التي تستوجب عقوبة الحبس مدة تزيد على ستة أشهر، ٢-إذا عارض مأمور الضبط القضائي أثناء قيامه بواجبات وظيفته، أو كان موقوفاً بوجه مشروع وفر، أو حاول الفرار من مكان التوقيف، ٣-إذا ارتكب جرماً أو اتهم أمامه بارتكاب جريمة، ورفض إعطاءه اسمه أو عنوانه أو لم يكن له مكان سكن معروف أو ثابت في فلسطين"[١].

كما لا يكفي توافر الشبهات أو الظنون أو بلاغ مقدم من المجني عليه لكي تتوافر الدلائل الكافية للقبض على أي شخص[٢].

ونص كذلك المشرع الأردني على الحالات التي يجوز فيها لمأمور الضبط القضائي القبض على المشتبه بهم وهي على نحو ما هو تالٍ: "لأي موظف من موظفي الضابطة العدلية أن يأمر بالقبض على المشتكي عليه الحاضر الذي توجد دلائل كافية على اتهامه في الأحوال الآتية: ١- في الجنايات، ٢- في أحوال التلبس بالجنح اذا كان القانون يعاقب عليها لمدة تزيد على ستة أشهر، ٣- إذا كانت الجريمة جنحة معاقباً عليها بالحبس وكان المشتكى عليه موضوعاً تحت مراقبة الشرطة أو لم يكن له محل إقامة ثابت ومعروف في المملكة، ٤- في جنح السرقة والغصب والتعدي الشديد ومقاومة رجال السلطة العامة بالقوة او بالعنف والقيادة للفحش وانتهاك حرمة الآداب"[٣].

وأحاط المشرع القبض بضمانات قوية كونها تمس بحرية الإنسان، حيث منح هذه السلطة للنيابة العامة وحدها، وأجاز لمأمور الضبط القضائي القيام بها في حالات استثنائية مثل حالة التلبس[٤].

وفي الواقع إن الطبيعة العملية لرجال الشرطة والمباحث تتطلب وجود بعض الصلاحيات بين يديهم، ولكن المشرع لم يمنحهم هذه الصلاحيات، وذلك حرصاً منه على حقوق المواطنين والتي لم يجعل المساس بها ممكناً إلا في أضيق نطاق وبإجراءات قضائية متعددة، فقصر هذه

---

[١] راجع المادة رقم ٣٠ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م

[٢] نائل عبد الرحمن صالح، **محاضرات في أصول المحاكمات الجزائية**، المرجع السابق، ص٢٦٩.

[٣] راجع المادة رقم ٩٩ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

[٤] عبد الرحمن توفيق أحمد، المرجع السابق، ص٧٦.

الصلاحيات للنيابة العامة والتي هي بمثابة الحارسة للعدالة، وبالرغم من ذلك إلا أن هناك حالات مثل التلبس يفترض على مأمور الضبط القضائي أن يتخذ إجراءات مستعجلة مثل القبض والتفتيش[١]، والتي هي من اختصاصات النيابة أصلاً، فقد منح المشرع لمأمور الضبط القضائي هذه الصلاحيات، ولكن بشروط وفي ظروف محددة، وذلك للحفاظ على متطلبات سير العدالة.

الفرع الثاني

الإجراءات المتاحة في حالة التلبس

تعد حالة التلبس من الحالات التي يباح فيها لمأمور الضبط القضائي أن يتخذ إجراءات لم يكن باستطاعته مباشرتها في الظروف العادية وذلك مراعاة لظروف الاستعجال التي تتطلب كشف الحقيقة وجمع الأدلة[٢]، ونص المشرع الفلسطيني على حالات التلبس على سبيل الحصر وهي: "١-حال ارتكابها أو عقب ارتكابها ببرهة وجيزة، ٢-إذا تبع المجني عليه مرتكبها أو تبعته العامة بصخب أو صياح أثر وقوعها، ٣-إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملاً آلات أو أسلحة أو أمتعة أو أوراقاً أو أشياء أخرى يستدل منها على أنه فاعل أو شريك فيها، أو إذا وجدت به في هذا الوقت آثار أو علامات تفيد ذلك"[٣].

فالأصل أن مأمور الضبط القضائي لا يملك اتخاذ إجراءات ماسة بالحريات، ولكن استثنيت من ذلك حالة التلبس التي أجيز فيها اتخاذ بعض الإجراءات التي هي في الأصل من اختصاصات النيابة العامة[٤]. ومن شروط صحة قيام حالة التلبس أن تكون منتجة لآثارها القانونية بأن يدرك مأمور الضبط بنفسه حالة التلبس، وأن يكون هذا الأدراك تم بطريقة مشروعة[٥].

---

[١] نصت المادة رقم ٤١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م على أنه: " تفتيش المنازل يجب أن يكون نهاراً ولا يجوز دخولها ليلاً، إلا إذا كانت الجريمة متلبساً بها، أو كانت ظروف الاستعجال تستوجب ذلك".

[٢] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٥٧٩.

[٣] راجع المادة رقم ٢٦ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٤] عبد الرؤوف مهدي، المرجع السابق، ص٣٨١.

[٥] إدوارد غالي الدهبي، المرجع السابق، ص٣٨٥.

ونص المشرع الأردني على حالة التلبس في المادة رقم ٢٨ من قانون أصول المحاكمات الجزائية الاردني لسنة ١٩٦١م على أنها: "١- الجرم المشهود (هو الجرم الذي يشاهد حال ارتكابه أو عند الانتهاء من ارتكابه)، ٢- وتلحق به أيضا الجرائم التي يقبض على مرتكبيها بناء على صراخ الناس أثر وقوعها او يضبط معهم أشياء أو أسلحة أو أوراق يستدل منها أنهم فاعلو الجرم، وذلك في الأربع والعشرين ساعة من وقوع الجرم، أو إذا وجدت بهم في هذا الوقت أثار أو علامات تفيد ذلك"[١].

ونخلص مما سبق أن المشرع الفلسطيني أقرب وأوضح من المشرع الأردني في تحديد حالات التلبس على سبيل الحصر، كما أن فترة أربع وعشرين ساعة التي نص عليها المشرع الأردني طويلة لبقاء حالة التلبس، ففي هذه الفترة يتمكن الجاني من إخفاء كل أدوات أو أسلحة جريمته أو إتلافها، وبالتالي كان المشرع الفلسطيني أدق عندما قرر عبارة بعد وقوعها بوقت قريب، فنفهم من هذه العبارة قرب وقت ارتكاب الجريمة.

وتحقق حالة التلبس في الجريمة من شأنه أن يجعل من أدلة الجريمة الظاهرة أدلة ثبوتية تبيح منح عضو الضابطة القضائية اختصاصات واسعة في التحقيق لجمع كل الأدلة المتوفرة في مسرح الجريمة، والتي يبنى عليها أثناء الاتهام والمحاكمة[٢].

كما يعد التلبس في الجرائم الإلكترونية متصور وليس صعباً أو مستحيلاً، فقد يتم الإمساك بالجاني في حالة تلبس وهو يقوم بنشر مواد إباحية عبر الإنترنت، أو وهو يخترق إحدى أنظمة البنوك لسرقة أموال منها، أو يضبط الشخص وهو يرسل عبارات القذف والتشهير بالغير عبر أحدى المواقع المنتشرة عبر الإنترنت، وقد يضبط الجاني في حالة تلبس في مكان عام كما لو استخدم حاسوب في أحدى مقاهي الإنترنت، أو قد يضبط الجاني في مكان خاص مثل منزلة[٣].

وكون حالة التلبس حالة استثنائية فقد منح المشرع لمأمور الضبط القضائي مجموعة من الإجراءات التي يجب عليه اتخاذها إذا توافرت حالة التلبس، مثل أن يقوم بالانتقال لمحل الواقعة على وجه السرعة وأثبات الحالة التي عليها مسرح الجريمة، ومنع كل من وجده في مكان الجريمة

---

[١] راجع المادة رقم ٢٨ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٢] ممدوح خليل البحر، المرجع السابق، ص٢٠٦.

[٣] محمد محمد الألفي، المرجع السابق، ص٣٦٣.

من المغادرة حتى يتأكد من هويته وصلته بالجريمة، وإذا كان هناك أيٌ من الحاضرين تحوم حوله الشبهات في أنه من أرتكب الواقعة يأمر بالقبض عليه، أما لو علم من خلال تحرياته الأولية وجود متهم غائب فيستصدر أمر بالقبض عليه[١]، ويجب على مأمور الضبط أن يفتش المقبوض عليهم ويجردهم من الاسلحة والأدوات ويعمل على تدوين أقوالهم[٢].

وبما أن الجرائم الإلكترونية كغيرها من الجرائم تنطبق عليها حالة التلبس، فيترتب على ذلك أنه في حال ارتكاب جريمة إلكترونية أن يقوم مأمور الضبط بتفتيش الفاعل وضبط كل ما يتعلق بالجريمة[٣].

فلمأمور الضبط القضائي عند ضبط شخص متلبس بجريمة إلكترونية أن يقوم بتفتيش هذا الشخص وضبط ما يحمله من أجهزة إلكترونية مثل جهاز اللابتوب أو الهاتف المحمول، ومثال التفتيش والضبط في الجرائم الإلكترونية أن يمسك مأمور الضبط بأحد الأشخاص وهو يتصفح المواقع في أحدى مقاهي الإنترنت ويطبع صور إباحية، فيحق لمأمور الضبط في هذه الحالة القبض على هذا الشخص وتفتيشه وضبط الأوراق والمواد التي لها صلة بجريمته[٤]. وسوف نتناول بالتفصيل عملية التفتيش كونها من اختصاص النيابة العامة وذلك في المبحث التالي.

---

[١] عبد القادر جرادة، **موسوعة الإجراءات الجزائية**، المجلد الأول، المرجع السابق، ص٣٤١ وما بعدها.

[٢] نصت المادة رقم ٢٧ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م على أنه: " يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى مكان الجريمة، ويعاين الآثار المادية لها ويتحفظ عليها، ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، ويسمع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الجريمة ومرتكبيها، ويجب عليه أن يخطر النيابة العامة فوراً بانتقاله، ويجب على عضو النيابة المختص بمجرد إخطاره بجناية متلبس بها الانتقال فوراً إلى مكان الجريمة".

[٣] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت**، المرجع السابق، ص٢٦٧، د . علي جبار الحسيناوي، المرجع السابق، ص١١٤.

[٤] محمد محمد الألفي، مرجع سابق، ص٣٦٤.

المبحث الثاني

التحقيق الابتدائي في الجرائم الإلكترونية

التحقيق الابتدائي من المهام التي قصرها المشرع على النيابة العامة وحدها، وذلك حرصاً منه على ضمان سير التحقيق على أكمل وجه وصولاً لكشف الحقيقة[١]، ولأن إجراءات التحقيق الابتدائي يترتب عليها آثار تمس بالمواطنين وخصوصياتهم، وقد تصل في بعض الأحيان إلى تقييد حريتهم، وللنيابة العامة أن تقوم بتفويض بعض اختصاصاتها لمأموري الضبط القضائي بهدف استيعاب الكم الكبير من القضايا التي يفترض على النيابة العامة إنجازها، ولكن ذلك التفويض يجب أن يتم بالشروط والشكلية التي فرضها القانون، وتكمن أهمية مرحلة التحقيق الابتدائي في أنه مرحلة تحضيرية للمحاكمة، فيتم فيها جمع الأدلة وتمحيصها تمهيداً للمحاكمة[٢].

فالتحقيق الابتدائي أول مرحلة من مرحلتي الدعوى الجزائية، وهو عبارة عن إجراءات تتخذها السلطات من أجل تمحيص الأدلة التي اسفرت عنها مرحلة جمع الاستدلالات، مع محاولة جمع أدلة جديدة تساعد في التحقيق في الجريمة التي وقعت[٣].

ومن الإجراءات التي تختص بها النيابة العامة دون غيرها تفتيش مسرح الجريمة وضبط كل ما يتعلق بالجريمة، وسماع اقوال الشهود تحت القسم القانوني، واستجواب المتهمين وتوجيه الاتهام لهم، وتنظيم المواجهة بين المتهمين والشهود، وغيرها من الإجراءات التي تساعد في كشف الحقيقة، وعلى ضوء ذلك سنتناول بالدراسة ما ذكرناه بالتفصيل من خلال المطالب التالية:

المطلب الأول : الجهة المختصة بالتحقيق الابتدائي.

المطلب الثاني : إجراءات التحقيق الابتدائي.

---

[١] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٦٩٠.

[٢] محمود نجيب حسني، **شرح قانون الإجراءات الجنائية**، الطبعة الثانية، دار النهضة العربية، القاهرة، ١٩٩٨م، ص٦١٤.

[٣] عبد الرؤوف مهدي، المرجع السابق، ص٣٠١.

المطلب الأول

الجهة المختصة بالتحقيق الابتدائي

النيابة العامة هي صاحبة الاختصاص الأصيل في التحقيق الابتدائي، إذ هي وحدها الجهة المخولة في ذلك، ولكن المشرع الفلسطيني قد منح وكيل النيابة صلاحية تفويض بعض المهام إلى مأموري الضبط القضائي وذلك للتخفيف من كم القضايا المعروضة على النيابة العامة، وعليه سنبين ما ذكرناه عبر الفرعين التاليين:

الفرع الأول

النيابة العامة

النيابة العامة هي صاحبة الاختصاص الأصيل في تحريك الدعوى الجزائية[١]، فهي وحدها من تملك مباشرة التحقيق الابتدائي حيث يملك النائب العام أو أحد مساعديه تحريك الدعوى الجزائية ولا يشمل ذلك باقي أعضاء النيابة العامة[٢]، وذلك لأنها تملك الخبرة والقدرة على مباشرة التحقيق في الجنايات والجنح، وتعتبر مرحلة التحقيق الابتدائي من أخطر مراحل الدعوى الجزائية كون هذه المرحلة تسبق مرحلة المحاكمة، فالمحكمة التي تنظر النزاع المعروض عليها تبني في الغالب أحكامها على النتائج التي أسفر عنها التحقيق الابتدائي.

وحرص المشرع الفلسطيني على ضمان سير الدعوى الجزائية بكل حيادية ونزاهة، فقد اوكل مهمة التحقيق الابتدائي إلى النيابة العامة كونها سلطة تتسم بالشفافية والموضوعية في التحقيق، ولاكتساب هذه السلطة الخبرة الكافية للموازنة بين حقوق الأفراد، وقدرتها على بناء قراراتها على الأدلة التي تتحراها لتقديم المتهمين إلى القضاء ليقول كلمته الأخيرة فيهم[٣].

---

[١] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٦١٣.

[٢] ممدوح خليل البحر، المرجع السابق، ص٢٢٩.

[٣] عبد القادر جرادة، **موسوعة الإجراءات الجزائية في التشريع الفلسطيني**، المجلد الثاني، مكتبة آفاق، غزة، عدد بئر السبع، ٢٠٠٩م، ص٤٢٠.

وتعتبر النيابة العامة طرفاً رئيسياً في كل دعوى جزائية، حتى تلك الدعاوي التي يحركها المدعي بالحق المدني عن طريق الادعاء المباشر[١].

كما أكد على ذلك المشرع الفلسطيني حيث نص على أنه: " تختص النيابة العامة دون غيرها بإقامة الدعوى الجزائية ومباشرتها ولا تقام من غيرها إلا في الأحوال المبينة في القانون..."[٢]، ونص كذلك على أنه: "١-تختص النيابة العامة دون غيرها بالتحقيق في الجرائم والتصرف فيها"[٣]، كما نص المشرع الأردني على أنه : "١-تختص النيابة العامة بإقامة دعوى الحق العام ومباشرتها ولا تقام من غيرها إلا في الاحوال المبينة في القانون"[٤].

ونرى مما سبق أن المشرع الفلسطيني والأردني قد قصرا إجراءات التحقيق الابتدائي على النيابة العامة دون غيرها، إلا أن هناك حالات يجوز فيها لوكيل النائب العام أن يفوض بعض صلاحياته لمأموري الضبط القضائي وهذا ما سنوضحه في الفرع التالي.

الفرع الثاني

التفويض بالتحقيق الابتدائي

يمكن تعريف التفويض أو ندب مأمور الضبط القضائي للتحقيق الابتدائي، هو تكليفه من سلطة التحقيق المختصة بعمل محدد أو أكثر من أعمال التحقيق، ويترتب على ذلك اعتبار العمل كما لو كان صادراً من سلطة التحقيق نفسها[٥]. وبناءاً على هذا التعريف فلمأمور الضبط القضائي أن يتولى عملاً معيناً من أعمال التحقيق في جريمة وقعت، بناء على ندب له من سلطة التحقيق للقيام بهذا العمل[٦].

ونظراً لكثرة عدد القضايا التي تعرض على النيابة العامة، ولأن أغلبها من الجنح البسيطة والتي يكون فيها الخصمان في حالة تصالح، فإن المشرع قد خول النيابة العامة تفويض بعض

---

[١] عبد الرؤوف مهدي، المرجع السابق، ص٣٠٧.

[٢] راجع المادة رقم ١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] راجع المادة رقم ٥٥/١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٤] راجع المادة رقم ٢/١ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

[٥] إدوارد غالي الدهبي، المرجع السابق، ص٣٩١.

[٦] رمسيس بهنام، **الإجراءات الجزائية**، منشأة المعارف، الإسكندرية، ص٥٠٥.

صلاحياتها في التحقيق الابتدائي لمأموري الضبط القضائي، وذلك لتتمكن النيابة العامة من إنجاز هذه القضايا وتتفرغ هي للتحقيق في الجنايات.

ومن الشروط الواجب اتباعها في التفويض أن يفوض وكيل النيابة مأمور الضبط في إجراء أو إجراءات محددة، دون أن يجعل الأمر مفتوحاً للتحقيق في القضايا بكاملها، ويجب على مأمور الضبط ألا يتجاوز الإجراءات المفوضة إليه، فكل إجراء يتخذه دون تفويض يعتبر أنه باطلاً، ومن الشكليات المهمة في التفويض بالتحقيق أن يكون أمر التفويض مكتوباً ومقيداً بمدة محددة[١].

ونص المشرع الفلسطيني على أنه: "...٢-للنائب العام أو وكيل النيابة العامة المختص تفويض أحد أعضاء الضبط القضائي المختص بالقيام بأي من أعمال التحقيق في دعوى محددة، وذلك عدا استجواب المتهم في مواد الجنايات، ٣-لا يجوز أن يكون التفويض عاماً، ٤-يتمتع المفوض في حدود تفويضه بجميع السلطات المخولة لوكيل النيابة"[٢].

ويتعين على مأمور الضبط تنفيذ الأمر الذي ندب له متى صدر إليه وكان صحيحاً ومستوفياً لشروطه، ويجب عليه تنفيذه في حدود التفويض، وله جميع السلطات المخولة لوكيل النيابة[٣]، ويستثنى من ذلك فض المظاريف المغلقة إذ يجب أن تكون بمعرفة النيابة العامة.

وكذلك فقد نص المشرع الأردني على أنه: "١-يمكن للمدعي العام أثناء قيامه بالوظيفة في الاحوال المبينة في المادتين (٢٩ و ٤٢) أن يعهد الى أحد موظفي الضابطة العدلية كل حسب اختصاصه بقسم من الأعمال الداخلة في وظائفه، إذا رأى ضرورة لذلك، ما عدا استجواب المشتكى عليه، ٢-في غير الأحوال المبينة في الفقرة (١) من هذه المادة إذا عهد المدعي العام إلى أي من موظفي الضابطة العدلية بقسم من الأعمال الداخلة في وظائفه وفقاً لأحكام هذا القانون وجب عليه أن يصدر مذكرة خطية بذلك تتضمن الزمان والمكان المعين لإنفاذ مضمونها كلما كان ذلك ممكنا"[٤].

---

[١] فخري عبد الرازق الحديثي، **شرح قانون أصول المحاكمات الجزائية**، المرجع السابق، ص٢٢٦، ٢٢٧.

[٢] راجع المادة رقم ٥٥ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] ساهر إبراهيم الوليد، المرجع السابق، ص٢٥١.

[٤] راجع المادة رقم ٤٨ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

ويجب أن يكون محل التفويض إجراء تحقيق مثل سماع الشهود أو إجراء تفتيش أو قبض، فإذا أشر وكيل النيابة على محضر جمع الاستدلالات بطلب تحريات المباحث مثلاً فلا يعتبر هذا ندباً لإجراء تحقيق لأن جمع التحريات من إجراءات جمع الاستدلالات[1]، ولأن الندب يجب أن يكون صريحاً.

وخلاصة القول إن المشرع الفلسطيني قد أصاب في إقرار التفويض بالتحقيق في الجنح، وقصر الاستجواب في الجنايات على النيابة العامة، فالجنايات موضوعها أخطر من أن توكل لمأموري الضبط القضائي، كما أن الواقع العملي أثبت بأن مأموري الضبط القضائي ليس لديهم الخبرة الكافية للاستجواب في الجنايات، ومن خلال نصوص القانون الفلسطيني والأردني التي عرضناها فيما سبق نجد أن القانونين متفقان إلى حد بعيد في موضوع التفويض، إلا أن المشرع الأردني قصر الاستجواب على النيابة العامة، على خلاف المشرع الفلسطيني الذي جعل الاستجواب في الجنايات فقط للنيابة العامة، مع إمكانية تفويض مأموري الضبط القضائي لاستجواب الجنح[2]، ونحن نفضل ما ذهب إليه المشرع الفلسطيني، نظراً لأن الكم الهائل من الجنح التي تعرض على النيابة العامة يومياً لن تستطيع النيابة العامة وحدها الاستجواب فيها، فلا بد من معاون لها، كما أن مأموري الضبط القضائي يصلحون لذلك.

المطلب الثاني

إجراءات التحقيق الابتدائي

إجراءات التحقيق الابتدائي هي الإجراءات التي تسبق مرحلة المحاكمة، وهذه الإجراءات هي التي تبحث في مدى حقيقة التهمة الموجه للمتهم، ولوكيل النيابة صلاحيات واسعة في هذه المرحلة، وذلك بهدف معرفة مدى صدق الواقعة المعروضة أمامه، كما أن هذه الصلاحيات غير مقيدة بالقضية المعروضة، فله أن يباشر التحقيق في أي واقعة أخرى تظهر أثناء التحقيق، كما أن وكيل النيابة غير ملزم بما يصبغه مأمور الضبط القضائي على القضية المعروضة[3]، وسنتناول بالبيان هذه الإجراءات عبر الفروع التالية:

---

[1] عبد الرؤوف مهدي، المرجع السابق، ص٥٧٣.

[2] ساهر إبراهيم الوليد، المرجع السابق، ص٢٤٥.

[3] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت**، المرجع السابق، ص٢٦٠.

الفرع الأول

التفتيش في الجرائم الإلكترونية

التفتيش[١] من أخطر الإجراءات التي منحها المشرع للنيابة العامة، كون هذا الإجراء يمّكن وكيل النيابة من اقتحام الحياة الشخصية، والاطلاع على خصوصيات الأفراد التي كفلها القانون الأساسي بالحماية[٢]، ويعرف التفتيش بأنه إجراء من إجراءات التحقيق التي تؤدي إلى ضبط أدلة الجريمة موضوع التحقيق من أجل كشف الحقيقة، وبالتالي فهو ليس من إجراءات كشف الجرائم قبل وقوعها، بل هو من إجراءات تحقيقها بعد ارتكابها[٣].

ويهدف التفتيش إلى البحث عن الأدلة الموجودة في مسرح الجريمة وكل ما يفيد في كشف الحقيقة[٤] لمعرفة مدى حقيقة التهمة المنسوبة للمتهم، وقد عرف الفقه التفتيش بأنه: "إجراء من إجراءات التحقيق تقوم به النيابة العامة أو تأذن به؛ بهدف الحصول على عناصر الحقيقة لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه"[٥].

والتفتيش في الجرائم الإلكترونية إما أن يكون عن المكونات المادية للحاسب الآلي، أو يكون عن المكونات المعنوية مثل البيانات والمعلومات، كما أن هناك إشكالات تواجه التفتيش في الجرائم الإلكترونية، وهذا ما سنتناوله بالدراسة عبر ما هو تال:

أولاً: التفتيش عن المكونات المادية للحاسب الآلي:

ليس هناك خلاف بين الفقهاء على أنه يجوز التفتيش عن المكونات المادية للحاسب الآلي، وأن هذا التفتيش قد يساعد على الكشف عن الحقيقة في جريمة إلكترونية معينة، ولكن وقبل

---

[١] نص قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١ في المادة رقم ٣٩ على أنه: "١- دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها، بناءً على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة.٢- يجب أن تكون مذكرة التفتيش مسببة.٣- تحرر المذكرة باسم واحد أو أكثر من مأموري الضبط القضائي".

[٢] راجع المادة رقم ٣٢ من القانون الأساسي الفلسطيني المعدل لسنة ٢٠٠٣م.

[٣] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٧٥٣.

[٤] إدوارد غالي الدهبي، المرجع السابق، ص٣٥٤.

[٥] عبد القادر جرادة، **موسوعة الإجراءات الجزائية**، المجلد الثاني، المرجع السابق، ص٤٥٢، ٤٥٣.

التفتيش عن المكونات المادية للحاسب الآلي يجب معرفة إذا كانت هذه المكونات موجودة في مكان عام أو مكان خاص، فإذا كانت في مكان خاص مثل منزل سكني فيجب أن يكون التفتيش بالشروط التي فرضها القانون لتفتيش الأماكن الخاصة، أما لو كان الجهاز المراد التفتيش عنه في مكان عام مثل الشوارع والميادين، أو كانت في الاماكن العامة بالتخصيص مثل المطاعم والمقاهي أو مقاهي الإنترنت فإن التفتيش في هذه الحالات يخضع لأحكام تفتيش الأشخاص وبنفس الشروط والضوابط التي فرضها القانون في ذلك[١].

وعند ضبط أي أجهزة إلكترونية لها علاقة بجريمة إلكترونية، يجب التمييز إذا ما كانت هذه الأجهزة متصلة بأجهزة أخرى في نفس المكان الذي تم تفتيشه أو كانت متصلة بأجهزة أخرى في أماكن مختلفة، وإذا كان التفتيش عن هذه الأجهزة سيسفر عن كشف حقائق تتعلق بموضوع الجريمة، فيجب أن يراعى في تفتيش هذه الأماكن الأحكام والضوابط التي فرضها القانون في ذلك[٢]، ولا يشكل التفتيش عن المكونات المادية للأجهزة الإلكترونية أي خلاف أو إشكالية، فالمشكلة تثور حين يجري التفتيش عن المكونات المعنوية للحاسب الآلي وهذا ما سنبينه عبر ما هو تال.

ثانياً: التفتيش عن المكونات المعنوية للحاسب الآلي:

إن التفتيش عن المكونات المعنوية أو المنطقية للحاسب الآلي، والتي تشمل البيانات والمعلومات وكل البرامج المعنوية التي تستخدم في تشغيل الحاسب الآلي، تثير خلافاً بين الفقهاء بشأن مدى جواز التفتيش عليها، فقد ذهب رأي بالقول أنه إذا كان الهدف من التفتيش هو ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة في الجرائم الإلكترونية، فإن ذلك الرأي يذهب بجواز التفتيش عن البيانات الإلكترونية بمختلف أشكالها، وقد ذهب القانون اليوناني في المادة رقم ٢٥١ من قانون الإجراءات الجنائي بالقول " بأي شيء يكون ضرورياً لجمع وحماية الدليل" وقد فسر جانب من الفقه اليوناني كلمة أي شيء بأنها تشمل المكونات المعنوية للحاسب الآلي على مختلف أشكالها[٣].

---

[١] خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠١٠م، ص١٩٥، ١٩٦.

[٢] هلالي عبد اللاه أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي**، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠٨م، ص٧٤.

[٣] عبد العال الديربي، محمد صادق إسماعيل، المرجع السابق، ص٣٠٠.

كما أن هناك انقسام لدى الفقه على غرار الرأي السابق بعدم جواز التفتيش عن الأدلة الإلكترونية، وذلك لأنها غير ملموسة فالتفتيش يكون فقط على الأدلة الملموسة، وذهب أصحاب هذا الرأي بأنه يتم الاطلاع على البيانات والمعلومات الإلكترونية من خلال مطالبة صاحبها بتقديمها للسلطات المختصة لتتمكن من الاطلاع عليها، وفي حالة رفضة يعتبر انه مرتكب جريمة، وهذا ما اخذ به غالبية الفقه اليوناني في المادة ٢٥١ من قانون الإجراءات الجنائي اليوناني، بينما ذهب الرأي الآخر بأن التفتيش يشمل كل البيانات الملموسة والغير ملموسة، فإذا كانت البيانات ملموسة فلا يثار أي خلاف، أما لو كانت البيانات غير ملموسة فيتم تحويلها إلى بيانات ملموسة سواء مرئية أو مقروءة أو مسموعة عن طريق الأجهزة الإخراجية المتصلة بالحاسب الآلي أو الهاتف المحمول، أو أي جهاز إلكتروني، وذلك ليتمكن المحقق من تفتيشها، وقد اخذ بهذا الرأي الفقه في فرنسا وانجلترا وامريكا واليابان[١].

ورأى جانب من الفقه وجوب حضور المتهم عند إجراء التفتيش في العالم الافتراضي أو التفتيش عن الكيانات المعنوية للحاسب الآلي، وذلك لضمان سلامة الإجراء و صحة الضبط، ولذلك إذا تعذر حضور المتهم يجب إنابة شاهدين على التفتيش[٢]، وهذا الإجراء أصبح إلزام من قبل المشرع خاصة إذا تم تفتيش الحاسب الموجود في المنزل.

ونص المشرع الأردني على موضوع التفتيش عن الكيانات المعنوية للحاسب الآلي حيث نص على أنه: "يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل الى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم...."[٣]، فنرى من النص السابق أن المشرع الأردني أحسن حين نص صراحة على جواز التفتيش عن الكيانات المعنوية للحاسب الآلي، وتلاشى بذلك الخلاف الذي قد يحصل إذا لم يقر ذلك النص، على خلاف المشرع الفلسطيني الذي لم ينص صراحة على التفتيش عن الكيانات المعنوية للحاسب الآلي في قانون الإجراءات الفلسطيني إلا أنه نص على التفتيش على الأشياء ويمكننا القياس عليها

---

[١] بكري يوسف بكري، **التفتيش عن المعلومات في وسائل التقنية الحديثة**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠١١م، ص٧٠ وما بعدها.

[٢] نبيلة هبة هروال، المرجع السابق، ص ٢٥٨.

[٣] راجع المادة رقم ١٢ فقرة أ من قانون جرائم أنظمة المعلومات الأردني رقم ٩ لسنة ٢٠١٠م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي: http://www.lob.gov.jo/ l.

بأنها تشمل المكونات المعنوية للحاسب الآلي، ولذلك ندعو المشرع الفلسطيني إلى الانتباه إلى هذه النقطة الحساسة في موضوع التفتيش، وأن يقر قانون خاص بالجرائم الإلكترونية ينص فيه صراحة على جواز التفتيش عن الكيانات المعنوية للحاسب الآلي، أما الإشكالات التي تواجه التفتيش في الجرائم الإلكترونية سنتناولها عبر ما هو تال.

ثالثاً: الإشكالات التي تواجه التفتيش في الجرائم الإلكترونية:

هناك عدة صعوبات تواجه التفتيش في الجرائم الإلكترونية، ومن أبرز هذه الصعوبات إذا وقعت الجريمة الإلكترونية بين دولتين، فتثور هنا عدة مشاكل من بينها قبول الدولة التفتيش في الشبكات الإلكترونية الخاصة بها، وعدم قبول بعض الدول إعطاء إذن بالتفتيش لديها لكون ذلك انتهاك لسيادتها وتعدي عليها[1]، وتناولت اتفاقية بودابست موضوع التفتيش، حيث نصت على ضرورة تسهيل جميع الإجراءات التي تتعلق بالتحقيق لكل الدول الأعضاء في الاتفاقية من حيث تفتيش الأنظمة الإلكترونية، وتخويل سلطات التحقق الولوج لأنظمة المعلومات المراد تفتيشها والتي تتعلق بجريمة إلكترونية[2].

ومن الصعوبات التي تواجه التفتيش هو تفتيش شبكات الحاسوب، فقد يكون هناك عدة أجهزة متصلة مع بعضها البعض عن طريق الهاتف أو الإنترنت، فإن تفتيش جهاز المتهم قد يتطلب تفتيش جهاز آخر متصل به، وقد يكون الشخص الآخر غير متهم في ارتكاب الجريمة[3]، وإذا كان الجهاز المتصل بموضوع الجريمة مشترك في ذات الجريمة فإن المشكلة هنا تثور إذا قام صاحب الجهاز الثاني بمحو وإتلاف البيانات والمعلومات التي تشكل دليل إدانة ضده، وكذلك يعتبر الحصول على الرقم السري للدخول للأنظمة المراد تفتيشها مشكلة إذ لا يعرف هذه الأرقام إلا

---

[1] ناير نبيل عمر، المرجع السابق، ص١٤١.

[2] نصت المادة رقم ١٩ في الفقرة رقم ١ من الاتفاقية المتعلقة بالجريمة الإلكترونية، بودبست – المجر، ٢٠٠١/١١/٢٣م، مجموعة المعاهدات الأوروبية بمجلس أوروبا – رقم ١٨٥، على أنه: "يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك لمنح سلطات ذلك الطرف صلاحية التفتيش أو الدخول على : أ- أي نظام حاسوب أو جزء منه والبيانات المخزنة فيه، ب- أي وسيط تخزين، يجوز أن تكون البيانات مخزنة فيه في إقليم ذلك الطرف".

[3] خالد عياد الحلبي، المرجع السابق، ص ١٦٣ .

صاحب الجهاز، وللخروج من ذلك يجب أن يشمل إذن التفتيش جميع الأجهزة والأنظمة التي لها علاقة بالجريمة[1].

إن الشبكة الدولية – الإنترنت – من أكثر وسائل الاتصال التي تستخدم في العصر الراهن، وذلك نظراً لتوافرها وسهولة استخدامها وعدم تكلفتها المادية، ومن المرسلات التي تستخدم عن طريق الإنترنت الإيميل والشات وغيرها من مواقع التواصل الاجتماعي، ولكن قد يساء استخدام هذه الشبكة من خلال اقتراف جريمة إلكترونية عن طريقها، فعندها تقع الاشكالية، ولكن الاتجاه الغالب في الفقه القانوني هو صلاحية مراقبة المراسلات والاتصالات عبر الشبكات الإلكترونية وتفتيشها، وهذا ما ذهب إليه الفقه في فرنسا وهولندا وأمريكا[2].

ونخلص مما سبق أن التفتيش عن المكونات المنطقية للحاسب الآلي يواجه العديد من المشاكل والصعوبات، وأكثر هذه الصعوبات والتي تواجه المحققين هو الحاجة إلى خبير في مجال البرمجيات للقيام بالتفتيش، فمأموري الضبط القضائي وأعضاء النيابة العامة معظمهم ليس لديهم القدرة على تفتيش الأنظمة الإلكترونية لاستخراج الأدلة المطلوبة، كما أن الخبير الإلكتروني يحتاج إلى أجهزة حديثة حتى يستطيع القيام بعمله، فلا بد لوزارة الداخلية أن تقوم بتوظيف خبراء فنيين في مجال البرمجيات والأنظمة الإلكترونية لكي يستطيعوا مواكبة التطور الإجرامي في الفضاء التقني.

الفرع الثاني

الضبط في الجرائم الإلكترونية

الضبط من أهم الإجراءات التي يسفر عنها التفتيش، وذلك للتحفظ على أدلة الجريمة التي يمكن استخدامها فيما بعد أثناء المحاكمة كدليل أدانة ضد المتهم بارتكاب جريمة إلكترونية، وعليه سنبين مسألة الضبط عبر ما هو تالٍ:

أولاً: ضبط المكونات المادية للأجهزة الإلكترونية:

إن ضبط المكونات المادية للأجهزة الإلكترونية لا يشكل أي خلاف بين الفقهاء، فجميع الأجزاء التي تتصل بالحاسب الآلي تصلح لأن تكون موضوع للضبط، ومن أمثلة هذه الأجزاء أجهزة الإدخال مثل لوحة المفاتيح والفارة والقلم الضوئي، ووحدات الحساب والمنطق بما تشمله من

---

[1] أمير فرج يوسف، المرجع السابق، ص٢٣٦، ٢٣٧.

[2] أسامة أحمد المناعسة وآخرين، **جرائم الحاسب الآلي والإنترنت**، المرجع السابق، ص٢٨٣ وما بعدها.

دوائر إلكترونية، ووحدات الاتصال مثل المودم والذي يمّكن الاتصال بالإنترنت[١]، وكذلك وحدات التخزين مثل الذاكرة الرئيسية والأقراص الصلبة والمرنة، ووحدات الإخراج مثل الطابعة والشاشة، ومن التشريعات التي تجيز ضبط المكونات المادية للحاسب الآلي التشريع اليوناني والكندي[٢].

ثانياً: ضبط المكونات المعنوية للأجهزة الإلكترونية:

أثار موضوع ضبط الكيانات المعنوية للأجهزة الإلكترونية خلافاً واسعاً بين الفقهاء، حيث ذهب رأي منهم إلى القول بأن الكيانات المعنوية للحاسب الآلي لا تصلح أن تكون محلاً للضبط، والعلة في ذلك أن نصوص القوانين الإجرائية تشترط الطابع المادي الملموس في هذه الكيانات لكي تصلح أن تكون محلاً للضبط، وقال هذا الرأي بأن المخرج لذلك هو إخراج الكيانات المعنوية وتحويلها إلى كيان مادي مثل طباعتها أو تصويرها أو غيرها من الوسائل المادية[٣]، وهذا الأمر يتطلب تدخل من قبل المشرع للنص على صلاحية ضبط الكيانات المعنوية، ورفع كفاءة مأموري الضبط القضائي ليستطيعوا مواجهة مثل هذه الحالات[٤].

أما الرأي الثاني من الفقه وهو ما ذهب إليه الفقه اليوناني والكندي بأن الكيانات المعنوية للأجهزة الإلكترونية تصلح لأن تكون محلاً للضبط، مثلها مثل الكيانات المادية[٥]، وهذا الرأي ما نؤيده.

ونص المشرع الفلسطيني على أنه: "...٢-يتم ضبط جميع الأشياء التي يعثر عليها أثناء إجراء التفتيش، والمتعلقة بالجريمة وتحرز وتحفظ وتثبت في محضر التفتيش، وتحال إلى الجهات المختصة.."[٦]، وكذلك نص المشرع الأردني على أنه: "...١-يضبط المدعي العام الأسلحة وكل ما يظهر أنه استعمل في ارتكاب الجريمة، أو أعد لهذا الغرض كما يضبط كل ما يرى من آثار الجريمة وسائر الأشياء التي تساعد على إظهار الحقيقة"[٧].

---

[١] خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، المرجع السابق، ص١٩٥، ١٩٦.

[٢] هلالي عبد اللاه أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي**، المرجع السابق، ص٢٧٦.

[٣] رامي متولي القاضي، المرجع سابق ، ص١٢٢ .

[٤] بكري يوسف بكري، المرجع السابق، ص١٣٦، ١٣٧.

[٥] خالد عياد الحلبي، المرجع السابق، ص ١٧٥ .

[٦] راجع المادة رقم ٥٠/٢ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٧] راجع المادة رقم ٣٢/١ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

ويعد التفتيش والضبط من الإجراءات الهامة في عملية الكشف عن الحقيقة في الجرائم الإلكترونية، والتي يجب أن تتم طبقاً للشروط التي حددها القانون، وفي ذلك صدر حكم بالبراءة في أحدى محاكم الجنح المصرية عام ٢٠٠٦م لشاب أتهم باختراقه لموقع المنظمة العربية للتنمية الإدارية التابعة لجامعة الدول العربية على الإنترنت، وعطل هذا الشاب الموقع وأجرى تعديل لبعض الملفات، وجاء الحكم بالبراءة لبطلان إجراءات التفتيش والضبط[١].

ونخلص مما سبق أن ضبط كل ما يتعلق بجريمة إلكترونية يساعد في الكشف عن الحقيقة، خاصة أن الكيانات المعنوية للحاسب الآلي هي أهم بكثير من الكيانات المادية، فالرسائل والبرامج والمنشورات هي التي ينبغي على النيابة العامة ضبطها، وهذه غالباً ما تكون مخزن في ذاكرة الحاسب الآلي أو على الإيميل، فعلى سبيل المثال عند قيام شخص بنشر صور فاضحة لآخر، فإن موضوع الجريمة والمراد ضبطه فيها هو تلك الصور وليس الأجهزة الإلكترونية، وعليه فإذا أمكن تحويل الكيانات المعنوية الإلكترونية إلى كيانات مادية فذلك أفضل، حيث أن هذه الكيانات ستعرض على القاضي المختص بنظر النزاع، وإن عرضها على هيئة مادية هو أسهل من عرضها إلكترونية، أما إذا لم يكن ممكناً تحويل هذه الكيانات إلى وسائل مادية، فنفضل عرضها كما هي على القاضي، وله في النهاية سلطة تقدير مدى أمكانية الأخذ بها كدليل أثناء المحاكمة.

الفرع الثالث

الاستماع لشهادة الشهود في الجرائم الإلكترونية

الشاهد طرف محايد في الدعوى الجزائية، فهو يدلي بشهادته أمام وكيل النيابة تحت القسم القانوني حول جريمة وقعت أمامه وأدركها بحاسة من حواسة، ولذلك يتعين على النيابة احترام الشاهد ومعاملته معاملة حسنه كونه خادماً للعدالة[٢]. ويعد المحقق هو صاحب القرار في شأن الاستماع للشهود، فهو من يقرر من يسمع من الشهود ومن لا يسمعه، ويرجع ذلك إلى ذكاء المحقق وفطنته، كما أن للمحقق أن يستمع لأي شاهد يحضر من تلقاء نفسه للإدلاء بالشهادة،

---

[١] عبد الصبور عبد القوي مصري، **الجريمة الإلكترونية**، دار العلوم للنشر والتوزيع، القاهرة، ٢٠١٠م، ص٦٥.

[٢] عبد الرحمن توفيق أحمد، المرجع السابق، ص٣٠٢.

فالمبدأ في ذلك أن الشاهد لا يرد[١]، ويجب على المحقق أن يقوم بتحليف الشاهد اليمين قبل تدوين أقواله[٢].

والشاهد في مجال الجريمة الإلكترونية قد يكون الفني أو الخبير، والتي تكون لديه المعلومات الجوهرية التي تتعلق بجريمة إلكترونية معينة قد انتدب لها، ولذلك يعد الخبير شاهد كونه يطلع على أسرار الواقعة وهو وحده يعلم خفاياها، ومن هؤلاء الشهود المبرمجون والمحللون ومهندسو الصيانة والاتصالات، ولذلك يجب على الشاهد الإلكتروني أن يقوم بتقديم كل المعلومات التي يعلمها لسلطات التحقيق والتي تساعد في الدخول إلى نظام المعالجة الآلية للبيانات وذلك بحثاً عن أدلة الجريمة[٣].

ويجب على الشاهد في الجرائم الإلكترونية أن يقوم بتزويد سلطات التحقيق بجميع البيانات والمعلومات التي يعلمها والتي تفيد في كشف الحقيقة، وهو ملزماً في ذلك، ومن العناصر الجوهرية التي يجب على الشاهد أن يخبر بها سلطات التحقيق البيانات والمعلومات المخزنة على الجهاز الإلكتروني، وأن يقوم بطباعتها متى أمكن ذلك، ويجب على الشاهد الإفصاح عن كلمات المرور السرية التي يعلم بها، وعن الشفرات الخاصة بالبرامج والأنظمة[٤].

---

[١] عبد العال الديربي، محمد صادق إسماعيل، المرجع السابق، ص٣١٢.

[٢] نصت المادة رقم ٨٠ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م على أنه: " يدلي الشهود بأقوالهم فرادى أمام وكيل النيابة بعد حلف اليمين بحضور كاتب التحقيق، ويحرر محضر بإفادتهم والأسئلة الموجهة إليهم"، وكذلك نصت المادة رقم ٩٣ من قانون البينات الفلسطيني رقم ٤ لسنة ٢٠٠١م على أنه: " على الشاهد أن يحلف يميناً بأن يقول الحق و لا شيء غير الحق وإلا لا تسمع شهادته، ويكون الحلف على حسب الأوضاع الخاصة بديانته ومعتقداته إن طلب ذلك"، كما نصت المادة رقم ٧١ من قانون أصول المحاكمات الجزائية الأردني لسنة ١٩٦١م على أنه: " يتثبت المدعي العام من هوية الشاهد ثم يسأله عن اسمه وشهرته وعمره ومهنته وموطنه وهل هو في خدمة أحد الفريقين أو من ذوي قرباه وعن درجة القرابة ويحلفه بأن يشهد بواقع الحال بدون زيادة أو نقصان وبدون جميع ذلك في المحضر".

[٣] الشحات إبراهيم منصور، **الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠١١م، ص١٩٧، ١٩٨.

[٤] هلالي عبد اللاه أحمد، **التزام الشاهد بالإعلام في الجرائم المعلوماتية**، الطبعة الأولى، دار النهضة العربية، الإسكندرية، ١٩٩٧م، ص٥٩ وما بعدها.

الفرع الرابع

الاستجواب في الجرائم الإلكترونية

يعرف الاستجواب بأنه: "إجراء من إجراءات التحقيق يتم بمناقشة المشتبه فيه حول الواقعة ومعرفة مدى صلته بها، ومناقشته حول الأدلة القائمة ضده تفصيلاً، سواء كانت هذه الأدلة مادية أو بأقوال المجني عليه والشهود أو غيره من الشركاء"[١].

والاستجواب من أهم إجراءات التحقيق الابتدائي، حيث يقوم المحقق باستجواب المتهم ومناقشته بالأدلة التي تدينه مناقشة تفصيلية[٢]، فإما أن ينكر المتهم وإما أن يعترف، والاستجواب يتم في مرحلة التحقيق الابتدائي ولا يتم في مرحلة المحاكمة إلا إذا قبل المتهم ومحاميه بذلك، ولا يتم الاستجواب بدون توجيه التهمة المناسبة للجاني، ومناقشته بالأدلة التي تؤكد هذه التهمة، ويجب إحاطة المتهم بكافة النتائج التي سيسفر عنها التحقيق[٣].

ولا يجوز للمحقق أن يباشر في استجواب المتهم إلا بعد أن يستمع إلى أقوال الشهود، وبعد جمع الأدلة الكافية التي يناقش فيها المتهم تفصيلاً، ويبني عليها في النهاية اتهامه للمتهم، كما يعطي القانون ضمانات عديدة للمتهم أثناء الاستجواب، من ضمنها حق المتهم في الامتناع عن الاجابة، ويحق للمتهم أن يطالب بتأجيل الاستجواب ٢٤ ساعة إلى حين حضور المحامي، ولا يجوز لسلطات التحقيق أن تحلّف المتهم اليمين، أو تستخدم وسائل الإكراه أو الإغراء ضده[٤].

ويفضل عند إجراء الاستجواب حضور خبير إلكتروني، لأن الخبير قد يساعد المحقق في توجيه الأسئلة الفنية التي قد لا يعلم بها المحقق، وكذلك يمّكن الخبير المحقق من استيعاب بعد الألفاظ التي قد يرددها المتهم[٥].

---

[١] أمين محمد نوفل، تمام يوسف نوفل، **الوجيز في أصول التحقيق الجنائي**، كلية الشرطة الفلسطينية، غزة، ٢٠١٣م، ص١٠٩.

[٢] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٨١٤.

[٣] خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، المرجع السابق، ص٢٤١، ٢٤٢.

[٤] سليم الزعنون، **التحقيق الجنائي**، الجزء الأول، الطبعة الرابعة، المؤسسة العربية للدراسات والنشر، بيروت، ٢٠٠١م، ص١٩٦.

[٥] عبد القادر جرادة، **دستور الاستدلال والتحقيق الجنائي**، المرجع السابق، ص٣٦٤.

ونرى مما تقدم وجود حاجة ماسة للنهوض لرفع كفاءات المحققين لدي الشرطة وكذلك النيابة العامة، مع توفير الأجهزة الإلكترونية الحديثة التي تساعد في التحقيق في الجرائم الإلكترونية، أما في الوقت الحالي فيجب الاستعانة بالخبراء في المجال الإلكتروني في جميع مراحل التحقيق وكذلك الاستدلال، وذلك للبحث عن الأدلة الإلكترونية والتحفظ عليها من الضياع أو الإتلاف، فالخبير يساعد على التفتيش والضبط والتحقيق مع المشتبه بهم وسماع أقوال الشهود وكذلك استجواب المتهمين، وأما النقطة الأخيرة والتي تتعلق بالتفتيش والضبط خارج حدود الدولة، فكما نعلم أن الجريمة الإلكترونية عابر للحدود، فيجب على الدول العربية العمل على إنشاء قانون عربي موحد يكافح الجرائم الإلكترونية، ويجب أيضاً أن تنضم دولة فلسطين للاتفاقيات الدولية التي تعني بمكافحة الجرائم الإلكترونية، لتستطيع من خلالها أن تجري تحقيقاتها المتعلقة بالجرائم الإلكترونية داخل وخارج حدود الوطن.

وبعد الانتهاء من إجراءات التحقيق الابتدائي نرى حاجة التشريع الفلسطيني إلى استحداث نصوص قانونية جديدة تنظيم إجراءات التحقيق الابتدائي بما تشمله من التفتيش والضبط وتدوين أقوال الشهود واستجواب المتهمين، وكذلك فيما يتعلق بالضمانات التي يجب أن يحاط بها المتهمين في الجرائم الإلكترونية، خاصة أصحاب الأجهزة الإلكترونية التي يتم ضبطها ومصادرتها لاسيما إذا كانت تحتوي على بيانات أو معلومات تمس حياتهم الشخصية.

المبحث الثالث

المحاكمة في الجرائم الإلكترونية

السلطة القضائية هي السلطة الوحيدة التي خولها القانون صلاحية الفصل في المنازعات التي تنشأ بين الأفراد، وقد منح القانون هذه السلطة الاستقلالية التامة[1]، فهي تصدر أحكامها في الوقائع التي تنظر فيها دون تدخل من أي سلطة أخرى[2]، وأكد على ذلك نص المادة رقم ١ و٢ من قانون السلطة القضائية الفلسطيني رقم ١ لسنة ٢٠٠٢م حيث نص على أن: "السلطة القضائية

[1] نصت المادة رقم ٩٨ من القانون الأساسي الفلسطيني المعدل لسنة ٢٠٠٣م على أنه: " القضاة مستقلون، لا سلطان عليهم في قضائهم لغير القانون، ولا يجوز لأية سلطة التدخل في القضاء أو في شؤون العدالة".

[2] سالم أحمد الكرد، **أصول الإجراءات الجزائية في التشريع الفلسطيني**، الكتاب الثاني، الطبعة الثالثة، كلية الشرطة الفلسطينية، غزة، ٢٠٠٨م، ص٥.

مستقلة، ويحظر التدخل في القضاء أو في شؤون العدالة"، و" القضاة مستقلون لا سلطان عليهم في قضائهم لغير القانون"[١].

وتختلف مرحلة المحاكمة –أو كما سماها البعض مرحلة التحقيق النهائي– عن مرحلة التحقيق الابتدائي، فالسلطة التي تختص بالتحقيق الابتدائي هي النيابة العامة، أما السلطة القائمة على المحاكمة فهم قضاة المحاكم، وتختلف المرحلتان في أن التحقيق الابتدائي يهدف للبحث عن الأدلة التي تدين المتهم أو تبرءه وأحاله الدعوى إلى المحكمة المختصة، أما المحكمة فإن عملها يكمن في الفصل في الدعوى القائمة أمامها والفصل فيها إما بالإدانة أو البراءة أو أي قرار آخر يصدر عنها مثل الإسقاط أو عدم الاختصاص[٢].

وفي الواقع إن إجراءات المحاكمة في الجرائم الإلكترونية لا تختلف عن إجراءات المحاكمة في الجرائم التقليدية، مع العلم أن القاضي ينظر في جرائم جديدة عليه، لم يسبق له النظر فيها، فعلى سبيل المثال استعان قاضي محكمة باريس في إحدى القضايا بخبيرين أحدهما انجليزي والثاني أمريكي بالإضافة الى فرنسي لأعداد تقرير حولَ إمكانية رصد مسار الإنترنت[٣]، ولذلك يجب العمل على توظيف خبراء ليستعين بهم القضاة أثناء المحاكمة، حيث أن الجرائم الإلكترونية كما نعلم جرائم حديثة ومعقدة، وهناك بعض المصطلحات التي يصعب على القضاة فهمها، فإن الخبير يساعد في تيسير هذه المصطلحات على القضاة في أبسط صورة.

وعلى ضوء ما سبق سنبين مرحلة المحاكمة في الجرائم الإلكترونية من خلال المطلبين التاليين:

المطلب الأول : الجهة المختصة بالمحاكمة في الجرائم الإلكترونية.

المطلب الثاني : إجراءات المحاكمة في الجرائم الإلكترونية.

---

[١] راجع المادة رقم ١، ٢ من قانون السلطة القضائية الفلسطيني رقم ١ لسنة ٢٠٠٢م.

[٢] فخري عبد الرازق الحديثي، **شرح قانون أصول المحاكمات الجزائية**، المرجع السابق، ص٣٠٤.

[٣] أنظر توصيات عمر محمد يونس، **الجرائم الناشئة عن استخدام الإنترنت**، رسالة دكتوراه، جامعة عين شمس/كلية الحقوق، ٢٠٠٤م.

المطلب الأول

الجهة المختصة بالمحاكمة في الجرائم الإلكترونية

يختص القضاء الفلسطيني بالنظر في الدعاوي والطلبات المدنية والجزائية التي تعرض أمامه، وهناك قواعد قانونية تحدد اختصاص كل محكمة[١] للنظر بالدعاوي الجزائية، وتعتبر هذه القواعد آمره بحيث لا يجوز لأطراف النزاع الاتفاق على ما يخالفها[٢]، ونصت المادة رقم ١ من قانون تشكيل المحاكم النظامية الفلسطيني رقم ٥ لسنة ٢٠٠١م على أنه: "١-تنظر المحاكم النظامية في فلسطين في المنازعات والجرائم كافة إلا ما استثني بنص قانوني خاص، وتمارس سلطة القضاء على جميع الأشخاص، ٢-تحدد قواعد اختصاص المحاكم وتباشر اختصاصها وفقاً للقانون"[٣].

ولذلك فعند وقوع جريمة معينة يجب أن تكون هناك محكمة محددة من بين المحاكم الجنائية تتولى سلطة الفصل في الدعوى الجنائية الناشئة عن ارتكاب تلك الجريمة[٤]. فالاختصاص هنا هو السلطة التي يقررها القانون للقضاء في أن ينظر في دعوى من نوع معين حدده القانون[٥].

ونص المشرع الأردني على المحاكم النظامية وجعلها صاحبة الاختصاص بالنظر في الدعاوي المدنية والجزائية حيث نص المشرع الأردني على أنه: " تمارس المحاكم النظامية في المملكة حق القضاء على جميع الاشخاص في جميع المواد المدنية والجزائية باستثناء المواد التي يفوض فيها حق القضاء الى محاكم دينية أو محاكم خاصة بموجب أحكام أي قانون اخر"[٦].

---

[١] عرف القانون التفسيري الفلسطيني رقم ٩ لسنة ١٩٤٥م في المادة رقم ٢ المحكمة بأنها: " أية محكمة من محاكم فلسطين ذات اختصاص".

[٢] عبد القادر جرادة، **موسوعة الإجراءات الجزائية في التشريع الفلسطيني**، المجلد الثالث، مكتبة آفاق، غزة، عدد بئر السبع، ٢٠٠٩م، ص١٠٢٢ وما بعدها.

[٣] راجع المادة رقم ١ من قانون تشكيل المحاكم النظامية الفلسطيني رقم ٥ لسنة ٢٠٠١م.

[٤] عبد الرؤوف مهدي، المرجع السابق، ص١٠٦٥.

[٥] محمود نجيب حسني، المرجع السابق، ص٣٥٩.

[٦] راجع المادة رقم ٢ من قانون تشكيل المحاكم النظامية الأردنية رقم ١٧ لسنة ٢٠٠١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:I /http://www.lob.gov.jo.

الفرع الأول

الاختصاص القضائي في القانون الفلسطيني

يعتبر الاختصاص القضائي هو صلاحية القاضي العادي لمباشرة ولايته القضائية في نطاق معين، ومن هنا يجب التمييز بين ولاية القضاء والاختصاص، فالأولى تضفي على القاضي الصلاحية المجردة لمباشرة جميع إجراءات الخصومة المدنية والجنائية، أما الثانية تقصر هذه الصلاحية على نوع معين من الإجراءات وفي حدود معين[١].

وتختص المحاكم الفلسطينية بالنظر في القضايا والدعاوي المعروضة أمامها وفقاً لأحكام القانون، ونص المشرع الفلسطيني على أنه: "يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة، أو الذي يقيم فيه المتهم، أو الذي يقبض عليه فيه"[٢]، ونستنتج من نص القانون السابق أن هناك ثلاث قواعد أساسية لتحديد المحكمة المختصة للنظر بموضوع الجريمة، القاعدة الأولى مكان وقوع الجريمة، فإذا أخترق جهاز إلكتروني، أو نظام بنكي معين فإن المحكمة صاحبة الاختصاص هي محكمة وقوع الجريمة، والقاعدة الثانية مكان إقامة المتهم، فإذا وقعت جريمة نشر صور إباحية عبر الإنترنت فإن المحكمة المختصة هي المحكمة التي تختص بمكان إقامة المتهم، والقاعدة الثالثة المكان الذي يقبض عليه المتهم، فإذا ارتكب الجاني جريمة إلكترونية وهرب فإن المحكمة المختصة هي المحكمة صاحبة الاختصاص في المكان الذي يقبض عليه المتهم[٣].

ولذلك يعد الاختصاص قيد على سلطة القاضي في مباشرة أعمال وظيفته إذ يحدد الإطار الذي في داخلة يستطيع كل قاضي أن يمارس أعمال وظيفته[٤].

ونص المشرع الفلسطيني على حالات الشروع والجرائم المستمرة وجرائم الاعتياد والجرائم المتتابعة، وحدد اختصاص النظر فيها بالمكان أو الأماكن التي وقعت ضمنها الجريمة، " في حالة الشروع تعتبر الجريمة أنها وقعت في كل مكان يقع فيه عمل من أعمال البدء في التنفيذ، وفي

---

[١] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٧٠٤.

[٢] راجع المادة رقم ١٦٣ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] سالم أحمد الكرد، المرجع السابق، ص٤٤.

[٤] أمال عبد الرحيم عثمان، **شرح قانون الإجراءات الجنائية**، الهيئة المصرية العامة للكتب، ١٩٩١م، ص٢٨٦.

الجرائم المستمرة يعتبر مكاناً للجريمة كل محل تقوم فيه حالة الاستمرار، وجرائم الاعتياد والجرائم المتتابعة يعتبر مكاناً للجريمة كل محل يقع فيه أحد الأفعال الداخلة فيها"[١].

أما الجرائم التي تقع خارج حدود فلسطين، وينطبق عليها قانون العقوبات الفلسطيني فإن المتضرر يحق له أن يرفع الدعوى الجزائية أمام المحكمة في العاصمة القدس[٢]، وهنا نقف لأن هذه الحالة قد تترتب على الجرائم الإلكترونية، مثل أن يقوم فلسطيني بارتكاب جريمة من الجرائم الإلكترونية – التي يعاقب عليها قانون العقوبات الفلسطيني – على فلسطيني آخر فيحق للمجني عليه أن يرفع الدعوى أمام المحاكم في العاصمة القدس، ونأتي هنا إلى إشكالية ثانية، وهي أنه يصعب أن تقام دعوى في المحاكم في العاصمة القدس وذلك بسبب الاحتلال الإسرائيلي والذي قسم الوطن وشتت البشر، ولذلك فإننا نفضل أن تقام الدعوى أمام المحاكم الفلسطينية في أي مدينة فلسطينية[٣].

وإذا تعدد المتهمون في الدعوى وقبض على أحدهم فينعقد الاختصاص للمحكمة التي يقيم ضمن اختصاصها أحدهم أو يقبض عليه فيها، وذلك تماشياً مع مبدأ وحدة الدعوى الجزائية[٤].

ونخلص مما سبق أن الاختصاص هو الذي يحدد نصيب القاضي الذي تقررت له ولاية القضاء من الدعاوي التي تكون له صلاحية الفصل فيها، إذ من غير المعقول أن يكون لكل قاض صلاحية الفصل في جميع القضايا[٥].

---

[١] راجع المادة رقم ١٦٤ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٢] ساهر إبراهيم الوليد، **الوجيز في شرح قانون الإجراءات الجزائية الفلسطيني**، الجزء الثاني، الطبعة الثالثة، ٢٠١١م، ص٤٢.

[٣] نصت المادة رقم ١٦٥ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م على أنه: " إذا وقعت في الخارج جريمة من الجرائم التي تسري عليها أحكام القانون الفلسطيني، ولم يكن لمرتكبها محل إقامة في فلسطين، ولم يضبط فيها، ترفع عليه الدعوى أمام المحكمة المختصة في العاصمة القدس".

[٤] طارق محمد الديراوي، **الوجيز في شرح قانون الإجراءات الجزائية الفلسطيني**، الجزء الثاني، الطبعة الاولى، ٢٠١٣م، ص٥٧.

[٥] عبد الرؤوف مهدي، المرجع السابق، ص١٠٦٤.

ومن أمثلة الجرائم التي يتوافر فيها تعدد في أماكن وقوعها مثل جريمة التصنت على معلومات حاسب آلي، أو نشر فايروس بهدف إتلاف النظام الإلكتروني، أو الدخول بطريقة الغش إلى نظام المعالجة الآلية للمعطيات الإلكترونية[١].

ونص المشرع الفلسطيني على أنه: "إذا ارتكب فعل بعضه داخل نطاق اختصاص المحاكم الفلسطينية وبعضه خارج نطاق اختصاصها، وكان ذلك الفعل يؤلف جرماً تنطبق عليه أحكام قانون العقوبات الفلسطيني فيما لو ارتكب بأكمله ضمن نطاق اختصاص المحاكم الفلسطينية، فكل شخص ارتكب أي جزء من ذلك الفعل ضمن نطاق اختصاص المحاكم الفلسطينية، تجوز محاكمته بمقتضى قانون العقوبات الفلسطيني كما لو كان قد ارتكب ذلك الفعل بأكمله ضمن نطاق اختصاص تلك المحاكم"[٢]، وتعتبر هذه المادة من أهم المواد التي تنطبق عليها الجرائم الإلكترونية، وذلك لأن أغلب الجرائم الإلكترونية ترتكب من دولة وآثارها في دولة أخرى، وقد تتعدى آثار هذه الجريمة إلى عدة دول مثل جريمة نشر الفيروسات أو المواد الإباحية، فإن توافرت الحالات التي ذكرها المشرع في النص السابق، فإن الاختصاص يترتب للمحاكم الفلسطينية كما لو وقعت الجريمة كاملة داخل حدود فلسطين.

الفرع الثاني

الاختصاص القضائي في القانون الأردني

الاختصاص كما قلنا هو صلاحية أداة وظيفة قضائية معينة، على نحو يعترف فيه القانون بالأعمال التي تمارس بها هذه الوظيفة، ومصدر تحديد الاختصاص هو القانون[٣].

فلا يكفي لكي يستجمع الحكم سلامته القانونية أن يكون صادراً من محكمة قضائية مشكلة تشكيلاً قانونياً، إنما يلزم فوق ذلك أن يكون الحكم صادر من محكمة لها الاختصاص في اصداره[٤].

ولم يختلف القانون الأردني عن القانون الفلسطيني من حيث تعيين اختصاص النظر بالدعاوي الجزائية، إلا أن المشرع الأردني نص صراحة على الجرائم الإلكترونية، وحدد اختصاص

---

[١] عبد القادر جرادة، **موسوعة الإجراءات الجزائية**، المجلد الثالث، المرجع السابق،ص١٠٥٧.

[٢] راجع المادة رقم ١٦٦ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] محمود نجيب حسني، المرجع السابق، ص٣٥٩.

[٤] محمد زكي ابو عامر، **الإجراءات الجنائية**، منشأة المعارف، الإسكندرية، ١٩٩٤م، ص٧٣٥.

المحاكم الأردنية بالنظر فيها إذا ارتكبت الجريمة الإلكترونية خارج الأردن وترتبت آثارها كلياً أو جزئياً داخل الأردن.

ونص المشرع الأردني على أن: "١-تقام دعوى الحق العام على المشتكى عليه أمام المرجع القضائي المختص التابع له مكان وقوع الجريمة، أو موطن المشتكى عليه، أو مكان إلقاء القبض عليه، ولا أفضلية لمرجع على آخر الا بالتاريخ الأسبق في إقامة الدعوى لديه..."[١]، وتدرج المشرع الأردني في تعيين قواعد الاختصاص، الأولى مكان وقوع الجريمة، والثانية موطن المتهم، والثالثة مكان القبض على المتهم[٢].

ونص المشرع الأردني على الشروع والجرائم المستمرة والجرائم المتتابعة وجرائم الاعتياد، وحدد المشرع في الحالات السابقة محل وقوع أفعال الشروع[٣]، أو محل وقوع الجرائم المستمرة أو المتتابعة أو الاعتياد، هو محل إقامة الدعوى الجزائية، ونص المشرع الاردني في ذلك على أنه: "٢-في حالة الشروع تعتبر الجريمة أنها وقعت في كل مكان وقع فيه عمل من أعمال البدء في التنفيذ، وفي الجرائم المستمرة يعتبر مكاناً للجريمة كل محل تقوم فيه حالة الاستمرار، وفي جرائم الاعتياد والجرائم المتتابعة يعتبر مكاناً للجريمة كل محل يقع فيه أحد الأفعال الداخلة فيها..."[٤].

وإذا وقعت جريمة مما نص عليه القانون الأردني خارج حدود الأردن، ولم يكن الجاني له محل اقامة معروف في الأردن ولم يتم إلقاء القبض عليه فتقام عليه الدعوى في العاصمة[٥]، "٣-إذا وقعت في الخارج جريمة من الجرائم التي تسري عليها أحكام القانون الاردني، ولم يكن لمرتكبها محل إقامة معروف في المملكة الأردنية الهاشمية، ولم يلُق القبض عليه فيها فتقام دعوى الحق العام عليه أمام المراجع القضائية في العاصمة"[٦].

---

[١] راجع المادة رقم ٥/١ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٢] فخري عبد الرازق الحديثي، **شرح قانون أصول المحاكمات الجزائية**، المرجع السابق، ص٣٢٧.

[٣] طارق محمد الديراوي، المرجع السابق، ص٥٦.

[٤] راجع المادة رقم ٥/٢ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٥] سالم أحمد الكرد، المرجع السابق، ص٥٠.

[٦] راجع المادة رقم ٥/٣ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

إن القاعدة العامة في الفقه القانوني الدولي أن الاختصاص القضائي للجرائم الإلكترونية التي ترتكب عبر الإنترنت هو محل تحقق النتيجة الإجرامية، سواء كان الجاني يقيم في دولة أخرى أو كان في نفس الدولة[١]، وهذا ما أكد عليه المشرع الأردني حيث نص على أنه: "٤- يجوز اقامة دعوى الحق العام على المشتكى عليه أمام القضاء الأردني إذا ارتكبت الجريمة بوسائل إلكترونية خارج المملكة وترتبت آثارها فيها، كلياً أو جزئياً، أو على أي من مواطنيها"[٢].

ونرى مما سبق أن القانون الأردني قد تميز عن القانون الفلسطيني في الجزئية السابقة، حيث نص المشرع الأردني على الجرائم الإلكترونية وتعيين الاختصاص القضائي عند ارتكابها، ولذا ندعو المشرع الفلسطيني أن ينص صراحة على الاختصاص القضائي للجرائم الإلكترونية، مثلما نص عليها المشرع الأردني.

المطلب الثاني

إجراءات المحاكمة في الجرائم الإلكترونية

الإحالة هو الإجراء الذي يترتب عنه دخول الدعوى في حوزة المحكمة، ويصدر قرار الإحالة من وكيل النيابة ويعتبر قراره نهائي لا يخضع لعرضه على النائب العام في الجنح، أما في الجنايات فإن الإحالة من اختصاص النائب العام، وقد تخل الدعوى في حوزة المحكمة بطرق أخرى مثل التكليف بالحضور[٣]. كما أن قرر الإحالة لا يقبل للطعن فيه من أي خصم من الخصوم، ولهم أن يتقدموا بدفوعهم أمام محكمة الموضوع[٤].

إن أول ما تتبعه المحكمة بعد انعقاد الرابطة الإجرائية القضائية أمامها هو اعلان المتهم كي يحضر وكذلك الخصوم[٥]، وصنف المشرع الفلسطيني الجرائم الإلكترونية في قانون العقوبات رقم ٧٤ لسنة ١٩٣٦م على أنها جنح، وكانت العقوبة عليها هي الحبس مدة لا تزيد عن سنة أو

---

[١] عادل عزام الحيط، المرجع السابق، ص٣٨٠.

[٢] راجع المادة رقم ٥/٤ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:I /http://www.lob.gov.jo.

[٣] راجع المادة رقم ٥٣، ١٥٢ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٤] طارق محمد الديراوي، المرجع السابق، ص١١٨، ١١٩.

[٥] رمسيس بهنام، المرجع السابق، ص٦٢٧.

الغرامة أو كلتا العقوبتان[١]، وبما أن الجرائم الإلكترونية قد صنفت جنح فالمحكمة المختصة بالنظر فيها هي محكمة الصلح، حيث نص المشرع الفلسطيني على أنه: " تختص محكمة الصلح بالنظر في جميع المخالفات والجنح، ما لم ينص القانون على خلاف ذلك"[٢].

والأصل في المحاكمة أن تتم بصورة علنية لضمان الصالح العام، إلا أن القانون أجاز نظر بعض الدعاوي في جلسات سرية لا يحضرها الجمهور، وذلك مراعاة للنظام العام والآداب العامة، ويجب على المحكمة بيان أسانيد ذلك تفصيلياً[٣].

أما المشرع الأردني فقد صنف الجرائم الإلكترونية إلى جنح وجنايات، وأصاب في ذلك فجريمة الدخول إلى نظام إلكتروني لا تتساوى مع جريمة الاستغلال الجنسي للأطفال عبر الإنترنت[٤].

الفرع الأول

إجراءات المحاكمة أمام محكمة الصلح

تدخل الدعوى الجزائية أمام قاضي الصلح بعد أن تودع لائحة اتهام بحق المتهم من قبل النيابة العامة، فقد نص المشرع على أنه: "لا يحال شخص إلى المحاكمة أمام محاكم الصلح في دعاوى الجنح، ما لم تودع بحقه لائحة اتهام من قبل النيابة العامة"[٥]، فالجهة المختصة بإحالة الدعوى إلى المحكمة هي النيابة العامة، وتبدأ المحكمة بالمناداة على الخصوم والشهود وسؤال المتهم عن أسمه ومهنته وبياناته والتي تحدد شخصيته، كما تطلع المحكمة على بطاقته الشخصية للتأكد من هذه البيانات[٦].

وتسير محكمة الصلح في المملكة الأردنية وفقاً لقانون أصول المحاكمات الجزائية وقانون محاكم الصلح، وتحال قضايا الجنح من وكيل النيابة، أو من محكمة أخرى إذا رأت المحكمة أنها

---

[١] راجع المادة رقم ٢٦٢ مكرر من قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ المعدل لسنة ٢٠١٠م.

[٢] راجع المادة رقم ٣٠٠ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، المرجع السابق، ص٧٤٢ وما بعدها.

[٤] راجع المادة رقم ٣، ٨ من قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

[٥] راجع المادة رقم ٣٠١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٦] عبد الرؤوف مهدي، المرجع السابق، ص١٢٩٦.

ليست من اختصاصها، أو من خلال مأموري الضبط القضائي بشكل مباشر، أو إذا وقعت الجنحة في قاعة المحكمة[١]، ونص المشرع الأردني على أنه: " يباشر القاضي النظر في الدعوى الجزائية الداخلة في اختصاصه بناء على شكوى المتضرر، أو تقرير من مأموري الضابطة العدلية، ويسير فيها وفق الأحكام المبينة في قانون أصول المحاكمات الجزائية إلا ما نص عليه في قانون محاكم الصلح هذا"[٢].

وتبدأ الإجراءات في محكمة الصلح بعد دخول الدعوى في حوزتها، من خلال تبليغ الخصوم وحضورهم[٣]، ونص المشرع الفلسطيني في ذلك على أنه: "١- عندما تودع لائحة الاتهام لدى قلم المحكمة، تنظم مذكرات بالحضور وتبلغ إلى النيابة العامة والمتهم والمدعي بالحق المدني والمسئول عن الحق المدني"[٤]، ونص المشرع الأردني في ذلك على أنه: "أ-في اليوم المعين للمحاكمة ، يستدعي القاضي الطرفين..."[٥].

ويجب أن تجري المحاكمة بصورة علنية إلا إذا قررت المحكمة جعل المحاكمة سرية حفاظاً على الآداب والأخلاق العامة[٦]، ومن ثم يتم الاستماع إلى البينات فيقوم وكيل النيابة بتلاوة التهم على المتهم، ومن ثم تدعم هذه التهم بالبينات، فتستمع المحكمة إلى الشهود شاهداً شاهداً، ويقوم الدفاع كذلك بتقديم البينات التي يحصل عليها ويقدمها إلى القاضي[٧]، وإن كان هناك أدلة أخرى مثل الأدلة الإلكترونية أو الأدلة الرقمية فيجوز تقديمها للأثبات أمام قاضي الصلح، ولكن يشترط لتقديم الأدلة الرقمية أمام القاضي أن يكون الحصول عليه تم بشكل مشروع، فإذا تم الحصول على الدليل من خلال تفتيش الأجهزة الإلكترونية يجب أن يكون التفتيش قد تم وفقاً للإجراءات القانونية[٨].

---

[١] فخري عبد الرازق الحديثي، **شرح قانون أصول المحاكمات الجزائية**، المرجع السابق، ص٣٥٩-٣٦١.

[٢] راجع المادة رقم ١٥ من قانون محاكم الصلح الأردني رقم ١٥ لسنة ١٩٥٢م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

[٣] طارق محمد الديراوي، المرجع السابق، ص١٢٢.

[٤] راجع المادة رقم ٣٠٣ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٥] راجع المادة رقم ٧ من قانون محاكم الصلح الأردني رقم ١٥ لسنة ١٩٥٢م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

[٦] عبد الرحمن توفيق أحمد، المرجع السابق، ص٣٤٤.

[٧] عبد القادر جرادة، **موسوعة الإجراءات الجزائية**، المرجع السابق، ص١٢١٦ وما بعدها.

[٨] خالد عياد الحلبي، المرجع السابق، ص٢٣٨ وما بعدها.

كما للنيابة العامة والمجني عليه والمدعي بالحقوق المدنية أن يستجوبوا الشهود المذكورين مرة ثانية لإيضاح الوقائع التي أدوا الشهادة عنها في أجوبتهم[١].

وفي إطار ذلك فقد نصت كلاً من إنجلترا والولايات المتحدة على تشريعات خاصة تنظم أدلة الأثبات المتحصل عليها من مخرجات الحاسب الآلي، ومن ذلك اعتبر الدليل الإلكتروني معترفاً به وذات أهمية في الدول التي ذكرناها وأكد على ذلك تشريعها لقوانين تنظم البينات الإلكترونية[٢].

وفي النهاية وبعد اطلاع قاضي الصلح على البينات التي يقدمها وكيل النيابة ويقدمها كذلك الدفاع يقوم القاضي بالنطق بالحكم، حيث نص المشرع الفلسطيني على أنه: "٢- يصدر القاضي حكمه خلال عشرة أيام، ما لم يوجب القانون صدوره خلال مدة أقصر من ذلك"[٣].

وكذلك نص المشرع الاردني على أنه: "٢- يصدر القاضي حكمه في ميعاد عشرة أيام ما لم يوجب القانون ميعاد أقصر من ذلك"[٤].

ومن خلال ما سبق تعد الأحكام الصادرة عن محكمة الصلح أحكام ابتدائية، ولذلك فهي تقبل الطعن أمام محاكم الاستئناف، وهذا ما سنوضحه في الفرع التالي.

الفرع الثاني

الطعن أمام محكمة الاستئناف

إن الحكم الصادر عن محكمة الصلح هو حكم قابل للاستئناف، حيث تعرض القضية بعد نظرها من قبل محكمة أول درجة على محكمة الدرجة الثانية، ويرجع استئناف الأحكام إلى مبدأ التقاضي على درجتين[٥]، والذي أخذ به الكثير من التشريعات ومنها القانون الفلسطيني والأردني،

---

[١] أمال عبد الرحيم عثمان، المرجع السابق، ص٦٤١.

[٢] محمد محمد الألفي، المرجع السابق، ص٤٠١ .

[٣] راجع المادة رقم ٣٠٩/٢ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٤] راجع المادة رقم ١٩٥/٢ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي: http://www.lob.gov.jo/ l.

[٥] عبد الرؤوف مهدي، المرجع السابق، ص١٥٩٧، محمد زكي ابو عامر، المرجع السابق، ص١٠٤٧.

ويتميز الاستئناف في إعادة طرح القضية أمام محكمة ثانية، وذلك بهدف الطعن في الحكم إذا كان يشوبه خطأ في الواقعة أو القانون[١].

ونص المشرع الفلسطيني في ذلك على أنه: "١-يجوز للخصوم استئناف الأحكام الحضورية والمعتبرة بمثابة الحضورية في الدعاوى الجزائية على النحو التالي: أ-إذا كانت صادرة عن محاكم الصلح تستأنف أمام محاكم البداية بصفتها الاستئنافية"[٢]، حيث أقر المشرع الفلسطيني أن الأحكام الصادرة عن محكمة الصلح تقبل الطعن أمام محكمة البداية بصفتها استئنافية، وهذا ما يمثل مبدأ التقاضي على درجتين، ويجب أن يقدم الاستئناف خلال خمسة عشر يوماً تبدأ من اليوم التالي لتاريخ النطق بالحكم[٣]. فالاستئناف تنظيم إجرائي مقصود به تصحيح سائر الاخطاء التي تصيب الحكم[٤].

ونص المشرع الأردني على أنه: " تقبل الطعن بطريق الاستئناف: ٢- الاحكام الصلحية التي ينص قانون محاكم الصلح على انها تستأنف الى محكمة الاستئناف"[٥]، فكذلك نص المشرع الأردني على أن الأحكام الصادر عن محكمة الصلح تقبل الاستئناف، ذلك مثلما نص عليه المشرع الفلسطيني، وهذا هو الطريق المألوف الذي يسلكه المحكوم عليه من محكمة أول درجة، للتظلم إلى محكمة أعلا درجة وأكثر كفاءة[٦].

---

[١] سالم أحمد الكرد، المرجع السابق، ص٤٤.

[٢] راجع المادة رقم ٣٢٣/١ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] نصت المادة رقم ٣٢٨ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١معلى أنه: " يكون الاستئناف بإيداع عريضة الاستئناف لدى قلم المحكمة التي أصدرت الحكم، أو قلم محكمة الاستئناف خلال خمسة عشر يوماً تبدأ من اليوم التالي لتاريخ النطق بالحكم إذا كان حضورياً، أو من تاريخ تبليغه إذا كان بمثابة الحضوري".

[٤] محمد زكي ابو عامر، المرجع السابق، ص١٠٤٨.

[٥] راجع المادة رقم ٢٥٦/٢ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي: http://www.lob.gov.jo/l.

[٦] محمد علي الحلبي، **الوسيط في شرح قانون أصول المحاكمات الجزائية**، الجزء الثالث، دار الثقافة، عمان، ١٩٩٦، ص٢٣٥.

الفرع الثالث

الطعن بالنقض

الطعن بالنقض من طرق الطعن الغير عادية، والتي يهدف من خلالها المشرع إلى التأكد من سلامة الحكم الذي صدر، ومدى مطابقته للقانون[١] من حيث القواعد الموضوعية أو القواعد الإجرائية التي استند إليها خلال مرحلة المحاكمة، ونص المشرع الفلسطيني على أنه: "تقبل الأحكام الصادرة من محكمة البداية بصفتها الاستئنافية ومن محكمة الاستئناف في الجنايات والجنح الطعن بالنقض، ما لم ينص القانون على خلاف ذلك"[٢]، ويتميز الطعن بالنقض عن الطعن بالاستئناف في أن الطعن بالنقض لا يهدف إلى إعادة الدعوى من جديد أمام المحكمة، بل يهدف إلى البحث عن مدى صحة التكييف القانوني للواقع المنظور فيها أمام المحكمة، وتعتبر الأحكام الصادرة عن محكمة البداية بصفتها استئنافية قابلة للطعن أمام محكمة النقض[٣]، وإذا قررت محكمة النقض رد الطعن فيعتبر الحكم هنا باتاً غير قابل للطعن بأي شكل من الأشكال، ونص في ذلك المشرع الفلسطيني على أنه: "إذا قررت محكمة النقض رد طلب الطعن بالنقض، أصبح الحكم باتاً، ولا يجوز بأي حال لمن رفعه أن يرفع طعناً آخر عن الحكم ذاته لأي سبب كان"[٤]، وإذا قررت المحكمة قبول طلب الطعن فإنها تنظر في الدعوى.

تعد محكمة التمييز في الأردن محكمة قانون، والطعن أمامها بالأحكام من طرق الطعن الغير عادية، ولذلك سميت هذه المحكمة بمحكمة التمييز أو محكمة النقض أو محكمة التعقيب، وتنظر هذه المحكمة في الأحكام الجنائية فقط، والأحكام التي تصدر عن محكمة أمن الدولة[٥]، وفي وفي ذلك فقد نص المشرع الأردني على أنه: "يقبل الطعن بطريق التميز جميع الأحكام والقرارات الجنائية الصادرة عن محكمة الاستئناف، وقرار منع المحاكمة الصادرة من النائب العام في القضايا الجنائية"[٦].

---

[١] محمود نجيب حسني، المرجع السابق، ص١١٣٩.

[٢] راجع المادة رقم ٣٤٦ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٣] سالم أحمد الكرد، المرجع السابق، ص٤٤.

[٤] راجع المادة رقم ٣٧٣ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

[٥] عبد الرحمن توفيق أحمد، المرجع السابق، ص٤١٢.

[٦] راجع المادة رقم ٢٧٠ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo/ l.

الفرع الرابع

إعادة المحاكمة

إعادة المحاكمة من طرق الطعن الغير عادية، وبطبيعة الحال فإن إعادة المحاكمة لا يجوز الالتجاء إليها إلا في حالة ظهور حادثة لم يكن يعلم بها القاضي، أو كان الحكم الذي صدر مشوب بخطأ أو عيب فادح[١]، ونص المشرع الفلسطيني والمشرع الأردني على الحالات التي يجوز فيها تقديم طلب إعادة المحاكمة وذلك على سبيل الحصر[٢]، ومن الحالات التي يمكن تطبيقها على الجرائم الإلكترونية إذا صدر حكمان في واقعة واحدة بحيث أن الحكمان متناقضان ويسمح ببراءة الأول[٣]، ويمكن إعادة المحاكمة أيضاً إذا صدر الحكم بناءً على شهادة كاذبة، أو إذا ظهرت بعد الحكم وقائع جديدة أو أدلة كانت مجهولة وكان من شأن هذه الأدلة إثبات براءة المتهم، والحالة الأخيرة هي إذا كان الحكم صادر من محكمة مدنية أو إحدى محاكم الأحوال الشخصية وألغي هذا الحكم[٤].

الفرع الخامس

الاشكاليات التي تواجه المحاكمة في الجرائم الإلكترونية

وبعد استعراضنا لمرحلة المحاكمة كان هناك بعض الصعوبات التي تواجه هذه المرحلة، مثل اقتناع القاضي بالدليل الإلكتروني، ومشكلة تسليم المجرمين في حال كانت الجريمة الإلكترونية وقعت في أكثر من دولة، وهذا ما سنتناوله عبر ما هو آت:

---

[١] فخري عبد الرازق الحديثي، **شرح قانون أصول المحاكمات الجزائية**، المرجع السابق، ص٣٥٩-٣٦١.

[٢] أنظر المادة رقم ٣٧٧ من قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م، والمادة رقم ٢٩٢ من قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م، مشار إليه في الموقع الرسمي للتشريعات الأردنية، ديوان التشريع والرأي، عبر الرابط التالي:l /http://www.lob.gov.jo.

[٣] صدر حكم من محكمة صلح جباليا بإدانة شخص لقيامه بنشر صور لفتاه عبر الفيسبوك، وبعد فترة قصيرة صدر حكم آخر من نفس المحكمة يدين شخص ثاني على نفس الواقعة، مما دفع المدان الأول بطلب إعادة المحاكمة الأمر الذي انتهى ببراءته على هذه الواقعة.

[٤] سالم أحمد الكرد، المرجع السابق، ص٢٨٣ وما بعدها.

أولاً: مدى اقتناع القاضي بالدليل الإلكتروني:

من الاشكاليات التي تواجه الجرائم الإلكترونية أثناء المحاكمة مدى حجية الأدلة المستخلصة من الوسائل الإلكترونية، وقد انقسم الفقه في ذلك على ثلاثة آراء، الأول يذهب إلى تحديد وسائل الاثبات للقاضي، والرأي الثاني هو حرية القاضي في الاقتناع بكافة الأدلة التي تقدم إليه، وهذا الرأي هو أكثر توافقاً مع الواقع العملي للمحاكمات، أما الرأي الثالث وهو الخلط بين الرأيين السابقين وهو الجمع بين تحديد الأدلة واقتناع القاضي بها[١]، وللخروج من هذه الإشكالية نرى أنه يمكننا أن نقوم بتحويل الأدلة الإلكترونية إلى أدلة مادية –كما ذكرنا سابقاً[٢]– ونعرضها على هيئة مادية أمام القاضي، مثل طباعة الرسائل والمنشورات التي تحتوي على عبارات سب أو تشهير للآخرين، أو طباعة المواد الإباحية المعروضة على شبكة الإنترنت، أما الأدلة التي لا يمكن عرضها على صورة مادية فنرى عرضها عن طريق خبير إلكتروني للقاضي الذي ينظر النزاع، فالخبير هو من سيوضح للقاضي مدى اهمية هذا الدليل من عدمه.

ومن الحلول العملية التي يوصي بها الباحث لكي يصبح الدليل الإلكتروني ذو حجية قانونية أمام القضاء، أن يستحدث المشرع في تشريعاته النصوص القانونية التي تقبل بالوسائل الإلكترونية كدليل أثناء المحاكمة وتضع الثقة بها، كما يجب أن تعمل الحكومة على ترخيص النظم المعلوماتية التي تقدر على أثبات المخرجات الإلكترونية، بحيث لا تقبل أي وسيلة إلكترونية غير قابلة لهذا النظام[٣].

ثانياً: الاشكالية التي تتعلق بتسليم المجرمين:

كون الجرائم الإلكترونية جرائم عابرة للحدود كما ذكرنا[٤] فذلك سبب إشكاليات كثيرة في تهرب الجناة من قبضة العدالة، وإن الحل الأمثل لتجنب هذه الإشكالية هو التعاون الدولي المثمر لتسليم المجرمين، ويقوم مبدأ تسليم المجرمين على أن تقوم الدولة التي يتواجد على إقليمها شخص قام بجريمة إلكترونية بمحاكمته إذا كان قانون هذه الدولة يسمح بذلك، وإلا عليها أن تقوم بتسليمة للدولة التي وقعت فيها الجريمة، ويعتبر موضوع تسليم المجرمين من المواضيع التي تثير خلافات

---

[١] علي جبار الحسيناوي، المرجع السابق، ص١٤١، ١٤٢.

[٢] أنظر ما سبق ص ١٢٩.

[٣] فريد صبحي اللولو، **استخدام المستند الإلكتروني في الإثبات أمام القضاء، مجلة الشريعة والقانون**، مجلة غير دورية تصدر عن كلية الشريعة والقانون بالجامعة الإسلامية، غزة، العدد الأول، ٢٠٠٨م، ص١٣٣.

[٤] أنظر ما سبق ص ٢١.

بين الدول نظراً لتعلقه بموضوع السيادة، وقد ترفض بعض الدول تسليم المجرمين لديها بحجة السيادة[1]، وللخروج من هذه الإشكالية لا بد من وجود تعاون دولي فعّال يحكمه اتفاقيات دولية لتسهيل مهمة تسليم المجرمين.

[1] جميل عبد الباقي الصغير، **الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، المرجع السابق، ص٨٨ وما بعدها.

خاتمة الدراسة:

وبعد أن انتهينا بفضل الله وحمده من إنجاز هذه الدراسة، لا يزال موضوع الجرائم الإلكترونية موضوع كبير وشائك ويحتاج إلى المزيد من الدراسة، خاصة وأن هناك جرائم جديدة تظهر من حين لآخر وقد توصل الباحث إلى العديد من النتائج والتوصيات، والتي يمكن حصرها في النقاط الأتية:

أولاً: النتائج:

١. الجريمة الإلكترونية هي الجريمة التي تتكون من فعل أو امتناع عن فعل باستخدام إحدى الوسائل الإلكترونية بشكل غير مشروع، يوقع ضرراً يلحق بالغير يعاقب عليه المشرع الجزائي.

٢. تتميز الجريمة الإلكترونية بعدة خصائص لا نجدها في الجرائم التقليدية، مثل الطابع التقني لهذه الجريمة، وكونها عابرة للحدود.

٣. الوسائل الإلكترونية الحديثة أصبحت جزءاً مهماً من حياتنا الشخصية والمهنية.

٤. أسبغ الفقه والقانون الجزائي صفة المال على الكيانات المعنوية للحاسب الآلي، مما أدى إلى تمتع هذه المعطيات بصفة المال الذي يخضع للحماية القانونية والجزائية.

٥. من أسباب انتشار الجريمة الإلكترونية وجعلها عابرة للحدود الإنترنت، حيث جعل الإنترنت العالم كالقرية الصغيرة، فالجريمة الإلكترونية قد ترتكب في دولة وتتحقق نتيجتها في دولة أخرى.

٦. إن أكثر الأساليب التي تستخدم في مهاجمة البيانات وإتلافها الفيروسات، حيث تظهر فيروسات جديدة من حين لآخر، ويكون الفيروس الجديد أقوى من القديم.

٧. لم يتناول قانون العقوبات الفلسطيني ولا مشروع قانون العقوبات الذي لا يزال تحت أروقة المجلس التشريعي جميع صور الجرائم الإلكترونية.

٨. من الممكن تصور المحاولة في الجرائم الإلكترونية.

٩. اعتبر قانون العقوبات الفلسطيني الجرائم الإلكترونية من جرائم الجنح، وبالتالي فالجزاء الجنائي الذي قرره قانون العقوبات والمشروع غير رادع، ولا يتناسب مع جسامة الخسائر التي توقعها بعض الجرائم، فقد تؤدي بعض الجرائم إلى خسائر بالمليارات أو تؤدي إلى أفشاء أسرار مهمة تتعلق بالأمن القومي للدولة.

١٠. استحدثت وزارة الداخلية والأمن الوطني في قطاع غزة إدارة المباحث الفنية التي تتخصص في التحقيق في الجرائم الإلكترونية.

١١. الاستعانة بالخبراء في الجرائم الإلكترونية أمر لا بد منه في جميع مراحل الدعوى الجزائية، جمع الاستدلالات والتحقيق الابتدائي والمحاكمة.

١٢. التفتيش في الجرائم الإلكترونية قد يكون للبحث عن الأدلة المادية أو للبحث عن الأدلة المعنوية، وكذلك الضبط قد ينصب على الكيانات المادية أو المعطيات الإلكترونية والتي يتم إخراجها على شكل كيانات مادية متى أمكن ذلك.

١٣. تتخذ عملية المحاكمة في الجرائم الإلكترونية نفس الإجراءات التي تتم في الجرائم التقليدية، مع اختلاف الأدلة في الاخيرة والتي قد تكون على هيئة معطيات إلكترونية.

ثانياً: التوصيات:

١. العمل على تشريع قانون خاص يكافح الجرائم الإلكترونية، وأن ينص هذا القانون على كافة الجرائم الإلكترونية التي ظهرت في العصر الحديث.

٢. تصنيف الجرائم الإلكترونية بين جنح وجنايات، ورفع سقف العقوبات على بعض الجرائم التي ينتج عنها آثار جسيمة.

٣. تطوير قانون الإجراءات الجزائية لينظم الإجراءات التي تتعلق بالتحري والتحقيق في الجرائم الإلكترونية.

٤. عقد الدورات المتخصصة لمأموري الضبط القضائي وأعضاء النيابة العامة والقضاة، لتعريفهم بالجرائم الإلكترونية وكيفية التعامل معها، وتوضيح مدى خطورتها، وتعليمهم آليات مواجهتها وطرق التحقيق والأثبات فيها.

٥. العمل على وضع حماية قانونية وجزائية للبيانات والمعلومات الإلكترونية، للحد من وقوعها اهدافاً للمجرمين والهواه.

٦. التواصل مع الشرطة الدولية الإنتربول للاستفادة من خبراتهم في مجال الجرائم الإلكترونية عن طريق تبادل المعلومات.

٧. ضرورة وضع حماية إلكترونية للمواقع الحكومية والمواقع المهمة في الدولة مثل مواقع الوزارات والبنوك والجامعات والمستشفيات، للحد من عملية اختراقها.

٨. الانضمام إلى الاتفاقيات والمعاهدات العربية والدولية التي تتعلق بمكافحة الجرائم الإلكترونية.

٩. يجب تطوير قانون الإجراءات كما قلنا بحيث يمتد التفتيش في الجرائم الإلكترونية إلى أي حاسوب أو شبكة إلكترونية أو موقع إلكتروني آخر ثبت أن له صلة بالجريمة محل التحقيق.

١٠. يجب استحداث نصوص قانونية جديدة فيما يتعلق بالضمانات التي يجب أن يحاط بها المتهمين في الجرائم الإلكترونية، خاصة أصحاب الأجهزة الإلكترونية التي يتم ضبطها ومصادرتها لاسيما إذا كانت تحتوي على بيانات أو معلومات تمس حياتهم الشخصية.

١١. نشر الوعي والتعليمات المهمة للمواطنين لتعريفهم بخطورة الجرائم الإلكترونية، وتحذيرهم من دخول المواقع المشبوهة مثل المواقع الجنسية والتي لها آثار مدمرة على الصعيد النفسي والاجتماعي، وتوعية طلبة المدارس والجامعات عن مخاطر هذه الجرائم، وفتح تخصصات جامعية تفيد في مجال المكافحة التقنية، وتنظيم إجراءات لمراقبة الشبكات ومزودي خدمة الإنترنت.

قائمة المراجع

أولاً: الكتب القانونية:

- إبراهيم محمود اللبيدي، السلوك الإجرامي في جرائم الإنترنت، مركز الأعلام الأمني، نسخة إلكترونية، غير متضمنه سنة النشر.

*** أحمد فتحي سرور:**

- الوسيط في قانون الإجراءات الجنائية، الطبعة الثامنة، دار النهضة العربية، القاهرة، ٢٠١٢م.
- الوسيط في قانون العقوبات، الجزء الأول، القسم العام، دار النهضة العربية، القاهرة، ١٩٨١م.
- إدوارد غالي الدهبي، الإجراءات الجنائية، الطبعة الثانية، مكتبة غريب، القاهرة، ١٩٩٠م.
- أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، ٢٠١٠م.
- أسامة أحمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والإنترنت، الطبعة الأولى، دار وائل للنشر، عمان، ٢٠٠١م.
- الشحات إبراهيم منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠١١م.
- أمال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، الهيئة المصرية العامة للكتب، ١٩٩١م.
- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الاسكندرية، ٢٠٠٨م.
- أمين محمد نوفل، قانون العقوبات العام، كلية الشرطة الفلسطينية، غير متضمن تاريخ النشر.

- أمين محمد نوفل، تمام يوسف نوفل، الوجيز في أصول التحقيق الجنائي، كلية الشرطة الفلسطينية، غزة، ٢٠١٣م.
- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠١١م.
- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨م.
- جلال ثروت، قانون العقوبات، القسم العام، الدار الجامعية، بيروت، غير متضمن سنة النشر.
- جمال محمد غيطاس، أمن المعلومات والأمن القومي، الطبعة الاولى، نهضة مصر للطباعة والنشر، القاهرة، ٢٠٠٧م.

*** جميل عبد الباقي الصغير:**

- الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢م.
- الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢م.
- الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، القاهرة، ٢٠٠٣م.
- حسن محمد ربيع، شرح قانون العقوبات الاتحادي، القسم العام، الجزء الثاني، الطبعة الثانية، أكاديمية شرطة دبي، ١٩٩٣م.
- خالد عياد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى ، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م.

*** خالد ممدوح إبراهيم:**

- الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩م.
- حوكمة الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، ٢٠١١م.
- فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠١٠م.
- خليل حسن الجريسي، اساليب التحقيق والبحث الجنائي الفني، الطبعة الثالثة، مطبعة دار المنارة، غزة، ٢٠٠٣م.
- رامي متولي القاضي ، مكافحة الجرائم المعلوماتية ، الطبعة الأولى ، دار النهضة العربية، القاهرة، ٢٠١١م.
- رمسيس بهنام، الإجراءات الجزائية، منشأة المعارف، الإسكندرية.
- سالم أحمد الكرد، أصول الإجراءات الجزائية في التشريع الفلسطيني، الكتاب الثاني، الطبعة الثالثة، كلية الشرطة الفلسطينية، غزة، ٢٠٠٨م.
- سليم الزعنون، التحقيق الجنائي، الجزء الأول، الطبعة الرابعة، المؤسسة العربية للدراسات والنشر، بيروت، ٢٠٠١م.

***ساهر إبراهيم الوليد:**

- الوجيز في شرح قانون الإجراءات الجزائية الفلسطيني، الجزء الأول، الطبعة الثانية، ٢٠٠٨م.
- الوجيز في شرح قانون الإجراءات الجزائية الفلسطيني، الجزء الثاني، الطبعة الثالثة، ٢٠١١م.
- طارق محمد الديراوي، الوجيز في شرح قانون الإجراءات الجزائية الفلسطيني، الجزء الثاني، الطبعة الاولى، ٢٠١٣م.
- عادل عزام الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، الطبعة الأولى، دار الثقافة، عمان، ٢٠١١م.

- عبد الرحمن توفيق أحمد، شرح الإجراءات الجزائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م.
- عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠٠٦م.
- عبد الصبور عبد القوي مصري، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، القاهرة، ٢٠١٠م.
- عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية، الطبعة الاولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢م.

***د. عبد الفتاح بيومي حجازي:**

- التجارة الإلكترونية، الكتاب الثاني، دار الكتب القانونية،القاهرة، ٢٠٠٧م.
- الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١م.
- الجريمة في عصر العولمة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٠م.
- الحكومة الاليكترونية ونظامها القانوني، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.

***عبد القادر جرادة:**

- مبادئ قانون العقوبات الفلسطيني، الجريمة والمجرم، المجلد الأول، مكتبة أفاق، غزة، ٢٠١٠م.
- مبادئ قانون العقوبات الفلسطيني، الطبعة الثانية، عدد كفر كنا، مكتبة أفاق، غزة، ٢٠١٣م.
- موسوعة الإجراءات الجزائية في التشريع الفلسطيني، المجلد الأول، مكتبة آفاق، غزة، عدد بئر السبع، ٢٠٠٩م.
- موسوعة الإجراءات الجزائية في التشريع الفلسطيني، المجلد الثاني، مكتبة آفاق، غزة، عدد بئر السبع، ٢٠٠٩م.

- موسوعة الإجراءات الجزائية في التشريع الفلسطيني، المجلد الثالث، مكتبة آفاق، غزة، عدد بئر السبع، ٢٠٠٩م.
- دستور الاستدلال والتحقيق الجنائي، الطبعة الأولى، مكتبة آفاق، غزة، عدد الطيبة، ٢٠١٢م.
- علي جبار الحسيناوي، جرائم الحاسوب و الإنترنت، دار اليازوري للنشر والتوزيع، ٢٠٠٩م، عمان.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الاسكندرية، ١٩٩٧م.
- علي عدنان الفيل، النظام القانوني للمعاملات الإلكترونية في الوطن العربي، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١م.
- فخري عبد الرازق الحديثي، خالد حميدي الزعبي، شرح قانون العقوبات، القسم العام، الموسوعة الجنائية١، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠م.
- فخري عبد الرازق الحديثي، شرح قانون أصول المحاكمات الجزائية، الموسوعة الجنائية ٤، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م.
- فريد صبحي اللولو، استخدام المستند الإلكتروني في الإثبات أمام القضاء، مجلة الشريعة والقانون، مجلة غير دورية تصدر عن كلية الشريعة والقانون بالجامعة الإسلامية، غزة، العدد الأول، ٢٠٠٨م.
- كميت طالب البغدادي، الاستخدام غير المشروع لبطاقات الائتمان، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨م.
- مبارك عبد العزيز النوبيت، نظرية الشروع في الجريمة، العدد الثاني، الطبعة الأولى، مجلة الحقوق والشريعة، الكويت، ١٩٧٨م.
- محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، ٢٠٠٨م.
- محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت / الجريمة المعلوماتية ، الطبعة الرابعة ، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م.

- محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٣م.
- محمد حمّاد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠م.
- محمد زكي ابو عامر، الإجراءات الجنائية، منشأة المعارف، الإسكندرية، ١٩٩٤م.

***محمد صبحي نجم:**

- المدخل إلى علم الإجرام وعلم العقاب، الجامعة الأردنية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ١٩٩٨م.
- قانون العقوبات، القسم العام، الطبعة الأولى، الإصدار الرابع، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٠م.
- محمد علي الحلبي، الوسيط في شرح قانون أصول المحاكمات الجزائية، الجزء الثالث، دار الثقافة، عمان، ١٩٩٦م.
- محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة ، الاسكندرية، ٢٠١١م.
- محمد محمد الألفي، المواجهة الأمنية والتشريعية لجرائم الإرهاب عبر الإنترنت، المكتبة المصرية الحديثة، القاهرة.
- محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية ، الطبعة الأولى / الإصدار الثاني ، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٩م.
- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، ١٩٩٨م.
- د. ممدوح خليل البحر، مبادئ قانون أصول المحاكمات الجزائية، دار الثقافة، عمان، ١٩٩٨م.
- منير محمد الجنيهي، ممدوح محمد الجنيهي، جرائم الإنترنت والحاسب الآلي، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.

- نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥م.

*** نائل عبد الرحمن صالح:**

- محاضرات في أصول المحاكمات الجزائية، الطبعة الأولى، دار الفكر للنشر والتوزيع، عمان، ١٩٩٧م.
- محاضرات في قانون العقوبات القسم العام، الجامعة الأردنية، الطبعة الأولى، دار الفكر للنشر والتوزيع، عمان، ١٩٩٥م.
- ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، ٢٠١٢م.
- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠١٣م.
- نظام توفيق المجالي، شرح قانون العقوبات القسم العام، الكتاب الأول، مكتبة دار الثقافة للنشر والتوزيع، عمان، ١٩٩٨م.
- هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة.

*** هلالي عبد اللاه أحمد:**

- التزام الشاهد بالإعلام في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، الإسكندرية، ١٩٩٧م.
- تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠٨م.
- يسر أنور علي، د. أمال عبد الرحيم عثمان، أصول علمي الأجرام والعقاب، الجزء الأول في علم الأجرام، غير متضمن دار النشر، ١٩٩٤م.

- يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، الطبعة الأولى، دار العدالة، القاهرة، ٢٠١١م.

***يوسف حسن يوسف:**

- الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، ٢٠١١م.
- جريمة غسل الأموال بالطرق التقليدية عبر شبكات الإنترنت وبنوك الويب، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١م.
- دليل الإجراءات الجزائية، كتيب صادر عن وزارة العدل ووزارة الداخلية، غزة، ٢٠٠٧م.

ثانياً: الرسائل العلمية:

- عمر محمد يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة عين شمس/كلية الحقوق، ٢٠٠٤م.
- عبد الرحمن جميل حسين، الحماية القانونية لبرامج الحاسب الآلي، رسالة ماجستير، جامعة النجاح الوطنية، ٢٠٠٨م.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، رسالة ماجستير، الطبعة الثانية، دار الثقافة، عمان، ٢٠١٠م.
- مروان مرزوق الروقي، القصد الجنائي في الجرائم المعلوماتية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، ٢٠١١م.

ثالثاً: القوانين:

القوانين الفلسطينية:

الوقائع الفلسطينية، العدد الخامس والسبعون.

القانون الأساسي الفلسطيني المعدل لسنة ٢٠٠٥م.

قانون العقوبات الفلسطيني رقم ٧٤ لسنة ١٩٣٦ المعدل لسنة ٢٠١٠م.

قانون العقوبات المطبق في الضفة الغربية رقم ١٦ لسنة ١٩٦٠.

مشروع قانون العقوبات الفلسطيني لسنة ٢٠١٠م.

قانون الإجراءات الجزائية الفلسطيني رقم ٣ لسنة ٢٠٠١م.

القانون التفسيري الفلسطيني رقم ٩ لسنة ١٩٤٥م.

التعليمات القضائية للنائب العام الفلسطيني رقم ١ لسنة ٢٠٠٦م.

قانون البينات الفلسطيني رقم ٤ لسنة ٢٠٠١م.

قانون السلطة القضائية الفلسطيني رقم ١ لسنة ٢٠٠٢م.

قانون تشكيل المحاكم النظامية الفلسطيني رقم ٥ لسنة ٢٠٠١م.

-القرار الوزاري رقم ٢٠١٢/٣٣ والصادر عن وزير الاتصالات وتكنولوجيا المعلومات بتاريخ ٢٠١٢/٨/٢٢م.

القوانين الأردنية:

قانون تشكيل المحاكم النظامية الأردنية رقم ١٧ لسنة ٢٠٠١م.

قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م.

القانون المدني الأردني رقم (٤٣) لسنة ١٩٧٦م.

قانون محاكم الصلح الأردني رقم ١٥ لسنة ١٩٥٢م.

قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠.

الدستور الأردني لسنة ١٩٥٢م.

قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠.

القوانين الأخرى:

نظام مكافحة جرائم المعلوماتية السعودي رقم (م/١٧) ، لسنة ١٤٢٨هـ.

قانون الجزاء الكويتي رقم ١٦ لسنة ١٩٦٠م.

قانون العقوبات المصري رقم ٩٥ لسنة ٢٠٠٣م.

قانون تحقيق الجنايات البلجيكي لسنة ٢٠٠٠م.

قانون العقوبات القطري رقم (١١) لسنة ٢٠٠٤م.

الاتفاقية المتعلقة بالجريمة الإلكترونية، بودبست – المجر، ٢٠٠١/١١/٢٣م، مجموعة المعاهدات الأوروبية بمجلس أوروبا – رقم ١٨٥.

قانون العقوبات الفرنسي لسنة ١٩٨٨ .

القانون الاتحادي رقم٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات في الإمارات.

قانون إساءة استخدام الحاسوب في بريطانيا لسنة ١٩٩٠م.

مشروع القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات.

قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢ العُماني.

المواقع الإلكترونية:

الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات الفلسطينية عبر الرابط التالي: http://www.mtit.gov.ps

الموقع الرسمي لقناة الجزيرة الفضائية، عبر الرابط التالي، http://www.aljazeera.net

الموقع الرسمي للتشريعات الأردنية ديوان التشريع والرأي، عبر الرابط التالي:http://www.lob.gov.jo .

الموقع الرسمي لمجلس الوزراء السعودي عبر الرابط التالي:http://www.boe.gov.sa .

موقع منتدى كلية الحقوق لجامعة المنصورة، مصر، عبر الرابط التالي:http://www.flaw.net

الموقع الرسمي لوزارة العدل المصرية عبر الرابط التالي:/http://www.arablegalportal.org .

موقع الميزان، البوابة القانونية القطرية عبر الرابط التالي: http://www.almeezan.qa .

موقع تقنية المعلومات العُماني عبر الرابط التالي: /http://www.ita.gov.om.

التقارير وأوراق عمل:

-تقرير بعنوان " الحرب الإلكترونية تقلق إسرائيل" ، مشار إليه عبر الموقع الرسمي لقناة الجزيرة الفضائية، بتاريخ ٢٠١٣/٦/١٣.

-تقرير بعنوان "قرار وزارة الاتصالات بفلترة المواقع المخلة بالآداب ينجح في حماية نسيج المجتمع"، صحيف الرأي، المكتب الاعلامي الحكومي، وزارة الأعلام، غزة، العدد (٢٤٩)، ٢٠١٣/٨/٢٩م.

-محمد الزرد، تقرير بعنوان "المصادر الفنية بالمباحث العامة تحارب الجريمة إلكترونياً"، جريدة الداخلية ملحق يصدر مع صحيفة الرأي، العدد ١٢٣، ٢٠١٣/٥/٢٣م.

-المحامي الدكتور يونس عرب، ورقة عمل بعنوان " صور الجرائم الإلكترونية " ، مقدمة لورشة عمل بعنوان " تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية " هيئة تنظيم الاتصالات / مسقط – سلطنة عمان ٢-٤ ابريل ٢٠٠٦م.

الفهرس

تم بحمد الله وتوفيقه