جامعة النجاح الوطنية
كليَّة الدّراسات العليا

دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية

إعداد
ياسر حسين سليمان ابو لبدة

اشراف
د. عمر البزور

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، من كلية الدراسات العليا في جامعة النجاح الوطنية، نابلس– فلسطين.
2025

دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية

إعداد

ياسر حسين سليمان ابو لبدة

نوقشت هذه الرسالة بتاريخ 2025/06/19م، وأجيزت:

د. عمر البزور	
المشرف الرئيسي	التوقيع
د. مرسي عبد الرازق	
المشرف الخارجي	التوقيع
د. بهاء الأحمد	
المشرف الداخلي	التوقيع

الإهداء

إلى من غرسَا في قلبي بذور الطموح، وسقَياه بالعطاء والحنان، إلى من كانت دعواتهما زادي في دروب الحياة... إلى **والديّ رحمه ووالدتي حفظها الله واطال في عمرها**

إلى رفيقة الدرب، ومصدر السكينة، من شاركتني الأحلام، التي كانت السند والصوت الذي لا يخفت في كل المراحل.. إلى **زوجتي العزيزة.**

إلى **ابنتي فلذة كبدي** من أجلها أطمح، ومنعينيها أستمد أملي... أنتي الدافع، أنتي الغاية، وأنتي الامتداد.

إلى **إخوتي وأخواتي،** الذين كانوا دائماً اليد الحانية والصوت المشجّع.

إلى **زملائي وأصدقائي** الذين رافقوني بالفكر، وبالدعم، كنتم العزم في لحظات التردد.

إليكم جميعاً... أهدي ثمرة هذا الجهد، وفاء ومحبة وامتنان.

الشكر والتقدير

أتقدّم بجزيل الشكر وخالص الامتنان لمشرفي الأكاديمي...

الدكتور عمر البزور

الذي كان لنصائحه وتوجيهاته العلمية الأثر الكبير في إخراج هذه الرسالة على النحو الذي أطمح إليه.

لقد كان مثالاً للعطاء العلمي، والدقة البحثية.

كما أعبّر عن تقديري العميق **لأعضاء الهيئة التدريسية في كلية القانون – جامعة النجاح الوطنية**، الذين تركوا في مسيرتي الأكاديمية بصمات لا تُنسى، وكانوا منارات علمٍ وفكرٍ أغنوا تجربتي، وفتحوا أمامي آفاق المعرفة والبحث.

ولا يفوتني أن أتوجه بالشكر والعرفان إلى **أعضاء لجنة مناقشة هذه الرسالة**، الذين شرفوني بقراءتهم المستفيضة، وملاحظاتهم القيمة، ومداخلاتهم العلمية التي أثرت العمل وأغنته.

لكم جميعاً، كل الاحترام والتقدير.

الإقرار

أنا الموقع أدناه مقدمة الرسالة التي تحمل عنوان:

دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية

أقر بأن ما اشتملت عليه هذه الرسالة هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة اليه حيثما ورد، وأن هذه الرســـالة ككل أو أي جزء منها لم يقدم من قبل لنيل أية درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

اسم الطالبة: **ياسر حسين سليمان ابو لبدة**

التوقيع: ياسر ابو لبدة

التاريخ: **2025/06/19**

فهرس المحتويات

فهرس الجداول

فهرس الملاحق

دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية

إعداد

ياسر حسين سليمان ابو لبدة

اشراف

د. عمر البزور

الملخَّص

هدفت هذه الدراسة للتعرف إلى دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية، وتكوّن مجتمع الدراسة من من جميع منتسبي وحدة الجرائم الالكترونية (بكافة مسمياتهم الوظيفية) في محافظة رام الله، حيث بلغ عدد مجتمع الدراسة (250)، وتم استخدام أسلوب العينة العشوائية البسيطة، وقام الباحث بتوزيع الاستبيان على افراد العينة البالغ عددهم (148) وتم استرداد (148) استبانة صالحة للتحليل الاحصائي، وتم استخدام الاستبانة أداة الدراسة لجمع البيانات؛ من خلال المنهج الوصفي التحليلي.

وتوصلت الدراسة إلى أنّ وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية تسهم في التوعية بالجرائم الالكترونية متوسطة، وأن الأساليب المستخدمة من قبل وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية لمكافحة الجرائم الإلكترونية متوسطة، وكذلك فإن آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية متوسطة، وأن وحدة الجرائم الإلكترونية تقوم بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية بدرجة متوسطة، ويتضح كذلك أن المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية مرتفعة.

ومن أهم توصيات الدراسة: على وحدة الجرائم الإلكترونية تنظيم ورش عمل تفاعلية تستهدف قطاعات معينة من المجتمع مثل المدارس والجامعات، بالإضافة إلى التعاون مع وسائل الإعلام المحلية لتوسيع نطاق

التوعية، وضرورة قيام وحدة الجرائم الإلكترونية بتطوير محتوى مرئي تفاعلي حول كيفية حماية الأفراد لأنفسهم عبر الإنترنت وتوزيعه عبر منصات مثل فيسبوك، إنستغرام، ويوتيوب.

الكلمات المفتاحية: وحدة الجرائم الالكترونية، المؤسسة الأمنية الفلسطينية، الجرائم الالكترونية.

الفصل الأول

مقدمة الدراسة والإطار النظري

1.1 المقدمة

تشير الجرائم الإلكترونية إلى الأنشطة غير القانونية التي تُمارَس عبر الإنترنت أو باستخدام التكنولوجيا الرقمية، مثل الاختراق والاحتيال والابتزاز الإلكتروني، تزايدت هذه الجرائم بشكل ملحوظ في السنوات الأخيرة نتيجة للتطور السريع في التكنولوجيا وازدياد الاعتماد على الإنترنت في مختلف القطاعات، بحيث تشمل الجرائم الإلكترونية سرقة الهوية، خرق البيانات، والتلاعب بالمعلومات المالية، وتعاني الحكومات والمؤسسات والأفراد من آثارها السلبية التي تتراوح بين الخسائر المالية إلى التهديدات الأمنية، إذ تشير الأدبيات إلى أن التصدي لهذه الجرائم يتطلب إطاراً قانونياً متيناً وتعاوناً دولياً، بجانب تعزيز الوعي العام بمخاطر الإنترنت، مع الإشارة إلى الحاجة لتحديث مستمر للسياسات وتطوير التكنولوجيا المستخدمة في التحقيق والمراقبة، من خلال الشراكة ما بين القطاعين العام والخاص لتعزيز الأمن السيبراني، من خلال تبادل الموارد والخبرات لتحسين التصدي للهجمات السيبرانية وتقليل تأثيرها السلبي على المجتمع (Imran, 2023).

ومن هنا تُعَد الجرائم الإلكترونية من أبرز التحديات التي تواجه المجتمعات في العصر الرقمي، حيث تطال تأثيراتها الأفراد والمؤسسات والحكومات على حدٍ سواء، إذ تتمثل هذه الجرائم في أنشطة غير قانونية تُمارَس عبر التكنولوجيا الرقمية، مثل الاحتيال الإلكتروني، اختراق البيانات، والابتزاز عبر الإنترنت، وقد أدت العولمة الرقمية إلى تسهيل انتشار هذه الجرائم عبر الحدود، مما يزيد من صعوبة مواجهتها، فالجرائم الإلكترونية تتسم بتطورها السريع، حيث يعتمد المجرمون على التقنيات الحديثة كالأدوات الخبيثة والعملات الرقمية لتحقيق أهدافهم، وهذا التطور يتجاوز أحياناً قدرة الأطر القانونية الحالية على التعامل مع التهديدات الناشئة، علاوة على ذلك، تواجه الدول تحديات كبيرة في التعاون الدولي بسبب تفاوت التشريعات وصعوبة

تتبع الجرائم التي تُرتكب عبر أنظمة مجهولة الهوية (Widodo, Adam, Hsb, Prayitno, & Bhaskoro, 2024).

فالجرائم الإلكترونية تمثل تحدياً معقداً يتطلب استجابة شاملة ومتعددة الجوانب، للمساهمة بشكل فعال في رفع الوعي لدى الجمهور حول المخاطر المرتبطة بالجرائم الإلكترونية (نبيل، 2024)، مما يعزز في نشر الوعي والتوعية للمواطنين بأساليب الحماية من هذه الجرائم، إذ أن غياب الرقابة الكافية على الفضاء الإلكتروني قد أسهم في زيادة الجرائم الإلكترونية، مما يشير إلى ضرورة تطوير التشريعات لمواكبة التطورات السريعة في هذا المجال (أبو القاسم، 2024).

في هذا السياق، تتجلى أهمية تعزيز دور وحدة الجرائم الإلكترونية في التصدي لهذه الجرائم بالتعاون مع الجهات التشريعية، وعليه وقد جاء قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية في فلسطين لينظم عملية مكافحة الجرائم الالكترونية من خلال إنشاء وحدة مختصة بمكافحة الجريمة الإلكترونية في فلسطين تكون تابعة للمؤسسة الأمنية الفلسطينية، إذ عرفّت مواد القانون الجريمة الالكترونية على أنها مجموعة من الجرائم التي تتم عبر استخدام تكنولوجيا المعلومات والشبكات الإلكترونية بطريقة غير قانونية، وتشمل مجموعة واسعة من الأفعال التي قد تضر بالأفراد أو المؤسسات أو الدولة (قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية).

وتعد "وحدة الجرائم الإلكترونية" في فلسطين إحدى الوحدات الأمنية المتخصصة التي تم إنشاؤها بموجب قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، حيث أوكلت إليها مهمة التصدي للجرائم الإلكترونية بمختلف أشكالها، وتعمل الوحدة تحت إشراف النيابة العامة، وتتكامل جهودها مع اختصاصات المحاكم النظامية في التحقيق والملاحقة القانونية لمرتكبي هذه الجرائم، كما نصت عليه المادة (3) من القانون، وبالنظر إلى طبيعة هذه الجرائم وأبعادها التقنية، يُعد دور الوحدة حيوياً في حماية الأفراد والمؤسسات

من التهديدات التي تفرضها تكنولوجيا المعلومات (قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية في فلسطين).

وعلى الرغم من تلك الجهود إلا أن هناك العديد من المعوقات الفنية والقانونية لمكافحة الجرائم الإلكترونية، والتي تشمل نقص التشريعات المناسبة وضعف القدرات الفنية، وبالتالي تمثل تحديات كبيرة في مواجهة هذه الجرائم (الشوابكة، 2022)، مما يتطلب ضرورة تحديث الأدوات القانونية والتقنية في المؤسسة الأمنية الفلسطينية لمواكبة هذا النوع من الجرائم، ويبرز الحاجة إلى تحسين قدرات وحدة الجرائم الإلكترونية في تطوير استراتيجيات وقاية فعالة وحماية البيانات الشخصية، وتعزيز آليات التعاون الدولي في هذا المجال، فالجرائم الإلكترونية ليست مجرد مشكلة تقنية فحسب، بل هي معضلة تشمل أيضاً التوعية، والتشريعات، والتقنيات اللازمة للتعامل معها، مما يفرض على وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية أن تواجه تحديات متعددة تتطلب تكاملاً بين القطاعات المختلفة وتحديثاً مستمراً للأدوات والاستراتيجيات لمجابهة هذه الجرائم.

من خلال ما تقدم يستهدف الباحث من خلال الدراسة الحالية البحث في دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية.

1.2 الإطار النظري

مفهوم الجرائم الالكترونية:

تتباين وجهات النظر حول تعريف الجريمة الإلكترونية تبعاً للزاوية التي يتم من خلالها النظر إلى هذا النوع من الجرائم، فمن جهة، يتم تصنيفها بأنها الأنشطة المتعلقة بالحاسوب إلى أنواع مختلفة، مع تحديد تصور خاص للجريمة لكل نوع، ومن جهة أخرى، يمكن أن يكون الحاسوب أو المعلومات المخزنة فيه هدفاً للجريمة، أو يمكن أن يكون أداة لتنفيذها، وبناءً على ذلك، يمكن تعريف الجريمة الإلكترونية بأنها أي جريمة ترتكب

باستخدام نظام حاسوبي أو داخله، وتشمل جميع الجرائم التي يمكن ارتكابها في البيئة الرقمية (بن سويد، 2024).

ويُمكن تعريف الجريمة الإلكترونية بأنها "الفعل الإجرامي الذي يُرتكب باستخدام التقنيات والوسائل الإلكترونية والأنظمة المعلوماتية، حيث يتم استغلال شبكات الاتصال الحديثة لتحقيق أغراض غير مشروعة تُستغل فيها القدرات التكنولوجية للتغلب على الحواجز الجغرافية والقانونية، مما يجعلها جريمة عابرة للحدود وصعبة الكشف والملاحقة؛ إذ يُستخدم فيها كل من أحدث التقنيات والوسائل الرقمية لتأمين تنفيذ الأفعال الإجرامية بطريقة تُظهر تعقيدها وخطورتها في العصر الرقمي الحديث، وهو ما يستدعي ضرورة تبني آليات قانونية خاصة لمواجهتها" (فهمي، 2025).

وتُعرّف الجرائم الإلكترونية بأنها الأفعال الإجرامية التي تُرتكب ضد البيانات أو وسائل تخزين البيانات أو أنظمة الحاسوب أو مزودي الخدمات باستخدام التكنولوجيا الرقمية، وتشمل هذه الجرائم أشكالاً متعددة مثل الوصول غير المصرح به، العبث بالبيانات أو أنظمة الحاسوب، الاحتيال، التزوير، اعتراض البيانات بشكل غير قانوني، استخدام الأجهزة غير القانونية، استغلال الأطفال، وانتهاك حقوق الملكية الفكرية، ويمكن أن تُستخدم الحواسيب كأداة لارتكاب الجريمة أو كهدف لها (Massawe & Mshana, 2023).

يشير الرواشدة (2025) إلى الجريمة الإلكترونية على أنها: "أي فعل إجرامي يتم باستخدام الحواسيب أو الشبكات الإلكترونية لارتكاب جريمة أو تسهيلها، سواء كان ذلك عن طريق الوصول غير المشروع إلى البيانات، أو التلاعب بالمعلومات، أو الاحتيال الإلكتروني، أو نشر الفيروسات والبرامج الضارة، أو انتهاك الخصوصية، وتتميز هذه الجرائم بتطورها السريع، وصعوبة تعقب مرتكبيها نظراً للطبيعة الافتراضية للفضاء الإلكتروني، مما يجعل مكافحتها تتطلب أدوات قانونية وتقنية متقدمة".

ويتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، وتعرف الجرائم الالكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية (صالحي، 2024).

وهناك من عرّف الجرائم الالكترونية على أنها: تلك الجرائم التي تتم من خلال أجهزة الكمبيوتر بهدف القرصنة أو التصيّد الاحتيالي، وتُستخدم للإضرار بالأشخاص من خلال الوصول إلى معلومات شخصية أو أسرار تجارية وغيرها (محمد، 2021).

وهي كذلك فعل غير مشروع بتطبيق آلية وتقنية باستعمال بعض الأساليب التكنولوجية بفضل الانترنت قصد التعدي على ممتلكات الآخرين أو بدافع ربحي او أخرى (Fansher & Randa, 2019).

وتُعرَّف الجريمة الإلكترونية بناءً على ما جاء في مواد قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية الفلسطيني بأنها أي نشاط غير قانوني أو مُخالف للقانون يتم تنفيذه باستخدام وسائل التكنولوجيا الحديثة، مثل الإنترنت أو الشبكات الإلكترونية أو أجهزة الكمبيوتر، وتشمل هذه الجرائم مجموعة متنوعة من الأفعال التي قد تضر بالأفراد أو المؤسسات، مثل اختراق الأنظمة أو سرقة البيانات الشخصية أو المالية، التلاعب بالمعلومات، أو نشر الفيروسات والبرمجيات الخبيثة، يمكن أن تكون هذه الجرائم محلية أو دولية، وتمثل تهديداً كبيراً للأمن السيبراني والاستقرار الرقمي للمجتمعات.

وحدة الجرائم الإلكترونية الفلسطينية:

وفقاً لقرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته، تم تأسيس "وحدة الجرائم الإلكترونية" في جهاز الشرطة وقوى الأمن الفلسطيني، التي تُمثل الجهة المسؤولة عن مكافحة الجرائم الإلكترونية، وتتولى هذه الوحدة التعامل مع الجرائم المرتكبة باستخدام تكنولوجيا المعلومات، مثل اختراق الأنظمة الإلكترونية أو التلاعب بالبيانات أو سرقة المعلومات، وتخضع هذه الوحدة للإشراف القضائي من

النيابة العامة، كما تحدد المادة (3) من القانون اختصاصات المحاكم النظامية والنيابة العامة في النظر في القضايا المتعلقة بالجرائم الإلكترونية، بما في ذلك التحقيق في القضايا ومتابعة الإجراءات القانونية ذات الصلة[1].

قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية في فلسطين وتعديلاته:

تشمل الجرائم الإلكترونية التي يعاقب عليها القانون الدخول غير المصرح به إلى المواقع الإلكترونية أو النظم أو الشبكات الإلكترونية (المادة 4)، حيث يعاقب الشخص الذي يدخل عمداً إلى هذه النظم أو يستمر في التواجد فيها بعد أن علم بعدم حصوله على تصريح بذلك، بالحبس أو غرامة مالية، وإذا تعلق الأمر بالبيانات الحكومية، تكون العقوبة أشد حيث تتراوح بين الحبس والغرامة العالية، كما يعاقب القانون من يقوم بتعطيل أو إعاقة الوصول إلى الخدمات أو الأنظمة الإلكترونية باستخدام وسائل تكنولوجيا المعلومات (المادة 5)، وكذلك من يقوم بتخريب البيانات أو تعديلها أو إتلافها عن عمد، وهو ما يمكن أن يؤدي إلى عقوبات بالسجن والغرامات المالية الكبيرة (المادة 6)، علاوة على ذلك، تشمل الجرائم الإلكترونية "الالتقاط" غير المشروع للبيانات المرسلة عبر الشبكات الإلكترونية، والتي يعاقب عليها بالحبس أو غرامة مالية (المادة 7).

ومن الجرائم الإلكترونية الأخرى التي يعاقب عليها القانون، فك التشفير غير المشروع للبيانات أو التلاعب في أدوات التشفير، حيث تتراوح العقوبات من الحبس والغرامات المالية إلى السجن في الحالات الأكثر خطورة (المادة 8)، كذلك يعاقب القانون من يقوم باستخدام أو الاستفادة من خدمات الاتصال الإلكترونية بشكل غير قانوني (المادة 9)، بالإضافة إلى معاقبة من يقوم بتزوير المستندات الإلكترونية أو تقديم بيانات غير صحيحة بغرض الحصول على خدمات بطريقة غير قانونية (المادة 10).

[1] قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته.

بناءً على هذه المواد القانونية، فإن الجرائم الإلكترونية تشكل تهديداً خطيراً للأمن الإلكتروني، سواء على مستوى الأفراد أو المؤسسات، ويتخذ القانون الفلسطيني إجراءات صارمة لمكافحة هذه الجرائم وحماية المجتمع من أضرارها.

اركان الجرائم الالكترونية:

للجريمة الإلكترونية عدد من الأركان، كما أشار إليها فتح الله (2021)، وهي كما يلي:

1. الركن المادي: ترتبط بجرائم الإلكترونية المرتبطة بالمشكلات المثارة، وهي ترتبط بالأنظمة المستخدمة إلكترونياً بطريقة غير شرعية، منها سرقة المعلومات للبطاقة الإئتمانية، تدمير المعلومات السرية ونشرها.
2. الركن المعنوي: ويقصد به الحالة النفسية والمزاجية لمرتكبي الجريمة الإلكترونية، مع الربط بين الجانب المادي لمرتكب الجريمة وشخصيته.
3. الركن الشرعي: ويقصد بها الصفات غير الشرعية التي يعاقب عليها القانون والشرع ضمن قواعد تجريم وعقوبات مفروضة على الجرائم الإلكترونية المرتبطة بأنظمة المعلومات.

خصائص الجرائم الإلكترونية:

تتميز الجرائم الإلكترونية بجملة من الخصائص التي تجعل منها فارقا بينها وبين الجرائم التقليدية، ويمكن تناول تلك الخصائص على النحو الآتي (إبراهيم، 2023؛ جندل، 2022؛ المناعسة، 2014):

أولا: تعد الجرائم الإلكترونية عابرة للحدود الوطنية:

بهذه الخاصية التي تتميز بها الجرائم الإلكترونية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجرائم، وكذلك حول تحديد القانون الواجب التطبيق، بالإضافة إلى إشكالية تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام، ونتيجة لهذه الطبيعة الخاصة للجرائم الإلكترونية، ونظرا للخطورة التي تشكلها على

المستوى الدولي، والخسائر التي تتسبب بها، ظهرت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم، وتجدر الإشارة هنا إلى جهود الإنتربول الواسع في هذا المجال، من خلال ضباط الارتباط المنتشرين في كافة الدول عبر العالم، والمكلفين بتوفير قاعدة بيانات ضخمة يمكن أن تشكل نقطة انطلاق للمكافحة والتصدي لهذه الجرائم الإلكترونية (المناعسة، 2014).

ثانيا: وقوع الجرائم الإلكترونية أثناء المعالجة الآلية:

عرف المشرع الفلسطيني المعالجة الآلية بأنها إجراء وتنفيذ عملي أو مجموعه عمليات على البيانات سواء تعلقت بأفراد أو خلافه بما في ذلك جمع تلك البيانات أو استلامها أو تخزينها أو تعديلها أو نقلها أو استرجاعها ومحوها أو نشرها أو إعادة نشر بيانات أو حجب الوصول إليها او بإيقاف عمل الأجهزة أو إلغائها أو تعديل محتوياتها (المادة 1 من قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية).

وعلى ذلك يرى الباحث لتحقق الجرائم الإلكترونية، أن تقع الجرائم الإلكترونية نتيجة لقيام مجموعه من العلاقات بين المدخلات والمخرجات وترابطها مع بعضها البعض للقيام بتحقيق نتيجة لنظام الحماية لمثل هذه المعلومات الإلكترونية، ويجب ايضاً أن يكون لهذا النوع من الجرائم حماية تبين الآلية القانونية لمكافحتها وكذلك حماية الأموال المتداولة عبر الشبكة الإلكترونية وفق القانون الفلسطيني.

ثالثا: الدليل الإلكتروني متنوع في الإثبات ما بين صعوبة الاكتشاف وسهولة الاسترجاع:

نظراً للطبيعة الخاصة التي تتميز بها الجريمة الإلكترونية فإن إثباتها بالكاد يكون صعب الإثبات كون الاعتداء يكون على الومضات الإلكترونية وبتالي لا يترك أثراً، وإذا ما تم اكتشاف الجريمة الإلكترونية فإن من السهل في أغلب الجرائم تدمير ومحو دليل الإدانة (جندل، 2022).

رابعا: خصوصية مرتكب الجرائم الإلكترونية:

ينصف المجرم الإلكتروني بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي معرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة للجرائم الإلكترونية، فهي جرائم فنية تقنية في الغالب، والأشخاص الذين يقومون بارتكابها عادةً يكونون من ذوي الاختصاص الفني في مجال تقنية المعلومات الإلكترونية أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال النظم الإلكترونية، والتعامل مع الشبكة الإلكترونية، كما أن البواعث إلى ارتكاب المجرم لهذا النوع من الجرائم قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي (إبراهيم، 2023).

ويضيف الدويري (2023) لخصائص الجريمة الالكترونية ما يلي:

- الخفاء وصعوبة الكشف: الجرائم الإلكترونية تتميز بقدرتها على التسلل والخفاء، حيث يمكن تنفيذها دون ترك أثر مادي واضح، فغالباً ما يجهل الضحايا وقوع الجريمة إلا بعد فترة طويلة، مما يجعل اكتشافها صعباً للغاية، فعلى سبيل المثال، يمكن سرقة البيانات أو اختراق الأنظمة في ثوانٍ معدودة دون أن يلاحظ أحد ذلك.
- الطبيعة التقنية: تعتمد الجرائم الإلكترونية على استخدام تقنيات متقدمة وأدوات حاسوبية، مما يجعلها مرتبطة بشكل وثيق بالبيئة الرقمية، وتتطلب هذه الجرائم معرفة تقنية عالية من مرتكبيها، كما أنها تستهدف أنظمة معلوماتية أو أجهزة حاسوب معينة.
- غياب الأدلة المادية: بخلاف الجرائم التقليدية، تفتقر الجرائم الإلكترونية إلى أدلة مادية ملموسة، فالأدلة غالباً تكون رقمية مثل سجلات الدخول أو البيانات المخزنة، مما يجعل جمع الأدلة وتحليلها أمراً معقداً.
- التطور المستمر: تتطور الجرائم الإلكترونية باستمرار مع تطور التكنولوجيا، بحيث يستخدم المجرمون أدوات وأساليب جديدة لمواكبة التقدم التكنولوجي، مما يزيد من صعوبة مكافحتها.

- الطابع العابر للحدود: تتميز الجرائم الإلكترونية بأنها لا تعرف الحدود الجغرافية، حيث يمكن تنفيذها من أي مكان في العالم ضد أهداف في دول مختلفة، مما يعقد جهود التحقيق والملاحقة القانونية.
- التشابك بين الأطراف: غالباً ما تتطلب الجرائم الإلكترونية تعاون أكثر من شخص واحد أو جهة واحدة، حيث يمكن أن تشمل شبكات معقدة من الفاعلين الذين يعملون معاً لتحقيق أهدافهم.
- الأثر الكبير على الضحايا: قد تكون آثار الجرائم الإلكترونية مدمرة للضحايا سواء كانوا أفراداً أو مؤسسات، حيث تشمل سرقة البيانات الشخصية، خسائر مالية كبيرة، أو حتى تعطيل خدمات حيوية.

أنواع الجرائم الالكترونية:

تتعدد أنواع الجرائم الالكترونية على النحو التالي (العجمي، 2014):

- جرائم الاحتيال الإلكتروني: وتشمل التلاعب بالمعلومات للحصول على مكاسب مادية أو معنوية، كسرقة البيانات الشخصية، الاحتيال في المعاملات المالية عبر الإنترنت.
- جرائم الاختراق: وتتعلق بالدخول غير المصرح به إلى أنظمة الحاسب الآلي أو الشبكات، كاختراق المواقع الإلكترونية أو الأنظمة للحصول على معلومات سرية.
- جرائم انتهاك الخصوصية: تتضمن الوصول إلى بيانات شخصية دون إذن صاحبها، كنشر صور أو معلومات خاصة دون موافقة.
- جرائم التزوير الإلكتروني: تشمل تزوير المستندات أو البيانات الرقمية، كتزوير بطاقات الائتمان أو الوثائق الإلكترونية.
- جرائم الابتزاز الإلكتروني: وتهدف إلى تهديد الضحايا بنشر معلومات حساسة مقابل المال أو خدمات معينة.

- الجرائم المتعلقة بالمحتوى غير القانوني: وتتضمن نشر مواد إباحية أو محتوى يحض على الكراهية، كتداول المواد الإباحية للأطفال.

- جرائم التشهير والإساءة عبر الإنترنت: تشمل نشر شائعات أو معلومات كاذبة بهدف الإضرار بسمعة شخص أو جهة.

- جرائم القرصنة البرمجية: وتتعلق بسرقة البرامج أو استخدامها بشكل غير قانوني.

- أمثلة: تحميل برامج مقرصنة دون الحصول على تراخيص.

- جرائم الإرهاب الإلكتروني: من خلال استخدام الإنترنت للترويج لأعمال إرهابية أو التخطيط لها.

- جرائم الاحتيال المالي والسرقة الإلكترونية: وتشمل سرقة الأموال من الحسابات المصرفية عبر الإنترنت.

مخاطر الجرائم الالكترونية:

تتعدد مخاطر الجرائم الالكترونية على النحو التالي (الحناحنة، 2023):

1. هدم بناء الأسرة وتفككها: فالجرائم الإلكترونية قد تؤدي إلى استهداف أحد أفراد الأسرة، مما يُسبب انهيار العلاقات الأسرية نتيجة الابتزاز أو التشهير أو نشر معلومات حساسة، فهذه الأفعال قد تُضعف الثقة بين أفراد الأسرة وتؤدي إلى الانفصال أو التفكك.
2. الإساءة لسمعة الأفراد: ويتمثل ذلك في نشر صور أو معلومات غير لائقة عن الضحايا، مما يُلحق ضرراً بسمعتهم أمام المجتمع، هذا النوع من الهجمات قد يؤدي إلى العزلة الاجتماعية للضحايا أو تعريضهم للتنمر.
3. الأضرار الاقتصادية للدولة: وتشمل هذه المخاطر التطفل على خصوصيات الدولة وسرقة الأموال العامة، بالإضافة إلى تدمير النظام الاقتصادي من خلال الهجمات السيبرانية على البنية التحتية

الاقتصادية، قد تؤدي هذه الجرائم أيضاً إلى زعزعة الاستقرار السياسي من خلال الانقلابات أو الأعمال الإرهابية.

4. تنشئة جيل فاسد: فانتشار الجرائم الإلكترونية يُسهم في تدهور القيم الأخلاقية والإنسانية، حيث يتعلم الشباب ممارسات غير أخلاقية مثل الاحتيال، التزوير، والابتزاز، مما يؤدي إلى خلق جيل يفتقر إلى المبادئ.

5. الأضرار النفسية للضحايا: فالضحايا قد يعانون من ضغوط نفسية شديدة نتيجة الابتزاز أو التهديدات، مما قد يدفعهم للتفكير في إيذاء أنفسهم أو حتى الانتحار، الخوف والعجز عن مواجهة المجرمين يزيد من تفاقم حالتهم النفسية.

6. نشر الأخبار الكاذبة: فالجرائم الإلكترونية تُستخدم لنشر الشائعات والمعلومات المضللة التي تُخل بالنظام العام والأخلاق، هذا النوع من التضليل قد يؤثر على استقرار المجتمعات ويُسبب الفوضى.

7. الإضرار بالذمة المالية للأفراد: فالضحايا قد يُجبرون على دفع مبالغ مالية كبيرة للتخلص من التهديدات التي تواجههم، مما يؤدي إلى خسائر مالية ضخمة لهم.

اتفاقية بودابست بشأن الجريمة الإلكترونية:

اتفاقية بودابست بشأن الجريمة الإلكترونية، المعتمدة في 23 نوفمبر 2001 بمدينة بودابست، تمثل أول صك دولي ملزم لتعزيز مكافحة الجرائم الإلكترونية، إذ تسعى اتفاقية بودابست إلى تأمين إطار متكامل لمكافحة الجرائم الإلكترونية، بحيث تدعو الاتفاقية الدول إلى تبني قواعد جنائية حد أدنى لتجريم الأفعال التي تمس سرية وسلامة وتوافر أنظمة وبيانات الكمبيوتر، مثل الوصول غير المصرح به (المادة 2)، والتلاعب بالبيانات (المادة 4)، والتدخل في نظام الكمبيوتر (المادة 5)، والتزوير والاحتيال المتصلان بالكمبيوتر (المادتان 7 و8)، بالإضافة إلى استغلال الأطفال والاعتداء على حقوق الملكية الفكرية عبر الوسائل، بهذا تُسدّ الثغرات

التي قد يستغلها الجاني لتحييد العقاب، وتُنسّق التشريعات المحلية مع الحد الأدنى الدولي، لتعزيز الردع ويُسهل التنسيق عبر الحدود.

فالاتفاقية تفتح آفاقاً واسعة للتدابير الإجرائية لا سيما أمر حفظ البيانات (المادة 16) وحفظ بيانات حركة الاتصالات (المادة 18)، والإذن بالبحث والمصادرة الإلكترونية (المادة 19)، مع ضوابط كافية لحماية الحقوق الأساسية (المادة 15)، وهذا الإطار قدرة الأجهزة على تأمين الأدلة الرقمية قبل فوات الأوان، مع الحفاظ على التوازن بين فعالية التحقيق وضمانات الخصوصية.

وتتطرق الاتفاقية إلى التحديات العابرة للحدود من خلال المساعدة القانونية المتبادلة وتسليم المجرمين (المادتان 23 و24)، ويقرّ حالات النفاذ العابر للحدود المباشر إلى البيانات دون الانتظار لإجراءات المساعدة المتبادلة (المادة 32)، فضلاً عن حفظ البيانات الطارئ لمدة قصيرة لضمان توفرها عند طلب السلطات الأجنبية (المادة 29).

فمن خلال هذا البناء القانوني المتشعب، توفر اتفاقية بودابست إطاراً علمياً متيناً لوحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية لتعزيز قدراتها على التشريع المتوافق (مواد 2–11)، والإجراءات الاستباقية (مواد 15–21)، والتعاون الدولي الفعال (مواد 23–35)، مما يرفع من كفاءة مكافحة الجرائم الإلكترونية ويحدّ من تأثيرها عبر الحدود.

البروتوكول الإضافي الأول (2003): البروتوكول الإضافي للاتفاقية بشأن الجريمة الإلكترونية والمتعلق بتجريم أعمال ذات طبيعة عنصرية أو كارهة للأجانب تُرتكب من خلال أنظمة الحواسيب:

تم اعتماده في 28 يناير 2003 (ستراسبورغ) ودخل حيز التنفيذ في 1 مارس 2006، كملحق باتفاقية الجريمة الإلكترونية، والصادر عن مجلس أوروبا، بحيث يشكل تطوراً في التعامل القانوني مع مظاهر العنصرية وكراهية الأجانب عندما تُرتكب عبر نظم الحواسيب، ويهدف هذا البروتوكول إلى سد ثغرة تشريعية في القانون

الجنائي الدولي فيما يتعلق باستخدام الفضاء الرقمي كمنصة للتحريض على الكراهية والعنف والتمييز، مع الحرص على التوازن بين مكافحة خطاب الكراهية وحماية حرية التعبير، بحيث يحدد البروتوكول غرضه الأساسي، وهو استكمال أحكام اتفاقية بودابست لعام 2001 الخاصة بالجريمة الإلكترونية، من خلال التركيز على تجريم الأفعال ذات الطبيعة العنصرية أو الكارهة للأجانب عندما ترتكب باستخدام نظم الحاسوب. هذا يضع الأساس القانوني لتوسيع نطاق الاتفاقية لتشمل الأبعاد الأخلاقية والاجتماعية للجريمة الإلكترونية، لا سيما تلك التي تمس كرامة الإنسان (المادة 1 من البروتوكول الاضافي 2003).

ويفرض البروتوكول على الدول الأطراف اتخاذ التدابير التشريعية اللازمة لتجريم نشر أو توزيع المواد العنصرية والكارهة للأجانب عبر نظم الحاسوب، بشرط أن يتم ذلك عن قصد ودون مبرر قانوني، كما تتيح الفقرتان الثانية والثالثة من هذه المادة للدول هامشاً للاحتفاظ بحق عدم تجريم بعض أشكال التمييز، خاصة إذا لم ترتبط مباشرة بالكراهية أو العنف، وذلك حفاظاً على التوازن مع المبادئ الوطنية المتعلقة بحرية التعبير. هذا التدرج في الالتزام يُظهر مرونة البروتوكول في احترام الخصوصيات التشريعية للدول الأعضاء (المادة 3 من البروتوكول الاضافي 2003)، من خلال إلزام الدول بتجريم التهديد، عبر نظم الحاسوب، بارتكاب جريمة جسيمة بحق شخص أو جماعة بسبب انتمائهم العرقي أو الديني أو الإثني، وهنا يبرز مدى إدراك واضعي البروتوكول لخطورة التهديدات الرقمية، ليس فقط من حيث الأثر النفسي، بل أيضاً لقدرتها على التحريض والتهيئة لجرائم مادية لاحقة (المادة 4 من البروتوكول الاضافي 2003).

ويضع الملحق أيضاً تجريم الإهانة العلنية عبر نظم الحاسوب للأفراد أو الجماعات على خلفية عرقية أو دينية. ويمنح البروتوكول للدول خيارين: إما اشتراط أن تؤدي الإهانة إلى تحقير أو كراهية أو سخرية فعلية، أو استثناء المادة كلياً أو جزئياً من التطبيق، مما يؤكد مرة أخرى حرص البروتوكول على احترام التوازن الدقيق بين التجريم وحرية التعبير (المادة 5 من البروتوكول الاضافي 2003).

بالنظر إلى البروتوكول الإضافي لعام 2003 الملحق باتفاقية الجريمة الإلكترونية، يوسّع من دائرة التجريم لتشمل الأفعال ذات الطبيعة العنصرية وكراهية الأجانب عندما تُرتكب عبر نظم الحاسوب، مما يضع على عاتق الجهات الأمنية، وخصوصاً الوحدات المختصة بالجرائم الإلكترونية، مسؤولية مضاعفة في رصد وملاحقة هذا النوع من الجرائم التي أصبحت أكثر شيوعاً في الفضاء الرقمي الفلسطيني، من خلال اتخاذ تدابير تشريعية لتجريم نشر المواد العنصرية والتهديدات الإلكترونية والإهانات ذات الطابع العرقي أو الديني، وبذلك يصبح من الضروري أن تكون وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية قادرة على رصد هذه الانتهاكات، وتطوير أدوات فنية وتشريعية لمواجهتها، بما يتوافق مع المعايير الدولية، علاوة على ذلك، فإن البروتوكول يُبرز الحاجة إلى التوازن بين حرية التعبير ومكافحة خطاب الكراهية، وهو ما ينسجم مع مهمة وحدة الجرائم الالكترونية في احترام الحقوق الرقمية والحريات الأساسية أثناء تنفيذ مهامها، وبذلك، يمثل هذا البروتوكول إطاراً مرجعياً دولياً يمكن أن تستند إليه المؤسسة الأمنية الفلسطينية عند تطوير سياساتها، أو بناء قدرات كوادرها في مجال مكافحة الجرائم الإلكترونية، وخاصة تلك التي تهدد السلم المجتمعي من خلال التحريض أو التمييز أو بث الفُرقة داخل المجتمع الفلسطيني أو ضده.

البروتوكول الإضافي الثاني (2022): بشأن تعزيز التعاون وتبادل المعلومات الإلكترونية بين الدول والأطراف الخاصة:

في إطار التطورات المتسارعة في مجال تكنولوجيا المعلومات والاتصالات، وما نجم عنها من تحديات متنامية تتعلق بالجريمة الإلكترونية، تم توقيع الملحق الثاني لاتفاقية بودابست بشأن الجريمة الإلكترونية في عام 2022 تحت عنوان "تعزيز التعاون والإفصاح عن الأدلة الإلكترونية"، وقد جاء هذا البروتوكول الإضافي كمكمل للاتفاقية الأصلية الموقعة عام 2001، والبروتوكول الأول الموقع في عام 2003، وذلك استجابةً لتزايد التهديدات الإلكترونية العابرة للحدود، وازدياد الحاجة إلى آليات قانونية وتقنية تسمح بالتعاون الدولي الفعّال في ملاحقة مرتكبي هذه الجرائم، إذ يهدف الملحق الثاني إلى تعزيز التعاون بين الدول الأطراف، وتسهيل جمع الأدلة الإلكترونية في سياق التحقيقات والملاحقات الجنائية، من خلال أدوات إضافية تُعزز

المساعدة المتبادلة وتُمكِّن من التواصل المباشر بين الجهات المختصة ومزودي الخدمات أو الكيانات التي تملك أو تتحكم في البيانات ذات الصلة، سواء في الحالات العادية أو في حالات الطوارئ، كما ينص البروتوكول على ضمانات لحماية الحقوق والحريات الأساسية، بما في ذلك الحق في الخصوصية وحماية البيانات الشخصية، بما يتوافق مع الالتزامات الدولية لحقوق الإنسان (البروتوكول الإضافي الثاني، 2022).

وتنبع أهمية هذا الملحق، لا سيما في الحالة الفلسطينية، من كونه يوفر إطاراً قانونياً دولياً يمكن أن تستند إليه الجهات الوطنية مثل دائرة مكافحة الجرائم الإلكترونية، لتطوير تعاونها مع الدول الأخرى والجهات المزودة للخدمات الرقمية، وللحصول على الأدلة الرقمية الضرورية لملاحقة الجريمة الإلكترونية، التي أصبحت تمثل تهديداً مباشراً للأمن المجتمعي والنظام العام، كما يتيح الملحق إمكانية الطلب المباشر لمعلومات المشتركين وأسماء النطاقات، والتعامل مع الحالات العاجلة بشكل أكثر مرونة وسرعة، وهو ما يشكل أداة مهمة في يد الجهات الفلسطينية المختصة في ظل التحديات التي تفرضها الحدود السياسية والسيادة المحدودة في الفضاء الرقمي.

اتفاقية الرياض العربية للتعاون القضائي لسنة 1983:

تتضمن اتفاقية الرياض العربية للتعاون القضائي لسنة 1983 عدداً من البنود المباشرة التي تشكّل الأساس القانوني للتعاون بين الدول الأعضاء في جمع الأدلة الجنائية وتبادل المعلومات الجنائية وتسليم المتهمين، مما يهيئ الإطار القانوني الفعّال لمكافحة الجرائم الإلكترونية، حيث ينصّ المادة (5) على "تبادل صحف الحالة الجنائية" بين وزارات العدل بنصوص دقيقة تتيح للجهات القضائية في كل دولة الحصول مباشرةً على سجل المتهم الجنائي لدى أي طرف متعاقد آخر عند توجيه الاتّهام ضده، الأمر الذي يُسهم في تتبّع مسار الجرائم العابرة للحدود بسرعة وفاعلية دون انتظار إجراءات طويلة[1].

[1] المادة (5) من اتفاقية الرياض العربية للتعاون القضائي لسنة 1983.

كما يتيح "الإنابة القضائية" بمقتضى المادة (14) طلبات إجراء كل أو بعض الإجراءات القضائية المتعلقة بدعوى قائمة، ويشمل ذلك استدعاء الشهود، والحصول على إفادات خبراء في مجال الأدلة بما يضمن تضافر جهود الدول الأعضاء في فحص الأدلة للجرائم وتنميتها وتحليلها وفق الإجراءات المعمول بها في بلد التنفيذ دون إخلال بسيادتها، أما بالنسبة لتسليم المتهمين فإن الباب السادس (المواد 38–47) يؤكّد على إلزامية تسليم الأشخاص الموجه إليهم الاتهام عن "أفعال معاقب عليها بعقوبة سالبة للحرية مدًى سنة أو أكثر"، وهو ما يشتمل على الجرائم التي يحكم عليها وفقاً للتشريعات الوطنية بعقوبات لا تقل عن سنة سجن (المادة (40) أ)؛ إضافة إلى اشتراط تقديم "أمر القبض أو الحكم بالإدانة" والمستندات الداعمة له، وهو ما يختزل متطلبات الحد الأدنى للإجراءات لتسريع إرجاع المتهمين في القضايا التقنية المعقدة دون تعطيل (المواد (42–44).

وبذلك، تؤسس الاتفاقية لإطار تعاون قضائي متكامل في مجال مكافحة الجرائم ومن ضمنها الجرائم المستجدة (الالكترونية)، عبر تبادل المعلومات الجنائية الفورية وإنفاذ طلبات الإنابة والتحقيق في الأدلة التقنية وتسليم المتهمين عند توفر الشروط المنصوص عليها في بنودها، مما يضمن تجاوز العراقيل الإجرائية وتحقيق التضامن الأمني والقضائي بين الدول العربية في مواجهة التحديات المتنامية للجرائم السيبرانية.

الربط بين قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته وقانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م[1]:

في ضوء تسريع وتيرة مكافحة الجرائم الإلكترونية وتعزيز التنسيق بين الأجهزة الأمنية والقضائية، أُنشئت بموجب قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته وحدة متخصصة للضبط القضائي في الجرائم الإلكترونية، ينصّ على ذلك صراحةً المادة (3)، حيث تُعهد إلى هذه الوحدة مهام البحث والتحري في الجرائم المعلوماتية عبر فرق تقنية مدربة ومستندة إلى أحدث الأساليب العلمية، ويُعدّ هذا

[1] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

التخصيص تفعيلاً لمبدأ التخصص في الضبط القضائي الذي حدده قانون الإجراءات الجزائية رقم (3) لسنة 2001م، إذ تُعرِّف المادة (19) مأموري الضبط القضائي بأنهم "الجهات المسؤولة عن البحث والاستقصاء عن الجرائم وجمع الاستدلالات اللازمة للتحقيق" فتصبح صلاحيات الوحدة الخاصة المتولية للجرائم الإلكترونية متطابقة مع صلاحيات مأموري الضبط القضائي العامة، ولكن مع توجه تركيزها نحو الجرائم المعلوماتية فقط.

وتتجلى أوجه التكامل التشريعي عند ربط عملية ضبط الأدلة الإلكترونية بالتدابير والإجراءات المنصوص عليها في قانون الإجراءات الجزائية، لا سيما فيما يتعلق بإجراءات تفتيش المواقع وجمع البيانات الرقمية، حيث يشترط البند (ثانياً) من المادة (120) في قانون الإجراءات الجزائية الحصول على إذن من الجهة القضائية المختصة قبل تفتيش المنازل والحواسيب والأجهزة الإلكترونية، وهو ما تعتمده وحدة الجرائم الإلكترونية عند اتخاذها إجراءات الحجز والفحص الفني، وبذلك، يستند عمل الوحدة إلى قاعدة قانونية مشتركة تضمن سلامة الإجراءات وضمان حقوق المتهمين وفقاً للضوابط المنصوص عليها.

كما أن إحالة القضايا المتصلة بالجرائم الإلكترونية إلى النيابة العامة تمثل صلب التنسيق بين القانونين، إذ تنص المادة (55) من قانون الإجراءات الجزائية على "اختصاص النيابة العامة دون غيرها بالتحقيق في الجرائم والتصرف فيها"، فتتلقى النيابة العامة الملفات التي ترفعها وحدة الجرائم الإلكترونية لاستكمال التحقيق ومباشرة الملاحقة القضائية، وفي الوقت ذاته، تعطي المادة (10) من قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته الحق لنائب عام الدولة أو من ينوب عنه في الإشراف المباشر على تحقيقات الجرائم المعلوماتية، مما ينسجم مع نطاق اختصاص النيابة العامة العام ويعزز درجة الشفافية والرقابة على الإجراءات المتخذة

وعليه يتضح أن قرار بقانون رقم (10) لسنة 2018م وتعديلاته يُكمل البنية الإجرائية القائمة في قانون الإجراءات الجزائية رقم (3) لسنة 2001م عبر تأسيس وحدة ضابطة قضائية تقنية متخصصة تطبق

صلاحيات مأموري الضبط القضائي المنصوص عليها في المادة (19)، وتتقيد بضوابط التفتيش التي حددها المادة (120)، مع إحالة النتائج إلى النيابة العامة وفقاً لـالمادة (55)، ووفق إشراف نائب عام الدولة المنصوص عليه في المادة (10) من قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته، مما يضمن انسجام الأطر التقنية مع الإجراءات القانونية ويحافظ على حقوق الأطراف كافة.

الموازنة ما بين مكافحة الجريمة الإلكترونية والحفاظ على حقوق الإنسان وعدم التعدي على الخصوصيات التي كفلها القانون:

تنبع ضرورة الموازنة بين تمكين أجهزة الأمن من مكافحة الجرائم الإلكترونية من جهة، والحفاظ على الحقوق والحريات الأساسية للمواطنين من جهة أخرى، من قيام التشريع الإلكتروني على مبدأ التخصص المقترن بضوابط قضائية تكفل سلامة الإجراءات وحيادية التحقيق. فقد أكّد قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته في المادة (1/22) على "حظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته"، مع معاقبة مرتكبي هذا التدخل بالسجن والغرامة المنصوص عليهما في المادة (2/22)، وهو ما يرسّخ حق الأفراد في خصوصية حياتهم الخاصة، وفي الوقت نفسه، تمنح المادة (35) للأجهزة المختصة سلطة ضبط الأجهزة والبيانات الإلكترونية، "مع اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة ... وخصوصيتها محل التحفظ إلى حين صدور قرار من الجهات القضائية ذات العلاقة"، مما يؤكد ضرورة ارتباط إجراءات الضبط القضائي بموافقة قضائية مسبقة تحفظ حق المتهمين في المحاكمة العادلة وعدم التعسف في الحجز

وعلى صعيد قانون الإجراءات الجزائية رقم (3) لسنة 2001م، يُلزِم البند (2) من المادة (39) مأموري الضبط القضائي بالحصول على مذكرة تفتيش مسبّبة يوقّعها عضو النيابة المختص، محددة المكان والزمان والجهة موضوع التفتيش، كما يقضي البند (2) من المادة (32) بعدم جواز تجديد إذن التفتيش إلا إذا انطبقت أسباب الاستمرار، وذلك مع ضرورة حضور المتهم أو شاهدين من محيطه لإجراء التفتيش، ومن شأن هذه

الضوابط أن تمنع الانتهاك التعسفي لمنازل المواطنين وأجهزتهم، وتحقق التوازن المطلوب بين مصلحة الأمن العام وحق الأفراد في الخصوصية، علاوة على ذلك، لا يجوز بموجب المادة (1/36) من قرار الجرائم الإلكترونية اعتراض الاتصالات أو تسجيلها إلا بناءً على "قرار من المحكمة المختصة يتضمن جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض ومدته"، مع وجوب إعلام النيابة العامة بتاريخ الانطلاق وهذه الضوابط تنسجم مع أحكام المادة (19) من قانون الإجراءات الجزائية التي تُلزم مأموري الضبط القضائي بمراعاة الضوابط القانونية في جمع الاستدلالات، بما يحقق احتراماً لسرية المراسلات والاتصالات.

وعليه يتبيّن أن التشريع الإلكتروني يزوّد الأمن بآليات متقدمة لمكافحة الجرائم المعلوماتية، لكنه في الوقت ذاته يستند إلى أحكام المادة (22) من قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته وضوابط المادتين (32) و (39) من قانون الإجراءات الجزائية لضمان عدم التعدّي على الحريات والخصوصيات، لتحقيق توازنٍ ديناميكيٍ يحقق الفاعلية الأمنية مع حفاظٍ صارمٍ على حقوق الإنسان.

1.3 الدراسات السابقة

أولا: الدراسات العربية:

دراسة نبيل (2024): دور الإعلام الأمني في التوعية بمخاطر الجرائم الإلكترونية في القنوات الجزائرية.

هدفت الدراسة إلى استكشاف دور الإعلام الأمني في التوعية بمخاطر الجرائم الإلكترونية من خلال القنوات الجزائرية، مع التركيز على برنامج (تحري الجريمة) في قناة البلاد، واعتمدت الدراسة المنهج المسحي واستخدمت استبياناً على عينة قصدية من متابعي البرنامج، وأظهرت النتائج أن الإعلام الأمني يلعب دوراً محورياً في التوعية بالجرائم الإلكترونية، حيث أفاد 39% من المشاركين أن البرنامج ساهم في زيادة وعيهم لتجنب ارتكاب الجرائم، وأكد 33% أن المحتوى الوقائي ساعد في تنبيه الرأي العام لمواجهة الجرائم

الإلكترونية، كما بيّنت الدراسة أن 87% من أفراد العينة يرون البرنامج ناجحاً في نشر الحقائق وتعديل السلوك العام، مما يعزز دوره في تسليط الضوء على قضايا الجرائم الإلكترونية وتحقيق السلامة المجتمعية.

يمكن الاستفادة من هذه الدراسة في تحليل الدور المهم الذي يمكن أن تلعبه المؤسسات الرسمية، خاصة في توعية الجمهور حول الجرائم الإلكترونية، في الدراسة الحالية، سيتم التركيز على دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية، من خلال وحدة متخصصة داخل الجهاز الأمني بدلاً من الإعلام العام

دراسة أبو القاسم (2024): دور وسائل الضبط الاجتماعي في الحد من الجرائم الالكترونية (المستحدثة).

تهدف الدراسة إلى استكشاف مفهوم الضبط الاجتماعي والجريمة الإلكترونية المستحدثة، والعوامل التي تدفع الأفراد إلى ارتكابها أو تحد من انتشارها، واعتمدت الدراسة على المنهج الوصفي التحليلي لتقديم فهم شامل لهذه الظاهرة، وتوصلت الدراسة إلى أن العوامل المؤدية لارتكاب هذه الجرائم متعددة وتشمل أبعاداً نفسية، اجتماعية، اقتصادية، وسياسية، وأوضحت الدراسة أن الجرائم الإلكترونية لها آثار مدمرة على الأفراد، الأسر، والمجتمع، وأن غياب الرقابة على الفضاء الإلكتروني زاد من انتشارها، وأوصى الباحث بضرورة تحديث التشريعات لتواكب التطورات السريعة في الجرائم الإلكترونية، إنشاء مراكز مختصة لمكافحتها، وتعزيز الوعي المجتمعي بخطورتها عبر وسائل الإعلام، التعليم، والأسرة.

توفر هذه الدراسة فهماً متعمقاً عن العوامل التي تدفع الأفراد إلى ارتكاب الجرائم الإلكترونية وطرق الحد من انتشارها، ويمكن الاستفادة من توصيات الدراسة بخصوص ضرورة تحديث التشريعات وإنشاء مراكز مختصة لمكافحة الجرائم الإلكترونية، والإضافة التي تقدمها الدراسة الحالية هي تسليط الضوء على التحديات التي تواجه وحدة الجرائم الإلكترونية في فلسطين، مما يتيح فرصة لتحليل المعوقات الخاصة بالبيئة المحلية في فلسطين.

دراسة العنوز (2024): دور الأمن السيبراني في التقليل من أعداد الجرائم الإلكترونية في محافظة العقبة" باستخدام نظم المعلومات الجغرافية.

تهدف الدراسة إلى توضيح دور الأمن السيبراني في الحد من الجرائم الإلكترونية أو زيادتها، واستُخدمت برامج نظم المعلومات الجغرافية (GIS) لتحديد التدرج اللوني الذي يعكس نسب الجرائم الإلكترونية، حيث يدل اللون الغامق على أعلى النسب والفاتح على أدناها، واعتمدت الدراسة على المنهج الوصفي والتحليلي مع استخدام التحليل المكاني والخرائط الرقمية لتوضيح العلاقات بين المتغيرات، ومن أبرز النتائج: قدرة نظم المعلومات الجغرافية على دعم صانعي القرار من خلال خرائط رقمية توضح بيانات الجرائم بفعالية، ضعف وعي المواطنين باستخدام برامج التواصل الاجتماعي بشكل صحيح، ندرة الدراسات التي تربط بين الأمن السيبراني والجرائم الإلكترونية، وانخفاض إدراك المواطن الأردني للعقوبات المرتبطة بسوء استخدام الإنترنت، وأكدت الدراسة على أهمية الأمن السيبراني وأمن المعلومات في تعزيز الحماية والوعي للحفاظ على البيانات الشخصية.

تقدم دراسة العنوز (2024) مثالاً على كيفية استخدام تقنيات تحليل البيانات لدراسة الجرائم الإلكترونية، بينما تقدم الدراسة الحالية بُعداً آخر حول أساليب مكافحة الجرائم الإلكترونية داخل المؤسسة الأمنية الفلسطينية، مع التركيز على التوعية والتحديات التي تواجه هذه الوحدة، مما يعزز الفهم العملي لكيفية التعامل مع الجرائم الإلكترونية في السياق الفلسطيني.

دراسة علي (2024): دور المواقع الإخبارية في مكافحة الجرائم الإلكترونية وعلاقته باتجاهات الجمهور نحوها (دراسة تطبيقية).

تهدف الدراسة إلى التعرف على دور المواقع الإخبارية في مكافحة الجرائم الإلكترونية وعلاقته باتجاهات الجمهور نحو هذه الجرائم، واعتمدت الدراسة على منهج المسح الإعلامي، حيث شملت في جانبها الميداني عينة من الجمهور المصري المستخدم للمواقع الإخبارية، بلغ عدد أفرادها 400 مفردة، كما تم في الجانب

التحليلي إجراء مسح شامل على ثلاثة مواقع إخبارية إلكترونية، وأظهرت النتائج وجود علاقة ارتباطية بين متابعة الجمهور لأنشطة المواقع الإخبارية في مكافحة الجرائم الإلكترونية واتجاهاتهم تجاهها، وأكدت الدراسة أن موقع "اليوم السابع" كان الأكثر تغطية للجرائم الإلكترونية بين المواقع الثلاثة، كما تبين أن المواقع الإخبارية حققت دوراً مهماً في تقديم المعلومات المرتبطة بالجريمة الإلكترونية.

ركزت الدراسة أعلاه على كيفية تأثير المواقع الإخبارية في مكافحة الجرائم الإلكترونية من خلال توجهات الجمهور، والدراسة الحالية يمكن أن تستفيد من هذه الفكرة في دراسة تأثير المؤسسات المختلفة على الوعي بالجرائم الإلكترونية، لكن ما يميز الدراسة الحالية هو التركيز على دور وحدة الجرائم الإلكترونية داخل المؤسسة الأمنية الفلسطينية، وتحديد الأساليب التي تستخدمها هذه الوحدة لمكافحة الجرائم.

دراسة القحطاني (2024): دور الإعلام الرقمي السعودي في توعية المواطنين بتقنيات الجرائم الإلكترونية في المملكة العربية السعودية.

هدفت الدراسة إلى تقييم دور الإعلام الرقمي السعودي في توعية المواطنين بتقنيات الجرائم الإلكترونية في المملكة العربية السعودية، واستخدمت الدراسة المنهج المسحي القائم على الاستبانة، حيث تم جمع البيانات من عينة عشوائية تضم 200 مواطن ومواطنة عبر منصات التواصل الاجتماعي، وأظهرت النتائج اهتمام المواطنين بالتعرف على تقنيات الجرائم الإلكترونية، حيث كانت نسبة حذرهم مرتفعة رغم أن وقوعهم الشخصي في الجرائم الإلكترونية كان منخفضاً، كما تبين أن الاتصالات الهاتفية ومواقع التواصل الاجتماعي تشكل بيئة خصبة لانتشار الجرائم الإلكترونية، وأظهرت الدراسة أن الإعلام الرقمي السعودي كان فعالاً في التوعية، وأن المواطنين يفضلون تلقي الرسائل التوعوية عبر منصات التواصل الاجتماعي مثل WhatsApp وSnapchat، كما أشارت إلى ضرورة تنظيم برامج توعوية، تطوير متصفح إنترنت وطني آمن، وإدراج مقرر "تربية إعلامية رقمية" في التعليم العام، كما كشفت الدراسة عن وجود علاقة ارتباطية إيجابية متوسطة بين حذر المواطنين ووعيهم بالجرائم الإلكترونية.

يمكن الاستفادة من الدراسة أعلاه في بناء أداة الدراسة والإطار النظري، ومع ذلك، تضيف الدراسة الحالية بُعداً مهماً من خلال التركيز على وحدة الجرائم الإلكترونية كجهة مسؤولة مباشرة داخل المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية، مما يتيح استكشاف التحديات والأساليب الميدانية الفعالة في هذا المجال.

دراسة النعامي (2023): دور الجهات المسئولة عن الجريمة الإلكترونية في اليمن في توعية الجمهور بمخاطر الجريمة الإلكترونية.

تهدف الدراسة إلى الكشف عن واقع الجريمة الإلكترونية في اليمن وتقييم دور الجهات المسؤولة في توعية الجمهور بمخاطرها، واعتمدت الدراسة على المنهج الوصفي، حيث تم جمع البيانات الكمية والكيفية باستخدام استبانة تم تطبيقها على عينة عشوائية من 400 مستخدم للإنترنت في أمانة العاصمة صنعاء، كما تم جمع البيانات الكيفية من خلال أداة المجموعات المركزة والمقابلات المعمقة مع مدراء ومسؤولي إدارات الإعلام والعلاقات العامة بالجهات المعنية بالجريمة الإلكترونية، وأظهرت النتائج أن نسبة 47% من عينة الدراسة تعرضوا لنوع واحد على الأقل من الجرائم الإلكترونية، وأن المبحوثين لديهم معرفة جيدة بالمفاهيم العامة للجريمة الإلكترونية، إلا أن وعيهم بطرق الوقاية كان ضعيفا، كما كشفت الدراسة عن فشل إدارات الإعلام والعلاقات العامة في توعية الجمهور بمخاطر الجريمة الإلكترونية.

يمكن الاستفادة من الدراسة أعلاه في تطوير وبناء بعض محاور الدراسة الحالية، فيما تُقدّم الدراسة الحالية تحليلا لدور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في توعية الجمهور، إضافة إلى التحديات التي تواجهها في هذا الصدد.

دراسة العسقلاني (2022): دور مجلس التعاون الخليجي القانوني والتعاوني في مكافحة الجرائم الإلكترونية.

هدفت الدراسة إلى استكشاف الجرائم الإلكترونية باعتبارها ظاهرة إجرامية تزايدت خطورتها نتيجة للتطور التكنولوجي والاعتماد على الأجهزة وبرامج الحاسوب، وكذلك الشبكات المعلوماتية العالمية، واعتمدت الدراسة على تحليل التطورات التقنية وأثرها على تزايد الجرائم الإلكترونية، مع التركيز على دور المملكة العربية السعودية ودولة الإمارات العربية المتحدة في التصدي لهذه الظاهرة، وأظهرت النتائج أن هذه الدول كانت من الأوائل في المنطقة في مواجهة الجرائم الإلكترونية، سواء من خلال التشريعات أو التعاون الإقليمي، كما أكدت الدراسة على ضرورة التعاون الدولي لمكافحة هذه الجرائم نظراً لخطورتها على البنية التحتية الحيوية في الفضاء الإلكتروني.

يمكن الاستفادة من الدراسة أعلاه في إطار تحليل التعاون داخل المؤسسات الفلسطينية وداخل حدود دولة فلسطين لمكافحة الجرائم الالكترونية، فيما تتميز الدراسة الحالية من خلال تركيزها على التحديات الداخلية التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية وتدابيرها الذاتية.

دراسة الشوابكة (2022): معوقات مكافحة الجرائم الإلكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص.

هدفت الدراسة إلى التعرف على المعوقات الفنية والقانونية لمكافحة الجرائم الإلكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص، شمل مجتمع الدراسة جميع المختصين في مجال الجرائم الإلكترونية من وحدة الجرائم الإلكترونية في مديرية الأمن العام، المركز الوطني للأمن السيبراني، القضاة المتخصصين في الجرائم الإلكترونية، والخبراء الفنيين المعتمدين لدى القضاء الأردني، حيث بلغ عددهم 106 مختصين، وتم اختيار عينة استطلاعية من 20 مختصاً وعينة أساسية من 80 مختصاً، وأظهرت نتائج الدراسة أن المعوقات القانونية جاءت في المرتبة الأولى بدرجة مرتفعة، تلتها المعوقات الفنية التي كانت بدرجة متوسطة، أوصى

الباحث بضرورة زيادة الوعي المجتمعي حول الجرائم الإلكترونية من خلال وسائل الإعلام المختلفة، وتنظيم مؤتمرات دولية لتطوير التشريعات المتعلقة بمكافحة الجرائم الإلكترونية، بالإضافة إلى عقد دورات تدريبية محلية ودولية لذوي الاختصاص لتحسين مهاراتهم في التعامل مع هذه الجرائم بكفاءة.

دراسة الشوابكة (2022) تقدم رؤى هامة حول المعوقات الفنية والقانونية التي تواجه مكافحة الجرائم الإلكترونية وهو مجال يمكن الاستفادة منه في الدراسة الحالية، بينما يمكن رصد تميز الدراسة الحالية من خلال التركيز على التحديات التي تواجه وحدة الجرائم الإلكترونية في فلسطين، وستساهم هذه المقارنة في تحديد كيفية تأثير العوامل القانونية والفنية على فعالية هذه الوحدة في محاربة الجرائم الإلكترونية.

دراسة العنزي (2020): دور الإعلام الأمني في مواجهة الجرائم الإلكترونية والحد منها من وجهة نظر العاملين في الأجهزة الأمنية في دولة الكويت.

هدفت الدراسة إلى التعرف على دور الإعلام الأمني في الوقاية والحد من الجرائم الإلكترونية، والكشف عن أساليب تعزيز دوره ومعوقاته من وجهة نظر العاملين في الأجهزة الأمنية في الكويت، واستخدمت الدراسة المنهج المسحي بالعينة، واعتمدت على استبيان حيث شملت عينة الدراسة (767) ضابطاً وضابط صف وأفراد من مختلف قطاعات الشرطة والأمن في الكويت، وأظهرت النتائج أن الإعلام الأمني يلعب دوراً كبيراً في خلق وعي أمني بخطورة الجرائم الإلكترونية، وإبراز أنماطها وأساليب الوقاية منها، ونشر التشريعات ذات الصلة، كما تبين أن أساليب تعزيز دور الإعلام الأمني جاءت بمستوى مرتفع خاصةً عبر استخدام وسائل التواصل الاجتماعي والاستفادة من الخبرات الدولية، وأشارت النتائج إلى وجود معوقات على مستوى متوسط أبرزها ضعف التنسيق بين إدارة الإعلام الأمني والمؤسسات ذات الصلة.

يمكن الاستفادة من الدراسة أعلاه في بناء تصور حول الدور المهم الذي تلعبه المؤسسات في مكافحة الجرائم الإلكترونية، بينما تختلف وتتميز الدراسة الحالية من خلال التركيز على دور وحدة الجرائم الإلكترونية في فلسطين، والتوجه نحو تحديد الأساليب العملية المباشرة التي تستخدمها الوحدة الأمنية.

ثانيا: الدراسات الأجنبية:

دراسة Mijwil & Aljanabi (2023):

Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime.

هدفت الدراسة إلى استكشاف دور الذكاء الاصطناعي في تعزيز الأمن السيبراني ومكافحة الجرائم الإلكترونية، استخدمت الدراسة منهجاً نوعياً لتحليل التحديات والاستراتيجيات المتعلقة بحماية الفضاء الرقمي من الهجمات السيبرانية، تم جمع البيانات من مصادر أولية مثل الأبحاث السابقة ومقالات الدوريات، وأظهرت النتائج أن الأمن السيبراني يواجه تحديات متعددة، من بينها الهجمات المعقدة والاعتماد على مزودي خدمات الطرف الثالث وقلة الوعي بأمن المعلومات، وأوصت الدراسة باستخدام تقنيات الذكاء الاصطناعي لتعزيز دفاعات الأمن السيبراني، مثل الكشف عن الثغرات وإدارة الحوادث الأمنية، كما أكدت أهمية التعاون بين القطاعين العام والخاص لتطوير آليات حماية البيانات، وخلصت الدراسة إلى أن الذكاء الاصطناعي يمكن أن يلعب دوراً حاسماً في تحسين البيئة الرقمية من خلال توفير حلول متقدمة لمكافحة الجرائم السيبرانية، ودعت إلى وضع استراتيجيات شاملة تشمل تدريب الموظفين وتطوير أنظمة حماية البيانات لضمان سلامة المعلومات في العصر الرقمي.

يمكن الاستفادة من هذه الدراسة في البحث الحالي لتطوير فهم شامل حول كيفية توظيف التقنيات الحديثة لتحليل الجرائم الإلكترونية والتصدي لها، في حين فإن الإضافة التي تقدمها الدراسة الحالية تتمثل في تحليل هذا الدور ضمن سياق محلي خاص بالمؤسسة الأمنية الفلسطينية، مع التركيز على التحديات التي تواجهها الوحدة في مكافحة الجريمة الالكترونية.

دراسة Mphatheni, M. R., & Maluleke (2022):

Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions.

تهدف الدراسة إلى استكشاف الأمن السيبراني كاستجابة لمكافحة الجرائم الإلكترونية، مع التركيز على تفكيك التهديدات السائدة وتقديم توصيات للمناطق الإفريقية، واستخدم الباحثان منهجية البحث النوعي وتصميم غير تجريبي، حيث اعتمدوا على مراجعة منهجية للأدبيات والمصادر الأولية المنشورة بين عامي 2010 و2022، وقد أظهرت الدراسة أنه لا يوجد تعريف موحد للجرائم الإلكترونية، كما أن هذه الجرائم تشمل انتهاك حقوق الطبع والنشر، الاحتيال المتعلق بالحاسوب، والانتهاكات الأمنية على الشبكات، كما أكدت الدراسة على الحاجة إلى مهارات ومعرفة متقدمة لمواجهة هذه الجرائم في إفريقيا، حيث تفتقر معظم البلدان الإفريقية إلى الكوادر المدربة والاستثمار الكافي في الأمن السيبراني، وأوصى الباحثان بتعزيز التعاون بين الحكومات والمنظمات لمكافحة الجرائم الإلكترونية وتطوير استراتيجيات أمنية مبتكرة.

تقدم هذه الدراسة فرصة لفهم تأثير نقص الكفاءات والبنية التحتية على مواجهة هذه الجرائم، وهو ما يمكن أن يثري البحث الحالي، أما الإضافة الجديدة التي تقدمها الدراسة الحالية هي دراسة هذه التحديات في سياق المؤسسة الأمنية الفلسطينية وتقديم مقترحات ملائمة للبيئة الفلسطينية.

دراسة Anwary (2022):

The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia.

هدفت الدراسة إلى تقييم دور الإدارة العامة في مكافحة الجرائم الإلكترونية في إندونيسيا من خلال تحليل الإطار القانوني المعمول به، استخدمت الدراسة منهجاً نوعياً معتمداً على تحليل المحتوى، حيث جمعت البيانات من مصادر أولية مثل القوانين واللوائح، ومصادر ثانوية كالمقالات والأبحاث، وأظهرت النتائج وجود سياسات وقوانين شاملة في إندونيسيا للتعامل مع الأمن السيبراني ومكافحة الجرائم الإلكترونية، إلا أن تنفيذها

يعاني من ضعف كبير، تم تحديد تحديات رئيسية، منها غياب التنسيق بين المؤسسات المعنية، وقصور في تطبيق مبادئ الحوكمة الفعالة مثل المشاركة والمساءلة والشفافية، كما أكدت الدراسة الحاجة إلى سياسات أكثر تحديداً وتطوير بنية تحتية قوية لمكافحة الجرائم الإلكترونية وتعزيز التعاون بين القطاعين العام والخاص، وخلصت الدراسة إلى ضرورة تحسين تنفيذ القوانين الحالية ورفع مستوى الوعي بالأمن السيبراني، مع تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية.

يمكن الاستفادة من الدراسة أعلاه من نتائج الدراسة لتقييم فعالية القوانين والإجراءات المتبعة في فلسطين، لكن الدراسة الحالية ستضيف بُعداً جديداً من خلال تسليط الضوء على المعيقات العملية التي تواجه وحدة الجرائم الإلكترونية بشكل خاص، وربطها بالإطار التنظيمي الفلسطيني.

دراسة Sviatun, Goncharuk, Roman, Kuzmenko, & Kozych (2021):

Combating cybercrime: economic and legal aspects.

تناولت الدراسة التي أجراها سفياتون وآخرون (2021) تحليل أسباب الجرائم الإلكترونية وتبعاتها الاقتصادية عالمياً، بالإضافة إلى تقييم الآليات القانونية لمكافحتها، استخدمت الدراسة مناهج تحليلية متعددة، مثل التحليل المقارن والتعميم ونماذج الاتجاهات الإحصائية، لتحليل البيانات الإحصائية المتعلقة بالجرائم الإلكترونية واتجاهاتها، مع التركيز على تأثيرها الاقتصادي ووسائل مواجهتها القانونية، وأظهرت الدراسة أن تكلفة الجرائم الإلكترونية تجاوزت تريليون دولار أمريكي في عام 2020، ما يعادل أكثر من 1% من الناتج المحلي الإجمالي العالمي، وتناولت الأسباب التي تؤدي إلى زيادة الجرائم الإلكترونية، مثل رقمنة القطاعات الاقتصادية، وضعف التعاون الدولي، وعدم توافق السياسات القانونية مع تطورات الجرائم الإلكترونية، وأوصت الدراسة بتعزيز التعاون الدولي وتطوير استراتيجيات شاملة للحد من الجرائم الإلكترونية، مع التركيز على آليات قانونية ووقائية وتنظيمية لتحسين مواجهة هذه التحديات.

يمكن للدراسة الحالية أن تستفيد من هذا التحليل لتوضيح الأبعاد الاقتصادية للجرائم الإلكترونية في السياق الفلسطيني، أما الجديد الذي تضيفه الدراسة الحالية هو التركيز على دور وحدة الجرائم الإلكترونية في الحد من هذه التأثيرات الاقتصادية على المستوى المحلي من خلال التوعية والوقاية.

دراسة Paek, Nalla, Chun, & Lee **(2021)**:

The perceived importance of cybercrime control among police officers: Implications for combatting industrial espionage.

هدفت الدراسة إلى تحديد العوامل التي تؤثر في تصورات ضباط الشرطة حول أهمية مكافحة الجرائم الإلكترونية" تهدف إلى فهم كيفية تقييم ضباط الشرطة لأهمية مكافحة الجرائم الإلكترونية، خاصة تلك التي تتعلق بسرقة المعلومات السرية للأعمال، تم استخدام منهج البحث الاستطلاعي على عينة من ضباط الشرطة الكوريين الجنوبيين الذين يحضرون تدريباً في معهد تطوير الموارد البشرية للشرطة وذلك من خلال استبيان كأداة للدراسة، وأظهرت النتائج أن تصورات الضباط حول آراء زملائهم والمنظمة بشأن مكافحة الجرائم الإلكترونية كان لها تأثير كبير على مواقفهم، كما تبين أن تصوراتهم حول جدية سرقة المعلومات عبر الإنترنت وكفاءتهم في استخدام الحاسوب أثرت أيضاً في وجهات نظرهم حول أهمية مكافحة هذه الجرائم، خلصت الدراسة إلى ضرورة أن تتخذ الشرطة نهجاً تنظيمياً استباقياً لمكافحة الجرائم الإلكترونية، من خلال برامج توعية وتدريب تساهم في الوقاية من التجسس الصناعي وتعزيز الوعي لدى الضباط.

تساعد نتائج الدراسة أعلاه في فهم الدور الإدراكي للعاملين في المؤسسات الأمنية، إذ تستفيد الدراسة الحالية من هذه الرؤية من خلال تحليل آراء العاملين في وحدة الجرائم الإلكترونية حول أدوارهم وتحدياتهم، مع تقديم الجديد عبر تحليل تأثير المتغيرات الشخصية (مثل سنوات الخدمة والمؤهل العلمي) على استجاباتهم، وهو جانب لم تتناوله الدراسات السابقة بشكل موسع.

دراسة Neethu (2020):

Role of International Organizations in Prevention of Cyber-Crimes: An Analysis.

تهدف الدراسة إلى تحليل دور المنظمات الدولية في مكافحة الجرائم الإلكترونية، التي تهدد الأمن الرقمي على مستوى العالم، استخدمت الدراسة منهجاً جمع بين الأساليب الإحصائية وغير الاحصائية، واستخدمت مصادر أولية وثانوية للتحليل النقدي، تم تناول جرائم الإنترنت وأنواعها مثل القرصنة والسرقة الإلكترونية والتسلل غير القانوني للاتصالات، كما تم تسليط الضوء على التحديات التي تواجه المنظمات الدولية مثل تباين السياسات الوطنية ونقص البنية التحتية، وقد استعرضت الدراسة دور العديد من المنظمات الدولية في مكافحة هذه الجرائم مثل الإنتربول، الأمم المتحدة، ومنظمة التعاون الاقتصادي والتنمية (OECD)، خلصت الدراسة إلى أن التعاون الدولي والتشريعات الموحدة أمران مهمان للحد من الجرائم الإلكترونية، وأوصت بإنشاء محكمة دولية للجرائم الإلكترونية وتنفيذ برامج توعية على المستوى الشعبي.

يمكن الاستفادة من هذه الدراسة في البحث الحالي لفهم أهمية التعاون والتنسيق بين الجهات المختلفة في مكافحة الجرائم الإلكترونية، خاصة على المستوى الدولي، وربط ذلك بتجربة المؤسسة الأمنية الفلسطينية، الإضافة الجديدة التي تقدمها الدراسة الحالية تتمثل في التركيز على دور وحدة الجرائم الإلكترونية ضمن المؤسسة الأمنية الفلسطينية كجهة محلية، وتحليل دورها ليس فقط في التصدي للجرائم الإلكترونية بل أيضاً في التوعية والتثقيف، مع تسليط الضوء على التحديات الداخلية والخارجية التي تواجهها هذه الوحدة.

1.4 التعقيب على الدراسات السابقة

تتعدد الدراسات السابقة التي تناولت موضوع الجرائم الإلكترونية وأساليب مكافحتها في مختلف السياقات العربية والدولية، مع التركيز على دور الإعلام، الأمن السيبراني، ومؤسسات الدولة في التصدي لهذه الجرائم، فدراسة نبيل (2024) أبرزت دور الإعلام الأمني في توعية المواطنين بمخاطر الجرائم الإلكترونية، أما دراسة أبو القاسم (2024)، فقد تناولت دور وسائل الضبط الاجتماعي في الحد من الجرائم الإلكترونية

المستحدثة، بينما دراسة العنوز (2024) في الأردن استخدمت نظم المعلومات الجغرافية لتحليل دور الأمن السيبراني في مكافحة الجرائم الإلكترونية، وفي نفس السياق، دراسة علي (2024) استكشفت تأثير المواقع الإخبارية في مكافحة الجرائم الإلكترونية، موضحة العلاقة بين متابعة الجمهور للمواقع الإخبارية واتجاهاتهم نحو هذه الجرائم.

من جهة أخرى، تناولت دراسة القحطاني (2024) دور الإعلام الرقمي في توعية المواطنين بتقنيات الجرائم الإلكترونية، وقد تطرقت دراسة النعامي (2023) إلى واقع الجريمة الإلكترونية في اليمن، مبرزاً معوقات التوعية بالجريمة الإلكترونية، كما تناولت دراسة العسقلاني (2022) دور التعاون الإقليمي في مكافحة الجرائم الإلكترونية، وتناولت دراسة الشوابكة (2022) المعوقات الفنية والقانونية لمكافحة الجرائم الإلكترونية، بينما ركزت دراسة العنزي (2020) في الكويت على دور الإعلام الأمني في الوقاية من الجرائم الإلكترونية، وأظهرت أهمية الإعلام في توعية المجتمع وإبراز طرق الوقاية.

على الصعيد الدولي، تناولت دراسة Mijwil & Aljanabi (2023) دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، مشيرة إلى أهمية استخدام هذه التقنيات في الكشف عن الثغرات الأمنية وإدارة الحوادث، وكذلك دراسة Mphatheni & Maluleke (2022) التي استعرضت التهديدات السائدة في الأمن السيبراني وأكدت على أهمية تطوير المهارات اللازمة لمواجهة الجرائم الإلكترونية في المناطق الإفريقية، حيث تفتقر العديد من البلدان إلى الكوادر المتخصصة لمكافحة هذه الجرائم.

تميز الدراسة الحالية عن الدراسات السابقة:

تتميز الدراسة الحالية عن الدراسات السابقة في تركيزها على دور وحدة الجرائم الإلكترونية داخل المؤسسة الأمنية الفلسطينية بشكل خاص، وهو ما يعد فجوة بحثية هامة، حيث تركز الدراسات السابقة على دور الإعلام أو الجهات الأمنية بشكل عام، كما تسعى الدراسة الحالية إلى استكشاف التحديات التي تواجه وحدة الجرائم الإلكترونية في فلسطين، مثل المعوقات الفنية والتشريعية، وتحليل تأثير المتغيرات المختلفة على

استجابة الموظفين في هذه الوحدة، وهذا يضيف بُعداً محلياً متعلقاً بالواقع الفلسطيني، ويعزز الفهم حول كيفية مواجهة الجرائم الإلكترونية في ظل التحديات الخاصة التي يواجهها الأمن الفلسطيني.

1.5 مشكلة الدراسة

يشير الباحث إلى أن وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية تضطلع بأدوار ومهام كبيرة في مكافحة الجرائم الإلكترونية، خصوصاً في ظل التطور التكنولوجي السريع وانتشار استخدام الإنترنت في فلسطين وغيرها، ومع ذلك، تواجه هذه الوحدة تحديات متعددة تتعلق بالوعي المجتمعي، وفعالية الأساليب المتبعة في المكافحة، والمعوقات القانونية والفنية التي تعيق العمل الفعلي لهذه الوحدة في مواجهة الجرائم الإلكترونية.

وفي حين أن التوعية بمخاطر الجرائم الإلكترونية تُعد جزءاً أساسياً من مهام الوحدة، إلا أن الملاحقة القانونية تلعب دوراً محورياً في التصدي لهذه الجرائم، حيث ينص قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية في فلسطين على العقوبات التي تفرض على مرتكبي هذه الجرائم، مما يبرز أهمية تفعيل وتنفيذ النصوص التشريعية بما يضمن تحقيق الردع والعدالة.

ومن هنا جاء التركيز على دراسة دور وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية، بما يشمل التوعية بمخاطرها، الملاحقة القانونية، التعرف على الأساليب المتبعة في المكافحة، وتحليل المعوقات التي تواجهها، خاصة في ظل المستجدات القانونية والتشريعية التي أقرتها السلطة الفلسطينية، وفي إطار ذلك، يبرز دور التعاون الدولي في تعزيز قدرات الوحدة في مواجهة التحديات التقنية واللوجستية التي قد تتجاوز الحدود الوطنية، إذ أن الجرائم الإلكترونية بطبيعتها عابرة للحدود، مما يجعل التعاون مع المنظمات الدولية والهيئات الأمنية الخارجية أمراً حيوياً لتعزيز الكفاءة في تتبع المجرمين، وتبادل المعلومات، واستخدام التكنولوجيا المتقدمة.

وفي هذا السياق، يُلاحظ تزايد الاهتمام بأدوار المؤسسات المختلفة في مكافحة الجرائم الإلكترونية، فقد أظهرت دراسة نبيل (2024) أن الإعلام الأمني يلعب دوراً كبيراً في توعية الجمهور بمخاطر الجرائم الإلكترونية، وأن التوعية تزيد من وعي الأفراد بالوقاية منها، كما أكدت دراسة أبو القاسم (2024) أهمية الضبط الاجتماعي في الحد من الجرائم الإلكترونية، وضرورة تطوير التشريعات ومواكبتها للمتغيرات التكنولوجية السريعة، أما دراسة العنوز (2024) فقد بيّنت دور المؤسسات في التصدي لهذه الجرائم من خلال تعزيز الأمن السيبراني،

فهذه النتائج تدعم إشكالية الدراسة من حيث ضرورة تحديث السياسات والبرامج التوعوية، وتعزيز الملاحقة القانونية، وتوسيع نطاق التعاون بين الجهات المختلفة لضمان مكافحة الجرائم الإلكترونية بشكل فعال.

من هنا يمكن صياغة مشكلة الدراسة من خلال السؤال الرئيسي الآتي:

ما مدى فاعلية وحدة الجرائم الإلكترونية في المؤسسة الامنية الفلسطينية في مكافحة الجرائم الإلكترونية؟

1.6 أسئلة الدراسة

وينبثق عن السؤال الرئيس للدراسة الأسئلة الفرعية الآتية:

- كيف تسهم وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بمخاطر الجرائم الإلكترونية؟
- ما الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين؟
- إلى أي مدى يتجسد التعاون الدولي في مواجهة الجرائم الإلكترونية، وما أبرز آلياته؟
- في أي إطار تقوم وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية؟

- ما أبرز المعيقات والتحديات التي تعترض عمل وحدة الجرائم الإلكترونية في التصدي للجرائم الإلكترونية؟

- هل هناك فروق في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى للمتغيرات (النوع الاجتماعي، المؤهل العلمي، سنوات الخدمة، الرتبة العسكرية)؟

1.7 فرضيات الدراسة

1. لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى لمتغير النوع الاجتماعي.
2. لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى لمتغير المؤهل العلمي.
3. لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى لمتغير سنوات الخدمة.
4. لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى لمتغير الرتبة العسكرية.

1.8 أهداف الدراسة

تهدف الدراسة بشكل أساسي للتعرف على دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية، وينبثق عن الهدف الرئيسي الأهداف الفرعية الآتية:

1. تحديد دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بالجرائم الإلكترونية.
2. استكشاف الأساليب المستخدمة من قبل وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية لمكافحة الجرائم الإلكترونية.
3. دراسة آليات وأوجه التعاون الدولي في مكافحة الجرائم الإلكترونية.
4. تحديد دور وحدة الجرائم الإلكترونية في تطبيق الملاحقة القانونية ومتابعة مرتكبي الجرائم الإلكترونية وفقاً للتشريعات المحلية والدولية.
5. التعرف على المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية.
6. تحليل مدى وجود فروق في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية استناداً إلى المتغيرات (النوع الاجتماعي، المؤهل العلمي، سنوات الخدمة، الرتبة العسكرية).

1.9 أهمية الدراسة

يرى الباحث بأن أهمية الدراسة تكمن في المجالين التاليين:

اولاً: الأهمية النظرية:

تتمثل الأهمية النظرية لهذه الدراسة في دراسة وتوضيح المتغيرات المتعلقة بدور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية، فالدراسة تستعرض أهمية التوعية في الوقاية من الجرائم الإلكترونية، كما توضح كيف يمكن للمؤسسات الأمنية أن تساهم في زيادة الوعي من خلال برامج توعية مجتمعية، وكذلك تسهم الدراسة في تحديد الأساليب التكنولوجية المتبعة من قبل وحدة الجرائم الإلكترونية، مثل تقنيات الأمن السيبراني، وكذلك التعاون الدولي ودور وحدة الجرائم الإلكترونية في الملاحقة القانونية ومتابعة مرتكبي الجرائم الإلكترونية وفقاً للتشريعات المحلية والدولية حول تلك القضية، وعليه تكمن أهمية نظرية اخرى من خلال الدراسة، إذ يتم تناول التحديات القانونية والفنية والاجتماعية التي تواجه وحدة الجرائم الإلكترونية، وهي موضوعات بحثية حديثة تتطلب فهما عميقا للظروف المحيطة بالعمل الأمني في هذا المجال.

الأهمية العملية:

تتمثل الأهمية العملية في الفجوة البحثية في قلة الدراسات التي تناولت دور وحدة الجرائم الإلكترونية في المؤسسات الأمنية الفلسطينية، وخاصة في ظل التحديات التقنية والتشريعية الخاصة بالسياق الفلسطيني، وعليه تسهم الدراسة في سد هذه الفجوة من خلال استكشاف كيف يمكن لوحدة الجرائم الإلكترونية التعامل مع هذه التحديات وكيفية تطوير سياسات وتقنيات مكافحة الجرائم الإلكترونية بما يتناسب مع المستجدات القانونية والتكنولوجية في فلسطين، والعمل على تطوير آليات التعاون الدولي في مجال المكافحة لتلك الجرائم وتطوير التشريعات القانونية في هذا المجال.

وتبرز كذلك الأهمية العملية من خلال الخروج بنتائج يمكن أن يكون لها تأثير كبير على المعنيين والمختصين في مجالات الأمن السيبراني، المؤسسات الأمنية في المجتمع الفلسطيني، بحيث يأمل الباحث أن تساهم نتائج الدراسة في فهم دور وحدة الجرائم الإلكترونية في مكافحة الجرائم الالكترونية، وعليه تقديم الدراسة توصيات بشأن تعزيز السياسات والتشريعات المتعلقة بالجرائم الإلكترونية لمواكبة التطور التكنولوجي السريع، كما يمكن أن تساعد في فهم كيفية تعزيز التعاون بين المؤسسات التشريعية والأمنية في هذا المجال.

1.10 حدود الدّراسة

تم تحديد الدراسة وفق الحدود الآتية:

1. **الحدود البشرية:** تتمثل في منتسبي وحدة الجرائم الالكترونية في المؤسسة الأمنية الفلسطينية بكافة مسمياتهم الوظيفية.
2. **الحدود المكانية:** محافظة رام الله.
3. **الحدود الزمانية:** تتحدد الدراسة زمانيا في العام الدراسي 2024 – 2025.
4. **الحدود الموضوعية:** تم تحديد الدراسة موضوعياً في التعرف على دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية.

1.11 مصطلحات الدراسة

وحدة الجرائم الإلكترونية: وفقاً للقرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، وحدة الجرائم الإلكترونية هي وحدة متخصصة تنشأ في جهاز الشرطة وقوى الأمن، وتتمثل مهام هذه الوحدة في التعامل مع الجرائم الإلكترونية ومتابعة القضايا المتعلقة بها، كما تُشرف النيابة العامة عليها ضمن دائرة اختصاصها، ويتم النظر في القضايا المرتبطة بالجرائم الإلكترونية من قبل المحاكم النظامية والنيابة العامة، وفقاً لاختصاصاتهما.

وحدة الجرائم الإلكترونية إجرائياً: وحدة الجرائم الإلكترونية هي وحدة متخصصة ضمن جهاز الشرطة الفلسطينية، تتولى هذه الوحدة مسؤولية مكافحة الجرائم الإلكترونية، مثل الاختراقات والتهديدات الأمنية التي تتم عبر الشبكة الإلكترونية أو وسائل تكنولوجيا المعلومات، وتشمل مهام الوحدة التعامل مع الجرائم المتعلقة بالقرصنة، التسلل إلى الأنظمة أو الشبكات الإلكترونية، التلاعب بالبيانات والمعلومات الإلكترونية، بالإضافة إلى مكافحة استخدام وسائل التشفير بطرق غير قانونية.

المؤسسة الأمنية الفلسطينية: وهي قوات الامن والشرطة كقوات نظامية وهي القوة المسلحة في البلاد والتي ينحصر وظيفتها في الدفاع عن الوطن وحماية المجتمع والسهر على حفظ الأمن والنظام العام والآداب العامة وتؤدي واجبها في الحدود التي رسمها القانون في استخدام كامل الحقوق والحريات[1].

الجرائم الإلكترونية: أي جريمة يكون متطلباً لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب، فهي مجموعة من الأفعال والأنشطة المعاقب عليها قانوناً، والتي تربط بين الفعل الإجرامي والثورة التكنولوجية، فهي الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح (رجب، 2023).

الجرائم الإلكترونية إجرائياً: وهي الجرائم المرتكبة من خلال الحاسوب او الثورة التكنولوجية والتي يعاقب عليها القانون الفلسطيني من خلال قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية الفلسطيني.

[1] (المادة رقم 84 من القانون الأساسي المعدل لسنة 2003م.

الفصل الثاني

الطريقة والاجراءات

2.1 تمهيد

يعد البحث العلمي طريقة منظمة لجمع البيانات والمعلومات وتحليلها من أجل الوصول إلى إجابات أو حلول للمشكلات التي تواجه الأفراد والمنظمات، وتعتبر منهجية الدراسة وإجراءاتها أساساً يتم من خلاله إنجاز الجانب التطبيقي من الدراسة، وعن طريقها يتم الحصول على البيانات المطلوبة لإجراء التحليل الاحصائي للتوصل إلى النتائج التي يتم تفسيرها في ضوء أدبيات الدراسة المتعلقة بها، وبالتالي تحقق الأهداف التي تسعى إلى تحقيقها.

وقد تناول الباحث في هذا الفصل وصفاً للمنهج المتبع ومجتمع الدراسة، وكذلك أداة الدراسة المستخدمة وطريقة إعدادها وكيفية بنائها وتطويرها، ومدى صدقها وثباتها، بالإضافة إلى وصف للإجراءات التي قام بها الباحث في تصميم أداة الدراسة وتقنينها، والأدوات التي استخدمتها لجمع بيانات الدراسة، وينتهي الفصل بالمعالجات الاحصائية التي استخدمتت في تحليل البيانات واستخلاص النتائج، وفيما يلي وصف لهذه الاجراءات.

2.2 منهجية الدراسة

نظرا لطبيعة الدراسة والأهداف التي تسعى لتحقيقها فقد استخدم الباحث المنهج الوصفي التحليلي والذي يحاول التعرف على دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية ؛ ويحاول المنهج الوصفي التحليلي أن يصف الظاهرة موضوع الدراسة كما توجد في الواقع وصفاً دقيقاً يعبر عنها تعبيراً كيفياً وكمياً وأيضاً تحليل بياناتها وتوضيح العلاقة بين مكوناتها والآراء التي تطرح حولها والعمليات التي تتضمنها والآثار التي تحدثها.

ويعرف الحمداني (100:2006) المنهج الوصفي التحليلي بأنه "المنهج الذي يسعى لوصف الظواهر أو الأحداث المعاصرة، أو الراهنة فهو أحد أشكال التحليل والتفسير المنظم لوصف ظاهرة أو مشكلة، ويقدم بيانات عن خصائص معينة في الواقع، وتتطلب معرفة المشاركين في الدارسة والظواهر التي ندرسها والأوقات التي نستعملها لجمع البيانات.

2.3 مجتمع وعينة الدراسة

يعرف مجتمع الدراسة بأنه جميع مفردات الظاهرة التي يدرسها الباحث وبناءً على مشكلة الدراسة وأهدافها فإن مجتمع الدراسة يتكون من جميع منتسبي وحدة الجرائم الالكترونية (بكافة مسمياتهم الوظيفية) في محافظة رام الله، حيث بلغ عدد مجتمع الدراسة 250، وتم استخدام أسلوب العينة العشوائية البسيطة، وقام الباحث بتوزيع الاستبيان على افراد العينة البالغ عددهم 148 وتم استرداد 148 استبانة صالحة للتحليل الاحصائي، وبلغت نسبة الاسترداد 100%.

2.4 خصائص عينة الدراسة

تم حساب التكرارات والنسب المئوية لأفراد عينة الدراسة وفقاً للمتغيرات التالية: (النوع الاجتماعي، المؤهل العلمي، سنوات الخدمة، الرتبة العسكرية).

جدول (2.1)

توزيع أفراد العينة حسب النوع الاجتماعي

المتغير	فئات المتغير	التكرار	النسبة المئوية
النوع الاجتماعي	ذكر	126	%85.1
	انثى	22	%14.9
المجموع		**148**	**%100**

يتضح من الجدول (2.1) أن 85.1% من أفراد العينة ذكور، بينما نسبة 14.9% من أفراد العينة اناث، ويعزو الباحث تلك النتيجة الى الطبيعة الهيكلية والتوزيع الديموغرافي للمؤسسة الأمنية الفلسطينية، حيث يهيمن الذكور على معظم الوظائف الأمنية بسبب مجموعة من العوامل الثقافية، والاجتماعية، والتنظيمية. فغالباً ما ترتبط الوظائف الأمنية والعسكرية بتحديات بدنية وظروف عمل تتطلب الجاهزية المستمرة والتعامل مع المخاطر، مما يجعلها تقليدياً مجالاً يغلب عليه الذكور، وقد يكون لسياسات التوظيف والتأهيل داخل المؤسسة دور في تحديد نسب مشاركة الإناث، حيث قد تواجه النساء تحديات في الانخراط في مثل هذه المجالات بسبب محدودية الأدوار المخصصة لهن أو تفضيل توظيفهن في وظائف إدارية وداعمة أكثر من الميدان الأمني المباشر، كما أن العوامل المجتمعية والثقافية تلعب دوراً في توجيه خيارات الأفراد المهنية، مما يعزز الفجوة بين الجنسين في هذا القطاع.

جدول (2.2)

توزيع أفراد العينة حسب المؤهل العلمي

المتغير	فئات المتغير	التكرار	النسبة المئوية
المؤهل العلمي	ثانوية فأقل	7	%4.7
	دبلوم- بكالوريوس	119	%80.4
	دراسات عليا	22	%14.9
	المجموع	**148**	**%100**

يتضح من الجدول (2.2) أن 4.7% من أفراد العينة مؤهلهم العلمي (ثانوية فأقل)، وأن 23.3% من أفراد العينة مؤهلهم العلمي (دبلوم- بكالوريوس)، بينما 14.4% من أفراد العينة مؤهلهم العلمي (دراسات عليا)، ويعزو الباحث تلك النتيجة الى متطلبات التوظيف والمعايير الأكاديمية المعتمدة داخل المؤسسة الأمنية الفلسطينية، حيث تعكس البيانات ميل المؤسسة إلى استقطاب الكوادر ذات المؤهلات المتوسطة والعليا، بما يتماشى مع التطورات الحديثة في العمل الأمني الذي يتطلب مهارات متخصصة ومعرفة تقنية وإدارية متقدمة،

ويظهر انخفاض نسبة الأفراد الحاصلين على مؤهل (ثانوية فأقل) كنتيجة لاعتماد المؤسسة على سياسات توظيف تفضل المؤهلات الأكاديمية الأعلى لضمان كفاءة الأداء الأمني والإداري.

كما أن النسبة المرتفعة نسبياً لحملة الدبلوم والبكالوريوس وتعكس تركيز المؤسسة على توظيف أفراد يتمتعون بتعليم جامعي يمكنهم من أداء مهامهم بفاعلية أكبر، خاصة في المجالات التي تتطلب تحليلاً واستراتيجيات متقدمة، أما نسبة الحاصلين على الدراسات العليا، فتشير إلى وجود فئة متخصصة في الأدوار البحثية، التخطيطية، والقيادية داخل المؤسسة، وهو ما يعكس التوجه نحو تطوير الأداء الأمني من خلال استثمار الخبرات الأكاديمية والعلمية المتقدمة.

جدول (2.3)

توزيع أفراد العينة حسب سنوات الخدمة

المتغير	فئات المتغير	التكرار	النسبة المئوية
سنوات الخدمة	أقل من 5 سنوات	22	%14.9
	من 5_ أقل من 10 سنوات	55	%37.2
	من 10 – أقل من 15 سنة	32	%21.6
	15 سنة فأكثر	39	%26.4
	المجموع	**148**	**%100**

يتضح من الجدول (2.3) أن 14.9% من أفراد العينة سنوات خدمتهم (أقل من 5 سنوات)، بينما 37.2% من أفراد العينة سنوات خدمتهم (من 5– أقل من 10 سنوات)، بينما 37.2% من أفراد العينة سنوات خدمتهم (من 10 – أقل من 15 سنة)، بينما 37.2% من أفراد العينة سنوات خدمتهم (15 سنة فأكثر)، ويعزو الباحث تلك النتيجة الى الطبيعة التنظيمية للمؤسسة الأمنية الفلسطينية، والتي تعكس استقرار الكوادر الأمنية واستمراريتها في الخدمة لفترات طويلة، ويشير الباحث الى ان النسب المرتفعة للأفراد الذين تتراوح سنوات خدمتهم بين (5 – أقل من 15 سنة) إلى اعتماد المؤسسة على الخبرة التراكمية في أداء المهام الأمنية، حيث يُفضل الاحتفاظ بالعناصر ذوي الخبرة لضمان كفاءة العمليات الأمنية والإدارية.

كما أن انخفاض نسبة الأفراد الذين خدموا أقل من 5 سنوات قد يكون مرتبطاً بسياسات التوظيف والتدرج الوظيفي، حيث قد تتطلب بعض المناصب فترات تدريب وتأهيل طويلة قبل تثبيت الأفراد في المؤسسة، كما ان ارتفاع نسبة من لديهم خبرة طويلة يشير إلى محدودية معدلات التقاعد المبكر أو الاستقالات، مما يعكس الاستقرار الوظيفي والرضا المهني داخل المؤسسة.

جدول (2.4)

توزيع أفراد العينة حسب الرتبة العسكرية

المتغير	فئات المتغير	التكرار	النسبة المئوية
الرتبة العسكرية	أقل من ملازم	13	%8.8
	من ملازم – رائد	105	%70.9
	مقدّم فأعلى	30	%20.3
المجموع		**148**	**%100**

يتضح من الجدول (2.4) أن 2.8% من أفراد العينة رتبتهم العسكرية (أقل من ملازم)، وأن 10.6% من أفراد العينة رتبتهم العسكرية (من ملازم – رائد)، وأن 5% من أفراد العينة رتبتهم العسكرية (مقدّم فأعلى)، ويعزو الباحث تلك النتيجة إلى الهيكل التنظيمي للمؤسسة الأمنية الفلسطينية، الذي يعكس توزيعاً هرمياً للرتب العسكرية، حيث تتركز الغالبية العظمى من الأفراد في الرتب المتوسطة والعليا، مما يشير إلى اعتماد المؤسسة على الكوادر ذات الخبرة والتأهيل العالي في القيادة واتخاذ القرارات، وتوضح النسبة المنخفضة للأفراد الذين يحملون رتباً أقل من ملازم أن المؤسسة قد تكون تضع معايير صارمة للتجنيد والترقية، مما يحد من عدد الأفراد في الرتب الدنيا.

كما أن النسبة الأكبر في فئة (ملازم – رائد) تعكس توجه المؤسسة نحو التدرج الوظيفي والاستفادة من الخبرات المكتسبة ضمن هذه الفئة، حيث تمثل هذه الرتب النواة الأساسية للقيادة الميدانية والإدارية، أما

انخفاض نسبة الضباط الحاصلين على رتبة مقدّم فأعلى، فقد يكون ناتجاً عن عوامل مثل طبيعة الترقيات العسكرية التي تعتمد على سنوات الخدمة والأداء الوظيفي والاحتياجات التنظيمية.

2.5 أداة الدراسة

ولتحقيق أهداف الدراسة واختبار الفرضيات التي بنيت عليها فإن الأمر يستلزم الاعتماد على نوعين من البيانات:

1. البيانات الثانوية: وهي التي استخدمت لتكوين الاطار النظري للدراسة إذ تمت الاستعانة بالمصادر التالية:

- الدوريات المتخصصة والنشرات والتقارير الدورية والكتب المنهجية والمراجع العلمية التي تبحث في القانون العام.
- الرسائل العلمية (ماجستير ودكتوراه) التي تبحث في القانون العام.
- مواقع الانترنت.

2. البيانات الأولية: وهي البيانات التي تم جمعها باستخدام أداة الدراسة والتي تم إعدادها خصيصاً لموضوع الدراسة.

2.6 صدق الأداة وثباتها

صدق الاستبانة:

صدق الاستبانة يعني أن تقيس الاستبانة ما وضعت لقياسه الجرجاوي (2010)، كما يقصد بالصدق "شمول الاستقصاء لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها ومفرداتها من ناحية ثانية، بحيث تكون مفهومة لكل من يستخدمها عبيدات، وعدس، وعبد الحق (2001) وتم توزيع عينة

استطلاعية حجمها 30 استبانة لاختبار الاتساق الداخلي والصدق البنائي وثبات الاستبانة، وقد قام الباحث بالتأكد من صدق الاستبانة بطريقتين:

1. صدق الاستبانة من وجهة نظر المحكمين "الصدق الظاهري":

يقصد بالصدق من وجهة نظر المحكمين "هو أن يختار الباحث عدداً من المحكمين المتخصصين في مجال الظاهرة أو المشكلة موضوع الدراسة" (الجرجاوي،2010: 107) حيث تم عرض الاستبانة على مجموعة من المحكمين تألفت من (4) من متخصصين القانون العام ملحق رقم (1)، وقد استجاب الباحث لآراء المحكمين وقامت بإجراء ما يلزم من حذف وتعديل في ضوء المقترحات المقدمة، وبذلك خرجت الاستبانة في صورتها النهائية كما في الملحق رقم (3).

2. صدق المقياس

الاتساق الداخلي Internal Validity

يقصد بصدق الاتساق الداخلي مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي إليه هذه الفقرة، وقد قام الباحث بحساب الاتساق الداخلي للاستبانة وذلك من خلال حساب معاملات الارتباط بين كل فقرة من فقرات مجالات الاستبانة والدرجة الكلية للمجال نفسه؛ وقد تم ذلك على العينة الاستطلاعية المكونة من (30) مفردة، وفيما يلي توضيح نتائج الاتساق الداخلي لأداة الدراسة.

صدق الاتساق الداخلي:

يتبين من الجدول (2.5) ملحق (د) أن قيم مستوى الدلالة الإحصائية أقل من (0.05)، وكانت جميعها دالة إحصائيا، وبذلك يعتبر جميع الفقرات صادقة لما وضع لقياسه وبالتالي الفقرات تفي بأغراض الدراسة.

الصدق البنائي العام لأبعاد الاستبانة:

يعتبر الصدق البنائي أحد مقاييس صدق الأداة الذي يقيس مدى تحقق الأهداف التي تريد الأداة تحقيقها، ويبين مدى ارتباط كل بُعد من أبعاد الدراسة بالدرجة الكلية لفقرات الاستبانة.

جدول (2.6)

معاملات الارتباط بين الدرجة الكلية لكل بُعد في الاستبانة والدرجة الكلية للاستبانة

المجال	معامل بيرسون للارتباط	القيمة الاحتمالية
إسهام وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بمخاطر الجرائم الإلكترونية	0.542**	0.000
الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين	0.617**	0.000
آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية	0.497**	0.000
قيام وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية	0.546**	0.000
المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية	0.781**	0.000

** دال احصائياً عند مستوى الدلالة (0.01).

يتبين من الجدول (2.6) أن قيم مستوى الدلالة الإحصائية لكل بعد ومحور في الاستبانة والدرجة الكلية للاستبانة أقل من 0.05، وكانت جميعها دالة إحصائيا، وبذلك يعتبر البعد والمحور صادقاً لما وضع لقياسه وبالتالي الأبعاد والمحاور تفي بأغراض الدراسة.

ثبات الاستبانة:

ثبات أداة الدراسة يعني التأكد من أن الاجابة ستكون واحدة بمعنى أن تُعطى نفس النتيجة في حال تكرَّر توزيعها تحت نفس الظروف والشروط.

وقد تحقق الباحث من ثبات أداة الدراسة باستخدام معامل ألفا كرونباخ، وكانت النتائج كما هي مبينة في جدول (2.7).

جدول (2.7)

معاملات الثبات بطريقة ألفا كرونباخ

المجال	عدد الفقرات	معامل الفا كرونباخ
إسهام وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بمخاطر الجرائم الإلكترونية	7	0.941
الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين	7	0.897
آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية	7	0.896
قيام وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية	7	0.895
المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية	24	0.914
الدرجة الكلية للاستبانة	**52**	**0.928**

يتضح من الجدول رقم (2.7) أن قيم معاملات الثبات لأبعاد الاستبانة والمحاور جاءت بقيم عالية، وبلغت قيمة معامل الثبات الكلي للأبعاد 0.928، وتشير هذه القيم من معاملات الثبات إلى صلاحية الاستبانة للتطبيق وامكانية الاعتماد على نتائجها والوثوق بها.

2.7 إجراءات تنفيذ الدراسة

1. قام الباحث بإعداد استبانة الدراسة.
2. تم التأكد من مدى صلاحية الاستبانة لقياس متغيرات الدراسة.
3. وزعت الاستبانة على جميع أفراد الدراسة والبالغ عددهم148 مفردة.
4. تم استرداد 148 استبانة صالحة للتحليل الاحصائي.
5. تم تفريغ البيانات من خلال برنامج التحليل الإحصائي SPSS وتحليلها.

2.8 التوزيع الطبيعي لمتغيرات الدراسة

يستخدم الاحصائيون نوعين من الاختبارات الاحصائية لاختبار الفرضيات، النوع الأول الاختبارات المعلمية (Parametric Tests) والنوع الثاني الاختبارات اللامعلمية (Non Parametric Tests) ويشترط لاستخدام الاختبارات المعلمية شرط التوزيع الطبيعي للبيانات Parametric Tests المراد اجراء الاختبارات الاحصائية عليها، بينما تستخدم الاختبارات اللامعلمية كبديل للاختبارات المعلمية في حال عدم تحقق شرط التوزيع الطبيعي للبيانات ولكن ذلك يكون فقط في حال العينات الصغيرة التي يقل حجمها عن 30 مفردة، بينما العينات التي يزيد حجمها عن 30 مفردة يمكن التخلي عن شرط التوزيع الطبيعي، وذلك وفقاً لما تُقرُّه نظرية النزعة المركزية (ربيع، 2007)، وفي هذه الدراسة سيتم استخدام الاختبارات المعلمية وفقاً للسبب الذي تم ذكره دون اللجوء للتحقق من شرط التوزيع الطبيعي للبيانات.

2.9 المعالجات الاحصائية

اعتمدت هذه الدارسة بشكل أساسي على استخدام الحزمة الاحصائية للعلوم الاجتماعية (Statistical Package for Social Sciences-spss v.26) في معالجة وتحليل البيانات وفيما يلي أهم الأساليب الإحصائية الوصفية والاستدلالية التي تم استخدامها في معالجة بيانات هذه الدّراسة:

1. التكرارات (Frequencies)، والنسب المئوية (Percentages): للتعرف على خصائص أفراد الدراسة، وتوزيعهم حسب البيانات الشخصية.

2. الوسط الحسابي (Mean): وذلك لمعرفة مدى ارتفاع أو انخفاض استجابات مفردات الدّراسة على الفقرات والأبعاد الرئيسة للاستبانة.

3. الانحراف المعياري (Standard Deviation): للتعرف على مدى انحراف استجابات مفردات الدّراسة لكل عبارة من الفقرات عن وسطها الحسابي، إلى جانب الأبعاد الرئيسة، فكلما اقتربت قيمته من الصفر تركزت الاستجابات وانخفض تشتتها.

4. معامل ارتباط بيرسون (Pearson Correlation): للتحقق من صدق الاتساق الداخلي لأداة الدّراسة.

5. معامل الثبات ألفا كرونباخ (Cronbach's Alpha): للتحقق من ثبات أداة الدّراسة، ولفحص العلاقة بين المتغيرات.

6. اختبار (T-test for two independent samples): لاختبار الفروق بين استجابات أفراد الدراسة لعينتين مستقلتين.

7. اختبار (One-way ANOVA): لاختبار الفروق بين استجابات أفراد الدراسة لأكثر من عينتين مستقلتين.

الفصل الثالث

نتائج الدراسة

3.1 المقدمة

بعد الانتهاء من مرحلة جمع البيانات الميدانية بوساطة الاستبانة، والتي قام الباحث بإعدادها خصيصاً لتحقيق اهداف هذه الدراسة، والتي وزعت على مجتمع الدراسة المستهدف وهم منتسبي وحدة الجرائم الالكترونية (بكافة مسمياتهم الوظيفية) في محافظة رام الله، وفي هذا الفصل يتناول نتائج الدراسة، حيث تمت الاجابة عن أسئلة الدراسة، ومن ثم تفسير النتائج والتعقيب عليها، بالإضافة الى أوجه التشابه والاختلاف مع الدراسات السابقة.

ومن أجل الإجابة عن أسئلة الدراسة، استخدم الباحث المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لكل فقرة من فقرات كل مجال من مجالات الدراسة.

وقد أعطي للفقرات (5) درجات عن كل إجابة (موافق بشدة)، و(4) درجات عن كل إجابة (موافق)، و(3) درجات عن كل إجابة (لا رأي)، ودرجتان عن كل إجابة (أُعارض)، ودرجة واحدة عن كل إجابة (أُعارض بشدة)، ومن أجل تفسير النتائج، أعتمد مقياس ليكرت الخماسي الآتي للنسب المئوية لاستجابة عينة الدراسة ومن أجل تفسير النتائج اعتمدت الدراسة مقياس ليكرت الخماسي لقيم المتوسطات الحسابية للاستجابات كما هو موضح في الجدول (3.1) التالي:

جدول (3.1)

معيار الحكم وفقا لمقياس ليكرت الخماسي

الرقم	المتوسط الحسابي		الوزن النسبي المئوي		درجة الموافقة
	من	إلى	من	إلى	
1	1.00	اقل من1.80	%20.00	%36.00	منخفضة جدا
2	1.81	اقل من2.60	%36.00	%52.00	منخفضة
3	2.61	اقل من3.40	%52.00	%68.00	متوسطة
4	3.41	اقل من4.20	%68.00	%84.00	مرتفعة
5	4.21	5.00	%84.00	%100.00	مرتفعة جدا

وتبين الجداول التالية النتائج المتعلقة بالمتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات المبحوثين حول مجالات وأبعاد الدراسة.

3.2 نتائج الدراسة

وفيما يلي عرض وتحليل نتائج اجابات المبحوثين على أسئلة الدراسة:

النتائج المتعلقة بالسؤال الأول: كيف تسهم وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بمخاطر الجرائم الإلكترونية؟

جدول (3.2)

المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية للمجال الاول

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة
1	تقدم الوحدة برامج توعية دورية حول الجرائم الإلكترونية.	4.128	0.851	82.6%	مرتفعة
2	تستخدم الوحدة وسائل الإعلام المختلفة لنشر الوعي بخطورة الجرائم الإلكترونية.	3.905	0.883	78.1%	مرتفعة
3	تنظم الوحدة حملات توعوية في المدارس والجامعات.	3.926	0.926	78.5%	مرتفعة
4	توفر الوحدة كتيبات إرشادية للجمهور حول كيفية حماية أنفسهم إلكترونياً.	3.655	1.028	73.1%	مرتفعة
5	تستهدف الوحدة فئات المجتمع الأكثر عرضة للجرائم الإلكترونية بالتوعية.	3.872	0.898	77.4%	مرتفعة
6	تعزز الوحدة من ثقافة الاستخدام الآمن للإنترنت عبر منصاتها.	3.973	0.903	79.5%	مرتفعة
7	تقدم الوحدة ورش عمل تدريبية للتوعية بمخاطر الجرائم الإلكترونية.	3.959	0.932	79.2%	مرتفعة
	الدرجة الكلية للمجال الاول	**3.917**	**0.790**	**78.3%**	**مرتفعة**

يتبين من الجدول رقم (3.2) أن استجابات المبحوثين المتعلقة بالمجال الاول: دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بالجرائم الالكترونية كانت بدرجة مرتفعة، ويرى الباحث أن أعلى

متوسط حسابي كان للفقرة الاولى (تقدم الوحدة برامج توعية دورية حول الجرائم الإلكترونية) بنسبة مئوية 82.6%، وأن اقل متوسط حسابي كان للفقرة الرابعة (توفر الوحدة كتيبات إرشادية للجمهور حول كيفية حماية أنفسهم إلكترونياً.)، بنسبة مئوية 73.4%، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية 78.3% وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة على دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بالجرائم الالكترونية، وهذه النتيجة تتفق مع دراسة نبيل (2024) ويعزو الباحث تلك النتيجة الى الجهود الفعالة التي تبذلها وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مجال التوعية بالجرائم الإلكترونية، من خلال تقديم برامج توعوية متخصصة، وتنظيم حملات إعلامية، وإعداد مواد إرشادية تستهدف مختلف فئات المجتمع، كما أن استخدام الوحدة لأساليب متعددة، مثل الندوات، وورش العمل، والتواصل عبر المنصات الرقمية، يعزز من وعي الأفراد بمخاطر الجرائم الإلكترونية وسبل الوقاية منها، وكما يعزو الباحث ذلك الى إدراك أفراد العينة لأهمية الدور الذي تؤديه الوحدة في مواجهة التهديدات السيبرانية المتزايدة، خاصة في ظل التطور التكنولوجي السريع والاعتماد المتزايد على الأنظمة الرقمية في مختلف المجالات. كما أن التعاون بين الوحدة والجهات الأكاديمية والمؤسسات ذات الصلة قد ساهم في تعزيز جودة وفعالية هذه البرامج التوعوية، مما زاد من مستوى الوعي لدى الأفراد وأدى إلى توافقهم العالي مع أهمية هذا الدور.

النتائج المتعلقة بالسؤال الثاني: ما الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين؟

جدول (3.3)

المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية للمجال الثاني

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة
1	تعتمد الوحدة على تقنيات حديثة في تتبع الجرائم الإلكترونية.	4.081	0.821	81.6%	مرتفعة
2	تستخدم الوحدة برامج متقدمة لتحليل البيانات الرقمية.	3.919	0.845	78.4%	مرتفعة
3	تتعاون الوحدة مع شركات التكنولوجيا لتطوير أدوات مكافحة الجرائم الإلكترونية.	3.730	0.846	74.6%	مرتفعة
4	تعتمد الوحدة على أساليب تحقيق رقمية متطورة.	3.865	0.862	77.3%	مرتفعة
5	تطبق الوحدة آليات حديثة لاسترجاع البيانات المسروقة.	3.905	0.844	78.1%	مرتفعة
6	تستخدم الوحدة أنظمة مراقبة إلكترونية للكشف عن الجرائم قبل وقوعها.	3.716	1.010	74.3%	مرتفعة
7	توفر الوحدة خطاً ساخناً للإبلاغ عن الجرائم الإلكترونية.	3.736	0.971	74.7%	مرتفعة
	الدرجة الكلية للمجال الاول	**3.850**	**0.699**	**77.0%**	**مرتفعة**

يتبين من الجدول رقم (3.3) أن استجابات المبحوثين المتعلقة بالمجال الثاني: الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين كانت بدرجة مرتفعة، ويرى الباحث أن أعلى متوسط حسابي كان للفقرة الاولى (تعتمد الوحدة على تقنيات حديثة في تتبع الجرائم الإلكترونية) بنسبة مئوية 81.6%، وأن اقل متوسط حسابي كان للفقرة السادسة (تستخدم الوحدة أنظمة مراقبة إلكترونية للكشف عن الجرائم قبل وقوعها)، بنسبة مئوية 74.3%، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية 77.0% وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة. ويعزو الباحث تلك النتيجة الى الأساليب المستخدمة من قبل وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية لمكافحة الجرائم الإلكترونية، وجاءت هذه الدراسة متفقة مع نتائج دراسة العنوز (2024)، ويعزو الباحث تلك النتيجة الى فاعلية الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية، والتي تتسم بالتطور

التقني، والاستجابة السريعة، والتكامل بين الجوانب القانونية، التقنية، والتوعوية، حيث تستخدم الوحدة تقنيات حديثة في الرصد والتحليل، وتعتمد على أنظمة مراقبة متقدمة، بالإضافة إلى تعزيز التعاون مع الجهات المحلية والدولية المتخصصة في مجال الأمن السيبراني.

كما أن الإجراءات الوقائية والاستباقية التي تتبعها الوحدة، مثل التوعية المستمرة، والتحقيقات الرقمية المتخصصة، وتطوير آليات الإبلاغ عن الجرائم الإلكترونية، تساهم في تعزيز الثقة بأدائها، كما إن التكامل بين الكوادر الأمنية والتقنية المتخصصة، ودعم التشريعات المنظمة لهذا المجال، قد ساهم في رفع مستوى فعالية الوحدة، مما انعكس على درجة الموافقة المرتفعة من قبل أفراد العينة بشأن دورها في مكافحة الجرائم الإلكترونية.

النتائج المتعلقة بالسؤال الثالث: إلى أي مدى يتجسد التعاون الدولي في مواجهة الجرائم الإلكترونية، وما أبرز آلياته؟

جدول (3.4)

المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية للمجال الثالث

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة
1	تشارك الوحدة في مؤتمرات دولية متعلقة بمكافحة الجرائم الإلكترونية.	4.149	0.750	83.0%	مرتفعة
2	تتعاون الوحدة مع منظمات دولية لمكافحة الجرائم الإلكترونية.	3.966	0.836	79.3%	مرتفعة
3	تنسق الوحدة مع وحدات جرائم إلكترونية في دول أخرى لتبادل المعلومات.	3.899	0.797	78.0%	مرتفعة
4	تعتمد الوحدة على اتفاقيات دولية لتسليم المجرمين الإلكترونيين.	3.716	0.926	74.3%	مرتفعة
5	تستفيد الوحدة من الخبرات الدولية في مكافحة الجرائم الإلكترونية.	4.074	0.775	81.5%	مرتفعة
6	تعمل الوحدة على تطوير شراكات دولية لتعزيز جهودها.	3.966	0.742	79.3%	مرتفعة
7	تتابع الوحدة التشريعات الدولية المتعلقة بالجرائم الإلكترونية.	3.926	0.817	78.5%	مرتفعة
	الدرجة الكلية للمجال الاول	**3.957**	**0.634**	**79.1%**	**مرتفعة**

يتبين من الجدول رقم (3.4) أن استجابات المبحوثين المتعلقة بالمجال الثالث: آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية كانت بدرجة مرتفعة، ويرى الباحث أن أعلى متوسط حسابي كان للفقرة الاولى (تشارك الوحدة في مؤتمرات دولية متعلقة بمكافحة الجرائم الإلكترونية) بنسبة مئوية 83%، وأن اقل متوسط حسابي كان للفقرة الرابعة (تعتمد الوحدة على اتفاقيات دولية لتسليم المجرمين الإلكترونيين)، بنسبة مئوية 74.3%، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية 79.1% وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة على آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية، وتتفق هذه النتيجة مع دراسة العسقلاني (2022) دور مجلس التعاون الخليجي القانوني والتعاوني في مكافحة الجرائم الإلكترونية.

ويعزو الباحث تلك النتيجة الى الدور المهم الذي تلعبه آليات وأوجه التعاون الدولي في تعزيز فعالية مكافحة الجرائم الإلكترونية داخل المؤسسة الأمنية الفلسطينية، فمع تزايد التهديدات السيبرانية عبر الحدود، أصبحت الشراكات والتنسيق مع الجهات الأمنية الدولية والمنظمات المتخصصة ضرورة ملحّة لتعزيز القدرات المحلية في مواجهة الجرائم الإلكترونية. ويعكس هذا المستوى المرتفع من الموافقة إدراك أفراد العينة لأهمية هذا التعاون في تبادل المعلومات الاستخباراتية، وتحديث أساليب التحقيق، والاستفادة من الخبرات والتقنيات المتقدمة التي تمتلكها الجهات الدولية، كما ويفسر الباحث أن مشاركة المؤسسة الأمنية الفلسطينية في الاتفاقيات والبروتوكولات الدولية، إضافةً إلى التعاون مع المنظمات الإقليمية والدولية المختصة بالأمن السيبراني، قد ساهم في تحسين إمكانيات الرصد، التتبع، والاستجابة للجرائم الإلكترونية، كما إن الدورات التدريبية المشتركة، وورش العمل المتبادلة، وتطوير التشريعات المتوافقة مع المعايير الدولية، كلها عوامل تعزز من فعالية التعاون الدولي، مما أدى إلى هذا المستوى العالي من الموافقة من قبل أفراد العينة.

النتائج المتعلقة بالسؤال الرابع: في أي إطار تقوم وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية؟

جدول (3.5)

المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية للمجال الرابع

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة
1	تتابع الوحدة القضايا الإلكترونية بالتنسيق مع الجهات القضائية.	4.297	0.733	85.9%	مرتفعة
2	تقدم الوحدة أدلة رقمية موثوقة للمحاكم.	4.270	0.734	85.4%	مرتفعة
3	تساعد الوحدة في صياغة تقارير فنية حول الجرائم الإلكترونية.	4.318	0.729	86.4%	مرتفعة
4	تنسق الوحدة مع النيابة العامة لملاحقة المتهمين بالجرائم الإلكترونية.	4.297	0.654	85.9%	مرتفعة
5	توفر الوحدة خبراء قانونيين متخصصين في الجرائم الإلكترونية.	4.054	0.823	81.1%	مرتفعة
6	تدعم الوحدة الضحايا في تقديم شكاوى قانونية.	4.142	0.650	82.8%	مرتفعة
7	تساهم الوحدة في تعزيز تطبيق القوانين المتعلقة بالجرائم الإلكترونية.	4.115	0.778	82.3%	مرتفعة
	الدرجة الكلية للمجال الاول	**4.213**	**0.572**	**84.3%**	**مرتفعة**

يتبين من الجدول رقم (3.5) أن استجابات المبحوثين المتعلقة بالمجال الرابع: قيام وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية كانت بدرجة مرتفعة، ويرى الباحث أن أعلى متوسط حسابي كان للفقرة الثالثة (تساعد الوحدة في صياغة تقارير فنية حول الجرائم الإلكترونية) بنسبة مئوية 86.4%، وأن اقل متوسط حسابي كان للفقرة الخامسة (توفر الوحدة خبراء قانونيين متخصصين في الجرائم الإلكترونية)، بنسبة مئوية 81.1%، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية 84.3% وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة على دور وحدة الجرائم

الإلكترونية في تطبيق الملاحقة القانونية ومتابعة مرتكبي الجرائم الإلكترونية وفقاً للتشريعات المحلية والدولية، وتتفق هذه الدراسة مع دراسة (عبد الباقي، 2018).

ويعزو الباحث تلك النتيجة الى كفاءة وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في تطبيق الملاحقة القانونية ومتابعة مرتكبي الجرائم الإلكترونية، وذلك من خلال التزامها بالتشريعات المحلية والدولية ذات الصلة، ويعكس هذا المستوى المرتفع من الموافقة إدراك أفراد العينة لفاعلية الوحدة في استخدام الأدلة الرقمية، وإجراءات التحقيق المتقدمة، والتعاون مع الجهات القضائية لضمان تحقيق العدالة، كما أن امتثال الوحدة للمعايير القانونية الدولية يعزز من مصداقيتها في ملاحقة الجرائم الإلكترونية، خاصة مع تبنّيها استراتيجيات متطورة تشمل التنسيق مع المنظمات الإقليمية والدولية، وتفعيل الاتفاقيات الثنائية والمتعددة الأطراف لتسليم المطلوبين، وتحديث آليات التحقيق الرقمي بما يتماشى مع المستجدات التكنولوجية، كما إن وجود كوادر قانونية متخصصة داخل الوحدة، ودورها في تعزيز الوعي القانوني بجرائم الإنترنت، ساهم بشكل كبير في تعزيز فعاليتها في تطبيق القانون، مما أدى إلى ارتفاع مستوى الموافقة بين أفراد العينة بشأن دورها في هذا المجال.

النتائج المتعلقة بالسؤال الخامس: ما المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية؟

يتبين من الجدول رقم (3.6) ملحق (د) أن استجابات المبحوثين المتعلقة بالمجال الخامس: المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية كانت بدرجة مرتفعة، ويرى الباحث أن أعلى متوسط حسابي كان للمحور الرابع (التحديات الاجتماعية والثقافية) بنسبة مئوية (83.9%)، وأن اقل متوسط حسابي كان للمحور الاول (التحديات القانونية والتشريعية)، بنسبة مئوية (76.3%)، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية (79.9%) وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة على وجود معيقات وتحديات تواجه وحدة الجرائم الإلكترونية

في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية، وتتفق هذه الدراسة مع دراسة الشوابكة (2022) معوقات مكافحة الجرائم الإلكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص، المعوقات القانونية بالدرجة الأولى ومن ثم التحديات الفنية، ويعزو الباحث تلك النتيجة الى وجود مجموعة من المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية، والتي تؤثر على كفاءة عملها وتحد من قدرتها على التصدي لهذه الجرائم بالشكل الأمثل. ويعكس هذا المستوى المرتفع من الموافقة إدراك أفراد العينة للعقبات التي تواجه الوحدة، والتي قد تشمل نقص الموارد التقنية المتطورة، والحاجة إلى تحديث مستمر في الأدوات والبرمجيات المستخدمة لمواكبة التطورات السريعة في عالم الجريمة الإلكترونية، كما أن التحديات القانونية والإجرائية، مثل عدم وجود تشريعات متكاملة تواكب التطورات الرقمية، وصعوبة تنفيذ بعض القوانين بسبب الطبيعة العابرة للحدود لهذه الجرائم، قد تشكل عائقاً أمام فعالية الملاحقة القانونية.

النتائج المتعلقة بالسؤال السادس: هل هناك فروق في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى للمتغيرات (النوع الاجتماعي، المؤهل العلمي، سنوات الخدمة، الرتبة العسكرية)؟

للتحقق من صحة الفرضية، قام الباحث باستخدام اختبار "ت" لعينتين واختبار "تحليل التباين الأحادي ANOVA" لاختبار مدى وجود فروق ذات دلالة إحصائية بين متوسط استجابة المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية، فكانت النتائج على النحو التالي:

أولاً: الفروق وفقاً للنوع الاجتماعي:

يتضح من الجدول (3.7) ملحق (د) ما يلي:

أنَّ القيمة الاحتمالية لدور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تساوي (0.72)، وهي أكبر من مستوى الدلالة (0.05)؛ مما يدل على عدم وجود فروق ذات دلالة إحصائية عند

مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى إلى متغير (النوع الاجتماعي).

ثانياً: الفروق وفقاً المؤهل العلمي:

يتضح من الجدول (3.8) ملحق (د) ما يلي:

أنَّ القيمة الاحتمالية حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تساوي (0.730)، وهي أكبر من مستوى الدلالة (0.05)؛ مما يدل على عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى إلى متغير (المؤهل العلمي).

ثالثاً: الفروق وفقاً لسنوات الخدمة:

يتضح من الجدول (3.9) ملحق (د) ما يلي:

أنَّ القيمة الاحتمالية حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تساوي (0.263)، وهي أكبر من مستوى الدلالة (0.05)؛ مما يدل على عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى إلى متغير (سنوات الخدمة).

رابعاً: الفروق وفقاً الرتبة العسكرية:

يتضح من الجدول (3.10) ملحق (د) ما يلي:

أنَّ القيمة الاحتمالية حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تساوي (0.145)، وهي أكبر من مستوى الدلالة (0.05)؛ مما يدل على عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في

المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى إلى متغير (الرتبة العسكرية)، ويعزو الباحث هذه النتيجة الى أن الرتبة العسكرية لا تفسر الاختلاف في آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية. وبالتالي، قد يكون من الأفضل البحث عن متغيرات أخرى أكثر تأثيراً، مثل الخبرة في التعامل مع الجرائم الإلكترونية، التدريب، أو القسم الذي يعمل فيه الفرد داخل المؤسسة الأمنية.

الفصل الرابع

مناقشة النتائج والتوصيات

تناول الباحث من خلال هذا الفصل أسئلة الدراسة، عبر توضيح نتيجة كل سؤال ومناقشته وتوضيح الرأي الشخصي، وأخيراً تقديم التوصيات والمقترحات المستقبلية للدراسة:

4.1 مناقشة نتائج الدراسة

تفسير نتائج السؤال الأول ومناقشته: كيف تسهم وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بمخاطر الجرائم الإلكترونية؟

يتبين من النتائج أن استجابات المبحوثين حول إسهام وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بالجرائم الالكترونية كانت بدرجة مرتفع، فأعلى متوسط حسابي كان للفقرة الاولى (تقدم الوحدة برامج توعية دورية حول الجرائم الإلكترونية) بنسبة مئوية (82.6%)، وأن اقل متوسط حسابي كان للفقرة الرابعة (توفر الوحدة كتيبات إرشادية للجمهور حول كيفية حماية أنفسهم إلكترونياً.)، بنسبة مئوية (73.4%)، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية (78.3%) وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة على دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بالجرائم الالكترونية.

يعزو الباحث تلك النتيجة إلى مجموعة من العوامل التي تعكس فعالية وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في تعزيز الوعي المجتمعي حول الجرائم الإلكترونية، فمن خلال استعراض الفقرات المختلفة، يظهر أن وحدة الجرائم الإلكترونية تقدم برامج توعية دورية، وتستخدم وسائل الإعلام المتنوعة لنشر الوعي بخطورة هذه الجرائم، وهذا يشير إلى استراتيجية شاملة تهدف إلى تغطية جميع فئات المجتمع، بما في ذلك الفئات الأكثر عرضة للجرائم الإلكترونية، مثل الشباب والمستخدمين غير المتمرسين في التقنيات

الحديثة، وعليه فالباحث يرى أن فعالية الحملات التوعوية في المدارس والجامعات تعكس اهتمام الوحدة بالتوعية المبكرة، وهو أمر بالغ الأهمية في مجتمع يشهد تطوراً سريعاً في التكنولوجيا والإنترنت، إذ تساهم هذه الحملات في إكساب الطلاب المهارات اللازمة لحماية أنفسهم على الشبكة الإلكترونية في مرحلة مبكرة من حياتهم التعليمية، كما أن تنظيم ورش العمل التدريبية يعد جزءاً من هذه الاستراتيجية الفعالة، حيث توفر منصة لتعليم الجمهور كيفية التعامل مع الجرائم الإلكترونية وكيفية تجنبها.

علاوة على ذلك، يعتبر الباحث أن تقديم كتيبات إرشادية يمثل خطوة إضافية تسهم في نشر الوعي بطريقة أكثر تخصيصاً وسهولة في الوصول إليها، فالجمهور الذي قد لا يكون لديه القدرة على حضور ورش العمل أو المشاركة في الحملات يمكنه الاستفادة من هذه المواد التي تقدم معلومات مبسطة وموثوقة، وعلى الرغم من أن النتائج قد تشير إلى أن هناك جانباً من التفاوت في الردود حول بعض الأساليب المعتمدة، إلا أن النتيجة الكلية التي تم الوصول إليها تشير إلى أن وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية تقوم بجهود مستمرة ومتعددة الأوجه لتوعية المجتمع حول الجرائم الإلكترونية، ويعزو الباحث هذا الأداء الجيد إلى التنوع في الأدوات والوسائل التي تستخدمها الوحدة، مثل الإعلام والورش التدريبية والكتيبات، مما يعكس تخطيطاً استراتيجياً لزيادة الوعي وتحقيق التأثير المطلوب في المجتمع.

وتتفق النتيجة أعلاه مع عدد من الدراسات السابقة التي أكدت على فعالية التوعية في الحد من الجرائم الإلكترونية، فقد بيّنت دراسة نبيل (2024) ودراسة القحطاني (2024) أن الإعلام الأمني والرقمي يلعبان دوراً محورياً في تعزيز الوعي العام بمخاطر الجرائم الإلكترونية، كما أظهرت دراسة العنزي (2020) أن الإعلام الأمني يسهم في نشر ثقافة الوقاية، في المقابل، تختلف نتائج الدراسة الحالية عن نتائج دراسة النعامي (2023) التي كشفت عن ضعف أداء الجهات المسؤولة في اليمن في توعية الجمهور.

تفسير نتائج السؤال الثاني ومناقشتها: ما الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين؟

يتبين من النتائج أن استجابات المبحوثين المتعلقة بالمجال الثاني: الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين كانت بدرجة مرتفعة، فأعلى متوسط حسابي كان للفقرة الاولى (تعتمد الوحدة على تقنيات حديثة في تتبع الجرائم الإلكترونية) بنسبة مئوية (81.6%)، وأن اقل متوسط حسابي كان للفقرة السادسة (تستخدم الوحدة أنظمة مراقبة إلكترونية للكشف عن الجرائم قبل وقوعها)، بنسبة مئوية (74.3%)، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية (77.0%) وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة.

يعزو الباحث النتيجة التي تم الوصول إليها إلى الأساليب المتقدمة والتقنيات الحديثة التي تعتمد عليها وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية لمكافحة الجرائم الإلكترونية، فمن خلال استعراض الأساليب المتبعة، يظهر أن الوحدة تعتمد بشكل كبير على تقنيات متطورة في تتبع الجرائم الإلكترونية، وهو ما يعكس قدرتها على استخدام الأدوات التكنولوجية الحديثة في مواجهة التحديات الرقمية، وهذا يشير إلى أن الوحدة تدرك أهمية مواكبة التطور السريع في التقنيات التي يستخدمها المجرمون الإلكترونيون، مما يمكنها من التعرف على الجرائم في مراحل مبكرة.

ويرى الباحث أن استخدام البرامج المتقدمة لتحليل البيانات الرقمية هو جزء أساسي من استراتيجيات المكافحة، فهذه البرامج تساعد الوحدة في فحص كميات ضخمة من البيانات بشكل فعال ودقيق، مما يسمح لها بالكشف عن الأنماط أو السلوكيات المشبوهة بسرعة، وبذلك، تسهم هذه البرامج في تحسين كفاءة العمل الأمني وتقليل الوقت اللازم للكشف عن الجرائم الإلكترونية، وبالتالي يعكس التعاون الذي تقيمه الوحدة مع شركات التكنولوجيا اهتمامها بتطوير أدوات مكافحة الجرائم الإلكترونية بشكل مستمر، فهذا التعاون يسهم في تعزيز قدرة الوحدة على التعامل مع التقنيات المتطورة التي تطرأ في المجال الرقمي، ما يتيح لها تحديث أساليب المكافحة بما يتناسب مع أحدث الابتكارات التكنولوجية.

علاوة على ذلك، الأساليب المتطورة للتحقيق الرقمي التي تطبقها الوحدة، حيث تُستخدم أساليب دقيقة ومبتكرة في جمع الأدلة وتحليلها، فهذه الأساليب تمكن الوحدة من تقديم نتائج موثوقة في التحقيقات الرقمية، مما يعزز مصداقية العمليات الأمنية ويزيد من فعاليتها، وكذلك فإن تطبيق آليات حديثة لاسترجاع البيانات المسروقة يمثل خطوة هامة في استعادة المعلومات المفقودة أو المسروقة نتيجة الجرائم الإلكترونية، فهذه الآليات تُعد من الأدوات الأساسية التي تساهم في تقليص الأضرار الناجمة عن هذه الجرائم.

إضافة إلى ذلك، يعتبر الباحث أن استخدام أنظمة المراقبة الإلكترونية للكشف عن الجرائم قبل وقوعها من أبرز الأساليب الوقائية التي تعتمد عليها الوحدة، فهذه الأنظمة تتيح مراقبة الشبكة الإلكترونية في الوقت الحقيقي، مما يساهم في الحد من الجرائم قبل أن تحدث ويزيد من مستوى الأمان الرقمي، وأخيراً، يعد توفير خط ساخن للإبلاغ عن الجرائم الإلكترونية من ضمن الأساليب الهامة التي تسهم في رفع مستوى التفاعل بين الجمهور ووحدة الجرائم الإلكترونية، فهذا الخط يوفر وسيلة مباشرة وسريعة للأفراد للإبلاغ عن أي نشاط مشبوه، مما يعزز من دور المجتمع في مكافحة الجرائم الإلكترونية.

تتفق نتائج الدراسة مع العديد من الدراسات السابقة التي أكدت أهمية استخدام الوسائل التقنية والأمن السيبراني لمواجهة هذه الجرائم، مثل دراسة العنوز (2024) التي شددت على دور الأمن السيبراني ونظم المعلومات في دعم متخذي القرار، ودراسة العسقلاني (2022) التي أشارت إلى فاعلية التعاون والتشريعات في التصدي للجرائم الإلكترونية.

تفسير نتائج السؤال الثالث ومناقشتها: إلى أي مدى يتجسد التعاون الدولي في مواجهة الجرائم الإلكترونية، وما أبرز آلياته؟

يتبين من النتائج أن استجابات المبحوثين المتعلقة بالمجال الثالث: آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية كانت بدرجة مرتفعة، ويرى الباحث أن أعلى متوسط حسابي كان للفقرة الاولى (تشارك الوحدة في مؤتمرات دولية متعلقة بمكافحة الجرائم الإلكترونية) بنسبة مئوية (83%)، وأن اقل متوسط حسابي

كان للفقرة الرابعة (تعتمد الوحدة على اتفاقيات دولية لتسليم المجرمين الإلكترونيين)، بنسبة مئوية (74.3%)، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية (79.1%) وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة على آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية.

يعزو الباحث النتيجة التي تم الوصول إليها في هذا المجال إلى الدور الفاعل والمستمر الذي تلعبه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية ضمن الإطار الدولي في مكافحة الجرائم الإلكترونية، فمن خلال الاستعراض المتكامل للأساليب المتبعة في التعاون الدولي، يرى الباحث أن الوحدة تشارك بفعالية في مؤتمرات دولية مخصصة لمناقشة التحديات المتعلقة بالجرائم الإلكترونية، وهذه المشاركة تؤكد على اهتمام الوحدة بتبادل المعرفة والخبرات مع مختلف الجهات الدولية المعنية، مما يساهم في تعزيز قدراتها على مواجهة التهديدات الرقمية التي أصبحت عابرة للحدود.

بالإضافة إلى ذلك فإن التعاون مع المنظمات الدولية يعد من أوجه التعاون الهامة التي تعزز من فاعلية مكافحة الجرائم الإلكترونية على مستوى عالمي، وهذا التعاون لا يقتصر على تبادل المعلومات فقط، بل يشمل أيضاً التنسيق المباشر مع وحدات الجرائم الإلكترونية في دول أخرى، وهذا التنسيق يسمح للوحدة بتبادل أفضل الممارسات والتقنيات الحديثة في مواجهة الجرائم الإلكترونية، ما يعزز من قدرتها على التعامل مع هذا النوع من الجرائم بفعالية أكبر، ومن هنا تعكس نتيجة التعاون الدولي في تبادل المعلومات بين الوحدات الأمنية في دول مختلفة خطوة هامة نحو التنسيق المشترك لمكافحة الجريمة الإلكترونية، ففي عالم مترابط ومتسارع، يعد هذا النوع من التعاون أمراً بالغ الأهمية في كشف الجرائم قبل أن تنتشر أو تتفاقم، فالمعلومات المشتركة بين البلدان تساهم في بناء قاعدة بيانات واسعة تتيح للدول تبادل المعرفة حول الأساليب التي يستخدمها المجرمون الإلكترونيون وطرق مكافحتها.

وأحد الجوانب الأخرى التي يعزو الباحث لها هذه النتيجة هو الاعتماد على الاتفاقيات الدولية التي تسهم في تسليم المجرمين الإلكترونيين، وهذا النوع من الاتفاقيات يعكس التزام الوحدة بالممارسات الدولية التي تضمن

العدالة والملاحقة القضائية للمجرمين الذين يتنقلون عبر الحدود، فالتحديات التي تطرحها الجرائم الإلكترونية لا يمكن معالجتها على المستوى المحلي فقط، لذا فإن التعاون الدولي في هذا المجال يعد أساسياً لضمان محاكمة المجرمين وتقديمهم للعدالة.

بالإضافة إلى ذلك، يبرز دور الاستفادة من الخبرات الدولية في تعزيز قدرات الوحدة في مكافحة الجرائم الإلكترونية، فمن خلال التعاون مع الدول التي تمتلك خبرات واسعة في هذا المجال، يمكن للوحدة التعلم من التجارب المختلفة، وتطوير أساليب وتقنيات تتناسب مع الواقع المحلي، وهذا التعاون يُمكّن الوحدة من تنفيذ استراتيجيات أمنية أكثر فعالية، ويعزز من قدرتها على التصدي للأشكال المتطورة والمتغيرة من الجرائم الإلكترونية.

ويضيف الباحث أيضا حرص الوحدة على تطوير شراكات دولية في هذا المجال، فالشراكات تعتبر محورية في تطوير استراتيجيات شاملة لمكافحة الجرائم الإلكترونية، مما يسمح بتبادل الموارد، الدعم الفني، والتكنولوجيا الحديثة التي تساهم في تعزيز فعالية الإجراءات الأمنية المتبعة، وفيما يتعلق بالتشريعات الدولية، فإن متابعة التشريعات الخاصة بالجرائم الإلكترونية تساهم في الحفاظ على توازن قانوني بين الدول في محاربة هذه الجرائم، فمن خلال الالتزام بالقوانين والمعاهدات الدولية، تضمن الوحدة توافق جهودها مع المعايير القانونية العالمية، مما يعزز التنسيق بين الدول المختلفة في محاربة الجرائم الإلكترونية.

بناءً على ذلك، يرى الباحث أن التعاون الدولي هو ركيزة أساسية في تعزيز قدرة وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية على مواجهة التحديات التي تطرأ في مجال مكافحة الجرائم الإلكترونية، وهذه النتيجة توضح أن الوحدة لا تعمل في عزلة، بل هي جزء من شبكة دولية متكاملة تهدف إلى تحقيق الأمان الرقمي وحماية الأفراد من المخاطر الإلكترونية على مستوى العالم.

تفسير نتائج السؤال الرابع ومناقشتها: في أي إطار تقوم وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية؟

يتبين من النتائج أن استجابات المبحوثين المتعلقة بالمجال الرابع: قيام وحدة الجرائم الإلكترونية في تطبيق الملاحقة القانونية ومتابعة مرتكبي الجرائم الإلكترونية وفقاً للتشريعات المحلية والدولية كانت بدرجة مرتفعة، ويرى الباحث أن أعلى متوسط حسابي كان للفقرة الثالثة (تساعد الوحدة في صياغة تقارير فنية حول الجرائم الإلكترونية) بنسبة مئوية (86.4%)، وأن اقل متوسط حسابي كان للفقرة الخامسة (توفر الوحدة خبراء قانونيين متخصصين في الجرائم الإلكترونية)، بنسبة مئوية (81.1%)، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية (84.3%) وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة على دور وحدة الجرائم الإلكترونية في تطبيق الملاحقة القانونية ومتابعة مرتكبي الجرائم الإلكترونية وفقاً للتشريعات المحلية والدولية.

يعزو الباحث هذه النتيجة إلى الدور الحيوي والمهم الذي تلعبه وحدة الجرائم الإلكترونية في تطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، فمن خلال استعراض النتائج، يرى الباحث أن الوحدة تتابع القضايا الإلكترونية بشكل دقيق وبالتنسيق المستمر مع الجهات القضائية، مما يعكس التزامها الكبير بضمان تطبيق العدالة، وهذه المتابعة المستمرة تساهم في تحقيق تنسيق فعّال بين جميع الأطراف المعنية، مثل الشرطة والنيابة العامة، مما يعزز سرعة الإجراءات القانونية ويضمن عدم تفويت أي أدلة أو معلومات مهمة قد تكون أساسية في القضايا المطروحة.

ويضيف الباحث هنا أن قدرة الوحدة على تقديم أدلة رقمية موثوقة للمحاكم تساهم بشكل كبير في إرساء العدالة في القضايا المتعلقة بالجرائم الإلكترونية، في ظل الطابع الرقمي المتزايد للجرائم، تصبح الأدلة الرقمية أحد الركائز الأساسية لإثبات التهم في المحاكم، وبذلك، تؤكد الوحدة على أهمية دقة وجدية التعامل مع هذه الأدلة وتقديمها بأعلى مستوى من المصداقية، مما يساهم في تعزيز الثقة في النظام القضائي ويزيد من فعالية ملاحقة الجرائم الإلكترونية.

من ناحية أخرى، يرى الباحث أن مساعدة الوحدة في صياغة تقارير فنية حول الجرائم الإلكترونية تُمثل خطوة مهمة في تزويد القضاة والمحاكم بمعلومات فنية دقيقة تساهم في فهم طبيعة الجرائم الإلكترونية بشكل

أفضل، فالتقارير الفنية المدعومة بالتحليل الدقيق للأدلة الرقمية تساهم في تسريع الإجراءات القضائية، حيث تُعتبر هذه التقارير بمثابة مرجع أساسي في اتخاذ القرارات القانونية، وهذا يدل على الدور البارز الذي تلعبه الوحدة في دعم سير القضايا القانونية المتعلقة بالجرائم الإلكترونية.

ويشير الباحث هنا إلى أهمية التنسيق الذي تقوم به الوحدة مع النيابة العامة في ملاحقة المتهمين بالجرائم الإلكترونية لتعزيز فعالية النظام القانوني، فمن خلال التنسيق الوثيق مع النيابة العامة، يتم اتخاذ الإجراءات القانونية المناسبة في الوقت المناسب، مما يساهم في سرعة التحقيقات والمحاكمات، وهذا التنسيق بين الجهات المختلفة يعكس التوجه التكاملي الذي تعتمد عليه وحدة الجرائم الإلكترونية في عملها لتحقيق أقصى قدر من الفاعلية في الملاحقة القانونية للمتهمين.

بالإضافة إلى ذلك، يرى الباحث أن توفير الوحدة لخبراء قانونيين متخصصين في الجرائم الإلكترونية يمثل عاملاً هاماً في تعزيز تطبيق الملاحقة القانونية بشكل سليم، فالخبراء القانونيون المتخصصون في هذا المجال يوفرون الإرشادات القانونية الضرورية التي تساعد على توجيه القضايا بشكل صحيح، كما أنهم يسهمون في إعداد وتقديم المشورة القانونية للجهات المعنية بمكافحة الجرائم الإلكترونية، ويعتبر الباحث أيضاً أن الدعم الذي تقدمه الوحدة للضحايا في تقديم شكاوى قانونية يعكس التزاماً بمساعدة الأفراد المتضررين من الجرائم الإلكترونية، فهذا الدعم يعزز من قدرة الضحايا على متابعة حقوقهم القانونية ويشجع على تقديم البلاغات القانونية التي يمكن أن تساهم في اكتشاف الجرائم والمجرمين، ومن خلال هذا الدور، تسهم الوحدة في توفير بيئة قانونية آمنة للمواطنين تشجعهم على اتخاذ الخطوات القانونية ضد الجرائم التي يتعرضون لها.

تفسير نتائج السؤال الخامس ومناقشتها: ما المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية؟

يتبين من النتائج أن استجابات المبحوثين المتعلقة بالمجال الخامس: المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية كانت بدرجة مرتفعة، ويرى

الباحث أن أعلى متوسط حسابي كان للمحور الرابع (التحديات الاجتماعية والثقافية) بنسبة مئوية (83.9%)، وأن اقل متوسط حسابي كان للمحور الاول (التحديات القانونية والتشريعية)، بنسبة مئوية (76.3%)، وبشكل عام فإن المجال الاول ككل جاء بنسبة مئوية (79.9%) وهذا يعني أن افراد عينة الدراسة يوافقون بدرجة مرتفعة على وجود معيقات وتحديات تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية.

يعزو الباحث النتيجة إلى مجموعة من التحديات المتنوعة التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية أثناء محاربتها للجرائم الإلكترونية، إذ يرى الباحث أن هذه التحديات لا تقتصر فقط على جانب واحد، بل هي متعددة الأبعاد وتشمل مجالات قانونية، تكنولوجية، اجتماعية، أمنية، وغيرها من الأبعاد التي تساهم في تعقيد مهمة الوحدة في مكافحة الجرائم الإلكترونية، فمن خلال استعراض التحديات القانونية والتشريعية، يرى الباحث أن الإطار القانوني المحلي قد لا يكون دائماً قادراً على مواكبة التطورات السريعة في مجال التكنولوجيا والجرائم الرقمية، وبالنظر إلى الطبيعة المتطورة والمتجددة للجرائم الإلكترونية، فإن التحديات التي تواجه الوحدة تكمن في ضرورة تعديل وتحديث القوانين المحلية بشكل مستمر لتلائم الأشكال الحديثة لهذه الجرائم، وعدم توافق بعض التشريعات مع المستجدات التكنولوجية قد يُعيق عمل الوحدة ويُصعب عملية الملاحقة القانونية، مما يجعل من الضروري إصلاح التشريعات لتتناسب مع التحديات العالمية في هذا المجال.

ويُلاحظ الباحث أن التحديات التكنولوجية والفنية تشكل أيضاً عبئاً على وحدة الجرائم الإلكترونية، وذلك بسبب تزايد تعقيد التكنولوجيا التي يستخدمها المجرمون الإلكترونيون، فالتقدم السريع في البرمجيات والأدوات التقنية التي يستخدمها الجناة يجعل من الصعب على الوحدة مواكبة هذه التقنيات، ما يتطلب باستمرار تحديث المهارات والموارد الفنية التي تعتمد عليها الوحدة في عمليات التحقيق والبحث، ومن جهة أخرى، تزداد الحاجة إلى تقنيات متطورة تُمكن الوحدة من تتبع الجرائم الإلكترونية والتصدي لها قبل أن تتفاقم.

إلى جانب ذلك، يعزو الباحث التحديات المالية واللوجستية إلى نقص الموارد المالية المخصصة لوحدة الجرائم الإلكترونية، مما يؤثر سلباً على قدرتها على توفير الأجهزة والتقنيات الحديثة اللازمة لمكافحة الجرائم الإلكترونية، فهذه التحديات تتجسد أيضاً في صعوبة تأمين التدريب المستمر للعاملين في الوحدة، مما يؤثر على مستوى كفاءتهم وقدرتهم على التعامل مع أحدث أساليب الجرائم الإلكترونية، والباحث يلفت أيضاً إلى التحديات الاجتماعية والثقافية باعتبارها من العوامل المؤثرة في عمل الوحدة، ففي بعض الأحيان، يعوق التوجه الاجتماعي أو الثقافي في المجتمع الفلسطيني من التفاعل الإيجابي مع الأنشطة التوعوية التي تقوم بها الوحدة، وقد تكون هناك مقاومة من بعض الفئات أو نقص في الوعي الكافي حول المخاطر التي تنجم عن الجرائم الإلكترونية، ما يؤدي إلى قلة التعاون من المواطنين أو التقليل من أهمية موضوع الجرائم الإلكترونية، وبالتالي يؤثر ذلك على فعالية الإجراءات الوقائية التي تقوم بها الوحدة.

من جانب آخر، يرى الباحث أن التحديات الأمنية والسياسية تلعب دوراً مهماً في تعقيد مهام الوحدة، فالتوترات الأمنية والسياسية في المنطقة قد تؤثر على عمليات التنسيق والتعاون مع جهات محلية ودولية، مما يعرقل تبادل المعلومات أو التعاون الفعال في التحقيقات المتعلقة بالجرائم الإلكترونية، وهذه التحديات تؤدي إلى زيادة تعقيد مساعي الوحدة في تأمين بيئة آمنة ومستقرة لتنفيذ مهامها بكفاءة.

أخيراً، يعزو الباحث التحديات المتعلقة بالتعاون والتنسيق إلى الصعوبات التي قد تواجهها الوحدة في التنسيق مع مختلف الجهات الأمنية المحلية والدولية، وقد تكون هناك صعوبة في تنسيق الجهود بين الجهات المختلفة، سواء في القطاع العام أو مع المنظمات الدولية، بسبب الاختلافات في الاستراتيجيات أو نقص في الفهم المشترك حول طبيعة الجرائم الإلكترونية وسبل مكافحتها، وهذا النقص في التنسيق يمكن أن يحد من فعالية الاستجابة السريعة والتعامل مع الجرائم التي تحدث عبر الحدود.

تفسير نتائج السؤال السادس ومناقشتها: هل هناك فروق في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى للمتغيرات (النوع الاجتماعي، المؤهل العلمي، سنوات الخدمة، الرتبة العسكرية)؟

تشير النتائج إلى عدم وجود فروق في استجابات المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى للمتغيرات (النوع الاجتماعي، المؤهل العلمي، سنوات الخدمة، الرتبة العسكرية).

يعزو الباحث هذه النتيجة إلى أن وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية تعتمد على مجموعة من العوامل المهنية والعملية المشتركة بين جميع موظفيها بغض النظر عن المتغيرات الشخصية مثل النوع الاجتماعي، المؤهل العلمي، سنوات الخدمة، أو الرتبة العسكرية، فمن خلال النتائج، يرى الباحث أن جميع أفراد الوحدة يتشاركون في نفس الوعي والهدف في مكافحة الجرائم الإلكترونية، وأن هذا الهدف المهني يتجاوز الفروقات الشخصية أو الخلفيات الفردية، وهذا الأمر يشير إلى أن التدريب والتوجيه الذي يحصل عليه الموظفون في الوحدة له تأثير أكبر من المؤهلات الفردية أو الخبرات السابقة في تحديد كيفية التعامل مع الجرائم الإلكترونية، فمن خلال التوجهات المعتمدة على المعرفة والتدريب المستمر ، أصبح الجميع في الوحدة يتعامل مع المهام الموكلة إليهم بناءً على الكفاءة المهنية والمهارات المتخصصة وليس على أسس أخرى قد تتعلق بالمؤهلات التعليمية أو الرتبة العسكرية.

ويضيف الباحث هنا بانه من الممكن أن يكون هناك أيضاً تأثير لثقافة الوحدة وأسلوب القيادة في المؤسسة الأمنية الفلسطينية، حيث تركز على ضمان أن جميع الموظفين يتعاملون مع المهام بشكل موحد ويأخذون نفس المسؤولية في مكافحة الجرائم الإلكترونية، وهذه الوحدة في الرؤية والتوجه تؤدي إلى تقليص الفروقات الفردية، مما يعكس التماسك الداخلي والروح الجماعية في العمل داخل الوحدة.

وعليه فإن طبيعة عمل وحدة الجرائم الإلكترونية تقتضي التركيز على المهارات التقنية والمعرفية التي يمتلكها الموظفون في التعامل مع الجرائم الإلكترونية، وهو ما لا يتأثر بشكل كبير بالمتغيرات الشخصية مثل النوع الاجتماعي أو سنوات الخدمة، فالتقنيات الحديثة وأساليب التحقيق الرقمي تحتاج إلى تخصص وتقنيات معينة، وبالتالي فإن العامل الأساسي في هذه الوحدة هو الكفاءة الفنية والقدرة على التعامل مع التحديات الرقمية التي قد يواجهها أي موظف بغض النظر عن خلفيته الشخصية.

وبالإضافة إلى ذلك، يعزو الباحث النتيجة إلى أن المؤسسة الأمنية الفلسطينية قد تكون قد عملت على تقليص الفجوات الموجودة بين موظفيها عبر استراتيجيات تدريبية متقدمة، مما يساهم في تعزيز التساوي في الفرص والمهارات بين الموظفين، وهذه الاستراتيجيات تساعد في جعل جميع العاملين في وحدة الجرائم الإلكترونية يمتلكون نفس القدرة على أداء مهامهم بشكل فعال، بما يضمن عدم وجود تأثيرات تمييزية بسبب المتغيرات التي تم ذكرها.

4.2 استنتاجات الدراسة

بعد قيام الباحث بتحليل بيانات الدراسة الميدانية، واختبار فرضياتها، قامتت باستخلاص النتائج التي جاءت كما يأتي:

1. هناك درجة موافقة مرتفعة على دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بالجرائم الالكترونية بوزن نسبي 78.3%.
2. هناك درجة موافقة مرتفعة على توفر الأساليب المستخدمة من قبل وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية لمكافحة الجرائم الإلكترونية بوزن نسبي 81.6%.
3. هناك درجة موافقة مرتفعة على وجود آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية بوزن نسبي 79.1%.

4. هناك درجة موافقة مرتفعة على دور وحدة الجرائم الإلكترونية في تطبيق الملاحقة القانونية ومتابعة مرتكبي الجرائم الإلكترونية وفقاً للتشريعات المحلية والدولية بوزن نسبي 84.3%.

5. هناك درجة موافقة مرتفعة على وجود معيقات وتحديات تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية بوزن نسبي 79.9%.

6. عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى إلى متغير (النوع الاجتماعي).

7. عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى إلى متغير (المؤهل العلمي).

8. عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى إلى متغير (سنوات الخدمة).

9. عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية تعزى إلى متغير (الرتبة العسكرية).

4.3 التوصيات:

بناء على نتائج الدراسة يوصي الباحث بما يلي:

1. على وحدة الجرائم الإلكترونية تنظيم ورش عمل تفاعلية تستهدف قطاعات معينة من المجتمع مثل المدارس والجامعات، بالإضافة إلى التعاون مع وسائل الإعلام المحلية لتوسيع نطاق التوعية.
2. ضرورة قيام وحدة الجرائم الإلكترونية بتطوير محتوى مرئي تفاعلي حول كيفية حماية الأفراد لأنفسهم عبر الإنترنت وتوزيعه عبر منصات مثل فيسبوك، إنستغرام، ويوتيوب.
3. يوصي الباحث بضرورة الاستثمار في التكنولوجيا الحديثة بشكل أكبر، مثل استخدام الذكاء الاصطناعي والتحليل المتقدم للبيانات لمكافحة الجرائم الإلكترونية، من خلال التعاون مع شركات البرمجيات العالمية لتطوير برامج وتقنيات متقدمة لمكافحة الجرائم الإلكترونية.
4. ضرورة الموازنة ما بين مكافحة الجريمة الإلكترونية والحفاظ على حقوق الإنسان وعدم التعدي على الخصوصيات التي كفلها القانون.
5. يوصي الباحث بتوسيع وتحسين آليات المراقبة الإلكترونية لضمان الكشف المبكر والفعال عن الجرائم الإلكترونية، عبر تطوير أنظمة مراقبة تعتمد على الذكاء الاصطناعي التي تتفاعل مع الأنماط غير الطبيعية في الإنترنت بشكل أسرع وأكثر دقة.
6. يوصي الباحث بتوسيع وتعزيز التعاون مع المنظمات الدولية لمكافحة الجرائم الإلكترونية، عبر تنظيم دورات تدريبية مشتركة مع نظرائها في الدول الأخرى وتبادل الخبرات والتقنيات الحديثة.
7. يوصي الباحث بتطوير الاتفاقيات الدولية لتشمل أطر قانونية أكثر شمولية تتماشى مع التطورات السريعة في التكنولوجيا من خلال التعاون مع الجهات التشريعية لتوسيع نطاق الاتفاقيات الدولية لتشمل الجرائم الإلكترونية العابرة للحدود.

8. يوصي الباحث بتدريب الخبراء القانونيين على القوانين الدولية المتجددة، فضلاً عن تقوية التعاون مع الجهات القضائية لتعزيز القدرة على تطبيق الملاحقة القانونية بشكل أكثر فعالية، من خلال تنظيم ورش تدريبية قانونية مستمرة لتحسين مهارات الخبراء القانونيين في مواجهة القضايا الجديدة.

9. يوصي الباحث بتطوير حلول للتحديات التكنولوجية مثل توفير أدوات وتقنيات متقدمة لتحليل البيانات الرقمية والحد من الصعوبات التقنية، من خلال تخصيص ميزانية لتحسين البنية التحتية التكنولوجية وتوفير التدريب المستمر للموظفين في استخدام هذه التقنيات المتطورة.

10. يوصى بالانضمام إلى "اتفاقية بودابست بشأن الجريمة الإلكترونية" وتطبيق أحكامها لما تقدّمه من إطار قانوني متكامل لتعزيز قدرات وحدة الجرائم الإلكترونية في كشف الجرائم وملاحقتها، مع التحفظ صراحةً على أي بنود تتعارض مع خصوصية الأسرة وعاداتنا وتقاليدنا، مع العمل على تضمين هذه التحفظات بوضوح عند التصديق وصدورها في التشريعات الوطنية[1].

[1] اتفاقية بودابست بشأن الجريمة الإلكترونية، المعتمدة في 23 نوفمبر 2001.

الدراسات المستقبلية:

يقترح الباحث بعض الدراسات المستقبلية للطلبة والدارسين على النحو التالي:

1. مدى فعالية البرامج التوعوية التي تقدمها وحدة الجرائم الإلكترونية في المجتمع الفلسطيني.
2. دراسة مقارنة حول تقنيات مكافحة الجرائم الإلكترونية في الدول المتقدمة والدول النامية.
3. دراسة حول تأثير التعاون الدولي على مكافحة الجرائم الإلكترونية في فلسطين.
4. تحليل التحديات القانونية والتشريعية في مكافحة الجرائم الإلكترونية في فلسطين.
5. دراسة حول آثار التحديات الثقافية والاجتماعية على نشر الوعي بالجرائم الإلكترونية في المجتمع الفلسطيني.
6. دراسة حول استخدام الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية في فلسطين.

المصادر العلمية

المراجع العربية:

إبراهيم، خالد. (2023). *فن التحقيق الجنائي في الجرائم الإلكترونية: دراسة مقارنة*، دار الفكر الجامعي، الاسكندرية.

أبو القاسم، سالم. (2024). دور وسائل الضبط الاجتماعي في الحد من الجرائم الالكترونية (المستحدثة). *مجلة القلعة*، (23)، 142-155.

اتفاقية الرياض العربية للتعاون القضائي لسنة 1983.

اتفاقية بودابست بشأن الجريمة الإلكترونية، المعتمدة في 23 نوفمبر 2001 .

البروتوكول الإضافي الأول. (2003). *البروتوكول الإضافي للاتفاقية بشأن الجريمة الإلكترونية والمتعلق بتجريم أعمال ذات طبيعة عنصرية أو كارهة للأجانب تُرتكب من خلال أنظمة الحواسيب.*

البروتوكول الإضافي الثاني. (2022). *بشأن تعزيز التعاون وتبادل المعلومات الإلكترونية بين الدول والأطراف الخاصة.*

بن سويد، تهاني محمد (2024). حماية الأطفال من الجرائم الإلكترونية مسؤولية مجتمعية. *مجلة مستقبل العلوم الاجتماعية*، 18(3)، 195-210.

الجرجاوي، زياد بن علي. (2010). *القواعد المنهجية التربوية لبناء الاستبيان*. سلسلة أدوات البحث العلمي، مطبعة أبناء الجراح. فلسطين.

جندل، جاسم. (2022). *الجرائم الإلكترونية*، دار المعتز للنشر والتوزيع، الأردن.

الحناحنة، سيف. (2023). دراسة العوامل المؤثرة في ارتكاب الجرائم الإلكترونية في الأردن: دراسة نوعية، (رسالة ماجستير غير منشورة)، جامعة مؤتة، الأردن.

الدويري، فراس. (2023). دور خصائص البيانات الضخمة في الحد من الجرائم الإلكترونية من خلال استراتيجية الأمن السيبراني في جهاز الأمن العام الأردني، (رسالة ماجستير غير منشورة)، جامعة مؤتة، الأردن.

ربيع، هادي. (2007). *طرق البحث التربوي*، مكتبة المجتمع العربي، عمّان.

رجب. عيد. (2023). الجرائم الإلكترونية ووعى الشباب بانتهاكها لخصوصية الفرد. *حوليات أداب عين شمس*، 51(6)، 299-332.

الرواشدة. مصطفى. (2024). القواعد الإجرائية للملاحقة والمحاكمة في الجرائم الإلكترونية، *مجلة الفنون والادب وعلوم الانسانيات*، ع99، 418-431.

الشوابكة، عدي. (2022). معوقات مكافحة الجرائم الإلكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص، *المجلة العربية للنشر العلمي*، ع43، 331-356.

صالحي, محمود. (2024). سبل وآليات مكافحة الجريمة الإلكترونية في المجتمع العربي. *المجلة العلمية للتكنولوجيا وعلوم الإعاقة*، 6(2)، 119-139.

عبد الباقي، مصطفى. (2018). التحقيق في الجريمة الالكترونية واثباتها في فلسطين: دراسة مقارنة. *دراسات علوم الشريعة والقانون*، 45(4)، 284-299 .

عبيد، ذوقان، وعدس، عبد الرحمن، وعبد الحق، كايد. (2001). *البحث العلمي مفهومه وأدواته وأساليبه*، المكتبة الوطنية، مصر.

العجمي، عبد الله. (2014). المشكلات العملية والقانونية للجرائم الالكترونية: دراسة مقارنة، (رسالة ماجستير غير منشورة)، جامعة الشرق الأوسط، الأردن.

العسقلاني، أيمن. (2022). دور مجلس التعاون الخليجي القانوني والتعاوني في مكافحة الجرائم الإلكترونية، *مجلة الدراسات الدولية*، ع32، 107-155.

علي، يارا. (2024). دور المواقع الإخبارية في مكافحة الجرائم الإلكترونية وعلاقته باتجاهات الجمهور نحوها (دراسة تطبيقية)، *مجلة كلية الآداب. جامعة الإسكندرية*، 74(116)، 1-37.

العنزي، باسل. (2020). دور الإعلام الأمني في مواجهة الجرائم الإلكترونية والحد منها من وجهة نظر العاملين في الأجهزة الأمنية في دولة الكويت، *مجلة التربية*، 39(186)، 41-84.

العنوز، سوزان. (2024). دور الأمن السيبراني في التقليل من أعداد الجرائم الإلكترونية في محافظة العقبة" باستخدام نظم المعلومات الجغرافية". *مجلة العلوم الإنسانية و الاجتماعية*، 8(8)، 14-29.

فتح الله، محمود. (2021). *مسرح الجريمة الإلكترونية: دراسة تطبيقية مقارنة*، دار الجامعة الجديدة، مصر.

فهمي، ياسر سيد. (2025). الركن المادي في الجرائم الإلكترونية، المجلة القانونية، 23(2)، 905-966.

قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

القانون الأساسي المعدل لسنة 2003م.

القحطاني، اللولو. (2024). دور الإعلام الرقمي السعودي في توعية المواطنين بتقنيات الجرائم الإلكترونية في المملكة العربية السعودية، *مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع*، (104)، 283–327.

قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته.

محمد، سيد. (2021). *الجرائم الإلكترونية: ماهيتها، صورها، إثباتها، مكافحتها*، دار التعليم الجامعي، الإسكندرية.

المناعسة، أسامة (2014). *جرائم تقنية نظم المعلومات*، مكتبة دار الثقافة للنشر والتوزيع، الأردن.

نبيل، مخفي. (2024) دور الإعلام الأمني في التوعية بمخاطر الجرائم الإلكترونية في القنوات الجزائرية، (رسالة ماجستير غير منشورة)، جامعة الجزائر، الجزائر.

النعامي، فهمي. (2023). دور الجهات المسئولة عن الجريمة الإلكترونية في اليمن في توعية الجمهور بمخاطر الجريمة الإلكترونية. *مجلة جامعة صنعاء للعلوم الإنسانية*، 3(1)، 361–396.

المراجع الاجنبية:

Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology, 16*(2), 216-227.

Fansher, A. K., & Randa, R. (2019). Risky social media behaviors and the potential for victimization: A descriptive look at college students victimized by someone met online. *Violence and gender, 6*(2), 115-123.

Imran, M. F. (2023). Preventing and Combating Cybercrime in Indonesia. *International Journal of Cyber Criminology, 17*(1), 223-235.

Massawe, E. R., & Mshana, J. A. (2023). Preventing and Combating Cybercrimes: Case of Cybercrimes Investigation Unit of Tanzania Police. , 1(5), 1179-1190. *European Journal of Theoretical and Applied Sciences, 1*(5), 1179-1190.

Mijwil, M., & Aljanabi, M. (2023). Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime. *Iraqi Journal For Computer Science and Mathematics, 4*(1), 65-70.

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science, 11*(4), 384-396.

Neethu, N. (2020). *Role of International Organizations in Prevention of Cyber-Crimes: An Analysis.* Hyderabad: Nalsar University of Law.

Paek, S. Y., Nalla, M. K., Chun, Y. T., & Lee, J. (2021). The perceived importance of cybercrime control among police officers: Implications for combatting industrial espionage . *Sustainability, 13*(8), 4351.

Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics, 18*, 751-762.

Widodo, M., Adam, S., Hsb, P. H., Prayitno, A. H., & Bhaskoro, A. (2024). International Legal Dynamics in Combating Cybercrime: Challenges and Opportunities for Developing Countries. *Global International Journal of Innovative Research, 2*(1), 314-321.

الملاحق

ملحق (أ)

قائمة بأسماء المحكمين

الرقم	اسم الدكتور	التخصص	الرتبة العلمية	الجامعة
1	محمد تلالوة	المالية والمحاسبة التنظيمية	استاذ مشارك	جامعة القدس المفتوحة
2	عبد الحميد شعبان	اقتصاد	استاذ مساعد	جامعة القدس المفتوحة
3	مرسي عبد الرازق	القانون العام	استاذ مساعد	الكلية العصرية الجامعية
4	ميرفت حبايبة	القانون العام		

ملحق (ب)

الاستبانة بصورتها الأولية (قبل التعديل)

جامعه النجاح الوطنية

كلية الدراسات العليا

الأخوة والأخوات

تحية طيبة وبعد,

تعد هذه الإستبانة جزء من رسالة الماجستير التي يقوم بها الباحث بعنوان" **دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية** " وذلك استكمالا لمتطلبات الحصول على درجة الماجستير في برنامج القانون العام بكلية الدراسات العليا في جامعة النجاح الوطنية.

يرجى من حضرتكم الإجابة على أسئلة هذه الإستبانة لما لها من أهمية لإنجاز هذه الرسالة, علماً بأن البيانات التي ستقدمونها سوف تستخدم فقط لأغراض البحث العلمي.

مع جزيل الشكر

الباحث: ياسر ابو لبدة

المشرف: د. عمر البزور

القسم الأول: يرجى وضع إشارة (X) في المكان المناسب:

النوع الاجتماعي: ذكر ( ) أنثى ( )

المؤهل العلمي: ثانوية فأقل ( ) دبلوم– بكالوريوس ( ) دراسات عليا ( )

سنوات الخدمة: أقل من 5 سنوات ( ) من 5_ أقل من 10 سنوات ( )
من 10 – أقل من 15 سنة ( ) 15 سنة فأكثر ( ).

الرتبة العسكرية: أقل من ملازم ( ) من ملازم – رائد ( ) مقدّم فأعلى ( )

القسم الثاني: يرجى وضع إشارة (X) في المربع الذي يتفق ورأيك، وذلك أمام كل فقرة من الفقرات الآتية:

الرقم	الفقرة	موافق بشدة	موافق	لا رأي	أُعارض	أُعارض بشدة
المحور الأول: إسهام وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بمخاطر الجرائم الإلكترونية						
1	تقدم الوحدة برامج توعية دورية حول الجرائم الإلكترونية.					
2	تستخدم الوحدة وسائل الإعلام المختلفة لنشر الوعي بخطورة الجرائم الإلكترونية.					
3	تنظم الوحدة حملات توعوية في المدارس والجامعات.					
4	توفر الوحدة كتيبات إرشادية للجمهور حول كيفية حماية أنفسهم إلكترونياً.					
5	تستهدف الوحدة فئات المجتمع الأكثر عرضة للجرائم الإلكترونية بالتوعية.					
6	تعزز الوحدة من ثقافة الاستخدام الآمن للإنترنت عبر منصاتها.					
7	تقدم الوحدة ورش عمل تدريبية للتوعية بمخاطر الجرائم الإلكترونية.					
المحور الثاني: الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين						
8	تعتمد الوحدة على تقنيات حديثة في تتبع الجرائم الإلكترونية.					
9	تستخدم الوحدة برامج متقدمة لتحليل البيانات الرقمية.					
10	تتعاون الوحدة مع شركات التكنولوجيا لتطوير أدوات مكافحة الجرائم الإلكترونية.					
11	تعتمد الوحدة على أساليب تحقيق رقمية متطورة.					
12	تطبق الوحدة آليات حديثة لاسترجاع البيانات المسروقة.					
13	تستخدم الوحدة أنظمة مراقبة إلكترونية للكشف عن الجرائم قبل وقوعها.					
14	توفر الوحدة خطاً ساخناً للإبلاغ عن الجرائم الإلكترونية.					
المحور الثالث: آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية						
15	تشارك الوحدة في مؤتمرات دولية متعلقة بمكافحة الجرائم الإلكترونية.					
16	تتعاون الوحدة مع منظمات دولية لمكافحة الجرائم الإلكترونية.					
17	تنسق الوحدة مع وحدات جرائم إلكترونية في دول أخرى لتبادل المعلومات.					
18	تعتمد الوحدة على اتفاقيات دولية لتسليم المجرمين الإلكترونيين.					
19	تستفيد الوحدة من الخبرات الدولية في مكافحة الجرائم الإلكترونية.					
20	تعمل الوحدة على تطوير شراكات دولية لتعزيز جهودها.					
21	تتابع الوحدة التشريعات الدولية المتعلقة بالجرائم الإلكترونية.					

المحور الرابع: قيام وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية						
22	تتابع الوحدة القضايا الإلكترونية بالتنسيق مع الجهات القضائية.					
23	تقدم الوحدة أدلة رقمية موثوقة للمحاكم.					
24	تساعد الوحدة في صياغة تقارير فنية حول الجرائم الإلكترونية.					
25	تنسق الوحدة مع النيابة العامة لملاحقة المتهمين بالجرائم الإلكترونية.					
26	توفر الوحدة خبراء قانونيين متخصصين في الجرائم الإلكترونية.					
27	تدعم الوحدة الضحايا في تقديم شكاوى قانونية.					
28	تساهم الوحدة في تعزيز تطبيق القوانين المتعلقة بالجرائم الإلكترونية.					
المحور الخامس: المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية						
29	تعاني الوحدة من نقص في الكوادر البشرية المتخصصة.					
30	تواجه الوحدة صعوبات في الحصول على الأدوات التقنية اللازمة.					
31	تعاني الوحدة من نقص في التمويل المخصص لمكافحة الجرائم الإلكترونية.					
32	تواجه الوحدة تحديات قانونية في تتبع المجرمين الدوليين.					
33	تصطدم الوحدة بصعوبة تحديد هوية مرتكبي الجرائم الإلكترونية.					
34	تعاني الوحدة من ضعف التعاون بين الجهات الحكومية ذات الصلة.					
35	تواجه الوحدة صعوبات في مواكبة التطورات التكنولوجية الحديثة.					

ملحق (ج)

الاستبانة بصورتها النهائية

جامعه النجاح الوطنية

كلية الدراسات العليا

الأخوة والأخوات

تحية طيبة وبعد,

تعد هذه الإستبانة جزء من رسالة الماجستير التي يقوم بها الباحث بعنوان" **دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية** " وذلك استكمالا لمتطلبات الحصول على درجة الماجستير في برنامج القانون العام بكلية الدراسات العليا في جامعة النجاح الوطنية.

يرجى من حضرتكم الإجابة على أسئلة هذه الإستبانة لما لها من أهمية لإنجاز هذه الرسالة, علماً بأن البيانات التي ستقدمونها سوف تستخدم فقط لأغراض البحث العلمي.

مع جزيل الشكر

الباحث: ياسر ابو لبدة

المشرف: د. عمر البزور

القسم الأول: يرجى وضع إشارة (X) في المكان المناسب:

النوع الاجتماعي: ذكر ( ) أنثى ( )

المؤهل العلمي: ثانوية فأقل ( ) دبلوم– بكالوريوس ( ) دراسات عليا ( )

سنوات الخدمة: أقل من 5 سنوات ( ) من 5_ أقل من 10 سنوات ( )
من 10 – أقل من 15 سنة ( ) 15 سنة فأكثر ( ).

الرتبة العسكرية: أقل من ملازم ( ) من ملازم – رائد ( ) مقدّم فأعلى ( )

القسم الثاني: يرجى وضع إشارة (X) في المربع الذي يتفق ورأيك، وذلك أمام كل فقرة من الفقرات الآتية:

الرقم	الفقرة	موافق بشدة	موافق	لا رأي	أُعارض	أُعارض بشدة
المجال الأول: مساهمة وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بالجرائم الالكترونية						
1	تقدم الوحدة برامج توعية دورية حول الجرائم الإلكترونية.					
2	تستخدم الوحدة وسائل الإعلام المختلفة لنشر الوعي بخطورة الجرائم الإلكترونية.					
3	تنظم الوحدة حملات توعوية في المدارس والجامعات.					
4	توفر الوحدة كتيبات إرشادية للجمهور حول كيفية حماية أنفسهم إلكترونياً.					
5	تستهدف الوحدة فئات المجتمع الأكثر عرضة للجرائم الإلكترونية بالتوعية.					
6	تعزز الوحدة من ثقافة الاستخدام الآمن للإنترنت عبر منصاتها.					
7	تقدم الوحدة ورش عمل تدريبية للتوعية بمخاطر الجرائم الإلكترونية.					
المجال الثاني: الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية لمكافحة الجرائم الإلكترونية						
8	تعتمد الوحدة على تقنيات حديثة في تتبع الجرائم الإلكترونية.					
9	تستخدم الوحدة برامج متقدمة لتحليل البيانات الرقمية.					
10	تتعاون الوحدة مع شركات التكنولوجيا لتطوير أدوات مكافحة الجرائم الإلكترونية.					
11	تعتمد الوحدة على أساليب تحقيق رقمية متطورة.					
12	تطبق الوحدة آليات حديثة لاسترجاع البيانات المسروقة.					
13	تستخدم الوحدة أنظمة مراقبة إلكترونية للكشف عن الجرائم قبل وقوعها.					
14	توفر الوحدة خطاً ساخناً للإبلاغ عن الجرائم الإلكترونية.					
المجال الثالث: آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية						
15	تشارك الوحدة في مؤتمرات دولية متعلقة بمكافحة الجرائم الإلكترونية.					
16	تتعاون الوحدة مع منظمات دولية لمكافحة الجرائم الإلكترونية.					
17	تنسق الوحدة مع وحدات جرائم إلكترونية في دول أخرى لتبادل المعلومات.					
18	تعتمد الوحدة على اتفاقيات دولية لتسليم المجرمين الإلكترونيين.					
19	تستفيد الوحدة من الخبرات الدولية في مكافحة الجرائم الإلكترونية.					
20	تعمل الوحدة على تطوير شراكات دولية لتعزيز جهودها.					
21	تتابع الوحدة التشريعات الدولية المتعلقة بالجرائم الإلكترونية.					
المجال الرابع: قيام وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية						

22	تتابع الوحدة القضايا الإلكترونية بالتنسيق مع الجهات القضائية.					
23	تقدم الوحدة أدلة رقمية موثوقة للمحاكم.					
24	تساعد الوحدة في صياغة تقارير فنية حول الجرائم الإلكترونية.					
25	تنسق الوحدة مع النيابة العامة لملاحقة المتهمين بالجرائم الإلكترونية.					
26	توفر الوحدة خبراء قانونيين متخصصين في الجرائم الإلكترونية.					
27	تدعم الوحدة الضحايا في تقديم شكاوى قانونية.					
28	تساهم الوحدة في تعزيز تطبيق القوانين المتعلقة بالجرائم الإلكترونية.					
المجال الخامس: المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية						
المحور الاول: التحديات القانونية والتشريعية						
29	تعاني الوحدة من نقص التشريعات الحديثة التي تواكب تطور الجرائم الإلكترونية.					
30	تواجه الوحدة صعوبة في إثبات الجرائم الإلكترونية بسبب تعقيد الأدلة الرقمية وإمكانية إخفائها أو التلاعب بها.					
31	تعيق العقبات القانونية الدولية عملية التعاون مع الجهات المختصة خارج فلسطين.					
32	تعاني الوحدة من غياب لوائح وإجراءات قانونية واضحة لتنظيم عملها في التعامل مع الجرائم الإلكترونية.					
المحور الثاني: التحديات التكنولوجية والفنية						
33	تعاني الوحدة من نقص الكوادر المتخصصة في مجال الأمن السيبراني وتحليل الأدلة الرقمية.					
34	تتطور أساليب الجرائم الإلكترونية بشكل متسارع يفوق الإمكانيات التقنية للوحدة.					
35	تعاني الوحدة من ضعف في البنية التحتية التكنولوجية اللازمة لمتابعة ورصد الجرائم الإلكترونية بكفاءة.					
36	تواجه الوحدة تحديات في الحصول على البرامج والأدوات الحديثة اللازمة لتحليل وتتبع الجرائم الإلكترونية.					
المحور الثالث: التحديات المالية واللوجستية						
37	تعاني الوحدة من محدودية الميزانية المخصصة لها، مما يؤثر على قدرتها في تطوير الأدوات والتقنيات المستخدمة.					
38	تفتقر الوحدة إلى دعم لوجستي كافٍ، مثل مراكز بيانات متطورة وأنظمة اتصال مشفرة.					
39	تؤثر قلة الموارد المالية على إمكانية تدريب الكوادر وتأهيلهم لمواجهة تطورات الجرائم الإلكترونية.					
40	تعاني الوحدة من نقص في المعدات والأجهزة الحديثة التي تساهم في رفع كفاءة التحقيقات الرقمية.					

المحور الرابع: التحديات الاجتماعية والثقافية						
41	يعاني المجتمع من ضعف الوعي بخطورة الجرائم الإلكترونية، فينعكس على مستوى التعاون بين الطرفين.					
42	تفتقر بعض الفئات في المجتمع إلى الثقافة الرقمية، مما يزيد من احتمالية تعرضهم للجرائم الإلكترونية.					
43	يواجه العاملون في الوحدة تحديات اجتماعية مرتبطة بعدم تقدير المجتمع لأهمية مكافحة الجرائم الإلكترونية.					
44	تؤدي المفاهيم الخاطئة حول الخصوصية والأمان الرقمي إلى صعوبة توعية الأفراد بمخاطر الجرائم الإلكترونية.					
المحور الخامس: التحديات الأمنية والسياسية						
45	تؤثر القيود السياسية المتمثلة بالاحتلال على قدرة الوحدة في الوصول إلى التقنيات الحديثة أو التعاون مع جهات دولية متخصصة.					
46	تواجه الوحدة تحديات أمنية مرتبطة بصعوبة الوصول لمرتكبي الجرائم الالكترونية.					
47	تؤثر الأوضاع الأمنية والسياسية على استقرار عمل الوحدة وتحد من قدرتها على تنفيذ مهامها بكفاءة.					
48	تعاني الوحدة من غياب الحماية القانونية الكافية للعاملين فيها أثناء تنفيذ مهامهم المتعلقة بالتحقيقات الإلكترونية.					
المحور السادس: تحديات التعاون والتنسيق						
49	تعاني الوحدة من ضعف في التنسيق مع الجهات الأمنية الأخرى، مما يؤثر على سرعة الاستجابة للجرائم الإلكترونية.					
50	يواجه العاملون في الوحدة صعوبات في بناء شراكات فعالة مع القطاع الخاص، مثل شركات التكنولوجيا ومزودي الإنترنت.					
51	تعاني الوحدة من غياب قاعدة بيانات موحدة تتيح تبادل المعلومات بسهولة بين الجهات المختصة.					
52	تؤثر البيروقراطية الإدارية على سرعة اتخاذ القرارات المتعلقة بمكافحة الجرائم الإلكترونية.					

ملحق (د)

الجداول

جدول (2.5)

صدق الاتساق الداخلي للفقرات

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية
المجال الأول: إسهام وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في التوعية بمخاطر الجرائم الإلكترونية			
1	تقدم الوحدة برامج توعية دورية حول الجرائم الإلكترونية.	0.828**	0.000
2	تستخدم الوحدة وسائل الإعلام المختلفة لنشر الوعي بخطورة الجرائم الإلكترونية.	0.909**	0.000
3	تنظم الوحدة حملات توعوية في المدارس والجامعات.	0.846**	0.000
4	توفر الوحدة كتيبات إرشادية للجمهور حول كيفية حماية أنفسهم إلكترونياً.	0.857**	0.000
5	تستهدف الوحدة فئات المجتمع الأكثر عرضة للجرائم الإلكترونية بالتوعية.	0.901**	0.000
6	تعزز الوحدة من ثقافة الاستخدام الآمن للإنترنت عبر منصاتها.	0.847**	0.000
7	تقدم الوحدة ورش عمل تدريبية للتوعية بمخاطر الجرائم الإلكترونية.	0.842**	0.000
المجال الثاني: الأساليب التي تعتمدها وحدة الجرائم الإلكترونية في مكافحة الجرائم الإلكترونية داخل فلسطين			
1	تعتمد الوحدة على تقنيات حديثة في تتبع الجرائم الإلكترونية.	0.832**	0.000
2	تستخدم الوحدة برامج متقدمة لتحليل البيانات الرقمية.	0.812**	0.000
3	تتعاون الوحدة مع شركات التكنولوجيا لتطوير أدوات مكافحة الجرائم الإلكترونية.	0.735**	0.000
4	تعتمد الوحدة على أساليب تحقيق رقمية متطورة.	0.849**	0.000
5	تطبق الوحدة آليات حديثة لاسترجاع البيانات المسروقة.	0.841**	0.000
6	تستخدم الوحدة أنظمة مراقبة إلكترونية للكشف عن الجرائم قبل وقوعها.	0.744**	0.000
7	توفر الوحدة خطاً ساخناً للإبلاغ عن الجرائم الإلكترونية.	0.726**	0.000
المجال الثالث: آليات وأوجه التعاون الدولي في مكافحة الجرائم الالكترونية			
1	تشارك الوحدة في مؤتمرات دولية متعلقة بمكافحة الجرائم الإلكترونية.	0.817**	0.000
2	تتعاون الوحدة مع منظمات دولية لمكافحة الجرائم الإلكترونية.	0.837**	0.000
3	تنسق الوحدة مع وحدات جرائم إلكترونية في دول أخرى لتبادل المعلومات.	0.758**	0.000
4	تعتمد الوحدة على اتفاقيات دولية لتسليم المجرمين الإلكترونيين.	0.792**	0.000
5	تستفيد الوحدة من الخبرات الدولية في مكافحة الجرائم الإلكترونية.	0.783**	0.000
6	تعمل الوحدة على تطوير شراكات دولية لتعزيز جهودها.	0.783**	0.000
7	تتابع الوحدة التشريعات الدولية المتعلقة بالجرائم الإلكترونية.	0.733**	0.000
المجال الرابع: قيام وحدة الجرائم الإلكترونية بتطبيق الملاحقة القانونية لمرتكبي الجرائم الإلكترونية، استناداً إلى التشريعات المحلية والدولية			
1	تتابع الوحدة القضايا الإلكترونية بالتنسيق مع الجهات القضائية.	0.837**	0.000
2	تقدم الوحدة أدلة رقمية موثوقة للمحاكم.	0.801**	0.000

3	تساعد الوحدة في صياغة تقارير فنية حول الجرائم الإلكترونية.	**0.789	0.000
4	تنسق الوحدة مع النيابة العامة لملاحقة المتهمين بالجرائم الإلكترونية.	**0.738	0.000
5	توفر الوحدة خبراء قانونيين متخصصين في الجرائم الإلكترونية.	**0.784	0.000
6	تدعم الوحدة الضحايا في تقديم شكاوى قانونية.	**0.755	0.000
7	تساهم الوحدة في تعزيز تطبيق القوانين المتعلقة بالجرائم الإلكترونية.	**0.785	0.000
المجال الخامس: المعيقات والتحديات التي تواجه وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية			
المحور الاول: التحديات القانونية والتشريعية			
1	تعاني الوحدة من نقص التشريعات الحديثة التي تواكب تطور الجرائم الإلكترونية.	**0.762	0.000
2	تواجه الوحدة صعوبة في إثبات الجرائم الإلكترونية بسبب تعقيد الأدلة الرقمية وإمكانية إخفائها أو التلاعب بها.	**0.831	0.000
3	تعيق العقبات القانونية الدولية عملية التعاون مع الجهات المختصة خارج فلسطين.	**0.614	0.000
4	تعاني الوحدة من غياب لوائح وإجراءات قانونية واضحة لتنظيم عملها في التعامل مع الجرائم الإلكترونية.	**0.807	0.000
المحور الثاني: التحديات التكنولوجية والفنية			
1	تعاني الوحدة من نقص الكوادر المتخصصة في مجال الأمن السيبراني وتحليل الأدلة الرقمية.	**0.798	0.000
2	تتطور أساليب الجرائم الإلكترونية بشكل متسارع يفوق الإمكانيات التقنية للوحدة.	**0.825	0.000
3	تعاني الوحدة من ضعف في البنية التحتية التكنولوجية اللازمة لمتابعة ورصد الجرائم الإلكترونية بكفاءة.	**0.862	0.000
4	تواجه الوحدة تحديات في الحصول على البرامج والأدوات الحديثة اللازمة لتحليل وتتبع الجرائم الإلكترونية.	**0.718	0.000
المحور الثالث: التحديات المالية واللوجستية			
1	تعاني الوحدة من محدودية الميزانية المخصصة لها، مما يؤثر على قدرتها في تطوير الأدوات والتقنيات المستخدمة.	**0.899	0.000
2	تفتقر الوحدة إلى دعم لوجستي كافٍ، مثل مراكز بيانات متطورة وأنظمة اتصال مشفرة.	**0.816	0.000
3	تؤثر قلة الموارد المالية على إمكانية تدريب الكوادر وتأهيلهم لمواجهة تطورات الجرائم الإلكترونية.	**0.790	0.000
4	تعاني الوحدة من نقص في المعدات والأجهزة الحديثة التي تساهم في رفع كفاءة التحقيقات الرقمية.	**0.846	0.000
المحور الرابع: التحديات الاجتماعية والثقافية			
1	يعاني المجتمع من ضعف الوعي بخطورة الجرائم الإلكترونية، فينعكس على مستوى التعاون بين الطرفين.	**0.769	0.000

2	تفتقر بعض الفئات في المجتمع إلى الثقافة الرقمية، مما يزيد من احتمالية تعرضهم للجرائم الإلكترونية.	**0.790	0.000
3	يواجه العاملون في الوحدة تحديات اجتماعية مرتبطة بعدم تقدير المجتمع لأهمية مكافحة الجرائم الإلكترونية.	**0.790	0.000
4	تؤدي المفاهيم الخاطئة حول الخصوصية والأمان الرقمي إلى صعوبة توعية الأفراد بمخاطر الجرائم الإلكترونية.	**0.735	0.000
	المحور الخامس: التحديات الأمنية والسياسية		
1	تؤثر القيود السياسية المتمثلة بالاحتلال على قدرة الوحدة في الوصول إلى التقنيات الحديثة أو التعاون مع جهات دولية متخصصة.	**0.727	0.000
2	تواجه الوحدة تحديات أمنية مرتبطة بصعوبة الوصول لمرتكبي الجرائم الالكترونية.	**0.801	0.000
3	تؤثر الأوضاع الأمنية والسياسية على استقرار عمل الوحدة وتحد من قدرتها على تنفيذ مهامها بكفاءة.	**0.807	0.000
4	تعاني الوحدة من غياب الحماية القانونية الكافية للعاملين فيها أثناء تنفيذ مهامهم المتعلقة بالتحقيقات الإلكترونية.	**0.743	0.000
	المحور السادس: تحديات التعاون والتنسيق		
1	تعاني الوحدة من ضعف في التنسيق مع الجهات الأمنية الأخرى، مما يؤثر على سرعة الاستجابة للجرائم الإلكترونية.	**0.855	0.000
2	يواجه العاملون في الوحدة صعوبات في بناء شراكات فعالة مع القطاع الخاص، مثل شركات التكنولوجيا ومزودي الإنترنت.	**0.825	0.000
3	تعاني الوحدة من غياب قاعدة بيانات موحدة تتيح تبادل المعلومات بسهولة بين الجهات المختصة.	**0.829	0.000
4	تؤثر البيروقراطية الإدارية على سرعة اتخاذ القرارات المتعلقة بمكافحة الجرائم الإلكترونية.	**0.784	0.000

** دال احصائياً عند مستوى الدلالة (0.01) لمعامل بيرسون للارتباط .

جدول (3.6)

المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية للمجال الخامس

الرقم	المحور	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة
1	التحديات القانونية والتشريعية	3.813	0.666	76.3%	مرتفعة
2	التحديات التكنولوجية والفنية	3.880	0.771	77.6%	مرتفعة
3	التحديات المالية واللوجستية	4.047	0.657	80.9%	مرتفعة
4	التحديات الاجتماعية والثقافية	4.196	0.482	83.9%	مرتفعة
5	التحديات الأمنية والسياسية	4.150	0.557	83.0%	مرتفعة
6	تحديات التعاون والتنسيق	3.899	0.684	78.0%	مرتفعة
الدرجة الكلية للمجال الاول		**3.997**	**0.469**	**79.9%**	**مرتفعة**

جدول (3.7)

نتائج اختبار "T" بين متوسطات آراء المبحوثين حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية وفقاً لمتغير (النوع الاجتماعي)

النوع الاجتماعي	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة " T"	القيمة الاحتمالية
ذكر	126	4.01	0.365	1.868	0.72
أنثى	22	3.85	0.361		

جدول (3.8)

نتائج تحليل التباين الأحادي حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية وفقاً لمتغير (المؤهل العلمي)

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة " F "	القيمة الاحتمالية
بين المجموعات	.086	2	.043	.315	.730
داخل المجموعات	19.846	145	.137		
المجموع	19.932	147			

جدول (3.9)

نتائج تحليل التباين الأحادي حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية وفقاً لمتغير (سنوات الخدمة)

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة " F "	القيمة الاحتمالية
بين المجموعات	.542	3	.181		
داخل المجموعات	19.389	144	.135	1.343	.263
المجموع	19.932	147			

جدول (3.10)

نتائج تحليل التباين الأحادي حول دور وحدة الجرائم الإلكترونية في المؤسسة الأمنية الفلسطينية في مكافحة الجرائم الإلكترونية وفقاً لمتغير (الرتبة العسكرية)

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة " F "	القيمة الاحتمالية
بين المجموعات	.523	2	.261		
داخل المجموعات	19.409	145	.134	1.953	.145
المجموع	19.932	147			

An-Najah National University
Faculty of Graduate Studies

THE ROLE OF THE CYBERCRIME UNIT IN THE PALESTINIAN SECURITY INSTITUTION IN COMBATING CYBERCRIMES

By

Yasser Abu Labda

Supervisor

Dr. Omar Al-Bazur

This Thesis was Submitted in Parital Fullfilemt of the Requirements for the Degree of Master of Private Law, Faculty of Graduate Studies, An-Najah National University, Nablus - Palestine

2025

THE ROLE OF THE CYBERCRIME UNIT IN THE PALESTINIAN SECURITY INSTITUTION IN COMBATING CYBERCRIMES

By

Yasser Abu Labda

Supervisor

Dr. Omar Al-Bazur

Abstract

This study aimed to identify the role of the Cybercrime Unit within the Palestinian Security Institution in combating cybercrimes. The study population comprised all members of the Cybercrime Unit (in all their job titles) in Ramallah Governorate, totaling 250 individuals. A simple random sampling technique was employed, and questionnaires were distributed to 148 members of the sample; all 148 were returned and deemed valid for statistical analysis. Data were collected via a questionnaire, and the research followed a descriptive-analytical approach.

The study found that: The Cybercrime Unit's role in raising awareness of cybercrimes is moderate, and the methods used by the Cybercrime Unit to combat cybercrimes are moderate. The mechanisms and forms of international cooperation in combating cybercrimes are moderate, amd the Cybercrime Unit's role in enforcing legal prosecution and tracking cybercrime offenders under national and international legislation is moderate. The obstacles and challenges facing the Cybercrime Unit in the Palestinian Security Institution in combating cybercrimes are considerable.

Among the key recommendations: the Cybercrime Unit should organize interactive workshops targeted at specific community sectors such as schools and universities; collaborate with local media to broaden the scope of awareness campaigns; and develop and distribute interactive visual content on how individuals can protect themselves online via platforms like Facebook, Instagram, and YouTube.

Keywords: Cybercrime Unit; Palestinian Security Institution; Cybercrimes.