عمادة الدراسات العليا

جامعة القدس

إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً

ليالي كايد حسين دودين

رسالة ماجستير

القدس – فلسطين

1446هـ/2025م

إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً

إعداد:

ليالي كايد حسين دودين

بكالوريوس علم الجريمة والقانون – جامعة الاستقلال/ فلسطين

المشرف: د. جهاد الكسواني

قدمت هذه الرسالة استكمالاً لمتطلبات درجة الماجستير في علم الجريمة من عمادة الدراسات العليا/ كليّة الآداب/ جامعة القدس

1446 هـ – 2025 م

جامعة القدس
عمادة الدراسات العليا
برنامج علم الجريمة

إجازة الرسالة

إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً

اسم الطالبة: ليالي كايد حسين دودين
الرقم الجامعي: 21911874

إشراف: الدكتور جهاد الكسواني

نوقشت هذه الرسالة وأجيزت بتاريخ: 2025/01/05م من أعضاء لجنة المناقشة المدرجة أسماؤهم وتواقيعهم:

1- رئيس لجنة المناقشة: د. جهاد الكسواني التوقيع: .....

2- ممتحناً داخلياً: د. صالح البرغوثي التوقيع: .....

3- ممتحناً خارجياً: د. عصام الأطرش التوقيع: .....

القدس – فلسطين
1446هـ /2025م

إهداء

إلى من تعجز الكلمات عن وصفهما، وتعجز الحروف عن ذكر فضلهما

إلى والدتي ووالدي

إلى من أشدّ بهم أزري إخوتي

ضياء ومحمد

إلى مهجات قلبي أخواتي

لمياء، لبنى، لميس، هيا، سجى

إلى رفيقات الدرب

داليا، آنا، آلاء، وداد ونورا

إليكم جميعاً أهدي هذا العمل المتواضع

الباحثة/ ليالي دودين

إقرار:

أقر أنا معدّ الرسالة أنها قدمت لجامعة القدس لنيل درجة الماجستير، وإنها نتيجة أبحاثي الخاصة، باستثناء ما تمّت الإشارة له حيثما ورد، وأن هذه الرسالة، أو أيّ جزء منها، لم يقدم لنيل أيّة درجة علمية عُليا لأي جامعة أو معهد أخر.

التوقيع:.....

الاسم: ليالي كايد حسين دودين.

التاريخ: 5 / 1 /2025م

شكر وتقدير

الحمد لله حمدًا يليق بجلاله وعظمته، أحمده وأشكره سبحانه وتعالى الذي منَّ علي بتوفيقه لإتمام هذا الجهد المتواضع وكلَّله بالنجاح، وصلِّ اللهم على خاتم النبيين، صلاة تقضي لنا بها الحاجات، وترفعنا بها أعلى الدرجات، وتُبَلِّغنا بها أقصى الغايات، أما بعد:

قال جل وعلا: ﴿وَمَنْ شَكَرَ فَإِنَّمَا يَشْكُرُ لِنَفْسِهِ ﴾[النمل: 40] يشرفني أن أتقدم بجزيل الشكر والعرفان لجامعتي الموقرة، صانعة العلماء وعمادة الدراسات العليا وكليتي العامرة كلية الآداب، وأستاذي ومشرفي الفاضل **الدكتور/ جهاد الكسواني** الذي شرفني بقبول الإشراف على هذه الرسالة وما بذله من جهد ومتابعة وإشراف طوال فترة إعداد هذه الرسالة، حتى خرجت إلى النور.

كما أتوجه بشكري الجزيل إلى عضوي لجنة المناقشة، كل من:

الدكتور الفاضل/ صالح البرغوثي (مناقشاً داخلياً)

الدكتور الفاضل/ عصام الأطرش (مناقشاً خارجياً)

وذلك لتفضلهما بالموافقة على مناقشة هذه الرسالة، وعلى ملاحظاتهما في إثرائها بالتوجيهات السديدة، والإرشادات الصائبة، فبارك الله فيهما.

والشكر موصول إلى كل من مد يد العون وكان له الأثر الطيب في إثراء وإنجاز هذه الرسالة، وكل من أنار لي الطريق ودعمني في مسيرتي العلمية بكلمة أو دعوة خير في ظهر الغيب.

وختامًا أتمنى من الله أن ينال جهدي القبول والرضا، فحسبي أنني اجتهدت، ولكل مجتهدٍ نصيب، والكمال لله وحده، فإن وُفِّقتُ فمن الله، وإن قَصَّرتُ، فمن نفسي ومن الشيطان، والحمد لله رب العالمين.

الباحثة/ ليالي دودين

الملخص

تهدف هذه الدراسة إلى التعرف على إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً، وذلك باستخدام المنهج الوصفي الكمي من خلال استخدام أداة الاستبانة التي صممت للحصول على البيانات من العاملين في هيئات العدالة الجنائية (القضاء، النيابة العامة، الشرطة) في محافظة أريحا، ويتكون مجتمع الدراسة من جميع العاملين في هيئات العدالة الجنائية والبالغ عددهم (363) موظف/ ة تم اختيار عينة عشوائية بسيطة منهم مكونة من (188) من العاملين، تم توزيع استبانة الدراسة عليهم.

توصلت الدراسة إلى مجموعة من النتائج لعل من أهمها: أن الإجراءات المتبعة من قبل هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة (86.4%) للشرطة، و(95%) للنيابة العامة و(93.4%) للقضاء، كما وأشارت النتائج إلى أن أهم الصعوبات التي تواجه هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية تتمثل في قلة وعي المجتمع بالجريمة الإلكترونية، إذ حصلت على نسبة (85.6%)، وأن أهم آليات الوقاية المتبعة من قبل هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية تتمثل في تنمية الثقة بين المواطنين والعاملين في هيئات العدالة الجنائية، إذ حصلت على نسبة (80.8%)، كما وبينت النتائج عدم وجود فروق ذات دلالة إحصائية في درجة الصعوبات التي تواجه هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تعزى لمتغير الجنس، في حين توجد فروق ذات دلالة إحصائية في درجة الصعوبات التي تواجه هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تعزى لمتغيرات (العمر، المستوى التعليمي، الخبرة العملية)، إلى جانب عدم وجود فروق ذات دلالة إحصائية في مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تعزى لمتغيرات (الجنس، العمر، الخبرة العملية)، في حين توجد فروق ذات دلالة إحصائية في مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي، وبناء على هذه النتائج أوصت الدراسة بمجموعة من التوصيات منها: (توعية المواطنين بماهية الجرائم الإلكترونية، وأهمية الإبلاغ عنها في حال وقوعهم ضحايا لها، وتدريب العاملين في هيئات العدالة الجنائية مع كل ما هو مستحدث في الجرائم الإلكترونية خاصة في ظل وجود ما يسمى بتقنية الذكاء الاصطناعي في الوقت الراهن، مع ضرورة مواكبة المشرع الفلسطيني للتطورات السريعة في وسائل الاتصالات وتكنولوجيا المعلومات والجرائم الإلكترونية من حيث مواكبته للجرائم التي تستحدث في هذا المجال والأساليب الجديدة في ارتكابها).

الكلمات المفتاحية: هيئات العدالة الجنائية، القضاء، النيابة العامة، الشرطة، الجرائم الإلكترونية.

Procedures of Criminal Justice Bodies in Addressing Cybercrimes: Challenges and Prevention Mechanisms – A Case Study of Jericho Governorate.

Prepared by: layali kayed hussan dodeen.

Supervisor: DR. Jihad Al-Kiswani

Abstract

This study aims to explore the procedures of criminal justice bodies in addressing cybercrimes, examining challenges and prevention mechanisms, using Jericho Governorate as a case study. A quantitative descriptive methodology was adopted, utilizing a questionnaire designed to collect data from employees of criminal justice entities (judiciary, public prosecution, and police) in Jericho. The study population included all employees of these entities, totaling (363) individuals, from which a Simple random sample of (188) staff, and the questionnaire was distributed among them.

The study yielded several key findings, including:

- Criminal justice entities adopt highly effective procedures in addressing cybercrimes, with 86.4% effectiveness for police, 95% for the public prosecution, and 93.4% for the judiciary.
- The primary challenge facing criminal justice bodies is the lack of societal awareness of cybercrimes, which scored 85.6%.
- The most effective prevention mechanism involves fostering trust between citizens and criminal justice entities, achieving an 80.8% rating.

The results also revealed:

- No statistically significant differences in the challenges faced by criminal justice entities in combating cybercrimes based on gender. However, significant differences were noted based on age, educational level, and professional experience.
- No statistically significant differences in the level of prevention mechanisms based on gender, age, or professional experience. However, differences were observed based on educational level.

Based on these findings, the study recommends:

- Raising public awareness about cybercrimes and the importance of reporting them.
- Training criminal justice personnel on emerging cybercrime issues, especially with advancements in artificial intelligence.
- Ensuring Palestinian legislation keeps pace with rapid developments in communication technology and cybercrimes, addressing emerging crimes and new methods of perpetration.

Keywords: Criminal justice bodies, judiciary, public prosecution, police, cybercrimes.

الفصل الأول

الإطار العام للدراسة

1.1 مقدمة

شهد النصف الثاني من القرن العشرين ثورة تكنولوجية هائلة في مجال التقنية والاتصالات والصناعات، فأصبح العالم يعتمد على التكنولوجيا بصورة كبيرة سواء على المستوى الرسمي أو الشخصي، خاصة في مجال تجميع المعلومات وتخزينها ومعالجتها ليتم نقلها وتبادلها بين الأفراد والمؤسسات المختلفة داخل الدولة أو خارجها، فأصبح اعتماد إدارات الدولة ومرافقها في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية باعتبار أن هذه الأخيرة تقدم خدمة بجودة عالية وبتكلفة أقل وبسرعة أكثر وبدقة متناهية، وبذلك يقاس مدى تقدم أي دولة بمدى تطور التقنيات التي تمتلكها (التميمي، 2019).

وبالرغم من الدور الإيجابي الذي تحققه التكنولوجيا في كافة مجالات الحياة، وتقديمها إيجابيات وفوائد عظيمة لا يمكن حصرها، إلا أنه قد رافقها ظهور نوع جديد من الجرائم القائمة على الاستغلال غير المشروع لهذه التكنولوجيا والتي اصطلح على تسميتها بالجرائم الإلكترونية التي بدورها ساهمت في ظهور نسل جديد من المجرمين المختصين بتقنية المعلومات وتكنولوجيا الاتصالات التي أتاحت لهم فرصة ارتكاب الجرائم بيسر وخديعة بل واستخدمها في إخفاء جرائمه للإفلات من العقاب (الشهري، 2011).

وتكمن خطورة هذه الجرائم في أنها تؤدي إلى إضعاف وتقويض المجتمع، ذلك أن القطاعات الرئيسية في أغلب المجتمعات أصبحت تعتمد على التقنيات الرقمية بكافة أشكالها وإن أي تهديد لها إنما يشكل تهديد لأنظمة الدولة ومؤسساتها، فما كان من الدول إلا أن تكرس كافة جهودها لمحاربة هذه الجرائم، والتعاون في سبيل السيطرة عليها ومكافحتها كونها عابرة للحدود وصعبة الإثبات إلى جانب الأضرار الفادحة التي تخلفها (هلال، 2008).

وعلى الصعيد الفلسطيني فقد عانى المجتمع ونظام العدالة الجنائية بكافة مكوناته لسنوات عديدة من إشكاليات تتعلق بمواجهة الجرائم الإلكترونية، فمنها ما يتعلق بالجوانب القانونية، ومنها ما يتعلق بواقع الجرائم الإلكترونية وملاحقتها، كونها تعتبر حالة مختلفة عن باقي الدول، ذلك بسبب قيود الاحتلال الإسرائيلي الذي يسيطر على الأرض والسماء والفضاء الإلكتروني سيطرة تامة، ما يشكل تحدياً خاصاً عند ملاحقة هذه الجرائم، الذي يفرض بدوره ضرورة دراسة إجراءات هيئات العدالة الجنائية الفلسطينية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية.

وقد أجريت العديد من الدارسات التي تناولت موضوع الجرائم الإلكترونية من عدة جوانب فهناك دراسة (العتيبي، 2016) التي ترى أن دور التحريات في الكشف عن الجرائم المعلوماتية ضعيف، ووجود صعوبات تواجه التحريات والبحث الجنائي عند الكشف عن الجرائم المعلوماتية. وكذلك دراسة (عموري، 2018) التي ترى أن التفتيش في الجرائم الإلكترونية من أدق وأخطر إجراءات التحقيق، والتفتيش في تلك الجرائم بحاجة إلى نظام إجرائي يراعي خصوصيتها، وبحاجة إلى أشخاص مؤهلين ومدربين تدريباً قانونياً وفنياً للتعامل مع وسائل تكنولوجيا المعلومات. أما دراسة (عصام ومحمد، 2019) فهي ترى أن أهم معوقات مكافحة الجرائم مرتبطة بآليات التحقيق الجنائي.

حيث أن هذه الدراسات قد تناولت دراسة بعض الجوانب المتعلقة بالآليات المتبعة في مواجهة الجرائم الإلكترونية والمعوقات التي تواجهها، ومن هنا وبناء على ما سبق من معلومات ومن خلال الدراسة الحالية سوف نختبر إجراءات هيئات العدالة الجنائية في محافظة أريحا في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية ممثلة في القضاة وأعضاء النيابة العامة والشرطة كجهات ضبط فضائي متخصصة في ملاحقة مرتكبي الجرائم الإلكترونية.

2.1 مشكلة الدراسة

يشهد العالم اليوم إجماعاً فيما يخص انتشار ونمو الجرائم الإلكترونية في ظل التطور التكنولوجي الكبير على مستوى الأجهزة وتقنيات الاتصال، بالأخص مع نمو وتوسع شبكة الانترنت في كل بقاع العالم، فالبرغم من جميع الإجراءات والآليات المتبعة دولياً ومحلياً إلا أنها في تزايد مستمر من عام

إلى آخر، حيث بلغت نسبة الجرائم الإلكترونية حسب ما ورد في إحصائيات الشرطة الفلسطينية للأعوام ما بين (2015– 2023) على النحو الآتي: عام (2015) بلغت (502) جريمة، وفي عام (2016) بلغت (1327) جريمة، وعام (2017) بلغت (2025) جريمة، وعام (2018) بلغت (2568) جريمة، كما وبلغت في عام (2019) (2420) جريمة، وعام (2020) بلغت (2720) جريمة وعام (2021) بلغت (2589) جريمة وعام (2022) بلغت (3067) جريمة وعام (2023) بلغت (1228) جريمة (جهاز الشرطة الفلسطينية، 2023). ومن خلال الإحصائيات السابقة نرى أن الجريمة الإلكترونية في المجتمع الفلسطيني تضاعفت بشكل كبير خاصة في ظل وجود قانون مكافحة الجرائم الإلكترونية لعام (2018)، الأمر الذي يوجه أنظارنا للبحث عن إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية والصعوبات التي تواجهها وآليات الوقاية المتبعة من قبلها.

هذا وتتسم الجرائم الإلكترونية بالحداثة وسرعة التنفيذ وسهولة الإخفاء ودقة محو آثارها، فقد صارت تشكل أهم جرائم هذا العصر وأعقدها، فطبيعة هذه الجرائم تستدعي سرعة التأهب نحو نقلة علمية وتقنية عملية دائبة تحققها بالذات مجالات الضابطة القضائية والنيابة والقضاء لمكافحة هذه الجرائم، فبسبب تفاقمها وتعدد أنواعها وازدياد حجم خسائرها وأضرارها أصبحت مهدداً حقيقياً لأمن المعلومات في كافة المجالات العامة والحيوية بالقطاع العام والخاص والأفراد، فيجب علينا أن ندرسها بشكل معمق كونها عابرة للحدود، فذلك يجعل دراستها ومواجهتها في المجتمع الفلسطيني أو غيره من المجتمعات أمراً لا ينفصل عن التعرف بشكل عام على ماهيتها ومفهومها وأسبابها وتطوراتها وآثارها والجهود المبذولة لمكافحتها لمعرفة ما تأثير الاستراتيجيات الفلسطينية للقضاء عليها أو على الأقل الحد من آثارها، فمن هنا تكمن مشكلة الدراسة في الإجابة على السؤال الرئيس الآتي: ما هي إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية والصعوبات التي تواجهها وآليات الوقاية المتبعة من قبلها للحد منها في محافظة أريحا؟

3.1 أهميّة الدراسة

تكتسب الدراسة أهميتها من أهمية التحديات الأمنية والتقنية والقانونية المصاحبة لاستخدامات تقنية المعلومات والحاسب الآلي والإنترنت ومن خطورة الوضع الراهن للجريمة الإلكترونية، فالتطور الحاصل في تكنولوجيا الإعلام والاتصال بقدر ما أحدث من آثار إيجابية ومن تغيير لنمط الحياة في جميع المجالات، بقدر ما كان لها الأثر السلبي بسبب استغلال هذه الوسائل في ارتكاب الجرائم وصعوبة الوصول إلى مرتكبيها. وتتمثل أهمية الدراسة من الناحية النظريّة والعملية على النحو الآتي:

1.3.1 الأهمية النظريّة:

- تنبع أهمية الدراسة من أهمية الموضوع الذي تتناوله وهو الجرائم الإلكترونية فهي من الجرائم المستحدثة، وهي متعددة الأنواع ومتطورة بشكل مستمر فهي بحاجة إلى آليات مكافحة متقدمة بشكل يواكب تطورها، حيث أن معرفة الإجراءات المتبعة لمواجهتها ضروري لخطورتها كون الأضرار المترتبة على وقوعها فادحة وفي بعض الأحيان لا يمكن تجاوزها.
- التطور التكنولوجي المستمر يؤدي إلى تطور الآلات بالتالي تطور الجريمة فالجرائم الإلكترونية تتنوع وتتطور بشكل مستمر، هذا يجعلنا بحاجة ماسة إلى تطوير إجراءات مكافحتها واختبار فعالية هذه الإجراءات فهناك جدل فقهي دائم حول مدى فعالية هذه الإجراءات والحاجة إلى تطويرها لمواكبة هذه الجرائم.
- تزويد المكتبات الفلسطينية بدراسة توضح إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً.
- استفادة الباحثين منها من خلال اطلاعهم على نتائج الدراسة مما يمكنهم من البناء عليها في أبحاث أخرى ذات علاقة بالموضوع.

2.3.1 الأهمية العملية:

تختلف الأهمية العملية التطبيقية حسب الجهة التي سوف تستفيد من نتائج هذه الدراسة على النحو الآتي:

- المشرعون: الاستفادة منها من خلال معرفة الإجراءات التي تتبعها هيئات العدالة الجنائية في مواجهة الجرائم والإلكترونية، وهل هذه الإجراءات ساعدت في القضاء على هذا النوع من الجرائم أو التخفيف منه على الأقل، فقد تساعدهم تلك النتائج بوضع سياسات وقوانين وتشريعات مناسبة لمواجهة هذه الجريمة والحد من آثارها كونها تتطور وتتعدد أنواعها بشكل مستمر.
- القضاء الجالس والنيابة العامة: الاستفادة من نتائج الدراسة من خلال معرفة واقع الجريمة الإلكترونية، والإجراءات المتبعة لمواجهتها، وضرورة تطوير هذه الإجراءات بما يسهل آلية القبض على مرتكبيها ومحاكمتهم محاكمة عادلة، وإيقاع العقوبة الرادعة عليهم.
- الشرطة: كونهم خط الدفاع الأول لمواجهة هذه الجرائم، فمن خلال النتائج التي ستتوصل إليها الدراسة سيتضح لهم ما أهم الإجراءات التي يجب أن يتبعوها في ميدان عملهم للتصدي للجريمة الإلكترونية وضرورة العمل على تطوير الوحدة المتخصصة بمكافحة الجرائم الإلكترونية وتدريب

العاملين فيها، والتأكيد على ضرورة إشراك مؤسسات المجتمع المدني من أجل مواجهة هذه الجرائم.

4.1 أهداف الدراسة

تكمن أهداف الدراسة في هدف رئيس وأهداف أخرى فرعية، وأما الهدف الرئيس فيتمثل في التعرف على إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية، في حين تتمثل الأهداف الفرعية في التعرف إلى:

- الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية.
- الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية.
- الإجراءات المتبعة من قبل القضاء في مواجهة الجرائم الإلكترونية.
- الصعوبات التي تواجه هيئات العدالة الجنائية في مكافحة الجرائم الإلكترونية.
- آليات الوقاية المُتبعة من قبل هئيات العدالة الجنائية للحد من الجرائم الإلكترونية.
- تأثير خصائص المبحوثين الديموغرافية على إجاباتهم حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية ومستوى آليات الوقاية المتبعة من قبلها للحد من الجرائم الإلكترونية في محافظة أريحا من وجهة نظر العاملين.

5.1 أسئلة الدراسة وفرضياتها

تكمن أسئلة الدراسة في سؤال رئيس يتمثل في الإجابة عن: ما هي إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية والصعوبات التي تواجهها وآليات الوقاية التي تتبعها للحد منها في محافظة أريحا؟، ينبثق عن السؤال الرئيس أسئلة فرعي أخرى تتمثل في الاجابة عن:

- ما هي الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية؟
- ما هي الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية؟
- ما هي الإجراءات المتبعة من قبل القضاء في مواجهة الجرائم الإلكترونية؟

- ما الصعوبات التي تواجه هيئات العدالة الجنائية في مكافحة الجرائم الإلكترونية؟
- ما أهم آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية للحد من الجرائم الإلكترونية؟
- ما تأثير خصائص المبحوثين الديموغرافية على إجاباتهم حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تعزى لمتغيرات (الجنس، العمر، المستوى التعليمي، الخبرة العملية)؟
- ما تأثير خصائص المبحوثين الديموغرافية على إجاباتهم حول مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تعزى لمتغيرات (الجنس، العمر، المستوى التعليمي، الخبرة العملية)؟

وأمّا فيما يخص فرضيات الدراسة:

سعت الدراسة إلى التأكد من صحة الفرضيات الآتية :

- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات عينة الدراسة حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية ومستوى آليات الوقاية المتبعة من قبلها للحد من الجرائم الإلكترونية تعزى لمتغير (النوع الاجتماعي).
- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات عينة الدراسة حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية ومستوى آليات الوقاية المتبعة من قبلها للحد من الجرائم الإلكترونية تعزى لمتغيرات (العمر).
- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات عينة الدراسة حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية ومستوى آليات الوقاية المتبعة من قبلها للحد من الجرائم الإلكترونية تعزى لمتغيرات (المستوى التعليمي).
- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات عينة الدراسة حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية ومستوى آليات الوقاية المتبعة من قبلها للحد من الجرائم الإلكترونية تعزى لمتغيرات (الخبرة العملية).

6.1 حدود الدراسة

تكمن حدود الدراسة في:

- **الحدود المكانية:** سوف تقتصر هذه الدّراسة في تطبيقها على هيئات العدالة الجنائية بمفهومها الضيق (الشرطة، النيابة العامة، القضاء) في محافظة أريحا.
- **الحدود الزمانية:** تمت الدراسة في الفترة الواقعة بين الفصل الدراسي الأول من العام الأكاديمي (2022–2023) وحتى نهاية الفصل الدراسي الأول من العام الأكاديمي (2024– 2025).
- **الحدود البشرية:** سوف تقتصر هذه الدّراسة في تطبيقها على جميع العاملين في الشرطة والبالغ عددهم (353) موظف/ة والعاملين في النيابة العامة والبالغ عددهم(5) موظفين والعاملين في المحاكم والبالغ عددهم (5) موظفين في محافظة أريحا حسب إحصائيات (الجهاز المركزي للإحصاء الفلسطيني، 2023).
- **الحدود الموضوعية:** تتمثل في موضوع الدراسة الذي يتمحور حول "إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً".

الفصل الثاني

الإطار النظري والدراسات السابقة وذات الصلة

يتمثل هذا الفصل بالإطار النظري للدراسة، حيث سيتم الحديث عن الموضوعات ذات العلاقة بهيئات العدالة الجنائية فتعرف العدالة الجنائية وفقاً لما ورد في (قلالوة، 2020: 27) بأنها:" مجموعة من النظم والتشريعات الخاصة بالشأن الجنائي ومختلف الأجهزة والمؤسسات الرسمية التي تعمل بالحقل الجنائي لرسم السياسة الجنائية والتخطيط الجنائي ووضع الاستراتيجيات الهادفة إلى مكافحة الجريمة وفقاً للمعايير والقواعد الدولية ذات الصلة، ابتداء من تغيير البيئة الخصبةثم بالمحاكمة مروراً بالإصلاح والتأهيل داخل السجون وإنتهاء بالرعاية اللاحقة بهدف خلق مجتمع آمن من الجريمة قدر الإمكان". حيث يتكون نظام العدالة الجنائية من هيئات مختلفة فمنها ما ينتمي للسلطة التشريعية (المجلس التشريعي) ومنها ما يتصل بالسلطة القضائية (المحاكم، النيابة) والسلطة التنفيذية (الشرطة، مراكز الاصلاح والتأهيل) إلى جانب المؤسسات المدنية الناشطة في القضاء (كنقابة المحامين، ومنظمات حقوق الإنسان) وغيرها من المؤسسات التي تعمل معاً على حدٍ سواء تحت سيادة القانون باعتبارها الوسيلة الرئيسية للمحافظة على سيادة القانون في المجتمع (هلال، 2003: 13).

وفي موضوع دراستنا الحالي سوف نتناول هيئات العدالة الجنائية بمفهومها الضيق (الشرطة، النيابة العامة، القضاء) ودورها في مواجهة الجريمة الإلكترونية وكل ما يتعلق بالجريمة الإلكترونية من حيث المفهوم والنظريات، ثم يلي ذلك عرض للدراسات السابقة وذات الصلة التي تناولت موضوع الدراسة.

1.2 الشرطة

1.1.2 مقدمة:

إن حفظ الأمن والنظام العام هو الغاية الأساسية من إنشاء المؤسسة الشرطية، وذلك لتحقيق الأمان والاستقرار للمواطن والمجتمع وبالتالي الوطن، فالأمن حاجة أساسية للأفراد والمجتمعات ومرتكز أساسي لبناء دولة المؤسسات وتجسيدها على أرض الواقع وتحقيق التنمية الشاملة المستدامة، فهي تعمل ضمن إطار قانوني للحفاظ على مبدأ سيادة القانون وتسعى لتقديم خدمات شرطية فعّالة بكفاءة ومهنية تفي باحتياجات المجتمع وتقوم بمهامها بصدق وأمانة واتقان واحترام لحقوق الإنسان، لبلوغ الأهداف الأمنية وغيرها من الأهداف لتحقيق الاستقرار والتنمية وتطوير المجتمع نحو الأفضل، ومهما تعددت النظم تبقى الشرطة الركيزة الأساسية لبسط سلطة المجتمع صاحب المصلحة الحقيقية في بسط الأمن والأمان (البطاط، 2017: 35).

فدور الشرطة ومهامها وواجباتها لم تعد محصورة بإنفاذ القوانين وضبط الجريمة، أو الوقاية منها فقط، إنما امتد دورها للأخذ بالأسباب والدوافع التي أدت إلى ارتكابها، فالشرطة مؤسسة أمنية تقدم خدماتها لأفراد المجتمع كافة وتضع على عاتقها مسؤوليات اجتماعية تقتضي أداء أدوار غير تقليدية ضمن مهامها ووظائفها.

فيعتبر جهاز الشرطة الفلسطينية من أهم الأجهزة الأمنية في دولة فلسطين، والتي يرتبط وجودها بحفظ الأمن والأمان كأحد الحاجات الأساسية للمواطن في المجتمع الفلسطيني (سليمان،2011: 10).

2.1.2 مفهوم الشرطة:

لغوياً: ورد في لسان العرب"الشرطة بالتحريك" معناها العلامة. وقولهم أشرط فلان نفسه لكذا، أي أعملها وأعدها لإمر ما، ومنه سمي الشرط لأن لهم علامة يعرفون بها. الواحد شرطي وشرطة والجمع شرط، سموا بذلك لأنهم أعدوا لمهمات خاصة وعلموا أنفسهم بعلامات مميزة (عمر، 1997). كما وردت في المعجم الوسيط أن" الشرطة تعني حفظ الأمن في البلاد" (مصطفى وآخرون، 2011: 479).

اصطلاحاً: تعرف الشرطة بأنها "هيئة مدنية تابعة للدولة ومسؤولة عن استتباب النظام العام بمعناه التقليدي (الأمن العام، الصحة العامة، السكينة العامة) ومعناه الجديد من خلال الحفاظ على (البيئة، جماليات المدينة، أخلاقيات المجتمع) فالصفة المدنية للشرطة تنطوي على ضمانه لحقوق الإنسان ذلك لمساءلة هذه الجهة عند تعسفها وتجاوزها للقانون" (أبو عواد، 2017: 8).

وعرفها القرار بقانون رقم (23) لسنة (2017م) بشأن الشرطة: بأنها قوة نظامية تمارس اختصاصات مدنية، تتبع الوزارة، وتؤدي مهامها واختصاصاتها بموجب أحكام هذا القرار بقانون.

ويعرفها عبد الفتاح غراب بأنها "جماعة الجند كان يعتمد عليهم الخليفة أو الوالي في حفظ النظام والقبض على المجرمين، ويقترن عملهم بنظام الحراسة والعسس في الليل" ويقال أيضاً عن تعريف الشرطة بأنها "الهيئة النظامية المكلفة بحفظ الأمن والنظام وتنفيذ أوامر الدولة ونظمها" (صبره، 2017: 20).

وعرفت الشرطة بشكلها الحديث على أنها "هيئة مدنية تعمل على بث روح الطمأنينة والأمان، للمحافظة على النظام، والأمن العام، ومكافحة الجريمة والحد منها، وتنفيذ القوانين واللوائح والواجبات لخدمة المجتمع" (الطناني، 2010: 52).

إجرائياً: الجهة المختصة بإنفاذ القانون في الأراضي الفلسطينية وحفظ الأمن والنظام العام من خلال حماية الحقوق والممتلكات والقبض على الجناة في حال وقوع الجرائم.

3.1.2 نشأة الشرطة الفلسطينية:

لقد مرت نشأة الشرطة الفلسطينية بمراحل عديدة، موضحة كما يأتي:

- **المرحلة الأولى:** كان أول تشكيل للشرطة الفلسطينية في الأول من تموز سنة (1920) بأمر من المندوب السامي البريطاني هربرت صموئيل وتزامن مع إنشاء الإدارة المدنية الانتدابية في فلسطين وقوة الشرطة الفلسطينية كانت تتكون من الدرك الفلسطيني والدرك البريطاني، حيث تم إصدار العديد من القوانين في تلك الفترة التي تحدد وتبين صلاحيات الشرطة، والتي استمر العمل بها إلى أن جاء الاحتلال الصهيوني سنة (1948) وكانت مهام الشرطة آنذاك تطبيق القانون وحفظ الأمن والكشف عن الجرائم ومحاربتها.

- **المرحلة الثانية:** بعد عام (1948) وبعد قيام (إسرائيل) باحتلال القسم الأكبر من أرض فلسطين تم إصدار قرار مشترك من جامعة الدول العربية بضم الضفة الغربية إلى السلطة الأردنية؛ حيث طبقت كافة القوانين الأردنية عليها، في حين أنشأت مصر إدارة خاصة في قطاع غزة (إدارة الحاكم العام لقطاع غزة)، وتم إصدار قانون خاص بالشرطة سمي بقانون الشرطة رقم (6) لعام (1936).

- **المرحلة الثالثة:** بعد احتلال (إسرائيل) لجميع أراضي فلسطين في الضفة الغربية وقطاع غزة عام (1967) تم حل الشرطة وشكلت قوة شرطية جديدة بالتعاون مع الجيش الإسرائيلي حيث كان

تشكيلها بالأمر العسكري الإسرائيلي رقم (37) لعام (1967)، المعدل بالأمر العسكري رقم (74) لعام (1967)، والأمر رقم (647) لعام (1980) (جهاز الشرطة الفلسطينية، 2023).

- **المرحلة الرابعة:** في عام (1948) تم دمج الشرطة الفلسطينية بالشرطة الأردنية نتيجة الاحتلال الإسرائيلي، وفي عام (1967) وبعد احتلال الضفة الغربية ترك رجال الشرطة عملهم إلا القليل منهم انضموا إلى الشرطة الإسرائيلية، وفي عام (1987) قدم عناصر الشرطة الفلسطينية استقالاتهم بناء على قرار من القيادة الموحدة للانتفاضة، وقد نشأت الشرطة الموجودة حالياً وبشكلها ونظامها الحالي في مكان تواجد السلطة الفلسطينية بالأراضي الفلسطينية بتاريخ (1994/7/1) بقرار من الرئيس الراحل الشهيد ياسر عرفات والتي كان يرأسها في تلك الفترة اللواء/ غازي الجبالي وذلك بعد اتفاق إعلان المبادئ (أوسلو) عام (1993)، وبعدها اتفاق (غزة أريحا عام 1994) وجاءت الاتفاقية الانتقالية بواشنطن والتي حلت محل اتفاقية القاهرة وتحت فصل ترتيبات الأمن والنظام العام والتي اشتملت في المادة (12) على نص تشكيل قوة شرطية فلسطينية قوية، تم إنشاء الشرطة الفلسطينية من جديد عقب دخول السلطة الفلسطينية إلى أريحا وغزة واندمج معها عدد من أفراد الشرطة ممن استقالوا عام (1987) (سليمان، 2011: 28).

4.1.2 الوظائف والمهام المناطة بجهاز الشرطة الفلسطيني:

تمارس الشرطة الفلسطينية عملها من خلال عدة إدارات تعمل بشكل متكامل منها (إدارة العلاقات العامة والإعلام، دائرة البحوث والتخطيط والتطوير، إدارة الشؤون الإدارية، إدارة القوى البشرية، وحدة النوع الاجتماعي، اتحاد الشرطة الرياضية، إدارة التدريب، إدارة التسليح، إدارة الجودة الشاملة، إدارة الحراسات، دائرة الشرطة القضائية، إدارة المباحث العامة ووحدة الجرائم الإلكترونية، إدارة المعابر والحدود، إدارة شرطة السياحة والآثار، إدارة شرطة المرور، إدارة مراكز الإصلاح والتأهيل، إدارة مكافحة المخدرات، إدارة هندسة المتفجرات، الإدارة المالية، دائرة المظالم وحقوق الإنسان، إدارة الأمن الداخلي، قوات الشرطة الخاصة، كلية الشرطة الفلسطينية، مفوضية التوجيه السياسي، ووحدة حماية الأسرة والطفل (جهاز الشرطة الفلسطينية، 2023).

فوجود هذه الإدارات والتي تختص كل منها بعمل معين فرض على جهاز الشرطة الفلسطيني عدد كبير من الوظائف الأساسية التي تتمثل في الوظائف (الإدارية، القضائية، الاجتماعية، الاقتصادية، السياسية)، إن هذه الوظائف توضح لنا أن طبيعة الواجب المنوط بالمؤسسة الشرطية والذي يتمثل في حماية مصالح الدولة (السياسية، الاقتصادية، والاجتماعية)، حيث يمكن تفسير تلك الوظائف كما على النحو الآتي:

- **الوظيفة الإدارية:** وهي مهام الشرطة بدورها سلطة إدارية تمارسها من أجل الحفاظ على الأمن العام وتشمل كافة الأعمال التي ترمي إلى منع ارتكاب الجرائم من حيث أعمال الحراسة والدوريات وتنظيم المرور ومراقبة الأشخاص والأماكن إلى غير ذلك من الأعمال الوقائية بهدف منع وقوع الجريمة وتقليل فرص ارتكابها، وتنحصر الوظيفة الإدارية للشرطة بأهداف أساسية تتمثل في المحافظة على الأمن العام، ويقصد به جميع الإجراءات والتدابير الوقائية التي من شأنها منع وقوع أي إخلال أو اضطراب يعكر صفو المجتمع، وكذلك التدابير اللازمة للمحافظة على كيان الدولة السياسي وقت وقوع الأزمات والكوارث، والمحافظة على النظام العام بمكوناته المتمثلة في السكينة العامة، الصحة العامة، وتنفيذ ما تفرضه القوانين واللوائح والأنظمة من مهام، وهذا يتحقق من خلال التعاون مع أجهزة إنفاذ القانون الأخرى. (البطاط، 2017: 41).
- **الوظيفة القضائية:** هي الإجراءات التي تنفذها الشرطة بعد وقوع الجريمة لإثبات وقوع الجريمة وجمع أدلتها والبحث عن مرتكبيها قبل فتح تحقيق ابتدائي فيها، فدور الشرطة القضائي لا يبدأ إلا بعد وقوع الجريمة، وهو محدد بضوابط وهذا ما عالجه قانون الإجراءات الجزائية، أما دور الشرطة الإداري فهو دور مستمر لا يرتبط بوقوع الجريمة لأن هدفه منعها، ولم يحدد القانون طريقاً مرسوماً لها بل ترك الأمر للسلطة الإدارية للشرطة مع الحفاظ على عدم الإخلال بالحريات العامة التي كفلها الدستور للأفراد، أي بمعنى آخر أعمال الضبط الإداري تستمد صفتها من أوامر السلطة الإدارية، أما أعمال الضبط القضائي تستمد صفتها من القانون بمعنى أن السلطات الممنوحة لرجال الضبط القضائي ترتكز في القيام بإجراءات التحري والبحث عن الجرائم ومرتكبيها وملاحقتهم، ولأن هذا التدخل يعتبر مساساً بصميم حرية الأفراد لما يستلزمه من إجراءات ضبط وتفتيش، فإنه من الواجب أن تكون ممارسة هكذا أعمال تحت إشراف السلطة القضائية، والتي تتمثل بالنائب العام ووكلائه، ضماناً لعدم إساءة استخدام السلطة، فاستقصاء الجرائم والتحري وجمع الاستدلالات هي المهمة الأصلية لرجال الضبط القضائي (سليمان، 2011: 19).

وقد منحت القوانين الإجرائية الجنائية أو القوانين الأخرى الخاصة صفة الضبط القضائي لفئة محددة من الأشخاص والتي تخولهم القيام بأعمال قضائية تتمثل في البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى الناتجة عن وقوعها (قراريه، 2017: 29).

وخوّلت الشرطة الفلسطينية صفة الضبط القضائي وفق نص المادة (21) من قانون الإجراءات الجزائية رقم (3) لسنة (2001م)، والتي بينت أن مأموري الضبط القضائي هم: "مدير الشرطة

ونوابه ومساعدوه ومديرو شرطة المحافظات والإدارات العامة، ضباط وضباط صف الشرطة كل في دائرة اختصاصه".

مما سبق نستنتج أن الشرطة تُعتبر من مأموري الضبط القضائي العام المخول لهم صلاحيات البحث والتحري واستقصاء الجرائم، والقبض والتحقيق وجمع الأدلة بشأن واقعة إجرامية وقعت، تمهيداً لإحالة الدعوى إلى المحكمة من أجل البت فيها بحكم نهائي، حيث يمارس مأموري الضبط القضائي أعمالهم تحت إشراف السلطة القضائية ممثلة بالنائب العام ووكلائه.

- **الوظيفة الاجتماعية:** هي الإجراءات التي يتم العمل بها وفقاً لما تنص عليه القوانين واللوائح في جهاز الشرطة وتعمل على حماية أخلاقيات المجتمع ورعاية سلوك الأفراد واحترام قيمهم الإنسانية وإعلاء مبادئ الحرية والعدالة حتى تتحقق لهم الحياة الهادئة والمطمئنة، وتأخذ هذه الوظيفة شكل الإجراءات ذات الطابع الاجتماعي والتي تقدمها الشرطة الفلسطينية للجماهير، أو تساهم في تقديمها مع الهيئات المختصة ذات الشأن، ومن ذلك تأهيل نزلاء مراكز الإصلاح والتأهيل، والتوعية بأضرار ومخاطر المخدرات، والتوعية بخصوص إجراءات السلامة على الطرق وفي مجالات الحفاظ على النفس والمال، هذا بالإضافة إلى بناء علاقات اجتماعية قوية تهدف إلى زيادة الثقة بالشرطة الفلسطينية وفعاليتها من خلال المشاركة في الأنشطة المجتمعية المختلفة مع كافة الفئات.

فعند قيام جهاز الشرطة بوظائفه يمارس العديد من المهام وفقاً لما ورد في المادة (3) من القرار بقانون رقم (23) لسنة (2017م) لمزيد من المعلومات أنظر/ي للملحق رقم (4) والتي بينت المهام المخول بها جهاز الشرطة للحفاظ على استقرار المجتمع وهي: "المحافظة على النظام والأمن العام، والآداب العامة، والسكينة العامة، حماية الأرواح والأعراض والأموال، منع ومكافحة الجريمة، وضبط مرتكبيها بموجب القوانين المعمول بها، مكافحة أعمال الشغب وكافة مظاهر الإخلال بالأمن العام، حماية الحقوق والحريات المشروعة التي يكفلها القانون الأساسي والقوانين ذات الصلة، والاتفاقيات الدولية التي تكون الدولة طرفاً بها، حماية الممتلكات العامة والخاصة للدولة والأفراد، مساعدة قوى الأمن والسلطات العامة الأخرى في أداء مهامها بموجب أحكام القانون، التعاون الشرطي العربي والإقليمي والدولي في مجال مكافحة الجريمة من خلال جمع وتوثيق وتبادل المعلومات والبيانات والأدلة عن الجرائم ومرتكبيها، وتقديم خدمات التعاون الشرطي والأمني وفقاً للتشريعات والقوانين النافذة، والاتفاقيات الدولية التي تكون الدولة طرفاً فيها، تنفيذ ما تفرضه عليها القوانين واللوائح والأنظمة من واجبات ومهام، تقديم المعلومات والإرشادات للمواطنين بالوسائل التي تساعد على مكافحة الجريمة، ووقايتهم منها، وتسهيل تنفيذ واجبات الشرطة بما يحقق ضمان مساهمة المواطنين في معاونتها ودعمها في كافة

واجباتها، توعية المواطنين بحقوقهم وواجباتهم، لضمان المشاركة المجتمعية في حفظ النظام والأمن العام في المجتمع، تحقيق الأمن الداخلي للوطن والمواطنين، والمساهمة في تحقيق الأمن القومي بالتنسيق والتعاون مع الأجهزة الأمنية المختصة، والمؤسسات العامة، ومؤسسات المجتمع المدني، ووسائل الإعلام، ولها تنظيم مذكرات تفاهم بهذا الخصوص".

5.1.2 دور جهاز الشرطة الفلسطيني في مواجهة الجرائم الإلكترونية:

مع التطور السريع المستمر لوسائل الاتصالات وتكنولوجيا المعلومات ظهرت العديد من الجرائم منها (الابتزاز الإلكتروني، السرقة، التهديد، غسيل الأموال) ومن أجل مواجهة هذا النوع من الجرائم كان لا بد من إنشاء وحدة متخصصة للتحقيق في الجرائم الإلكترونية تتكون من محققين وطاقم من ذوي الاختصاص والكفاءة في مجال تقنية المعلومات، فأنشأ جهاز الشرطة الفلسطيني وحدة متخصصة للتحقيق في الجرائم الإلكترونية وجمع أدلتها وإعداد التقارير اللازمة حتى إحالتها إلى النيابة العامة، وهذه الوحدة تابعة لإدارة المباحث العامة في الشرطة الفلسطينية في منتصف عام (2013)، وذلك بمبادرة من مدير عام الشرطة وأضحى عمل هذه الوحدة والإجراءات التي تقوم بها محددة مع دخول القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية حيز التنفيذ، فقانون الجرائم الإلكترونية هو الذي أنشاء وحدة مكافحة الجرائم الإلكترونية وفق ما ورد في المادة (3) من القانون التي تنص على "إنشاء وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية"، وتتولى النيابة العامة الإشراف القضائي عليها".

والذي تم تعديله وفقاً للقرار بقانون رقم (28) لسنة (2020م) بتعديل قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية، وفيما بعد تم تعديل المادة (3) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية في المادة (4) وفقاً للقرار بقانون رقم (38) لسنة 2021م بتعديل قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية لمزيد من المعلومات أنظر/ي للملاحق رقم (5، 6، 7) والتي نصت على أنه تعدل المادة (3) من القانون الأصلي لتصبح على النحو الآتي: "إنشاء وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات"، وتتولى النيابة العامة الإشراف القضائي عليها، وعلى المحاكم النظامية والنيابة العامة، وفقاً لاختصاصاتهما، النظر في دعاوى الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات".

مما سبق نستنتج أن إجراءات استقصاء وتحري الجرائم الإلكترونية كان محصوراً على الشرطة فقط إلا أن المشرع وسع نطاقها من خلال السماح للأجهزة الأمنية الأخرى بالتحقيق فيها فالمشرع أدرك

حاجة تعاون الأجهزة الأمنية وضرورة تبادل الخبرات فيما بينها وذلك في سبيل مكافحة الجرائم الإلكترونية لما تتسم به هذه الجرائم من خصائص فهي تفرض تكاتف وتعاون المؤسسات الأمنية في سبيل مكافحتها في حال وقوعها نظراً لإدراكهم لخطورة آثارها على المجتمع إلى جانب الوقاية منها للتصدي لها ومنع وقوعها.

فالهدف من إنشاء هذه الوحدة هو عدم مقدرة مأموري الضبط العاديين على التعامل مع البيئة الإلكترونية، حيث يعتبر إنشائها نوع من الإجراءات والضمانات المحافظة على أموال الغير وأسرارهم، وأصبح لتلك الوحدة اختصاص نوعي محدد، ذلك بهدف مواجهة التحديات القائمة في هذا المجال لمكافحة الجرائم الالكترونية كظاهرة من الظواهر الإجرامية المستحدثة والتي تتطلب طواقم وإجراءات ومعدات خاصة والتي ترتكب إما عن طريق وسائل الاتصال المختلفة أو باستخدام الحاسوب والإنترنت، وتعمل هذه الوحدة جاهدة وباستخدام الطرق التكنولوجية الحديثة للكشف عن الجرائم، وكذلك التعرف على الجناة بهدف تقديمهم إلى العدالة (عموري، 2018: 30-34).

وكما يقوم كل قسم من أقسام الشرطة بمهامه ودوره المناط به تمارس وحدة الجرائم الإلكترونية الفلسطينية عدة إجراءات عند وقوع الجرائم الإلكترونية وفق للإجراءات المخولة لها قانوناً فتبدأت بمرحلة جمع الاستدلالات والتي تعرف بأنها "مجموعة التحريات التي يقوم بها رجال الشرطة قبل وضع النيابة العامة يدها على القضية قصد التأكد من حدوث الجريمة وجمع الأدلة عنها وكشف مرتكبها"، وتكمن أهمية إجراءات جمع الاستدلالات بأنها تعطي صورة واضحة عن وقوع الجريمة، وكيفية حدوثها وملاحقة مرتكبيها وضبطهم، تمهيداً لتسليمهم إلى الجهة المخولة بالتحقيق الابتدائي أي النيابة العامة (عبدالباقي، 2015: 145).

فالسلطات القائمة على مرحلة جمع الاستدلالات هم الشرطة العاملين في وحدة الجرائم الإلكترونية كونهم من مأموري الضبط القضائي ذوي الاختصاص العام والذين من اختصاصهم ضبط الجرائم الإلكترونية الواقعة في حدود جغرافية معينة، فهم يقومون بدور لا غنى عنه في التحري عن الجرائم وكشفها وجمع أدلتها على أن تتم تأدية هذا العمل تحت إشراف النيابة العامة كونها الجهة المخولة بالرقابة على عمل مأموري الضبط القضائي أثناء أدائهم لمهامهم، فالأصل أن النيابة العامة هي من تختص بمرحلة جمع الاستدلالات والتحري عن الجرائم ومرتكبيها، بهدف منع وقوع الجريمة وتأمين سلامة المجتمع، فللحفاظ على هذا الهدف فإنها تقوم بتفويض مأموري الضبط القضائي لتحرير محاضر جمع الاستدلال والتحري وذلك للمبررات التالية كما وردت في (حربيات، 2023: 32):

1- سرعة إنجاز التحقيق.

2- توفير وقت المحقق.

3- مساعدة النيابة في توفير المحاضر اللازمة لتقديمها للقضاء.

4- تشعب أعمال التحقيق المطلوبة من سلطة التحقيق.

5- كفاءة مأموري الضبط القضائي على تنفيذ بعض أعمال التحقيق.

6- تسير ظروف عمل سلطة التحقيق للانتقال والتحرك إلى الوجهة اللازمة.

فيتمتع مأموري الضبط القضائي من الشرطة وفي حال وقوع أي جريمة عادية أو إلكترونية بصلاحيات في مرحلة جمع الاستدلالات تمكنهم من معاينة الجرائم وجمع أدلتها والبحث عن مرتكبيها وتقديمهم

للمحاكمة والصلاحيات الممنوحة لهم نوعان:

صلاحيات أصيلة للضابطة القضائية:

بهدف رفع فعالية أعمال مأموري الضبط القضائي، فقد سعى المشرع الفلسطيني إلى تخويل الأشخاص القائمين على مرحلة جمع الاستدلالات عدد من الصلاحيات تتمثل في :

1- تلقي البلاغات والشكاوى.

2- البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى.

3- إجراء الكشف والمعاينة للحصول على الايضاحات اللازمة لتسهيل التحقيق.

4- ترتكز مرحلة جمع الاستدلالات على ضرورة تكمن في التثبت من هوية المشبه به والحيلولة دون تمكينه من الإفلات من رقابة العدالة، خاصة إذا لم يكن له مقر معلوم، فقد تطول مدتها لتصل إلى سنوات عديدة وإلى تجنيد قدرات بشرية غير محدودة تعتمد على الإخباريات والتقارير الأمنية، كما يرتكز جمع الاستدلال على ضرورة التحقق من الشبهة التي تحوم حول الشخص.

5- الاستماع للمشتبه به للحصول على الإيضاحات اللازمة لتسهيل التحقيق عبر ما يسمى بالواقع العملي بأخذ إفادته.

6- التوجه إلى مسرح الجريمة لجمع الأدلة المادية والتفتيش والحجز (الكسواني، 2019: 59-66).

الصلاحيات الاستثنائية للضابطة القضائية:

قد يتعرض الفرد محل الملاحقة أثناء مرحلة جمع الاستدلالات إلى القبض وإلى انتهاك حريته الشخصية وإلى الاعتداء على شخصه وكرامته، ففي مثل هذه الظروف منح المشرع الفلسطيني صلاحيات استثنائية للضابطة القضائية تخولهم القيام بأعمالهم على أكمل وجه يكون نطاق الصلاحيات الاستثنائية في حالة التلبس في الجريمة أو ما يعرف بحالة الجرم المشهود: فتكون الجريمة متلبساً بها في إحدى الحالات التالية: في حال ارتكاب الجريمة أو عقب ارتكابها ببرهة وجيزة، إذا تبع المجني عليه مرتكبها أو تبعته العامة بصخب أو صياح إثر وقوعها، إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملا آلات أو أسلحة أو أمتعة أو أورقا أو أشياء أخرى يستدل منها على أنه فاعل أو شريك فيها، أو إذا وجدت به في هذا الوقت آثاراً أو علامات تفيد ذلك.

وتتمثل الصلاحيات الاستثنائية في :

1- الضبط: يعرف بأنه وضع اليد على الشيء وحبسه محافظة عليه لمصلحة التحقيق، ويقصد به وضع اليد على أشياء تتعلق بالمتهم أو غيره لجمع أدلة تتعلق بمسرح الجريمة، والضبط إجراء من إجراءات التحقيق الابتدائي إلا أن للنيابة العامة سلطة تفويض مأموري الضبط القضائي للممارسته، ويتم التحرز على المضبوطات وفق إجراءات شكلية محددة قانوناً ويتم تحرير محضر بها.

2- تفتيش ذي الشبهة: أحد إجراءات الاستدلال التي تقوم بها السلطات المختصة في إطار بحثها عن الجريمة، بغية الكشف عن أدلة الجريمة سواء للعثور على أدوات الجريمة أو للعثور على محل الجريمة أو العثور على مرتكب الجريمة أو شركائه، وقد يكون التفتيش للشخص بهدف التنقيب عن دليل الجريمة في جسمه أو ملابسه أو ما يحمله، فالتفتيش عمل تحقيقي يرجع بالأساس إلى السلطة القضائية ويفوض إلى مأموري الضبط القضائي بصورة استثنائية كون تفتيش جسد شخص ينطوي على المساس بحريته الشخصية ويمس من كرامته ، إذ أن تفتيش شخص المتهم يؤدي إلى معاملته وكأنه مدان. لذا لا بد من فرض واجب التحري إلى أقصى حد، قبل إعطاء الإذن بإجراء التفتيش، أو قبل القيام بتفتيش أحد الأفراد أو المنازل.

3- القبض على ذي الشبهة: هو أحد إجراءات الاستدلال والتحقيق يهدف إلى احتجاز ذي الشبهة مدة محددة قانوناً للتحقق من شخصيته لسبب الاشتباه به تمهيداً لاتخاذ إجراءات بحقه. إما بتوقيفه أو بعرضه على المحكمة المختصة أو الإفراج عنه. فالقبض إجراء استثنائي يؤدي إلى

الحد من حرية الفرد وإن مصلحة الفرد تقتضي تقييد مدة القبض بشكل مطلق بحيث لا تزيد عن 24 ساعة (حريبات، 2023: 18-22).

وهذه المهام مخول بها مأموري الضبط القضائي من العاملين في الشرطة كافة كونهم يمتلكون تفويضاً عاماً وأيضاً في القرار بقانون بشأن الجرائم الإلكترونية تم توضيح الإجراءات المتبعة من قبل مأموري الضبط القضائي بما لا يتعارض والإجراءات المتبعة عند وقوع أية جريمة من الجرائم وفقاً لأحكام قانون الإجراءات الجزائية الفلسطيني ومن الإجراءات المتبعة من قبلهم كما ورد في المادة (52) من القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته لمزيد من المعلومات أنظر/ي للملحق رقم(8) والتي نصت على أن:

أ. "للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة.

ب. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة.

ت. 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.

ث. 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.

ج. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية ولجرائم الاتصالات وتكنولوجيا المعلومات".

فما يتنج عن ممارسة إجراءات التفتيش والضبط سوف يكون كدليل من أدلة الإثبات التي سوف يواجه بها المتهم أمام المحاكم المختصة وهذا وفقاً للمادة (57) من القرار بقانون رقم (18) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته لمزيد من المعلومات أنظر/ي للملحق رقم(8) والتي نصت على أنه: "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".

والمادة (58) من ذات القرار والتي نصت على أنه: "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".

فيجب على مأموري الضبط القضائي بعد القيام بالبحث والتحري تحرير محاضر الاستدلال في الجرائم الإلكترونية وفقاً للإجراءات القانونية المحددة كوسيلة إثبات لتحديد مدى مشروعية أعمال الضابطة القضائية أثناء قيامها بأعمال الاستدلال مع ذي الشبهة، وتخضع هذه المحاضر إلى شروط شكلية معينة أهمها: التنصيص على صفة المأمور المحرر للمحضر، كما ينبغي أن تكون المحاضر موقعة ومؤرخة، وإن إفادة المشتبه به يجب أن تحرر كاملة صلب المحضر، ولا يجوز التنقيص منها.

إلى جانب هذه الشروط الشكلية هنالك شرط جوهري بشخصية المأمور فيجب أن يتحلى بالسرية والنزاهة والحياد حيال سماع المشتبه به، كما ويفترض بالمحضر أن يتسم بالوضوح والشفافية المطلقة، بحيث يبين بصورة لا لبس فيها حقيقة الاستدلالات الأولية كما هي، لا سيما الإجراءات التي تم اتخاذها كي تتثبت الهيئات القضائية فيما بعد من شرعية هذه الإجراءات، كون هذه المحاضر من الوسائل الكتابية التي اعترف بها القانون في إثبات الجريمة، وهنا تكمن خطورتها فقد تؤدي هذه المحاضر حسب ما يرد فيها من تصريحات يحررها مأمورو الضابطة القضائية بالشخص محل الملاحقة إما بالبراءة أو الإدانة، ويأتي المحضر سابقاً للتحقيق الابتدائي، مما يجعل له أثراً مباشراً في الإجراءات اللاحقة كونه التصوير الأول للحادث، وقد تنتفي في تقدير القاضي أية مصلحة لمحرر المحضر في إخفاء الحقيقة أو محاولة تغييرها، وهذا يعطي محاضر البحث والاستدلال نظرة واقعية وأهمية عملية تساند حجيتها القانونية. فلا يعتمد المحضر الذي يحرره مأمورو الضبط القضائي إلا إذا كان محرراً وفق الشروط الشكلية المحددة قانوناً، وإن تحرير محاضر الاستدلال لا بد أن يكون مقتصراً على إجراءات البحث (الاستدلالات)، ومن خلال هذه المحاضر يتم تزويد سلطات التحقيق والحكم بأوفر قدر ممكن من المعلومات التي توفر لها العناصر اللازمة لإقامة الدعوى العمومية والتقرير والحكم فيها (الكسواني، 2019: 81-88).

تختص وحدة الجرائم الإلكترونية في الشرطة بتلقي البلاغات والشكاوي عن الجرائم الإلكترونية وتتولى مهمة التوجه إلى مسرح الجريمة لجمع الأدلة وتحرير محاضر الاستدلال وذلك بعد حصولها على التفويض من النيابة العامة للقيام بإجراءات البحث والتحري (التفتيش والضبط) وتحرير محاضر بها علماً أن وحدة الجرائم الإلكترونية في فلسطين يقتصر وجودها على مرتب مدير عام الشرطة في محافظة رام الله، وتتكون من عدة أقسام وهي: قسم جرائم الإنترنت وجرائم التقنية، وقسم الأدلة الرقمية الذي ينقسم إلى (مختبر الأدلة الرقمية، ومخزن الأدلة الرقمية) وهو القسم المختص بالتفتيش وضبط

الأدلة وتخزينها، قسم التوعية والإرشاد، قسم الاتصالات وتأمين المعلومات، وقسم التحقيق والدائرة القانونية.

وتتمثل مهامها في العمل على استقبال الاحتياج الوارد من قبل رئيس نيابة الجرائم الإلكترونية، لتحديد وسائل تكنولوجيا المعلومات، والاتصالات التي ارتكبت بواسطتها الجريمة الإلكترونية وتزويد رئيس النيابة بتقرير فني بالمعلومات المطلوبة، وثاني مهامها تنفيذ أمر النيابة بالنفاذ المباشر إلى وسائل تكنولوجيا المعلومات المضبوطة وتفتيشها، للحصول على المعلومات والأدلة المطلوبة، وثالثاً في حالات معينة متابعة بعض القضايا المعقدة التي لا يقدر عليها ضباط الشرطة في المحافظات، وإن من يختص بتلقي الشكاوى المتعلقة بالجرائم الإلكترونية هم من ضبابط فرع المباحث العامة في كافة محافظات الوطن وهم مدربين على التعامل ومتابعة قضايا الجرائم الإلكترونية الواردة إلى الشرطة في مناطقهم ويمارسون عملهم تحت إشراف عضو النيابة المختص، وتنفيذ قراراته، فهم من يتلقون الشكاوي وبعد ذلك يقومون بإحالتها إلى دائرة الجرائم الإلكترونية والتي بدورها تخاطب النائب العام بالاحتياج الذي يرغبون وبه وهو بدوره يخاطب شركات الاتصالات ومزودي الإنترنت للحصول على المعلومات اللازمة لاستكمال إجراءات البحث والتحري وبعد تفريغها بمحضر استدلال وفق لما هو محدد قانوناً يتم إحالتها إلى النيابة العامة (عموري، 2018: 33- 34).

مما سبق نستنتج أن الشرطة الفلسطينية تسعى جاهدة ومن خلال الموارد المتاحة من أجل محاربة الجريمة الإلكترونية سواء أكان بكشفها وملاحقة مرتكبيها بعد وقوعها أو بتوعية وإرشاد المواطنين من أجل منع وقوعها أو على الأقل الحد من انتشارها.

2.2 النيابة العامة

1.2.2 مقدمة:

تعد النيابة الممثل القانوني للدولة وهي الشخص الإجرائي الرئيس الذي أوكلت إليه الدولة صلاحية مباشرة اقتضاء حقها في العقاب، وهي البيئة التي أنيط بها تحريك الدعوى الجزائية والتحقيق بها ومباشرتها أمام القضاء ومتابعتها إلى حين الفصل بها بحكم بات، حيث كان ذلك نتاج تطور النظرة إلى الجريمة بصفتها اعتداء على المجتمع أكثر منها اعتداء على مصالح خاصة للأفراد، فالنيابة العامة لا تمارس دورها بوصفها خصماً عادياً وإنما تنوب عن الدولة من أجل تحقيق سيادة القانون، وإن كان لكل دعوى طرفان المدعي والمدعى عليه حيث قد يكونا شخصاً طبيعياً وشخصاً معنوياً ودائماً تكون النيابة العامة في الدعوى الجزائية هي من تمثل المدعي كونها الهيئة الاجتماعية التي تمثل المجتمع والحق العام للدولة في اقتضاء العقاب (الجعبري، 2019: 11)

وفي فلسطين وعند استقراء نصوص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة (2001م) نجد أن هذا القانون نص على الاختصاص الأصيل للنيابة العامة وهو تحري الدعوى العمومية، حيث نص في المادة (1) على أنه " تختص النيابة العامة دون غيرها بإقامة الدعوى الجنائية ومباشرتها ولا تقام من غيرها إلا في الأحوال المبينة في القانون" وبالتالي فإن هذا النص جعل من النيابة العامة تستأثر بصلاحية تحري الدعوى العمومية في مواجهة المتهم وذلك نيابة عن المجتمع الذي تمثله، فالنيابة العامة هي الممثل القانوني للمجتمع في مواجهة كل من تسول له نفسه ارتكاب جريمة معاقب عليها في القانون، فالجرائم لا يقتصر أثرها فقط على الضحية وإنا تمتد إلى المجتمع وتهدد أمنه واستقراره وعليه ومن خلال البحث في تاريخ النظام القانوني الفلسطيني والغاية التي أنشئت من أجلها النيابة العامة فهي جهة قضائية وتمثل عموم المجتمع، وظيفتها الأساسية هي تحري الدعوى العمومية وتختص بها دون غيرها من الجهات القضائية (مصري: 2020، 8)

2.2.2 مفهوم النيابة العامة:

لغوياً: "ناب والنائب من قام مقام غيره في أمر أو عمل يقال نائب الرئيس ونائب القاضي ونائب الشعب والنائب العمومي، هيئة قضائية تقوم بإقامة الدعوى على المتهم ونحوه نيابة عن المجني عليه فرداً كان أو مجتمعاً" (مصطفى وآخرون، 2011: 960).

اصطلاحاً: "النيابة العامة ممثلة الدولة في تنفيذها للقانون، وهي السلطة المناط بها توجيه الاتهام ومباشرته نيابة عن الدولة والمجتمع، وفي أدائها لهذا الدور لا تعتبر خصماً عادياً للأفراد، وإنما تعتبر نائبة عن الدولة في تأدية عمل من الأعمال من أجل تأكيد السيادة القانونية للدولة" (صعابنه، 2011:7).

إجرائياً: هي جهة قضائية تختص دون غيرها بتحريك الدعوى الجزائية ومباشرتها نيابة عن الدولة والمجتمع.

3.2.2 نشأة النيابة العامة:

فعند تتبع تاريخ النظام القانوني الفلسطيني، نجد أن فلسطين قد مرت بعدد من الحقب التاريخية والقانونية وهي على النحو الآتي:

- **المرحلة الأولى:** هي المرحلة الخاصة بفترة الحكم العثماني حيث حرص المشرع العثماني على سن القوانين الجزائية، وكان على رأسها قانون المحاكمات الجزائية العثماني، وعمد المشرع على وضع

سلطة التحقيق والاتهام في يد جهة عمومية، يتم تعيين هذه الجهة وأفرادها من قبل الدولة ووفقاً للقانون، وتكون هذه الجهة مختصة بتحري الدعوى العمومية في مواجهة المتهم بارتكاب جريمة معاقب عليها.

- **المرحلة الثانية:** في هذه المرحلة كانت فلسطين خاضعة للانتداب البريطاني الذي أبقى على القوانين العثمانية سارية المفعول مع إخضاعها للإدارة العسكرية، وأعطى صلاحية إقامة الدعوى العمومية إلى النائب العام أو من يمثله أو مأمور بوليسي، وبعد ذلك خضع قطاع غزة إلى الإدارة المصرية التي أعطت النيابة العامة صلاحية تحري الدعوى العمومية، ولها سلطة التحقيق والاتهام.
- **المرحلة الثالثة:** بعد إنشاء السلطة الوطنية الفلسطينية عمدت إلى توحيد القوانين بين شقي الوطن غزة والضفة الغربية، وقامت بسن قانون الإجراءات الجزائية الفلسطيني النافذ حالياً، وكذلك قانون السلطة القضائية الفلسطيني وغيرها من القوانين التي تعنى بشؤون القضاء، وجميع هذه القوانين اعترفت بالنيابة العامة أنها ممثل المجتمع والمختصة دون غيرها في إقامة الدعوى العمومية في مواجهة المتهم، وللنيابة العامة سلطة التحقيق والاتهام (مصري: 2020، 7).

4.2.2 مهام النيابة العامة:

تقوم النيابة العامة بعدد من المهام المخولة لها بموجب القانون كما ورد في (التقرير السنوي للنيابة العامة، 2018: 14) وهي على النحو الآتي:

- مباشرة التحقيق الابتدائي فور علمها بالجريمة ومن ثم تحريك الدعوى الجزائية وإحالتها ومتابعتها أمام المحكمة المختصة والترافع فيها حتى آخر درجات التقاضي (سلطة الاتهام والتحقيق) أمام المحاكم المختصة.
- الإشراف على مأموري الضبط القضائي.
- تنفيذ الأحكام الواجبة التنفيذ.
- الطعن في الأحكام.
- تمثيل المؤسسات الحكومية أمام كافة المحاكم في الدعاوى والطلبات التي تقام منها أو عليها وفقاً للقانون في الدعاوى الحقوقية والإدارية والدستورية.
- الإشراف على دور الرعاية الاجتماعية ومراكز الإصلاح والتأهيل من خلال إجراء زيارات دورية والاطلاع على سجلاتها والاتصال مع أي نزيل أو موقوف فيها والتحقيق في شكواه.
- إقامة الدعوى التأديبية على القضاة وأعضاء النيابة العامة ومباشرتها.

فتختص النيابة العامة دون غيرها بإجراء التحقيق الابتدائي، فبعد أن يقع البحث عن الجريمة من خلال مرحلة جمع الاستدلالات، والتي يقوم بها مأمورو الضابطة القضائية يتم إحالة ملف القضية إلى النيابة العامة كسلطة تحقيق ابتدائي والتي من خلالها يتم القيام بمجموعة من الإجراءات والتحريات المأذونة من سلطات التحقيق والرامية إلى تحقيق أدلة الإدانة أو البراءة، والسعي إما إلى تدعيم الاتهام وإحالة المتهم إلى المحكمة المختصة، أو إلى حفظ الدعوى أو حفظ ملفها (أوراقها) حيث لا وجه شرعي لملاحقة المتهم، وهذه الإجراءات قد تكون موجه للمتهم من خلال استجوابه فيجب توجيه الاتهام له ويحق له الإجابة أو الصمت لحين توكيل محامي، التفتيش، وقد تكون ماسة بحرية الفرد كالتوقيف والإفراج، وهناك عدد من الإجراءات تمارسها النيابة العامة لمسنادتها في العمل كتفويض مأموري الضبط القضائي، وإصدار المذكرات القضائية (مذكرة حضور، مذكرة إحضار، مذكرة توقيف) إلى جانب إجراءات الاستعانة بالغير والتي تتمثل بسماع الشهود وندب الخبراء (الكسواني، 2019: 91-142).

إلا أنه يجب الالتزام بسرية التحقيق فهو من الضمانات العامة الممنوحة للمتهم، على اعتبار أن هذه السرية من شأنها عدم الإساءة للمتهم والتشهير به قبل إدانته، فسرية التحقيق تعني أن تتم إجراءات التحقيق في غير علانية، وأن تخفى عن كل من لا يهمه أمر التحقيق بصورة شرعية، فمن خلال سرية التحقيق يبقى المحقق بعيداً عن التأثيرات التي تقع عليه وبالتالي تحقق استقلاليته في عمله، إلا أن هذه السرية تكون اتجاه الغير، ويتم إقرار علانية التحقيق تجاه الأطراف (الأحمد، 2008: 28).

فانتهاء التحقيق الابتدائي يقتضي التصرف فيه ويكون بإصدار النيابة العامة لأحد القرارين الأول: إحالة ملف الدعوى الجزائية مقروناً بلائحة اتهام إلى المحكمة المختصة والثاني حفظ الدعوى الجزائية، وبالتالي تخرج الدعوى الجزائية من حوزة النيابة العامة وتدخل في حوزة القضاء حيث لا يجوز للنيابة العامة بعد ذلك اتخاذ أي من إجراءات التحقيق الابتدائي وهذا ما سوف يتم توضيحه على النحو الآتي:

1- قرار الإحالة: بعد انتهاء التحقيق في الجريمة تصدر النيابة العامة هذا القرار، فيتم إحالة ملف الدعوى الجزائية مشتملاً على لائحة اتهام إلى المحكمة المختصة وقرار الإحالة يصدر عن عضو النيابة العامة دون تصديق النائب العام في الجنح، أما في الجنايات فإن قرار الإحالة الصادر يكون عن عضو النيابة العامة يحتاج إلى مصادقة النائب العام أو أحد مساعديه.

ولائحة الاتهام هي: القرار الذي يصدر عن عضو النيابة العامة بتوجيه اتهام رسمي للمتهم لإحالته إلى المحكمة المختصة لمحاكمته وتكون لائحة الاتهام وفق إجراءات شكلية محددة قانوناً،

فلا يجوز تقديم أي شخص للمحاكمة في الدعاوي الجزائية إلا إذا صدر بحقة لائحة اتهام من النائب العام أو من يقوم مقامه من أعضاء النيابة العامة، ولا يجوز لوكيل النيابة العامة عندما يترافع أمام المحكمة أن يدعي قيام المتهم بجرائم أو أفعال لم تشتمل عليها لائحة الاتهام وإلا كان ادعاؤه باطلاً.

2- قرار حفظ الدعوى الجزائية: إن قرار وقف سير إجراءات الدعوى الجزائية عند حفظ الدعوى ومنع إحالتها إلى المحكمة لعدم وجود أدلة على نسبة الجريمة للمتهم أو عدم كفايتها، وتكون هذه النتيجة قد توصلت إليها النيابة العامة من خلال التحقيق الذي أجرته، ويجب أن يكون قرار الحفظ ثابتاً بالكتابة ويجب أن تكون فيه البيانات الضرورية للمتهم وتسبيب الحفظ كما ويجب إعلان الأمر بالحفظ من النيابة العامة للمجني عليه والمدعي بالحق الشخصي (عبدالباقي، 2015: 301-307).

5.2.2 دور النيابة العامة في مكافحة الجرائم الالكترونية في فلسطين:

لكي تحقق النيابة العامة في فلسطين هدفها في محاربة الجرائم بجميع أنواعها وتطبيق القانون على الجميع، وفي خطوة هامة للقضاء على الجرائم الإلكترونية والتي زادت بشكل ملحوظ مع التطور التكنولوجي الحاصل في العالم، وإدراكها للتطور المتسارع في كافة نواحي الحياة وباستقراء الوضع الجرمي الحالي والمستقبلي ثبت بأنه لم تعد حدود الزمان والمكان حائلاً أمام ارتكاب الجرائم بفعل ثورة الاتصالات والتقنيات الحديثة وظهور أشكال جديدة للجرائم بأساليب مبتكرة لتنفيذها، تبنت النيابة العامة مهمة التصدي لهذه الجرائم من خلال إنشاء نيابة مكافحة الجرائم المعلوماتية "الإلكترونية" في مكتب النائب العام بناء على قرار صادر عن عطوفة النائب العام بتاريخ (2016/3/20)، حيث تعمل تلك النيابة تحت إشراف النائب العام مباشرة، وتم تكليف رئيس النيابة بتولي شأنها يعاونه عدد من وكلاء ومعاوني النيابة العامة يساندهم في العمل كادر إداري، وبتاريخ (2017/1/2) تم تخصيص أعضاء نيابة عامة مختصين لمتابعة قضايا الجرائم الإلكترونية وتدريبهم وإعدادهم للتعامل مع هذه الجرائم في كافة النيابات الجزئية في مختلف محافظات الوطن.

وتتولى النيابة المختصة متابعة الطلبات المتعلقة بالجرائم الإلكترونية والاتصالات وكافة الطلبات الواردة من النيابات الجزئية والأجهزة الأمنية والدعاوى ذات العلاقة والتنسيق معها بالشأن، وكذلك تتعاون تلك النيابة مع وحدة مكافحة الجرائم الالكترونية في الشرطة والأجهزة المعنية ذات الاختصاص والأجهزة الأمنية الأخرى، وتتولى التواصل مع الجهات والمؤسسات والشركات المختصة فيما يتعلق بالجرائم الإلكترونية والاتصالات والحصول على الدليل الفني الإلكتروني وربط الجناة فيه، فالنيابة

مخولة بهذه الإجراءات وفقاً لما ورد في المادة (53) من القرار بقانون بشأن الجرائم الإلكترونية وتعديلاته لمزيد من المعلومات أنظر/ي للملحق رقم (8) والتي تنص على أن: "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، ولها 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، وأنها يجب أن تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها، وأن 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".

والمادة (54) من ذات القرار والتي تنص على أنه:

أ. " 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.

ب. 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".

بحيث يتم التعامل بالقضايا الواردة لتلك النيابة بالسرعة الممكنة والسرية التامة، ورفع الملف التحقيقي إلى المحكمة المختصة للسير بإجراءات المحاكمة العادلة وإدانة الجناة (التقرير السنوي للنيابة العامة، 2018: 19).

6.2.2 اختصاصات نيابة مكافحة الجرائم الالكترونية وآلية عملها:

تخصص نيابة مكافحة الجرائم الإلكترونية بعدد من الإجراءات المخولة للقيام بها وهي على النحو الآتي:

- متابعة الطلبات المتعلقة بالجرائم الإلكترونية وكافة الطلبات ذات العلاقة الواردة من النيابات الجزئية والأجهزة الأمنية ومخاطبة الجهات المختصة (شركات الاتصالات ومزودي خدمات الإنترنت).
- التعاون مع المختبر الجنائي الإلكتروني في وحدة مكافحة الجرائم الإلكترونية والمباحث العامة والأجهزة الأمنية ذات الاختصاص.
- التواصل والتنسيق مع الجهات والمؤسسات والشركات ذات العلاقة فيما يتعلق بالجرائم الإلكترونية والاتصالات والحصول على الدليل الفني الإلكتروني وربط الجناة فيه، بحيث يتم التعامل مع القضايا الواردة بالسرعة والسرية الممكنة.

أما فيما يتعلق بآلية عمل نيابة مكافحة الجرائم الإلكترونية فهي على النحو الآتي:

- استقبال الشكاوى ذات العلاقة من قبل النيابات الجزئية.
- استقبال الاحتياج المعلوماتي من قبل النيابات المختلفة والأجهزة الأمنية والتدقيق فيها من قبل نيابة الجرائم الإلكترونية – مكتب النائب العام.
- العمل بسرية وسرعة مطلقة على مدار 24 ساعة مع الشركاء.
- تحليل وتقييم الدليل الإلكتروني في الجرائم المختلفة وفقاً للاحتياجات التي ترد إلى نيابة مكافحة الجرائم الإلكترونية – مكتب النائب العام.
- تنظيم الوقت اللازم لإنجاز الطلبات مع الاخذ بعين الاعتبار الطلبات العاجلة من قبل نيابة الجرائم الإلكترونية – مكتب النائب العام.
- التحقيق والترافع في الشكاوى الواردة بالخصوص وفقا للمعايير التي تتناسب مع طبيعة وخصوصية تلك الجرائم ومتطلباتها من قبل أعضاء النيابة المتخصصين بالمحافظات.
- فحص المضبوطات وفقاً للإجراءات القانونية المحددة.
- تحليل الكشوفات من قبل أعضاء نيابة الجرائم الإلكترونية المكلفين بالنيابات الجزئية.
- ممارسة الدور الوقائي والعقابي في ذات الوقت لصد ومكافحة هذا النوع من الجرائم وفقا للقانون

والأصول.

- الاشتراك بالجانب التوعوي مع المؤسسات الشريكة.

7.2.2 آلية تقديم شكوى لدى نيابة مكافحة الجرائم الإلكترونية:

تقدم الشكوى من خلال المواطن نفسه أو وكيله الخاص أو ينوب عنه مثل الولي (إذا كان عمر المجني عليه أقل من 15 عاماً أو مصاباً بعاهة في عقله) أو الوصي أو القيم (إذا كانت الجريمة واقعة على المال) أو النيابة إذا تعارضت مصلحة المجني عليه أو من يمثله أو لم يكن له من يمثله. فيتم تقديم شكوى في جريمة إلكترونية لدى كل من:

- **تقدم الشكوى لدى وكيل النيابة العامة المختص في المحافظة:** حيث يتولى عضو النيابة الشكوى وسماع أقوال المشتكي وتحديد الاحتياج، ليتم مخاطبة النائب العام بها لمتابعتها من قبل رئيس نيابة مكافحة الجرائم الإلكترونية والتي تعمل على الاحتياج للحصول على الدليل الرقمي أو الفني، ومن ثم تعيد الملف لنيابة المحافظة لمباشرة التحقيق وإحضار المتهم ومواجهته بالدليل الرقمي وبالتقرير الفني وبعد انتهاء التحقيق يتم إحالة الملف للمحكمة المختصة.
- **تقديم الشكوى لدى وحدة الجرائم الإلكترونية في الشرطة:** بدورها تقوم بالبحث والتحري لجمع محاضر الاستدلال، وتخاطب النائب العام للحصول على احتياجاتها سواء أكانت (أمر نفاذ أو التوصل مع شركات الاتصالات ومزودي خدمة الإنترنت للحصول على معلومات) وغيرها من الاحتياجات التي تسهل الحصول على الدليل الرقمي، ومن ثم تسلم النتيجة للشرطة لاستكمال ملف التحري والاستدلال وصولاً إلى الفاعل فيتم تنظيم لائحة شرطة وإحالتها إلى النيابة العامة التي بدورها تقوم بإحالتها إلى المحكمة المختصة مكانياً (النيابة العامة، 2022).

مما سبق نستنتج أن العلاقة بين نيابة الجرائم الإلكترونية ووحدة الجرائم الإلكترونية علاقة تكاملية في سبيل ضبط الجرائم الإلكترونية وتقديم مرتكبيها إلى العدالة لمحاكمتهم، ويتجلى ذلك من خلال الصلاحيات المخولة من النيابة العامة للشرطة كمأموري ضبط قضائي لاستقصاء الجريمة الإلكترونية وتزويدهم بالأذونات اللازمة لجمع الأدلة وكشف المجرمين، كما أن إنشاء نيابة متخصصة في الجرائم الإلكترونية يساعد في تسهيل العمل وتحقيق نتائج أكبر في كشف المجرمين وضبطهم كون الجرائم الإلكترونية تتمتع بطبيعة خاصة تتطلب تعيين أشخاص متخصصين للتحقيق فيها.

3.2 القضاء :

1.3.2 مقدمة:

يُعبر القضاء في الدولة عن نهضتها ومعيار تقدمها ومظهر رقيها، وما من دولة تخلف فيها القضاء إلا تخلفت عن ركب المَدنية وأسباب الارتقاء، ذلك وأن القضاء هو سياج للحقوق والحريات وفي كنفه يستقر الأمن وتزدهر الحياة الاجتماعية والاقتصادية والسياسية.

فالقوانين مهما بلغت دقتها في الصياغة، فهي لا تستطيع أن تحقق العدالة ولن تبلغ ذلك إلا إذا قام على تطبيقها قضاء مستقل ونزيه، قادر على تحقيق محاكمة عادلة تحكم ببراءة المتهم أو إدانته وإيقاع العقوبات الرادعة عليه للتأكد من عدم عودته لارتكاب الجريمة مرة أخرى إلى جانب انصاف الضحية باقتصاص حقها من الجاني.

فتكمن أهمية القضاء في دوره الذي يتمثل في إقامة العدل، ومنع الظلم، فالعدل هو الذي يحفظ الحقوق، ويؤسس لحياة إنسانية كريمة يشعر فيها الناس بالأمن والاستقرار والطمأنينة وبوجود قضاء عادل نضمن استمرارية المجتمعات وتطورها كون كل فرد يعلم ما له من حقوق وما عليه من واجبات يجب الالتزام بها دون التعدي على الآخرين بأي شكل من الأشكال (نصرالله، 2014: 24).

2.3.2 مفهوم القضاء :

لغوياً: "قضى والقاضي هو القاطع للأمور المحكم لها ومن يقضي بين الناس بحكم الشرع، والقضاء الحكم وعمل القاضي ورجال الهيئة القضائية التي يوكل إليها بحث الخصومات للفصل فيها وفق القوانين" (مصطفى وآخرون،2011: 742).

اصطلاحاً: عند البحث في أقوال العلماء وتعريفاتهم للقضاء، فإننا لا نجد اختلافاً بين التعريف اللغوي والشرعي، حيث يشتركان في أن كلاً منهما حكم، وهذا يظهر معنا من خلال تعريف جمهور الفقهاء للقضاء، فلقد عرفه بعضهم بالقول "الحكم بين الناس بالحق، والحكم بما أنزل الله عز وجل"، وعرفه بعضهم "بالقول، قول ملزم يصدر عن ولاية عامة كذا في خزانة المفتين" (حمد،2017: 5).

وعرف: "بأنه الفصل بين الناس فيما يقع بينهم من مظالم أو نزاعات " (أبوهربيد،2009: 5).

ويعرف إجرائياً: بأنه الجهة المفوضة بتطبيق القانون والفصل في الدعاوي الجزائية لحل النزاع بين الخصوم من خلال الوقائع المعروضة أمامه فهو الضمانة لحماية الحقوق والحريات.

3.3.2 المبادئ التي يستند عليها القضاء:

تحكم عملية التقاضي العديد من المبادئ التي ويعتمد كل منها على الآخر بحيث إن غياب أحدها أو اختلال التوزان بينها يؤدي إلى تقويض العدالة وحقوق المواطنين، وهذه المبادئ على النحو الآتي كما ذكرها (عبدالباقي، 2015: 317- 324):

1- مبدأ استقلال القضاة: وهو أن تكون السلطة القضائية جهازاً وفرداً مستقلاً في منأى عن التدخل في شؤونهم من قبل أي جهة أو شخص سواء أكان داخلياً أو خارجياً.

2- مبدأ حياد ونزاهة القاضي: وهو قدرة القاضي على حل الخلاف دون الالتفات لأي مصلحة حقيقية أو محتملة، فالقاضي ينظر للنزاع وفقاً لحيثيات القضية وعلى هدي من القانون دون أية قيود أو تدخل أو تأثير من أية جهة ولأي سبب.

3- مبدأ المساءلة: وهو الرقابة على عمل القضاة لضمان سير عملية التقاضي وفق القانون وبما يحقق المحاكمة العادلة لمختلف أطراف الدعوى الجزائية.

4.3.2 مرحلة المحاكمة في فلسطين:

المحاكمة العادلة هي حق للمتهم في محاكته فيما يتعلق بالاتهام الجنائي الموجه له أمام جهة قضائية محايدة ومستقلة، فبعد أن تستوفي أجهزة الاستدلال إجراءاتها في البحث عن الأدلة المثبتة عن الجريمة، وبعد أن تقوم النيابة العامة بممارسة عملها بالتحقيق الابتدائي في الجريمة تحيل الشخص المتهم بالجريمة والذي يرجح اقترافه للفعل للمحكمة المختصة، والتي يأتي دورها للموازنة بين أدلة البراءة وأدلة الادانة، عن طريق محكمة مستقلة ومحايدة ينشئها القانون، يضمن فيها السير العادل للمحاكمة ويضمن أن ينبني الحكم الجزائي والنطق به وفق إجراءات سليمة يضمن فيها حق الطعن بالأحكام وهذا ما سوف يتم توضيحه على النحو الآتي:

أولا: السير العادل للمحاكمة:

فيعد إجراء المحاكمة تتويجاً للمراحل الإجرائية السابقة، وهي النظر في وقائع الدعوى، وهي مرحلة إظهار الحقيقة وتوضيحها، من خلال ما تصدره من أحكام تقر بالبراءة أو الإدانة، ولتحقيق المحاكمة العادلة يجب الموازنة بين مصلحة المجتمع ومصلحة الأفراد باحترام حقهم في التمتع بالبراءة من خلال احترام المحكمة للحق في المواجهة ومن خلال السعي لتدعيم ذلك الحق، لذا يشرط وجود ضمانات للمحاكمة العادلة وهي على النحو التالي:

1- **الحق في المواجهة:** كل إجراء من إجراءات الدعوى العمومية لا بد أن يبنى على ضمان تحقيق المواجهة ما بين أطراف الدعوى العمومية ومناقشة ما يقدمه كل طرف من أدلة ومؤيدات، وقد ترتب على هذا الحق العديد من الواجبات والحقوق التي تضمن تحقيق محاكمة عادلة وتضمن عدم إفلات المجرم من العقاب ومن هذه الواجبات ما يلي:

أ- واجب الحضور: يكلف الخصوم بالحضور إلى المحكمة ويبلغوا بذلك قبل انعقاد الجلسة، ويحق لهم الاطلاع على أوراق الدعوى كي يتمكنوا من تحضير أنفسهم للمواجهة في الخصومة الجزائية.

ب- حق الاستعانة بمحامٍ: يحق للمتهم الاستعانة بمحامٍ للدفاع عنه، ففي حال كانت التهمة الموجهة له من الجنايات على القاضي أن يسأل المتهم هل قام بتوكيل محام للدفاع عنه أم لا؟، فإذا لم يكن قد فعل بسبب ضعف حالته المادية انتدب له رئيس المحكمة محامياً، فالاستعانة بمحام تمكن المتهم من التبصر القانوني بالتهمة المسندة إليه، كما يمكنه التعرف على آراء الشهود والاستماع إلى أقوالهم كي يتمكن من تفنيدها أو التصديق عليها، ولا يكون كل هذا الوعي والتبصر إلا بالاستعانة بمحام (الكسواني، 2019: 145-150).

2- **علنية المحاكمة:** أي أنه يسمح لغير أطراف الدعوى من الاطلاع على إجراءاتها ومناقشتها بدون قيد، فمن خلال العلانية تبرز مدى نزاهة القضاء من خلال تجنب الحيل والخزعبلات، وتبين مدى شفافية العمل القضائي وتجعل من جمهور العامة والناس المراقب الأول على سلوك الجهاز القضائي، وتوفر الضمانات الرئيسية للمتهم، والتي تمكنه من الدفاع عن نفسه بحرية لكشف الحقيقة، وتعطي العلنية صورة عامة للجمهور عن مدى احترام كرامة الإنسان، وتبين مدى تقدير هيبة العدالة، إلا أنه وفي ظروف استثنائية يتم إجراء الجلسات سرية وذلك بحظر حضور وقائع المحاكمة على الجمهور العام وذلك من أجل حماية حياة المتهم والعمل على المحافظة على النظام العام والاخلاق، فالمرافعات تكون سرية إلا أن النطق بالحكم لا يكون إلا بجلسة علنية (النمري، 2016: 23-26).

3- **شفوية إجراءات المحاكمة:** أي أن تجري المحاكمة شفوياً وبصوت مسموع في جل الإجراءات التي تتم في جلسة المحكمة، فكل الطلبات والدفوع تقدم شفوياً، فلا تقام الأحكام إلا على التحقيقات والمناقشات والمرافعات العلنية، التي تحصل شفوياً أمام المحاكم، وفي مواجهة الخصوم، لكي يتم توضيح الأدلة، وكشف غموضها وحقيقتها، حتى تكون المحكمة في ظروف تستطيع تكوين قناعاتها في وزن الأدلة وتقدير قيمتها وبالتالي قدرة القاضي على تأسيس قناعاته الوجدانية للفصل في الدعوى الجزائية (طاهر، 2017: 23-24).

ثانيا: إجراءات المحاكمة الجزائية:

تستند إجراءات المحاكمة الجزائية على ركائز تضمن سلامة الأحكام في مواجهة سلطات العدالة ومنع تعسف الخصوم، فتجري المحاكمة التي تصدر فيها الأحكام الجزائية، ويتبعها الحق الذي يتم من خلاله مراقبة صحة الأحكام والمتمثل في الطعون الجزائية، فتكون على النحو الآتي:

- **ركائز سلامة المحاكمة الجزائية:** تبرز هذه الدعائم في القناعة الوجدانية للقاضي الجزائي وفي مبدأ التقاضي على درجتين من خلال:

أ- القناعة الوجدانية للقاضي الجزائي: فيجب أن يمتلك القاضي الخبرة التي تمكنه من التعامل مع المتقاضين والتعامل مع الأحداث والوقائع وتمكنه من تمحيص الأدلة للوصول إلى حكم سليم، ويكون لقاضي الأصل وحده سلطة وحق تقدير الأدلة وموازنتها وفقا لما يمليه عليه وجدانه الخالص، فلا يبني اقتناعه إلا على الدليل الذي وصل إلى مرتبة الجزم أو اليقين، وإنه يبني قناعته بناء على تقدير قانوني للوقائع لكي يتكمن من إصدار حكمه بالطريقة السليمة (الكسواني، 2019: 160-165).

ب- مبدأ التقاضي على درجتين: فيحق لكل الفرد أن يتم النظر في دعواه مرتين، من خلال اللجوء إلى محكمة أعلى درجة لمراجعة الحكم الصادر بحقه، فهو بذلك يوفر له فرصة النظر من جديد في الدعوى إذا ما تراءى له أن محكمة الدرجة الأولى أهملت جانباً من جوانبها، وهو أيضاً ضمان للمتضرر الذي يرى أن الحكم الصادر ليس منصفاً له، وكذلك الشأن بالنسبة للنيابة العامة، التي يوفر لها فرصة عرض الدعوى الجزائية من جديد وبالتالي الحصول على حكم نهائي وبات، فيهدف المشرع من مبدأ التقاضي على درجتين ضمان تحقيق العدالة، وصدور أحاكم عادلة تضع الأمور في نصابها (عبدالباقي، 2015: 332).

- **الأحكام الجزائية:**

تنظر المحاكم في المنازعات والجرائم كافة، وقد حدد المشرع المحاكم التي تصدر عنها الأحكام الجزائية المختلفة وعليه فإن الأحكام الجزائية تتمثل في :

1- **أحكام محاكم الصلح:** تتألف محاكم الصلح من قاض فرد، وتختص محاكم الصلح بنظر جميع المخالفات والجنح الواقعة ضمن اختصاصها ما لم ينص القانون على خلاف ذلك، ولتحريك الدعوى العمومية في محكمة الصلح يجب إيداع لائحة اتهام بحق المتهم من النيابة العامة، وعندما توضع هذه اللائحة تنظم مذكرات بالحضور لأطراف الدعوى، فيجب أن تتم إجراءات

التبليغ وفق ما هو محدد قانوناً فيكون تكليف الخصوم بالحضور أمام المحكمة قبل انعقاد الجلسة بيوم كامل في المخالفات وبثلاثة أيام على الأقل في الجنح مع مراعاة مسافة الطريق، وإذا لم يحضر المتهم يتم الحكم عليه غيابياً.

2- **أحكام محكمة البداية:** تنشأ محاكم البداية في مراكز المحافظات حسب مقتضى الحال، تشكل محكمة البداية من رئيس وعدد كاف من القضاة، فتنعقد هيئة المحكمة من ثلاثة قضاة، تكون الرئاسة لأقدمهم، وتنعقد من قاضٍ فرد في الأحوال التي يحددها القانون، وتختص بالنظر في جميع الجنايات، وجرائم الجنح المتلازمة معها والمحالة إليها بموجب قرار الاتهام، فيقوم النائب العام بإصدار قرار اتهام، ويدون كاتب المحكمة جميع وقائع المحاكمة في محضر الجلسة، ويوقع عليه من هيئة المحكمة، وتنعقد جلسة المحاكمة بحضور المتهم، وتسمع فيها المحكمة شهادات الشهود وتستوفي كافة البيات اللازمة مع تمكين المتهم حق الاستعانة بمحامٍ، وبعد ذلك تختلي المحكمة في غرفة المداولة وتدقق فيما طرح أمامها من بينات وادعاءات، وتضع حكمها بالإجماع أو بالأغلبية فيما عدا عقوبة الإعدام التي يجب أن تكون بإجماع الآراء، ويصدر الحكم بصورة علنية ولو كانت الدعوى نظرت في جلسة سرية، كما وتختص محكمة البداية بالنظر في الاستئنافات المقدمة ضد الأحكام الصادرة عن محاكم الصلح (الكسواني، 2019: 168-171).

- **الطعون الجزائية:**

الطعون هي نوع من أنواع الرقابة التي يمكن أن تمارس على أعمال القضاء، ومن خلالها نضمن سير العدالة، وتحقيق مقومات المحاكمة العادلة، والطعون نوعان وهما:

1- **الطعون العادية:** وهو ما أجازه القانون لكل خصم، أيا كان العيب الذي يطلقه على الحكم، سواء أكان العيب موضوعياً أو قانونياً، فتهدف طرق الطعن العادية إلى إعادة طرح الدعوى على القضاء مرة أخرى، أي تجديد النزاع أمام القضاء، وهي على النحو الآتي:

أ- **الطعن بالاستئناف:** يعد الطعن بالاستئناف من طرق الطعن العادية، وذلك تجسيداً لمبدأ التقاضي على درجتين فيهدف هذا المبدأ إلى تصحيح الأخطاء التي تقع بالحكم الابتدائي، فالطعن في حكم محكمة الدرجة الأولى أمام محكمة الدرجة الثانية، يهدف إلى تجديد النزاع، والتوصل إلى فسخ الحكم أو تعديله. فإذا كانت الأحكام الحضورية صادرة عن محاكم الصلح تستأنف أمام محاكم البداية بصفتها الاستئنافية، وإذا كانت هذه الأحكام صادرة عن محاكم البداية بصفتها محاكم أول

درجة تستأنف أمام محاكم الاستئناف، وعند الطعن بالاستئناف يكون الحكم الصادر ابتدائياً بالإدانة بالإمكان إيقاف تنفيذه وفق قرار المحكمة كضمانة لعدم الإضرار بالمحكوم عليه ابتدائي لحين صدور حكم نهائي بات، وقدد حدد المشرع الفلسطيني مدة الاستئناف للمتهم بخمسة عشر يوماً تبدأ في اليوم التالي لتاريخ النطق بالحكم إذا كان حضورياً أو من تاريخ تبليغه إذا كان بمثابة الحضوري، ويرد الاستئناف شكلاً إذا تم تقديمها بعد الميعاد المحدد، فالاستئناف يكفل حق المتهم في تمحيص دفاعه مرتين وبالتالي التأكيد على عدالة سير إجراءات المحاكمة بحقه، ويكون للنيابة العامة مدة (30) يوماً لاستئناف الأحكام الجزائية تبدأ من اليوم التالي لصدور الحكم، وقد اشترط المشرع أن تشمل عريضة الاستئناف بياناً كاملاً بالحكم بالاستئناف، ورقم الدعوى التي صدر بشأنها، وصفة المستأنف والمستأنف ضده، وأسباب الاستئناف، وطلبات المستأنف (شرباتي، 2015: 79-99).

ب- الطعن بالاعتراض: هو طريق من طرق الطعن العادية، يكون في الأحكام الغيابية أي الأحكام التي تصدر في غيبة المتهم دون أن تتاح له فرصة الدفاع عن نفسه، حيث يكفل الطعن بالاعتراض للمتهم حضور المحاكم، كما يمكنه من إبداء دفاعه وتفنيد الأدلة المقدمة ضده، كما يحقق مصلحة الجماعة حتى تتأكد من أن الحكم قد صدر في حدود القانون وبصورة ترضي العدالة، فيكون للمحكوم عليه غيابياً في مواد الجنح والمخالفات أن يعترض على الحكم خلال العشر أيام التالية لتبليغه بالحكم، فإذا انتهت هذه المدة سقط حقه في الطعن بالاعتراض، ويتم تقديم الاعتراض بطلب إلى المحكمة التي أصدرت الحكم، ويوقع عليه من قبل المحكوم عليه أو وكيله، ويتوجب على المحكمة أن تحدد جلسة للنظر في الاعتراض وأن يبلغ الخصوم بموعد الجلسة، وإذا تخلف المعترض عن الحضور بدون عذر فإن الاعتراض الثاني يرفض ولا يتسنى له الطعن بالحكم إلا بطريق الاستئناف (عبد الباقي، 2015: 440- 441).

2- الطعون الاستثنائية:

أقر المشرع الفلسطيني نطاقاً استثنائياً للطعون يرتكز الأول على مبدأ الفصل بين محاكم الموضوع ومحكمة القانون، فتنظر الأولى في أصل النزاع في حين تنظر الثانية في صحة تطبيق القانون وفق حالات محددة يجوز من خلالها الطعن بالنقض، أما الطعن الاستثنائي الثاني فيركز على صدور أحكام احتوت أخطاء واقعية يجوز فيها الطعن بطلب إعادة المحاكمة، والتي سوف يتم توضيحها فيما يلي:

أ- الطعن بالنقض: هو طعن استثنائي للأحكام النهائية الصادرة عن آخر درجة في الجنايات والجنح غايته فحص الحكم المطعون فيه للتحقق من مطابقته للقانون، فيخول لمحكمة النقض الرقابة والإشراف على صحة تطبيق القانون، لذا فهي تقوم بتدقيق الأحكام المرفوعة إليها من ناحية مخالفتها لأحكام القانون دون التعرض للوقائع، وتقوم بتقرير المبادئ القانونية الصحيحة في النزاع المعروض عليها إذا كان الطعن في الحكم المرفوع إليها مبنياً على مخالفة القانون أو على خطأ في تطبيقه أو في تأويله، فهي لا تقييم مسؤولية ولا تقرر عقوبة أو تنتقضها وإنما يقتصر عملها على مراقبة أعمال محاكم الموضوع، والطعن بالنقض يكون للأحكام النهائية التي استوفت درجتي التقاضي من حيث الموضوع، وقد حدد المشرع الفلسطيني مدة الطعن بالنقض بأربعين يوماً تبدأ من اليوم التالي للذي صدر فيه الحكم حضورياً، وفي اليوم الذي يلي تبليغ المتهم بالحكم إذا كان الحكم بمثابة الحضوري، ويحق لمحكمة النقض قبول الطعن أو رفضه، ويكون الطعن بالنقض بأمر خطي فيقدم طلباً خطياً من وزير العدل إلى النائب العام لعرض الملف على محكمة النقض وذلك إذا كان الحكم مخالفاً للقانون، وقد اكتسب درجة الحكم القطعي ولم يسبق لمحكمة النقض البت فيه، وفي حالة قبول المحكمة للطعن فإنها تبطل الإجراء أو الحكم أو القرار المطعون فيه، ولقد أصدرت محكمة النقض الفلسطينية العديد من الطعون ومن الأمثلة عليها أنظر/ي لما ورد في الملحق رقم () والملحق رقم () (المدبوح، 2018: 9- 29).

ب- الطعن بإعادة المحاكمة: وهي طريقة استثنائية للطعن يلتمس فيها المحكوم عليه إعادة النظر في الأحكام الباتة الصادرة بعقوبة في مواد الجنيات أو الجنح، بهدف الرجوع فيها، أو تعديلها، أو تخفيفها، إذا ظهر أنها مشوبة بخطأ جسيم في الوقائع، فيجوز إعادة المحاكمة في الأحكام التي اكتسبت الدرجة الباتة في مواد الجنايات والجنح في الأحوال التالية: إذا حكم على شخص في جريمة قتل، ثم ظهرت أدلة تثبت أن المدعى بقتله قد وجد حياً، إذا صدر حكم على شخص من أجل واقعة ثم صدر حكم على شخص آخر من أجل الواقعة عينها، وكان بين الحكمين تناقض بحيث يستنتج براءة أحد المحكوم عليهما، إذا كان الحكم مبنياً على شهادة قضي بأنها كاذبة، أو على وثيقة قضي بعد صدور الحكم بأنها مزورة، وكان لهذه الشهادة أو الوثيقة تأثير في الحكم، إذا ظهرت وقائع جديدة بعد صدور الحكم، أو أظهرت وثائق وأدلة كانت مجهولة حين صدور الحكم وكان من شأن هذه الوقائع أو الوثائق إثبات براءة المحكوم عليه، إذا كان الحكم مبنياً على حكم صادر من محكمة مدنية أو إحدى محاكم الأحوال الشخصية وألغي هذا الحكم، ويقدم مطلب التماس إعادة المحاكمة إلى وزير العدل من المحكوم عليه أو وكيله وفي حال رفض طلب إعادة المحاكمة، فلا يجوز تجديده بناء على ذات الوقائع التي بني عليها، أما في حال قبوله يوجه وزير العدل طلب إعادة المحاكمة إلى النائب العام الذي يحيل الطلب مع التحقيقات التي يكون قد

أجراها إلى محكمة النقض وعلى النائب العام أن يبين رأيه والأسباب التي يستند عليها في إحالة إعادة المحاكمة إلى محكمة النقض، خلال شهر من تسلمه الطلب، وإذا قررت محكمة النقض قبول طلب إعادة المحاكمة أحالت القضية إلى محكمة ذات درجة المحكمة التي أصدرت الحكم بالأساس، وفي حال كانت نتيجة إعادة المحاكمة براءة المحكوم عليه فإنه يبطل الحكم السابق، وينشر الحكم القاضي بالبراءة على نفقة الدولة بالجريدة الرسمية وصحيفتين يوميتين يعينهما صاحب الشأن، ويرد الاعتبار لمن وقع في حقه الخطأ القضائي، ويحق لمن حكم ببراءته بعد قبول إعادة المحاكمة أن يطالب الدولة بتعويضه عن الضرر الناشئ له من الحكم السابق (الكسواني، 2019: 182- 185).

نستنتج مما سبق أن القضاء الفلسطيني يمثل صمام أمن وأمان المواطن والمجتمع وركزية الاستقرار والتوزان في مختلف العلاقات والمعاملات التي تتم بين أفراد المجتمع من خلال قيام السلطة القضائية للدور المناط بها، إلا أنه وأثناء ممارسته لهذا الدور يواجه العديد من المعيقات لعل من أهمها فيما يتعلق بمواجهة الجرائم الإلكترونية، كونها جرائم مستحدثة بحاجة إلى تنظيم تشريعاتها بما يواكب حداثتها لضمان معاقبة مرتكبيها، لتحقيق العدل في المجتمع، فقصور التشريعات من الناحية الإجرائية فيما يتعلق بالتعامل مع مسرح الجريمة الإلكترونية يحول دون إمكانية اتخاذ الإجراءات اللازمة والصحيحة عند التعامل معه مما يترتب عليه عدم القدرة على التوصل إلى الفاعل، وبالتالي شعور الضحايا بالسخط على الأنظمة القانونية وعدم الانصياع لها والاستعانة بما يسمى بالهاكرز في سبيل التعرف على الجاني، وسعيهم لاقتصاص حقوقهم بأنفسهم، فقوة القضاء تكمن في قدرته على فرض سيادة القانون والمحافظة على الحقوق والحريات لجميع أفراد المجتمع على حد سواء.

4.2 الجريمة الإلكترونية:

1.4.2 مقدمة:

إن التطور المتسارع في وسائل الاتصالات وتكنولوجيا المعلومات ودخولها في شتى مجالات الحياة أدى إلى تفاقم دورها بشكل غير محدود، ومع شيوع الوسائل الإلكترونية الحديثة بين الأفراد والتوسع في التعامل من خلالها، أصبح لدى كل فرد القدرة على التفاعل والتواصل دون اعتبار لحدود المكان أو الزمان، وعلى الرغم مما وفرته التكنولوجيا الحديثة من فوائد وإيجابيات لا حصر لها إلا أن ذلك رافقه العديد من المعضلات والسلبيات التي ألقت بظلالها على المجتمع والتي من أبرزها تطور الجريمة التي أصبحت ترتكب بسهولة عبر الفضاء الإلكتروني باستخدام الوسائل التكنولوجية الحديثة،

فلم يعد الأمر يقتصر على الجريمة التقليدية بل تعداه إلى ظهور ما يسمى بالجريمة الإلكترونية (ربايعه، 2016: 2)

2.4.2 مفهوم الجريمة:

يمكن تعريف الجريمة كما على النحو الآتي:

تعرف الجريمة لغوياً: "الجريمة أصلها في اللغة العربية جرم وإجرام، أي أذنب وارتكب جرماً" (مصطفى وآخرون، 2011: 118).

وأما الجريمة اصطلاحاً: "هي سلوك يحرمه القانون، ويرد عليه بعقوبة جزائية أو تدبير احترازي، أو أنها فعل غير مشروع صادر عن إرادة جنائية، يقرر له القانون عقوبة أو تدبيراً احترازياً" (الأطرش والهاجري، 2021: 33).

في حين تُعرف الجريمة قانونياً: "بأنها سلوك ضار بالمجتمع وقيمه يقرر له القانون جزاء جنائي توقعه السلطة المختصة" (زرارة، 2014: 46).

وأما من ناحية اجتماعية: تُعرف الجريمة "بأنها نوع من أنواع الخروج عن القواعد السلوكية والعادات والتقاليد والأعراف التي يحددها المجتمع لأفراده، كون أن المجتمع هو الذي يحدد ماهية السلوك العادي وماهية السلوك الإجرامي المنحرف وفقاً لقيمه ومعاييره" (الخواجة، 2005: 16).

وعرفت أيضا "بأنها الحكم الذي تصدره الجماعة على بعض أنواع السلوك بغض النظر عن نص القانون" (الكبيسي، 2010: 940).

وأما الجريمة من ناحية إجرائية: هي مظهر من مظاهر السلوك المنحرف الذي يصدر من فرد ينتمي إلى مجتمع معين يتعارض هذا السلوك مع معايير ونظم وقوانين ذلك المجتمع مما يعرض صاحبه للعقوبة.

مما سبق يتضح لنا بأن تجريم الأفعال في أي دولة بما يتناسب مع قيمها وعاداتها وتقاليدها، فالفعل الذي يعتبر جريمة في دولة معينة قد لا يكون جريمة في دولة أخرى، فالقانون يتناسب مع قيم وثقافة كل مجتمع، وهذا ما خلق صعوبة في الحد من انتشار الجريمة الإلكترونية كونها جريمة عابرة للحدود، حيث تظهر نتائجها في دول عدة تجرم الفعل الجرمي في حين أن الدول الأخرى لا تجرمه فلا يتم ملاحقة الجاني أو معاقبته.

3.4.2 مفهوم الجرائم الإلكترونية:

هناك العديد من التعريفات التي تناولت مفهوم الجرائم الإلكترونية، على الرغم من اختلاف المسميات لتلك الجريمة (الجرائم المعلوماتية، جرائم الإنترنت، التعسف في استعمال الحاسب الآلي، الجرائم المرتبطة بالحاسب الآلي، جرائم التقنية العالية، جرائم الهاكرز، جرائم أصحاب الياقات البيضاء، السيبر كرايم) إلا أن مضمون المفهوم واحد، من بين تلك المفاهيم ما يلي:

عرفها (المليحي، 2019: 147) بأنها "بأنها الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية"

في حين عرفتها (المضحكي، 2014: 25) بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب عن طريق الحاسب الآلي".

وهناك من يعرفها بأنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف تنفيذ الفعل الإجرامي المقصود" (موسى، 2009: 112).

فيما ترى (القشوش، 2007: 140) أن الجريمة الإلكترونية "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه".

إن قانون الجرائم الإلكترونية الفلسطيني لم يتطرق إلى تحديد مفهوم دقيق للجرائم الإلكترونية، وإنما حدد العديد من المظاهر والسلوكيات التي تشكل جرائم إلكترونية، وقد تبين في مجمل أحكامه بأن الجريمة الإلكترونية "تمثل كل فعل مخالف يمكن أن يؤدي إلى الإضرار سواء للأفراد أو الشركات أو المجموعات، من خلال استخدام الوسائل التكنولوجية المختلفة في القيام بأعمال مختلفة من شأنها أن تؤدي إلى الابتزاز أو التخريب أو تعطيل المصالح العامة، أو كشف الخصوصية والسرية للمعلومات الخاصة بالأفراد، أو التزوير للتوقيع أو البيانات الشخصية أو العقود الإلكترونية، أو الانتحال للشخصية أو الاحتيال، أو السرقة، أو الاستدراج بهدف المساومة، أو الاعتداء، وكل ما يفضي إلى إيذاء الأفراد في المجتمع مخالفاً للقانون والأعراف والتقاليد، وكل ما يحاسب عليه من الجرائم العادية إذا ما ارتكبه الشخص إلكترونياً، فهو بهذا ارتكب جرماً له كافة الأركان المادية والمعنوية والنية المسبقة"، لمزيد من التوضيح حول القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته أنظر/ي إلى الملحق رقم(8).

بعد استعراض التعريفات السابقة يمكننا استنتاج أن الجريمة الإلكترونية هي: كل فعل ضار يأتيه الفرد أو الجماعة عبر استعمال الأجهزة الإلكترونية أو الذكية، للاعتداء على مصلحة يحميها القانون بغرض الحصول على منفعة مادية أو معنوية، كما ويمكننا استنتاج أن الجريمة الإلكترونية لوقوعها يجب توافر الأداة الإلكترونية المستخدمة، وفي حال توافر العناصر الثلاثة للجريمة تقع الجريمة الإلكترونية ويعاقب عليها وفق القانون، وهذا يدعمه نظرية النشاط الرتيب التي سيتم الإشارة لها في النظريات المفسرة للجريمة الإلكترونية، فهي ترى أن ممارسة الجريمة الإلكترونية يحتاج إلى وجود المجرم ذو الرغبة (الجاني) والهدف المناسب (المجني عليه) وغياب الرقابة (غياب القانون).

4.4.2 التطور التاريخي للجرائم الإلكترونية:

إن التطور التاريخي لجرائم الإنترنت مرّ بثلاث مراحل، تتمثل تلك المراحل حسب وجهة نظر (مطر، 2016: 4-6) في الآتي:

- **المرحلة الأولى:** بدأت من شيوع استخدام الحواسيب من ستينيات وسبعينيات القرن العشرين، اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة إجرامية مستحدثة، وحول ما إذا كانت الجرائم بالمعنى القانوني أو هي مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة.

- **المرحلة الثانية:** ظهرت في الثمانينيات من القرن العشرين، بظهور مفهوم جديد لجرائم الكمبيوتر والإنترنت ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد، وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج سواء الشخصية أو الحكومية وشاع اصطلاح "الهاكرز" المُعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصوراً في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقني، لكن هؤلاء المغامرون أصبحوا أداة إجرام، وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة، هذا المجرم القادر على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية والاجتماعية والسياسية والعسكرية .

- **المرحلة الثالثة:** ظهرت هذه المرحلة مع تطور الإنترنت في نهاية القرن العشرين وبداية القرن الواحد والعشرين، إذ ظهر ازدياد ملحوظ في الجرائم الإلكترونية وتغيراً في نطاقها ومفهومها، كان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات

كما ظهرت أنماط جديدة تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، وكان ذلك ضد مواقع الإنترنت التسويقية المهمة مما أدى إلى انقطاعها عن الخدمة لساعات عديدة مخلفاً وراءه خسائر مالية بالملايين، وفي تلك المرحلة نشطت جرائم نشر الفيروسات عبر المواقع الإلكترونية حيث تميزت بسهولة انتقالها إلى ملايين المستخدمين عبر البريد الإلكتروني، كذلك انتشرت الرسائل المنطوية على إثارة الأحقاد أو المساس بالكرامة، أو تلك المروجة لمواد غير قانونية وغير مشروعة.

5.4.2 خصائص الجريمة الالكترونية وأركانها:

أولاً: خصائص الجريمة الالكترونية:إن الجريمة الإلكترونية كما غيرها من الجرائم، تتمتع بمجموعة من الخصائص لعل من أهم تلك الخصائص ما يلي:

- **التوافر والقيمة والديمومة:** تتمثل هذه الخاصية بأن المعلومات جاهزة في كل مكان، تلك المعلومات القيمة مثل (بطاقات الائتمان، الحسابات المصرفية، التصاميم)، هذا بالإضافة كون المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة (الجنابي، 2017: 46).
- **جريمة ناعمة:** تمتاز بأنها جرائم لا تتطلب عنفاً على العكس من بعض الجرائم التقليدية التي تحتاج من مرتكبها إلى قوة عضلية أحياناً لتنفيذها كما في جرائم الإرهاب والسطو المسلح، إن الجرائم الإلكترونية لا تحتاج إلى مثل هذه القوة العضلية وإنما تحتاج إلى قوة علمية وقدر من الذكاء في توظيف ذلك، إن نقل بيانات مخزنة أو التلاعب بأرصدة البنوك مثلاً لا تحتاج إلا إلى لمسات أزرار حتى تنفذ بسرعة، أي أنها تتميز بإمكانية تنفيذها بسرعة (هلال، 2008: 18).
- **عابرة للحدود:** بمعنى أنها لا تعترف بعنصري الزمان والمكان فهي تتميز أحياناً بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه، إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمراً ممكناً وشائعاً لا يعترف بالحدود الإقليمية للدول ولا بالمكان ولا بالزمان حيث أصبحت ساحتها العالم أجمع، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة تجعل بالإمكان ارتكاب جريمة عن طريق حاسب موجود في دولة معينة، بينما يتحقق الفعل الإجرامي في دولة أخرى، فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية للدول، لأنه مجتمع منفتح عبر شبكات تخترق الزمان والمكان ولا تخضع لحدود معينة توقفها، إن ذلك أدى إلى وجود مشاكل قانونية في التعامل مع هذه الجرائم، كمشكلة السيادة والاختصاص القضائي وقبول الأدلة المتحصلة عليها في دولة ما أمام

قضاء دولة أخرى، ولهذا فمكافحة هذه الجرائم تتطلب تعاوناً بين الدول وتوافقاً كبيراً بين تشريعاتها (المومني، 2010: 50).

- **صعوبة الإثبات:** فيعود السبب في ذلك إلى الطبيعة الذاتية للدليل في الجرائم الإلكترونية وسهولة إتلاف الأدلة من قبل الجناة، تتميز هذه الجرائم بأنها غير مرئية في الغالب لأنها تتعلق بمعطيات في شكل نبضات أو ذبذبات إلكترونية ويسهل على الجاني محو وتدمير الأدلة المتعلقة بها في وقت وجيز، فكونها بيانات مرئية لا تفصح عن شخصية معينه فهي صعبة الاكتشاف والمتابعة، وكونها لا تترك أثراً فهي مجرد أرقام تتغير في السجلات، حيث يصعب تقصي الدليل فيها ولا يمكن إثباتها إلا من خلال الفحص الفني لآثارها ولا يوجد فيها شهوداً فهي تحتاج إلى الخبرة الفنية العالية، والتي يصعب على المحقق العادي التعامل معها، وتظهر هذه المشكلة بصفة خاصة بالنسبة لجرائم الإنترنت مثل الجرائم التي ترتكز على البريد الإلكتروني بارتكابها، فيكون من الصعب على جهات التحري تحديد جهة الإرسال أو الوصول إلى شخص المرسل، من هنا تأتي صعوبة الكشف عنها وإثباتها (وهيب، 2014: 344).

- **خصوصية الجاني في الجريمة الإلكترونية:** في بعض الجرائم الإلكترونية كالهجمات السيبرانية تحتاج أن يكون مرتكبها على دراية ومعرفة فائقة وذو خبرة كبيرة في مجال استخدام الحاسوب فهو له صفات مميزة من حيث الخبرة والعلم والقدرة على استخدام التكنولوجيا بصورة متقدمة، فضلاً عن الصفات التي تتوفر في المجرم العادي في الجرائم الأخرى، وإن مستوى الخبرة التقنية في الجرائم المعلوماتية نسبي يختلف من جريمة لأخرى إذ أن بعض الجرائم المرتكبة عبر الإنترنت لا تحتاج لخبرة تقنية عالية ويمكن أن يرتكبها أي شخص يمتلك أبجديات استخدام الحاسوب مثل جرائم السب والقذف عبر مواقع التواصل الاجتماعي، وهناك جرائم تحتاج لخبرات تقنية عالية نحو جريمة تعطيل أو عرقلة نظام معلوماتي وجريمة إتلاف المعلومات عن طريق زرع الفيروسات، وما يميز مجرم المعلومات هي الدوافع التي تدفعه لارتكاب الجريمة، فهي متعددة ومختلفة فقد تكون السعي لتحقيق الربح وقد تكون الرغبة في الانتقام وقد تكون الرغبة في التفوق على وسائل التقنية وتعقيدها، وقد يرتبط الدافع بحب التعلم والاستكشاف (نقادي، 2014: 172).

- **الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص:** وذلك بهدف الإضرار بالجهة المجني عليها، وغالباً ما يشترك في تنفيذ الجريمة الإلكترونية شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه، فالاشتراك قد يكون اشتراكاً إيجابياً أو سلبياً، فالإيجابي يتمثل بتقديم مساعدة للمجرم سواء كانت فنية أو مادية، أما الاشتراك

السلبي فيترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها (المومني،2010: 58).

- **الجريمة الإلكترونية فادحة الأضرار:** فاعتماد الأشخاص على الحاسوب في إدارة كافة الأعمال ضاعف الأضرار والخسائر التي تخلفها الاعتداءات على معطيات الحاسوب، لا سيما إذا كانت تمثل قيمة مالية، خاصة مع ازدياد اعتماد البنوك والمؤسسات الحكومية والخاصة على الحاسوب في تسييرها (نقادي، 2014: 172).

فحسب برنامج مشاريع الأمن السيبراني، من المتوقع أن تكلف جرائم الإنترنت العالم (8) تريليونات دولار في العالم، وإذا تم قياس الجريمة الإلكترونية كدولة، فستكون ثالث أكبر اقتصاد في العالم بعد الولايات المتحدة والصين، بينما تتوقع العديد من التقارير الدولية أن تزداد تكاليف الأضرار الناجمة عن الجرائم الإلكترونية على مستوى العالم بنسبة (15%) سنوياً على مدى السنوات الثلاث المقبلة، لتصل إلى (10.5) تريليونات دولار سنويًا بحلول عام (2025)، ارتفاعًا من 3 تريليونات عام (2015) (الجزيرة نت، 2023).

- **التكتم عليها من قبل المجني عليهم:** لا يتم في الغالب الإبلاغ عن الجرائم الإلكترونية، وذلك يرجع إما إلى كون الضحية لم يكتشفها أو الخشية من التشهير، فالجهات المجني عليها غالباً ما تكون إما مصرفًا أو مؤسسة مالية أو شركة أو مشروعاً صناعياً ضخماً، والملاحظ عدم تعاون هذه الجهات بالإبلاغ عن هذه الجرائم وذلك خوفاً من الإضرار بمركزها المالي وحفاظاً على شعور المساهمين بالأمان والثقة ولمحاولة عدم انتشار أساليب ارتكابها منعا للتقليد، لذلك نجد أن معظم الجرائم المرتكبة في هذا الحقل تم اكتشافها بالمصادفة وأحياناً بعد وقت طويل من ارتكابها، وحتى التي يتم اكتشافها فهي أقل بكثير من تلك الجرائم التي ارتكبت فعلياً، وذلك لا يسمح بإعطاء صورة حقيقية عن الوضع الراهن للجرائم الإلكترونية (شهوان، 2018: 11).

- **صعوبة اكتشافها:** إن الجرائم الإلكترونية يصعب اكتشافها من قبل الجهات الأمنية فهي تتميز عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي المتمثل في (بصمات، تخريب، شواهد مادية)، فإذا كانت الجريمة التقليدية تمتاز بكونها تترك خلفها آثار خاصة مرئية كالجثث أو الدماء المسفوكة فإن ذلك غير متوافر في إطار الجريمة الإلكترونية كونها ترتكز على تغيير أو تعديل البيانات كلياً أو جزئياً بالدخول إلى السجلات المخزنة في ذاكرة الحاسب الآلي، الأمر الذي يجعل إمكانية اكتشافها تكتنفه الصعوبة، بالتالي الصعوبة في توقيع الجزاء على مرتكبها (المومني، 2010: 22)

يتضح مما سبق أن هذه الخصائص المتعددة والمجتمعة في جريمة واحدة جعلت منها جريمة خطيرة بحاجة إلى جهود مضاعفة للتعامل معها للسيطرة عليها وعلى آثارها التي قد لا تطال دولة واحدة فقط بل عدة دول والتي تسبب خسائر فادحة تؤثر على الاقتصاد العام للدولة.

ثانياً: أركان الجريمة الالكترونية:

وأما فيما يخص أركان الجريمة الإلكترونية فهي مثلها مثل باقي الجرائم الأخرى يلزم توافر الأركان المتفق عليها لضرورة قيامها ولكي تتواجد على أرض الواقع، وبالتالي فإنه لا بد من وجود الثلاث أركان التي تتألف منها كل جريمة وهي النحو الآتي:

1- **الركن المادي:** يتحقق الركن المادي للجريمة بحدوث سلوك جرمي (فعل أو امتناع عن فعل) ونتيجة جرمية وعلاقة سببية بينهما، حيث سيتم شرح كل مكون من مكونات الركن المادي على النحو الآتي:

أ. **السلوك الاجرامي:** هو ما يأتي به الشخص من فعل يؤدي إلى إحداث النتيجة التي يسعى إليها، بما أن الجاني في الجرائم الإلكترونية يختلف عن الجاني في غيرها من الجرائم فقد يكون ذو خبرة كافية في مجال استخدام التقنيات الحديثة وقد يكون يتمتع بمستوى عادي من الخبرة الفنية بالتقنية المعلوماتية، فإن السلوك الجرمي الذي سيصدر منه في مجال ارتكاب الجريمة الإلكترونية حتماً سيختلف عن الجاني التقليدي في الجرائم التقليدية، وأيضاً مسرح الجريمة الإلكترونية الذي يرتكب فيه السلوك الإجرامي يختلف عن المسرح الجريمة التقليدية (الطحطاوي، 2015: 53).

ومن الأمثلة على السلوك الاجرامي الذي تتحقق به جرائم إلكترونية وهي كثيرة، منها جريمة الإرهاب الإلكتروني فإن السلوك الجرمي هنا هو إطلاق صفحات أو مواقع تدعو وتحرض على الانضمام لمثل هذه الجماعات، أو مثلاً تبيين كيفية صنع قنابل، أو قد تكون عن طريق البريد الإلكتروني، حيث يقوم المخترق بإرسال رسالة إلى المجني عليه فيقوم بفتحها فإذا بها تحتوي على ملفات تحمل برنامج الاختراق ضمنها ملف التجسس، وقد يتحقق السلوك في الدخول العمدي غير المشروع على نظم معالجة البيانات ذات العلاقة بالتجارة الإلكترونية والتلاعب فيها، مما سبق نلاحظ بأن السلوك الإجرامي في جرائم الإنترنت لم يرد على سبيل الحصر مثله مثل السلوك الذي تتحقق به الجرائم الأخرى، وعليه فإن أي سلوك إجرامي يتناسب مع طبيعة الحق المعتدى عليه يمكن أن تتحقق به جريمة إلكترونية (خلف، 2009: 8).

ب. **علاقة السببية:** ليكتمل الركن المادي في أي جريمة يجب أن تتحقق علاقة السببية بين سلوك الجاني وبين النتيجة التي ترتبت على فعله، أي أن النتيجة الجرمية سببها سلوك الجاني، وقد نستطيع تطبيق ذات القواعد العامة المطبقة على الجرائم العادية على الجرائم الإلكترونية فيما يتعلق بعلاقة السببية إذا انطبقت عليها، ففي جريمة سرقة المعلومات، إن اختلاس المعلومات يتحقق بالنشاط المادي الصادر عن الجاني سواء بتشغيله للجهاز للحصول على المعلومة أو البرنامج أو الاستحواذ عليها، وهو ليس بحاجة لاستعمال العنف لانتزاع الشيء، يكفي تشغيل الجهاز لاختلاس المعلومة لتتحقق النتيجة بحصوله عليها، فرابطة السببية إذن متوافرة بين نشاطه المادي والنتيجة الإجرامية (الطحطاوي، 2015: 54).

ت. **النتيجة الجرمية:** وهي التي وقعت بسبب ارتكاب الفعل، فلا يكفي قيام الجاني بسلوكه الإجرامي مهما بلغت جسامته، بل لا بد من أن يترتب عن هذا السلوك نتيجة، وهي التغيير الذي يحدث في العالم الخارجي كأثر للفعل الجرمي أو الأثر الذي يحدثه السلوك الجرمي والذي يرتب عليه المشرع أحكام قانونية، والنتيجة الضارة لها مدلولان أحدهما المدلول المادي والآخر هو المدلول القانوني، أما المدلول المادي فهو يعني الآثار التي تحدثها الجريمة في العالم الخارجي والمدلول القانوني يكون بأن يترتب على وقوعها عقوبة على سبيل المثال القيام باختراق بيانات شخص معين وأخذ صور شخصة خاصة به والقيام بنشرها بقصد التشهير به مما يؤدي إلى الإضرار بسمعته وعمله وحياته الاجتماعية، فالفعل حدت من خلال الوسائل التكنولوجية إلى أن الأثر كان على حياته الواقعية ومحيطه الاجتماعي، وهذا الفعل مجرم بنصوص قانونية فبهذا يكون اكتمل الركن المادي للجريمة.

ونظراً لأن الجرائم الإلكترونية تعتبر من الجرائم المستحدثة فمن الصعب تحديد أركانها بشكل واضح وجازم كونها تتطور بشكل مستمر وسريع فالنتيجة الجرمية تشكل مشكلة في موضوع التوقيت والاختصاص، بحيث يمكن أن تدخل دولتين وثلاثة في ذات الجريمة، مما يشكل التنازع في تطبيق القوانين، بالتالي عدم وجود قانون خاص أو دولي يجاري حداثتها يشكل عائق أمام اكتشافها ومعاقبة مرتكبيها (خلف، 2009: 8).

2- **الركن المعنوي:** يتمثل الركن المعنوي بالقصد الجرمي وهو ما يعني العلم بعناصر الجريمة، بالتالي فإن هذا الركن يتكون من علم وإرادة، وأما العلم فهو فهم الأحداث والأمور كما هي في الواقع أي أنه يسبق الإرادة، وأما الإرادة فهي التوجه لفعل ولتحقيق الفعل الجرمي (المضحكي، 2014: 91)، فعلى سبيل المثال من يقوم بالسب أو القذف أو السرقة أو التجسس أو إتلاف عبر الإنترنت بلا شك فإنه لديه العلم والإرادة بما يقوم به، وهما عنصرا القصد الجنائي بمعنى

آخر (الركن المعنوي للجريمة) وقد ينتفي القصد الجرمي للشخص مثل قيام شخص بفتح روابط أو مواقع دون أخذ الحيطة والحذر مما أدى لتدمير النظام الإلكتروني لمكان عمله وأدى ذلك لتسريب بيانات مهمة على أن يثبت أن هذا السلوك قد صدر منه عن طريف الخطأ دون قصد أو نية إجرامية (خلف، 2009: 8).

3- **الركن الشرعي (القانوني):** إن الركن الشرعي يعني السند القانوني لتجريم الفعل وذلك تطبيقاً لمبدأ الشرعية بأن "لا جريمة ولا عقوبة إلا بنص" وإعمالاً لذلك فإنه من غير الممكن بحال الاجتهاد من القاضي الجزائي، بمعنى لا يجوز القياس في التجريم، والجرائم الإلكترونية حديثة وذات تقنية عالية، ووضع نصوص خاصة بها ليس بالأمر السهل، وعلى الرغم من ذلك إلا أن الدول سعت لوضع قوانين لمثل هذه الجرائم (عمايرة، 2023: 26) وقد عالج المشرع الفلسطيني الجرائم الإلكترونية من خلال سن قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته لمزيد من التوضيح حول القرار بقانون أنظر/ي ملحق رقم (8).

6.4.2 أطراف الجريمة الإلكترونية:

تتكون الجريمة الإلكترونية من ثلاثة أطراف رئيسية هي:

أولاً: الجاني (المجرم المعلوماتي):

أضافت المعلوماتية الكثير من الجوانب الإيجابية إلى حياتنا إلا أنها في المقابل جلبت معها نسلاً جديداً من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية.

تعريف المجرم المعلوماتي: هناك العديد من التعريفات التي تناولت مفهوم المجرم المعلوماتي منها:

- تعريف (موسى، 2009: 143) بأنه "الشخص الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسب الآلي الإلكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه".
- كما تم تعريفه بأنه "المجرم الذي له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو الامتناع عنه، مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محلياً أو دولياً" (خليلي، 2017: 401).

- كماعرفته (مرداوي، 2021: 30) بأنه "الشخص الذي قام بارتكاب السلوك الجرمي الإلكتروني، وهو على دراية وخبرة وعلم بشؤون الحاسوب".

نستنتج من التعريفات السابقة أنها ركزت على أن المجرم المعلوماتي شخص يمتلك مهارات تقنية تمكنه من إتيان فعل عبر استخدام نظام الحاسوب الآلي، ولكن نظراً للتطور المتسارع لاستخدام وسائل تكنولوجيا المعلومات والاتصالات أصبح ارتكاب الجرائم الإلكترونية من أشخاص عاديين وقد لا يجيدون القراءة والكتابة ولكنهم قد يمارسون أفعالاً بسيطة عبر الفضاء الإلكتروني تشكل جرائم إلكترونية كالإزعاج عبر تطبيقات التواصل الاجتماعي.

أنماط المجرم المعلوماتي:

يصعب وضع تصنيف ثابت لأنماط مجرمي المعلوماتية وذلك يعود إلى التطور والتغيير السريع والمستمر في أنماط الجريمة الإلكترونية وصورها، ولكن يمكن لنا وفقاً لما توصلت له الدراسات والأبحاث التي تناولت مجرمي المعلوماتية أن نبين بعض هذه الأنماط لهؤلاء المجرمين، لكن لا بد من الإشارة أولاً إلى أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة بل يمكن أن يكون المجرم الواحد مزيجاً من لأكثر من فئة، ومنها:

- **التصنيف حسب صفات مرتكبيها:** يمكن تصنيف المجرمين المعلوماتيين حسب صفاتهم وفقاً لما ورد في (خلدون، 2012: 81) إلى:

أ. **الهواة:** وهم شباب فضوليين ارتكابهم للجريمة الإلكترونية بمثابة تسلية ولا تشكل أي خطورة.

ب. **المخادعون:** وهم أشخاص يتمتعون بقدرات عالية وكفاءات لأنهم متخصصين في المعلوماتية وتنصب جرائمهم على الأموال والتلاعب في حسابات المصارف والمؤسسات المالية الاقتصادية ولهم قدرة هائلة في إخفاء الأدلة.

ج. **الجواسيس:** مهمتهم استخبارية لجمع المعلومات لمصلحة دولهم أو بعض الأشخاص أو الشركات فلهم كفاءة عالية في تشغيل الحاسب الآلي وإخفاء الأدلة.

- **في حين صنفهم (الردفاني، 2014: 165) إلى الفئات الآتية:**

أ. **فئة العاملون على أجهزة الحاسبات الآلية في منازلهم:** نظراً لسهولة اتصالهم بدون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.

ب. **فئة الموظفون الساخطون على منظماتهم التي يعملون فيها:** إن بعدهم عن مكان عملهم بعد انتهاء مواعيد العمل يساعدهم على تخريب المواقع الخاصة بالمنظمة على شبكة الإنترنت أو إتلافها أو التشهير حتى بالمنظمة.

ت. **فئة المتسللين (الهاكر):** منهم الهواة أو العابثون بقصد التسلية، وهناك المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته، وتقع أغلب جرائم الإنترنت حالياً تحت هذه الفئة بقسميها.

ث. **فئة العاملون في الجريمة المنظمة:** مثل عصابات سرقة السيارات حيث يحددون بواسطة شبكة الإنترنت أسعار قطع الغيار المسروقة، ومن ثم يبيعونها في الأسواق الأعلى سعراً.

خصائص المجرم المعلوماتي:

هناك عدة خصائص يتميز بها المجرم المعلوماتي تميزه عن غيره من المجرمين العاديين، يمكن حصر هذه الخصائص في الآتي:

- **السن:** تتراوح أعمار مرتكبي جرائم الإنترنت عادة ما بين 18 و 46 سنة والمتوسط العمري لهؤلاء هو 25 سنة (جواد ،2015: 30).

- **مجرم متخصص:** فهو محترف في الجرائم الإلكترونية له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور والشيفرات، فشعوره بالأمن نتيجة الثقة الزائدة بالنفس وجهل الكثير بعلوم وتقنيات الحاسب الآلي لا سيما استخدام الإنترنت يغريه بإمكانية ارتكاب الجريمة دون أن يتم اكتشافها فقدراته الفنية في التعامل مع الحاسوب تمكنه من ارتكاب الجريمة المعلوماتية بسهولة وفي وقت قصير (ذياب وبوترعة، 2020: 13).

- **مجرم ذكي:** إن خبرة ومعرفة المجرم المعلوماتي في هذا المجال تخوله إمكانيات هامة تجاوزاً لأي مفاجأة قد تفشل مخططاته حيث يستطيع أن يكون تصوراً شاملاً لجريمته، فيعمل على تنقيب أي أنظمة مماثلة لتلك المستهدفة حتى تتم جريمته هذه في مستويات عالية من الدقة والإتقان، الأمر الذي يثبت إمتلاكه قدرات وطاقات عقلية لا يستهان بها فهو قادر على تحدي معظم العقبات التي يواجهها أثناء ارتكابه الجريمة، حيث يمتلك هذا المجرم من المهارات ما تؤهله للقيام بتعديل وتطوير الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتابع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب فالإجرام المعلوماتي هو إجرام ذكاء (المومني، 2010: 77).

- **مجرم غير عنيف:** إن الإجرام الإلكتروني إجرام ناعم كون المجرم المعلوماتي يلجأ إلى الحيلة عند ارتكابه الجرائم الإلكترونية على العكس من المجرم التقليدي الذي يميل إلى العنف عند تنفيذ جريمته، فالجرائم الإلكترونية سواء تلك التي ترتكب بشكل فردي أو ضمن عصابات منظمة هي جرائم غير عنيفة (شهوان، 2018: 13).

- **مجرم متكيف اجتماعياً:** فهو شخص قادر على التواصل مع مجتمعه ومتوافق معه وغير منبوذ، يمارس حياته اليومية كسائر أفراد المجتمع، دون قلق أو حيرة فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به وهو قادر على التوافق والتصالح مع الغير بل إن بعضهم يتمتع بثقة كبيرة داخل مجال العمل، فهذه الخاصية تعطي للمجرم المعلوماتي الشعور بالثقة في محيطه وتكرس إحساسه بأنه ليس محل شبهة الأمر الذي قد يدفعه إلى التمادي في ارتكاب جرائمه (المليحي، 2019: 156).

- **العود في هذه الجرائم:** يعود معظم المجرمين في الجرائم الإلكترونية لارتكاب جرائمهم مرة أخرى في مجال الحاسوب، فهم يوظفون مهاراتهم في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به، إما لشغفهم بالمعلومات أو حصولهم على الأرباح أو إضراراً بالغير إلى جانب رغبته في تجاوز الأخطاء والثغرات التي أدت وساعدت المحققين إلى التعرف عليه وكشفه (المعمري، 2013: 253).

- **المجرم المعلوماتي يبرر ارتكاب الجريمة:** يوجد شعور لدى مرتكبي الجريمة الإلكترونية أن ما يقومون به لا يدخل في عداد الجرائم فهم يعتبرونها أفعالاً مباحة لا يستحقون العقاب عليها، وهو سلوك شائع ومقبول في أوساط هذه الفئة، تحديداً وأنهم يمارسون هذه الأفعال لتحقيق الربح المادي أو للتسلية في أوقات الفراغ، ومما لا شك فيه أن التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد في إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل حيث يُفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غير أخلاقي وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصادياً تحمل نتائج تلاعبهم، لكن هذا لا ينفي وجود فئة من المجرمين المعلوماتيين على علم وإدراك تام بأن ما يقترفونه جريمة وأن لديهم قصد جنائي واتجاه إجرامي خطير لارتكاب هذه الجرائم (المليحي، 2019: 156).

نستنتج مما سبق أن مرتكبي الجرائم الإلكترونية لا يمكن حصرهم بصنف أو خصائص معينه فهم يتطورون بتطور الوسائل التكنولوجية وتتطور أهدافهم ووسائلهم في ارتكاب الجريمة، فهم يسعون لكل ما هو حديث من هذه الوسائل من أجل تحقيق غاياتهم حتى ولو كانت مخالفة للقانون، كما أنه قد

يرتكب هذه الجرائم أشخاص عاديين غير محترفين بتكنولوجيا المعلومات ولا يمتلكون أية خصائص معينة كجرائم السب والشتم .

ثانياً: المجني عليه:

تتحقق النتيجة الجرمية للجرائم الإلكترونية على نوعين من الأشخاص ذوي صفات مختلفة قد بينتهم (مرداوي، 2021: 31) على النحو الآتي:

- **أشخاص لهم صفة معنوية:** كالمؤسسات في القطاعين العام والخاص (الشركات، البنوك، الدوائر الحكومية) والشخصيات الاعتبارية التي تعتمد في عملها على الحاسوب.
- **أشخاص لهم صفات طبيعية:** كالأفراد الذين يستخدمون الحاسوب في ممارسة أعمالهم أو للترفيه أو غيرها من الأنشطة المتعددة.

مما سبق نلاحظ أن تصنيفات مرداوي للمجني عليهم تضمنت عاملاً مشتركاً سواء كان الشخص طبيعي أو معنوي وهو اشتراكهم في استخدام أجهزة الحاسوب وهذا المعيار لم يعد عملي في يومنا هذا مع انتشار الجرائم الإلكترونية بصور وأشكال متعددة حتى باتت معظم الجرائم التقليدية ترتكب بصورة إلكترونية، فلا يشترط أن يكون المجني عليه مستخدماً للحاسوب أو وسائل الاتصال فعلى سبيل المثال قد يتعرض شخص للتشهير عبر مواقع التواصل الاجتماعي رغم عدم استخدامه لها.

ثالثاً: محل الجريمة:

هذه الجرائم إما أن تقع على الحاسوب ذاته وإما بواسطته، وذلك باعتباره محل للجريمة تارة ووسيلة لارتكابها تارة أخرى، فالحاسب الآلي هو أساس التعامل الإلكتروني والمعلوماتي، بالتالي فهو المحور الأساسي الذي تدور حوله وعليه الجرائم الالكترونية وذلك من أجل استهداف إما:

- **المعلومات:** ونعني بها أن الجاني يقوم بالإطلاع غير المشروع على المعلومات أو الدخول غير المصرح به إلى الشبكات أو قواعد البيانات وكذلك إدخال المعلومات بقصد التزييف والتزوير، وأيضاً مسح المعلومات أو إخفائها أو عدم إدخالها أو تغييرها، إضافة إلى التشفير والكلمات السرية.
- **الأجهزة:** وفيها يتم التعدي على الكيان المادي للحاسوب من خلال الإتلاف أو السرقة أو الاستيلاء، فهنا يستهدف الجاني الجهاز بإرسال فيروسات أو برامج ضارة لتعطيل البرامج الموجودة على الحاسوب (ربايعه، 2016: 8).

- **الأشخاص والجهات:** هنا يكون هدف الجاني من ارتكاب الجريمة الإلكترونية (التهديد، الابتزاز المالي، السرقة، ممارسة الرذيلة) (مرداوي،2021: 31).

وتقسم الجرائم بالنظر إلى نتيجتها إلى: جرائم ضرر وجرائم خطر. حيث تكون جريمة ضرر إذا ترتب على الفعل الإجرامي ضرر فعلي بالمصالح المصانة، كالقتل والسرقة، ففيهما اعتداء على النفس والمال، ويكون الضرر على صور أو أنواع متعددة، تتساوى في القانون كركن في الجريمة، فلا فرق بين ضرر مادي أو معنوي أو بين ضرر فعلي (حال، أو محقق) وآخر محتمل، أو بين ضرر فردي وضرر اجتماعي، أو بين ضرر جسيم وآخر يسير.

وتكون جريمة خطر إذا اكتفى تحقيقها خلق حالة من الخوف، الخطر يلحق بالمصالح المصانة، مثال ذلك: حمل الأسلحة بصورة غير مشروعة، وهذا النوع من الجرائم تأسس على ضرورة حماية المصالح المعتبرة من الخطر الذي يتهددها، بعض النظر عن وقوع ضرر فعلي بالحقوق المحمية.

والجريمة إضرار بحق ومصلحة يحميها القانون، ويكون الضرر في غالبية الجرائم(وهي تامة)– كالقتل والسرقة والضرر والابتزاز الإلكتروني وانتحال الشخصية– نتيجة لازمة مترتبة على الفعل المادي في الجريمة اللاصقة به على نحو لا يمكن فصلها عنه، بحكم طبيعة الأشياء وحقائق الأمور، وقد يكون في جرائم أخرى عنصراً مندمجاً في الركن المعنوي، أي في قصدها الجنائي في الإضرار من عدمه كما في الحال في جرائم التزوير (غباري، 2018: 23– 25).

مما سبق نستنتج أن الجرائم الإلكترونية تعتبر من جرائم الضرر لما يترتب على وقوعها من نتائج لا تؤثر على الفرد فقط بل على المجتمع ككل كجرائم اختراق الأنظمة ونشر الفايروسات وسرقة البيانات بهدف إلحاق ضرر معنوي بهذه المؤسسات وتكبيدها خسائر مادية فادحة إلى جانب نشر بيانات عملائها.

7.4.2 تصنيف الجرائم الإلكترونية:

بسبب تشعب هذه الجرائم وسرعة تطورها كان من الصعب على الباحثين تحديد معيار واحد لتصنيفها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم أو على أساس محل الجريمة، وعلى هذا الأساس قسمها (زبيدي وحفوظة، 2017 : 79) إلى ما يلي:

- **الجرائم الواقعة على الأموال:** مع وجود وسائل الاتصالات وتكنولوجيا المعلومات تحولت المعاملات التجارية التقليدية إلى معاملات تجارية إلكترونية، وما أنجر عنه من تطور في وسائل الدفع، وفي خضم التداول المالي عبر الإنترنت أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم.

- **الجرائم الواقعة على الأشخاص:** مع تطور شبكة الإنترنت أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة مما جعلها عرضة للانتهاك من طرف هؤلاء المجرمين وجعلت سمعة الأفراد مستباحة.

- **الجرائم الواقعة على أمن الدولة:** من أهم الجرائم الإلكترونية التي تهدد أمن الدول ما يلي :

1. **هجمات الجماعات الإرهابية:** استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للإنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها.

2. **الجريمة المنظمة:** استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الاتصال والإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة.

3. **الجرائم الماسة بالأمن الفكري:** وهي من أخطر الجرائم المرتكبة عبر الإنترنت، فوسائل الاتصالات وتكنولوجيا المعلومات توفر بيئة خصبة يمكن من خلالها التأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى.

4. **جريمة التجسس الإلكتروني:** سهلت وسائل الاتصالات وتكنولوجيا المعلومات الأعمال التجسسية بشكل كبير حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي (التجسس العسكري، التجسس السياسي والتجسس الاقتصادي).

وتم تصنيف الجرائم الإلكترونية على المستوى الأوربي من خلال الاتفاقية الأوربية لجرائم الكومبيوتر والإنترنت لعام (2001)، حيث تم العمل في هذه الاتفاقية من أجل وضع إطار عام لتصنيف هذه الجرائم أو على الأقل وضع قائمة الحد الأدنى محل التعاون الدولي في حقل مكافحة الجريمة المعلوماتية، وهو جهد تقوده دول أوروبا لكن بنفس الوقت بمساهمة من قبل بعض الدول الأخرى، فتصنف الجرائم الإلكترونية وفق هذه الاتفاقية كما ورد في (درف، 2006: 310) إلى:

- الجرائم التي تضم المعطيات والنظم التي تستهدف عناصر (السرية والسلامة) وتضم الدخول غير القانوني وتدمير المعطيات واعتراض النظم وإساءة استخدام الأجهزة.

- الجرائم المرتبطة بالحاسب وتضم التزوير والاحتيال المرتبطان بالحاسب.

- الجرائم المرتبطة بالمحتوى وتضم الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.

- جرائم الملكية الفكرية وتضم الجرائم المرتبطة بالاعتداء على حقوق المؤلفين، وقرصنة البرمجيات.

8.4.2 دوافع مرتكبي جرائم الإنترنت:

توجد العديد من الدوافع التي تحرك الجناة تجاه استخدام وسائل الاتصالات وتكنولوجيا المعلومات لارتكاب أفعال وجرائم مختلفة، لعل من أهم تلك الدوافع ما يلي:

- **الدوافع المادية (تحقيق الربح وكسب المال):** تحصيل مكاسب مادية هامة وكبيرة وفي زمن قياسي هو من أكثر الدوافع التي تحرك الجاني لاقتراف الجرائم الإلكترونية، ولتحقيق هذه المآرب يلجأ المجرم المعلوماتي غالباً إلى المساومة على البرامج أو المعلومات المحملة بطريقة الاختلاس من جهاز الحاسوب أو استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية أو التلاعب بالأنظمة المعلوماتية للبنوك والمؤسسات ثم بيع المعلومات التي حصل عليها بأسعار باهضه، أو تحويل الأموال لحساباتهم الشخصية فهذه تعد بعض من الأساليب التي يتبعها المجرم في سبيل تحقيق هدفه، فحجم الربح الكبير الذي يمكن تحقيقه من خلالها يتيح تعزيز كل من تسول له نفسه ارتكاب هذه الجرائم فيسعى لها ويقوم بتطوير نفسه حتى يواكب كل حديث، فهو يغتنم الفرص ويسهر على الاحتراف في عمله حتى يحقق أعلى المكاسب وبأقل جهد، ودون ترك أي أثر يذكر (المومني، 2010: 90).

- **المتعة والتحدي والرغبة في إثبات الذات:** قد يشعر المجرم المعلوماتي بمتعة كبيرة وهو بصدد اختراق الأنظمة الإلكترونية والحواجز الأمنية المحيطة بها رغبة في إثبات الذات، وتحقيق انتصار على تقنية الأنظمة المعلوماتية، وإظهار نوع من التفوق على الوسائل التكنولوجية الحديثة، فالصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنت غالباً هي صورة البطل الذكي الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، من هذه المنطلقات يتسابق الأشخاص لخرق هذه الأنظمة، وقد أطلق على هذه الطائفة من مرتكبي الجرائم الإلكترونية تسمية (الهاكر)، وهم أشخاص متطفلون لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، وإنما ينطلقون من دافع التحدي و إثبات المقدرة (المليحي، 2019: 154).

- **الانتقام:** وهو من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة لأنه غالباً ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها فيأتي هذا الانتقام عادة من قبل الموظفين الحاقدين أو الذين يصيبهم ضرر نتيجة طردهم من وظيفتهم أو إيقاع مسؤولية تأديبية أو جزائية مشينة عليهم أو تخطيهم في الحوافز أو الترقية، وعلى إثر ذلك يقوم بالانتقام من صاحب العمل بإلحاق الضرر به وبعمله من خلال أفعال مختلفة تتعلق بأجهزة

الحاسب الآلي الموجودة داخل العمل، كزرع الفيروسات أو سرقة المعلومات أو الأسرار الخاصة بالمؤسسة وغيرها من الأفعال الانتقامية بنية التهديد وإلحاق الضرر (إيديو، 2020: 347).

- **الدوافع الدينية:** أصحاب هذه الدوافع هم طائفة تدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو دينية، ويرغبون في فرض هذه المعتقدات باللجوء أحياناً إلى النشاط الإجرامي، ويرتكز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه، حيث يقوم هؤلاء ونتيجة عدم اتفاقهم مع المعتقدات والثقافات الأخرى، ونظراً لما يملكون من خبرة في مجال الحاسب الآلي والإنترنت، بخرق الأنظمة الأمنية محاولين الحصول على أية معلومات أو إرسال فيروسات لمحو أو تعطيل الأنظمة، أو يقومون بإرسال الرسائل التي تحتوي على تهديدات أمنية أو غيرها من الأفعال التي ترتبط بالحاسوب، على سبيل المثال مواقع الإلحاد التي تطالب بإلغاء الدين والدولة والأسرة وتحرر الإنسان من الاضطهاد والقيود، إن دفاع هذه الفئات عن أفكارها ومعتقداتها سبب في ارتكاب أفعال إجرامية معلوماتية بهدف الترويج لها وإشعار العالم بوجودها (المليحي، 2019: 155).

- **الدوافع السياسية:** قد تكون السياسات المتبعة في الدولة من الدوافع الرئيسية التي تدفع الأفراد لارتكاب الجرائم الإلكترونية، فطبيعة النظام السياسي السائد في الدولة ودرجة انتماء المواطنين له قد يدفعهم لارتكاب الجرائم الإلكترونية، فالسياسات غير العادلة التي تنتهجها بعض الدول ضد مواطنيها والكبت السياسي الذي تمارسه عليهم، وتهميش دورهم وانتهاك حقوقهم وعدم المساواة في توزيع الثروة الوطنية، والتفاوت في توزيع الخدمات، كل هذا من شأنه أن يولد المنظمات السرية المعارضة للنظام السياسي القائم، وهذا بدوره يولد ردود الأفعال الغاضبة تجاه هذا النظام، قد تكون هذه الأفعال أنشطة تتعلق بممارسة الإرهاب الإلكتروني الذي يعد من أخطر وأشرس الجرائم التي يواجهها العالم حالياً (الفتلاوي، 2016: 11).

نستنتج مما سبق أن الجرائم الإلكترونية ذات تأثير كبير جداً على النظام السياسي القائم فإذا حظي هذا النظام بالدعم والتشجيع على أرض الواقع، فإن ذلك سوف ينعكس على الفضاء الإلكتروني في الدولة، أما إذا حدث العكس فإنهم سوف يلجؤون إلى هذا الفضاء كونه بيئة خصبة لإظهار المعارضة السياسية في ظل ما يتيحه لمستخدميه من إمكانية إخفاء هويتهم بعيداً عن أنظار أجهزة الدولة، والدليل على ذلك الثورات العربية التي كانت شرارتها تنطلق عبر مواقع التواصل الاجتماعي سواء عبر الترويج لأفكار سياسية معارضة أو لحشد الحشود وتنفيذ نشاطات معارضة لسياسة الدولة.

- **حب الاكتشاف والتعلم:** إن حب الاستكشاف وشغف المعرفة بكل ما يتعلق بأنظمة الحاسوب والشبكات الإلكترونية، قد تكون دافع وراء ارتكاب الجرائم الإلكترونية، فالرغبة الجامحة في الحصول على الجديد من المعلومات المتسارعة النمو والتطور، تجعل بعض الأشخاص يعملون في إطار الجماعة وتبادل الخبرات على اكتشاف الأنظمة وقد كرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية فقد يصل البعض إلى حد الإدمان والانعزال عن العالم الخارجي من أجل مواكبة كل ما هو جديد في هذه التقنيات (خلدون، 2012: 119).

- **الدوافع الاقتصادية:** متمثلة بالسعي للحصول على المكاسب المادية من أقوى العوامل المساهمة في امتهان الجريمة، فهذه العوامل دفعت الأفراد إلى استغلال الموارد التكنولوجية التي في متناول أيديهم لتحقيق مكاسب اقتصادية حتى ولو كان بالطرق غير المشروعة من خلال الاحتيال والتزوير والسرقة الإلكترونية في سبيل تحسين أوضاعهم الاقتصادية حتى إن البعض منهم يرتكب الجرائم الإلكترونية لأنها مصدر دخله الأساسي (الفتلاوي، 2016: 12).

- **دافع التهديد والمنافسة:** لا يقتصر ارتكاب الجرائم الإلكترونية على الأفراد فحسب بل ترتكب من قبل الدول أيضاً مثلما يحصل في المنافسة التجارية أو الهجوم العسكري بين هذه الدول فالمجرم هنا يسعى للتجسس لمحاولة اكتشاف أسرار المنافسين وتهديدهم، فالدافع هنا يكون نتيجة الوقوع تحت تهديد ضغط الغير (ذياب وبوترعة، 2020: 15).

- **الدوافع الاجتماعية:** هناك العديد من المبررات والأسباب الاجتماعية الدافعة لارتكاب الجرائم الإلكترونية لعل من أهمها غياب نظام العدالة الاجتماعية في المجتمع، وانتشار الفقر والبطالة والذي بدوره ساعد في شيوع الجريمة في المجتمع، فوجود فجوة في الطبقات الاجتماعية بين فئات المجتمع ووجود مواقع التواصل الاجتماعي التي عززت إظهار الأشخاص الذين يمتلكون الأموال ويتفاخرون بها حتى ولو كان هذا عكس واقعهم الحقيقي، فهذا دفع الأشخاص من ذوي الدخل المحدود وعندهم عدم رضا عن وضعهم المادي ويمتلكون مهارات وقدرات استخدام الوسائل التكنولوجية لارتكاب الجرائم الإلكترونية، من خلال عمليات الاختراق وسرقة بطاقات الائتمان، واستخدامها للحصول على الأموال، أو بابتزاز الأشخاص المجني عليهم، باختراق حساباتهم وتهديدهم بنشر معلوماتهم على مواقع التواصل الاجتماعي للحصول على المال وغيره حسب الوضع الجتماعي والاقتصادي للضحية (مرداوي، 2021: 36).

مما سبق نرى أن الدوافع وراء ارتكاب الجرائم الإلكترونية كثيرة ولا تنحصر في ما تم ذكره مسبقاً بل هناك دوافع تتعلق بالجوانب السيكولوجية لمجرمي الحاسوب والإنترنت، فهم غالباً يتملكهم عدم الشعور

بالمسؤولية حول اقترافهم لهذه الجرائم، وكذلك شعورهم بعدم استحقاقهم للعقاب عن هذه الأفعال، فحدود الشر والخير متداخلة لديهم، كما أن هنالك دوافع نفسية مرضية متعلقة بالجاني وما تلقاه منذ صغره من تربية قاسية وسيئة المستوى أو عنف أسري وغيرها من العوامل التي قد تؤدي لانحرافه عن المسلكيات الصحيحة فلا يمكننا تحديد سبب مانع جامع يدفع الأفراد لارتكاب هذه الجرائم.

9.4.2 مبررات الحماية الجنائية للتقنية المعلوماتية:

انتشرت التقنيات التكنولوجية في جميع مناحي الحياة فأصبحت هناك ضرورة ملحة تستدعي إعادة النظر في مجال توسعها وطرق استغلالها مع شيوعها في الاستخدام بين الجهات والمؤسسات والأفراد والدول الذي أضاف بعداً جديداً للجريمة الإلكترونية، موجباً على جميع الدول العربية والغربية استحداث قوانين لمواجهتها.

فيعد الإثبات الجنائي بالأدلة الرقمية من أبرز تطورات العصر الحديث في كافة النظم القانونية، تلك التطورات التي جاءت لتلائم الثورة المعلوماتية والتكنولوجية والتقنية في عصرنا الحالي، والتي تطور معها الفكر الإجرامي، إن ظهور نوع جديد من الجرائم يعرف بالجرائم الإلكترونية أو الجرائم الرقمية، ألقى على عاتق القائمين على مكافحة الجريمة في الدولة عبئاً شديداً، ومهاماً كثيرة تفوق القدرات المتاحة لهم وفق أسس وقواعد إجراءات البحث الجنائي والإثبات الجنائي التقليدي، نظراً لعدم كفاية وملائمة هذه النظم التقليدية في إثبات تلك الجرائم سواء من الناحيتين القانونية أو التقنية، حيث كان حتمياً على المشرع أن يستحدث من التشريعات ما يلائم هذا النوع من الجرائم، فضلاً عن إنشاء أجهزة فنية متخصصة يناط بها عملية الإثبات العلمي الفني لهذه الجرائم (الطحطاوي، 2015: 4).

انطلاقاً من مبدأ شرعية العقوبة والجريمة فإن مبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوفر النص القانوني فلا جريمة ولا عقوبة إلا بنص قانوني، ومتى ما انتفى النص على تجريم مثل هذه الأفعال التي لا تطالها النصوص تنتفي المسؤولية وهذا من أول الأسباب الداعية إلى استحداث قانون يتعلق بالجرائم الإلكترونية (المضحكي، 2014: 32)، أما المبرر الثاني فيتمثل في الحاجة إلى سن تشريعات كفيلة لتنظيم كل ما يتعلق بالتقنية المعلوماتية، فحماية المعلومات والوسائل التقنية يهدف بالدرجة الأولى لحماية الحياة الخاصة لأفراد المجتمع وصولاً لحماية المعلومات الماسة بأمن الدولة الداخلي والخارجي واستقرارها كون الوسائل التقنية شملت جميع مجالات ومناحي الحياة (كلاب وعباسة، 2019: 10)، وهنا يجب علينا أن لا ننسى أهم جانب من تلك الجوانب المتعلق بالخصائص التي تتميز بها هذه الجرائم والتي تتم في بيئة معنوية وذلك على خلاف الجرائم التقليدية مما يثير

بعض الإشكاليات في عملية الإثبات المادي لهذه الجرائم وبحث تحقق أركانها حيث يكون من الصعب إثبات وقوعها ومعاقبة مرتكبيها (المضحكي، 2014: 32).

أما المبرر الآخر فهو يتعلق بالجانب الاقتصادي لأن شبكة الإنترنت هي الأكثر انتشاراً وتواجداً بين أنظمة المعلومات العالمية وتعد الوسيلة الأسرع والأكثر نمواً من الناحية الاقتصادية في الوقت الحالي في الدول، فحماية البرامج والمعلومات الموجودة في التقنيات المعلوماتية من شأنه أن ينعكس على حماية وتحقيق أهداف التنمية الاقتصادية للدول (كلاب وعباسة، 2019: 10).

مما سبق نرى أن جميع الدول في كافة أنحاء العالم كرست تشريعاتها وقوانينها لحماية الحقوق الخاصة بالأفراد والمجتمعات واستخدمت المعاهدات والمواثيق الدولية لحماية هذا الحق بل وعدلت قوانينها الداخلية بما يتناسب مع هذه المعاهدات والاتفاقيات، وفلسطين كغيرها من الدول حيث قامت السلطة الوطنية الفلسطينية بالتوقيع على مجموعة من الاتفاقيات الدولية والإقليمية الثنائية لمواجهة الجرائم العابرة للحدود التي من ضمنها الجرائم الإلكترونية واستخدام الفضاء الإلكتروني العالمي كمسرح لهذه الجرائم، لعل من أهم هذه الاتفاقيات ما يلي:

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة (2010): تكونت من (43) مادة تحدثت عن كل ما يخص الجريمة الإلكترونية والعقوبات ومرتكبيها، وتبادل المجرمين في هذا المجال.
- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لسنة (2010): تضمنت نصاً خاصاً من خلال المادة (21) خاص بالاستعمال غير المشروع لتقنية أنظمة المعلومات، وحددت هذه الاتفاقيات سبل التعاون فيما يتعلق بقضايا الإنترنت وتبادل المعلومات وتسليم المجرمين المتهمين في القضايا الجرمية المتعلقة بالإنترنت.
- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام (2000) التي دخلت حيز النفاذ عام (2003) تضم في عضويتها حوالي (180) دولة، تتألف من (70) مادة، خلت موادها من نصوص صريحة فيما يتعلق بالجرائم الإلكترونية، هذه الاتفاقيات تفرض على دولة فلسطين التزامات من أهمها تعديل القوانين الفلسطينية بما يتماشى مع ما جاء في هذه الاتفاقيات التي أضحت فلسطين طرفاً فيها، كذلك الالتزام بالإجراءات الفنية التي قد تحتويها مثل هذه الاتفاقيات (مرداوي، 2021: 21).

مما سبق نستنتج أن هذا العصر يتميز بالسرعة المذهلة في تطور تقنية المعلومات واعتماد جل المجالات عليها بما تحققه للفرد والمجتمع من توفير الوقت والسرعة في انجاز الأعمال، فهذه المميزات

فرضت على كافة مكونات المجتمع من أفراد ومنظمات عامة وخاصة استخدام تلك التقنية للاستفادة منها إلا أن الشبكة العالمية للمعلومات والتقنية المصاحبة لها من الحاسبات والشبكات الأخرى أصبحت عرضه للاعتداءات، وإن النصوص التقليدية تقف عاجزة أمام هذه الاعتداءات على الخصوصيات الفردية والأسرار، لذا فان الحاجة تغدو ملحة لسد فراغ تشريعي في حماية ما يتم تداوله من معلومات وأسرار على هذه الشبكة، ولحماية الاتصالات والمراسلات بين الناس لجأت العديد من الدول لاستحداث قوانين وطنية ودولية لمواجهة هذه الجريمة كونها أصبحت خطراً ليس على الفرد من خلال انتهاك خصوصيته فقط بل وعلى المجتمع كونها تهدد أمنه واستقراره.

فالمشرع الفلسطيني أصدر القرار بقانون بشأن الجرائم الإلكترونية وتعديلاته بما يتوافق وهذه الاتفاقيات ونظم آلية التعامل معها وفق للمادة (62) لمزيد من التوضيح حول القرار بقانون أنظر/ي للملحق رقم (8)، "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، والمساعدة على التحقيق فيها، وتتبع مرتكبيها، كما وعلى الدولة الأجنبية المعنية الحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعينة بهذا القرار بقانون".

والمادة (63) من ذات القرار والتي نصت على أنه "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. ولا 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".

نستنتج مما سبق أن فلسطين كغيرها من الدول سعت لمواجهة الجرائم الإلكترونية من خلال إصدار قانون لمعاقبة مرتكبيها في حال وقوعها، وهذا القانون يتوافق مع ما ورد في الاتفاقيات الدولية الموقعة عليها، كونه يوجد تعاون دولي يسعى للتصدي للجريمة الإلكترونية، فوسائل الاتصالات وتكنولوجيا

المعلومات جعلت العالم كالقرية الصغيرة وهذه الاتفاقيات جاءت للسيطرة على الجرائم الإلكترونية الناتجة عن هذه الوسائل كون أثرها قد يمتد لعدة دول في آن واحد.

10.4.2 الصعوبات التي تواجه مكافحة الجرائم الإلكترونية:

هناك العديد من الصعوبات التي تواجه مكافحة الجرائم الإلكترونيّة، لعل من أهمها ما يلي:

أولاً: صعوبات على المستوى الوطني:

تتعدد الصعوبات التي تواجه الدور الذي تقوم به مؤسسات الدولة (الأمنية والمدنية) في مكافحة الجرائم الإلكترونية على المستوى الوطني، لعل من أهم هذه الصعوبات ما يلي:

- **صعوبات تتعلق بالجريمة الإلكترونية ذاتها:**

تتمثل أهم الصعوبات التي تتعلق بالجريمة الإلكترونية ذاتها على النحو الآتي كما ذكرها كل من (شهوان، 2018: 22) و (العكلة، 2012: 329) و (الجنابي، 2017: 54) و (مطر، 2018: 400):

1- اختفاء آثار الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه إذ إن جرائم الحاسب الآلي والإنترنت تتميز بأنها جرائم لا يتخلف عنها أية آثار مادية، فالآثار الناتجة عن الجرائم الإلكترونية ليست كالآثار التي تتخلف عن الجرائم التقليدية وذلك لأنها عبارة عن نبضات إلكترونية ولا يترك فيها الجاني آثاراً مادية ملموسة كالبصمات أو الحامض النووي أو سلاح الجريمة أو حتى المسروقات أو الجثة كما هو الحال في الجرائم التقليدية.

2- الضخامة البالغة في المعلومات والبيانات الواجب فحصها وإمكانية خروجها عن نطاق إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية، بالتالي يتعين على المحقق أن يتحلى بالصبر والقدرة على فحص ودراسة هذا الكم الهائل من البيانات والمعلومات المخزنة في النظام المعلوماتي.

3- قلة المتخصصين الجنائيين في مجال الجرائم الإلكترونية مقارنة بحجم المعلومات الرقمية وانتشار التقنية الرقمية، والذي يلزم تطوير التحقيق الجنائي في الجرائم المعلوماتية بشكل مستمر لمتابعة مستجدات التقنية، فهذه الجرائم متجددة باستمرار ومتطورة بحاجة إلى كادر بشري خبير لمواجهتها.

4- ضعف الحماية الأمنية للمعلومات الرقمية الهائلة المتوفرة في فضاء العالم الرقمي نظراً لضخامة المعلومات الرقمية واتساعها فوق إمكانيات الحماية الأمنية المتوفرة.

5- صعوبة اكتشاف الجريمة إلى جانب عدم المعرفة بمكونات الجريمة الإلكترونية من قبل بعض الأطراف المعنية حين وقوعها.

- **صعوبات مرتبطة بالمجني عليه:**

تتمثل هذه الصعوبات كما بينها (الأطرش وعساف، 2019: 637) و (مسمار والكريمين، 2019: 91) و (العكلة، 2012: 329) في:

1- أن الوسائل التكنولوجية تعد مجال استثمار أساسي في يومنا هذا لذا تتسابق الشركات في تبسيط الإجراءات، وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني مما أدى ذلك إلى جعلها فريسة سهلة في أيدي المترصدين من المجرمين التكنولوجيين.

2- عدم إدراك خطورة الجرائم الإلكترونية من قبل المسؤولين بالمؤسسات وإغفال جانب التوعية لإرشاد المستخدمين وتوعيتهم بمخاطر الجرائم الإلكترونية.

3- الامتناع عن الإبلاغ أهم وأخطر المشكلات التي تتعلق بعملية الإبلاغ عن الجرائم الإلكترونية، حيث يمتنع البعض عن إبلاغ السلطات المختصة عن الجرائم التي ارتكبت بحقهم، خاصة المؤسسات والشركات التجارية حتى في الدول المتقدمة من الناحية التقنية والتي ترتفع فيها معدلات هذا النوع من الجرائم، وذلك للتخوف من الآثار التي تنتج عند الكشف عن الجريمة، ويمكن أن يعزى إحجام البعض عن الإبلاغ لعدة أسباب كما بينها (شهوان، 2018: 22) و (العكلة، 2012: 329) على النحو التالي:

أ. يمتنع الأفراد ومسؤولي الشركات الإبلاغ عن الجرائم التي وقعت وتم اكتشافها، نتيجة لعدم إدراكهم لأن مثل هذه الأفعال والهجمات تعتبر جرائم يمكن معاقبة مرتكبيها بموجب التشريعات والأنظمة المطبقة ضمن إقليم الدولة أو المطبقة دولياً.

ب. الحفاظ على سمعة بعض المؤسسات والأفراد، حيث يكون الإحجام عن الإبلاغ عن هذا النوع من الجرائم بسبب عدم رغبة الجهات المتضررة في الظهور بمظهر مشين أمام الآخرين، لأن تلك

الجرائم ارتكبت ضدها ما قد يترك انطباعاً بإهمالها أو قلة خبرتها أو عدم وعيها الأمني ولم تشحذ الاحتياطات اللازمة لحماية معلوماتها.

ت. خوف المؤسسات والشركات التجارية من أن تؤدي أعمال التحقيق التي تقوم بها الشرطة إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية، والواقع أنه في بعض الأحيان قد تتسبب إجراءات التحقيق الخاطئة في خسائر مادية تفوق تلك التي تسبب فيها الجريمة في المقام الأول.

ث. عدم ثقة الضحايا بمقدرة رجال إنفاذ القانون على التعامل مع الجرائم الإلكترونية، بسبب اعتقادهم بعدم توفر الخبرة الفنية لدى رجل الضبط أو المحقق أو عدم توفر المعدات والتجهيزات اللازمة للتحقيق في هذا النوع من الجرائم، بالتالي امتناعهم عن الإبلاغ عن الجريمة في حال اكتشاف حدوثها.

ج. الرغبة في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليده من الآخرين مستقبلاً.

ح. عدم معرفة الضحية بوجود جريمة أصلاً، أو يكون قد اكتشف وقوعها ولكن ولكونها محدودة الأثر لا يتم الإبلاغ عنها.

خ. بعض الجرائم الإلكترونية ترتبط بجرائم أخلاقية، لذا يرفض المجني عليه الإبلاغ عنها تفادياً للفضيحة والعار.

إن ما سبق يؤكد لنا ضرورة قيام الأجهزة المعنية والمختصة بنشر الوعي بين المواطنين حول مخاطر الجرائم الإلكترونية وتأثيراتها السلبية على الأفراد وعلى المجتمع، وضرورة قيام المواطنين بالإبلاغ عن الجرائم الإلكترونية حيث من الممكن أن تقوم الأجهزة الأمنية بنشر الوعي من خلال التعاون مع مؤسسات المجتمع المختلفة سواء كانت حكومية أم مؤسسات المجتمع المدني وزرع الثقة بين المواطن والأجهزة الأمنية وكسر حاجز الخوف عند المواطن وذلك لأهمية الإبلاغ عن الجرائم الإلكترونية.

- **صعوبات مرتبطة بالتحقيق الجنائي:**

تتمثل هذه الصعوبات كما وردت في (الأطرش وعساف، 2019: 639) (العكلة، 2012: 329) بالآتي:

1- صعوبات تتعلق بالنواحي الفنية، كنقص المهارة الفنية المطلوبة للتحقيق في الجرائم الإلكترونية ونقص المهارة في استخدام الحاسب الآلي وشبكة الإنترنت، وعدم توفر المعرفة بأساليب ارتكاب

الجرائم الإلكترونية، وقلة الخبرة في مجال التحقيق فيها، وضعف المعرفة باللغة الإنجليزية، لا سيما وأن العاملين في مجال الحاسب الآلي والإنترنت يستخدمون مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم، فهم خلقوا لغة تواصل خاصة بهم.

2- تعدد المجالات التقنية وتوسعها ودخولها في جميع مناحي الحياة، حيث يحتاج كل نوع من هذه المجالات التقنية إلى إجراءات تحقيق جنائي مختلفة.

3- عدم التنسيق بين المحققين في هيئات التحقيق والعاملين في مجال المعلومات والأنظمة الإلكترونية والحاسوب.

4- بعض هذه الصعوبات ترجع إلى شخصية المحقق مثل ضعف الخبرة في استخدام جهاز الحاسوب والتخوف من استخدام الإنترنت بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الإلكترونية بينما في المقابل نجد أن مرتكبي هذه الجرائم يتابعون كل جديد ويعملون على تطوير سبل إخفاء أدلة جرائمهم.

5- قلة البرامج والأدوات التقنية المخصصة للمساعدة في عملية التحقيق الجنائي مقارنة بالتطور الهائل والسريع للتقنية، وارتفاع تكاليف جمع الأدلة من قبل الخبراء والمختصين بضبط واستخلاص الأدلة الرقمية من الحاسبات وأجهزة تقنية المعلومات، فهم يطلبون مبالغ مالية نظير قيامهم بذلك.

- **صعوبات مرتبطة بالدليل الرقمي:**

تتمثل الصعوبات المرتبطة بالدليل الرقمي كما بينها (شهوان، 2018: 25) و (الجنابي، 2017: 54) على النحو الآتي:

1- عدم وجود دليل مادي واضح: فالدليل المادي الذي يتوفر قد يكون في الغالب أوراق تم الحصول عليها من الطابعة من خلال الجهاز والدليل هنا يكون الأوراق التي تم الحصول عليها وجمعها وليس ما يحتويه الجهاز في حد ذاته، هذا إلى جانب سهولة محو الدليل أو تدميره في زمن قصير، فالجاني يمكنه محو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جداً حيث يصعب على الجهات الأمنية التحقيق وكشف الجريمة.

2- صعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والاطلاع على محتواها أو استنساخها.

3- يخضع المحقق في عمله في هذه الجرائم على اعتبارات المعرفة الأساسية لمفهوم الجرائم الإلكترونية، وهل ما قام به يعد جريمة في قانون الدولة التي ينتمي إليها من عدمه، وكذلك قانون الدولة المتواجد بها المشتبه فيه، الأمر الذي تنشأ عنه مشكلة أخرى، الأمر الذي يتحتم أن يكون لدى المحقق المعرفة الكافية للبدء في التحقيقات، فإذا لم تحدد الجريمة ولم يتم التحفظ على الدليل فإن الأثر المباشر لهذا عدم وجود الجريمة.

- **صعوبات تتمثل في قصور التشريعات الخاصة بمكافحة الجرائم الإلكترونية وضعف إنفاذ القانون:**

من الصعوبات التي تواجه القائمين على مكافحة الجرائم الإلكترونية قصور التشريعات والقوانين التقليدية عن مواجهة هذا النوع من الجرائم المستحدثة، فالتطور التقني المتسارع الكبير في استخدام تقنية الحاسب الآلي وشبكة الإنترنت واكبه انتشار الجرائم التي تستخدم فيها هذه التقنية لأن الجريمة الإلكترونية تتقدم وتنتشر بسرعة كبيرة توازي سرعة تقدم التقنية نفسها مما يؤثر سلباً في محاربة هذه الجرائم ومعاقبة مرتكبيها فهذا التطور الكبير في تقنية الحاسب الآلي والإنترنت لا يواجهه بذات المستوى تطور في النصوص والتشريعات القانونية، وهذا لا يتوقف عند التشريعات وإنما يشمل الجهات المنفذة للقانون وهم الشرطة والنيابة والقضاء وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني كما هو الحال على المستوى الدولي، إن ما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية وضعف الممارسات العدلية والشرطية والقضائية في المحاكمة والتحقيق في الجرائم الإلكترونية وغالباً ما تجد في دول كثيرة تواضع التقنيات التكنولوجية المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية (مسمار والكريمين، 2019: 94).

يمكننا أن نستنتج مما سبق أن الصعوبات التي تواجه التحقيق في الجرائم الإلكترونية كثيرة كونها من الجرائم المستحدثة والغريبة عن المجتمع، وغريبة أيضاً عن الأجهزة الأمنية، لذلك فإن مؤسسات المجتمع بشقيها(الأمني والمدني) بحاجة إلى وقت أكثر لتكون قادرة على التعامل مع هذه الجرائم بالطريقة المناسبة، وذلك من خلال إعداد كادر فني متخصص في التحقيق الجرائم الإلكترونية، وبحاجة أيضاً إلى نشر الوعي لدى المواطنين حول مخاطر الجرائم الإلكترونية إلى جانب ضرورة

تعديل القانون بشكل مستمر ليواكب كل ما هو جديد من هذه الجرائم كونها أصبحت المهدد الأول لأمن وأمان واستقرار واستمرار المجتمعات.

ثانياً: الصعوبات على المستوى الدولي:

إن التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وإن كان يعد مطلباً تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها إلا أن ثمة صعوبات تحول دون تحقيقه في كثير من الأحيان لعل من أهمها ما يلي:

- **عدم وجود نموذج موحد للنشاط الإجرامي:** فعند النظر بتعمق في الأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم الإلكترونية ومنها الجرائم المتعلقة بوسائل الاتصالات وتكنولوجيا المعلومات يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحاً في أحد الأنظمة قد يكون مجرماً وغير مباح في نظام آخر، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والأديان والثقافات من مجتمع إلى آخر، وبالتالي اختلاف السياسات التشريعية من مجتمع إلى آخر (العكلة، 2012: 331).

- **الصعوبات الخاصة بالمساعدات القضائية الدولية وعدم وجود قنوات اتصال:** تتمثل هذه الصعوبات في التباطؤ في الرد، حيث أن الدولة التي تتلقى الطلب غالباً ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب، إلى جانب عدم وجود نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فذلك يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالباً ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين، بالتالي يكون هذا التعاون دون جدوى (عيسى، 2016: 60).

- **تنوع واختلاف النظم القانونية الإجرائية بين الدول:** إن تنوع واختلاف النظم القانونية الإجرائية يتسبب في أن نجد طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها، كما الحال بالنسبة للمراقبة الإلكترونية والتسليم المراقب والعمليات المستترة وغيرها من الإجراءات الشبيهة، وإذا ما اعتبرت طريقة ما من طرق جمع الأدلة والتحقيق أنها قانونية في دولة معينة فإنها قد تكون غير مشروعة في دولة أخرى (العكلة، 2012: 332).

- **مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت:** تعد الجرائم الإلكترونية من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى الدولي ولا توجد أي مشكلة بالنسبة للاختصاص الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانوناً لذلك، لكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية التي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود، ففي هذه الجرائم يرتكب الشخص الفعل في جانب ما من العالم وتظهر النتيجة الإجرامية على الجانب الآخر، فهي عابرة للحدود غير مسيطر عليها، لذلك يجب وضع قانون موحد لجميع دول العالم يخضع له مرتكبي هذه الجرائم (عيسى، 2016: 61).

- **التجريم المزدوج:** يعتبر التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، إلا أنه قد يكون عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم الإلكترونية سيما وأن بعض الدول لا تجرم أنواع معينة من هذه الجرائم، بالإضافة إلى أنه من الصعوبة تحديد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أم لا، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين بالتالي يحول دون جمع الأدلة ومحاكمة مرتكبي الجرائم الإلكترونية وهذا بدوره يترك ثغرة يستغلها مجرمي الإنترنت لارتكاب جرائمهم دون مانع أو رادع (العكلة، 2012: 332).

11.4.2 واقع الجريمة الإلكترونية في فلسطين:

أولاً: الإطار القانوني والمؤسساتي لمكافحة الجريمة الإلكترونية في فسطين:

نظراً للتطور المتسارع والذي شمل كافة مناحي الحياة فأصبحت التكنولوجيا والثورة المعلوماتية جزءاً لا يتجزأ من حياتنا، وبدراسة الوضع الجرمي الحالي والمستقبلي للثورة الرقمية، ثبت عدم وجود حدود للزمان أو المكان أمام ارتكاب الجرائم الإلكترونية، لا بل وتظهر منها أشكال جديدة يتم تنفيذها بأساليب مبتكرة عبر مختلف أجهزة الاتصال الحديثة، نتيجة لذلك صدر قرار بشأن الجرائم الإلكترونية سنة (2017) ولكن لم يمر عام عليه حتى قام المشرع الفلسطيني بإلغائه وأصدر قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية، فالتشريع السابق كان يجرم في الغالب المخالفات ضد الأصول والهويات المادية دون الافتراضية، وبعد اعتراض مؤسسات المجتمع المدني المؤسسات (المدنية والحقوقية) على الثغرات في الأساس القانوني للملاحقة القضائية كونها تمس بالحقوق والحريات للمواطنين تم تداركه في القرار بالقانون رقم (10) لسنة (2018) والذي تم تعديله فيما بعد بالقرار بقانون رقم (38) لسنة (2021م) بتعديل قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم

الإلكترونية وتعديلاته. والذي نص ضمن مواده على تعديل اسم القانون ليصبح قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته لمزيد من التوضيح انظر/ي لملحق رقم (5، 7، 8).

بناء على هذا القانون تم إنشاء وحدة الجرائم الإلكترونية في الشرطة وذلك لإعداد كادر متخصص في الشرطة لتقلي البلاغات والشكاوي المتعلقة بالجرائم الإلكترونية وجمع محاضر الاستدلال للوصول إلى المتهم وإحالته إلى النيابة العامة أصولاً، وتم إنشاء نيابة متحصصة لمكافحة الجرائم الإلكترونية، إذ تم تكليف أعضاء من النيابة العامة كمختصين لمتابعة قضايا الجرائم الإلكترونية وتدريبهم وإعدادهم للتعامل مع هذه الجرائم في كافة النيابات الجزائية في مختلف محافظات الوطن، وتتولى النيابة المختصة كجهة قانونية متابعة الطلبات المتعلقة بالجرائم الإلكترونية بالتعاون مع الشرطة والأجهزة الأمنية ذات الاختصاص بصفتهم مأموري ضبط قضائي وتتولى الاتصال مع الجهات والمؤسسات والشركات المختصة فيما يتعلق بالجرائم الإلكترونية والاتصالات والحصول على الدليل الفني الإلكتروني وربط الجناة فيه (مرداوي، 2021: 38- 39).

ولعل ما يؤكد لنا أن الجرائم الإلكترونية في تزايد مستمر هو نسبة الجرائم الإلكترونية المرتكبة في ظل جائحة كورونا (COVID19) وما ترتب عليها من إجراءات فرضت على كافة الأفراد الحجر المنزلي لحين السيطرة على الوباء فاتجه الأفراد للوسائل التكنولوجية من أجل ملئ وقت فراغهم، الأمر الذي أدى إلى زيادة الجرائم الإلكترونية بسبب ازدياد أعداد المستخدمين للإنترنت ورواد مواقع التواصل الاجتماعي، فكلما زاد عدد المستخدمين للإنترنت زادت الجريمة الإلكترونية.

وفي فلسطين ظهرت هذه الجريمة وارتُكبت بحق عدد من الأشخاص وتنوعت أشكالها بين الابتزاز والتهديد والتشهير والقرصنة والاحتيال المالي وإفساد الرابطة الزوجية وانتحال الشخصية والسب والشتم وسرقة حسابات مواقع التواصل والبريد الإلكتروني ففي إطار متابعة الجريمة الالكترونية فقد تلقت دائرة الجرائم الإلكترونية في المديرية العامة للشرطة منذ بداية عام (2020) وحتى نهايته ورغم الظروف الاستثنائية التي عاشها العالم وفلسطين في مواجهة جائحة كورونا (2720) شكوى سُجلت في المحافظات وعبر الموقع الإلكتروني للشرطة الفلسطينية من خلال الزاوية الخاصة بدائرة الجرائم الإلكترونية ومن خلال أفرع المباحث العامة في مديريات الشرطة بكافة المحافظات مسجلة نسبة ارتفاع بلغت (11.2%) عن عام (2019) والذي تلقت فيه الدائرة (2420) قضية و تمكنت من خلال عملها وأدائها من انجاز (1246) قضية بنسبة انجاز بلغت (59%) توزعت بين الإنجاز المحلي والدولي وقد وصلت نسبة الإنجاز للقضايا على المستوى الدولي (11%) بالتعاون مع المكتب المركزي الوطني للإنتربول في فلسطين وهذه السنة الأولى التي تحصل الدائرة منه على ردود دولية

بهذا المستوى وأصبحت الشرطة الفلسطينية تحصل على ردود من الجهات الدولية، وبمتابعة الشكاوي المقدمة للدائرة تبين بأن الذكور الذين تعرضوا للجرائم الإلكترونية تقدموا ب (1392) شكوى بنسبة (51%) من مجموع القضايا بينما شكلت قضايا النساء ما نسبته (42%) بعدد قضايا (1130) شكوى وكانت نسبة (7%) قضايا مشتركة، هذا ويمكن القول بأن أبرز أنواعها وأكثرها تسجيلاً لدى الدائرة كان التهديد وبلغ عدد هذا النوع من القضايا (599) قضية ومن ثم جاءت القرصنة وبلغ عددها (475) وكان الابتزاز في المرتبة الثالثة وبلغت عدد قضاياه (414) شكوى وكانت قضية إفساد الرابطة الزوجية في المرتبة الأخيرة وبلغت (57) قضية، نستطيع أن نرى الارتفاع في عدد الجرائم الإلكترونية المرتكبة في العام (2020) فكونها كانت الملاذ الوحيد للأفراد في ظل الحجر الصحي إلا أن البعض استغلها من أجل تنفيذ رغباته وأهدافه الإجرامية فخصائص الجريمة الإلكترونية إلى جانب وجود مجرم لديه دافع وغياب الرقابة كون السلطات ومختلف أفراد المجتمع يركزون على الجانب الصحي وتطوراته كل هذه العناصر مجتمعية عززت على ارتكابها، فهذه الأرقام تدل على ازدياد الجرائم الإلكترونية بالرغم من أنها تعتبر من جرائم الأرقام السوداء كونه يوجد جرائم غير مبلغ عنها أو غير مكتشفة أو ظاهرة أصلاً إما لخوف الضحية من الفضيحة أو العار أو لعدم اكتشاف الجريمة أساساً فهذه الجرائم تتطلب توظيف كادر مختص مؤهل للتعامل معها إلى جانب قوانين تواكب حداثة الجريمة وسرعة تطورها (الشرطة الفلسطينية، 2021).

ثانياً: الصعوبات التي تواجه مكافحة الجريمة الإلكترونية وآليات الوقاية المتبعة في فلسطين:

فلسطين كغيرها من الدول تعاني العديد من الصعوبات في مواجهة الجرائم الإلكترونية لعل من أهمها القصور التشريعي وعدم ملائمة نصوص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة (2001) للتحقيق وجمع أدلة الجرائم الإلكترونية، فالقانون المذكور لا يشتمل على نصوص توضح كيفية التعامل مع الأدلة الإلكترونية (الرقمية/ غير المادية) خاصة بما يتعلق بضبطها وتحريزها أو قيمتها في الإثبات، فهذا يشكل عقبة في وجه مأموري الضبط القضائي والنيابة العامة في سبيل القيام بالتحقيق في الجرائم الإلكترونية والذي بدوره يؤثر على قرار الجهات القضائية المختصة بالنظر في هذه القضايا وبالتالي عدم تحقيق العدالة الجنائية، إلى جانب نقص الكفاءات والخبرات اللازمة من أجل مواجهة الجريمة الإلكترونية سواء من ناحية الكادر البشري أو من ناحية المعدات والتجهيزات التي تواكب التطور التكنولوجي المتسارع، وجهل الناس بالجريمة الإلكترونية وامتناعهم عن الإبلاغ عنها خوفاً من الفضيحة (عبد الباقي، 2018: 294).

وبوجود دولة الاحتلال زادت هذه الصعوبات كما على النحو الآتي:

- سيطرة الاحتلال على فضاء الإنترنت والاتصالات مما يشكل معيقاً في متابعة الجرائم الإلكترونية في فلسطين، وخشية الاحتلال في حال سيطرة السلطة على الإنترنت والاتصالات أن تكشف عن أسرارها مما يهدد أمنها.
- تصنيف المناطق الفلسطينية إلى ثلاثة مناطق (A.B.C) حيث إن الاحتلال يسيطر بشكل كامل على مناطق (C) مما يعزز ارتكاب الجرائم في تلك المناطق بسبب ضعف الرقابة عليها من قبل الأجهزة الأمنية الفلسطينية من جهة وعدم التمكن من ممارسة الإجراءات المشروعة (التحري، الضبط، التفتيش) في الكشف عن الجرائم الإلكترونية في حال وقوعها من جهة أخرى، واتخاذ المجرمين هذه المناطق ملاذاً للفرار من وجه العدالة في حال ارتكاب جرائمهم مما يعطل سير العدالة ويعزز انتشار الجريمة.
- الفرق بالإمكانيات والتجهيزات ما بين دولة فلسطين والاحتلال فهو لا يسمح بإدخال أي معدات متطورة تتعارض مع سيطرته التكنولوجية على الفضاء الإلكتروني الفلسطيني.

إن فلسطين كدولة واقعة تحت الاحتلال الإسرائيلي الذي يسطر عليها من كافة جوانب الحياه بما في ذلك فضاء الاتصالات والإنترنت، فقوة البت القويّة لشبكاته في مناطق مختلفة من الأراضي الفلسطينية تدفع المواطنين إلى استخدام شبكاتهم والإحجام عن استخدام الشبكات الفلسطينية مما يجعلهم تحت رقابته وسيطرته بشكل دائم، وكون هذه الشبكات غير خاضعة لسيطرة السلطات الفلسطينية فإن بعض الأشخاص يلجؤون إليها لارتكاب جرائمهم الإلكترونية وذلك لصعوبة اكتشافهم والتعرف عليهم بالتالي لا يتم محاسبتهم، فالاحتلال بذلك وفر بيئة خصبة تعزز ارتكاب هذه الجرائم، هذا إلى جانب إنشائه وحدة متخصصة تحمل مسمى الوحدة رقم (8200) كذراع للتجسس الإلكتروني مهمتها التجسس على المواطنين الفلسطينيين والاطلاع على خصوصياتهم وإسقاطهم من خلال الابتزاز الإلكتروني من أجل تكوين خلايا وعملاء لهم، حيث يقوم الاحتلال بشن حملات اعتقال لكل من يستخدم التكنولوجيا بأي شكل يتعارض مع مصالحه وأهدافه، وبذلك يعد الاحتلال المرتكب الأول للجرائم الإلكترونية كونه مسيطر على الفضاء الإلكتروني الفلسطيني بدون أي وجه قانوني أو حق شرعي (مرداوي، 2021: 14- 37).

مما سبق نستنتج أن وجود الاحتلال يمثل معيق أساسي أمام هيئات العدالة الجنائية الفلسطينة في مواجهة الجرائم الإلكترونية، هذا إلى جانب الانقسام بين الضفة وقطاع غزة والذي يعزز الاحتلال وجوده والذي بدوره يفرض عقبة أمام ملاحقة مرتكبي الجرائم الإلكترونية في حال كونهم من قطاع غزة فهي منطقة غير خاضغة لسيطرة السلطة الفلسطينية، هذا بدوره جعلها بيئة خصبة لاحتواء مرتكبي الجرائم الإلكترونية وخاصة جرائم الابتزاز الإلكتروني فهم يبتزون الضحايا ويجبرونهم على تحويل

مبالغ مالية لهم سواء من خلال محفظة جوال أو من خلال تحويل رصيد عادي أو بأي وسيلة أخرى، فهم متأكدون من عدم إمكانية المجني عليه ملاحقتهم قضائياً، إلى جانب أن العديد من الضحايا الذين يحجمون عن إبلاغ الجهات الرسمية ويلجأون إلى ما يسمى بالهاكرز لحل مشكلاتهم، وللتخلص من مبتزيهم، كون الجاني يكون قد أفهمهم أنه لا يمكن إلقاء القبض عليه ومحاسبته ليجبرهم على الخضوع له.

إلى جانب ضعف التعاون الدولي فيرتكب مجرمون من خارج فلسطين الجرائم الإلكترونية داخل الأراض الفلسطينية إلا أنه يصعب ملاحقتهم قانونياً وبالأخص من دول المغرب العربي والتي تعمل من خلال شبكات إجرامية منظمة على ارتكاب جرائم الابتزاز الإلكتروني ونشر فيديوهات فاضحة للضحايا في حال عدم خضوعهم لها، وما يؤكد ذلك ما ورد في (مردواي، 2021: 90) والتي بينت أن الابتزاز الإلكتروني بجميع أشكاله من أعلى نسبة الجرائم المرتكبة التي تعامل معها جهاز الأمن الوقائي الفلسطيني، لذا فإنه ومن أجل مواجهة الجرائم الإلكترونية في فلسطين فهي تحتاج إلى متابعة أمنية حثيثة من كافة هيئات العدالة الجنائية، مع ضرورة عملها بالشراكة مع مؤسسات المجتمع المدني على توعية المواطنين بماهية الجرائم الإلكترونية وكل المستجدات التي تحصل عليها، وذلك لضمان العمل على الحد من انتشار هذه الجرائم، إلى جانب تعديل القانون بما يواكب حداثتها وتطبيق القانون على من يثبت تورطه بمثل هذه الجرائم.

وقد سعى المشرع الفلسطيني للوقاية من الجرائم الإلكترونية من خلال ما نص عليه في القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته في المادة مادة(59) لمزيد من التوضيح حول القرار بقانون أنظر/ي للملحق رقم (8):

أ. "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 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.

ب. 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".

والمادة (61) ذات القرار: "تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بالآتي:

أ. اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية، ومواقعها الإلكترونية، وشبكاتها المعلوماتية، والبيانات والمعلومات الإلكترونية الخاصة بها.
ب. 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.
ت. الاحتفاظ ببيانات تكنولوجيا المعلومات، ومعلومات المشترك لمدة لا تقل عن (120) يوماً، وتزويد الجهة المختصة بتلك البيانات.
ث. التعاون مع الجهة المختصة لتنفيذ اختصاصاتها".

وأيضاً أكد على أهمية تيسير التعاون الدولي و الإسراع في تبادل المعلومات، بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال، وتفادي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها، وتقديم المساعدة القانونية المتبادلة، وتسليم المجرمين في التحقيقات، وفقاً للقواعد التي يقررها قانون الإجراءات الجزائية النافذ والاتفاقيات الثنائية أو متعددة الأطراف التي تكون الدولة طرفاً فيها.

مما سبق نستنتج أن المشرع الفلسطيني مثلما نص على الإجراءات التي يجب اتباعها عند وقوع الجرائم الإلكترونية لمكافحتها والحد منها، فهو نص على الإجراءات الوقائية وذلك للتصدي لها ومنع وقوعها، فهو يسعى إلى توحيد الجهود بين المؤسسات الرسمية وغير الرسمية في سبيل إدراكه لخطورة هذه الجرائم ومحاولة منه لمجاراة كل التطورات التي تحصل على وسائل تكنولوجيا الاتصالات والمعلومات وآخرها الذكاء الاصطناعي الذي يحاول العالم التأقلم معه وفهم آلية عمله في حين أن البعض الآخر أخذ يسخره لارتكاب نوع جديد من الجرائم الإلكترونية باستخدام هذه التقنيات، فالحكومة الفلسطينية مدركة لأهمية الوسائل التكنولوجية وضرورة توظيفها في كافة جوانب الحياة إلى جانب إدراكها لخطورة الهجمات المترتبة على اختراقها وأثرها الكبير على المجتمع لذا قرر مجلس الوزراء 11/21/ 2022 إنشاء "الهيئة الوطنية للأمن السبيراني" وتكليف فريق حكومي لإعداد مسودات التشريعات والإجراءات اللازمة، كوسيلة لمواجهة الهجمات والاختراقات السبيرانية.

وعليه نصل إلى نتيجة وهي أنّ الجرائم الإلكترونية بخصائصها وطبيعتها تفرض على العاملين في هيئات العدالة الجنائية عدة أدوار لعل من أهمها: دورها في تقديم التوعية المجتمعية بالشراكة مع

مؤسسات الشرطة المجتمعية، ودورها في ملاحقة مرتكبي الجرائم الإلكترونية في حال وقوعها من خلال ممارسة الإجراءات المخولين بها بموجب القانون، إلى جانب دورهم في مساعدة السلطات التشريعية على تحسين القانون الخاص بالجريمة الإلكترونية من خلال تزويدهم بالثغرات القانونية والصعوبات التي تواجههم أثناء تطبيق التشريعات الحالية كون هذه الجرائم متطورة باستمرار نتيجة تطور وحداثة وسائل ارتكابها فنحن بحاجة إلى تشريعات تتناسب وهذا التطور.

5.2 النظريات المفسرة للدراسة:

هناك العديد من النظريات التي فسرت السلوك الإجرامي، لعل من أبزر هذه النظريات نظرية النشاط الرتيب، نظرية الاحتواء، نظرية الضبط الاجتماعي، نظرية الاختيار العقلاني، نظرية تباين الفرصة نظرية الصراع، حيث سيتم ربط واستثمار هذه النظريات في تفسير موضوع الدراسة كما على النحو الآتي:

5.2.1 نظرية النشاط الرتيب:

طرح هذه النظرية كل من فيلسون وكوهن (Larry Cohen And Marcus Felson) في نهاية السبعينيات واشتهرت بالثمانينيات، والتي تقوم على تفسير الجريمة والانحراف الاجتماعي، فلها قدرة على تفسير سلوك المجني عليه، وقدرة على الربط بين البيئة والجريمة، وهذه النظرية امتداد لمدرسة شيكاغو والتي ركزت على عوامل البيئة والتفاعل الاجتماعي في ممارسة الجريمة، فالجريمة هنا مرتبطة بالأنشطة اليومية الإنسانية من خلال التفاعل الاجتماعي، فكلما تغيرت أنماط هذا التفاعل تغيرت معدلات الجرائم، والعالم أموس هاولي (Amos Hawley) ركز على البعد المكاني لكنه تعدى ذلك إلى الزمان سواء على مستوى الساعة أو اليوم واعتبر ذلك من الأنشطة الإنسانية اليومية، وقصد بالنشاط الرتيب أي نشاط من الأنشطة اليومية مثل الذهاب إلى المدرسة أو الجامعة أو النوم أو التسوق، وعليه تتكون هذه النظرية من ثلاث أجزاء هي: المجرم ذو الرغبة (الشخص الراغب بارتكاب الجريمة)، الهدف المناسب وقد يكون هذا الهدف (شخصاً أو شيئاً ما)، غياب الرقابة (ليس المقصود هنا رجال الأمن فقط بل الجيران وربما وسائل الرقابة الإلكترونية والأقفال وغيرها)، إذن الأنشطة الروتينية تجمع بين الجاني والمجني عليه في الزمان والمكان بمعنى وجود المجرم الذي يملك الرغبة والمجني عليه إلى جانب غياب الرقابة، فإذا لم تتوافر الأجزاء الثلاثة معاً تقل احتمالية حدوث الجريمة (نسيب وبوبيدي، 2023: 171).

وبتطبيق نظرية النشاط الرتيب على الجريمة الإلكترونية، نجد أنه لوقوع الجريمة يجب أن تتوافر ثلاثة عناصر: المجرم ذو الرغبة، الهدف المناسب، غياب الرقابة القادرة فمنها نجد أن الفرد يسخر وسائل التكنولوجيا والإنترنت لتحقيق هدفه الإجرامي فمثلاً قد يكون لدى الشخص رغبات جنسية يسعى إلى إشباعها هنا يسعى من أجل البحث عن ضحيته فيتعرف على فتاة عن طريق الإنترنت، قد تكون الفتاة مراهقة فيستغلها ويمارس معها الجنس أو الاغتصاب الإلكتروني من خلال خداعها فهو يستغل غياب رقابة الأهل كونه تعرف على الضحية ونمط حياتها فتمكن من تحقيق هدفه الجرمي، إن المثال السابق يؤكد لنا أن العناصر الثلاث اجتمعت معاً، حيث اجتمع المجرم الذي لديه رغبة جنسية والهدف المناسب والمتمثل في الفتاة المراهقة والعنصر الثالث هو غياب الرقابة من قبل الأهل إلى جانب عدم وجود رقابة على وسائل الإنترنت فكل ذلك ساعد المجرم على ارتكاب السلوك الإجرامي لا بل وسهل من ارتكابه لهذه الجريمة.

هذا إلى جانب أن البعض من المجرمين سخروا الوسائل التكنولوجية من أجل تسهيل عملية ارتكابهم للجرائم التقليدية فبعض الأشخاص ينشرون جميع تحركاتهم وتنقلاتهم أي جدول ممارسة نشاطاتهم اليومية عبر الإنترنت، الأمر الذي ساعد بعض المجرمين لتحقيق دوافعهم الإجرامية فبعض اللصوص استغلوا ذلك فقاموا بسرقة المنازل كونهم متأكدين من عدم وجود أصحابها بداخلها لأنهم وثقوا ذلك من خلال مواقع التواصل الاجتماعي عبر الإنترنت إلى جانب عدم وجود رقابة على هذه المنازل، فذلك عزز وجود العناصر الثلاثة لارتكاب الجريمة وهي المجرم الذي يرغب بالسرقة والهدف المتمثل في المنزل كون أصحابه ليسوا بداخله وعدم اتخاذهم وسائل الحيطة والحذر إلى جانب عدم وجود رقابة من قبل المحيطين فإن ذلك سهل وقوع الفعل الإجرامي.

5.2.2 نظرية نظرية الاحتواء لـ "والتر ركلس" (Walter Reckless, 1961):

تبرر نظرية الاحتواء ميل الإنسان إلى ارتكاب الجرائم بسبب الضغوط التي يواجهها والتي قد تكون داخلية ناتجة عن قوى سيكولوجية وصفها ركلس "بضعف الاحتواء الداخلي للفرد" مثل ضعف الضبط الذاتي وعدم القدرة على تحمل الإحباط، والضغوط الناتجة عن قوى اجتماعية خارجية خارجة عن ذات الفرد، وهو ما وصفه ركلس "بضعف الاحتواء الخارجي للفرد" مثل عدم تعزيز السلوك الجيد والقيم والمعايير وعدم طاعة الأوامر، ووفق هذه النظرية فإن المقصود بضعف الاحتواء الداخلي للفرد هو عجزه على ضبط ذاته وعدم قدرته على التحكم في نزعاته، فيستسلم لرغباته ويسعى إلى إشباعها بطرق منافية للقيم والمعايير الاجتماعية، نتيجة الضغوط النفسية الداخلية كالإحباط والقلق والاغتراب وعقدة النقص تجاه نفسه وتجاه المجتمع والصراع العقلي وغيرها، أما المقصود بضعف الاحتواء الخارجي فهو تعبير عن عدم قدرة الجماعة بنظمها الاجتماعية على أن تجعل لمعاييرها الاجتماعية

أثراً واضحاً على الأفراد، لأن الفرد غالباً ما يكون مدفوعاً للانحراف بفعل قوى اجتماعية ضاغطة خارجة عن نطاق الفرد مثل الفقر والبطالة، صحبة السوء والجماعات المنحرفة وغيرها.

ويؤكد ركلس في هذا الصدد أن وقوع الأفراد ضحية بسبب القوى الداخلية والخارجية، قد يولد لديهم ميلاً جانحاً لخرق القوانين والأعراف الاجتماعية وعدم احترامها (رحال، 2019: 315-316)، وبتطبيق نظرية الاحتواء على الجريمة الإلكترونية، نجد أن الأفراد يرتكبون الجريمة الإلكترونية لنفس الأسباب المذكورة أعلاه والمتمثلة في صعوبة قيام الفرد بضبط ذاته نتيجة ضغوط نفسية داخلية كالقلق والإحباط وضغوط خارجية كالفقر والبطالة وصحبة السوء، فالشباب في المجتمع الفلسطيني يعانون من وضع خاص بسبب الاحتلال وكونهم يعانون من مختلف أنواع الضغوط سواء أكانت الداخلية أو الخارجية فإنهم يتجهون إلى الوسائل التكنولوجية لتفريغ طاقاتهم مما يدفعهم لارتكاب جرائم كونهم يستخدمون هذه الوسائل للهرب من الواقع الذي يعيشونه من خلال استخدامها بالطرق السلبية.

فالأفراد ونتيجة للضغوط التي يعيشونها نتيجة القلق والإحباطات المتكررة إلى جانب الأوضاع الاقتصادية المتردية ونسبة البطالة العالية يلجؤون إلى شبكة الانترنت لتعبئة أوقاتهم إلا أن البعض يستخدمها بالشكل الخاطئ ويلحق الضرر بالآخرين فمنهم من يستهدف الفتيات ويبدأ بتكوين العلاقات إلا أنه وبعد مدة يبدأ بتهديدهن وابتزازهن مقابل مبلغ مالي والعكس صحيح، والبعض الآخر يقوم باختراق حسابات الغير والاطلاع على خصوصياتهم وتهديدهم فهم غير قادرين على ضبط ذاتهم وغير منتمين لمجتمعهم.

5.2.3 نظرية الضبط الاجتماعي (1969):

يعتبر هيرشي (Hirshi) رائد نظرية الضبط الاجتماعي التي تقدم الإجابة حول لماذا نمتثل للقواعد، الإجابة أننا نمتثل لها لأن الضوابط الاجتماعية تمنع ارتكاب الجرائم، فكلما خرقت هذه الضوابط أو ضعفت فالنتيجة هي الانحراف على الأرجح، حيث تحاول نظرية الضبط المجادلة بأن الضوابط الاجتماعية تدفع الناس إلى الامتثال، لكن دون الحاجة إلى أي دافع خاص لانتهاك القانون، هذا أمر طبيعي في ظل غياب الضوابط، حيث لا يشير هذا الافتراض إلى أن الدافع الطبيعي للجريمة يشير إلى نزعات وراثية، بل يشير إلى افتراض عدم وجود اختلاف فردي يدفع إلى ارتكاب الجريمة، فالباعث نحو الجريمة موحد أو موزع بين أفراد المجتمع، وبسبب هذه الدافعية الموحدة للجريمة فإننا سندفع جميعاً ضد قواعد المجتمع ما لم يتم ضبطنا، هكذا يؤكد منظرو الضبط أن الهدف ليس تفسير الجريمة إنما يفترضون أنه باستطاعة كل شخص أن ينتهك القانون إذا كان بإمكانه الإفلات منه، فبدلاً من ذلك فقد شرعوا في التساؤل لماذا لا يرتكب الناس الجريمة؟ (الوريكات، 2013: 264) .

وتقسم وسائل الضبط الاجتماعي إلى نوعين هما: وسائل غير رسمية مثل التنشئة الاجتماعية والتربية والدين والعرف، ووسائل رسمية مثل القانون، ولا شك في أن تلك الوسائل تتكامل مع بعضها البعض لخلق عوامل الضبط الاجتماعي في المجتمع، وإن كانت وسائل الضبط غير الرسمية التي من خلالها يتم التزام الفرد بالأعراف والعادات والتقاليد ومن ثم تعليمها لأفراده موزعة بين هيئات مختلفة وجماعات شتى مثل الأسرة والهيئة الدينية والمجتمع، إلا أن الوسائل الرسمية والمتمثلة في القانون لها هيئات رسمية واضحة ومحددة تسهر عليه وتشرف على مدى تنفيذه، تبدأ هيئات الضبط الرسمي بالهيئة التشريعية التي تسن القانون ثم تمثل الشرطة بعد ذلك واحدة من أهم أجهزة الضبط الاجتماعي التي تسهر على حماية القانون وتنفيذه وعقاب من يخرج عن القانون ويعرض سلامة الأفراد والمجتمع للخطر، وعليه يتمثل الغرض الوظيفي للضبط الاجتماعي في المجتمع فيما يؤدي إليه من توافقات اجتماعية، أو يقوي من عرى التماسك الاجتماعي في المجتمع، وهو ما يعني أيضاً استمرارية تضامن الأفراد، واستمرارية الجماعة في المجتمع، ذلك لأن الضبط الاجتماعي يدعم عوامل حفظ النظام والاستقرار في المجتمع، ومن ثم يحافظ على استمرار المجتمع وبقائه سليماً معافى من أي خلل أو توتر أو انهيار، حيث تعمل قواعد الضبط الاجتماعي على تحقيق العدالة وشيوع الأمن والاستقرار وسلامة المجتمع ومن ثم تساعد على تقدمه ونهضته (درعاوي، 2018: 52).

وبتطبيق نظرية الضبط الاجتماعي على الجريمة الإلكترونية، نجد أنه نظراً لحداثة الوسائل التكنولوجية وصعوبة التعامل معها من قبل الكثير من الأفراد خاصة الفجوة التي سببتها التكنولوجيا في بداية ظهورها بين الآباء والأبناء كون الآباء لا يعرفون الكثير عن استخدام هذه الوسائل والتعامل معها، في حين أن الأبناء يستخدمونها بشتى الطرق وبقدرات عالية، الأمر الذي أدى إلى إضعاف دور الأسرة في الرقابة على سلوكيات أبنائهم والسيطرة عليها، هذا أثر بدوره على وسائل الضبط غير الرسمية المتمثلة بالأسرة هذا من جانب، ومن جانب آخر إن حداثة القانون المتعلق بالجرائم الإلكترونية وتطور أشكالها وأنواعها بشكل مستمر وصعوبة القبض على مرتكبيها كل ذلك أضعف من وسائل الضبط الرسمي فقلل من تأثيره على الأفراد ولم يردعهم عن ارتكاب مثل هذه الجرائم فكون وسائل الضبط الرسمي وغير الرسمي غير مجدية في التعامل مع الجريمة الإلكترونية فإن ذلك سوف يدفع الأفراد إلى ارتكابها بدون أي رادع.

5.2.4 نظرية الاختيار العقلاني (1986-1987):

يعد الباحث كلارك (Klark) مؤسس النظرية التي قدمها للمرة الأولى مع الباحث كورنش (Kornish)، بدأت هذه النظرية بفرضية إن المجرمين يرغبون أو يبحثون في سلوكهم الإجرامي للحصول على فائدة وغنيمة ذات عائد وقيمة عالية وليس فيها خطورة أو صعوبة، هذا يلزمهم باتخاذ القرار المناسب

والصائب من وجهة نظرهم قبل ارتكاب الجريمة، كذلك يلزمهم بالاختيار الدقيق لنوعية الأهداف ذات الحراسة المعدومة أو الضعيفة وذات القيمة الثمينة (المردود النفعي)، بمعنى إذا تحقق هذان الشرطان للجناة يكون منطقياً بالنسبة لهم الإقدام على استغلال هذه الفرصة وارتكاب الفعل الإجرامي دون النظر للأمور والعواقب الأخرى، فيكون الفعل الإجرامي حسب رأي رواد هذه النظرية ليس إلا تفاعلاً بين ردة فعل المجرم بطريقة منطقية ومعقولة من وجهة نظره للفرصة الموجودة والمساعدة، ودافع لأن يرتكب جريمته بناء على التفكير والموازنة بين تأثير وإغراء الفرصة والهدف الإجرامي المتوفر والظروف المحيطة به (نسيب وبوبيدي، 2023: 172).

ترتكز هذه النظرية على مبدأ المنفعة المتوقعة مقابل تنفيذ الفعل، فهذا المبدأ بكل بساطة يعتمد على أن الناس سوف يتخذون قرارات عقلانية قائمة على ما إذا كان الخيار الذي سوف يختارونه سيعظم من مكاسبهم ويقلل من خسائرهم أو العكس، فقرار المجرم في سلوك الطريق الانحرافي متعلق في الفائدة التي سوف يجنيها من اتخاذ هذا الفعل المنحرف كوسيلة لتحقيق منفعته، فالوسائل التكنولوجية جعلت ارتكاب الجريمة أسهل بكثير مما لو أنها حصلت على أرض الواقع وجعلتها ذات مردود مادي كبير قد يؤدي إلى تدمير اقتصاد دول في بعض الأحيان هذا إلى جانب صعوبة الوصول إلى مرتكبيها، فالمجرم كل ما يحتاجه في هذه الجرائم هو جهاز حاسوب يساعده على ارتكاب جريمة عابرة للحدود ذات مردود مالي كبير وبأقل جهد ممكن.

5.2.5 نظرية تباين الفرص (1960):

يرى كلوارد وأوهلن (Richard And Cloand) أن الضغوط تدفع إلى السلوك المنحرف نتيجة للفجوة بين الأهداف والوسائل وأن الكثير من الممارسات الجانحة ما هي إلا وسائل تأقلم للضغوط البنائية وأن التناقض واضح بين الطموحات والقنوات المشروعة وأن جنوح الأحداث شائع في الطبقات الدنيا بسبب انسداد الفرص وأن الفرص قيم متعلمة ومهارات وأن طبيعة القيم والمعرفة هي مفردات الثقافة وهكذا تؤثر الثقافة في سلوك الجنوح الناجم عن الضغوط فعندما تسد الفرص المشروعة وتتوافر الفرص غير المشروعة تقع الجريمة وترى هذه النظرية أن نمط الثقافة الفرعية المنحرفة يعتمد على درجة الاندماج الموجود في المجتمع، فعندما تغلق الفرص والوسائل المشروعة يلجأ بعضهم إلى الفرص غير المشروعة (سلامه، 2023: 409). وبتطبيق نظرية تباين الفرص على الجريمة الإلكترونية نرى أن السلوك المنحرف جاء نتيجة للفجوة بين الأهداف والوسائل وأن الكثير من الممارسات الجانحة ما هي إلا وسائل تأقلم للضغوط البنائية وأن التناقض واضح بين الطموحات والقنوات المشروعة فعندما يكون لدى الأفراد طموحات معينة وهذه الطموحات تتعارض مع الواقع الذي يعيشه الفرد فإنه يلجأ إلى الطرق غير المشروعة لتحقيق هذا الطموح أو الهدف، فقد يكون هدف الشخص تحقيق مكاسب ومرابح

مادية إلا أنه نظراً لارتفاع نسبة البطالة وقلة فرص العمل وانخفاض نسبة الأجور قد يلجأ الفرد إلى تحقيق طموحه بالوسائل غير المشروعة كونه يمتلك خبرات تمكنه من ذلك مثل اختراق الحسابات المالية أو البنوك أو عن طريق تهديد الآخرين وابتزازهم لتحقيق مكاسب مادية.

5.2.6 نظرية الصراع:

في منتصف القرن التاسع عشر، وتحديداً في عام (1848م) شهد العالم نشأة نظرية الصراع الاجتماعي وميلادها على يد الفيلسوف الاقتصادي الألماني كارل ماركس(Karl Marx) الذي يرى أن المجتمع متفق على السلوكيات المرتكبة فيه من حيث الخطأ والصواب وأنه المسؤول عن انحراف الفرد، حيث جاءت لتوضح أن السبب للجريمة يعود لوجود جماعات متعددة داخل المجمع وأن هذه الجماعات متباينة في مصالحها وقيمها الاجتماعية، حيث قسم علماء الاجتماع النظرية الصراعية إلى مجموعتين (المجموعة الصراعية المحافظة والمجموعة الصراعية الرديكالية الماركسية).

تقوم نظريّة الصراع على تحميل المجتمع المسؤوليّة الكاملة عن ارتكاب الفرد للجريمة، كون المجتمع هو المسؤول الأول والأخير عن انحراف الأفراد وذلك بسبب تعدد الجماعات داخله، حيث يرى العالم (Vold، 1958) أن هناك صراع مستمر بين الجماعات الاجتماعية حول المصالح وأن صناعة القوانين لهذا الصراع هي عمليات اجتماعية مستمرة، وأن عدم قدرة الفقراء على التأثير في هذه التشريعات والقوانين يؤدي إلى وصف سلوكياتهم بالمنحرفة لأن هذه السلوكيات لا تتفق مع مصالح وآراء الأقوياء.

وفي هذا السياق أوضح (Bonger، 1916) الذي يعتبر أول من حاول ربط تطبيق النظرية الماركسية في تفسير الجريمة والانحراف أن النظام الرأسمالي يزرع الأنانية في نفس البشر لا حب الإيثار للجماعة وإن التنافس غير العادل حول المصالح التي خلقها الرأسماليون أدى إلى اختلال في الأنظمة الاقتصادية والاجتماعية وظهور حالة من عدم المساواة والظلم والحرمان (الوريكات، 2004: 166 – 170).

مما سبق نستنتج أن الجريمة الإلكترونية وفق النظرية الصراعية مردها إلى أن حالة الصراع تؤدي إلى ظهور حالة من انتشار الحقد والكراهية بين طبقات المجتمع التي تتمثل في الطبقة المالكة والطبقة الفقيرة، فنظراً لما تقوم به الطبقة الحاكمة من سيطرة على خطوط الإنتاج ومنافذ التوزيع حسب ما تراه يخدم مصالحها دون أي مراعاة لباقي طبقات المجتمع، مما يؤدي بالكثير من هذه الطبقات إلى الوقوع في براثين الفقر والبطالة، ولتجنب النزوح نحو الجريمة يجب العمل على إعادة التوزيع العادل لوسائل الإنتاج وتطوير المجتمع والتخلص من الهوة الطبقية ووجود رقابة وهيئات قانونية مستقلة تعمل بنزاهة

وشفافية، فمواقع التواصل الاجتماعي في الوقت الراهن عززت الطبقية، فبعض روادها يعرضون تفاصيل حياتهم على هذه المواقع حيث يعرضون الثراء الفاحش والرفاهية التي يعيشون فيها ويظهرون بصورة تبدو مثالية حتى ولو كان الواقع عكس ذلك، مما يؤدي إلى ردات فعل عكسية عند بعض من يشاهد هذه المواقع الامر الذي قد يدفعهم إلى ارتكاب سلوكيات لا سوية ضد هؤلاء الرواد كتوجيه رسائل تهديدية لهم أو اختراق حساباتهم وغيرها من العديد من السلوكيات غير السوية التي تصنف كجرائم والتي يرتكبها الأفراد نتيجة مرورهم باضطرابات نفسية وحقدهم على المجتمع.

5.2.7 النظرية التحليلية: يعد سيجموند فرويد(1899) من أهم روادها، حيث يعتقد فرويد أنَّ الناس لديهم خبرات حياتية متنوعة، تلك الخبرات تؤثر في عمليات التكيف الاجتماعي، وركّز فرويد على خبرات الطفولة المبكرة، وبالذات السلبية كما رأى أنها تؤثر بشكل غير مباشر على العمليات الباثولوجية، والتي تعد الجريمة أحد تجلياتها. كما يرى فرويد أنَّ الإنسان غير اجتماعي بطبعه، ويتميز بالأنانية, فالإنسان يسعى إلى تحقيق سعادته ولديه نزاعات تحطيمية، وهذه النزاعات في صراع مع التوقعات الاجتماعية والثقافية من أجل البقاء الاجتماعي. وقد افترض فرويد أنَّ هناك ثلاثة نظم تتكون منها الشخصية، وهي: الأول هو الهو ويمثل الأنانية غير العقلانية، ويشمل الدوافع الفطرية الأولية، الثاني هو الأنا ويمثل القوى العقلانية ويتسم بأنه واقعي وشعوري، الثالث الأنا الأعلى التي تمثل معايير المجتمع، القوى الأخلاقية وتشمل مجموعة القيم والعادات والمعايير والمبادئ الأخلاقية. حيث إنَّ السلوك الإنساني يعتمد على التوازن لنسق أو نظام الطبقة النفسية، حيث تعد الأنا الأعلى مسألة مركزية في هذه النظرية، وإنَّ الاضطراب وعدم التوازن بين مكونات الشخصية يؤدي إلى الاضطراب وسوء التكيف والنمو. (الوريكات، 2013: 104).

وبتطبيق النظرية التحليلية على الجريمة الإلكترونية نرى أن السلوك المنحرف جاء نتيجة لوجود رغبات وغرائز عند الفرد يسعى لتحقيقها بطريقة عقلانية يتقبلها المجتمع المحيط به وفقاً للقيم والعادات والتقاليد، إلا أنه وعندما تسيطر الغريزة على الفرد ينشأ صراع عند الإنسان بسبب تصادم الغريزة مع العادات والتقاليد والدين والأخلاق؛ مما يؤدي إلى الانحراف، فيرتكب الفرد الجريمة اللاأخلاقية من خلال الوسائل الإلكترونية فيقوم بإشباع غريزته الجنسية بكل أنانية حتى لو استخدم الابتزاز الإلكتروني فالمهم أنْ يحصل على ما يريد ويشعر بالسعادة والإشباع، فهو يريد أن يشبع رغباته وغريزته ولكن العادات والتقاليد تمنع ذلك إلا من خلال الطريقة الرسمية والمشرروعة وهي الزواج بالتالي يلجأ إلى ممارسة هذه الجرائم بطرق مخفية بحيث يتولد لديه صراع بين الحاجة لإشباع الرغبة وعدم وجود السبل المشروعة لإشباعها ونتيجة لذلك يصبح لديه انحراف بالتالي ارتكاب الجرائم اللاأخلاقية.

6.2 الدراسات السابقة وذات الصلة

يتفق معظم المشتغلين بالبحث العلمي على أن الدراسات السابقة والبحوث تلقي الضوء على القضايا التي يمكن الاستفادة منها في الدراسات أثناء صياغة الفروض وتحديد عينة البحث والأدوات المستخدمة وأساليب المعالجة الإحصائية وتعتبر الدراسات التحليلية النقدية نقطة انطلاق لمعظم البحوث، فمن خلال هذه الدراسات يستطيع الدارس أن يُدخل متغيرات جديدة أو اختبار فرضيات توصل لها الباحثون في مجالات قديمة أو حديثة، والتعرف على نتائج تلك الدراسات ومقارنتها مع الدراسة الحالية، حيث تم العثور على مجموعة من الدراسات السابقة وذات الصلة كما على النحو الآتي:

1.6.2 الدراسات العربية:

1- دراسة عصام ومحمد (2019) بعنوان "معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية"،

هدفت الدراسة إلى التعرف على معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية والمتعلقة بكل من (الجريمة المعلوماتية ذاتها، والمجني عليه، والتحقيق الجنائي) من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية، استخدم الباحثان المنهج الوصفي التحليلي والمقارن واستخدما أداة الاستبانة لجمع المعلومات حيث قاما بتوزيع (150) استبانة على جميع العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية (الشرطة، الأمن الوقائي، المخابرات العامة) تم اختيارهم بطريقة العينة العشوائية المتيسرة وقد تم استرجاع 125 استبيان وهي شكلت العينة النهائية للدراسة، وقد توصلت الدراسة إلى مجموعة من النتائج تتمثل في أن معوقات مكافحة الجرائم المعلوماتية المتعلقة بالجريمة المعلوماتية ذاتها كانت بدرجة كبيرة حيث بلغ الوسط الحسابي لها (3.51) في حين جاءت درجة المعوقات المتعلقة بالمجني عليه بدرجة متوسطة حيث بلغ وسطها الحسابي (3.39)، أما درجة المعوقات المتعلقة بالتحقيق الجنائي كانت كبيرة حيث بلغ الوسط الحسابي الخاص بها (3.55)، وفي ضوء نتائج الدراسة أوصى الباحثان بعدد من التوصيات أبرزها ضرورة تدريب وتأهيل العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية، وضرورة التنسيق بين الأجهزة الأمنية لمكافحة تلك الجرائم، وتشجيع المواطنين على الإبلاغ عن الجرائم المعلوماتية، وزيادة وعي المواطن بمخاطر تلك الجرائم.

2- دراسة النجاجره (2019) بعنوان "خصوصية التحقيق في الجرائم الإلكترونية"،

هدفت هذه الدراسة إلى توضيح المقصود بخصوصية التحقيق في الجرائم الإلكترونية وبيان العقبات والصعوبات التي تواجه التحقيق في الجرائم الإلكترونية وسبل مواجهتها، اتبع الباحث المنهجين الوصفي والتحليلي، وقد توصل الباحث إلى عدد من النتائج أهمها أن الجرائم الإلكترونية غالباً لا تترك أثراً مادياً في مسرح الجريمة كما في الجرائم التقليدية، كما أن مرتكبيها لديهم القدرة على إتلاف وتشويه أو إضاعة الدليل في فترة قصيرة، إضافة إلى أنه يتم إجراء التفتيش والضبط في الجرائم الإلكترونية من خلال مجموعة من الإجراءات التقنية الفنية والتي تحتاج إلى كوادر متخصصة قادرة على تحقيق أهداف التفتيش وضبط الأدلة القانونية الإلكترونية، إضافة إلى أنها توصلت إلى أن التحقيق في الجرائم الإلكترونية يواجه العديد من الصعوبات، وذلك كونها جريمة عابرة للحدود يمكن ارتكابها من خارج إطار الدولة وفي ضوء نتائج الدراسة أوصى الباحث بضرورة إعداد مأموري ضبط قضائي وأعضاء نيابة عامة وقضاة لديهم القدرة الفنية على البحث والتحقيق والمحاكمة في مجال الجرائم الإلكترونية، وضرورة إقرار مادة علمية حول مخاطر الجرائم الإلكترونية ومكافحتها في المدارس والكليات والجامعات، والتوعية الإعلامية المستمرة للمخاطر الناجمة عن سوء استخدام الإنترنت وما قد يترتب على ذلك من أضرار جسيمة على أمن واقتصاد المجتمع.

3- دراسة بغدادي (2018) بعنوان "وسائل البحث والتحري عن الجرائم الإلكترونية"،

هدفت إلى معرفة وسائل البحث والتحري عن الجرائم الإلكترونية، اعتمد الباحث على المنهج الوصفي التحليلي، من خلال تحليل النصوص القانونية ذات الصلة بالمضوع وبيان المبدأ القانوني التي تقوم عليه وجمع الحقائق والبيانات ووصفها في البحث وقد توصل الباحث إلى عدد من النتائج أهمها أنه يوجد اختلاف ملموس في الأدلة لكل من الجرائم التقليدية والجرائم الحديثة، فالجرائم التقليدية يكون الدليل ظاهر للعيان ومحسوس ويمكن كشفها، أما الأدلة في الجرائم الإلكترونية ليست بالصورة المذكورة في الجرائم التقليدية، كما وتوصلت إلى أهمية البحث والتحري عن الجرائم الإلكترونية فمن الواجب على سلطات التحقيق الانتقال فوراً إلى مكان ارتكاب الجريمة والمحافظة على الأدلة والتعامل بحذر شديد معها، وعليه أوصى الباحث بعدد من التوصيات منها من الضروري لجهات التحقيق أن يتوفر لديهم كوادر بشريه قادرة على البحث والتحري في الجرائم الإلكترونية بواسطة الوسائل الحديثة، وضرورة التعاون المشترك من قبل سلطات التحقيق مع مزودي خدمة الاتصال، فهذا يساعد في عملية البحث والتحري عن الجرائم الالكترونية.

4- دراسة عموري (2018) بعنوان "التفتيش في الجرائم الإلكترونية"،

هدفت إلى إظهار خصوصية التفتيش في الجرائم الإلكترونية، وبيان كيفية الحصول على الأدلة الإلكترونية وطرق ضبطها، اتبع الباحث المنهج الوصفي التحليلي المقارن، لتحليل نصوص القانون الخاصة بالتفتيش والضبط في الجرائم الإلكترونية في فلسطين، وقد توصل الباحث إلى عدد من النتائج أهمها أن التفتيش في الجرائم الإلكترونية من أدق وأخطر إجراءات التحقيق، كونه يمس خصوصية الناس بالاطلاع على أسرارهم المخزنة في الوسائل التكنولوجية، والتفتيش بتلك الجرائم بحاجة إلى نظام إجرائي خاص يراعى خصوصيتها، وبحاجة إلى أشخاص مؤهلين ومدربين تدريباً قانونياً وفنياً للتعامل مع وسائل تكنولوجيا المعلومات، وعليه أوصى الباحث بضرورة وجود النص بوضوح على أن تكون مذكرة التفتيش مكتوبة، وتحتوي على جميع بياناتها الإلزامية، والتحديد بوضوح الوسيلة الإلكترونية المراد تفتيشها، ووجود النص بوضوح فيما يخص المكونات غير المادية لوسائل تكنولوجيا المعلومات للتفتيش والضبط، وبيان طرق ضبطها، كما وأوصى بضرورة وجود النص بوضوح فيما يخص حضور المتهم أو الشهود أثناء إجراء التفتيش على وسائل تكنولوجيا المعلومات.

5- دراسة المصري (2017) بعنوان "خصوصية الجرائم المعلوماتية"،

هدفت الدراسة إلى التركيز على خصوصية الجريمة المعلوماتية ومدى اختلافها عن الجريمة التقليدية وإيجاد حلول قانونية لتحقيق التوازن بين مصلحة المجتمع في الاستفادة من الثورة المعلوماتية من جهة، وحق الفرد في حماية خصوصيته من جهة أخرى، وقد اتبعت الباحثة منهجاً تأصيلياً وتحليلياً ومقارناً، وقامت بتحليل النصوص القانونية ذات الصلة، وعرض مواقف عدة دول فيما يخص التشريعات المختلفة لمعالجة الجرائم المعلوماتية، توصلت الدراسة إلى مجموعة من النتائج لعل من أهمها أن الجرائم المعلوماتية أصبحت تمثل أهمية كبرى بالمجتمع خصوصاً بعد ظهور أنماط جديدة منها، وتثير الجرائم المعلوماتية الكثير من الصعوبات في مجال الحصول على الأدلة الجنائية والتحقيق، وذلك لعدم إلمام رجال الشرطة والمحققين بمجالات الحاسب الآلي والإنترنت، وعدم تدريبهم على آليات الوصول إلى الأدلة المعلوماتية والحفاظ عليها من التلف والضياع، ووجود قصور في القواعد والتشريعات الإجرائية الواجب اتباعها في مرحلة التحقيق الابتدائي ومرحلة المحاكمة، وفي ضوء نتائج الدراسة أوصت الباحثة بضرورة قيام المشرعين في الدول المختلفة بإصدار تشريعات خاصة بالجرائم المتعلقة بالحاسب الآلي، وتطوير قواعد الإجراءات الجنائية وقواعد الإثبات، وعقد اتفاقات دولية ثنائية وذلك من أجل تسليم المجرمين المعلوماتيين، وضرورة تأهيل القضاة ورجال الشرطة والمحققين تأهيلاً يستطيع معه كل منهم التعامل مع هذا النوع من الجرائم.

6- دراسة العتيبي (2016) بعنوان "دور التحريات والبحث الجنائي في الكشف عن الجرائم المعلوماتية"

هدفت الدراسة إلى التعرف على دور التحريات والبحث الجنائي في الكشف عن الجرائم المعلوماتية، ومن أجل تحقيق أهداف الدراسة استخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي وقام باستخدام أداة الاستبانة لجمع المعلومات، وقد تمثل مجتمع الدراسة من الضباط العاملين في إدارات التحريات والبحث الجنائي بشرطة منطقة مكة المكرمة والتي بلغ عددهم (48) ضابط، بالإضافة إلى عينة عشوائية عنقودية من القضايا المعلوماتية في شرطة جدة بلغ عددها (150) قضية، توصلت الدراسة إلى مجموعة من النتائج لعل من أهمها موافقة أفراد مجتمع الدراسة على أن دور التحريات في الكشف عن الجرائم المعلوماتية ضعيف، وموافقة أفراد مجتمع الدراسة على أن دور التسجيل الجنائي في الكشف عن الجرائم المعلوماتية جيد، إلى جانب وجود صعوبات تواجه التحريات والبحث الجنائي عند الكشف عن الجرائم المعلوماتية، وعليه أوصت الدراسة بضرورة العمل على تأهيل وتدريب ضباط التحريات والبحث الجنائي، وضرورة دعم الإدارات بضباط حاصلين على مؤهلات علمية في مجال علوم وهندسة الحاسب الآلي وأجهزة تقنية المعلومات وشبكة الاتصالات.

2.6.2 الدراسات الأجنبية:

1- دراسة جراهام وتيرسا وفرانكس (Graham, & Teresa, & Francis, 2020) بعنوان: (Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice)

هدفت إلى المقارنة بين العدالة الإجرائية في الجريمة التقليدية والجريمة الإلكترونية، ولتحقيق هذا الهدف استخدم الباحثون المنهج التحليلي المقارن وأداة الاستبانة واستطلاع اختياري أجاب عنه (534) مستجيباً في جميع أنحاء الولايات المتحدة، وبعد تحليل آراء العينة كشفت النتائج أن العدالة الإجرائية في الجرائم الإلكترونية لا تتضمن فهم نوايا مرتكبي الجرائم الإلكترونية كما هو الحال في إجراءات الجرائم التقليدية، ودور العدالة الإجرائية في تفسير مصادر التباين والاختلاف بينها محدود، وأن إجراءات العدالة لا تتماشى مع مرات الإبلاغ لكل من الجرائم التقليدية والجرائم الإلكترونية، فقد كانت مرات الإبلاغ أعلى بشكل عام قليلاً بالنسبة للحوادث التي وقعت في العالم المادي (الجرائم التقليدية)، على عكس ما يحدث عبر الإنترنت، وتوصلت الدراسة إلى وجود اعتقاد بين الأفراد بأن الشرطة يمكنها تحديد هوية الجاني واعتقاله بنسبة أقل في الجرائم الإلكترونية مقارنة بالجرائم التقليدية، واتضح أيضاً وجود مشكلة في الجرائم الإلكترونية تتعلق بإجراءات العدالة وهي عدم فهم أو تقدير التنبؤات

لسلوكيات ومعتقدات مرتكبي الجرائم الإلكترونية، وتكون ظروف ارتكاب الفعل الجرمي إلكترونياً أكثر غموضاً مقارنة بالواقع المادي والجرائم التقليدية.

2- دراسة كوزياريسك ولي (Koziarski, & Lee, 2020) التي حملت عنوان:
(Connecting evidence-based policing and cybercrime)

وهدفها هو الكشف عن التحديات المختلفة والمرتبطة بمكافحة الجرائم الإلكترونية، ولتحقيق هذا الهدف استخدم الباحثان المنهج التحليلي وأسلوب التحليل القائم على الأدلة، واستخدم الباحثان عينة مكونة من ثلاث شركات تعرضت لجرائم إلكترونية مثل الابتزاز واختراق البيانات، وهي: أماندا تود، وآشلي ماديسون، وتارجت، ولم تحدد الدراسة مكان إجرائها، حيث تم استخدام أداة المقابلة وتحليل البيانات لهذه الشركات الثلاث، وبعد تحليل الآراء والبيانات اتضح وجود تحديات تتعلق بطريقة مكافحة الجريمة الإلكترونية، وتتمثل في الفشل وعدم القدرة في تحسين استجابات إنفاذ القانون للجرائم الإلكترونية، وعدم الربط بين الجرائم الإلكترونية ونماذج التحقيق الشرطية القائمة على الأدلة، وقصور في الربط بين العوامل الاجتماعية والسياسية مع ارتكاب الجرائم الإلكترونية، وأظهرت النتائج أيضاً بوجود احتمالية ضعيفة بأن تؤدي نماذج الشرطة القائمة على الأدلة في مكافحة الجرائم الإلكترونية على تحسين فعالية الأساليب الحالية والمستقبلية لتدريب وتجنيد الضباط على مكافحة الجرائم الإلكترونية، فضلاً عن عدم كفاية استعداد الضباط ووعيهم بالجرائم الإلكترونية المختلفة.

3- دراسة براون (Brown, 2015) بعنوان:
(Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice)

هدفت إلى الكشف عن التبعيات الجنائية والحواجز أمام العدالة عند التحقيق في الجرائم الإلكترونية وملاحقتها، وزيادة الوعي بشأن الثغرات القانونية والتقنيات التمكينية التي تسهل أعمال الجرائم الإلكترونية، وتحديد العوائق النظامية التي تعيق تحقيقات الشرطة والملاحقات القضائية والاستجوابات الجنائية الرقمية، ولتحقيق هذه الأهداف اتبع الباحث المنهج الوصفي المسحي لبيانات ثلاث مراكز شرطة في إستراليا مخصصة للتحقيق في الجرائم الإلكترونية، وتحديداً في ثلاثة دوائر شرطية، وهي: مكتب التحقيقات، وقسم الملاحقات القضائية، وقسم الاستجوابات الجنائية والرقمية، وبعد تحليل البيانات التي حصل عليها الباحث إلى نتائج عدة، أبرزها أن تطور وتقدم التكنولوجيا يعيق قدرة الشرطة على فهم أصول الجريمة، وإن استمرار الجرائم الإلكترونية وانتشارها يتطلب استجابة أوسع لأن التكنولوجيا أصبحت متشابكة بعمق مع نسيج المجتمع، وأنه يدرك المجرمون أن التكنولوجيا تشكل قوة مضاعفة فعالة يمكن إساءة استخدامها لتمكين الأنشطة غير المشروعة، والاستفادة منها لتسهيل

الوصول إلى دائرة عالمية من الضحايا عبر شبكة الإنترنت، وإن مظاهر الجريمة الصادرة عن المجال الإلكتروني من بين التحديات الأكثر صعوبة التي يواجهها العاملون في أنظمة العدالة الجنائية.

4- دراسة ساريكا ومِنّار (Sarika, & Minnaar, 2015) بعنوان:
(Cybercrime investigations: Cyber-processes for detecting of cybercriminal activities, cyber-intelligence and evidence gathering)

هدفت إلى الكشف عن الصعوبات أثناء التحقيقات في الجرائم الإلكترونية التي تشمل أنشطة المجرمين الإلكترونيين، والاستخبارات الإلكترونية وجمع الأدلة، ولتحقيق هذا الهدف استخدمت الدراسة المنهج الوصفي التحليلي وأداة المقابلة مع عدد (18) من موظفي دوائر التحقيق في الجرائم الإلكترونية في جنوب إفريقيا، وعلى المستويين المحلي والدولي، وبعد تحليل آراء العينة اتضح من النتائج وجود صعوبات عدة أثناء التحقيقات في الجرائم الإلكترونية، ومنها اعتماد المجتمعات بشكل متزايد على تكنولوجيات المعلومات غير المركزية التي لا تعرف الحدود أدى إلى أن يكون الفضاء الإلكتروني هدف سهل للمجرمين، إذ لم يعد التشفير مضموناً، والتجارة الإلكترونية غير آمنة، وأصبح التحكم في الفضاء الإلكتروني متاحاً للجميع، ولا يوجد شيء محصن ضد الاختراق مع انهيار نماذج الأمن الإلكتروني القديمة ونتيجة لذلك أصبح تعقب المجرمين الإلكترونيين مهمة صعبة بشكل متزايد لوكالات إنفاذ القانون، فضلاً عن التعقيدات التي يفرضها التحقيق في مثل هذا الطابع المتعدد الاختصاصات، فإن مهمة تحديد هوية المجرمين الإلكترونيين والتحقيق معهم وملاحقتهم قضائياً تعكس تحديات متزايدة تواجه وكالات إنفاذ القانون عبر جميع الحدود في جنوب إفريقيا، سواء المادية أو في الفضاء الإلكتروني، ولا تلبي إجراءات التحقيق التقليدية متطلبات التحديات المرتبطة بالتحقيق في الجرائم الإلكترونية، وفي البيئة الرقمية يتم جمع الأدلة ومعالجتها بشكل مختلف عن الوسائل التقليدية، وأن الإجراءات الفنية للتحقيقات في الجرائم الإلكترونية لا تزال تتطور استجابة للنمو السريع وتغير أسلوب عمل الهجمات الإلكترونية والقرصنة من قبل مجرمي الإنترنت، ويواجه التحقيق في الجرائم الإلكترونية صعوبة أخرى تتمثل في أكثر من إجراء للفحص التكنولوجي البسيط أو استرداد الأدلة الرقمية، حيث يتطلب وجوداً صريحاً لمجموعة متنوعة من الضوابط المتخصصة الفنية وغير الفنية والمساعدات التحقيقية.

5- دراسة الكابي ومكلواج (Alkaabi, & McCullagh, 2011) بعنوان:
(Dealing with the problem of cybercrime)

هدفها الكشف عن المعيقات عند التعامل مع الجرائم الإلكترونية محلياً ودولياً، ولتحقيق هذا الهدف استخدمت الدراسة المنهج التحليلي وأداة تحليل البيانات، إذ تم تحليل بيانات على مستوى العالم صادرة من عدة جهات دولية تتعلق بالجرائم الإلكترونية، منها المعهد الوطني الأمريكي والمعهد الوطني الاسترالي الخاصين بمتابعة الجرائم الإلكترونية، وشركة سيمانتك العالمية، وبعد تحليل بيانات هذه المؤسسات اتضح أن المؤسسات على المستويين الحكومي والخاص تواجه العديد من المشكلات المتعلقة بإجراءات العدالة الجنائية في مواجهة الجرائم الإلكترونية، ومنها غياب تصنيف قانوني شامل ومقبول عالمياً للجرائم الإلكترونية، مما يعيق جهود أكثر من دولة في تحديد اتجاهات الجرائم الإلكترونية ومراقبتها بدقة، ووجود فجوة قانونية على الصعيد الدولي فيما يتصل بالتشريعات الخاصة بالجرائم الإلكترونية، ولا تترابط القوانين المحلية أو تتفق على تعريف الجريمة الإلكترونية على أنها جريمة تستحق العقاب، حيث يتم تعريفها قانونياً بشكل موسع فتكون أية جريمة تُرتكب باستخدام جهاز كمبيوتر أو شبكة أو جهاز مادي، مقابل ذلك، توجد جرائم إلكترونية تتضمن الاحتيال عبر الإنترنت وغسيل الأموال عبر الإنترنت وسرقة الهوية والاستخدامات الإجرامية لاتصالات الإنترنت، لكن هذا التعريف لا يتضمن الجرائم ضد بيانات وأنظمة الكمبيوتر، مما يؤدي عدم متابعة إجراءات الاحتيال.

6- دراسة مارتن ورايس (Martin, & Rice, 2011) بعنوان:
(Cybercrime: Understanding and addressing the concerns of stakeholders)

تناولت الجرائم الإلكترونية من حيث فهم ومعالجة مخاوف أصحاب المصالح من المعتمدين على الإنترنت في أعمالهم، وكان عنوانها ، وهدف دراستهما الكشف عن الصعوبات التي تواجهها العدالة في مواجهة الجرائم الإلكترونية في أستراليا، ولتحقيق هذا الهدف استخدم الباحثان المنهج الوصفي التحليلي وأداة الاستبانة التي استجاب لها (66) من المستخدمين والمؤسسات المعتمدين على الإنترنت في تعاملاتهم، حيث تم أخذ العينة بطريقة قصدية من المعرضين للجرائم الإلكترونية، وبعد تحليل آرائهم باستخدام تقنيات تحليل المفاهيم ورسم الخرائط من أجل تحديد القضايا الرئيسية ومجالات الاهتمام، أظهرت النتائج أن الصعوبات التي تواجهها العدالة في مواجهة الجرائم الالكترونية هي تكرار خروقات أمن المعلومات وهجمات البرامج الضارة، وعدم الوعي بالأمن الإلكتروني وبالأدوار التي يؤديها القانون في مواجهة هذه الجرائم، وعدم المعرفة بتثبيت برامج وأنظمة الأمان.

التعقيب على الدراسات السابقة وذات العلاقة:

أجمعت الدراسات السابقة وذات العلاقة على حتمية مكافحة الجريمة من قبل أجهزة الأمن المختصة وضرورة تأهيل الكادر الأمني المختص في مكافحة تلك الجرائم، كما اتفقت أيضاً على ضرورة إجراء إصلاحات تشريعية وقانونية، ذلك من خلال تشديد العقوبات على تلك الجرائم لتكون رادعة، كما أشارت معظم الدراسات السابقة وذات العلاقة إلى المعوقات التي تواجه العاملين في مجال مكافحة الجرائم الإلكترونية، فأجمعت على وجود معوقات خاصة بالعاملين في الهيئات المختصة كعدم تأهيلهم التأهيل المناسب، ومعوقات خاصة بطبيعة الجرائم نفسها وصعوبة الحصول على أدلة مادية ذات علاقة بتلك الجرائم، لأن مسرح الجريمة فيها افتراضي وليس واقعي مما يصعب الحصول على أدلة مادية، إلى جانب وجود معوقات تتعلق بالمجني عليه ودوره في تلك الجرائم كعدم إبلاغه عن الجرائم الإلكترونية التي يكون ضحيتها، إضافة إلى أن بعض الدراسات السابقة وذات العلاقة استخدمت المنهج الوصفي في الوصول إلى نتائجها واستخدمت الاستبانة كأداة لجمع المعلومات، وهناك بعض الدراسات السابقة استخدمت المنهج التحليلي الذي يعتمد على تحليل نصوص الاتفاقيات الدولية والتشريعات الداخلية، والمنهج المقارن من خلال المقارنة بين التشريعات المختلفة، ومن هذه التحديات أيضاً ما هو قانوني لا يقدم الإجراءات المماثلة كما في الجرائم التقليدية، ومن الصعوبات عدم معرفة الظروف المؤدية لوقوع الجريمة لوجودها في فضاء إلكتروني.

في حين تميزت الدراسية الحالية عن الدراسات السابقة وذات العلاقة بما يلي:

- اختلاف المنهج المستخدم حيث سيتم استخدام المنهج الوصفي التحليلي، كما واختلفت بمجتمع الدراسة وعينته حيث ستستهدف هذه الدراسة العاملين في هيئات العدالة الجنائية المختصين في مكافحة الجرائم الالكترونية، فهو مجتمع يتعامل بشكل مباشر في التحقيق بالجرائم الالكترونية والوقاية منها، وهم الأكثر قدرة على تحديد فعالية مواجهة تلك الجرائم والمعوقات التي تواجههم في مكافحتها، بينما كان اعتماد بعض الدراسات السابقة على عينة من أفراد ومؤسسات خاصة، وبعض من دوائر ومراكز متخصصة في متابعة وملاحقة الجرائم الالكترونية.

- الدراسات السابقة تناولت الجريمة الإلكترونية من جوانب معينة، فمنها من تناول خصوصية الجرائم الإلكترونية والمعوقات التي تتعلق بمكافحتها، ومنها من تناولها من ناحية آليات ومهارات التحقيق فيها وآلية التفتيش المتبعة ودوره في الكشف عنها، في حين أن الدراسة الحالية تناولت هذه الجرائم من عدة جوانب فهي ستدرس هيئات العدالة الجنائية ومدى فعاليتها في مواجهة هذه الجرائم سواء من ناحية (القوانين المعمول بها أو آليات واجراءات التحقيق التفتيش والضبط ... إلخ).

- تعد الدراسة الحالية من الدراسات النادرة التي تبحث حول "إجراءات هئيات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً"، إذ أن هناك ندرة في الدراسات التي تبحث في ذلك.

الفصل الثالث

الطريقة والإجراءات

يتناول هذا الفصل وصفاً مفصلاً في تنفيذ الدراسة، حيث يتضمن تعريف منهج الدراسة، ووصف مجتمع الدراسة، وتحديد عينة الدراسة، إعداد أداة الدراسة (الاستبانة)، التأكد من صدقها وثباتها، بيان إجراءات الدراسة، والأساليب الإحصائية التي استخدمت في معالجة النتائج، وفيما يلي وصف لهذه الإجراءات.

1.3 منهج الدراسة:

من أجل تحقيق أهداف الدراسة تمّ استخدام منهج الوصفي التحليلي بشقه الكمي من خلال استخدام أداة الاستبانة، ويعرف بأنه المنهج الذي يدرس ظاهرة أو حدثاً أو قضية موجودة حالياً يمكن الحصول منها على معلومات تجيب عن أسئلة البحث دون تدخل، يتم من خلالها وصف الظاهرة موضوع الدراسة، وتحليل بياناتها، وبيان العلاقة بين المكونات والآراء التي تطرح حولها والعمليات التي تتضمنها والآثار التي تحدثها، وهو أحد أشكال التحليل والتفسير العلمي المنظم لوصف الظاهرة أو المشكلة، وتصنيفها وتحليلها وإخضاعها للدراسات الدقيقة بالفحص والتحليل.

2.3 مجتمع الدراسة:

تكون مجتمّع الدراسة من جميع العاملين في جهاز الشرطة، والنيابة العامة والقضاة في محافظة أريحا والأغوار، والبالغ عددهم (363) موظف/ة حسب إحصائيات (جهاز المركزي للإحصاء الفلسطيني، 2023).

3.3 عينة الدراسة:

اشتملت عينة الدراسة على عينة عشوائية بسيطة تكونت من (188) استبانة، أي بنسبة (50.8%) من مجتمع الدراسة، الجدول (1.3) يوضح توزيع أفراد عينة الدراسة حسب متغيرات الدراسة:

4.3 وصف متغيرات أفراد العينة:

يبين الجدول رقم (1.3) توزيع أفراد عينة الدراسة حسب متغير الجنس حيث بلغت نسبة (91%) للذكور، ونسبة (9%) للإناث، ويبين متغير العمر أن نسبة (50.5%) من (20 – أقل من 30 سنة)، ونسبة (25.5%) من (30- أقل من 40 سنة)، ونسبة (23.9%) من (40 سنة فأكثر)، ويبين متغير المستوى التعليمي أن نسبة (18.1%) ثانوية عامة فأقل، ونسبة (25.5%) دبلوم متوسط، ونسبة (46.8%) بكالوريوس، ونسبة (9.6%) دراسات عليا، ويبين متغير الخبرة العملية أن نسبة (36.7%) (لأقل من 5 سنوات)، ونسبة (16.5%) من (5- أقل من 10 سنوات)، ونسبة (12.8%) من (10- أقل من 15 سنة)، ونسبة (17%) من (15- أقل من 20 سنة)، ونسبة (17%) (ل20 سنة فأكثر).

جدول 1.3: توزيع أفراد عينة الدراسة حسب النوع الاجتماعي.

المتغير	المستوى	العدد	النسبة المئوية
الجنس	ذكر	171	91.0
	أنثى	17	9.0
العمر	من 20- أقل من 30 سنة	95	50.5
	من 30-أقل من 40 سنة	48	25.5
	40 سنة فأكثر	45	23.9
المستوى التعليمي	ثانويّة عامة فأقل	34	18.1
	دبلوم متوسط	48	25.5
	بكالوريوس	88	46.8
	دراسات عليا	18	9.6
الخبرة العملية	أقل من 5 سنوات	69	36.7
	من 5- أقل من 10 سنوات	31	16.5
	من 10- أقل من 15 سنة	24	12.8
	من 15- أقل من 20 سنة	32	17.0
	20 سنة فأكثر	32	17.0

5.3 أداة الدراسة:

لأغراض جمع البيانات تم الاعتماد على الاستبانة بشكل أساسي، وبشكل ثانوي على مراجعة الأدبيات ذات العلاقة بموضوع البحث، وقد تكونت الاستبانة من قسمين:

- القسم الأول: شمل على المعلومات الخاصة بالمبحوثين (البيانات الديموغرافية) وهي (الجنس، العمر، المستوى التعليمي، الخبرة العملية).
- القسم الثاني شمل على مجالات الاستبانة الخمس وهي:

- **المجال الأول:** تكون من (8) فقرات تضمنت الإجراءات المُتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية.
- **المجال الثاني:** تكون من (8) فقرات تضمنت الإجراءات المُتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية.
- **المجال الثالث:** تكون من (8) فقرات تضمنت الإجراءات المُتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية.
- **المجال الرابع:** تكون من (19) فقرة تضمنت الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية.
- **المجال الخامس:** تكون من (23) فقرة تضمنت آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية.

1.5.3 صدق الأداة:

تم تصميم الاستبانة بصورتها الأولية كما في الملحق رقم (1)، بعد ذلك تمّ أخذ الموافقة عليها من مشرف الرسالة، ومن ثم تمّ التحقق من صدقها بعرضها على مجموعة من المحكمين من ذوي الاختصاص والخبرة، حيث تمّ توزيع الاستبانة على عدد من المحكمين لإبداء الرأي في أسئلة وفقرات الاستبانة من حيث مدى وضوح لغة الفقرات وسلامتها لغوياً، ومدى شمول الفقرات للجانب المدروس، وإضافة أي معلومات أو تعديلات أو فقرات يرونها مناسبة، لمزيد من التوضيح حول أسماء المحكمين أنظر/ي للملحق رقم(3)، ووفق هذه الملاحظات تمّ إخراج الاستبانة بصورتها النهائية، كما في ملحق رقم (2). من ناحية أخرى تمّ التحقق من صدق الأداة أيضاً بحساب معامل الارتباط بيرسون لفقرات

الاستبانة، واتضح وجود دلالة إحصائية في جميع فقرات الاستبانة ويدل على أن هناك التساق داخلي بين الفقرات، والجداول التالية تبين ذلك:

جدول 2.3: نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الإجراءات المتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.541**	0.000	4	0.550**	0.000	7	0.666**	0.000
2	0.637**	00.00	5	0.586**	0.000	8	0.608**	0.000
3	0.679**	0.000	6	0.631**	0.000			

** داله احصائية عند 0.001

* داله احصائية عند 0.050

جدول 3.3: نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.430**	0.000	8	0.427**	0.000	15	0.561**	0.000
2	0.415**	00.00	9	0.510**	0.000	16	0.404**	0.000
3	0.602**	0.000	10	0.369**	0.000	17	0.527**	0.000
4	0.547**	0.000	11	0.374**	0.000	18	0.481**	0.000
5	0.471**	0.000	12	0.580**	0.000	19	0.426**	0.000
6	0.454**	0.000	13	0.602**	0.000			
7	0.472**	0.000	14	0.495**	0.000			

** داله احصائية عند 0.001

* داله احصائية عند 0.050

جدول 4.3: نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية

م	قيمة R	الدالة الإحصائية	م	قيمة R	الدالة الإحصائية	م	قيمة R	الدالة الإحصائية
1	0.438**	0.000	9	0.514**	0.000	17	0.608**	0.000
2	0.430**	00.00	10	0.673**	0.000	18	0.498**	0.000
3	0.584**	0.000	11	0.545**	0.000	19	0.609**	0.000
4	0.410**	0.000	12	0.578**	0.000	20	0.566**	0.000
5	0.590**	0.000	13	0.656**	0.000	21	0.515**	0.000
6	0.571**	0.000	14	0.716**	0.000	22	0.679**	0.000
7	0.624**	0.000	15	0.756**	0.000	23	0.552**	0.000
8	0.584**	0.000	16	0.611**	0.000			

** داله احصائية عند 0.001

* داله احصائية عند 0.050

2.5.3 ثبات الدراسة:

تم التحقق من ثبات الأداة من خلال حساب ثبات الدرجة الكلية لمعامل الثبات لمجالات الدراسة حسب معادلة الثبات كرونباخ ألفا، وكانت النتيجة تشير إلى تمتع هذه الأداة بثبات يفي بأغراض الدراسة، والجدول رقم (4.3) يبين معامل الثبات للمجالات.

جدول 5.3: نتائج معامل الثبات للمجالات

المجالات	عدد الفقرات	معامل الثبات
الإجراءات المتبعة من قبل هيئات العدالة الجنائية (القضاء، النيابة العامة، الشرطة)	8	0.762
الصعوبات التي تواجه هيئات العدالة الجنائية	19	0.817
آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية	23	0.910

6.3 إجراءات الدراسة:

تم العمل على بناء الأدب النظري للدراسة والدراسات السابقة، ثم بناء أداة الدراسة وعرضها على المشرف والمحكمين ثم الحصول على صدق وثبات الأداة، بعد ذلك تم توزيع (188) استبانة على المبحوثين، تم استرجاعها جميعها، بعد ذلك تم تحليل الاستبانات الصالحة باستخدام برنامج الحزم الإحصائية(SPSS) للوصول إلى النتائج النهائية.

7.3 المعالجة الإحصائية:

بعد جمع الاستبيانات والتأكد من صلاحيتها للتحليل تم ترميزها (إعطائها أرقام معينة)، وذلك تمهيداً لإدخال بياناتها إلى جهاز الحاسوب الآلي لإجراء المعالجات الإحصائية المناسبة، وتحليل البيانات وفقا لأسئلة الدراسة بيانات الدراسة، وقد تمت المعالجة الإحصائية للبيانات باستخراج المتوسطات الحسابية والانحرافات المعيارية لكل فقرة من فقرات الاستبانة، واختبار (ت) (t-test)، واختبار تحليل التباين الأحادي (one way ANOVA)، ومعامل ارتباط بيرسون، ومعادلة الثبات كرونباخ ألفا (Cronbach Alpha)، وذلك باستخدام الرزم الإحصائية (SPSS) (Statistical Package For Social Sciences)، كما هو واضح في الفصل الرابع الخاص بعرض النتائج.

الفصل الرابع

عرض نتائج الدراسة

1.4 مقدمة:

تضمن هذا الفصل عرضاً لنتائج الدراسة، التي تمّ التوصل إليها عن موضوع الدراسة وهو "**إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً** " وبيان أثر كل من المتغيرات من خلال استجابة أفراد العينة على أداة الدراسة، وتحليل البيانات الإحصائية التي تم الحصول عليها، وحتى يتم تحديد درجة متوسطات استجابة أفراد عينة الدراسة تم اعتماد الدرجات التالية حسب المعادلة التالية: الحد الأعلى- الحد الأدنى / عدد المحاور= طول الفترة بين كل درجة. (أعلى درجة موافق بشدة 5 درجات، أقل درجة معارض بشدة درجة واحدة) والفترات بينهم (5-1)= 4 فترات، يتم تقسيم هذه الفترات على 3 درجات (3/4= 1.33) وبذلك تكون طول كل فترة (1.33) وعليه تكون أقل درجة هي (1) نضيف عليها طول الفترة (1.33) فتصبح (2.33) فما دون تكون الدرجة منخفضة، والدرجة المتوسطة(2.34) نضيف عليها طول الفترة(1.33) تصبح (2.34- 3.67) متوسطة، وأعلى من ذلك تكون درجة عالية.

جدول 1.4: مددى المتوسط الحسابي

الدرجة	مدى المتوسط الحسابي
منخفضة	2.33 فأقل
متوسطة	3.67-2.34
عالية	3.68 فأعلى

2.4 عرض نتائج أسئلة الدراسة:

سوف يتم عرض النتائج التي تمّ التوصل إليها بعد عملية التحليل الإحصائي للبيانات التي تمّ الحصول عليها من عينة الدراسة، كما على النحو الآتي:

1.2.4 النتائج المتعلقة بالسؤال الأول:

ما مستوى الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية؟

للإجابة عن هذا السؤال تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن مستوى الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية، الجدول رقم (1.4) يبين ذلك.

جدول 2.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئويّة
1	الاستجابة بسرعة لشكاوى المواطنين حول الجرائم الإلكترونية	4.53	0.654	**عالية**	90.6
4	يعمل مأمورو الضبط القضائي على جمع المعلومات (البحث والتحري) وتحرير محاضر بها	4.43	0.675	**عالية**	88.6
2	يوجد برامج إعداد كادر متخصص في البحث والتحري في الجرائم الإلكترونية	4.35	0.679	**عالية**	87.0
5	توثيق محاضر الاستدلال من قبل مأموري الضبط القضائي وفق الإجراءات القانونية المحددة	4.34	0.716	**عالية**	86.8
6	يلتزم العاملون بسرية المعلومات أثناء التحري والاستدلال عن الجرائم الإلكترونية	4.27	0.829	**عالية**	85.4
3	يتم التعامل مع مسرح الجريمة الإلكترونية بالمعدات التقنية اللازمة	4.25	0.847	**عالية**	85.0
7	رفع مستوى الوعي العام اتجاه مخاطر الجرائم الإلكترونية	4.20	0.863	**عالية**	84.0
8	تعزيز التعاون مع المجتمع المحلي للكشف عن الجرائم الالكترونية	4.20	0.812	**عالية**	84.0
الدرجة الكلية		**4.3214**	**0.47253**	**عالية**	**86.4**

يلاحظ من الجدول رقم (1.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على مستوى الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية أن المتوسط الحسابي للدرجة الكلية (4.32) وانحراف معياري (0.472) وهذا يدل على أن مستوى الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية وبنسبة مئوية (86.4%).

كما وتشير النتائج في الجدول رقم (1.4) أن جميع الفقرات جاءت بدرجة عالية، وحصلت الفقرة "الاستجابة بسرعة لشكاوى المواطنين حول الجرائم الإلكترونية" على أعلى متوسط حسابي (4.53)، ويليها فقرة "يعمل مأمورو الضبط القضائي على جمع المعلومات (البحث والتحري) وتحرير محاضر بها" بمتوسط حسابي (4.43)، وحصلت الفقرة "رفع مستوى الوعي العام اتجاه مخاطر الجرائم الإلكترونية" والفقرة "تعزيز التعاون مع المجتمع المحلي للكشف عن الجرائم الالكترونية" على أقل متوسط حسابي (4.20)، يليها الفقرة "يتم التعامل مع مسرح الجريمة الإلكترونية بالمعدات التقنية اللازمة" بمتوسط حسابي (4.25).

2.2.4 النتائج المتعلقة بالسؤال الثاني:

ما مستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية؟

تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن مستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية، الجدول رقم (2.4) يبين ذلك.

جدول 3.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئوية
2	العمل على تسهيل تحويل شكاوى الجرائم الإلكترونية من خلال النيابات الجزئية	5.00	0.000	**عالية**	100.0
3	يجري التحقيق في الشكاوى المتعلقة بالجرائم الإلكترونية وفقا للإجراءات التي تتناسب وخصوصية كل نوع من أنواعها	5.00	0.000	**عالية**	100.0
4	توثيق محاضر التحقيق وفق الإجراءات القانونية المحددة	5.00	0.000	**عالية**	100.0
6	التعامل مع المضبوطات ذات العلاقة بالجريمة الإلكترونية وفقا للإجراءات القانونية المحددة	5.00	0.000	**عالية**	100.0
7	التعاون مع المختبر الجنائي للتعامل مع الدليل المضبوط من مسرح الجريمة الإلكترونية	5.00	0.000	**عالية**	100.0
8	الاشتراك بالجانب التوعوي مع المؤسسات الشريكة للتوعية بمخاطر الجرائم الإلكترونية وآثارها	4.67	0.577	**عالية**	93.4
5	التعامل مع قضايا الجرائم الإلكترونية الواردة بالسرية التامة	4.33	1.155	**عالية**	86.6
1	إنشاء نيابة متخصصة في الجرائم الإلكترونية	4.00	1.732	**عالية**	80.0
الدرجة الكلية		**4.7500**	**0.33072**	**عالية**	**95.0**

يلاحظ من الجدول رقم (2.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على مستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية أن المتوسط الحسابي للدرجة الكلية (4.75) وانحراف معياري (0.330) وهذا يدل على أن مستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة مئوية (95%).

كما وتشير النتائج في الجدول رقم (2.4) أن جميع الفقرات جاءت بدرجة عالية، وحصلت الفقرة "العمل على تسهيل تحويل شكاوى الجرائم الإلكترونية من خلال النيابات الجزئية" والفقرة "يجري التحقيق في الشكاوى المتعلقة بالجرائم الإلكترونية وفقاً للإجراءات التي تتناسب وخصوصية كل نوع من أنواعها" والفقرة "توثيق محاضر التحقيق وفق الإجراءات القانونية المحددة" والفقرة "التعامل مع المضبوطات ذات العلاقة بالجريمة الإلكترونية وفقاً للإجراءات القانونية المحددة" والفقرة "التعاون مع المختبر الجنائي للتعامل مع الدليل المضبوط من مسرح الجريمة الإلكترونية" على أعلى متوسط

حسابي (5.00)، ويليها فقرة "الاشتراك بالجانب التوعوي مع المؤسسات الشريكة للتوعية بمخاطر الجرائم الإلكترونية وآثارها" بمتوسط حسابي (4.67)، وحصلت الفقرة "إنشاء نيابة متخصصة في الجرائم الإلكترونية" على أقل متوسط حسابي (4.00)، يليها الفقرة "التعامل مع قضايا الجرائم الإلكترونية الواردة بالسرية التامة" بمتوسط حسابي (4.33).

3.2.4 النتائج المتعلقة بالسؤال الثالث:

ما مستوى الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية؟

تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن مستوى الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية، الجدول رقم (3.4) يبين ذلك:

جدول 4.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئوية
1	يلتزم القضاء بالتشريعات النافذة في مواجهة الجرائم الالكترونية.	4.67	0.577	**عالية**	93.4
2	يمتلك القضاة القدرة على وزن البينات الفنية في الجرائم الالكترونية.	4.67	0.577	**عالية**	93.4
5	يستعين القضاة بالخبراء الفنيين في مجال الجرائم الإلكترونية.	4.67	0.577	**عالية**	93.4
3	يعمل القضاء على سد الثغرات التشريعية في القوانين ذات العلاقة بالجرائم الالكترونية بالاسترشاد بقوانين أخرى.	4.33	1.155	**عالية**	86.6
4	يتبنى القضاة فلسفتي الردع والاصلاح في الاحكام الصادرة والمتعلقة بالجرائم الإلكترونية.	4.33	0.577	**عالية**	86.6
7	يتلقى القضاة دورات تدريبية في مجال الجرائم الإلكترونية.	4.33	0.577	**عالية**	86.6
8	العمل على تنظيم ورش عمل وندوات لمناقشة مدى ملائمة التشريعات القانونية المتعلقة بالجرائم الإلكترونية بحداثتها وتطورها	3.67	1.528	**متوسطة**	73.4
6	لدى القضاء الأجهزة التقنية والفنية اللازمة لاستعراض أدلة الوقائع المتعلقة بالجرائم الإكترونية.	3.33	1.155	**متوسطة**	66.6
	الدرجة الكلية	**4.2500**	**0.2500**	**عالية**	**85.0**

يلاحظ من الجدول رقم (3.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على مستوى الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية أن المتوسط الحسابي للدرجة الكلية (4.25) وانحراف معياري (0.250) وهذا يدل على أن مستوى الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة مئوية (85%).

كما وتشير النتائج في الجدول رقم (3.4) أن (6) فقرات جاءت بدرجة عالية وفقرتين جاءتا بدرجة متوسطة، وحصلت الفقرة "يلتزم القضاء بالتشريعات النافذة في مواجهة الجرائم الإلكترونية" والفقرة "يمتلك القضاة القدرة على وزن البينات الفنية في الجرائم الإلكترونية" والفقرة "يستعين القضاة بالخبراء الفنيين في مجال الجرائم الإلكترونية" على أعلى متوسط حسابي (4.67)، ويليها فقرة "يعمل القضاء على سد الثغرات التشريعية في القوانين ذات العلاقة بالجرائم الإلكترونية بالاسترشاد بقوانين أخرى" والفقرة "يتبنى القضاة فلسفتي الردع والإصلاح في الاحكام الصادرة والمتعلقة بالجرائم الإلكترونية" والفقرة "يتلقى القضاة دورات تدريبية في مجال الجرائم الإلكترونية" بمتوسط حسابي (4.33)، وحصلت الفقرة "لدى القضاء الأجهزة التقنية والفنية اللازمة لاستعراض أدلة الوقائع المتعلقة بالجرائم الإلكترونية" على أقل متوسط حسابي (3.33)، يليها الفقرة "العمل على تنظيم ورش عمل وندوات لمناقشة مدى ملائمة التشريعات القانونية المتعلقة بالجرائم الإلكترونية بحداثتها وتطورها" بمتوسط حسابي (3.67).

4.2.4 النتائج المتعلقة بالسؤال الرابع:

ما درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية؟

تمَ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية، الجدول رقم (4.4) يبين ذلك.

جدول 5.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لدرجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئوية
10	قلة وعي المجتمع بالجريمة الإلكترونية	4.34	0.802	عالية	86.8
5	صعوبة تعقب الشرائح الإسرائيلية المستخدمة في ارتكاب الجرائم الإلكترونية	4.22	0.873	عالية	84.4
9	قلة البرامج والأدوات التقنية المختصة للمساعدة في عملية التحقيق الجنائي مقارنة بالتطور الهائل والسريع للتقنية	4.20	0.895	عالية	84.0
11	إحجام الضحايا عن الإبلاغ عن الجريمة الإلكترونية	4.18	0.846	عالية	83.6
8	قلة خبرة أجهزة العدالة من مأموري ضبط وسلطة تحقيق في التعامل مع الجرائم الإلكترونية نسبيا	4.12	0.906	عالية	82.4
7	نقص الكادر المختص للتعامل مع الجرائم الإلكترونية	4.11	0.840	عالية	82.2
19	عدم وجود خطة استراتيجية مشتركة بين هيئات العدالة الجنائية لمواجهة الجرائم الإلكترونية	4.10	0.847	عالية	82.0
14	البعد الجغرافي بين مرتكب الجريمة والضحية	4.07	0.970	عالية	81.4
6	ضخامة حجم البيانات المتعين فحصها للحصول على أدلة إثبات	4.06	0.828	عالية	81.2
3	صعوبة إجراءات ضبط الأدلة في الجرائم الإلكترونية	4.05	0.900	عالية	81.0
15	يوجد نقص في التنظيم الإجرائي لمكافحة الجرائم الإلكترونية في التشريع الفلسطيني	4.03	0.843	عالية	80.6
16	حداثة التشريعات القانونية الخاصة بالجرائم الإلكترونية	4.03	0.824	عالية	80.6
1	عدم سيطرة هيئات العدالة الجنائية على الفضاء الإلكتروني الفلسطيني	4.02	0.959	عالية	80.4
18	الإجراءات المتبعة من هيئات العدالة الجنائية للتحقيق في الجرائم الإلكترونية معقدة وطويلة	4.01	0.824	عالية	80.2
2	صعوبة إجراءات التفتيش وجمع الأدلة في مسرح الجريمة الإلكترونية	3.92	0.833	عالية	78.4
17	العقوبات المفروضة على ارتكاب الجرائم الإلكترونية غير رادعة	3.91	1.158	عالية	78.2
4	صعوبة الحصول على أدلة الإثبات كون الدليل غير مادي	3.90	0.872	عالية	78.0
13	صعوبة كشف الجناة كونهم ينتحلون شخصيات وهمية	3.81	1.135	عالية	76.2
12	عدم توفير حماية للمبلغين عن الجرائم الإلكترونية	3.73	1.145	عالية	74.6
	الدرجة الكلية	**4.04**	**0.442**	عالية	**80.8**

يلاحظ من الجدول (4.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية أن المتوسط الحسابي للدرجة الكلية (4.04) وانحراف معياري (0.442) وهذا يدل على أن درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة مئوية (85.6%).

كما وتشير النتائج في الجدول رقم (4.4) أن جميع الفقرات جاءت بدرجة عالية، وحصلت الفقرة "قلة وعي المجتمع بالجريمة الإلكترونية" على أعلى متوسط حسابي (4.34)، ويليها فقرة "صعوبة تعقب الشرائح الإسرائيلية المستخدمة في ارتكاب الجرائم الإلكترونية" بمتوسط حسابي (4.22)، وحصلت الفقرة "عدم توفير حماية للمبلغين عن الجرائم الإلكترونية" على أقل متوسط حسابي (3.73)، يليها الفقرة "صعوبة كشف الجناة كونهم ينتحلون شخصيات وهمية" بمتوسط حسابي (3.81).

5.2.4 النتائج المتعلقة بالسؤال الخامس:

ما مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية؟

تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية، جدول رقم(5.4) يبين ذلك.

جدول 6.4-أ: المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئوية
13	تنمية الثقة بين المواطنين والعاملين في هيئات العدالة الجنائية	4.35	0.868	**عالية**	87.0
23	إصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة	4.28	0.914	**عالية**	85.6
18	عمل رقم موحد لدى جهات الاختصاص للتبليغ فورا عن التعرض للجريمة الإلكترونية	4.27	0.755	**عالية**	85.4
10	الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب	4.25	0.771	**عالية**	85.0
19	تطوير قدرات العاملين في مجال الجرائم الإلكترونية من خلال(التدريب، المؤتمرات، ورشات العمل)	4.25	0.714	**عالية**	85.0
8	تجنب فتح أي رسائل إلكترونية مجهولة المصدر	4.24	0.776	**عالية**	84.8
12	مساعدة المواطنين في تطبيق نظام الأمن الذاتي للوسائل الإلكترونية	4.24	0.797	**عالية**	84.8
22	زيادة أعداد الطاقم العاملين القائمين على البحث والتحري في الجرائم الإلكترونية	4.23	0.883	**عالية**	84.6
15	مواكبة التطورات التقنية لتتبع مرتكبي الجرائم الإلكترونية للحد من انتشارها	4.21	0.900	**عالية**	84.2
7	وضع سياسة أمنية للشبكة وحشد كل الإمكانيات البشرية والمادية لتطبيقها	4.20	0.815	**عالية**	84.0
11	العمل على تغيير كلمات المرور الخاصة بالحاسوب بشكل دوري	4.19	0.803	**عالية**	83.8
5	استخدام نظام إعلامي متطور للنشر عن طرق الوقاية من الجرائم الإلكترونية	4.14	0.822	**عالية**	82.8
6	تنظيم برامج توعوية حول الآثار المترتبة عن الجرائم الإلكترونية	4.13	0.784	**عالية**	82.6
4	التنسيق بين هيئات العدالة الجنائية ومؤسسات المجتمع الدولي للحد من الجرائم الإلكترونية	4.12	0.699	**عالية**	82.4
20	توفد هيئات العدالة الجنائية العاملين فيها للخارج لاكتساب الخبرات حول مكافحة الجرائم الإلكترونية	4.12	0.768	**عالية**	82.4

جدول 6.4–ب: المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية

9	فصل جهاز الحاسوب عن شبكة الإنترنت في حالة عدم الاستخدام	4.10	0.893	**عالية**	82.0
1	تبادل هيئات العدالة الجنائية المعلومات فيما بينها حول الجرائم الإلكترونية	4.08	0.895	**عالية**	81.6
16	تأمين الأجهزة باستخدام نظام برنامج حماية متقدم وتخزين آمن للمعلومات الحساسة	4.07	0.902	**عالية**	81.4
3	التنسيق بين هيئات العدالة الجنائية ومؤسسات المجتمع المحلي المعنية للحد من الجرائم الإلكترونية	4.06	0.844	**عالية**	81.2
14	التزام هيئات العدالة الجنائية بمراقبة وتتبع المواقع الإلكترونية	4.06	0.891	**عالية**	81.2
21	وضع نظام حوافز مادية ومعنوية للمتميزين من العاملين في التحقيق في الجرائم الإلكترونية	4.05	0.823	**عالية**	81.0
2	وضع خطة استراتيجية مشتركة بين هيئات العدالة الجنائية لمواجهة الجرائم الإلكترونية	4.04	0.734	**عالية**	80.8
17	استخدام تكنولوجيا الذكاء الصناعي لاكتشاف الجرائم الإلكترونية قبل وقوعها وذلك لمكافحتها	4.00	0.953	**عالية**	80.0
	الدرجة الكلية	**4.1603**	**0.48041**	**عالية**	**83.2**

يلاحظ من الجدول رقم (5.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية أن المتوسط الحسابي للدرجة الكلية (4.16) وانحراف معياري (0.480) وهذا يدل على أن مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة مؤية (80.8%)، كما وتشير النتائج في الجدول رقم (5.4) أن جميع الفقرات جاءت بدرجة عالية، وحصلت الفقرة "تنمية الثقة بين المواطنين والعاملين في هيئات العدالة الجنائية" على أعلى متوسط حسابي (4.35)، ويليها فقرة "إصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة" بمتوسط حسابي (4.28)، وحصلت الفقرة "استخدام تكنولوجيا الذكاء الصناعي لاكتشاف الجرائم الإلكترونية قبل وقوعها وذلك لمكافحتها" على أقل متوسط حسابي (4.00)، يليها الفقرة "وضع

خطة استراتيجية مشتركة بين هيئات العدالة الجنائية لمواجهة الجرائم الإلكترونية" بمتوسط حسابي (4.04).

6.2.4 النتائج المتعلقة بالسؤال السادس:

هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α≤ 0.05) في المتوسطات الحسابية لإجابات المبحوثين حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية تعزى لمتغيرات (الجنس، العمر، المستوى التعليمي، الخبرة العملية)؟ للإجابة عن هذا السؤال تم تحويله للفرضيات التالية:

1.6.2.4 نتائج الفرضية الأولى: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05 ≥α) بين متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية تعزى لمتغير الجنس"

تم فحص الفرضية الأولى بحساب نتائج اختبار "ت" والمتوسطات الحسابية لاستجابة أفراد عينة الدراسة في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الجنس، الجدول رقم (6.4) يبين ذلك.

جدول 7.4: نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الجنس

الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة"t"	مستوى الدلالة
ذكر	171	4.0397	0.45029	0.224	0.823
أنثى	17	4.0650	0.37054		

يتبين من خلال الجدول السابق أن قيمة "ت" للدرجة الكلية (0.224)، ومستوى الدلالة (0.823)، أي أنه لا توجد فروق في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الجنس، بذلك تمّ قبول الفرضية الأولى.

2.6.2.4 نتائج الفرضية الثانية: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة 0.05 (α≥ في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر"

تم فحص الفرضية الثانية بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر، جدول(7.4) يبين ذلك.

جدول 8.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمتوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر

العمر	العدد	المتوسط الحسابي	الانحراف المعياري
من 20 سنة – أقل من 30 سنة	95	3.9008	0.47374
من 30– أقل من 40 سنة	48	4.1842	0.39550
40 سنة فأكثر	45	4.1883	0.31629

يلاحظ من الجدول رقم (7.4) وجود فروق ظاهرية في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (8.4):

جدول 9.4: نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	3.827	2	1.914	10.777	0.000
داخل المجموعات	32.850	185	0.178		
المجموع	36.677	187			

يلاحظ أن قيمة ف للدرجة الكلية (10.777) ومستوى الدلالة (0.000) وهي أقل من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه توجد فروق دالة إحصائياً في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر، وبذلك تم رفض الفرضية الثانية، وتم فحص نتائج اختبار (LSD) لبيان اتجاه الفروق وهي كما يلي:

جدول 10.4: نتائج اختبار (LSD) للمقارنات البعدية بين المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حسب متغير العمر

المتغيرات		الفروق في المتوسطات	مستوى الدلالة
من 20 سنة – أقل من 30 سنة	من 30– أقل من 40 سنة	-0.28338*	0.000
	40 سنة فأكثر	-0.28747*	0.000
من 30– أقل من 40 سنة	من 20 سنة – أقل من 30 سنة	0.28338*	0.000
	40 سنة فأكثر	-0.00409	0.963
40 سنة فأكثر	من 20 سنة – أقل من 30 سنة	0.28747*	0.000
	من 30– أقل من 40 سنة	0.00409	0.963

يلاحظ أن الفروق كانت بين عمر (من 30– أقل من 40 سنة) و(من 20 سنة – أقل من 30 سنة) لصالح (من 30– أقل من 40 سنة)، وبين عمر (40 سنة فأكثر) و(من 20 سنة – أقل من 30 سنة) لصالح (40 سنة فأكثر).

3.6.2.4 نتائج الفرضية الثالثة: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05 ≥α) في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي"

تمّ فحص الفرضية الثالثة بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي.

جدول 11.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمتوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي

المستوى التعليمي	العدد	المتوسط الحسابي	الانحراف المعياري
ثانوية عامة فأقل	34	4.0000	0.42245
دبلوم متوسط	48	3.9375	0.49974
بكالوريوس	88	4.0592	0.42270
دراسات عليا	18	4.3158	0.30154

يلاحظ من الجدول رقم (10.4) وجود فروق ظاهرية في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (11.4):

جدول 12.4: نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف"المحسوبة	مستوى الدلالة
بين المجموعات	1.960	3	0.653	3.462	0.017
داخل المجموعات	34.717	184	0.189		
المجموع	36.677	187			

يلاحظ أن قيمة ف للدرجة الكلية (3.462) ومستوى الدلالة (0.017) وهي أقل من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه توجد فروق دالة إحصائياً في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي، وبذلك تم رفض الفرضية الثالثة، وتم فحص نتائج اختبار (LSD) لبيان اتجاه الفروق وهي كما يلي:

جدول 13.4: نتائج اختبار (LSD) للمقارنات البعدية بين المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حسب متغير المستوى التعليمي

المتغيرات		الفروق في المتوسطات	مستوى الدلالة
ثانوية عامة فأقل	دبلوم متوسط	0.06250	0.522
	بكالوريوس	-0.05921	0.500
	دراسات عليا	-.031579*	0.014
دبلوم متوسط	ثانوية عامة فأقل	-0.06250	0.522
	بكالوريوس	-0.12171	0.120
	دراسات عليا	-0.37829*	0.002
بكالوريوس	ثانوية عامة فأقل	0.05921	0.500
	دبلوم متوسط	0.12171	0.120
	دراسات عليا	-0.25658*	0.024
دراسات عليا	ثانوية عامة فأقل	0.31579*	0.014
	دبلوم متوسط	0.37829*	0.002
	بكالوريوس	0.25658*	0.024

يلاحظ أن الفروق كانت بين المستوى (دراسات عليا) و(ثانوية عامة فأقل) لصالح (دراسات عليا)، وبين المستوى (دراسات عليا) و(دبلوم متوسط) لصالح (دراسات عليا)، وبين المستوى (دراسات عليا) و(بكالوريوس) لصالح (دراسات عليا).

4.6.2.4 نتائج الفرضية الرابعة: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية"

تم فحص الفرضية الرابعة بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية.

جدول 14.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمتوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية

الخبرة العملية	العدد	المتوسط الحسابي	الانحراف المعياري
أقل من 5 سنوات	69	3.8268	0.46746
من 5- أقل من 10 سنوات	31	4.1358	0.38838
من 10- أقل 15 سنة	24	4.1491	0.44434
من 15- أقل من 20 سنة	32	4.1694	0.31937
20 سنة فأكثر	32	4.2072	0.37905

يلاحظ من الجدول رقم (13.4) وجود فروق ظاهرية في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (14.4):

جدول 15.4: نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية:

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	5.135	4	1.284	7.449	0.000
داخل المجموعات	31.541	183	0.172		
المجموع	36.677	187			

يلاحظ أن قيمة ف للدرجة الكلية (7.449) ومستوى الدلالة (0.000) وهي أقل من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه توجد فروق دالة إحصائياً في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية، وبذلك تم رفض الفرضية الرابعة، وتم فحص نتائج اختبار (LSD) لبيان اتجاه الفروق وهي كما يلي:

جدول 16.4: نتائج اختبار (LSD) للمقارنات البعدية بين المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حسب متغير الخبرة العملية

المتغيرات		الفروق في المتوسطات	مستوى الدلالة
أقل من 5 سنوات	من 5- أقل من 10 سنوات	-0.30897*	0.001
	من 10- أقل 15 سنة	-0.32227*	0.001
	من 15- أقل من 20 سنة	-0.34256*	0.000
	20 سنة فأكثر	-0.38039*	0.000
من 5- أقل من 10 سنوات	أقل من 5 سنوات	0.30897*	0.001
	من 10- أقل 15 سنة	-0.01330	0.906
	من 15- أقل من 20 سنة	-0.03358	0.749
	20 سنة فأكثر	-0.07141	0.496
من 10- أقل 15 سنة	أقل من 5 سنوات	0.32227*	0.001
	من 5- أقل من 10 سنوات	0.01330	0.906
	من 15- أقل من 20 سنة	-0.02029	0.857
	20 سنة فأكثر	-0.05811	0.605
من 15- أقل من 20 سنة	أقل من 5 سنوات	0.34256*	0.000
	من 5- أقل من 10 سنوات	0.03358	0.749
	من 10- أقل 15 سنة	0.02029	0.857
	20 سنة فأكثر	-0.03783	0.716
20 سنة فأكثر	أقل من 5 سنوات	0.38039*	0.000
	من 5- أقل من 10 سنوات	0.07141	0.496
	من 10- أقل 15 سنة	0.05811	0.605
	من 15- أقل من 20 سنة	0.03783	0.716

يلاحظ أن الفروق كانت بين الخبرة (من 5- أقل من 10 سنوات) و(أقل من 5 سنوات) لصالح (من 5- أقل من 10 سنوات)، وبين الخبرة(من 10- أقل 15 سنة) و(أقل من 5 سنوات) لصالح (من 10- أقل 15 سنة)، وبين الخبرة(من 15- أقل من 20 سنة) و(أقل من 5 سنوات) لصالح (من 15- أقل من 20 سنة)، وبين الخبرة(20 سنة فأكثر) و(أقل من 5 سنوات) لصالح (20 سنة فأكثر).

7.2.4 النتائج المتعلقة بالسؤال السابع:

هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α≤ 0.05) بين المتوسطات الحسابية لإجابات المبحوثين حول مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية تعزى لمتغيرات (الجنس، العمر، المستوى التعليمي، الخبرة العملية)؟ للإجابة عن هذا السؤال تم تحويله للفرضيات التالية:

1.7.2.4 نتائج الفرضية الأولى: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α≤ 0.05) بين متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية تعزى لمتغير الجنس"

تمّ فحص الفرضية الأولى بحساب نتائج اختبار "ت" والمتوسطات الحسابية لاستجابة أفراد عينة الدراسة في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الجنس.

جدول 17.4: نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الجنس

الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة"t"	مستوى الدلالة
ذكر	171	4.1414	0.45960	1.720	0.087
أنثى	17	4.3504	0.64093		

يتبين من خلال الجدول السابق أن قيمة "ت" للدرجة الكلية (1.720)، ومستوى الدلالة (0.087)، أي أنه لا توجد فروق في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير جنس، وبذلك تم قبول الفرضية الأولى.

2.7.2.4 نتائج الفرضية الثانية: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α≤ 0.05) في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر"

تم فحص الفرضية الثانية بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر.

جدول 18.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمتوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر

العمر	العدد	المتوسط الحسابي	الانحراف المعياري
من 20 سنة – أقل من 30 سنة	95	4.1314	0.53851
من 30– أقل من 40 سنة	48	4.2011	0.43797
40 سنة فأكثر	45	4.1778	0.39052

يلاحظ من الجدول رقم (17.4) وجود فروق ظاهرية في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (18.4):

جدول 19.4: نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	0.173	2	0.087	0.373	0.689
داخل المجموعات	42.985	185	0.232		
المجموع	43.158	187			

يلاحظ أن قيمة ف للدرجة الكلية(0.373) ومستوى الدلالة (0.689) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه لا توجد فروق دالة إحصائياً في متوسطات مستوى آليات الوقاية المُتبعة من

قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر، وبذلك تم قبول الفرضية الثانية.

3.7.2.4 نتائج الفرضية الثالثة: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α≤ 0.05) في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي"

تم فحص الفرضية الثالثة بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي.

جدول 20.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمتوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي

المستوى التعليمي	العدد	المتوسط الحسابي	الانحراف المعياري
ثانوية عامة فأقل	34	4.0831	0.56571
دبلوم متوسط	48	3.9846	0.57774
بكالوريوس	88	4.2737	0.36041
دراسات عليا	18	4.2198	0.40056

يلاحظ من الجدول رقم (19.4) وجود فروق ظاهرية في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (20.4):

جدول 21.4: نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	2.880	3	0.960	4.386	0.005
داخل المجموعات	40.278	184	0.219		
المجموع	43.158	187			

يلاحظ أن قيمة ف للدرجة الكلية (4.386) ومستوى الدلالة (0.005) وهي أقل من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه توجد فروق دالة إحصائياً في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي، وبذلك تم رفض الفرضية الثالثة. وتم فحص نتائج اختبار (LSD) لبيان اتجاه الفروق وهي كما يلي:

جدول 22.4: نتائج اختبار (LSD) للمقارنات البعدية بين المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حسب متغير المستوى التعليمي

المتغيرات		الفروق في المتوسطات	مستوى الدلالة
ثانوية عامة فأقل	دبلوم متوسط	0.09852	0.349
	بكالوريوس	-0.19060*	0.045
	دراسات عليا	-0.13669	0.318
دبلوم متوسط	ثانوية عامة فأقل	-0.09852	0.349
	بكالوريوس	-0.28911*	0.001
	دراسات عليا	-0.23521	0.071
بكالوريوس	ثانوية عامة فأقل	0.19060*	0.045
	دبلوم متوسط	0.28911*	0.001
	دراسات عليا	0.05391	0.657
دراسات عليا	ثانوية عامة فأقل	0.13669	0.318
	دبلوم متوسط	0.23521	0.071
	بكالوريوس	-0.05391	0.657

يلاحظ أن الفروق كانت بين المستوى (بكالوريوس) و(ثانوية عامة فأقل) لصالح (بكالوريوس)، وبين المستوى (بكالوريوس) و(دبلوم متوسط) لصالح (بكالوريوس).

4.7.2.4 نتائج الفرضية الرابعة: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α≤ 0.05) في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية"

تم حساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية.

جدول 23.4: المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمتوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية

الخبرة العملية	العدد	المتوسط الحسابي	الانحراف المعياري
أقل من 5 سنوات	69	4.1493	0.54674
من 5- أقل من 10 سنوات	31	4.2342	0.41638
من 10- أقل 15 سنة	24	4.0688	0.56265
من 15- أقل من 20 سنة	32	4.1875	0.38231
20 سنة فأكثر	32	4.1535	0.41790

يلاحظ من الجدول رقم (22.4) وجود فروق ظاهرية في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (23.4):

جدول 24.4: نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	0.404	4	0.101	0.432	0.785
داخل المجموعات	42.754	183	0.234		
المجموع	43.158	187			

يلاحظ أن قيمة ف للدرجة الكلية(0.432) ومستوى الدلالة (0.785) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه لا توجد فروق دالة إحصائياً في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية، وبذلك تم قبول الفرضية الرابعة.

الفصل الخامس

مناقشة النتائج والتوصيات

1.5 مقدمة:

يتناول هذا الفصل مناقشة النتائج التي توصلت إليها الدراسة في ضوء الإطار النظري والنظريات المفسرة للدراسة والدراسات السابقة ذات العلاقة على النحو الآتي:

2.5 مناقشة أسئلة الدراسة:

1.2.5 مناقشة النتائج المتعلقة بالسؤال الأول:

ما مستوى الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية؟

أشارت نتائج الإجابة على هذا السؤال كما بين الجدول رقم (1.4) أن المتوسطات الحسابية والانحرافات المعيارية لفقرات الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية أن المتوسط الحسابي للدرجة الكلية (4.32) وانحراف معياري (0.472)، هذا يدل على أن الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية جاءت بدرجة عاليّة، وبنسبة مئوية (86.4%)، فقد بينت النتائج أنّه يتم الاستجابة بسرعة لشكاوى المواطنين حول الجرائم الإلكترونية، كما ويعمل مأمورو الضبط القضائي

على جمع المعلومات (البحث والتحري) ويحررون محاضر بها، وأنه يوجد برامج إعداد كادر متخصص في البحث والتحري في الجرائم الإلكترونية، ويتم تحرير محاضر الاستدلال من قبل مأموري الضبط القضائي وفق الإجراءات القانونية المحددة، ويتم التعامل مع مسرح الجريمة الإلكترونية بالمعدات التقنية اللازمة، ورفع مستوى الوعي العام اتجاه مخاطر الجرائم الإلكترونية، إلى جانب تعزيز التعاون مع المجتمع المحلي للكشف عن الجرائم الإلكترونية.

نستنتج مما سبق أن مستوى الإجراءات المرتفع من قبل وحدة الجرائم الإلكترونية في مواجهة الجريمة الإلكترونية من شأنه مكافحة الجرائم الإلكترونية للحد منها، فوحدة الجرائم الإلكترونية تقوم بالإجراءات المخولة لها وفقاً لما هو مبين في القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته والذي نص في المادة (3) على إنشاء هذه الوحدة، والمادة (52) في الفقرة (5) اشترط أن يكون مأمور الضبط القضائي مؤهلًا للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية ولجرائم الاتصالات وتكنولوجيا المعلومات فوجود هذه البنود في القرار بقانون بشأن الجرائم الإلكترونية وتعديلاته يعزز أهمية هذه الإجراءات المتبعة لمواجهة الجرائم الإلكترونية في فلسطين.

كما أكدت النتائج أنه من أهم إجراءات وحدة الجرائم الإلكترونية الاستجابة بسرعة لشكاوى المواطنين حول الجرائم الإلكترونية وهذا يتوافق مع ما ورد في (الكسواني، 2019) والذي أكد أنه من ضمن الاختصاصات الأصيلة لمأموري الضبط القضائي تلقي البلاغات والشكاوى والبحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى والتوجه إلى مسرح الجريمة وإجراء الكشف والمعاينة للحصول على الإيضاحات اللازمة لتسهيل التحقيق، ومن الاختصاصات الاستثنائية المخولة لهم القيام بأعمال التفتيش والضبط والقبض على المشتبه به وإن ما يترتب على الإجراءات السابقة سوف يكون كدليل من أدلة الإثبات التي سوف يواجه بها المتهم أمام المحكمة المختصة وهذا ما أكدته المادة (57) والمادة (58) من القرار بقانون بشأن الجرائم الإلكترونية، وأوجب على مأمور الضبط القضائي بعد القيام بالبحث والتحري تحرير محاضر الاستدلال وفقاً لما هو محدد قانوناً كوسيلة إثبات لتحديد مدى مشروعية أعمال الضابطة القضائية أثناء قيامها بأعمال الاستدلال مع المشتبه به وأن المحضر يكون محدد وفق إجراءات شكلية محددة قانوناً وأنه لا بد أن يكون مقتصراً على إجراءات الاستدلال فقط.

فنرى أن وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطيني تقوم بدورها القضائي ويؤكد هذا ما ورد في (سليمان،2011) والذي أكد أن العاملين في الشرطة هم من مأموي الضبط القضائي ذوي الاختصاص العام وذلك وفقاً لنص المادة (21) من قانون الإجراءات الجزائية رقم (3) لسنة (2001)

وأن لهم وظيفة قضائية تتمثل بمجموعة من الإجراءات التي تبدأ بمباشرتها بعد وقوع الجريمة لجمع أدلتها والبحث والتحري عن مرتكبيها قبل فتح تحقيق ابتدائي فيها، فإجراءات مأموري الضبط القضائي العاملين في وحدة الجرائم الإلكترونية تهدف للكشف عن الجرائم الإلكترونية وضبط الأدلة وتحرير محاضر بها والقبض على المشتبه به لإحالته إلى مرحلة التحقيق الابتدائي وهذه الإجراءات على درجة عالية من الخطورة كونها ماسة لحقوق الأشخاص وحرياتهم الفردية.

وأيضاً أكد على أهمية هذه الإجراءات لكشف الجرائم الإلكترونية ما ورد في دراسة (البغدادي، 2018) بعنوان "وسائل البحث والتحري عن الجرائم الإلكترونية" التي أكدت على أنه يوجد اختلاف في الأدلة للجرائم التقليدية عنها في الجرائم الإلكترونية، فالأدلة في الجرائم التقليدية واضحة وملموسة أما الأدلة في الجرائم الإلكترونية فمن السهل إخفاؤها ومسحها وأكدت على أهمية الإجراءات المتبعة من سلطة التحقيق بالانتقال فوراً إلى مسرح الجريمة وضبط الأدلة من خلال كادر مختص قادر على البحث والتحري بالجرائم الإلكترونية، وضرورة التعاون مع مزودي خدمة الاتصال فهذا يساعد في عملية البحث والتحري وهذا ما أكد عليه القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية وجرائم التصالات وتكنولوجيا المعلومات وتعديلاته والذي يلزم مزودي خدمة الإنترنت على تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة.

بالرغم من أن الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في الشرطة جاءت بدرجة عالية إلا أن نسبة الجرائم الإلكترونية بازدياد حتى بعد إصدار القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية فعام (2018) بلغت (2568) جريمة، كما وبلغت في عام (2019) (2420) جريمة وعام (2020) بلغت (2720) جريمة وعام (2021) بلغت(2589) جريمة وعام (2022) بلغت(3067) جريمة وعام (2023) بلغت (1228) جريمة (جهاز الشرطة الفلسطينية، 2023)، فيمكن تفسير هذا من خلال دراسة (عصام ومحمد ،2019) بعنوان "معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية"، التي بينت أن هناك معوقات لمكافحة الجرائم الإلكترونية منها ما يتعلق بطبيعة الجريمة الإلكترونية والخصائص التي تتمتع بها من حيث سهولة إخفاء أثرها وبالتالي من الصعب إثباتها، ومنها ما يتعلق بالمجني عليه كونه يتكتم عن الجريمة لأنه قد يكون لم يكتشفها أو يخشى من التشهير به وبالتالي لم تتلقَ الجهات المختصة أية بلاغ بها لاتخاذ الإجراءات المحددة قانوناً، ومنها معوقات مرتبطة بالتحقيق الجنائي فسهولة محو الدليل في الجرائم الإلكترونية وسهولة فقدانه وهو من أهم أدوات الإثبات التي سوف يواجه بها المتهم أمام المحكمة المختصة، فكل هذه المعيقات من شأنها أن توفر فرصة للجاني للممارسة جريمته الإلكترونية حسب نظرية النشاط الرتيب.

هذا من جانب ومن جانب آخر كون فلسطين خاضعة لسيطرة الاحتلال الإسرائيلي فذلك ضاعف من المعوقات المترتبة على عاتق وحدة الجرائم الإلكترونية فسيطرته على الفضاء الإلكتروني الفلسطيني، وحصر عملها في مناطق (أ) وضعف عملها في المناطق المصنفة (ب) و(ج)، يساعد في هروب المجرمين إلى هذه الأماكن، وقد يستخدمون هذه المناطق كأوكار لارتكاب أفعالهم الإجرامية، إلى جانب استخدامهم شبكات اتصالات إسرائيلية والتي بدورها تسهل عملية القيام بهذا النوع من الجرائم، كون هذه الشبكات يصعب متابعتها من قبل الجهات الفلسطينية وترفض جهات الاحتلال المالكة لهذه الشبكات تزويد وحدة الجرائم الإلكترونية بأية بيانات تتعلق بالمستخدمين.

فتقوم إجراءات العاملين في وحدة الجرائم الإلكترونية وفق كل ما هو متاح لهم وضمن الإمكانيات المادية والمعلوماتية المتوفرة، إلا أنه لا يوجد هيئة في العالم يمكنها السيطرة المطلقة على الجريمة، أو يكون لديها القدرة على منع حدوث الجرائم الإلكترونية، لكن هذه الإجراءات هي وسائل وطرق تستخدم من أجل ضبط ومراقبة المجرمين للحد من وقوع هذه الجرائم والتصدي لها، لذا تم إصدار القرار بقانون رقم (10) لسنة (2018) والذي تم تعديله بالقرار بقانون رقم (28) لسنة (2020م) وثم تم تعديله بقرار بقانون رقم (38) لسنة 2021م بشأن الجرائم الإلكترونية ليبين ويحدد الإجراءات التي يتم اتخاذها من قبل جهات إنفاذ القانون المختصة لتعزيز عملها.

2.2.5 مناقشة النتائج المتعلقة بالسؤال الثاني:

ما مستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية؟

أشارت النتائج المتعلقة بمستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية كما بين الجدول رقم (2.4) أن المتوسط الحسابي للدرجة الكلية (4.75) والانحراف المعياري (0.330)، هذا يدل على أن مستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة مئوية (95%)، فقد بينت أنها تعمل على تسهيل تحويل شكاوى الجرائم الإلكترونية من خلال النيابات الجزئية، وتحقق في الشكاوى المتعلقة بالجرائم الإلكترونية وفقاً للإجراءات التي تتناسب وخصوصية كل نوع من أنواعها، وتوثق محاضر التحقيق وفق الإجراءات القانونية المحددة، وتتعامل مع المضبوطات ذات العلاقة بالجريمة الإلكترونية وفقاً للإجراءات القانونية المحددة، كما و تتعاون مع المختبر الجنائي للتعامل مع الدليل المضبوط من مسرح الجريمة الإلكترونية فجميع هذه الإجراءات جاءت بدرجة عالية حيث بلغت نسبتها(100%).

ومما سبق نستنتج أن مستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية، فكما بين (الكسواني، 2019) تختص النيابة العامة دون غيرها بإجراء التحقيق

الابتدائي، فبعد أن يقع البحث عن الجريمة من خلال مرحلة جمع الاستدلالات، والتي يقوم بها مأمورو الضابطة القضائية يتم إحالة ملف القضية إلى النيابة العامة كسلطة تحقيق ابتدائي والتي من خلالها يتم من خلالها القيام بمجموعة من الإجراءات والتحريات المأذونة من سلطات التحقيق والرامية إلى تحقيق أدلة الإدانة أو البراءة، والسعى إما إلى تدعيم الاتهام وإحالة المتهم إلى المحكمة المختصة، أو إلى حفظ الدعوى أو حفظ ملفها(أوراقها) حيث لا وجه شرعي لملاحقة المتهم، وتباشر نيابة الجرائم الإلكترونية عملها بالإجراءات المخولة لها وفقاً لما هو مبين في القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم التصالات وتكنولوجيا المعلومات وتعديلاته والذي نص في المادة (52) على للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، ونص في المادة (53) أن للنيابة العامة الحصول على الأجهزة أو الأدوات الإلكترونية وأن لها الإذن بالضبط والتحفظ على كامل نظام المعلومات وتحرر قائمة بالمضبوطات المتحفظ عليها، فوجود هذه المواد في القرار بقانون بشأن الجرائم الإلكترونية تعزز قانونية وأهمية هذه الإجراءات المتبعة من قبل النيابة لمواجهة الجرائم الإلكترونية في فلسطين.

وتؤكد النتائج أعلاه قيام النيابة العامة بالمهام الموكلة لها بموجب القانون وذلك يتوافق مع ما ورد في(النيابة العامة، 2022) والذي بين مهام النيابة العامة واختصاصها والتي من ضمنها: استقبال الشكاوى ذات العلاقة من قبل النيابات الجزئية، ومتابعة الطلبات المتعلقة بالجرائم الإلكترونية وكافة الطلبات ذات العلاقة الواردة من النيابات الجزئية والأجهزة الأمنية ومخاطبة الجهات المختصة (شركات الاتصالات ومزودي خدمات الإنترنت)، والتعاون مع المختبر الجنائي الإلكتروني في وحدة مكافحة الجرائم الإلكترونية في المباحث العامة والأجهزة الأمنية ذات الاختصاص، تحليل وتقييم الدليل الإلكتروني في الجرائم المختلفة وفقاً للاحتياجات التي ترد إلى نيابة مكافحة الجرائم الإلكترونية، ففي عام (2023) وفقاً للتقرير السنوي للنيابة العامة بلغ عدد الاحتياجات الإلكترونية الواردة إلى نيابة مكافحة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات (8748) احتياج وتشمل هذه الاحتياجات (شركات الاتصالات المحلية ومزودي خدمة الإنترنت، الطلبات المحالة الى المختبر الجنائي – وحدة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات في الشرطة والمضبوطات)، فهذه الإجراءات تهدف إلى التوصل إلى الجاني لإحالته إلى المحكمة المختصة، إلى جانب ذلك تشترك بالجانب التوعوي مع المؤسسات الشريكة ففي عام (2023) قامت نيابة مكافحة الجرائم الإلكترونية وبالتعاون مع وسائل الإعلام الرسمية والمحلية لتطبيق خطة توعوية لرفع ثقافة المواطنين فيما يتعلق بالجرائم

الإلكترونيــة وذلــك بالتنســيق مــع وحــدة العلاقــات العامــة والإعــلام بالنيابــة العامــة حيــث تــم مونتــاج العديــد مــن الملصقــات التوعويــة ونشــرها، بالإضافــة إلــى إجــراء العديــد مــن المقــابلات الإعلامية حول القانون وأنواع الجرائم الإلكترونية وخطورتها.

إن ماسبق يوضح لنا أنه يوجد التزام تام من قبل أعضاء النيابة العامة عند تنفيذ الإجراءات المتعلقة بمكافحة الجرائم الإلكترونية إلا أن أعداد الجرائم المرتكبة في ازدياد ففي عام (2022) ورد إلى النيابة العامة (1429) قضية تم إحالة (1245) قضية منها إلى المحاكم المختصة، وخلال العام (2023) باشرت نيابة مكافحة الجرائم الإلكترونية التحقيق في (1306) قضية تحقيقية، منها (1228) قضية تحقيقية وردت في العام (2023)، وأنهت النيابة العامة إجراءاتها التحقيقية في (1198) قضية تحقيقية أي ما نسبته (92%) من مجمل القضايا الواردة والمدورة (التقرير السنوي للنيابة العامة، 2023)، فإن سبب ازدياد الجرائم الإلكترونية المحالة إلى المحاكم يعود للخصوصية التي تتمتع بها الجرائم الإلكترونية وهذا يتفق مع دراسة (النجاجرة، 2019) بعنوان "خصوصية التحقيق في الجرائم الإلكترونية " والتي بينت العقبات والصعوبات التي تواجه إجراءات التحقيق في الجرائم الإلكترونية والتي تتمثل في أن الجرائم الإلكترونية غالباً لا تترك أثراً مادياً في مسرح الجريمة كما في الجرائم التقليدية، كما أن مرتكبيها لديهم القدرة على إتلاف وتشويه أو إضاعة الدليل في فترة قصيرة، وكونها جريمة عابرة للحدود يمكن ارتكابها من خارج إطار الدولة، فالتفتيش في الجرائم الإلكترونية بحاجة إلى مساندة وتعاون بين الدول كون أنه لا تستطيع دولة واحدة بمفردها مكافحة تلك الجريمة لوحدها، فبوجود هذه الصعوبات لن يكون هناك إمكانية لتنفيذ الإجراء بالشكل السليم إلا إذا كان هناك تفاهم وتعاون بين الدول تسعى من خلاله لمواجهة الجرائم الإلكترونية والقبض على مرتكبيها.

إلى جانب وجود صعوبات تتعلق بشخصية الجاني المرتكب للجرائم الإلكترونية من خلال ما يتميز به من سمات حيث إنه مجرم ذكي، غير عنيف، متكيف اجتماعياً، ويبرر قيامه بارتكاب الجريمة المعلوماتية كونه يمتلك العديد من الدوافع لعل من أهمها الدوافع المادية وهذا يتفق مع نظرية الاختيار العقلاني والتي ترتكز على مبدأ أن المجرمين يرغبون أو يبحثون في سلوكهم الإجرامي للحصول على فائدة وغنيمة ذات عائد وقيمة عالية وليس فيها خطورة أو صعوبة، فقرار المجرم في سلوك الطريق الانحرافي متعلق في الفائدة التي سوف يجنيها من اتخاذ هذا الفعل المنحرف كوسيلة لتحقيق منفعته، فالوسائل التكنولوجية جعلت ارتكاب الجريمة أسهل بكثير مما لو أنها حصلت على أرض الواقع وجعلتها ذات مردود مادي كبير هذا إلى جانب صعوبة الوصول إلى مرتكبيها، فالمجرم كل ما يحتاجه في هذه الجرائم هو جهاز حاسوب يساعده على ارتكاب جريمة عابرة للحدود ذات مردود مالي كبير وبأقل جهد ممكن، وهذا يتوافق مع دراسة دراسة براون (Brown, 2015) بعنوان (Investigating

(and prosecuting cyber crime: Forensic dependencies and barriers to justice التي بينت أن تطور وتقدم التكنولوجيا يعيق قدرة الشرطة على فهم أصول الجريمة، وإن استمرار الجرائم الإلكترونية وانتشارها يتطلب استجابة أوسع لأن التكنولوجيا أصبحت متشابكة بعمق مع نسيج المجتمع، وأنه يدرك المجرمون أن التكنولوجيا تشكل قوة مضاعفة فعّالة يمكن إساءة استخدامها لتمكين الأنشطة غير المشروعة، والاستفادة منها لتسهيل الوصول إلى دائرة عالمية من الضحايا عبر شبكة الإنترنت.

وقد حازت جريمة التهديد باستعمال الوسائل الإلكترونية والتهديد عبر الهاتف على أكبر عدد قضايا مسجلة بواقع (642) قضية، تليها جريمة الذم والقدح والتشهير بواسطة الوسائل الإلكترونية بواقع (482) قضية، وجريمة الابتزاز الإلكتروني بواقع (233) قضية (التقرير السنوي للنيابة العامة، 2023)، فالبرغم من الإجراءات المتبعة من جهة هيئات العدالة الجنائية لا زال الأشخاص يرتكبون الجرائم الإلكترونية بل ويطورون من أساليبهم في ارتكبها، فبينت نظرية الاحتواء أن الأفراد يرتكبون الجريمة بسبب الضغوطات التي يعانون منها سواء أكانت ضغوطات داخلية أو خارجية فالضغوطات الداخلية تتمثل بصعوبة ضبط الفرد لذاته نتيجة لضغوط نفسية داخلية كالقلق والإحباط وضغوط خارجية كالفقر والبطالة وصحبة السوء، فالشباب في المجتمع الفلسطيني يعانون من وضع خاص بسبب الاحتلال وكونهم يعانون من مختلف أنواع الضغوط سواء أكانت الداخلية أو الخارجية فإنهم يتجهون إلى وسائل التكنولوجيا لتفريغ طاقاتهم مما يدفعهم لارتكاب جرائم كونهم يستخدمون هذه الوسائل للهرب من الواقع الذي يعيشونه، أو بسبب سوء الوضع المادي مما يدفعهم لارتكاب جرائم تحقق لهم مكاسب مادية كالابتزاز الإلكتروني أو النصب والاحتيال والسرقة عبر الوسائل الإلكترونية.

3.2.5 مناقشة النتائج المتعلقة بالسؤال الثالث:

ما الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية؟

أظهرت النتائج أن المتوسط الحسابي للدرجة الكلية لاستجاباب أفراد العينة حول الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية قد بلغ (4.25)، وهذا يدل على أن مستوى الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة مئوية (85%)، وأشارت النتائج أيضاً إلى أن القضاء يلتزم بالتشريعات النافذة في مواجهة الجرائم الالكترونية، وأنه يمتلك القضاة القدرة على وزن البينات الفنية في الجرائم الالكترونية، وأن القضاة يستعينون بالخبراء الفنيين في مجال الجرائم الإلكترونية بدرجة عالية حيث بلغت نسبتها (93.4%) لكل منها، وإنه يعمل على سد الثغرات التشريعية في القوانين ذات العلاقة بالجرائم الإلكترونية بالاسترشاد بقوانين أخرى،

ويتبنى القضاة فلسفتي الردع والإصلاح في الاحكام الصادرة والمتعلقة بالجرائم الإلكترونية، كما ويتلقى القضاة دورات تدريبية في مجال الجرائم الإلكترونية بدرجة عالية حيث بلغت نسبتها (86.6%) لكل منها، إن لدى القضاء الأجهزة التقنية والفنية اللازمة لاستعراض أدلة الوقائع المتعلقة بالجرائم الإكترونية جاءت بدرجة متوسطة حيث بلغت (73.4%)، أما العمل على تنظيم ورش عمل وندوات لمناقشة مدى ملائمة التشريعات القانونية المتعلقة بالجرائم الإلكترونية جاء بدرجة متوسطة وبنسبة بلغت (66.6%).

يتضح مما سبق أن مستوى الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية، فبعد أن تقوم النيابة العامة بممارسة عملها بالتحقيق الابتدائي في الجريمة تحيل الشخص المتهم بالجريمة والذي يرجح اقترافه للفعل للمحكمة المختصة، والتي يأتي دورها للموازنة بين أدلة البراءة وأدلة الإدانة، عن طريق محكمة مستقلة ومحايدة، يضمن فيها السير العادل للمحاكمة ويضمن أن ينبني الحكم الجزائي والنطق به وفق إجراءات سليمة، مع ضمان حقه بالطعن في الحكم، فالهدف الأسمى للقضاء هو تحقيق محاكمة عادلة للمتهم لحين الوصول إلى حكم نهائي وبات بحقه.

فالبرغم من التزام المحاكم بالسير في إجراءات المحاكم العادلة للمتهم ووضع ضمانات لتحقيق ذلك، إلا أن المحاكم تعاني من قصور في التشريعات المتعلقة بالجرائم الإلكترونية فأكدت دراسة (المصري،2017) بعنوان "خصوصية الجرائم المعلوماتية"، على ووجود قصور في القواعد والتشريعات الإجرائية الواجب اتباعها في مرحلة التحقيق الابتدائي ومرحلة المحاكمة، وأوصت بضرورة قيام المشرعين في الدول المختلفة بإصدار تشريعات خاصة بالجرائم المتعلقة بالحاسب الآلي، وتطوير قواعد الإجراءات الجنائية وقواعد الإثبات بما يتواكب وحداثة هذه الجريمة، ولتكون أدلة الإثبات قانونية فيجب أن يتم الحصول عليها بالطرق القانونية السليمة لكي تثبت حجيتها أمام القضاة فقصور التشريعات في تحديد الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية ونيابتها يدفع للإفراج عن مرتكبها لعدم مشروعية الأدلة الموجهة ضدده كون الإجراءات المتبعة في الوصول إليها باطلة.

وبين (العموري، 2018) في دراسته بعنوان "التفتيش في الجرائم الإلكترونية" في أن القرار بقانون بشأن الجرائم الإلكترونية نص على بعض ضمانات التفتيش ولم ينص على الضمانات الأخرى التي أقرها قانون الإجراءات الجزائية للتفتيش في الجرائم العادية، منها حضور المتهم وغيره اجراء التفتيش، ووقت التفتيش، ولم يأمر بتنظيم محضر التفتيش، ولم يحيل الأمر إلى قانون الإجراءات الجزائية النافذ، فأوصى بضرورة النص بوضح على التفتيش والآلية التي سوف يتم بها، والنص بوضوح على مكان حفظ الأدلة الإلكترونية المضبوطة، لضمان الحفاظ عليها على الحالة التي ضبطت بها، ولضمان عدم العبث فيها أو تغيير محتواها، والنص بوضوح على طرق التصرف بالمضبوطات

الإلكترونية، ومنح السلطة القضائية خيارات التصرف بها إما بردها إلى أصحابها أو مصادرتها بقرار مسبب، سواء تم تحريك دعوى الحق العام أو تم حفظ أوراق الدعوى لدى النيابة العامة، النص بوضوح على أن الدليل الإلكتروني يعود تقدير قيمته للمحكمة، ليكون بإمكان المحكمة التيقن من سلامته، والنص بوضوح على الجهة المختصة بالتعارف الدولي وطلب المساعدة القضائية في التفتيش بالجرائم الإلكترونية، والجهة المختصة بالتعاون مع الشرطة الدولية، السماح للسلطات المختصة بالتفتيش في الجرائم الإلكترونية بتجاوز حدود الدولة في الحالات والشروط الواردة بالمادة (40) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وإصدار مرشد للتفتيش والضبط في الجرائم الإلكترونية، يكون دليلاً للقائم بالتفتيش، العمل على إنشاء مجلس وطني لمكافحة الجرائم الإلكترونية، يضم بين أعضائه ممثل عن نيابة مكافحة الجرائم الإلكترونية، وممثل عن وحدات مكافحة الجرائم الإلكترونية في قوى الأمن، وممثل عن وزارة الاتصالات وتكنولوجيا المعومات، وخبراء وأكاديميين فنيين في البيئة الرقمية، وخبراء في القانون الإلكتروني المحلي والدولي، ويكون لهذا المجلس صلاحية وضع معايير السياسة الجنائية في الميدان الإلكتروني، ودراسة القوانين المتعلقة به، وتقييمها، واقتراح التعديلات اللازمة عليها، ودراسة الاتفاقيات الثنائية والإقليمية والدولية الخاصة بالجرائم الإلكترونية قبل المصادقة عليها من الجهة المختصة.

فبعدم وجود تشريعات تتناسب مع الجرائم الإلكترونية وطبيعتها وتوضح آلية التصرف فيها منذ لحظة وقوعها إلى حين إلقاء القبض على مرتكبها وإحالته للمحكمة المختصة للفصل فيها، يجعل الإجراءات المتبعة في مرحلة جمع الاستدلالات من قبل وحدة الجرائم الإلكترونية، والإجراءات المتبعة في مرحلة التحقيق باطلة وبالتالي عند عرضها على المحكمة المختصة والتي تتأكد من سلامة الإجراءات لضمان المحاكمة العادلة، تجبر على أن تحكم ببراءة المتهم كون الإجراءات باطلة وما يترتب عليها يكون باطل.

و كونه لا يوجد معيار واحد لتصنيف الجرائم الإلكترونية ذلك بسبب تشعب هذه الجرائم وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم أو على أساس محل الجريمة، فعلى هذا الأساس قسمها (زبيدي وحفوظة، 2017) إلى ما يلي: الجرائم الواقعة على الأموال، الجرائم الواقعة على الأشخاص، الجرائم الواقعة على أمن الدولة فمهما كان تنفيذ الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية والنيابة والمحاكم بدرجة فائقة من الالتزام إلا أن غياب التشريعات والقوانين التي تنظم الجرائم الإلكترونية وتواكب تطورها وما هو مستحدث منها، يعزز انتشارها فالأفراد يرتكبون هذه السلوكيات لغياب القوانين التي تجرمها نظراً لحداثة الوسائل التكنولوجية وصعوبة التعامل معها من قبل الكثير من الأفراد فغياب وسائل الضبط غير الرسمية المتمثلة بالأسرة

إلى جانب حداثة القانون المتعلق بالجرائم الإلكترونية وتطور أشكالها وأنواعها بشكل مستمر وصعوبة القبض على مرتكبيها كل ذلك أضعف من وسائل الضبط الرسمي المتمثلة بالقانون فقلل من تأثيره على الأفراد ولم يردعهم عن ارتكاب مثل هذه الجرائم فكون وسائل الضبط الرسمي وغير الرسمي غير مجدية في التعامل مع الجريمة الإلكترونية فإن ذلك سوف يدفع الأفراد إلى ارتكابها بدون أي رادع حسب نظرية الضبط الاجتماعي.

4.2.5 مناقشة النتائج المتعلقة بالسؤال الرابع:

ما درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية؟

بينت نتائج الدراسة أن مستوى الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية جاءت بدرجة عالية وبنسبة مئوية (85.6%) حيث بلغ المتوسط الحسابي للدرجة الكلية (4.04)، كما تبين من النتائج أن أهم الصعوبات والتي جاءت بدرجة عالية تتمثل في قلة وعي المجتمع بالجريمة الإلكترونية حيث بلغت نسبتها(86.6%)، وإن صعوبة تعقب شرائح الاتصال الإسرائيلية المستخدمة في ارتكاب الجرائم الإلكترونية جاءت بدرجة عالية حيث بلغت نسبتها (84.4%)، إلى جانب قلة البرامج والأدوات التقنية المختصة للمساعدة في عملية التحقيق الجنائي مقارنة بالتطور الهائل والسريع للتقنية والتي أيضاً جاءت بدرجة عالية حيث بلغت نسبتها (84.0%).

يتضح مما سبق أن العاملين في الشرطة في وحدة الجرائم الإلكترونية، والنيابة العامة والمحاكم يجمعون على أن قلة وعي المجتمع بالجريمة الإلكترونية تشكل أول الصعوبات التي تواجه عملهم، فغياب الوعي لدى الأفراد ضحايا الجرائم الإلكترونية يؤدي إلى عدم مساعدة رجال الأمن في الكشف عن المجرم، فهم قد لا يعلمون بالجريمة أساساً كون الضحية يحجم عن الإبلاغ عنها، خوفاً من الفضيحة فيرضخ لكل ما يطلبه الجاني خاصة إذا كان هناك علاقة بين الضحية والجاني وبينهم ثقة عالية للحديث بشكل مطلق في أمور خاصة وإرسال الرسائل والمعلومات والصور الخاصة لهم فهذا يسهم في ارتفاع نسبة هذه الجرائم، فالعمل في مجال الجريمة الإلكترونية يحتاج إلى الصبر والجهد والصلاحيات ليتم على أكمل وجه إلى جانب تعزيز الثقة مع المواطنين والتأكيد على سرية الإجراءات التي يتم اتباعها في حال وقوع الجريمة الإلكترونية، لدفعهم للإبلاغ عنها فور وقوعهم ضحايا لها، وذلك للقبض على المجرم لكي لا يصل إلى ضحية أخرى، وبذلك يسهمون في الحد من انتشارها، وهذا يتفق مع دراسة (عصام ومحمد، 2019) بعنوان "معوقات مكافحة الجرائم المعلوماتية في

الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية" التي أكدت على ضرورة تشجيع المواطنين عن الإبلاغ عن الجرائم الإلكترونية وإعطاء المواطنين الضمانات التي تكفل سرية التحقيق في الجرائم المعلوماتية.

إلى جانب ذلك نرى أنهم أجمعوا على أن صعوبة تعقب الشرائح الإسرائيلية المستخدمة في ارتكاب الجرائم الإلكترونية من أحد أهم الصعوبات التي تواجههم أثناء ممارستهم لعملهم في مواجهة الجرائم الإلكترونية، فكون فلسطين تحت الإحتلال الاسرائيلي فهذا يعرقل عمل هيئات العدالة الجنائية، كونه يضيف معيقات أخرى أمام آلية عملهم لمواجهة الجرائم الإلكترونية والتي تتطلب جهود خاصة من قبلهم لمواجهتها تتناسب وخصوصية هذه الجريمة، فقد بينت دراسة (مرداوي، 2021) أن الاحتلال الإسرائيلي يسيطر على كافة جوانب الحياة بما في ذلك فضاء الاتصالات والإنترنت، فقوة البث القويّة لشبكاته في مناطق مختلفة من الأراضي الفلسطينية تدفع المواطنين إلى استخدام شبكاتهم والإحجام عن استخدام الشبكات الفلسطينية مما يجعلهم تحت رقابته وسيطرته بشكل دائم، وكون هذه الشبكات غير خاضعة لسيطرة السلطات الفلسطينية وبالتالي يصعب متابعتها فإن بعض الأشخاص يلجؤون إليها لارتكاب جرائمهم الإلكترونية وذلك لصعوبة اكتشافهم والتعرف عليهم بالتالي لا يتم محاسبتهم، فالاحتلال بذلك وفر بيئة خصبة تعزز ارتكاب هذه الجرائم، كما أن العديد من الشباب الفلسطيني أجبر على العمل لصالح قوات الجيش الإسرائيلي كونهم كانوا ضحايا لجرائم الإسقاط الإلكترونية التي يمارسها الإحتلال على أبناء الشعب الفلسطيني فهو عمل على إنشاء وحدة خاصة كاملة تحمل مسمى الوحدة رقم (8200) من أجل ممارسة هذه المهام لتجنيد العملاء، وهو على درجة عالية من التيقن بأهمية هذه الوسائل وسهولة استخدمها في سبيل تحقيق أهدافه ومساعيه، و من ناحية أخرى فهو يحافظ على التفوق بالإمكانيات والتجهيزات بينه وبين دولة فلسطين، حيث لا يسمح بإدخال أي معدات متطورة تتعارض مع سيطرته التكنولوجية على الفضاء الإلكتروني الفلسطيني مما يجعل هناك نقص في البرامج والأدوات التقنية المختصة للمساعدة في عملية التحقيق الجنائي مقارنة بالتطور الهائل والسريع للتقنية.

أما في ما يخص قلة خبرة أجهزة العدالة من مأموري ضبط وسلطة تحقيق في التعامل مع الجرائم الإلكترونية، فالعاملين في وحدة الجرائم الإلكترونية والنيابة والمحاكم يعملون بكل ما هو متاح لديهم من أجل السيطرة على الجرائم الإلكترونية وملاحقة مرتكبيها، وهو ما توافق مع ما توصلت إليه دراسة (العتيبي، 2016) بعنوان "دور التحريات والبحث الجنائي في الكشف عن الجرائم المعلوماتية"، حيث توصلت إلى أن هناك حاجة لتعزيز مستوى التحري، ورفع قدرات المحققين في الدوائر الإلكترونية وإطلاعهم باستمرار على كل المستجدات في مجال الجريمة الإلكترونية ليكونوا على إطلاع كامل

وجهوزية مطلقة، كذلك ما توصلت إليه دراسة كوزياريسك ولي (Koziarski, & Lee, 2020) التي حملت عنوان (Connecting evidence-based policing and cybercrime) والتي هدفت إلى الكشف عن التحديات المرتبطة بمكافحة الجرائم الإلكترونية والتي أظهرت وجود احتمالية ضعيفة بأن تؤدي نماذج الشرطة القائمة على الأدلة في مكافحة الجرائم الإلكترونية على تحسين فعالية الأساليب الحالية والمستقبلية لتدريب وتجنيد الضباط على مكافحة الجرائم الإلكترونية، فضلاً عن عدم كفاية استعداد الضباط ووعيهم بالجرائم الإلكترونية المختلفة، فالجريمة الإلكترونية تتطور بشكل مستمر ومتسارع إلا أن القوانين والأنظمة والتقنيات الموضوعة لمواجهتها لا تتقدم بنفس حداثتها وسرعتها، وذلك يخلق صعوبات أمام الجهات المختصة بمواجهتها والتصدي لها.

مما سبق نستنتج أن الصعوبات التي تواجه التحقيق في الجرائم الإلكترونية كثيرة كونها من الجرائم المستحدثة والغريبة عن المجتمع، وغريبة أيضاً عن هيئات العدالة الجنائية، إلى جانب أنها متطورة باستمرار لذلك فإن مؤسسات المجتمع بشقيها (الأمني والمدني) بحاجة إلى تكاتف جهودها ووضع خطط مشتركة ووقت أكثر لتكون قادرة على التعامل مع هذه الجرائم بالطريقة المناسبة، فالوسائل التكنولوجية والأجهزة الإلكترونية خلقت للأفراد سبلاً لتحقيق أهدافهم حتى ولو كانت بالطرق غير المشروعة بطريقة سهلة وبسيطة رغم عدم قدرتهم على تحقيق هذه الإهداف على أرض الواقع، فقد يكون هدف الشخص تحقيق مكاسب ومرابح مادية إلا أنه نظراً لارتفاع نسبة البطالة وقلة فرص العمل وانخفاض نسبة الأجور قد يلجأ الفرد إلى تحقيق طموحه بالوسائل غير المشروعة كونه يمتلك خبرات تمكنه من ذلك مثل اختراق الحسابات المالية أو البنوك أو عن طريق تهديد الآخرين وابتزازهم لتحقيق مكاسب مادية، فهو يرتكب جريمة إلكترونية في سبيل تحقيق هدفه وفسرت ذلك نظرية تباين الفرص والتي ترى أن السلوك المنحرف جاء نتيجة للفجوة بين الأهداف والوسائل وأن الكثير من الممارسات الجانحة ما هي إلا وسائل تأقلم للضغوط البنائية وأن التناقض واضح بين الطموحات والقنوات المشروعة فعندما يكون لدى الأفراد طموحات معينة وهذه الطموحات تتعارض مع الواقع الذي يعيشه الفرد فإنه يلجأ إلى الطرق غير المشروعة لتحقيق هذا الطموح أو الهدف.

5.2.5 مناقشة النتائج المتعلقة بالسؤال الخامس:

ما مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية؟

أشارت النتائج إلى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية جاءت بدرجة عالية وبنسبة مئوية (80.8%)، إذ بلغ المتوسط

الحسابي للدرجة الكلية (4.16)، حيث تبين أن من أهم آليات الوقاية تمثلت في تنمية الثقة بين المواطنين والعاملين في هيئات العدالة الجنائية، وضرورة إصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة، إلى جانب أهمية عمل رقم موحد لدى جهات الاختصاص للتبليغ فوراً عن التعرض للجريمة الإلكترونية، والحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب، ووجوب تطوير قدرات العاملين في مجال الجرائم الإلكترونية من خلال (التدريب، المؤتمرات، ورشات العمل).

تبين النتائج إلى أن من أهم آليات الوقاية التي يجب القيام بها من قبل العاملين في هيئات العدالة الجنائية تنمية الثقة بين المواطنين والعاملين في هيئات العدالة الجنائية، كون المواطنيين هم ضحايا الجرائم الإلكترونية وهم المتضرر الأول منها، وفي حال كان هناك توافق وتفاهم من قبل هيئات العدالة الجنائية مع المواطنين فإنهم سوف يكونوا شركاء في عملية التصدي للجرائم الإلكترونية من خلال التزامهم بالتعليمات الوقائية الصادرة عن هيئات العدالة الجنائية سواء من خلال القوانين المفروضة أو من خلال التوعية الإعلامية، وسوف يسرعون للإبلاغ عن الجرائم في حال وقوعهم ضحايا لها فهم يثقون بأجهزة إنفاذ القانون وأنهم سوف يتوصلون إلى الجاني وسوف ينال العقاب المناسب على السلوك الإجرامي الذي ارتكبه.

هذا من جانب ومن جانب آخر تم التأكيد على ضرورة إصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة، فعند إصلاح النزلاء مرتكبي الجرائم الإلكترونية نحد من فرصة عودهم لارتكاب الجرائم، فهم عند انتهاء مدة عقوبتهم سوف يعودون لحياتهم المعتادة التي تعد وسائل الاتصالات وتكنولوجيا المعلومات جزءاً أساسياً منها فلضمان عدم عودتهم لارتكاب هذه الجرائم يجب التأكد من إصلاحهم وتأهيلهم والبحث عن المسببات التي دفعتهم لارتكاب السلوك الإجرامي فالداوفع لارتكاب الجرائم الإلكترونية متعددة ولعل من أهمها الدوافع المادية الناتجة حسب النظرية الصراعية عن الصراع الطبقي في الوقت الراهن والذي تروج له وتنميه مواقع التواصل الإجتماعي، فعندما يرتكب هؤلاء الأفراد الجرائم الإلكترونية يقع على عاتق هيئات العدالة الجنائية كونهم جهات إنفاذ قانون إصلاحهم وتأهيلهم لإعادة دمجهم في المجتمع فهم جزء لا يتجزأ منه، وحث جهات تشريع القوانين على إصدار قوانين تدعو لإصلاحهم وتأهيلهم بما يتناسب مع قدراتهم وإمكاناتهم.

فيجب عليها أن تسعى أيضاً لحصار دوافع الجناة في مهدها قبل تحولها لسلوك إجرامي، هذا الأمر يحتاج إلى تنسيق وتعاون بين هيئات العدالة الجنائية ومؤسسات المجتمع المدني حيث يجب عليها جميعاً التكاتف لوضع خطة استراتيجة تفرض على كل مؤسسة منها ممارسة الدور الوقائي من الجرائم الإلكترونية، إلى جانب تخصيص رقم للتبليغ فوراً عند التعرض للجريمة الإلكترونية، وتكثيف حملات

التوعية والإرشاد بما يتناسب مع دور ووظيفة كل مؤسسة من هذه المؤسسات والتركيز على التوعية الإعلامية كونها جزء من عالم التكولوجيا والاتصالات فوسائل الإعلام تعمل كجسر تواصل بين هذه المؤسسات والجمهور، وبهذا التعاون يفرض جو من الأمان للأفراد في المجتمع من خلال ما تقوم به المؤسسات من تأمين للحرية والحقوق الخاصة بحياتهم ويمنع المجرمين من الوصول إليهم أو السيطرة على الضحية في حال وقوع الجريمة.

وعلى صعيد وجوب تطوير قدرات العاملين في مجال الجرائم الإلكترونية من خلال (التدريب، المؤتمرات، ورشات العمل)، فهم بحاجة إلى دورات مستمرة ليكونوا على إطلاع دائم حول جميع مستجدات الجرائم الإلكترونية من حيث ظهور أنواع جديدة منها، والتطورات التي يدخلها مرتكبي الجرائم الإلكترونية على أساليب ارتكابهم لها، فركزت الكثير من الدراسات على ضرورة تدريب الكادر العامل في الجريمة الإلكترونية بشكل دائم، كما في دراسة كل من (النجاجره،2019) بعنوان "خصوصية التحقيق في الجرائم الإلكترونية" والتي بينت أنه يتم إجراء التفتيش والضبط في الجرائم الإلكترونية من خلال مجموعة من الإجراءات التقنية الفنية والتي تحتاج إلى كوادر متخصصة قادرة على تحقيق أهداف التفتيش وضبط الأدلة القانونية الإلكترونية، وأوصت بضرورة إعداد مأموري ضبط قضائي وأعضاء نيابة عامة وقضاة لديهم القدرة الفنية على البحث والتحقيق والمحاكمة في مجال الجرائم الإلكترونية، ودراسة (بغدادي، 2018) بعنوان "وسائل البحث والتحري عن الجرائم الإلكترونية "، والتي بينت أنه من الضروري لجهات التحقيق أن يتوفر لديهم كوادر بشريه قادرة على البحث والتحري في الجرائم الإلكترونية بواسطة الوسائل الحديثة.

إضافة لما سبق إن من أهم الآليات لرفع مستوى الأداء في مواجهة سياسات الاحتلال تكون من خلال التدريب بشكل مستمر والاطلاع على كل ما هو مبتكر وحديث في عالم الجرائم الإلكترونية، وقد بينت (مرداوي،2021) أنه قد يكون من الصعب السيطرة على الشبكات الإسرائيلية، فتكون آلية الوقاية من خلال توعية الأفراد بالتقليل من استخدامها كونها تستخدم لارتكاب الجرائم الإلكترونية ولا يسجل اسم المستخدم أيضاً ويمكن التخلص منها مما يعني صعوبة تعقبها، إلى جانب توعيتهم بعد التعاطي مع الأرقام المجهولة أو الأرقام المخفية كونها من مصدر مجهول.

إن ما سبق يبين أن آليات الوقاية المقترحة واقعية وبالإمكان تنفيذها، إذ يمكن استخدامها وتطبيقها لتحقيق مستوى متقدم في الحد من الجريمة الإلكترونية، فتوعية الأفراد من خلال دروس توعوية في التلفاز والنشرات والندوات التي توجه الأفراد نحو الطريقة السليمة لاستخدام وسائل الاتصال والتكنولوجيا، كالحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب، والعمل على تغيرها بشكل دوري، وتجنب فتح أي رسائل إلكترونية مجهولة المصدر

ووجوب فصل جهاز الحاسوب عن شبكة الإنترنت في حالة عدم الاستخدام، فهذ الآليات البسيطة إذا أصحبت جزء من روتين حياتهم اليومي في تعاملهم مع وسائل التكنولوجيا والاتصال تقيهم من الوقوع ضحايا للمجرمين الذين يستغلون هذه الثغرات لارتكاب فعلهم الإجرامي.

إن آليات الوقاية المقترحة بدءاً من تبادل هيئات العدالة الجنائية المعلومات فيما بينها حول الجرائم الإلكترونية وانتهاءاً بإصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة، آليات وقائية يمكن تعزيز عملها على أرض الواقع، وذلك في سبيل مواجهة الجرائم الإلكترونية التي تهدد أمن واستقرار المجتمعات في الوقت الراهن.

3.5 مناقشة نتائج فرضيات الدرسة:

1.3.5 النتائج المتعلقة بالسؤال السادس:

هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) المتوسطات الحسابية لإجابات المبحوثين حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية تعزى لمتغيرات (الجنس، العمر، المستوى التعليمي، الخبرة العملية)؟

1.1.3.5 نتائج الفرضية الأولى: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) المتوسطات الحسابية لإجابات المبحوثين حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية تعزى لمتغير الجنس".

يتبين أنّه لا توجد فروق في درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الجنس، وبذلك تم قبول الفرضية الأولى، يمكن تفسير هذه النتيجة بأن العاملين في هيئات العدالة الجنائية من الذكور والإناث لديهم نفس التصورات حول درجة الصعوبات التي تواجههم في مواجهة الجرائم الإلكترونية، فالإجراءات المتبعة من قبلهم متكاملة وتهدف جميعها إلى مواجهة الجرائم الإلكترونية منذ لحظة وقوعها إلى حين إلقاء القبض على مرتكبها ومحاسبته وفق القانون، فالصعوبات التي تواجههم تعيق عملهم جميعاً وبنفس الدرجة كون كل إجراء من هذه الإجراءات يهدف إلى تحقيق نتيجة وفي حال وجود عسر في تنفيذ إجراء فذلك سوف يؤثر على منحى السير في الدعوى ككل.

ويرى العاملين في هيئات العدالة الجنائية من الجنسين أن هناك العديد من الصعوبات التي تواجههم تطورت بتطور الجرائم الإلكترونية؛ فمنها ما بتعلق بطبيعة الجريمة وما تتمتع بها من صفات كونه من السهل إخفاؤها وعابرة للحدود ومتطورة بشكل دائم، ومنها ما يتعلق بالمجني عليه كونه يحجم عن الإبلاغ عن الجرائم الإلكترونية، ومنها ما بتعلق بالجاني والذي يتميز بعدد من السمات لعل من أهمها أنه ذكي وغير عنيف إلى جانب أنه يطور أساليبه وفق كل ما هو مستحدث على الوسائل الإلكترونية، بالإضافة إلى قصور التشريعات المحلية والدولية عن مواكبة الجرائم الإلكترونية وتطوراتها، هذا إلى جانب وضع دولة فلسطين كونها تحت الاحتلال والذي بدوره زاد عدد الصعوبات، إلا أن أجهزة العدالة الجنائية تحاول بكل ما هو متاح من أجل تنفيذ الإجراءات المفروضة عند وقوع الجرائم الإلكترونية وضمان قانونيتها لإدانة الجاني ومحاسبته وفق محاكمة عادلة، فجميعهم يسعون إلى تحقيق العدالة والمحافظة على أمن المجتمع واستقراره.

2.1.3.5 نتائج الفرضية الثانية: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات المبحوثين حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر".

أشارت النتائج أنّه توجد فروق دالة إحصائياً في متوسطات درجة الصعوبات التي تواجه هيئات العدالة (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر، وبذلك تم رفض الفرضية الثانية، يمكن تفسير هذه النتيجة بأن العاملين في هيئات العدالة الجنائية لا يمتلكون نفس التصورات فيما يخص درجة الصعوبات التي تواجههم في مواجهة الجرائم الإلكترونية كون المبحوثين من فئات عمرية مختلفة وكون نظرتهم لمفهوم الجرائم الإلكترونية وخصائصها وتصنيفاتها والدوافع لارتكابها وسمات مرتكبيها ونتائجها يختلف وفق الأفكار والمعتقدات التي نشأت عليها كل فئة عمرية منهم، وكل فئة عمرية من المبحوثين تكون وجهة نظرها حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تختلف أيضاً كون كل فئة تتعامل مع المواقف بشكل معين وفق قدراتها وخبراتها المكتسبة.

فيلاحظ أن الفروق كانت بين عمر (من 30- أقل من 40 سنة) و(من 20 سنة – أقل من 30 سنة) لصالح (من 30- أقل من 40 سنة)، وبين عمر (40 سنة فأكثر) و(من 20 سنة – أقل من 30 سنة) لصالح (40 سنة فأكثر)، فنجد أن الفئات العمرية الأكبر سناً من العاملين في هيئات العدالة الجنائية كان لديها توافق أكبر مع وجود العديد من الصعوبات التي تواجهها أثناء مواجهتها للجرائم الإلكترونية، فهذه الجرائم مستحدثة ودخيلة على مجتمعاتنا بل غزت جميع جوانب حياتنا وهذا خلق

فجوة بين الفئات العمرية التي خلقت في ظل وجود هذه الوسائل والتي تستخدمها بكل سهولة ويسر فدرجة الصعوبات ستكون بالنسبة لهم أقل من الفئة العمرية الأكبر التي تحاول فهم هذه التطورات التكنولوجية وآلية التعامل معها لمواكبة تطورها المتسارع مما يضع أمامهم الكثير من العراقيل كونهم معتادين على الوسائل التقليدية، وأجبروا على استخدام الوسائل التكنولوجية لجعلها جزء من روتين حياتهم وهذا بدوره وضعهم أمام العديد من الصعوبات والتحديات، والتي يحاولون جاهدين للتخلص منها.

3.1.3.5 نتائج الفرضية الثالثة: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) المتوسطات الحسابية لإجابات المبحوثين حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي".

أشارت النتائج أنّه توجد فروق دالة إحصائياً في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي، وبذلك تم رفض الفرضية الثالثة، تشير هذه النتيجة إلى أن هناك اختلاف في الآراء حسب المستوى التعليمي للعاملين في هئيات العدالة الجنائية عينة الدراسة، كون المبحوثين يحملون شهادات علمية بمستويات علمية مختلفة وكل مستوى ينظر للجرائم الإلكترونية من منظور معين وبالتالي الصعوبات للحد من الجرائم الإلكترونية تختلف وفق هذا المنظور وأيضاً الصعوبات التي يواجهونها تختلف فما قد يكون معيق لشخص قد لا يكون معيق لشخص آخر كونه بموجب أن مستواه التعلمي قد اكسبه آلية للتعامل مع هذه الصعوبات وأيضاً كل شخص ومن خلال تراكمه المعرفي الذي اكتسبه من خلال سنواته التعليمية اكتسب مفهوم معين حول الجرائم الإلكترونية وبالتالي كون صورة معينة حول الصعوبات التي تعترضه عند مواجهة الجرائم الإلكترونية للحد منها.

فيلاحظ أن الفروق كانت بين المستوى (دراسات عليا) و(ثانوية عامة فأقل) لصالح (دراسات عليا)، وبين المستوى (دراسات عليا) و(دبلوم متوسط) لصالح (دراسات عليا)، وبين المستوى (دراسات عليا) و(بكالوريوس) لصالح (دراسات عليا)، فنجد أن فئة الدراسات العليا كان لديها توافق أكبر من الفئات الأخرى مع وجود العديد من الصعوبات التي تواجه هيئات العدالة الجنائية للحد من الجرائم الإلكترونية، فبحكم خبراتهم المعرفية المتراكمة على طول السنين يدركون مفهوم الجرائم الإلكترونية وخطورتها على المجتمع لما تتمتع به من خصائص والتي من أهمها تطورها بشكل مستمر وهذا بدوره يخلق نوعاً جديداً من التحديات والصعوبات التي تعترضهم أثناء مواجهتهم للجرائم الإلكترونية، فهم يدركون درجة الصعوبات الحالية إلى جانب إداركهم إمكانية ارتفاعها في حال استحدث نوع جديد من

الجرائم الإلكترونية، أو قام أحد مرتكبي الجرائم الإلكترونية بتطوير أسلوبه في ارتكابها، والذي بدوره يزيد من أضرارها ودرجة خطورتها على المجتمع.

4.1.3.5 نتائج الفرضية الرابعة: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) المتوسطات الحسابية لإجابات المبحوثين حول درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية".

يتبين أنّه توجد فروق دالة إحصائياً في متوسطات درجة الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية، وبذلك تم رفض الفرضية الرابعة، يمكن تفسير هذه النتيجة بأن العاملين في هيئات العدالة الجنائية لا يمتلكون نفس التصورات فيما يخص درجة الصعوبات التي تواجههم في مواجهة الجرائم الإلكترونية، كون المبحوثين لهم سنوات خبرة عملية مختلفة فذلك يؤثر على نظرتهم للجرائم الإلكترونية وآلياتهم للتعامل معها عند وقوعها وأيضاً طريقتهم في التصدي لها فهم يدركون كم الصعوبات التي سوف تواجههم أثناء ممارستهم لهذا العمل، فخبراتهم العملية الطويلة تساعدهم في التعامل مع هذه الجرائم كونهم اكتسبوا مهارات وفنيات تخولهم ذلك إلى جانب إيقانهم التام أنهم سوف يواجهون تحديات أثناء عملهم للتصدي للجرائم الإلكترونية فطبيعة هذه الجريمة وخصائصها تفرض ذلك.

حيث يلاحظ أن الفروق كانت بين الخبرة (من 5- أقل من 10 سنوات) و(أقل من 5 سنوات) لصالح (من 5- أقل من 10 سنوات)، وبين الخبرة (من 10- أقل 15 سنة) و(أقل من 5 سنوات) لصالح (من 10- أقل 15 سنة)، وبين الخبرة (من 15- أقل من 20 سنة) و(أقل من 5 سنوات) لصالح (من 15- أقل من 20 سنة)، وبين الخبرة (20 سنة فأكثر) و(أقل من 5 سنوات) لصالح (20 سنة فأكثر)، فنجد أن أن العاملين في هيئات العدالة الجنائية ولديهم سنوات خدمة طويلة لديهم توافق أكبر مع وجود العديد من الصعوبات التي تواجههم أثناء مواجهة الجرائم الإلكترونية للحد منها، فهم بالتأكيد تعاملوا على مدى السنوات الطويلة مع أنواع مختلفة من الجرائم و تبين لهم أن مرتكبيها يتبعون آليات وأساليب متجددة باستمرار عند تنفيذها فلكل جريمة من هذه الجرائم خصوصية وآلية تحقيق معينة لتقصي الحقائق فيها فلا يمكن القياس عليها كما في الجرائم التقليدية، فهم على طول سنوات عملهم كلما عملو على التصدي لصعوبات تواجههم أثناء التحقيق في جريمة معينة وحاولوا إيجاد الحلول لتخطي هذه الصعوبة تظهر صعوبات أخرى كون هذا النوع من الجرائم يتطور باستمرار والذي بدوره يفرض صعوبات جديدة وهذا ما يوقنه من يمتلكون سنوات خبرة طويلة من العاملين في هيئات العدالة الجنائية عينة الدراسة.

2.3.5 النتائج المتعلقة بالسؤال السابع:

هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين المتوسطات الحسابية لإجابات المبحوثين حول مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية تعزى لمتغيرات (الجنس، العمر، المستوى التعليمي، الخبرة العملية)؟

1.2.3.5 نتائج الفرضية الأولى: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين المتوسطات الحسابية لإجابات المبحوثين حول مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية تعزى لمتغير الجنس".

أشارت النتائج أنّه لا توجد فروق في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الجنس، وبذلك تم قبول الفرضية الأولى، يمكن تفسير هذه النتيجة بأن العاملين في هيئات العدالة الجنائية يمتلكون نفس التصورات فيما يخص مستوى آليات الوقاية المتبعة في مواجهة الجرائم الإلكترونية، فهم يسعون للعمل بشكل متكاتف من أجل مواجهة الجرائم الإلكترونية وتطوراتها، ومن خلال وضعهم لآليات الوقاية يسعون للحد من هذه الجرائم، وإن آليات الوقاية تتم ممارستها في جميع الهيئات على حد سواء، وهذه الآليات تتطور بما يتناسب مع حداثة وتطور الجرائم الإلكترونية حتى تحقق الهدف من إيجادها وهو التصدي للجرائم الإلكترونية.

ويرى العاملين في هيئات العدالة الجنائية من الجنسين أن آليات الوقاية إذا ما تم الالتزام بها وتنفيذها سوف تسهم بالحد من الجرائم الإلكترونية فمن خلال هذه الآليات تمارس هي دورها القانوني المخولة به كجهة إنفاذ قانون إلى جانب دورها التوعوي الذي يفرض عليها استقطاب المواطنين للالتزام بجميع التعليمات الصادرة منها حول آليات الوقاية من الجرائم الإلكترونية بل وجعلهم شركاء ولهم دور فعّال في مواجهة الجرائم الإلكترونية للحد منها من خلال توعيتهم بمخاطر الجرائم الإلكترونية وأضرارها على الفرد الواحد وعلى المجتمع ككل.

2.2.3.5 نتائج الفرضية الثانية: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات المبحوثين حول مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر".

أشارت النتائج إلى أنّه لا توجد فروق دالة إحصائياً في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير العمر، وبذلك تم قبول الفرضية الثانية، يمكن تفسير هذه النتيجة بأن العاملين في هيئات العدالة الجنائية على اختلاف أعمارهم يدركون أهمية آليات الوقاية ودورها الأساسي في الحد من الجرائم الإلكترونية، فهم يأكدون على أهمية اتباع هذه الآليات ويوقنون دورهم التوعوي الذي هو جزء من المهام المخولة إليهم فيفرض عليهم تذكير المواطنين بشكل دائم عن مخاطر الجرائم الإلكترونية وآثارها السلبية والإجراءات التي يجب أن يتبعونها للوقاية منها قبل وقوعها وأيضاً الإجراءات التي يجب أن يتبعونها في حال وقوعهم ضحايا لها، إلى جانب وعيهم وإدراكهم إلى أن هذه الآليات يجب أن تتبع من قبلها بالتعاون مع مؤسسات المجتمع المدني والتي تساهم بشكل أساسي في مواجهة الجرائم الإلكترونية.

3.2.3.5 نتائج الفرضية الثالثة: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) المتوسطات الحسابية لإجابات المبحوثين حول مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي".

أشارت النتائج إلى أنّه توجد فروق دالة إحصائياً في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير المستوى التعليمي، وبذلك تم رفض الفرضية الثالثة، يمكن تفسير هذه النتيجة بأن هناك اختلاف في الآراء حسب المستوى التعليمي للعاملين في هئيات العدالة الجنائية عينة الدراسة فيما يخص مستوى آليات الوقاية المتبعة في مواجهة الجرائم، كون المبحوثين يحملون شهادات علمية بمستويات مختلفة وكل مستوى ينظر للجرائم الإلكترونية من منظور معين وبالتالي ضرورة وجود مستوى مرتفع من آليات الوقاية من هذه الجرائم تختلف وفقاً لهذا المنظور وأيضاً درجة إدراكهم لأهمية وفعّالية وجود آليات وقائية من الجرائم الإلكترونية بدرجة عالية وذلك لمحاولة السيطرة عليها والحد منها، فالأشخاص من خلال تراكمهم المعرفي الذي يكتسبونه من خلال سنواتهم التعليمية يكتسبون مفهوم معين حول الجرائم الإلكترونية وبالتالي تكوين صورة معينة حول آليات الوقاية التي يجب اتباعها لمواجهة الجرائم

الإلكترونية والتي يجب تطويرها باستمرار بما يتناسب وحداثتها وذلك للحد من انتشارها لما لها من آثار سلبية تنعكس على المجتمع ككل.

فالفروق كانت بين المستوى (بكالوريوس) و(ثانوية عامة فأقل) لصالح (بكالوريوس)، وبين المستوى (بكالوريوس) و(دبلوم متوسط) لصالح (بكالوريوس)، فنجد أن فئة البكالوريس كان لديها توافق أكبر من الفئات الأخرى مع ضرورة وجود آليات وقاية مُتبعة من قبل هيئات العدالة الجنائية للحد من الجرائم الإلكترونية، فبحكم خبراتهم المعرفية المتراكمة من دراستهم لتخصصات علمية معينة يدركون مفهوم الجرائم الإلكنترونية وخطورتها على المجتمع لما تتمتع به من خصائص والتي من أهمها تطورها بشكل مستمر وهذا بدوره يفرض عليهم تطوير آليات الوقاية لمواجهتها والحد منها بما يتناسب معها، فهم يدركون أهمية وجود آليات الوقاية المتبعة إلى جانب إداركهم أهمية تطويرها بما يتناسب مع حداثة وتطور هذه الجريمة فالآلية التي قد تكون مجدية في مرحلة تكون غير مؤثرة في مرحلة أخرى كون مرتكبي هذه الجرائم وجدوا أساليب إجرامية تمكنهم من تخطيها وتجاوزها، فبقدر وجود أهمية لإجراءات مكافحة الجرائم الإلكتؤرونية وضرورة تحديثها من حين لآخر من أجل إلقاء القبض على مرتكبيها يجب تطوير آليات الوقاية لمنع الجريمة الإلكترونية قبل وقوعها أو على الأقل الحد منها .

4.2.3.5 نتائج الفرضية الرابعة: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) المتوسطات الحسابية لإجابات المبحوثين حول مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية".

أشارت النتائج إلى أنّه لا توجد فروق دالة إحصائياً في متوسطات مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية يعزى لمتغير الخبرة العملية، وبذلك تم قبول الفرضية الرابعة، يمكن تفسير هذه النتيجة بأن العاملين في هيئات العدالة الجنائية يمتلكون نفس التصورات فيما يخص مستوى آليات الوقاية المتبعة في مواجهة الجرائم الإلكترونية، فمهما بلغت الخبرة العملية للأشخاص العاملين في هيئات العدالة الجنائية فهم مخولين للقيام بوظيفتين الأولى الوظيفة القضائية والتي تتضمن القيام بالإجراءات وقفاً لما هو محدد قانوناً وتكون بعد وقوع الجرائم على اختلاف أشكالها ومن ضمنها الجرائم الإلكترونية والوظيفة الإدارية والتي تتمثل بالأعمال الوقائية التي تتبعها هذه الهئيات لمنع وقوع الجرائم فجميع العاملين هيئات العدالة الجنائية مدركون لطبيعة عملهم والمهام المطلوبة منهم مهما كانت خبراتهم العملية مختلفة.

4.5 ملخص النتائج :

أشارت نتائج الدراسة إلى:

- أن مستوى الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية جاءت بدرجة مرتفعة، وبنسبة مئوية (86.4%).
- أن هناك استجابة سريعة من قبل وحدة الجرائم الإلكترونية في الشرطة لشكاوى المواطنين حول الجرائم الإلكترونية، حيث جاء ذلك بنسبة مرتفقة بلغت (90.6%).
- أن مستوى الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة مئوية (95%).
- أن من أهم الإجراءات التي تلتزم بها النيابة العامة هي: العمل على تسهيل تحويل شكاوى الجرائم الإلكترونية من خلال النيابات الجزئية، والتحقيق في الشكاوى المتعلقة بالجرائم الإلكترونية وفقاً للإجراءات التي تتناسب وخصوصية كل نوع من أنواعها، والعمل على توثيق محاضر التحقيق وفق الإجراءات القانونية المحددة، والتعامل مع المضبوطات ذات العلاقة بالجريمة الإلكترونية وفقاً للإجراءات القانونية المحددة، إلى جانب التعاون مع المختبر الجنائي التابع لوحدة الجرائم الإلكترونية للتعامل مع الدليل المضبوط من مسرح الجريمة الإلكترونية، حيث جاءت جميعها بدرجة مرتفعة بلغت (100%).
- أن مستوى الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية جاءت بدرجة مرتفعة، وبنسبة مئوية (85%).
- أن القضاة يلتزمون بالتشريعات النافذة في مواجهة الجرائم الإلكترونية، ويمتلكون القدرة على وزن البينات الفنية في الجرائم، ويستعينون بالخبراء الفنيين في مجال الجرائم الإلكترونية فهذه الإجراءات جاءت جميعها بدرجة مرتفعة بلغت (93.4%).
- أن الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية جاءت بدرجة عالية، وبنسبة مؤية (85.6%)، وكان أهم تلك الصعوبات قلة وعي المجتمع بالجريمة الإلكترونية، إذ جاءت هذه الصعوبة بدرجة عالية بلغت(86.6%).
- أن مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية للحد من الجرائم الإلكترونية جاءت بدرجة عالية، فمن أهم تلك الآليات تنمية الثقة بين المواطنين والعاملين في هيئات العدالة الجنائية، وإصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة، وعمل

رقم موحد لدى جهات الاختصاص للتبليغ فوراً عند التعرض للجريمة الإلكترونية، وجاءت هذه الآليات بدرجة كلية (82.3%).

- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة في درجة الصعوبات التي تواجه هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تبعاً لمتغير الدراسة (الجنس).
- وجود فروق ذات دلالة إحصائية عند مستوى الدلالة في درجة الصعوبات التي تواجه هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تبعاً لمتغيرات الدراسة (العمر، المستوى التعليمي، الخبرة العملية).
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة في مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تبعاً لمتغيرات الدراسة (الجنس، العمر، الخبرة العملية).
- توجد فروق ذات دلالة إحصائية عند مستوى الدلالة في مستوى آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية للحد من الجرائم الإلكترونية تبعاً لمتغير الدراسة (المستوى التعليمي).

5.5 توصيات الدراسة:

تتمثل توصيات الدراسة بما يلي:

- ضرورة قيام جهاز الشرطة الفلسطيني كونه على تماس مباشر مع الجمهور بتمنية الثقة مع المواطنين، وتوعيتهم بماهية الجرائم الإلكترونية، وأهمية الإبلاغ عنها في حال وقوعهم ضحايا لها، وأهمية الدليل الرقمي في الإثبات وإدانة الجاني وكيفية التعامل معه وعدم العبث به للحفاظ عليه من الاندثار.
- ضرورة التعاون بين هيئات العدالة الجنائية(الشرطة، النيابة العامة، القضاء) لوضع خطة استراتيجية لمكافحة الجرائم الإلكترونية، وذلك ليتمكنوا من الكشف عن الجرائم الإلكترونية فور الإبلاغ عنها، ووضع خطة استراتيجية للتوعية بالجرائم الإلكترونية ومخاطرها وتهديدها لأمن المجتمع واستقراره.
- ضرورة الاهتمام بتعزيز العاملين في جهاز الشرطة، وذلك بتدريبهم على كيفية التعامل مع الجريمة الإلكترونية حين وقوعها، وتدريبهم على كيفية التعامل مع مسرح الجريمة الإلكترونية وكيفية ضبط الدليل الرقمي وحفظه ورفع عددهم، وتزويدهم بالبرامج والأدوات التقنية المختصة للمساعدة في عملية التحقيق الجنائي بما يتواكب مع التطور الهائل والسريع للتقنية.
- ضرورة قيام العاملين في هيئات العدالة الجنائية (الشرطة، النيابة العامة، القضاء) من نفس الهيئة بعمل اجتماعات دورية حول واقع الجريمة الإلكترونية والصعوبات التي تواجههم وآليات الوقاية المتبعة للحد منها، فالأقسام في الهيئة تعمل بشكل متكامل ويمكن الاستفادة من الخبرات المختلفة للأفراد على اختلاف مستوى فئاتهم العمرية والتعليمية وسنوات خبرتهم.
- ضرورة قيام المجلس التنسيقي الأعلى لقطاع العدالة بالمتابعة الحثيثة لموضوع الجرائم الإلكترونية والآليات المتبعة من قبل هيئات العدالة في سبيل مواجهتها وتداوله بشكل متكرر خلال اجتماعاته، ودراسة التشريعات المتعلقة بالجرائم الإلكترونية وتعديلها باستمرار بما يتناسب مع حداثتها وتطورها.
- حث المشرع الفلسطيني النص بوضوح على إجراءات التفتيش المتبعة في الجرائم الإلكترونية فقانون الإجراءات الجزائية الفلسطيني وضح إجراءات التفتيش المتعلقة بالجرائم التقليدية في حين أن القرار بقانون بشأن الجرائم الإلكترونية لم يتضمن أية مواد حول آلية التفتيش الواجب اتباعها عند وقوعها.

- حث المشرع الفلسطيني للعمل على مواءمة التشريعات الوطنية التي تتعلق بالجرائم الإلكترونية مع الاتفاقيات الدولية ذات الاختصاص في الجرائم الإلكترونية التي انضمت فلسطين إليها.
- ضرورة عمل مراكز الإصلاح والتأهيل على إصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة، والتركيز على تزويدهم ببرامج إصلاحية تتناسب وقدراتهم وإمكاناتهم العلمية والعملية لحين انتهاء مدة العقوبة المفروضة عليهم.
- حث مراكز الإصلاح والتأهيل على إعداد برامج رعاية لاحقة لمرتكبي الجرائم الإلكترونية والذين أنهوا مدة عقوبتهم ووجب الإفراج عنهم، وتوجيههم نحو استخدام وسائل الاتصالات وتكنولوجيا المعلومات بالطرق السليمة وتذكيرهم بأنهم يمكن أن يسخروها لخدمتهم بالطريق الإيجابية فيكون
- تعمل هيئات العدالة الجنائية (القضاء، النيابة، الشرطة) على حث المواطنين على الإحجام عن استخدام الشبكات الإسرائيلية، واللجوء إلى الشبكات الفلسطينية إلى جانب العمل على توجيه شركات الاتصالات الفلسطينة على تخفيض أجور الخدمات التي تقدمها لكي يكون هناك إقبال من قبل المواطنين عليها. وذلك للحد من ارتكاب الجرائم الإلكترونية من خلال الشبكات الإسرائيلية.
- حيث هيئات العدالة الجنائية (الشرطة، النيابة العامة، القضاء) على تكريس وسائل الاتصالات وتكنولوجيا المعلومات في الكشف عن الجرائم واستخدام تقنيات الذكاء الاصطناعي للتحقيق في فيها وفهم مسرح الجريمة فهو يخلق صوراً تحاكي الواقع وهذا يساعدنا على بناء تصور فعلي عن كيفية ارتكاب الجريمة عند وقوعها.
- عمل هيئات العدالة الجنائية (الشرطة، النيابة العامة، القضاء) على استقطاب الأشخاص ذوي المهارات الفنية العالية في استخدام وسائل الاتصالات وتكنولوجيا المعلومات أو ما يسمى بالهاكرز للاستفادة من خبراتهم في سبيل توظيفها في مكافحة الجرائم الإلكترونية.
- حث وسائل الإعلام على عرض القضايا المتعلقة بالجرائم الإلكترونية ومخاطرها وآثرها على الفرد والمجتمع ككل، مما يساعد على تكوين رأي عام لقبول وفهم الإجراءات المتبعة عند وقوع الجرائم الإلكترونية إلى جانب تطبيق آليات الوقاية منها للحد من انتشارها من خلال وسائل الإعلام.
- يجب على الباحثين والمهتمين تناول موضوع الجرائم الإلكترونية وطرق مكافحتها وآليات الوقاية المتبعة لمواجهتها، ذلك من خلال التطرق إلى استطلاع آراء عينات مختلفة لتوضيح جميع وجهات النظر، لما لذلك من أهمية كبيرة في المساهمة للحد منها.

قائمة المصادر والمراجع:

أولاً: المراجع العربية:

- أبو عواد، ر. (2017): مكونات عمل الشرطة الفلسطينية في مجال الوقاية من الجريمة من وجهة نظر ضباطها في محافظات الخليل ورام الله ونابلس. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس.
- أبو هربيد، ع. (2009): أهمية القضاء في الإسلام، بحث مقدم لليوم الدراسي ديوان المظالم ودوره في تحقيق العدالة الشاملة في المجتمع الذي تنظمه كلية الشريعة والقانون، الجامعة الإسلامية.
- الأحمد، أ. (2008): المتهم ضماناته وحقوقه في الاستجواب والتوقيف" الحبس الاحتياطي" في قانون الإجراءات الجزائية الفلسطيني" دراسة مقارن". (رسالة ماجستير غير منشورة). فلسطين: جامعة النجاح الوطنية.
- أحمد، ط. (2015): الإدلة الإلكترونية ودورها في الإثبات الجنائي دراسة مقارنة. الطبعة الأولى. دار النهضة العربية للنشر والتوزيع. القاهرة.
- الأطرش، ع. والهاجري، د. (2021): المدخل الى علم الاجرام. دار الثقافة للنشر والتوزيع. عمان.
- الأطرش، ع، وعساف، م. (2019): معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية، مجلة جامعة الشارقة للعلوم القانونية. 16 (1)، ص ص 632- 662.
- إيديو، ل. (2020): دور مؤسسات التنشئة في الوقاية من مخاطر الجريمة الواقعة على الأشخاص عبر شبكات المعلومات (الإنترنت)، مجلة الباحث في العلوم الإنسانية والاجتماعية. 12 (5)، ص ص 341- 356.
- البطاط، ر. (2017): سياسات الدعم والتمويل من الاتحاد الأوروبي لجهاز الشرطة الفلسطينية 2006 -2016. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس-أبوديس.
- بغدادي، أ. (2018): وسائل البحث والتحري عن الجرائم الإلكترونية. (رسالة ماجستير غير منشورة). فلسطين: جامعة النجاح الوطنية.
- التميمي، د. (2019): جريمة الابتزاز الإلكتروني "دراسة مقارنة". (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس.

- جعبري، ش. (2019): الطبيعة القانونية للنيابة العامة الفلسطينية(دراسة مقارنة). (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس.
- الجنابي، ل. (2017): فعالية القوانين الوطنية والدولية بشأن الجرائم الإلكترونية، مجلة الأكاديمية العربية المفتوحة بالدنمارك. (20)، ص ص41- 98.
- الجهاز المركزي للإحصاء الفلسطيني (2023): القضاة في الضفة الغربية حسب نوع المحكمة والجنس. منشورات الجهاز المركزي للإحصاء الفلسطيني. رام الله.
- الجهاز المركزي للإحصاء الفلسطيني (2023): عدد أعضاء النيابة العامة في فلسطين حسب مكان العمل والجنس. منشورات الجهاز المركزي للإحصاء الفلسطيني. رام الله.
- الجهاز المركزي للإحصاء الفلسطيني (2023): عدد أفراد الشرطة حسب القيادة العامة والمحافظة والجنس. منشورات الجهاز المركزي للإحصاء الفلسطيني. رام الله.
- جواد، أ. (2015): الجريمة المعلوماتية أو الإلكترونية: أنواعها وخصائصها وطرق الوقاية منها، مجلة الدراسات المالية والمصرفية. 23 (1)، ص ص29- 33.
- حريبات، آ. (2023): "تفويض مأموري الضبط القضائي في التحقيق لابتدائي". (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس أبو ديس.
- حمد، م. (2017): استقلال القضاء: دراسة مقارنة بين الشريعة الإسلامية وقانون السلطة القضائية الفلسطيني، مجلة الحقوق والعلوم السياسية. 8 (1)، ص ص 1-19.
- خلدون، ع. (2012): الطبيعة الخاصة للجريمة الإلكترونية وصورها، دراسات وأبحاث. (9). ص ص 113- 127.
- خلف، ج. (2009): الضبط القضائي في جرائم الإنترنت، مجلة جامعة ذي قار. 4 (4)، ص ص1- 26.
- خليلي، س. (2017): خصوصية المجرم الإلكتروني، مجلة الفكر. (15)، ص ص401- 414.
- الخواجة، م. (2005): الانحراف والمجتمع. الطبعة الأولى. دار مصطفى للنشر والتوزيع. القاهرة.
- درعاوي، ج. (2018): دور العرف العشائري في الحد من جريمة القتل في جنوب الضفة الغربية وسبل تطويره من وجهة نظر ذوي الاختصاص. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس.
- درف، ع. (2006): متطلبات هيئة الادعاء في الجرائم الإلكترونية، مجلة العدل. 18 (18)، ص ص 306- 322.

- ذياب، س. وبوترعة، ب. (2020): الجريمة الإلكترونية: الأسس والمفاهيم، مجلة تطوير العلوم الاجتماعية. 13 (1)، ص ص7- 20.
- ربايعة، ع. (2016): الجرائم الإلكترونية- التجريم والملاحقة والإثبات، المؤتمر الأول للجرائم الإلكترونية في فلسطين، نابلس: جامعة النجاح الوطنية.
- رحال، ن. (2019): الضبط الاجتماعي ودوره في مكافحة الجريمة والانجراف، مجلة الحقوق العلوم السياسية. (11)، ص ص312- 336.
- الردفاني، محمد قاسم أسعد (2014): تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية. 31 (61)، ص ص 157 – 192.
- زبيدي، ب. وحفوظة، أ. (2017)، واقع جرائم تكنولوجيا الإعلام والاتصال في العالم وآليات مكافحتها، مجلة الدراسات الاقتصادية المعاصرة. (3)، ص ص77- 86.
- زرارة، خ. (2014): الجريمة والمجتمع: دراسة مقارنة، الطبعة الأولى. دار وائل للنشر. عمان.
- سلامه، ن. (2023): الجرائم الإلكترونية وأثرها على المجتمع، مجلة القاهرة للخدمة الاجتماعية. (39)، ص ص389- 422.
- سليمان، و. (2011): دور المؤسسة الشرطية في مساعدة مؤسسات المجتمع المدني على أداء دورها التنموي في مؤسسات الضفة الغربية. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس المفتوحة.
- شرباتي، إ. (2015): الطعون العادية في الدعوى الجزائية"دراسة مقارنة". (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس- أبوديس.
- الشهري، ح. (2011): قانون دولي موحد لمكافحة الجرائم الإلكترونية: تصور مقترح. المجلة العربية للدراسات الأمنية. 27 (53)، ص ص 4- 54.
- شهوان، و. (2018): دور المؤسسة الأمنية في الحد من الجرائم المستحدثة في الضفة الغربية من وجهة نظر ذوي الاختصاص. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس.
- صبره، أ. (2017): دور الشراكة الاوروبية الفلسطينية في تخطيط وتطوير عمل جهاز الشرطة الفلسطينية. (رسالة ماجستير غير منشورة). فلسطين: جامعة النجاح الوطنية.
- صعابنه، م. (2011): دور النيابة العامة في إقامة الدعوى العمومية في فلسطين دراسة مقارنة. (رسالة ماجستير غير منشورة). فلسطين: جامعة النجاح الوطنية.
- طاهر، م. (2017): القناعة الوجدانية للقاضي الجزائي. (رسالة ماجستير غير منشورة). فلسطين: جامعة النجاح.

- الطناطي، ر. (2010): مهارات رجل الشرطة في التعامل مع الجمهور وأثرها على فعالية تقديم الخدمة الأمنية "دراسة تطبيقية على رجال الشرطة العاملين بمحافظة غزة". (رسالة ماجستير غير منشورة). غزة: الجامعة الإسلامية.
- عبد الباقي، م. (2015): شرح قانون الإجراءات الجزائية الفلسطيني رقم(3) لسنة (2001) "دراسة مقارنة"، الطبعة الأولى. دار الثقافة والنشر. عمان.
- عبد الباقي، م. (2018): التحقيق في الجريمة وإثباتها في فلسطين دراسة مقارنة، مجلة دراسات علوم الشريعة والقانون بالجامعة الأردنية. 4 (45)، ص ص284- 299.
- العتيبي، س. (2016): دور البحث الجنائي في الكشف على الجرائم المعلوماتية. (رسالة دكتوراه غير منشورة). الرياض: جامعة نايف العربية للعلوم الأمنية السعودية.
- العكلة، و. (2012): التعاون الدولي في مواجهة جرائم الإنترنت، مجلة العلوم الاقتصادية والإدارية. 18 (68)، ص ص322- 334.
- عمايره، م. (2023): "التعاون الدولي في مواجهة الجريمة الإلكترونية". (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس.
- عموري، أ. (2018): التفتيش في الجرائمالإلكترونية. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس أبو ديس.
- عيسى، م. (2016): التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني. 14 (2)، ص ص50- 66.
- غباري، ث. (2018): الشروع في الجريمة "دراسة فقهية مقارنة. (رسالة ماجستير غير منشورة). جامعة النجاح، فلسطين.
- الفتلاوي، ص. (2016): جريمة الإرهاب الإلكتروني، مجلة القانون للدراسات والبحوث القانونية. (13).
- قراريه، أ. (2017): سلطات مأموري الضبط القضائي في النظام الجزائي الفلسطيني دراسة مقارنة. (رسالة ماجستير غير منشورة). فلسطين: جامعة النجاح الوطنية.
- القشوش، هـ. (2007): جرائم الحاسب الآلي في التشريع المقارن. الطبعة الأولى. الجامعية للنشر والتوزيع. الاسكندرية.
- قلالوة، ع. (2020): التنظيم القانوني للمختبرات ودورها في تحقيق العدالة الجنائية. (رسالة ماجستير غير منشورة). جامعة النجاح ، فلسطين.
- الكبيسي، ن. (2010): الأمية والجريمة: دراسة نظرية وميدانية على عينة من النزلاء بسجون جمهورية مصر العربية، المؤتمر السنوي الثامن، مركز تعليم الكبار، مصر: جامعة عين شمس، ص ص961 – 937.

- الكسواني، ج. (2019): الإجراءات الجزائية في التشريع وفقه القضاء والفقه. الطبعة الأولى. مركز راصد للدراسات والتدريب بالمحاماة. فلسطين
- كلاب، ع. وعباسة، ط. (2019): المخاطر والجرائم المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات الحديثة. مجلة بحوث. (12).
- المدبوح، م. (2018): طرق الطعن غير العادية في الأحكام الجزائية "دراسة مقارنة". (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس– أبوديس.
- مرداوي، ح. (2021): دور المؤسسة الأمنية في الحد من الجرائم الإلكترونية الأمن الوقائي أنموذجاً. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس.
- مسمار، م.؛ والكريمين، أ. (2019): تحديات إثبات الجرائم الإلكترونية: دراسة قانونية، مجلة الدراسات الأمنية. (15)، ص ص 78–102.
- مصري، ص. (2020): علاقة النيابة العامة بمأمور الضابطة القضائية في قانون اصول المحاكمات الجزائية الفلسطيني. (رسالة ماجستير غير منشورة). فلسطين: جامعة النجاح الوطنية.
- المصري، ن. (2017): خصوصية الجرائم المعلوماتية، رسالة ماجستير غير منشورة، فلسطين: جامعة النجاح الوطنية.
- مصطفى، إ. والزيات، أ.، حامد والنجار، م. (2011): المعجم الوسيط. الطبعة الخامسة. مكتبة الشروق للنشر والتوزيع. القاهرة.
- المضحكي، ح. (2014): الجرائم المعلوماتية "دراسة مقارنة. الطبعة الأولى. منشورات الحلبي الحقوقية. بيروت.
- مطر، ح. (2018): إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، مجلة الكوفة للعلوم القانونية والسياسية، 11 (36)، ص ص 396– 410.
- مطر، ك. (2016): الجريمة الإلكترونية، ورقة مقدمة في الندوة العلمية الجرائم المستحدثة في المتغيرات والتحولات الإقليمية والدولية، عمان: الجامعة الأردنية.
- المعمري، ع. (2013): التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، 22 (86)، ص ص 243– 272.
- المليحي، ع. (2019): الجريمة الإلكترونية: مدخل إلى الإطار المفاهيمي، المنارة للدراسات القانونية والإدارية. (5)، ص ص145–159.
- موسى ، م. (2009): التحقيق الجنائي في الجرائم الإلكترونية. الطبعة الأولى. مطابع الشرطة. القاهرة.
- المومني، ن. (2010): الجرائم المعلوماتية. الطبعة الثانية. دار الثقافة للنشر والتوزيع. عمان.

- النجاجره، ع. (2019): خصوصية التحقيق في الجرائم الإلكترونية. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس– أبوديس.
- نسيب، ج. وبوبيدي، ل. (2023): قراءة سوسيو نقدية لمضامين بعض النظريات السوسيولوجية الحديثة المفسرة للجرينة: الاختيار العقلاني، أسلوب الحياة والنشاط الرتيب أنموذجاً، مجلة دراسات وأبحاث. 15 (1)، ص ص167– 178 .
- نصرالله، أ. (2014): دور القضاء في تعزيز الحكم الرشيد في فلسطين. (رسالة ماجستير غير منشورة). فلسطين: جامعة الأقصى.
- نقادي، ح. (2014): معالم الجريمة المعلوماتية في القانون الجزائري، مجلة الحقوق والعلوم الإنسانية، (20)، ص ص 169– 178.
- النمري، س. (2016): ضمانات المتهم والمحاكمة العادلة. (رسالة ماجستير غير منشورة). فلسطين: جامعة القدس– أبوديس.
- هلال، ج. (2003): "نظام العدالة الجنائية فلسطين: دراسة اجتماعية– قانونية"، فلسطين: جامعة بيرزيت، معهد الحقوق.
- هلال، ن. (2008): البعد الاجتماعي لجرائم الحاسب الآلي، مجلة الفكر الشرطي. 17 (65)، ص ص 2–56.
- الوريكات، ع. (2004): نظريات علم الجريمة. الطبعة الأولى. عمان: دار الشروق للنشر والتوزيع.
- الوريكات، ع. (2013): نظريات علم الجريمة. الطبعة الأولى. دار وائل للنشر والتوزيع. عمان.
- وهيب، م. (2014): مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها، مجلة العلوم القانونية والسياسية. 3 (1)، ص ص 333–410.

ثانياً: المواقع الإلكترونية:

- الجزيرة نت (2023): الجرائم الإلكترونية كظاهرة عالمية. رام الله: فلسطين، تاريخ الاطلاع: 10/ 11/ 2024، رابط الموقع: https://www.aljazeera.net/opinions/2023/8/5/%D8%B9%D9%86-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%83%D8%B8%D8%A7%D9%87%D 8%B1%D8%A9
- جهاز الشرطة الفلسطينية (2021): الجريمة الإلكترونية في الضفة بين الواقع والمواجهة. رام الله: فلسطين. تاريخ الاطلاع: في 20/ 5/ 2022 رابط الموقع: https://www.palpolice.ps/content/425828.html

- جهاز الشرطة الفلسطينية (2023): الإدارات المتخصصة. رام الله: فلسطين. تاريخ الاطلاع: 11/ 10/ 2023 رابط الموقع: https://www.palpolice.ps/specialized-departments
- جهاز الشرطة الفلسطينية (2023): عن الشرطة. رام الله: فلسطين. تاريخ الاطلاع: 11/ 10/ 2023 رابط الموقع: https://www.palpolice.ps/about
- جهاز الشرطة الفلسطينية. (2023): الإحصائيات السنوية. رام الله: فلسطين. تاريخ الاطلاع: 2023/10/2، الساعة: 00:17، رابط الموقع: https://www.palpolice.ps/annual-statistics
- النيابة العامة (2022): نيابة مكافحة الجرائم الإلكترونيّة وجرائم الاتصالات وتكنولوجيا المعلومات. رام الله: فلسطين. تاريخ الاطلاع: 21/ 2/ 2022 رابط الموقع: https://pgp.ps/Home/getredirectPage?page=56#Anti%20Cybercrime,%20Telecom,%20&%20IT%20Crimes%20Prosecution
- النيابة العامة (2023): التقرير السنوي التاسع للنيابة العامة 2018. رام الله: فلسطين. تاريخ الاطلاع: 11/ 5/ 2024 رابط الموقع: https://pgp.ps/Home/GetDocument/289

ثالثاً: القوانين والقرارات:

- قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة (2001م).
- قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته.
- قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية.
- قرار بقانون رقم (23) لسنة (2017م) بشأن الشرطة.
- قرار بقانون رقم (28) لسنة (2020م) بتعديل قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.
- قرار بقانون رقم (38) لسنة (2021م) بتعديل قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وتعديلاته.

رابعاً: المراجع الأجنبية:

- Alkaabi, Mohay, & McCullagh, Chantler, (2011): Dealing with the problem of cybercrime. In Digital Forensics and Cyber Crime: Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates, October 4-6, 2010, Revised Selected Papers 2 (pp. 1-18). Springer Berlin Heidelberg.

- Brown, Cameron (2015): Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9 (1), p 55 – 119.
- Graham, Amanda, & Teresa Kulig, & Francis T. Cullen (2020): Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. Policing: An International Journal, 43 (1), p 1-16.
- Koziarski, Jacek, and Lee, Jin Ree (2020): Connecting evidence-based policing and cybercrime. Policing: An International Journal, 43 (1) p 198-211.
- Martin, Nigel, & Rice, John. (2011): Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security, 30 (8) , p 803-814.
- Sarika, Kader, & Minnaar, Anthony (2015): Cybercrime investigations: Cyber-processes for detecting of cybercriminal activities, cyber-intelligence and evidence gathering. Acta Criminologica: African Journal of Criminology & Victimology, sed-5, p 67-81.

ملاحق الدراسة

ملحق (1): الاستبانة في صورتها الأولية.

بسم الله الرحمن الرحيم

جامعة القدس

عمادة الدراسات العليا

برنامج ماجستير علم الجريمة

أخي العزيز/ أختي العزيزة

تحية طيبة وبعد

تقوم الباحثة بإجراء دراسة بعنوان: **(إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً)**، وذلك إستكمالاً لمتطلبات الحصول على درجة الماجستير في علم الجريمة من جامعة القدس، وعليه أرجو التكرم بالإجابة على فقرات الاستبيان بوضع إشارة(X) أمام العبارة التي تتفق ووجهة نظركم، شاكرة لكم جهودكم وأمانتكم وحرصكم على إنجاح هذه الدراسة، علماً بأن إجاباتكم ستكون سرية ولا تشكل أي نوع من الاختبار ولن تستخدم إلى لغايات البحث العلمي فقط.

شاكرة لكم حسن تعاونكم

إعداد الباحثـــة: ليالـــي دوديـــن

إشراف: الدكتور جهاد الكسواني

القسم الأول: البيانات الشخصية:

الرجاء وضع علامة (X) في الخانة التي تناسبكم:

- الجنس: ذكر ( ) أنثى ( )
- العمر: 20- أقل من 30 سنة ( ) 30- أقل من 40 سنة ( ) 40 سنة فأكبر ( )
- المستوى التعليمي: ثانوية عامة فأقل ( ) دبلوم متوسط ( ) دبلوم عالي ( ) بكالوريوس( ) دراسات عليا ( )
- مكان العمل: القضاء ( ) النيابة العامة ( ) الشرطة ( ) مركز الإصلاح والتأهيل ( )
- الخبرة العملية: أقل من 5 سنوات ( ) 5- أقل من10 سنوات ( ) 10- أقل من15 سنوات فأعلى ( ) 15 – أقل من 20 سنة ( ) 20سنة فأكثر ( )

القسم الثاني: مجالات ومحاور الاستبانة:

يرجى وضع إشارة(X) في المربع الذي يتفق مع وجهة نظركم أمام كل فقرة من الفقرات التالية:

المجال الأول: الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية:

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
ما الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية؟						
.1	إنشاء وحدة متخصصة في الجرائم الإلكترونية					
.2	تتم الاستجابة بسرعة لشكاوى المواطنين حول الجرائم الإلكترونية					
.3	يوجد برامج إعداد كادر متخصص في التحقيق في الجرائم الإلكترونية					
.4	المعدات التقنية للتعامل مع مسرح الجريمة الإلكترونية متوفرة					
.5	يعمل مأمورو الضبط القضائي على جمع المعلومات (البحث والتحري) وتحرير محاضر الاستدلال					
.6	يعمل مأمورو الضبط القضائي على توثيق محاضر الاستدلال المتعلقة بالجرائم الإلكترونية وفق الإجراءات القانونية المحددة					
.7	يلتزم العاملون بسرية المعلومات أثناء التحقيق في الجرائم الإلكترونية					
.8	يتم العمل على رفع مستوى الوعي العام اتجاه مخاطر الجرائم الإلكترونية من خلال (ندوات، مؤتمرات، ورشات عمل)					
.9	يزود الجهات ذات العلاقة بالتغذية الراجعة حول واقع الجرائم الإلكترونية					
.10	يتم العمل على تعزيز التعاون مع المجتمع المحلي للكشف عن الجرائم الالكترونية					

المجال الثاني: الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية:

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
ما الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية؟						
.11	إنشاء نيابة متخصصة للتحقيق في الجرائم الإلكترونية					
.12	العمل على تسهيل استقبال شكاوى الجرائم الإلكترونية من خلال النيابات الجزئية					
.13	يجري التحقيق في الشكاوى المتعلقة بالجرائم الإلكترونية وفقا للمعايير التي تتناسب وخصوصية كل نوع من أنواعها					
.14	التعامل مع القضايا الواردة إليها بأقصى سرعة ممكنة					
.15	التعامل مع القضايا الواردة إليها بالسرية التامة مع الشركاء					
.16	فحص المضبوطات وفقا للإجراءات المقررة بقرار بقانون رقم (10) لسنة (2018)					
.17	التعاون مع المختبر الجنائي للتعامل مع الدليل المضبوط من مسرح الجريمة الإلكترونية وتحليله دون إتلافه					
.18	العمل على ممارسة الدور (الوقائي، العقابي) في ذات الوقت (لصد، مكافحة) هذا النوع من الجرائم وفقا للقانون والأصول					
.19	الاشتراك بالجانب التوعوي مع المؤسسات الشريكة للتوعية بمخاطر الجرائم الإلكترونية وآثارها					

المجال الثالث: الإجراءات المتبعة من قبل القضاء في مواجهة الجرائم الإلكترونية:

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
ما الإجراءات المتبعة من قبل القضاء في مواجهة الجرائم الإلكترونية؟						
.20	ينظر القضاء الى الجريمة الالكترونية بنظرة الاهمية موازية للجرائم في العالم الواقعي.					
.21	يمتلك القضاة القدرة في وزن البينات الفنية في الجرائم الالكترونية.					
.22	يلتزم القضاء بالتشريعات النافذة في مواجهة الجرائم الالكترونية.					
.23	يعمل القضاء على سد الثغرات التشريعية في القوانين ذات العلاقة بالجرائم الالكترونية بالاسترشاد بقوانين اخرى.					
.24	يتعامل القضاة بالجدية الكافية بالنظر في قضايا الجرائم الالكترونية.					
.25	يتبنى القضاة فلسفتي الردع والاصلاح في الاحكام الصادرة والمتعلقة بالجرائم الالكترونية.					
.26	يتلقى القضاة دورات تدريبية في مجال الجرائم الالكترونية.					
.27	يستعين القضاة بالخبراء الفنيين في مجال الجرائم الالكترونية.					
.28	لدى القضاء الاجهزة التقنية والفنية اللازمة لاستعراض ادلة الوقائع المتعلقة بالجرائم الالكترونية.					
.29	العمل على تنظيم ورش عمل وندوات لمناقشة مدى ملائمة التشريعات القانونية المتعلقة بالجرائم الإلكترونية بحداثتها وتطورها					

المجال الرابع: الإجراءات المتبعة من قبل مراكز الإصلاح والتأهيل في مواجهة الجرائم الإلكترونية:

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
ما الإجراءات المتبعة من قبل مراكز الإصلاح والتأهيل في مواجهة الجرائم الإلكترونية؟						
.30	تعمل على تقديم البرامج الإصلاحية والتأهيلية اللازمة لمرتكبي الجرائم الإلكترونية					
.31	تعمل على توفير كادر مختص للتعامل مع النزلاء					
.32	تعمل بالشراكة مع مؤسسات المجتمع المدني على وضع خطط لتطوير آليات عملها والخدمات التي تقدمها					
.33	تعمل على تسهيل زيارة أهالي النزلاء وتواصلهم معهم					
.34	تسهم في توعية المجتمع بأهميتها ودورها في إصلاح النزيل وتأهيله لإعادة دمجه في مجتمع					
.35	تسيير أعمالها وفق القواعد المنصوص عليها بقانون مراكز الإصلاح والتأهيل الفلسطيني					
.36	تُعلم النزيل بأية قرارات قضائية صادرة بحقه					
.37	تعمل على تطوير برامج الرعاية الصحية والنفسية المقدمة للنزلاء					
.38	تعمل على تطوير البرامج التأهيلية والتدريبة المقدمة للنزلاء					

المجال الخامس: الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم، مراكز الإصلاح والتأهيل) في مكافحة الجرائم الإلكترونية:

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
ما الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم، مراكز الإصلاح والتأهيل) في مكافحة الجرائم الإلكترونية؟						
.39	عدم سيطرة هيئات العدالة الجنائية على الفضاء الإلكتروني الفلسطيني					
.40	صعوبة إجراءات التفتيش وجمع الأدلة في مسرح الجريمة الإلكترونية					
.41	صعوبة إجراءات ضبط الأدلة في الجرائم الإلكترونية					
.42	صعوبة أدلة الإدانة والإثبات كون الدليل غير مادي					
.43	صعوبة تعقب الشرائح الإسرائيلية المستخدمة في ارتكاب الجرائم الإلكترونية					
.44	ضخامة حجم البيانات المتعين فحصها					
.45	نقص الكادر المختص للتعامل مع الجرائم الإلكترونية					
.46	تضاؤل خبرة أجهزة العدالة من مأموري ضبط وسلطة تحقيق ومحاكمة في التعامل مع الجرائم الإلكترونية					
.47	قلة البرامج والأدوات التقنية المختصة للمساعدة في عملية التحقيق الجنائي مقارنة بالتطور الهائل والسريع للتقنية					
.48	قلة وعي المجتمع بالجريمة الإلكترونية					
.49	إحجام الضحايا عن الإبلاغ عن الجريمة الإلكترونية					
.50	لجوء ضحايا الجرائم الإلكترونية إلى ما يسمى بالهاكرز					
.51	عدم توفير حماية للمبلغين عن الجرائم الإلكترونية					

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
.52	صعوبة كشف الجناة كونهم ينتحلون شخصيات وهمية					
.53	البعد الجغرافي بين مرتكب الجريمة والضحية					
.54	عدم ثقة المواطنين بهيئات العدالة الجنائية					
.55	يعاني التحقيق الإلكتروني في التشريع الفلسطيني من الفراغ التشريعي					
.56	حداثة التشريعات القانونية الخاصة بالجرائم الإلكترونية					
.57	العقوبات المفروضة على ارتكاب الجرائم الإلكترونية غير رادعة					
.58	الإجراءات المتبعة من قبل هيئات العدالة الجنائية للتحقيق في الجرائم الإلكترونية معقدة وطويلة					
.59	عدم وجود خطة استراتيجية مشتركة بين هيئات العدالة الجنائية لمواجهة الجرائم الإلكترونية					
.60	محدودية البرامج الإصلاحية والتأهيلية المقدمة لمرتكبي الجرائم الإلكترونية					
.61	ضعف البنية التحتية لمراكز الإصلاح والتأهيل وبالتالي عجزها عن تحقيق قواعد الحد الأدنى للنزلاء					

المجال السادس: آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم، مراكز الإصلاح والتأهيل) للحد من الجرائم الإلكترونية:

الرقم	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
ما آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم، مراكز الإصلاح والتأهيل) للحد من الجرائم الإلكترونية؟						
.62	تبادل مؤسسات هيئات العدالة الجنائية المعلومات فيما بينها حول الجرائم الإلكترونية					
.63	وضع خطة استراتيجية مشتركة بين هيئات العدالة الجنائية لمواجهة الجرائم الإلكترونية					
.64	التنسيق بين مؤسسات هيئات العدالة الجنائية ومؤسسات المجتمع المحلي المعنية للحد من الجرائم الإلكترونية					
.65	التنسيق بين مؤسسات هيئات العدالة الجنائية ومؤسسات المجتمع الدولي للحد من الجرائم الإلكترونية					
.66	استخدام نظام إعلامي متطور للنشر عن طرق الوقاية من الجرائم الإلكترونية					
.67	تنظيم برامج توعوية حول الآثار المترتبة عن الجرائم الإلكترونية					
.68	وضع سياسة أمنية للشبكة وحشد كل الإمكانيات البشرية والمادية لتطبيقها					
.69	تجنب فتح أي رسائل إلكترونية مجهولة المصدر					
.70	فصل جهاز الحاسوب عن شبكة الإنترنت في حالة عدم الاستخدام					
.71	الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب					
.72	العمل على تغيير كلمات المرور الخاصة بالحاسوب بشكل دوري					
.73	مساعدة المواطنين في تطبيق نظام الأمن الذاتي					
.74	تنمية الثقة بين المواطنين والعاملين في					

الرقم	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
	هيئات العدالة الجنائية					
.75	التزام هيئات العدالة الجنائية بمراقبة وتتبع المواقع الإلكترونية					
.76	مواكبة التطورات التقنية لتتبع مرتكبي الجرائم الإلكترونية للحد من انتشارها					
.77	تأمين الأجهزة باستخدام نظام برنامج حماية متقدم وتخزين آمن للمعلومات الحساسة					
.78	استخدام تكنولوجيا الذكاء الصناعي لاكتشاف الجرائم الإلكترونية قبل وقوعها وذلك لمكافحتها					
.79	عمل رقم موحد لدى جهات الاختصاص للتبليغ فورا عن التعرض للجريمة الإلكترونية					
.80	تطوير قدرات العاملين في مجال الجرائم الإلكترونية من خلال(التدريب، المؤتمرات، ورشات العمل)					
.81	توفد هيئات العدالة الجنائية العاملين فيها للخارج لاكتساب الخبرات حول مكافحة الجرائم الإلكترونية					
.82	وضع نظام حوافز مادية ومعنوية للمتميزين من العاملين في التحقيق في الجرائم الإلكترونية					
.83	زيادة أعداد الطاقم العاملين في التحقيق في الجرائم الإلكترونية					
.84	سن تشريعات قانونية بما يتواكب مع حداثة الجرائم الإلكترونية					
.85	تشديد العقوبات على مرتكبي الجرائم الإلكترونية					
.86	سن تشريعات لحماية ضحايا الجرائم الإلكترونية					
.87	إصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة					

وتقبلوا فائق الاحترام والتقدير

ملحق (2): الاستبانة في صورتها النهائية

بسم الله الرحمن الرحيم

جامعة القدس

عمادة الدراسات العليا

برنامج ماجستير علم الجريمة

أخي العزيز/ أختي العزيزة

تحية طيبة وبعد

تقوم الباحثة بإجراء دراسة بعنوان: **(إجراءات هيئات العدالة الجنائية في مواجهة الجرائم الإلكترونية بين الصعوبات وآليات الوقاية/ محافظة أريحا أنموذجاً)**، وذلك إستكمالاً لمتطلبات الحصول على درجة الماجستير في علم الجريمة من جامعة القدس، وعليه أرجو التكرم بالإجابة على فقرات الاستبيان بوضع إشارة(X) أمام العبارة التي تتفق ووجهة نظركم، شاكرة لكم جهودكم وأمانتكم وحرصكم على إنجاح هذه الدراسة، علماً بأن إجاباتكم ستكون سرية ولا تشكل أي نوع من الاختبار ولن تستخدم إلى لغايات البحث العلمي فقط.

شاكرة لكم حسن تعاونكم

إعداد الباحثـــة: ليالـــي دوديـــن

إشراف: الدكتور جهاد الكسواني

القسم الأول: المتغيرات الديموغرافية:

الرجاء وضع علامة (X) في الخانة التي تناسبكم:

1- النوع الاجتماعي: ذكر ( ) أنثى ( ).
2- العمر: 20- أقل من 30 سنة ( ) 30- أقل من 40 سنة ( ) 40 سنة فأكبر( )
3- المستوى التعليمي: ثانوية عامة فأقل ( ) دبلوم متوسط ( ) دبلوم عالي ( ) بكالوريوس( ) دراسات عليا ( )
4- مكان العمل: القضاء ( ) النيابة العامة ( ) الشرطة ( )
5- الخبرة العملية: أقل من 5 سنوات ( ) 5سنوات - إلى أقل من10 سنوات ( ) 10سنوات- إلى أقل من15 سنة( ) 15سنة - إلى أقل من 20 سنة ( ) 20سنة فأكثر ( )

القسم الثاني: مجالات ومحاور الدراسة:

يرجى وضع إشارة(x) في المربع الذي يتفق مع وجهة نظركم أمام كل فقرة من الفقرات التالية:

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
المجال الأول: الإجراءات المتبعة من قبل وحدة الجرائم الإلكترونية في جهاز الشرطة في مواجهة الجرائم الإلكترونية:						
.1	الاستجابة بسرعة لشكاوى المواطنين حول الجرائم الإلكترونية					
.2	يوجد برامج إعداد كادر متخصص في البحث والتحري في الجرائم الإلكترونية					
.3	يتم التعامل مع مسرح الجريمة الإلكترونية بالمعدات التقنية اللازمة					
.4	يعمل مأمورو الضبط القضائي على جمع المعلومات (البحث والتحري) وتحرير محاضر بها					
.5	توثيق محاضر الاستدلال من قبل مأموري الضبط القضائي وفق الإجراءات القانونية المحددة					
.6	يلتزم العاملون بسرية المعلومات أثناء التحري والاستدلال عن الجرائم الإلكترونية					
.7	رفع مستوى الوعي العام اتجاه مخاطر الجرائم الإلكترونية					
.8	تعزيز التعاون مع المجتمع المحلي للكشف عن الجرائم الالكترونية					
المجال الثاني : الإجراءات المتبعة من قبل النيابة العامة في مواجهة الجرائم الإلكترونية:						
.1	إنشاء نيابة متخصصة في الجرائم الإلكترونية					
.2	العمل على تسهيل تحويل شكاوى الجرائم الإلكترونية من خلال النيابات الجزئية					
.3	يجري التحقيق في الشكاوى المتعلقة بالجرائم الإلكترونية وفقا للإجراءات التي تتناسب وخصوصية كل نوع من أنواعها					

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
.4	توثيق محاضر التحقيق وفق الإجراءات القانونية المحددة					
.5	التعامل مع قضايا الجرائم الإلكترونية الواردة بالسرية التامة					
.6	التعامل مع المضبوطات ذات العلاقة بالجريمة الإلكترونية وفقاً للإجراءات القانونية المحددة					
.7	التعاون مع المختبر الجنائي للتعامل مع الدليل المضبوط من مسرح الجريمة الإلكترونية					
.8	الاشتراك بالجانب التوعوي مع المؤسسات الشريكة للتوعية بمخاطر الجرائم الإلكترونية وآثارها					
المجال الثالث: ما الإجراءات المتبعة من قبل المحاكم في مواجهة الجرائم الإلكترونية؟						
.1	يلتزم القضاء بالتشريعات النافذة في مواجهة الجرائم الالكترونية.					
.2	يمتلك القضاة القدرة على وزن البينات الفنية في الجرائم الالكترونية.					
.3	يعمل القضاء على سد الثغرات التشريعية في القوانين ذات العلاقة بالجرائم الالكترونية بالاسترشاد بقوانين أخرى.					
.4	يتبنى القضاة فلسفتي الردع والاصلاح في الأحكام الصادرة والمتعلقة بالجرائم الإلكترونية.					
.5	يستعين القضاة بالخبراء الفنيين في مجال الجرائم الإلكترونية.					
.6	لدى القضاء الأجهزة التقنية والفنية اللازمة لاستعراض أدلة الوقائع المتعلقة بالجرائم الإكترونية.					
.7	يتلقى القضاة دورات تدريبية في مجال الجرائم الإلكترونية.					
.8	العمل على تنظيم ورش عمل وندوات لمناقشة مدى ملائمة التشريعات القانونية المتعلقة بالجرائم الإلكترونية بحداثتها وتطورها					

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
المجال الرابع: الصعوبات التي تواجه هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية:						
.1	عدم سيطرة هيئات العدالة الجنائية على الفضاء الإلكتروني الفلسطيني					
.2	صعوبة إجراءات التفتيش وجمع الأدلة في مسرح الجريمة الإلكترونية					
.3	صعوبة إجراءات ضبط الأدلة في الجرائم الإلكترونية					
.4	صعوبة الحصول على أدلة الإثبات كون الدليل غير مادي					
.5	صعوبة تعقب الشرائح الإسرائيلية المستخدمة في ارتكاب الجرائم الإلكترونية					
.6	ضخامة حجم البيانات المتعين فحصها للحصول على أدلة إثبات					
.7	نقص الكادر المختص للتعامل مع الجرائم الإلكترونية					
.8	قلة خبرة أجهزة العدالة من مأموري ضبط وسلطة تحقيق في التعامل مع الجرائم الإلكترونية نسبيا					
.9	قلة البرامج والأدوات التقنية المختصة للمساعدة في عملية التحقيق الجنائي مقارنة بالتطور الهائل والسريع للتقنية					
.10	قلة وعي المجتمع بالجريمة الإلكترونية					
.11	إحجام الضحايا عن الإبلاغ عن الجريمة الإلكترونية					
.12	عدم توفير حماية للمبلغين عن الجرائم الإلكترونية					
.13	صعوبة كشف الجناة كونهم ينتحلون شخصيات وهمية					
.14	البعد الجغرافي بين مرتكب الجريمة والضحية					

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
15.	يوجد نقص في التنظيم الإجرائي لمكافحة الجرائم الإلكترونية في التشريع الفلسطيني					
16.	حداثة التشريعات القانونية الخاصة بالجرائم الإلكترونية					
17.	العقوبات المفروضة على ارتكاب الجرائم الإلكترونية غير رادعة					
18.	الإجراءات المتبعة من هيئات العدالة الجنائية للتحقيق في الجرائم الإلكترونية معقدة وطويلة					
19.	عدم وجود خطة استراتيجية مشتركة بين هيئات العدالة الجنائية لمواجهة الجرائم الإلكترونية					
المجال الخامس: آليات الوقاية المُتبعة من قبل هيئات العدالة الجنائية (الشرطة، النيابة العامة، المحاكم) للحد من الجرائم الإلكترونية:						
1.	تبادل هيئات العدالة الجنائية المعلومات فيما بينها حول الجرائم الإلكترونية					
2.	وضع خطة استراتيجية مشتركة بين هيئات العدالة الجنائية لمواجهة الجرائم الإلكترونية					
3.	التنسيق بين هيئات العدالة الجنائية ومؤسسات المجتمع المحلي المعنية للحد من الجرائم الإلكترونية					
4.	التنسيق بين هيئات العدالة الجنائية ومؤسسات المجتمع الدولي للحد من الجرائم الإلكترونية					
5.	استخدام نظام إعلامي متطور للنشر عن طرق الوقاية من الجرائم الإلكترونية					
6.	تنظيم برامج توعوية حول الآثار المترتبة عن الجرائم الإلكترونية					
7.	وضع سياسة أمنية للشبكة وحشد كل الإمكانيات البشرية والمادية لتطبيقها					
8.	تجنب فتح أي رسائل إلكترونية مجهولة المصدر					
9.	فصل جهاز الحاسوب عن شبكة الإنترنت في حالة عدم الاستخدام					

م	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
.9	الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب					
.11	العمل على تغيير كلمات المرور الخاصة بالحاسوب بشكل دوري					
.12	مساعدة المواطنين في تطبيق نظام الأمن الذاتي للوسائل الإلكترونية					
.13	تنمية الثقة بين المواطنين والعاملين في هيئات العدالة الجنائية					
.14	التزام هيئات العدالة الجنائية بمراقبة وتتبع المواقع الإلكترونية					
.15	مواكبة التطورات التقنية لتتبع مرتكبي الجرائم الإلكترونية للحد من انتشارها					
.16	تأمين الأجهزة باستخدام نظام برنامج حماية متقدم وتخزين آمن للمعلومات الحساسة					
.17	استخدام تكنولوجيا الذكاء الصناعي لاكتشاف الجرائم الإلكترونية قبل وقوعها وذلك لمكافحتها					
.18	عمل رقم موحد لدى جهات الاختصاص للتبليغ فورا عن التعرض للجريمة الإلكترونية					
.19	تطوير قدرات العاملين في مجال الجرائم الإلكترونية من خلال(التدريب، المؤتمرات، ورشات العمل)					
.20	توفد هيئات العدالة الجنائية العاملين فيها للخارج لاكتساب الخبرات حول مكافحة الجرائم الإلكترونية					
.21	وضع نظام حوافز مادية ومعنوية للمتميزين من العاملين في التحقيق في الجرائم الإلكترونية					
.22	زيادة أعداد الطاقم العاملين القائمين على البحث والتحري في الجرائم الإلكترونية					
.23	إصلاح وتأهيل مرتكبي الجرائم الإلكترونية للحفاظ على عدم عودتهم للجريمة					

وتقبلوا فائق الاحترام والتقدير

ملحق (3): أسماء محكمي الاستبانة:

الرقم	اسم المحكم	الجامعة
.1	د. عصام الأطرش	جامعة الاستقلال
.2	د. فادي ربايعة	جامعة القدس
.3	د.عبداللطيف ربايعة	جامعة الاستقلال
.4	د. محمد بيدوسي	جامعة الاستقلال
.5	د. توفيق أبو حديد	جامعة الاستقلال
.6	د. رؤوف أبو عواد	جامعة الاستقلال

ملحق (4): قرار بقانون رقم (23) لسنة (2017م) بشأن الشرطة

رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية استناداً لأحكام القانون الأساسي المعدل لسنة (2003م) وتعديلاته، لا سيما أحكام المادة (43) منه، وبعد الاطلاع على أحكام قانون الخدمة في قوى الأمن الفلسطينية رقم (8) لسنة 2005م، والاطلاع على أحكام قانون التقاعد العام رقم (7) لسنة (2005م) وتعديلاته، وعلى أحكام قانون التأمين والمعاشات لقوى الأمن الفلسطينية رقم (16) لسنة 2004م وتعديلاته، وعلى أحكام قانون الإجراءات الجزائية رقم (3) لسنة 2001م وتعديلاته، وعلى أحكام قانون الأمن العام المؤقت رقم (38) لسنة (1965م) وتعديلاته، بشأن الشرطة، النافذ في المحافظات الشمالية، وعلى أحكام القرار بقانون رقم (6) لسنة 1963م، بشأن الشرطة، النافذ في المحافظات الجنوبية، وبناءً على تنسيب مجلس الوزراء بتاريخ 2016/01/05م، وعلى الصلاحيات المخولة لنا، وتحقيقاً للمصلحة العامة، وباسم الشعب العربي الفلسطيني، أصدرنا القرار بقانون الآتي:

مادة (1): يكون للكلمات والعبارات الواردة في هذا القرار بقانون المعاني المخصصة لها أدناه، ما لم تدل القرينة على خلاف ذلك:

الدولة: دولة فلسطين.

الرئيس: رئيس دولة فلسطين، رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية، القائد الأعلى لقوى الأمن الفلسطينية.

المجلس: مجلس وزراء الدولة.

رئيس الوزراء: رئيس مجلس الوزراء. الوزارة: وزارة الداخلية.

الوزير: وزير الداخلية.

قانون الخدمة: قانون الخدمة في قوى الأمن الفلسطينية رقم (8) لسنة 2005م.

الشرطة: قوة نظامية تمارس اختصاصات مدنية، تتبع الوزارة، وتؤدي مهامها واختصاصاتها بموجب أحكام هذا القرار بقانون.

المـدير العـام: مـدير عـام المديريـة العامـة للشـرطة المعـين بموجـب أحكـام هـذا القـرار بقـانون.
المـدير: مـدير شـرطة المحافظـة أو مـدير الإدارة المتخصصـة ومـن فـي حكمهـم، حسـب الهيكليـة المعتمدة للشرطة.

المديرية العامة: المديرية العامة للشرطة.

عناصر الشرطة: ضباط وضباط الصف وأفراد الشرطة من كلا الجنسين.

الضابط: من يحمل رتبة ملازم حتى رتبة فريق.

ضابط الصف: من يحمل رتبة عريف حتى رتبة مساعد أول.

الشرطي: كل فرد من أفراد الشرطة يحمل رتبة شرطي.

الرتبـة: كـل رتبـة تمـنح لأحـد عناصـر الشـرطة عنـد تعيينـه أو ترقيتـه إليهـا وفقـاً لأحكـام هـذا القرار بقانون، وقانون الخدمة.

اللجنة: اللجنة العليا لشؤون الشرطة المشكلة وفقاً لأحكام هذا القرار بقانون.

المجـالس التأديبيـة: المجـالس المشـكلة بموجـب أحكـام هـذا القـرار بقـانون، والمسـؤولة عـن النظر في الأمور التأديبية لعناصر الشرطة.

القضاء: القضاء النظامي وفقاً لأحكام قانون السلطة القضائية النافذ.

النيابة العامة: النيابة العامة النظامية وفقاً لأحكام قانون السلطة القضائية النافذ.

مـادة (2): يهـدف هـذا القـرار بقـانون لإدارة وتنظـيم شـؤون وعمـل الشـرطة، وصـلاحياتها واختصاصاتها، وتسري أحكامه على عناصر الشرطة.

مادة (3): تختص الشرطة بالمهام الآتية:

1. المحافظة على النظام والأمن العام، والآداب العامة، والسكينة العامة.
2. حماية الأرواح والأعراض والأموال.

3. منع ومكافحة الجريمة، وضبط مرتكبيها بموجب القوانين المعمول بها.

4. مكافحة أعمال الشغب وكافة مظاهر الإخلال بالأمن العام.

5. حماية الحقوق والحريات المشروعة التي يكفلها القانون الأساسي والقوانين ذات الصلة، والاتفاقيات الدولية التي تكون الدولة طرفاً بها.

6. حماية الممتلكات العامة والخاصة للدولة والأفراد.

7. مساعدة قوى الأمن والسلطات العامة الأخرى في أداء مهامها بموجب أحكام القانون. 8. التعاون الشرطي العربي والإقليمي والدولي في مجال مكافحة الجريمة من خلال جمع وتوثيق وتبادل المعلومات والبيانات والأدلة عن الجرائم ومرتكبيها، وتقديم خدمات التعاون الشرطي والأمني وفقاً للتشريعات والقوانين النافذة، والاتفاقيات الدولية التي تكون الدولة طرفاً فيها.

9. تنفيذ ما تفرضه عليها القوانين واللوائح والأنظمة من واجبات ومهام.

10. تقديم المعلومات والإرشادات للمواطنين بالوسائل التي تساعد على مكافحة الجريمة، ووقايتهم منها، وتسهيل تنفيذ واجبات الشرطة بما يحقق ضمان مساهمة المواطنين في معاونتها ودعمها في كافة واجباتها.

11. توعية المواطنين بحقوقهم وواجباتهم، لضمان المشاركة المجتمعية في حفظ النظام والأمن العام في المجتمع.

12. تحقيق الأمن الداخلي للوطن والمواطنين، والمساهمة في تحقيق الأمن القومي بالتنسيق والتعاون مع الأجهزة الأمنية المختصة، والمؤسسات العامة، ومؤسسات المجتمع المدني، ووسائل الإعلام، ولها تنظيم مذكرات تفاهم بهذا الخصوص.

مادة (4): تلتزم الشرطة أثناء تأدية واجباتها بالآتي:

1. القيام بكافة وظائفها واختصاصاتها وواجباتها، وفقاً للقانون الأساسي والقوانين والأنظمة واللوائح والتعليمات، ومعايير الشفافية والحيادية والنزاهة والمساءلة، واحترام حقوق الإنسان والحريات العامة، واحترام الأحكام القضائية وتنفيذها.

2. احترام وترسيخ سيادة القانون واستقلال القضاء وتحقيق مبدأ عدم التمييز بين المواطنين بسبب العرق أو الجنس أو اللون أو الدين أو الرأي السياسي أو الإعاقة. 3. مراعاة الحصانة الممنوحة وفقاً للقوانين النافذة في الدولة.

مادة (5):

1. تؤدي الشرطة وظائفها، وتباشر اختصاصاتها تحت إشراف ورقابة الوزير.
2. يتولى المدير العام المسؤولية المباشرة لإدارة شؤون عمل الشرطة، وكل ما يتعلق بتنظيمها وتدريبها وتجهيزها وتسليحها، ومراقبة نفقاتها.

مادة (6): يتمتع الضباط وضباط صف الشرطة بصفة الضبطية القضائية أثناء تأدية واجباتهم، كل في حدود اختصاصه، وفقاً لأحكام قانون الإجراءات الجزائية النافذ. ويباشرون أعمالهم بصفتهم ضابطة قضائية تحت إشراف النائب العام بصفته رئيس الضابطة القضائية.

مادة (7): يكون المقر الرئيس للمديرية العامة للشرطة في العاصمة القدس، ويكون لها مقر مؤقت في كل من مدينتي رام الله وغزة.

مادة (8): تتمثل رتب عناصر الشرطة بالآتي:

1. الضباط: ملازم، ملازم أول، نقيب، رائد، مقدم، عقيد، عميد، لواء، فريق.

2. ضباط الصف: عريف، رقيب، رقيب أول، مساعد، مساعد أول.

3. الشرطي: كل فرد من أفراد الشرطة يحمل رتبة شرطي.

مادة (9):

1. يعين المدير العام بقرار من الرئيس، وبتنسيب من مجلس الوزراء، بناءً على توصية الوزير.
2. يكون تعيين المدير العام لمدة أربع سنوات، ويجوز تمديدها سنوياً بما لا يتجاوز ثلاث سنوات إضافية حسب الإجراءات المشار إليها في الفقرة (1) من هذه المادة.
3. يتولى المدير العام إدارة الشرطة، ويكون مسؤولاً مسؤولية كاملة أمام الرئيس والوزير في كل ما يتعلق بتنظيم وإدارة شؤون الشرطة.

4. يعاون المدير العام في العمل نائب له، ومفتش عام، وعدد من المساعدين، وله أن يفوض خطياً أي من صلاحياته المخولة إليه بموجب أحكام هذا القرار بقانون إلى النائب أو المفتش العام أو أي من مساعديه.

مادة (10): يعين نائب المدير العام، والمفتش العام، ومساعدو المدير العام بقرار من الوزير، بناءً على تنسيب المدير العام وتوصية اللجنة، وتحدد واجباتهم بتعليمات خاصة يصدرها المدير العام.

مادة (11): يعين المدراء بقرار من المدير العام وفق الآتي:

1. مدراء الإدارات المتخصصة، ومدراء شرطة المحافظات، ومدراء الدوائر ونوابهم، بناءً على توصية اللجنة.
2. مدراء فروع إدارات الشرطة المتخصصة ونوابهم، بقرار من المدير العام، بناءً على تنسيب من مدراء إداراتهم.
3. مدراء مراكز ومخافر الشرطة في المحافظات، بقرار من المدير العام، بناءً على تنسيب من مدراء شرطة المحافظات، كل في حدود اختصاصه.

مادة (12): يتولى نائب المدير العام والمفتش العام ومساعدو المدير العام ومديرو الإدارات المتخصصة ومديرو شرطة المحافظات ومن في حكمهم، إدارة وتنظيم أعمال وأنشطة الشرطة، كل في حدود اختصاصه، ونطاق إشرافه، وفقاً لما يحدده المدير العام من تعليمات وإجراءات.

مادة (13):

1. يكون للشرطة بند موازنة مستقل ضمن موازنة الوزارة، ويتم إعدادها وإقرارها بموجب قانون تنظيم الموازنة العامة والشؤون المالية النافذ.
2. يعين الوزير مراقب مالي داخلي، بناءً على توصية من المدير العام، يتولى القيام بالمهام الآتية:

   أ. الرقابة على آليات الصرف وتنفيذ الموازنة.

   ب. الإشراف المباشر على تدقيق الحسابات، والتأكد من سلامتها.

   ج. تقديم التقارير اللازمة للوزير من خلال المدير العام.

3. يكون المدير العام مسؤولاً عن تنفيذ وإدارة الموازنة، ويقدم تقريراً للوزير بشأن ذلك.

مادة (14):

1. تشكل بمقتضى أحكام هذا القرار بقانون لجنة عليا للشرطة، بقرار من المدير العام ومصادقة الوزير.
2. تتألف اللجنة من الآتي: أ. المدير العام رئيساً. ب. نائب المدير العام. ج. المفتش العام. د. مساعدو المدير العام. هـ. خمسة ضباط من مدراء الإدارات المتخصصة. و. مدراء شرطة المحافظات.
3. يصدر المدير العام قراراً بتعيين أعضاء اللجنة في بداية كل عام.
4. يصدر المدير العام التعليمات والإجراءات الخاصة بعمل اللجنة واجتماعاتها، وكل ما يتعلق بتنظيم أعمالها، ويرأس الوزير اجتماعات اللجنة في حال حضوره.
5. يقوم المدير العام بعرض توصيات اللجنة على لجنة الضباط فيما يتعلق باختصاصاتها، وتكون هذه التوصيات نافذة بعد مصادقة الرئيس أو الوزير كل في حدود اختصاصه.
6. فيما عدا اختصاص لجنة الضباط، تكون توصيات اللجنة نافذة بعد مصادقة الوزير أو المدير العام عليها، كل في حدود اختصاصه.

مادة (15): تختص اللجنة بالنظر في كافة الأمور المتعلقة بتنظيم وإدارة شؤون الشرطة، والمتمثلة بالآتي:

1. رسم السياسة العامة للشرطة في إطار التوجهات العامة للوزير، ومتابعة تنفيذ وتقييم خططها مقارنة بالأهداف المحددة للشرطة في إطار الخطة العامة للوزارة، والتوصية بما يلزم.
2. تنظيم وتنسيق عمل إدارات الشرطة المتخصصة، وشرطة المحافظات ومن في حكمها، في إطار التعاون والعمل الجماعي لتطوير العمل.
3. إعداد خطة التنقلات السنوية.
4. النظر في تظلمات الضباط من تقارير الكفاءة الخاصة بهم، والنظر في أهليتهم للترقية، أو الاستمرار بالخدمة إذا كانت تقارير الكفاءة الخاصة بهم لا تؤهلهم للخدمة، أو كانوا غير أهل للخدمة والتوصية بما يلزم.
5. تحديد الاحتياجات الضرورية من الخبرات غير المتوفرة في الشرطة، والتوصية بالتعاقد مع الخبراء في التخصصات المطلوبة حسب الأصول
6. إعداد مشروع الموازنة المالية السنوية للشرطة.

7. إعداد مشروع الهيكلية العامة للشرطة.
8. أي مهام أخرى تكلف بها اللجنة أو تحال إليها من الوزير أو المدير العام.

مادة (16): يتم إنشاء وحدات تنظيمية بالمديرية العامة وفق الآتي:

1. إدارة المفتش العام: تختص بمهام الرقابة الإدارية والمالية والقانونية على جميع إدارات ودوائر الشرطة ومديريات شرطة المحافظات، ويصدر المدير العام القرارات والتعليمات اللازمة لتنظيم شؤون عملها واختصاصاتها.
2. دائرة المظالم وحقوق الإنسان: تختص بمهمة تلقي شكاوى وتظلمات المواطنين وعناصر الشرطة فيما يتعلق بالشأن الشرطي، ومتابعتها والتحقيق بشأنها، وإحالتها مع التوصيات إلى المدير العام.
3. إدارة الشرطة الدولية (الإنتربول): تختص في القيام بأعمال التعاون الجنائي الدولي، ويصدر الوزير القرارات والتعليمات اللازمة لتنظيم شؤون عملها واختصاصاتها بالتشاور مع المدير العام والنائب العام.

مادة (17): تسري على عناصر الشرطة أحكام قانون الخدمة، من حيث التعيين والأقدمية والترقية، والندب والإلحاق والنقل والإعارة والبعثات الدراسية، والرواتب والعلاوات والحوافز والإجازات، والواجبات والأعمال المحظورة، والأوسمة والأنواط والميداليات، والإحالة إلى الاستيداع وانتهاء الخدمة، وأي أمر آخر لم يرد بشأنه نص وفقاً لأحكام هذا القرار بقانون.

مادة (18):

1. يؤدي عناصر الشرطة عند بدء تعيينهم وقبل مباشرة أعمال وظائفهم اليمين التالية: (أقسم بالله العظيم أن أكون مخلصاً للوطن والشعب، وأن أحترم الدستور والقانون، وأن أحافظ على وحدة الوطن، واستقراره، وسلامة أراضيه، وأن أرعى مصالح الشعب وحرياته رعاية كاملة، وأن أنفذ أوامر رؤسائي المشروعة، وأن أقوم بجميع واجباتي بالذمة والصدق والأمانة، والله على ما أقول شهيد).
2. يكون أداء اليمين للضباط أمام الرئيس أو من ينيبه لذلك.
3. يكون أداء اليمين لمن هم دون الضباط أمام الوزير أو من ينيبه لذلك.
4. يوقع عناصر الشرطة على نموذج تأدية اليمين، ويحفظ في ملف خدمتهم.

مـادة (19): تقوم إدارة القوى البشرية في الشرطة بتنظيم سجل عام للأقدمية لكافة عناصر الشرطة العاملين، ويشطب من السجل اسم كل من انتهت خدماته.

مادة (20):

1. لغايات تطبيق أحكام هذا القرار بقانون، يعتبر عناصر الشرطة في الوظيفة بحالة استمرار وتحت الطلب للعمل في أي وقت، ويترتب على كل منهم الالتحاق بأي مديرية شرطة عند الطلب أو أن يخدم في أي وحدة عند الضرورة.
2. يصدر المدير العام القرارات والتعليمات اللازمة لتنظيم ساعات الدوام لعناصر الشرطة.

مادة (21):

1. يشترط في الأشخاص المترشحين للدراسة في كليات الشرطة أو الكليات الأمنية أو المعاهد الشرطية والأمنية، التي ستؤهلهم للتخرج برتبة ضابط، الشروط الآتية: أ. أن يكون فلسطيني الجنسية. ب. أن يكون قد أتم من العمر ثمانية عشر عاماً ميلادية، ولم يتجاوز العشرين عاماً. ج. أن يكون لائقاً طبياً للخدمة في الشرطة بقرار من اللجنة الطبية المختصة. د. أن يكون حسن السيرة والسلوك، وألا يكون قد سبق الحكم عليه بعقوبة جنائية أو جنحة مخلة بالشرف أو الأمانة، ما لم يكن قد رد إليه اعتباره من محكمة مختصة. هـ. ألا يكون قد فصل من الخدمة في أي من قوى الأمن الأخرى. و. أن يكون حاصلاً على شهادة الدراسة الثانوية العامة أو ما يعادلها. ز. أن يجتاز بنجاح الاختبارات المقررة لصلاحيته للعمل في الشرطة. ح. أن يستوفي شروط اللياقة الصحية، والبدنية، والطول، والنسبة المئوية لمجموع الدرجات المطلوبة لقبول الترشح للدراسة في كلية الشرطة أو الكليات الأمنية، أو المعاهد الشرطية والأمنية، وأي شروط أخرى يحددها الوزير أو المدير العام.
2. تشكل لجنة للقبول بقرار من المدير العام لاختيار الطلاب المرشحين للدراسة في كلية الشرطة والكليات الأمنية، والمعاهد الشرطية والأمنية.

مادة (22):

1. يشترط على الطالب المقبول للدراسة أن يوقع على تعهد عدلي يقضي بالخدمة لمدة عشر سنوات على الأقل من تاريخ تعيينه في الشرطة، وفي حال عدم الالتزام بالتعهد طوال المدة المحددة، يتم تغريمه بكافة المصاريف التي أنفقت عليه أثناء التدريب.

2. يخضع الطالب المقبول للدراسة لأنظمة الدراسة والتدريب التي يحدد مدتها وشروطها نظام الكلية أو المعهد.

مادة (23): يصدر مجلس الوزراء نظاماً خاصاً يحدد فيه العلاوات والحوافز والمكافآت، وشروط وآليات منحها، وقواعد صرفها لعناصر الشرطة.

مادة (24): مع عدم الإخلال بإقامة الدعوى المدنية أو الجزائية، يعاقب عناصر الشرطة تأديبياً عند القيام بالآتي:

1. مخالفة الواجبات المنصوص عليها في هذا القرار بقانون.
2. مخالفة القرارات والتعليمات الصادرة عن الوزير أو المدير العام أو من في حكمه.
3. الخروج عن مقتضيات الضبط والربط للوظيفة الشرطية.
4. القيام بسلوك أو الظهور بمظهر من شأنه الإخلال بكرامة الوظيفة.

مادة (25):

1. يتحمل المسؤول المباشر كافة المسؤوليات القانونية عن أي أمر مخالف للقانون فيما أمر أو أشار بتنفيذه.
2. لا يعفى أي من عناصر الشرطة من العقوبة إلا في حال ثبت أن ارتكابه للمخالفة كان تنفيذاً لأمر صادر إليه من قبل القائد أو المسؤول عنه، بالرغم من تنبيهه إلى المخالفة، وفي هذه الحالة تكون المسؤولية على مصدر الأمر وحده.
3. تتحمل الدولة دفع أي تعويض قانوني عن عناصر الشرطة المكلفين قانوناً عن الأضرار التي تحدث للغير أثناء تأديتهم للعمل الرسمي ضمن القانون.
4. لا يُسأل أياً من عناصر الشرطة مدنياً إلا عن خطأهم الشخصي.

مادة (26):

1. يتم مساءلة المدير العام أمام مجلس تأديبي في حال الإخلال أو الإهمال أو التقصير بكل ما يتعلق بأداء وظيفته أو بسببها.
2. يشكل المجلس المنصوص عليه في الفقرة (1) من هذه المادة، من: أ. رئيس لجنة الضباط رئيساً. ب. عضوين يعينهما الرئيس لهذا الغرض.
3. ترفع توصيات مجلس التأديب إلى الرئيس لاتخاذ القرار المناسب.

مادة (27):

1. تتشكل مجالس التأديب للضباط بقرار من الوزير، بناءً على توصية المدير العام، وتكون هذه المجالس مسؤولة عن المخالفات التأديبية المحالة إليها.
2. تنقسم مجالس التأديب للضباط إلى: أ. مجلس التأديب الابتدائي: ينظر بالمخالفات التأديبية لضباط الشرطة لمن هم دون رتبة عميد. ب. مجلس التأديب الأعلى: ينظر بالمخالفات التأديبية لضباط الشرطة من رتبة عميد فما فوق.
3. يصدر الوزير بالتشاور مع المدير العام القرارات والتعليمات بشأن الإجراءات الخاصة بعمل المجالس التأديبية، وكل ما يتعلق بتنظيم أعمالها، مع مراعاة الأحكام الواردة في قانون الخدمة والقوانين النافذة ذات الصلة، بشأن المخالفات والعقوبات المقررة لها.

مادة (28):

يصدر قرار الإحالة إلى المجالس التأديبية من قبل الوزير أو المدير العام كل حسب اختصاصه، ويتضمن بياناً بالمخالفات المنسوبة إلى الضابط.

مادة (29):

1. لا يجوز التوصية بالعقوبة على الضابط إلا بعد اتخاذ الإجراءات الآتية: أ. التحقيق معه، وتدوين التحقيق بمحضر مكتوب. ب. سماع أقواله، وتمكينه من حقه بالدفاع عن نفسه.
2. يجب أن يكون القرار الصادر بالتوصية مسبباً، ولا يجوز التوصية بتوقيع أكثر من عقوبة عن المخالفة الواحدة.
3. يقوم المدير العام بعرض توصيات المجالس التأديبية على لجنة الضباط فيما يتعلق باختصاصاتها، وتكون هذه التوصيات نافذة بعد مصادقة الرئيس أو الوزير كل في حدود اختصاصه.
4. فيما عدا اختصاص لجنة الضباط، تكون توصيات المجالس التأديبية نافذة بعد مصادقة المدير العام عليها.

مادة (30):

1. تسقط الملاحقة التأديبية بحق الضابط بمضي أي من المدتين التاليتين، أيهما أقرب: أ. ستة أشهر من تاريخ علم المدير العام، أو القادة المباشرين ومن في حكمهم، بارتكاب المخالفة، كل في حدود اختصاصه ونطاق إشرافه. ب. سنة من تاريخ ارتكاب المخالفة.

2. تنقطع المدد المحددة في الفقرة (1) من هذه المادة، بأي إجراء من إجراءات المجالس التأديبية، وتسري المدد من جديد من تاريخ آخر إجراء.

مادة (31):

1. لا يمنع ترك الضابط للخدمة، من الاستمرار في إجراءات المجالس التأديبية، بشرط أن يكون قد بدأ التحقيق قبل انتهاء مدة خدمته.
2. يجوز في المخالفات المالية التي يترتب عليها ضياع حق من حقوق الدولة مساءلة الضابط تأديبياً، ولو لم يكن قد تم البدء في التحقيق قبل انتهاء خدمته، وذلك خلال الخمس سنوات اللاحقة على انتهاء خدمته.

مادة (32): لا تجوز ترقية أي من ضباط الشرطة المحالين إلى المحاكمة الجزائية في جناية أو جريمة مخلة بالشرف أو الأمانة، إلا إذا صدر حكماً ببراءته فترد له أقدميته من تاريخ وقفها، وفي حال الإدانة يفصل من الخدمة بحكم القانون.

مادة (33): يتم إيقاع العقوبات الانضباطية على الضباط من قبل المدير العام أو القادة المباشرين، كل في حدود اختصاصه، وفقاً للإجراءات والأحكام المعمول بها في القوانين النافذة، على أن يصدر قرار عن الوزير بلائحة المخالفات الانضباطية والعقوبات المقررة بشأنها.

مادة (34):

1. توفر الشرطة المساعدة القانونية المجانية لعناصر الشرطة العاملين الذين تتم إحالتهم إلى النيابة العامة والقضاء بسبب مهامهم الوظيفية، أو المتقاعدين بسبب مهام قاموا بتأديتها أثناء الخدمة.
2. يتم تحديد طرق تقديم المساعدة القانونية بقرار من الوزير، وبالتشاور مع المدير العام.

مادة (35):

1. يتم الاختيار للتعيين في رتبة شرطي طبقاً للشروط والأوضاع التي يحددها هذا القرار بقانون، وطبقاً للاحتياجات الفعلية لهذه الرتبة من الشرطة، وحسب طبيعة المهام الموكلة إليهم مستقبلاً.

2. يتم تعيين الأفراد الحاصلين على رتبة شرطي بعد التخرج بنجاح من المنشآت التدريبية المخصصة لذلك بتنسيب من المدير العام، ومصادقة الوزير.

مادة (36):

1. يشترط في الأشخاص المترشحين للتعيين في رتبة شرطي، توافر الشروط الآتية: أ. أن يكون فلسطيني الجنسية. ب. أن يكون قد أتم من العمر ثمانية عشر عاماً ميلادية، ولم يتجاوز الثانية والعشرين عاماً. ج. أن يكون لائقاً طبياً للخدمة في الشرطة بقرار من اللجنة الطبية المختصة. د. أن يكون حسن السيرة والسلوك، وألا يكون قد سبق الحكم عليه بعقوبة جنائية، أو جريمة مخلة بالشرف أو الأمانة، ما لم يكن قد رد إليه اعتباره من محكمة مختصة. هـ. أن يكون حاصلاً على مؤهل علمي لا يقل عن الشهادة الإعدادية، وأن يجيد القراءة والكتابة إجادة تامة. و. أن يجتاز بنجاح الاختبارات المقررة لصلاحيته للعمل في الشرطة. ز. أن يستوفي شروط اللياقة الصحية، والبدنية، والطول، والنسبة المئوية لمجموع الدرجات المطلوبة لقبول الترشح للتعيين في الشرطة.
2. يتم تشكيل لجنة لقبول التعيين في الشرطة بقرار من المدير العام، ويلحق الشرطي المقبول بالمنشأة التدريبية المخصصة، وللفترة المحددة للتدريب التأسيسي.

مادة (37):

1. يشترط على الفرد المقبول للتعيين في رتبة شرطي أن يوقع على تعهد عدلي يقضي بإلزامه بالخدمة لمدة خمس سنوات على الأقل من تاريخ تعيينه.
2. في حال عدم الالتزام بالتعهد يتم تغريمه بكافة المصاريف التي أنفقت عليه أثناء التدريب.

مادة (38):

1. يتولى الإجراءات التأديبية لضباط الصف والشرطي مجلس تأديبي أو لجنة تحقيق، يتم تشكيلهما بقرار من الوزير أو المدير العام، كل في حدود اختصاصه.
2. يتشكل المجلس التأديبي أو لجنة التحقيق من الآتي: أ. ضابط من إدارة التفتيش. ب. ضابط من إدارة الأمن الداخلي. ج. ضابط لا تقل رتبته عن رائد حقوقي. د. عضوين احتياطيين حقوقيين لا تقل رتبتهما عن ضابط، يسميهما المدير العام.

3. يصدر المدير العام التعليمات والإجراءات الخاصة بعمل المجالس التأديبية، وكل ما يتعلق بتنظيم أعمالها، مع مراعاة الأحكام الواردة في قانون الخدمة، والقوانين النافذة ذات الصلة بشأن المخالفات والعقوبات المقررة لها.

مادة (39): يصدر قرار الإحالة إلى المجالس التأديبية أو لجان التحقيق من الوزير أو المدير العام، كل في حدود اختصاصه، ويتضمن القرار بياناً بالمخالفات المنسوبة لضابط الصف أو الشرطي.

مادة (40):

لا يجوز التوصية بتوقيع عقوبة على ضابط الصف أو الشرطي إلا بعد اتخاذ الإجراءات الآتية: أ. التحقيق معه، وتدوين التحقيق بمحضر مكتوب، ب. سماع أقواله وتمكينه من ممارسة حقه بالدفاع عن نفسه.

1. يجب أن يكون قرار التوصية بإيقاع العقوبة مسبباً، ولا يجوز التوصية بتوقيع أكثر من عقوبة عن المخالفة الواحدة.

مادة (41): لا تعتبر توصيات مجالس التأديب أو لجان التحقيق نهائية إلا بعد التصديق عليها من قبل الوزير أو المدير العام، كل في حدود اختصاصه، مع مراعاة الأحكام الواردة في المواد (27، 30، 31، 33) من هذا القرار بقانون، وتطبيقها على ضباط الصف والشرطي.

مادة (42): تقوم المجالس التأديبية أو لجان التحقيق بإحالة القضايا ذات الطبيعة الجزائية إلى المدير العام، لإحالتها إلى النيابة العامة لاتخاذ المقتضى القانوني، وفقاً لأحكام قانون الإجراءات الجزائية النافذ.

مادة (43): يصدر الرئيس قراراً بناءً على توصية المدير العام يحدد فيه الزي الرسمي لعناصر الشرطة، وعلامات رتبهم، وشعار الشرطة، والشعارات الخاصة بالإدارات والدوائر.

مادة (44): يصدر المدير العام التعليمات اللازمة للرقابة والتفتيش والمتابعة وتقييم الأداء في الشرطة، وفقاً لمعايير محددة يخضع لها جميع عناصر الشرطة.

مادة (45):

1. للشرطة الحصول على البيانات الشخصية، وتخزينها، واستعمالها وفقاً لأحكام القوانين المعمول بها، والمبادئ الدولية لحماية البيانات.
2. يقتصر الحصول على البيانات الشخصية، وتخزينها، واستعمالها على الحد اللازم لتحقيق الغايات الشرطية المشروعة، وبما لا يتعارض مع القوانين المعمول بها.

مادة (46): يضع المدير العام بالتشاور مع اللجنة مدونة السلوك وأخلاقيات عناصر الشرطة، وتصدر عن الوزير.

مادة (47):

1. تنشأ بموجب أحكام هذا القرار بقانون كلية فلسطين للقانون وعلوم الشرطة، يتبعها عدد من المعاهد المتخصصة.
2. يصدر مجلس الوزراء نظاماً خاصاً لتنظيم عمل كلية فلسطين للقانون وعلوم الشرطة، على أن يتضمن النظام الأحكام الآتية: أ. العملية التدريبية والتعليمية الخاصة بكلية الشرطة. ب. تحديد الخطط والبرامج التعليمية والتدريبية والامتحانات. ج. آلية منح الشهادات واعتمادها، ومدة التدريب، والدرجات العلمية، والرتب العسكرية التي تمنحها عند التخرج.
3. يصدر الوزير التعليمات الخاصة بتنظيم مدارس ومراكز تدريب الشرطة، وحقوق الطلاب خلال مدة الدراسة والتدريب.

مادة (48): يتم إنشاء أندية اجتماعية ورياضية لعناصر الشرطة، بقرار يصدر عن المدير العام، وموافقة الوزير.

مادة (49): إذا توفي أي من عناصر الشرطة وهو في الخدمة أو بعد إحالته إلى التقاعد، تصرف نفقات الجنازة للأرامل أو لأولاده أو لمن يثبت قيامه بصرف هذه النفقات، وفق النظام المعمول به في قوى الأمن الفلسطينية، تتكفل الدولة على نفقتها القيام بكافة الإجراءات اللازمة لإعادة جثمان المتوفى من الخارج، إذا كان في مهمة رسمية أو في بعثة دراسية أو تدريبية أو إجازة دراسية أو للعلاج أو الإعارة.

مـادة (50): تـتم ترقيـة مـن استشـهد مـن عناصـر الشـرطة خـلال أداء وظيفتـه أو بسـببها للرتبـة التاليـة لرتبتـه التـي يشـغلها دون التقيـد بشـروط الترقـي، ويعتمـد شـهيداً بالرتبـة المرقـى إليهـا، ويستحق ذويه راتب أول مربوط الرتبة.

مادة (51):

1. يستحق عناصر الشرطة تعويضاً مادياً عن الأضرار التي تصيب أموالهم الخاصة أثناء الخدمة أو بسببها عن غير إهمال منهم في حال تعذر تعويضها بالطرق القانونية أمام القضاء.
2. يصدر الوزير قراراً بناءً على توصية المدير العام بتشكيل لجنة خاصة لتقدير التعويض المناسب لكل حالة، ويحدد فيه القواعد اللازمة للتعويض.

مادة (52):

1. لعناصر الشرطة اللجوء إلى استعمال القوة واستعمال السلاح الناري بالقدر اللازم لأداء الواجبات والمهام المشروعة في الحالات التي تجيزها التشريعات النافذة، بشرط مراعاة الآتي:

أ. أن تكون هي الوسيلة الوحيدة بعد استنفاذ كافة الوسائل الأخرى غير العنيفة.

ب. أن يكون استعمال القوة عند الضرورة وبشكل تدريجي يتناسب مع الهدف الذي ترغب عناصر الشرطة في تحقيقه.

ج. أن يكون استعمال القوة بالقدر اللازم لدرء الخطر.

2. يتم مراعاة الإجراءات والوسائل في حالات استخدام القوة والسلاح الناري وفق ما نصت عليه القوانين النافذة، على أن يصدر الوزير التعليمات اللازمة لاستخدام القوة والسلاح الناري.

مادة (53):

1. يخضع عناصر الشرطة للمساءلة الجزائية أمام القضاء في حال ارتكاب أي منهم لجريمة معاقب عليها وفقاً للقوانين النافذة.
2. على الرغم مما ورد في الفقرة (1) من هذه المادة، ودون الإخلال بأحكام المادة (54) من قانون الإجراءات الجزائية، يخضع عناصر قوة الشرطة للمساءلة الجزائية أمام

القضـــاء العســكري فـــي حـــال ارتكـــاب أي مـــنهم لجريمـــة تتعلـــق بالشـــأن العســـكري، وفقـــاً للتشريعات والقوانين النافذة ذات الصلة.

مـــادة (54): بمـــا لا يتعـــارض مـــع أحكـــام هـــذا القـــرار بقـــانون، تبقـــى جميـــع الأنظمـــة والقـــرارات والتعليمـــات الصـــادرة فيمـــا يتعلـــق بشـــأن الشـــرطة نافـــذة لحـــين صـــدور الأنظمـــة والقـــرارات اللازمـــة لتنفيذ أحكامه.

مادة (55):

1. يصدر مجلس الوزراء اللوائح والأنظمة ذات الصلة لتنفيذ أحكام هذا القرار بقانون.
2. يصدر الوزير القرارات ذات الصلة لتنفيذ أحكام هذا القرار بقانون.
3. يصدر المدير العام التعليمات ذات الصلة لتنفيذ أحكام هذا القرار بقانون.

مادة (56):

1. يلغـــى قـــانون الأمـــن العـــام المؤقـــت رقـــم (38) لســـنة 1965م وتعديلاتـــه، بشـــأن الشـــرطة النافذ في المحافظات الشمالية.
2. يلغى القرار بقانون رقم (6) لسنة 1963م، بشأن الشرطة النافذ في المحافظات الجنوبية.
3. يلغى كل ما يتعارض مع أحكام هذا القرار بقانون.

مادة (57): يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره.

مـــادة (58): علـــى الجهـــات المختصـــة كافـــة، كـــل فيمـــا يخصـــه، تنفيـــذ أحكـــام هـــذا القـــرار بقـــانون، ويعمل به من تاريخ نشره في الجريدة الرسمية.

صـــدر فـــي مدينـــة رام الله بتـــاريخ: 2017/12/26 ميلاديـــة الموافـــق: 08/ربيـــع الثـــاني/1439 هجريـــة

محمود عباس رئيـــس دولـــة فلسطـــين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية.

ملحق (5): قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية:

رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية استناداً لأحكام القانون الأساسي المعدل لسنة (2003 م) وتعديلاته، لا سيما أحكام المادة (43) منه، وبعد الاطلاع على أحكام قانون العقوبات رقم (74) لسنة (1936 م) وتعديلاته، الساري في المحافظات الجنوبية، والاطلاع على أحكام قانون العقوبات رقم (16) لسنة (1960 م) وتعديلاته، الساري في المحافظات الشمالية، وعلى أحكام قانون الاتصالات السلكية واللاسلكية رقم (3) لسنة (1996 م)، وعلى أحكام قانون الإجراءات الجزائية رقم (3) لسنة (2001 م) وتعديلاته، وعلى أحكام القرار بقانون رقم (18) لسنة (2015 م)، بشأن مكافحة المخدرات والمؤثرات العقلية، وعلى أحكام القرار بقانون رقم (20) لسنة (2015 م)، بشأن مكافحة غسل الأموال وتمويل الإرهاب وتعديلاته، وعلى أحكام القرار بقانون رقم (6) لسنة (2017 م) ، بشأن تنظيم نقل وزراعة الأعضاء البشرية، وعلى أحكام القرار بقانون رقم (15) لسنة (2017 م) ، بشأن المعاملات الإلكترونية، وعلى أحكام القرار بقانون رقم (16) لسنة (2017 م) بشأن الجرائم الإلكترونية، وبناءً على تنسيب مجلس الوزراء بتاريخ (17/04/2018 م)، وعلى الصلاحيات المخولة لنا، وتحقيقاً للمصلحة العامة، وباسم الشعب العربي الفلسطيني، أصدرنا القرار بقانون الآتي:

مادة (1): يكون للكلمات والعبارات الواردة في هذا القرار بقانون المعاني المخصصة لها أدناه، ما لم تدل القرينة على خلاف ذلك:

الوزارة: وزارة الاتصالات وتكنولوجيا المعلومات.

الوزير: وزير الاتصالات وتكنولوجيا المعلومات.

معالجة البيانات: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات، سواء تعلقت بأفراد أو خلافه، بما في ذلك جمع تلك البيانات أو استلامها أو تسجيلها أو تخزينها أو تعديلها أو نقلها أو استرجاعها أو محوها أو نشرها، أو إعادة نشر بيانات أو حجب الوصول إليها، أو إيقاف عمل الأجهزة أو إلغاؤها أو تعديل محتوياتها.

تكنولوجيا المعلومات: أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أي وسيلة أخرى، سواء أكانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة.

البيانات والمعلومات الإلكترونية: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات، وغيرها.

الشبكة الإلكترونية: ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العا لمية (الإنترنت).

السجل الإلكتروني: مجموعة المعلومات التي تشكل بمجملها وصفاً لحالة تتعلق بشخص أو شيء ما، والتي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية.

المستند الإلكتروني: السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات على وسيط مادي أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه.

الموقع الإلكتروني: مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد.

الشخص: الشخص الطبيعي أو المعنوي.

التطبيق الإلكتروني: برنامج إلكتروني مصمم لأداء مهمة محددة بشكل مباشر للمستخدم أو لبرنامج إلكتروني آخر، يستخدم من خلال وسائل تكنولوجيا المعلومات أو ما في حكمها.

بيانات المرور: أي بيانات أو معلومات إلكترونية تنشأ عن طريق تكنولوجيا المعلومات تبين مصدر الإرسال، والوجهة المرسل إليها، والطريق الذي سلكه، ووقته، وتاريخه، وحجمه، ومدته، ونوع خدمة الاتصال.

كلمة السر: كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات، وما في حكمها، للتأكد من هويته، وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها.

وسيلة التعامل الإلكتروني: البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو ما في حكمها من تكنولوجيا المعلومات أو تطبيق إلكتروني، تحتوي هذه الوسيلة على بيانات أو معلومات إلكترونية تصدرها الجهات المرخصة بذلك.

البيانات الحكومية: البيانات الخاصة بالدولة والهيئات والمؤسسات العامة أو الشركات التابعة لها.

التشفير: تحويل بيانات إلكترونية إلى شكل يستحيل به قراءتها وفهمها دون إعادتها إلى هيئتها الأصلية.

الشفرة: مفتاح أو مفاتيح سرية خاصة، لشخص أو لجهة معينة تستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز والبصمات أو ما في حكمها.

الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها.

الاختراق: الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية.

التوقيع الإلكتروني: بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها، ويميزه عن غيره بغرض الموافقة على مضمون المعاملة.

أداة التوقيع: برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة.

الشهادة: شهادة التصديق الإلكترونية التي تصدرها الوزارة أو الجهة المفوضة من قبلها لإثبات العلاقة والارتباط بين الموقع وبيانات التوقيع الإلكتروني.

مزود الخدمة: أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أي خدمة إلكترونية أو مستخدمي هذه الخدمة.

الإتلاف: تدمير البرامج الإلكترونية، سواء أكان كلياً أم جزئياً، أو جعلها على نحو غير صالحة للاستعمال.

معلومات المشترك: المعلومات الموجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات حول نوع خدمة الاتصالات المستخدمة، والشروط الفنية، وفترة الخدمة، وهوية المشترك، وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة، وأي معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة.

الموظف: كل من يعمل في القطاع العام أو الخاص أو المؤسسات الخاصة أو الهيئات المحلية والأهلية أو الجمعيات أو الشركات الخاصة التي تساهم بها الدولة، وكل من هو في حكمهم.

الحبس: وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين أسبوع إلى ثلاث سنوات.

السجن: وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين ثلاث سنوات إلى خمس عشرة سنة.

مادة (2):

1. تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء كان الفاعل أصلياً أم شريكاً أم محرضاً أم متدخلاً، على أن تكون الجرائم معاقباً عليها خارج فلسطين، مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ.
2. يجوز ملاحقة كل من يرتكب خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات الآتية:

أ. إذا ارتكبت من مواطن فلسطيني.
ب. إذا ارتكبت ضد أطراف أو مصالح فلسطينية.
ت. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد بالأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية.

مادة (3):

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.

مادة (4):

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.

مادة (5): 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.

مادة (6): كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو إتلاف البرامج أو حذفها أو تعديلها، 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.

مادة (7): 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.

مادة (8):

1. كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، 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. كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية أو أداة إنشاء التوقيع الإلكتروني المتعلقة بتوقيع شخص غيره، 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.
3. كل من ارتكب جريمة باستخدام أي من الوسائل المذكورة في الفقرة (2) من هذه المادة، يعاقب بالسجن وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (9):

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.

مادة (10): 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.

مادة (11): تتضمن على:

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.

مادة (12): تتمضن على:

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.

مادة (13): كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال أو اختلاسها، يعاقب بالسجن 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.

مادة (14): 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 وعن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (15): تتضمن على:

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 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.

مادة (16): تتضمن على:

1. كل من أرسل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن هم فوق الثامنة عشر سنة ميلادية دون رضاه، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنتين، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2. كل من أرسل أو نشر عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن لم يكمل الثامنة عشر سنة ميلادية أو تتعلق بالاستغلال الجنسي لهم، 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.
3. كل من قام قصداً باستخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشر سنة ميلادية أو من هو من ذوي الإعاقة، 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، أو بكلتا العقوبتين.

مادة (17): 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.

مادة (18): دون الإخلال بالأحكام الواردة في القرار بقانون بشأن مكافحة غسل الأموال وتمويل الإرهاب النافذ، يعاقب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو إحدى وسائل تكنولوجيا المعلومات بقصد:

1. القيام بارتكاب جريمة غسل الأموال 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.
2. القيام بارتكاب جريمة تمويل الإرهاب بالسجن 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.

مادة (19): 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.

مادة (20): كل من انتهك حق من حقوق الملكية الفكرية أو الأدبية أو الصناعية وفقاً للتشريعات النافذة، عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس مدة لا تزيد على 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.

مادة (21): تتضمن على:

1. لكل إنسان حق التعبير عن رأيه بالقول أو الكتابة أو التصوير أو غير ذلك من وسائل التعبير والنشر وفقاً للقانون.
2. حرية الإبداع الفني والأدبي مكفولة، ولا يجوز رفع أو تحريك الدعاوى لوقف أو مصادرة الأعمال الفنية والأدبية والفكرية أو ضد مبدعيها إلا بأمر قضائي، ولا توقع عقوبة سالبة للحرية أو التوقيف الاحتياطي في الجرائم التي ترتكب بسبب علانية المنتج الفني أو الأدبي أو الفكري.
3. حرية الصحافة والطباعة والنشر الورقي والمرئي والمسموع والإلكتروني مكفولة، وللفلسطينيين من أشخاص طبيعية أو اعتبارية عامة أو خاصة، حق ملكية وإصدار الصحف، وإنشاء وسائل الإعلام المرئية والمسموعة ووسائط الإعلام الرقمي وفقاً للقانون.
4. لا يجوز فرض قيود على الصحافة أو مصادرتها أو وقفها أو إنذارها أو إلغاؤها إلا وفقاً للقانون، وبموجب حكم قضائي.

مادة (22):

1. يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته.
2. كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بقصد نشر أخبار أو صور أو تسجيلات صوتية أو مرئية، سواء كانت مباشرة أو مسجلة، تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، 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.

مادة (23): كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد إدارة مشروع مقامرة أو تسهيله أو تشجيعه أو الترويج له أو عرض ألعاب مقامرة، 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.

مادة (24): كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد عرض أي كلمات مكتوبة أو سلوكيات من شأنها أن تؤدي إلى إثارة الكراهية العنصرية أو الدينية أو التمييز العنصري بحق فئة معينة بسبب انتمائها العرقي أو المذهبي أو اللون أو الشكل أو بسبب الإعاقة، يعاقب بالحبس مدة لا تزيد عن سنة، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (25): 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.

مادة (26): كل من حاز بغرض الاستخدام جهازاً أو برنامجاً أو أي بيانات إلكترونية معدة أو كلمة سر أو تراميز دخول أو قدمها أو أنتجها أو وزعها أو استوردها أو صدرها أو روج لها، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، 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.

مادة (27):

1. كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار بقانون، مستغلاً صلاحياته وسلطاته أثناء تأدية عمله، أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلث.
2. كل من ارتكب، من موظفي مزودي الخدمة، أياً من الجرائم المنصوص عليها في هذا القرار بقانون، أثناء تأدية عمله أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلثين.

مادة (28): كل من حرض أو ساعد أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون، بأي وسيلة إلكترونية، ووقعت الجريمة بناءً على هذا التحريض أو المساعدة أو الاتفاق، يعاقب بالعقوبات المقررة لفاعلها الأصلي.

مادة (29): إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات أو أن تقضي بحله في حال كانت الجريمة معاقب عليها بالحبس لمدة لا تقل عن سنة، وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له.

مادة (30): كل من نشر قصداً معلومات عن موقع إلكتروني محجوب بموجب أحكام المادة (39) من هذا القرار بقانون، باستخدام أنظمة أو موقع أو تطبيق إلكتروني، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (31): يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي:

1. تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة.
2. حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية، مع مراعاة الإجراءات الواردة في المادة (39) من هذا القرار بقانون.

3. الاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات لغايات ما ورد في الفقرة(1) من هذه المادة.
4. التعاون ومساعدة الجهات المختصة وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ المؤقت بها.

مادة (32):

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.

مادة (33):

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.

مادة (34):

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.

مادة (35): على الجهات المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة أو الأدوات أو وسائل تكنولوجيا المعلومات أو الأنظمة الإلكترونية أو البيانات أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها.

مادة (36):

1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له، ومدته.
2. تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط.
3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.

مادة (37): 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.

مادة (38): 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.

مادة(39):

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 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.

مادة (40): 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.

مادة (41): 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.

مادة (42):

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.

مادة (43):

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.

مادة (44): مع عدم الإخلال بأي عقوبة أشد، ينص عليها قانون العقوبات الساري أو أي قانون آخر، يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات المنصوص عليها فيه.

مادة (45): كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها أو تدخل فيها أو حرض على ارتكابها، ولم ينص عليها في هذا القرار بقانون، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع.

مادة (46): كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون، في غير الأحوال المصرح بها قانوناً، 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.

مادة (47): كل من أقدم على العبث بأدلة قضائية معلوماتية أو أقدم على إتلافها أو إخفائها أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (48): يعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة أو التدخل في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب بنصف العقوبة.

مادة (49): 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.

مادة (50): 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.

مادة (51): تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أياً من الجرائم المنصوص عليها فيه، سواء ارتكبت في فلسطين أو خارجها، وتعتبر الأحكام الأجنبية سابقة في التكرار بحق الجاني.

مادة (52): 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.

مادة (53): يعفى من العقوبات المنصوص عليها في هذا القرار بقانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأي معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، ويجوز للمحكمة أن تقضي بوقف تنفيذ العقوبة إذا حصل الإبلاغ بعد علم السلطات المختصة، وأدى إلى ضبط باقي الجناة.

مادة (54): تتولى الوزارة وفقاً لاختصاصها تقديم الدعم والمساعدة الفنية لجهات إنفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون.

مادة (55):

1. يلغى القرار بقانون رقم (16) لسنة 2017 م، بشأن الجرائم الإلكترونية.

2. يلغى كل ما يتعارض مع أحكام هذا القرار بقانون.

مادة (56): يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره.

مادة (57): على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به من تاريخ نشره في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ:29/04/2018 ميلادية الموافق:13/شعبان/1439 هجرية
محمود عباس/ رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية.

ملحق (6): قرار بقانون رقم (28) لسنة (2020م) بتعديل قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية:

رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية استناداً للنظام الأساس لمنظمة التحرير الفلسطينية، وللقانون الأساسي المعدل لسنة (2003م) وتعديلاته، وبعد الاطلاع على قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية، وبناءً على الصلاحيات المخولة لنا، وتحقيقاً للمصلحة العامة، أصدرنا القرار بقانون الآتي:

مادة (1): يشار إلى قرار بقانون رقم (10) لسنة 2018م، بشأن الجرائم الإلكترونية، لغايات إجراء هذا التعديل بالقانون الأصلي.

مادة (2): تعدل المادة (15) من القانون الأصلي، لتصبح على النحو الآتي:

أ. 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.

ب. 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 قانوناً.

مادة (3): على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به من تاريخ نشره في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ: 01/09/2020 ميلادية الموافق: 13/محرم/1442 هجرية محمود عباس رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

ملحق (7): قرار بقانون رقم (38) لسنة 2021م بتعديل قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته

رئيـــس دولــة فلسطـــين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية استنادًا للنظام الأساس لمنظمة التحرير الفلسطينية، وللقانون الأساسي المعدل لسنة 2003م وتعديلاته، وبعد الاطلاع على القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته، وعلى قرار بقانون رقم (37) لسنة 2021م بشأن الاتصالات وتكنولوجيا المعلومات، وبناءً على الصلاحيات المخولة لنا، وتحقيقًا للمصلحة العامة، أصدرنا القرار بقانون الآتي:

مادة (1): يشار إلى القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته، لغايات إجراء هذا التعديل بالقانون الأصلي.

مادة (2): يعدل عنوان القانون الأصلي ليصبح "قرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

مادة (3): تضاف التعاريف التالية إلى المادة (1) من القانون الأصلي على النحو الآتي:

الهيئة: هيئة تنظيم قطاع الاتصالات.

الرخصة: الشهادة الصادرة عن الهيئة بأن الشخص قد استوفى الشروط القانونية للسماح له بإنشاء أو تشغيل أو إدارة شبكة اتصالات عامة، أو تقديم خدمات اتصالات عامة، أو استخدام ترددات راديوية أو موجات راديوية، وفقًا للقانون.

المرخص له: الشخص الذي حصل على الرخصة من الهيئة. الاتصالات: نقل أو إرسال أو استقبال أو بث أو تمرير الصوت، والبيانات، والإشارات، والرموز ، والفيديو، والصور بوسائل سلكية أو لاسلكية أو راديوية أو بصرية أو كهرومغناطيسية أو أي وسيلة أخُرى للاتصالات.

خدمة الاتصالات: الخدمة التي تتكون كليًا أو جزئيًا من إرسال المعلومات أو البيانات أو استقبالها أو تمريرها على شبكات الاتصالات باستخدام أي من عمليات الاتصالات. خدمة الاتصالات العامة: خدمة الاتصالات المقدمة للمشتركين والمرخص لهم الآخرين مقابل أجر ، والاتجار واستيراد أجهزة الاتصالات السلكية واللاسلكية وتصنيعها.

أجهزة الاتصالات: الأجهزة التي تستخدم في نقل أو إرسال أو استقبال أو بث أو تمرير الصوت ، والبيانات، والإشارات، والرموز، والفيديو، والصور بوسائل سلكية أو لاسلكية أو راديوية أو بصرية أو كهرومغناطيسية أو أي وسيلة أخرى للاتصالات.

مادة (4): تعدل المادة (3) من القانون الأصلي لتصبح على النحو الآتي:

1- تنشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات"، وتتولى النيابة العامة الإشراف القضائي عليها، كل في دائرة اختصاصه.
2- تتولى المحاكم النظامية والنيابة العامة، وفقًا لاختصاصاتهما، النظر في دعاوى الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

مادة (5): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (31) تنص على الآتي:

1. كل من نشر أو أشاع مضمون أي اتصال أو مكالمة هاتفية بواسطة شبكة اتصالات أو بواسطة تقنيات تكنولوجيا المعلومات، أو رسالة هاتفية اطلع عليها بحكم وظيفته أو قام بتسجيلها دون سند قانوني، أو ساعد أو شارك في ذلك، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة مالية لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني ، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

2. كل من أقدم أو ساعد أو شارك بكتم رسالة أو مكالمة عليه نقلها بواسطة شبكات الاتصالات إلى شخص آخر، أو رفض نقل رسائل أو مكالمات طلب منه نقلها وفقًا للقانون أو الرخصة، أو عبث بالبيانات المتعلقة بأحد المشتركين بما في ذلك أرقام الهواتف غير المعلنة والفواتير، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن سبعة آلاف دينار أردني ولا تزيد على خمسة عشر ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

مادة (6): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (32) تنص على الآتي:

1. كل من أقدم أو ساعد أو شارك قصدًا بتخريب منشآت الاتصالات أو تكنولوجيا المعلومات أو ألحق بها ضررًا، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، وبغرامة مالية لا

تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

2. كل من تسبب إهمالًا في تخريب منشآت الاتصالات أو تكنولوجيا المعلومات أو إلحاق الضرر بهما، يعاقب بغرامة مالية لا تقل عن مائة دينار أردني، ولا تزيد على خمسمائة دينار أردني ، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (7): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (33) تنص على الآتي:

1. كل من قام أو ساهم أو ساعد أو شارك بتقديم خدمات اتصالات بوسائل من شأنها قيام منافسة غير مشروعة، بين شبكات الاتصالات المرخصة وشبكات اتصالات أجنبية أو غير مرخصة، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة، أو بغرامة مالية لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين ، وفي جميع الأحوال الحكم بمصادرة الأجهزة والأدوات المستخدمة في تقديم الخدمات.

2. كل من استخدم أو ساعد أو شارك باستخدام وسائل غير مشروعة لإجراء اتصالات دون دفع الرسوم يعاقب بالحبس مدة ثلاثة أشهر، وغرامة مالية لا تقل عن خمسمائة دينار أردني ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

3. كل من استخدم شبكة اتصالات خاصة لتزويد خدمات اتصالات عامة أو قام أو ساعد أو شارك بربط شبكة اتصالات خاصة بشبكة اتصالات عامة دون موافقة الهيئة، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة مالية لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، وإزالة المخالفة على نفقة الفاعل.

مادة (8): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (34) تنص على الآتي:

1. كل من أنشأ أو شغل أو أدار شبكة اتصالات عامة بهدف تقديم خدمات اتصالات خلافًا لأحكام قرار بقانون بشأن الاتصالات وتكنولوجيات المعلومات النافذ والأنظمة الصادرة بمقتضاه ، أو ساعد أو شارك في ذلك، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة ، أو

بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

2. إذا كان مرتكب المخالفة المحددة في الفقرة رقم (1) من هذه المادة، شخصًا اعتباريًا، يعاقب بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانونًا، وفي جميع الأحوال الحكم بمصادرة الأجهزة المستخدمة.

مادة (9): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (35) تنص على الآتي:

1. مع مراعاة الأحكام الواردة في قرار بقانون بشأن الاتصالات وتكنولوجيا المعلومات النافذ، كل من شغل محطة راديوية أو استخدم ترددات أو أرقام دون ترخيص، أو ساعد أو شارك في ذلك قصدًا يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

2. إذا كان مرتكب المخالفة المشار إليها في الفقرة (1) من هذه المادة، شخصًا اعتباريًا يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، ومصادرة الأجهزة المستخدمة.

3. كل من قام دون الحصول على موافقة الهيئة، بالتنازل للغير عن الترخيص الصادر له باستخدام تردد أو أرقام أو أي موارد اتصالات نادرة، يعاقب بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، وإلغاء الترخيص وإبطال التصرف.

مادة (10): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (36) تنص على التالي:

مع عدم الإخلال بأي عقوبة أشد ينص عليها أي قانون آخر، كل من اعترض أو أعاق أو غير أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو تكنولوجيا المعلومات أو حرض أو ساعد أو شارك غيره على القيام بهذا العمل، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

مادة (11): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (37) تنص على الآتي:

1. كل من قام متعمدًا أو ساعد أو شارك بأي إجراء لاعتراض موجات راديوية مخصصة للغير أو بالتشويش عليها أو بقطعها، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، وفي جميع الأحوال الحكم بمصادرة الأجهزة المستخدمة بالتشويش.

2. إذا ارتكب المخالفة المحددة في الفقرة (1) من هذه المادة شخصًا اعتباريًا، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، والحكم بمصادرة الأجهزة المستخدمة.

مادة (12): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (38) تنص على الآتي:

1. كل من أدخل إلى أراضي الدولة أجهزة أو أنظمة أو برامج اتصالات أو تكنولوجيا معلومات مخالفة للمواصفات أو المعايير الفنية المعتمدة من الهيئة، أو تحمل بيانات أو معلومات غير صحيحة، بقصد تسويقها أو بيعها أو ساعد أو شارك في ذلك، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على ألفي دينار أردني ،أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، والحكم بمصادرة الأجهزة المضبوطة.

2. كل من قام بحيازة أو ببيع أو تداول أو عرض أجهزة التنصت بأنواعها، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، والحكم بمصادرة الأجهزة المضبوطة.

مادة (13): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (39) تنص على التالي:

كل من قام دون ترخيص بممارسة أي حرفة أو مهنة اتصالات أو تكنولوجيا معلومات تستوجب الترخيص وفقًا لأحكام القرار بقانون بشأن الاتصالات وتكنولوجيات المعلومات النافذ والتشريعات الصادرة بمقتضاه، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

مادة (14): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (40) تنص على التالي:

إذا لم يلتزم المرخص له بتغطية كامل المنطقة الجغرافية المعينة له بالخدمة المرخصة بموجب الرخصة، يعاقب بغرامة لا تقل عن مائة ألف دينار أردني ولا تزيد على خمسمائة ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (15): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (41) تنص على التالي:

كل شخص ألغيت رخصته ولم يتوقف فورًا عن استقبال مشتركين جدد، أو عن تزويد خدمات الاتصالات، إلا بالقدر الكافي لتحويل مشتركيه إلى مرخص له آخر وفقًا لما تقرره الهيئة لهذه الغاية ، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني ، أو ما يعادلها بالعملة المتداولة قانونًا، والحكم بمصادرة الأجهزة والشبكة.

مادة (16): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (42) تنص على التالي:

1. كل شخص رفضت الهيئة تجديد رخصته، وقام بإزالة شبكة أو شبكات الاتصالات التي أنشأها أو أي جزء منها دون موافقة خطية من الهيئة، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانونًا.

2. إذا كان الشخص المذكور في الفقرة (1) من هذه المادة، مرخص له لتقديم خدمات الاتصالات الثابتة أو المتنقلة أو البنية التحتية للاتصالات أو تكنولوجيا المعلومات، يعاقب بغرامة لا تقل عن عشرة ملايين دينار أردني ولا تزيد على خمسين مليون دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (17):

تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (43) تنص على الآتي:

1. إذا استخدم المرخص له ترددات أو أرقام أو أي موارد هامة أخرى لم تخصص له من الهيئة ، يعاقب بغرامة لا تقل عن عشرين ألف دينار أردني ولا تزيد على خمسين ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانونًا، وسحبها منه فورًا وإعادتها للهيئة.

2. إذا استخدم المرخص له الترددات أو الأرقام المخصصة له من الهيئة أو أي موارد هامة أخرى في غير الغاية المرخصة أو المخصصة من أجلها، أو إذا لم يلتزم بأي شرط من شروط تخصيصها،

يعاقب بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، وسحبها منه فورًا وإعادتها للهيئة.

مادة (18): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (44) تنص على الآتي:

1. إذا خالف المرخص له أي حكم من الأحكام الواردة في الفصل الثامن من قرار بقانون بشأن الاتصالات وتكنولوجيا المعلومات النافذ، بشأن الربط البيني والنفاذ والمشاركة في البنية التحتية، يعاقب بغرامة لا تقل عن ثلاثين ألف دينار أردني ولا تزيد على خمسين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

2. إذا كان الشخص المذكور في الفقرة (1) من هذه المادة، مرخص له لتقديم خدمات الاتصالات الثابتة أو المتنقلة أو البنية التحتية للاتصالات أو تكنولوجيا المعلومات، يعاقب بغرامة لا تقل عن مائة ألف دينار أردني ولا تزيد على مائتي ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (19): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (45) تنص على التالي: كل مرخص له لم يلتزم بالإعلان عن أسعار خدمات الاتصالات المقدمة للجمهور بالكيفية التي تقرها أو توافق عليها الهيئة، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (20): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (46) تنص على الآتي:

1. إذا خالف المرخص له أي حكم من الأحكام الواردة في الفصل العاشر من قرار بقانون بشأن الاتصالات وتكنولوجيا المعلومات النافذ بشأن العلاقة بين المرخص له والمشترك، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

2. إذا كان المرخص له في الفقرة (1) من هذه المادة، مرخص له لتقديم خدمات الاتصالات الثابتة أو الخلوية المتنقلة أو البنية التحتية للاتصالات أو تكنولوجيا المعلومات، يعاقب بغرامة لا تقل عن ثلاثين ألف دينار أردني ولا تزيد على خمسين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (21): تضاف مادة جديدة إلى القانون الأصل تحمل الرقم (47) تنص على التالي:

1. كل مرخص له قام بغش أو خداع أو تضليل المشترك بأي طريقة كانت، أو الإثراء على حسابه دون مسوغ قانوني، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

2. إذا كان المرخص له في الفقرة (1) من هذه المادة، مرخص له لتقديم خدمات الاتصالات الثابتة أو الخلوية المتنقلة أو البنية التحتية للاتصالات أو تكنولوجيا المعلومات، يعاقب بغرامة لا تقل عن خمسين ألف دينار أردني ولا تزيد على مائة ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (22): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (48) تنص على التالي:

إذا خالف المرخص له أي حكم من أحكام خطة الترقيم الوطنية، يعاقب بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (23): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (49) تنص على التالي:

إذا قام المرخص له بفعل أو امتنع عن فعل أدى إلى الإضرار بمواقع أثرية أو سياحية أو أدى إلى الإضرار بالبيئة أو الصحة العامة، يعاقب بغرامة لا تقل عن خمسين ألف دينار أردني ولا تزيد على مائة ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (24): تضاف مادة جديدة إلى القانون الأصلي تحمل الرقم (50) تنص على الآتي:

1. كل من منع أو أعاق بأي شكل من الأشكال عمل موظفي الهيئة المكلفين بالرقابة، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على ستة أشهر، وبغرامة لا تقل عن ألف دينار أردني ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

2. إذا كان المرخص له أو أحد موظفيه هو مرتكب المخالفة المحددة في الفقرة (1) من هذه المادة يعاقب من تسبب بالمنع أو الإعاقة بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، ويعاقب المرخص له بغرامة لا تقل عن خمسين ألف دينار أردني ولا تزيد على مائة ألف دينار أردني ، أو ما يعادلها بالعملة المتداولة قانونًا.

3. إذا امتنع المرخص له أو تأخر عن تزويد الهيئة بأي تقارير أو مستندات أو وثائق أو اتفاقيات أو معلومات أو بيانات تطلبها، يعاقب بغرامة لا تقل عن خمسين ألف دينار أردني ولا تزيد على مائة ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (25): تعدل الفقرة (5) من المادة (32) من القانون الأصلي لتصبح على النحو الآتي:

5. يشترط في مأمور الضبط القضائي أن يكون مؤهلًا للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية ولجرائم الاتصالات وتكنولوجيا المعلومات.

مادة (26): تلغى المادة (54) من القانون الأصلي.

مادة (27):

1. يعاد ترقيم مواد القانون الأصلي من المواد (31 – 53) لتصبح (51 – 73).

2. يعاد ترقيم مواد القانون الأصلي من المواد (55– 75) لتصبح (74 – 76).

مادة (28): يلغى كل ما يتعارض مع أحكام هذا القرار بقانون.

مادة (29): على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به بعد ثلاثين يومًا من تاريخ نشره في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ: 2021/10/02 ميلادية

الموافق: 25/صفر/1443 هجرية

محمود عباس

رئيـــــــــس دولـــــــــة فلسطـــــــين

رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

ملحق (8): قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته

رئيس دولة فلسطين

رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

استناداً لأحكام القانون الأساسي المعدل لسنة (2003 م) وتعديلاته، لا سيما أحكام المادة (43) منه، وبعد الاطلاع على أحكام قانون العقوبات رقم (74) لسنة (1936 م) وتعديلاته، الساري في المحافظات الجنوبية، والاطلاع على أحكام قانون العقوبات رقم (16) لسنة (1960 م) وتعديلاته، الساري في المحافظات الشمالية، وعلى أحكام قانون الاتصالات السلكية واللاسلكية رقم (3) لسنة (1996 م)، وعلى أحكام قانون الإجراءات الجزائية رقم (3) لسنة (2001 م) وتعديلاته، وعلى أحكام القرار بقانون رقم (18) لسنة (2015 م)، بشأن مكافحة المخدرات والمؤثرات العقلية، وعلى أحكام القرار بقانون رقم (20) لسنة (2015 م)، بشأن مكافحة غسل الأموال وتمويل الإرهاب وتعديلاته، وعلى أحكام القرار بقانون رقم (6) لسنة (2017 م) ، بشأن تنظيم نقل وزراعة الأعضاء البشرية، وعلى أحكام القرار بقانون رقم (15) لسنة (2017 م) ، بشأن المعاملات الإلكترونية، وعلى أحكام القرار بقانون رقم (16) لسنة (2017 م) بشأن الجرائم الإلكترونية، وبناءً على تنسيب مجلس الوزراء بتاريخ (17/04/2018 م)، وعلى الصلاحيات المخولة لنا، وتحقيقاً للمصلحة العامة، وباسم الشعب العربي الفلسطيني،

أصدرنا القرار بقانون الآتي:

مادة (1): يكون للكلمات والعبارات الواردة في هذا القرار بقانون المعاني المخصصة لها أدناه، ما لم تدل القرينة على خلاف ذلك:

الوزارة: وزارة الاتصالات وتكنولوجيا المعلومات.

الوزير: وزير الاتصالات وتكنولوجيا المعلومات.

معالجة البيانات: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات، سواء تعلقت بأفراد أو خلافه، بما في ذلك جمع تلك البيانات أو استلامها أو تسجيلها أو تخزينها أو تعديلها أو نقلها أو

استرجاعها أو محوها أو نشرها، أو إعادة نشر بيانات أو حجب الوصول إليها، أو إيقاف عمل الأجهزة أو إلغاؤها أو تعديل محتوياتها.

تكنولوجيا المعلومات: أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أي وسيلة أخرى، سواء أكانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة.

البيانات والمعلومات الإلكترونية: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات، وغيرها.

الشبكة الإلكترونية: ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العا لمية (الإنترنت).

السجل الإلكتروني: مجموعة المعلومات التي تشكل بمجملها وصفاً لحالة تتعلق بشخص أو شيء ما، والتي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية.

المستند الإلكتروني: السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات على وسيط مادي أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجا ع بشكل يمكن فهمه.

الموقع الإلكتروني: مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد.

الشخص: الشخص الطبيعي أو المعنوي.

التطبيق الإلكتروني: برنامج إلكتروني مصمم لأداء مهمة محددة بشكل مباشر للمستخدم أو لبرنامج إلكتروني آخر، يستخدم من خلال وسائل تكنولوجيا المعلومات أو ما في حكمها.

بيانات المرور: أي بيانات أو معلومات إلكترونية تنشأ عن طريق تكنولوجيا المعلومات تبين مصدر الإرسال، والوجهة المرسل إليها، والطريق الذي سلكه، ووقته، وتاريخه، وحجمه، ومدته، ونوع خدمة الاتصال.

كلمة السر: كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات، وما في حكمها، للتأكد من هويته، وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها.

وسيلة التعامل الإلكتروني: البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو ما في حكمها من تكنولوجيا المعلومات أو تطبيق إلكتروني، تحتوي هذه الوسيلة على بيانات أو معلومات إلكترونية تصدرها الجهات المرخصة بذلك.

البيانات الحكومية: البيانات الخاصة بالدولة والهيئات والمؤسسات العامة أو الشركات التابعة لها.

التشفير: تحويل بيانات إلكترونية إلى شكل يستحيل به قراءتها وفهمها دون إعادتها إلى هيئتها الأصلية.

الشفرة: مفتاح أو مفاتيح سرية خاصة، لشخص أو لجهة معينة تستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز والبصمات أو ما في حكمها.

الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها.

الاختراق: الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية.

التوقيع الإلكتروني: بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها، ويميزه عن غيره بغرض الموافقة على مضمون المعاملة.

أداة التوقيع: برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة.

الشهادة: شهادة التصديق الإلكترونية التي تصدرها الوزارة أو الجهة المفوضة من قبلها لإثبات العلاقة والارتباط بين الموقع وبيانات التوقيع الإلكتروني.

مزود الخدمة: أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أي خدمة إلكترونية أو مستخدمي هذه الخدمة.

الإتلاف: تدمير البرامج الإلكترونية، سواء أكان كلياً أم جزئياً، أو جعلها على نحو غير صالحة للاستعمال.

معلومات المشترك: المعلومات الموجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات حول نوع خدمة الاتصالات المستخدمة، والشروط الفنية، وفترة الخدمة، وهوية المشترك، وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة، وأي معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة.

الموظف: كل من يعمل في القطاع العام أو الخاص أو المؤسسات الخاصة أو الهيئات المحلية والأهلية أو الجمعيات أو الشركات الخاصة التي تساهم بها الدولة، وكل من هو في حكمهم.

الحبس: وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين أسبوع إلى ثلاث سنوات.

السجن: وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين ثلاث سنوات إلى خمس عشرة سنة.

الهيئة: هيئة تنظيم قطاع الاتصالات.

الرخصة: الشهادة الصادرة عن الهيئة بأن الشخص قد استوفى الشروط القانونية للسماح له بإنشاء أو تشغيل أو إدارة شبكة اتصالات عامة، أو تقديم خدمات اتصالات عامة، أو استخدام ترددات راديوية أو موجات راديوية، وفقًا للقانون.

المرخص له: الشخص الذي حصل على الرخصة من الهيئة. الاتصالات: نقل أو إرسال أو استقبال أو بث أو تمرير الصوت، والبيانات، والإشارات، والرموز ، والفيديو، والصور بوسائل سلكية أو لاسلكية أو راديوية أو بصرية أو كهرومغناطيسية أو أي وسيلة أخُرى للاتصالات.

خدمة الاتصالات: الخدمة التي تتكون كليًا أو جزئيًا من إرسال المعلومات أو البيانات أو استقبالها أو تمريرها على شبكات الاتصالات باستخدام أي من عمليات الاتصالات. خدمة الاتصالات العامة: خدمة الاتصالات المقدمة للمشتركين والمرخص لهم الآخرين مقابل أجر ، والاتجار واستيراد أجهزة الاتصالات السلكية واللاسلكية وتصنيعها.

أجهزة الاتصالات: الأجهزة التي تستخدم في نقل أو إرسال أو استقبال أو بث أو تمرير الصوت ، والبيانات، والإشارات، والرموز، والفيديو، والصور بوسائل سلكية أو لاسلكية أو راديوية أو بصرية أو كهرومغناطيسية أو أي وسيلة أخرى للاتصالات.

مادة (2):

1- تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء كان الفاعل أصلياً أم شريكاً أم محرضاً أم متدخلاً، على أن تكون الجرائم معاقباً عليها خارج فلسطين، مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ.
2- يجوز ملاحقة كل من يرتكب خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات الآتية:

أ.إذا ارتكبت من مواطن فلسطيني.

ب. إذا ارتكبت ضد أطراف أو مصالح فلسطينية.

ت. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد بالأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية.

مادة (3):

1- تنشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات"، وتتولى النيابة العامة الإشراف القضائي عليها، كل في دائرة اختصاصه.
2- تتولى المحاكم النظامية والنيابة العامة، وفقًا لاختصاصاتهما، النظر في دعاوى الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

مادة (4):

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.

مادة (5): 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.

مادة (6): كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو إتلاف البرامج أو حذفها أو تعديلها، 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.

مادة (7): 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.

مادة (8):

1- كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، 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- كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية أو أداة إنشاء التوقيع الإلكتروني المتعلقة بتوقيع شخص غيره، 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.

3- كل من ارتكب جريمة باستخدام أي من الوسائل المذكورة في الفقرة (2) من هذه المادة، يعاقب بالسجن وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (9):

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.

مادة (10): 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.

مادة (11): تتضمن على:

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.

مادة (12): تتمضن على:

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.

مادة (13): كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال أو اختلاسها، يعاقب بالسجن 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.

مادة (14): 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 وعن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (15): تتضمن على:

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 مائتي دينار 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، ثلاثة 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 قانوناً.

مادة (16): تتضمن على:

1- كل من أرسل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن هم فوق الثامنة عشر سنة ميلادية دون رضاه، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنتين، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2- كل من أرسل أو نشر عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن لم يكمل الثامنة عشر سنة ميلادية أو تتعلق بالاستغلال الجنسي لهم، 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.
3- كل من قام قصداً باستخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشر سنة ميلادية أو من هو من ذوي الإعاقة، 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، أو بكلتا العقوبتين.

مادة (17): 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.

مادة (18): دون الإخلال بالأحكام الواردة في القرار بقانون بشأن مكافحة غسل الأموال وتمويل الإرهاب النافذ، يعاقب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو إحدى وسائل تكنولوجيا المعلومات بقصد:

1- القيام بارتكاب جريمة غسل الأموال 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.

2- القيام بارتكاب جريمة تمويل الإرهاب بالسجن 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.

مادة (19): 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.

مادة (20): كل من انتهك حق من حقوق الملكية الفكرية أو الأدبية أو الصناعية وفقاً للتشريعات النافذة، عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس مدة لا تزيد على 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.

مادة (21): تتضمن على:

1- لكل إنسان حق التعبير عن رأيه بالقول أو الكتابة أو التصوير أو غير ذلك من وسائل التعبير والنشر وفقاً للقانون.
2- حرية الإبداع الفني والأدبي مكفولة، ولا يجوز رفع أو تحريك الدعاوى لوقف أو مصادرة الأعمال الفنية والأدبية والفكرية أو ضد مبدعيها إلا بأمر قضائي، ولا توقع عقوبة سالبة للحرية أو التوقيف الاحتياطي في الجرائم التي ترتكب بسبب علانية المنتج الفني أو الأدبي أو الفكري.
3- حرية الصحافة والطباعة والنشر الورقي والمرئي والمسموع والإلكتروني مكفولة، وللفلسطينيين من أشخاص طبيعية أو اعتبارية عامة أو خاصة، حق ملكية وإصدار الصحف، وإنشاء وسائل الإعلام المرئية والمسموعة ووسائط الإعلام الرقمي وفقاً للقانون.
4- لا يجوز فرض قيود على الصحافة أو مصادرتها أو وقفها أو إنذارها أو إلغاؤها إلا وفقاً للقانون، وبموجب حكم قضائي.

مادة (22):

1- يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته.

2- كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بقصد نشر أخبار أو صور أو تسجيلات صوتية أو مرئية، سواء كانت مباشرة أو مسجلة، تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، 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.

مادة (23): كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد إدارة مشروع مقامرة أو تسهيله أو تشجيعه أو الترويج له أو عرض ألعاب مقامرة، 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.

مادة (24): كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد عرض أي كلمات مكتوبة أو سلوكيات من شأنها أن تؤدي إلى إثارة الكراهية العنصرية أو الدينية أو التمييز العنصري بحق فئة معينة بسبب انتمائها العرقي أو المذهبي أو اللون أو الشكل أو بسبب الإعاقة، يعاقب بالحبس مدة لا تزيد عن سنة، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (25): 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.

مادة (26): كل من حاز بغرض الاستخدام جهازاً أو برنامجاً أو أي بيانات إلكترونية معدة أو كلمة سر أو تراميز دخول أو قدمها أو أنتجها أو وزعها أو استوردها أو صدرها أو روج لها، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، 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.

مادة (27):

1- كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار بقانون، مستغلاً صلاحياته وسلطاته أثناء تأدية عمله، أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلث.
2- كل من ارتكب، من موظفي مزودي الخدمة، أياً من الجرائم المنصوص عليها في هذا القرار بقانون، أثناء تأدية عمله أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلثين.

مادة (28): كل من حرض أو ساعد أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون، بأي وسيلة إلكترونية، ووقعت الجريمة بناءً على هذا التحريض أو المساعدة أو الاتفاق، يعاقب بالعقوبات المقررة لفاعلها الأصلي.

مادة (29): إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات أو أن تقضي بحله في حال كانت الجريمة معاقب عليها بالحبس لمدة لا تقل عن سنة، وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له.

مادة (30): كل من نشر قصداً معلومات عن موقع إلكتروني محجوب بموجب أحكام المادة (39) من هذا القرار بقانون، باستخدام أنظمة أو موقع أو تطبيق إلكتروني، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (31):

1. كل من نشر أو أشاع مضمون أي اتصال أو مكالمة هاتفية بواسطة شبكة اتصالات أو بواسطة تقنيات تكنولوجيا المعلومات، أو رسالة هاتفية اطلع عليها بحكم وظيفته أو قام بتسجيلها دون سند قانوني، أو ساعد أو شارك في ذلك، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة مالية لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني ، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

2. كل من أقدم أو ساعد أو شارك بكتم رسالة أو مكالمة عليه نقلها بواسطة شبكات الاتصالات إلى شخص آخر، أو رفض نقل رسائل أو مكالمات طلب منه نقلها وفقًا للقانون أو الرخصة، أو عبث بالبيانات المتعلقة بأحد المشتركين بما في ذلك أرقام الهواتف غير المعلنة والفواتير، يعاقب بالحبس

مدة لا تقل عن ستة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن سبعة آلاف دينار أردني ولا تزيد على خمسة عشر ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

مادة (32):

1. كل من أقدم أو ساعد أو شارك قصدًا بتخريب منشآت الاتصالات أو تكنولوجيا المعلومات أو ألحق بها ضررًا، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، وبغرامة مالية لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

2. كل من تسبب إهمالًا في تخريب منشآت الاتصالات أو تكنولوجيا المعلومات أو إلحاق الضرر بهما، يعاقب بغرامة مالية لا تقل عن مائة دينار أردني، ولا تزيد على خمسمائة دينار أردني ، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (33):

1. كل من قام أو ساهم أو ساعد أو شارك بتقديم خدمات اتصالات بوسائل من شأنها قيام منافسة غير مشروعة، بين شبكات الاتصالات المرخصة وشبكات اتصالات أجنبية أو غير مرخصة، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة، أو بغرامة مالية لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين ، وفي جميع الأحوال الحكم بمصادرة الأجهزة والأدوات المستخدمة في تقديم الخدمات.

2. كل من استخدم أو ساعد أو شارك باستخدام وسائل غير مشروعة لإجراء اتصالات دون دفع الرسوم يعاقب بالحبس مدة ثلاثة أشهر، وغرامة مالية لا تقل عن خمسمائة دينار أردني ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

3. كل من استخدم شبكة اتصالات خاصة لتزويد خدمات اتصالات عامة أو قام أو ساعد أو شارك بربط شبكة اتصالات خاصة بشبكة اتصالات عامة دون موافقة الهيئة، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة مالية لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، وإزالة المخالفة على نفقة الفاعل.

مادة (34):

1. كل من أنشأ أو شغل أو أدار شبكة اتصالات عامة بهدف تقديم خدمات اتصالات خلافًا لأحكام قرار بقانون بشأن الاتصالات وتكنولوجيات المعلومات النافذ والأنظمة الصادرة بمقتضاه ، أو ساعد أو شارك في ذلك، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة ، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

2. إذا كان مرتكب المخالفة المحددة في الفقرة رقم (1) من هذه المادة، شخصًا اعتباريًا، يعاقب بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانونًا، وفي جميع الأحوال الحكم بمصادرة الأجهزة المستخدمة.

مادة (35):

1. مع مراعاة الأحكام الواردة في قرار بقانون بشأن الاتصالات وتكنولوجيا المعلومات النافذ، كل من شغل محطة راديوية أو استخدم ترددات أو أرقام دون ترخيص، أو ساعد أو شارك في ذلك قصدًا يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

2. إذا كان مرتكب المخالفة المشار إليها في الفقرة (1) من هذه المادة، شخصًا اعتباريًا يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، ومصادرة الأجهزة المستخدمة.

3. كل من قام دون الحصول على موافقة الهيئة، بالتنازل للغير عن الترخيص الصادر له باستخدام تردد أو أرقام أو أي موارد اتصالات نادرة، يعاقب بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، وإلغاء الترخيص وإبطال التصرف.

مادة (36): مع عدم الإخلال بأي عقوبة أشد ينص عليها أي قانون آخر، كل من اعترض أو أعاق أو غير أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو تكنولوجيا المعلومات أو حرض أو ساعد أو شارك غيره على القيام بهذا العمل، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

مادة (37):

1. كل من قام متعمدًا أو ساعد أو شارك بأي إجراء لاعتراض موجات راديوية مخصصة للغير أو بالتشويش عليها أو بقطعها، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، وفي جميع الأحوال الحكم بمصادرة الأجهزة المستخدمة بالتشويش.

2. إذا ارتكب المخالفة المحددة في الفقرة (1) من هذه المادة شخصًا اعتباريًا، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، والحكم بمصادرة الأجهزة المستخدمة.

مادة (38):

1. كل من أدخل إلى أراضي الدولة أجهزة أو أنظمة أو برامج اتصالات أو تكنولوجيا معلومات مخالفة للمواصفات أو المعايير الفنية المعتمدة من الهيئة، أو تحمل بيانات أو معلومات غير صحيحة، بقصد تسويقها أو بيعها أو ساعد أو شارك في ذلك، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على ألفي دينار أردني ،أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، والحكم بمصادرة الأجهزة المضبوطة.

2. كل من قام بحيازة أو ببيع أو تداول أو عرض أجهزة التنصت بأنواعها، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على أربعة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، والحكم بمصادرة الأجهزة المضبوطة.

مادة (39): كل من قام دون ترخيص بممارسة أي حرفة أو مهنة اتصالات أو تكنولوجيا معلومات تستوجب الترخيص وفقًا لأحكام القرار بقانون بشأن الاتصالات وتكنولوجيات المعلومات النافذ والتشريعات الصادرة بمقتضاه، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين.

مادة (40): إذا لم يلتزم المرخص له بتغطية كامل المنطقة الجغرافية المعينة له بالخدمة المرخصة بموجب الرخصة، يعاقب بغرامة لا تقل عن مائة ألف دينار أردني ولا تزيد على خمسمائة ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (41): كل شخص ألغيت رخصته ولم يتوقف فورًا عن استقبال مشتركين جدد، أو عن تزويد خدمات الاتصالات، إلا بالقدر الكافي لتحويل مشتركيه إلى مرخص له آخر وفقًا لما تقرره الهيئة لهذه الغاية ، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني ، أو ما يعادلها بالعملة المتداولة قانونًا، والحكم بمصادرة الأجهزة والشبكة.

مادة (42):

1. كل شخص رفضت الهيئة تجديد رخصته، وقام بإزالة شبكة أو شبكات الاتصالات التي أنشأها أو أي جزء منها دون موافقة خطية من الهيئة، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانونًا.

2. إذا كان الشخص المذكور في الفقرة (1) من هذه المادة، مرخص له لتقديم خدمات الاتصالات الثابتة أو المتنقلة أو البنية التحتية للاتصالات أو تكنولوجيا المعلومات، يعاقب بغرامة لا تقل عن عشرة ملايين دينار أردني ولا تزيد على خمسين مليون دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (43):

1. إذا استخدم المرخص له ترددات أو أرقام أو أي موارد هامة أخرى لم تخصص له من الهيئة ، يعاقب بغرامة لا تقل عن عشرين ألف دينار أردني ولا تزيد على خمسين ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانونًا، وسحبها منه فورًا وإعادتها للهيئة.

2. إذا استخدم المرخص له الترددات أو الأرقام المخصصة له من الهيئة أو أي موارد هامة أخرى في غير الغاية المرخصة أو المخصصة من أجلها، أو إذا لم يلتزم بأي شرط من شروط تخصيصها، يعاقب بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، وسحبها منه فورًا وإعادتها للهيئة.

مادة (44):

1. إذا خالف المرخص له أي حكم من الأحكام الواردة في الفصل الثامن من قرار بقانون بشأن الاتصالات وتكنولوجيا المعلومات النافذ، بشأن الربط البيني والنفاذ والمشاركة في البنية التحتية، يعاقب بغرامة لا تقل عن ثلاثين ألف دينار أردني ولا تزيد على خمسين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

2. إذا كان الشخص المذكور في الفقرة (1) من هذه المادة، مرخص له لتقديم خدمات الاتصالات الثابتة أو المتنقلة أو البنية التحتية للاتصالات أو تكنولوجيا المعلومات، يعاقب بغرامة لا تقل عن مائة ألف دينار أردني ولا تزيد على مائتي ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (45): كل مرخص له لم يلتزم بالإعلان عن أسعار خدمات الاتصالات المقدمة للجمهور بالكيفية التي تقرها أو توافق عليها الهيئة، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (46):

1. إذا خالف المرخص له أي حكم من الأحكام الواردة في الفصل العاشر من قرار بقانون بشأن الاتصالات وتكنولوجيا المعلومات النافذ بشأن العلاقة بين المرخص له والمشترك، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

2. إذا كان المرخص له في الفقرة (1) من هذه المادة، مرخص له لتقديم خدمات الاتصالات الثابتة أو الخلوية المتنقلة أو البنية التحتية للاتصالات أو تكنولوجيا المعلومات، يعاقب بغرامة لا تقل عن ثلاثين ألف دينار أردني ولا تزيد على خمسين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (47): تنص على التالي:

1. كل مرخص له قام بغش أو خداع أو تضليل المشترك بأي طريقة كانت، أو الإثراء على حسابه دون مسوغ قانوني، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

2. إذا كان المرخص له في الفقرة (1) من هذه المادة، مرخص له لتقديم خدمات الاتصالات الثابتة أو الخلوية المتنقلة أو البنية التحتية للاتصالات أو تكنولوجيا المعلومات، يعاقب بغرامة لا تقل عن خمسين ألف دينار أردني ولا تزيد على مائة ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (48): إذا خالف المرخص له أي حكم من أحكام خطة الترقيم الوطنية، يعاقب بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا.

مادة (49): إذا قام المرخص له بفعل أو امتنع عن فعل أدى إلى الإضرار بمواقع أثرية أو سياحية أو أدى إلى الإضرار بالبيئة أو الصحة العامة، يعاقب بغرامة لا تقل عن خمسين ألف دينار أردني ولا تزيد على مائة ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (50): تنص على الآتي:

1. كل من منع أو أعاق بأي شكل من الأشكال عمل موظفي الهيئة المكلفين بالرقابة، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على ستة أشهر، وبغرامة لا تقل عن ألف دينار أردني ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

2. إذا كان المرخص له أو أحد موظفيه هو مرتكب المخالفة المحددة في الفقرة (1) من هذه المادة يعاقب من تسبب بالمنع أو الإعاقة بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، ويعاقب المرخص له بغرامة لا تقل عن خمسين ألف دينار أردني ولا تزيد على مائة ألف دينار أردني ، أو ما يعادلها بالعملة المتداولة قانوناً.

3. إذا امتنع المرخص له أو تأخر عن تزويد الهيئة بأي تقارير أو مستندات أو وثائق أو اتفاقيات أو معلومات أو بيانات تطلبها، يعاقب بغرامة لا تقل عن خمسين ألف دينار أردني ولا تزيد على مائة ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (51): يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي:

1- تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة.

2- حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية، مع مراعاة الإجراءات الواردة في المادة (39) من هذا القرار بقانون.
3- الاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات لغايات ما ورد في الفقرة(1) من هذه المادة.
4- التعاون ومساعدة الجهات المختصة وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ المؤقت بها.

مادة (52):

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 ولجرائم الاتصالات وتكنولوجيا المعلومات.

مادة (53):

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.

مادة (54):

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.

مادة (55): على الجهات المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة أو الأدوات أو وسائل تكنولوجيا المعلومات أو الأنظمة الإلكترونية أو البيانات أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها.

مادة (56):

1- للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له، ومدته.

2- تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط.
3- يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.

مادة (57): 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.

مادة (58): 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.

مادة(59):

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 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.

مادة (60): 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.

مادة (61): 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.

مادة (62):

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.

مادة (63):

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.

مادة (64): مع عدم الإخلال بأي عقوبة أشد، ينص عليها قانون العقوبات الساري أو أي قانون آخر، يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات المنصوص عليها فيه.

مادة (65): كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها أو تدخل فيها أو حرض على ارتكابها، ولم ينص عليها في هذا القرار بقانون، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع.

مادة (66): كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون، في غير الأحوال المصرح بها قانوناً، 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.

مادة (67): كل من أقدم على العبث بأدلة قضائية معلوماتية أو أقدم على إتلافها أو إخفائها أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (68): يعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة أو التدخل في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب بنصف العقوبة.

مادة (69): 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.

مادة (70): 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.

مادة (71): تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أياً من الجرائم المنصوص عليها فيه، سواء ارتكبت في فلسطين أو خارجها، وتعتبر الأحكام الأجنبية سابقة في التكرار بحق الجاني.

مادة (72): 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.

مادة (73): يعفى من العقوبات المنصوص عليها في هذا القرار بقانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأي معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، ويجوز للمحكمة أن تقضي بوقف تنفيذ العقوبة إذا حصل الإبلاغ بعد علم السلطات المختصة، وأدى إلى ضبط باقي الجناة.

مادة (74):

1. يلغى القرار بقانون رقم (16) لسنة 2017 م، بشأن الجرائم الإلكترونية.

2. يلغى كل ما يتعارض مع أحكام هذا القرار بقانون.

مادة (75): يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره.

مادة (76): على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به من تاريخ نشره في الجريدة الرسمية.

محمود عباس

رئيـــــــــس دولـــــــــة فلسطـــــــين

رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطيني

ملحق (9): طعون جزائية (تهمة الذم بواسطة النشر عبر وسائل تكنولوجيا المعلومات)

السنة:2021.

الرقم: 113.

تاريخ الفصل: 30يونيو، 2021.

المحكمة : محكمة النقض.

نوع التقاضي: طعون جزائية

التصنيفات: جزاء – العقوبات – تهمة الذم بواسطة النشر عبر وسائل تكنولوجيا المعلومات

دولـــة فـلســـطين– السلطـــة القضائيـــة– محكمـــة النقض

"الحكـــم"

الصادر عن محكمـة النقض المنعقدة فـي رام الله المأذونـه بإجراء المحاكمـة وإصداره، بإسم الشعب العربـي الفلسطيني، الهيئـــة الحاكمـــة برئاســـة الســـيد القاضـــي خليل الصياد، وعضويـــة السيدين القاضيين: عماد مسوده ، عوني البربراوي.

الطاعن : الحق العام – النيابة العامة

المطعون ضده : ا.ا / رام الله

الإجـــــراءات: تقدمت النيابـة العامـة بهذا الطعن بتاريخ 2021/6/8 ، لنقض الحكم الصـادر عن محكمـة بدايـة رام الله بصفتها الاستئنافية بتـاريخ 2021/5/3 فـي الاستئناف جزاء رقم 2020/268 والقاضي برد الاستئناف وتأييد الحكم المستأنف من حيث النتيجة.

ويستند الطعن للأسباب التالية–:

بأن الحكم المطعون فيه مبني على خطأ في تطبيق القانون وجاء قاصراً في التسبيب والتعليل وجاء خالياً من أسباب الحكم الواقعية سيما ان البينات المقدمة في الدعوى كافية لربط المتهم بما هو منسوب اليه وان تكييف التهمة والوصف القانوني هو من اختصاص المحكمة.

وبالنتيجة التمست الجهة الطاعنة قبول الطعن موضوعاً واجراء المقتضى القانوني.

تبلغ وكيل المطعون ضده لائحة الطعن ولم يتقدم بلائحة جوابية.

المـحـكمة: بعد التـدقيق والمداولـة ولما كان الطعن مقدماً ضمن المدة القانونية فإن المحكمة تقرر قبوله شكلاً.

وفي الموضوع وبما تجاهر به الأوراق فإن النيابة العامة قد احالت المتهم – المطعون ضده – الى محكمة صلح رام الله في القضية الجزائية رقم 2018/4898 لمحاكمته عن تهمة الذم بواسطة النشر عبر وسائل تكنولوجيا المعلومات خلافاً لاحكام المادة 45 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية بدلالة المادتين (188) و (358) من قانون العقوبات رقم 16 لسنة 60. وبعد ان باشرت المحكمة إجراءات الدعوى وبنتيجة المحاكمة أصدرت حكمها القاضي بإعلان براءة المطعون ضده (المتهم) من التهمة المنسوبة اليه لعدم كفاية الأدلة.

لم تقبل الجهة الطاعنة بهذا الحكم فطعنت به استئنافاً لدى محكمة بداية رام الله بصفتها الاستئنافية والتي بنتيجة المحاكمة أصدرت حكمها الوارد في صدر هذا الحكم.

لم تقبل النيابة العامة بهذا الحكم فتقدمت بالطعن الماثل للأسباب الواردة استهلالاً.

وعن أسباب الطعن والتي حاصلها بأن الحكم محل الطعن مبني على خطأ في تطبيق القانون وجاء قاصراً في التسبيب والتعليل وجاء خالياً من أسباب الحكم الواقعية سيما ان البينات جاءت تكفي لربط المتهم بما هو سند اليه وان تكييف التهمة والوصف القانوني هو من اختصاص المحكمة.

وفي ذلك نجد ابتداءً لا بد من الإشارة بأنه يجب على النيابة العامة تضمين لائحة الاتهام اسم المتهم وتاريخ توقيعة ونوع الجريمة المرتكبة ووصفها القانوني وتاريخ ارتكابها وتفاصيل التهمة وظروفها ولمواد القانونية التي تنطبق عليها واسم المجني عليه وأسماء الشهود ولا يجوز للنيابة العامة ان تدعي بافعال خارجاً عن قرار الاتهام والا كان ادعائها باطلاً.

تطبيقاً لنصوص المواد 239 ، 419 من قانون الإجراءات الجزائية وعينية الدعوى الجزائية.

وبالعودة الى لائحة الاتهام وما تضمنته من تفاصيل نجد بأن عبارة الذم بواسطة النشر عبر وسائل التواصل الاجتماعي الموجه للمتهم – المطعون ضده – قد تمثلت بأن ما تم نشره من قبل المتهم بأن المركز الطبي الذي يعود للمشتكي لن يتم ترخيصه مدى الحياة وان كل من يتعامل معه سوف يتعرض للمسؤولية ، وان هذه العبارة قد ورت على صفحة نقابة الطب المخبري الفلسطيني.

وبعد ان استمعت محكمة الموضوع الى كافة البينات خلصت الى نتيجة ببراءة المتهم – المطعون ضده – من التهم المسندة اليه لعدم توافر اركان الجريمة معلله حكمها ومبينه على النحو التالي:

–وفي ذلك نقول انه من المتفق عليه قانوناً وفقهاً ان من قواعد المحاكمة الجزائية امام المحاكم العادية (عينية الدعوى) بحيث يحظر على المحكمة معاقبة المتهم عن واقعة لم ترفع بها الدعوى ولو اثبتتها البينة ذلك ان البينة التي تصلح اساساً للادانة هي تلك التي تنصب على الوقائع المرفوعة بها الدعوى والتي يتضمنها قرار الاتهام ، وبعكس ذلك تكون المحكمة قد فصلت فيما لم يعرض عليها قانوناً ونصبت نفسها مكان النيابة العامة. وعليه فإن محكمتنا ستعالج ما جاء في لائحة الاتهام من

وقائع حيث نجد ان تصريح المتهم ان من يتعامل مع المركز يتعرض للمسألة فان ذلك لا يشكل عناصر التهديد المبحوث عنها في المادة 15 من القرار بقانون رقم 10 لسنة 2018.

وحيث ان ما قضت به محكمة الموضوع وحملت حكمها عليه له اصله الثابت في أوراق الدعوى وجاء نتيجة محاكات واقع الدعوى من ان المشتكي اصلاً يعمل طبيب بتخصص القلب وان المختبر الذي يعود له يمارس مهنة الطب المخبري وقد حصل على الترخيص عن طريق شخص ثاني لديه شهادة الطب المخبري وان نقيب الطب المخبري – المتهم – وجد ان ممارسة المختبر الطبيب المخبري عن طريق المشتكي يشكل مخالفة لقانون مهنة الطبيب وعلى اثر ذلك صرح المتهم – المطعون ضده – بما جاء في لائحة الاتهام – بأن هذا المركز لن يتم ترخيصه وان كل من يتعامل معه سوف يتعرض للمسؤولية فإن هذا الذي جاء به المتهم لا يشكل جريمة الذم بواسطة النشر عبر وسائل تكنولوجيا المعلومات.

وان ما خلصت اليه محكمة الموضوع جاء متفقاً وصحيح القانون وبالتالي فإن أسباب الطعن لا ترد على الحكم المطعون فيه ويكون الطعن مردود موضوعاً.

<u>لهذه الأسباب</u>: تقرر المحكمة رد الطعن موضوعاً.

حكماً صدر تدقيقاً باسم الشعب العربي الفلسطيني بتاريخ 2021/6/30.

ملحق (10): طعون جزائية (قرار توجيه الاتهام)

السنة: 2023

الرقم: 332

تاريخ الفصل: 24 سبتمبر، 2023

المحكمة: محكمة النقض

نوع التقاضي: طعون جزائية.

التصنيفات: جزاء – الإجراءات الجزائية – قرار توجيه الاتهام

دولـــة فـلســـطين– السلطــة القضائيــة– المحكمة العليا / محكمـة النقض

"الحكم"

الصادر عن المحكمة العليا / محكمة النقض المنعقدة في رام الله المأذونة بإجراء المحاكمة وإصداره

بإسم الشعب العربي الفلسطيني، الهيئة الحاكمــة برئاسة القاضـــي الســـــيد خليل الصياد، وعضوية القاضيين السيدين : عماد مسوده، عوني البربراوي

الطـــــاعن :الحق العام

المطعون ضدهم :1- أ.ن/الظاهرية.

2- أ.ن/ الظاهرية.

3- م.ن/الظاهرية.

الإجراءات

بتاريخ 2023/6/26 تقدمت النيابة العامة بهذا الطعن لنقض الحكم الصادر عن محكمة بداية الخليل بصفتها الاستئنافية بتاريخ 2023/5/21 في الاستئناف الجزائي رقم(2022/69) والقاضي برد الاستئناف موضوعاً وتأييد الحكم المستأنف بخصوص المستأنف الأول فارس إبراهيم سالم جبرين، وقبول الإستئناف موضوعاً وإلغاء الحكم المستأنف بخصوص المستأنفين الثانية أزهار جبرين والثالث أمير جبرين والرابع محمد جبرين، والحكم بإعلان برائتهم من التهم المسندة إليهم، وهي استعمال الشبكة العنكبوتية أو إحدى وسائل تكنولوجيا المعلومات وإسناد أمور خادشة للشرف أو الإعتبار المعاقب

عليها بنص المادة(2/15) من القرار بقانون رقم(10) لسنة 2018 بشأن الجرائم الإلكترونية والذم بواسطة النشر عبر وسائل تكنولوجيا المعلومات المعاقب عليها بنص المادة(45) من ذات القانون.

وتتلخص أسباب الطعن بما يلي- :

1- الحكم المطعون فيه جاء مخالف للأصول والقانون وغير معلل تعليلاً قانونياً سليماً ولم تذكر المحكمة مصدرة الحكم المطعون فيه أسباب البراءة بخصوص المطعون ضدهم.

2- أخطأت المحكمة في تفسيرها لمبدأ عينية الدعوى الجزائية حيث أن لائحة الإتهام قد تضمنت موجز للأفعال المسندة للمتهمين -المطعون ضدهم- وأوردت النيابة العامة الأدلة الكافية على ارتكاب الجريمة.

وبالنيتجة التمست النيابة العامة قبول الطعن موضوعاً ونقض الحكم المطعون فيه.

تبلغت وكيلة المطعون ضدهم لائحة الطعن ولم تتقدم بلائحة جوابية.

المحكمة

بعد التدقيق والمداولة ولما كان الطعن مقدماً ضمن المدة القانونية تقرر قبوله شكلاً.

وعن أسباب الطعن.

وبخصوص السبب الأول فإنه قد جاء بصيغة العموم وتعتريه الجهالة التي تحول دون معالجة من قبل المحكمة مما يستدعي ذلك عدم قبول هذا السبب.

وبخصوص السبب الثاني.

فإنه من القواعد المقدرة قانوناً في الدعوى الجزائية(عينية الدعوى) بحيث يحظر على المحكمة معاقبة المتهم عن واقعة لم ترد بها الدعوى ولو أثبتتها البينة، ذلك ان البينة التي تصلح أساساً للإدانة هي تلك التي تنصب على الوقائع المرفوعة بها الدعوى والتي يتضمنها قرار سلطة الإتهام، وبعكس ذلك تكون المحكمة قد فصلت فيما لم يعرض عليها قانوناً ونصبت نفسها مكان النيابة العامة، حيث جاءت المادة (239) من قانون الإجراءات الجزائية مؤكداً لمبدأ عينية الدعوى إذ نصت(ولا يسوغ لوكيل النيابة أن يدعي بأفعال خارجة عن قرار الإتهام وإلا كان ادعاءه باطلاً).

ولما كانت وقائع الدعوى كما جاءت في قرار الاتهام تشير الى أن المتهمين المطعون ضدهم مع المتهم الأول ف.س قد ارسلوا منشورات وتعليقات عبر الفيس بوك تتضمن القول للمشتكية(يا شرموطة يا بنت الشرموطة يا حرمية يا مريضة نفسية)، وأن المتهم الأول قد إتصل بالمشتكية عبر الهاتف وشتم المشتكية من خلال القول لها (يا شرموطة يا بنت الشرموطة يا قحبة يا بنت القحبة والله إلا اربيكي.....).

ولم تتضمن منشورات الفيس بوك(المبرز م/1) الخاص بالمتهم أ.ن ما جاء من وقائع قرار الإتهام(لائحة الاتهام)، وجاء على لسان الشاهدة المشتكية بان المتهم الأول ف.س هو من قام فقط بالإتصال على المشتكية عبر الهاتف وقال لها العبارات سالفة الذكر وأن باقي أقوال المشتكية أمام المحكمة لم تثبت الوقائع الواردة في قرار الإتهام، وبالتالي فإن المحكمة الإستئنافية عندما حكمت ببراءة المطعون ضدهم من التهم المنسوبة إليهم جاء متفقاً ووقائع الدعوى والبينة المقدمة فيها، وبالتالي فإن أسباب الطعن والالة هذه تكون حرية بالرد وتكون النتيجة التي توصلت إليها المحكمة متفقة وصحيح القانون.

لـــذلك: تقرر المحكمة رد الطعن موضوعاً.

حكماً صدر تدقيقاً باسم الشعب العربي الفلسطيني بتاريخ 2023/9/24

قائمة الملاحق:

قائمة الجداول:

قائمة المحتويات: