عمادة الدراسات العليا

جامعة القدس

دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية

الأمن الوقائي أنموذجاً

حنان بسام عبدالله مرداوي

رسالة ماجستير

القدس– فلسطين

1443هـ / 2021م

دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية

الأمن الوقائي أنموذجاً

إعداد:

حنان بسام عبدالله مرداوي

بكالوريوس علوم عسكرية وإدارة عامة من جامعة الإستقلال/ فلسطين

المشرف: د. وفاء الخطيب

قدمت هذه الدراسة إستكمالاً لمتطلبات الحصول على درجة الماجستير في

تخصص علم الجريمة، كليّة الدراسات العليا/ جامعة القدس

1443هـ/2021م

جامعة القدس

عمادة الدراسات العليا

برنامج ماجستير علم الجريمة

إجازة الرسالة

دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية/ الأمن الوقائي أنموذجاً

إسم الطالبة: حنان بسام عبدالله مرداوي

الرقم الجامعي: 21711750

المشرف: د. وفاء الخطيب

نوقشت هذه الرسالة وأجيزت بتاريخ: 2021/12/20 من لجنة المناقشة المدرجة أسمائهم وتواقيعهم:

1. رئيس لجنة المناقشة: د. وفاء الخطيب التوقيع: .....
2. ممتحناً داخلياً: د. عصام الأطرش التوقيع: .....
3. ممتحناً خارجياً: د. محمد الفرارجة التوقيع: .....

القدس– فلسطين

1443هـ/ 2021م

الإهداء

إلى الذي علمني كيف أمسك القلم ... وكيف أخط الكلماتَ بلا ندم ... إلى معلمي وأستاذي وإلى حضن احتواني في كل أزماني ... أنحني أمامك عرفاناً بالجميل ... يا من ستبقى سر الإنسان الأصيل.. يا من أحمل إسمك بكل فخر... يا من أفتقدك كل يوم ... يا من يرتعش قلبي لذكراك يا من أودعتني لله أهديك هذا البحث (والدي الغالي).

إلى التي رعاني قلبُها قبل عينيها وحضنتني بين أحشائها ... إلى رمز الحياة والعطاء والأمل إلى من جرعت الكأس فارغاً لتسقِني قطرة حب إلى من حصدت الأشواك عن دربي لتمّهد لي طريق العلم إليكِ (أمي الغالية).

إلى شاطئي عندما أضيع ... ومنبع الحنان عندما تقسو الأيام، وقلبي الكبير عندما أفقد كل القلوب أخوتي وأخواتي (مهران، ثائر، فادي، عدي، فادية، أنصاف).

إقرار:

أقر أنا معدة الرسالة بأنّها قدمت لجامعة القدس، لنيل درجة الماجستير، وأنّها نتيجة أبحاثي الخاصة، باستثناء ما تمّ الإشارة إليه حيثما ورد، وأنّ هذه الدراسة أو أيّ جزء منها لم يقدم لنيل درجة عليا لأية جامعة أو معهد أخر.

التوقيع:.....

الاسم: حنان بسام عبدالله مرداوي

التاريخ:20/ 12 /2021

الشكر والتقدير

قال تعالى (**لَئِنْ شَكَرْتمّ لَأَزِيدَنَّكُمْ**). (سورة إبراهيم، آية 7)

يقول عليه الصلاة والسلام " **من لا يَشكُر الناس لا يَشكُر الله**"

أتقدمُ بجزيلِ الشكرِ والعرفانِ والتقديرِ إلى الدكتورة الفاضلة وفاء الخطيب؛ لإشرافها على الرسالة، كما أتقدم بالعرفان لجهودها العظيمة التي قدمتها لي خلالَ مرحلةِ إعدادِ الرسالة من خلال الملاحظات والتعديلات والصبر كي تخرجُ الرسالة إلى النور بهذا الشكل، أدامكِ الله ذخراً لطلبة العلم.

كما أتقدمُ بجزيل الشكر والعرفان إلى أعضاء لجنة المناقشة الدكتور محمد الفرارجة والدكتور عصام الأطرش لملاحظاتهم التي ستثري الرسالة وتزيدُ من عمقها.

كما أتقدم بجزيل الشكر والتقدير لجهاز الأمن الوقائي على كل ما قدمه لي من مساعدة خلال مرحلةِ إعداد الرسالة ممثلاً بسيادة اللواء زياد هب الريح مدير عام الجهاز، واللواء عبد القادر التعمري نائب المدير العام، ومدير قسم الضبط الفني في جهاز الأمن الوقائي العقيد محمد أبو رعية ونائبه الرائد محمد جبعاوي وللضباط الذين ساندوني ودعموني في هذا القسم خلال إعداد رسالتي.

وأخيراً اتقدمُ بالشكر والتقدير للدكتور رياض شريم والدكتور سامح الكبج على دعمهم المستمّر لي دائماً، والشكر موصول لكل من قدم ليّ يد المساعدة لإخراج هذا العمل إلى النور.

الباحثة: حنان المرداوي

الملخص:

هدفت الدراسة التعرف إلى دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية/ الأمن الوقائي أنموذجاً)، استخدمت الدراسة المنهج الوصفي بنوعيه الكمي من خلال استخدام أداة الإستبانة التي صممت للحصول على البيانات من العاملين في جهاز الأمن الوقائي، والكيفي من خلال مقابلة تمّت مع العاملين في وحدة الجرائم الإلكترونية في المقر العام لجهاز الأمن الوقائي في مدينة رام الله، تكون مجتمّع الدراسة من جميع العاملين المُختصين في الجرائم الإلكترونيّة بجميع وحداتها في جهاز الأمن الوقائي في الضفة الغربية البالغ عددهم (650) موظف/ة حسب إحصائيات (جهاز الأمن الوقائي، 2020)، تمّ اختيار عيّنة قصدية مكونة من (200) ضابط من مجتمّع الدراسة تمّ توزيع إستبانة الدراسة عليهم، إضافة إلى أنه ثمّ عمل مقابلة مع (5) من الأفراد العاملين في وحدة الجرائم الإلكترنية في المقر العام لجهاز الأمن الوقائي في مدينة رام الله.

توصلت الدراسة إلى مجموعة من النتائج لعل أهُمها: أنّ مستوى الإجراءات المتبعة من قبل جهاز الأمن الوقائي للحد من الجريمة الإلكترونية جاءت بدرجة عاليّة، وبنسبة (79.8%)، ثم أشارت النتائج إلى أنّ دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة جاءت بدرجة عاليّة وبنسبة (77.5%)، كما وأشارت النتائج إلى أنّ أنواع الجرائم الإلكترونية التي يتعامل معها في جهاز الأمن الوقائي: هي الابتزاز والسرقة والانتحال، إذ حصلت على نسبة (80.3%)، كما أشارت النتائج إلى أنّ أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية تتمّثل في تنظيم برامج توعويّة حول مخاطر الجريمة الإلكترونية، وتجنبُ فتح أي رسائل إلكترونية مجهولة المصدر، ورفع مستوى الرقابة الاسريّة على الأبناء، إذ حصلت على نسبة (87%).

كما بينت النتائج عدم وجود فروق ذات دلالة إحصائية في مستوى الإجراءات المتبعة من قبل جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تبعاً لمتغير(الجنس، المؤهل العلمي، العمر، الرتبة العسكرية، سنوات الخدمة، طبيعة العمل في جهاز الأمن الوقائي)، وبناء على هذه النتائج أوصت الدراسة بمجموعة من التوصيات منها: (توعية المواطنين بأهمية التعامل مع شبكات التواصل الاجتمّاعي، التأكيد على تغليظ العقوبة بحق كل من يحاول التشهير أو الابتزاز للآخرين، أو الاعتداء على حقوقهم وسرقتهم بدوافع مختلفة).

الكلمات المفتاحية: المؤسسة الأمنيّة، الجرائم الإلكترونية، الأمن الوقائي.

The role of the security establishment in reducing cybercrime/preventive security as a model

Prepared by: Hanan Bassam Abdallah Al-Mardawi

Supervision: Dr. Wafa Al-Khatib

Abstract:

This study is aimed to identify (the role of the security establishment in reducing cybercrime/ preventive security as a model)، the study used the quantitative descriptive approach through the use of a questionnaire tool that was designed to obtain data from workers in the Preventive Security Service، and qualitative approach through an interview with workers in the cybercrimes unit In the headquarters of the Preventive Security Service in the city of Ramallah، the study community consisted of all 650 employees of the Preventive Security Service، according to (Preventive Security Statistics /2020).

An interview was conducted with (5) members of the cybercrime unit at the headquarters of the Preventive Security Service in Ramallah. The study reached a set of results، the most important of which is that the level of procedures followed in the Preventive Security Service to reduce cybercrime came to a high degree of (79.8%)، then the results indicated that the motives for committing cybercrime by the criminals came to a high degree of (77.8%).

and the results indicated that the types of cybercrime that the Preventive Security Service deals with are blackmail، theft and plagiarism، which got a percentage of (80.3%)، and the results indicated that the most important solutions that help reduce cybercrime are: Organizing awareness raising programs about the dangers of cybercrime، avoiding opening any anonymous messages، and raising the level of family supervision over children، as it got a percentage of (87%).

In addition، the results showed that there are no statistically significant differences in the level of procedures followed in the Preventive Security Service to reduce cybercrime according to the variable (gender، educational qualification، age، military rank، years of service، nature of work in the Preventive Security Service) based on These results، the study recommended a set of recommendations، including (educating citizens about the importance of dealing with social media networks،

emphasizing the severity of the penalty against anyone who tries to defame or blackmail others، or assaulting their rights and stealing them with different motives).

Keywords: security establishment, cybercrime, preventive security.

الفصل الأول

الإطار العام للدراسة

1.1 مقدمة:

في ظل التطور المتسارع في مجال تقنية المعلومات، وازدياد رواد البيئة الإلكترونية، ظهرت الكثير من مواقع التواصل الاجتمّاعي التي شكلت حلقة الوصل بين الكثير من الأفراد في المجتمّعات، هذه المواقع تعد وسيلة ايجابية لنقل المعلومات والتعليم والثقافة، وفي ذات الوقت شكلت نقمة إذ استغلها بشكل خاطيء ضعفاء النفوس والمجرمين (العجمي، 2014).

وفي ظل التطور المستمّر، وانتشار الإنترنت في كافة المناطق، ووصوله لكافة البيوت، وبسبب انخفاض أثمان الأجهزة المحمولة واقتنائها من قبل جميع الأفراد باختلاف أعمارهم وثقافاتهم وانتمّائهم، وبسبب ضعف مستوى الرقابة والأمن لدى الأسر الفلسطينية، الأمر الذي تسبب بظهور أشكال مختلفة من الجرائم منها الجرائم الإلكترونية التي تحدث في الفضاء الرحب الخاص بالشبكة العنكبوتية من خلال التواصل الالكتروني (لطرش، 2016).

إنّ ما سبق يوضح أنّ الجريمة ورغم وجودها في كافة المجتمّعات، إلا أنّها قديماً تختلف عما هي عليه اليوم، إذ يكمن الإختلاف بما يُسمى بالمجال الالكتروني، هذا المجال الذي أصبح عالماً افتراضياً نتج عنه أنواع جديدة من الجرائم انتقلت إلى تلك المجتمّعات، وعملت على تمّكين مجرمي الفضاء الإلكتروني من خلال خلق فرص جديدة للمجرمين لارتكاب جرائم متعددة منها (القرصنة، الاحتيال، التخريب، الإتجار بالمخدرات، المواد الإباحية، الابتزاز، والنصب المالي، السرقات، الإغتصاب، القتل)

وغيرها من الجرائم الأخرى، إذ تكون الشبكة مسرح الاستهداف ثم يتمّ الانتقال إلى الواقع لتنفيذ تلك الجرائم (المطيري، 2016).

وكون الأمن حاجة أساسية في المجتمّعات، ويجب أن تشمل كافة مناحي الحياة؛ إذ إنّ وجوده يغطي كل افتراض لأي اختراق يهدد ويربك حياة الأفراد، فالاهتمّام بتحقيق الأمن لا يقتصر على أفراد المجتمّع وحدهم، بل هو مشاركة بين الأفراد والأجهزة الأمنيّة، تلك المشاركة يمكن لها تحقيق الأمن المطلوب للأفراد والمجتمّع معاً (البيانوني، 2008).

وبرغم الحاجة للأمن وضرورة التنسيق بين الأفراد والأجهزة الأمنيّة إلا أنّ هناك العديد من الجرائم تظهر على السطح بين الفينةِ والأخرى نتيجة التطور والتقدم الذي نشهدة يوماً بعد يوم، من بين تلك الجرائم (الجرائم الإلكترونية) التي تواجه صعوبات في الإثبات لدى القضاء لعدة أسباب أهمها:

- عدم وجود تشريعات قضائية كافية لمعالجة هذه الجرائم.
- صعوبة إثبات الركن المادي من قبل مرتكب الجريمة.
- سهولة ارتكاب الجريمة الإلكترونية كونها تتمّ في الخفاء من خلال الأجهزة الخلوية، بسبب التوسع الهائل بالأنظمة التقنية والحاسوبية وانتشارها بشكل شامل في مختلف المجالات.
- عدم وجود خبرات تراكمية لدى الأجهزة الأمنيّة في معالجة الجرائم الإلكترونية والحد منها.

وعلى الرغم من الصعوبات سابقة الذكر، إلا إنّ الأجهزة الأمنيّة الفلسطينية تعملُ وبإستمّرار على محاربة الجريمة بشكل عام، والجريمة الإلكترونية بشكل خاص، ذلك من خلال وحدات خاصة بتلك الجريمة في كل جهاز أمني تُسمى وحدة الجرائم الإلكترونية، لعل من بين تلك الأجهزة التي يقع عليها جزء من مسؤوليّة مكافحة الجرائم الداخلية، جهاز الأمن الوقائي أحد الأذرع الأمنيّة التابعة لوزارة الداخلية الفلسطينية.

وعليه وبناء على ما سبق تسعى تلك الدراسة إلى توضيح الدور الذي يلعبه جهاز الأمن الوقائي في الضفة الغربية للحد من الجرائم الإلكترونية بمختلف أشكالها، وتوضيح مستوى المتابعة التي يرصدها الجهاز لهذه الجرائم والطرق المستخدمة في محاربتها، إضافة إلى الصعوبات التي تواجهه في رصد تلك الجرائم والتعامل معها، والحلول المقترحة من جانبهم للحد من الجرائم الإلكترونية في فلسطين.

1.2 مشكلة الدراسة:

شهد نمو استخدام الشبكة العنكبوتية في فلسطين انتشار الجريمة الإلكترونية بدرجة أكبر، كما أدى وجود التسوق من خلال الانترنت إلى انتشار جرائم الاحتيال والنصب في المعاملات المالية، كما أشارت إحصائيات (جهاز الشرطة الفلسطينية، 2021) إلى ارتفاع معدل الجريمة الإلكترونية في فلسطين عن الأعوام السابقة، إذ سجلت عام (2015) وقوع (502) قضية، وفي عام (2016) بلغت (1327) قضية، كما ارتفعت عام (2017) إلى (2025) قضية، وعام (2018) ارتفعت أيضاً إلى (2568) قضية، أيّ بزيادة (26.6%) عن العام (2017)، وانخفضت في العام (2019) إلى (2420) قضية، ثم عادت إلى الارتفاع في العام (2020) وسجلت (2720) قضية بارتفاع (11.2%) عن العام (2019)، كما سجلت محافظة الخليل أعلى نسبة في عدد القضايا التي بلغت (477) قضية، تلتها محافظة جنين بلغ عدد القضايا فيها (432) قضية، بينما كانت محافظة أريحا الأقل عدداً في تسجيل هذه القضايا وكانت (61) قضية، كما بينت دائرة الجرائم الإلكترونية في جهاز الأمن الوقائي وجود عدد من البلاغات الخاصة بالجرائم الإلكترونية بلغت (120) بلاغاً في العام (2019) ، وعليه يكون الاستخدام الخاطئ لشبكة الإنترنت ومواقع التواصل الاجتمّاعي والثقة بالجانب الآخر عوامل تساعد على حدوث الجريمة الإلكترونية، إضافة إلى أن اشتراك كافة الفئات في استخدام الانترنت أدى إلى ارتفاع نسب استخدام شبكة الانترنت في فلسطين كما على النحو الآتي (51.7%)

في العام (2017)، ارتفعت في العام (2018) الى (62.1%)، ثم ارتفعت إلى (84%) في العام (2019)، أما في العام (2020) فقد ارتفعت النسبة لتصل لأكثر من (90%) (وفا الاخبارية، 2020)، من هنا ونتيجة الزيادة المستمّرة في عدد الجرائم الإلكترونية، كان لا بد من عمل دراسة علمية تتمّثل في الإجابة عن السؤال الرئيس الآتي: **ما دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية/ الأمن الوقائي أنموذجاً؟**

1.3 أهمية الدراسة:

تكمن أهمية الدراسة من أهمية موضوعها، إذ إنّ انتشار الجريمة الإلكترونية في كافة المجتمّعات بشكل عام، وفلسطين بشكل خاص، وقلة الدراسات التي ناقشت هذا الموضوع من قبل الأجهزة الأمنيّة الأخرى غير الشرطة والنيابة العامة زاد من أهميتها، كما وتكمن أهمية الدراسة من أهمية نظرية وأخرى تطبيقية، وأما الأهمية النظريّة تتمّثل في:

- إضافة دراسة جديدة حول الجرائم الإلكترونية ودور الأمن في الحد منها.

في حين تتمّثل الأهمية التطبيقية في النتائج التي سيستفيد منها الجهات المختلفة ذوي العلاقة والمتضررين من الجرائم الإلكترونية، لعل من أهم تلك الجهات ما يلي:

- **المواطنون:** تتمّثل إستفادتهم من نتائج الدراسة في رفع مستوى الوعي الخاص بالجرائم الإلكترونية لديهم بهدف حماية أبناؤهم من التعرض لمثل تلك الجرائم.
- **المرشدين الاجتمّاعيين والنفسيين العاملين في المؤسسات الخاصة وحماية الأسرة:** من خلال نتائج الدراسة سوف يتعرفون على أهم الصعوبات التي تواجه مواجهة الجرائم الإلكترونية في الضفة الغربية والحلول المقترحة لتجاوز تلك الصعوبات، إلى جانب التعرف

إلى أكثر أنواع الجرائم الإلكترونية انتشاراً في الضفة الغربية بهدف التركيز عليها ونشر الوعي حولها.

- إضافة إلى وضع مقترحات وتوصيات يمكن لجهات الاختصاص الاستفادة منها في كيفية التعامل مع المجرمين ذوي الخبرة في المجال الإلكتروني.

1.4 أهداف الدراسة:

تكمن أهداف الدراسة في هدف رئيس يتمّثل في التعرف إلى "**دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية/ الأمن الوقائي أنموذجاً**"، ينبثق عن الهدف الرئيس أهداف أخرى فرعية تتمّثل في التعرف إلى:

- الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية.
- دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة.
- أنواع الجرائم الإلكترونية التي يتمّ التعامل معها في جهاز الأمن الوقائي.
- الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية.
- أهم الحلول التي تساعد في الحد من الجريمة الإلكترونية.

1.6 أسئلة الدراسة وفرضياتها:

تكمن أسئلة الدراسة في سؤال رئيس يتمّثل في الإجابة عن السؤال الآتي: **(ما دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية/ الأمن الوقائي أنموذجاً؟**"، ينبثق عن السؤال الرئيس أسئلة أخرى فرعية تتمّثل في الإجابة عن:

- ما الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية؟
- ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة؟
- ما أنواع الجرائم الإلكترونية التي يتمّ التعامل معها في جهاز الأمن الوقائي؟

- ما الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية؟
- ما أهم الحلول التي تساعد من الحد من الجريمة الإلكترونية؟

وأمّا فيما يخص فرضيات الدراسة:

سعت الدراسة التأكد من صحة الفرضيات الآتية:

- لا توجد فروق ذات دلاله إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات المبحوثين حول مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تُعزى لمتغير الجنس.
- لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات المبحوثين حول مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تُعزى لمتغير المؤهل العلمي.
- لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات المبحوثين حول مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تُعزى لمتغير العمر.
- لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات المبحوثين حول مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تُعزى لمتغير الرتبة العسكرية.
- لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لإجابات المبحوثين حول مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تُعزى لمتغير عدد سنوات الخدمة.

- لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في المتوسطات الحسابية لإجابات المبحوثين حول مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تُعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي.

1.7 حدود الدراسة:

تكمن حدود الدراسة في:

- **الحدود المكانية:** تمّثلت في جميع وحدات الجرائم الإلكترونية في جهاز الأمن الوقائي في الضفة الغربية.
- **الحدود الزمانية:** تمّت الدراسة في الفترة الواقعة بين الفصل الدراسي الأول من العام الاكاديمي 2019–2020، وحتى نهاية الفصل الدراسي الأول من العام الأكاديمي 2021–2022.
- **الحدود البشرية:** تكونت من جميع العاملين المُختصين في الجرائم الإلكترونيّة بجميع وحداتها في جهاز الأمن الوقائي في الضفة الغربية البالغ عددهم (650) موظف/ة حسب إحصائيات (جهاز الأمن الوقائي، 2020)
- **الحدود الموضوعية:** تتمّثل في موضوع الدراسة الذي يتمّحور حول "دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية/ الأمن الوقائي أنموذجاً".

الإطار النظري والدراسات السابقة وذات العلاقة

2.1 مقدمة:

الأمن من أهم الحاجات التي يجب توفرها لتحقيق مستوى عالي من الطمأنينة النفسية لدى الأفراد، إذ يؤدي إلى الاستقرار الأسري والمجتمّعي ويرفع من مستوى التنمية في المجالات المختلفة، ويعزز الإنتاج من أجل تحقيقه، ولأهميته السابقة تعمل المؤسسات الأمنيّة على توفير كل ما يحتاجه المواطن للشعور بالامن، إضافة إلى قيامها بتوعيتهم وتنبيههم بالظواهر السلبية التي تؤدي إلى خلق حالة من عدم الأمان في المجتمّع، التي من أهمها ظاهرة الجريمة التي تستدعي استخدام التوعية الأمنيّة لمواجهتها في ضوء قدرة ومرونة الأجهزة الأمنيّة على إيصال الحقائق لجميع أفراد المجتمّع وتحصينهم من أخطار الجريمة والانحراف، ذلك من خلال الإعلام الأمني الذي يلعب دوراً مهماً في عملية التوعية المجتمّعية بمخاطر الجريمة (العايد، 2010)، التي من بينها الجرائم الإلكترونية المستحدثة التي غزت العالم بمختلف أشكالها وأنواعها سواء ذات العلاقة بـ(التواصل الاجتمّاعي، الاقتصاد، الثقافة العامة، القرصنة) وغيرها من القضايا المختلفة، إذ سيتمّ الحديث في هذا الفصل عن كل ما يتعلق بالجريمة الإلكترونية من حيث المفهوم والنظريات، ودور جهاز الامن الوقائي في الضفة الغربية في الحد من هذه الجرائم.

2.2 مفهوم الأمن:

يعد الأمن من المفاهيم المهمة في حياة الإنسان، فهو ذُكر في الكتب السماوية رديفاً لمفردة الخوف، والدليل على ذلك قوله تعالى "فَلْيَعْبُدُوا رَبَّ هَذَا الْبَيْتِ، الَّذِي أَطْعَمَهُمْ مِنْ جُوعٍ وَآمَنَهُمْ مِنْ خَوْفٍ" (سورة قريش، آية 3–4)

الأمن في اللغة نقيض الخوف. "أمنت فأنا آمن، وأمنت غيري أي ضد أخفته، فالأمن ضد الخوف، والأمانة ضد الخيانة، والإيمان ضد الكفر" (ابن منظور، 1993: 140).

أمّا في الاصطلاح فهو "الشعور بالطمأنينة من قبل الفرد والجماعة، وتوفر الحوافز الكافية لتحقيق ونشر الثقة والمحبة في المجتمّع، والتخلّص من الفساد، والقضاء على كل ما يهدّد استقرار الدولة ومعيشتها" (امحمدي، 2006: 14).

مما سبق يتضح أنّ الامن مفهوم يشير إلى تحقيق حالة من عدم الشعور بالخوف، باعتباره قيمة وحاجة إنسانية ضرورية حسب سلم الحاجات لماسلو، ولا يقتصر على فئة اجتمّاعية معينة دون أخرى، فالفقير كالغني يحتاج إلى الشعور بالأمان ويسعى إلى تحقيقه، وإن اختلفت درجات المتمّتع به، ونظراً لصعوبة تحقيق الأمان الكامل، أصبح يُنظر للأمن على أنّه مسألة نسبية مرهونة بالسعي لتعزيز أفضل الشروط لتوافره (العايد، 2010).

وعليه يتبين أنّ مفهوم الأمن من المفاهيم المختلفة التي يتضمن الكثير من المتغيرات، كما يتضمن العديد من الأبعاد التي تشكل عناصر قوة الدول والمجتمّعات، هذه الأبعاد تتغير بتغير الزمان، فقد كان الأمن في السابق يعنى أمن الدول من خلال الحفاظ على كيان الدولة الكلي من العبث الداخلي والخارجي الذي كان يعتمّد على الأفراد، أمّا الأمن اليوم في عالم متغير فرض نفسه بصورة مختلفة عما كان عليه سابقاً من خلال الأخطار العابرة للحدود(الأمن العابر للحدود) من خلال شبكة

الانترنت، حيث أصبح دور الأمن يتمّثل في تشكيل الحضارات وتطورها وضبط النسيج الاجتمّاعي وحماية وحدة المجتمّع.

2.3 مفهوم الأجهزة الأمنيّة ونشأتها:

يمكن تعريف الأجهزة الأمنيّة حسب (حسن، 2014: 315) بأنّها "الاجهزة التي تعمل على تطبيق القانون واستقرار النظام في المجتمّع وحماية أفراده وتحقيق العدالة، ملتزمة بالحياد دون استثناء طائفي أو عرقي أو فئوي أو طبقي"، إنّ تحقق الأمن هو الغاية الأساسية لوجود هذه الأجهزة، إذ يعد دورها جزء من المنظومة الكليّة المتمّثلة بالقانون والقضاء وتطبيق الجزاءات والعقوبات التي تحد من الجريمة اعتمّاداً على مبدأ أنّ العقاب يحقق منفعة (فردية، اجتمّاعية، علاجية، وقائية)، يشير هذا المفهوم إلى المؤسسات والأجهزة الرسمية العسكرية والأمنيّة التي تمّ انشاؤها استناداً للقانون، حيث يعمل كل جهاز وفقاً لاختصاصه وصلاحياته من أجل توفير الأمن للسكان وإحقاق العدالة والدفاع عن البلاد، وينظم الأطار القانوني السياسات العامة لهذه الاجهزة والمهام التي تقوم بها، كما يحكم سلطاتها وهيكليتها التنظيمية (الخطاطبة، 2013).

استناداً إلى ما سبق يمكن القول أنّ السلطة الوطنية الفلسطينية عملت وفقاً للاتفاقيات الموقعه من الجانب الإسرائيلي على تشكيل أجهزة أمنية متعددة، بهدف خدمة أبناء الشعب الفلسطيني، حيث اعتمّد قادة هذه الأجهزة في تطوير عملهم على الخبرة الذاتية، كون أغلب قادة الأجهزة كان لهم معرفة بالعمل الأمني خلال تواجدهم مع الثورة الفلسطينية في الخارج، إضافة الى الخبرات الآخرى من خلال ارسال الأفراد للتدريب سواء لدى الدول العربية أو الأجنبية، بقيت هذه الأجهزة لا تستند إلى هيكل تنظيمي واضح لفترة طويلة من الزمن، إذ كان يغلب عليها الارتجال أو الإعتمّاد على القائد بدرجة كبيرة، ولم تبنى على أهداف أو عقيدة أمنية موحدة حيث عملت أغلب الاجهزة بشكل منفصل، واستمّر هذا الحال

في المؤسسات الأمنيّة الفلسطينية حتى الانتفاضة الثانية عام (2000) التي على أثرها دمر الاحتلال مقار الأجهزة الأمنيّة، فيما بعد بدأ التنظيم الفعلي بعد عام (2003) لإعادة بناء المؤسسة الأمنيّة وهيكليتها (حمد الله، 2018).

مما سبق يمكن القول إنّ العمل الأمني في فلسطين بدأ من خلال أجهزة أمنية منفصلة عن بعضها البعض، ومع عملية إصلاح أجهزة الأمن في العام (2003) تمّ العمل على دمج بعض الأجهزة لتقليل عددها، فتمّ جمع الأجهزة ذات العمل المتشابه معاً، إذ تمّ إلحاق قوات الـ(17) بالأمن الوطني، وقوات البحرية بالمخابرات، والقوات الخاصة بالأمن الوطني، أمّا الشرطة والدفاع المدني والأمن الوقائي فتتبع وزارة الداخلية والأمن الوطني، لاحقاً لما سبق عمد الرئيس أبو مازن على سن قانون الخدمة في قوى الأمن الفلسطينية الذي حدد فترة عمل قادة الأجهزة الأمنيّة بأربعة أعوام، كما حدد الأوامر والواجبات الملقاة على عاتق الأجهزة الأمنيّة في عملية مأسسة المؤسسة الأمنيّة قانونياً وإعطائها الصِبغة الشرعية لعملها ضمن القانون المنظم لأمورها، كما أصدر الرئيس أبو مازن مرسوماً رئاسياً تحديداً في العام (2005) يخص عملية إصلاح الأجهزة الأمنيّة الذي يقضي بدمج جميع الأجهزة الأمنيّة الفلسطينية في ثلاثة أجهزة فقط، تمّثلت في قوات الأمن الداخلي وهي (الشرطة، الأمن الوقائي، الدفاع المدني) وقوات الأمن الوطني وجهاز المخابرات العامة (الخطاطبة، 2013).

وعليه يمكن القول إنّ المرحلة الأولى من وجود السلطة الوطنية الفلسطينية ركزت على التأسيس بشكل أساسي، فالسلطة الوطنية الفلسطينية انبثقت من منظمة التحرير الفلسطينية، بذلك تمّ تطبيق النظام الثوري المعمول به في منظمة التحرير الفلسطينية على أجهزة الأمن الفلسطيني في حينه، حيث لم تكن هيكلية العمل الأساسية لكل جهاز واضحة، إضافة إلى قلة الخبرة في المجال الإداري، هذا الأمر الذي أدى إلى تداخل العمل وأسهم في إضعاف مستوى الخدمات المقدمة، كون الهدف الأساسي الذي

سعت إليه القيادة الفلسطينية في حينه هو الحصول على سيادة على الأرضي الفلسطينية، وكان للنكسة التي تعرضت لها الأجهزة الأمنيّة الفلسطينية خلال انتفاضة الأقصى من قيام قوات الاحتلال الإسرائيلي بهدم المقرات الرئيسية للأجهزة الأمنيّة دور في إعادة النظر لضرورة إصلاح الأجهزة الأمنيّة والعمل على تنظيمها بتجديد هياكلها بما يتناسب مع طبيعة عملها وتوافقها مع الأنظمة والقوانين الخاصة بالعمل الأمني الفلسطيني.

2.4 مهام المؤسسة الأمنيّة وطبيعة عملها:

إنّ طبيعة النظام السائد في الدولة هو الذي يحدد طبيعة مهام الأجهزة الأمنيّة، فالدول الديمقراطية قامت بخصخصة بعض القطاعات الأمنيّة، هذا يعني أنّه في بعض النظم الديمقراطية تقوم الشركات الخاصة ببعض المهام الأمنيّة التي كانت حكراً على الدولة، أمّا في النظم الشمولية التي تعتمّد على نظام الحزب الحاكم، فإنّ أجهزة الأمن لا زالت تقوم بكافة الأدوار في الدولة، بالرغم من ذلك يوجد قواسم مشتركة للعمل الأمني في مختلف النظم، أهمها المحافظة على النظام العام وحماية الدولة من التخريب وتحقيق الأمن والأمان للمواطن، وملاحقة الجريمة رغم الاختلاف في الإجراءات بين النظم (الشروف، 2010).

وأمّا فيما يخص طبيعة عمل الأجهزة الأمنيّة فهي طبيعة وقائية وعلاجية:

- الطبيعة الوقائية: تتمّثل في التصدي لأي عمل يخل بأمن الدولة والإجراءات الدفاعية، ويتمّثل عملها من خلال التحري عن الجريمة، ومراقبة فاعليها والتوعية الأمنيّة والتدريب واقتناء الوسائل التقنية والحديثة للمساعدة في منع الجريمة.
- الطبيعة العلاجية: وتتمّثل في التعامل مع الجريمة من حيث البحث عن المتهمين وإلقاء القبض عليهم والتفتيش عن أماكنهم وجمع الأدلة وإحالتها لجهة التحقيق في القضايا وفقاً

للقوانين (مصلح والبرغوثي، 2015)، والمقصود بالقوانين هنا تلك التي تستخدم لردع المجرمين كقانون العقوبات العام، إذ لم يكن حينها أي قوانين خاصة بالجريمة الإلكترونية، ثم تطور التشريع الخاص بالجريمة الإلكترونية في فلسطين بدءاً بالقانون رقم (16) لسنه (2017)، الذي تمّ تعديله بقانون رقم (10) لسنه (2018)، ثم تعديله بقانون آخر رقم (28) لسنه (2020) لمزيد من التوضيح حول القوانين أنظر/ي كل من ملحق رقم (6،7،8)، حيث تمّ تعديل المادة رقم (15) من القانون رقم رقم (10) لسنة 2018، التي كان نصها "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".

إذ أصبحت في التعديل الجديد رقم (28) لسنة (2020م) ما يأتي:

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 الفعليّة،

وبغرامة لا تقل عن ألف دينار أردني ولا تزيد على ثلاثة آلآف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً".

2. "إذا كان التهديد بإرتكاب 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".

2.5 تأثير الإحتلال على عمل الأجهزة الأمنيّة الفلسطينية:

يعد الاحتلال القيد الأساس على عمل المؤسسة الأمنيّة الفلسطينية، ذلك بسبب قطع التواصل الجغرافي بين المناطق الفلسطينية، ووجود مناطق (C) حسب اتفاقية أوسلو التي لا يستطيع الأمن الفلسطيني الدخول إليها، بذلك تكون مهمة المؤسسة الأمنيّة الفلسطينية محصورة في العمل ضمن المناطق المصنفة (أ) بدرجة أساسية ثم المناطق المصنفة (ب) بدرجة ثانية في حالة وجود تنسيق أمني مع الاحتلال، لذلك تضعف قدرة المؤسسة الأمنيّة على حفظ الأمن بشكل عام لكافة المواطنين الفلسطينين، هنا يكون مستوى الجريمة في المناطق التي لا يتواجد فيها الأمن الفلسطيني أعلى من المناطق التي يتواجد فيها الأمن الفلسطيني (صلاحات، 2008).

إذ كان لما تقوم به قوات الاحتلال الإسرائيلي منذ عام (2000م) من خلال تطبيق سياسة أمنية وعسكرية بإهدار حق المواطن الفلسطيني في التمّتع بالأمن والسلامة الشخصية، وإضعاف قدرة المؤسسة الأمنيّة الفلسطينية على القيام بدورها في حفظ النظام والأمن وتحقيق سيادة القانون، مما أثر سلباً على أداء المؤسسة الأمنيّة الفلسطينية عامة، إضافة لذلك قام الاحتلال أيضاً باختراق مناطق

السيطرة الفلسطينية الكاملة (أ) من أجل القيام باعتقال الأفراد الفلسطينين، ذلك بهدف تكريس ادعاء ضعف السلطة وأجهزتها الأمنيّة وعدم قدرتها على ضبط الأمن وفرض النظام واحترام القانون (الهيئة الفلسطينية المستقلة لحقوق المواطن، 2005).

إضافة لما سبق تسيطر دولة الاحتلال على فضاء الاتصالات والإنترنت في فلسطين بشكل كبير، فلا يزال هناك تداخل في أرقام الهاتف الدولي لها مع أرقام الهاتف الدولي لفلسطين، إنّ مقدمة هاتف فلسطين الدولي هي (00970) بينما مقدمة الهاتف الدولي للاحتلال (00972) إلا أنّ قيام أي شخص من الخارج بطلب أي رقم فلسطيني يجد أنّ المقدمة تتجاوب بشكل أفضل وأسرع عند استخدامه مقدمة دولة الاحتلال إسرائيلي، هذا إن دل على شيء فإنّه يدل على خضوع جميع الاتصالات الفلسطينية للرقابة الإسرائيلية، إضافة لتشكيل دولة الاحتلال الإسرائيلي الوحدة رقم (8200) كذراع لتجسسها الالكتروني، بالتالي يعد الاحتلال المرتكب الأول للجرائم الإلكترونية في فلسطين، كونه يقوم بعمليات غير شرعية ضد المواطن الفلسطيني من خلال التجسس على الخصوصية ومراقبة مواقع التواصل الاجتمّاعي، إضافة إلى المراقبة العامة للهواتف وشبكة الانترنت (الشلالدة وربعي، 2015)

مما سبق يمكن القول إنّ الاحتلال الاسرائيلي شريك في الجرائم الإلكترونية التي تحدث في فلسطين، فعلى سبيل المثال إنّ عملية إعاقة الأجهزة الأمنيّة الفلسطينية من القيام بعملها في المناطق (C) التي يسيطر عليها الاحتلال الإسرائيلي، يعزز إرتفاع مستوى الجرائم في تلك المناطق بسبب ضعف مستوى الرقابة على الانترنت فيها من قبل الأجهزة الأمنيّة الفلسطينية من جهة، ومن جهة أخرى الاحتلال الذي لا يهتمّ إلا بأمن المواطن الإسرائيلي فلا يعمل على منع الجريمة الإلكترونية إلا في المناطق الإسرائيليّة، أما المناطق (C) التي يصعب فيها عمليّة الضبط والإحضار والتي تعتبر ملاذ للفارين من

وجه العدالة لا يهتمّ بها، نتيجة لذلك يتجه بعض المجرمين إلى تلك المناطق من أجل الافلات من قبضة الامن الفلسطيني وتعطيل سير العدالة وظهور الخوف لدى المواطنين كونها خارج السيطرة الفلسطينية.

2.6 نشأت جهاز الأمن الوقائي الفلسطيني وأهدافه:

أدى التوقيع على اتفاقية أوسلو إلى نشأة السلطة الوطنية الفلسطينية التي كانت بحاجة إلى أجهزة أمنية من أجل ضبط الحياة العامة في فلسطين، تمّ بناء جهاز الأمن الوقائي كجهاز يمكنه الحفاظ على الأمن الداخلي للسكان الفلسطينيين منذ تولي السلطة الوطنية الفلسطينية للحكم في الأراضي الفلسطينية في العام (1994)، بقي هذا الجهاز يمارس أعماله بشكل مستقل دون أن يكون هناك قانون ينظم عمل الجهاز حتى العام (2002)، وبموجب مرسوم رئاسي ألحق جهاز الأمن الوقائي بوزارة الداخلية، وفي العام (2005) صدر قانون الخدمة في قوة الامن الفلسطيني بهذا أصبح هناك وضوح في عمل الجهاز بدرجة أكبر (ملحم والبرغوثي، 2015: 22)

وفي العام (2007) أصدر الرئيس محمود عباس قراراً بقانون بشأن الأمن الوقائي حمل رقم (11) لسنه (2007)، الذي ضم (16) مادة تعمل على تنظيم هذا الجهاز وتبين طبيعة عمله والمهام الموكله إليه، لمزيد من التوضيح انظر/ ي ملحق رقم (9)، إذ أشارت المادة (2) من مواد القرار إلى أنّ جهاز الأمن الوقائي يعد:

- إدارة عامة أمنية نظامية ضمن قوى الأمن الداخلي التي تتبع الوزارة المختصة وتعمل في مجال الأمن.

- يكون المقر الدائم للإدارة العامة في مدينة القدس ولها مقران مؤقتان في مدينتي رام الله وغزة ويجوز لهما فتح إدارات فرعية في المدن الأخرى (قرار بقانون الامن الوقائي، 2007).

كما نصت المادة (7) من ذات القرار "يكون لضباط وضباط صف الإدارة العامة للأمن الوقائي في سبيل تسهيل مباشرة اختصاصاتهم المقررة بموجب أحكام هذا القانون صفة الضبطية القضائية"

وفيما يتعلق بأهداف جهاز الأمن الوقائي كما تمّ الإشارة لها في (مدرسة الشهيد ماجد أبو شرار لإعداد الكادر، 2004) تتمّثل في:

- الحفاظ على أسرار الدولة من خلال تأمين سلامتها من الداخل ودفع أي ضرر خارجي قد يؤثر على أمنها بما يكفل للشعب حياة مستقرة توفر له استغلال طاقاته للنهوض والتقدم والاستقرار.
- حماية النظام السياسي للدولة ممثلاً بالسلطة الوطنية من خلال حماية المشروع السياسي.
- منع ما شأنه إفساد العلاقة ما بين الشعب والسلطة السياسية.

أمّا صلاحيات الجهاز فقد بينت المادة (7) من (قرار بقانون الامن الوقائي، 2007) أنّها تتمّثل في:

- العمل على حماية الأمن الداخلي الفلسطيني.
- متابعة الجرائم التي تهدد الأمن الداخلي.
- الكشف عن الجرائم التي تستهدف الإدارات الحكومية والهيئات والمؤسسات العامة والعاملين فيها.

2.7 دور الأمن الوقائي في مواجهة الجرائم الإلكترونية:

في العقد الأخير ومع تنامي وسائل التواصل الاجتمّاعي ظهرت العديد من الجرائم المستحدثة خصوصاً المرتبطة بالجرائم الإلكترونية مثل (الابتزاز الالكتروني، السرقة، غسيل الاموال، التنمر الالكتروني) في المجتمّع الفلسطيني، من هنا أصبح هناك حاجة ملحة إلى إنشاء وحدة متخصصة للتحقيق في الجرائم الإلكترونية تتكون من محققين وطاقم من ذوي الاختصاص والكفاءة في مجال تقنية المعلومات، لهذا أُنشئت في الأجهزة الأمنيّة خصوصاً جهاز الأمن الوقائي مؤخراً وحدة للتحقيق في الجرائم الإلكترونية وجمع أدلتها، قوامها عدد محدود من الكوادر والأجهزة والبرامج، الهدف من وجود هذه الوحدة المساهمة بشكل فعال في رفد الجهات القضائية بالقضايا ذات الاختصاص الالكتروني، ويكمن دور الأمن الوقائي في وحدة وقسم الجرائم الإلكترونية في ثلاث قضايا خاصة بمواجهة الجرائم الإلكترونية هي:

- **التوعيّة المجتمّعيّة:** أنّ دور الأجهزة الأمنيّة في دعم برامج التوعية الأمنيّة يتحقق من خلال سلطات ممنوحة لرجال الأجهزة الأمنيّة وفقاً لما تتطلبه مقتضيات الوظيفة ومقتضيات المواقف، إذ يستلزم ذلك ضرورة توعية رجال الأجهزة الأمنيّة بصورة دائمة بحدود استخدام السلطات الممنوحة لهم في نطاق عملهم، وتوعية المواطنين إعلامياً بأنّ الأمن العام يمثل خدمة للمواطنين وليس سلطة عليهم، وأنّ السلطات الممنوحة لرجال الأجهزة الأمنيّة إنّما تستهدف بالدرجة الأولى حماية أمن المواطن وتحقيق سلامة المجتمّع الذي يعكسه مفهوم الأمن (الشهري، 2010).

مما سبق يمكن القول إنّ التوعية الأمنيّة في مجال تكنولوجيا المعلومات أصبح ضرورة من ضروريات التوعية الأمنيّة قي ظل الاستخدام الكبير للثورة الرقمية، إنّ التوعية بكل مستجد في مجال تقنية المعلومات يعد من المهام الأساسية لرجال الأمن في مجال الجرائم الإلكترونية

والتوعية بها من أجل سد الثغرات الأمنيّة في مجال الاستخدام الأمثل للانترنت، حيث تعتبر التوعية الأمنيّة في مجال جرائم الانترنت عملاً مهماً في المحافظة على الأمن الشخصي والاجتمّاعي والمجتمّعي.

- **ملاحقة مرتكبي الجرائم الإلكترونية:** إنّ واقع الجرائم الإلكترونية وملاحقتها في فلسطين يعتبر حالة مختلفة عن واقع هذه الجرائم في مختلف الدول بسبب وقوع دولة فلسطين تحت الاحتلال الإسرائيلي الذي يسيطر على سماء وفضاء فلسطين الإلكتروني سيطرة تامة، مما يضفى لوناً خاصاً عند ملاحقة هذه الجرائم، وقد أوكلت مهمة ملاحقة جرائم الانترنت إلى النيابة العامة التي تُحيل الموضوع إلى الجهة صاحبة الاختصاص وهي الأجهزة الأمنيّة التي تحصل على إذن قضائي من أجل متابعة الحالة الجرمية، فالنيابة العامة هي صاحبة الاختصاص الأصيل في ذلك، بينما تقوم الأجهزة الأمنيّة بمهام جمع الاستدلالات وبعض المهام التحقيقية "المقيدة" الأخرى، وتقوم النيابة العامة بتوجيه طلبات الأجهزة الأمنيّة من خلال كتاب النائب العام لجهات الاختصاص إلى موزعي الانترنت في الأراضي الفلسطينية لتزويدها بما يسمى ب(IP address) لأسماء الأشخاص المتهمين أو المستخدمة أرقامهم ليتسنى لها إحالة الأمر لجمع الاستدلالات والتحري من قبل الأجهزة الأمنيّة حول أصحاب تلك الأسماء لاستكمال التحقيقات المطلوبة، كما وتمّتلك الأجهزة الأمنيّة الوسائل التكنولوجية الحديثة التي تمّكنها من فحص أجهزة الكمبيوترات والهواتف والأجهزة الأخرى وفك الرموز
- **مساعدة الجهات التشريعية على تحسين القوانين الخاصة بالجريمة الإلكترونية:** لقد شاركت الأجهزة الأمنيّة في تصوراتها لدى ديوان الفتوى والتشريع حول القانون الفلسطيني رقم (16) لعام (2017) بعد رفض مؤسسات المجتمّع المدني والقانونيين ما ورد فيه، وكان لمشاركة

الاجهزة الأمنيّة في تلك التصورات أسهم في الخروج ببعض التعديلات المهمة، جاءت هذه المشاركة انطلاقاً من روح الخبرة التراكمية لدى هذه الأجهزة في هذا المجال، مما أدى إلى تحسين القانون ليتوافق مع ما تريده المؤسسات، فهي تريد ضمان حقوق وحريات المواطنين كحرية التعبير وخصوصية حياتهم، لمزيد من المعلومات الخاصة بالقانون رقم (16) لسنه (2017) أنظر/ي ملحق رقم (6) (الشلالدة والربعي، 2015).

2.8 الجهود والإتفاقيات الدوليّة والإقليميّة والعربيّة المبذولة لمكافحة الجريمة الإلكترونية:

شاركت فلسطين في التوقيع على الاتفاقية العربية والدولية لمكافحة الجريمة الإلكترونية، ذلك من أجل ضمان الأمن الداخلي من الجرائم المختلفة تحديداً ذات الخطر الخارجي، إضافة الى قيام السلطة الوطنية الفلسطينية بالتوقيع على مجموعة من الاتفاقيات الدولية والإقليمية والثنائية لمواجهة الجرائم العابرة للحدود التي من ضمنها الجرائم الإلكترونية واستخدام الفضاء الالكتروني العالمي كمسرح لهذه الجرائم، لعل من هذه الاتفاقيات ما يلي:

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة (2010): تكونت من (43) مادة تحدثت عن كل ما يخص الجريمة الإلكترونية والعقوبات على مرتكبيها، 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 الانترنت وتبادل المعلومات وتسليم المجرمين المُتهمين في القضايا الجرمية المتعلقة بالانترنت.

- 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 يتمّاشى مع ما جاء في هذه الاتفاقيات التي أضحت فلسطين طرفاً فيها، كذلك الالتزام بالإجراءات الفنية التي قد تحويها مثل هذه الاتفاقيات (عبد الباقي، 2018).

2.9 دور مؤسسات المجتمّع المدني في دعم المؤسسة الأمنيّة الفلسطينيّة لمكافحة الجريمة الإلكترونية:

تُعرف منظمات المجتمّع المدني بأنّها "المنظمات التي لا تخضع لسلطة الدولة أو الحكومة، تتكون من الهيئات التي تسمى المؤسسات الثانوية مثل الجمعيات الأهلية، النقابات المهنية والعمالية، شركات الأعمال، الغرف التجارية والصناعية، المؤسسات الخيرية، الجمعيات المدنية، الهيئات التطوعية وجمعيات حقوق الإنسان، جمعيات حقوق المرأة والنوادي الرياضية، جمعيات حماية المستهلك، وما شابهها من المؤسسات التطوعية"، المقصود هنا أنّ نطاق المجتمّع المدني ينحصر في المؤسسات والمنظمات غير الحكومية التي يقوم نشاطها على العمل التطوعي، فهو مجتمّع مستقل إلى حد كبير عن إشراف الدولة المباشر، كثيرة هي المصطلحات التي تتردد في الأدبيات التي تتعلق بواقع منظمات المجتمّع المدني مثل(المنظمات الأهلية، المنظمات غير الحكومية، مؤسسات العمل الخيري، المؤسسات غير الربحية، المؤسسات التطوعية، مؤسسات العمل التطوعي)، لذلك فإن المنظمات غير الحكومية ليست محل اتفاق حتى في الدول المتقدمة، ففي فرنسا يسمونها الاقتصاد الاجتمّاعي، وفي بريطانيا يطلق عليها الجمعيات الخيرية العامة، في حين يسميها الألمان الجمعيات والاتحادات، وفي اليابان مؤسسات المصلحة العامة (ملاوي، 2008: 280).

وعليه فإنّ الاتجاهات الحديثة للشرطة تتبنى مفهوم الشرطة المجتمّعية التي تهدف إلى عقد اللقاءات التشاورية بصفة مستمّرة بين رجال الشرطة وأفراد المجتمّع بكل أطيافه أفراد وجماعات ومؤسسات محلية لأنّ ذلك يشكل عنصراً من عناصر تدعيم العلاقات الايجابية بين المؤسسة الأمنيّة والمجتمّع، حيث يشكل ذلك جسراً للتعاون بين المؤسسة الأمنيّة ومؤسسات المجتمّع في تحقيق السلم الأهلي والمجتمّعي (الحميدان، 2003).

في ضوء هذا المفهوم العصري للمؤسسة الأمنيّة عموماً تلعب مؤسسات المجتمّع المدني دوراً محورياً في التوعية الأمنيّة، وجسراً بين المؤسسة الأمنيّة والمجتمّع المحلي في عملية توجيه وتنوير المجتمّع عن السلوك الإجرامي والإنحرافي ذلك بفضل طبيعتها البنيوية وأهدافها السامية وسهولة الحركة والمبادرة لديها، فعلى المؤسسة الأمنيّة أن تعي أهمية هذا الدور بتوثيق العلاقة معها، وتفعيل العمل بغية إيصال الرسالة المناسبة إلى جمهور المواطنين، التي تتوجه إليه هذه الجمعيات وفقا للمجالات التي تُعنى بها، حيث تعتبر المؤسسات المحلية في المجتمّع العمود الفقري لعملية التوعية الأمنيّة انطلاقاً من توطيد العلاقة بين المؤسسة الأمنيّة والجمهور، إذ إنّ التوعية هي الجانب الثقافي التي تعمل علية هذه المؤسسات لزيادة ثقافة الجمهور الأمنيّة.

ولسد الفجوة الحاصلة تمّ اسناد بعض المهمات التي تساهم في الحد من انتشار الجرائم بشكل عام والإلكترونية بشكل خاص لدوائر العلاقات العامة والتعبئة والتوجيه في الأجهزة الأمنيّة لتعزيز العلاقة التكاملية بين الأمن والمجتمّع من خلال الزيارات المتكررة لمؤسسات المجتمّع المدني لايجاد أرضية مشتركة بينها وبين هذه المؤسسات في مجال التوعية الأمنيّة بمخاطر الجريمة الإلكترونية، حيث عقدت دائرة التعبئة والتوجيه في جهاز الأمن الوقائي بالتعاون مع مؤسسات المجتمّع المدني في المدن

والقرى الفلسطينية الكثير من الندوات حول الموضوع من أجل ترسيخ مفهوم الأمن الالكتروني لدى المجتمّع وكيفية مواجهة عمليات السرقة الإلكترونية (الشهري، 2010).

نستنتج مما سبق أنّ التعاون والتواصل بين المؤسسة الأمنيّة ومؤسسات المجتمّع المختلفة يساعد في الحد من الجرائم الإلكترونية، فوجود هذه العلاقة التكاملية يساعد في سرعة الإبلاغ عن الجرائم الإلكترونية للجهات المختصة، بالتالي الحد من وقوعها أو سرعة معالجتها، وهذا يشجع أفراد المجتمّع للإبلاغ عن الجرائم التي تحصل معهم دون خوف، الأمر الذي يساعد على تحقيق متطلبات السلم الأهلي والأمن المجتمّعي، كما أنّها تلعب دوراً مهماً في التوعية الأمنيّة من خلال علاقتها مع المؤسسة الأمنيّة لتكون رديفاً للمؤسسة الأمنيّة في تحقيق الوعي الأمني المطلوب.

2.10 الجريمة الإلكترونية:

1.2.10 مقدمة:

يؤثر التطور الذي نشهده اليوم بشكل عام على الحياة البشرية في كافة المجالات، إذ كان للتطور التكنولوجي أثر كبير في مجالات عدة، منها ما يتعلق بالتواصل الإجتمّاعي عبر المواقع الخاصة التي تشكل العالم الحقيقي الذي يعبر من خلاله كافة أفراد المجتمّع عن الآراء والمعتقدات وتدور بسببه نقاشات مختلفة، كما أنّها أصبحت سوقاً أدى إلى تشابك العلاقات بين أفراد المجتمّع في كافة أنحاء العالم، هذا ساعد المجرمين ومن لديهم ميول عدوانية لاستغلال ذلك للقيام بالجرائم بمستوى رقابي أقل من المستوى الرقابي بوجود الأجهزة الأمنيّة، الأمر الذي ساعد في التلاعب بالأمن والسلم الأهلي في المجتمّع من قبل هؤلاء الأشخاص من خلال بث الأكاذيب وترويج الشائعات والاغتصاب والقتل والتهديد وسرقة الملفات الخاصة من أجل الابتزاز وتشويه السمعة، كل ذلك من خلال استخدام شبكة

الانترنت، أضف إلى ذلك الهجمات السبرانية من قبل مجموعات أو دول اتجاه مجموعات ودول أخرى تؤدي أحيانا إلى شلل المؤسسات الحكومية (العجمي، 2014).

1.2.10 مفهوم الجريمة:

الجريمة في اللغة "هي قطع الشيء ويقال الجريم الثمر اليابس والجرامة ما سقط من ثمر النخل والجريمة النواة للثمر" (ابن منظور، 1990: 91).

أمّا الجريمة من ناحية إصطلاحيّة وإجتمّاعية وقانونية، فقد اهتمّ علماء القانون والاجتمّاع بالجريمة كونها ذات أبعاد مختلفة، فيُنظَر لها من الناحية الاجتمّاعية باعتبارها "كل فعل مخالف للأخلاق، منافٍ للآداب، لا يتوافق مع العادات والتقاليد السائدة في المجتمّع، ويخالف المنظومة الاجتمّاعية المتعارف عليها، وهو بذلك يشمل كل ما له علاقة بالإضرار بمصالح الأفراد أو الخروج عن القيم والعادات المتعارف عليها" (قطامي، 2008: 72).

ويحددها (الكبيسي، 2010: 940) بقوله "الحكم الذي تصدره الجماعة على بعض أنواع السلوك بصرف النظر عن النص القانون"، قد لا يكون كل ما يخالف المنظومة الاجتمّاعية جريمة بشكل عام، فهناك تغيرات على العادات والتقاليد في المجتمّعات العربية مع التطور الحضاري والتكنولوجي، ولم يتمّ احتسابها جرائم، لكن هذا التغير يمكن أن يؤدي الى حدوث جريمة فيما بعد.

وفي القانون عُرفت الجريمة "بأنّها فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيرا احترازيا" (نجيب، 1977: 45).

إضافة لما سبق تُعرف الجريمة بأنّها "الواقعة التي ترتكب إضراراً بمصلحة حماها المشرع في قانون العقوبات ورتب عليها أثراً جنائياً متمّثلاً في العقوبة" (سلامة، 1979: 84)، وهي أيضًاً "إتيان فعل محرم معاقب على فعله أو تركه" (يوسف، 2004: 81).

مما سبق نستنتج أنّ هناك علاقة تكاملية بين التعريف القانوني الذي يركز على النية والإرادة لدى المجرم في ارتكاب الجرم، والتعريف الاجتمّاعي الذي يركز على أي خرق في العادات والتقاليد والقيم في المجتمّعات.

والجريمة بكونها ظاهرة لها شروط أساسية، فهي مقيدة حسب المجتمّع، فكل مجتمّع له عادات وثقافات وقيم مختلفة عن المجتمّع الآخر، فالجريمة تقع إذا ما بلغ الفرد حداً معيناً من تجاوز العادات والتقاليد والأعراف المتبعة في المجتمّع (السمري ولطفي وعبد الفتاح، 2010).

تعليقاً على ما سبق المجتمّعات الغربية لا تعتبر بعض الجرائم التي يمكن اعتبارها في المجتمّعات العربية جريمة، كجريمة القتل على خلفية الشرف؛ كون الدين والثقافة العامة لديهم لا ترى فيما يحدث بين الرجل والمرأة بلا زواج ما يخالف الدين والأخلاق، وعليه يمكن اعتبار الجريمة بشكل عام هي كل فعل أو سلوك مقصود يخالف عادات المجتمّع وتقاليده، ويسعى الفرد من خلاله للإعتداء على حُرمات الآخرين من أفراد المجتمّع المقيم فيه أو المجتمّعات الأخرى، ويؤدي هذا الفعل لحدوث إيذاء لهم.

2.2.10 مفهوم الجريمة الإلكترونية:

حظي مفهوم الجريمة الإلكترونية بالعديد من الاجتهادات لاختلاف الأطر النظريّة التي تفسر هذا المفهوم، هناك من عرفها من زاوية فنية، وأخرى قانونية، وهناك من نظر إليها من خلال الوسيلة المستخدمة في الجريمة وهو الحاسب الآلي، إذ يرى (الجهيني والجهيني، 2006: 14) أنّ الجريمة الإلكترونية "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب".

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

كما يمكن تعريفها حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها بأنّها "أي فعل غير مشروع يعتمّد على مستوى معرفة المجرم بتكنولوجيا المعلومات" (العريان، 2009: 170).

وقد بين القرار بقانون رقم (10) لسنه (2018) فيما يخص الجريمة الإلكترونية، في مجمل مواده بأنّ الجريمة الإلكترونية كل فعل مخالف يمكن أنْ يؤدي إلى الإضرار سواء للأفراد أو الشركات أو المجموعات أو أي كان، 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 للتواقيع أو البيانات الشخصية أو العقود الإلكترونية، أو الانتحال للشخصية أو الاحتيال، أو السرقة أو الاستدراج بهدف المساومة، أو الاعتداء، أو الاغتصاب أو القتل، وكل ما يفضي إلى إيذاء الأفراد في المجتمّع مخالفاً للقانون والاعراف والتقاليد، ويحاسب عليه الفرد في الجرائم العادية إذا ما ارتكبه إلكترونياً، فهو بهذا ارتكب جرماً له كافة الأركان المادية والمعنوية والنية المسبقة.

مما سبق نستنتج أنّ الجريمة الإلكترونية لوقوعها يجب توفر الأداة الإلكترونية المستخدمة، وهي كثيرة في القرن الواحد والعشرين منها على سبيل المثال (الحاسوب، اللاب توب، التابلت، الموبايل بكافة أنواعه) وغيرها من الأجهزة الذكية التي يمكن استخدامها في سبيل الوصول الى الضحية وكشف ستره من الناحية المعنوية أو من الناحية المادية، كالتعرض لسمعته والتشهير به أو الاعتداء المادي بالابتزاز والتعرض له، أو ما يخص التزوير في كل ما له علاقة بالاعمال التجارية المختلفة التي تسبب الخسارة للمال والوقت، وفي حال توافقها كعناصر للجريمة تقع الجريمة الإلكترونية ويعاقب عليها القانون، لقد عمل المشرع الفلسطيني على توضيح ذلك بالتفصيل في القانون بقرار رقم (10) فيما يخص الجريمة الإلكترونية للعام(2018) لمزيد من التوضيح انظر/ي ملحق رقم (8).

3.2.10 التطور التاريخي لجرائم الكمبيوتر والانترنت:

إنّ التطور التاريخي لجرائم الإنترنت مر بثلاث مرحل، تتمّثل كما بينها (العريان، 2009) بالآتي:

- **المرحلة الأولى:** بدأت منذ شيوع استخدام الحواسيب في 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 شئ عابر أم ظاهرة إجرامية مستحدثة، وإنّ الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة.
- **المرحلة الثانية:** بدأت هذه المرحلة في الثمانينات من القرن العشرين، بظهور مفهوم جديد لجرائم الكمبيوتر والانترنت ارتبطت بعمليات اقتحام نظام الكمبييوتر عن بعد، وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج سواء الشخصية أو الحكومية، وشاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورًا 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 والإقتصادية والاجتمّاعية والسياسية والعسكرية.
- **المرحلة الثالثة:** ظهرت هذه المرحلة مع تطور الإنترنت في نهاية القرن العشرين وبداية القرن الواحد والعشرين، إذ ظهر إزدياد ملحوظ في مجال الجرائم الإلكترونية وتغييراً في نطاقها ومفهومها، كان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات كما ظهرت أنماط جديدة من إنكار الخدمة التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، وكان ذلك ضد مواقع الانترنت التسويقية

المهمة مما أدى إلى انقطاعها عن الخدمة لساعات عديدة مخلفاً وراءه خسائر مالية بالملايين، هنا وفي تلك المرحلة نشطت جرائم نشر الفيروسات عبر المواقع الإلكترونية حيث سهولة انتقالها إلى ملايين المستخدمين عبر البريد الالكتروني، كذلك انتشرت الرسائل المنطوية على إثارة الأحقاد أو المساس بالكرامة، أو تلك المروجة للمواد غير القانونية وغير المشروعة.

4.2.10 خصائص الجرائم الإلكترونية وأركانها:

تتمّيز الجرائم الإلكترونية إلى جانب أنّها صعبة الاكتشاف والإثبات بعدة خصائص ومميزات، لعل من أهمها ما يلي:

- إنّ هذه الجريمة تتمّ بواسطة الحاسب الآلي، فلا يوجد دمار ولا دماء أو دلائل على الجريمة كونها ترتكز على تغيير أو تعديل أو مسح البيانات كلياً أو جزئياً بالدخول إلى السجلات المخزنة في ذاكرة الحاسب الآلي، الأمر الذي يجعل إمكانية اكتشافها تكتنفه الصعوبة، هذا ما يجعل القيام بها أمراً مغرياً لدى الأشخاص مستخدمي الانترنت.
- جريمة عابرة للحدود بمعنى قد تقع الجريمة في بلد والجاني في بلد آخر، حيث أن الشبكة العنكبوتية (الانترنت) تنتشر في جميع دول العالم مما جعل العالم عبارة عن قرية كونية متواصلة مع بعضها البعض مما يُسهل القيام بالجريمة الإلكترونية من بلد آخر(المومني، 2010).
- خبرة الجاني الإلكترونية: الجريمة العادية لا تحتاج إلى أنّ يكون الجاني متعلماً، بينما الجريمة الإلكترونية تحتاج إلى شخص متمّرس ومتعلم وذو دراية وعلم بأنظمة الحاسوب، إلى جانب معرفته أنّ الدافع لإرتكاب هذه الجريمة الحصول على المنفعة الشخصية والربح المادي.

- تقع أثناء المعالجة الآلية للبيانات: حيث يمثل هذا الشرط أحد أركان الجريمة الإلكترونية الخاصة بالتعدي على البيانات الخاصة، وأنّ انتفاء هذا الشرط هو انتفاء لحصول الجريمة الإلكترونية (العجمي، 2014).
- جريمة تعاونية: إذ يشترك في تنفيذها مجموعة من الأشخاص أو الجماعات المنظمة كالهجمات السبرانية على بلد ما، يشتمّل التعاون على تقديم التقنيات اللازمة للجريمة وتسهيل تحويل المكاسب إلى منطقة أخرى (حسنية، 2017).
- عدم الإبلاغ عن هذه الجرائم خوفاً من التشهير إذا كانت بشكل مباشر، أو لعدم معرفة الجاني أنّ هناك من يتجسس عليه، حيث توجد فجوة كبيرة في مجال التبليغ عن الجرائم الإلكترونية.
- سهولة إتلاف الأدلة من قبل الجناة.
- سهولة ارتكاب الجريمة بعيداً عن الرقابة الأمنيّة.
- صعوبة تحديد حجم الضرر الناتج عن هذه الجرائم (البداينة، 2014).

وأمّا فيما يخص أركان الجريمة الإلكترونية، تتكون من ثلاث أركان رئيسية هي:

- **الركن الشرعي:** يُقصد به الصفة غير المشروعة للسلوك، أساسه انطباق السلوك على نص أو قاعدة قانونية (عقابية) تجرمه، نصت عليها القوانين الفلسطينية المطبقة بالأراضي الفلسطينية المتعلقة بالجرائم الإلكترونية مثل القانون (10) لسنة (2018).
- **الركن المادي:** يقصد به السلوك الجرمي الذي سلكه الجاني في الجرائم الإلكترونية الذي يتنافى مع القانون، كذلك وجود نتيجة جرمية لهذا الفعل كالابتزاز وغيرة، ثم وجود علاقة سببيه بين السلوك الجرمي والنتيجة التي أحدثها الفعل وهي الحصول على المال مثلاً، نستنتج مما سبق أنّ الركن المادي هو العلاقة بين الفعل الجرمي وماديات هذا الفعل وشخصية الجاني.

- **الركن المعنوي:** يهتمّ الركن المعنوي بالحالة النفسية للجاني، أي توفر عنصر القصد عند القيام بالجريمة الإلكترونية باعتباره المحور الهام في تحديد طبيعة السلوك الذهني للجاني عند الإقدام على الجريمة الإلكترونية، في هذا الركن تتوفر المسؤولية الجنائية عن الفعل الجرمي من حيث توفر الإرادة للفعل والعلم بالفعل والإقدام عليه والاثم المترتب عليه، حيث إنّه يترتب على الركن المعنوي طبيعة العقاب الذي يستحقه الجاني (الجبور، 2010).

5.2.10 أطراف الجريمة الإلكترونية:

تتكون أطراف الجريمة الإلكترونية من ثلاث أطراف أساسية هي:

- **الجاني:** هو الشخص الذي قام بارتكاب السلوك الجرمي الالكتروني، وهو على دراية وخبرة وعلم بشؤون الحاسوب، والجناة في الجريمة الإلكترونية يصنفون إلى ثلاث فئات هي حسب (العجمي، 2014) هم:
  - **المخترقون** (الهاكرز): هم أشخاص لديهم البراعة الفائقة في استخدام الانترنت ولديهم تطفل لاستخدام حسابات الآخرين عبر طرق غير مشروعة بهدف إثبات أنفسهم في هذا المجال وقدراتهم على الاختراق.
  - **المحترفون:** هم أخطر جناة الانترنت، إذ أن هذه الفئة تقوم بهذه الأفعال من أجل الاعتداء وتحقيق الكسب غير المشروع من خلال اختراق الحسابات البنكية، وآخرين لتحقيق أغراض سياسية بهدف التجسس أو التخريب، غالباً يكون هؤلاء الأشخاص أصحاب الهجمات السبرانية على دول أو منظمات أو مراكز حكومية.
  - **المتعصبون:** هؤلاء تدفعهم العصبية الطائفية سواء كانت اثنياً أو دينياً للإضرار بمصالح الفئات الأخرى وليس لديهم النية (الركن المعنوي) للجريمة، لكن تدفعهم

مصالحهم الطائفية للقيام بسلوكيات للإضرار بالطوائف الأخرى، وهم لا يسعون لتحقيق مكاسب مادية أو سياسية.

- **المجني عليه:** إن الفعل الجرمي الذي يقوم به الجاني يقع على نوعين من الأشخاص ذات صفات مختلفة هي:
  - **أشخاص لهم صفة معنوية:** كالبنوك والمؤسسات التجارية والوزارات، المؤسسات والهيئات المالية، المؤسسات الحكومية والشخصيات الاعتبارية التي تعتمّد اعمالهم على الحاسوب.
  - **أشخاص لهم صفة طبيعية:** وهم الأشخاص الذين يعتمّدون على الحاسوب في أعمالهم أو يستخدمون الحاسوب بشكل عام للترفية أو التعليم وغيرها من الأمور (ياسين، 2016).
- **محل الجريمة:** هي الأنواع التي تستهدفها الجريمة الإلكترونية إذ يتنوع هذا الاستهداف إلى مجموعة من العناصر المستهدفة تتمّثل في:
  - **المعلومات:** هنا يقوم الجاني بسرقة المعلومات الموجودة على الحاسوب المستهدف أو تغييرها أو حذفها والعبث بمحتويات البريد الإلكتروني وانتهاك الخصوصية والملكية الفكرية.
  - **الأجهزة:** هنا يقوم الجاني بتخريب البرامج الموجودة على الحاسوب المستهدف من خلال إرسال برامج ضارة أو فيروسات أو شل البرامج الموجودة على الحاسوب، أو إرسال فيروسات تقوم على أن يصبح جهاز المجني عليه ضمن تبعية الجاني، بالتالي

يتعرف من خلال ذلك على جميع العمليات التي تتمّ عليه، هنا يجب النظر إلى خطورة هذا الإجراء خصوصاً في اختراق البنوك والمؤسسات الحكومية والعسكرية.

- **الأشخاص والجهات:** هنا يقوم الجاني بهذا العمل من أجل (الابتزاز المالي، التهديد، السرقة، ممارسة الرذيلة، رسائل التهديد الارهابي) (ربايعة، 2016).

يمكن تلخيص ما سبق أنّ أطراف الجريمة ثلاث فئات رئيسية، هي الجاني والمجني عليه ومحل الجريمة كما في أي جريمة عادية، لكن الجاني هنا يجب أن يكون ذو خبرة ودراية بالحاسوب كنقطة انطلاق من أجل ارتكاب جريمته، فيرتكب الجريمة من خلال استخدام الاجهزة الإلكترونية الحديثة، سواء كان الهدف من الجريمة التخريب أو التعطيل على الجهات المختلفة حكومية أو خاصة، أو ابتزاز لها أو للافراد العاديين.

وعليه فالجاني يتعامل ضمن برامج محددة يتمّ من خلالها الاستدراج أو التخريب، وهي تعد أداة الجريمة مع الحاسوب، وكون الأفراد العاديين ليس لديهم أي معرفة بما يقوم به الجناة، فيكون استخدام الانترنت بالنسبة لهم آمن كما في الواقع العادي، فيرون في الشارع أو البيت أو مكان العمل مكاناً آمناً ولا يتوقعون فيه أي نوع من الجرائم، وعلى الرغم أنّ هناك اختلاف في محل الجريمة بين المعلومات أو المال أو التخريب لكن الهدف واحد يتمّثل في القيام بجريمة مخطط لها بشكل كامل ضمن عناصرها الكاملة.

6.2.10 أنواع الجريمة الإلكترونية وصورها:

تأخذ الجريمة الإلكترونية أنواعاً متعددة منها كما بينها (صغير، 2013) الآتي:

- **الجرائم ضد الأفراد أو الأشخاص:** كجرائم الانترنت الشخصية مثل سرقة الهوية الرقمية ومنها البريد الإلكتروني أو سرقة الاشتراك في موقع شبكة الإنترنت وسرقة حساب على الفيسبوك أو مواقع التواصل الاجتمّاعي .
- **الجرائم ضد الملكية:** وهي الجرائم التي تهدد المصالح العامة والخاصة للأفراد حيث يتمّ نقل برمجيات ضارة إلى البرامج التطبيقية والخدمية أو غيرها، ذلك بهدف إحداث أضرار في الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى ممتلكات شخصية مثل الهجمات الفيروسية.
- **جرائم ضد المحتوى:** والتي تضم طائفة الجرائم المتعلقة بالأفعال الإباحية واللا أخلاقية ودعارة الأطفال.
- **الجرائم ضد الحكومات:** يهدف هذا النوع من الجرائم إلى مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية التي تستخدم التطبيقات الحاسوبية على الشبكة العالمية (الانترنت) سواء المحلية أو الدوليّة، وذلك من خلال الهجمات الإرهابية التي يشنها الهاكرز المحترفين على شبكة الانترنت، وتركز على تدمير الخدمات والبنى التحتيّة للأهداف التي يتمّ مهاجمتها، كذلك مهاجمة شبكات الكمبيوتر للتأثير السلبي على الخدمات العامة والخاصة، وغالباً ما يكون هدفها سياسي بحت، وهي التي يتمّ الحديث عنها تحت مسمى الهجمات السايبرية.

أمّا فيما يخص صور الجريمة الإلكترونية، فلها العديد من الصور لعل أهمها:

- سرقة المعلومات والاعتداء على خصوصيتها وإساءة استخدامها وتحريف السجلات الرسمية، وسرقة المعلومات وبيعها كالبحوث أو الدراسات ذات العلاقة بالتطوير التقني أو الصناعي أو العسكري (البداينه، 2014).
- التنصت والتجسس وسرقة الاختراعات خاصة في المجالات العلمية بهدف بيعها، والدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات وقرصنة البرمجيات، ويشمل ذلك النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى (يس، 2016).
- استغلال الأطفال للإتجار بهم ونشر صور خاصة للأطفال من الجنسين "الجنس السياحي"، وإفشاء معلومات وأسرار الأفراد والشركات الخاصة(صور، فيديوهات، معلومات شخصية) وغيرها ونشرها على شبكة الانترنت، إضافة إلى الاحتيال المالي من خلال سرقة البطاقات، هذا كله ناتج عن الاستخدام غير الشرعي للبطاقات الماليّة وبطاقات التسوق والهاتف المحمول (عوض، 2018).
- الابتزاز الجنسي للإناث والذكور من أجل الحصول على المال أو المتعة، أضف إلى ذلك استخدام بطاقات الائتمّان للشراء دون علم صاحبها، إلى جانب ذلك المراسلات الجنسية.
- تزوير المعلومات والدخول لقواعد النظام التعليمي وتغيير المعلومات كتغيير علامات الطلاب، ووضع سجلات شهادات لم تصدر عن النظام التعليمي، وانتهاك الخصوصية بنشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها (البداينه، 2014).

7.2.10 دوافع ارتكاب الجريمة الإلكترونية:

لكل جريمة مرتكبة سواء كانت تقليديّة أو حديثة دوافع متعددة تجعل الفرد يقدم على ارتكابها، لكن دوافع الجرائم التقليدية تختلف عن دوافع جرائم الانترنت الحديثة على النحو الآتي:

- **الدوافع الشخصيّة:** تعد الدوافع الشخصية من أهم الدوافع التي تؤدي إلى ارتكاب الجريمة الإلكترونية، ومن أهم هذه الدوافع حب الظهور والرغبة في إثبات الذات من خلال اختراق أنظمة المعلومات في الحاسوب، والتمّتع بذكاء جيد من خلال إثبات عجز هذه التقنية المعلوماتية، إنّ توفر البيئة السبرانية تعطي فرصة للقيام بالجرائم بسبب سهولة الولوج إلى الحسابات لعدم وجود رقابة تخص الممنوع اجتمّاعيا، وعملية الكشف الفاعل عنها ضئيلة بشكل عام، هذا يشكل فرصة للقيام بالجريمة الإلكترونية في ظل وجود المحفزات السابقة لها والرغبة في الانتقام والإضرار بمصالح الآخرين، ويكون الدافع وراء ارتكاب جرائم الانترنت عادة الرغبة الجامحة في إلحاق الضرر بالأشخاص ومصالحهم، بسبب خلافات مادية أو اجتمّاعية، إضافة الى نقمة الشخص على المجتمّع (البداينة، 2014).

أمّا على المستوى النفسي، فالظروف التكوينية لعمليّة النمو والبيئة المحيطة التي تشكل الأساس القيمي والأخلاقي المكون لشخصية المجرم، تشكل دافعاً في دفع المجرم نحو الجريمة، إذ إن ظروف الفقر والبطالة والأميّة والظروف الضاغطة من قبل المجتمّع يدفع المجرم للإنتقام من خلال الحاق الضرر بالاخرين، معترضاً على الظروف التي يعيشها والتي يعتقد أنها دخيلة عليه (بحري وخرموش، 2021).

- **الدوافع الفكريّة:** الاختلاف الفكري كغيرة يسهم في إنشاء عداوات بين الأفراد سواء كانوا ضمن جماعات معينة متشددة، أو أنظمة سياسية وأحزاب، ومع التطور التكنولوجي تمّ استخدام شبكة الانترنت لنشر الأفكار الخاصة بالجماعات المختلفة، إذ يسعى كل طرف إلى تهديد الأفراد

بالتشهير أو القتل إذ لم يتخلوا عن أفكارهم المعادية للفطرة الدينية حسب الجماعات الدينية (نجم الدين، 2018)

- **الدوافع الاقتصاديّة والاجتمّاعية:** إنّ غياب نظام العدالة الاجتمّاعية في المجتمّع، وانتشار الفقر والبطالة ساعد في شيوع الجريمة في المجتمّع، فهو من يدفع الأفراد الذين لديهم معرفة بالتكنولوجيا وأنظمة المعلومات لاستثمار ذلك في الجرائم الإلكترونية، من خلال عمليات الإختراق وسرقة بعض البطاقات الإلكترونية، واستخدامها في عمليات البيع والشراء للحصول على المال، أو بابتزاز الأشخاص المجني عليهم، وتهديدهم بنشر معلوماتهم الخاصة على المواقع الاجتمّاعية للحصول على المال وغيره حسب الوضع الاجتمّاعي والاقتصادي للضحية.
- **الدوافع السياسيّة:** أسهم التطور التكنولوجي في قيام بعض الدول برفع المعلومات الخاصة بالمواطنين من خلال المواقع الإلكترونية الحكومية، وهذا أدى إلى قيام بعض المنظمات أو مخابرات بعض الدول في البحث عن المعلومات الدقيقة والسريّة خاصة التي يمكن استخدامها فيما بعد سياسياً للضغط للحصول على امتيازات مختلفة (لطرش، 2016).

8.2.10 الصعوبات التي تواجه مكافحة الجريمة الإلكترونية في فلسطين:

هناك العديد من الصعوبات التي تواجه مكافحة الجريمة الإلكترونية في مناطق السلطة الفلسطينية، لعل من أهم تلك الصعوبات كما بينها (مطر، 2014) ما يأتي:

- سيطرة دولة الاحتلال على فضاء الإنترنت والاتصالات في فلسطين مما يصعب من متابعة الجريمة الإلكترونية، إذ تخشى دولة الاحتلال من أن يكون لسيطرة السلطة على فضاء الانترنت والإتصالات دور في كشف العملاء الذين يعملون معها.

- الفرق التكنولوجي ما بين دولة فلسطين ودولة الاحتلال إذ لا يسمح الاحتلال بوجود معدات وأجهزة تتعارض مع سيطرتها التكنولوجية على الفضاء السبراني لفلسطين.
- نقص الخبرات اللازمة في ملاحقة الجريمة الإلكترونية سواء من ناحية القدرات البشرية أو التكنولوجية المواكبة للتطور التكنولوجي المتسارع.
- المعيقات الإجرائية التي تتعلق بالناحية القانونية ومشروعية الإجراءات والأدلة المستخلصة من التحقيق في الجريمة الإلكترونية.
- جهل الناس بالجريمة الإلكترونية وعدم التبليغ عنها خوفاً من كشف معلومات أو افتضاح طبيعة الجريمة مما يؤدي إلى التستر عليها.
- سوء الضبط والتفتيش عن الجريمة الإلكترونية لجهل القائمين بعملية الضبط والتفتيش، مما يؤدي إلى تدمير بعض الأدلة المعنوية على وجودها.
- قصور القوانين في تحديد طبيعة الجريمة الإلكترونية وإجراءات الضبط القضائي والإجرائي والتفتيش تحت مسمى حماية الحرية الشخصية مما يعيق عمل الأجهزة الأمنيّة في إثبات هذه الجريمة.

9.2.10 الإطار القانوني والمؤسساتي لمكافحة الجريمة الإلكترونية في فلسطين:

إدراكاً للتطور المتسارع في كافة مناحي الحياة، وباستقراء الوضع الجرمي الحالي والمستقبلي للثورة الرقمية، ثبت عدم وجود حدود للزمان والمكان أمام ارتكاب الجرائم بفعل ثورة الاتصالات والتقنيات الحديثة، وظهور أشكال جديدة من الجرائم بأساليب مبتكرة لتنفيذها عبر تقنيات الحاسوب، نتيجة لذلك صدر قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية لمزيد من التوضيح انظر/ي ملحق رقم (7) الخاص بالتعديل على القانون رقم (16) لسنة (2017) بشأن الجرائم الإلكترونية الذي

يمكن الاطلاع عليه من خلال ملحق رقم (6)، فالتشريع السابق كان يُجرّم في الغالب المخالفات ضدّ الأصول والهويّات الماديّة دون الافتراضية، وبعد اعتراض مؤسسات المجتمّع المدني(المدنية والحقوقية) على الثغرات في الأساس القانوني للملاحقة القضائية كونها تمّس بالحقوق والحريات للمواطنين تمّ تداركه في القرار بالقانون (10) لسنة (2018)، وفي هذا المجال يرى (عبد الباقي، 2018) أن الإطار القانوني الموجود في فلسطين قبل إصدار قانون الجرائم الإلكترونية ليس كافياً لمكافحة إساءة استخدام الإنترنت والبيانات ونُظُم الكمبيوتر، لهذا لا بد من تطوير في تعريف الجرائم الرقمية، والدليل على ضرورة التطوير أنّ الشرطة الفلسطينية تشاركه هذا الرأي مُؤكِّدة أن القانون الجديد رقم (10) لسنة (2018) سيُمكِّن من التجريم الفعّال والملاحقة القضائية وجمع الأدلّة المُتعلِّقة بالجرائم الرقمية.

حيث تمّثلت التعديلات على القانون رقم (16) لسنه (2017) بإلغاء النصوص العامة والفضفاضة بشكل صريح مثل المادة (15) لعدم استيفائها الشروط الاجرائية القانونية، وتحديد النائب العام وليس النيابة من يتخذ القرار بناءاً على قرار من المحكمة المختصة بالجرائم الإلكترونية، والمادة (30) والمادة (33) التي تمّنح الصلاحية للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي، ودون أمر من المحكمة المختصة بتفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة وضبط الأجهزة والأدوات والبيانات والمعلومات الإلكترونية، والتحفظ على كامل نظام المعلومات أو أي وسيلة من وسائل تكنولوجيا المعلومات من شأنها أنّ تساعد على كشف الحقيقة دون حضور المتهم أو حيازة الأجهزة لإجراءات التفتيش والضبط، والمادة (34، 40، 46) التي تتعارض مع الاتفاقيات الدولية والعربية بهذا الشأن وغيرها من النصوص التي تمّ تداركها في القانون رقم (10) لسنة (2018).

على أثر هذا القانون قامت النيابة العامة الفلسطينية باستحداث مكتب مكافحة الجرائم المعلوماتية "الإلكترونية"، إذ تمّ تخصيص 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 الأمنيّة الأخرى ذات الاختصاص، وتتولى التواصل مع الجهات والمؤسسات والشركات المختصة فيما يتعلق بالجرائم الإلكترونية والاتصالات والحصول على الدليل الفني الالكتروني وربط الجناة فيه (براك وجراده، 2019).

ومع وجود هذه القوانين الصارمة فيما يخص الجرائم الإلكترونية وما تمّ استحداثه من دوائر خاصة بالجرائم الإلكترونية، فقد أشارت (الشرطة الفلسطينية،2021) إلى أنّ هناك تزايد في معدلات الجريمة الإلكترونية في فلسطين، فقد بين (ارزيقات، 2018) أنّ الشرطة الفلسطينية سجلت في العام (2015) (502) قضية، وفي عام (2017) (1327) قضية، وفي عام (2018) سُجل (2568) قضية.

وفي عام (2020) أصبح التوجه نحو الانترنت بشكل أكبر بسبب جائحة كورونا، مما يعني إزدياد نسبة الجريمة بسبب ممارستها بشكل أكبر، ذلك بسبب ارتفاع البطالة وفقدان الكثير من الأفراد لمصدر دخلهم، كذلك لتوجه وزارة التربية والتعليم للدراسة من خلال الانترنت، هذا سمح بانتشار برامج الفيديو (Zoom,Microsoft Teams) وغيرها من البرامج المستخدمة في التعليم التي تسمح بالمشاهدة بالصوت والصورة، مما يعني اختراق كبير لخصوصية الفرد، وعليه يمكن حدوث اخطاء في برامج معينة قد يستغلها المجرم لعدم دراية الضحية بها، إضافة إلى انعدام الرقابة على الانترنت لوجود مبرر، فيكون هناك فرص أعلى للقيام بجرائم الكترونية على كافة الأصعدة، الشخصية بسرقة

المعلومات أو الصور، أو مالية بسرقة الحسابات وبطاقات الائتمّان، أو بتزوير الصور والمعلومات والبطاقات وغيرها.

وعليه نصل إلى نتيجة أنّ الجرائم الإلكترونية تحتاج إلى متابعة أمنية حثيثة من كافة الأجهزة، مع ضرورة العمل على توعية أفراد المجتمّع من قبل الأجهزة المختلفة، ومن الوحدات الخاصة بالجرائم الإلكترونية في جهاز الشرطة الفلسطينية والنيابة العامة وحماية الأسرة والأمن الوقائي، ذلك لضمان العمل على الحد من انتشار هذه الجرائم، وهذا يحتاج أيضاً إلى المتابعة القانونية وتطبيق القانون على من يثبت تورطه بمثل تلك الجرائم.

10.2.10 النظريات المفسرة للجريمة الإلكترونية:

تعددت النظريات المفسرة للجريمة الإلكترونية، ومن أهمها:

- **نظريّة النشاط الرتيب والفرصة:** من أشهر روادها ماركوس فيلسون ولاريكوهين (1979)، وترى هذه النظريّة أنّ النزعة الإجرامية موجودة عند الأفراد، لكنها بحاجة إلى عناصر تساعد على إظهارها لحدوث الجريمة، ومن أهم هذه العناصر أولاً: توفر الإرادة الجرميّة (الجاني) وثانياً: وجود الضحية وثالثاً: غياب القانون، وتكون الفرصة أكبر في ظل توفر هذه العناصر معاً (عابدين، 2020).

نستنتج من هذه النظريّة أن حدوث الجريمة ناشئ عن العلاقة بين الأفراد في المجتمّع، هذه العلاقة إجبارية في التعامل اليومي بين الأفراد سواء في التعليم أو العمل أو غيرها من الأماكن، ومع التطور التكنولوجي وانتشار شبكة الإنترنت وسهولة التواصل مع الآخرين بتوفر أجهزة الجوال التي تتيح لأي فرد امتلاكه، واستخدام المواقع المختلفة عبر اشتراك الانترنت، أصبح الاتصال سهلاً بين الأفراد وازداد صعوبة من خلال توفر إمكانية التواصل صوتاً

وصورة، هذا الأمر أدى إلى تعمق العلاقات بين الجاني والضحية، وهي فرصة للحصول على المعلومات التي يريدها، واستغلالها كما يشاء بناء على الدافع الجرمي الذي قصده، عادةً ما يكون هذا الدافع موجود لدى الضحية كالرغبة في الزواج، أو نقص العاطفة والبحث عنها، كما تمّ استغلال سهولة التخفي والدخول بأسماء مستعارة، وأيضاً حذف المعلومات والحسابات الخاصة بسهولة، كل ذلك أتاح للجاني الفرصة لاستغلال الظروف الخاصة بالضحية والايقاع بها في ظل هذا العالم الافتراضي.

كما تمّثلت الفرصة أيضاً في استغلال الجاني لعدم قدرة الأجهزة الأمنيّة متابعته كونه يستخدم وسيلة اتصال لا يمكن متابعتها أيضاً، وهي شرائح الاتصال الإسرائيلية، وبالتالي توفر فرصة كاملة للقيام بالجريمة على أكمل وجه، علماً بأنّ نظرية الفرصة التي بينت أنّ الفرصة تشكل عاملاً مساعداً على حدوث الجريمة إذا تعرض الفرد للضغوط، تحديداً إذا كان ذلك في مجتمّع متفاوت الثقافات ظهرت في العام (1960) وأهم من تحدث عنها (كلوارد وأوهلن).

- **نظريّة الضبط الذاتي:** أشهر من نادى بها عالم الاجتمّاع الامريكي هورتون كولي وذلك في العام (1991)، وبينت أنّ المجتمّع يعتمّد في تنظيمه الاجتمّاعي على القيم والأنماط والمثل المختلفة ضمن مستويات مختلفة، فالضبط الاجتمّاعي يُعد عملية مستمّرة لخلق تصور ذاتي للمجمع من خلال المجتمّع نفسه، فالأفراد ليسوا منعزلين عن التكوين الاجتمّاعي (السمري ولطفي وعبد الفتاح، 2010).

وتبين هذه النظريّة أنّ للمجتمّع دور في عملية الضبط الاجتمّاعي للقيم والمعتقدات التي يمارسها الفرد في المجتمّع، وهي تتكون نتيجة لعملية الضبط الأسري بداية ثم انتشارها لتشمل المجتمّع ككل، وعليه يسهم المجتمّع في بناء عملية الضبط الاجتمّاعي، وتحديد المفاهيم

الأخلاقية التي يتعامل من خلالها، فلكل مجتمّع قيمه الخاصة التي تحكمه، والتي ورثها الأبناء عن الآباء والأجداد.

وتنشأ الجريمة الإلكترونية تبعاً للتنشئة الاجتمّاعية للأفراد وما يحدث حولهم في المجتمّع، فالمجتمّع الذي لا يطبق مبدأ العدالة الاجتمّاعية بين الأفراد، وتكثر فيه السرقات والفساد ويرتفع فيه مستوى الفقر والبطالة، يكون مستوى الضبط الاجتمّاعي فيه متدني وعليه تكثر فيه الجريمة بشكل عام، والجريمة الإلكترونية بشكل خاص.

وفي ظل التطور التكنولوجي واستهداف الأفراد من خلال مواقع التواصل الاجتمّاعي التي أصبحت كثيرة ومتنوعة منها (الفيس بوك، تويتر، سناب شات، واتس اب، تك توك) وغيرها، إضافة إلى أنّ أغلب الأفراد والمؤسسات والشركات وحتى الحكومات تتيح فرصة كبيرة للتعامل الشبكي من خلال الانترنت في كافة المجالات، وهذا شجع على ارتفاع مستوى الجريمة الإلكترونية في العالم.

في فلسطين كونها تخضع للاحتلال الاسرائيلي، ويعمل الكثير من الشباب في الداخل المحتل، اكتسب هؤلاء الشباب قيماً دخيلة على المجتمّع العربي بسبب الانفتاح في الأماكن التي يعملون بها، وفي محاولة لنقل تلك التجربة على المناطق الفلسطينية أدى ذلك إلى رفع مستوى الجريمة الإلكترونية بدوافع التطور والتقدم الحضاري والعولمة.

- **النظرية الصراعيّة:** ظهرت عام (1904) وأهم روادها العالم (كارل ماركس)، هذه النظريّة تعتبر بدرجة كبيرة أنّ سبب حدوث الجريمة يعود للتفاوت الطبقي وضعف المستوى المادي للفرد، هنا السلوك الجرمي لدى الأفراد نابع من ضعف قدرتهم على الإيفاء بالالتزام المالي المطلوب منهم وعدم قدرتهم على تحقيق حاجاتهم وحاجات أبنائهم، ترى هذه النظريّة أنّ المال

يُعتبر السبب في التفاوت الطبقي، إذ يجب تقسيم المال ليحصل الجميع على كافة الاحتياجات، حتى لا يضطر ذوي الطبقة المسحوقة والمقهورة التوجه نحو السلوكيات الجرمية من أجل الحصول على المال وتلبية احتياجاتهم (عودة، 2014).

كما أنّها تركز على الجانب الاقتصادي وحده، وأنّ هذا الجانب هو الأهم في تعزيز حياة الفرد وتمّكينه من تحقيق رغباته، فالمال هو الطريق المؤدي إلى الاستثمار والحد من البطالة والفقر، وارتفاع مستوى الحياة العامة لدى الأفراد يقلل من فرص توجههم نحو الانحراف، إذ إنّ تحقيق الرغبات العامة والحاجات الأساسية يتطلب توفر مستوى معيشي متوسط بالحد الأدنى، لذلك فالمال سبب في التوجه نحو الانحراف، وعلى مستوى الجريمة الإلكترونية فإنّ نسبة عاليّة من الابتزاز الالكتروني يسعى أصحابه للحصول على المال بسبب الفقر والبطالة وضعف المستوى المعيشي وعدم القدرة على تلبية الاحتياجات الأساسية لأسرهم فيقع الجاني في وحل الجريمة لكن الهدف الأساسي يتمّثل في الحصول على المال.

وعلى الصعيد الفلسطيني بين (الجهاز المركز للاحصاء الفلسطيني، 2019) أنّ ما نسبته (25.3%) يعانون من البطالة والفقر، لذلك من الممكن أن تؤدي دوافع الحصول على المال إلى ارتكاب الجريمة سواء بتخطيط مسبق للقيام بالجريمة، أم من خلال استدراج الضحية لاستلاب المال منها وتركها فيما بعد.

- **النظريّة التحليليّة:** يعد سيجمود فرويد (1899) من أهم روادها وترى أنّ السلوك الجرمي ناتج عن السلوك غير السوي النابع من شخصية ضعيفة بلا قيم أو معتقدات تسيطر عليها الشهوات والأنا والنزعة الذاتية، ويتحكم بها الهوى والنفس الدنيئة، وهو مرض نفسي وليس بيولوجي، وتبين أنّ السيطرة تكون نابعة من نقص الضمير وضعف مستوى الإحساس

والشعور، وعادة ما يكون مرتكبي الجرائم من هذه الفئة لديهم مشكلات نفسية كالشعور بالدونية (رويمل، 2012).

وعليه فإنّ الحالة النفسية لها دور كبير في الحد من الجريمة، فالشخصية السوية ذات القيم والمعتقدات والمبادئ، يكون مستوى توجهها نحو الجريمة أقل من الشخصية غير السوية، فتقدير الذات وصحوة الضمير والإنبساط وحب الخير والانتفاح على الآخرين، يساعد بشكل كبير في الوصول إلى النجاح والحصول على تقدير المجتمّع، فيكون مستوى التوجه نحو الجريمة لديه أقل، لذلك تشكل الحالة النفسية لاعباً أساسياً في توجهات الفرد، إضافة إلى توفر الحاجات والشعور بالثقة والطمأنينة، والرغبة في العيش والتعاون مع الآخرين ومساعدتهم.

وفي المجتمّع الفلسطيني فإنّ مستوى الفقر والبطالة، والكبت الذي يعاني منه الشباب بعدم القدرة على توفير متطلبات الحياة وارتفاع مستوى المعيشة وتدني والأجور وضعف فرص الحصول على عمل، كل ذلك أسهم في تكون حالة نفسية سيئة لدى الشباب أسهمت في التفكير في الحصول على المال بشتى الطرق.

- **النظريّة البنائية:** تعتمّد هذه النظريّة النسق الاجتمّاعي لدراسة كافة التغيرات التي يمكن أن تحدث في المجتمّع، وهو ما عبر عنه (بارسونز) عام (1951)، فهي ترى بأنّ المجتمّع أجزاء مترابطة، ولكل جزء وظيفة خاصة به يؤديها، وعليه يكون توازن المجتمّع معتمّداً على ترابط أجزائه (المغذوي، 2014) و (السلايمة، 2018).

استناداً إلى هذه النظريّة فوجود ترابط بين الأجهزة الأمنيّة وقيامها بالمهام المطلوبة منها في حفظ الأمن، إضافة إلى قيام الجهات الحكومية بتوفير كافة الاحتياجات الخاصة بالمواطنين، ودعم المواطنين للقيم والأخلاق والعقائد، كل هذا مُجتمّعاً يؤدي إلى الحد من الجريمة، وفي

المجتمّع الفلسطيني فإنّ نسبة الترابط بين المجتمّع والجهات الحكومية متدني، لعدم وجود بنية تحتية قادره على دعم هذا التوافق، فنسب البطالة والفقر والوضع الاقتصادي المتردي ووجود الاحتلال، كل هذه العوامل ساهمت في عدم وجود ترابط بين الوظائف المجتمّعية، إضافة إلى الفجوة بين الأجهزة الأمنيّة والمواطنين، كل ذلك عرقل عملية البناء المجتمّعي المتكامل، وأسهم في التوجه نحو الجريمة، وعليه فإنّ قيام الأجهزة الأمنيّة والحكومة بشكل عام بكامل وظائفها يسهم في الحد من حدوث الجريمة الإلكترونية في فلسطين.

- **نظريّة الوصم:** تعود بداية نظرية الوصم إلى ما كتبه العالم (تاننبوم) عام (1938)، ترى هذه النظرية بأنّ وجود المجرم ناتج عن الكيفية التي يعامله بها الآخرون، تُركز نظرية الوصم الاجتمّاعي على ردود فعل المجتمّع على الانحراف والجريمة وتأثيرها على تزايد مدى الجريمة، تستند النظريّة على فكرة أنّ المجتمّع وبعض أفراده تكون لهم قدرة على بناء وتطبيق صفات معينة لأفراد آخرين من نفس المجتمّع، غالباً ما تكون عملية وصم الأفراد في المجتمّع سلبية وتؤثر عليهم، إنّ ما سبق يوضح لنا أنّ العنصر الأساس في النظريّة ليس سلوك الفرد بل هو ردة فعل المجتمّع على سلوك معين، باعتباره سلوك انحرافي بناءً على القيم والمعايير السائدة في المجتمّع، بالتالي فإنّ الانحراف يعود لطبيعة النظرة الاجتمّاعية تجاه سلوك الأفراد في المجتمّع (Breen, 2011).

استناداً إلى هذه النظريّة فإن الخوف من الفضحية وردة فعل المجتمّع، تدفع الضحية إلى عدم الإفصاح عما حصل معها من تهديد أو تحرش أو ابتزاز، فلا تلجأ للقانون أو الحديث عن هذا الفعل، بهذا يتحكم المجرم فيها مبتزاً سواء مالياً أو جنسياً أو غير ذلك، وفي الجرائم

الإلكترونية يكون عادة الابتزاز من خلال الحصول على صور أو فيديوهات أو مقتنيات شخصية للضحية، وتهديدها بالنشر والفضحية إذا لم يتمّ تلبية مطالب الجاني.

- **نظريّة الردع:** تُعتبر نظرية الردع من النظريات التي اهتمّت بالردع كوسيلة لمنع حدوث الجريمة، ذ يتمّ تحقيق الردع من خلال القبض على كل من ينتهك القانون ومعاقبته بشدة حتى يتمّ منعهم من تكرار الجرائم في المستقبل، هذا ما يُطلق عليه الردع الخاص، في حين يتمّثل الردع العام فيما تقوم به الدولة من خلال ردع المنتهكين للقانون كوسيلة لمنع الاخرين من ارتكاب الجرائم، فالدولة تزرع فيهم الخوف الكافي من العقاب الذي يمكن أن يتعرضوا له اذا ما قاموا بخرق القوانين وفكروا بارتكاب الجرائم (البداينة والخريشا، 2013).

والجرائم الالكترونية يمكن أن تدمج بين النوعين السابقين، فالطريقة تختلف في التنفيذ لكن الدواعي الأساسية ثابته، فالسرقة والقتل والاغتصاب والتهديد يمكن أن تحدث إذا كان هناك هدف، فعلى صعيد المجتمّع الفلسطيني يمكن القول إنّ وجود قانون ردع مناسب وشامل يسهم في الحد من ممارسة الجريمة الالكترونية، وأيضاً تشكل قيم المجتمّع رادع آخر في الحد من حدوثها، كون أن الاخلاقيات العامة للمجتمّع الفلسطيني ترفض الجريمة بكافة اشكالها وتدعوا إلى نبذها.

- **النظريّة التكامليّة (متعددة العوامل):** وضح أصحابها (هيرمان وجوليا سونجرز) (1979)، بأنّ العوامل التي تتحكم في الجريمة نوعان، عوامل بيئية وأخرى ذاتية، وربطت هذه النظريّة بين الجريمة والعوامل البيئة الداخلية والخارجية والظروف التي يعيشها الفرد، ويتفاعل من خلالها معها، أي هناك عوامل شمولية وتكاملية تؤدي إلى حدوث الجريمة لها علاقة بالمجتمّع والفرد والبيئة (الوريكات، 2013).

استناداً الى هذه النظريّة فإنّ المصالح الخاصة بالمراهقين واحتياجاتهم وسعيهم وراء سلوكياتهم الفردية ذات المصالح الشخصية النابعة من تحقيق الحاجات والرغبات، يؤدي إلى اتباع سلوكات منحرفة تؤدي إلى الجريمة، فالبحث عن الغرائز من خلال شبكة الأنترنت تحديداً بسبب التطور التكنولوجي الحالي، يؤدي في النهاية تورط هؤلاء الأفراد بجرائم مختلفة سببها تقديم المصالح الشخصية والحاجات الفردية إلى مصالح الجماعة والمجتمّع، وعادة ما يكون أصحاب الطبقة الدنيا هم من يقوم ببعض الجرائم التي تخص تحقيق المصالح الفردية أكثر من غيرهم، فيما يمكن أنْ يقوم أصحاب الطبقات العليا بهذه الجرائم من باب التسلية، أو التمّلك لمن هم أقل منهم في المستوى الاقتصادي والاجتمّاعي.

والفرد في المجتمّع الفلسطيني قد يتحقق لديه تكامل في الظروف التي يعيشها، بناءً عليه تكون فرصة التوجه نحو الجريمة مرتفعة، يعود ذلك إلى طبيعة البيئة والمجتمّع الذي يعاني من ظروف اجتمّاعية وسياسية واقتصاية تسهم في السيطرة على الفرد وتحد من تفكيره بالوازع الديني والقيم والعادات والتقاليد واهمالها في سبيل تحقيق مستوى مغاير لحياته الحالية.

2.11 الدراسات السابقة وذات العلاقة:

تستمّد الدراسة المعلومات الأساسية لها من الدراسات السابقة وذات العلاقة التي تمّت في هذا المجال، التي توصل الباحثون فيها إلى نتائج مهمة تفيد الدراسة، فيما يلي استعراض لأهم الدراسات السابقة وذات العلاقة بموضوع الدراسة:

أولاً: الدراسات العربية:

- دراسة الاطرش (2018) بعنوان "**معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الاجهزة الأمنيّة**"، هدفت الدراسة

التعرف إلى معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الاجهزة الأمنيّة، بلغت عينة الدراسة (125) شخص، تمّ اختيارهم من العاملين في اقسام الجرائم في الاجهزة الأمنيّة، وتمّ استخدام الاستبانه كاداة للدراسة، توصلت الدراسة إلى أنّ أهم معوقات مكافحة الجرائم التي جاءت بدرجة كبيرة سهولة محو الدليل أو تدميره في زمن قصير جداً، أمّا المعوقات الخاصة بالمجني عليه جاءت بدرجة متوسطة، وجاءت المعوقات المتعلقة بالتحقيق الجنائي نقص المهارة الفنية المطلوبة للتحقيق في هذه الجرائم بدرجة كبيرة، وأوصى الباحث بضرورة تدريب وتأهيل العاملين في اقسام الجرائم المعلوماتية في الأجهزة الأمنيّة والتنسيق بين الاجهزة في العمل الموحد.

- دراسة شهوان (2018) بعنوان "**دور المؤسسة الأمنيّة في الحد من الجرائم المستحدثة في الضفة الغربية**"، هدفت الدراسة التعرف إلى دور المؤسسة الأمنيّة في الحد من الجرائم المستحدثة في الضفة الغربية، بلغت عينة الدراسة (140) فرداً، تمّ استخدام الاستبانة على عينة بلغت (95) فرداً، والمقابلة على (45) فرداً، استخدمت الدراسة المنهج التحليلي المدمج بين النوعي والكمي، توصلت الدراسة إلى أنّ غياب الوعي الثقافي والإلكتروني من قبل المواطنين، وطبيعة الجرائم الإلكترونية كانت من أبرز معوقات مكافحة الجرائم الإلكترونية، كذلك يعد تشديد العقوبة على الجرائم الإلكترونية والتنسيق بين الأجهزة المختصة من أبرز آليات مكافحة الجرائم الإلكترونية، وأوصى الباحث بضرورة التنسيق بين الأجهزة العاملة في هذا المجال ونشر الوعي بمخاطر هذه الجرائم أمام الناس.
- دراسة عبد الباقي (2018) بعنوان "**التحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة الرقمية**"، هدفت الدراسة التعرف إلى التحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة

الرقمية وجميعها من الموضوعات المستجدة في فلسطين، استخدم الباحث المنهج المقارن ودراسة الحالة على القوانين الخاصة بالجريمة الإلكترونية في فلسطين مع الاتفاقيات الدولية كمعاهدة بودابيست والاتفاقية العربية لمحافحة الجرائم، والقانون النموذجي للاجراءات الجزائية، توصلت الدراسة الى ضعف التخصص لدى القائمين على التحقيق (النيابة العامة)، وضعف طرق جمع الأدلة لهذا النوع من الجرائم، إضافة الى عدم وجود كادر مختص مدرب في التعامل مع الجرائم الإلكترونية، وأوصت الدراسة بضرورة تدريب وتأهيل كفاءات قادرة على القيام بالمهام الإلكترونية بشكل سريع.

- دراسة العتيبي (2016) بعنوان "**دور التحريات والبحث الجنائي في الكشف عن الجرائم المعلوماتية**"، هدفت الدراسة التعرف إلى دور التحريات والبحث الجنائي في الكشف عن الجرائم المعلوماتية، بلغت عينة الدراسة (150) قضية من القضايا المعلوماتية في شرطة جدة، استخدم الباحث المنهج الوصفي، توصلت الدراسة أنّ دور التحريات في الكشف عن الجرائم المعلوماتية ضعيف، كما تبين أنّ دور التسجيل الجنائي في الكشف عن الجرائم المعلوماتية جيد، وتبين وجود صعوبات تواجه التحريات والبحث الجنائي عند الكشف عن الجرائم المعلوماتية، أوصى الباحث بالعمل على تأهيل وتدريب ضباط التحريات والبحث الجنائي، إضافة إلى استحداث فهارس ووحدات تتعلق بالجريمة المعلوماتية في أقسام التسجيل الجنائي بإدارات التحريات والبحث الجنائي.
- دراسة الحقباني (2013) بعنوان "**مهارات البحث والتحقيق في الجرائم المعلوماتية لدى ضباط شرطة مدينة الرياض**"، هدفت الدراسة التعرف الى مهارات البحث والتحقيق في الجرائم المعلوماتية لدى ضباط شرطة مدينة الرياض، تكونت عينة الدراسة من (140) ضابطاً، تمّ

استخدام المنهج الوصفي في الدراسة، تمّثلت أداة جمع البيانات في الاستبانه، توصلت الدراسة إلى توفر مهارات البحث والتحقيق بدرجة متوسطة لدى ضباط الشرطة، كذلك توصلت الى وجود معوقات تحد من تطوير البحث والتحقيق بدرجة عاليّة، في حين أوصت الدراسة بمزيد من التدريب والتطوير في هذا المجال لضباط الجرائم المعلوماتية، كون ذلك يقلل من امكانية حدوث الجرائم الإلكترونية ويسهل السيطرة عليها.

ثانياً: الدراسات الاجنبية:

- دراسة (Harkin & Whelan & Chang, 2018) بعنوان "**التهديد المتزايد للجرائم الإلكترونية**"، تبحث هذه الدراسة التجريبية عن الأجهزة والوحدات الأمنيّة المتخصصة في الجريمة الإلكترونية في أستراليا من أجل تقرير القضايا والمشكلات التي يواجهها أفراد الشرطة في الخطوط الأمامية لقسم مكافحة الجرائم الإلكترونية، ذلك باستخدام مزيج من بيانات المسح وإجراء المقابلات المتعمقة مع المشرفين والمحققين من وحدتين متخصصتين في الجريمة الإلكترونية، توصلت الدراسة لمستوى متوسط من الرضا عن العمل في مجال مكافحة الجريمة من قبل أفراد الشرطة، كذلك رفع مستوى قدرات الأفراد العاملين في مجال الجريمة الإلكترونية كونها أصبحت مشكلة اجتمّاعية متزايدة، وأوصت الدراسة بضرورة زيادة البرامج التدريبية التي تحاكي التطور الحاصل في النواحي التكنولوجية.
- دراسة (Hadlington et al, 2018) بعنوان "**تجارب ضباط الشرطة وتحدياتهم وتصوراتهم عن الجرائم الإلكترونية**"، هدفت الدراسة إلى توضيح نسبة الخداع والإيذاء من جرائم الإنترنت بشكل كبير خلال القرن العشرين، تكونت عينة الدراسة من (16) ضابطاً من الشرطة الخاصة بالجرائم الإلكترونية، استخدم الباحثون المنهج الوصفي التحليلي في الدراسة، تمّ

استخدام الاستبانه كاداة للدراسة، توصلت الدراسة إلى مستوى العاملين في دائرة الجرائم الإلكترونية في التعامل مع الجرائم الإلكترونية متوسط، وأوصت الدراسة بأنّ هناك حاجة إلى التدريب المستمّر لرفع قدرتهم فيما يخص سرعة التحقيق في الجرائم والقدرة على ضبطها قبل هروب المجرمين لسهولة ذلك في الجرائم الإلكترونية.

- دراسة (Pool & Custers, 2017) بعنوان "**عمليات الاختراق الرجعية التي تقوم بها الشرطة: تأثيرات وتداعيات المشرعية والضرورة والخصوصية للخطوة القادمة في محاربة الجريمة الإلكترونية**"، هدفت الدراسة التعرف إلى تعزيز وتحسين موقف الشرطة الهولندية في مكافحة الجريمة الإلكترونية، تكونت عينة الدراسة من (45) من العاملين في قسم الجرائم الإلكترونية، تمّ استخدام المنهج الوصفي في الدراسة، وتمّ استخدام الاستبانه كاداة للدراسة، توصلت الدراسة إلى أنّ مستوى العقوبات في القوانين الضابطة للجرائم الإلكترونية متدنية، كما توصلت إلى أن مستوى تقييد سلطات المحققين في عمليات التحقيق مرتفع، وقد أوصت الدراسة بضرورة منح المحققين سلطات أعلى خلال عملية التحقيق، وضرورة أن يكون هناك صلاحيات لتثبيت برامج تجسس إذا اقتضى التحقيق ذلك، كذلك أن يتمّ تشريع عقوبات رادعة على المجرمين حتى لا يتمّ العودة مرة اخرى للجرم.
- دراسة (Williamson, 2014) بعنوان "**التحديات التي تقلل من ضبط مجرمي الانترنت**"، هدفت الدراسة التعرف الى التحديات التي تقلل من ضبط مجرمي الانترنت، اعتمّدت الدراسة المنهج الوصفي بشقه الكيفي، واعتمّدت على المقابلة كاداة لجمع البيانات من عينة الدراسة المتمّثلة في مجموعة من الخبراء، توصلت الدراسة إلى أنّ هناك ضعف في دراسة تحديات ضبط مجرمي الانترنت، وضعف في مستوى المتابعة من قبل الاجهزة لهؤلاء المجرمين، كما

توصلت الى الحاجة لتوسيع نطاق العمل بين الجهات المختلفة فيما يخص الجرائم الإلكترونية، وأوصت الدراسة ببذل المزيد من الجهود لمراقبة شبكة الانترنت، وسن التشريعات التي تسمح بالمراقبة العامة لها كون ذلك يقلل من فرص حدوث الجرائم.

2.12 أوجه التشابه والإختلاف بين الدراسة الحالية والدراسات السابقة:

ركزت الدراسات السابقة على دور الاجهزة الأمنيّة في محاربة الجريمة الإلكترونية، تمّ الاستفادة من هذه الدراسات في بناء أدوات الدراسة والأدب النظري، إضافة إلى الاستفادة من نتائجها وتوصياتها، حيث تتفق الدراسة الحالية مع الدراسات السابقة في المنهج المستخدم المُتمّثل بالمنهج الوصفي كذلك إداة جمع البيانات، في حين تختلف الدراسة الحالية في أنّها جمعت بين الشق الكمي والكيفي معاً من خلال إستخدام أداة الإستبيان والمقابلة في جمع البيانات من عينة الدراسة، هذا لم يوجد في أي دراسة سابقة، إضافة لذلك تختلف الدراسة الحالية في أنّها تركز على جهاز الأمن الوقائي بشكل خاص، كونه من الاجهزة التي تهتمّ بالأمن الداخلي ولديه فريق خاص بجرائم المعلومات، كذلك في كونها تركز على الاجراءات المتبعة من قبل الجهاز في الحد من هذه الجرائم، إضافة إلى البحث في الدوافع التي تؤدي الى التوجه نحو هذا النوع من الجرائم، والصعوبات والحلول الممكنة في الحد منها، كما أنّها تعد من الدراسات الأولى التي ركزت على البحث في دور جهاز الامن الوقائي في الحد من الجرائم الإلكترونية حسب ما توفر من معلومات، إذ ركزت اغلب الدراسات السابقة على جهاز الشرطة والنيابة العامة أو الاجهزة الأمنيّة بشكل عام، كونها هي الأجهزة الأكثر ممن تتابع الجرائم بأشكالها وأنواعها المُختلفة بما فيها الجرائم الإلكترونية.

الطريقة والإجراءات

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

3 . 1 منهج الدراسة:

من أجل تحقيق أهداف الدراسة تمّ استخدام منهج المسح الاجتمّاعي بالعينة، كما تمّ إستخدام المنهج الوصفي بشقيّه الكمي من خلال الإستعانة بأداة الإستبيان والنوعي من خلال الإستعانة بدليل المقابلة، حيث يعرف هذا المنهج بأنه المنهج الذي يدرس ظاهرة أو حدثاً أو قضية موجودة حالياً يمكن الحصول منها على معلومات تجيب عن أسئلة البحث دون تدخل، يتمّ 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 (عليان، 2001).

3 .2 مجتمّع الدراسة:

تكون مجتمّع الدراسة من جميع العاملين المُختصين في الجرائم الإلكترونيّة بجميع وحداتها في جهاز الأمن الوقائي في الضفة الغربية البالغ عددهم (650) موظف/ة حسب إحصائيات (جهاز الأمن الوقائي، 2020)

3 .3 عينة الدراسة:

اشتمّلت عينة الدراسة على عينة قصدية تكونت من (200) استبانة بنسبة (30.8%) من مجتمّع الدراسة، الجداول رقم (1.3) يوضح توزيع أفراد عينة الدراسة حسب متغيرات الدراسة:

3 .4 وصف متغيرات أفراد العينة:

يبين الجدول رقم (1.3) توزيع أفراد عينة الدراسة حسب متغير الجنس حيث بلغت نسبة الذكور (86%) والإناث نسبة (14%)، ويبين متغير المؤهل العلمي أنّ نسبة (8.5%) ثانوية عامة فأقل، ونسبة (16.5%) للدبلوم المتوسط، ونسبة (61%) للبكالوريوس، ونسبة (14%) دراسات عليا، ويبين متغير العمر أن نسبة (22.5%) لأقل من (25 سنة،) ونسبة (35.5%) للعمر من (25- أقل من 35 سنة)، ونسبة (24.5%) للعمر من (35- أقل من 45 سنة) ونسبة (17.5% ل 45 سنة) فأعلى، وأما متغير الرتبة العسكرية يتضح منها أنّ نسبة (32%) كانت لصالح ملازم فما دون، ونسبة (40.5%) كانت لصالح ملازم أول-رائد، ونسبة (27.5%) لمقدم فأعلى، في حين يبين متغير عدد سنوات الخدمة ان نسبة (26.5%) كانت لصالح أقل من (5 سنوات) ، ونسبة (22%) كانت لصالح من (5- أقل من 10 سنوات)، ونسبة (10%) كانت لصالح سنوات الخبرة من (10- أقل من سنة 15) ، ونسبة (15%) من (15- أقل من 20 سنة) ونسبة (26.5%) كانت لصالح (20 سنة فأكثر)، وأما متغير طبيعة العمل في جهاز الأمن الوقائي يبين أن نسبة (40%) للتقني، ونسبة (8.5%) للإداري، ونسبة (51.5%) للعمليات.

جدول رقم (1.3): توزيع أفراد عينة الدراسة حسب متغيرات الدراسة

المتغير	المستوى	العدد	النسبة المئويّة
الجنس	ذكر	172	86.0
	أنثى	28	14.0
المؤهل العلمي	ثانوية عامة فأقل	17	8.5
	دبلوم متوسط	33	16.5
	بكالوريوس	122	61.0
	دراسات عليا	28	14.0
العمر	أقل من 25 سنة	45	22.5
	من 25- أقل من 35 سنة	71	35.5
	من 35- أقل من 45 سنة	49	24.5
	45 سنة فأعلى	35	17.5
الراتبة العسكرية	ملازم فما دون	64	32.0
	ملازم أول – رائد	81	40.5
	مقدم فأعلى	55	27.5
عدد سنوات الخدمة	أقل من 5 سنوات	53	26.5
	من 5- أقل من 10 سنوات	44	22.0
	من 10- أقل من 15 سنة	20	10.0
	من 15- أقل من 20 سنة	30	15.0
	20 سنة فأكثر	53	26.5
طبيعة العمل في جهاز الأمن الوقائي	تقني	80	40.0
	إداري	17	8.5
	عمليات	103	51.5

5.3 أدوات الدراسة:

تكونت أدوات جمع البيانات في الدراسة من أداتين رئيسيتين هما:

- **الاستبانة:** تمّ بناء أداة الدراسة الأولى التي تكونت من قسمين هما:
  - **القسم الأول:** شمل على المعلومات الخاصة بالمبحوثين (البيانات الديمغرافية) وهي (الجنس، المؤهل العلمي، سنوات الخبرة، العمر، الرتبة العسكرية).
  - **القسم الثاني:** شمل على مجالات الاستبانة الخمس هي:

- **المجال الاول:** تكون من (16) فقرة تضمنت الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية.
- **المجال الثاني:** تكون من (16) فقرة تضمنت دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة.
- **المجال الثالث:** تكون من (16) فقرة تضمنت أكثر أنواع الجرائم الإلكترونية التي تمّ التعامل معها في جهاز الأمن الوقائي.
- **المجال الرابع:** تكون من (17) فقرة تضمنت الصعوبات التي تواجه جهاز الأمن الوقائي في الحدّ من الجريمة الإلكترونية.
- **المجال الخامس:** تكون من (19) فقرة تضمنت أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية، لمزيد من التوضيح حول أداة الإستبانة بصورتها النهائية أنظر/ي ملحق رقم (2).

- **المقابلة:** تكونت المقابلة من (5) اسئلة ذات علاقة مباشرة بأسئلة الدراسة، تمّ طرحها على (5) أفراد من وحدة الجرائم الإلكترونية في المديرية العامة للأمن الوقائي في مدينة رام الله.

5.3.1 صدق الأداة:

تمّ تصميم الاستبانة بصورتها الأولية كما في ملحق رقم (1)، بعد ذلك تمّ أخذ الموافقة عليها من مشرفة 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 فقراتها 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 ملحق رقم (3)، ووفق هذه الملاحظات تمّ إخراج الاستبانة بصورتها النهائية، كما في ملحق رقم (2).

من ناحية أخرى تمّ التحقق من صدق الأداة بحساب معامل الارتباط بيرسون لفقرات الاستبانة مع الدرجة الكليّة للأداة، إذ اتضح وجود دلالة إحصائية في جميع فقرات الاستبانة، هذا إذا دل على شيء فإنّه يدل على أن هناك التساق داخلي بين الفقرات، والجداول التالية تبين ذلك:

جدول رقم (2.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات درجة الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.644**	0.000	7	0.641**	0.000	13	0.569**	0.000
2	0.758**	0.000	8	0.721**	0.000	14	0.682**	0.000
3	0.709**	0.000	9	0.663**	0.000	15	0.806**	0.000
4	0.696**	0.000	10	0.652**	0.000	16	0.152*	0.032
5	0.716**	0.000	11	0.725**	0.000			
6	0.781**	0.000	12	0.768**	0.000			

** داله احصائية عند 0.001
* داله احصائية عند 0.050

جدول رقم (3.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظر موظفي جهاز الأمن الوقائي

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.385**	0.000	7	0.643**	0.000	13	0.514**	0.000
2	0.563**	0.000	8	0.556**	0.000	14	0.446**	0.000
3	0.579**	0.000	9	0.515**	0.000	15	0.534**	0.000
4	0.486**	0.000	10	0.522**	0.000	16	0.602**	0.000
5	0.489**	0.000	11	0.485**	0.000			
6	0.530**	0.000	12	0.479**	0.000			

** داله احصائية عند 0.001
* داله احصائية عند 0.050

جدول رقم (4.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات أكثر أنواع الجرائم الإلكترونية التي تتعامل معها في جهاز الأمن الوقائي

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.444**	0.000	7	0.647**	0.000	13	0.742**	0.000
2	0.614**	0.000	8	0.754**	0.000	14	0.651**	0.000
3	0.660**	0.000	9	0.759**	0.000	15	0.622**	0.000
4	0.676**	0.000	10	0.732**	0.000	16	0.693**	0.000
5	0.631**	0.000	11	0.734**	0.000			
6	0.701**	0.000	12	0.715**	0.000			

** داله احصائية عند 0.001
* داله احصائية عند 0.050

جدول رقم (5.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات درجة الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.395**	0.000	7	0.560**	0.000	13	0.556**	0.000
2	0.696**	0.000	8	0.602**	0.000	14	0.452**	0.000
3	0.668**	0.000	9	0.715**	0.000	15	0.652**	0.000
4	0.576**	0.000	10	0.671**	0.000	16	0.646**	0.000
5	0.584**	0.000	11	0.647**	0.000	17	0.671**	0.000
6	0.618**	0.000	12	0.480**	0.000			

** داله احصائية عند 0.001
* داله احصائية عند 0.050

جدول رقم (6.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الحلول التي تساعد على الحد من الجريمة الإلكترونية

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.735**	0.000	8	0.765**	0.000	15	0.735**	0.000
2	0.767**	0.000	9	0.736**	0.000	16	0.752**	0.000
3	0.713**	0.000	10	0.689**	0.000	17	0.754**	0.000
4	0.722**	0.000	11	0.736**	0.000	18	0.748**	0.000
5	0.762**	0.000	12	0.793**	0.000	19	0.715**	0.000
6	0.767**	0.000	13	0.761**	0.000			
7	0.685**	0.000	14	0.821**	0.000			

** داله احصائية عند 0.001
* داله احصائية عند 0.050

5.3.2 ثبات الاداة:

تمّ التحقق من ثبات الأداة من خلال حساب ثبات الدرجة الكليّة لمعامل الثبات لمجالات الدراسة حسب معادلة الثبات كرونباخ الفا، كانت الدرجة الكليّة لدور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية (0.942)، هذه النتيجة تشير إلى تمّتع هذه الأداة بثبات يفي بأغراض الدراسة، والجدول رقم (7.3) يبين معامل الثبات للمجالات والدرجة الكليّة.

جدول رقم (7.3): نتائج معامل الثبات للمجالات

المجالات	عدد الفقرات	معامل الثبات
الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية	16	0.914
دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة	16	0.816
أكثر أنواع الجرائم الإلكترونية التي تتعامل معها في جهاز الأمن الوقائي	16	0.919
الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية	17	0.889
أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية	19	0.905
الدرجة الكليّة	**84**	**0.942**

3 . 6 إجراءات الدراسة:

تمّ العمل على بناء الأدب النظري للدراسة والدراسات السابقة، ثم بناء أداة الدراسة وعرضها على المشرفة والمحكمين ثم الحصول على صدق وثبات الأداة، بعد ذلك تمّ توزيع (230) استبانة على المبحوثين، تمّ استرجاع (200) استبانة صالحة للتحليل الإحصائي واستبعاد (30) استبانة لعدم صلاحيتها للتحليل، بعد ذلك تمّ تحليل الاستبانات الصالحة باستخدام برنامج الحزم الإحصائية (SPSS) للوصول الى النتائج النهائية.

3 . 7 المعالجة الإحصائية:

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

عرض نتائج الدراسة

4 . 1 مقدمة:

تضمن هذا الفصل عرضا لنتائج الدراسة التي تمّ التوصل إليها عن موضوع الدراسة وهو "**دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية: الأمن الوقائي أنموذجاً**" وبيان أثر كل من المتغيرات من خلال استجابة أفراد العينة على أداة الدراسة، وتحليل البيانات الإحصائية التي تمّ الحصول عليها، وحتى يتمّ تحديد درجة متوسطات استجابة أفراد عينة الدراسة تمّ اعتمّاد الدرجات التالية حسب المعادلة التاليّة: 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، يتمّ تقسيم هذه الفترات على 3 درجات (4–3=1.33) بذلك 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 المنخفضة، والدرجة المتوسطة (2.34) نضيف عليها طول الفترة (1.33) تصبح (2.34–3.67) متوسطة، وأعلى من ذلك تكون الدرجة عاليّة.

الدرجة	مدى متوسطها الحسابي
منخفضة	1 – 2.33
متوسطة	2.34 – 3.67
عاليّة	3.68 – 5

4 . 2 عرض نتائج أسئلة الدراسة:

سوف يتمّ 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 الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية ؟

للإجابة عن هذا السؤال تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تبين مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية، الجدول رقم (1.4) يبين ذلك.

جدول رقم (1.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئويّة
15	يعمل على متابعة التحقيق في قضايا الجرائم الإلكترونية	4.20	0.682	**عاليّة**	84.0
5	يعمل على التحديث المستمّر لبرامج حماية الحواسيب تجنباً للإختراق	4.14	0.761	**عاليّة**	82.8
14	يعمل على متابعة الشكاوي المُرتبطة بالجريمة الإلكترونية	4.12	0.708	**عاليّة**	82.4
1	يُزود الجهات ذات العلاقة بالتغذية الراجعة حول واقع الجريمة الإلكترونية	4.08	0.743	**عاليّة**	81.6
12	يعمل على رفع مستوى تدريب الكوادر البشريّة العاملة في مجال مكافحة الجرائم الإلكترونية	4.05	0.781	**عاليّة**	81.0
2	يُوفر مُعدات تقنية لمتابعة الجرائم الإلكترونية	4.04	0.742	**عاليّة**	80.8
4	يعمل على تأمين المواقع الحساسة في الدولة من الإختراق	4.04	0.726	**عاليّة**	80.8
11	يعمل على رفع مستوى الوعي العام بإتجاه مخاطر الإنترنت من خلال (ندوات، ورشات عمل، مؤتمّرات)	4.04	0.785	**عاليّة**	80.8
3	يعمل على مراقبة البرامج (التطبيقات) التقنيّة المستحدثة التي تقود الى الجريمة الإلكترونية بشكل مستمّر	4.01	0.702	**عاليّة**	80.2
6	يعمل على رفع مستوى المعرفة الرقميّة لضباطه العاملين في مجال الجرائم الإلكترونية بشكل دوري	3.99	0.836	**عاليّة**	79.8
13	يعمل على مراقبة الحسابات الشخصيّة للمشتبه بهم	3.89	0.703	**عاليّة**	77.8
16	يعمل على متابعة التهديدات الإلكترونية (للأفراد، للمؤسسات)	3.88	0.909	**عاليّة**	77.6
10	يعمل على التطبيق الفعلي لقانون الجرائم الإلكترونية	3.87	0.766	**عاليّة**	77.4

8	يعمل على التنسيق المستمّر مع الشركاء من الأجهزة الأمنيّة الأخرى العاملة في مجال مكافحة الجريمة الإلكترونية	3.86	0.845	**عاليّة**	77.2
7	يندرج عمل الجهاز في الجرائم الإلكترونية ضمن منظومة دوليّة لحاية البنية التحتية للمعلومات	3.85	0.728	**عاليّة**	77.0
9	يعمل على التنسيق المستمّر مع مؤسسات المجتمّع المدني العاملة في مجال مكافحة الجريمة الإلكترونية	3.76	0.818	**عاليّة**	75.2
الدرجة الكليّة		**3.98**	**0.506**	**عاليّة**	**79.8**

يلاحظ من الجدول رقم (1.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية أنّ المتوسط الحسابي للدرجة الكليّة (3.98) وانحراف معياري (0.506)، هذا يدل على أنّ مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية جاء بدرجة عاليّة وبنسبة مئوية (79.8%)، كما وتشير النتائج أنّ جميع الفقرات جاءت بدرجة عاليّة، إذ حصلت الفقرة "يعمل على متابعة التحقيق في قضايا الجرائم الإلكترونية" على أعلى متوسط حسابي بنسبة (4.20)، يليها فقرة "يعمل على التحديث المستمّر لبرامج حماية الحواسيب تجنباً للإختراق" بمتوسط حسابي (4.14)، وحصلت الفقرة "يعمل على التنسيق المستمّر مع مؤسسات المجتمّع المدني العاملة في مجال مكافحة الجريمة الإلكترونية" على أقل متوسط حسابي (3.76)، يليها الفقرة "يندرج عمل الجهاز في الجرائم الإلكترونية ضمن منظومة دوليّة لحاية البنية التحتية للمعلومات" بمتوسط حسابي (3.85).

2.2.4 النتائج المتعلقة بالسؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة؟

تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة، الجدول رقم (2.4) يبين ذلك.

جدول رقم (2.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لدوافع ارتكاب الجريمة الإلكترونية من قبل الجناة

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئويّة
2	عدم وجود رقابة حكوميّة على مواقع التواصل الاجتمّاعي	4.36	0.723	**عاليّة**	87.2
3	ضعف الرقابة الأسريّة على الأبناء	4.28	0.840	**عاليّة**	85.6
7	دوافع (جنسية، عاطفية، سياسية)	4.09	0.735	**عاليّة**	81.8
8	الاختلاط بأصدقاء السوء	3.98	0.850	**عاليّة**	79.6
16	عدم إلمام بعض الأفراد باستخدام (المواقع الإلكترونية، مواقع التواصل الاجتمّاعي)	3.98	0.839	**عاليّة**	79.6
14	السلوك العدواني لدى مرتكبي الجريمة الإلكترونية	3.93	0.715	**عاليّة**	78.6
9	ضغوط الحياة العامة (الاقتصادية، الاجتمّاعية، السياسية، البطالة، التفكك الأسري)	3.91	0.816	**عاليّة**	78.2
15	الفضول في التعرف على الأفراد عبر شبكة الإنترنت	3.91	0.775	**عاليّة**	78.2
12	عدم إلمام مرتكبي الجريمة الإلكترونية بالعواقب القانونية	3.90	0.880	**عاليّة**	78.0
1	عدم الإستغلال الجيد لوقت الفراغ	3.72	0.902	**عاليّة**	74.4
11	التنمر الإلكتروني	3.72	0.756	**عاليّة**	74.4
10	التنمر المُجتمّعي	3.71	0.734	**عاليّة**	74.2
13	إرتباط مرتكبي الجريمة الإلكترونية مع الإسرائيلين	3.69	0.823	**عاليّة**	73.8
6	حب المغامرة لدى بعض الأفراد	3.65	0.788	**متوسطة**	73.0
5	عدم تطبيق القانون ضد مرتكبي الجريمة الإلكترونية	3.63	1.082	**متوسطة**	72.6
4	الحصول على المنفعة المادية من خلال ابتزاز الضحية بمعلومات شخصية	3.56	0.727	**متوسطة**	71.2
	الدرجة الكليّة	**3.8762**	**0.42120**	**عاليّة**	**77.5**

يلاحظ من الجدول (2.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة أن المتوسط الحسابي للدرجة الكليّة (3.87) وانحراف معياري (0.421)، هذا يدل على أن درجة دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة جاء بدرجة عاليّة وبنسبة مئوية (77.5%)، كما وتشير النتائج في الجدول رقم (2.4) أنّ (13) فقرة جاءت بدرجة عاليّة و(3) فقرات جاءت بدرجة متوسطة، كما وحصلت الفقرة "عدم وجود رقابة حكوميّة على مواقع التواصل الاجتمّاعي لمرتكبي تلك الجرائم ومن يُشتبه بهم" على أعلى متوسط حسابي بنسبة (4.36)، يليها فقرة "ضعف الرقابة الأسريّة على الأبناء" بمتوسط حسابي بنسبة (4.28)، في حين حصلت الفقرة "الحصول على المنفعة المادية من خلال ابتزاز الضحية بمعلومات شخصية" على أقل متوسط حسابي بنسبة (3.56)، يليها الفقرة "عدم تطبيق القانون ضد مرتكبي الجريمة الإلكترونية" بمتوسط حسابي بنسبة (3.63).

3.2.4 النتائج المتعلقة بالسؤال الثالث: ما أنواع الجرائم الإلكترونية التي تعامل معها في جهاز الأمن الوقائي؟

تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن أنواع الجرائم الإلكترونية التي تتعامل معها في جهاز الأمن الوقائي، الجدول رقم (3.4) يبين ذلك.

جدول رقم (3.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لأنواع الجرائم الإلكترونية التي تتعامل معها في جهاز الأمن الوقائي

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئويّة
8	الابتزاز بجميع أشكاله	4.17	0.758	**عاليّة**	83.4
16	سرقة الحسابات الشخصية على مواقع التواصل الاجتمّاعي	4.17	0.726	**عاليّة**	83.4
15	إنتحال شخصية الغير	4.15	0.678	**عاليّة**	83.0
3	جرائم الإرهاب الالكتروني (الفكر المتطرف)	4.11	0.728	**عاليّة**	82.2
9	النيل من الشخصيات الإعتبارية بهدف التشهير بهم من خلال استخدام المعلومات الخاصة ونشرها بقصد الإساءة	4.11	0.755	**عاليّة**	82.2
6	انتهاك خصوصية الأفراد من خلال الدخول لحساباتهم الإلكترونية بهدف نشر معلوماتهم الشخصية دون علمهم	4.10	0.783	**عاليّة**	82.0
14	التجسس بكافة أشكاله	4.09	0.778	**عاليّة**	81.8
13	قرصنة المعلومات (الهكر)	4.06	0.751	**عاليّة**	81.2
10	نشر الرذيلة على شبكات التواصل الاجتمّاعي	3.98	0.820	**عاليّة**	79.6
4	جرائم تزوير المعلومات	3.97	0.708	**عاليّة**	79.4
2	جرائم المعلومات الأمنيّة	3.96	0.704	**عاليّة**	79.2
1	الجرائم السياسية	3.95	0.758	**عاليّة**	79.0
11	إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية	3.93	0.760	**عاليّة**	78.6
12	الوصول للمواقع المشفرة الممنوعة بطرق غير مشروعة	3.92	0.711	**عاليّة**	78.4
7	التنصت على الغير	3.85	0.807	**عاليّة**	77.0
5	استغلال الأطفال جنسياً	3.69	0.811	**عاليّة**	73.8
	الدرجة الكليّة	**4.01**	**0.506**	**عاليّة**	**80.3**

يلاحظ من الجدول رقم (3.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على أنواع الجرائم الإلكترونية التي تتعامل معها في جهاز الأمن الوقائي أن المتوسط الحسابي للدرجة الكليّة (4.01) وانحراف معياري (0.506)، هذا يدل على أن أنواع الجرائم الإلكترونية التي تتعامل معها في جهاز الأمن الوقائي جاء بدرجة عاليّة وبنسبة مئوية (80.3%)، كما وتشير النتائج أن جميع الفقرات جاءت بدرجة عاليّة وحصلت الفقرة "الابتزاز بجميع أشكاله" والفقرة "سرقة الحسابات الشخصية على مواقع التواصل الاجتمّاعي"على أعلى متوسط حسابي بنسبة (4.17)، يليها فقرة "إنتحال شخصية الغير" بمتوسط حسابي (4.15)، في حين حصلت الفقرة

"استغلال الأطفال جنسياً" على أقل متوسط حسابي بنسبة (3.69)، يليها الفقرة "التنصت على الغير" بمتوسط حسابي (3.85).

4.2.4 النتائج المتعلقة بالسؤال الرابع: ما الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية؟

تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية، الجدول رقم (4.4) يبين ذلك.

جدول رقم (4.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئويّة
12	صعوبة تعقب شرائح الإتصالات الإسرائيلية المُستخدمة في إرتكاب الجريمة الإلكترونية	4.44	0.713	**عاليّة**	88.8
14	تكتمّ الضحية تعرضها للجريمة الإلكترونية خوفاً من الفضيحة عند التبليغ	4.21	0.649	**عاليّة**	84.2
1	قلة الوعي المجتمّعي بالجريمة الإلكترونية	4.18	0.658	**عاليّة**	83.6
13	خوف الضحية من نتائج التحقيق	4.05	0.689	**عاليّة**	81.0
9	حداثة الجرائم الإلكترونية فهي تحتاج إلى (خبرات، كفاءات) للتعامل معها	3.97	0.829	**عاليّة**	79.4
10	حداثة التشريعات القانونية الخاصة بقانون الجريمة الإلكترونية	3.97	0.729	**عاليّة**	79.4
11	التغيير المُستمّر في طبيعة الجرائم الإلكترونية	3.97	0.729	**عاليّة**	79.4
15	انتحال المجرم الالكتروني لأسماء وهمية مما يصعب الكشف عن الجاني	3.92	0.785	**عاليّة**	78.4
16	عرقلة أطراف مُجتمّعيّة للتحقيقات المُرتبطة بالجرائم الإلكترونية	3.91	0.738	**عاليّة**	78.2
5	قصور التعاون الدولي بين الدول في مجالات مكافحة الجريمة الالكرونية	3.80	0.777	**عاليّة**	76.0
4	عدم وجود مفهوم قانوني دولي مشترك لتعريف الجريمة الإلكترونية	3.74	0.765	**عاليّة**	74.8
17	صعوبة متابعة الجُناة	3.74	0.791	**عاليّة**	74.8
2	صعوبة التوصل للأدلة الرقمية	3.71	0.817	**عاليّة**	74.2
8	نقص الكادر المتخصص للتعامل مع الوسائل الإلكترونية	3.56	0.928	**متوسطة**	71.2
3	صعوبة التحفظ على الإدلة الرقمية	3.54	0.850	**متوسطة**	70.8
7	ضعف كفاءة الكادر الذي يتعامل مع الجريمة الإلكترونية	3.33	0.966	**متوسطة**	66.6
6	ضعف مهارة الكادر الذي يتعامل مع الجريمة الإلكترونية	3.29	0.949	**متوسطة**	65.8
	الدرجة الكليّة	**3.84**	**0.474**	**عاليّة**	**76.9**

يلاحظ من الجدول رقم (4.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على مستوى الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية أن المتوسط الحسابي للدرجة الكليّة (3.84) وانحراف معياري (0.474)، هذا يدل على أنّ مستوى الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية جاء بدرجة عاليّة وبنسبة مئوية (76.9%).

كما وتشير النتائج أنّ (13) فقرة جاءت بدرجة عاليّة و(4) فقرات جاءت بدرجة متوسطة، وحصلت الفقرة "صعوبة تعقب شرائح الإتصالات الإسرائيلية المُستخدمة في إرتكاب الجريمة الإلكترونية" على أعلى متوسط حسابي بنسبة (4.44)، يليها فقرة "تكتمّ الضحية تعرضها للجريمة الإلكترونية خوفاً من الفضيحة عند التبليغ" بمتوسط حسابي (4.21)، وأما فقرة "ضعف مهارة الكادر الذي يتعامل مع الجريمة الإلكترونية" حصلت على أقل متوسط حسابي بنسبة (3.29)، يليها الفقرة "ضعف كفاءة الكادر الذي يتعامل مع الجريمة الإلكترونية" بمتوسط حسابي (3.33).

5.2.4 النتائج المتعلقة بالسؤال الخامس: ما أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية؟

تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية، الجدول رقم (5.4) يبين ذلك.

جدول رقم (5.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لأهم الحلول التي تساعد على الحد من الجريمة الإلكترونية

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة	النسبة المئويّة
19	تنظيم برامج توعويّة حول مخاطر الجريمة الإلكترونية	4.46	0.656	**عاليّة**	89.2
12	تجنب فتح أي رسائل إلكترونية مجهولة المصدر	4.41	0.620	**عاليّة**	88.2
18	رفع مستوى الرقابة الاسريّة على الأبناء	4.41	0.674	**عاليّة**	88.2
4	تشديد العقوبة على مرتكبي الجرائم الإلكترونية	4.40	0.729	**عاليّة**	88.0
6	تطوير قدرات العاملين في مجال مكافحة الجريمة الإلكترونية من خلال (التدريب، المؤتمّرات، ورش العمل)	4.39	0.678	**عاليّة**	87.8
17	رفع مستوى الوعي المُجتمّعي في تجنب نشر معلومات شخصيّة على مواقع التواصل الاجتمّاعي	4.39	0.707	**عاليّة**	87.8
11	تجنب إستخدام أي برامج مجهولة المصدر	4.38	0.647	**عاليّة**	87.6
13	تجنب إدخال كلمات مرور مجهولة المصدر تجنباً من التعرض لسرقة الحسابات المُستخدمة	4.38	0.705	**عاليّة**	87.6
16	مواكبة التطورات التقنيّة لتتبع مرتكبي الجرائم الإلكترونية للحدّ من انتشارها	4.37	0.675	**عاليّة**	87.4
3	عدم التحييز في تطبيق قانون الجريمة الإلكترونية على الافراد (توفير محاكمة عادلة للجناة)	4.35	0.678	**عاليّة**	87.0
5	تفعيل دور الرقابة المجتمّعية كوسيلة من وسائل الضبط الاجتمّاعي	4.35	0.728	**عاليّة**	87.0
8	تجنب تحميل أي برنامج مجهول المصدر	4.35	0.679	**عاليّة**	87.0
14	تجنب استخدام الحسابات الخاصة في الأماكن العامة غير الموثوقة تجنباً من التعرض للإبتزاز الإلكتروني	4.33	0.695	**عاليّة**	86.6
9	حماية الضحية أثناء التحقيق	4.31	0.717	**عاليّة**	86.2
15	تثبيت برامج حماية من إختراق الأجهزة الشخصية من أجل حماية ما به من معلومات شخصية	4.31	0.668	**عاليّة**	86.2
1	التعاون المشترك مع المؤسسات الدوليّة المعنية للحد من الجرائم الإلكترونية	4.27	0.685	**عاليّة**	85.4
10	حماية الضحية بعد الإنتهاء من التحقيق	4.27	0.733	**عاليّة**	85.4
7	وجود رقم موحد لدى جهات الاختصاص للتبليغ فور التعرض لجريمة إلكترونية	4.26	0.747	**عاليّة**	85.2
2	التعاون المشترك مع المؤسسات المحليّة المعنية للحد من الجرائم الإلكترونية	4.23	0.714	**عاليّة**	84.6
	الدرجة الكليّة	**4.348**	**0.5147**	**عاليّة**	**87**

يلاحظ من الجدول رقم (5.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية أن المتوسط الحسابي للدرجة الكليّة (4.34) وانحراف معياري (0.514)، هذا يدل على أن درجة أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية جاء بدرجة عاليّة وبنسبة مئوية (87%)، كما وتشير النتائج أن جميع الفقرات جاءت بدرجة عاليّة وحصلت الفقرة "تنظيم برامج توعويّة حول مخاطر الجريمة الإلكترونية" على أعلى متوسط حسابي بنسبة (4.46)، يليها الفقرة "تجنب فتح أي رسائل إلكترونية مجهولة المصدر" وفقرة "رفع مستوى الرقابة الاسريّة على الأبناء" بمتوسط حسابي (4.41)، وحصلت الفقرة "التعاون المشترك مع المؤسسات المحليّة المعنية للحد من الجرائم الإلكترونية" على أقل متوسط حسابي بنسبة (4.23)، يليها الفقرة "وجود رقم موحد لدى جهات الاختصاص للتبليغ فور التعرض لجريمة إلكترونية" بمتوسط حسابي (4.26).

6.2.4 النتائج المتعلقة بالفرضيات:

نتائج الفرضية الأولى: "لا توجد فروق ذات دلاله إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الجنس"

تمّ فحص الفرضية الأولى بحساب نتائج اختبار "ت" والمتوسطات الحسابية لاستجابة أفراد عينة الدراسة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية حسب متغير الجنس، الجدول رقم (6.4) يبين ذلك.

جدول رقم (6.4): نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية حسب متغير الجنس

الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة"t"	مستوى الدلالة
ذكر	172	3.9989	0.50961	0.703	0.483
أنثى	28	3.9263	0.48801		

يتبين من خلال الجدول السابق أن قيمة "ت" للدرجة الكليّة (0.703)، ومستوى الدلالة (0.483)، أي أنه لا توجد فروق في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الجنس، بذلك تمّ قبول الفرضية الأولى.

نتائج الفرضية الثانية: "لا توجد فروق ذات دلاله إحصائية عند مستوى الدلالة (α ≤ 0.05) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير لمؤهل العلمي"

تمّ فحص الفرضية الثانية بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير المؤهل العلمي، الجدول رقم (7.4) يبين ذلك.

جدول رقم (7.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير المؤهل العلمي

المؤهل العلمي	العدد	المتوسط الحسابي	الانحراف المعياري
ثانوية عامة فأقل	17	4.0956	0.55950
دبلوم متوسط	33	3.9318	0.37577
بكالوريوس	122	4.0302	0.53790
دراسات عليا	28	3.8103	0.43150

يلاحظ من الجدول رقم (7.4) وجود فروق ظاهرية في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير المؤهل العلمي، ولمعرفة دلالة الفروق تمّ استخدام تحليل التباين الأحادي (One Way ANOVA) كما يظهر في الجدول رقم (8.4):

جدول رقم (8.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير المؤهل العلمي

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	1.403	3	0.468	1.849	0.140
داخل المجموعات	49.564	196	0.253		
المجموع	50.967	199			

يلاحظ أن قيمة ف للدرجة الكليّة (1.849) ومستوى الدلالة (0.140) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه لا توجد فروق دالة إحصائياً في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير المؤهل العلمي، بذلك تمّ قبول الفرضية الثانية.

نتائج الفرضية الثالثة: "لا توجد فروق ذات دلاله إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير العمر"

تمّ فحص الفرضية الثالثة بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير العمر، الجدول رقم (9.4) يبين ذلك.

جدول رقم (9.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير العمر

العمر	العدد	المتوسط الحسابي	الانحراف المعياري
أقل من 25 سنة	45	3.9236	0.45166
من 25- أقل من 35 سنة	71	3.9824	0.46185
من 35- أقل من 45 سنة	49	4.0128	0.66585
45 سنة فأعلى	35	4.0518	0.39919

يلاحظ من الجدول رقم (9.4) وجود فروق ظاهرية في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير العمر، ولمعرفة دلالة الفروق تمّ استخدام تحليل التباين الأحادي (One Way ANOVA) كما يظهر في الجدول رقم (10.4):

جدول رقم (10.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير العمر

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	0.361	3	0.120	0.466	0.706
داخل المجموعات	50.606	196	0.258		
المجموع	**50.967**	**199**			

يلاحظ أن قيمة ف للدرجة الكليّة (0.466) ومستوى الدلالة (0.706) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه لا توجد فروق دالة إحصائياً في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير العمر، بذلك تمّ قبول الفرضية الثالثة.

نتائج الفرضية الرابعة: "لا توجد فروق ذات دلاله إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتبة العسكرية"

تمّ فحص الفرضية الرابعة بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتبة العسكرية، الجدول رقم (11.4) يبين ذلك.

جدول رقم (11.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتبة العسكرية

الرتبة العسكرية	العدد	المتوسط الحسابي	الانحراف المعياري
ملازم فما دون	64	4.0049	0.47940
ملازم أول – رائد	81	3.9498	0.56036
مقدم فأعلى	55	4.0273	0.45433

يلاحظ من الجدول رقم (11.4) وجود فروق ظاهرية في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتبة العسكرية، ولمعرفة دلالة الفروق تمّ استخدام تحليل التباين الأحادي (One Way ANOVA) كما يظهر في الجدول رقم (12.4):

جدول رقم (12.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير الرتبة العسكرية

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	0.221	2	0.110	0.429	0.652
داخل المجموعات	50.746	197	0.258		
المجموع	**50.967**	**199**			

يلاحظ أن قيمة ف للدرجة الكليّة (0.429) ومستوى الدلالة (0.652) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه لا توجد فروق دالة إحصائياً في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتبة العسكرية، بذلك تمّ قبول الفرضية الرابعة.

نتائج الفرضية الخامسة: "لا توجد فروق ذات دلاله إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير عدد سنوات الخدمة"

تمّ فحص الفرضية الخامسة بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير عدد سنوات الخدمة، الجدول رقم (13.4) يبين ذلك.

جدول رقم (13.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير عدد سنوات الخدمة

عدد سنوات الخدمة	العدد	المتوسط الحسابي	الانحراف المعياري
أقل من 5 سنوات	53	3.9752	0.43756
من 5- أقل من 10 سنوات	44	3.9347	0.49945
من 10- أقل من 15 سنة	20	3.9688	0.44171
من 15- أقل من 20 سنة	30	4.0083	0.60523
20 سنة فأكثر	53	4.0436	0.54838

يلاحظ من الجدول رقم (13.4) وجود فروق ظاهرية في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير عدد سنوات الخدمة، ولمعرفة دلالة الفروق تمّ استخدام تحليل التباين الأحادي (One Way ANOVA) كما يظهر في الجدول رقم (14.4):

جدول رقم (14.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير عدد سنوات الخدمة

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	0.318	4	0.079	0.306	0.874
داخل المجموعات	50.649	195	0.260		
المجموع	**50.967**	**199**			

يلاحظ أن قيمة ف للدرجة الكليّة (0.306) ومستوى الدلالة (0.874) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه لا توجد فروق دالة إحصائياً في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير عدد سنوات الخدمة، بذلك تمّ قبول الفرضية الخامسة.

نتائج الفرضية السادسة: "لا توجد فروق ذات دلاله إحصائية عند مستوى الدلالة (α ≤ 0.05) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي"

تمّ فحص الفرضية السادسة بحساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي، الجدول رقم (15.4) يبين ذلك.

جدول رقم (15.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي

طبيعة العمل في جهاز الأمن الوقائي	العدد	المتوسط الحسابي	الانحراف المعياري
تقني	80	3.8883	0.49590
إداري	17	4.0441	0.42434
عمليات	103	4.0576	0.51744

يلاحظ من الجدول رقم (15.4) وجود فروق ظاهرية في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي، ولمعرفة دلالة الفروق تمّ استخدام تحليل التباين الأحادي (One Way ANOVA) كما يظهر في الجدول رقم (16.4):

جدول رقم (16.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	1.349	2	0.674	2.677	0.071
داخل المجموعات	49.618	197	0.252		
المجموع	**50.967**	**199**			

يلاحظ أن قيمة ف للدرجة الكليّة (2.677) ومستوى الدلالة (0.071) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$) أي أنه لا توجد فروق دالة إحصائياً في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي، بذلك تمّ قبول الفرضية السادسة.

7.2.4: نتائج المقابلات المُعمقة:

المقابلة هي الأداة الثانية في الدراسة، حيث تمّ مقابلة مجموعة من الأفراد العاملين في وحدة الجرائم الإلكترونية في جهاز الأمن الوقائي، ذلك بهدف الحصول منهم على معلومات وبيانات حول الجرائم الإلكترونية، بعد الانتهاء من عمل المقابلات مع (5) من العاملين في وحدة الجريمة الإلكترونية في جهاز الأمن الوقائي، تمّ التوصل إلى النتائج الآتية:

القسم الأول: البيانات الشخصية:

الرقم	الاسم	العمر	المستوى التعليمي	المسمى الوظيفي	الرتبة	عدد سنوات الخبرة
.1	م. ر	43	بكالوريوس	مدير دائرة الضبط الفني	عقيد	20 سنوات
.2	م.ج	34	بكالوريوس	نائب مدير دائرة الضبط الفني	نقيب	10 سنوات
.3	ر. م	32	بكالوريوس	مدير قسم التشفير	نقيب	10 سنوات
.4	هـ.ق	29	بكالوريوس	مدير قسم الجوالات	نقيب	6 سنوات
.5	خ.ح	27	بكالوريوس	مدير قسم الاختراق	مساعد	5 سنوت

القسم الثاني: نتائج أسئلة المقابلات:

تمّ الإجابة على أسئلة المقابلات المُعمقة كما هو موضح في الجدول أدناه:

السؤال الأول: ما الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية؟	
م. ر	أشارت النتائج الخاصة بالسؤال الأول إلى أنّ عمل وإجراءات جهاز الامن الوقائي في حماية المجتمّع والمؤسسات بالكشف عن الجرائم والجرائم الإلكترونية، تتمّثل في الآتي: • أولاً: بالنسبة للمؤسسات والوزارات يتمّ فحص انظمة الحماية الإلكترونية الموجودة لديهم والتاكد من عدم وجود ثغرات بشكل دوري. • ثانياً: بالنسبة للمدارس والجامعات تقوم وحدة خاصة بالجهاز بترتيب لقاءات مع طلاب المدارس لنشر الوعي وطريقة استخدام الانترنت الامن، ذلك للحد من الجرائم الإلكترونية.
م.ج	جهاز الأمن الوقائي هو جهاز أمني يعمل على الكشف عن "الجرائم" منها الجرائم الإلكترونية المحتمّلة قبل حدوثها، لعل من أهم الاجراءت المتبعة التي يقوم بها نذكر بعضها: • قيام الجهاز بإعطاء دورات ونشرات توعوية في مؤسسات الدولة منها التعليمية كالجامعات والمدارس وغيرها تتعلق بموضوع الجرائم الإلكترونية وإبراز مخاطرها على المجتمّع وعواقبها. • التشبيك مع بعض المؤسسات لفحص اجراءات الحماية على الانظمة الإلكترونية المتعبة لديهم، وعلى مواقعهم الإلكترونية وفحص نقاط الضعف فيها وبشكل دوري.
ر. م	يتمّثل عمل جهاز الأمن الوقائي في نشر الوعي والتحذير من الجريمة الإلكترونية من خلال صفحة الجهاز الرسمية ومن خلال ادارة العلاقات العامة التي قامت بعدة محاضرات توعوية في المؤسسات التعليمية ومؤسسات المجتمّع المدني ومن خلال نشرات مختصة بهذا الغرض، إضافة إلى عقد مؤتمّرات متخصصة تناولت الجريمة الإلكترونية من كافة الجوانب الأمنيّة والقانونية والاجتمّاعية منها مؤتمّر الجريمة الإلكترونية عابرة للحدود والقارات ودعوة شرائح متعددة لحضور هذه المؤتمّرات وبثها عبر تلفزيون وشاشة فلسطين، إضافة الى انه قام جهاز الامن الوقائي ايضا بتطوير وحدات متخصصة في الجهاز لمتابعة قضايا الجرائم الإلكترونية وكشفها، كما أن الجهاز لم يتوانى في اتخاذ الاجراءات القانونية اللازمة من اعتقال وتحويل الضالعين بهذه الجرائم للقضاء لاخذ المقتضى القانوني بحقهم.
هـ.ق	يقوم الجهاز بتوعية الناس للاستخدام الامن لمواقع التواصل الاجتمّاعي والاجهزة الذكيه ومواقع الويب، إضافة إلى كشف واغلاق الحسابات الوهميه والمشبوهه للاشخاص الذين يعملون في مجال الاختراق والابتزاز.

خ.ح	يقوم الجهاز بحملات توعية بمختلف انواعها سواء مؤتمّرات وجاهية أو الكترونية من خلال الاعلانات الإلكترونية الممولة في مواقع التواصل الاجتمّاعي والفيديوهات التوضيحية والتوعوية على مواقع التواصل، إضافة إلى متابعة الشكاوي من المشتكين من قبل متخصصين في المجال والحرص على معاقبة المخالفين دون تهاون لردع امثالهم.
السؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظركم؟	
م. ر	تكمن دوافع ارتكاب الجريمة الإلكترونية في دوافع (مادية، دوافع شخصية (تسلية ، انتقام ، جنسية)، دوافع سياسية (منظمات، اجندات).
م.ج	دوافع ارتكاب الجريمة من قبل الجناة (دوافع مادية، دوافع شخصية، دوافع جنسية، دافع الانتقام، دافع التسلية، دوافع سياسية).
ر. م	دوافع ارتكاب الجريمة الإلكترونية من الجناة يحمل ايضا عدة نقاط واسباب منها (دافع مادي لكسب المال والثراء، دافع المتعة، دافع الرغبة في الانتقام واحداث اكبر ضرر، دافع نفسي او شذوذ، دافع الاجرام المنظم).
هـ.ق	تتمّثل الدوافع في دوافع (مالية، شخصية، سياسية).
خ.ح	هناك العديد من الدوافع لعل من أهمها: • استهانة الجناة بالعواقب لجهلهم بها بسبب حداثة قانون الجرائم الإلكترونية وتتشكل لديهم هذه الدوافع للانتقام من الضحايا بهذه الاساليب لتوهمهم بقدرتهم على التخفي وعدم قدرة جهات تنفيذ القانون من الوصول اليهم. • استهتار الضحايا وقلة وعيهم للاخذ باحتياطات الامان، إذ عليهم عدم مشاركة خصوصياتهم على المواقع من صور وغيرها وضرورة حذفها في المحادثات او الايميلات مثلا او المواقع الإلكترونية التي تمّ تخزينها عليها. • الدافع المادي، إذ يعتبرها الجناة مصدرا ماليا من خلال حصوله على أموال مقابل ما يفعله، إضافة للدوافع الانتقامية من شخصيات اعتبارية وتمّزيق سمعتها في المجتمّع.
السؤال الثالث: ما أكثر أنواع الجرائم الإلكترونية التي يتعامل معها جهاز الأمن الوقائي؟	
م. ر	اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي (جرائم الابتزاز والتشهير، جرائم النصب، جرائم التهديد، الجرائم السياسية).
م.ج	اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي (الابتزاز، النصب، التهديد، الجرائم

	السياسية)
ر. م	تعامل جهاز الامن الوقائي مع العديد من الجرائم الإلكترونية منها (جرائم ضد الافراد من انتحال شخصية وابتزاز الكتروني وسرقة معلومات شخصية وتشهير بالضحية والنصب والاحتيال، جرائم الارهاب الالكتروني، جرائم الملكية للمؤسسات من استهداف ملفات وسرقة معلومات ونشرها، الجرائم الاقتصادية والتجارة الإلكترونية الغير مشروعة من خلال العملات الإلكترونية، جرائم نشر الاشاعات وتلفيق وفبركة الاخبار، جرائم القرصنة لاتلاف المحتوى، العنف ضد الاطفال من خلال استدراج الاطفال واستغلالهم جنسيا عبر شبكات التواصل الاجتمّاعي وبرامج الالعاب).
هـ.ق	اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي (الابتزاز، التهديد، انتحال الشخصيات، سرقة معلومات، اختراق اجهزه من قبل اشخاص).
خ.ح	اكثر انواع الجرائم هي (الابتزاز للضحايا مقابل الحصول على اموال او مقابل عمل شيء معين من قبل الضحية او للانتقام من سمعته في المجتمّع).

السؤال الرابع : ما الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟	
م. ر	الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية (وجود مرتكبي الجرائم خارج الضفة الغربية مثل قطاع غزة والداخل، هذا يعني القصور في القبض عليهم، عدم امكانية تحديد مرتكبي الجرائم الذين يستخدمون شرائح الاتصال الاسرائيلية).
م.ج	الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية (استخدام شرائح الاتصال الاسرائيلية، وجود مرتكبي الجرائم خارج مناطق الضفة الغربية تحديداً مناطق الداخل).
ر. م	هناك العديد من الصعوبات التي تواجه الجهاز للحد من الجريمة الإلكترونية من هذه الصعوبات (قلة الوعي بمخاطر الجرائم الإلكترونية لدى الافراد وبعض المؤسسات التي لا تتخذ اي اجراءات حماية، استغلال التطور التكنولوجي من الجناة للتخفي واستخدام برامج ذكية في اخفاء اي دليل متعلق بهم، استخدام شبكات الاتصال الاسرائيلية في تنفيذ الجريمة الإلكترونية، الانقسام بين الضفة وغزة).
هـ.ق	من أهم الصعوبات التي تواجه الجهاز للحد من الجريمة الإلكترونية (الشرائح والاتصالات الاسرائيليه، قلت وعي الناس في استخدام التكنولوجيا).
خ.ح	الصعوبات تتمّثل في (حداثة قانون الجرائم الاكترونية الذي يترتب عليه الاستهتار من قبل الجناة لقلة وعيهم بالعواقب، ايضا استهتار الضحايا وقلة وعيهم بوجوب تأمين حساباتهم على الانترنت وعدم التعاطي مع الكل

	ومشاركة خصوصياتهم معهم، ايضا هناك صعوبة كبرى في تعقب الشرائح الاسرائيلية من قبل جهات تنفيذ القانون التي يلجأ اليها الجناة خاصة المحترفون والملمين بالامور التي تبعد عنهم الشبهات، ايضا قلة الامكانيات والخبرات مقارنة بالدول الاخرى).
السؤال الخامس : ما أهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟	
م. ر	أهم الحلول التي تساعد في الحد من الجرائم الإلكترونية (وجود عقاب رادع لمرتكبي الجرائم الإلكترونية، منع تداول واستعمال الشرائح الاسرائيلية او ايجاد الية تواصل مع هذه الشركات لتقديم المعلومات المطلوبة منهم بخصوص مرتكبي الجرائم، زيادة برامج االتوعية في المدارس والجامعات والتاكيد على مخاطرها على المجتمّع وعواقبها الاجتمّاعية، عمل خطوط دعم على صفحات مواقع التواصل الاجتمّاعي لمساعدة الاشخاص والإجابة على استفساراتهم).
م.ج	اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية (اعطاء نشرات توعوية في المدارس والجامعات وابراز مخاطرها على المجتمّع وعواقبها الاجتمّاعية واظهار ايضا عقوبة مرتكب الجريمة من ناحية قانونية، منع تداول واستعمال الشرائح الاسرائيلية).
ر. م	من اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية (نشر الوعي الذي يشكل عامل مهم واساسي، استخدام برامج حماية، عدم نشر صور وملفات هامة على مواقع التواصل او تبادل صور مع جهات غير موثوقة، وجود عقوبات رادعة واحكام عاليّة لمرتكبي الجرائم الإلكترونية).
هـ.ق	من اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية (الغاء الاتصالات الاسرائيليه، عدم التعاطي مع اشخاص مجهولين على المواقع الإلكترونية، عدم استقبال ملفات مجهوله المصدر).
خ.ح	تتمّثل الحلول في (التوعية وعدم التهاون في تطبيق القانون على الجناة، زيادة مهارات العاملين في تنفيذ القانون من خلال دورات في الدول المتقدمة).

1.5 مقدمة:

يتناول هذا الفصل مناقشة النتائج التي توصلت إليها الدراسة في ضوء النظريات المفسرة للدراسة والدراسات السابقة وذات العلاقة على النحو الآتي:

2.5 مناقشة أسئلة الدراسة:

1.2.5 مناقشة النتائج المتعلقة بالسؤال الأول: ما مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية؟

أشارت نتائج الاجابة على هذا السؤال كما بين الجدول (1.4) أنّ المتوسطات الحسابية والانحرافات المعيارية لفقرات مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية أن المتوسط الحسابي للدرجة الكليّة (3.98) وانحراف معياري (0.506)، هذا يدل على أن مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية جاء بدرجة عاليّة وبنسبة مئوية (79.8%)، فقد بينت النتائج أنّ أفراد الجهاز وحسب اختصاصهم يعملون على متابعة التحقيق في قضايا الجرائم الإلكترونية، كما يعملون على التحديث المستمّر لبرامج حماية الحواسيب تجنباً للإختراق، ومتابعة الشكاوي المُرتبطة بالجريمة الإلكترونية.

إنّ ما يؤكد ذلك ما توصلت إليه المقابلات من نتائج، إذ توصلت إلى أنّ أهم إجراءات جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تمّثلت بفحص الأنظمة الإلكترونية لدى الوزارات والمؤسسات

المختلفة، أمّا فيما يتعلق بالمدارس والجامعات تقوم وحدة خاصة بجهاز الأمن الوقائي بترتيب لقاءات مع طلاب المدارس لنشر الوعي وطريقة استخدام الانترنت الأمن ذلك للحد من الجرائم الإلكترونية كما أشار إلى ذلك الضابط (م.ر) في المقابلة، فيما أشار الضابط (م.ج) إلى قيام الجهاز باعطاء دورات ونشرات توعوية تتعلق بموضوع الجرائم الإلكترونية وإبراز أهم مخاطرها على المجتمّع، وعواقبها على مؤسسات الدولة منها التعليمية كالجامعات والمدارس وغيرها، فيما اتفق الضابط (ر. م) والضابط (هـ.ق) والضابط (خ.ح) على أنّ الجهاز مهتمّ بدرجة كبيرة في نشر الوعي والتحذير من الجريمة الإلكترونية من خلال الصفحة الرسمية للجهاز والتي تضمنت مجموعة من الإرشادات التي تحذر من الجريمة الإلكترونية.

نستنتج مما سبق أنّ مستوى الإجراءات المرتفع من قبل الدوائر المختصة بمتابعة الجريمة الإلكترونية في جهاز الأمن الوقائي من شأنها المساعدة في الحد من هذه الجرائم، لكن على المستوى العام الجريمة الإلكترونية في فلسطين في ازدياد فقد بلغت (2720) جريمة في نهاية العام (2020م) حسب آخر إحصائية (للشرطة الفلسطينية، 2021)، يعود ذلك بسبب الإستخدامات الموتفعة لشبكة الإنترنت ومواقع التواصل الاجتمّاعي كما أشرت من قبل تحديداً خلال فترة انتشار فايروس كورونا، كما ويعود السبب إلى أن المتابعة من قبل جهاز الأمن الوقائي والأجهزة الأمنيّة تتمّثل في القضايا التي تصل إلى الجهاز من قبل المواطنين، أو تلك القضايا التي يكون لدى الجهات المختصة معلومات مسبقة عنها من قبل مصادرهم الخاصة، ومع أنّ مستوى التنسيق بين الأجهزة الأمنيّة مرتفع، إلا إنّ هناك ارتفاعاً في الجرائم الإلكترونية، ويمكن تفسير ذلك بأنّ حجم النشاط الإلكتروني للأفراد في فلسطين بين ذكور وإناث مرتفع بالتالي يكون من الصعوبة السيطرة المطلقة على كافة الجرائم التي يمكن أن تحدث، فيما يمكن أن تكون بعض الجرائم سرية ولم تستطع الأجهزة الأمنيّة رصد أي معلومة تخصها،

إضافة إلى الصعوبات الخاصة بالجرائم غير الواقعة في منطقة السيطرة الفلسطينية التي تحتاج لتنسيق مسبق ويمكّن للمجرم التخلص من أدوات الجريمة قبل القبض عليه.

كما تبين أنّ الجهاز يعمل بشكل كبير لحفظ الموارد الإلكترونية الخاصة بالدولة كالمواقع الحكومية من محاولات الاختراق أو السيطرة عليها سواء الخارجية أو الداخلية، وضمان أمن عملها وخصوصية المعلومات الواردة فيها، فهذه المهمة تعد أيضاً مهمة في تأمين خصوصيات الأفراد من عبث من يحاولون السيطرة على المعلومات أو القرارات المهمة والابتزاز بها، وترتبط الإجراءات عادة بما هو متاح لهم وضمن الإمكانيات المادية والمعنوية والمعلوماتية المتوفرة لديهم في العالم أجمع، إذ لا يوجد جهاز في كافة أنحاء العالم يمكن له السيطرة المطلقة على الجريمة، أو يكون لديه القدرة على منع حدوث الجرائم الإلكترونية، لكن هناك وسائل وطرق تستخدم من أجل ضبط ومراقبة المجرمين للحد من وقوع هذه الجرائم، لذلك جاءت القوانين من أجل دعم عمل الأجهزة الأمنيّة الفلسطينية في هذا الخصوص كقرار بقانون رقم (16) لسنه (2017)، والتعديلات التي طرأت عليه في القرار بقانون رقم (10) لسنه (2018)، كل هذا يصب في الإجراءات التي يتمّ اتخاذها من قبل الجهات القضائية لتعزيز عمل الأجهزة الأمنيّة التي من ضمنها جهاز الأمن الوقائي.

هذا من جانب ومن الجانب الآخر يمكن القول إنّ انحسار عمل الأجهزة الأمنيّة في مناطق (أ) وضعف عملها في مناطق (ب) و(ج) بدرجة كبيرة، يمكن أن يساعد في هروب المجرمين إلى هذه الأماكن، وقد تكون هذه المناطق أيضاً مناطق انطلاقهم للقيام بهذه الجرائم، حينها يكون مستوى المتابعة ضعيف، إضافة إلى ذلك فإنّ وجود شبكات الاتصال الخاصة بالإسرائيليين يسهل عملية القيام بهذا النوع من الجرائم، كون هذه الشبكات لا يمكن متابعها من قبل أجهزة الأمن الفلسطينية تحديداً جهاز الأمن الوقائي، الأمر الذي يُسهم في رفع مستوى الجرائم بشكل عام، إنّ ما يؤكد ذلك نتائج

دراسة الشلالدة وربعي (2015) والتي بينت أنّ السيطرة المطلقة على أجهزة الاتصال في فلسطين تتبع للكيان الاحتلالي، الذي يمتلك السيطرة المطلقة على الشبكات حتى الفلسطينية منها كونه المصدر الأول للإنترنت في فلسطين، هذه السيطرة تعرقل من عمل الأجهزة الفلسطينية التي لا تستطيع المتابعة بالدرجة المطلوبة، إضافة لرفض الاحتلال الاسرائيلي ادخال المعدات الدقيقية التي يمكن أن تساعد الاجهزة في التعقب والمتابعة، إذ تعتبرها سلطات الاحتلال أجهزة دقيقة يمكن أن تؤثر على أمنها، إضافة لذلك أنّ التوجه نحو الشركات الأسرائيلية للحصول على شرائح منها يساعد ويسهل في ممارسة الفرد للجريمة الإلكترونية، تتفق هذه النتيجة مع نتيجة دراسة شهوان (2018) بعنوان "دور المؤسسة الأمنيّة في الحد من الجرائم المستحدثة في الضفة الغربية"، حيث بينت الدراسة أنّ هناك مستوى عالي من المتابعة من قبل الاجهزة الأمنيّة واجراءتها في مكافحة الجريمة الإلكترونية، إنّ ما سبق يوضح أن الاجراءات من قبل جهاز الامن الوقائي لمثل هذا النوع من الجرائم ومتابعتها والتدريب على مكافحتها يعود لتأثيرها على استقرار المجتمّع، وكونها تقوض دعائمه، إذ يسعى المجرمون من خلالها إلى الفتنة والسيطرة على الآخرين وسلبهم حريتهم، ذلك من خلال السيطرة على معلوماتهم الشخصية وسلبهم خصوصيتهم التي كفلها لهم القانون، هذا الاعتداء على الحقوق يحتاج إلى متابعة واهتمّام من قبل الأجهزة الأمنيّة بما فيه جهاز الأمن الوقائي الذي من مهامه توفير الأمن كما بينت دراسة (براك وجراده، 2019) بعنوان "الجرائم الإلكترونية في التشريع الفلسطيني".

يتضح مما سبق أنّ الاجراءات التي اتبعها جهاز الأمن الوقائي وقعت ضمن الامكانيات المتوفرة للأفراد العاملين في وحدة الجرائم الإلكترونية من حيث المعدات والتدريب، على الرغم من ضعف الإمكانيات إلا أنّ الأفراد بذلوا في سبيل ذلك كل إمكاناتهم المعرفية والعملية للحد من انتشار الجريمة الإلكترونية في فلسطين، فتمّكن أفراد وحدة الجرائم الإلكترونية من التحري والمراقبة وجمع المعلومات

ذات العلاقة، إضافة إلى ما استمّدوه من معلومات كان مصدرها أفراد الجهاز، إذ أسهمت تلك المعلومات فيما بعد في القبض على المجرمين، بشكل عام فقد أشارت إحصائيات الجهاز أنّ عدد القضايا التي وصلت الوحدة، وتمّ فيها إلقاء القبض على المجرمين شكلت ما نسبته (85%) من مجموع قضايا الجرائم الإلكترونية لدى الجهاز (جهاز الامن الوقائي، 2020).

وفي نفس السياق أكد المؤتمّر الامني الرابع في أكاديمية الأمن الوقائي في أريحا عام (2019) في توصياته على ضرورة العمل باستخدام كافة الاجراءات الممكنة والمتوفرة لدى الأجهزة الأمنيّة لمكافحة كافة أنواع الجرائم الإلكترونية ومتابعتها، وتتفق نتيجة هذا السؤال مع نتيجة دراسة (شهوان، 2018) بعنوان "دور المؤسسة الأمنيّة في الحد من الجرائم المستحدثة في الضفة الغربية"، والتي بينت أنّ هناك مستوى عالي من المتابعة، ويعترض ذلك مجموعة من المعوقات تحد من التطور فيما يخص الجرائم الإلكترونية كونها مستحدثة، لعل أهمها ضعف مستوى التدريب لمتابعة هذه الجرائم، وقدرة الجناة على التخفي واستخدام برامج خاصة لحذف البيانات من الحاسوب، وعدم قيام بعض الأفراد بإبلاغ الأجهزة الأمنيّة عن الجريمة التي حصلت معهم، كذلك وجود الاحتلال الذي يسهل هروب الجناة، وهو ما أكدته دراسة (الاطرش، 2018) بعنوان معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الاجهزة الأمنيّة، وكل تلك المعيقات التي من شأنها أن توفر فرصة للجاني للممارسة جريمته الإلكترونية حسب نظرية الفرصة.

2.2.5 مناقشة النتائج المتعلقة بالسؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة؟

أشارت النتائج المتعلقة بدوافع ارتكاب الجريمة الإلكترونية من قبل الجناة حسب الجدول (2.4) أنّ المتوسط الحسابي للدرجة الكليّة (3.87) والانحراف المعياري (0.421) هذا يدل على أنّ دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة جاءت بدرجة عاليّة وبنسبة مئويّة (77.5%).

كما بينت النتائج أنّ من أهم الدوافع لارتكاب هذه الجرائم، ضعف مستوى الرقابة على مواقع التواصل الاجتمّاعي لمرتكبي الجرائم الالكترونيّة ومن يُشتبه بهم التي حصلت على نسبة (87.2 %)، يليها ضعف الرقابة الأسرية على الأبناء بنسبة (85.6%) إضافة إلى وجود الدوافع الجنسية والعاطفية والسياسية بنسبة (81.8%)، إضافة إلى الدوافع المادية، هذا يعني أن الدوافع متعددة ومختلفة ولا تتعلق بالقانون فقط، حيث يتمّ تطبيق القانون على من يقومون بمثل هذه الجرائم، فهناك الكثير من الضغوطات اليومية التي يتعرض لها الأفراد في حياتهم تدفعهم لارتكاب وممارسة الجريمة الإلكترونية.

إنّ ما يؤكد ذلك ما تمّ الإشارة له خلال المقابلات، إذ يرى الضابط (م.ر) والضابط (م.ج) والضابط (هـ.ق) أن دوافع ارتكاب الجريمة الإلكترونية هي دوافع مادية وأخرى شخصية كالتسلية والانتقام والدوافع الجنسية، وأخرى سياسية لها علاقة بالمنظمات والاجندات، فيما أضاف الضابط (ر.م) دوافع الحصول على المال والكسب غير المشروع والمتعة والرغبة في الانتقام والدافع النفسي والشذوذ. أما الضابط (خ.ح) فيرى أن الاستهانه بالعقاب من أهم دوافع الجريمة الإلكترونية، كذلك استهتار الضحايا وقلة وعيهم، هذا ما توضحه نظرية الردع، إذ إن عدم وجود عقوبة رادعه لا يقلل من حدوث الجريمة، لذلك يجب الاهتمّام بفكرة انّ العقاب مهم وضروري في الجرائم الالكترونية كونها مستحدثة ويمكن بالعقاب الحد منها.

إضافة لما سبق هناك دوافع أخرى يمكن أنْ تؤدي إلى القيام بالجريمة دون معرفة بها بشكل مسبق، فعدم المعرفة بشبكة الانترنت يمكن أن تسهم في قيام الفرد ببعض أفعال تحسب في مضمونها جرائم الكترونية، كالحصول على أموال مسروقة مثلاً، أو القيام ببعض الصفقات المالية المشبوهة، أو الدخول إلى بعض المواقع السوداء، أو الوقوع ضحية لأحد النصابين، كل هذه الدوافع تساعد بشكل عام في الوصول إلى الجريمة الإلكترونية، منها ما هو مقصود ومنها ما يتسبب به الآخرون بسبب عدم المعرفة بخبايا الشبكة العنكبوتية، فيكون المجرم شريكاً أو متعاوناً دون أن يعي النتيجة النهائية.

واستناداً إلى النظريّة الاقتصادية فإنّ الاهتمّام بالمجتمّع وتوعيته وتثقيفه والحد من مستويات البطالة والفقر فيه من خلال توفير فرص عمل مناسبة للشباب العاطلين عن العمل، يساعد بشكل كبير على الحد من هذه الدوافع، فهناك دوافع تنتج عن الفراغ المحيط بالأفراد وعدم تقديره لذاته كونه لا يستطيع العمل وتلبية كافة احتياجاته اليومية، بالاضافة الى الاحباط الذي يصاحب البطالة وقلة العمل الذي يدفع الشباب إلى الانخراط في أعمال مرتبطة بالجرائم بشكل عام والجرائم الإلكترونية بشكل خاص، خاصة مع وجود وقت فراغ كبير غير مستغل في الأمور الايجابية.

أمّا فيما يخص الدوافع الجنسية والعاطفية، فقد بينت النظريّة التحليلية أنّ عدم السيطرة على الأنا بسبب ضعف المعتقدات الدينية والأخلاقية والقيم والمبادئ التي تحكم المجتمّع ككل، والاشخاص بشكل فردي يؤدي إلى التمّادي في هذه النزاعات ومحاولة إرضائها بشكل كامل، فالحاجات الجنسية والعاطفية والسلوكيات غير المرغوب بها مجتمّعياً، بحاجة إلى أساليب توعوية وتثقيفية للحد منها ذلك من خلال استضافة الخبراء والمختصين من ذوي الكفاءة والمهنية في التعامل مع مثل هذه الحالات، لتقديم العلاج اللازم والمناسب لهم للحد منها.

وفي نفس السياق فإنّ الفضاء الالكتروني ساعد في ارتفاع مستوى التواصل الاجتمّاعي بين الأفراد، كما أسهم بوجود الكثير منهم ضمن وقت واحد، هذا ساعد في التواصل بشكل مكثف للأفراد إذ يمكن الحديث مع أكثر من شخص في نفس الوقت ومن مختلف دول العالم، إنّ قرب المسافات ساعدت في إمكانية قيام الجنسين بمراسلة بعضهم البعض دون حواجز وبشكل سري، الأمر الذي أدى إلى تعزيز فرص حدوث الجرائم وارتكاب الأخطاء، إنّ اختلاف الدوافع في القيام بالجريمة الإلكترونية، يعني أنّ هناك الكثير من القيم المفقودة في المجتمّع التي تمّ نقلها إلى العالم الافتراضي، كما كانت في الواقع المعاش، وهو ما وضحته نظرية الفرصة التي بنيت وجود دوافع للقيام بالجريمة، إذ في ظل غياب تطبيق القانون وتوفر الدافع تحدث الجريمة، ففي ظل غياب الرقابة الأسرية على التواصل بين الافراد، سواء بدوافع التجارة الإلكترونية بمختلف أشكالها، أو العلاقات بين الذكور والإناث في المواقع الاجتمّاعية، فإنّ الدوافع هنا تشكل أرضية خصبة لحدوث الجريمة، فبدافع التواصل التجاري يمكن حدوث الجريمة، وبدوافع الزواج يمكن حدوث الجرائم.

وكون فلسطين تقع تحت الاحتلال فقد يكون من الصعب السيطرة المطلقة من قبل الاجهزة الأمنيّة على النظام العام، لعدم تمّكنهم من الوصول الى الكثير من المناطق، لكن المحاولات الايجابية المستمّرة التي من الممكن أن تساعد في الحد من هذه الجرائم أو العود لها تكمن في استخدام سياسية العقاب وتطبيق القانون على المجرمين، وهو ما تنص عليه نظرية الردع التي ترى بأن العقوبة الرادعه تقلل من الجرائم ذات البعد الاداتي، أي التي لها هدف يسعى المجرم لتحقيقه.

تتفق هذه النتيجة مع دراسة (الاطرش، 2018) التي بينت أن الدوافع الاجتمّاعية تسبب بشكل كبير جرائم الابتزاز الالكتروني ذلك بدوافع انتقامية من قبل الجاني، بسبب فقره او جهله أو غير ذلك من الاسباب التي أدت به لأن يكون منبوذاً في المجتمّع، كما بينت دراسة (عابدين، 2020) في دراستها

بعنوان "الذكاء العاطفي وعلاقته بممارسة جرائم الإبتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية"، إن أهم الاسباب المؤدية الى الابتزاز الالكتروني أيضاً النقص العاطفي والفراغ الذي يعيشه بعض الافراد الذين لم يحصلوا على علاقات حب مع الشريك بشكل طبيعي وبشكل عام تتفق هذه النتيجة مع منطلقات النظريّة التكامليّة (نظرية العوامل المتعددة).

3.2.5 مناقشة النتائج المتعلقة بالسؤال الثالث: ما أنواع الجرائم الإلكترونية التي تعامل معها في جهاز الأمن الوقائي؟

أشارت النتائج إلى أنّ المتوسط الحسابي للدرجة الكليّة لاستجابات أفراد عينة الدراسة على أنواع الجرائم الإلكترونية التي يتعامل معها في جهاز الأمن الوقائي (4.01)، هذا يدل على أنّ أنواع الجرائم الإلكترونية التي يتعامل معها في جهاز الأمن الوقائي جاء بدرجة عاليّة وبنسبة مئوية (80.3%)، كما وأشارت النتائج أيضاً أنّ الابتزاز بجميع أشكاله جاء بدرجة عاليّة حيث بلغت نسبته (83.4 %) في الجرائم التي تعامل معها الجهاز، كذلك سرقة الحسابات الشخصية على مواقع التواصل الاجتمّاعي بنسبة بلغت (83.4%)، وانتحال شخصية الغير بنسبة (83%)، وجرائم الإرهاب الالكتروني (الفكر المتطرف) بنسبة (82.2%)، أما أقل الجرائم فكانت الوصول للمواقع المشفرة الممنوعة بطرق غير مشروعة بنسبة (78.4%)، والتنصت على الغير بنسبة (77%)، واستغلال الأطفال جنسياً بنسبة (73.8%).

في حين أشارت نتائج المقابلات كما عبر عنها الضابط (م.ر) والضابط (م.ج) والضابط (هـ.ق) والضابط (ح.خ) إلى أنّ أنواع الجرائم التي تعامل معها الجهاز تمّثلت في جرائم الابتزاز المالي والجنسي بدرجة كبيرة، تلك الجرائم التي تعتمّد على الضغط والتشهير بالضحية من خلال الحصول على المعلومات الخاصة بها، التي يتمّ الاحتفاظ بها في جهاز الحاسوب، إضافة الى وجود أنواع أخرى من التشهير كالتشهير السياسي الذي يمس بعض الشخصيات ويكون متعلقاً بمواقفهم المختلفة،

إضافة الى ذلك هناك جرائم الكترونية اقتصادية كما بينت النظريّة الاقتصادية إذ تعتمّد على سرقة المال من خلال السيطرة على بطاقات الائتمّان، حيث تبين أن هذا النوع قليل الحدوث في فلسطين، فيما أضاف الضابط (ر.م) جرائم اخرى تعامل معها الجهاز كالانتحال الشخصي وجرائم الارهاب الالكتروني، ونشر الاشاعات والقرصنة والعنف ضد الاطفال.

نستنتج مما سبق أن جرائم التهديد والابتزاز تشكل أول الجرائم التي تعامل معها الجهاز، وهي من الجرائم التي تنتشر بدرجة كبيرة في المجتمّعات التي من بينها المجتمّع الفلسطيني، ويمكن ايعاز ذلك إلى الحالة التي يعاني منها المجرم الذي يقوم بعملية الابتزاز، تلك الحالة النابعة من الدونية التي يعيشها أو من الظلم الذي وقع عليه من بعض الفئات أو بسبب الغرائز التي تسيطر عليه، إضافة للبطالة وتفشي حالة الفقر ووجود الاحتلال وضعف مستوى العمل وغيرها من الأسباب المجتمّعية التي تؤدي بالفرد الى التوجه نحو الجريمة والانحراف، يمكن تفسير هذه النتيجة ضمن نظرية العوامل المتعددة (النظريّة التكاملية) التي تبين أنّ الجريمة الإلكترونية تنشأ من تظافر مجموعة من العوامل المختلفة.

4.2.5 مناقشة النتائج المتعلقة بالسؤال الرابع: ما الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية؟

أشارت نتائج الدراسة أنّ مستوى الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية جاءت بدرجة عاليّة وبنسبة مئوية (76.9%)، حيث بلغ المتوسط الحسابي للدرجة الكليّة (3.84)، كما تبين من النتائج ان اهم الصعوبات تمّثلت في صعوبة تعقب شرائح الإتصالات الإسرائيلية المُستخدمة في إرتكاب الجريمة الإلكترونية، ثم تكتمّ الضحية تعرضها للجريمة الإلكترونية

خوفاً من الفضيحة عند التبليغ، فيما تبين أنّ مستوى الكادر العامل مع الجريمة الإلكترونية ذو إمكانيات متوسطة.

وأمّا نتائج المقابلات فأكدت أنّ أهم الصعوبات كما أشار لها الضابط (م.ر) تتمثّل في وجود مرتكبي الجرائم خارج الضفة الغربية، مثل قطاع غزة والداخل وبالتالي لا يمكن القبض عليهم، في حين أشار كل من الضابط (م.ج) والضابط (هـ.ق) إلى أن أهم الصعوبات تكمن في عدم امكانية تحديد مرتكبي الجرائم الذين يستخدمون شرائح الاتصال الإسرائيلية، واستغلال التطور التكنولوجي من الجناة للتخفي واستخدام برامج ذكية في اخفاء اي دليل متعلق بهم، فيما أضاف الضابط (ر.م) صعوبات لها علاقة بقلة الوعي بمخاطر الجرائم الإلكترونية، والاحتلال الإسرائيلي، إضافة إلى الانقسام بين الضفة وغزة الذي عزز الجريمة الإلكترونية.

وكون الحالة الفلسطينية تخضع لظرف خاص فيما يتعلق بالجرائم الإلكترونية، إذ إنّ وجود فلسطين تحت الاحتلال الإسرائيلي يعرقل العمل الأمني، فالسيطرة الأمنيّة على المناطق الفلسطينية محدودة، ووجود الشرائح الخاصة بالشركات الإسرائيلية التي لا تستطيع الأجهزة الأمنيّة الفلسطينية تعقبها تساعد بشكل كبير في قيام المجرمين باستخدامها في تضليل الأجهزة الأمنيّة وفي استدراج الضحايا، إضافة لتوفر خدمة إخفاء الرقم المتوفرة لدى الشرائح الخاصة بالإتصالات الإسرائيلية، وعليه تصبح مهمة التعقب والمراقبة من قبل الوحدات الخاصة بالجرائم الإلكترونية صعبة للغاية.

أضف إلى ذلك إنّ خوف الضحية من الفضحية وإخفاءها المعلومات عن الأجهزة الأمنيّة يؤدي الى استمّرار استغلال الضحية من قبل المجرم ويقلل من فرص القبض عليه، باعتبار أنّ أدلة الجريمة سيتمّ اخفاؤها من قبل المجرم مع الوقت، وهنا تصبح الضحية بلا دليل ولا تستطيع الجهات الأمنيّة المختلفة ايقاع العقوبة بالمجرم أو حتى اتهامه بالجرم، وفي نفس السياق أيضاً فإنّ كثيراً من المجرمين

يهربون إلى داخل الأراضي الإسرائيلية التي لا سيطرة للأجهزة الأمنيّة الفلسطينية عليها، فيصبح من الصعب عليهم المتابعة ويؤدي ذلك إلى هروب المجرم وبقاء الضحية دون استعادة لحقوقها، إضافة لذلك ما أشار إليه بعض الضباط خلال المقابلات التي أجريت معهم، حيث هناك من يقوم بالتخفي الإلكتروني من خلال البرامج التي تعمل على تغيير ما يطلق عليه (IP)، هذا التخفي يقلل من فرص الملاحقة والمتابعة لهم، بهذا لا يمكن السيطرة عليهم أو اثبات التهم عليهم، يمكن تدعيم هذه النتيجة من خلال نظرية الوصم، التي ترى أنّ الضحية وخوفاً من الفضيحة لا تتحدث عما يحصل معها لا بل بالعكس ترضى بكل ما يحصل معها مقابل عدم الفضحية.

أمّا فيما يخص التدريب وقدرة العناصر على المتابعة، فهناك ضعف بسيط في قدرة الكادر على المتابعة والعمل من النواحي التقنية، إذ إنّ الكادر لديه القدرة على المتابعة اليومية والسيطرة في حال كانت منطقة الضحية ضمن نطاق عمل الأجهزة الأمنيّة، وهو ما توافق مع ما توصلت إليه دراسة (العتيبي، 2016) بعنوان "دور التحريات والبحث الجنائي في الكشف عن الجرائم المعلوماتية"، حيث توصلت الى أنّ هناك حاجة لتعزيز مستوى التحري، ورفع قدرة افراد الاجهزة الأمنيّة في الدوائر الإلكترونية واطلاعهم باستمّرار على كل المستجدات في مجال الجريمة الإلكترونية ليكونوا على اطلاع كامل وعلى جهوزية مطلقة، كذلك ما توصلت اليه دراسة (Williamson, 2014) بعنوان "التحديات التي تقلل من ضبط مجرمي الانترنت"، التي توصلت إلى أنّ هذا النوع من الجرائم يحتاج إلى دراسة معمقة ومستمّرة بشكل يومي للحد من هذه الجرائم، كونه يعتمّد على الذكاء الاصطناعي وعلى القدرات الخاصة بالافراد فيما يتعلق بالتخفي واستخدام الطرق الحديثة في البرمجة التي تقلل من مستوى التعقب.

كما ويرى بعض ضباط الجهاز أنّ غياب الوعي والثقافة الإلكترونية لدى كثير من الافراد في المجتمّع يشكل أيضاً صعوبة من الصعوبات التي تواجه العمل، إنّ غياب الوعي لدى الأفراد الضحايا يؤدي إلى عدم مساعدة رجال الأمن في الكشف عن المجرم، فالضحية في غالبية الأحيان تعمد الى إخفاء ذلك خوفاً أو جهلاً، إضافة لما سبق إن ارتفاع مستوى الثقة بالآخرين والحديث معهم بشكل مطلق في أمور خاصة وإرسال الرسائل والمعلومات والصور الخاصة لهم يسهم في ارتفاع مثل هذه الجرائم، لذلك فهم يتفقون على أن العمل في مجال الجريمة الإلكترونية يحتاج الى الكثير من الصبر والجهد والصلاحيات ليتمّ على أكمل وجه ويتمّ الحد من مستوى الجريمة، إن ما يؤكد النتيجة السابقة ما توصلت اليه دراسة (شهوان، 2018) بعنوان دور المؤسسة الأمنيّة في الحد من الجرائم المستحدثة في الضفة الغربية، التي توصلت إلى أنّ مستوى الوعي مهم في الحد من الجرائم الإلكترونية، إذ يساعد على رفع مستوى الحذر لدى الأفراد ويقلل من مستوى سيطرة المجرم عليهم.

كما اتفقت الصعوبات في مجملها مع ما أشار له (مطر، 2014) من كون الاحتلال الاسرائيلي من أهم الصعوبات التي تقيد حركة الأمن الفلسطيني في مواجهة الجريمة الإلكترونية، إذ لم يسمح الاحتلال بوجود معدات واجهزة يمكن ان تسهم في متابعة المجرمين في الجرائم الإلكترونية، كذلك فيما يخص النواحي القانونية وعدم وصول فلسطين إلى أنّ تمّتلك قانوناً يمكن أن يكون نافذاً ومحققاً لكل ما يحتاجه المواطن الفلسطيني لتجنب التعرض للجرائم الإلكترونية، كذلك ما يخص الجهل لدى الأفراد فيما يتعلق بالجرائم الإلكترونية والكشف عنها حال وقوعهم فيها، كل ذلك يسبب المزيد من التعقيدات والصعوبات التي تؤثر في تفكيك الجريمة الإلكترونية والسيطرة عليها والحد منها.

5.2.5 مناقشة النتائج المتعلقة بالسؤال الخامس: ما أهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟

أشارت النتائج إلى أنّ أهم الحلول التي تساعد في الحد من الجريمة الإلكترونية والمقترحة جاءت بدرجة عاليّة وبنسبة مئوية (87%)، إذ بلغ المتوسط الحسابي للدرجة الكليّة (4.34)، حيث تبين إن من أهم الحلول المقترحة (العمل على تنظيم برامج توعويّة حول مخاطر الجريمة الإلكترونية، تجنب فتح أي رسائل إلكترونية مجهولة المصدر، رفع مستوى الرقابة الاسريّة على الأبناء، التعاون المشترك مع المؤسسات المحليّة المعنية للحد من الجرائم الإلكترونية، عدم نشر صور وملفات هامة على مواقع التواصل أو تبادل صور مع جهات غير موثوقة)، في حين أشارت نتائج المقابلات إلى أنّ أهم الحلول كما أشار لها الضابط (م.ر) تتمّثل في ضرورة تطبيق القانون على الجناة وزيادة مهارات العاملين في تنفيذ القانون من خلال دورات في الدول المتقدمة، والحد من عمل شركات الاتصال الإسرائيلية في الأراضي الفلسطينية، في حين أشار كل من الضابط (م.ج) والضابط (ر.م) بضرورة رفع مستوى التوعية في المدارس والجامعات لخطر الجريمة الإلكترونية من خلال ندوات ومؤتمّرات وورش عمل، في حين يرى الضابط (هـ.ق) ضرورة الغاء التعامل بالشرائح الاسرائيلية في الاراضي الفلسطينية، وعدم التعاطي مع اشخاص مجهولين على مواقع التواصل الاجتمّاعي.

إضافة لما سبق إنّ من أهم الحلول رفع مستوى الأفراد لمواجهة سياسات الاحتلال بطرق ذكية ومبتكرة، ومواكبة التطورات المتسارعة في عالم الجرائم الإلكترونية من خلال التدريب المستمّر للضباط المتخصصين في هذا المجال، وتوفير كل ما يلزم من أجهزة ومعدات حديثة متخصصة، وتعزيز الدوائر المتخصصة بالكوادر البشرية، وتعزيز التنسيق والتعاون مع بقية أذرع المؤسسة الأمنيّة الفلسطينية، وتكثيف جهود التوعية الجماهيرية في إطار الإجراءات الوقائية الهادفة لمحاصرة الجرائم الإلكترونية.

وعليه فالحلول تقتضي تطوير إجراءات وقائية كافية تعمل على حصار دوافع الجناة في مهدها قبل تحولها لسلوك جرمي، هذا الأمر يحتاج لتنسيق وتعاون مع بقية أذرع المؤسسة الأمنيّة الفلسطينية، وبقية الدوائر ذات العلاقة في السلطة الوطنية الفلسطينية كالجامعات وبعض الوزارات خاصة التربية والتعليم ومراكز الأبحاث المتخصصة وهيئة الإذاعة والتلفزيون وغيرها، إذ يسهم كل ذلك في بناء دوائر خاصة بمحاربة الجريمة الإلكترونية ذات امكانيات عاليّة، وذات توجهات ثابته وقدرات كبيرة، تؤدي في النهاية الى السيطرة بنسبة كبيرة على الجرائم الإلكترونية وخلق جو من الأمان للافراد في المجتمّع من خلال تأمين الحرية والحقوق الخاصة بحياتهم الشخصية ومنع المجرمين من الوصول اليها، أو السماح لهم من السيطرة على الضحية.

إنّ ما سبق يوضح لنا أنّ الحلول المقترحة هي حلول ممكنة وواقعية، إذ يمكن استخدامها وتطبيقها لتحقيق مستوى متقدم في الحد من الجريمة، فتحقيق مستوى عالي من الوعي يساعد على اخذ الحيطة والحذر من التعامل غير المدروس مع الشبكة العنكبوتية والتعامل مع الأفراد الذين يتمّ التعرف عليهم للمرة الأولى بما يتناسب مع ما يريدون، كذلك توعية الأفراد في المجتمّع من خلال دروس توعية الكترونية في التلفاز والنشرات والندوات بعدم فتح الملفات المشبوهه وعدم استقبال الرسائل مجهولة المصدر، أيضاً فيما يخص التعاون مع المؤسسات المختلفة فهناك ضرورة ملحة في بناء قاعدة بيانات مشتركة بين المؤسسات المختلفة التي تقدم التوعية والنشاطات الثقافية الإلكترونية.

وعلى صعيد تعزيز مستوى الأفراد من الأجهزة الأمنيّة والعاملين في مجال الجريمة الإلكترونية، فهم بحاجة إلى دورات مستمّرة بشكل دائم ليكونوا على اطلاع على آخر ما يستجد من برامج يمكن استخدامها من قبل المجرمين في التخفي أو في استدراج الضحية، إذ ركزت الكثير من الدراسات على ضرورة تدريب الكادر العامل في الجريمة الإلكترونية بشكل دائم، كما في دراسة كل من (شهوان،

2018) و(الاطرش، 2018)، كذلك بينت دراسة (عبد الباقي، 2018) بعنوان التحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة الرقمية، أنّ هناك نقص في المهارة الفنية المطلوبة للتحقيق في هذه الجرائم، يعود ذلك إلى الحاجة إلى التدريب والتأهيل المستمّر للكوادر في الدول المتقدمة ممن لديها دراية واسعة بالتكنولوجيا مثل روسيا والهند والصين وأمريكا، حيث يساعد تدريب الكادر رفع مستوى خبراتهم في تحديد هوية المجرم واثبات التهم عليه.

أمّا فيما يخص الشبكات الإسرائيلية، فقد يكون من الصعب منعها بشكل كامل في الأراضي الفلسطينية، إلا أنّ محاربتها والتقليل منها قدر الامكان يساعد في الحد من الجريمة كونها تستخدم بدرجة كبيرة في مثل هذه الجرائم وكونها لا تسجل باسم الشخص الذي يستخدمها، أيضاً يمكن التخلص منها في نفس اللحظة مما يعني صعوبة تعقبها، كما أنّ على الأفراد الاهتمّام بعدم التعاطي مع الأرقام المجهولة أو الأرقام المخفية كونها مجهولة المصدر.

وعليه فإنّ الحلول المقترحة من قبل ضباط جهاز الأمن الوقائي فيما يخص الجريمة الإلكترونية هي قابلة للتطبيق، ويمكن العمل على تعزيزها على أرض الواقع بدءاً من التوعيه للمواطنين وانتهاء بالدورات التدريبية للافراد، ذلك في سبيل الحد من الجرائم الإلكترونية في العالم الجديد الذي بدأ افتراضيا، وأصبح حقيقياً لدى جميع فئات المجتمّع (صغير وكبير) (رجل وإمرأة) (متعلم وجاهل) فالجميع يتعامل معه بشكل يومي.

3.5 مناقشة نتائج فرضيات الدراسة:

1.3.5 نتائج الفرضية الأولى: "لا توجد فروق ذات دلاله إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الجنس".

يتبين أنه لا توجد فروق في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الجنس، بذلك تمّ قبول الفرضية الأولى، يمكن تفسير هذه النتيجة بأنّ الضباط من الذكور والاناث لديهم نفس التصورات فيما يخص الاجراءات المتبعة، فالأوامر تصدر للجميع من نفس المصدر، وعليه يكون تنفيذ التعليمات من قبل الجميع بشكل متساوٍ، لذلك فإنّ التعامل مع هذا النوع من الجرائم لدى العاملين من كلا الجنسين يسير في نفس الإتجاه تحديداً فيما يخص إجراءات التعامل مع تلك الجرائم الإلكترونية باعتبارها جرائم تمّس بأفراد المجتمّع والواجب حمايتهم من قبل الجهاز.

ويرى الضباط من الجنسين أنّ هناك خطورة للجرائم الإلكترونية بأنواعها المختلفة، كونها تضعف الروابط المجتمّعية، وتؤسس لخطر انتشار السرقة والتشوية والابتزاز والاحتيال وغيرها من الجرائم، وتؤدي للابتعاد عن المنظومة الاخلاقيّة والقيميّة التي بُني عليها المجتمّع العربي الفلسطيني، فاستغلال أسرار الافراد ومحاولة سرقتها والمقايضة عليها، يعد أمر مشين وخارج عن الأعراف والقانون، وباعتبار البعد الاخلاقي اهم ما تسعى الاجهزة الأمنيّة الى ترسيخه في المجتمّع لتعزيز صموده، فإنها تعمل على تعزيز المواطنة، والحد من انتشار مثل هذه الجرائم، وهذا يتفق عليه الجنسين الذكور والاناث، ويستمّعون إليه من قادتهم، ويحصلون عليه في التدريبات الخاصة بهم.

2.3.5 نتائج الفرضية الثانية: "لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة(α ≤ 0.05) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير المؤهل العلمي".

أشارت النتائج إلى أنّه لا توجد فروق دالة إحصائياً في مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير المؤهل العلمي، بذلك تمّ قبول الفرضية الثانية، يمكن تفسير هذه النتيجة أن الاجراءات التي يستخدمها الجهاز ذات أبعاد ثابته كونها تصدر من الجهات العليا، وأيضاً تحكمها قواعد عامة، فلا يمكن لأفراد الجهاز تجاوزها بدرجة كبيرة، إضافة الى كون العاملين في الدائرة من ذوي التخصصات المتشابهة ذات العلاقة بالحاسوب والانترنت، والبرامج المتعلقة بها، بالاضافة الى أن عامل الخبرة الطويلة في نفس المجال له دور مهم في تقليص الفجوة المتعلقة باختلاف المؤهل العلمي، حيث يكتسب العاملون في دوائر مكافحة الجريمة الإلكترونية مهارات خاصة بطبيعة العمل حتى وان اختلفت مؤهلاتهم العلمية، إضافة إلى ان هناك قانون يحكم العمل في الدائرة الإلكترونية لا يمكن تجاوزه تبعا لاختلاف التخصص أو المؤهل أو أي متغير آخر، اضافة لتلقي الضباط لتدريب مهني متخصص واحد للجميع دون التمّييز بين العاملين في نفس الحقل.

3.3.4 نتائج الفرضية الثالثة: "لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α ≤ 0.05) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير العمر".

أشارت النتائج إلى أنّه لا توجد فروق دالة إحصائياً في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير العمر، بذلك تمّ قبول الفرضية الثالثة، يمكن تفسير ذلك بأنّ الدائرة الإلكترونية هي من الدوائر الفتية، لذلك فإنّ أغلب العاملين فيها متقاربين على

المستوى المهني وعلى مستوى التجارب والخبرات من ناحية التعامل مع الجرائم الإلكترونية، حيث لا أهمية للعمر فيما يخص الاجراءات التي يتمّ اتباعها في جهاز الامن الوقائي الخاصة بالجرائم الإلكترونية، فتلك الاجراءات يجب ان تكون بمستوى عالي بغض النظر عن عمر من يقوم بها من العاملين في الجهاز، لذلك لا يشكل العمر فارقاً، فالفارق هنا هو مستوى وحجم الاجراءات المتبعة التي يجب ان تكون عاليّة من أجل التمّكن من الحد من الجرائم الإلكترونية.

4.3.5 نتائج الفرضية الرابعة: "لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتبة العسكرية".

أشارت النتائج إلى أنّه لا توجد فروق دالة إحصائياً في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتبة العسكرية، بذلك تمّ قبول الفرضية الرابعة، يمكن تفسير هذه النتيجة بأنّ تفاوت الرتب العسكرية لا يؤثر على طريقة العمل فيما يخص اجراءات القبض والتحقيق والمتابعة للجرائم الإلكترونية، فهذا التسلسل في العمل يتشكل من خلال العمل المستمّر في الدائرة ومن خلال القضايا وتنوعها في هذا المجال، سواء كانت قضايا تزوير أو قضايا ابتزاز أو مراقبة أو سرقة بيانات أو غيرها من القضايا التي يستخدم فيها الحاسوب كوسيلة للسيطرة على الضحية.

بالإضافة إلى أنّ هرمية الرتب العسكرية في المؤسسة الأمنيّة الفلسطينية ذات مميزات إدارية ومالية في الأساس ولا تخضع للتراتيبية العسكرية الصارمة بالضرورة كما هو الحال في الجيوش النظامية، فهي أكثر مرونة، بالتالي يبدو من المنطقي عدم وجود فروق ذات دلالة إحصائية في مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتب العسكرية

التي تشكل طموحا للوصول لمسميات وظيفية أعلى، هذا يبين أن الرتبة لا تلعب دوراً مهماً في مستوى الإجراءات المتبعة في مواجهة الجرائم الإلكترونية، إذ من الممكن وجود ضباط صغار الرتب لديهم من الكفاءة والمهنية أعلى من أصحاب الرتب العليا.

5.3.5 نتائج الفرضية الخامسة: "لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير عدد سنوات الخدمة".

أشارت النتائج إلى أنّه لا توجد فروق دالة إحصائياً في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير عدد سنوات الخدمة، بذلك تمّ قبول الفرضية الخامسة، يمكن تفسير ذلك التوافق في الآراء باختلاف سنوات الخبرة إلى أنّ أغلب الكادر له سنوات خدمة متقاربة في هذا المجال، كون الدوائر الخاصة بالجرائم الإلكترونية حديثة من حيث النشأة، إذ إنّ ظهورها في فلسطين متاخر، وجاءت بشكل كبير بعد انتشار مواقع التواصل الاجتمّاعي، واستخدام الهواتف المحمولة، حيث لم تكن قبل ذلك الا حالات بسيطة قد لا تذكر، لكن وبسبب التطور التكنولوجي المتسارع في بداية القرن الواحد والعشرين الذي أسهم في ظهور منصات مختلفة وانتشار الهواتف ذات الكميرات بجودة عاليّة، الأمر الذي ساعد في انتشار الصور على مواقع التواصل الاجتمّاعي أو الاحتفاظ بها في الهواتف التي قد تتعرض للسرقة أو للتجسس من قبل بعض المجرمين ذوي الميول المختلفة مما يسهم في زيادة حدوث مثل هذه الجرائم، فعامل سنوات الخدمة ليس حاسماً في تحديد مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية، حيث أن الامر الحاسم هو عمليات التدريب المستمّر والاطلاع على ما هو جديد في ميدان الجرائم الإلكترونية من حيث اختلاف الاسباب والدوافع حسب المجتمّعات وثقافتها المختلفة.

6.3.5 نتائج الفرضية السادسة: "لا يوجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α ≤ 0.05) في المتوسطات الحسابية لاجابات المبحوثين حول مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي".

أشارت النتائج إلى أنّه لا توجد فروق دالة إحصائياً في مستوى الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي، بذلك تمّ قبول الفرضية السادسة، تشير هذه النتيجة إلى أن هناك توافق في الإراء حسب طبيعة العمل في الجهاز، ذلك كون العاملين في الجهاز لديهم نفس الاطلاع على هذه القضايا والجرائم الإلكترونية ذات الطبيعة والأهداف الواحدة، ومرتكبيها عادة لديهم سجل جرمي، فكون الشخص الذي يسرق في الواقع يمكن له البحث عن السرقة من خلال الشبكة العنكبوتية، والذي يبحث عن الابتزاز سواء للذكور أو الإناث في الحياة اليومية أيضاً يمكنه أن يبحث عنها في الشبكة العنكبوتية، لذلك جاءت الآراء ثابته لدى العاملين في الجهاز، كون الحدث معروف لديهم ومروا بقضايا مشابهة وكانت الاجراءات الخاصة بهذا الموضوع ذاتها.

بالإضافة إلى أنّ طبيعة العمل المتخصص الدقيق في مجال مكافحة الجرائم الإلكترونية يعمل على إعادة صقل قيم ومعارف ومهارات الضباط العاملين فيه مهما كانت طبيعة عملهم السابق في الجهاز، بالتالي يخلق معايير مهنية جديدة موجودة لديهم، هذه المعايير تستفيد من طبيعة العمل السابق وتعمل على توظيفها في منظومة العمل الجديد، بالاضافة لذلك الاهنمام المتزايد من قبل الجهاز بعمليات التدريب المستمّر لكافة الضباط العاملين في الجرائم الإلكترونية، على سبيل المثال أن جميع العاملين في وحدة الجرائم الإلكترونية رغم إختلاف دوائرهم وأقسامهم داخل تلك الوحدة إلا أنهم يعملون تحت

موضوع واحد الا وهو الجرائم الإلكترونية التي تحتاج الى مستوى عالي من الاجراءات لمواجهتها من قبل جميع العاملين بغض النظر عن طبيعة عملهم داخل وحدة الجرائم الإلكترونية.

4.5 ملخص النتائج:

أشارت نتائج الدراسة إلى:

- أنّ مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية مرتفعة، وجاءت بنسبة (79.8%).
- أنّ القدرات التكنولوجية لدى جهاز الأمن الوقائي مرتفعة حيث حصلت على نسبة بلغت (82.8%)، إذ يعمل الجهاز على تحديث البرامج بشكل مستمّر لمنع الاختراق.
- أنّ هناك متابعة حثيثة من قبل جهاز الأمن الوقائي للشكاوى الواردة إليه فيما يخص الجرائم الإلكترونية، حيث يتمّ تقديم تغذيّة راجعة حسب نوعها، حيث جاء ذلك بنسبة مرتفعة بلغت (82.4%).
- أنّ دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة حصلت على نسبة مرتفعة إذ بلغت نسبتها الكليّة (77.5%)، كان من بين تلك الدوافع ضعف مستوى الرقابة على الابناء من قبل الوالدين، كذلك ارتفاع الدوافع الجنسية والعاطفية والمادية لدى الجناة.
- أن هناك ضعف فيما يخص الرقابة على مواقع التواصل الاجتمّاعي من قبل الحكومة الفلسطينية لمرتكبي الجرائم الإلكترونيّة أو المُشتبه بهم، حيث حصلت على درجة مرتفعة بلغت نسبتها (87.2%).

- أنّ أنواع الجرائم الإلكترونية التي تعاملت معها وحدة الجرائم الإلكترونية في جهاز الأمن الوقائي تتمّثل في الابتزاز والسرقة والانتحال وغيرها من الجرائم، وجاءت بدرجة عاليّة بلغت (80.3%).
- أنّ الابتزاز بكافة أشكاله جاء بدرجة مرتفعة حيث بلغت (83.4%).
- أنّ الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية جاءت بدرجة عاليّة، حيث بلغت الدرجة الكليّة لها (76.9%)، وكان من أهم تلك الصعوبات تعقب الشرائح الاسرائيلية، إذ جاءت هذه الصعوبة بنسبة (88.8%).
- أنّ أهم الحلول التي تساعد في الحد من الجريمة الإلكترونية تتمّثل في تنظيم برامج توعويّة حول مخاطر الجريمة الإلكترونية، وتجنب فتح أي رسائل إلكترونية مجهولة المصدر، ورفع مستوى الرقابة الاسريّة على الأبناء، وجاءت هذه الحلول بدرجة كليّة (87%)
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تبعا لمتغيرات الدراسة (الجنس، المؤهل العلمي، العمر، الرتبة العسكرية، سنوات الخدمة، طبيعة العمل في جهاز الأمن الوقائي).

5.5 توصيات الدراسة:

تتمثل توصيات الدراسة بما يلي:

- رفع مستوى الإجراءات الخاصة بالجريمة الالكترونية من خلال التنسيق مع الأجهزة الأمنية الاخرى، ذلك للحد من الجرائم الالكترونية.
- الاهتمّام بمواكبة التطورات المختلفة المتعلقة بالتطور التكنولوجي في مجال الجريمة والأمن والحصول عليها كونها تسهم في الحد من الجريمة ومتابعتها حال وقوعها بشكل أسرع.
- ضرورة التعاون والتشبيك بين الوحدات الخاصة بالجرائم الإلكترونية في الاجهزة الفلسطينية المختلفة بشكل مستمّر، ذلك لبناء جسم موحد يستطيع الكشف عن الجرائم الإلكترونية بمجرد الابلاغ عنها.
- ضرورة أن يتمّ التعميم على المواطنين بضرورة تقديم الشكاوى كون هذا يسهم في حمايتهم من التعرض للجرائم الالكترونيّة.
- ضرورة حثّ الأهالي على مراقبة أبنائهم بشكل مستمّر، ووضع برامج حماية لمنع فتح المواقع المّضرة، إضافة إلى مراقبة الأبناء على صفحات التواصل الاجتماعي.
- ضرورة الاهتمّام برفع مستوى الرقابة على المواقع الاجتمّاعية المختلفة من قبل الحكومة لمرتكبي الجرائم الإلكترونية أو المُشتبه بهم، دون ان يمس ذلك بالخصوصية الشخصية.
- ضرورة التشديد من قبل المشرع الفلسطيني على رفع عقوبة الابتزاز، حتى تشكل العقوبة رادعاً لكل من تسول له نفسه محاولة ابتزاز المواطنين.

- ضرورة التعاون بين المواطنين والاجهزة الامنية في التصدي للجرائم الالكترونية كون الظروف تحديدا الاحتلال تشكل عائقا أمام تمّكّن الاجهزة الامنية من القبض على كل مرتكبي الجرائم الالكترونية.
- ضرورة الاهتمّام بتعزيز وحدة الجرائم الإلكترونية في جهاز الأمن الوقائي، ذلك بتدريب العاملين فيها ورفع عددهم، وتزويدهم بالمعدات التكنولوجية الحديثة في مجال مكافحة الجريمة الإلكترونية.
- الاهتمّام بدراسة الأسباب المؤدية لانتشار جرائم الابتزاز والسرقة والانتحال بشكل كبير في المجتمّع الفلسطيني، وتقديم الحلول المناسبة لها بما يتناسب مع الوضع الفلسطيني، ويتوافق مع قدرات الأجهزة الأمنيّة الفلسطينية.
- العمل مع شركات الاتصالات الفلسطينية على تخفيض أجور المكالمات وحزم الانترنت لضمان عدم لجوء الأفراد لاستخدام وسائل الاتصال الاسرائيلية، ذلك للحد من ارتكاب الجرائم الإلكترونية من خلالها.
- القيام بمزيد من الدراسات والابحاث حول الجريمة الإلكترونية بدراسة تشمل الأجهزة الأمنيّة في فلسطين، ودورها في الحد من انتشار الجريمة الإلكترونية، إضافة للقيام بدراسات خاصة بالجريمة الإلكترونية من خلال دراسة الدوافع النفسية والاقتصادية كمتغيرات تساعد في حدوث الجريمة الإلكترونية.

قائمة المصادر والمراجع:

أولاً: القرآن الكريم

ثانياً: القوانين:

- قانون رقم (10) لسنة (2018) قانون الجرائم الإلكترونية المعدل.
- قانون رقم (16) لسنة (2017) قانون الجرائم الإلكترونية.
- قانون رقم (8) لسنة (2005) قانون قوى الأمن الفلسطينية.
- القرار بقانون بشأن الأمن الوقائي رقم (11) لسنة (2007)، المنشور في الوقائع الفلسطينية، عدد (74)، المؤرخ بتاريخ 2008/6/9.
- المرسوم الرئاسي رقم (12) لسنة (2002)، القاضي بإلحاق قوات الشرطة وقوات الأمن الوقائي والدفاع المدن بوزارة الداخلية.

ثالثاً: المراجع العربية:

- ابن منظور، محمد (1990). **لسان العرب**، بيروت: دار صادر للطباعة والنشر.
- أمحمدي، فاطمة (2006). **الدراسات الاستراتيجية والأمنيّة**، الجزائر: جامعة قسنطينة.
- بحري، صابر، وخرموش، منى (2021). أهم الدوافع السيكولوجية وراء الجريمة الالكترونية، **مجلة دراسات في سيكولوجية الانحراف**، مجلد(6)، عدد(1)، ص ص (36-59).
- البداينة، ذياب (2014). **الجريمة الإلكترونية- المفهوم والاسباب**، ورقة مقدمة في الندوة العلمية الجرائم المستحدثة في المتغيرات والتحولات الاقليمية والدولية، عمان: الجامعة الاردنية.
- البداينة، ذياب والخريشا، رافع (2013) **نظريات علم الجريمة**، ط1، عمان: دار الفكر للنشر والتوزيع.

- براك، أحمد وجراده، عبد القادر (2019). **الجرائم الإلكترونية في التشريع الفلسطيني**، رام الله: دار الشروق للنشر والتوزيع.
- البيانوني، محمد (2008). تنمية الحس الأمني عند المسلم ضرورة حتمّية، **مجلة الامن**، كليّة الملك فهد، العدد (1)، ص ص 49-69.
- الجبور، محمد (2010). **الوسيط في قانون العقوبات– القسم العام**، عمان: دار وائل للنشر والتوزيع.
- جهاز الامن الوقائي (2020)، إحصائيات الجرائم الإلكترونية، رام الله: الإدارة العامة للأمن الوقائي.
- الجهاز المركزي للإحصاء الفلسطيني(2019) **مسوحات الاسرة**، رام الله: منشورات الجهاز المركزي للاحصاء الفلسطيني.
- الجهيني، مازن والجهيني، محمد (2006). **بروتوكولات وقوانين الانترنت**، ط1، الاسكندرية: دار الفكر الجامعي للنشر والتوزيع.
- حسنية، أحمد (2017). الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، **مجلة جامعة الازهر**، غزة، مجلد(19) (عدد خاص)، ص ص (1-42).
- الحميدان، عايد (2003). **الاتجاهات الحديثة في التوعية الوقائية، ندوة الاتجاهات الحديثة في توعية المواطن بطرق وأساليب الوقاية من الجريمة**، الرياض: أكاديمية نايف العربية للعلوم الأمنيّة.

- الخطاطبة، إبراهيم (2013). **إصلاح القطاع الأمني في السلطة الوطنية الفلسطينية من وجهة نظر العاملين فيها وأثر ذلك على التنمية السياسية الضفة الغربية أنموذجاً**، رسالة ماجستير غير منشورة، نابلس: جامعة النجاح الوطنية.
- ربايعة، عبد اللطيف (2016). **الجرائم الإلكترونية–التجريم والملاحقة والإثبات**، المؤتمّر الأول للجرائم الإلكترونية في فلسطين، نابلس: جامعة النجاح الوطنية.
- رويمل، نوال (2012). الاتجاهات النظريّة الحديثة المفسرة لظاهرة الجريمة، نحو قراءة تحليلية تكاملية، **مجلة التواصل في العلوم الانسانية والاجتمّاعية**، العدد(30)، ص ص (27–41).
- سلامة، مأمون (1979). **قانون العقوبات القسم العام**، بيروت: دار الفكر العربي للنشر والتوزيع.
- السلايمة، ميس (2018). **الظروف الاقتصادية والاجتمّاعية وتأثيرها على ارتفاع معدلات الجريمة لدى نزلاء مراكز الاصلاح والتأهيل في الضفة الغربية**، رسالة ماجستير غير منشورة، فلسطين: جامعة القدس.
- السمري، عادل ولطفي، طلعت وعبد الفتاح، عايدة (2009). **علم الاجتمّاع الجريمة والانحراف**، عمان: دار المسيرة للنشر والتوزيع.
- الشروف، حابس (2010). **دور المؤسسة الأمنيّة في الفلسطينية بناء الدولة**، رسالة ماجستير غير منشورة، فلسطين: جامعة القدس.

- الشلالدة، محمد وربعي، عبد الفتاح (2015). **الجرائم الإلكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية**، بحث مقدم إلى المؤتمّر العلمي الحادي عشر حول الجرائم المعلوماتية، عمان: جامعة جرش.
- الشهري، موسى (2010). **تطوير التعاون بين الإدارة المدرسية والمؤسسات الأمنيّة في مجال التوعية الأمنيّة لطلاب المرحلة الثانوية (دراسة ميدانية في منطقة عسير)**، رسالة ماجستير غير منشورة، الرياض: جامعة الملك خالد.
- صغير، يوسف (2013). **الجريمة المرتكبة عبر الإنترنت**، رسالة ماجستير غير منشورة، الجزائر: جامعة مولود معمري.
- صلاحات، نظام (2008). **إصلاح القطاع الأمني الفلسطيني**، ورقة عمل مقدمة للمؤتمّر الأول حول إصلاح القطاع الأمني الفلسطيني، اريحا: جامعة الاستقلال.
- عابدين، نورهان (2020). **الذّكاء العاطفيُّ وعَلاقته بممارسة جرائِمِ الابتزاز الإلكترونيِّ لَدى عَيِّنَة من الضَّحَايا في الضفة الغربيّة**، رسالة ماجستير غير منشورة، فلسطين: جامعة القدس.
- العايد، حسن (2010). **توظيف تطبيقات مادة التربية الوطنية في التوعية الأمنيّة**، عمان: الجامعة الأردنية.
- عبد الباقي، مصطفى (2018). التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، **مجلة دراسات علوم الشريعة والقانون**، الجامعة الأردنية، مجلد (4)، عدد (45)، ص ص (284-299).
- العجمي، عبد الله (2014). **المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة**، رسالة ماجستير غير منشورة، عمان: جامعة الشرق الأوسط.

- العريان، محمد (2009). **الجرائم المعلوماتية**، القاهرة: دار النهضة العربية للنشر والتوزيع.
- عودة، يحيى(2014). البيئة والسلوك الاجرامي: دراسة في نظرية الانثربولوجيا الجنائية، **مجلة كلية الاداب**، جامعة بغداد، عدد (107)، ص ص (387-424).
- عوض، السيد (2018). التطور التكنولوجي والجريمة، **المجلة الدولية للآداب والعلوم الانسانية والاجتمّاعية**، عدد (16)، ص ص (226-249).
- القشوش، هدى (2007). **جرائم الحاسب الآلي في التشريع المقارن**، الاسكندرية: الدار الجامعية للنشر والتوزيع.
- القطامي، قطامي محمد (2008). **المفهوم الاجتمّاعي للجريمة**، البحرين: منشورات الإدارة العامة للإعلام الأمني.
- الكبيسي، ناجي (2010). **الأمية والجريمة: دراسة نظرية وميدانية على عينة من النزلاء بسجون جمهورية مصر العربية**، مصر: جامعة عين شمس.
- لطرش، فيروز (2016). الجريمة الإلكترونية في الجزائر من جريمة فردية الى جريمة منظمة، **مجلة آفاق للعلوم**، مجلد (1)، العدد (1): ص ص (323-335).
- مدرسة الشهيد ماجد أبو شرار لإعداد الكوادر(2004). **صلاحيات ومهام الأجهزة الأمنيّة الفلسطينية بين محاذير التداخل وضرورة التنسيق**، البيرة: التوجيه السياسي والوطني.
- مطر، كامل (2014). **الجريمة الإلكترونية**، ورقة مقدمة في الندوة العلمية الجرائم المستحدثة في المتغيرات والتحولات الاقليمية والدولية، عمان: الجامعة الاردنية.
- المطيري، نواف (2016). **دور شبكات التواصل الاجتمّاعي في الابتزاز المؤدي الى الجرائم غير الاخلاقية**، رسالة ماجستير غير منشورة، السعودية: جامعة نايف العربية للعلوم الأمنيّة

- المغذوي، عادل (2014). **قضايا مجتمّعية معاصرة، سلسلة محاضرات**، جامعة الملك سعود، الرياض: المملكة العربية السعودية.
- ملاوي، أحمد (2008). أهمية منظمات المجتمّع المدني في التنمية، **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**، دمشق، مجلد (2)، عدد (24)، ص ص (275-305).
- ملحم، فراس والبرغوثي، معين (2015). **الإطار القانوني الناظم لقطاع الأمن في فلسطين/ دراسة تحليلية للتشريعات الصادرة بعد العام 1994م**، رام الله: فلسطين.
- المومني، نهلا (2010). **الجرائم المعلوماتية**، عمان: دار الثقافة للنشر والتوزيع.
- نجم الدين، فيصل (2018). واقع الجريمة الإلكترونية في مواقع التواصل الاجتمّاعي: الحماية النظامية في دول مجلس التعاون الخليجي، **المجلة الدولية للاتصال الاجتمّاعي**، مجلد5، العدد (4)، ص ص (7-31).
- نجيب، محمود (1977). **شرح قانون العقوبات-القسم الخاص**، القاهرة: دار النهضة العربية.
- الهيئة الفلسطينية المستقلة لحقوق المواطن (2005). **سلسلة تقارير خاصة (43) حول حالة الانفلات الأمني وضعف سيادة القانون في أراضي السلطة الوطنية الفلسطينية**، رام الله: الهيئة الفلسطينيّة لحقوق المواطن.
- الوريكات، عايد (2013). **نظريات علم الجريمة**، عمان: دار وائل للنشر والتوزيع.
- يوسف، ياسين (2004). **النظريّة العامة للقانون الجنائي السوداني لسنة 1991م**، بيروت: دار الهلال للطباعة والنشر.

ثالثاً: المواقع الإلكترونية:

- ارزيقات، لؤي (2018). **الجريمة الإلكترونية جريمة العصر**، لمزيد من التوضيح أنظر/ي الرابط التالي:

https://www.palpolice.ps/specialized-departments/396760.html، 29.11.2021، 2 PM

- جهاز الشرطة الفلسطينية (2021). **الجريمة الإلكترونية في الضفة الغربية بين الواقع والمواجهة**، لمزيد من التوضيح أنظر/ي الرابط التالي:

https://www.palpolice.ps/content/425828.html، 1.3.2021، 4 PM.

- جهاز الشرطة الفلسطينية (2021). **احصائية الجرائم الإلكترونية**، لمزيد من التوضيح أنظر/ي الرابط التالي:

https://www.palpolice.ps/content/425828.html، 19.11.2021، 5 PM.

- شبكة وفا الاخبارية (2020). **4.5 مليون مشترك في الاتصالات الخلوية**، لمزيد من التوضيح أنظر/ي الرابط التالي:

https://wafa.ps/ar_page.aspx?id=EhRoWma876325622997aEhRoWm, 12.1.2022, 5 PM.

رابعاً: المراجع الاجنبية:

- Breen, Amanda (2011). **The effects labeling and stereotype threat on offender reintegration,** A thesis submitted fulfillment of the requirements for the degree of masters in criminology, University of Ontario Institute of Technology.
- Hadlington, Lee & Lumsden, Karen & Black, Alesandra & Ferra, Fenia (2018). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime, **Journal of Policy and Practice**, 15 (1), PP 34-43
- Harkin, Diarmaid & Whelan, Chad & Chang, Lennon (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. **Police Practice and Research**, 19(6), PP 519-536.

- Pool, Ronald & Custers, Bart (2017). The police hack back: legitimacy, necessity and privacy implications of the next step in fighting cybercrime. **European journal of crime, criminal law and criminal justice**, 25(2), PP 123-144.
- Williamson, Nancy (2014). **Deep wep:Chalienges of catching the cyber criminal.** (Doctoral dissertation, Utica College).

قائمة الملاحق

ملحق رقم (1): الإستبانة في صورتها الاولية:

بسم الله الرحمن الرحيم

جامعة القدس

كلية الدراسات العليا

برنامج علم الجريمة

إستبيانة الدراسة

تحية طيبة وبعد

تقوم الباحثة بإجراء دراسة بعنوان: **(المؤسسة الأمنيّة ودورها في الحد من الجرائم الإلكترونية: الأمن الوقائي أنموذجاً ")**، ذلك استكمالا للحصول على درجة الماجستير في علم الجريمة من جامعة القدس، أرجو التكرم بالإجابة على فقرات الاستبيان بوضع إشارة (×) أمام العبارة التي تتفق ووجهة نظركم، شاكرة لكم جهودكم وأمانتكم وحرصكم على إنجاح هذه الدراسة، علما بان إجاباتكم ستكون سرية ولا تشكل أي نوع من الاختبار ولن تستخدم إلا لغايات البحث العلمي فقط.

شاكرة لكم حسن تعاونكم

الباحثة: حنان مرداوي

إشراف: د. وفاء الخطيب

القسم الأول: البيانات الديموغرافية:

1) الجنس: ☐ ذكر ☐ أنثى

2) **المؤهل العلمي:** ☐ ثانوية عامة فأقل ☐ دبلوم متوسط ☐ بكالوريوس
☐ دراسات عليا

3) العمر: ☐ أقل من 25 سنة ☐ 25- أقل من 35 سنة ☐ 35- أقل من 45 سنة
- ☐ 45 سنة فأكبر

4) الرتبة العسكرية: ☐ عريف-مساعد أول ☐ ملازم-مقدم ☐ عقيد-لواء

5) **عدد سنوات الخدمة:** ☐ أقل من 5 سنوات ☐ 5- أقل من 10 سنوات
☐ 10- اقل من 15 سنة ☐ 15 - اقل من 20 سنة
☐ 20 سنة فأكثر

6) **طبيعة العمل في جهاز الأمن الوقائي:** ☐ تقني
☐ إداري ☐ تحرّي ☐ تحليل ☐ إستجواب
☐ غير ذلك حدد/ي:.....

القسم الثاني: مجالات ومحاور الدراسة:

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

الرقم	الفقرات	موافق بشدة	موافق	محايد	معارض	معارض بشدة
المجال الأول: الإجراءات المتبعة في جهاز الأمن الوقائي لمكافحة الجريمة الإلكترونية من وجهة نظركم						
.1	توفير مُعدات تقنيّة لمتابعة الجرائم الإلكترونية.					
.2	توفير برامج تقنيّة تُسهم في متابعة الجرائم الإلكترونية.					
.3	تأمين المواقع الحساسة في الدولة من الإختراق.					
.4	التحديث المستمّر لبرامج حماية الحواسيب تجنباً للإختراق.					
.5	تأسيس نظام وطني لرصد أمن المعلومات (الأمنيّة، الشخصية، السياسية).					
.6	رفع مستوى المعرفة الرقميّة للعاملين في مجال الجرائم الإلكترونية.					
.7	تعزيز التعاون الدولي في مجال حماية البنية التحتيّة الحيويّة للمعلومات (الأمنيّة، السياسية).					
.8	التنسيق مع الشركاء في مجال مكافحة الجريمة الإلكترونية.					
.9	التنسيق مع مؤسسات المجتمّع المدني في مجال مكافحة الجريمة الإلكترونية.					
.10	تطبيق قانون الجرائم الإلكترونية بفعاليّة (الإحالات القانونية).					
.11	العمل على رفع مستوى الوعي العام بإتجاه مخاطر الإنترنت من خلال (ندوات، ورشات عمل، مؤتمّرات).					
.12	رفع مستوى تدريب الكوادر البشرية العاملة في مجال مكافحة الجرائم الإلكترونية.					
.13	الرقابة على الحسابات الشخصية للمشتبه بهم.					
.14	متابعة الشكاوي المُرتبطة بالجريمة الإلكترونية.					
.15	متابعة التحقيق في قضايا الجرائم الإلكترونية.					
.16	متابعة التهديدات الإلكترونية (للأفراد، للمؤسسات).					
.17	حماية الأمن الفكري المجتمّعي على شبكة المعلومات.					
.18	الحفاظ على خصوصيات الأفراد على شبكة المعلومات.					
المجال الثاني: دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة						
.19	عدم الإستغلال الجيد لوقت الفراغ.					
.20	عدم وجود رقابة حكومية على مواقع التواصل الاجتمّاعي.					
.21	الحصول على المنفعة المادية من خلال ابتزاز الضحية بمعلومات شخصية.					

.22	عدم توفر فرص عمل لدى الشباب الفلسطيني.					
.23	عدم تطبيق القانون ضد مرتكبي الجريمة الإلكترونية.					
.24	حب المغامرة لدى بعض الأفراد.					
.25	دوافع (جنسية، عاطفية، سياسية).					
.26	الاختلاط بأصدقاء السوء.					
.27	التفكك الأسري.					
.28	ضغوط الحياة (الاقتصادية ،الاجتمّاعية).					
.29	التنمر المُجتمّعي.					
.30	التنمر الإلكتروني.					
.31	صعوبة متابعة الجُناة.					
.32	عدم الإلمام بالعواقب القانونية لدى مرتكبي الجريمة الإلكترونية.					
.33	الإرتباط مع الإسرائيلين.					
.34	السلوك العدواني لدى مرتكبي الجريمة الإلكترونية.					
.35	الفضول في التعرف على الأفراد عبر شبكة الإنترنت.					
.36	الجهل باستخدام (المواقع الإلكترونية، مواقع التواصل الاجتمّاعي).					
المجال الثالث: أكثر أنواع الجرائم الإلكترونية التي تمّ التعامل معها في مجال عملكم في جهاز الأمن الوقائي						
.37	الجرائم السياسية.					
.38	جرائم المعلومات الأمنيّة.					
.39	الإرهاب الالكتروني (الفكر المتطرف).					
.40	تزوير المعلومات بكافة أشكالها.					
.41	استغلال الأطفال جنسياً.					
.42	انتهاك خصوصية الأفراد من خلال الدخول لحساباتهم الإلكترونية بهدف نشر معلوماتهم الشخصية دون علمهم.					
.43	التنصت على الغير.					
.44	الابتزاز (الجنسي، العاطفي، المادي، السياسي، الاقتصادي، الحزبي).					
.45	النيل من الشخصيات الإعتبارية بهدف التشهير بهم من خلال استخدام المعلومات الخاصة ونشرها بقصد الإساءة.					

.46	نشر الرذيلة على شبكات التواصل الاجتمّاعي.					
.47	إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية.					
.48	الوصول للمواقع المشفرة الممنوعة .					
.49	قرصنة المعلومات (الهكر).					
.50	التجسس الاقتصادي.					
.51	إنتحال شخصية الغير.					
.52	سرقة الحسابات الشخصية على مواقع التواصل الاجتمّاعي.					
المجال الرابع: الصعوبات التي تواجه جهاز الأمن الوقائي في مكافحة الجريمة الإلكترونية من وجهة نظركم						
.53	قلة الوعي المجتمّعي بالجريمة الإلكترونية.					
.54	صعوبة التوصل إلى الأدلة الرقمية.					
.55	صعوبة التحفظ على الإدلة الرقمية.					
.56	عدم وجود مفهوم قانوني دولي مشترك لتعريف الجريمة الإلكترونية.					
.57	قصور التعاون الدولي بين الدول في مجالات مكافحة الجريمة الالكرونية.					
.58	ضعف مهارة الكادر المتخصص للتعامل مع الجريمة الإلكترونية.					
.59	ضعف كفاءة الكادر المتخصص للتعامل مع الجريمة الإلكترونية.					
.60	نقص الكادر المتخصص للتعامل مع الوسائل الإلكترونية.					
.61	حداثة الجرائم الإلكترونية فهي تحتاج إلى (خبرات، كفاءات) للتعامل معها.					
.62	حداثة التشريعات القانونية الخاصة بقانون الجريمة الإلكترونية.					
.63	التغيير المُستمّر في طبيعة الجرائم الإلكترونية.					
.64	صعوبة تعقب شرائح الإتصالات الإسرائيلية المُستخدمة في إرتكاب الجريمة الإلكترونية.					
.65	خوف الضحية من نتائج التحقيق.					
.66	التكتمّ من قبل الضحايا على هذه الجرائم خوفاً من الفضيحة عند التبليغ.					
.67	انتحال المجرم الالكتروني لأسماء وهمية مما يصعب الكشف عن الجاني.					
.68	عرقلة أطراف مُجتمّعيّة للتحقيقات المُرتبطة بالجرائم					

	الإلكترونية.					
المجال الخامس: أهم الحلول التي تساعد على مكافحة الجريمة الإلكترونية من وجهة نظركم						
.69	التعاون المشترك مع المؤسسات الدوليّة المعنية لمكافحة الجرائم الإلكترونية.					
.70	التعاون المشترك مع المؤسسات المحليّة المعنية لمكافحة الجرائم الإلكترونية.					
.71	عدم التحييز في تطبيق قانون الجريمة الإلكترونية على الافراد (توفير محاكمة عادلة للجناة).					
.72	تشديد العقوبة على مرتكبي الجرائم الإلكترونية.					
.73	تفعيل دور الرقابة المجتمّعية كوسيلة من وسائل الضبط الاجتمّاعي.					
.74	تطوير قدرات العاملين في مجال مكافحة الجريمة الإلكترونية من خلال (التدريب، المؤتمّرات، ورش العمل).					
.75	وجود رقم موحد لدى جهات الاختصاص للتبليغ فور التعرض لجريمة إلكترونية.					
.76	تجنب تحميل أي برنامج مجهول المصدر.					
.77	حماية الضحية أثناء التحقيق.					
.78	حماية الضحية بعد الإنتهاء من التحقيق.					
.79	تجنب إستخدام أي برامج مجهولة المصدر.					
.80	تجنب فتح أي رسائل إلكترونية مجهولة المصدر.					
.81	تجنب إدخال كلمات مرور مجهولة المصدر تجنباً من التعرض لسرقة الحسابات المُستخدمة					
.82	تثبيت برامج حماية من إختراق الأجهزة الشخصية من أجل حماية ما به من معلومات شخصية.					
.83	مواكبة التطورات التقنيّة لتتبع مرتكبي الجرائم الإلكترونية للحد من انتشارها.					
.84	رفع مستوى الوعي المُجتمّعي في تجنب نشر معلومات شخصية على مواقع التواصل الاجتمّاعي.					
.85	تنظيم برامج توعوية حول مخاطر الجريمة الإلكترونية.					

مع الشكر والتقدير

الباحثة: حنان المرداوي

ملحق رقم (2): الاستبانة في صورتها النهائية:

بسم الله الرحمن الرحيم

جامعة القدس

كلية الدراسات العليا

برنامج علم الجريمة

إستبيانة الدراسة

تحية طيبة وبعد

تقوم الباحثة بإجراء دراسة بعنوان: **(دور المؤسسة الأمنيّة في الحد من الجرائم الإلكترونية: الأمن الوقائي أنموذجاً)**، ذلك استكمالا للحصول على درجة الماجستير في علم الجريمة من جامعة القدس، أرجو التكرم بالإجابة على فقرات الاستبيان بوضع إشارة (×) أمام العبارة التي تتفق ووجهة نظركم، شاكرة لكم جهودكم وأمانتكم وحرصكم على إنجاح هذه الدراسة، علما بان إجاباتكم ستكون سرية ولا تشكل أي نوع من الاختبار ولن تستخدم إلا لغايات البحث العلمي فقط.

شاكرة لكم حسن تعاونكم

الباحثة: حنان مرداوي

إشراف: د. وفاء الخطيب

القسم الأول: البيانات الديموغرافية:

1) الجنس: ☐ ذكر ☐ أنثى

2) المؤهل العلمي: ☐ ثانوية عامة فأقل ☐ دبلوم متوسط ☐ بكالوريوس
☐ دراسات عليا

3) العمر: ☐ أقل من 25 سنة ☐ 25- أقل من 35 سنة ☐ 35- أقل من 45 سنة
- ☐ 45 سنة فأعلى

4) الرتبة العسكرية: ☐ ملازم فما دون ☐ ملازم أول-رائد ☐ مقدم فأعلى

5) عدد سنوات الخدمة: ☐ أقل من 5 سنوات ☐ 5- أقل من 10 سنوات
☐ 10- اقل من 15 سنة ☐ 15 - اقل من 20 سنة ☐ 20 سنة فأكثر

6) طبيعة العمل في جهاز الأمن الوقائي: ☐ تقني ☐ إداري ☐ عمليات
☐ تحليل ☐ إستجواب ☐ غير ذلك حدد/ي:.....

القسم الثاني: مجالات ومحاور الدراسة:

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

الرقم	الفقرات	موافق بشدّة	موافق	محايد	معارض	معارض بشدّة
المجال الأول: الإجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية						
.1	يُزود الجهات ذات العلاقة بالتغذية الراجعة حول واقع الجريمة الإلكترونية.					
.2	يُوفر مُعدات تقنيّة لمتابعة الجرائم الإلكترونية.					
.3	يعمل على مراقبة البرامج (التطبيقات) التقنيّة المستحدثة التي تقود الى الجريمة الإلكترونية بشكل مستمّر.					
.4	يعمل على تأمين المواقع الحساسة في الدولة من الإختراق.					
.5	يعمل على التحديث المستمّر لبرامج حماية الحواسيب تجنباً للإختراق.					
.6	يعمل على رفع مستوى المعرفة الرقميّة لضباطه العاملين في مجال الجرائم الإلكترونية بشكل دوري.					
.7	يندرج عمل الجهاز في الجرائم الإلكترونية ضمن منظومة دوليّة لحاية البنية التحتية للمعلومات.					
.8	يعمل على التنسيق المستمّر مع الشركاء من الأجهزة الأمنيّة الأخرى العاملة في مجال مكافحة الجريمة الإلكترونية.					
.9	يعمل على التنسيق المستمّر مع مؤسسات المجتمّع المدني العاملة في مجال مكافحة الجريمة الإلكترونية.					
.10	يعمل على التطبيق الفعلي لقانون الجرائم الإلكترونية.					
.11	يعمل على رفع مستوى الوعي العام بإتجاه مخاطر الإنترنت من خلال (ندوات، ورشات عمل، مؤتمّرات).					
.12	يعمل على رفع مستوى تدريب الكوادر البشريّة العاملة في مجال مكافحة الجرائم الإلكترونية.					
.13	يعمل على مراقبة الحسابات الشخصيّة للمشتبه بهم.					
.14	يعمل على متابعة الشكاوي المُرتبطة بالجريمة الإلكترونية.					
.15	يعمل على متابعة التحقيق في قضايا الجرائم الإلكترونية.					
.16	يعمل على متابعة التهديدات الإلكترونية (للأفراد، للمؤسسات).					
المجال الثاني: دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة						
.17	عدم الإستغلال الجيد لوقت الفراغ.					
.18	عدم وجود رقابة حكوميّة على مواقع التواصل الاجتمّاعي.					
.19	ضعف الرقابة الأسريّة على الأبناء.					

الرقم	الفقرات	موافق بشدّة	موافق	محايد	معارض	معارض بشدّة
.20	الحصول على المنفعة المادية من خلال ابتزاز الضحية بمعلومات شخصية.					
.21	عدم تطبيق القانون ضد مرتكبي الجريمة الإلكترونية.					
.22	حب المغامرة لدى بعض الأفراد.					
.23	دوافع (جنسية، عاطفية، سياسية).					
.24	الاختلاط بأصدقاء السوء.					
.25	ضغوط الحياة العامة (الاقتصادية، الاجتمّاعية، السياسية، البطالة، التفكك الأسري).					
.26	التنمر المُجتمّعي.					
.27	التنمر الإلكتروني.					
.28	عدم إلمام مرتكبي الجريمة الإلكترونية بالعواقب القانونية.					
.29	إرتباط مرتكبي الجريمة الإلكترونية مع الإسرائيلين.					
.30	السلوك العدواني لدى مرتكبي الجريمة الإلكترونية.					
.31	الفضول في التعرف على الأفراد عبر شبكة الإنترنت.					
.32	عدم إلمام بعض الأفراد باستخدام (المواقع الإلكترونية، مواقع التواصل الاجتمّاعي).					
المجال الثالث: أكثر أنواع الجرائم الإلكترونية التي تمّ التعامل معها في جهاز الأمن الوقائي						
.33	الجرائم السياسية.					
.34	جرائم المعلومات الأمنيّة.					
.35	جرائم الإرهاب الالكتروني (الفكر المتطرف).					
.36	جرائم تزوير المعلومات.					
.37	استغلال الأطفال جنسياً.					
.38	انتهاك خصوصية الأفراد من خلال الدخول لحساباتهم الإلكترونية بهدف نشر معلوماتهم الشخصية دون علمهم.					
.39	التنصت على الغير.					
.40	الابتزاز بجميع أشكاله.					
.41	النيل من الشخصيات الإعتبارية بهدف التشهير بهم من خلال استخدام المعلومات الخاصة ونشرها بقصد الإساءة.					
.42	نشر الرذيلة على شبكات التواصل الاجتمّاعي.					
.43	إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية.					

الرقم	الفقرات	موافق بشدّة	موافق	محايد	معارض	معارض بشدّة
44.	الوصول للمواقع المشفرة الممنوعة بطرق غير مشروعة .					
45.	قرصنة المعلومات (الهكر).					
46.	التجسس بكافة أشكاله.					
47.	إنتحال شخصية الغير.					
48.	سرقة الحسابات الشخصية على مواقع التواصل الاجتمّاعي.					
المجال الرابع: الصعوبات التي تواجه جهاز الأمن الوقائي في الحدّ من الجريمة الإلكترونية						
49.	قلة الوعي المجتمّعي بالجريمة الإلكترونية.					
50.	صعوبة التوصل للأدلة الرقمية.					
51.	صعوبة التحفظ على الإدلة الرقمية.					
52.	عدم وجود مفهوم قانوني دولي مشترك لتعريف الجريمة الإلكترونية.					
53.	قصور التعاون الدولي بين الدول في مجالات مكافحة الجريمة الالكرونية.					
54.	ضعف مهارة الكادر الذي يتعامل مع الجريمة الإلكترونية.					
55.	ضعف كفاءة الكادر الذي يتعامل مع الجريمة الإلكترونية.					
56.	نقص الكادر المتخصص للتعامل مع الوسائل الإلكترونية.					
57.	حداثة الجرائم الإلكترونية فهي تحتاج إلى (خبرات، كفاءات) للتعامل معها.					
58.	حداثة التشريعات القانونية الخاصة بقانون الجريمة الإلكترونية.					
59.	التغيير المُستمّر في طبيعة الجرائم الإلكترونية.					
60.	صعوبة تعقب شرائح الإتصالات الإسرائيلية المُستخدمة في إرتكاب الجريمة الإلكترونية.					
61.	خوف الضحية من نتائج التحقيق.					
62.	تكتمّ الضحية تعرضها للجريمة الإلكترونية خوفاً من الفضيحة عند التبليغ.					
63.	انتحال المجرم الالكتروني لأسماء وهمية مما يصعب الكشف عن الجاني.					
64.	عرقلة أطراف مُجتمّعيّة للتحقيقات المُرتبطة بالجرائم الإلكترونية.					
65.	صعوبة متابعة الجُناة.					
المجال الخامس: أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية						
66.	التعاون المشترك مع المؤسسات الدوليّة المعنية للحد من الجرائم الإلكترونية.					

الرقم	الفقرات	موافق بشدّة	موافق	محايد	معارض	معارض بشدّة
.67	التعاون المشترك مع المؤسسات المحليّة المعنية للحد من الجرائم الإلكترونية.					
.68	عدم التحييز في تطبيق قانون الجريمة الإلكترونية على الافراد (توفير محاكمة عادلة للجناة).					
.69	تشديد العقوبة على مرتكبي الجرائم الإلكترونية.					
.70	تفعيل دور الرقابة المجتمّعية كوسيلة من وسائل الضبط الاجتمّاعي.					
.71	تطوير قدرات العاملين في مجال مكافحة الجريمة الإلكترونية من خلال (التدريب، المؤتمّرات، ورش العمل).					
.72	وجود رقم موحد لدى جهات الاختصاص للتبليغ فور التعرض لجريمة إلكترونية.					
.73	تجنب تحميل أي برنامج مجهول المصدر.					
.74	حماية الضحية أثناء التحقيق.					
.75	حماية الضحية بعد الإنتهاء من التحقيق.					
.76	تجنب إستخدام أي برامج مجهولة المصدر.					
.77	تجنب فتح أي رسائل إلكترونية مجهولة المصدر.					
.78	تجنب إدخال كلمات مرور مجهولة المصدر تجنباً من التعرض لسرقة الحسابات المُستخدمة					
.79	تجنب استخدام الحسابات الخاصة في الأماكن العامة غير الموثوقة تجنباً من التعرض للإبتزاز الإلكتروني					
.80	تثبيت برامج حماية من إختراق الأجهزة الشخصية من أجل حماية ما به من معلومات شخصية.					
.81	مواكبة التطورات التقنيّة لتتبع مرتكبي الجرائم الإلكترونية للحدّ من انتشارها.					
.82	رفع مستوى الوعي المُجتمّعي في تجنب نشر معلومات شخصيّة على مواقع التواصل الاجتمّاعي.					
.83	رفع مستوى الرقابة الاسريّة على الأبناء					
.84	تنظيم برامج توعويّة حول مخاطر الجريمة الإلكترونية.					

مع الشكر والتقدير

الباحثة: حنان المرداوي

ملحق رقم (3): أسماء محكمي الإستبانة:

الرقم	اسم المحكم	الجامعة
.1	د.رياض شريم	جامعة الاستقلال
.2	د.علي عيايدة	جامعة الاستقلال
.3	د.رجاء سويدان	جامعة الاستقلال
.4	د. عصام الأطرش	جامعة الاستقلال
.5	د. عبد اللطيف الربايعة	جامعة الاستقلال
.6	د. نادر شوامره	جامعة الاستقلال
.7	د. محمد الفرارجة	جامعة القدس
.8	د. سمير شقير	جامعة القدس
.9	د. زياد قنام	جامعة القدس
.10	د. علا الحسين	جامعة القدس
.11	د. فريد غريب	جامعة القدس
.12	د. عزمي أبو السعود	جامعة القدس
.13	أ. زياد لافي	جامعة القدس
.14	د. صالح البرغوثي	الكليّة العصريّة
.15	د. محمد خلاف	الجامعة الأهلية

ملحق رقم (4): دليل المقابلة المُعمقة:

القسم الأول: البيانات الشخصية:

الاسم: _____

العمر: _____

المستوى التعليمي: _____

المسمى الوظيفي: _____

الرتبة: _____

عدد سنوات الخبرة:_____

القسم الثاني:أسئلة المقابلة:

السؤال الاول: ما الاجراءات المتبعة في جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

_____

_____

_____

_____

_____

_____

السؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظرك؟

السؤال الثالث: ما اكثر انواع الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي؟

السؤال الرابع: ما الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

السؤال الخامس: ما اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟

_____

_____

_____

_____

_____

_____

مع الشكر والتقدير

الباحثة: حنان المرداوي

ملحق رقم (5): نتائج الاجابات على المقابلة المُعمقة:

مقابلة رقم (1):

إنه وبتاريخ 2020/11/3م تمّ مقابلة (م.ر) من جهاز الامن الوقائي في وحدة الجرائم الإلكترونية، تمّ طرح الأسئلة الآتية عليه:

السؤال الأول: ما الاجراءات المتبعة في جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

يتمّثل عمل جهاز الامن الوقائي في حماية المجتمّع والمؤسسات بالكشف عن الجرائم والجرائم الاكترونية، حيث تتمّثل الاجراءات المتبعة للحد من الجريمة الإلكترونية في:

- اولا: بالنسبة للمؤسسات والوزارات يتمّ فحص انظمة الحماية الإلكترونية الموجودة لديهم والتاكد من عدم وجود ثغرات حيث يتمّ ذلك بشكل دوري.
- ثانيا: بالنسبة للمدارس والجامعات تقوم وحدة خاصة بالجهاز بترتيب لقاءات مع طلاب المدارس لنشر الوعي وطريقة استخدام الانترنت الامن، ذلك للحد من الجرائم الإلكترونية.

السؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظرك؟

تكمن دوافع ارتكاب الجريمة من قبل الجناة في دوافع مادية وأخرى شخصية (تسلية، انتقام، جنسية)، إضافة للدوافع السياسية (منظمات، اجندات).

السؤال الثالث: ما اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي؟

اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي جرائم الابتزاز والتشهير من الدوافع الشخصية، إضافة إلى جرائم النصب وجرائم التهديد والجرائم السياسية.

السؤال الرابع: ما الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

تكمن الصعوبات في وجود مرتكبي الجرائم خارج الضفة الغربية، مثل قطاع غزة والداخل بالتالي لا يمكن القبض عليهم، إضافة إلى عدم امكانية تحديد مرتكبي الجرائم الذين يستخدمون شرائح الاتصال الاسرائيلية.

السؤال الخامس: ما اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟

من أهم الحلول وجود عقاب رادع لمرتكبي الجرائم الإلكترونية ومنع تداول واستعمال الشرائح الاسرائيلية، او ايجاد الية تواصل مع هذه الشركات لتقديم المعلومات المطلوبة منهم بخصوص مرتكبي الجرائم، والعمل على زيادة برامج االتوعية في المدارس والجامعات والتاكيد بمخاطرها على المجتمّع وعواقبها الاجتمّاعية، إضافة لعمل صفحات على مواقع التواصل الاجتمّاعي كخط دعم واستفسارات لمساعدة الاشخاص.

مقابله رقم (2):

إنه وبتاريخ 2020/11/8م تمّ مقابلة (م.ج) من ضباط جهاز الامن الوقائي في وحدة الجرائم الإلكترونية، تمّ طرح الأسئلة الآتية عليه:

السؤال الاول: ما الاجراءات المتبعة في جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

جهاز الامن الوقائي هو جهاز أمني يعمل على الكشف عن "الجرائم" منها الجرائم الإلكترونية المحتمّلة قبل حدوثها، ومن الاجراءت المتبعة التي يقوم بها نذكر بعضها:

- قيام الجهاز باعطاء دورات ونشرات توعوية في مؤسسات الدولة ومنها التعليمية كالجامعات والمدارس وغيرها من المؤسسات ذات العلاقة بموضوع الجرائم الإلكترونية وابراز مخاطرها على المجتمّع وعواقبها.
- التشبيك بين المؤسسات لفحص اجراءات الحماية على الانظمة الإلكترونية المتعبة لديهم وعلى مواقعهم الإلكترونية وفحص نقاط الضعف فيها وبشكل دوري.

السؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظرك؟

تكمن دوافع ارتكاب الجريمة من قبل الجناة في دوافع مادية وشخصية وجنسية، إلى جانب دافع الانتقام ودافع التسلية والدوافع السياسية.

السؤال الثالث: ما اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي؟

تعامل الجهاز مع جرائم الابتزاز والنصب والتهديد والجرائم السياسية.

السوال الرابع: ما الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

تكمن الصعوبات في استخدام شرائح الاتصال الاسرائيلية ووجود مرتكبي الجرائم خارج الضفة الغربية مثل قطاع غزة والداخل.

السؤال الخامس: ما اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟

تتمّثل الحلول في اعطاء نشرات توعوية في المدارس والجامعات وابراز مخاطرها على المجتمّع وعواقبها الاجتمّاعية واظهار عقوبة مرتكب الجريمة من ناحية قانونية، ومنع تداول واستعمال الشرائح الاسرائيلية.

مقابله رقم (3):

إنه وبتاريخ 2020/11/10م تمّ مقابلة (ر.م) من ضباط جهاز الامن الوقائي في وحدة الجرائم الإلكترونية، تمّ طرح الأسئلة الآتية عليه:

السؤال الأول: ما الاجراءات المتبعة في جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

قام جهاز الامن الوقائي بالعديد من الاجراءات للحد من الجريمة الإلكترونية لعل من أهمها:

- نشر الوعي والتحذير من الجريمة الإلكترونية من خلال صفحة الجهاز الرسمية ومن خلال ادارة العلاقات العامة التي قامت بعدة محاضرات توعوية في المؤسسات التعليمية ومؤسسات المجتمّع المدني ومن خلال نشرات مختصة بهذا الغرض.
- عقد مؤتمّرات متخصصة تتناول الجريمة الإلكترونية من كافة الجوانب الأمنيّة والقانونية والاجتمّاعية ودعوة شرائح متعددة لحضور هذه المؤتمّرات وبثها عبر تلفزيون وشاشة فلسطين.
- قام جهاز الامن الوقائي ايضا بتطوير وحدات متخصصة في الجهاز لمتابعة قضايا الجرائم الإلكترونية وكشفها.
- إضافة إلى أنه لم يتوانى الجهاز في اتخاذ الاجراءات القانونية اللازمة من اعتقال وتحويل الضالعين بهذه الجرائم للقضاء لاخذ المقتضى القانوني بحقهم.

السؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظرك؟

تكمن دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة بدوافع مادية لكسب المال والثراء ودوافع المتعة والرغبة في الانتقام واحداث اضرار اما لاسباب نفسية او شذوذ، إضافة لدوافع الاجرام المنظم.

السؤال الثالث: ما اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي؟

تعامل جهاز الامن الوقائي مع العديد من الجرائم الإلكترونية منها جرائم ضد الافراد من انتحال شخصية وابتزاز الكتروني وسرقة معلومات شخصية وتشهير بالضحية والنصب والاحتيال، كذلك جرائم الارهاب الالكتروني وجرائم الملكية للمؤسسات من استهداف ملفات وسرقة معلومات ونشرها، والجرائم الاقتصادية والتجارة الإلكترونية الغير مشروعة من خلال العملات الإلكترونية مثل البتكوين (عملة رقمية)، وجرائم نشر الاشاعات وتلفيق وفبركة الاخبار، وجرائم القرصنة لاتلاف المحتوى، إضافة لجرائم العنف ضد الاطفال من خلال استدراج الاطفال واستغلالهم جنسيا عبر شبكات التواصل الاجتمّاعي وبرامج الالعاب.

السؤال الرابع: ما الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

هناك العديد من الصعوبات التي تواجه الجهاز للحد من الجريمة الإلكترونية لعل من أهم تلك الصعوبات ما يلي:

- قلة الوعي بمخاطر الجرائم الإلكترونية لدى الافراد وبعض المؤسسات التي لا تتخذ اي اجراءات حماية.
- استغلال التطور التكنولوجي من الجناة للتخفي واستخدام برامج ذكية في اخفاء اي دليل متعلق بهم.
- استخدام شبكات الاتصال الاسرائيلية في تنفيذ الجريمة الإلكترونية.
- بسبب الانقسام بين الضفة وغزة.

السؤال الخامس: ما اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟

لعل من أهم الحلول ما يلي:

- نشر الوعي الذي يشكل عامل مهم واساسي.
- استخدام برامج حماية.
- عدم نشر صور وملفات هامة على مواقع التواصل او تبادل صور مع جهات غير موثوقة.
- وجود عقوبات رادعة واحكام عاليّة لمرتكبي الجرائم الإلكترونية.

مقابله رقم (4):

إنه وبتاريخ 2020/11/12م تمّ مقابلة (هـ.ق) من ضباط جهاز الامن الوقائي في وحدة الجرائم الإلكترونية، تمّ طرح الأسئلة الآتية عليه:

السؤال الاول: ما الاجراءات المتبعة في جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

هناك العديد من الإجراءات المُتبعة لعل من أهمها:

- توعية الناس بطرق الاستخدام الآمن لمواقع التواصل الاجتمّاعي والاجهزة الذكيه ومواقع الويب.
- كشف واغلاق الحسابات الوهميه والمشبوهه للاشخاص الذين يعملون في مجال الاختراق والابتزاز.

السؤال الثاني : ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظرك؟

تكمن دوافع إرتكاب الجريمة الإلكترونية من قبل الجناة بدوافع مالية وشخصية وسياسية.

السؤال الثالث: ما اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي؟

تتمّثل أكثر الأنواع بـ:

- الابتزاز والتهديد.
- انتحال الشخصيات.
- سرقة معلومات.
- اختراق الاجهزه من قبل اشخاص.

السؤال الرابع: ما الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

تتمّثل الصعوبات في:

- وجود الشرائح والاتصالات الاسرائيليه.
- قلة وعي الناس في استخدام التكنولوجيا.

السؤال الخامس: ما اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟

لعل من أهم الحلول ما يلي:

- الغاء الشرائح الاسرائيليه في مناطق الضفة.
- عدم التعاطي مع اشخاص مجهولين على المواقع الإلكترونية.
- عدم استقبال ملفات مجهوله المصدر وعدم التعامل معها.

مقابله رقم (5):

إنه وبتاريخ 2020/11/15م تمّ مقابلة (ح.خ) من ضباط جهاز الامن الوقائي في وحدة الجرائم الإلكترونية، تمّ طرح الأسئلة الآتية عليه:

السؤال الاول: ما الاجراءات المتبعة في جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

تتمّثل الإجراءات في القيام بـ:

- حملات التوعية بانواعها من خلال مؤتمّرات وجاهية او الكترونياً ومن خلال الاعلانات الإلكترونية الممولة في مواقع التواصل الاجتمّاعي والفيديوهات التوضيحية.
- متابعة الشكاوي المقدمة من المشتكين من قبل متخصصين في المجال.
- الحرص على معاقبة المخالفين دون تهاون لردع امثالهم.

السؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظرك؟

تتمّثل الدوافع بالآتي:

- الاستهانة بالعواقب لجهلهم بها بسبب حداثة قانون الجرائم الإلكترونية في البلاد التي تشكل دافع لديهم للانتقام من الضحايا بهذه الاساليب لتوهمهم بقدرتهم على التخفي وعدم قدرة جهات تنفيذ القانون من الوصول اليهم.
- استهتار الضحايا وقلة اتخاذهم باحتياطات الامان التي تقلل من احتمّالية تعرضهم للجرائم الإلكترونية من تأمين حساباتهم من الاختراق ومشاركة خصوصياتهم على المواقع من صور وغيرها وعدم حذفها في المحادثات او الايميلات مثلا او المواقع الإلكترونية التي تمّ تخزينها عليها وقلة وعيهم بخطر ذلك حيث يلجأ الجناة لها ايضا لكونها سلاح مضر ضد الضحية وشبه مجاني.
- ممكن ان يكون الدافع دافع من قبل الاحتلال لتمّزيق المجتمّع والاسقاطات.
- دوافع مادية كمصدر مالي للجاني وحصوله على أموال مقابل ما يفعله.
- هناك اسباب انتقامية من شخصيات اعتبارية و تمّزيق سمعتها في المجتمّع.

السؤال الثالث: ما اكثر انواع الجرائم الجرائم الإلكترونية التي تعامل معها جهاز الامن الوقائي؟

اكثر انواع الجرايم هي الابتزاز للضحايا مقابل الحصول على اموال او مقابل عمل شيء معين من قبل الضحية او للانتقام من سمعته في المجتمّع.

السؤال الرابع: ما الصعوبات التي تواجه جهاز الامن الوقائي للحد من الجريمة الإلكترونية؟

الصعوبات تتمّثل في:

- حداثة قانون الجرايم الاكترونية الذي يترتب عليه الاستهتار من قبل الجناة لقلة وعيهم بالعواقب.
- استهتار الضحايا وقلة وعيهم بوجوب تأمين حساباتهم على الانترنت وعدم التعاطي ومشاركة خصوصياتهم مع من يعرفونهم ومن لا يعرفونهم.
- صعوبة تعقب الشرائح الاسرائيلية من قبل جهات تنفيذ القانون التي يلجأ اليها الجناة خاصة المحترفون والملمين بالامور التي تبعد عنهم الشبهات.
- قلة الامكانيات والخبرات مقارنة بالدول الاخرى.

السؤال الخامس: ما اهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟

تتمّثل الحلول في التوعية وعدم التهاون في تطبيق القانون على الجناة وزيادة مهارات العاملين في تنفيذ القانون من خلال دورات في الدول المتقدمة في هذا المجال.

ملحق رقم (6): قانون الجرائم الإلكترونية رقم (16) لسنه (2017):

قرار بقانون رقم (16) لسنة (2017)م بشأن الجرائم الإلكترونية:

رئيس دولة فلسطين:

رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية:

استنادا لأحكام القانون الأساسي المعدل لسنة (2003م) وتعديلاته، لا سيما أحكام المادة (43) منه، وبعد الاطلاع على قانون رقم (74) لسنة (1963م) وتعديلاته، الساري في المحافظات الجنوبية، وعلى أحكام قانون العقوبات الأردني رقم (16) لسنة (1960م) وتعديلاته، الساري في المحافظات الشمالية، وعلى قانون رقم (3) لسنة(1996م)، بشأن الاتصالات السلكية واللاسلكية، وعلى قانون الإجراءات الجزائية رقم (3) لسنة 2001م وتعديلاته، وعلى القرار بقانون رقم (18) لسنة (2015م)، بشأن مكافحة المخدرات والمؤثرات العقلية، وعلى قرار بقانون رقم (20) لسنة (2015م)، بشأن مكافحة غسل الأموال وتمّويل الإرهاب وتعديلاته، وبناءً على تنسيب مجلس الوزراء بتاريخ (2017/06/20)م، وعلى الصلاحيات المخولة لنا، وتحقيقا 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 إلغاؤه أو تعديل محتوياته .

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

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

المعلومات الإلكترونية: أية معلومة يمكن تخزينها ومعالجتها وتوريدها ونقلها بوسائل تكنولوجيا المعلومات بوجه خاص بالكتابة، أو الصور، أو الصوت، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات، وغيرها .

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

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

المستند الإلكتروني: هو السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتمّ إنشاؤه أو تخزينها 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: هو مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد .

الشخص: الشخص الطبيعي أو المعنوي

التطبيق الإلكتروني: هو 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: أية 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: هي 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: هي 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: يشمل ذلك بيانات الدولة والهيئات والمؤسسات العامة أو الشركات التابعة لها .

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

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

الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها .

الاختراق: هو 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:** هي 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: هو 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 وحدة عن أية خدمة إلكترونية أو مستخدمي هذه الخدمة .

الإتلاف: هو تدمير البرامج الإلكترونية سواء أكان كليا أم جزئيا، أو جعلها على نحو غير صالحة للاستعمال.

معلومات المشترك: أية معلومة موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات بما في ذلك

أ. نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.

ب. هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة.

ت. أية 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 .

مادة (2):

أ. 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 أكان 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.

ب. يجوز ملاحقة كل من يرتكب خارج فلسطين إحدى الجرائم المنصوص عليها بهذا 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 يوجد محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد في الأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية .

مادة (3):

أ. تنشأ وحدة متخصصة في الجرائم الإلكترونية في الأجهزة الشرطيّة وقوى الأمن على أن تتمّتع بصفة الضابطة القضائية، وتتولى الوحدة العامة الإشراف على مأموري الضبط القضائي كل في دائرة اختصاصه.

ب. تتولى المحاكم النظامية والوحدة العامة، وفقاً لاختصاصاتهما، بالنظر في دعاوى الجرائم الإلكترونية.

مادة (4):

أ. كل من دخل عمداً وبدون وجه حق بأية وسيلة موقعاً إلكترونياً، أو نظاماً، أو شبكة إلكترونية، أو وسيلة تكنولوجيا معلومات، أو جزء منها، أو تجاوز الدخول المصرح به،

أو استمّر في التواجد بها بعد علمه بذلك، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو بالعقوبتين كلتيهما.

ب. إذا ارتكب الفعل المحدد في الفقرة (1) من هذه المادة على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة شهور أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو بالعقوبتين كلتيهما.

ت. إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو حذفها، أو إضافتها، أو إفشاؤها، أو إتلافها، أو تدميرها، 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 بالأشغال الشاقة المؤقتة مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

ث. إذا ارتكب الفعل المحدد في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة 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، بأية 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 بالعقوبتين كلتيهما .

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 تدمير البرامج، أو حذفها، أو إتلافها، أو تعديلها، يعاقب بالأشغال الشاقة المؤقتة وبغرامة مالية لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة 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، أو بالغرامة التي لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني أو بالعقوبتين كلتيهما .

مادة (8):

كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بالغرامة التي لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

أ. كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية، أو أداة إنشاء التوقيع الإلكتروني المتعلقة بتوقيع شخص غيره، يعاقب بالحبس أو بالغرامة التي لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة ألاف دينار أردني أو بالعقوبتين كلتيهما.

ب. كل من ارتكب جريمة باستخدام أي من المذكور في الفقرة (2) من هذه المادة، يعاقب بالأشغال الشاقة المؤقتة وبالغرامة التي لا تقل عن ألفي دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (9):

أ. 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 شهور، أو بالغرامة التي لا تقل عن خمسمائة دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ب. إذا كان الانتفاع المحدد في الفقرة (1) من هذه المادة بقصد الربح، يعاقب بالحبس مدة لا تقل عن سنة، أو بالغرامة التي لا تقل عن ألف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

المادة (10):

كل من قام عمداً 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 وبالغرامة التي لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (11):

أ. كل من زور مستنداً إلكترونياً رسمياً من مستندات الدولة، أو الهيئات والمؤسسات العامة، معترفاً به قانوناً في نظام معلوماتي، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد عن عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

ب. إذا وقع التزوير فيما عدا ذلك من المستندات، وكان من شأن ذلك إحداث ضرر يعاقب بالحبس أو بالغرامة التي لا تقل عن خمسمائة دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ت. كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة التزوير حسب الأصول.

ث. كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تمّ ذلك باصطناعه، أو إتلافه، أو تعييبه، أو تعديله، أو تحويره، أو بأية طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته، أو معلوماته، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبالغرامة التي لا تقل عن خمسة آلاف دينار أردني، ولا تزيد عن عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

ج. إذا وقع التزوير أو التلاعب فيما عدا ذلك من التواقيع الإلكترونية في الفقرة (4) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ح. 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 بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (12):

أ. 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 شهور، أو بغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ب. كل من زور وسيلة تعامل إلكترونية بأية 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.

ت. كل من استخدم أو سهل استخدام وسيلة تعامل إلكترونية مزورة مع علمه بذلك، أو قبل وسيلة تعامل إلكترونية غير سارية، أو مزورة، أو مسروقة، أو مسروقة مع علمه بذلك، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.

ث. إذا قصد من ذلك استخدامها في 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 عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.

ج. إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال غيره، يعاقب مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.

مادة (13):

كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال، أو اختلاسها يعاقب بالأشغال الشاقة المؤقتة، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما .

مادة (14):

كل من توصل عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات إلى الاستيلاء لنفسه، أو لغيره على مال منقول، أو على سند، أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني، أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب، أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما .

مادة (15):

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 أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ب. إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف والاعتبار، يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلهما بالعملة المتداولة قانوناً.

مادة (16):

أ. كل من أنتج ما من شأنه المساس بالآداب العامة، أو أعده أو هيأه أو أرسله أو خزنه بقصد الاستغلال، أو التوزيع أو العرض على غيره عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، أو الرسوم المتحركة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ب. كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات؛ تدعو إلى تسهيل برامج وأفكار تروج لما من شأنه المساس بالآداب العامة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة

مالية لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ت. إذا كان الفعل المحدد في الفقرتين (1،2) من هذه المادة موجهاً إلى طفل، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

ث. إذا كان محتوى الفعل الوارد في الفقرة (1) من هذه المادة طفل أو هيئة طفل أو صور محاكاة للطفل، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (17): كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الاتجار في البشر والأعضاء البشرية أو تسهيل التعامل فيه، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (18): دون الإخلال بالأحكام الواردة في قرار بقانون مكافحة غسل الأموال وتمّويل الإرهاب، كل من أنشأ موقعاً، أو تطبيقاً أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد ارتكاب جريمة غسل الأموال وتمّويل

الإرهاب، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (19): كل من أنشأ موقعاً على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار أو الترويج للمخدرات والمؤثرات العقلية، أو ما في حكمها، أو سهل التعامل فيها، أو لبيعها، أو شرح، أو عرض طرق إنتاج المواد المخدرة، يعاقب بالحبس مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (20):

أ. كل من أنشأ موقعا إلكترونياً، أو أداره عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات؛ بقصد نشر أخبار من شأنها تعريض سلامة الدولة، أو نظامها العام، أو أمنها الداخلي أو الخارجي للخطر، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ب. كل من روّج بأية وسيلة تلك الأخبار بالقصد ذاته أو بثها أو نشرها، يعاقب بالحبس مدة لا تزيد على سنة، أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد عن ألف دينار أردني، أو بالعقوبتين كلتيهما.

ت. إذا كان الفعل الوارد في الفقرتين (1،2) من هذه المادة في حالة الطوارئ تضاعف العقوبة المقررة له.

مادة (21): كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الإساءة أو سب إحدى المقدسات أو الشعائر المقررة للأديان، أو أحد المعتقدات الدينية، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما .

مادة (22): كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الاعتداء على أي من المبادئ أو القيم الأسرية، من خلال نشر أخبار، أو صور، أو تسجيلات صوتية أو مرئية، سواء أكانت مباشرة أو مسجلة تتصل بحرمة الحياة الخاصة، أو العائلية للأفراد ولو كانت صحيحة، أو تعدى بالذم، أو القدح، أو التحقير أو التشهير بالآخرين وإلحاق الضرر بهم، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما .

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 شهور، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما .

مادة (24): كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد نشر وتوزيع معلومات تثير النعرات العنصرية، وتهدف إلى التمّييز العنصري بحق فئة معينة، أو أقدم على تهديد شخص، أو تحقيره، أو التعدي عليه بسبب انتمّائه العرقي أو المذهبي، أو اللون، أو الشكل، أو سبب الإعاقة، يعاقب بالأشغال الشاقة المؤقتة، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشر آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (25): كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، من شأنه التبرير لأعمال إبادة جماعية، أو جرائم ضد الإنسانية نصت عليها المواثيق والقوانين الدولية، أو المساعدة قصداً، أو التحريض على ارتكاب جرائم ضد الإنسانية، يعاقب بالأشغال الشاقة المؤبدة، أو الأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات .

مادة (26): كل من حاز جهازاً بغرض الاستخدام، أو برنامجاً، أو أية بيانات إلكترونية معدة، أو كلمة سر، أو تراميز دخول، أو قدمها، أو أنتجها، أو وزعها، أو استوردها، أو صدرها، أو روّج لها، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالأشغال الشاقة المؤقتة مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (27):

أ. كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار بقانون مستغلاً صلاحياته وسلطته في أثناء تأدية عمله، أو بسببها أو سهل ذلك لغيره، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

ب. كل من ارتكب من موظفي مزودي الخدمة، أياً من الجرائم المنصوص عليها في هذا القرار بقانون في أثناء تأدية عمله، أو بسببها، أو سهل ذلك لغيره، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن ثلاث سنوات، أو بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (28): كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات؛ بقصد ارتكاب أية جريمة معاقب عليها بموجب أي تشريع نافذ، أو اشترك أو حرض على ارتكابها، يعاقب بضعف العقوبة المنصوص عليها في ذلك التشريع .

مادة (29):

أ. كل من حرض، أو ساعد، أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون بأية وسيلة إلكترونية، ووقعت الجريمة بناءً على هذا التحريض أو المساعدة، أو الاتفاق، يعاقب بثلثي الحد الأقصى للعقوبة المقررة لفاعلها.

ب. إذا كان المجني عليه طفلا في الفقرة (1) من هذه المادة، يعاقب المجرم بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، ولو لم تقع الجريمة فعلا.

مادة (30): إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالغرامة التي 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 وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له .

مادة (31): يعاقب بالحبس مدة لا تقل عن ثلاثة شهور، وبغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني كل من قام باستخدام أنظمة أو موقع أو تطبيق إلكتروني؛ لتجاوز الحجب المفروض بموجب أحكام هذا القرار بقانون .

مادة (32): يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي :

أ. تزويد الجهات المختصة بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على طلب الوحدة أو المحكمة المختصة.

ب. حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية مع مراعاة الإجراءات الواردة في المادة (40)من هذا القرار بقانون.

ت. الاحتفاظ بالمعلومات عن المشترك لمدة لا تقل عن ثلاث سنوات.

ث. التعاون ومساعدة الجهات المختصة، وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ بها.

مادة (33):

أ. للوحدة 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 المحدد 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 الوحدة العامة لاتخاذ ما يلزم بشأنها.

ث. لوكيل الوحدة العامة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي، أو من يستعينون بهم من أهل الخبرة إلى أية 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.

مادة (34):

أ. للوحدة 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 المحتوى ذات الصلة بالجريمة الإلكترونية.

ب. للوحدة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات، أو جزء منه، أو أية وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة.

ت. 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.

ث. إذا استحال إجراء الضبط والتحفظ عليه بصفة فعلية؛ وحفاظاً على أدلة الجريمة يتعين استعمال كافة الوسائل المناسبة؛ لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات.

ج. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه بما في ذلك الوسائل الفنية لحماية محتواها.

ح. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم، أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويُحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف، أو مغلف مختوم، وتكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.

مادة (35):

أ. لقاضي الصلح أن يأذن للوحدة العامة بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها؛ للبحث عن الدليل المتعلق بالجريمة وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جديدة، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى الوحدة العامة.

ب. للوحدة العامة أن تأمر بالجمع والتزويد الفوري لأي بيانات بما فيها حركات الاتصالات، أو معلومات إلكترونية، أو بيانات مرور، أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات، باستعمال الوسائل الفنية المناسبة والاستعانة في ذلك عند الاقتضاء بمزودي الخدمة حسب نوع الخدمة التي يقدمها.

مادة (36): 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 (37):

أ. 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.

ب. تكون مدة الاعتراض المحدد في الفقرة (1) من هذه المادة ثلاثة شهور من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمّديد مرة واحدة فقط.

ت. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام الوحدة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.

مادة (38): لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية، بسبب طبيعة ذلك الدليل .

مادة (39): لا يجوز استبعاد أي من الأدلة المتحصل عليها بمعرفة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى لمجرد ذلك السبب، طالما أن الحصول عليها قد تمّ وفقاً للإجراءات القانونية والقضائية للتعاون الدولي .

مادة (40):

أ. لجهات التحري والضبط المختصة – إذا ما رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، بوضع أية عبارات، أو أرقام، أو صور، أو أفلام، أو أية مواد دعائية، أو غيرها، من شانها تهديد الأمن القومي، أو السلم الأهلي، 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.

مادة (41) :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 (42): تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي :

أ. اتخاذ التدابير الأمنيّة الوقائية اللازمة لحماية أنظمتها المعلوماتية، ومواقعها الإلكترونية وشبكاتها المعلوماتية، والبيانات والمعلومات الإلكترونية الخاصة بها.

ب. الإسراع في إبلاغ الجهة المختصة عن أية جريمة منصوص عليها في هذا القرار بقانون فور اكتشافها أو اكتشاف أية 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 الجهات المختصة لتنفيذ اختصاصاتها.

مادة (43):

أ. تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الإتفاقيات 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.

ب. يتوقف التعاون المشار إليه بالفقرة (1) من هذه المادة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعنية بهذا القرار بقانون.

مادة (44):

أ. 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 والإتفاقيات 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.

ب. 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 (45): مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون العقوبات النافذ، أو أي قانون آخر يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون بالعقوبات المنصوص عليها فيه .

مادة (46): كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها، أو تدخل، أو حرض على ارتكابها، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع .

مادة (47): كل من أنشأ موقعاً على الشبكة الإلكترونية، يهدف إلى الترويج لارتكاب أية جريمة من الجرائم المنصوص عليها في قانون العقوبات، أو أي من القوانين الخاصة، يعاقب بالسجن المؤقت وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (48): كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس وبغرامة لا تقل عن خمسمائة دينار ولا تزيد على ثلاثة آلاف دينار أردني أو بإحدى هاتين العقوبتين .

مادة (49): 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 ولا تزيد على خمسة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (50): كل من امتنع عن قصد في الإبلاغ، أو أبلغ عن قصد بشكل خاطئ عن جرائم معلوماتية، يعاقب بالحبس مدة لا تقل عن ستة شهور، وبغرامة لا تقل عن مائتي دينار ولا تزيد على ألف دينار أردني أو بإحدى هاتين العقوبتين .

مادة (51): إذا وقعت أية جريمة من الجرائم المنصوص عليها في هذا القرار بقانون بغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمّع وأمنه للخطر، أو تعريض حياة المواطنين للخطر، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القانون الأساسي أو القوانين أو اللوائح، أو بقصد الإضرار بالوحدة الوطنية، والسلام الاجتمّاعي، أو ازدراء الأديان أو الاعتداء على الحقوق والحريات التي يكفلها الدستور أو القانون الأساسي، تكون العقوبة الأشغال الشاقة المؤبدة أو المؤقتة .

مادة (52): 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 عليها بنصف العقوبة المقررة لها .

مادة (53): يعد مرتكبا لجريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها، في هذا القرار بقانون ويعاقب بنصف العقوبة المقررة لها .

مادة (54): تتضمن على:

أ. دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون، وحقوق الغير حَسَن النية، تصدر المحكمة قراراً بمصادرة 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.

ب. تصدر المحكمة قراراً بمدة إغلاق المحل وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم بحسب الأحوال.

مادة (55): تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أيا من الجرائم المنصوص عليها فيه سواء ارتكبت في فلسطين أم خارجها، وتعتبر الأحكام الأجنبية سابقة التكرار بحق الجاني .

مادة (56): تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون في أي من الحالات الآتية :

أ. إذا ارتكبها أو سهل ارتكابها موظف في مؤسسة خاصة، أو موظف عام مستغلا صلاحياته وسلطاته في ذلك، أو من في حكمه، كما يحكم على الموظف العام بالفصل من الوظيفة في حال الإدانة.

ب. 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.

ت. أرتكاب الجاني الجريمة من خلال عصابة منظمة.

ث. التغرير بالأحداث ومن في حكمهم واستغلالهم.

ج. إذا وقعت الجريمة على نظام معلومات، أو موقع إلكتروني، أو شبكة معلوماتية تتعلق بتحويل الأموال، أو بتقديم خدمات الدفع والتقاص، أو التسويات أو بأي من الخدمات المصرفية المقدمة من البنوك والشركات المالية.

مادة (57): يعفى من العقوبات المنصوص عليها في هذا القرار بقانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأية 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 (58): تتولى الوزارة وفقا 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 (59): يلغى كل ما يتعارض مع أحكام هذا القرار بقانون .

مادة (60): يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره .

مادة (61): 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: 2017/06/24) ميلادية

الموافق: 29/رمضان/(2017) هجرية

محمود عباس/ رئيس دولة فلسطين

رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

ملحق رقم (7): قرار بقانون رقم (10) لسنة 2018 م بشأن الجرائم الإلكترونية:

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 العقوبات رقم (74) لسنة (1936م) 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 (1996م) وعلى أحكام قانون الإجراءات الجزائية رقم (3) لسنة (2001م) وتعديلاته، وعلى أحكام القرار بقانون رقم (18) لسنة (2015م)، بشأن مكافحة المخدرات والمؤثرات العقلية، وعلى أحكام القرار بقانون رقم (20) لسنة (2015م)، بشأن مكافحة غسل الأموال وتمّويل 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 2018/04/17 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 العالمية (الإنترنت).

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

المستند الإلكتروني: السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتمّ 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): تتضمن على:

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): تتضمن على:

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): تتضمن على:

أ. 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 استمّر 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.

ب. 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.

ت. 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.

ث. 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): تتضمن على:

أ. 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.

ب. 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.

ت. 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): تتضمن على:

أ. 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.

ب. 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:

أ. 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.

ب. 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.

ت. كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة استعمال السند المزور وفق قانون العقوبات النافذ.

ث. كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تمّ 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.

ج. 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.

ح. 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.

خ. 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): تتضمن على:

أ. 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.

ب. 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.

ت. 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.

ث. إذا تمّ 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 عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (15): تتضمن على:

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 أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

ب. 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:

أ. 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.

ب. 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.

ت. 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 وتمّويل الإرهاب النافذ، يعاقب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو إحدى وسائل تكنولوجيا المعلومات بقصد:

أ. 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.

ب. القيام بارتكاب جريمة تمّويل 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:

أ. لكل إنسان حق التعبير عن رأيه بالقول أو الكتابة أو التصوير أو غير ذلك من وسائل التعبير والنشر وفقاً للقانون.

ب. 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.

ت. 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.

ث. لا يجوز فرض قيود على الصحافة أو مصادرتها أو وقفها أو إنذارها أو إلغاؤها إلا وفقاً للقانون، وبموجب حكم قضائي .

مادة (22): تتضمن على:

أ. يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته.

ب. 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 التمّييز العنصري بحق فئة معينة بسبب انتمّائها 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): تتضمن على:

أ. 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.

ب. 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:

أ. تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة.

ب. 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.

ت. الاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات لغايات ما ورد في الفقرة (1) من هذه المادة.

ث. التعاون ومساعدة الجهات المختصة وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ المؤقت بها .

مادة (32): تتضمن من الآتي:

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.

مادة (33): تتضمن من:

أ. 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.

ب. 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 .

ت. 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.

ث. إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات.

ج. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها.

ح. 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): تتضمن من الآتي:

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.

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): تتضمن على:

أ. 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.

ب. تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمّديد مرة واحدة فقط.

ت. 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 تمّ وفقاً للإجراءات القانونية والقضائية للتعاون الدولي .

مادة (39): تتضمن على:

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 .

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:

أ. اتخاذ التدابير الأمنيّة 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 .

مادة (42): تتضمن على:

أ. 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.

ب. 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): تتضمن على:

أ. 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.

ب. 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:

أ. مدة إغلاق المحل، وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم بحسب الأحوال.

ب. 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:

أ. 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.

ب. ارتكاب الجاني الجريمة من خلال عصابة منظمة.

ت. التغرير أو استغلال من لم يكمل الثامنة عشر سنة ميلادية.

ث. 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): يُعفى 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): تتضمن على:

أ. يلغى القرار بقانون رقم (16) لسنة (2017)م، بشأن الجرائم الإلكترونية.

ب. 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: 2018/04/29 ميلادية الموافق: 13/شعبان/1439 هجرية

محمود عباس رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

ملحق رقم (8): 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 (2018 م)، بشأن الجرائم الإلكترونية، وبناءً على الصلاحيات المخولة لنا، وتحقيقاً للمصلحة العامة، أصدرنا القرار بقانون الآتي :

مادة (1): يشار إلى القانون 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: 2020/09/01 ميلادية الموافق: 13/محرم/1442 هجرية

محمود عباس رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

ملحق رقم (9): قرار بقانون رقم (11) لسنة (2007م) بشأن الأمن الوقائي:

المادة (1): التعاريف:

لغايات تطبيق أحكام هذا القانون يكون للكلمات والعبارات الواردة فيه المعاني المخصصة لها أدناه من لم تدل على خلاف ذلك:

السلطة الوطنية: السلطة الوطنية الفلسطينية.

الرئيس: رئيس السلطة الوطنية الفلسطينية.

الوزارة المختصة: وزارة الداخلية.

الوزير المختص: وزير الداخلية.

الإدارة العامة للأمن الوقائي: جهاز الأمن الوقائي.

المدير العام: مدير عام الإدارة العامة للأمن الوقائي.

الفرد: الضابط أو ضباط الصف والعناصر المعينين في الأمن الوقائي.

المادة (2): جهاز الأمن الوقائي:

أ. جهاز الأمن الوقائي: هو إدارة عامة أمنية نظامية ضمن قوى الأمن الداخلي التي تتبع الوزارة المختصة وتعمل في مجال الأمن.

ب. يكون المقر الدائم للإدارة العامة في مدينة القدس، ولها مقران مؤقتان في مدينتي رام الله وغزة، ويجوز لها فتح إدارات فرعية في المدن الأخرى.

المادة (3): سريان القانون:

تسري أحكام هذا القانون على جميع العاملين في الإدارة العامة للأمن الوقائي، ويصادق مجلس الوزراء على الهيكلية التنظيمية لها.

المادة (4): تعيين المدير العام:

أ. يُعين المدير العام ونائبه بقرار يصدره رئيس السلطة الوطنية بناءً على توصية من الوزير المختص وتنسيب مدير عام الأمن الداخلي وتوصية لجنة الضباط ، ويؤديا اليمين القانونية أمام الرئيس قبل بدء أعمالها.

ب. مدة تعيين المدير العام أربع سنوات ويجوز تمّديدها إضافية بقرار من الرئيس.

المادة (5): سلطة الإشراف:

أ. يتولى المدير العام سلطة الإشراف على أعمال الإدارة العامة للأمن الوقائي والعاملين فيها، وتشكيل اللجان الضرورية لحسن سير عملها، وله أن يفرض بعض اختصاصاته إلى نائبه.

ب. يكون المدير العام مسئولا أمام الوزير المختص ومدير عام الأمن الداخلي عن عمله وعن المحافظة على سرية ونشاط الإدارة العامة للأمن الوقائي وفعالياتها.

المادة (6): مهام الإدارة العامة للأمن الوقائي:

بما لا يتعارض مع القوانين السارية تعتبر الإدارة العامة للأمن الوقائي الجهة المكلفة بما يلي:

أ. العمل على حماية الأمن الداخلي الفلسطيني.

ب. متابعة الجرائم التي تهدد الأمن الداخلي للسلطة الوطنية و /أو الواقعة عليه، والعمل على منع وقوعها.

ت. الكشف عن الجرائم التي تستهدف الإدارات الحكومية والهيئات والمؤسسات العامة والعاملين فيها.

المادة (7): صفة الضبطية القضائية:

يكون لضباط وضباط صف الإدارة العامة للأمن الوقائي في سبيل تسهيل مباشرة اختصاصاتهم المقررة بموجب أحكام هذا القانون صفة الضبطية القضائية.

المادة (8): احترام الحقوق والحريات:

على الإدارة العامة للأمن الوقائي الالتزام باحترام الحقوق والحريات والضمانات المنصوص عليها في القوانين الفلسطينية المواثيق والمعاهدات الدولية.

المادة (9): مراكز التوقيف:

يحدد الوزير المختص مراكز التوقيف الثابتة للإدارة العامة للأمن الوقائي بالتنسيق مع المدير العام، ويُعلم وزير العدل والنائب العام بحالتها وبأي تغيير يطرأ بشأنها، وتُعتبر تلك المراكز مراكز قانونية للتوقيف.

المادة (10): السرية:

أ. لا يجوز الإطلاع على تحريات ومعلومات الإدارة العامة للأمن الوقائي إلا بإذن خاص من الوزير المختص أو مدير عام الأمن الداخلي أو تنفيذاً لحكم قضائي.

ب. بما لا يتعارض مع أحكام الفقرة (1) علاه تعتبر المعلومات والأنشطة والوثائق المتعلقة بعمل الإدارة العامة للأمن الوقائي سرية لا يجوز إفشاؤها.

المادة (11): التعيين:

أ. 1.يعين مساعدو المدير العام ومديرو الدوائر في الأمن الوقائي بقرار يصدر عن الوزير لمختص بناء على نتسيب المدير العام وموافقة مدير عام الأمن الداخلي .

ب. 2.يخضع جميع أفراد الإدارة العامة للأمن الوقائي للتعليمات والضوابط والإجراءات الأمنيّة التي تصدر عن المدير العام.

المادة (12): التقرير يرفع الوزير المختص لرئيس السلطة الوطنية ورئيس الوزراء تقريراً دورياً كل ثلاثة أشهر عن أعمال الإدارة العامة للأمن الوقائي.

المادة (13): إصدار اللوائح التنفيذية يصدر مجلس الوزراء اللوائح التنفيذية اللازمة لتنفيذ أحكام هذا القانون.

المادة (14): الإلغاء يلغى كل من يتعارض مع أحكام هذا القانون.

المادة (15): العرض على المجلس التشريعي يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره.

المادة (16): التنفيذ والنفاذ والنشر على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام القانون ويعمل به من تاريخ صدوره وينشر في الجريدة الرسمية.

قائمة الجداول:

جدول رقم (1.3): توزيع أفراد عينة الدراسة حسب متغيرات الدراسة. 55

جدول رقم (2.3): نتائج معامل ارتباط بيرسون لمصفوفة ارتباط فقرات درجة الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية 57

جدول رقم (3.3): نتائج معامل ارتباط بيرسون لمصفوفة ارتباط فقرات دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة من وجهة نظر موظفي جهاز الأمن الوقائي 57

جدول رقم (4.3): نتائج معامل ارتباط بيرسون لمصفوفة ارتباط فقرات أكثر أنواع الجرائم الإلكترونية التي تتعامل معها في جهاز الأمن الوقائي 57

جدول رقم (5.3): نتائج معامل ارتباط بيرسون لمصفوفة ارتباط فقرات درجة الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية..... 58

جدول رقم (6.3): نتائج معامل ارتباط بيرسون لمصفوفة ارتباط فقرات الحلول التي تساعد على الحد من الجريمة الإلكترونية 58

جدول رقم (7.3): نتائج معامل الثبات للمجالات 59

جدول رقم (1.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية 61

جدول رقم (2.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لدوافع ارتكاب الجريمة الإلكترونية من قبل الجناة..... 63

جدول رقم (3.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لأنواع الجرائم الإلكترونية التي تتعامل معها في جهاز الأمن الوقائي 65

جدول رقم (4.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية 66

جدول رقم (5.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لأهم الحلول التي تساعد على الحد من الجريمة الإلكترونية 68

جدول رقم (6.4): نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية حسب متغير الجنس 70

جدول رقم (7.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير المؤهل العلمي 70

جدول رقم (8.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير المؤهل العلمي 71

جدول رقم (9.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير العمر 71

جدول رقم (10.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير العمر 72

جدول رقم (11.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير الرتبة العسكرية..... 73

جدول رقم (12.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير الرتبة العسكرية 73

جدول رقم (13.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية تعزى لمتغير عدد سنوات الخدمة.... 74

جدول رقم (14.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير عدد سنوات الخدمة..... 74

جدول رقم (15.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لمستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي 75

جدول رقم (16.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية يعزى لمتغير طبيعة العمل في جهاز الأمن الوقائي 75

قائمة الملاحق:

ملحق رقم (1) الإستبانة في صورتها الاولية.....114
ملحق رقم (2) الإستبانة في صورتها النهائية 120
ملحق رقم (3) محكمي الإستبانة.....126
ملحق رقم(4) أسئلة المقابلة.....127
ملحق رقم (5) نتائج الإجابات على المقابلة 130
ملحق رقم (6) قانون الجرائم الإلكترونية رقم (16) لسنه (2017).....140
ملحق رقم (7) قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية 169
ملحق رقم (8) قرار بقانون رقم (28) لسنة (2020م) بتعديل قرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الإلكترونية 197

قائمة المحتويات:

إقرار: ..... أ

الشكر والتقدير ..... ب

الملخص بالعربية: ..... ج

الملخص بالانجليزية..... هـ

الفصل الأول: الإطار العام للدراسة 1

1.1 مقدمة: 1

1.2 مشكلة الدراسة: 3

1.3 أهمية الدراسة: 4

1.4 أهداف الدراسة: 5

1.6 أسئلة الدراسة وفرضياتها:..... 5

1.7 حدود الدراسة: 7

الفصل الثاني: الإطار النظري والدراسات السابقة وذات العلاقة 8

2.1 مقدمة: 8

2.2 مفهوم الأمن: 9

2.3 مفهوم الأجهزة الأمنيّة ونشأتها: 10

2.5 تأثير الإحتلال على عمل الأجهزة الأمنيّة الفلسطينية: 14

2.6 نشأت جهاز الأمن الوقائي الفلسطيني وأهدافه: 16

2.7 دور الأمن الوقائي في مواجهة الجرائم الإلكترونية: 18

2.8 الجهود والإتفاقيات الدوليّة والإقليميّة والعربيّة المبذولة لمكافحة الجريمة الإلكترونية: 20

2.9 دور مؤسسات المجتمّع المدني في دعم المؤسسة الأمنيّة الفلسطينيّة لمكافحة الجريمة الإلكترونية: 21

2.10 الجريمة الإلكترونية: 23

1.2.10 مفهوم الجريمة: 24
2.2.10 مفهوم الجريمة الإلكترونية: 25
3.2.10 التطور التاريخي لجرائم الكمبيوتر والانترنت: 27
4.2.10 خصائص الجرائم الإلكترونية وأركانها: 28
5.2.10 أطراف الجريمة الإلكترونية: 30
6.2.10 أنواع الجريمة الإلكترونية وصورها: 33
7.2.10 دوافع ارتكاب الجريمة الإلكترونية: 35
8.2.10 الصعوبات التي تواجه مكافحة الجريمة الإلكترونية في فلسطين: 36
9.2.10 الإطار القانوني والمؤسساتي لمكافحة الجريمة الإلكترونية في فلسطين: 37
10.2.10 النظريات المفسرة للجريمة الإلكترونية: 40
2.11 الدراسات السابقة وذات العلاقة: 47
2.12 أوجه التشابه والإختلاف بين الدراسة الحالية والدراسات السابقة: 52
الفصل الثالث: الطريقة والإجراءات 53
1.3 منهج الدراسة: 53
3 .2 مجتمّع الدراسة: 53
3 .3 عينة الدراسة: 54
3 .4 وصف متغيرات أفراد العينة: 54
5.3 أدوات الدراسة: 55
5.3.1 صدق الأداة: 56
5.3.2 ثبات الاداة: 58
3 . 6 إجراءات الدراسة: 59
3 . 7 المعالجة الإحصائية: 59
الفصل الرابع: عرض نتائج الدراسة 60
4 . 1 مقدمة: 60

4 . 2 عرض نتائج أسئلة الدراسة:..... 61
1.2.4 النتائج المتعلقة بالسؤال الأول: ما مستوى الاجراءات المتبعة في جهاز الأمن الوقائي للحد من الجريمة الإلكترونية ؟..... 61
2.2.4 النتائج المتعلقة بالسؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة؟ 63
3.2.4 النتائج المتعلقة بالسؤال الثالث: ما أنواع الجرائم الإلكترونية التي تعامل معها في جهاز الأمن الوقائي؟..... 64
4.2.4 النتائج المتعلقة بالسؤال الرابع: ما الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية؟..... 66
5.2.4 النتائج المتعلقة بالسؤال الخامس: ما أهم الحلول التي تساعد على الحد من الجريمة الإلكترونية؟..... 67
6.2.4 النتائج المتعلقة بالفرضيات:..... 69
7.2.4: نتائج المقابلات المُعمقة:..... 76
الفصل الخامس: مناقشة النتائج والتوصيات 81
1.5 مقدمة: 81
2.5 مناقشة أسئلة الدراسة:..... 81
2.2.5 مناقشة النتائج المتعلقة بالسؤال الثاني: ما دوافع ارتكاب الجريمة الإلكترونية من قبل الجناة؟.. 86
3.2.5 مناقشة النتائج المتعلقة بالسؤال الثالث: ما أنواع الجرائم الإلكترونية التي تعامل معها في جهاز الأمن الوقائي؟..... 89
4.2.5 مناقشة النتائج المتعلقة بالسؤال الرابع: ما الصعوبات التي تواجه جهاز الأمن الوقائي في الحد من الجريمة الإلكترونية؟..... 90
5.2.5 مناقشة النتائج المتعلقة بالسؤال الخامس: ما أهم الحلول التي تساعد في الحد من الجريمة الإلكترونية؟..... 94
3.5 مناقشة نتائج فرضيات الدراسة:..... 97
4.5 ملخص النتائج:.....102
5.5 توصيات الدراسة:.....104

قائمة المصادر والمراجع: 106
قائمة الملاحق..... 114
قائمة الجداول: 203
قائمة المحتويات:..... 206