عمادة الدراسات العليا
جامعة القدس

أحكام الشروع في الجريمة الإلكترونية

جهاد جادالله محمود مسالمة

رسالة ماجستير

القدس – فلسطين

2024م – 1446هـ

أحكام الشروع في الجرائم الإلكترونية

إعداد :

جهاد جادالله محمود مسالمة

بكالوريوس قانون عام من جامعة الخليل- الخليل/ فلسطين

المشرف الرئيس : د. جميلة زيد

قدمت هذه الدراسة استكمالاً لمتطلبات درجة الماجستير في القانون العام من كلية من كلية الدراسات العليا في جامعة القدس، القدس – فلسطين.

2024م - 1446هـ

جامعة القدس

عمادة الدراسات العليا

برنامج القانون الجنائي

إجازة الرسالة

أحكام الشروع في الجرائم الإلكترونية

اسم الطالب: جهاد جاد الله محمود المسالمة

الرقم الجامعي: 21812090

المشرف: الدكتور جميلة زيد

نوقشت هذه الرسالة وأجيزت بتاريخ: 2024/6/10م من أعضاء لجنة المناقشة المدرجة أسماؤهم وتواقيعهم:

1- رئيس لجنة المناقشة د. جميلة زيد التوقيع:

2- ممتحناً داخلياً: د. فادي ربايعة التوقيع:

3- عضو لجنة: د. سامر نجم الدين التوقيع:

القدس – فلسطين

2024م-1446هـ

الإهداء

إلى الحبيب....

يا قلبي .... ونبض الحروف حين تلمسها الأنامل....

أنت الجواب حين أسأل التفاؤل....

بل الحياة أنت... وما بين النفس والنفس أنت....

إلى الحبيبة...

يا ملاكي في الحياة.... يا معنى الحب... يا معنى الحنان والتفاني...

يا بسمة الحياة وسر الوجود...

يا من كان دعاؤها سر نجاحي وحنانها بلسم جراحي إلى أغلى الحبايب (أمي الحبيبة)

إلى الحبيبة...

إلى توأم روحي... إلى ضلعي الثابت الذي لا يميل... إلى التي وقفت بجانبي طيلة أيام مسيرتي التعليمية... إلى أختي الأستاذة شهد حفظها الله ورعاها...

زوجي...

إلى من كان الأول دوماً في مساندتي وتشجيعي أهديه هذا البحث... إليك تلك الكلمات زوجي الحبيب...

إلى قرة عيني...

لروح روحي...

أولادي الذين أشعروني أنني أديت رسالتي على أكمل وجه... فلذات كبدي (جاد & ريتال)... وأشعر أنني معهم في برزخ السعادة...

جهاد مسالمة

إقرار:

أقر أنا مُعدة الرسالة بأنها قُدمت لجامعة القدس، لنيل درجة الماجستير، وأنها نتيجة أبحاثي الخاصة، باستثناء ما تم الإشارة له حيثما ورد، وأن هذه الدراسة، أو أي جزء منها، لم يُقدم لنيل درجة عليا لأي جامعة أو معهد آخر.

التوقيع: 

جهاد جادالله محمود مسالمة

التاريخ : 10 /6/ 2024م.

شكر وتقدير

إن الحمد لله بحمده سبحانه وتعالى حمداً يليق بجلال وجهه وعظيم سلطانه، فقد سدد الخطى، وشرح الصدر، وسهل الأمر، فلله الحمد كله، وإليه يرجع الشكر، والصلاة والسلام على أشرف الخلق سيدنا محمد _صلى الله عليه وسلم_ النبي الأمين.

الشكر لله عز وجل، وإلى أساتذتي الأفاضل وأخص بالذكر الدكتورة جميلة زيد الذي جادت بكرمها وأمدتني بعطائها فكانت الغذاء الذي أحيا بحثي وأشرف على نموه فكل الشكر والتقدير لها.

كما ويسعني أن أتقدم بعظيم الامتنان إلى إدارة جامعة القدس وعمادة الدراسات العليا.

ويسرني أن أشكر زملائي وزميلاتي وكل من وقف بجانبي ومد لي يد العون.

جهاد مسالمة

المُلخص

تناولت الدراسة مفهوم الشروع في الجرائم الإلكترونية من خلال تحديد مفهوم كل من الشروع والجريمة الإلكترونية، وبيان الإطار القانوني لها، كما تطرقت للتنظيم الموضوعي للشروع مبينة أهمية تجريمه، وموقف التشريعات من ذلك، بينما تناولت الأحكام الإجرائية من خلال كيفية التحري في مراحله المختلفة، والعقوبة على الشروع في الجنايات والجنح. وتتمثل الإشكالية الرئيسية بالآتي: هل تناول المشرع الفلسطيني الشروع في الجريمة الالكترونية بمفهومه الواسع أم اقتصر على ذكره بمفهومه الضيق؟

وتأسيساً على ذلك، خُصص الفصل الأول من الدراسة لمفهوم الشروع في الجرائم الإلكترونية بينما ركز الفصل الثاني من الدراسة على الأحكام الإجرائية المتعلقة بالشروع في الجرائم الإلكترونية، وفي سبيل تحقيق ذلك استخدمت الدراسة المنهج الاستنباطي والمنهج الوصفي التحليلي والنقدي، بحيث يتم البحث والتفصيل في كل جزئية من جزيئاتها، من الجانب الفقهي وما تضمنه من أراء واتجاهات مختلفة ومتباينة، وكذلك في الجانب التشريعي، وتحليل النصوص القانونية ذات الصلة في هذا الموضوع، حيث استندت على المصادر والمراجع والأبحاث المتوفرة طباعياً وإلكترونياً وغيرها من أدوات الدراسة المختلفة.

وخلصت إلى مجموعة من النتائج أهمها بأن الشروع في الجريمة الالكترونية هو البدء في تنفيذ سلوك إجرامي باستخدام الشبكة الالكترونية مؤدي إلى ارتكاب جناية أو جنحة ينتهي دون تحقق النتيجة الاجرامية، لأسباب لا دحل لإرادة الجاني فيها، ويتضح لنا من خلال دراسة مقتضيات القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته فإن المشرع الفلسطيني نص بشكل صريح على أن كل من شرع بارتكاب جناية أو جنحة من الجرائم الوارد ذكرها في هذا القرار بقانون يعد مرتكبا جريمة الشروع ويعاقب بنصف العقوبة المقررة، كما يتضح لنا من خلال القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته ومن خلال قراءة نصوصه بتمعن نجد بأنه لم يكن موفقا المشرع الفلسطيني في تناوله لأحكام الشروع في الجريمة الالكترونية وذلك يرجع إلى أنه لم يخصص فصلاً واحداً أو باباً لأحكام الشروع في الجريمة الالكترونية، بل اقتصر على تناوله من خلال مادتين فقط وهما (المادة 48 و49) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته.

من أبرز التوصيات التي توصلنا لهها من خلال هذه الدراسة، سن قانون شامل للجرائم الإلكترونية، يتضمن تعريفًا دقيقًا للشروع في الجريمة الإلكترونية، وتحديد العقوبات المناسبة لكل نوع من أنواع الشروع، وضرورة التركيز على مراجعة أحكام التفتيش في الجريمة الالكترونية والشروع فيها والعمل على تطويرها لتواكب طبيعة الجريمة الالكترونية وتنظيم ما يلزم من القواعد فيها.

Title "Provisions for attempted cybercrime"

Prepared by: Jihad Jadallah Masalmah

Supervisor: Dr. Jameela Zaid

Abstract

The study dealt with the concept of attempted cybercrime by defining the concept of both attempted and cybercrime, and the statement of its legal framework, as well as the objective organization of the attempt, indicating the importance of criminalizing it, and the position of legislation on that, while dealing with procedural provisions through how to investigate in its various stages, and the penalty for attempted felonies and misdemeanors.

The main problem is as follows: Did the Palestinian legislator address the initiation of cybercrime in a broad sense or did he limit himself to mentioning it in a narrow sense?

Based on this, the first chapter of the study was devoted to the concept of attempted cybercrime, while the second chapter of the study focused on the procedural provisions related to the attempt to commit cybercrime, and in order to achieve this, the study used the methodology , the researcher followed in this study the deductive approach Descriptive, analytical and critical, so that research and detail are carried out in each of its parts, from the jurisprudential side and the opinions it contained. And different and different trends, as well as in the legislative and judicial aspects in what allows us to access its provisions, and the analysis of the relevant legal texts on this subject, as it was based on sources, references and research available in print, electronically and other various study tools, and the descriptive analytical approach where the statistics were referred to in the Palestinian Central Agency on the number of electronic crimes in Palestine.

It is clear to us through studying the requirements of the resolution on Law No. 10 of 2018 on electronic crimes, the Palestinian legislator explicitly stated that anyone who attempted to commit a felony or misdemeanor of the crimes mentioned in this resolution by law is considered the perpetrator of the attempted crime and is punished with half of the prescribed penalty, As it is clear to us through the decision of Law No. 10 of 2018 on cybercrimes and by reading its texts carefully, we find that the Palestinian legislator was not successful in addressing the provisions of attempted cybercrime, due to the fact that he did not devote one chapter or a section to the provisions of attempted cybercrime, but was limited to addressing it through only two articles (articles 48 and 49) of the decision of Law No. 10 of 2018 on cybercrimes.

One of the most prominent recommendations we have reached through this study is the enactment of a comprehensive law on cybercrime, which includes a precise definition of attempted cybercrime, determining the appropriate penalties for each type of attempt, and the need to focus on reviewing and initiating inspection provisions in cybercrime and work on developing them to keep pace with the nature of cybercrime and regulating the necessary rules in it.

المقدمة

مع بداية الثورة الرقمية، ظهرت جرائم جديدة لم تكن موجودة في القوانين القديمة، مثل اختراق البيانات والابتزاز الإلكتروني، حيث أصبحت الحاسب والإنترنت أحد أخطار ظهور الجرائم الإلكترونية، وما يجب الإشارة إليه أن هذه الجرائم كالجرائم التقليدية لها مرتكبيها وضحاياها، إلا أنها قد تكون أخطر من الجرائم المتعارف عليها لأنه يتم ارتكابها عبر زر الحاسوب وهو ما سهل ارتكابها وجعل من الصعب رصد الجاني فيها وتتبعه والقبض عليه(نصار، 2017، ص 12).

لم تكن هناك قوانين محددة تجرّم هذه الأفعال، مما أدى إلى صعوبة معاقبة مرتكبيها، وفي سبعينيات القرن الماضي، بدأت بعض الدول في سن قوانين خاصة بالجرائم الإلكترونية، حيث ركزت هذه القوانين على حماية أنظمة الحاسوب والبيانات من الاختراق والسرقة، ومع ازدياد انتشار الإنترنت وتنوع أشكال الجرائم الإلكترونية، توسعت القوانين لتشمل المزيد من الأفعال، حيث شملت القوانين الجديدة جرائم مثل الاحتيال الإلكتروني ونشر المعلومات المضللة والتشهير الإلكتروني، ويعتبر عد قوانين الجرائم الإلكترونية ضرورية لمواكبة التطورات في مجال التكنولوجيا وحماية المجتمعات من أخطار الجرائم الإلكترونية، وتستمر هذه القوانين في التطور مع ازدياد انتشار الإنترنت وتنوع أشكال الجرائم الإلكترونية، وفي فلسطين كان يتم التعامل مع الجرائم الإلكترونية من خلال قوانين أخرى، مثل قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية وقانون الاتصالات اللاسلكية رقم (3) لسنة 1996، ثم عملت على وضع قوانين خاصة بها كقرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

فالشبكة العنكبوتية والتطور التكنولوجي أصبح سلاح ذو حدين، فبالرغم من الخدمات التي توفرها الشبكة العنكبوتية من سرعة الاتصال والتواصل، يستخدمها البعض بارتكابهم الجرائم واستخدامها واستغلالها على نحو غير مشروع، استغله مرتكبو الجرائم الإلكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الدول (المشرجي، 2014، ص 60).

حيث إن تقنية الحاسوب أصبحت تستخدم كأداة لارتكاب الجرائم الإلكترونية بشكل إلكترونية يخالف الجرائم التقليدية، وهو النوع المستحدث من الجرائم الإلكترونية يرتكب في بيئة افتراضية غير متعارف عليها، ولا تشبه هذه البيئة التقليدية للجرائم التقليدية، إلا أن هناك جانباً من الفقهاء قد اعتبروها امتداداً للجريمة التقليدية المتعارف عليها، وذلك على منظور تطور الجريمة من حيث الزمان، والبعض الآخر اعتبرها جريمة مستقلة بذاتها (الصغير، 2013، ص 2-5).

تكمن أهمية الدراسة في بيان مفهوم الشروع والجريمة الإلكترونية، وبيان أركانها وخصائصها، وبيان الجزاء الذي يقرره القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية بشكل خاص والتشريعات الجزائية الفلسطينية بشكل عام, على كل من يرتكب السلوك الاجرامي سواء تحققت النتيجة الاجرامية أم لم تتحقق، لأن في كلتا الحالتين هناك اعتداء وسلوك اجرامي حدث فعلاً.

ويعتبر الشروع في الجريمة الإلكترونية من القواعد الموضوعية التي نظمها القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية ونص بشكل صريح على الجزاء، والهدف من تطبيق هذا الجزاء على المخالفين تحقيق الردع العام والخاص.

واتبعت الباحثة في هذه الدراسة المنهج الاستنباطي والمنهج الوصفي التحليلي والنقدي، بحيث يتم البحث والتفصيل في كل جزئية من جزيئاتها، من الجانب الفقهي وما تضمنه من أراء واتجاهات مختلفة ومتباينة، وكذلك في الجانبين التشريعي والقضائي فيما تيسر لنا من اطلاع على أحكامه، وتحليل النصوص القانونية ذات الصلة في هذا الموضوع، حيث استندت على المصادر والمراجع والأبحاث المتوفرة طباعياً وإلكترونياً وغيرها من أدوات الدراسة المختلفة.

وقد هدفت الدراسة بأن الحياة اليومية تشهد تطوراً كبيراً في مجال تقنية المعلومات، وبما أن البيئة لها روادها فقد وجد بعض المجرمين في هذه البيئة مجالاً خصباً لارتكاب صور متعددة من الجرائم الالكترونية عبر وسائل الاتصال الحديثة، فهذه الجرائم ما وجدت إلا نتيجة استخدام وسائل التواصل الاجتماعي بشكل سيء وبالتالي فقد تكمن أهداف الدراسة في: تسليط الضوء على الشروع في الجرائم الإلكترونية، وبيان خطورتها وما تؤدي إليه من أخطار جسيمة على الأمن والنظام في المجتمع، والتعرف على فاعلية التشريعات والقوانين العربية في مكافحة الجرائم الإلكترونية، إضافة إلى الطبيعة القانونية للجريمة، وإفادة الباحثين والمختصين والجهات المعنية بموضوع الدراسة.

وتكمن إشكالية الدراسة بأنه عصر المعلومات أطلق وتنامى الاعتماد على التطبيقات الإلكترونية والرقمية، والاتجاه في التحول من التناظرية إلى الرقمية في خلق وحفظ وتداول ونقل النصوص والرسوم والصور والأفلام، ووجود بيئة لتداول المعرفة والمعلومات وتطور حلولها وتطبيقاتها في ميادين الأنشطة الإعلامية والمعرفية والاستثمارية إلى ظهور ما يسمى بالجرائم الإلكترونية، فهي عدواً صارخًا على البنيان الثقافي والعلمي والحضاري والاقتصادي وتؤثر في أمن الدولة واستقرارها، الأمر الذي يوجب مواجهتها والحد منها، وأبرز صور هذه المواجهة تكمن في المواجهة التشريعية عبر توسيع نطاق التجريم بحيث يطال أشكال هذه الجرائم كافة بما في ذلك الشروع فيها، لذلك لابد من التعرف على الشروع وحقيقته ومدى الفرق بين الشروع

والجريمة التامة وبالتالي فإن اشكالية الدارسة هي: هل تناول المشرع الفلسطيني الشروع في الجريمة الالكترونية بمفهومه الواسع أم اقتصر على ذكره بمفهومه الضيق؟

وللإجابة عن هذه الإشكالية تمت هذه الدراسة من خلال فصلين، على النحو التالي:

الفصل الأول: محددات الشروع في الجرائم الالكترونية

الفصل الثاني: الأحكام الإجرائية المتعلقة بالشروع في الجرائم الالكترونية

الفصل الأول

محددات الشروع في الجرائم الالكترونية

على الرغم من التقدم العلمي المتتابع الذي شهده الإنسان على مرّ العصور، إلا أن رحم الحياة العلمية حتى وقتنا الحاضر لا زال يدفع من حين لآخر بمولد الجديد الذي يحمل من المميزات والصفات التي لم تكن موجودة في سابقه، فالحياة العلمية لا زالت في مرحلة المخاض لم تتحدد معالمها بعد (ريضي، 2009، ص 15).

فالحياة في عصر التكنولوجيا الحديثة، التي أصبح فيها الجرائم الإلكترونية أمراً لا مفر منه، حيث تعتبر هذه الجرائم تهديداً حقيقياً للأفراد والشركات والمؤسسات على مستوى العالم، ومع تزايد استخدام الانترنت والتكنولوجيا الرقمية في حياتنا اليومية فإن التحديات القانونية التي تواجه جرائم الإنترنت أصبحت أكثر تعقيداً وضرورة.

والجريمة تقع على النفس الإنسانية سواء بإزهاق هذه النفس وبذلك نكون إزاء جريمة قتل، وسواء بالتعدي على صاحب هذه النفس بالإيذاء الجسماني بسيطاً كان أم في صورة عاهة، كما وتقع الجريمة على مال الإنسان كالسرقة والاحتيال وخيانة الأمانة وغير ذلك من جرائم الأموال، كذلك أن تقع الجريمة على حرية

الإنسان كما هو الحال في جرائم الخطف سواء في صورة الخطف الجنوحين أو الخطف الجنائي، وقد تقع الجريمة على العرض كما هو الحال في جرائم الاغتصاب وهتك العرض والأعمال المنافية للحياء وقد تقع على أمن الدولة الداخلي أو الخارجي كما تقع أيضاً على النظام المالي والاقتصادي للدولة (عبد الرحمن، 2012، ص 16).

في هذا السياق، يتطلب مكافحة الجرائم الإلكترونية تحديد وتعريف هذه الجرائم بشكل دقيق وبيان الإطار العام لمفهوم الشروع في الجرائم الإلكترونية، ويجب أن يكون تعاوناً دولياً فعالاً وتطوير آليات قانونية تمكن من تقديمها للعدالة، ويتضمن ذلك التعاون مع الجهات الأمنية القضائية المختصة في مجال مكافحة الجرائم الإلكترونية، بالإضافة إلى التعاون مع الشركات والمؤسسات التكنولوجية لتطوير وتعزيز أمن البيانات والحماية الرقمية.

فإن بيان الإطار العام لمفهوم الشروع في الجرائم الإلكترونية تتطلب من الباحثة أن تقوم ببحث مسألة أولية للشروع في الجريمة الإلكتروني والتنظيم الموضوعي للشروع في الجرائم الإلكترونية، وسأقوم ببحث هذا الفصل في مبحثين:

المبحث الأول: أحكام الشروع في الجريمة الإلكترونية.

المبحث الثاني: التنظيم الموضوعي للشروع في الجرائم الإلكترونية.

المبحث الأول

أحكام الشروع في الجرائم الالكترونية

يُعدّ موضوع الشروع في الجرائم الإلكترونية من المواضيع الحديثة والمستجدة التي برزت مع ظهور وانتشار تقنية المعلومات ووسائل الاتصال الحديثة. حيث عرّف الشروع في الجرائم الإلكترونية بأنه "البدء في تنفيذ جريمة إلكترونية بأي فعل يؤدي إلى تنفيذها لولا توقفه أو خذلانه لأسباب لا دخل لإرادة الفاعل فيها" (القيلوبي، 2010، ص 15).

وتتمثل أركان الشروع في الجرائم الإلكترونية بركنين أساسيين هما: البدء في التنفيذ بأي فعل يؤدي إلى ارتكاب الجريمة، وتوقف تنفيذ الجريمة لأسباب خارجة عن إرادة الجاني (الحياني، 2020، ص 105)، ومن خصائص الشروع في الجرائم الإلكترونية أنه يعاقب عليه رغم عدم اكتمال الجريمة، كما أن العقوبة

تكون أخف من عقوبة الجريمة التامة (السيد، 2019، ص 6)، أما الإطار القانوني للشروع في الجرائم الإلكترونية، فقد نظمته العديد من التشريعات العربية والدولية، مثل قانون مكافحة جرائم تقنية المعلومات الإماراتي واتفاقية بودابست بشأن الجريمة الإلكترونية (المناعي، 2018، ص 85–90) وفيما يخص طبيعته القانونية فهو يعد من قبيل جرائم الخطر التي يتحقق فيها الضرر الاحتمالي بمجرد الشروع(عبد الفتاح، 2018، ص 55).

فالجريمة الإلكترونية بوصفها ظاهرة إجرامية ذات طبيعة خاصة، صعّبت من جهود الفقه ففي هذا المبحث سيتم توضيح مفهوم كل من الشروع والجريمة الإلكترونية، وتعريف الشروع وأركانه، وكذلك التطرق لتعريف الجريمة وأركانها وخصائصها(المطلب الأول)، على أن تتناول الطبيعة القانونية للجرائم الإلكترونية، والتعرف على الآليات التي تنفذ بها الجرائم الإلكترونية (المطلب الثاني).

المطلب الأول: مفهوم الشروع والجريمة الإلكترونية

يحدث الشروع في الجرائم الإلكترونية في الجرائم ذات النتيجة وهي التي يتطلب المشرع لتمام ركنها المادي سلوك ونتيجة وعلاقة سببية أن يبدأ الجاني في ارتكاب السلوك الإجرامي بشكل كامل، وبعد ذلك يقوم عامل خارج عن إرادته يتدخل ويحول بينه وبين تمام تحقيق هذه النتيجة المتوقعة ففي هذه الحالة لا يلائم الجاني ارتكاب جريمة تامة لعدم تحقق النتيجة الاجرامية، ولكن الذي ينسب إليه هو ارتكاب جريمة ناقصة، وتسمى بالمحاولة (بن فردية، 2021)، وعليه سنتناول في هذا المطلب تعريف الشروع وأحكامه (الفرع الأول)، على أن نتناول في (الفرع الثاني) تعريف الجريمة الالكترونية وأركانها وخصائصها.

الفرع الأول: تعريف الشروع في الجريمة الالكترونية

توحي كلمة الشروع بصورة عامة إلى المحاولة المترافقة بالعزم مع وجود ما يظهر ذلك العزم من وقائع في العالم الخارجي، فهو مرحلة لاحقة على النية أو العزم على إتيان الأمر المشروع فيه، غير أن الشروع لا يقتصر على معنى ثابت ومحدد، وإنما له عدة دلالات مختلفة بحسب الأساس الذي ينظر إليه منه (صليحة، 2021، 73).

حيث تناول المشرع الفلسطيني الشروع من خلال المادة 49 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته والتي نصت على أنه:" يعد مرتكبا جريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها".

ذهب جانب من الفقه إلى تعريف الشروع في الجريمة الالكترونية بأنه: "كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يكن بلوغ الهدف المقصود سبب ظرف مادي يجهله مرتكبه" (فردية، 2010، ص 5).

بالرجوع لمقتضيات المادة (68) من قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية النافذ في فلسطين نجد أنها عرفت الشروع في الجريمة التقليدية بأنه البدء في تنفيذ فعل من الأفعال الظاهرة المؤدية إلى ارتكاب جناية أو جنحة، فإذا لم يتمكن الفاعل من إتمام الافعال اللازمة لحصول تلك الجناية أو الجنحة لحيلولة أسباب لا دخل لإرادته فيها عوقب على الوجه التي إلا إذا نص القانون على خالف ذلك.

ويستخلص من ذلك، أن الشروع في الجريمة هو البدء في تنفيذ سلوك إجرامي مؤدي إلى ارتكاب جناية أو جنحة، ينتهي دون تحقق النتيجة الإجرامية، لأسباب لا دخل لإرادة الجاني فيها (صليحة، 2021، ص 75).

لتوضيح مفهوم الشروع لا بد لنا من التطرق إلى صور الشروع وهي:

1- الشروع الناقص: وهو أن يأتي الفاعل بعضا من الأفعال التنفيذية اللازمة لإتمام الجريمة، وبهذا لا يكون السلوك الإجرامي قد تم كاملا، فالنتيجة لم تحقق لأن الفعل قد أوقف بعد البدء فيه وقبل نهايته.

ويتميز الشروع الناقص بأنه تعطيل للتصرف الجرمي أو إيقافه حيث يكون في هذه الحالة حدث أجنبي لا دخل لإرادة الجاني فيه ويتحقق معه حالات التوقف الجبري عن التنفيذ. لكن قد يكون راجعا لإرادة الجاني واختياره الحر، وهو العدول التلقائي الذي يرجع لأسباب نفسية خالصة أو يصدر عن الإرادة الحرة للجاني والذي من شأنه عدم استمراره في تنفيذ الجريمة. وهذا النوع من العدول قد يؤدي إلى عدم معاقبة الجاني، أو تخفيف عقوبة الشروع في الجريمة، إلا في حالة ما إذا كان فعل الجاني يعتبر جريمة أخرى غير الشروع فإنه يتعين محاسبته عن تلك الجريمة وتوقيع عقوبتها عليه.

أما الميزة الثانية للشروع الناقص فهي عدم استنفاذ التصرف الجرمي حيث أن هذا الشروع يقوم عند حدوث طارئ ما عطل، أو أوقف هذا التصرف الجرمي قبل اكتماله، وبالتالي لم يستنفذ من قبل الجاني، وبأنه لا يزال هناك جزء من هذا التصرف الجرمي وما تبقى منه، ومع ذلك ينبغي أن يرتبط عدم حدوث النتيجة الجرمية بعدم اكتمال التصرف الذي أوقف، وأنه لولا هذا التوقف لكانت قد تحققت الجريمة.

الشروع التام: يكون الشروع تاما إذا قام الفاعل بنشاطه الإجرامي كاملا ولكن نتيجة هذا النشاط لم تتحقق أيضا لسبب لا دخل لإرادته فيه، كما يطلق على هذه الجريمة في الشروع إما بالجريمة الخائبة أو الجريمة المستحيلة، حيث تتحقق الجريمة الخائبة عندما يقوم الفاعل على تنفيذ مشروعه الإجرامي بأن يقوم بكل الأفعال التنفيذية التي تحقق الجرم إلا أنه لا يصل إلى الهدف الذي قصده لسبب خارج عن إرادته. إن وجه الاختلاف بين الجريمة الخائبة والجريمة المستحيلة، هو أن في الأولى يمكن تحقيق النتيجة لولا تدخل سبب أو عامل خارجي، في حين أن النتيجة الإجرامية في الثانية من المستحيل تحقيقها منذ بداية اتخاذ السلوك الإجرامي، وبعبارة أخرى فإن الخيبة محتملة عند بدء الجاني في الجريمة الخائبة، ولكنها محققة عند بدئه في الجريمة المستحيلة (صليحة، 2021، ص 75- 76).

الفرع الثاني: تعريف الجريمة الالكترونية وأركانها وخصائصها

أولاً: تعريف الجريمة الإلكترونية

بالرغم من أن المشرع الفلسطيني لم يذكر تعريفاً محددا للجريمة الإلكترونية، إلا أن من يتمعن في نصوص القرار بقانون بشأن الجرائم الإلكترونية الفلسطيني يلاحظ شمولها: جرائم يكون المستهدف بها أنظمة المعلومات؛ كالتدمير أو الإتلاف أو النقل بشرط أن يتم ذلك بواسطة الوسائل التقنية من خلال الشبكة المعلوماتية (البياتي وآخرين، 1999، ص 24)، وجرائم تتم بواسطة استخدام أنظمة تكنولوجيا المعلومات وتكون ضمن إطار الشبكة الإلكترونية، وقد أوردها المشرع الأردني على سبيل الحصر، مثل جريمة نشر معلومات اباحية، فمصطلح الجريمة المعلوماتية، أو الإلكترونية، أو التقنية، أو جريمة تكنولوجيا المعلومات، يُطلق على جميع الجرائم التي يتم ارتكابها باستخدام وسائل الكترونية، سواء كانت أنظمة معلومات، أم شبكة معلوماتية أم موقع الكتروني، وكذلك الجرائم التي تقع عليها (النوايسة، 2017، ص 45).

اختلف الفقه والتشريع في استخدام المصطلحات التي تدل على جرائم أنظمة المعلومات، فالبعض استخدم مصطلح جرائم الإنترنت والآخر استخدم مصطلح الجرائم الإلكترونية أو جرائم الحاسوب، أما المشرع الأردني فقد عمل على استخدام مصطلح جرائم أنظمة المعلومات للدلالة على الجرائم الإلكترونية وما يتعلق بها، ومن ثم مصطلح الجرائم الإلكترونية للدلالة على الجرائم المتعلقة بالإنترنت وتكنولوجيا المعلومات، وقد استخدم المشرع الفلسطيني مصطلح الاختراق في بعض المواد، فإن المشرع الفلسطيني استخدم مصطلح الاختراق للدلالة على ذلك وهو الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية، ينظر: المادة(1) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية.

عرف جانب من الفقه الجريمة الالكترونية بأنها: "نشاط غير مشروع موجّه لنسخ، أو تغيير، أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه" (حامد، 1992، ص 5).

وعرفها جانب آخر من الفقه بأنها: "فعل غير مشروع ناتج عن إرادة آثمة يقرر لها القانون عقوبة" (عبد الكريم، 2011، ص 53).

في حين ذهب جانب آخر من الفقه بتعريف الجريمة الالكترونية بأنها: "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" (الموني، 2012، ص 50) (مأمون، 2010، ص 120) (الشاذلي، 2005، ص15).

وتعرفها الباحثة بأنها: فعل غير مشروع ينتج باستخدام الوسائل الإلكترونية الحديثة ويتطور بتطورها، ويشمل جميع الوسائل الإجرامية والأضرار التي يمكن ارتكابها باستخدام البيئة الإلكترونية.

ثانياً: أركان الجريمة الإلكترونية

1- الركن المادي: يتكون الركن المادي من سلوك جرمي تتمثل في فعل أو امتناع عن فعل ونتيجة جرمية والعلاقة السببية بينهما.

أ- السلوك الجرمي: يعتبر السلوك الجرمي في كافة الجرائم الواقعة على الأشخاص والأموال هو ما يأتي به الشخص من فعل يؤدي إلى إحداث النتيجة التي يسعى إليها، ففي جرائم القتل وفق نص المادة 326 من قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية فإن أي سلوك من الجاني يهدف إلى إزهاق الروح هو سلوك جرمي وهذا واضح من مطلع المادة المذكورة بقولها (كل من قتل انسانا).

وقد يكون السلوك الجرمي في جريمة القتل بالامتناع عن القيام بعمل معين واجب على الجاني القيام به بهدف إزهاق روح انسا، كامتناع الأم عن إرضاع طفلها بهدف التخلص منه (الإشكاليات الموضوعية والإجرائية في النظام القانوني الفلسطيني في الجريمة الالكترونية، 2024، ص 3-4)، بما أن الجاني في الجرائم الالكترونية يختلف عن الجاني في غيرها من الجرائم من حيث كونه ذو خبرة كافية في مجال استخدام التقنيات الحديثة. فإن السلوك الجرمي الذي سيصدر منه في مجال ارتكاب الجريمة الالكترونية حتما سيختلف عن الجاني التقليدي. ففي جريمة الإرهاب الإلكتروني، فإن السلوك الجرمي هنا، هو إطلاق صفحات أو مواقع تدعو وتحرض على الانضمام لمثل هذه الجماعات.

ب- النتيجة الجرمية: والنتيجة الجرمية في الجرائم التقليدية هي ما يترتب على الفعل الذي أتاه الجاني، فلا يكفي قيام الجاني بسلوكه الإجرامي مهما بلغت جسامته، بل لا بد من أن ينتج عن هذا السلوك نتيجة، ففي جريمة القتل لا بد من أن ينتج عن سلوك الجاني وفاة المجني عليه، فإذا لم تنتج الوفاة عن فعل القتل لا نكون أمام جريمة قتل وإنما نكون أمام جريمة شروع في القتل.

أما النتيجة الجرمية في الجريمة الالكترونية، يثور النقاش بشأنها فيما إذا كانت نتيجة الفعل الجرمي في العالم الافتراضي أم في العالم الحقيقي، وفي الحقيقة فإن الفرضيتان محتملات الحدوث في الجرائم الإلكترونية، فمن الممكن حدوثها بالعالم الحقيقي، مثل إزهاق روح إنسان كانت حياته مستمرة عن طريق جهاز كمبيوتر، فباختراق هذا الكمبيوتر(جريمة الكترونية) فإن نتيجتها تكون بالعالم الحقيقي بقتل هذا الإنسان.

ويبقى في كل الحالات الركن المادي متوافر، وكما سبق وأشرنا، فإن النتيجة الجرمية تشكل مشكلة في موضوع التوقيت والاختصاص، بحيث يمكن أن تدخل دولتين وثلاثة في ذات الجريمة، مما يشكل التنازع في تطبيق القوانين (الإشكاليات الموضوعية والإجرائية في النظام القانوني الفلسطيني في الجريمة الإلكترونية، ص 4-5).

ت- علاقة سببية: يجب أن تتحقق علاقة السببية بين سلوك الجاني وبين النتيجة التي ترتبت على فعله، أي أن النتيجة الجرمية سببها سلوك الجاني، ففي جريمة القتل وفاة المجني عليه سببه سلوك الجاني الإجرامي.

وقد نستطيع تطبيق ذات القواعد العامة المطبقة على الجرائم العادية على الجرائم الالكترونية فيما يتعلق بعلاقة السببية إذا انطبقت عليها، ففي جريمة سرقة الشيء المعلوماتي، فاختلاس الشيء المعلوماتي يتحقق بالنشاط المادي الصادر عن الجاني سواء بتشغيله للجهاز للحصول على المعلومة أو البرنامج أو الاستحواذ عليها، وهو ليس في حاجة لاستعمال العنف لانتزاع الشيء، وتشغيله الجهاز لاختلاس المعلومة تتحقق النتيجة بحصوله عليها، فرابطة السببية إذن متوافرة بين نشاطه المادي والنتيجة الإجرامية (مرجع سابق ذكره، ص5).

2- الركن المعنوي: لا بد من توافر الركن المعنوي إلى جانب الركن المادي، لذا يعد الركن المعنوي من العناصر الضرورية واللازمة لتحقق الجريمة الالكترونية، ويقصد بالركن المعنوي الإرادة الإجرامية أو الإرادة الآثمة المقترنة بالفعل سواء اتخذت صورة القصد الجرمي وعندئذ توصف

الجريمة بالعمدية، أم اتخذت صورة الخطأ غير العمدي وحينئذ تكون الجريمة غير العمدية (حسن، 2020، ص 14).

ويرى البعض وبحق في الجرائم الالكترونية أنه حتى لو كانت النتيجة الجرمية بسبب صدفة أو فضول، أي أن الجاني لم يقصد ابتداء أن يرتكب الجريمة، إلا أنه يبقى الركن المعنوي متوافر، حيث أن الأجدر بالفاعل أن يتراجع عن فعله لا أن يستمر، بالتالي فإن استمراره جعل الركن المعنوي متوافر (الإشكاليات الموضوعية والإجرائية في النظام القانوني الفلسطيني في الجريمة الإلكترونية، ص 5).

3- الركن الشرعي (القانوني): من المتعارف عليه أن الدساتير الجنائية الحديث ذهبت إلى إخراج مبدأ أساسي مهم وهو " لا جريمة ولا عقوبة إلا بناء على نص"، وهو ما يسمى بمبدأ شرعية الجريمة والعقوبة، ومفاد هذا الأخير هو حصر نصوص مصادر التجريم والعقاب في القانون المكتوب، هذا ما أكد عليه القانون الأساسي الفلسطيني المعدل لسنة 2003 في المادة 15 منه حيث جاء ضمن مقتضياتها أنه لا جريمة ولا عقوبة إلا بنص قانوني، حيث نصت المادة على أنه:" العقوبة شخصية، وتمنع العقوبات الجماعية، ولا جريمة ولا عقوبة إلا بنص قانوني، ولا توقع عقوبة إلا بحكم قضائي، ولا عقاب إلا على الأفعال اللاحقة لنفاذ القانون".

يمكننا القول أن لكل فعل مجرم في القانون يجب أن يكون له نص قانوني مكتوب يحدد العقوبة المقررة له، والمشرع هو الذي يملك السلطة في بيان وتحديد الأفعال المعاقب عليها والعقوبات المقررة لمرتكبي هذه الأفعال (الزعبي، 2021، ص282)، وقد ذكر المشرع الفلسطيني من خلال مقتضيات القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية على ذكر الجرائم الالكترونية على سبيل المثال وليس على سبيل الحصر والعقوبات المقررة لها، وبهذا يكون المشرع الفلسطيني قد أصاب عندما نص على الجرائم الالكترونية وعقوباتها كما ذهبت إلى ذلك مختلف التشريعات الحديثة.

ثالثاً: خصائص الجريمة الإلكترونية

من خصائص الجريمة الإلكترونية، أنها تقع في بيئة افتراضية، فتوصف بالجرائم التخيلية أو الوهمية، وتعمل على استهداف المعنويات لا الماديات حيث تقع في مجال المعالجة الآلية للمعلومات، بالتالي فهي أقل عنفاً وأكثر صعوبة في الإثبات، لأن مرتكبها لا يترك خلفه أي أثر مادي خارجي ملموس يمكن فحصه، وهذا يعمل على زيادة صعوبة في اكتشاف الجريمة والتعرف على الفاعل، بعكس الجرائم العادية التي عادة ما تترك وراءها أثر مادي أو شهادة شهود أو غيرها من أدلة الإثبات، وفيما يخص موضوع التفتيش والضبط فيمتد في بعض الأحيان إلى أشخاص آخرين غير الجاني، إلى جانب أن الجريمة الإلكترونية عابرة للحدود،

تحدث في مكان معين وضحاياها في مكان آخر، ولها خاصية السرعة في التنفيذ والسرعة في إتلاف الأدلة ومحو آثارها، حيث أن معظم الجرائم التي تم الكشف عنها ومعالجتها تتم عن طريق الصدفة، فهي ترتبط بنوع من الخصوصية أو الحرية الشخصية، وتتعدى إقليمية الاختصاص، والمجرم في الجرائم الإلكترونية ترتكب من قبل أشخاص متخصصين غير عاديين يتمتعون بذكاء وتقنية عالية في التعامل مع الأجهزة والتقنية المعلوماتية (عباينة، 2005، ص 38).

ومن خصائص الجريمة الإلكترونية أيضاً، أن حالات ارتكابها يرتكز خلالها مرتكبها التدخل في مجالات النظام المعلوماتي المختلفة؛ منها مجال المعالجة الإلكترونية للبيانات، ومجال المعالجة الإلكترونية للكلمات والنصوص الإلكترونية، ففي (المجال الأول) الذي يخص المعالجة الإلكترونية للبيانات يتدخل الجاني من خلال ارتكاب الجريمة، سواء من تجميعها أو تجهيزها حتى يتمكن من إدخالها إلى جهاز الحاسب الآلي، وبهدف الحصول على المعلومات، وأما (المجال الثاني) يتدخل فيه الجاني في مجال المعالجة الإلكترونية للنصوص والكلمات، وهي طريقة أوتوماتيكية تمكن مستخدم الحاسب الآلي من حيث كتابة الوثائق المطلوبة بدقة متناهية بفضل الأدوات المتوفرة تحت يده، وبفضل إمكانيات الحاسب الآلي تتاح للجاني فرصة التصحيح والتعديل والمحو والتخزين والاسترجاع والطباعة (الصغير، 2013، ص 14).

مما سبق أن تناولناه، نستخلص بأن خصائص الجريمة الالكترونية كما يلي:

1. جريمة عابرة للقارات: ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم.
2. جرائم ناعمة ومغرية للمجرمين: إذا كانت أن الجرائم التقليدية تحتاج أغلب الأحيان لمجهود عضلي كجرائم القتل والاغتصاب، فإن الجريمة الالكترونية على العكس لا تحتاج إلى أدنى مجهود عضلي، بل تركز وتعتمد على الدراية الذهنية والجهد الفكري المدروس القائم على معرفة بتقنيات الحاسب الآلي، حيث أن الجريمة الإلكترونية لا تحتاج عند ارتكابها إلى أي درجة من القرب أو التلامس المادي بين الجاني والضحية، ويمكن أن ترتكب الجريمة ضد مجني عليه يسكن في مدينة أخرى، لذلك تعتبر أقل عنفا وخشونة من الجرائم التقليدية، كالقتل أو السرقة المقرونة، حيث لا تلتقي الضحية المجرم في مكان واحد (بغدادي، 2017، ص50).
3. وقوع الجريمة المعلوماتية خلال المعالجة الآلية للبيانات، ووفقاً للفقه الفرنسي تعرف عملية المعالجة بأنها:" كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات والتي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب

خاضعة لنظام الحماية الفنية" (ممدوح، 2008، ص 50)، وعرفها المشرع الفلسطيني: بأنها "إجراء وتنفيذ عملية أو مجموعة عمليات على البيانات سواء تعلق بأفراد أو خلافه، بما في ذلك جميع تلك البيانات أو استلامها أو تخزينها أو تعديلها أو نقلها أو استرجاعها أو محوها أو نشرها أو إعادة نشر بيانات أو حجب الوصول إليها وإيقاف عمل أو إلغاؤه أو تعديل محتوياته" (المادة (1) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته).

4. تدني نسبة الإبلاغ عن تلك الجرائم من المجني عليه خاصة في شركات ومؤسسات الأعمال.
5. صعوبة إثبات الجريمة الإلكترونية يتفاوت القضاة في الأخذ بالأدلة الإلكترونية لأسباب مختلفة.

وقد ذكر بعض الفقه بأن الجريمة الإلكترونية جريمة مستحدثة، حيث تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي تنتج أخطاراً جسيمة في ظل العولمة (ممدوح، 2008، ص 86).

وترى الباحثة بأنه في ظل هذا التطور التكنولوجي وازدياد الجرائم الإلكترونية على الساحة الوطنية والعالمية، فمن الواجب أن يكون هناك علم ومعرفة كبيرة عند المحقق في المجال الإلكتروني، فهذه الخصائص التي وردت عن الجرائم الإلكترونية جميعها مهمة وتعمل على تميز الجرائم الإلكترونية بطابع خاص بها، وتتطلب الدقة في الكشف عنها وكذلك الحذر في التعامل معها، فهي من السهل الممتنع فالتعامل معها يجب أن يكون جدي ودقيق حتى لا يتسبب المحقق دون قصد أو بالخطأ إتلاف الدليل الإلكتروني أو ظنا منه بتجاهل أم غير مهم مرتبط بالجريمة الإلكترونية ولا يقوم بمصادرته كالطابعة مثلاً (ممدوح، 2008، ص 86).

المطلب الثاني: الإطار القانوني للجريمة الالكترونية

سنتحدث في هذا المطلب عن الطبيعة القانونية للجرائم الالكترونية (الفرع الأول)، على أن نتناول في (الفرع الثاني) الآليات التي تنفذ بها الجرائم الالكترونية.

الفرع الأول: الطبيعة القانونية للجرائم الإلكترونية

مما لاشك فيه أن دراسة الجرائم بشكل عام والجرائم المعلوماتية بشكل خاص تدخل في نطاق دراسة القسم الخاص لقانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية، ذلك الفرع المختص بدراسة كل جريمة على حدة متناولا عناصرها الأساسية والعقوبة المقررة لها إلا أن الجرائم المعلوماتية تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون، على اعتبار أن معظم هذا النمط من الجرائم يرتكب ضمن نطاق المعالجة الالكترونية الجنائي المعلوماتي للبيانات سواء أكان في تجميعها أم في تجهيزها أم

في ادخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة، كما قد ترتكب هذه الجرائم في مجال معالجة الكلمات أو معالجة النصوص وهذا النوع الأخير من الجرائم لا يعدو أن يكون طريقة أوتوماتيكية تمكن المستخدم من تحرير الوثائق. والنصوص على الحاسوب مع توفير إمكانية التصحيح والتعديل والمسح والتخزين والاسترجاع والطباعة فجميع تلك العمليات هي وثيقة الصلة بالجرائم محل البحث، وعليه لابد للجاني من استيعابها فضلا عن أن الجاني قد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل الاعتداء أو تستخدم وسيلة له (سالم، 2007، ص 91).

إن الطبيعة القانونية الخاصة لهذه الجرائم تتضح من خلال المجال الذي يمكن أن ترتكب فيه، ومن جانب آخر المحل الذي يقع عليه الاعتداء المذكور. فالتطور السريع في مجال المعلوماتية قد يفسح المجال لاقتناء وسائل الكترونية تمكن المتجاوزين لاستخدامها في ارتكاب جرائم مختلفة لأن الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيما يتعلق بالمعالجة الآلية لبيانات وإدخال المعلومات ونقلها ومن ثم يتحتم ضمه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارنة عاجزة عن مواكبه التطور المعلوماتي أو لما يحويه من فراغ تشريعي في هذا المجال (سالم، 2007، ص 91).

ومن جانب آخر تتخذ هذه الجرائم طبيعة خاصة من حيث تكييفها القانوني إذ لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة فالنصوص التقليدية وضعت وفقا لمعايير معينة، في حين كان مفهوم الحقوق الشخصية في شبكة المعلومات هو الذي يرد على نتاج الفكر البشري وهو يتعلق بشخص المرء وأمواله وممتلكاته، كما أن تطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الاثبات، كالحصول على أثر مادي إذ يمكن للجاني محو أدلة الإدانة في وقت قصير لا يتجاوز لحظات وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال فقد تكون البيانات التي يجري البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة ومن هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة، ومما يزيد من صعوبة الأمر ملاحقة جناة جرائم المعلوماتية الذين يقيمون في دولة أخرى لا تربطها اتفاقية بالدولة التي تحقق فيها السلوك الإجرامي أو جزء منه وفي ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة (سالم، 2007، ص 91– 92).

الفرع الثاني: الآليات التي تنفذ بها الجرائم الإلكترونية

تلعب وسائل الاتصال الإلكترونية دوراً كبيراً في مجال ارتكاب الجرائم الإلكترونية وفي مجال اكتشافها، وذلك على النحو التالي:

أولاً: قد تكون الشبكة العنكبوتية هدفاً للجريمة، وذلك كما في حالة الدخول غير المصرّح به إلى أنظمة البيانات في مواقع إلكترونية محددة لتدمير المعطيات أو بهدف الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم، أو أن يتم العبث في البيانات وإخفاء النشاط الجرمي بإعادة إنتاج وطرح البيانات خلال نفس الشبكة ولمشتركين يستخدمون الدفع عبر الإنترنت وهكذا، وهذا ما أكد عليه المشرع الأردني في المادتين (3،4) من قانون جرائم أنظمة المعلومات، وفي القانون رقم (20) لسنة 2017 حول جرائم تقنية المعلومات في فلسطين، أكد المشرع الفلسطيني في المادة الثانية عشر على أن من بين الجرائم الإلكترونية المحظورة في القانون هي جريمة الاعتداء على البيانات، والتي تشمل الوصول غير المصرح به إلى بيانات شخصية أو تعديلها أو تدميرها، والقرصنة والتجسس والتزوير الإلكتروني والاحتيال الإلكتروني، ويهدف القانون إلى تنظيم النشاطات الإلكترونية في فلسطين وحماية البيانات الشخصية والتجارية والحكومية من الاختراق والاستيلاء غير المصرح به عليها.

ثانياً: قد تستخدم الشبكة العنكبوتية أداة لارتكاب جرائم إلكترونية فقط، كما في حالة استغلال الإنترنت للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير، أو استخدام التقنية في عملية الاستيلاء على أرصدة وأرقام بطاقات ائتمان وإعادة استخدامها والاستيلاء على الأموال عن طريق ذلك، ومن ثم الدخول في عمليات تستخدم الدفع الإلكتروني والبيع والشراء عبر الانترنت لإخفاء المصدر الحقيقي غير المشروع للأموال القذرة، وقد نص المشرع الأردني بخصوص ذلك على تجريم مثل هذه الحالات بموجب المادة (6) من قانون جرائم أنظمة المعلومات، ومن أبرز الأنشطة في هذا الإطار غسل الأموال التي تتم عبر الإنترنت وما يرتبط بها من عمليات معقدة ظاهرها التجارة الإلكترونية والتعاقد عبر الإنترنت وباطنها إخفاء المصدر الأساسي والحقيقي الغير شرعي للأموال.

ثالثاً: وقد تكون الشبكة العنكبوتية هي الوسط والبيئة التي ينمو في رحمها الإجرام المعلوماتي وذلك كما في إبرام اتفاقيات لترويج المخدرات وأنشطة الشبكات الإباحية والإرهابية وغسل الأموال (عبد الكريم، 2011، ص 21).

رابعاً: دور الشبكة العنكبوتية في اكتشاف الجريمة الإلكترونية التي تتم عبرها فإن الإنترنت يستخدم الآن على مجال واسع في تتبع وتقصي الجرائم، عوضاً عن أن جهات إنفاذ القانون ترتكز على النظم التقنية في إدارة المهام عن طريق بناء قواعد البيانات المشتركة وأطر الطعون الدولي، ومع ارتفاع وتزايد نطاق الجرائم الإلكترونية، اعتمد مرتكبيها على استخدام وسائل التقنية المتجددة والمتطورة، فإنه أصبح لزاماً وإجباراً استخدام نفس التقنية ووسائل الجريمة المتطورة للكشف عنها، من هنا تلعب الشبكة العنكبوتية نفسها دوراً أساسياً في كشف الجرائم الإلكترونية والإنترنت وتتبع فاعليها، بل وإبطال أثرها (الرومي، 2003، ص 64).

خامساً: إن كثرة وسائل التواصل الاجتماعي في وقتنا الحاضر وتنوعها وجدت احتمالاً قل نظيره في ارتكاب الجرائم الإلكترونية، وعلى "تويتر" يعدّ من أبرز هذه الوسائل الذي استولى على مجال العالم الافتراضي والتواصل عن بعد وذلك بعد ان اقتنع مرتكبو الجرائم الإلكترونية بأنه وسيلة نشطة وفعالة لارتكاب هذه الجرائم وهذا عن طريق التغريدات وسهولة كتابتها وإرسالها (الحسيني، 2013، ص 3).

التنظيم الموضوعي للشروع في الجرائم الإلكترونية

يتناول هذا المبحث موضوع الشروع في الجرائم الإلكترونية وأهميته (المطلب الأول) وكذلك موقف التشريعات الداخلية والاتفاقيات الدولية من تجريم الشروع في الجرائم الإلكترونية (المطلب الثاني).

المبحث الثاني

المطلب الأول: الشروع في الجرائم الالكترونية وأهميته

عملت الدول تكنولوجياً على وضع قواعد موضوعية لمواجهة الاستخدام غير المشروع للأجهزة الإلكترونية، حيث أجرت تعديلات على قوانينها الإجرائية تكفل مكافحة الجرائم الإلكترونية في إطار الشرعية الجنائية، وذلك لأنها على يقين بأن هذه الجرائم تُرتكب بتقنيات حديثة في عالم مخالف عن العالم المادي الذي عادة ما تُرتكب فيه الجرائم عن طريق المجابهة بين الأشخاص كالقتل والإيذاء، وأن القانون الجنائي التقليدي بشقيه الموضوعي والإجرائي وضع من الناحية التاريخية لمكافحة الاعتداءات المادية والمواجهة وجهاً لوجه على عكس الجرائم الإلكترونية التي تستخدم التكنولوجيا فترتبك في عالم افتراضي وعلى مسافات بعيدة (طه، بدون تاريخ، ص 25)، ففي هذا المطلب تتناول الباحثة فرعين (الأول) تطرقت إلى مدى تصور الشروع في الجرائم الإلكترونية، و(الثاني) أهمية تجريم الشروع في الجرائم الإلكترونية.

الفرع الأول: مدى تصور الشروع في الجرائم الإلكترونية

استعان المشرع الفلسطيني في تحديد نطاق الشروع المعاقب عليه بتقسيم الجرائم إلى ثلاثة أصناف: جنايات وجنح ومخالفات، وعمومًا يعاقب دائمًا على الشروع في الجنايات وذلك وفقًا للمادة (68) من قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية ولكن لا يعاقب على الشروع في الجنح إلا بناءً على نص في القانون وفقًا للمادة (71) من نفس القانون. ولا يوجد عقاب على الإطلاق على الشروع في المخالفات، ويرجع السبب في ذلك إلى جسامة الجرائم، فإذا كانت جسيمة عدّ الشروع فيها جسيمًا ومعاقبًا

عليه كالجنايات، وإذا نقصت جسامة الجريمة نقصت خطورة الشروع فيها فيتوقف العقاب على الشروع في الجنح على نصٍ يجرمه (رضوان، 2017، ص 59).

ويتضح لنا من خلال قراءة نصوص القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية فإن المشرع الفلسطيني تناول الشروع في الجريمة الالكترونية من خلال ما جاء في مقتضيات المادة (48) منه على أن من يقوم بالاشتراك عن طريق الاتفاق أو التحريض أو المساعدة أو التدخل في ارتكاب جناية أو جنحة معاقب عليها بموجب هذا القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته، يعاقب العقوبات المقررة للفاعل الأصلي، في حين إذا لم يتم وقوع الجريمة فإنه يعاقب الشخص الذي قام بارتكاب هذه الجريمة بنصف العقوبة.

كما أن المشرع الفلسطيني قام بتجريم الشروع في الجرائم المتعلقة بالجنايات أو الجنح المنصوص عليها في القرار بقانون الذي سبق وأن قمنا بذكره بخصوص الجرائم الالكترونية، فإن كل من شرع في ارتكاب مثل هذه الجرائم يعاقب بنصف العقوبة المقررة لها، وذلك حسب ما جاء في المادة (49) من هذا القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته.

وترتيبا على هذا الأصل العام فيمكن القول أن الجرائم التي اعتبرها قانون الجرائم الالكترونية من قبيل الجنايات تخضع للقواعد العامة المقررة في قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية والتي تقرر مسائلة الجاني عن مجرد الشروع في ارتكاب جناية مما يعني جواز تصور الشروع في الجنايات الالكترونية، بل والعقاب عليها.

والجنايات الواردة في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية هي الجرائم الواردة في المادة الفقرة الرابعة من المادة (17) منه، حيث نصت المادة (17) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته على أنه: "دون الإخلال بالأحكام الواردة في القرار بقانون بشأن تنظيم نقل وزراعة الأعضاء البشرية النافذ، يعاقب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار في البشر أو الأعضاء البشرية أو تسهيل التعامل فيه، بالسجن مدة لا تزيد على سبع سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً".

كما ورد أيضا في المادة (19) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته والتي نصت على أنه:" دون الإخلال بالأحكام الواردة في القرار بقانون بشأن مكافحة المخدرات والمؤثرات العقلية النافذ، يعاقب كل من أنشأ أو نشر موقعاً على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا

المعلومات، بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية، أو ما في حكمها، أو سهل التعامل فيها، أو بيع أو شرح أو عرض طرق إنتاج المواد المخدرة، بالسجن مدة لا تقل عن عشر سنوات، أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

ومن الجرائم الواردة أيضا من خلال نصوص القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته نص المادة (25) والذي جاء فيها :" كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، من شأنه التشويه أو التبرير لأعمال إبادة جماعية أو جرائم ضد الإنسانية نصت عليها المواثيق والقوانين الدولية أو المساعدة قصداً أو التحريض على ارتكاب جرائم ضد الإنسانية، يعاقب بالسجن مدة لا تقل عن عشر سنوات".

أما فيما يتعلق بالجنح التي نص عليها القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته، لم ينص على المعاقبة على الشروع في الجريمة الالكترونية، ولذلك يجب الرجوع إلى الأصل العام المنصوص عليه في قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية والذي يقرر أن العقاب على الشروع في الجنح لا يكون إلا في الجنح التي نص القانون على العقاب عليها، حيث نصت المادة (71) في فقرتها الأولى من قانون العقوبات الأردني رقم 16 لسنة 1960 على أنه: "لا يعاقب على الشروع في الجنحة إلا في الحالات التي ينص القانون عليها صراحة"، إذ اشترطت المادة أن يكون القانون قد نص على العقاب على الشروع في جنحة ما وأن يكون هذا النص صريح، ولما كان القرار بقانون قد خلى من أي نص يشير إلى قيام جريمة الشروع في الجنح المشار إليها فيه أو في إحداها، فيترتب على ذلك القول بعدم جواز العقاب على الشروع في الجنح الالكترونية كون القانون لم ينص على ذلك.

أما بالنسبة لما يتعلق بمدى جواز تصور قيام جريمة الشروع في الجنح الالكترونية من عدمه فيجب أولا التأكيد إلى أن قيام جريمة الشروع يستلزم أولا استظهار الركن المادي للجريمة الالكترونية والمتمثل في الأفعال المادية والسلوك الإجرامي والذي قد يتمثل في إعداد البرامج والتطبيقات اللازمة للقيام بعملية الاختراق أو إعداد فيروسات وبرامج لمغمة بالفيروسات بقصد بثها، كما يجب أيضا استظهار الركن المعنوي وذلك بأن يثبت اتجاه نية الجاني لارتكاب الفعل وهذه الأمور إن كانت ممكنة الاثبات في الجرائم والجنح العادية إلا أنها في مجال الجرائم الالكترونية تزداد صعوبتها خاصة وأن هناك بعض الجرائم لا تتماشى بطبيعتها مع فكرة الشروع، مثل جريمة تقديم أو إتاحة المواد الإباحية الطفولية، فهي جريمة بطبيعتها لا تقبل فكرة الشروع بل يجب تمامها لقيام المسؤولية الجنائية، وتصبح في هذه الحالة القاعدة العامة من أنه لا شروع في الحالة التي يستعصى على طبيعة الجريمة أن يتصور الشروع فيها.

وكذلك من الجنح الالكترونية التي لا يتصور فيها أيضا الشروع جريمة الذم أو القدح أو التحقير فهي من الجرائم التي لا يتصور العقاب عليها إلا بتمامها لأن ما قبل تمامها لا يعدو أن يكون مجرد تفكير أو تبييت نية لا يصلح وحده للعقاب فهي جريمة إما أن تقع تامة أو لا تقع من الأساس.

أما الجنح التي يتصور فيها الشروع في الجرائم الالكترونية مثل الجنحة المنصوص عليها في المادة (4) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية، حيث نصت المادة (4) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته على أنه " 1- كل من دخل عمدا دون وجه حق بأي وسيلة موقعا الكترونيا أو نظاما أو شبكة الكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مئتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا، أو بكلتا العقوبتين. 2- إذا ارتكب الفعل المذكور في القرة (1) من هذه المادة، على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا، أو بكلتا العقوبتين. 3- إذا ترتب على الدخول إلغاء بيانات أو معلومات الكترونية مخزنة في النظام المعلوماتي أو حذفها أو إضافتها أو إفشائها أو إتلافها أو تغييرها أو نقلها أو التقاطها أو نسخها أو نشرها أو إعادة نشرها أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني أو إلغاؤه أو تعديل محتوياته أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين...".

ونحن إذ نذكر هذه الجنح الالكترونية فإننا نذكرها على سبيل المثال والتدليل وليس على سبيل الحصر، كما يجب أن نؤكد على القرار بقانون رقم (10) بشأن الجرائم الالكترونية لم ينص صراحة على المعاقبة على مجرد الشروع في ارتكاب تلك الجرائم وبالتالي فالذي يحكم المسألة هو قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية والذي لا يجيز المعاقبة على الشروع في الجنح إلا إذا كان منصوص عليها في القانون صراحة.

الفرع الثاني: أهمية تجريم الشروع في الجرائم الإلكترونية

الشروع في ارتكاب الجريمة أو ما يعرف ببعض النظم القانونية (المحاولة) أو ما يسمى (محاولة ارتكاب الجريمة) هو محاولة ارتكاب جريمة بأفعال ترمي مباشرة إلى اقترافها يحول دون إتمامها ظروف خارجة عن إرادة الفاعل (الفاضل، 1976، ص 179).

وقد تناول المشرع الأردني الشروع في المواد (68، 69، 70، 71) من قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية، حيث نص في المادة (68) على أن:" الشروع: هو البدء في تنفيذ فعل من الأفعال الظاهرة المؤدية إلى ارتكاب جناية أو جنحة فإذا لم يتمكن الفاعل من إتمام الأفعال اللازمة لحصول تلك الجناية أو الجنحة لحيلولة أسباب لا دخل لإرادته فيها عوقب على الوجه الآتي..."، لذلك يعاقب القانون على الأفعال المادية التي تتطابق مع نص التجريم والتي تكون ماديات الجريمة، حيث أن القانون لا يعمل على العقاب للنوايا مهما كانت إجرامية دون أن يُعبَّر عنها بفعل مادي ملموس ينتج أثره في العالم الخارجي، فالجريمة هي عبارة عن الاعتداء الذي يقوم به الجاني على المجني عليه مخلفاً له نتيجة ضارة، حيث يلاحظ أن عناصر الركن المادي للجريمة المادية هي السلوك أو الفعل الجرمي والنتيجة الجرمية المتحققة وأخيراً العلاقة التي تربط بين الفعل والنتيجة فإذا تحققت تمت الجريمة وفي حال عدم تحققها تبقى الجريمة ناقصة وبذلك فالنتيجة هي الأثر المادي الذي يتحقق (السمامعة، 2017، ص 58).

ولعدم النص على العقاب في بعض الجنح فإن المشرع الفلسطيني قد ساعد بعمل ثغرات في نظام العقاب على الشروع، بينما تقتضي مصلحة المجتمع سد تلك الثغرات، وأفضل مثال على ذلك الجنح التي تضمنها قانون الجرائم الإلكترونية لأن علة العقاب على الشروع متحققة فيها؛ فإذا كان القانون يعمل على المعاقبة بارتكاب الجريمة التامة لأنها تقع عدواناً على مصلحة أو حق جدير بالحماية، فإن العلة من تجريم الشروع التي هي حماية الحق من الخطر الذي يهدده –وحتى في حال عدم تحقق نتيجة الاعتداء– متوافرة في الجنح التي ترتكب في البيئة الرقمية نظراً لما سبق وأن أوردناه من طبيعة خاصة وخطورة لهذه الجرائم المستحدثة، ذلك أن عملية مراعاة الطبيعة الخاصة بالجريمة الإلكترونية كفعل جديد يتم ممارسته بواسطة الأجهزة التقنية والوسائل الحديثة مثل الهاتف أو الحاسب الآلي أو أحد برامجها أو ملحقاتها أو ما شابه من أجل تنفيذ أغراض غير قانونية كالتجسس والسرقة والدخول إلى معلومات وأنظمة مستهدفة أو التلاعب والتحايل أو الدخول غير المصرح به على شبكة المعلومات والمواقع الإلكترونية الخاصة يضفي على مطلب تجريم الشروع في هذه الأفعال أهمية ووجاهة بسبب زيادة التعاملات من بواسطة الإنترنت ونشاط التجارة الإلكترونية، الأمر الذي يعمل على جعل أمن هذه التعاملات مصلحة اجتماعية تستحق إضفاء الحماية القانونية لها بواسطة تجريم السلوكيات المذكورة والأفعال التي تفضي إليها (السمامعة، مرجع سابق ذكره، ص 67).

فالتطورات الحاصلة في نطاق المسؤولية الجزائية عن الجرائم الإلكترونية لا تزال تتفاعل ولم يكتمل عقدها بعد، حيث كثير من التوجهات الوطنية والاستراتيجيات الدولية نادت ومازالت تنادي بعملية اخذ التدابير والاحتياطات في الحقول المتقدمة، لكن إنفاذ هذه التدابير بقي في مراحله الأولية بالنظر إلى العلاقة بين

تشريعات حماية حق المؤلف وبقية تشريعات الملكية الفكرة وبين تشريعات الجرائم الإلكترونية، فالأخيرة تشريعات ظهرت في مجال التصدي لمختلف الانتهاكات التي تستهدف المعطيات والبيانات ومن بينها البرامج وتستهدف التعدي على التطبيقات والحلول في البيئة الرقمية وهي في جزء منها تعمل على التعامل مع الأفعال الجرمية التي تطال حقوق الملكية الفكرية المرتبطة بالمعلومات وتكنولوجيات المعلومات وتطبيقاتها، وهو ما يلزم إلى عمل فواصل مناسبة بين نطاق هاتين الطائفتين من التشريعات أو عملية إيجاد التكامل والانسجام بينها بما يفي بهدف إنهاء كل تعارض أو تناقض بشأن التدابير المقررة في كل طائفة منهما، وخصوصا بالنسبة للدول التي تبنت أو اتبعت منهج اتفاقية بودابست (بتاريخ 20 نيسان 2000 عملت اللجنة الأوروبية بتقديم مشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الأفكار والآراء خلال الفترة من إصدار مشروعها الأول وحتى اعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001 "اتفاقية الجرائم الإلكترونية –سايبر كرايم"، وقد طرح مشروع الاتفاقية ووزع على مختلف الجهات وتم اطلاقه ضمن مواقع عديدة أوروبية وأمريكية على شبكة الإنترنت لجهة إبداء الرأي، حيث عكست الاتفاقية الجهد الكبير والواسع والمميز للاتحاد الأوروبي ومجلس أوروبا ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ أكثر من عشرة أعوام، نقلاً عن يونس عرب، ورشة عمل "تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية"، هيئة تنظيم الاتصالات – مسقط– سلطنة عمان 2–4 أبريل 2006، ص 16) للجرائم الالكترونية لعام 2001 التي تضمنت من بين ما تضمنت وجوب تجريم صور الانتهاكات التي تستهدف الملكية الفكرية في البيئة الرقمية في وقت تقوم لدى هذه الدول حزمة متكاملة من التشريعات الملكية الفكرة سابقة على ظهور وشيوع الجرائم الإلكترونية بمختلف أنواعها.

ومن هنا تتضح أهمية تجريم الشروع في الجرائم الإلكترونية حيث يقبل ركنها المادي فكرة الشروع، وذلك باعتباره اعتداءً محتملاً يهدد المصالح المحمية بالخطر، ما يوجب على القانون أن يجرمه حماية للمجتمع، فالأفعال التي يقوم بها الشروع في الجرائم الإلكترونية من شأنها عمل الاعتداء بما أن مرتكبيها له نية إحداثه، ويوضح ذلك ويشير إلى وجود ثمة خطراً على الحق، وإذا كان الخطر "اعتداء محتملاً"، وكانت الحماية الكاملة للحق مقتضية وقايته من كل صور الاعتداء فلا بد من تجريم الشروع في الجنح الإلكترونية (السمامعة، مرجع سابق، ص 70).

وكذلك تنبع أهمية تجريم الشروع في جرائم الملكية الفردية من الطمأنينة التي تصب على أصحاب حق المؤلف والحقوق المجاورة في توفير المزيد من الحماية القانونية عند نشر مصنفهم على شبكة الإنترنت، فطرق التعدي وانتهاك حقوق المؤلف للمصنفات في البيئة الرقمية تختلف بين نشر المصنف من قبل دور

النشر الإلكترونية دون إذن المؤلف أو المتنازل إليه، وعملية النسخ واللصق وإعادة النسخ والتعديل والتوزيع وإعادة التوزيع، والتحميل على أجهزة الحاسب والتوزيع والتحوير للمصنفات والتثبيت على الدعائم الإلكترونية، ومجرد عملية نشر المصنف على شبكة الإنترنت دون ترخيص من صاحب الحق وبث الأغاني وتوزيعها عبر شبكة الإنترنت دون ترخيص يعد تقليداً لمصنف محمي، وكل ما يخالف الشروط التي نوفق عليها عند حصولنا شرعاً على هذه المنتجات (الدلالعة، 2005، ص 23-25).

وترى الباحثة بأن تجريم الشروع في الجرائم الإلكترونية أمرًا ضروريًا للحد من هذه الجرائم والحفاظ على الأمن الإلكتروني. فالأفعال التي تسبق ارتكاب الجريمة الإلكترونية يمكن أن تسبب أضرارًا كبيرة، ولذلك يجب أن يتم معاقبة المتورطين فيها.

المطلب الثاني: موقف التشريعات الداخلية والاتفاقيات الدولية من تجريم الشروع في الجرائم الالكترونية

قبل ظهور الإنترنت وجرائمه كانت توجد الأفعال الإجرامية، وكانت هذه الأفعال تشمل القتل والسرقة والنصب والتزوير وغيرها من الجرائم، فالشر قائم بيد ان الإنترنت ساعد على سهولة ارتكاب مثل هذه الجرائم، فالتقنيات التكنولوجية سهلت ارتكاب الجرائم ففضاء المعلومات ليس له مبادئ أخلاقية عامة فحدود السلوك المقبول أو حتى السلوك الأخلاقي في فضاء المعلومات ليست واضحة، فضيف الكمبيوتر يمكنه الوصول إلى بعض المعلومات وعدم الوصول إلى البعض الأخر، بينما في الإنترنت يمكن الوصول للمعلومات وقراءة البريد الإلكتروني للشخص بسهولة (عتيق، 2000، ص 3)، فلهذا يعتبر وجود الانترنت مطور للجرائم التقليدية واستحدث جرائم جديدة، ومن العوامل التي ساعدت أيضا على ظهور الجرائم المستحدثة التغيرات في البنية الاجتماعية والاقتصادية للمجتمعات الحالية، فمن الناحية الاجتماعية جاء تغير منظومة الأعراف والقيم الاجتماعية وتحولها من المحلية إلى العالمية ليولد سلوكيات جديدة منحرفة ومجرمة، لأنها خارج سياق القانون الوطني، ومن الناحية الاقتصادية فإن عولمة المال والاقتصاد الناجمة عن زيادة الترابط الإلكتروني والاعتمادية المتزايدة على التقنية والاتصالات في تسيير الأعمال الاقتصادية وما نجم عن ذلك من مؤسسات وشركات متعددة الجنسيات وشركات عابرة للحدود الوطنية (نصار، 2017، ص 24).

فإن العقاب على الشروع في الجرائم الإلكترونية يستوجب وصفاً جرمياً منضبطاً للسلوك الجرمي، وغالبية الجرائم الإلكترونية تتشكل بالاعتداءات التي تضمنها القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، وما تضمنته من ضوابط ومن حقوق ومن مزايا ومن مكنات لصاحب الحق وما قررته من محظورات على الغير (السمامعة، 2017، ص 71).

وعليه فإن الباحثة ستتناول في هذا المبحث لبيان موقف التشريعات الداخلية والاتفاقيات الدولية من تجريم الشروع في الجرائم الإلكترونية فرعين، (الأول) يتحدث عن موقف المشرع الأردني من تجريم الشروع في الجرائم الإلكترونية و(الفرع الثاني) يتحدث عن موقف الاتفاقيات الدولية من تجريم الشروع في الجرائم الإلكترونية.

الفرع الأول: موقف التشريع الفلسطيني من تجريم الشروع في الجرائم الالكترونية

وجد تجريم لبعض الجرائم الإلكترونية في قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية. نصت المادة 4 منه على ما يلي:" يعاقب بالسجن مدة لا تقل عن سنة وبغرامة لا تقل عن ألفي دينار ولا تزيد عن خمسة آلاف دينار أو ما يعادل ذلك بالعملة المتداولة قانوناً، كل من ارتكب أياً مما يأتي:

1. إنشاء موقع إلكتروني أو نشر معلومات على شبكة الإنترنت بقصد التحريض على ارتكاب أعمال عنف أو الإساءة للنظام العام.

2. إرسال رسائل تهديد أو ابتزاز عبر وسائل تقنية المعلومات."

وهكذا جرّم القرار بقانون بعض الجرائم المتعلقة بالتحريض على العنف والتهديد والابتزاز الإلكتروني. مع ذلك، يجب أن يعتبر المشرع الفلسطيني تجربة الأردن في هذا المجال، وأن يستفيد منها في وضع القوانين اللازمة لتجريم الشروع في الجرائم الإلكترونية. ويجب أن يحدد بدقة نوعية الجرائم التي يتم تجريم الشروع فيها، وكذلك العقوبات التي يتم فرضها على المتورطين في هذه الجرائم.

من المهم أن يتم تعزيز الوعي لدى المواطنين بأهمية الحفاظ على الأمن الإلكتروني، وكذلك بأن الأفعال التي تسبق ارتكاب الجريمة الإلكترونية يمكن أن تعاقب عليها القانون، ويمكن للمشرع الفلسطيني أن يتعاون مع الجهات المعنية لتوفير وسائل الحماية الإلكترونية والأدوات الضرورية للحفاظ على الأمن الإلكتروني، وذلك للحد من انتشار هذه الجرائم وتعزيز الأمن والسلامة الإلكترونية في فلسطين (تفتقر فلسطين حالياً إلى تشريعات خاصة بالشروع بالجرائم الإلكترونية، لذا لا توجد أحكام قضائية واضحة بشأن هذا النوع من الجرائم، ومع ذلك، فقد لجأت بعض المحاكم الفلسطينية إلى تطبيق بعض القوانين العامة للنظر في قضايا تتعلق بالجرائم الإلكترونية، مثل:

– قانون العقوبات رقم 16 لسنة 1960 وتعديلاته النافذ في الضفة الغربية: حيث استندت بعض المحاكم إلى نصوصه العامة كجرائم السرقة، والاحتيال، وانتهاك الخصوصية، وغيرها.).

فيما يخص موقف المشرع الفلسطيني من الجرائم الإلكترونية المصرفية فقد نصت المادة (52) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية الفلسطيني بأنه: " تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، في أي من الحالات الآتية: 1. إذا وقعت الجريمة على موقع أو نظام معلوماتي أو بيانات أو أرقام أو حروف أو شفرات أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها، بما في ذلك الهيئات المحلية. 2. ارتكاب الجاني الجريمة من خلال عصابة منظمة. 3. التغرير أو استغلال من لم يكمل الثامنة عشر سنة ميلادية. 4. إذا وقعت الجريمة على نظام معلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال أو بتقديم خدمات الدفع أو التقاص أو التسويات أو أي من الخدمات المصرفية المقدمة من البنوك والشركات المالية".

أما بالنسبة لحقوق الملكية الفكرية أو الأدبية أو الصناعية، قد قام المشرع الفلسطيني من خلال القرار بقانون المختص بشأن الجرائم الالكترونية النافذ بمعاقبة كل من انتهك حق من الحقوق السابق ذكرها، فإنه يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة مالية لا تقل عن خمسمائة دينار أردني ولا تزيد عن ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانونا، أو بكلتا العقوبتين (المادة (20)، من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته، 2018).

أما فيما يتعلق بجريمة تزوير مستند الكتروني رسمي من مستندات الدولة أو الهيئات أو المؤسسات العامة، فإن المشرع الفلسطيني نص من خلال القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية في المادة (11)، التي نصت على أنه:" 1. كل من زور مستنداً إلكترونياً رسمياً من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفاً به قانوناً في نظام معلوماتي، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً. 2. إذا وقع التزوير، فيما عدا ذلك من المستندات، وكان من شأن ذلك إحداث ضرر، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 3. كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة استعمال السند المزور وفق قانون العقوبات النافذ. 4. كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه أو إتلافه أو تعييبه أو تعديله أو تحويره، أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته أو معلوماته، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً. 5. إذا وقع التزوير أو التلاعب فيما عدا ذلك من التواقيع الإلكترونية المذكورة في الفقرة (4) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد

على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 6. كل من أنشأ بيانات توقيع أو أداة نظام توقيع إلكتروني رسمي أو للهيئات أو للمؤسسات العامة لا يحق له الحصول عليه، مستخدماً في ذلك معلومات أو بيانات كاذبة أو خاطئة، أو تواطأ مع غيره في إنشاء ذلك، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً. 7. إذا وقع الإنشاء فيما عدا ذلك من التواقيع الإلكترونية المذكورة في الفقرة (6) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد عن ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

يتضح لنا من خلال دراسة مقتضيات القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية، وبحسب نص المادة (49) منه بأن المشرع الفلسطيني نص بشكل صريح على أن كل من شرع بارتكاب جناية أو جنحة من الجرائم الوارد ذكرها في هذا القرار بقانون يعد مرتكبا جريمة الشروع ويعاقب بنص العقوبة المقررة لكل جريمة على حدة، التي نصت على أنه:" يعد مرتكباً جريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها".

الفرع الثاني: موقف الاتفاقيات الدولية من تجريم الشروع في الجرائم الالكترونية

على صعيد التعاون الدولي فهناك جهود تبذل ليس على مستوى إقليم بعينه ولا على مستوى دولة بحد ذاتها ولكن على المستوى الدولي وذلك عن طريق الاهتمام بالمؤتمرات الدولية بجرائم الحاسب الآلي، وان كان يدل ذلك على شيء فيدل على خطورة تلك الجرائم وجسامة الأضرار التي تعاني منها الدول، وقد يتبادر إلى أذهان البعض أن اهتمام المؤتمرات الدولية بالجريمة ليس بالأمر الجديد، ولكن هناك مؤتمرات دولية تعقد لهذا الشأن فما وجه الغرابة في ذلك، ولكن ما هو جديد أن نجد مؤتمرات تهتم بطائفة من الجرائم وتخرج بتوصيات محددة ويطلب من الدول على إثرها تجريم أنشطة بعينها وهذا هو الجديد (الهيتي، 2009، ص 163).

وفيما يخص إصدار التشريعات ضد جرائم الإنترنت، تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (1973م) فقد عالج قضايا الاحتيال بواسطة الحاسب الآلي إضافة إلى شموله فكانت فقراته شاملة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشرع عليها.

يعتمد التعاون الدولي على قوانين الجرائم الإلكترونية الوطنية المنسقة، التي تجرم الجريمة الإلكترونية، والقوانين الإجرائية الوطنية للجرائم الإلكترونية التي تحدد قواعد الإثبات والإجراءات الجنائية. كما يمكن أيضًا تسهيل التعاون الدولي من خلال تنسيق الصكوك الثنائية والإقليمية والمتعددة الأطراف بشأن الجريمة الإلكترونية، حيثما دعت الحاجة. وهناك حاجة أيضًا إلى الانضمام إلى صكوك الجريمة الإلكترونية الإقليمية والمتعددة الأطراف أو التصديق عليها لجعل هذه الصكوك ملزمة قانونًا. لمزيد من القراءة عن التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية بشكل عام.

ومع ذلك، قد يظل التعاون الدولي ممكنًا حتى بدون تفسير صارم لشرط ازدواجية التجريم. وعلاوة على ذلك، كلما اشترط توافر ازدواجية التجريم وجب اعتبار ذلك الشرط مستوفى بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن نفس فئة الجرائم التي تدرجه فيها الدولة الطرف الطالبة أو تستخدم في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف الطالبة، إذا كان السلوك الذي يقوم عليه الجرم الذي تُلتمس بشأنه المساعدة يعتبر فعلا إجراميا في قوانين كلتا الدولتين الطرفين (الفقرة الثانية من المادة 43 من اتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2003).

من الآليات الرسمية التي تتضمن التعاون الدولي هناك معاهدات ثنائية واقليمية ومتعددة الأطراف بشأن الجرائم الالكترونية، في حين أن واقع هذا التعاون هو عامل بارز في هذه المعاهدات، ونستحضر في هذا الصدد اتفاق بشأن التعاون على مكافحة الجرائم في مجال المعلومات المحاسبية لعام 2001 والذي تضمن عددا من المواد المخصصة للتعاون الدولي (المواد من 5-7)، والتي تغطي أنواع التعاون التي تغطيها هذه الاتفاقية (أي تبادل المعلومات، وتقديم المساعدة القانونية وفقا للصكوك الدولية، ومنع الجرائم الالكترونية واكتشافها وقمعها والتحقيق فيها على سبيل المثال لا الحصر، كذلك الطريقة التي يمكن للدول الأعضاء طلب المساعدة بها، والمبادئ التوجيهية للدول الأعضاء حول كيفية تنفيذ هذه الطلبات. وتتضمن المادة 8 من هذه الاتفاقية الظروف التي يمكن بموجبها رفض طلب المساعدة (أي عندما ينتهك هذا الطلب القانون الوطني للدولة) ومتطلبات الدولة الرافضة لإخطار الدولة الطالبة كتابيًا برفض الطلب وسبب (أسباب) الرفض (الوحدة التعليمية 7، التعاون الدولي على مكافحة الجريمة الالكترونية، سلسلة وحدات تعليمية منشورة على الموقع الالكتروني لمكتب الأمم المتحدة المعني بالمخدرات والجريمة: https://www.unodc.org/e/key-issues/formal-7j/ar/cybercrime/module-4/international-cooperation-mechanisms.html).

وبالرجوع إلى مقتضيات المادة 42 من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية الفلسطيني، نجد بأن المشرع الفلسطيني أوعز إلى الجهات المختصة على العمل على تيسير التعاون مع

نظيراتها في البلدان الأجنبية الأخرى وذلك كله في إطار الاتفاقيات الدولية والاقليمية والثنائية المصادق عليها أو طبق مبدأ المعاملة بالمثل، والقصد من ذلك هو الإسراع في تبادل المعلومات وذلك من شأنه أن يكفل الإنذار المسبق للجرائم المتعلقة بأنظمة المعلومات والاتصال من أجل تفادي ارتكابها والمساعدة أيضا على التحقيق فيها وتتبع مرتكبي تلك الجرائم، في حين ذهب المشرع الفلسطيني في نفس المادة المذكورة أعلاه إلى أن هذا التعاون في ذلك المجال يتوقف على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، مع التزامها بعدم ارسال المعلومات المحالة إليها إلى طرف آخر أو استغلالها لأغراض غير مكافحة الجرائم الواردة في هذا القرار بقانون، حيث نصت المادة على أنه "والتي نصت على أنه:" 1- تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات، بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال، وتفادي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها. 2- يتوقف التعاون المشار إليه في الفقرة السابقة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعينة بهذا القرار بقانون".

وترى الباحثة أنه بالنسبة للاتفاقيات الدولية لم تتطرق إلى الشروع في الجريمة الالكترونية بشكل خاص، في حين أشارت إلى الجريمة الالكترونية بشكل عام، وعليه كان من المفترض التطرق إلى الشروع في الجريمة الالكترونية كونه يمس مصالح المجتمع.

الفصل الثاني

الأحكام الإجرائية المتعلقة بالشروع في الجرائم الالكترونية

تُعدّ الجرائم الإلكترونية من الجرائم الحديثة التي ظهرت في العقود الأخيرة مع تطور تكنولوجيا المعلومات والاتصالات وانتشار استخدام الإنترنت والأجهزة الذكية (Gercke, M. Understanding cybercrime: Phenomena, challenges, and legal response. ITU (2012)، وقد عرّف المشرع الفلسطيني الجريمة الإلكترونية في المادة 4 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته بأنها: "أي جريمة ترتكب باستخدام شبكة الإنترنت، أو نظام المعلومات الإلكتروني ،أو وسيلة تقنية معلومات ،أو إحدى وسائل تكنولوجيا المعلومات".

كما منحت التشريعات أجهزة إنفاذ القانون صلاحيات واسعة في مجال التحقيق والتحري والتفتيش والاطلاع على الجرائم الإلكترونية والحصول على الأدلة الرقمية المتعلقة بها والبيانات والمعلومات المخزنة في الأنظمة والشبكات الإلكترونية (Clough, 2010).

حيث ستتطرق الباحثة في هذا الفصل حول الأحكام الإجرائية المتعلقة بالشروع في الجرائم الإلكترونية، ويتكون من مبحثين الأول كيفية التحري في الجرائم الإلكترونية، والثاني يتناول العقاب في الشروع في الجرائم الإلكترونية.

المبحث الأول: كيفية التحري في الجرائم الالكترونية

إن التمييز بين الجرائم الإلكترونية والجرائم التقليدية إجرائياً، سواء من حيث الاختصاص أو إجراءات وخطوات التحقيق أو عملية الإثبات ووسائله، هام جداً، فالتحقيق في الجرائم الإلكترونية تختص به نيابة متخصصة وفق إجراءات وقواعد إثبات خاصة، يساعدها في ذلك ضابطة قضائية متخصصة بالجرائم الإلكترونية، على عكس ما يسير في الجرائم التقليدية التي تعمل وتختص بالتحقيق فيها النيابة العامة تساعدها الضابطة القضائية ذات الاختصاص العام، وفقاً لقواعد التحقيق والإثبات التقليدية (الباقي، 2018، ص484).

تتطلب عملية التصدي للجرائم الإلكترونية التحقيق الفعّال والقدرة على جمع الأدلة والإثبات الجنائي، ولتحقيق ذلك من المهم تحديد نموذج تحقيقي أمثل، والاستجابة للتحديات القانونية التي تقف عائق وتعرقل تنفيذ القانون وصولاً لعملية التحقيق في الجريمة الإلكترونية وإثباتها، وقد أدركت السلطة الوطنية الفلسطينية أهمية تكنولوجيا المعلومات كمفتاح لتحسين أداء الإدارة والأمن على سواء (الباقي، 2018، ص 286).

سنتحدث في هذا المبحث عن كيفية التحري في الجرائم الإلكترونية وينقسم إلى مطلبين (الأول) خصوصية التحقيق في مرحلة ما قبل المحاكمة ويتفرع الى جمع الاستدلالات ومرحلة التحقيق الابتدائي، وفي (المطلب الثاني) التحقيق بالشروع في الجرائم الإلكترونية، ويتفرع إلى فرعين الأول مسرح الجرائم الإلكترونية، والثاني التفتيش في الجرائم الالكترونية.

المطلب الأول: خصوصية التحقيق الابتدائي

تواجه أجهزة إنفاذ القانون تحديات كبيرة في التحقيق في الجرائم الإلكترونية، نظراً للتطور الهائل في تقنية المعلومات والاتصالات، وضرورة مراعاة التوازن بين متطلبات التحقيق وحماية خصوصية أصحاب المعلومات، فالخصوصية أصبحت ركيزة أساسية للمجتمعات الديمقراطية والاقتصاديات الحديثة، إلا أن الوصول إلى المعلومات الشخصية من قِبل السلطات القضائية لا يزال يثير جدلاً كبيراً (Los Angeles Times, http://www.latimes.com/business/la-fi-mh-the-conflict-between-apple-and-the-fbi-.20160219-column.html).

وتختلف آليات التوفيق بين متطلبات التحقيق في الجرائم الإلكترونية وحماية الخصوصية من دولة لأخرى، إلا أنه ينبغي إيجاد صيغ توازن بين احتياجات إنفاذ القانون والحفاظ على الحقوق الأساسية للأفراد، فالتحدي الحقيقي هو كيفية تمكين أجهزة إنفاذ القانون من الوصول للمعلومات ذات الصلة بالتحقيقات، مع الالتزام التام بالضوابط والإجراءات القانونية التي تكفل عدم المساس بالخصوصية إلا بالقدر اللازم (Drewer,

Daniel and Jan Ellermann, Europol's data protection framework as an asset in the fight against. Cybercrime, ERA. (http://link.springer.com/article/10.1007/s12027-012-0268-6).

ينص قانون الإجراءات الجزائية رقم (3) لسنة 2001 المادة (51)، على أن للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق والبريد الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة وشخص مرتكبها، كما يجوز له مراقبة المحادثات السلكية واللاسلكية وإجراء تسجيلات لأحاديث في مكان خاص، حيث هذا النص يتعلق بتفتيش وضبط الأدلة المادية وليس الرقمية، أما القانون رقم (3) لسنة 1996 بشأن الاتصالات السلكية واللاسلكية، فينص على أن سرية الاتصالات على الأراضي الفلسطينية مصونة ولا يجوز المس بها إلا للسلطة العامة وفي حدود القانون، كما أورد المشرع أحكاماً عديدة وتفصيلية في القانون تتعلق بالخصوصية، إلا أنها غير كافية لتنطبق على القضاء الإلكتروني.

ونصت المادة (4) من قرار بقانون (10) لسنة (2018) بشأن الجرائم الالكترونية بأنه " 1. كل من دخل عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً، أو نظاماً، أو شبكة إلكترونية، أو وسيلة تكنولوجيا معلومات، أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. إذا ارتكب الفعل المذكور في الفقرة (1) من هذه المادة، على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 3. إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو حذفها أو إضافتها أو إفشاؤها أو إتلافها أو تغييرها أو نقلها أو التقاطها أو نسخها أو نشرها أو إعادة نشرها أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني أو إلغاؤه أو تعديل محتوياته أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 4. إذا ارتكب الفعل المذكور في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً."

ونصت المادة (7) من قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية بأنه: "كل من التقط ما هو مرسل عن طريق الشبكة أو إحدى وسائل تكنولوجيا المعلومات أو سجله أو اعترضه أو تنصت عمداً

دون وجه حق، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين."

وكذلك نصت المادة (9) من قرار بقانون (10) لسنة (2018) بشأن الجرائم الالكترونية على أنه "1. كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. إذا كان الانتفاع في الفقرة (1) من هذه المادة بقصد الربح، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.".

تجرم هذه المادة التنصت والتقاط المعلومات المرسلة عبر شبكات الاتصالات بدون وجه حق، ما يحمي خصوصية الاتصالات، لكنها لا تشير إلى كيفية التحقيق بما يراعي الخصوصية.

تتعلق المواد 4، 7، 9 من قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية بشكل مباشر بموضوع خصوصية التحقيق في الجرائم الإلكترونية، إذ إنها تتضمن أحكاماً تجرم الاعتداء على خصوصية الأفراد وبياناتهم عبر الوسائل الإلكترونية، وبالتالي فهي توفر إطاراً قانونياً يسمح لأجهزة إنفاذ القانون بالتحقيق في مثل تلك الجرائم الماسة بالخصوصية، إلا أنه لا بد من الموازنة بين حق المجتمع في ملاحقة الجرائم وحق الأفراد في خصوصيتهم، وعدم تجاوز الحدود أثناء عمليات التفتيش وجمع الأدلة والالتزام بالضمانات القانونية والإجرائية، لذا ينبغي وجود نصوص أخرى تكفل حماية خصوصية الأفراد أثناء التحقيقات بما يضمن التوزان بين متطلبات العدالة وحقوق الأفراد.

وترى الباحثة بأن القرار بقانون قد نظم الوصول إلى المعلومات، وحدد الأطراف المخولة بالوصول إليها، وكذلك حدد عقوبة الإفشاء غير المصرح بها، ويتعين على المحققين والجهات القضائية احترام هذه الضوابط وتنفيذها بدقة لضمان حفظ خصوصية التحقيق وتحقيق العدالة.

الفرع الأول: مرحلة جمع الاستدلالات

وبهذه المرحلة يقوم مأموري الضبط القضائي–الشرطة– بمجموعة من الإجراءات التي أجاز لهم القانون القيم بها لجمع الأدلة قبل إحالة هذه الاستدلالات للنيابة العامة للقيام بتحقيقها، وهذا ما تؤكد عليه المادة (3) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته التي نصت على أنه:" 1– تنشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية"، وتتولى النيابة العامة الإشراف القضائي عليها، كل في دائرة اختصاصه. 2– تتولى المحاكم

النظامية والنيابة العامة، وفقاً لاختصاصاتهما، النظر في دعاوى الجرائم الإلكترونية"، حيث أن المشرع الفلسطيني ذهب من خلال مقتضيات المادة (33) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية على أن للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الالكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات وغيريها من البيانات ذات الصلة بالجريمة الالكترونية، كما شرع للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة، فنصت المادة (33) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته والتي نصت على :" 1. للنيابة العامة الحصول على الأجهزة، أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعمليها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية. 2. للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة. 3. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات. 4. إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات. 5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها. 6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية". كما أن هذه الإجراءات نصت عليها المادة (22) من قانون الإجراءات الجزائية وهي على النحو التالي:

"1- قبول البلاغات والشكاوى التي ترد إليهم بشأن الجرائم وعرضها دون تأخير على النيابة العامة.

2- إجراء الكشف والمعاينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق، والاستعانة بالخبراء المختصين والشهود دون حلف يمين.

3- اتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة.

4- اثبات جميع الإجراءات التي يقومون بها في محاضر رسمية بعد توقيعها منهم ومن المعنيين بها."

فيما تقدم نستخلص مما سبق بأن الإجراءات التي يتوجب على مأمور الضبط القضائي في حال وقوع جريمة أن يقوموا بها جاءت لكافة الجرائم بشكل عام دون تخصيص، أي أن ذلك ينطبق على الجريمة الإلكترونية في حال حدوثها تباشر الشرطة بإجراءات جمع الاستدلالات فيما يخصها، فيحق لرجال الشرطة عملية الاستعانة بالخبراء وذوي الاختصاص الإلكتروني بهدف كشف الجريمة واتخاذ جميع الطرق والوسائل اللازمة للمحافظة على أدلة الجريمة.

وذكر في المادة (34) من قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية بأنه لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة، والتي نصت على أنه:" 1. لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جدية، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى النيابة العامة. 2. للنائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأي بيانات، بما فيها حركة الاتصالات أو معلومات إلكترونية أو بيانات مرور أو معلومات المشترك التي يراها لازمة لمصلحة التحقيقات لغايات الفقرة (1) من هذه المادة، باستعمال الوسائل الفنية المناسبة، والاستعانة بذلك عند الاقتضاء بمزودي الخدمات، حسب نوع الخدمة التي يقدمها".

حيث من خلال هذه المادة يتضح أن المشرع حاول مواكبة التطورات التي تحدث في مجال المعلوماتية والجرائم المرتكبة فيها والطرق المتطورة والمتقدمة في أساليب ارتكاب الجريمة وعملية التهرب من المسؤولية الجزائية وهذا ما أدى به للسماح للمكلفين بالتحقيق باتخاذ إجراءات تمس بالحقوق والحريات التي تكفلها جل التشريعات الداخلية والدولية، فقد أجاز عملية مراقبة واعتراض كل أنواع المراسلات بما فيها الإلكترونية كما أجاز التنصت والتقاط المكالمات الهاتفية ونسخ الرسائل القصيرة وغيره ما شابه ذلك والتقاط الصور ومن ثمة مواجهة المجرم الإلكتروني بها واستخدامها كدليل في مواجهته وإدانته بالاعتماد عليها.

وهنا عملية مراقبة المراسلات والاتصالات وتجميعها لا تكون بشكل عشوائي، بل يجب أن تتم في إطار قانوني وفقاً لمبدأ المشروعية (حسام، 2002، ص 35)، فقد نصت المادة مادة (40) على أنه فيما عدا الالتزامات المهنية المنصوص عليها في القانون، لا يجوز الاستناد إلى أسرار المهنة أو مقتضياتها للامتناع عن تقديم المعلومات أو الوثائق التي تطلب وفقاً لأحكام القانون."

وعليه نستطيع القول بأن مرحلة جمع الاستدلالات في الجريمة الإلكترونية يتم عبر شبكة الانترنت وأجهزة الحاسب الآلي، بهدف الحصول وكسب كافة البيانات والمعلومات المهمة والضرورية اللازمة المرتبطة

بالجرائم التي تقع بواسطة الحاسب الآلي أو أية وسيلة الكترونية لضبط جرائم الكمبيوتر والانترنت، فمرحلة جمع الاستدلالات هي مرحلة جمع المعلومات والأدلة (حسام، 2002، ص35).

وقد نصت المادة (37) من قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية بأنه "يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية من أدلة الإثبات." وكذلك المادة (38) من نفس القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته فقد نصت بأنه "تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي."

وهذا يتطلب بالضرورة إعداد وتجهيز طاقم خاص وكوادر بشرية من رجال الشرطة بهدف تمكنهم من التعامل مع الجريمة الالكترونية وإلا تعرضنا لفقدان الدليل، لأن الشرطة هنا ستتعامل مع بيانات دقيقة على الأجهزة الإلكترونية وعدم التعامل معها بشكل فني دقيق سيؤدي إلى فقدانها، لا سيما وأن نوعية المجرم في هذه الجريمة الإلكترونية تختلف في طريقته وأسلوبه الإجرامي عن المجرم في الجريمة التقليدية الذي يرتكب جريمته باستعمال أدوات مادية يسهل التعامل معها وضبطها والتحفظ عليها.

وقد نصت المادة (39) من نفس القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته بأنه "1. لجهات التحري والضبط المختصة، إذا ما رصدت قيام مواقع إلكترونية مستضيفة داخل الدولة أو خارجها، بوضع أي عبارات، أو أرقام، أو صور، أو أفلام، أو أي مواد دعائية ،أو غيرها، من شأنها تهديد الأمن القومي أو النظام العام أو الآداب العامة، أن تعرض محضراً بذلك على النائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية أو حجب بعض روابطها من العرض. 2. يقدم النائب العام أو أحد مساعديه طلب الإذن لمحكمة الصلح خلال (24) ساعة، مشفوعاً بمذكرة برأيه، وتصدر المحكمة قرارها في الطلب، في ذات يوم عرضه عليها إما بالقبول أو بالرفض، على ألا تزيد مدة الحجب على ستة أشهر، ما لم تجدد المدة وفقاً للإجراءات المنصوص عليها في هذه المادة."

بناءً على المادة (39) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية يتضح بأنه في عملية التحقيق عندما يرصد فريق التحقيق أو جهات التحري والضبط المختصة مواقع إلكترونية تحتوي على محتوى يهدد الأمن القومي أو النظام العام أو الآداب العامة، يتم جمع الأدلة والاستدلالات المتعلقة بهذه المواقع، حيث أنه في هذه المرحلة سيقوم فريق التحقيق بتحليل المحتوى الموجود من الروابط والمحتوى المتعلق بهذه المواقع، وتوثيق أي أدلة تشير إلى تهديد الأمن القومي والنظام العام أو الآداب العامة، بعد جمع الاستدلالات اللازمة يتعين على جهات التحقيق تقديم تقرير يحتوي على المعلومات والأدلة إلى النائب

العام أو أحد مساعديه، وطلب الإذن لحجب الموقع أو بعض روابطها من العرض، هذا يعني أن مرحلة جمع الاستدلالات تمهد الطريق لاتخاذ إجراءات قانونية أخرى، مثل حجب المواقع الإلكترونية، أو توجيه الاتهامات في حالة إثبات التهديد للأمن القومي أو النظام العام أو الآداب العامة، وفي الجريمة الالكترونية يكون الدليل مصدره ليس فقط داخل الدولة وفي حدود محصورة، حيث يتعدى الحدود وذلك لأنه من خصائص الجريمة الإلكترونية أنها عابرة للحدود، والتي نصت على أنه:" 1. لجهات التحري والضبط المختصة، إذا ما رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو غيرها، من شأنها هديد الأمن القومي أو النظام العام أو الآداب العامة، أن تعرض محضراً بذلك على النائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية أو حجب بعض روابطها من العرض. 2. يقدم النائب العام أو أحد مساعديه طلب الإذن لمحكمة الصلح خلال (24) ساعة، مشفوعاً بمذكرة برأيه، وتصدر المحكمة قرارها في الطلب، في ذات يوم عرضه عليها إما بالقبول أو بالرفض، على ألا تزيد مدة الحجب على ستة أشهر، ما لم تجدد المدة وفقاً للإجراءات المنصوص عليها في هذه المادة".

ويجب أن يتم جمع الاستدلالات بشكل دقيق ومنهجي لضمان قوة الحجة القانونية وتحقيق العدالة في عملية التحقيق، حيث تعد مرحلة جمع الاستدلالات وتحليلها جزءاً حاسماً من العملية القانونية للتحقيق، حيث تعتمد القرارات اللاحقة مثل حجب المواقع الإلكترونية، على قولة الأدلة والاستدلالات التي تم جمعها في هذه المرحلة.

الفرع الثاني: مرحلة التحقيق الابتدائي

إن الغاية من التحقيق الجنائي الوصول إلى الحقيقة عن طريق جمع الأدلة من خلال الاستماع إلى الشهود والاستعانة بالخبراء والاعتراف ومن جهة أخرى، تقدير كل ذلك لاتخاذ القرار الصحيح إما بالإحالة إلى المحكمة أو عدم السير في الدعوى فالقاعدة أنه لا يمكن بناء الاتهام دون أن يكون هناك منطق للتحقيق يضمن حق الفرد في مرحلة ما قبل المحاكمة وهذا يبين العلاقة ما بين مرحلة جمع الاستدلالات ومرحلة التحقيق الابتدائي فالهدف لكل منهما هو محاولة كشف الحقيقية.

تمر الدعوى الجنائية قبل أن توضع أمام القضاء بمرحلة التحقيق الابتدائي، هذه المرحلة يتم فيها جمع الأدلة والتصرف فيها، مما يعني أن التحقيق له معنيان يقصد بها إجراءات التحقيق التي تقوم بمباشرتها سلطة التحقيق مضافا إليها إجراءات جمع الاستدلالات التي يقوم بها مأموري الضبط القضائي بما فيهم

النيابة العامة إذا لم تكن لها سلطة التحقيق، والمعنى الآخر يقصد به ما يقوم به قاضي التحقيق أو النيابة العامة في الأحوال التي يباشر فيها التحقيق.

في هذه المرحلة يكون الدور للنيابة العامة في التحقيق والاستجواب في الجريمة الإلكترونية، وهي المرحلة الأهم ومنها نبدأ في تحريك الدعوى الجزائية ضد المتهم في الجريمة الإلكترونية، وفي هذه المرحلة فقد أجاز قانون الإجراءات الجزائية في المادة (64) بأنه "يستعين وكيل النيابة العامة بالطبيب المختص وغيره من الخبراء لإثبات حالة الجريمة المرتكبة، ويقوم الطبيب المنتدب لذلك وغيره من الخبراء باتخاذ الإجراءات اللازمة تحت إشراف الجهة المختصة بالتحقيق، وللمحقق الحضور أثناء مباشرة أعمال الخبراء، إذا قدر أن مصلحة التحقيق تقتضي بذلك".

ونصت المادة (32) من قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية بأنه: "1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. 2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة. 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية."

ونستنتج مما سبق، بأنه على الرغم من أن القانون أجاز لوكيل النيابة المختص بالتحقيق الاستعانة بأصحاب الخبراء وبمن يريد من المختصين في عالم الإلكترونيات، إلا أن ذلك لا يعني بأي حال من الأحوال عدم ضرورة إعداد كادر مختص من وكلاء النيابة للتحقيق في الجرائم الإلكترونية، فأخطر مرحلة من مراحل التحقيق التي تقع على عاتق وكلاء النيابة هي استجواب المتهم، فكيف سيتم استجواب المتهم في جريمة الكترونية دون أن يكون وكيل النيابة المحقق ملم بكافة نواحي وتفاصيل أركان الجريمة الإلكترونية من ناحية قانونية من جانب ومن الناحية الفنية التقنية من جانب آخر فيما يخص الأدلة التي بين يديه سواء في البيانات المخزنة على الأجهزة الالكترونية من أرقام وصور ودلالاتها في ارتكاب الجريمة، وفيما يخص خاصية الجريمة الإلكترونية بأنها عابرة للحدود فقد وردت مواد في قرار بقانون عملت على تسهيل وتيسير أمور مرحلة التحقيق الابتدائي فيها، مادة (42) من قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية بأنه: " 1. تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في

إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات، بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال، وتفادي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها. 2. يتوقف التعاون المشار إليه في الفقرة السابقة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعينة بهذا القرار بقانون." ونصت المادة (43) من قرار بقانون لسنة (2018) بأنه "1. يتعين على الجهات المختصة أن تقدم العون للجهات النظيرة في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة، وتسليم المجرمين في التحقيقات والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القرار بقانون، وفقاً للقواعد التي يقررها قانون الإجراءات الجزائية النافذ والاتفاقيات الثنائية أو متعددة الأطراف التي تكون الدولة طرفاً فيها، أو بمبدأ المعاملة بالمثل، وذلك بما لا يتعارض مع أحكام هذا القرار بقانون أو أي قانون آخر. 2. لا ينفذ طلب المساعدة القانونية أو طلب تسليم المجرمين، استناداً إلى أحكام هذا القرار بقانون، إلا إذا كانت قوانين الدولة الطالبة وقوانين الدولة تعاقب على الجريمة موضوع الطلب أو على جريمة مماثلة، وتعتبر ازدواجية التجريم مستوفاة، بغض النظر عما إذا كانت قوانين الدولة الطالبة تدرج الجريمة في فئة الجرائم ذاتها أو تستخدم في تسمية الجريمة المصطلح ذاته المستخدم في الدولة، بشرط أن يكون الفعل موضوع الطلب مجرماً بمقتضى قوانين الدولة الطالبة.".

المطلب الثاني: التحقيق بالشروع في الجرائم الالكترونية

هي مرحلة لاحقة لمرحلة التحري والاستدلال التي يقوم بها رجال الضبطية القضائية، وسابقة عن مرحلة المحاكمة وتختلف هذه المرحلة عن سابقتها فهي أشد خطورة عن الأخرى نظراً للسلطات التي خولها القانون لقاضي التحقيق بمناسبة القيام بعمله والإجراءات التي تميز التحقيق، فقد تعد إجراءات التفتيش والحجز ومراقبة الاتصالات الإلكترونية وسماعها والاطلاع على الرسائل أهم أعمال التحقيق في الجريمة الإلكترونية.

تعتبر هذه المرحلة بأنها عملية قانونية تتم بعد جمع الأدلة والاستدلالات المتعلقة بجرائم تتعلق بالتكنولوجيا المعلومات ويتطلب التحقيق فيها مهارات فنية وقانونية تختلف عن تحقيق الجرائم التقليدية.

الفرع الأول: مسرح الجرائم الالكترونية

يعرف مسرح الجريمة بأنه: " كل مكان اتصل بالنشاط الإجرامي الذي ترتب عليه وقوع الجريمة أو حوى دليلاً يتصل بها"، فمن المعروف بأن مهمة رجال الضبط القضائي الأساسية بمجرد علمهم بوقوع جريمة الانتقال إلى مسرح الجريمة وتأمينه إلى حين حضور وكيل النيابة المختص، وذلك بهدف مباشرة عمله

وإجراء كافة التحقيقات اللازمة في مسرح الجريمة من سماع شهود وتنظيم محضر كشف على مسرح الجريمة وتوصيفه بدقة وضبط أدوات الجريمة الموجودة في مسرح الجريمة لمواجه المتهم بها حين استجوابه (المعايطة، 2007، ص 53)، فالمحقق في مسرح الجريمة الالكترونية الذي ينتقل لمكان الجريمة يجب عليه الإلمام والمعرفة الكافية في الجريمة الالكترونية حتى يتمكن من تحديد الدليل الذي يبحث عنه، وعليه يتوجب على المحقق في محضر الكشف على مسرح الجريمة أن يراعي بعض الأمور أهمها:

1. توثيق حالة مسرح الجريمة، أي تصوير الحاسب والأجهزة المرتبطة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.
2. العناية بملاحظة الطريقة التي تم بها إعداد النظام، وتسجيل كافة التفاصيل المتعلقة بحالة الجهاز، مثل تحديد ما إذا كان في وضع التشغيل (مفتوحا) وقت ضبطه أم لا، وما إذا كان موصولاً بالإنترنت أم لا.
3. ملاحظة وإثبات حالة التوصيلات والكابلات المرتبطة والمتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة، وتحديد هوية توثيق جهاز الحاسوب والأجهزة الملحقة به التي يعثر عليها في مسرح الجريمة، حيث إن رمز بروتوكول الإنترنت (IP) يلعب دوراً كبيراً في تحديد موقع ومكان المشتبه به.
4. تحديد هوية وتوثيق أجهزة التخزين (مثل CDs وDVD) التي يعثر عليها في مسرح الجريمة.
5. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات بهدف عملية التأكد بأن محيطها الخارجي خالي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.
6. التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق ا لكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة، وفحصها، ويرفع من عليها البصمات ذات الصلة بالجريمة.
7. التحفظ على مستندات الإدخال والمخرجات الورقة للحاسب ذات الصلة بالجريمة، بهدف رفع ومضاهاة ما قد يوجد عليها من بصمات.
8. قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات، في ظاهرة الإجرام الإلكتروني ومخاطرها، أكاديمية شرطة دبي، مركز البحوث والدراسات، تاريخ الانعقاد: 26 نيسان 2003 تاريخ الانتهاء28 نيسان 2003 الدولة: دبي الإمارات

العربية المتحدة: " واتس آب ، فيسبوك ، أنترنت ، شروحات تقنية حصرية – المحترف (th3professional.com).

مما سبق يتضح لنا أن مسرح الجريمة الالكترونية له طبيعة خاصة، حيث يصعب التعامل معها بالطريقة التقليدية للتعامل مع مسرح الجريمة التقليدية، وذلك لوصفها بأنها جرائم خفية وأقل عنفا في التنفيذ وعابرة للحدود وسرعة التطور بارتكابها.

الفرع الثاني: التفتيش في الجرائم الالكترونية

يعتبر التفتيش والتحفظ على أجهزة الحاسوب وأنظمة تخزين المعلومات وسيلة هامة في الكشف عن الجرائم الإلكترونية، لم يتطرق قانون الإجراءات الجزائية الفلسطيني للتحفظ المستعجل على بيانات الحاسوب (عبد الباقي، 2018، ص 289).

ويتم التفتيش الإلكتروني عادة على مرحلتين: الأولى في الموقع on–site، وهنا يمكن أن يتم التفتيش في حضور صاحب الجهاز أو شاهدين؛ أما التفتيش الذي يتم خارج الموقع off–site، فإنه يتعذر حضور صاحب الجهاز أو الشاهدين كون أن البحث في المعلومات يستغرق وقتًا طويلاً. وفي المقابل، فإن المؤسسات، والأف أرد أيضاً، عادة ما يعارضون تحريز أجهزتهم ونقلها إلى أقسام التحقيق خوفاً على وثائقهم وملفاتهم من أن يتم الاعتداء عليها بانتحالها أو نسخها مثلاً؛ وبالتالي ضياع حقوق ملكيتهم الفكرية لها، كما أن ذلك قد يؤدي إلى خلل وانقطاع عن العمل في المؤسسة نتيجة لسحب أجهزة الحاسوب منها، خاصة المؤسسات والشركات التي يعتبر الكمبيوتر أساسي في عملها، ولا يتم العمل بدونها مثل البنوك وشركات التأمين، من ناحية أخرى، فإن التفتيش داخل الموقع عادةً ما يؤدي إلى تشويش وانقطاع في العمل، كما يؤدي إلى إضرار بالخصوصية. إن القرار بإجراء التفتيش في الموقع أو خارجه تحكمه، بالإضافة إلى ما تم ذكره، معايير أخرى منها أن جزءًا من التفتيش يجب أن يتم في الموقع أثناء وصل الجهاز بالكهرباء والانترنت، حيث إن فصل الجهاز تمهيدًا لنقله يؤدي إلى ضياع بعض المعلومات. وفي المقابل، فإن استرجاع المعلومات التي تم التخلص منها بحاجة إلى نقل الجهاز إلى المختبر، حيث لا يمكن أن يتم هذا العمل في الموقع، أو على الأقل يعتبر غير عملي كونه بحاجة إلى أجهزة وفريق عمل كبير، كما لا يمكن التحكم بدرجة الحرارة والظروف المحيطة الأخرى (عبد الباقي، 2018، ص 290).

قد تكون الأدلة الجاري التفتيش عنها على جسم الجهاز (Hardware) أو على البرمجيات (Software). لذلك يعتبر التفتيش الالكتروني في منتهى الصعوبة في كثير من الأحيان لأن البرامج والملفات تكون متداخلة عادة، حيث أن بعضها يخص المتهم والبعض الآخر قد يخص أشخاص آخرين. إلا أنه هناك بعض المعايير التي تساعد في حصر نطاق التفتيش، فمثلا إذا كانت التهمة حيازة صور أو فيديوهات

جنسية لأطفال على كمبيوتر المتهم، فيجب حصر نطاق التفتيش في الملفات والبرامج المخصصة للصور والفيديوهات دون غيرها، لكن لم ينل هذا الأمر اهتماما من قبل المشرع الفلسطيني فلا يتضمن قانون الاجراءات الجزائية رقم (3) لسنة 2001 أية نصوص تحدد نطاق التفتيش الالكتروني، وفي التطبيق العملي فإن ملفات المتهم الالكترونية مستباحة لمأموري الضبط القضائي ولأعضاء النيابة العامة، حيث يفتشون ويأخذون نسخا عن الملفات التي يريدونها دون ضوابط محددة، حيث يضبطون الأجهزة وتبقى لديهم فترات طويلة، دون مبرر لذلك، فهذا التصرف غير قانوني قطعا (عبد الباقي، 2018، ص 291).

إن التفتيش عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها، تبعاً لاتهام 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، ومن المهم أن تكون مذكرة التفتيش مسببة، وتحرر باسم واحد أو أكثر من مأموري الضبط القضائي، المادة (39) من قانون الإجراءات الجزائية رقم (3) لسنة 2001.

وتوقع مذكرات التفتيش من قبل عضو النيابة المختص وتشمل (اسم صاحب المنزل المراد تفتيشه وشهرته، عنوان المنزل المراد تفتيشه، الغرض من التفتيش، اسم مأمور الضبط القضائي المصرح له بالتفتيش، المدة التي تسري خلالها مذكرة التفتيش، تاريخ وساعة إصدارها) هذا ضمن ما ورد في مادة (40) من قانون الإجراءات الجزائية (المادة (40) من قانون الإجراءات الجزائية رقم (3) لسنة 2001).

ونصت المادة (42) من قانون الإجراءات الجزائية بأنه " تفتيش المنازل يجب أن يكون نهاراً ولا يجوز دخولها ليلاً، إلا إذا كانت الجريمة متلبساً بها، أو كانت ظروف الاستعجال تستوجب ذلك".

وقد نصت المادة (32) من قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية بأن "1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. 2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة. 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية".

بموجب المادة (32) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية يسمح للنيابة العامة وأعوانها المعينين تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، وذلك بناءً على أمر تفتيش مسبب ومحدد إذا تم ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة خلال التفتيش، يجب على مأموري الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على النيابة العامة، كما يشترط أن يكون مأمور الضبط القضائي مؤهلاً للتعامل مع الجرائم، التي نصت على أنه:" 1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. 2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة. 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية.

أعطى المشرع الفلسطيني صلاحيات للنيابة العامة في الحصول على الأجهزة والأدوات والوسائل والبيانات والمعلومات الإلكترونية ذات الصلة بالجريمة، يُمنح النيابة العامة إذناً بالضبط والتحفظ على نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي تساعد في كشف الحقيقة، إذا لم يكن الضبط والتحفظ على نظام المعلومات ممكناً بشكل فعلي، يُسمح بنسخ البيانات أو المعلومات ذات الصلة بالجريمة على وسيلة تكنولوجية، يجب اتخاذ الاحتياطات اللازمة للحفاظ على سلامة المضبوط المتحفظ عليه وتوثيق عملية الضبط.

المبحث الثاني: آثار الشروع في الجرائم الالكترونية

ساعد التقدم الهائل الذي أصبح واضحاً في المجال التكنولوجي، والزيادة المضطردة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة، من أشخاص طبيعية، أو هيئات وأشخاص معنوية، وكذلك استخدام متزايد لوسائل التواصل الاجتماعي، كل هذا أسهم في ظهور فئة جديدة من الاجرام، مرتبطة بالتكنولوجيا، ومنها جرائم الابتزاز والاحتيال الإلكتروني وكذلك السرقة الإلكترونية والتنصت الهاتفي، وغيرها الكثير من الجرائم، ونظراً لتزايد نسب ارتكاب هذه الجريمة في الآونة الأخيرة، ولأن مثل هذه الجرائم لها خصوصية، ووسائل وطرق تنفيذ خاصة بها، الأمر الذي أدى انعكاس هذه الخصوصية على مضمون الأنظمة والقوانين، حتى تتماشى مع طبيعة الجريمة ومعطياتها وآثارها (عبد العزيز، 2018، ص 29).

وتثير الجرائم الإلكترونية العديد من التحديات القانونية والتقنية أمام أجهزة إنفاذ القانون، خاصة فيما يتعلق بإثبات الجريمة وجمع الأدلة الرقمية، ومن المسائل الهامة في هذا المجال مدى تطبيق العقاب على الشروع في الجرائم الإلكترونية وفقاً للتشريعات النافذة، يهدف هذا المبحث إلى دراسة الأحكام القانونية المتعلقة بالشروع في الجرائم الإلكترونية، وبيان آليات تطبيقها في التشريع الفلسطيني والمقارن.

وبناءً على ذلك فتم تقسيم هذه المبحث إلى مطلبين، (الأول) العقاب على الشروع في الجرائم الإلكترونية ويتفرع العقوبة على الشروع في الجنح والمخالفات، والعقوبة على الشروع في الجنايات، و(المطلب الثاني) تطبيقات الشروع في الجرائم الإلكترونية، وقد تناولت الباحثة في هذه الدراسة الشروع في جريمة الابتزاز والاحتيال الإلكتروني، والشروع في جرائم السرقة الإلكترونية والتنصت الهاتفي على سبيل المثال وليس على سبيل الحصر.

المطلب الأول: العقاب على الشروع في الجرائم الالكترونية

تعد الجرائم الإلكترونية مشكلة متزايدة في العصر الحديث، حيث يستخدم المجرمون التكنولوجيا الحديثة لارتكاب أفعال غير قانونية عبر الإنترنت، يشمل ذلك تصميم مواقع الويب والتطبيقات التي تروج للتشويه أو التبرير لأعمال إبادة جماعية أو جرائم ضد الإنسانية وتشجيع ارتكاب جرائم ضد الإنسانية (Doe, 2020, p 45-61).

وبناء على ذلك، سنقوم في هذا المطلب بالتطرق إلى عقوبة الشروع في الجرائم الجنحوية (الفرع الأول)، على أن نتحدث في (الفرع الثاني) عن عقوبة الشروع في الجنايات.

الفرع الأول: عقوبة الشروع في الجرائم الجنحوية

بالرجوع إلى نصوص مواد القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية نجد أن المشرع الفلسطيني نص على مجموعة من الجرائم الجنحوية والعقوبات المقررة لها، ومن هذه النصوص ما ورد في المادة (4) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته والتي قام المشرع الفلسطيني من خلالها بتجريم الدخول العمد دون وجه حق أو بأي وسيلة من الوسائل إلى موقع الكتروني أو نظام أو شبكة أو تجاوز بذلك الدخول المصرح به أو استمر بالتواجد بها بعد علمه بذلك، كما نص من خلال نفس المادة أنه إذا ارتكب الفعل المذكور أعلاه على البيانات الحكومية يعاقب بالحبس لمدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ألفي دينار أردني أو ما يعادلها بالعملة المتداولة قانونا أو بكلتا العقوبتين، حيث ان المادة (4) من القرار بقانون رقم 10 لسنة 2018 بشأن

الجرائم الالكترونية وتعديلاته نصت على أنه:" 1. كل من دخل عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين"، 2. إذا ارتكب الفعل المذكور في الفقرة (1) من هذه المادة، على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين...".

ومن الجرائم الجنحوية الأخرى الواردة في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته المادة (5) والتي نصت على أنه:" كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين"، والتي عاقبت على أن كل من يعيق أو يعطل الوصول إلى حدمة أو الدخول إلى الأجهزة أو البرامج أو القيام بمصادرة البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الالكترونية أو إحدى وسائل تكنولوجيا المعلومات يعاقب بالحبس أو الغرامة لا تقل عن مئتي دينار أردني ولا تزيد على ألف دينار أردني. ونلاحظ هنا أن المشرع الفلسطيني لم يحدد مدة الحبس على هذه الجريمة من خلال نص المادة المذكور، لذلك يتوجب عليه مراعاة هذا النقص التشريعي.

كما أن المشرع الفلسطيني تناول الجرائم التي تعتبر جنحة من خلال ما جاء في المادة (7) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته، يعاقب كل من قام بالتقاط ما هو مرسل عن طريق الشبكة الالكترونية أو إحدى وسائل تكنولوجيا المعلومات أو قام بتسجيل ذلك أو اعترض أو تنصت عمدا دون وجه حق بالحبس مدة لا تقل عن سنة أو غرامة لا تقل عن ألف دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني أو بكلتا العقوبتين[1].

وكذلك نص في المادة (8) من نفس القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته بأن من يقوم عمدا بفك بيانات مشفرة في غير الأحوال المصرح بها قانونا يعاقب بالحبس أو بغرامة لا تقل

[1] المادة (7) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته على أنه:" كل من التقط ما هو مرسل عن طريق الشبكة أو إحدى وسائل تكنولوجيا المعلومات أو سجله أو اعترضه أو تنصت عمداً دون وجه حق، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

عن مئتي دينار أردني ولا تزيد على ألف دينار أردني، ومن قام باستعمال عناصر تشفير شخصية أو أداة إنشاء التوقيع الالكتروني المتعلقة بتوقيع شخص غيره بصفة غير مشروعة يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني أو بكلتا العقوبتين فالمادة (7) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته نصت على أنه:" كل من التقط ما هو مرسل عن طريق الشبكة أو إحدى وسائل تكنولوجيا المعلومات أو سجله أو اعترضه أو تنصت عمداً دون وجه حق، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين". ولهذا نستخلص مما سبق أن المشرع لم يكن موفقا في صياغة هذه المادة حيث إنه قام في الفقرة الأولى لم يقم بتحديد مدة الحبس، في حين قام بتحديدها في الفقرة الثانية من نفس المادة.

ومن الجرائم الجنحوية الأخرى التي وردت في هذا القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته جريمة من ينتفع دون وجه حق بخدمات الاتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو بكلتا العقوبتين، حيث إذا كان الانتفاع من هذه المادة بقصد الربح، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو بكلتا العقوبتين، فالمادة (9) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته نصت على أنه:" 1. كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. إذا كان الانتفاع في الفقرة (1) من هذه المادة بقصد الربح، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

واعتبر المشرع الفلسطيني أيضا أن من يقوم عمدا عبر استخدام الشبكة الالكترونية أو إحدى وسائل تكنولوجيا المعلومات بإنشاء أو نشر شهادة غير صحيحة أو قدم بيانات غير صحيحة عن هويته للجهات المختصة بموجب القوانين الخاصة بإصدار الشهادات بغرض طلب استصدار شهادة أو إلغائها أو إيقافها، يعاقب بالحبس والغرامة لا تقل عن مئتي دينار أردني، ولا تزيد على ألف دينار أردني، كما ورد في المادة (10) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته والتي نصت على أنه:" كل من قام عمداً، عبر استخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بإنشاء أو نشر

شهادة غير صحيحة أو قدم بيانات غير صحيحة عن هويته إلى الجهات المختصة بموجب القوانين الخاصة بإصدار الشهادات بغرض طلب استصدار شهادة أو إلغائها أو إيقافها، يعاقب بالحبس وبغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً".

ومن الجرائم الجنحوية الواردة في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته، جريمة تزوير مستند إلكتروني وذلك في المادة (12) منه والتي جاء فيها بأنه يعاقب كل من استخدم الشبكة الالكترونية أو إحدى وسائل تكنولوجيا المعلومات في الوصول دون وجه حق إلى أرقام أو بيانات وسيلة التعامل الالكترونية أو التلاعب فيها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ألف دينار أردني أو بكلتا العقوبتين، ويعاقب أيضا كل من زور أو استخدم أو سهل استخدام وسيلة تعامل الكترونية مزورة أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الالكتروني أو قبل وسيلة تعامل الكتروني غير سارية المفعول أو مسروقة ومع علمه بذلك يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة الأولى من نفس المادة (12) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته والتي نصت على أنه:" 1. كل من استخدم الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في الوصول، دون وجه حق، إلى أرقام أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. كل من زور وسيلة تعامل إلكترونية بأي وسيلة كانت، أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الإلكتروني، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة. 3. كل من استخدم أو سهل استخدام وسيلة تعامل إلكترونية مزورة مع علمه بذلك أو قبل وسيلة تعامل إلكترونية غير سارية أو مزورة أو مسروقة مع علمه بذلك، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة...".

وخلاصة القول، إن العقوبات التي قررها المشرع في هذه المواد لم تكن كافية، لاعتبار الجرائم الالكترونية جنح، ففي الحقيقة قد تصل الجرائم الالكترونية إلى درجة الجناية، فقد يؤدي نشر فايروس على شبكة الانترنت خسائر بالمليارات، أو قد يؤدي العبث في إحدى برامج المستشفيات إلى وفاة إحدى المرضى، أو قد يؤدي اختراق أحد الأنظمة الأمنية إلا إفشاء 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 (العفيفي، 2013، ص 78). وهذا ما سنقوم بالحديث عنه في الفرع الموالي.

الفرع الثاني: العقوبة على الشروع في الجنايات

ووفقاً للأصل العام فيمكن القول إن الجرائم التي اعتبرها القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية من قبيل الجنايات تخضع للقواعد العامة المقررة في قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية والتي تقرر مسائلة الجاني عن مجرد الشروع في ارتكاب جناية وما يعني جواز تصور الشروع في الجنايات الإلكترونية، بل والعقاب عليه.

تناول المشرع الفلسطيني بعض الجرائم التي تشكل جناية من خلال القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية، حيث ورد في المادة (11) منه أن من قام بتزوير سند من المستندات الالكترونية الرسمية للدولة أو الهيئات أو المؤسسات العامة المعترف به قانونا في نظام معلوماتي فإنه يعاقب بالسجن مدة لا تقل عن خمس سنوات وبغرامة لا تقل على ثلاث آلاف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، حيث أنه عاقب أيضا من خلال نفس المادة على أنه من قام بالتزوير أو التلاعب بتوقيه أو أداة أو أنظمة توقيع الكترونية رسمية سواء تم ذلك باصطناعه أو إتلافه أو تعييبه أو تعديله أو تحويره أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته ومعلوماته، يعاقب بالسجن مدة لا تقل عن خمس سنوات وغرامة لا تقل عن ثلاثة آلاف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، كم أن المشرع عاقب على نفس العقوبة المقررة التي قمنا بذكرها في هذه الفقرة على من أنشأ بيانات توقيع أو أداة نظام توقيع الكتروني رسمي أو للهيئات أو للمؤسسات العامة لا يحق له الحصول عليه مستخدما في ذلك بيانات أو معلومات خاطئة أو كاذبة، أو تواطئ مع غيره في إنشاء ذلك، فتناولت الفقرة الأولى والرابعة والسادسة من المادة (11) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته والتي نصت على أنه:" 1. كل من زور مستنداً إلكترونياً رسمياً من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفاً به قانوناً في نظام معلوماتي، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة لمتداولة قانوناً... 4. كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه أو إتلافه أو تعييبه أو تعديله أو تحويره، أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته أو معلوماته، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً... 6. كل من أنشأ بيانات توقيع أو أداة نظام توقيع إلكتروني رسمي أو للهيئات أو للمؤسسات العامة لا يحق له الحصول عليه، مستخدماً في ذلك معلومات أو بيانات كاذبة أو خاطئة، أو تواطأ مع غيره في إنشاء ذلك، يعاقب بالسجن مدة لا تقل عن

خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً...".

كما ذهب أيضا المشرع الفلسطيني من خلال المادة (17) من نفس القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته إلى أنه يعاقب كل من قام بإنشاء موقع أو تطبيق أو حساب الكتروني أو قام بنشر معلومات على الشبكة الالكترونية أو إحدى وسائلها، بقصد الاتجار في البشر أو الأعضاء البشرية أو تسهيل التعامل فيه يعاقب بالسجن مدة لا تزيد على سبعة سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، فنصت المادة (17) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته والتي نصت على أنه:" دون الإخلال بالأحكام الواردة في القرار بقانون بشأن تنظيم نقل وزراعة الأعضاء البشرية النافذ، يعاقب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار في البشر أو الأعضاء البشرية أو تسهيل التعامل فيه، بالسجن مدة لا تزيد على سبع سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً".

ومن المواد التي نص عليها المشرع في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية واعتبرها من الجرائم المتعلقة بالجنايات ما جاء في المادة (19) منه، والتي عاقب فيها من ينشأ أو ينشر موقعا على الشبكة الالكترونية بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية أو سهل التعامل فيها أو بيعها أو قام بشرحها أو قام أيضا بعرض طرق انتاجها بالسجن مدة لا تقل عن عشر سنوات أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني ولا تزيد على خمسة آلاف دينار أردني أو بكلتا العقوبتين، والتي نصت على أنه:" دون الإخلال بالأحكام الواردة في القرار بقانون بشأن مكافحة المخدرات والمؤثرات العقلية النافذ، يعاقب كل من أنشأ أو نشر موقعاً على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية، أو ما في حكمها، أو سهل التعامل فيها، أو بيع أو شرح أو عرض طرق إنتاج المواد المخدرة، بالسجن مدة لا تقل عن عشر سنوات، أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

قد نص القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على بعض التدابير الاحترازية، ومن هذه التدابير حجب الموقع الالكتروني المستخدم في الجريمة أو إغلاق المحل لمدة معينة أو مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون

أو الأموال المتحصلة منها، شريطة أن يتم إزالة تلك المخالفة على نفقة الفاعل، وهذا ما أكدت عليه المادة (50) من هذا القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته، والتي نصت بصريح العبارة على أنه:" دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون، وحقوق الغير حسن النية، على المحكمة أن تصدر قراراً يتضمن الآتي: 1. مدة إغلاق المحل، وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم بحسب الأحوال. 2. مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون أو الأموال المتحصلة منها، على أن تكون إزالة المخالفة على نفقة الفاعل".

نستنتج مما سبق، أن العقاب على الشروع في الجريمة الالكترونية وما قام به المشرع الفلسطيني بتقسيم الجرائم إلى جنح وجنايات، حيث نص من خلال القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية على الجرائم التي تشكل جنح والجرائم التي تشكل جنايات ووضع عقوبات على مرتكبي هذه الجرائم، ووضع أيضا تدابير احترازية لكنه خلط في نفس هذه المواد، حيث تحدث في آن واحد وفي نفس المادة عن الجريمة التي تكون جنحة والجريمة التي تكون جناية، حيث كان أولى له إفراد كل جريمة على حدة بمعنى أن يقوم بتخصيص فصل لكل من الجنايات وفصل آخر للجنح، كما قام في بعض الأحيان على عدم تحديد مدة الحبس في الجرائم التي تشكل جنحة، وهذا نقص تشريعي لا بد من تداركه.

المطلب الثاني: تطبيقات الشروع في الجرائم الإلكترونية

إن الجرائم بطبيعتها توجد بوجود الإنسان وتتطور بتطوره، وبما أن الإنسان في تطور مستمر بفعل ثورة تكنولوجيا المعلومات المتقدمة فإننا نجد العلماء والصالحون يحاولون الاستفادة منها، وبالمقابل نجد أن المجرمين أيضاً يحاولون الاستفادة من هذا التقدم التقني فأصبحت التكنولوجيا كلاً مباحاً للجميع الصالح والطالح، بل إن المجرمين كُثرُ، واستطاعوا اكتساب خبرات ومهارات أكثر في تعاملهم مع الانترنت وارتكابهم للجرائم الإلكترونية من خلال الأقمار الصناعية، ولم تعد جرائمهم تتوقف على إقليم دوله واحدة بعينها بل تجاوزت حدود الدولة، وهي جرائم مبتكرة ومستحدثة تمثل ضرباً من ضروب الذكاء الإجرامي، استعصى وصعب عملية إدراجها مع الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، مما أوجب تطوير وتحديث الأنظمة التشريعية الجنائية الوطنية بذكاء تشريعي مماثل للذكاء الإجرامي تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب تلك التقنيات وأبعادها الجديدة (عطايا، 2015، ص 360).

فالجرائم الالكترونية ليست نوعاً واحداً، بل تختلف تبعاً للأساس والمعيار الذي يستند إليه الفقهاء في تقسيمهم لهذه الجرائم، فيقسمها بعضهم إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته، وبعضهم

صنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يبني تقسيمه للجريمة على محل الاعتداء، ويتعدد الحق المعتدى عليه فيوزع جرائم الحاسوب وفق هذا التقسيم إلى جرائم تقع على الأموال باستخدام الحاسوب وتلك التي يقع على الحياة الخاصة (الطائي، 2007، ص 313).

وقد وصف بعض الباحثين تقسيمه للجريمة الإلكترونية تبعاً لمساسها بالأشخاص والأموال بأنه التقسيم الشائع في الدراسات والأبحاث الأمريكية كما أنه المعيار الذي يتبع في تقسيم الجرائم الإلكترونية في مشروعات القوانين النموذجية وأشار في هذا الصدد إلى مشروع نموذجي يسمى Model State Computer Crime Code وفي هذا النطاق القانوني النموذجي تقسم الجرائم الإلكترونية إلى (عرب، 2002، ص 10-13):

1. الجرائم الواقعة على الأشخاص.
2. الجرائم الواقعة على الأموال عدا السرقة.
3. جرائم السرقة والاحتيال.
4. جرائم التزوير والمقامرة والجرائم المنافية للآداب.
5. الجرائم الماسة بالمصالح الحكومية.

وترى الباحثة بأنه مهما اختلف التقسيم تبقى الجريمة المرتكبة واحدة، ولكن باختلاف مكان تصنيفها تبعاً لاجتهاد كل من الباحثين في تصنيفها، ولأن الجرائم لا يمكن حصرها وتعدادها، فهنا تعرض الباحثة عدد من الجرائم الإلكترونية وتأمل من الباحثين عرض ما يمكنهم من جرائم إلكترونية أخرى، بهدف زيادة المعرفة والمادة النظرية حول أكبر عدد من الجرائم الإلكترونية.

الفرع الأول: الشروع في جريمة الابتزاز والاحتيال الالكتروني

أصبحت جريمة الابتزاز الإلكترونية وهي أحد صور الجريمة الإلكترونية ظاهرة تخترق المجتمع وتهدد دعائمه، وتضرب في مقتل أهم أهداف أي مجتمع متحضر من تحقيق الأمن لأفراده، واحساسهم بالأمن والأمان في حياتهم، ولعل جوهر وسبب تجريم جريمة الابتزاز الالكتروني هو التهديد والابتزاز(عرب، 2002، ص 10-13)، والضغط الذي يمارس على الضحية، بتهديده بإفشاء وكشف سرٍ يعده معرة له وتعييب، مما يضطر معه إلى الانصياع والاذعان لرغبة الجاني، وتحقيق مطالبه المشروعة أو الغير مشروعة تحت اكراه من الخوف من الفضيحة، وهذا ما دعا إلى سن نظام يجرم السلوك الاجرامي الذي يمثل جريمة الابتزاز الإلكتروني، واهتم شراح القانون بتفسيره وشرحه، حتى أن خصوصية هذه الجريمة ألقت

بآثارها على طرق الإثبات فيها، حتى أن لدليل الجريمة الرقمي أسس وقواعد مختلفة للتعامل معه، في التحقيق والإثبات (عبد العزيز، 2018، ص 32).

وقام المشرع الفلسطيني بالنص على جريمة الابتزاز الإلكتروني بشكل واضح وصريح من خلال نص المادة (15) من القرار بقانون رقم (18) لسنة 2018 بشأن الجرائم الإلكترونية، بأن من يستعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل مشروع يعاقب بالحبس أو بغرامة فقد نصت المادة على ما يلي :" كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

بالنسبة للعقوبة المقررة لجريمة الابتزاز الالكترونية جرى عليها تعديل في القرار بقانون رقم (28) لسنة2020 بتعديل قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية لتصبح على النحو الأتي:"1. كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد على سنتين، وسنتين حبس مع وقف التنفيذ لمدة خمس سنوات تبدأ من انتهاء العقوبة الفعلية، وبغرامة لا تقل عن ألف دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً. 2. إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالحبس مدة لا تقل عن سنتين ولا تزيد على ثلاث سنوات، وثلاث سنوات حبس مع وقف التنفيذ لمدة خمس سنوات تبدأ من انتهاء العقوبة الفعلية، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا"، حيث إن الغموض الذي يحيط بجريمة الابتزاز الإلكتروني منذ بداية تنفيذ هذه الجريمة وحتى تمامها، مثلت تحدياً كبيراً على أبواب الضبط الجنائي والقضائي، حتى ان هذا الغموض قد صاحب تعريف الجريمة واختلفت التعريفات لهذه الجريمة، ولكن اتفق جميعها بان هناك خط أساسي واحد وهو استخدام التكنولوجيا والواقع الافتراضي كمسرح جريمة، وكذلك مرتكبها ذو المهارات والصفات المتمايزة عن المجرم التقليدي، وقد عرفت جريمة الابتزاز الإلكترونية بأنها إحدى صور الجرائم الإلكترونية (Cuber-crimes) وهي تتكون من مقطعين هما الجريمة (Crime)، والمقطع الآخر (Cyber)

وهي السيبرانية أو الفضاء، ويستخدم مصطلح الإلكترونية لوصف فكرة أن الجريمة تتم عن طريق التقنية الحديثة، أما الجريمة فهي تلك الأفعال المخالفة للقانون، وقد أصطلح على تعريف الجرائم الإلكترونية بأنها" المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي مباشر أو غير مباشر باستخدام شبكات الاتصال مثل الانترنت"، (البداينة، 2014، ص 3).

وتعتبر جريمة الابتزاز الإلكترونية هي نتاج الاستخدام السلبي لثورة التكنولوجيا التي لحقت بالعالم في القرن العشرين، وهي أثر من الآثار الغير مرغوبة لهذا التقدم العلمي المذهل، الذي جعل المجرم يختبئ خلف شاشة ما، ويمارس عملاً اجرامياً بالاعتداء على مصلحة يحميها النظام للضحية، وتتم الجريمة من خلال سلوك الجاني بطرق الضغط على المجني عليه المحتمل بالتهديد تارة، والوعيد تارة أخرى، وذلك بنشر معلومات أو صور أو تسجيلات لا يرغب المجني عليه في اظهارها على الملأ، فالابتزاز الإلكتروني أسلوب من أساليب الضغط والاكراه على المجني عليه، يعمل الجاني على ممارسته بهدف تحقيق مقاصده الاجرامية، وذلك للوصول إلى هدفه الذي قد يكون هدفاً مادياً أو معنوياً، وفي حال رفض الجاني من الاستجابة فإن الأخير سيقوم بنشر المعلومات السرية على الملأ، وهو ما يضع المجني عليه في مأزق إما بالرضوخ للجاني وتحقيق مطالبه، وإما بعد الرضوخ والتعرض للفضيحة (المطيري، 2015، ص 27).

وترى الباحثة بأن جريمة الابتزاز الإلكتروني تعتبر من الجرائم المستحدثة، ويطلق عليها في علم الجريمة الجرائم الناعمة، حيث تخلو من العنف، وهي من صور الجريمة الإلكترونية، والابتزاز الإلكتروني هو الوجهة المناظرة لجريمة الابتزاز التقليدية التي تنشأ وترتكب في عالم مادي، وفي مسرح جريمة تقليدي، حيث يعمل الجاني بترك بصمة أو نقطة دم، أما الابتزاز الإلكتروني فيتم في عالم افتراضي ملئ بالرموز والشفرات، ويزداد التحدي حين نجد العقبات والمطبات التي تواجه أجهزة التحقيق في عملية التحقيق فيها وفي التعامل مع الدليل الرقمي، وهذه الجريمة أصبحت تشكل هوساً لدى مستخدمي التكنولوجيا الرقمية الحديثة، وذلك بعد ثورة المعلومات والتكنولوجيا التي تفجرت بالقرن العشرين، فجريمة الابتزاز جريمة عابرة للحدود عندما تكون الالكترونية، فقد يكون المبتز في دولة بالعالم، ويقوم بابتزاز ضحية في أقصى العالم، وهذا ما تم ذكره في خصائص الجرائم الإلكترونية بالفصل الأول من الدراسة، وقد تعتبر جريمة الابتزاز جريمة قد تتسبب في حدوث جرائم أخرى بعدها، مثل (الزنا أو القتل أو جريمة عنف أو سرقة)، لذلك لا بد من ضرورة نشر الوعي المجتمعي بأخطار جريمة الابتزاز الإلكترونية.

وفيما يخص جرائم الاحتيال الالكتروني حيث تشبه جريمة الاحتيال العادية، فكلاهما يقومان على وسائل الغش والخداع، وكلاهما من جرائم الأموال هدف الجاني فيها الاستيلاء على أموال لست من ملكه أو حقه،

لهذا فكثير من الدول لم تشرع نصوصاً قانونية تجرم وتعاقب مرتكبي جريمة الاحتيال الالكتروني لان القضاء في أغلب الدول عمل على توسيع من تفسيره للنصوص القانونية الخاصة بجريمة الاحتيال العادية وجعلها تمتد لتشمل هذه الجريمة (الفيل، 2023، www.startimes.com)، وهذا ما اخذت به كافة الدول الأنجلوسكسونية كأستراليا وبريطانيا وكندا كما برزت اتفاقات على المستوى الإقليمي لعملية مواجهة جرائم الإنترنت مثل الاتفاقية الأوروبية حول الجريمة الافتراضية والقانون العربي الاسترشادية لجرائم المعلومات على المستوى العربي(الفيل، 2023، www.startimes.com)، هذا الذي أكدت عليه المادة (14) من قرار بقانون (10) لسنة 2018 بشأن الجرائم الالكترونية التي جاء فيها بأنه:" بأنه " كل من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

ومع ذلك فإنه يوجد اختلاف بين جريمة الاحتيال الالكتروني عن جريمة الاحتيال العادية كون أن الأولى تتم من خلال وسيلة الكترونية باستخدام شبكة المعلومات، في حين أن الثانية تكون وسيلة الخداع فيها بأي طريقة تهدف الى إيهام الغير وخادعه، فجريمة الاحتيال العادية أعم وأوسع من جريمة الاحتيال الإلكتروني، ثم أن محل جريمة الاحتيال العادية هو المال المنقول بينما محل جريمة الاحتيال الالكتروني يشمل المنافع والخدمات، وتقع جريمة الاحتيال العادية مباشرة بين الجاني والمجني عليه، ولكن يختلف ذلك في الاحتيال الالكتروني حيث تقع الجريمة بين أشخاص متواجدين في مناطق متفرقة ومتباعدة وفي دول مختلفة قاسمهم المشترك هو عملية استخدامهم لرسائل البريد الالكتروني عبر شبكة الانترنت (الفيل، 2023، www.startimes.com).

وترى الباحثة فيما تقدم بأنه بالرغم من وجود فوارق بين جريمة الاحتيال التقليدية وفق مفهومها الوارد في قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية وبين الجريمة الالكترونية، إلا أن هذه الفوارق تنحصر في الأسلوب الإجرامي فقط، فبدلاً من ان تكتمل الجريمة وتتم بأسلوب تقليدي أصبحت تواكب التطورات والتقدم التكنولوجي وتأخذ أسلوبا آخر، إلا أن ذلك لا يمنع تطبيق نص المادة (14) من قرار بقانون 10 لسنة 2018 بشأن الجرائم الالكترونية لعملية التصدي لجرائم الاحتيال التي تتم من خلال شبكات الانترنت بالوسائل الالكترونية.

الفرع الثاني: الشروع في جرائم السرقة الإلكترونية والتنصت الهاتفي

مع التطور التكنولوجي في هذا الفضاء الالكتروني فإن عملية السرقة الالكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك، وفيها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم عملية استخدامها والتصرف بالأموال من حساب الضحية أو إنشاء صفحة انترنت مماثلة جداً لموقع أحد البنوك الكبرى أو المؤسسات المالية الكبيرة والضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بهدف الحصول على بياناته المصرفية وسرقته، وبذلك أصبحت البنوك والمصارف مستهدفة من قبل محترفي الأجهزة الالكترونية الذين يعملون بالتلاعب في عملية كشوف حسابات العملاء ونقل الأرصدة من حساب لآخر، وقد تتم بصورة ثانية كإضافة بضعة أرقام أو أصفار إلى رقم ما في هذا الحساب الإشكاليات الموضوعية والإجرائية في النظام القانوني الفلسطيني في الجريمة الالكترونية.

بالرجوع إلى المادة (12) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية نجد بأن المشرع الفلسطيني نص على معاقبة كل من ارتكب بسوء نية إحدى صور الاعتداء على أمن المعلومات والبيانات والبرامج والأنظمة الإلكترونية، ومن ضمن هذه الصور: (الدخول غير المشروع والاستيلاء، أو الحجز، أو الاستعمال، أو النسخ، أو الحذف، أو التدمير)، حيث يرتبط هذا بجريمة السرقة الإلكترونية من حيث الاستيلاء غير المشروع على معلومات أو بيانات إلكترونية مملوكة للغير، حيث نصت على أنه:" 1. كل من استخدم الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في الوصول، دون وجه حق، إلى أرقام أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. كل من زور وسيلة تعامل إلكترونية بأي وسيلة كانت، أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الإلكتروني، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة. 3. كل من استخدم أو سهل استخدام وسيلة تعامل إلكترونية مزورة مع علمه بذلك أو قبل وسيلة تعامل إلكترونية غير سارية أو مزورة أو مسروقة مع علمه بذلك، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة. 4. إذا تم ارتكاب الأفعال المنصوص عليها في أحكام هذه المادة بقصد الحصول على أموال أو بيانات غيره أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 5. كل من استولى لنفسه أو لغيره على مال الغير بموجب الأحكام الواردة في هذه المادة، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف

دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.".

نستنتج أن الشروع في جرائم السرقة الإلكترونية وحسب ما ورد في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية وتحديداً نص المادة (49) منه، التي أكدت على يرتكب جريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم الواردة في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها ، وبهذا ينطبق هذا النص على الشروع في جريمة السرقة الإلكترونية، حيث تم النص عليها كجريمة في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته.

وفيما يخص العقوبة على جريمة السرقة الإلكترونية، فقد نص قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية في فلسطين على عقوبات محددة لمرتكب جريمة السرقة الإلكترونية، حيث نصت المادة (20) على أنه: "يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد عن ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين"، فهنا نص صريح على تجريم جريمة السرقة الإلكترونية وتحديد عقوبتها.

تعد سرية المكالمات والمحادثات الهاتفية من الحقوق الأساسية التي تواجه تحديات كبيرة في العصر الحديث، نظراً للتطور الهائل في تكنولوجيا الاتصالات والمعلومات، وتزايد قدرة أجهزة التنصت واختراق شبكات الاتصالات. مما أدى إلى تهديد خصوصية وسرية المكالمات بشكل متزايد، فقد عمل البعض باستعمال أجهزة التنصت التي تتيح باستراق السمع ورصد المكالمات الهاتفية الخاصة بين أطراف المكالمة دون رضا أو موافقة وإذن من أصحابها، وقد دفع ذلك المشرع إلى توفير الحماية الجنائية لهذا الحق الدستوري، نظراً لأهميته في صون خصوصية الأفراد وحرمة حياتهم الخاصة، التي تشكل جوهر الحريات الشخصية وركيزة مجتمع آمن ومستقر، وكما يعد الحق في حرمة الحياة الخاصة هو حق مصون ومن أهم الحقوق والذي يعتبر صلب الحقوق والحريات الشخصية الخاصة بالفرد والتي تشكل طمأنينة الإنسان الأمر الذي يؤدي بدوره لكون المجتمع مجتمعا سليما غير مهدد الأمان، وهذا الحق هو الإطار العام والفضاء القانوني الأمثل والواسع الذي يستطيع من خلاله الفرد أن يمارس حقه في حياته الخاصة دون الاطلاع على خصوصياته من قبل الآخرين، لذا ينبغي وضع ضوابط صارمة لحماية الحق في الخصوصية، ومعاقبة كل من ينتهكها أو يتجسس على المكالمات الهاتفية بدون موافقة أصحابها، حتى يشعر الأفراد بالطمأنينة والأمان في ممارسة حياتهم الخاصة (علي، 2023).

نصت المادة (41) من قرار بقانون (10) لسنة (2018) بشأن الجرائم الالكترونية بأنه "تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بالآتي: 1. اتخاذ التدابير الأمنية الوقائية اللازمة لحماية

أنظمتها المعلوماتية، ومواقعها الإلكترونية، وشبكاتها المعلوماتية، والبيانات والمعلومات الإلكترونية الخاصة بها. 2. الإسراع في إبلاغ الجهة المختصة عن أي جريمة منصوص عليها في هذا القرار بقانون، فور اكتشافها أو اكتشاف أي محاولة للالتقاط أو الاعتراض أو التنصت بشكل غير مشروع، وتزويد الجهة المختصة بجميع المعلومات لكشف الحقيقة. 3. الاحتفاظ ببيانات تكنولوجيا المعلومات، ومعلومات المشترك لمدة لا تقل عن (120) يوماً، وتزويد الجهة المختصة بتلك البيانات. 4. التعاون مع الجهة المختصة لتنفيذ اختصاصاتها."

نستخلص مما سبق هنا بأنه قد نص المشرع صراحة على تجريم فعل التنصت كونه فعلا خطرا بقوله "تنصت" وقد أحسن المشرع الفلسطيني بهذا النص ولم يشمله بجريمة أخرى كغيره من المشرعين، فإن الشروع في جريمة التنصت الهاتفي وارد، لأن المشرع نص على ذلك في المادة (49) من القرار بقانون رقم (10) اسنة 2018 بشأن الجرائم الإلكترونية والتي نصت على أنه:" يعد مرتكباً جريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها".

وجاءت المادة (34) من قرار بقانون (10) بشأن الجرائم الإلكترونية بالتأكيد على ذلك فقد نصت بأنه "1. لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جدية، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى النيابة العامة. 2. للنائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأي بيانات، بما فيها حركة الاتصالات، أو معلومات إلكترونية، أو بيانات مرور، أو معلومات المشترك التي يراها لازمة لمصلحة التحقيقات لغايات الفقرة (1) من هذه المادة، باستعمال الوسائل الفنية المناسبة، والاستعانة بذلك عند الاقتضاء بمزودي الخدمات، حسب نوع الخدمة التي يقدمها"، حيث هنا لم يترك المشرع الفلسطيني موضوع التسجيل والتنصت مباحا فقد عمل على تقيده بشروط وقيود صارمة منعا من انتهاك حرمة الدستور الذي أكد على خصوصية الأفراد.

خاتمة

نظراً لاتساع نطاق الجريمة الإلكترونية والتي أصبحت لا تقتصر على جريمة واحدة وإنما اتسعت إلى عدة جرائم، ومنها الشروع في الجريمة الإلكترونية، وعلى أساس أن القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الإلكترونية الحديثة، مما دفع المشرع الفلسطيني إلى استحداث قوانين خاصة لمواكبة هذا

النوع المستحدث من الجرائم، ومن أهم هذه القوانين هو القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته، والذي قمنا بالتركيز عليه في هذه الدراسة.

حيث نستخلص مما سبق بأن المشرع الفلسطيني تطرق لكل جريمة من الجرائم الالكترونية إلا أنه لم يتطرق للشروع في كل جريمة من هذه الجرائم على حدة، إلا أنه لم يضع مفهوما للشروع من خلال القرار بقانون بشكل دقيق وشامل، وكما أنه لم يخصص فصل خاص للجرائم التي تشكل جناية وفصل خاص للجرائم التي تشكل جنحة، حيث ذكر في بعض الأحيان في نفس المادة جرائم تشكل جناية وأخرى تشكل جنحة في آن واحد، كما نلاحظ أنه لم يحدد المشرع الفلسطيني مدة الحبس في الجريمة التي تشكل جنحة في بعض المواد.

وبناء على ما سبق، إن من أبرز النتائج والتوصيات التي توصلت إليها من خلال هذه الدراسة:

1- أن الشروع في الجريمة الالكترونية هو البدء في تنفيذ سلوك إجرامي مؤدي إلى ارتكاب جناية أو جنحة باستخدام إحدى وسائل تكنولوجيا المعلومات، ينتهي دون تحقق النتيجة الإجرامية، لأسباب لا دخل لإرادة الجاني فيها.
2- أن المشرع الفلسطيني نص بشكل صريح على أن كل من شرع بارتكاب جناية أو جنحة من الجرائم الوارد ذكرها في هذا القرار بقانون يعد مرتكبا جريمة الشروع ويعاقب بنص العقوبة المقررة لكل جريمة على حدة.
3- إن الاتفاقيات الدولية لم تتطرق إلى الشروع في الجريمة الالكترونية بشكل خاص، في حين أشارت إلى الجريمة الالكترونية بشكل عام.
4- تعد مرحلة التحقيق في الشروع بالجريمة الالكترونية عملية قانونية تتم بعد جمع الأدلة والاستدلالات المتعلقة بجرائم تتعلق بالتكنولوجيا المعلومات ويتطلب التحقيق فيها مهارات فنية وقانونية تختلف عن تحقيق الجرائم التقليدية.
5- أن مسرح الجريمة الالكترونية له طبيعة خاصة، حيث يصعب التعامل معها بالطريقة التقليدية للتعامل مع مسرح الجريمة التقليدية، وذلك لوصفها بأنها جرائم خفية وأقل عنفا في التنفيذ وعابرة للحدود وسرعة التطور بارتكابها.
6- إن العقوبات التي قررها المشرع في هذه المواد الوارد في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته لم تكن كافية، لاعتبار الجرائم الالكترونية جنح، ففي الحقيقة قد تصل الجرائم الالكترونية إلى درجة الجناية.

7- أن جريمة الابتزاز الإلكتروني تعتبر من الجرائم المستحدثة، ويطلق عليها في علم الجريمة الجرائم الناعمة، حيث تخلو من العنف، وهي من صور الجريمة الإلكترونية، والابتزاز الإلكتروني هو الوجهة المناظرة لجريمة الابتزاز التقليدية التي تنشأ وترتكب في عالم مادي.

8- إن المشرع الفلسطيني قد جرم الشروع في جريمة الابتزاز الالكتروني والسرقة الالكترونية والتنصت الهاتفي على سبيل المثال وليس عل سبيل الحصر، ونص على ذلك في المادة 49 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته.

9- إجراءات الاستدلال في الجريمة الالكترونية، تستلزم في الطالب المعرفة بنظام المعلومات ومعرفة طرق ارتكاب الجريمة فيه.

10- لرجال الضبط الجنائي مباشرة التحري في الشروع في الجريمة الالكترونية بالطرق التقليدية إن أمكن بالإضافة إلى الطرق المستحدثة الممكنة من خلال الشبكة الإلكترونية بناءً على أن وسائل التحري غير محصورة ويرافقها التطور في التقنية.

11- من خلال قراءة نصوص القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته بتمعن نجد بأنه لم يكن موفقا المشرع الفلسطيني في تناوله لأحكام الشروع في الجريمة الالكترونية وذلك يرجع إلى أنه لم يخصص فصلاً واحداً أو باباً لأحكام الشروع في الجريمة الالكترونية، بل اقتصر على تناوله من خلال مادتين فقط وهما (المادة 48 و49) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته.

التوصيات

1. سن قانون شامل للجرائم الإلكترونية، يتضمن تعريفًا دقيقًا للشروع في الجريمة الإلكترونية، وتحديد العقوبات المناسبة لكل نوع من أنواع الشروع.
2. تطوير آليات التحقيق في جرائم الشروع الإلكتروني بما يتناسب مع طبيعة هذه الجرائم.
3. تحديد شروط تجريم الشروع في الجرائم الإلكترونية مع مراعاة خطورة الجريمة ودرجة احتمال إتمامها.
4. تشديد العقوبات المقررة على الشروع في الجرائم الالكترونية الخطيرة.
5. ضرورة أن تتخذ المؤسسات مختلف الاجراءات لعمل الحماية الأمنية اللازمة والمقررة وفق المعايير العالمية لحماية بياناتها وأنظمتها الالكترونية من الاختراق، ووضع سياسة أمنية يتم مراجعتها بشكل دوري.

6. يجب العمل على ضرورة تحديث أساليب التحري والتحقيق وذلك في مجال الاجراءات من خلال تحديثها واستكمالها على نحو يكفل توفير سلطات ملاءمة لجهات التحري والتحقيق والادعاء وتتوازن على قدم المساواة مع كفالة احترام حقوق وحريات الأفراد.
7. ضرورة التركيز على مراجعة أحكام التفتيش في الجريمة الالكترونية والشروع فيها والعمل على تطويرها لتواكب طبيعة الجريمة الالكترونية وتنظيم ما يلزم من القواعد فيها.

قائمة المراجع والمصادر:

- **القران الكريم**
- **القوانين**
  - اتفاقية بودابست 2001 "اتفاقية الجرائم الإلكترونية –سايبر كرايم".
  - قانون الإجراءات الجزائية رقم 3 لسنة 2001، المنشور في جريدة الوقائع الفلسطينية، العدد 38/ 5 أيلول 2001.
  - القانون الأساسي المعدل لسنة 2003، منشور في جريدة الوقائع الفلسطينية، عدد ممتاز 2/ 19 مارس 2003.
  - قانون العقوبات الأردني رقم (16) لسنة 1960 النافذ في الضفة الغربية رقم 16 لسنة 1960 وتعديلاته.
  - قانون رقم (3) لسنة 1996 بشأن الاتصالات السلكية واللاسلكية، المنشور في جريدة الوقائع الفلسطينية، العدد 12/ 23 نيسان 1996.
  - قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية، دليل الوقائع الفلسطينية الثالث، العدد الممتاز 16/ 3 أيار 2018.
- **الكتب**
  - أبو خطوة، أحمد. (2000). التحقيق الجنائي في جرائم الكمبيوتر والإنترنت. منشأة المعارف، الإسكندرية.
  - البياتي، هلالي وآخرون. (1999). ندوة القانون والحاسب، سلسلة المائدة الحرة (رقم 37). بيت الحكمة، بغداد: مطبعة اليرموك.
  - حامد، هدى. (1992). جرائم الحاسب الإلكتروني في التشريع المقارن. دار النهضة العربية، القاهرة.
  - الحياني، صباح. (2020). جرائم الكمبيوتر والإنترنت. دار وائل للنشر، عمان.
  - ربضي، عيسى. (2009). القواعد الخاصة بالتوقيع الإلكتروني. ط1. دار الثقافة للنشر والتوزيع.
  - الرومي، محمد. (2003). جرائم الكمبيوتر والإنترنت. دار المطبوعات الجامعية، الإسكندرية.
  - الشاذلي، فتوح. (2005). جرائم الكمبيوتر والإنترنت. دار الفكر الجامعي، الإسكندرية.
  - الطائي، جعفر. (2007). جرائم تكنولوجيا المعلومات. ط1. دار البداية.

- طه، وليد. (بدون تاريخ). التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست. وزارة العدل، جمهورية مصر العربية.
- عباينة، محمود. (2005). جرائم الحاسوب وأبعادها الدولية. دار الثقافة، عمان.
- عبد الباقي، مصطفى. (2018). التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين، دراسة مقارنة. دراسات علوم الشريعة والقانون، 45(4، ملحق2).
- عبد الرحمن، أحمد. (2012). علم الإجرام والعقاب. ط1. دار الثقافة للنشر والتوزيع.
- عبد الكريم، عبد الله. (2011). جرائم المعلوماتية والإنترنت–الجرائم الإلكترونية. ط1. منشورات الحلبي الحقوقية، بيروت.
- عتيق، السيد. (2000). جرائم الإنترنت. دار النهضة العربية، القاهرة.
- عرب، يونس. (2006). تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية. هيئة تنظيم الاتصالات، مسقط، سلطنة عمان.
- الفاضل، محمد. (1976). المبادئ العامة في التشريع الجزائي. منشورات جامعة دمشق.
- القليوبي، سامح. (2010). جرائم الكمبيوتر والإنترنت. دار الفكر الجامعي، الإسكندرية.
- القهوجي، علي. (2016). شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي. مكتبة المستقبل، دبي.
- محمود، جابر. (2010). الجريمة المعلوماتية. دار الفكر الجامعي، الإسكندرية.
- ممدوح، إبراهيم خالد. (2008). أمن الجريمة الالكترونية. دار الجامعة، الإسكندرية.
- ممدوح، إبراهيم خالد. (2009). الجرائم المعلوماتية. ط1. دار الفكر الجامعي، الإسكندرية.
- المناعي، خالد. (2018). مكافحة جرائم الكمبيوتر والإنترنت – دراسة مقارنة. دار إثراء للنشر والتوزيع، عمان.
- المومني، نهلا عبد القادر. (2012). الجرائم المعلوماتية. ط1. دار الثقافة، عمان.
- نصار، غادة. (2017). الإرهاب والجريمة الإلكترونية. ط1. العربي للنشر والتوزيع، القاهرة.
- النوايسة، عبد الإله محمد. (2017). جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية. ط1. دار وائل للنشر والتوزيع، الأردن.
- نور، حسن. (2008). جرائم الكمبيوتر والإنترنت. دار الفكر الجامعي، الإسكندرية.
- الهيتي، محمد. (2006). جرائم الحاسوب. ط1. دار المناهج، عمان.

- **الرسائل العلمية**

- البداينة، ذياب. (2014). ورقة عمل عملية الجرائم الإلكترونية المفهوم والأسباب. الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان.
- بغدادي، أدهم. (2018). وسائل البحث والتحري عن الجرائم الإلكترونية (رسالة ماجستير غير منشورة). جامعة النجاح الوطنية، فلسطين.
- بن فردية، محمد. (2021). الشروع في الجريمة (سلسلة محاضرات، المحاضرة السادسة). جامعة الغردقة.
- حسام، محمد. (2002). الحماية الجنائية لتكنولوجيا الاتصالات: دراسة مقارنة. دار النهضة العربية.
- الدلالعة، سامر. (2005). الحماية القانونية الدولية والوطنية لتكنولوجيا المعلومات – برامج وأنظمة الحاسب الآلي: دراسة مقارنة (الجزء الأول). جامعة آل البيت.
- رضوان، خالد. (2017). الشروع في الجرائم الإلكترونية وفقًا لأحكام القانون الأردني: دراسة تحليلية مقارنة. المجلة الأردنية في القانون والعلوم السياسية، 9.(4)
- الصغير، يوسف. (2013). الجريمة المرتكبة عبر الانترنت (رسالة ماجستير غير منشورة). جامعة مولود معمري، الجزائر.
- عبد الفتاح، محمد. (2018). الوجيز في شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة. مكتبة الفلاح للنشر والتوزيع.
- عطايا، إبراهيم. (2015). الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية: دراسة تحليلية تطبيقية. (بدون ناشر).
- العفيفي، يوسف. (2013). الجرائم الالكترونية في التشريع الفلسطيني "دراسة تحليلية مقارنة" (رسالة ماجستير غير منشورة). الجامعة الإسلامية، غزة.
- المشجري، ليلى أحمد. (2014). الجرائم الاقتصادية عبر الشبكة العالمية للمعلومات (رسالة ماجستير منشورة). كلية الدراسات الإسلامية العربية، دبي.
- المطيري، سامي. (2015). المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي (رسالة ماجستير غير منشورة). جامعة نايف العربية للعلوم الأمنية، الرياض.
- المعايطة، عمر منصور. (2007). الطب الشرعي في خدمة الأمن والقضاء. جامعة نايف العربية للعلوم الأمنية، الرياض.

- **المجلات القانونية**

- حسن، شريهان. (2020). الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي. المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية(MECSJ) ، .(21)
- الحسيني، محمد. (2013، 12 فبراير). مختصون يطالبون بتشريع خاص للجرائم الإلكترونية في الكويت. هنا الكويت.
- سلامة، مأمون. (2010). الموسوعة الإلكترونية للقانون الجنائي (الجزء الثاني). دار الفكر والقانون، القاهرة.
- السمامعة، خالد. (2017). الشروع في الجرائم الإلكترونية وفقًا لأحكام القانون الأردني: دراسة تحليلية مقارنة. المجلة الأردنية في القانون والعلوم السياسية، 9.(4)
- صليحة، بن عودة. (2021). الشروع في الجرائم المعلوماتية بين الوقاية والردع. مجلة دفاتر الحقوق والعلوم السياسية، 1.(2)
- عبد العزيز، داليا. (2018). المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي: دراسة مقارنة. مجلة جيل الأبحاث القانونية المعمقة، .(25)
- عرب، يونس. (2002). إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات. ورقة عمل مقدمة إلى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي.
- عرب، يونس. (2006). تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية. ورشة عمل، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان.

- **المواقع الإلكترونية**

- أبو علي، محمد. (2022). جريمة التنصت الإلكتروني. مجلة الباحث، (46). تم الاسترجاع في 22 سبتمبر 2023، من https://www.allbahit.com/2022/09/46_66.html .
- أكاديمية شرطة دبي، مركز البحوث والدراسات. (2003). ظاهرة الإجرام الإلكتروني ومخاطرها. تم الاسترجاع في 1 أكتوبر 2023، من http://th3professional.com .
- جامعة النجاح الوطنية. (بدون تاريخ). الإشكاليات الموضوعية والإجرائية في النظام القانوني الفلسطيني في الجريمة الالكترونية. تم الاسترجاع في 25 أبريل 2024، من https://www.najah.edu/ar/ .

- الفيل، علي. (بدون تاريخ). الجرائم الإلكترونية. تم الاسترجاع في 17 سبتمبر 2023، من www.startimes.com.
- مكتب الأمم المتحدة المعني بالمخدرات والجريمة. (بدون تاريخ). التعاون الدولي على مكافحة الجريمة الالكترونية (الوحدة التعليمية 7). تم الاسترجاع في 19 أبريل 2024، من https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html.
- Drewer, D., & Ellermann, J. (2012). Europol's data protection framework as an asset in the fight against cybercrime. ERA. تم الاسترجاع في 1 أكتوبر 2023، من http://link.springer.com/article/10.1007/s12027-012-0268-6 .
- Los Angeles Times. (2016). The conflict between Apple and the FBI. تم الاسترجاع في 1 أكتوبر 2023، من http://www.latimes.com/business/la-fi-mh-the-conflict-between-apple-and-the-fbi-20160219-column.html .
- **المراجع الأجنبية:**
  - Clough, J. Principles of cybercrime. **Cambridge University Press**. (2010).
  - Doe, J. (2020). The rise of cybercrime: Challenges and solutions. **Journal of Cybersecurity**, 12(3), 61-45.
  - Gercke, M. **Understanding cybercrime: Phenomena**, challenges, and legal response. ITU. (2012).
  - Johnson, M. (2018). The impact of online pornography on minors: Legal perspectives. **Journal of Internet Law**, 6(4), 78-95.
  - La Cybersurveillance: " **Est al surveillance des reseaux de telecommunication** ", Voir Maximilien doste Amegee, op-cit, 2002. p50.
  - Smith, A. (2019). Online censorship and its legal implications. **International Journal of Law and Technology**, 8(2), 112-130

فهرس المحتويات